DİJİTAL KÜTÜPHANE KANALI

Keyifli Okumalar Dileriz

Binlerce kategoride milyonlarca PDF e-kitap, ders kitapları, dergiler ve romanlara platformumuz üzerinden ücretsiz ulaşabilirsiniz.

RESMİ WEB SİTEMİZ

https://rantey.org

Yedek ve Duyuru Kanallarımız
Sitemize erişim engeli gelmesi veya adres değişikliği durumunda aşağıdaki kanallardan güncel giriş adresine erişebilirsiniz:

• Telegram: https://t.me/birkitapbir

• WhatsApp Kanalımız : https://whatsapp.com/channel/0029VbDHv8uE50Us4IvMoc0Y

DÜNYANIN EN ÇOK ARANAN
BİLGİSAYAR KORSANINDAN

ALDATMA SANATI

KEVIN D. MITNICK

WILLIAM L. SIMON

ODTÜ YAYINCILIK

ALDATMA SANATI

Bilgi Güvenliğinde İnsan Faktörünün Kontrolü

Kevin D. Mitnick
William L. Simon

THE ART OF DECEPTION
Copyright © 2002 by Kevin D. Mitnick. All Rights Reserved.
Originally Published by Wiley Publishing, Inc., Indianapolis, Indiana
Published simultaneously in Canada

All Rights Reserved. Authorized translation from the
English language edition published by John Wiley & Sons, Inc.

ALDATMA SANATI
Kevin D. Mitnick

ISBN 978-975-7064-91-6

ODTÜ Geliştirme Vakfı
Yayıncılık ve İletişim A.Ş. Yayınları
ODTÜ Yayıncılık

© Tüm yayın hakları ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim A.Ş.'nindir. Yayıncının izni olmaksızın, hiçbir biçimde ve hiçbir yolla, bu kitabın içeriğinin bir bölümü ya da tümü yeniden üretilemez ve dağıtılamaz.

Çeviren
Nejat Eralp TEZCAN

Kapak Tasarımı
Burcu ERDOĞAN

Sayfa Düzeni
Emrullah ÖZ

6. Basım Nisan 2015
Tarcan Matbaacılık Yay. San.
Zebeyde Hanım Mah. Samyeli Sok. No: 15 İskitler-ANKARA
Tlf.: (312) 384 34 35 Faks: (312) 384 34 37
Sertifika no: 25744

ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim A.Ş.
Üveçler 1042. Cad. No: 57/1 Çankaya-ANKARA
Tlf.: 0(312) 480 15 97 - 480 15 98
Faks: 0(312) 480 15 99
Sertifika no: 15723
E-posta: odtuyayincilik@odtuyayincilik.com.tr
İnternet: www.odtuyayincilik.com.tr

Reba Vartanian, Shelly Jaffe, Chickie Leventhal, Mitchell Mitnick, ve müteveffa Alan Mitnick, Adam Mitnick ve Jack Biello için.
Ayrıca Arynne, Victoria ve David, Sheldon, Vincent ve Elena için.

Toplum Mühendisliği

Toplum mühendisliğinde, insanları kandırmak için karşı tarafı yönlendiren ya da toplum mühendisini başka birinin yerine koyan etkileme ve ikna yöntemleri kulanılır. Sonuç olarak toplum mühendisi teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanır.

İçindekiler

Önsöz vii
Sunuş ix
Giriş xiii

I. Perde Arkası
1. Bölüm: Güvenliğin En Zayıf Halkası 3

II. Saldırı Sanatı
2. Bölüm: Zararsız Gibi Görünen Bilgiler 15
3. Bölüm: Doğrudan Saldırı: İsteyivermek 29
4. Bölüm: Güven Uyandırmak 37
5. Bölüm: "Size Yardımcı Olabilirim" 51
6. Bölüm: "Bana Yardımcı Olabilir misiniz?" 71
7. Bölüm: Düzmece Siteler ve Tehlikeli Ekler 85
8. Bölüm: Acındırma, Suçluluk Duygusu ve Sindirme Tekniğini Kullanmak 97
9. Bölüm: Ters Dalavere 121

III. Davetsiz Misafirlere Dikkat
10. Bölüm: İçeriye Girmek 137
11. Bölüm: Teknolojiyi ve Toplum Mühendisliğini Birlikte Kullanmak 159
12. Bölüm: İşe Yeni Girenlere Yapılan Saldırılar 181
13. Bölüm: Zekice Oynanmış Oyunlar 191
14. Bölüm: Sanayi Casusluğu 209

IV. Çıtayı Yükseltmek
15. Bölüm: Bilgi Güvenliğinin Önemini Bilmek ve Eğitim 227
16. Bölüm: Şirket Bilgi Güvenliği Kuralları Önerileri 241

Bir Bakışta Güvenlik 303
Kaynaklar 310
Teşekkür 311
Dizin 317

Önsöz

Biz insanlar, çevremizi keşfetmeye yönelik bir içgüdüyle doğarız. Gençliğimizde hem Kevin Mitnick, hem de ben dünyayı keşfetmeye çok hevesliydik ve kendimizi kanıtlamak için yanıp tutuşuyorduk. Yeni şeyler öğrenme, bulmacaları çözme ve oyunları kazanma denemelerimizde sık sık başarılı olduk. Ama aynı zamanda da çevremizdeki dünya, bizi özgürce keşfetmeye iten bu dürtüyü kısıtlayan davranış kuralları getiriyordu. En cesur bilim adamları ve teknolojik girişimciler için olduğu kadar Kevin Mitnick gibi insanlar için de bu dürtüyü dinlemek, başkalarının yapılabileceğine inanmadığı şeyleri başarmamızı sağlayan büyük bir heyecan yaratıyordu.

Kevin Mitnick, tanıdığım en katışıksız insanlardan biridir. Ona sorduğunuzda, eskiden yaptığı işin toplum mühendisliği olduğunu ve insanları kandırma üzerine kurulu olduğunu açıkça söyleyiverir. Ama Kevin artık bir toplum mühendisi değil. Öyle olduğu zamanlarda bile amacı hiçbir zaman kendini zengin etmek ya da başkalarına zarar vermek değildi; ama bu, toplum mühendisliğini kullanarak ciddi zararlar veren tehlikeli ve yıkıcı suçluların olmadığı anlamına gelmez. Aslında Kevin'in bu kitabı yazma nedeni de tam olarak budur: Sizleri onlara karşı uyarmak.

Aldatma Sanatı, toplum mühendisinin müdahalelerine karşı hepimizin -devletin, şirketlerin ve tek tek her birimizin- ne kadar savunmasız olduğunu gösteriyor. Güvenliğin bilincine varmadığımız böyle bir devirde, bilgisayar ağlarını ve verilerini korumak için büyük miktarlarda paralar harcıyoruz. Bu kitap, içeriden birilerini kandırıp bütün bu teknolojik korumanın çevresinden dolaşmanın ne kadar kolay olduğunu gözler önüne seriyor. İster bir şirkette, ister devlette çalışıyor olun, bu kitap, toplum mühendislerinin nasıl çalıştıklarını ve onların çabalarını boşa çıkarmak için neler yapabileceğinizi anlamak konusunda sağlam bir yol haritası sunmaktadır. Kevin ve kitabın diğer yazarı Bill Simon hem ibret verici hem de eğlenceli olan hayali olaylar sunarak, toplum mühendisliğinin bilinmeyen dünyasına ait teknikleri ortaya seriyorlar. Her olaydan sonra, anlatılan açıklara ve tehditlere karşı savunmanıza yardımcı olacak basit yöntemler de sunuyorlar.

Teknolojiye dayalı güvenlik, Kevin gibi insanların kapatmamıza yardımcı olabileceği büyük açıklar bırakıyor. Bu kitabı okuyun. Bize yol göstermeleri için içimizdeki Mitnick'lere danışmamız gerektiğini sonunda anlayacaksınız.

Steve Wozniak

SUNUŞ

Bazı bilgisayar korsanları, insanların dosyalarını ya da tüm sabit disk içeriklerini yok ederler; bunlara *kırıcılar* ya da *vandallar* denir. Bazı acemi bilgisayar korsanları ise teknolojiyi öğrenmekle uğraşmaz, bilgisayar sistemlerine girmek için korsan yazılımlar indirirler; bunlara *yazılımcı veletler* denir. Programlama becerileri olan daha deneyimli korsanlar, kırıcı yazılımlar geliştirip bunları internete ve bülten panosu sistemlerine koyarlar. Ve bir de teknolojiyle hiç ilgisi olmayan, ancak bilgisayarı para, mal ve hizmet çalmakta kullandıkları bir aletten öte görmeyen bireyler vardır.

Basının yarattığı Kevin Mitnick efsanesinin aksine ben, kötü niyetli bir bilgisayar korsanı değilim.

Ama şimdi bunları konuşmanın sırası değil.

Yola Çıkış

Kaderim büyük olasılıkla yaşantımın ilk zamanlarında çizilmişti. Tasasız, gamsız bir çocuktum ama bir yandan da canım sıkılıyordu. Ben üç yaşındayken annemle babam ayrıldığında, annem bizi geçindirebilmek için garson olarak çalışmaya başladı. Beni o zamanlar görseydiniz -zaman zaman tutarsız çalışma saatleriyle dolu, uzun, sinir bozucu günler geçiren bir annenin tek çocuğu olarak- neredeyse bütün uyanık geçen saatleri boyunca kendi başına kalan bir çocuk tanırdınız. Ben kendi kendimin bakıcısıydım.

San Fernando Vadisi içinde büyümek bana Los Angeles'ın tümünü keşfetme olanağı tanımıştı ve on iki yaşıma geldiğimde Los Angeles'ın büyük bir bölümünde bedava yolculuk etmenin bir yolunu bulmuştum. Bir gün otobüste giderken, aktarmalı biletlerin kontrolünün garip şekilli bir zımba ile yapıldığını fark ettim. Şoförler bu zımbayı, günü, saati ve güzergâhı biletin üstüne işlemek için kullanıyordu. Arkadaş canlısı bir şoför, kendisine kibarca yönelttiğim bir soruyu yanıtlayarak bu özel zımbanın nereden alındığını bana söyledi.

Aktarmalı biletler, otobüs değiştirerek gitmek istediğiniz yere ulaşmanızı sağlamak içindir; ancak ben onları istediğim yerlere bedava gidebilmek için kullanıyordum. Boş abonmanları elde etmek çocuk oyuncağıydı. Otobüs garajlarındaki çöp tenekeleri, şoförlerin vardiyalarının sonunda attıkları yarı kullanılmış abonman koçanlarıyla doluydu. Bir tomar boş bilet ve bir zımbayla kendi aktarmalarımı işaretleyip Los Angeles'ta her yere gidebiliyordum. Çok geçmeden tüm güzergâhların otobüs saatlerini ezberlemiştim. (Bu, bazı bilgileri şaşırtıcı bir şekilde akılda tutabildiğimin ilk örneklerindendi; bugün bile çocukluğumda ezberlediğim telefon numaralarını, şifreleri ve diğer önemli olabilecek ayrıntıları hatırlayabiliyorum.)

Erken yaşlarda ortaya çıkan başka bir kişisel ilgi de sihirbazlık yapmaya olan hayranlığımdı. Bir numaranın nasıl yapıldığını bir kez öğrendikten sonra, iyice ustalaşana kadar durmaksızın üzerinde çalışıyordum. Gizli bilgileri elde etmenin eğlencesine, kısmen sihirbazlık sayesinde vardım.

Telefon Beleşçiliğinden Bilgisayar Korsanlığına

Zaman içerisinde toplum mühendisliği adını vereceğim olguyla ilk karşılaşmam lise yıllarımda, telefon beleşçiliği denen bir hobiye kendini vermiş başka bir çocukla tanışmamla oldu. Telefon beleşçiliği, telefon sistemlerini ve telefon şirketleri çalışanlarını sömürerek telefon ağını tanımanızı sağlayan bir çeşit korsanlıktı. Bana, telefon şirketinin herhangi bir müşterisiyle ilgili bilgileri elde etmek ve gizli bir test numarası kullanarak ücretsiz şehirlerarası görüşmeler yapmak gibi, telefonla yapılabilecek çok sıkı numaralar öğretti. (Doğrusu, o telefon görüşmeleri yalnızca bizim için ücretsizdi. O numaranın bir test numarası olmadığını çok sonradan öğrendim. Aramalar, aslında, zavallı bir şirketin MCI telefon şirketindeki aboneliğine faturalanıyormuş.)

Bu benim toplum mühendisliğine ilk girişim, deyim yerindeyse ilk adımlarımdı. Bir arkadaşım ve kısa süre sonra tanıştığım başka bir telefon beleşçisi, telefon şirketini uydurma nedenlerle ararlarken benim de dinlememe izin verdiler. Söylediklerinin inandırıcı olması için kullandıkları şeyleri duydum; farklı telefon şirketlerini, her şirketin kendine özgü teknik terimlerini ve süreçlerini öğrendim. Ama bu "eğitim" fazla uzun sürmedi, çünkü daha fazlasına gerek yoktu. Kısa süre sonra her şeyi kendi başıma yapıyor, yaparken de öğreniyordum. Hattâ ilk öğretmenlerimden bile daha iyi yapıyordum. Lisedeyken yapmayı en çok sevdiğim numara, telefon santralına kaçak olarak girip tanıdığım telefon beleşçilerinden birinin telefonunun hizmet sınıfını değiştirmekti. Evden bir arama yapmaya kalktığı zaman telefona jeton atması için bir mesaj duyuyordu, çünkü telefon şirketi santralı, bir ankesörlü telefondan arama yapıldığı sinyalini alıyordu.

Telefonlarla ilgili, yalnızca elektronik özelliklerini, santrallarını ve bilgisayar sistemlerini değil, aynı zamanda şirket yapısını, süreçlerini ve teknik terimlerini de yalayıp yutmuştum. Bir süre sonra telefon sistemini herhalde herhangi bir çalışanından daha iyi biliyordum. Toplum mühendisliği becerilerimi öyle bir noktaya getirmiştim ki, on yedi yaşımda çoğu telefon şirketi çalışanını, ister telefonda ister yüzyüze, neredeyse her konuda inandırmayı başarabiliyordum.

Çok reklamı yapılan korsanlık mesleğim aslında lisedeyken başlamıştı. Ayrıntılarını burada aktaramasam da, ilk korsanlık deneyimlerimin arkasındaki itici gücün korsan grubunda kabul görmek isteği olduğunu bilmeniz yeterli.

O zamanlar, daha etkili programlar yapmak ya da gereksiz basamakları atlayıp işi daha hızlı yapabilmek için zamanının çoğunu bilgisayarları ve yazılımları kurcalamakla geçiren kişilere *korsan* derdik. Bu kelimenin anlamı artık iyice kötüye çekilip, "kötü niyetli suçlu" anlamında kullanılıyor. Bu sayfalarda, bu kelimeyi her zaman kullandığım gibi, yani ilk zamanlardaki daha yumuşak anlamıyla kullanmaya devam edeceğim.

Liseden sonra, Los Angeles'taki Bilgisayar Eğitim Merkezi'nde bilgisayarlar üzerine dersler almaya başladım. Birkaç ay içerisinde okulun müdürü işletim sisteminde açık bulduğumu ve IBM mini-bilgisayarlarında tüm yönetici ayrıcalıklarına sahip olduğumu fark etti. Öğretim kadrosundaki uzmanlar bile bunu nasıl yaptığımı bulamadılar. Herhalde "*korsan kiralama*" uygulamasının ilk örneklerinden olabilecek bir şekilde bana reddedemeyeceğim bir teklifte bulunuldu: Ya okulun bilgisayar güvenliğini geliştirmeye yönelik bir mezuniyet projesi hazırlayacaktım ya da sisteme müdahale ettiğim için okuldan uzaklaştırılacaktım. Doğal olarak mezuniyet projesini yapmayı tercih ettim ve sonunda yüksek başarı derecesiyle mezun oldum.

Toplum Mühendisi Olmak

Bazı insanlar, her sabah yataklarından günlük, sıradan işlerinden bıkmış olarak kalkarlar. Ben, işimin tadını çıkarabilecek kadar şanslıydım. Özellikle de, özel dedektif olarak geçirdiğim süre zarfında aldığım keyfi, kazandığım paraları ve duyduğum heyecanı hayal bile edemezsiniz. Toplum mühendisliği (normalde insanların tanımadıkları biri için yapmayacakları şeyleri yaptırmalarını sağlamak) denen gösteri sanatıyla ilgili becerilerimi gittikçe geliştiriyordum ve bunun karşılığında da para kazanıyordum.

Benim için toplum mühendisliğinde ustalaşmak zor olmadı. Baba tarafımın ailesi nesillerdir pazarlama işinde çalışır, bu yüzden de etkileme ve ikna etme sanatı kalıtsal bir özellik olabilir. Bu yeteneği, insanları aldatmaya yönelik bir eğilimle birleştirirseniz, elinize tipik bir toplum mühendisi profili çıkar.

Bir üçkâğıtçının iş tanımında iki uzmanlık alanı olduğunu söyleyebilirsiniz. İnsanları kandırıp paralarını çalanlar *dolandırıcı* alt grubuna girerler. Genellikle bilgi edinmeyi hedefleyerek, şirketlere karşı aldatma, etkileme ve ikna etme yollarını kullananlar ise diğer alt gruba, *toplum mühendisliği* grubuna girerler. Yaptığım şeyin yanlış olduğunu kavramak için çok küçük olduğum, aktarmalı abonman numarasını kullandığım o ilk günlerde, bilmemem gereken şeyleri öğrenmek konusunda bir yeteneğim olduğunu fark etmeye başlamıştım. Aldatma teknikleri kullanarak, mesleki terimleri bilerek ve özenle yontulmuş bir insanları yönlendirme becerisi geliştirerek bu yeteneğimi kullanmayı öğrendim.

İşimle ilgili -eğer buna iş denebilirse- becerilerimi geliştirmek için kullandığım yollardan biri de aslında ilgimi çok çekmeyen bir ayrıntı seçip, yalnızca yeteneklerimi geliştirebilmek amacıyla, telefonun diğer ucundaki birinin bu bilgiyi bana vermesini sağlayıp sağlayamayacağımı görmekti. Sihirbazlık numaralarını çalıştığım gibi konuşmalarımı da önceden çalışıyordum. Bu provalar yoluyla, neredeyse istediğim her bilgiyi alabileceğimi bir süre sonra anladım.

Yıllar sonra Kongre'de, Senatör Lieberman ve Senatör Thompson'un karşısında verdiğim ifadede de açıkladığım üzere:

Dünyadaki bazı büyük şirketlerin bilgisayar sistemlerine yetkisiz giriş yaptım ve şimdiye kadar geliştirilmiş en esnek bilgisayar sistemlerini başarıyla kırdım. Çalışma tarzlarını ve açık noktalarını inceleyebilmek amacıyla, çeşitli işletim sistemlerinin ve telekomünikasyon araçlarının kaynak kodlarını elde edebilmek için hem teknik hem de teknik olmayan yöntemler kullandım.

Tüm bu faaliyetler aslında kendi merakımı tatmin etmek; ne yapabileceğimi görmek ve işletim sistemleri, cep telefonları ve ilgimi çeken herhangi birşeyle ilgili gizli bilgileri elde etmek içindi.

Son Düşünceler

Tutuklandıktan sonra, yaptıklarımın yasadışı olduğunu ve özel yaşama müdahale suçu işlediğimi itiraf ettim.

İşlediğim suçların kaynağı meraktı. Telefon ağlarının nasıl çalıştığını ve bilgisayar güvenliğinin içini dışını öğrenebildiğim kadar öğrenmek istiyordum. Sihirbazlık numaraları yapmayı seven bir çocuk olmaktan çıkıp, şirketlerin ve devletin korktuğu, dünyanın en ünlü bilgisayar korsanı durumuna geldim. Son otuz yıldaki yaşantıma dönüp baktığımda, merakımdan, teknolojiyi öğrenme isteğimden ve zekâmı zorlayacak konular bulma ihtiyacımdan kaynaklanan oldukça kötü kararlar verdiğimi gördüm.

Artık değiştim. Bilgi güvenliği ve toplum mühendisliğiyle ilgili edindiğim geniş bilgi ve becerilerimi, devletin, işletmelerin ve bireylerin, bilgi güvenliğine yönelik tehditleri engelleyebilmeleri, tespit edebilmeleri ve kendilerini koruyabilmeleri konusunda onlara yardım etmek üzere kullanıyorum.

Bu kitap, dünyadaki kötü huylu bilgi hırsızlarının çabalarına karşı, başkalarına yardım etmek için deneyimlerimi kullanabileceğim yöntemlerden biri. Sanırım anlatılanları eğlenceli, ibret verici ve eğitici bulacaksınız.

GİRİŞ

Bu kitap, bilgi güvenliği ve toplum mühendisliğiyle ilgili yoğun bilgiler içermektedir. Yolunuzu bulmanızı kolaylaştırmak için, işte size kitabın içeriğine hızlı bir bakış:

Perde Arkası başlığında güvenliğin en zayıf halkasını açıklayacak, sizin ve şirketinizin neden toplum mühendisliği saldırılarına maruz kalabileceğinizi göstereceğim.

Saldırı Sanatı başlığında, toplum mühendislerinin istediklerini elde etmek için güveninizle, yardımcı olma isteğinizle, sevecenliğinizle ve insanî saflıklarınızla nasıl oynadıklarını göreceksiniz. Sık görülen saldırılarla ilgili hayalî öyküler toplum mühendislerinin pek çok kimliğe ve yüze bürünebildiklerini size gösterecek. Eğer daha önce bir toplum mühendisiyle karşılaşmadığınızı düşünüyorsanız, büyük olasılıkla yanılıyorsunuzdur. Bakalım, bu öykülerde daha önce sizin de yaşadığınız bir senaryo görecek ve toplum mühendisliğinin size dokunup dokunmadığını merak edecek misiniz? Bu olmayacak bir şey değil. Ancak ikinci bölümden dokuzuncu bölüme kadar okuduktan sonra, sizi arayan ilk toplum mühendisinin nasıl hakkından geleceğinizi öğrenmiş olacaksınız.

Davetsiz Misafirlere Dikkat adlı başlıkta ise, toplum mühendislerinin, şirket alanınıza girerek, şirketinizi batıracak ya da çıkaracak sırları çalıp, sizin yüksek teknoloji güvenlik önlemlerinizi atlatarak riski nasıl artırdığını, uydurma öykülerle göreceksiniz. Bu başlık altında anlatılan senaryolar, bir çalışanın intikam almasından tutun da, sanal terörizme kadar oluşabilecek çeşitli tehditlerin farkına varmanızı sağlayacaktır. Eğer işletmenizi ayakta tutan bilgilere ve verilerinizin güvenliğine değer veriyorsanız, onuncu ve on dördüncü bölümleri baştan sona okumak isteyeceksiniz.

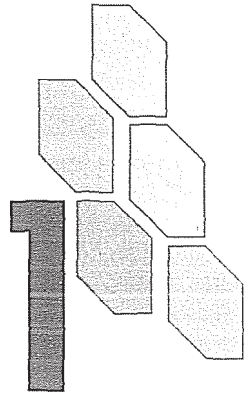
Aksi belirtilmediği takdirde, bu kitapta kullanılan tüm öykülerin uydurma öyküler olduklarını vurgulamakta yarar var.

Çıtayı Yükseltmek başlığında şirket yaklaşımını ele alıp kurumunuza yapılan toplum mühendisliği saldırılarının başarıya ulaşmalarının nasıl engellenebileceğinden söz edeceğiz. On beşinci bölüm başarılı bir güvenlik eğitimi programı için bir taslak sunmaktadır. Ve on altıncı bölüm tam hayatınızı kurtaracak şey olabilir; kurumunuza uyarlayabileceğiniz, şirketinizi ve bilgilerinizi emniyette tutmak için hemen uygulamaya geçirebileceğiniz, her yönüyle tam bir güvenlik kuralları metni.

En sona, işbaşında karşılaştıkları bir toplum mühendisliği saldırısını önleyebilmeleri için çalışanlarınıza yol göstermekte kullanabileceğiniz kilit bilgileri özetleyen kontrol listeleri, tablolar ve şemalar içeren **Bir Bakışta Güvenlik** adında bir bölüm ekledim. Bu araçlar aynı za-

manda, kendi güvenlik eğitimi programlarınızı oluşturmakta kullanabileceğiniz değerli bilgiler de içermektedir.

Kitapta pek çok faydalı unsurla karşılaşacaksınız: Terim kutuları, toplum mühendisliği ve bilgisayar korsanlığı terimlerinin açıklamalarını içerirler; Mitnick Mesajları güvenlik stratejinizi güçlendirmenize yardımcı olacak kısa bilgiler sunmaktadır; notlarda ise ek bilgiler ve ilginç ayrıntılar bulunmaktadır.



Perde Arkası

GÜVENLİĞİN EN ZAYIF HALKASI

Bir şirket, paranın alabileceği en iyi güvenlik teknolojilerini satın almış, çalışanlarını akşam eve giderken her şeylerini kilit altına alacak şekilde son derece iyi eğitmiş ve bina güvenlik görevlilerini sektörün en iyi güvenlik şirketinden kiralamış olabilir.

Bu şirket yine de tamamen savunmasızdır.

Bireyler, uzmanların önerdiği en iyi güvenlik uygulamalarını çalıştırıyor, önerilen her güvenlik ürününü bilgisayarına yüklüyor olabilirler ve uygun sistem yapılandırmasını ve güvenlik yamalarını kullanmak konularında son derece dikkatli davranabilirler.

Bu bireyler yine de tamamen savunmasızdırlar.

İnsan Unsuru

Yakın bir geçmişte Kongre'ye ifade verirken, başka birisi gibi davranarak ve yalnızca bu bilgiyi isteyerek, şifreleri ve diğer hassas bilgileri çoğu zaman şirketlerden alabildiğimi anlattım.

Tam anlamıyla güvende olduğunu bilmeyi istemek doğal bir duygudur ama bu, pek çok insanın sahte bir güvenlik hissiyle yetinmesine de neden olur. Karısını, çocuklarını ve evini korumak için ön kapısına, maymuncukla açılamaz olarak bilinen Medico marka bir silindirli kilit taktırmış, sorumluluk sahibi ve sevecen bir ev sahibini düşünün. Davetsiz misafirlere karşı ailesini güvenceye aldığı için içi rahat. Ama pencereyi kıran ya da garaj kapısının şifresini bozan hırsızlara ne olacak? Güçlü bir alarm sistemi yerleştirmek daha iyi olurdu ancak yine de bir garantisi yok. Pahalı kilitler olsun ya da olmasın, ev sahibinin saldırıya açık olma hali devam ediyor.

Neden? Çünkü insan unsuru aslında güvenliğin en zayıf halkasıdır.

Güvenlik çoğu zaman bir yanılgıdan ibarettir. İşin içine dikkatsizlik, saflık ve cahillik de girince daha kötü olur. Yirminci yüzyılın en saygın bilimadamı olan Albert Einstein şöyle demiştir: "Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim." Sonuç olarak, insanlar aptallarsa ya da daha sık görülen şekliyle, doğru güvenlik uygulamaları konusunda bilgisizlerse, toplum mühendisliği saldırıları başarılı olmaktadır. Pek çok bilişim teknolojileri (IT) sektörü çalışanı, güvenlik bilincine sahip aile reisimizle

aynı yaklaşımı kullanarak, güvenlik duvarları, müdahaleleri ortaya çıkarma sistemleri ya da daha güçlü tanıma sistemleri olan zaman tabanlı kartlar ve biyometrik akıllı kartlar gibi herkesçe kabul görmüş güvenlik ürünleri kullandıkları için şirketlerini saldırılara karşı büyük ölçüde güvende tuttukları doğrultusunda yanlış bir kanıya sahiptirler. Güvenlik ürünlerinin tek başlarına tam bir güvenlik sağlayacağına inanan biri, güvenlik konusunda kendini kandırıyor demektir. Bu ancak hayal aleminde görülebilecek bir durumdur. Bu insanlar er ya da geç, kaçınılmaz olarak bir güvenlik sorunu yaşayacaklardır.

Tanınmış bir güvenlik danışmanı olan Bruce Schneier'ın da dediği gibi, "Güvenlik bir ürün değil, bir süreçtir." Dahası, güvenlik bir teknoloji sorunu değildir; bir insan ve yönetim sorunudur.

Araştırmacılar sürekli olarak daha iyi güvenlik teknolojileri geliştirip teknik açıkları sömürmeyi giderek zorlaştırınca, saldırganlar insan unsurunu sömürme yoluna daha çok gideceklerdir. İnsanların güvenlik duvarını kırmak genellikle daha kolaydır ve bir telefon görüşmesinden başka yatırım istemediği gibi riski de çok düşüktür.

Klasik Bir Aldatma Olayı

İşletmenizin mal varlığının güvenliğine karşı en büyük tehdit nedir? Yanıtlaması kolay: Toplum mühendisi; siz sağ eline bakarken sol eliyle sırlarınızı çalan acımasız bir sihirbaz. Bu kişi çoğu zaman o kadar arkadaş canlısı, samimi ve yardımseverdir ki onunla karşılaştığınıza şükredebilirsiniz bile.

Bir toplum mühendisliği örneğine bakalım: Bugün pek çok insan Stanley Mark Rifkin adındaki genç adamı ve artık var olmayan Los Angeles'taki Pasifik Hisseleri Ulusal Bankası'yla olan macerasını hatırlamaz. Gerçekte ne olduğuyla ilgili çeşitli rivayetler vardır ve Rifkin de, benim gibi, hikâyesini kendi ağzından hiçbir zaman anlatmamıştır. Bu yüzden aşağıdakiler yayımlanmış makalelerden derlenmiştir.

Şifre Kırmak

1978 yılında bir gün Rifkin, Pasifik Hisseleri'nin yalnızca yetkili personelinin girebildiği ve odadakilerin her gün milyarlarca dolar tutarında havale gönderip aldıkları havale odasına doğru yollandı.

Ana bilgisayarın çökmesi olasılığına karşı, havale odasının verileri için yedekleme sistemi geliştirecek bir şirkette sözleşmeli olarak çalışıyordu. Bu görevi, banka yetkililerinin havaleleri nasıl gönderdikleri de dahil olmak üzere, tüm havale süreçlerini öğrenmesini sağlamıştı. Her sabah havale yapmaya yetkili banka çalışanlarına, havale odasını aradıklarında kullanmaları için, özenle korunan günlük bir şifrenin verildiğini öğrenmişti.

Havale odasındaki memurlar her gün değişen şifreyi ezberlemek için kendilerini yormuyorlardı: Şifreyi küçük bir kâğıda yazıp kolayca görebilecekleri bir yere asıyorlardı. Kasım ayının tam o gününde Rifkin'in odayı ziyaret etmesinin özel bir nedeni vardı. O kâğıda bakmak istiyordu.

Havale odasına gelerek, çalışma süreçleriyle ilgili notlar aldı; güya yedekleme sisteminin olağan sistemlerle tam olarak örtüştüğünden emin olmak istiyordu. Bu sırada asılı kâğıttaki güvenlik şifresini gizlice okudu ve ezberledi. Birkaç dakika sonra dışarı çıktı. Daha sonra söylediğine göre, o an kendini piyangoda büyük ikramiyeyi kazanmış gibi hissetmişti.

Bir De İsviçre'deki Şu Banka Hesabına...

Öğleden sonra saat üç sularında odadan çıkmış, doğruca binanın mermer kaplamalı girişindeki telefon kulübelerine gitmiş, telefona jeton atarak havale odasının numarasını çevirmişti. Sonra, telefonda başka bir kılığa bürünmüş, kendini, banka danışmanı Stanley Rifkin'den, bankanın Uluslararası İşlemler Birimi'nin bir çalışanı olan Mike Hansen'a dönüştürmüştü.

Bir kaynağa göre, yapılan görüşme aşağıdaki gibi gelişmişti:

"Merhaba, ben Uluslararası İşlemler'den Mike Hansen," dedi Rifkin, telefonun diğer ucundaki genç kadına.

Kadın ofis numarasını istedi. Bu olağan bir soruydu ve Rifkin hazırlıklıydı: "286," dedi.

Kadın sonra "Peki, şifre nedir?" diye sordu.

Rifkin'in adrenalinin etkisiyle zaten hızlı atan kalbi o anda iyice hızlandı. Duraksamadan yanıtladı, "4789." Sonra havale talimatlarını vermeye başladı: New York Irving Yatırım Ortaklığı'ndan Zürih Wozchod Handels Bankası'ndaki hesaba yatırılmak üzere "tam olarak on milyon iki yüz bin dolar." Bu hesabı önceden kendisi açtırmıştı.

Kadın söylenenleri not edip, "Tamam, bilgileri aldım. Şimdi de birimler arası takas numarasına ihtiyacım var." dedi

Rifkin'in başından aşağı kaynar sular döküldü; bu beklemediği bir soru, araştırmasında unuttuğu bir ayrıntıydı. Ama soğukkanlılığını koruyup her şey yolundaymış gibi davrandı ve hiç beklemeden cevap verdi, "Bir kontrol edeyim; sizi hemen ararım." Bu kez bankanın başka bir birimini aramak için tekrar telefonda kılık değiştirerek havale odasındaki bir çalışan gibi davrandı. Takas numarasını öğrendi ve genç kadını yeniden aradı.

Genç kadın numarayı aldı ve, "Teşekkürler" dedi. (Bu koşullar altında, teşekkür etmesi gerekenin aslında Rifkin olması gerektiği söylenebilir.)

Amaca Ulaşılması

Birkaç gün sonra Rifkin İsviçre'ye uçtu, parasını aldı ve 8 milyon dolarını bir yığın elmas karşılığında bir Rus acentasına verdi. Tekrar uçağa bindi ve taşları bir para kuşağına saklayarak A.B.D. gümrüğünden geçti. Tarihteki en büyük banka soygununu yapmıştı ve bunu bir silah, hattâ bir bilgisayar bile kullanmadan gerçekleştirmişti. Tuhaf olan, işlediği suçun bir süre sonra "en büyük bilgisayar dolandırıcılıkları" başlığı altında Guinness Rekorlar Kitabı'nın sayfalarında yer almasıydı.

Stanley Rifkin'in insanları aldatma sanatında kullandığı bu beceri ve teknikler bütününe artık *toplum mühendisliği* diyoruz. Aslında bu iş için gerekenler özenli bir planlama ve iyi laf yapma yeteneğinden ibaret.

Ve bu kitabın konusu işte bu -bendenizin ustası olduğu- toplum mühendisliği teknikleri ve şirketiniz üzerinde kullanılmaları durumunda nasıl karşı savunma yapacağınız.

Tehlikenin Boyutu

Rifkin'in öyküsü, güvende olduğumuz hissinin ne kadar yanlış bir düşünce olduğunu mükemmel bir şekilde açıklıyor. Bu tarz olaylar -belki 10 milyon dolarlık vurgunlar değil ama- her gün oluyor. Şu anda paralarınız gidiyor olabilir ya da birileri yeni ürünlerinizin tasarımlarını çalıyor olabilir ve siz bunun farkında bile değilsiniz. Eğer şirketinizin başına henüz böyle bir olay gelmediyse, sormanız gereken şey bunun olup olmayacağı değil, ne zaman olacağı.

Artan Endişe

Bilgisayar Güvenliği Enstitüsü'nün, 2001 yılında bilgisayar suçlarıyla ilgili yaptığı araştırmaya göre, geçen on iki ay içerisinde araştırmaya katılan kuruluşların yüzde 85'inin bilgisayarlarına yetkisiz giriş yapılmış. Bu şaşırtıcı bir rakam. Araştırmaya katılan her yüz kuruluştan yalnızca on beşi yıl boyunca güvenlik ihlâli yaşamadığını söyleyebilmiş. Bir o kadar şaşırtıcı olan başka bir veri de bilgisayarlarına izinsiz girişler sonucunda mali zarara uğrayan kuruluşların oranı: yüzde 64. Tek bir yıl içerisinde kuruluşların yarısından fazlası mali zarara uğramış.

Kendi deneyimlerim bu tarz araştırmalardaki rakamların biraz abartılı olduğunu söylüyor. Araştırmayı yapan kişilerin niyetlerinden kuşkuluyum. Ama bu, zararın az olduğu anlamına gelmez. Zarar büyük. Güvenlik ihlâllerine karşı hazırlıklı olmayanlar, aslında kaybetmeye hazırlanıyorlar.

Pek çok şirkette kullanılan ticari güvenlik ürünleri, çoğunlukla, *yazılımcı veletler* olarak bilinen amatör bilgisayar korsanlarına karşı koruma

sağlamayı amaçlamaktadırlar. İnternetten indirilmiş programlar kullanan bu yeniyetme korsanlar çoğu zaman biraz rahatsızlık vermekten öteye gidemiyorlar. Büyük kayıplar ve gerçek tehlike, maddi bir kazanç sağlamaya güdülenmiş, hedefleri iyi tanımlanmış, planlı saldırganlardan geliyor. Bu insanlar, amatörler gibi birçok sisteme birden girmeye çalışmaktansa, her seferinde tek bir hedef üzerinde yoğunlaşıyorlar. Amatör korsanlar sayıyı çok tutmayı amaçlarken, profesyoneller kaliteli ve değerli bilgiyi hedefliyorlar.

Kimlik tespiti için kullanılan tanıma araçları, sistem özkaynaklarına ve dosyalara erişimin yönetilmesi için erişim kontrolü sistemleri ve hırsız alarmlarının elektronik karşılığı olan izinsiz girişleri tespit sistemleri gibi teknolojiler, bir şirket güvenlik programı için önemlidirler. Yine de şirketler, güvenlik önlemlerine yatırım yapmaktansa, kahveye para harcamayı yeğliyorlar.

Suçluların aklı nasıl suç işlemeye yönelik çalışıyorsa, bilgisayar korsanının da aklı güçlü güvenlik teknolojilerinin açıklarını bulmaya yönelik çalışır. Çoğu zaman da bunu teknolojiyi kullanan kişileri hedefleyerek yaparlar.

Yanıltıcı Uygulamalar

En emniyetli bilgisayarın kapalı bir bilgisayar olduğuna dair yaygın bir söz vardır. Akıllıca ama yanlış: Art niyetli bir kişi ofise gidip bilgisayarı açması için birini ikna ederek işi bitirir. Elinizdeki bilgiye sahip olmak isteyen bir rakibiniz, çoğu zaman var olan pek çok farklı yoldan birini kullanarak onu elde edebilir. Bu iş yalnızca zamana, sabırlı olmaya, kişiliğe ve ısrarcılığa bakar. İşte bu noktada aldatma sanatı devreye girer.

Bir saldırganın, davetsiz misafirin ya da toplum mühendisinin güvenlik önlemlerini atlatmak amacıyla, bilgisini paylaşacak güvenilir bir kullanıcıyı kandırması ya da hiçbir şeyden kuşkulanmayan bir hedefi ona giriş hakkı tanıması için aldatması gerekir. Güvenilir çalışanlar, hassas bilgileri paylaşmaları için ya da saldırganın içeri sızmasını sağlayacak bir güvenlik açığı yaratmaları için kandırılabildiklerinde, ikna edilebildiklerinde ya da yönlendirilebildiklerinde dünyadaki hiçbir teknoloji bir şirketi koruyamaz. Tıpkı şifre çözümleyicilerinin şifre teknolojisini bertaraf edecek bir açık bularak, şifrelenmiş bir mesajın içeriğini öğrenebildikleri gibi, toplum mühendisleri de güvenlik teknolojilerini bertaraf etmek için çalışanlarınızı aldatma yöntemi kullanılar.

Güvenin Kötüye Kullanılması

Çoğu durumda, başarılı toplum mühendislerinin güçlü insan ilişkileri vardır. Hızlı dost olup güven sağlayabilmek için gerekli kişilik özelliklerine sahip; yani etkileyici, nazik ve sevimli kişilerdir. Deneyimli bir top-

lum mühendisi, sanatının stratejilerini ve taktiklerini kullanarak neredeyse hedeflediği her bilgiye ulaşabilir.

Yetenekli teknoloji uzmanları alın teri dökerek bilgisayar kullanımına bağlı riskleri en aza indirgemek için bilgi güvenliği çözümleri üretmişler, ancak en zayıf halka olan insan unsuruna dokunmamışlardır. Tüm zekâmıza karşın, biz insanlar -siz, ben ve diğer herkes- birbirimizin güvenliğine yönelik en büyük tehdidi oluşturuyoruz.

Ulusal Karakterimiz

Özellikle Batı dünyasında, bu tarz tehditlerin üzerinde durmuyoruz. Bize birbirimizden şüphelenmemiz öğretilmiyor. Bu en çok da Amerika'da böyle. Bize "komşumuzu sevmemiz", birbirimize güvenmemiz ve inanmamız öğretilir. Yerel güvenlik örgütlerinin, insanları evlerini ve arabalarını kilitlemeye ikna etmelerinin ne kadar zor olduğunu bir düşünün. Bu tarz açıkların verilebileceği gün gibi ortadadır ve hayal dünyasında yaşamayı tercih eden pek çokları tarafından göz ardı edilmektedir; ta ki ağızları yanana kadar.

Her insanın iyi niyetli ve dürüst olmadığını biliyoruz, ancak çoğu zaman sanki öyle değillermiş gibi davranıyoruz. Bu muhteşem saflık, Amerikalıların yaşamlarının temel taşıdır ve bundan vazgeçmek acı verici olacaktır. Bir ulus olarak, özgürlük anlayışımızın içine, yaşanacak en iyi yerin anahtarların ve kilitlerin en az gerekli olduğu yer anlayışını da koymuşuz.

Çoğu insan, kandırılma olasılığının çok düşük olduğu inancına dayanarak, başkaları tarafından kandırılmayacağı varsayımıyla hareket eder; bu ortak inancın bilincinde olan saldırgan, isteğini o kadar akıllıca sunar ki hiç kuşku uyandırmaz ve kurbanın güvenini sömürür.

Kurumsal Saflık

Ulusal karakterimizin bir parçası olan bu saflık, bilgisayarlar ilk olarak uzaktan birbirlerine bağlandıklarında da görülüyordu. Hatırlayın, İnternet'in ilk şekli olan ARPANet (Savunma Bakanlığı İleri Araştırma Projeleri Birimi Ağı) devlet, araştırma ve eğitim kurumları arasında bilgi paylaşmanın bir yolu olarak tasarlanmıştı. Amaç, teknolojik ilerlemenin yanısıra bilgi özgürlüğüydü. Böylece pek çok eğitim kurumu, ilk bilgisayar sistemlerini ya hiç ya da çok az güvenlik sağlayarak kurdular. Tanınmış bir yazılım özgürlükçüsü olan Richard Stallman, kendi hesabını bir şifreyle korumayı bile reddetmişti.

Ancak internet'in elektronik ticaret için kullanılmaya başlanması, zayıf güvenlik önlemlerinin, her şeyin biribirine kablolarla bağlı olduğu dünyamızda yaratacağı tehlikeleri ciddi şekilde açığa çıkardı.

Bugünün havaalanlarına bir bakın. Güvenlik en üst düzeye ulaşmış durumda ancak güvenliği aşıp, kontrol noktalarından tehlikeli olabilecek silahlar geçiren yolcularla ilgili basında duyduğumuz haberlerle dehşete düşüyoruz. Hava alanlarımız böyle bir alarm durumundayken bu nasıl mümkün olabiliyor? Metal dedektörleri mi doğru çalışmıyor? Hayır. Sorun makinelerde değil. Sorun insan unsurunda: Makineleri çalıştıran insanlarda. Hava alanı yetkilileri Ulusal Muhafızlar'ı kapıya koyup, metal dedektörleri ve yüz tanıma sistemleri yerleştirebilirler ama aktif güvenlik görevlilerini, yolcuları nasıl kontrol edecekleri konusunda eğitmek daha yararlı olur gibi görünüyor.

Aynı sorun, dünya çapında, tüm devlet kurumları, eğitim kuruluşları ve ticari işletmeler için de geçerli. Güvenlik uzmanlarının çabalarına karşın bilgiler savunmasız kalıyor ve güvenlik zincirinin en zayıf halkası olan insan halkası güçlendirilmediği sürece, toplum mühendisliği becerileri olan saldırganlarca iştah açıcı bir hedef olarak görülmeye devam ediyor.

Her zamankinden çok şu anda, pembe gözlüklerimizi çıkarıp, bilgisayar sistemlerimizin ve ağlarımızın gizliliğine, bütünlüğüne ve varlığına saldırmaya yeltenecek olanların kullandığı yöntemlere karşı daha gözü açık olmalıyız. Trafikte diğer arabaların herşeyi yapabileceği olasılığına karşı geliştirilen korunmacı sürücülüğün gerekliliğine zamanla inandık; artık korunmacı programcılık uygulamalarını da öğrenip onlara da inanma zamanımız geldi.

Özel yaşantınızı, aklınızı ya da şirketinizin bilgi sistemlerini ihlal eden bir saldırı tehlikesi, başınıza gelene kadar gerçekleşecekmiş gibi görünmeyebilir. Maliyetleri yüksek olan böylesi bir gerçekle yüzleşmekten kaçınmak için, bilgi varlıklarımızı, kendi kişisel bilgilerimizi ve ulusumuzun hassas alt yapılarını korumak konusunda hepimizin bilinçli, eğitimli ve uyanık olmamız gerekmektedir. Ve bu önlemleri bugünden almamız şarttır.

Teröristler ve Aldatmacalar

Aldatma sanatı, doğal olarak, yalnızca toplum mühendisine özgü bir araç değildir. Fiziksel terörizm büyük yankılar uyandırıyor ve dünyanın tehlikeli bir yer olduğunun daha önce hiç varmadığımız kadar farkına varmamıza yol açıyor. Sonuçta, medeniyet yalnızca ince bir kaplama gibi.

Eylül 2001'de, New York ve Washington'a yapılan saldırılar her birimizin -yalnızca Amerikalıların değil, tüm ulusların iyi niyetli insanlarının da- yüreğine hüzün ve korku saldı. Dünyanın her tarafında, iyi eğitilmiş ve yeni saldırılar yapmanın fırsatını kollayan, takıntılı teröristlerin olduğu gerçeğine karşı uyarıldık.

Devletlerin son zamanlarda artan çabaları, güvenlik bilinci düzeyimizi artırdı. Her tür terörizme karşı uyanık ve tetikte olmalıyız. Teröristlerin

nasıl büyük bir hainlikle sahte kimlikler yarattıklarını, öğrenci ve komşu rollerine büründüklerini ve kalabalığa karıştıklarını iyice anlamamız gerekir. Entrikalar çevirirlerken, bu sayfalarda okuyacaklarınıza benzer aldatma numaraları çekerek asıl niyetlerini gizliyorlar.

Bildiğim kadarıyla, teröristler şirketlere, içme suyu tesislerine, elektrik üretme tesislerine ya da ulusal altyapımızın başka yaşamsal önemi olan parçalarına sızmak için henüz toplum mühendisliği teknikleri kullanmadılarsa da, asıl sorun orada yatıyor. Bunu yapmak son derece kolay. Bu kitap sayesinde, şirket üst yönetimlerinin güvenlik bilincini yerleştirip yeni güvenlik politikalarını uygulamaya koyacağını umuyorum.

Bu Kitap Hakkında

Şirket güvenliği bir denge konusudur. Yetersiz güvenlik, şirketinizi çok savunmasız bırakırken, güvenliğin üzerinde fazla durmak ise işle ilgilenilmesini engelleyip, şirketin büyümesini ve kazancını kısıtlar. Asıl zor iş güvenlik ve üretkenlik arasındaki dengeyi kurmaktır.

Şirket güvenliğiyle ilgili başka kitaplar, yazılım ve donanım teknolojileri üzerine odaklanırlar ve en ciddi tehlikeye yeterince yer vermezler: insanların aldatılması. Bu kitabın amacı, diğerlerinden farklı olarak, sizin, beraber çalıştığınız insanların ve şirketinizin diğer çalışanlarının nasıl yönlendirilebileceğini anlamanıza yardımcı olmak ve kandırılan kişi konumundan çıkmak için ne gibi önlemler alabileceğinizi göstermektir. Elinizdeki kitap, çoğunlukla, saldırganların bilgi çalmak, güvenilir olduğu düşünülen ama aslında öyle olmayan bir bilgiyi doğrulamak ya da bir şirket ürününü tahrip etmek için kullandıkları, teknik olmayan yöntemler üzerinde duruyor.

Benim görevim, var olan basit bir gerçek nedeniyle daha da zorlaşıyor: Her okuyucu, toplum mühendisliğinin en büyük ustaları olan anne-babalar tarafından zaten yönlendirilmiş durumda. Anne ve babanız "sizin iyiliğiniz için," diyerek en doğru olduğunu düşündükleri şeyleri size yaptırmanın yollarını buldular. Toplum mühendisleri, hedeflerine ulaşmak için hikâyelerin, nedenlerin ve gerekçelerin üzerinde nasıl özenle ve maharetle oynuyorlarsa, anne-babalar da aynı yöntemleri kullanan başarılı birer hikâye anlatıcısıdırlar. Evet, hepimiz, iyi niyetli (ve bazen o kadar da iyi niyetli olmayan) toplum mühendisleri olan anne-babalarımız tarafından yoğrulduk.

Bu eğitimle şartlanmış olarak yönlendirilmeye açık hale geldik. Eğer her zaman tetikte olup başkalarına güvenmeseydik, bizden yararlanmak isteyen birinin kuklası olacağımız endişesiyle dolu olsaydık, zor bir yaşam sürüyor olurduk. Kusursuz bir dünyada kuşku bile duymadan başkalarına güvenir, karşılaştığımız insanların dürüst ve güvenilir olduklarından emin olurduk. Ama kusursuz bir dünyada yaşamıyoruz ve bu

yüzden rakiplerimizin yanıltıcı çabalarını engellemek için bir dereceye kadar ihtiyatlı olmalıyız.

Kitabın ana parçalarını oluşturan ikinci ve üçüncü ana başlıklar, toplum mühendislerini iş başında gösteren hayalî öyküler den oluşuyor. Bu bölümlerde şunları göreceksiniz:

- Telefon beleşçilerinin yıllar önce buldukları, telefon şirketinden rehberde geçmeyen bir numarayı almanın sağlam bir yolunu.
- Saldırganların kullandıkları, uyanık ve kuşkucu çalışanları bile bilgisayar kullanıcı adlarını ve şifrelerini vermeye ikna edecek çeşitli yöntemleri,
- Bir İşlem Merkezi yöneticisinin şirketinin en gizli ürün bilgisini çalabilmesi için bir saldırgana nasıl yardım ettiğini,
- Bir hanımı, her tuşa basışını kaydeden sonra da ayrıntıları saldırgana e-postalayan bir yazılım indirmesi için kandıran bir toplum mühendisinin kullandığı yöntemleri,
- Özel dedektiflerin şirketinizle ve sizinle ilgili nasıl bilgi topladıklarını okuyacaksınız. Bu sonuncunun içinizi ürperteceğinden eminim.

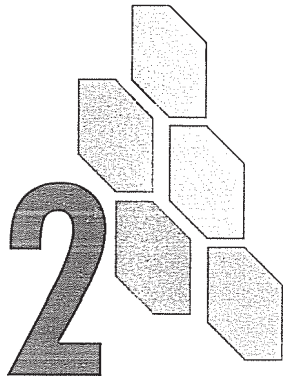
İkinci ve üçüncü ana başlıklarda geçen bazı hikâyeleri okurken, bunların mümkün olmadığını, bu sayfalarda yazılı yalanların, aşağılık numaraların ve dalaverelerin hiç kimsenin yanına kalmayacağını düşünebilirsiniz. Gerçek şu ki, her olayda anlatılan hikâyeler olmuş ve olabilecek olayları yansıtmaktadırlar: Pek çoğu dünyanın bir köşesinde her gün olmaktadır; hattâ siz bu kitabı okurken sizin kurumunuzun bile başına geliyor olabilir.

Kitabın içeriği, işinizi korumak söz konusu olduğunda gerçekten ibret verici olacaktır; kişisel yönden bakıldığında ise özel yaşamınızda bilginizin bütünlüğünü korumak için toplum mühendislerinin hamlelerini bertaraf etmenize de fayda sağlayacaktır.

Kitabın dördüncü ana başlığında konuyu farklı bir açıdan ele alıyoruz. Buradaki amacım, çalışanlarınızın toplum mühendisleri tarafından kandırılmaları olasılığını en aza indirgemek için gerekli işletme kurallarını ve bilinçlendirme eğitimlerini oluşturmanıza yardım etmek. Toplum mühendislerinin stratejilerini, yöntemlerini ve taktiklerini anlamak, şirketinizin üretkenliğini düşürmeden IT varlıklarınızı korumak için uygun kontroller yerleştirmenize yardımcı olacaktır.

Kısacası, bu kitabı, toplum mühendisliğinin oluşturduğu ağır tehlikeye karşı sizleri bilinçlendirmek ve şirketinizin ve çalışanlarınızın bu yolla sömürülmesi olasılığını en aza indirgemenize yardım etmek için yazdım.

Ya da belki şöyle söylemeliyim, bu olasılık bir daha hiç sömürülemeyecekleri kadar azalacaktır.



Saldırı Sanatı

ZARARSIZ GİBİ GÖRÜNEN BİLGİLER

Çoğu insana göre toplum mühendislerinden kaynaklanacak en büyük tehdit nedir? Kendinizi korumak için ne yapabilirsiniz?

Eğer amaç çok değerli bir ödül ele geçirmekse -diyelim ki, bir şirketin fikrî sermayesinin önemli bir parçasıysa- o zaman belki de gerekli olan şey, mecazî olarak, yalnızca daha güçlü bir kasa ve daha iyi silahlanmış bekçilerdir. Öyle değil mi?

Ama aslında bir şirketin güvenliğinin aşılması, genellikle kötü adamın şirketteki pek çok insanın korunması ve sınırlandırılması için bir neden görmediği, son derece masum, günlük ve önemsiz görünen bir bilgiyi ya da bir belgeyi elde etmesiyle başlar.

Bilginin Gizli Değeri

Çoğu toplum mühendisleri, bir şirketin elinde olan ve zararsız gibi görünen bilgileri el üstünde tutarlar çünkü bu bilgiler, kendilerini daha inandırıcı kılabilmelerinde can alıcı bir rol oynayabilir.

Bu sayfalarda, toplum mühendislerinin saldırılarına sizin de "tanık" olmanızı sağlayarak işlerini nasıl yaptıklarını göstereceğim; bazen olayı kurban rolündeki kişilerin bakış açısından sunacağım, böylece kendinizi onların yerine koyabilecek ve siz (belki de çalışanlarınızdan ya da iş arkadaşlarınızdan biri) olsaydınız nasıl bir yanıt verebileceğinizi tartabileceksiniz. Çoğu durumda aynı olayları toplum mühendisinin bakış açısından da göreceksiniz.

İlk öykü finans endüstrisindeki bir açık noktaya değinmektedir.

Creditchex

İngilizler, tutucu bir bankacılık sistemine uzun bir süre katlanmak zorunda kaldılar. Sıradan ve dürüst bir vatandaş olarak bir bankadan içeri girip bir hesap açtıramazdınız. Hatırlı müşterilerden biri sizin için bir tavsiye mektubu yazmadığı sürece banka sizi müşteri olarak kabul etmeyi düşünmezdi bile.

İngilizlerin bu sistemi günümüzün görünüşte eşitlikçi bankacılığından doğal olarak oldukça farklı. İş yapmaktaki çağdaş rahatlığımız, neredeyse herkesin bir bankaya girip kolaylıkla vadesiz çek hesabı açtıra-

bildiği, arkadaş canlısı ve demokratik Amerika'dan başka hiçbir yerde bu kadar göze çarpmıyor, öyle mi? Tam olarak değil. Gerçek şu ki, bankaların anlaşılabilir nedenlerden ötürü, geçmişte karşılıksız çek yazmış olabilecek biri adına -ki bu, kişinin adli sicilinde banka soygunu ya da zimmete geçirme suçlarının olması kadar kötü bir durumdur- hesap açmak konusunda doğal bir çekingenlikleri vardır. Bu yüzden, müstakbel bir müşteriyle ilgili hızlı bilgiler edinmek pek çok banka için olağan bir uygulamadır.

Bu tarz bilgileri edinmek için bankaların iş yaptıkları başlıca şirketlerden biri de bizim CreditChex adını vereceğimiz bir kuruluş. Müşterilerine çok önemli bir hizmet sunmakla birlikte, birçok şirkette olduğu gibi, işini bilen toplum mühendislerine de farkında olmadan kullanışlı bilgiler sağlayabiliyorlar.

İlk Görüşme: Kim Andrews

- Ulusal Banka, ben Kim. Size nasıl yardımcı olabilirim?

- Merhaba Kim. Sana bir sorum olacaktı. Sizler CreditChex kullanıyor musunuz?

- Evet.

- CreditChex'i aradığınız zaman, onlara verdiğiniz numaraya ne ad veriyorsunuz? Üye İşyeri Numarası mı?

Kız bir an duraksadı; soruyu tartıp, bunun neyle ilgili olduğunu ve yanıt verip vermemesi gerektiğini düşündü.

Bu arada, telefondaki ara vermeden konuşmayı sürdürdü:

- Sormamın nedeni şu: özel dedektiflik konusunda bir kitap yazıyorum.

- Evet, dedi kız, soruyu gönül rahatlığıyla yanıtlayarak. Bir yazara yardımcı olabildiği için memnun olmuştu.

- Üye İşyeri Numarası deniyor, öyle mi?

- Hı hı.

- Tamam, harika. Terimleri doğru kullanabilmek için sormuştum. Yani kitap için. Yardımların için teşekkürler. Hoşçakal, Kim.

İkinci Görüşme: Chris Talbert

- Ulusal Banka, Yeni Hesaplar, ben Chris.

- Merhaba, Chris. Ben Alex, dedi arayan. *CreditChex'in müşteri temsilcisiyim. Hizmetlerimizi geliştirebilmek için bir araştırma yapıyoruz. Bana birkaç dakikanı ayırabilir misin?*

Chris memnuniyetle ayırabileceğini söyledi ve arayan konuşmaya devam etti:

- *Pekâlâ. Şubenizin çalışma saatleri nedir?* Kadın yanıtladı ve ardarda gelen soruları yanıtlamaya devam etti.

- *Şubenizin kaç çalışanı bizim hizmetlerimizden yararlanıyor?*

- *Bilgi talebi için bizi ne sıklıkta arıyorsunuz?*

- *Sizin için ayırdığımız 800'lü numaralardan hangisini kullanıyorsunuz?*

- *Müşteri temsilcilerimiz her zaman size karşı nazikler mi?*

- *Talebinize yanıt verme süremiz ne kadar?*

- *Ne kadar süredir bankada çalışıyorsunuz?*

- *Şu anda kullandığınız Üye İşyeri Numarası nedir?*

- *Size sağladığımız bilgilerde hiç tutarsızlığa rastladınız mı?*

- *Hizmetlerimizi geliştirmemiz doğrultusunda önerileriniz olsaydı, bunlar neler olurdu?*

Ve:

- *Şubenize düzenli olarak göndereceğimiz anketleri doldurmak ister misiniz?*

Kadın yapabileceğini söyledi, biraz konuştular, arayan telefonu kapattı ve Chris işinin başına döndü.

Üçüncü Görüşme: Henry McKinsey

- *CreditChex, ben Henry McKinsey, size nasıl yardımcı olabilirim?*

Arayan, Ulusal Banka'dan aradığını söyledi. Doğru Üye İşyeri Numarasını, sonra da bilgi istediği kişinin adını ve sosyal güvenlik numarasını verdi. Henry kişinin doğum gününü sordu ve arayan onu da verdi.

Biraz sonra Henry bilgisayar ekranından kayıtları okudu.

- *Wells Fargo 1998'de, bir kerelik, 2.066 dolar tutarında YB rapor etmiş.*

YB (Yetersiz Bakiye), yazılan çeke karşılık hesapta yeterince para olmadığı durumlar için kullanılan bankacılık terimidir.

- *O zamandan beri başka hareket olmuş mu?*

- *Hayır, olmamış.*

- *Başka sorgulama olmuş mu?*

- *Bir bakalım. Evet, iki tane olmuş, ikisi de geçen ay. Chicago, Üçüncü Birleşik Kredi Birliği.*

Bir sonraki adı, Schenectady Yatırım Ortaklığı'nı, okurken bocaladı ve harf harf kodlamak zorunda kaldı.

- *New York Eyaleti'nde,* diye de ekledi.

Özel Dedektif İş Başında

Bu görüşmelerin üçü de aynı kişi tarafından, adına Oscar Grace diyeceğimiz bir özel dedektif tarafından yapılmıştı. Grace'in yeni bir müşterisi vardı ve bu onun ilk müşterilerinden biriydi. Birkaç ay öncesine kadar polis olan Grace, yeni işlerin bazılarını rahatlıkla çözebildiğini fark etmişti, ancak diğerleri kaynaklarını ve yaratıcılığını sonuna kadar kullanmasını gerektirecek kadar zorluydu. Bu seferki iş kesinlikle zorlular sınıfına giriyordu.

Polisiye romanların tanıdık özel dedektifleri -Sam Spades ve Philip Marlowes- eşini aldatan birini yakalayabilmek için saatlerce arabalarında oturup gece yarılarına kadar beklerlerdi. Gerçek hayattaki özel dedektifler de aynısını yapıyorlar. Özel dedektifler polisiye romanlara daha az konu olmuş ama didişen eşlerin işlerine burun sokmanın bir o kadar önemli başka bir çeşidini, yani gece nöbetleriyle cebelleşmekten çok, büyük ölçüde toplum mühendisliği becerilerine dayanan bir yöntem de kullanıyorlar.

Grace'in yeni müşterisi, giysiler ve mücevherler için oldukça geniş bir bütçe ayırabiliyor gibi görünen bir hanımdı. Bir gün ofisine gelmiş ve üstünde kağıt yığılı olmayan tek deri koltuğa oturmuştu. Gucci marka büyük el çantasını, markası ona dönük kalacak şekilde masaya koymuş ve boşanmak istediğini kocasına söylemeyi tasarladığını açıklamıştı, ancak "küçük bir sorun" olduğunu da itiraf etmişti.

Görünüşe göre kocası bir adım öndeydi. Tasarruf hesaplarındaki parayı ve yatırım hesaplarında duran daha da büyük bir tutarı çoktan çekmişti. Kadın paraların nereye kaçırıldığını bilmek istiyordu ve boşanma avukatı hiç yardımcı olmuyordu. Grace, avukatın, paranın nereye gittiği gibi pis işlere elini bulaştırmayacak, hızlı yükselen, yüksek gelirli danışmanlardan biri olduğunu tahmin etti.

Acaba Grace ona yardımcı olabilir miydi?

Bu işin çocuk oyuncağı olduğuna kadını ikna etti, bir fiyat verdi, masrafların, gerçekleştikçe faturalandırılacağını söyledi ve ilk ödeme için bir çek aldı.

Sonra da çözmesi gereken sorunla yüzleşti. Daha önce hiç böyle bir iş yapmadıysanız ve para izi sürmek konusunda pek bir şey bilmiyorsanız ne yaparsınız? Ufak adımlar atarak işe başlarsınız. İşte, bize aktarıldığı kadarıyla Grace'in öyküsü:

CreditChex'in ne olduğunu ve bu şirketin bankaların hangi konuda işine yaradığını -eski karım bir bankada çalışırdı- biliyordum. Ama kullanılan terimleri ve süreçleri bilmiyordum ve eski karıma sormak zaman kaybı olacaktı.

Birinci adım: Bankacılık terimlerini öğren ve istenen şeyin konuya

hakim biri tarafından istendiği izlenimini yaratmanın bir yolunu bul. Aradığım bankada, adı Kim olan genç hanım CreditChex'i aradıkları zaman kendilerini nasıl tanıttıklarını sorduğumda kuşkulandı. Duraksadı ve bana söyleyip söylememekten emin olamadı. Bu beni caydırdı mı? Elbette hayır. Üstelik bu duraksama bana önemli bir ipucu, onun için inandırıcı olacak bir neden bulmam gerektiğine dair bir işaret verdi. Ona bir kitap için araştırma yaptığım oyununu oynadığımda, bu, kuşkularını giderdi. Bir kitap ya da senaryo yazarı olduğunuzu söyleyin, herkesin dili çözülüverir.

Terimler

HEDEF: Bir dalaverenin kurbanı.

KAYNAĞI KURUTMAK: Bir saldırgan, gerçekleştirdiği saldırıyı kurbanının anlamasına izin verirse, o zaman buna kaynağı kurutmak denir. Kurban bir kez durumu anlar ve diğer çalışanlara ve yönetime bu girişimden söz ederse, gelecek saldırılarda aynı kaynağı sömürmek çok güçleşecektir.

Elimde Kim'in üzerinde işe yarayabilecek başka bilgiler de vardı; hakkında bilgi istediğiniz kişiyle ilgili CreditChex'in ne tür bilgiler istediğini, sizin o kişiyle ilgili neler isteyebileceğinizi ve en önemlisi Kim'in çalıştığı bankanın Üye İşyeri Numarası'nı biliyordum. Bu soruları sormaya hazırdım ama duraksaması bir tehlike işaretiydi. Kitap araştırması hikâyesini yutmuştu, ancak işin başında biraz kuşkulanmıştı. Eğer başından yardımcı olmaya hevesli olsaydı, süreçlerle ilgili daha fazla şey anlatmasını ondan isteyebilirdim.

İçinizden gelen sese kulak vermeli, hedefin söylediklerini ve nasıl söylediğini dikkatle dinlemelisiniz. Bu hanım, çok fazla olağandışı soru soracak olsaydım, kafasında alarm zilleri çalacak kadar zeki görünüyordu. Her ne kadar kim olduğumu ve hangi numaradan aradığımı bilmese de, eğer bu işin içindeyseniz, telefon ederek şirketle ilgili bilgi almaya çalışan birine karşı, birilerinin ortalığı ayağa kaldırmasını istemezsiniz. Bunun nedeni kaynağı kurutmak istememenizdir; aynı işyerini başka bir zaman bir kez daha aramak isteyebilirsiniz.

Bir insanın bana "Buyrun emrinize amadeyim," diyerek yardımcı mı olacağını yoksa "Bu adamın niyeti bozuk, polisi arayayım," diye ortalığı ayağa mı kaldıracağını anlamak amacıyla bana ipucu verecek küçük işaretleri yakalayabilmek için gözümü-kulağımı hep açık tutarım.

Kim'i biraz diken üstünde biri olarak derecelendirdim, bu yüzden farklı bir şubedeki başka birini aradım. Chris'le yaptığım ikinci görüşmede, araştırma numarası çok iyi iş gördü. Buradaki yöntem, inandırıcılığı artıracak ilgisiz soruların arasına önemli soruları sıkıştırmakta yatıyor. CreditChex'deki Üye İşyeri Numarası'nı sormadan önce, bankada ne kadar süredir çalıştığıyla ilgili ona kişisel bir soru yönelterek bir son dakika kontrolu yaptım.

Kişisel bir soru mayın gibidir; bazıları üzerinden geçer ve hiçbir zaman farketmezler; bazılarında ise patlar ve güvenli bir yer bulmak için telaş içinde kaçmalarına neden olur. Bu yüzden, eğer kişisel bir soru sorarsam, karşı taraf soruyu yanıtlarsa ve ses tonunda bir değişiklik olmazsa, büyük olasılıkla talebin içeriğinden şüphelenmemiş demektir. Yanıtlanmasını istediğim soruyu ona, kuşku uyandırmadan rahatlıkla sorabilirim ve büyük olasılıkla bana istediğim cevabı verir.

İyi bir özel dedektifin bildiği bir şey daha vardır: Hiçbir zaman, kilit bilgiyi elde ettikten sonra görüşmeyi hemen bitirme. Bir-iki soru, biraz sohbetten sonra veda etmek yerinde olabilir. Eğer kurban sorduklarınızla ilgili bir şeyleri daha sonra hatırlarsa, bunlar büyük olasılıkla son birkaç soru olacaktır. Kalanı genellikle unutulur.

Böylece Chris bana Üye İşyeri Numarası'nı ve taleplerini bildirmek için kullandıkları telefon numarasını verdi. CreditChex'ten ne kadar bilgi edinilebildiğini öğrenebileceğim sorular da sorabilseydim daha mutlu olurdum. Ancak şansımı zorlamak istemedim.

Bu, CreditChex'ten tutar hanesi boş bir çek almak gibi bir şeydi. Artık istediğim zaman arayıp bilgi elde edebilirdim. Aldığım hizmet için para ödememe bile gerek yoktu. Görünüşe göre CreditChex temsilcisi istediğim bilgileri benimle paylaşmaya hazırdı. Müşterimin kocasının hesap açtırmak için son zamanlarda başvurduğu iki yer vardı. O zaman, yakında eski eşi konumuna gelecek olan kadının aradığı paralar neredeydi? CreditChex'teki adamın saydığı bankalardan başka nerede olabilirdi ki?

Aldatmacanın İncelenmesi

Tüm bu düzen toplum mühendisliğinin temel taktiklerinden birinin üzerine kurulmuştur: öyle olmadığı halde, bir şirket çalışanının, zararsız olduğunu düşündüğü bir bilgiye ulaşmak.

İlk banka memuru CreditChex'i ararken kullanılan tanımlayıcı sayıyı anlatan Üye İşyeri Numarası terimini doğruladı. İkincisi, CreditChex'in telefon numarasını ve en can alıcı bilgi olan bankanın Üye İşyeri Numarası'nı sağladı. Tüm bu bilgiler memura zararsız görünüyordu. Bu sayıyı başkasına söylemenin ne zararı olabilirdi ki?

Mitnick Mesajı:

Üye İşyeri Numarası, bu durumda, bir şifre kadar önem taşır. Eğer banka çalışanları onu bir ATM şifresi olarak görürlerse, bilginin hassaslığını kavrayabilirler. Şirketinizde insanların yeterli özeni göstermedikleri katırım içi bir şifre ya da numara var mı?

Tüm bunlar üçüncü görüşme için gereken zemini hazırladı. Grace'in elinde CreditChex'i arayıp, kendini müşteri bankalardan biri olan Ulusal Banka'nın bir çalışanı gibi tanıttıktan sonra istediği bilgiyi alabilmesi için ihtiyacı olan her şey vardı.

Bilgi çalarken, iyi bir dolandırıcının paranızı çalmada gösterdiği becerikliliğe benzer bir beceriklilik gösteren Grace'in, insanları okumak için geliştirilmiş yetenekleri vardı. Sıkça uygulanan, masum soruların arasına anahtar soruları katma yöntemini o da biliyordu. Üye İşyeri Numarası'nı her şey yolundaymış gibi sormadan önce kişisel bir sorunun ikinci memurun işbirliği yapma eğilimini ölçeceğini de biliyordu.

İlk memurun, CreditChex üye numarası için kullanılan terimi onaylayarak yaptığı hataya karşı korunmaya neredeyse olanak yoktu. Bu bilginin bankacılık sektöründe o kadar geniş bir kullanımı var ki önemsiz gibi görünüyor; zararsız görünümlü bilgilere en iyi örnek. Ancak ikinci memur Chris, arayanın gerçekte söylediği kişi olup olmadığını doğrulamadan soruları yanıtlamaya bu kadar hevesli olmamalıydı. En azından adını ve telefon numarasını alıp onu geri aramalıydı; böylece daha sonra şüphe uyanırsa, karşı tarafın hangi telefon numarasını kullandığının bir kaydını tutmuş olabilirdi. Bu durumda, böyle bir arama yapmak, saldırganın CreditChex görevlisi gibi davranmasını daha da güçleştirirdi.

Daha da iyisi, CreditChex'i, arayanın verdiği numaradan değil, bankanın kayıtlarında bulunan bir numaradan arayıp, kişinin gerçekten orada çalışıp çalışmadığını ve şirketin gerçekten müşteri araştırması yapıp yapmadığını doğrulamak olurdu. Gerçek dünya uygulamalarını ve bugün çoğu insanın içinde bulunduğu zaman baskısını göz önüne aldığınızda, çalışanın bir çeşit saldırı gerçekleştirildiğinden kuşkulandığı durumlar dışında, bu tarz bir kontrol araması yapması beklentilerin çok ötesindedir.

Mühendislik Tuzağı

İnsan avcısı firmaların şirket içi yetenekleri bulmak için toplum mühendisliği taktiklerini kullandıkları yaygın olarak bilinir. İşte bunun nasıl olabileceğine dair bir örnek.

1990'ların sonlarında, pek de ahlağa uygun çalışmayan bir iş bulma acentası, telefon endüstrisinde deneyimli elektrik mühendisleri arayan bir şirketi yeni müşterisi olarak aldı. Bu görevin sorumlusu, buğulu bir ses tonuna ve çekici tavırlara sahip bir hanımdı. Bu yeteneklerini telefon üzerinden, güven veren ve dostça bir izlenim uyandırmak amacıyla kullanmayı da öğrenmişti.

Kadın, rakip bir şirkette çalışmak için ayartılabilecek mühendisler bulup bulamayacağına bakmak amacıyla bir cep telefonu hizmet sağlayıcısını yoklamaya karar verdi. Santralı arayıp, "Beş yıllık mühendislik

deneyimi olan herhangi biriyle görüşmek istiyorum" diyemezdi. Bunun yerine, biraz sonra göreceğiniz nedenlerle, yetenek avına hiçbir hassasiyeti yokmuş gibi görünen ve şirket çalışanlarının neredeyse isteyen herkese verdiği bir bilgiyi arayarak başladı.

İlk Görüşme: Danışma Görevlisi

Saldırgan, Didi Sands adını kullanarak, cep telefonu hizmet sağlayıcısının şirket binasına telefon etti. Konuşma, kısmen şöyle geçti:

Danışma Görevlisi: İyi günler. Ben Marie, sizenasıl yardımcı olabilirim?

Didi: Beni Nakliyat Bölümü'ne bağlar mısınız?

DG: Öyle bir bölümümüz olduğundan emin değilim, rehberime bakayım. Kim arıyordu?

D: Didi

DG: Binada mısınız, yoksa ...?

D: Hayır, dışardayım.

DG: Didi, soyadınız?

D: Didi Sands. Nakliye'nin dahilisini biliyordum ama unutmuşum.

DG: Bir saniye.

Kuşku uyandırmamak için, bu noktada Didi, sohbeti sürdürmek amacıyla, "içerden" olduğunu ve şirket binalarının yerlerini bildiğini göstermek üzere tasarlanmış sıradan gibi görünen bir soru sordu.

D: Hangi binadasınız? Lakeview'da mı yoksa ana binada mı?

DG: Ana binada (duraksama). *Numara 805 555 6469.*

Nakliye Bölümü'nü aramanın işe yaramayabileceğini de dikkate alarak kendini sağlama almak amacıyla Didi, Gayrımenkul Bölümü'yle de görüşmek istediğini söyledi. Danışma görevlisi o numarayı da verdi ve onu Nakliye Bölümü'ne bağlamayı denedi ama hatlar meşguldü.

Bu aşamada Didi üçüncü bir telefon numarasını, Austin-Texas'taki şirket binasında bulunan Tahsilat Ofisi'nin numarasını da istedi. Danışma görevlisi ondan biraz beklemesini rica etti ve hattan çıktı. Şüpheli bir telefon geldiğini ve bir şeylerin ters gittiğini düşündüğünü güvenliğe anlatıyor olabilir miydi? Kesinlikle olamaz, Didi'nin içinde en küçük bir endişe bile yoktu. Yalnızca biraz kızın başına bela olmuştu ama danışma görevlisi için bu sıradan bir iş gününün bir parçasıydı. Bir dakika sonra, danışma görevlisi yeniden hattı aldı, Tahsilat Ofisi'nin numarasına bakıp orayı aradı ve Didi'yi bağladı.

İkinci Görüşme: Peggy

Sonraki konuşma şöyle geçti:

Peggy: Tahsilat Ofisi, Peggy.

Didi: Merhaba Peggy. Ben Didi, Thousand Oaks'dan.

P: Merhaba Didi.

D: Nasıl gidiyor?

P: İyi.

Sonra Didi, iş dünyasında iyi bilinen ve belirli bir kuruluşun ya da çalışma grubunun bütçesine harcamaları mal etmek için kullanılan işlem kodunu ifade eden terimi kullandı.

D: Mükemmel. Sana bir sorum olacak. Belli bir bölümün maliyet merkezi kodunu nasıl öğrenebilirim?

P: O bölümün bütçe sorumlusuna ulaşman gerek.

D: Thousand Oaks'un bütçe sorumlusunun kim olduğunu biliyor musun? Bir form doldurmaya çalışıyorum ve doğru maliyet merkezi kodunu bilmiyorum.

P: Tek bildiğim, maliyet merkezi kodunu öğrenmen gerektiği zaman, bütçe sorumlusunu araman gerektiği.

D: Texas'daki bölümünüz için bir maliyet merkezi kodu var mı?

P: Burada bir maliyet merkezi var ama bize hepsinin listesini vermiyorlar.

D: Maliyet merkezi kodu kaç basamaklı? Örneğin, sizin maliyet merkezi kodunuz ne?

P: Şey, şöyle, sen 9WC'yle misin yoksa SAT'la mısın?

Bunların hangi bölümlere ya da gruplara karşılık geldiği konusunda Didi'nin en küçük bir fikri yoktu ama bu önemli değildi. Soruyu yanıtladı:

D: 9WC

P: O zaman genellikle dört basamaklıdırlar. Nereden olduğunu söylemiştin?

D: Thousand Oaks, Genel Müdürlük.

P: Evet, Thousand Oaks için bir tane söyleyebilirim. 1A5N, Nancy'nin N'si.

Yardım etmeye istekli biriyle yeterince uzun süre sohbet ederek, Didi ihtiyacı olan maliyet merkezi kodunu aldı; dışardan birinin işine yarayacakmış gibi görünmediği için kimsenin korumayı düşünmediği bilgi parçacıklarından biri daha.

Üçüncü Görüşme: İşe Yarayan Yanlış Numara

Didi'nin bir sonraki adımı, elindeki maliyet merkezi kodunu bir poker markası gibi kullanarak daha değerli bir şeye dönüştürmek olacaktı.

Gayrımenkul bölümünü arayıp, yanlış numara çevirmiş gibi yaptı. *"Sizi rahatsız ettiğim için özür dilerim, ama ..."* ile söze başlayarak şirket rehberini kaybetmiş bir çalışan olduğunu söyledi ve yeni bir rehber alabilmek için kiminle konuşması gerektiğini sordu. Adam rehber kitapçığının eski tarihli olduğunu ama şirketin intranet sitesinde telefon numaralarının bulunduğunu söyledi.

Didi basılmış bir rehber kullanmayı tercih ettiğini anlatınca, adam ona matbaayı aramasını söyledi ve sonra, hiçbir talep olmadan -belki de yalnızca çekici sesli kadını telefonda biraz daha uzun süre tutabilmek için- numarayı buldu ve kadına verdi.

Dördüncü Görüşme: Matbaa'dan Bart

Matbaa bölümünde Bart adında biriyle konuştu. Didi, Thousand Oaks'dan aradığını ve çalıştıkları yeni danışmanın şirket rehberine ihtiyacı olduğunu söyledi. Eski tarihli olsa da basılı bir rehberin danışmanın daha çok işine yarayacağını da vurguladı. Bart, bir talep formu doldurması ve kendisine göndermesi gerektiğini söyledi.

Didi elinde form kalmadığını, biraz acelesi olduğunu söyledi ve acaba Bart bir incelik yapıp formu onun yerine doldurabilir miydi? Adam biraz fazlaya kaçan bir hevesle kabul etti ve Didi ona ayrıntıları anlattı. Hayali danışmanın adresi olarak da, toplum mühendislerinin posta deliği dedikleri, Didi'nin şirketinin bu tarz durumlar için, Mail Boxes Etc. türünden ticari şirketlerden kiraladığı posta kutusunu verdi.

Edindiği ilk bilgi şimdi işine yarayacaktı: Rehberin maliyeti ve kargo için bir ücret alınacaktı. Didi. Thousand Oaks için maliyet merkezi kodunu verdi.

- *1A5N, Nancy'nin N'si.*

Şirket rehberi birkaç gün sonra geldiğinde, Didi beklediğinden daha da başarılı olduğunu gördü: Rehberde yalnızca adlar ve telefon numaraları listelenmekle kalmamış, kimin kimin için çalıştığı da gösterilmişti. Tüm şirketin kuruluş şeması elindeydi.

Boğuk sesli kadın insan avlayan telefon görüşmelerini yapmaya hazırdı. Her yetenekli toplum mühendisinin sonuna kadar geliştirdiği laf yapma becerisini kullanarak, akınlarını başlatmak için gerekli olan bilgileri dalavere yoluyla elde etmişti. Şimdi de semeresini toplamaya hazırdı.

Aldatmacanın İncelenmesi

Bu toplum mühendisliği saldırısında Didi, hedef şirketin üç ayrı bölümünün telefon numaralarını elde ederek işe koyuldu. İstediği numaralar sır olmadığı için bu kolaydı, özellikle de çalışanlar için. Bir toplum mühendisi içerden biriymiş gibi konuşmayı öğrenir ve Didi bu oyunda becerikliydi. Telefon numaralarından biri onu bir maliyet merkezi koduna yönlendirmiş, o kodu da şirketin telefon rehberinden bir kopya almak için kullanmıştı.

İhtiyacı olan temel araçlar; arkadaşça davranmak, biraz şirket içi terimleri kullanmak ve son kurbanda uyguladığı, işin içine küçük, sözel göz kırpmalar karıştırmaktı.

Ve kolay elde edilemeyen önemli bir diğer araç da, toplum mühendisinin yoğun çalışmalarla ve geçmiş nesillerin iyi dolandırıcılarının kâğıda dökülmemiş deneyimlerinden ders alarak geliştirdiği lafazanlık becerileridir.

Terimler

POSTA DELİĞİ: Toplum mühendislerinin kiralık posta kutusu için kullandıkları terim. Yaygın olarak sahte isimle kiralanır ve kurbanın göndermeye ikna edildiği evrakları ya da paketleri almak için kullanılır.

Başka Değersiz Bilgiler

Maliyet merkezi kodu ve dahili telefon numaralarının dışında, işe yaramaz gibi görünen başka hangi bilgiler rakibiniz için son derece değerli olabilir?

Peter Abel'in Telefon Görüşmesi

- *Merhaba,* der hattın öbür ucundaki ses.

- *Ben Parkhurst Seyahat Acentası'ndan Tom. San Francisco biletleriniz hazır. Onları size gönderelim mi yoksa kendiniz mi gelip almak istersiniz?*

- *San Francisco mu?* der Peter.

- *Ben San Francisco'ya gitmiyorum ki.*

- *Siz Peter Abel musunuz?*

- *Evet, ama yapmayı düşündüğüm bir yolculuk yok.*

- *Hım,* der arayan, dostça gülerek.

- *Yani San Francisco'ya gitmek istememekte kararlısınız, öyle mi?*

- *Eğer patronumu kandırabilirseniz ...* der Peter, oluşan tatlı sohbete uyum sağlayarak.

- *Bir karışıklık var gibi görünüyor,* der arayan.

- *Sistemlerimizde yolculuk ayrıntılarını özlük numarasına göre sıralıyoruz. Belki birileri yanlış numarayı kullanmıştır. Sizin Sosyal Güvenlik Numaranız nedir?*

Peter nazik bir şekilde numarayı verir. Neden olmasın? Doldurduğu, neredeyse her çalışan formunun üzerine bu numarayı yazar ve şirketteki

Mitnick Mesajı:

Tıpkı bir bulmacanın parçaları gibi her bilgi kendi başına ilgisiz durabilir. Ancak parçalar bir araya getirildiğinde, açık bir resim oluşur. Bu olayda toplum mühendisinin gördüğü resim şirketin iç yapısının tamamı olmuştur.

Mitnick Mesajı:

Öyküm'ü ana fikri: İstekte bulunan kişinin sesini tanımıyorsanız ve istemek için bir nedeni yoksa, hiç kimseye kişisel ya da şirket içi bilgileri ve tanımlayıcıları vermeyin.

pek çok insanın bunu öğrenme şansı vardır; insan kaynaklarının, maaş servisinin ve doğal olarak dışarıdaki bir seyahat acentasının da. Kimse Sosyal Güvenlik Numarası'nı sır gibi saklamaz. Ne fark eder ki?

Yanıtı bulmak zor değil. Etkili bir canlandırma (toplum mühendisinin kendini başka birinin kılığına sokması) için iki-üç parça bilgi fazlasıyla yeterlidir. Yarı yeterlilikte bir toplum mühendisi, bir çalışanın adını, telefon numarasını, Sosyal Güvenlik Numarası'nı -ve işi sağlama almak için yöneticisinin adını ve telefon numarasını- elde ettikten sonra, sıradaki hedefine yönelirken kendini inandırıcı göstermek için ihtiyacı olabilecek her şeyle donanmış olacaktır.

Eğer şirketinizin başka bir bölümünden olduğunu söyleyen biri dün aramış, makul bir neden vermiş ve özlük numaranızı sormuş olsaydı, bu bilgiyi ona vermekte tereddüt eder miydiniz?

- *Bu arada, Sosyal Güvenlik Numaranız neydi?*

Aldatmacanın Engellenmesi

Şirketinizin, herkese açık olmayan bilgilerin kötüye kullanılmasından doğabilecek ciddi sorunlara karşı çalışanlarını bilgilendirme sorumluluğu vardır. Üzerinde düşünülmüş bir bilgi güvenliği politikası, düzgün bir bilgilendirme ve eğitimle birleşince şirket bilgilerinin doğru kullanımıyla ilgili çalışan bilinci görünür şekilde artacaktır. Bir veri sınıflandırma politikası, bilgi vermeye yönelik uygun denetimler getirilmesine yardımcı olacaktır. Veri sınıflandırma politikası olmadan, tüm şirket içi bilgilerin -aksi belirtilmediği sürece- gizli olarak değerlendirilmesi gerekecektir.

Şirketinizi zararsız gibi görünen bilgilerin dışarı sızmasından korumak için şunları yapın:

- Bilgi Güvenliği Birimi'nin, toplum mühendislerinin kullandığı yöntemleri anlatan bilgilendirme eğitimleri düzenlemesi gerekir. Yukarıda anlatıldığı üzere, yöntemlerden biri, hassasmış gibi durmayan bir bilgiyi elde etmek ve bunu kısa vadede güven yaratmak için bir poker markası gibi kullanmaktır. Telefonla arayan birinin, şirket süreçleri, terimler ve şirket içi tanımlayıcılar konusunda bilgili olmasının ne şekil ve tarzda olursa olsun istek sahibini gerçek kılmadığından ya da bir şeyi bilmesi gerektiği konu-

sunda onu yetkili konuma getirmediğinden tek tek her çalışanın haberdar olması gerekir. Arayan kişi eski bir çalışan ya da gerekli şirket içi bilgilere sahip bir sözleşmeli olabilir. Buna göre, her kuruluş, tanımadığı insanlarla telefonda ya da yüzyüze iletişim kurarken çalışanlarının kullanması gereken uygun kimlik tespit yöntemini belirleme sorumluluğuna sahiptir.

- Bir veri sınıflandırma politikası tasarlamakla yükümlü kişi ya da kişiler, zararsız gibi görünen ama hassas bilgilere erişimi olan çalışanlara ulaşılmasını sağlayabilecek ayrıntıları gözden geçirmelidirler. ATM kartınızın şifresini hiçbir zaman dışarı vermemenize karşın, şirket yazılım ürünlerini geliştirmek için kullandığınız sunucunun hangisi olduğunu birine söyler misiniz? Bu bilgi, şirket ağına erişim hakkı varmış gibi davranan biri tarafından kullanılabilir mi?

- Bazen şirket içi terimleri bilmek bile toplum mühendisinin daha otoriter ve bilgili görünmesini sağlayabilir. Saldırgan, kurbanlarını ikna etmek için her an olabilecek bu yanlış anlamaya sık sık başvurur. Örneğin, Üye İşyeri Numarası, bir bankanın Yeni Hesaplar biriminde insanların her gün, üzerinde pek fazla düşünmeden kullandıkları bir tanımlayıcıdır. Ancak böyle bir tanımlayıcının bir paroladan farkı yoktur. Eğer her bir çalışan bu tanımlayıcının anlamını kavramışsa -yani istek sahibinin gerçek olup olmadığını kanıtlamak için kullanılıyorsa- o zaman bu veriye daha saygıyla bakabilirler.

- Hiçbir şirket -en azından birkaç tanesi- genel müdürlerinin ya da yönetim kurulu başkanlarının doğrudan telefon numaralarını dışarı vermezler. Buna karşın, çoğu şirkette, çoğu birim ve çalışma grubunun telefon numaralarını dışarı -özellikle de diğer bir çalışana ya da çalışan gibi görünen birine- vermekle ilgili bir çekince yoktur. Alınabilecek bir önlem: Çalışanların, sözleşmelilerin, danışmanların ve geçici görevlilerin dahili telefonlarının başkalarına verilmesini yasaklayan bir yönetmeliği yürürlüğe koyun. Daha da önemlisi, telefon numarası soran kişinin gerçekten bir çalışan olup olmadığını tam olarak belirlemek için adım adım bir süreç geliştirin.

- Çalışma gruplarının ve birimlerin muhasebe hesap numaraları da, (ister basılı, ister veri dosyası ya da intranet üzerinde elektronik telefon defteri olsun) telefon rehberleri kadar sık, toplum mühendislerinin hedefi olmaktadırlar. Her şirketin bu tarz bilgilerin dışarı verilmesiyle ilgili iyi anlatılmış, yazılı bir kurallar bütününe ihtiyacı vardır. Alınacak önlemler arasında, hassas bilgilerin şirket dışından insanlara verildiği durumların not edildiği bir kayıt defterinin tutulması da olmalıdır.

Mitnick Mesajı:

Eski bir deyişte de ifade edildiği gibi: Gerçek paranoyakların bile büyük olasılıkla düşmanları vardır. Her işletmenin de düşmanları olduğunu, şirket sırlarını tehlikeye sokmak amacıyla ağ altyapısına saldırabilecek saldırganlar bulunduğunu varsaymalıyız. Sonunuz bir bilgisayar suçları istatistiği olmasın. İyi düşünülmüş güvenlik kuralları ve süreçleri aracılığıyla uygun denetimleri yerleştirerek gerekli savunmaları kurmanın zamanı geldi de geçiyor bile.

- Sosyal Güvenlik Numarası gibi bilgiler, tek başlarına bir tanımlama aracı olarak kullanılmamalıdırlar. Her çalışan yalnızca istek sahibinin kimliğini doğrulamakla kalmamalı, aynı zamanda istediğin nedenini de sorgulamalıdır. Güvenlik eğitimleriniz sırasında çalışanlarınıza şu yaklaşımı öğretmeyi deneyin: Ne zaman tanımadığınız biri size bir soru sorar ya da sizden yardım isterse, herşeyden önce istek onaylanana kadar nazikçe geri çevirmeyi öğrenin. Sonra -bay ya da bayan Yardımsever olma yönündeki doğal dürtünüze yenik düşmeden önce- onaylama ve şirket içi verilerin dışarıya verilmesiyle ilgili yönetmelikleri ve süreçleri uygulayın. Bu yaklaşım, başkalarına yardım etmeye yönelik doğal eğilimimize ters düşebilir, ancak sağlıklı, azıcık bir şüphecilik, toplum mühendisinin bir sonraki kurbanı olmaktan kurtulmanızı sağlayabilir.

Bu bölümdeki öykülerin de gösterdiği gibi zararsız zannettiğiniz bilgiler şirketinizin en önemli sırlarının anahtarı olabilirler.

DOĞRUDAN SALDIRI: YALNIZCA İSTEYİVERMEK

Pek çok toplum mühendisliği saldırısı karmaşıktır. Bir teknik bilgi ve dalavere karışımının kullanıldığı bir dizi aşama ve ayrıntılı planlama içerir.

Ama becerikli bir toplum mühendisinin zaman zaman amacına basitçe, kolayca ve lafı dolandırmadan ulaşmasını da her zaman çarpıcı bulmuşumdur. Göreceğiniz gibi, bilgiyi doğrudan isteyivermek bile tek başına yeterli olabilir.

Bir MHBM Marifeti

Birinin rehberde geçmeyen telefon numarasını mı öğrenmek istiyorsunuz? Bir toplum mühendisi size, bir kısmını bu kitabın sayfalarında da bulabileceğiniz, çeşitli yöntemler sıralayabilir, ancak büyük olasılıkla en basit yöntem tek bir telefon konuşması yapmaktır. Tıpkı aşağıda anlatıldığı gibi.

Numara Lütfen

Saldırgan özel bir telefon şirketinin MHBM (Mekanik Hat Belirleme Merkezi) numarasını çevirir ve telefonu açan kadına şöyle der:

"Merhaba, ben Paul Anthony. Kablo tamircisiyim. Bir sorunum var, buradaki bir terminal kutusu bir yangında yanmış. Polisler, manyağın birinin sigortadan para alabilmek için evini yaktığını düşünüyorlar. Bütün bu iki yüz hatlık terminalin tümünü yeniden bağlamam için beni burada tek başıma bıraktılar. Şu anda gerçekten çok yardıma ihtiyacım var. 6723 South Main'de hangi hatların çalışır durumda olması gerektiğini bana söylebilir misin?"

Telefon şirketinin diğer birimlerinde, aranan kişi, rehberde geçmeyen numaralarla ilgili ters sorgulama bilgilerini yalnızca şirketin yetkili personeline vermeleri gerektiğini bilirler. Ancak MHBM'nin de yalnızca şirket çalışanları tarafından biliniyor olması gerekir. Dışarıya hiçbir zaman bilgi vermiyor olsalar da, ağır bir işin altından kalkmaya çalışan başka bir şirket çalışanına biraz yardım edilmesine kim itiraz edebilir ki? Kadın, adamın durumuna üzülür. Kendisinin de işbaşında zor günler geçirdiği olmuştur ve zor durumda olan başka bir çalışana yardım edebilmek için kuralları birazcık esnetir. Ona kablo çiftlerini söyler ve o adrese bağlı tüm açık numaraları verir.

Mitnick Mesajı:

Yanınızdaki adama güvenmek insan doğasının bir parçasıdır, özellikle de talep sağduyulu olup olmadığınızı ölçüyorsa. Toplum mühendisleri bu bilgiyi, kurbanlarını sömürmek ve amaçlarına ulaşmak için kullanırlar.

Aldatmaca'nın İncelenmesi

Bu öykülerde sık sık göreceğiniz gibi, bir şirkette kullanılan terminolojiyi ve şirket yapısını -çeşitli bürolarını ve birimlerini, her birinin ne yaptığını ve hangi bilgileri tuttuklarını- bilmek başarılı bir toplum mühendisinin kullandığı araçların önemli bir kısmını oluşturur.

Genç Bir Kanun Kaçağı

Kendisine Frank Parsons diyeceğimiz bir adam yıllardır polisten kaçmaktaydı ve Federal Hükümet tarafından, hâlâ, 1960'larda savaş karşıtı bir yeraltı örgütünün üyesi olduğu gerekçesiyle aranıyordu. Lokantalarda kapıya dönük otururdu ve diğer insanların sıkıntı verici bulduğu, arada bir omuzunun üzerinden geriye bakma huyu vardı. Birkaç yılda bir taşınırdı.

Arada bir yerde, Frank kendini daha önce bulunmadığı bir şehirde buldu ve iş aramaya koyuldu. Gelişmiş bilgisayar becerilerine sahip olan (aynı zamanda gelişmiş toplum mühendisliği becerilerine de sahipti, ancak bunları iş başvurularında hiç belirtmiyordu) Frank gibi biri için iyi bir iş bulmak genellikle sorun olmuyordu. Ekonominin sıkışık olduğu zamanlar dışında iyi bilgisayar bilgisi olan kişilerin yeteneklerine olan talep genellikle yüksek oluyordu ve böyleleri çoğu zaman dört ayak üstüne düşüyorlardı. Frank, yaşadığı yerin yakınlarındaki gelir düzeyi yüksek insanlara hizmet veren büyük bir bakım yurdunda yüksek gelirli bir işe girme fırsatı buldu.

Bu işin kendisi için biçilmiş kaftan olduğunu düşündü. Ancak başvuru evrakıyla boğuşmaya başlayınca bir noktada durmak zorunda kaldı. İşveren ondan Adli Sicil Belgesi istiyordu ve bunu eyalet polisinden şahsen alması gerekiyordu. İş başvuru evraklarının arasında bu belgenin istenmesi için kullanılan matbu dilekçe de vardı ve dilekçenin üzerinde parmak izi basmak için küçük bir kutucuk bulunuyordu. Her ne kadar yalnızca sağ işaret parmağının izini istiyor olsalar da, eğer parmak izini FBI veritabanındaki parmak iziyle karşılaştırırlarsa kısa süre içerisinde parasını devletin ödediği bir tatil köyünde yemek servisi yapıyor olurdu.

Öte yandan Frank, küçük bir olasılıkla da olsa, bundan sıyrılabileceğini düşünüyordu. Belki de eyalet polisi parmak izi örneklerini FBI'ya hiç göndermiyordu. Bu durumda gönderip göndermediklerini nasıl öğrenebilirdi?

Nasıl mı? O bir toplum mühendisiydi; nasıl öğrendi sanıyorsunuz?

Mitnick Mesajı:

Akıllı bilgi dolandırıcıları, emniyet teşkilatının asayişi sağlama süreçleriyle ilgili bilgi almak için devlet, eyalet ya da yerel yetkilileri aramaktan çekinmezler. Elinde böyle bir bilgiler varken toplum mühendisi şirketinizin sıradan güvenlik uygulamalarını atlatabilir.

Eyalet polisine telefon etti: "Merhaba. Adalet Bakanlığı için bir çalışma yapıyoruz. Yeni bir parmak izi tespit sistemi yerleştirmek için gerekli ön koşulları araştırıyoruz. Yapılan işi iyi bilen ve bize yardım edebilecek biriyle görüşebilir miyim?"

Yerel uzman telefona geldikten sonra Frank, kullandıkları sistemlerle ve parmak izi verilerini saklama ve tarama kapasiteleriyle ilgili bir dizi soru sordu. Kullandıkları donanım hiç onlara sorun çıkarmış mıydı? Ulusal Suç Bilgileri Merkezi'nin (USBM) Parmak İzi Tarama Ağı'na mı bağlıydılar yoksa yalnızca eyaletinkine mi? Donanım herkesin öğrenebileceği kadar kolay bir kullanıma sahip miydi?

Anahtar soruyu diğerlerinin arasına kurnazca sıkıştırmıştı.

Aldığı yanıt kulağına müzik gibi geldi. Hayır, USBM'ye bağlı değillerdi, ellerindekini yalnızca eyaletin Suç Bilgileri Dizini'yle karşılaştırıyorlardı. Frank'in de tüm bilmek istediği buydu. Bulunduğu eyalette suç kaydı yoktu, böylece başvurusunu yaptı. İşe alınmıştı ve hiç kimse bir gün masasının başına dikilip de ona, "Bu beyler FBI'dan geliyorlar, seninle konuşmak istiyorlarmış," demedi.

Ve kendi söylediğine bakılırsa işyerindeki herkese örnek bir çalışanın nasıl olması gerektiğini göstermişti.

Kapının Önü

Kâğıt kullanılmayan ofis inancına karşın şiketler her gün yüzlerce sayfa kâğıt tüketiyorlar. Şirketinizdeki basılı bilgiler, güvenlik önlemleri alıp üzerine "gizlidir" damgası vursanız da, açık bir nokta oluşturabilirler.

İşte size, toplum mühendislerinin en gizli belgelerinizi nasıl ele geçirdiklerini anlatan bir hikâye.

Hat Çevirme Dalaveresi

Telefon şirketi her yıl *Deneme Numaraları Rehberi* adında bir kitapçık çıkarır (ya da en azından eskiden çıkarırlardı, şartlı tahliye sürem henüz dolmadığı için çıkarmaya devam edip etmediklerini sormayacağım). Bu kitapçık, telefon beleşçilerinin el üstünde tuttukları bir belgedir, çünkü şirket görevlilerinin, teknisyenlerinin ve diğerlerinin sürekli meş-

Mitnick Mesajı:

Bilgi varlıklarını korumaya ilişkin şirket kurallarıyla ilgili güvenlik eğitimleri, yalnızca şirketin IT varlıklarına elektronik ya da maddi erişimi olan çalışanlara değil, şirketteki herkese yönelik olmalıdır.

gul çalan numaraları ya da şehirlerarası hatları kontrol etmek için kullandıkları, özenle korunan telefon numaralarıyla doludur.

Bu numaralardan, telefon beleşçileri argosunda *hat çeviren* olarak bilinen bir tanesi özellikle çok kullanışlıydı. Telefon beleşçileri, kendileri tek kuruş para ödemeden, konuşacak başka telefon beleşçileri bulmak için bunu kullanırlardı. Bu numara aynı zamanda, örneğin bir bankaya vermek üzere, geri arama numarası yaratmak için de kullanılırdı. Bir toplum mühendisi bankadaki birine ona ofisinden ulaşılabileceğini söyleyerek bu numarayı verirdi. Banka, numarayı kontrol etmek üzere telefon ettiğinde (hat çevirme), telefon beleşçisi telefona cevap verebilir, izi sürülemeyecek bir telefon numarası kullanmanın sağladığı korumadan da yararlanmış olurdu.

Bir *Deneme Numaraları Rehberi*, bilgiye aç ve testosteronu tavana vurmuş herhangi bir telefon beleşçisi tarafından kullanılabilecek bir sürü harika bilgi içerir. Bu yüzden her yıl yeni rehberler çıktığında, hobileri telefon ağını keşfetmek olan bir yığın genç derhal bu rehberlerin peşine düşer.

Stevie'nin Oyunu

Telefon şirketleri doğal olarak bu kitapçıkları kolay ulaşılabilir yerlere koymaz, bu yüzden telefon beleşçilerinin bir tane elde edebilmeleri için yaratıcı olmaları gerekir. Bunu nasıl yaparlar? Kafasını rehberi ele geçirmeye takmış hevesli bir genç aşağıdaki gibi bir oyun oynayabilir.

Bir gün, güney California sonbaharının serin akşamlarından birinde, kendisine Stevie diyeceğimiz biri; küçük bir telefon şirketinin genel müdürlüğünü arar. Hizmet bölgesi içerisindeki tüm evlere ve iş yerlerine telefon hatları da bu binadan dağılmaktadır.

Görev başındaki teknisyen telefonu açtığında, Stevie telefon şirketinin basılı malzemelerini basıp dağıtan bölümünde çalıştığını açıklar. "Yeni Deneme Numaraları Rehberiniz hazır," der. "Ancak güvenlik gerekçeleriyle eskisini geri almadan yenisini veremiyoruz. Dağıtımcımızın işi de oldukça uzadı. Eğer sizdeki rehberi kapınızın önüne bırakabilirseniz, geçerken eskisini alıp yenisini bırakabilir, sonra da kendi işine bakar."

Hiçbir şeyden kuşkulanmayan teknisyen bunun uygun olduğunu düşünmüş olmalıdır ki, isteneni tam olarak yapar. Kapağında büyük kırmızı harflerle, "GİZLİDİR VE ŞİRKET İÇİ KULLANIM İÇİNDİR-İHTİYAÇ

KALMADIĞI TAKDİRDE, BU BELGE KAĞIT ÖĞÜTME MAKİNASINDA ÖĞÜTÜLMELİDİR," uyarısı bulunan rehberi binanın önüne koyar.

Stevie arabasıyla gelir ve park edilmiş arabaların içinde bekleyen ya da ağaçların arkasına saklanmış polis ya da şirket güvenlik elemanlarına karşı etrafı dikkatle kolaçan eder. Görünürde kimse yoktur. Rahat tavırlarla ihtiyacı olan rehberi alır, arabasına biner ve gider.

İşte size, bir toplum mühendisinin "yalnızca isteyivermek" gibi basit bir yöntemi kullanarak istediklerini ne kadar kolay elde edebildiğini gösteren bir hikâye daha.

Gaz Saldırısı

Bir toplum mühendisliği senaryosunda tehlikede olan yalnızca şirket varlıkları değildir. Bazen kurbanlar şirket müşterileridir. Müşteri hizmet temsilcisi olarak çalışmanın getirdiği sıkıntılar, neşeli anlar ve masum hatalar vardır. Ancak bu hataların bazıları şirket müşterileri için kötü sonuçlar doğurabilir.

Janie Acton'un Öyküsü

Janie Acton, üç yıldan biraz fazla bir süredir, Washington'daki Hometown Elektrik Şirketi'nde müşteri hizmet temsilcisi olarak bir ofis bölmesini işgal etmektedir. Aklı ve çalışkanlığıyla, en iyi müşteri hizmet temsilcilerinden biri olarak görülmektedir.

Söz konusu telefon geldiğinde Şükran Haftası'dır. Arayan şöyle der, *"Ben Eduardo, Faturalama Bölümü'nden. Telefonda bir hanım var, genel müdür yardımcılarından birinin özel kaleminde sekreter. Bir bilgiye ihtiyacı var ve ben bilgisayarımı kullanamıyorum. İnsan Kaynaklarındaki şu kızdan 'SENİ SEVİYORUM' diyen bir e-posta aldım ve ekini açtığımda, bir daha bilgisayarımı kullanamaz oldum. Virüsmüş. Basit bir virüs tarafından avlandım. Herneyse, benim için bazı müşteri bilgilerine bakabilir misin?*

"Elbette," diye yanıtladı Janie. *"Bilgisayarını mı çökertti? Korkunç bir şey bu."*

"Evet."

"Nasıl yardımcı olabilirim?" diye sordu Janie.

Bu noktada saldırgan kendini inanılır kılmak için daha önce yaptığı araştırmalara başvurdu. İstediği bilginin Müşteri Fatura Bilgileri Sistemi denen bir yerde tutulduğunu ve çalışanların bu sisteme ne ad verdiklerini öğrenmişti. *"MFBS'den bir hesap numarasına bakabilir misin?"* diye sordu telefondaki adam.

"Evet, hesap numarası nedir?"

"Numarayı bilmiyorum. İsimden sorgulaman gerekecek."

"Tamam. İsim nedir?"

"Heather Manning." İsmin harflerini kodladı ve Janie de ismi bilgisayara girdi.

"Tamam. Geldi."

"Harika. Hesap geçerli mi?"

"Hı hı; geçerli."

"Hesap numarası nedir?" diye sordu adam.

"Kalemin var mı?"

"Hazırım."

"Hesap numarası, BAZ6573NR27Q."

Adam numarayı tekrarladı, sonra da, *"Hizmet adresi nedir?"* diye sordu.

Kadın ona adresi verdi.

"Telefon numarası nedir?"

Janie nazik bir şekilde o bilgiyi de okudu.

Arayan teşekkür etti, hoşçakal dedi ve telefonu kapadı. Janie beklemedeki aramaya yanıt verdi ve konunun üstünde de hiç durmadı.

Art Sealy'nin Araştırma Projesi

Art Sealy, yazarlar ve işletmeler için araştırma yaparak daha çok para kazanabileceğini öğrenince, küçük yayınevlerine serbest editör olarak çalışmayı bırakmıştı. İşin onu, yasallık ve yasadışılık arasındaki ince çizgiye yaklaştırdığı oranda ücretinin de artabileceğini kısa sürede fark etti. Art, hiç farkında olmadan ve kesinlikle yaptığına bir isim vermeden bir toplum mühendisi olmuştu. Her bilgi simsarının bildiği bütün teknikleri kullanıyordu. Yaptığı işe yönelik doğal bir yeteneğinin olduğu ortaya çıktı. Pek çok toplum mühendisinin başkalarından öğrendiği teknikleri kendi başına keşfediyordu. Bir süre sonra en ufak bir suçluluk duymadan o ince çizgiyi aştı:

Nixon dönemi kabinesiyle ilgili kitap yazan bir adam beni aradı. Nixon'un Hazine Müsteşarı olan William E. Simon'la igili özel bilgilere ulaşabilecek bir araştırmacı arıyordu. Bay Simon artık yaşamıyordu ama yazarın elinde onunla birlikte çalışmış bir kadının adı vardı. Kadının başkentte oturmaya devam ettiğinden de oldukça emindi, ancak adresini bulamamıştı. Kadının adına, en azından rehberde olanlar arasında, kayıtlı bir telefon yoktu. İşte o zaman beni aramıştı. Ona kesinlikle yapabilebileceğimi, sorun olmayacağını söyledim.

Eğer ne yaptığınızı biliyorsanız, çoğunlukla bir-iki telefon görüşmesiyle bulabileceğiniz bir bilgiydi bu. Her yerel hizmet şirketinin bu bilgi-

Mitnick Mesajı:

Bütün toplum mühendisliği saldırılarının, tamamlanmadan farkedilecek kadar karmaşık düzenler içerdiklerini sakın düşünmeyin. Bazıları gir-çık ya da vur-kaç şeklinde çok basit saldırılardır ve . . . kısacası, yalnızca istemek üzerine kuruludurlar.

yi çoğu zaman paylaşacağından emin olabilirsiniz. Doğal olarak biraz zırvalamanız gerekir. Arada bir küçük beyaz yalanlar söylemenin kime ne zararı dokunabilir ki?

İşleri ilginç kılmak için her seferinde farklı bir yöntem kullanmak hoşuma gider.

"Ben yönetim katından bilmem kim," numarası bende hiç şaşmamıştır. "Genel müdür yardımcısı bilmem kimin ofisinden biri şu anda diğer hattâ bekliyor," numarası da iyidir ve bu olayda da işe yaramıştır.

Telefonun diğer ucundaki kişinin işbirliği yapmaya ne kadar eğilimli olduğunu hissedecek kadar toplum mühendisliği içgüdünüzü geliştirmiş olmanız gerekir. Bu kez arkadaş canlısı yardımsever bir hanıma rast geldim. Tek bir görüşmede adresi ve telefon numarasını almıştım. Görev tamamlanmıştı.

Aldatmacanın İncelenmesi

Janie müşteri bilgilerinin ne kadar hassas olduğunu kesinlikle biliyordu. Bir müşterinin bilgilerini başka bir müşteriyle hiçbir zaman paylaşmaz ya da özel bilgileri dışarı vermezdi.

Ancak doğal olarak şirket içinden arayan biri için farklı kurallar geçerliydi. Bir mesai arkadaşı için bu bir takım oyunu meselesiydi ve işi bitirmek karşılıklı yardımlaşmaya dayanıyordu. Faturalamadaki adam eğer bilgisayarı bir virüs yüzünden çökmemiş olsaydı ilgili bilgileri kendi de bulabilirdi; bu yüzden Janie bir iş arkadaşına yardım edebilmiş olmaktan memnundu.

Art, peşinde olduğu kilit bilgilere ulaşırken yavaş yol aldı ve hesap numarası gibi aslında ihtiyacı olmayan şeylerle ilgili sorular da sordu. Ancak, aynı zamanda hesap numarası bilgisi emniyet sübabı görevi de görüyordu. Eğer görevli kuşkulanacak olsaydı, ikinci bir görevliyi arayacaktı ve böylece başarı şansı daha yükselecekti, çünkü hesap numarasını bilmek ulaşacağı bir sonraki görevliye kendini daha da inandırıcı göstermesine yardımcı olacaktı.

Birilerinin bu bilgiler için yalan söyleyebileceği, yani arayanın gerçekte faturalama bölümünden biri olmayabileceği, Janie'nin hiç aklına

gelmemişti. Suç elbetteki Janie'nin değildi. Bir müşteri dosyasındaki bilgileri paylaşmadan önce kiminle konuştuğundan emin olması konusunda kimse onu bilgilendirmemişti. Kimse ona Art'ın yaptığı gibi bir telefon görüşmesinin oluşturabileceği tehlikelerden söz etmemişti. Şirket kuralları arasında da yoktu, eğitimini de almamıştı ve yöneticisi de bundan hiç bahsetmemişti.

Aldatmacanın Engellenmesi

Güvenlik eğitimlerinde aktarılması gereken bir nokta: Telefonla arayan birinin ya da bir ziyaretçinin, şirketteki bazı kişilerin adlarını ya da şirket içi terimleri ya da süreçleri biliyor olması, onun iddia ettiği kişi olduğunu göstermez. Ve bu onu kesinlikle ticari bilgilerin ve bilgisayar sistemine ya da ağına erişim hakkının verilebileceği, yetkili biri durumuna da getirmez.

Güvenlik eğitiminin şunu vurgulaması gerekir: Bir kuşkun varsa, kontrol et, kontrol et, kontrol et.

İlk zamanlarda şirket içinde bir bilgiye ulaşmak bir konum göstergesiydi ve bir ayrıcalıktı. İşçiler kazanları doldururlar, makineleri çalıştırırlar, mektupları yazarlar ve evrakları dosyalarlardı. Ustabaşı ya da patron onlara neyin, ne zaman ve nasıl yapılacağını söylerdi. Bir vardiyada her işçinin kaç alet yapacağını; bu haftayı, gelecek haftayı ve ayın sonunu çıkarmak için fabrikanın hangi boyut ve renklerde ve kaç tane alet üretmesi gerektiğini ustabaşı ya da patron bilirdi.

İşçiler makineleri, araç ve gereçleri; patronlar ise bilgiyi kullanırlardı. İşçilerin yalnızca, yaptıkları işe özgü bilgilere ihtiyaçları vardı.

Günümüz tablosu biraz farklı, öyle değil mi? Pek çok fabrika işçisi bir çeşit bilgisayar ya da bilgisayarla çalışan makine kullanmaktadır. Sorumluluklarını yerine getirerek işleri yürütebilmeleri için, hassas bilgiler iş başındaki kullanıcıların bilgisayarlarına kadar iner. Bu durum iş gücünün büyük çoğunluğu için aynıdır. Bugünün ortamında çalışanların yaptığı neredeyse her şey bilgi kullanımını içermektedir.

Bu yüzden şirket güvenlik kurallarının konumdan bağımsız olarak tüm kurum içine dağıtılması gerekmektedir. Bir saldırganın peşinde olduğu bilgilere yalnızca amirlerin ve üst yöneticilerin sahip olmadığını herkesin anlaması şarttır. Bugün her düzeydeki çalışanlar, hattâ bilgisayar kullanmayanlar bile, hedef olmaya açıktırlar. Müşteri hizmetleri bölümünde işe yeni başlamış bir müşteri temsilcisi, bir toplum mühendisinin amacına ulaşmak için kırmak isteyeceği zayıf halka olabilir.

Güvenlik eğitimi ve şirket güvenliği kuralları bu halkayı güçlendirmelidir.

GÜVEN UYANDIRMAK

Bu öykülerden bazıları, iş dünyasındaki herkesin süzme salak olduğuna ve mesleğiyle ilgili her sırrı dışarı vermeye hazır, hattâ istekli olduğuna inandığımı düşünmenize neden olabilir. Toplum mühendisi bunun doğru olmadığını bilir. Neden toplum mühendisliği saldırıları bu kadar başarılı oluyor? İnsanlar salak ya da sağduyusuz olduğu için değil. Ancak bizler aldatılmaya fazlasıyla açığız, çünkü insanlar belli şekillerde yönlendirilirlerse yanlış şeylere güven duyabiliyorlar.

Toplum mühendisi, karşı taraftan kuşku ve direniş bekler ve her zaman güvensizliği güvene dönüştürmeye hazırdır. İyi bir toplum mühendisi, saldırısını bir satranç oyunu gibi planlar ve doğru yanıtları verebilmek için hedefinin sorabileceği soruları önceden tahmin eder.

En çok kullanılan yöntemlerden biri, kurbanda güven duygusu uyandırmaktır. Bir dolandırıcı ona inanıp güvenmenizi nasıl sağlayabilir ki? İnanın bana, bunu yapabilir.

Güven: Aldatmanın Anahtarı

Bir toplum mühendisi, kurduğu iletişimi ne kadar olağan bir işmiş gibi gösterebilirse, oluşan şüpheleri de o kadar kolay bastırabilir. İnsanların kuşkulanmak için bir nedenleri olmazsa, toplum mühendisinin, onların güvenini kazanması daha kolay olur.

Bir kez güvenlerini kazandıktan sonra, köprü iner ve kalenin kapıları ardına kadar açılır. Böylece toplum mühendisi içeri girip istediği bilgiyi alabilir.

Not: *Öykülerin çoğunda, toplum mühendislerine, telefon beleşçilerine ve dolandırıcılara bir erkekmiş gibi gönderme yaptığım dikkatinizi çekmiş olabilir. Bu şovenizm değildir; yalnızca, bu alanlarda çalışanların çoğunun erkek olduğu gerçeğini vurgular. Her ne kadar çok fazla kadın toplum mühendisi olmasa da, sayıları giderek artmaktadır. Dışarıda, sadece telefonda bir kadın sesi duyduğunuz için yelkenleri suya indirmemenizi sağlamaya yetecek kadar çok dişi toplum mühendisi vardır. Doğrusunu isterseniz, kadın toplum mühendisleri, işbirliği sağlamak için cinselliklerini kullanabildiklerinden, belirgin bir üstünlükleri de yok değildir. Bu sayfalarda bu kadınların birkaçından söz edildiğini de göreceksiniz.*

İlk Görüşme: Andrea Lopez

Andrea Lopez, çalıştığı video kiralama mağazasında çalan telefona baktı ve kısa bir süre sonra gülümsemeye başladı. Bir müşterinin işini gücünü bırakıp hizmetten ne kadar memnun kaldığını söylemek için aradığını duymak gibisi yoktu. Bu arayan, mağazayla iş yapmaktan çok memnun kaldığını ve yöneticiye bir mektup göndermek istediğini söylemişti.

Yöneticinin adını ve adresini sormuş, Andrea da ona yöneticinin adının Tommy Allison olduğunu söylemiş ve adresi vermişti. Arayan tam telefonu kapayacakken aklına başka bir şey gelmiş ve,

- *Şirket genel müdürlüğüne de birkaç satır yazabilirim. Mağaza kodunuz nedir,* diye sormuştu. Kadın ona mağaza kodunu da verdikten sonra adam teşekkür etmişti. Kendisine çok yardımcı olduğu için görevliye güzel bir şeyler daha söyledikten sonra iyi günler dileyerek telefonu kapatmıştı.

"Böyle bir telefon, her zaman mesainin daha hızlı geçmesini sağlıyor. İnsanlar bunu daha sık yapsalar ne kadar güzel olur." diye düşünmüştü Andrea.

İkinci Görüşme: Ginny

- *Studio Video'yu aradığınız için teşekkürler. Ben Ginny, nasıl yardımcı olabilirim?*

- *Merhaba, Ginny,* dedi arayan, heyecanla. Sesi Ginny'le daha önce her hafta konuşmuş gibi geliyordu.

- *Ben Tommy Allison, Forest Park, 863 kodlu mağazanın müdürü. Burada Rocky V'i kiralamak isteyen bir müşterimiz var ve bizdeki tüm kopyalar dışarıda. Sende olup olmadığına bakabilir misin?*

Ginny biraz sonra yeniden telefonu eline aldı ve,

- *Evet, bizde üç kopya var,* dedi.

- *Tamam. Müşteriye oraya gidip gidemeyeceğini soracağım. Teşekkür ederim. Eğer bizim mağazadan bir şeye ihtiyacın olursa, arayıp Tommy'i istemen yeterli. Senin için elimden geleni yapmaktan memnun olacağım.*

Sonraki birkaç hafta boyunca Tommy, bir takım konularda yardım etmesi için Ginny'i üç-dört kere daha aradı. İstekleri mantıklı şeylerdi ve kendisine asıldığı duygusunu uyandırmadan her zaman Ginny'e arkadaşça davranıyordu. Arada biraz gevezelik de ediyordu. *"Oak Park'taki büyük yangını duydun mu? Bir sürü yolu kapatmışlar"* gibi şeylerden söz ediyordu. Bu aramalar günün durağanlığından biraz uzaklaşma fırsatı tanıyordu ve Ginny onun aramasından her zaman memnun kalıyordu.

Bir gün Tommy'nin sesi gergindi.

- *Sizin bilgisayarda bir sorun var mı?* diye sordu.

- *Hayır,* diye yanıtladı Ginny.

- *Neden?*

- *Adamın biri arabasını bir telefon direğine çarpmış. Telefon şirketinden gelen tamircinin söylediğine göre şehrin bu bölgesi onarım tamamlanana kadar telefonlarını ve internet bağlantılarını kullanamayacakmış.*

- *Oh, çok kötü. Adam yaralanmış mı?*

- *Cankurtaranla götürdüler. Her neyse biraz yardımını isteyebilirim. Burada Godfather II'yi kiralamak isteyen bir müşteriniz var ve kredi kartı yanında değil. Bilgileri benim için kontrol edebilir misin?*

- *Elbette.*

Tommy müşterinin adını ve adresini verir. Ginny de adamı bilgisayardan bulup, müşteri numarasını Tommy'e söyler.

- *Geç getirmeleri ya da mağazaya borcu var mı?"* diye sorar Tommy.

- *Görünen bir şey yok.*

- *Tamam, harika. Ona burada kağıt üzerinde bir müşteri numarası vereceğim. Daha sonra bilgisayarlarımız yeniden çalışmaya başladığında veritabanımıza da eklerim. Ödemesini sizin mağazada kullandığı kredi kartıyla yapmak istiyor ama kartı yanında değilmiş. Kart numarası ve son kullanma tarihi nedir?*

Ginny son kullanma tarihiyle birlikte kart numarasını da ona verir.

- *Yardımın için teşekkürler. Yakında görüşürüz,* der Tommy ve telefonu kapatır.

Doyle Lonnegan'ın Öyküsü

Lonnegan, kapınızı açtığınızda karşınızda görmek isteyeceğiniz türden bir adam değil. Bir zamanlar ödenmeyen kumar borçlarını toplama işini yapan Doyle Lonnegan, kendi başını belaya sokmadığı sürece, arada bir birilerine yardım etmeyi de sürdürmekteydi. Bu olayda, bir video mağazasını birkaç kez telefonla araması için ona hatırı sayılır bir miktar para önerilmişti. Kulağa oldukça kolay geliyordu. Sorun "müşterilerinden" hiçbirininin böyle bir dolabın nasıl çevrileceğini bilmemesinden kaynaklanıyordu. Lonnegan'ın yeteneğine ve bilgisine sahip birine ihtiyaçları vardı.

İnsanlar poker masasında şanssız olduklarında ya da saçmaladıklarında bahislerini karşılamak için çek yazmazlar. Bunu herkes bilir. Benim arkadaşlarım, elindeki parayı masaya koymayan bir üçkağıtçıyla neden sürekli kumar oynarlar ki? Sormayın. Belki de kafalarında birkaç tahta eksiktir. Ama onlar benim arkadaşlarım; elden ne gelir?

Adamın parası yokmuş; bu yüzden de çek almışlar. Şu işe bakın! Onu alıp bir ATM'ye götürmeliydiler. Yapmaları gereken şey buydu. Ama hayır; çek aldılar. Hem de tam 3.230 dolarlık!

Doğal olarak, çek karşılıksız çıktı. Ne bekliyordunuz ki? O zaman beni aradılar; yardım edebilir miymişim? Üzerlerine kapı kapayarak insanların ellerini ezme işini artık bıraktım. Dahası artık çok daha iyi yöntemler var. Yüzde 30 komisyon alarak, onlara elimden geleni yapacağımı söyledim. Böylece bana adamın adını ve adresini verdiler ve ben de bilgisayardan ona en yakın video kiralama mağazasının neresi olduğuna baktım.

Çok acelem yoktu. Mağaza müdürünü hoş tutmak için dört telefon görüşmesi yapmış ve sonra, hop, üçkağıtçının kredi kartı numarasını alıvermiştim.

Başka bir arkadaşım yarı çıplak kızların dans ettiği bir bar işletiyordu. Elli dolar karşılığında adamın poker parasını bardaki POS makinasından çekti. Bakalım üçkâğıtçı bunu karısına nasıl açıklayacak? Bankaya bu harcamanın kendisine ait olmadığını söyleyeceğini mi düşünüyorsunuz? Bir daha düşünün. Bizim onu çok iyi tanıdığımızı biliyor. Ve eğer kredi kartı numarasına ulaşabiliyorsak, bunun yanısıra daha pek çok şeye de ulaşabileceğimizi anlayacaktır. İşin o tarafında endişelenecek hiçbir şey yok.

Aldatmacanın İncelenmesi

Tommy'nin Ginny'le yaptığı ilk konuşmalar tamamen güven uyandırmaya yönelikti. Asıl saldırı zamanı geldiğinde, kadın savunmaya geçmemiş ve Tommy'i iddia ettiği kişi, yani zincirdeki başka bir mağazanın müdürü olarak kabul etmişti.

Hem neden kabul etmesin ki; onu zaten tanıyordu. Doğal olarak onunla yalnızca telefonda görüşmüştü ama güven duymasını sağlayacak kadar bir iş arkadaşlığı yapısı kurulmuştu. Kadın onu bir kez bir müdür, aynı şirkette çalışan bir yönetici olarak gördükten sonra istenen güven sağlanmış ve gerisi tereyağından kıl çeker gibi olup bitmişti.

Mitnick Mesajı:

Belalılar (The Sting) filmindeki güven uyandırma tekniği toplum mühendislerinin en etkili taktiklerinden biridir. Konuştuğunuz kişiyi gerçekten tanıyıp tanımadığınızı düşünmeniz gerekir. Az da olsa bazı durumlarda karşı taraftaki söylediği kişi olmayabilir. Bu nedenle hepimizin düşünmesi, incelemesi ve yetkili olduğunu söyleyenleri sorgulamayı öğrenmesi gerekmektedir.

Konuya Farklı Bir Bakış: Kredi Kartı Ele Geçirme

Güven duygusu uyandırmak, bir önceki hikâyede anlatıldığı gibi, her zaman bir dizi telefon görüşmesi yapmayı gerektirmez. Bunun topu topu beş dakika tuttuğu bir olay hatırlıyorum.

Sürpriz!

Bir keresinde bir lokantada Henry ve babasıyla birlikte oturuyordum. Sohbet sırasında Henry, kredi kartı numarasını telefon numarası gibi sağa sola verdiği için babasına kızdı. *"Bir şey alırken tabi ki kart numaranı vereceksin"* dedi. *"Ama kart numaranı, onu kayıtlarında tutan bir mağazaya vermek; bu çok aptalca."*

"Bunu yaptığım tek yer Studio Video" dedi Bay Conklin, aynı video kiralama mağazaları zincirinin adını vererek. *"Ama fazla para çekişi var mı diye her ay kredi kartı ekstremi kontrol ediyorum."*

"Elbette anlardın" dedi Henry, *"ama kart numaranı onlara bir kere verdin mi, numarayı birinin çalması işten bile değil."*

"Kötü niyetli bir çalışan gibi mi?"

"Hayır, herhangi biri; sadece çalışanlar değil."

"Saçmalıyorsun" dedi Bay Conklin.

"Şimdi onları arayıp, bana senin Visa numaranı vermelerini sağlayabilirim" diye hemen atıldı Henry.

"Hayır, bunu yapamazsın" dedi babası.

"Beş dakika içinde yapabilirim, hem de tam burada, karşında. Masayı hiç terk etmeden."

Bay Conklin gözlerini kısmış ona bakıyordu. Kendinden emin olup da bunu göstermek istemeyen birinin havası vardı. *"Sen ne söylediğinin farkında değilsin"* diyerek güldü ve cüzdanını çıkarıp içinden çıkardığı bir elli dolarlık banknotu masaya çarptı. *"Eğer söylediğini yapabilirsen, şu senin."*

"Paranı istemiyorum baba" dedi Henry.

Cep telefonunu çıkardı, babasına hangi mağazayı kullandığını sordu ve oranın telefon numarasının yanısıra Sherman Oaks yakınlarındaki mağazanın telefonunu da öğrenmek amacıyla Bilinmeyen Numaralar'ı aradı.

Sonra Sherman Oaks'daki mağazayı aradı. Önceki öyküde anlatılan yaklaşıma oldukça yakın bir yöntem kullanarak, hemen müdürün adını ve mağazanın kodunu öğrendi.

Sonra da babasının müşterisi olduğu mağazayı aradı. müdürün adını

kendi adıymış gibi kullanıp, az önce elde ettiği mağaza kodunu da vererek, herkesin bildiği *yönetici ayağına yatma* numarasını çekti. Ve aynı oyunu yaptı. *"Bilgisayarlarınız düzgün çalışıyor mu? Bizimkiler gidip geliyor."* Karşı tarafın yanıtını dinledi ve sonra, *"Sizin müşterilerden biri buradan bir video kiralamak istiyor ama bizim bilgisayarlar şu anda çökmüş durumdalar. Müşteri numarasına bakıp mağazanızın müşterisi olup olmadığını kontrol etmenizi rica edebilir miyim?"* diye sordu.

Henry karşı tarafa babasının adını verdi. Ardından yöntemde küçük bir değişiklik yaparak, adresi, telefon numarasını ve müşteri numarasının verildiği tarihi de okumasını istedi. Sonra da, *"Burada bekleyen bir yığın müşterim var. Kredi kartı numarası ve son kullanma tarihi nedir?"* diye sordu.

Henry bir eliyle cep telefonunu kulağında tutarken diğer eliyle peçetenin üzerine numarayı yazdı. Konuşmayı bitirirken peçeteyi babasının önüne doğru itti. Babası ise ağzı açık bakakalmıştı. Zavallı adam tamamen şok olmuştu; sanki tüm emniyet hissi bir darbede yıkılıp gitmişti.

Aldatmacanın İncelenmesi

Tanımadığınız biri sizden bir şey istediği zaman kendi vereceğiniz tepkiyi düşünün. Pejmürde görünümlü bir yabancı kapınıza geldiğinde onu içeri alma olasılığınız düşüktür; eğer iyi giyimli, ayakkabıları boyalı, saçları taralı, nazik tavırlı ve gülümseyen bir yabancı kapınıza gelirse, herhalde o kadar şüpheci olmazsınız. Belki de gelen aslında Onüçüncü Cuma filmlerinden çıkmış Jason'dır, ama olağan görünümlü ve elinde keskin bir bıçak taşımayan biri varsa karşınızda işe ona güvenerek başlarsınız.

Bu kadar belirgin olmamakla birlikte telefonda konuştuğumuz insanlar hakkında da benzer bir şekilde hüküm veririz. Bu kişi bana bir şeyler mi satmaya çalışıyor? Arkadaşça ve açık mı davranıyor yoksa bir baskı ve saldırganlık seziyor muyum? Eğitimli biri gibi mi konuşuyor? Tüm bunları ve farkında olmadan bir düzine başka şeyi daha, göz açıp kapayıncaya kadar, konuşmanın ilk anlarında tartıveririz.

İşteyken insanlar sürekli bizden bir şeyler isterler. Bu adamın e-posta adresi sende var mı? Müşteri listesinin en son şekli nerede? Projenin bu kısmının taşeronu kim? Bana en son proje güncellemesini gönderir misin lütfen. Kaynak kodun yeni sürümüne ihtiyacım var.

Ve tahmin edin ne olur: Bu istekleri aldığınızın insanlar bazen şahsen tanımadığınız kişiler, şirketin başka bir bölümünde çalışan ya da orada çalıştıklarını söyleyen şahıslar olurlar. Ama eğer verdikleri bilgi doğruysa ve konu üzerinde bilgili gibi görünüyorlarsa ("Marianne dedi ki . . ."; "Dosya K-16 sunucusundaymış . . ."; "Yeni ürün planlarının 26

Mitnick Mesajı:

Aksi yönde düşünmemizi gerektirecek bir şey yoksa, kurduğumuz herhangi bir iletişimde kandırılma olasılığımızın düşük olduğunu düşünmek insan doğasının bir gereğidir. Riskleri tartarız sonra da çoğu zaman insanlara güvenmeyi tercih ederiz. Medeni insanların davranış biçimi budur...en azından daha önce hiç dolandırma, yönlendirme ve kandırma yoluyla büyük paralar kaptırmamış olan medeni insanlar için.

Çocukken anne-babamız bize yabancılara güvenmememizi öğretmişlerdi. Belki de bu eski nasihati bugünün iş ortamlarında hepimiz hatırlamalıyız.

numaralı tashihi . . ."), güven çemberimizi, onları da içine alacak şekilde genişletiriz ve hiç endişe duymadan istediklerini onlara veririz.

Arada bir duralayıp, kendi kendimize, "Dallas fabrikasından biri neden yeni ürün planlarını görmeye ihtiyaç duysun ki?" ya da "Hangi sunucuda olduğunu söylemek herhangi bir şeye zarar verir mi ki?" diye sorabiliriz. Böyle bir-iki soru daha sorarız. Eğer yanıtlar mantıklı görünür ve karşı tarafın tavrı da güven verici olursa kuşkulanmayı bırakır, karşımızdaki adama ya da kadına güvenme yolundaki doğal eğilimimize geri döneriz. Makul sınırlar içerisinde, bizden istenen neyse onu yaparız.

Bir an için bile saldırganın yalnızca şirket bilgisayar sistemlerinde çalışan kişileri hedefleyeceğini düşünmeyin. Ya haberleşme bürosundaki adam ne olacak? "Bana bir iyilik yapar mısın? Bunu şirket içi kurye torbasına atabilir misin?" Haberleşme odasında çalışan memur torbaya attığı şeyin, içine genel müdürün sekreteri için özel olarak hazırlanmış küçük bir program kaydedilmiş bir disket olduğunu biliyor mudur acaba? Artık saldırgan, genel müdürün e-postalarının bir kopyasını da kendine alabilecektir. İnanılmaz! Bu gerçekten sizin şirketinizde de olabilir mi? Neden olmasın?

Bir Sentlik Cep Telefonu

Pek çok insan bir mal alacakları zaman daha ucuzunu bulana kadar araştırırlar; toplum mühendisleri ise daha ucuzunu aramazlar, bir ürünün fiyatını daha aşağı çekmenin yollarını ararlar. Örneğin bazen bir şirket öyle bir pazarlama kampanyası düzenler ki göz ardı edemezsiniz. Buna karşın toplum mühendisi teklifi inceler ve bu alışverişten nasıl daha kazançlı çıkabileceğine bakar.

Bir süre önce, ülke çapında iş yapan bir GSM operatörü büyük bir promosyon yapmıştı. Şirketin tarifelerinden bir tanesine abone olduğunuzda bir sent ödeyerek yeni bir cep telefonuna sahip oluyordunuz.

Birçok insanın oldukça geç farkettiği üzere, bir cep telefonu tarifesine abone olmadan önce dikkatli bir müşterinin sorması gereken bir yığın soru vardır. Hizmetin analog, dijital ya da her ikisi birden olup olmadığı; sabit ücretlerin ne kadar olduğu gibi sorular. İşin başından, abonelik taahhüdü süresinin ne kadar olduğunun bilinmesi özellikle önemlidir. Yani, kaç ay ya da yıl abone kalmanız gerekecek?

Philadelphia'da oturan bir toplum mühendisini hayal edin. Bir cep telefonu şirketinin abone olunduğunda vereceğini söylediği ucuz cep telefonunu çok beğenmiş, ancak telefonla birlikte sattıkları tarifeden hiç hoşlanmamış. Sorun değil. İşte bu işi kotarmanın yollarından biri.

İlk Görüşme: Ted

Toplum mühendisi ilk iş olarak, bir elektronik eşya mağazalar zincirinin West Girard'daki mağazasına telefon eder.

- *Electron City. Ben Ted.*

- *Merhaba, Ted. Ben George. Birkaç gün önce bir cep telefonuyla ilgili olarak bir satış görevlisiyle konuşmuştum. Hangi tarifeyi istediğime karar verdiğimde onu arayacağımı söylemiştim ama adını unuttum. O bölümde akşam mesaisinde çalışan adamın adı nedir?*

- *Birden fazla kişi var. William olabilir mi?*

- *Emin değilim. Belki de William'dır. Görünüşü nasıl?*

- *Uzun boylu. Zayıfça.*

- *Sanırım o. Soyadı ne demiştin?*

- *Hadley. H-A-D-L-E-Y.*

- *Tamam, oydu. Ne zaman orada olacak?*

- *Bu haftaki mesai çizelgesini bilemiyorum ama akşamcılar beş gibi gelirler.*

- *Çok iyi. Onu bu gece bulmaya çalışırım o zaman. Teşekkürler, Ted.*

İkinci Arama: Katie

Bir sonraki görüşme, aynı mağazalar zincirinin North Broad Caddesi'ndeki mağazasıyla yapılır.

- *Merhaba, Electron City. Ben Katie, size nasıl yardımcı olabilirim?*

- *Katie, merhaba. Ben William Hadley, West Girard mağazasından. İşler nasıl bugün?*

- *Biraz yavaş. Ne oldu?*

- *Şu bir sentlik cep telefonu promosyonu için gelmiş bir müşterim var. Hangisini kastettiğimi biliyorsun değil mi?*

- *Biliyorum. Geçen hafta onlardan birkaç tane sattım.*

- O promosyon kapsamındaki telefonlardan elinde daha var mı?

- Bir yığın.

- Harika, çünkü az önce bir müşteriye ondan bir tane sattım. Adam kredi kartıyla ödedi; kontratı da imzaladık. Sonra depoya baktım ki elimizde hiç telefon kalmamış. Çok malıçup oldum. Bana bir iyilik yapabilir misin? Telefonu almak için müşteriyi sizin mağazaya göndereceğim. Ona bir sent karşılığında telefonu satıp, fatura düzenler misin? Bir de, nasıl programlayacağını anlatabilmem için, telefonu aldıktan sonra beni araması gerekiyor.

- Elbette. Gönder onu buraya.

- Tamam. Adı Ted. Ted Yancy.

Adının Ted Yancy olduğunu söyleyen bir adam North Broad Caddesi mağazasına geldiğinde, Katie bir fatura düzenler ve adama bir sent karşılığında cep telefonunu satar. Her şey "mesai arkadaşının" ondan rica ettiği şekilde gelişir. Kadın zokayı yutmuştur.

Ödeme zamanı geldiğinde müşterinin cebinde hiç bozuk para yoktur. Bu yüzden kasada bir sentlerin durduğu küçük bölmeye uzanır, bir tane alır ve ödeme yaparken bunu kadına verir. Telefonu bir senti bile ödemeden almıştır.

Artık aynı marka telefonu kullanan başka bir GSM operatörüne gitmekte ve istediği tarifeyi seçmekte özgürdür. Tercihen hiçbir taahhüt gerektirmeyen aydan aya bir tarife seçecektir.

Aldatmacanın İncelenmesi

Çalışan olduğunu öne süren ve şirket içi süreçleri ve terimleri bilen kişilere karşı insanların daha yüksek bir güven duyması doğaldır. Bu hikâyedeki toplum mühendisi, promosyonlarla ilgili ayrıntıları öğrenerek, kendini bir şirket çalışanı olarak tanıtmış ve başka bir şubeden bir kolaylık yapmasını rica ederek bundan yararlanmıştır. Böyle şeyler perakende zincirlerinin farklı mağazaları arasında ve bir şirketin farklı birimleri arasında olur. İnsanlar farklı ortamlardadırlar ve hiç karşılaşmadıkları mesai arkadaşlarıyla sürekli beraber çalışırlar.

Federal Ajanlar'ın Ağlarına Girmek

İnsanlar, kurumlarının internet üzerinde neleri tuttuğunu şöyle bir durup düşünmezler. Los Angeles, KFI Talk Radyosu'ndaki haftalık programım için yapımcı, internet üzerinde bir tarama yapmış ve Ulusal Suç Bilgileri Merkezi'nin veri tabanına erişmek için kullanılan USBM kılavuzunun bir kopyasını elde etmişti. Bu kılavuzun içinde FBI'ın ulusal suç veritabanından bilgi almaya yönelik tüm açıklamalar bulunuyordu. Yapımcı daha sonra internet üzerinde veri tabanının kendisini de bulmuştu.

Bu kılavuz, ulusal veri tabanından suç ve suçlulara yönelik bilgi çekebilmek için kullanılacak biçemleri ve komutları içeren, emniyet teşkilatı için hazırlanmış bir el kitabıdır. Ülke çapındaki tüm emniyet birimleri, kendi yetki bölgeleri içerisinde suçluları yakalamalarına yardımcı olması için aynı veri tabanından sorgulama yapabilirler. Kılavuz, dövmelerden tutun da, gemi omurgalarına ve çalıntı para ve senetlerin nominal değerlerine kadar, veri tabanı içerisinde herhangi bir şey için kullanılan kodları da kapsıyordu.

Kılavuza erişebilen biri ulusal veri tabanından bilgi çekebilmek için gerekli biçemlere ve komutlara bakabilir. Sonra da süreçler kılavuzundaki açıklamaları izleyerek, biraz da cesareti varsa, veri tabanından bilgi çekebilir. Kılavuzda ayrıca sistemi kullanırken danışabileceğiniz telefon numaraları da vardır. Sizin şirketinizde de ürün kodlarını ya da hassas bilgilere erişim kodlarını içeren benzer el kitapları olabilir.

FBI hassas kılavuzlarının ve süreç bilgilerinin internete bağlanabilen herkese açık olduğunu kesinlikle hiç fark etmedi. Eğer durumu bilselerdi bundan memnun kalacaklarını da pek sanmıyorum. Bir kopyası Oregon'daki bir devlet dairesi tarafından, bir diğeri de Texas'daki bir emniyet bürosu tarafından internete konmuştu. Neden? Herhalde birileri, bu bilginin önemli olmadığını ve onu internete koymanın bir zararının olmayacağını düşünmüştü. Belki de biri, kendi çalışanlarına kolaylık olması için onu intranete koymuştu. Bunu yapan, veri tabanını, internet üzerinde, Google gibi iyi bir arama motoruna erişimi olan, aralarında meraklıların, polis olma heveslilerinin, bilgisayar korsanlarının ve organize suç patronlarının da bulunduğu bir sürü insana açtığını hiçbir zaman fark etmemiştir.

Sisteme Açılmak

Böyle bir bilgiyi kamuda ya da özel sektörde çalışan bir kişiyi kandırmada kullanmanın kuralı aynıdır. Belirli veri tabanlarına ve uygulamalara nasıl erişileceğini, bir şirketin bilgisayar sunucularının adlarını ya da bunun gibi şeyleri bildiği için toplum mühendisi, inandırıcılığını artırır. İnandırıcılık ise güven doğurur.

Toplum mühendisinin elinde böyle kodlar olduktan sonra istediği bilgiyi elde etmesi kolay bir süreçtir. Örnek vermek gerekirse, bir yerel emniyet müdürlüğünün teleks bürosundaki bir memuru arayıp kılavuzdaki komutlardan biriyle ilgili bir soru sorarak işe başlayabilir. Örneğin işlenen suçlar koduyla ilgili birşey sorabilir. "USBM'de bir OFF sorgulaması yaptığımda, 'Sistem Arızalı' mesajı veriyor. Siz de OFF sorgulaması yaptığınızda aynı mesajı alıyor musunuz? Benim için deneyebilir misiniz?" Bundan başka belki bir AKD -aranan kişi dosyası için polisler arasında kullanılan kısaltma- aradığını da söyleyebilirdi.

Telefonun diğer ucundaki teleks memuru, arayanın USBM veritaba-

nın çalışma süreçlerine ve arama komutlarına aşina olduğu mesajını alacaktır. USBM kullanma konusunda eğitilmiş biri dışında başka kim bu süreçleri bilebilir ki?

Memur, sistemin düzgün çalıştığını doğruladıktan sonra, konuşma şöyle devam edebilir:

"Biraz yardıma ihtiyacım var."

"Ne arıyordun?"

"Martin Reardon adına bir OFF komutu çalıştırmanı isteyeceğim. Doğum tarihi 18/10/66."

"SOS nedir?" (ABD Emniyet teşkilatı çalışanları Sosyal Güvenlik Numarası'na bazen kısaca SOS derler.)

"700-14-7435."

Listeye baktıktan sonra, memur şöyle bir sonuç elde edebilir, "2602'si varmış."

Sayının anlamını öğrenmek için saldırganın çevrim içi USBM'ye bakması yeterli olacaktır: Adamın sicilinde bir dolandırıcılık suçu vardır.

Aldatmacanın İncelenmesi

Başarılı bir toplum mühendisi, USBM veri tabanına girmenin yollarını bulmakta hiç zorlanmaz. İstediği bilgiyi almak için tek yapması gereken, yerel emniyet müdürlüğüne bir telefon açıp, içerden biriymiş gibi ikna edici bir şekilde konuşmakken, neden tereddüt etsin ki? Her seferinde başka bir polis bürosunu arayıp aynı bahaneyi öne sürebilir.

Emniyet müdürlüklerini, karakolları ya da trafik şubelerini aramanın riskli olup olmadığını merak edebilirsiniz. Saldırgan kendini büyük bir risk altına sokmuyor mu?

Cevap: hayır. Ve bunun da bir nedeni var. Tıpkı ordu mensuplarına olduğu gibi, emniyet teşkilatı çalışanlarına da, rütbeye saygı kavramı akademideki ilk günlerinden beri yoğun bir şekilde benimsetilmiştir. Toplum mühendisi, bir komiser, komiser yardımcısı ya da konuştuğu kişiden daha yüksek rütbeli biri gibi davranırsa; kurban, üstlerinin sözlerini sorgulamaması gerektiğini söyleyen, iyi işlenmiş bir dersin etkisiyle hareket edebilecektir. Diğer bir deyişle, rütbenin, özellikle de alt rütbeliler tarafından sorgulanmamak gibi yararları vardır.

Terimler

SOS: Sosyal güvenlik numarası için ABD emniyet teşkilatında kullanılan gayriresmi kısaltma.

Ancak emniyet teşkilatının ve ordunun, bir toplum mühendisinin rütbeye olan saygıyı sömürülebileceği tek yer ol-

duğunu düşünmeyin. Bu sayfalarda geçen birkaç öyküde de göreceğiniz gibi, toplum mühendisleri, şirketlere yaptıkları saldırılarda da kurum içi unvan ve yetki makamlarını sık sık kullanırlar.

Aldatmacanın Engellenmesi

Toplum mühendislerinin, çalışanlarınızın insanlara güvenmeye yönelik doğal eğilimlerinden yararlanma olasılığını düşürmek için, kuruluşunuz ne gibi önlemler alabilir? İşte size birkaç öneri.

Müşterilerizi Koruyun

İçinde bulunduğumuz bilgi çağında müşteriye doğrudan satış yapan pek çok şirket, kredi kartı numaralarını bir dosyada tutmaktadır. Bunun çeşitli nedenleri vardır: Alışveriş yapmak için mağazayı ya da internet sitesini her ziyaret edişinde, müşteriyi kredi kartı bilgilerini yeniden verme sıkıntısından kurtarır. Ancak bu uygulamadan vazgeçilmelidir.

Eğer kredi kartı numaralarını bir dosyada tutmanız gerekiyorsa, şifreleme ve erişim sınırlamalarının ötesine çıkan güvenlik koşullarının bu işleme eşlik etmesi şarttır. Çalışanların, kitabın bu bölümde anlatılan türden toplum mühendisliği oyunlarını tespit edebilecek şekilde eğitilmeleri de gerekmektedir. Telefonda iyi ahbaplık kurduğunuz ama şahsen karşılaşmadığınız mesai arkadaşınız, aslında söylediği kişi olmayabilir. Hassas müşteri bilgilerine nasıl erişileceğini o kadar da bilmesi gerekmiyor olabilir, çünkü aslında şirket için çalışmıyordur.

Kime Güveneceğinizi Bilin

Müdahalelere karşı uyanık olması gerekenler, yalnızca yazılım mühendisleri, Ar-Ge çalışanları ve bunun gibi hassas bilgilere erişimi olan kişiler değildir. Kuruluşunuzdaki neredeyse herkes, kurumu sanayi casuslarına ve bilgi hırsızlarına karşı korumaya yönelik olarak eğitilmelidir.

Böyle bir çalışmanın başlangıcında, kurum çapında bilgi varlıkları incelenmeli; her bilgi, hassaslığı, ciddiyeti ve değeri açısından değerlendirilmeli ve bir saldırganın bu varlıkları tehdit etmek için hangi toplum mühendisliği yöntemlerini kullanacağı sorgulanmalıdır. Bu soruların ya-

Mitnick Mesajı:

Toplum mühendisinin temel çalışma yönteminden herkes haberdar olmalıdır: Hedefle ilgili mümkün olduğu kadar çok bilgi topla ve bu bilgiyi içerden birinin güvenini kazanmak için kullan. Sonra da onun gırtlağına yapış!

nıtları göz önüne alınarak, bu tarz bilgilere erişim hakkı verilmiş kişilere yönelik eğitimlerin tasarlanması gerekmektedir.

Şahsen tanımadığınız biri bir bilgi ya da belge istediğinde ya da bilgisayarda bir işlem gerçekleştirilmesini rica ettiğinde, çalışanların bazı soruları kendilerine sormalarını sağlayın. Eğer bu bilgiyi en büyük düşmanıma verirsem, bu, bana ya da çalıştığım şirkete zarar vermek için kullanılabilir mi? Bilgisayarıma girmem istenen komutların olası etkilerinin tamamen bilincinde miyim?

Karşılaştığımız her yeni insandan kuşkulanarak yaşantımızı sürdüremeyiz. Yine de, ne kadar güven duymaya meyilli olursak, karşımıza çıkacak bir toplum mühendisinin bizi şirketimize ait bilgileri vermeye kandırabilme olasılığı da o kadar yüksek olur.

İntranet'e Neler Koyulabilir?

İntranetin bazı bölümleri dışarıya açık, bazı bölümleri de çalışanlara kapalı olabilir. Şirketiniz, hassas bilgilerin yanlış kişilerin de erişebileceği bir yere konması olasılığına karşı ne kadar dikkatli? Herhangi bir hassas bilginin dikkatsizlik nedeniyle internet sitenizin herkese açık bölgelerinde de sunulup sunulmadığı, kuruluşunuzdan biri tarafından en son ne zaman kontrol edildi?

Eğer şirketiniz elektronik güvenlik tehditlerinden korunmak için ara güvenlik olarak proxy sunucular kurmuşsa, bu sunucular, doğru ayarlandıklarından emin olmak amacıyla yakın zamanda kontrol edildiler mi?

Aslına bakarsanız, şimdiye dek intranet güvenliğinizi hiç kontrol eden oldu mu?

SİZE YARDIMCI OLABİLİRİM

Sorunla boğuştuğumuz bir sırada bize yardım etmek için bilgili, becerikli ve istekli biri çıkageldiğinde çok memnun oluruz. Toplum mühendisi bunun farkındadır ve bundan nasıl yararlanacağını da bilir.

Size nasıl sorun çıkaracağını da bilir... sonra sorunu çözdüğünde ona minnettar kalmanızı sağlar... ve sonunda sizden, bu karşılaşmadan şirketinizi (belki de sizi) zararlı çıkaracak bir bilgi ya da küçük bir iş koparmak için bu minnettarlığınızı kullanır. Ama siz değerli birşey kaybettiğinizin hiçbir zaman farkına varmazsınız.

İşte size, toplum mühendislerinin "yardım etmek" için öne çıktıkları tipik yollardan bazıları.

Bilgisayar Ağı Zayiatı

Gün/Zaman: 12 Şubat, Pazartesi, öğleden sonra 3:25

Yer: Starboard Tersane İşletmeleri

İlk Görüşme: Tom DeLay

- *Tom DeLay, muhasebe.*

- *Selam Tom. Ben Yardım Masası'ndan Eddie. Bir bilgisayar ağı sorununu çözmeye çalışıyoruz. Ekibinde kimsenin çevrimiçi kalmakla ilgili bir sorunu var mı?*

- *Bildiğim kadarıyla hayır.*

- *Sen de hiçbir sorunla karşılaşmadın, öyle mi?*

- *Hayır, her şey yolunda görünüyor.*

- *Tamam, iyi o zaman. Dinle, etkilenmiş olabilecek insanları bulmaya çalışıyoruz. Eğer ağ bağlantın kesilirse bize hemen haber vermen çok önemli.*

- *Bu, kulağa hiç hoş gelmiyor. Sence böyle birşey olabilir mi?*

- *Umarım olmaz; ama olursa ararsın, değil mi?*

- *Bundan emin olabilirsin.*

- *Ağ bağlantısının kopması senin için gerçek bir sorun olacakmış gibi görünmüyor.*

- *Kesinlikle.*

- ... o zaman, hazır biz bunun üstünde çalışırken, sana cep telefonu vereyim. Böylece ihtiyacın olursa bana doğrudan ulaşabilirsin.

- Bu çok iyi olur. Numaranı alayım.

- 555 521 0871

- 555 521 0871. Tamam, Teşekkürler. Adın neydi?

- Eddie. Bir şey daha; ağa hangi noktadan bağlandığını kontrol etmem gerekiyor. Bilgisayarının bir yerlerinde, üzerinde 'Bağlantı Noktası Numarası' gibi birşey yazan bir etiket olup olmadığına bakabilir misin?

- Dur bakayım. Hayır, öyle birşey görmüyorum.

- Peki, bilgisayarın arkasındaki ağ kablosunu biliyor musun?

- Evet.

- Onu bağlı olduğu yere kadar takip et. Bak bakalım fişin takılı olduğu girişte bir etiket var mı.

- Bir saniye. Evet. Bir dakika, okuyabilmek için yere çömelmem gerekecek. Tamam, şöyle yazıyor: Bağlantı Noktası 6 tire 47.

- İyi. Elimdeki kayıtlarda da öyle geçiyorsun, emin olmak istemiştim.

İkinci Görüşme: Sistem Sorumlusu

İki gün sonra aynı şirketin Ağ Hizmetleri Merkezi'ne bir telefon gelir.

- Merhaba, ben Bob. Muhasebeden Tom DeLay'in ofisindeyim. Bir kablo sorununu çözmeye çalışıyoruz. 6-47 numaralı bağlantıyı devre dışı bırakmanızı isteyecektim.

Sistem sorumlusu birkaç dakika içinde yapabileceğini söyledi ve işleri bittiğinde bağlantının tekrar açılması için ona haber vermeleri gerektiğini hatırlattı.

Üçüncü Görüşme: Düşmandan Yardım Alma

Bir saat kadar sonra adının Eddie Martin olduğunu söyleyen adamın dışarda gezinirken telefonu çaldı. Eddie aramanın tersanecilik işletmesinden geldiğini görünce telefonunu açmadan önce hızla sessiz bir yer buldu.

- Yardım Masası, Eddie.

- Selam Eddie. Senin tarafında bir yankı var, neredesin?

- Bir kablo dolabının içindeyim. Kim arıyordu?

- Ben Tom DeLay. Seni bulabildiğime çok sevindim. Hatırlarsan geçen gün beni aramıştın. Söylediğin gibi ağ bağlantım az önce kesildi. Ne yapacağım şimdi?

- Evet, ekip olarak şu anda bunun üstünde çalışıyoruz. Akşama kadar bitirmiş oluruz. Bu uygun mu?

- HAYIR! Olmaz! Bu kadar uzun süre bağlantısız kalırsam işimde geri kalırım. En erken ne zaman halledebilirsin bu işi?

- Çok mu sıkışık durumdasın?

- Şu anda başka birkaç şeyle de ilgilenebilirim. Yarım saat içinde bunu halletmeniz mümkün olur mu?

- YARIM SAAT Mİ? Çok da birşey istemiyorsun. Peki, elimdeki işi bırakıp, senin sorununu çözmeye çalışacağım.

- Çok müteşekkir kalırım, Eddie.

Dördüncü Arama: Yakaladım Seni!

Kırk beş dakika sonra ...

- Tom? Ben Eddie. Ağ bağlantını bir deneyebilir misin?

Biraz sonra:

- Oh, çok iyi; çalışıyor. Harika.

- İyi, sorununu çözebildiğime sevindim.

- Evet, çok teşekkürler.

- Dinle, bağlantının yeniden kopmasını istemiyorsan çalıştırman gereken bir program var. Yalnızca birkaç dakika sürer.

- Şu an çok iyi bir zaman değil.

- Anlıyorum ama bu ağ sorunu yine ortaya çıkarsa ikimizi de büyük dertlerden kurtarır.

- Peki... birkaç dakika sürecekse.

- Yapman gereken şu...

Eddie. Tom'u bir web sitesinden küçük bir program indirmesi için adım adım yönlendirdi. Program indirildikten sonra, Tom'a programın üzerinde çift tıklamasını söyledi. Tom denedi ama:

- Çalışmıyor. Hiçbir şey yapmıyor, diye karşılık verdi.

- Of, çok kötü. Programla ilgili bir sorun olmalı. Silelim onu, başka bir zaman tekrar deneriz. Sonra Tom'a programı hem indirdiği yerden hem de çöp kutusundan sildirdi.

Toplam geçen zaman: on iki dakika.

Saldırganın Öyküsü

Bobby Wallace, bunun gibi iyi bir iş aldıktan sonra, bilginin neden istendiğiyle ilgili açık bir soruya müşterinin kaçamak yanıtlar vermesinin her zaman gülünç olduğunu düşünmüştü. Bu işte de aklına yalnızca iki neden geliyordu. Müşteri, hedef şirket olan, Starboard Tersane İşletmelerini satın almayı düşünen başka bir şirketi temsil ediyor ve şirketin mali durumunun gerçek yüzünü öğrenmek istiyor olabilirdi. Özellikle de, hedef şirketin olası bir alıcıdan saklamak isteyebileceği bilgileri. Ya da

Terimler

TRUVA ATI: Kurbanın bilgisayarından ve içinde bulunduğu ağdan bilgi toplamak ya da kurbanın bilgisayarına ve dosyalarına zarar verebilmek için tasarlanmış, kötü huylu ya da zararlı kod içeren programdır. Bazı Truva Atları bilgisayarın işletim sisteminin içinde saklanıp her işlemin ya da her tuşa basışın kaydını tutacak veya belirli işlevleri gerçekleştirebilmek için ağ bağlantısı üzerinden talimat alabilecek şekilde tasarlanmışlardır ve bunların hepsini, kendi varlıklarını kurbana sezdirmeden yaparlar.

belki para yönetiminde karanlık işlerin döndüğünü düşünen ve bazı üst düzey yöneticilerin yolsuzluk yapıp yapmadıklarını öğrenmek isteyen şirket ortakları da olabilirlerdi.

Belki de müşterisi ona gerçek nedeni söylemek istememişti, çünkü bilginin ne kadar değerli olduğunu bilirse Bobby işi yapmak için daha çok para isteyebilirdi.

Bir şirketin en gizli dosyalarını ele geçirmenin pek çok yolu vardır. Bobby birkaç gün seçeneklerin üzerinde düşünmüştü ve bir plan üstünde karar kılmadan önce küçük de bir araştırma yapmıştı. Sonunda özellikle sevdiği bir yöntemi, kurbanın saldırgandan yardım istemek üzere tuzağa düşürüldüğü oyunu oynamayı seçmişti.

Başlangıç olarak bir mağazadan 39 dolar 95 sente bir cep telefonu almıştı. Hedef olarak belirlediği adamı aramış ve kendini şirket yardım masasından biri gibi tanıtarak, ağda bir sorun çıktığı anda Bobby'i cep telefonundan araması doğrultusunda adamı ayarlamıştı.

Kendini açık etmemek için araya iki gün koymuştu ve sonra da şirketin Ağ Hizmetleri Merkezi'ne (AHM) telefon etmişti. Tom'un, yani hedefinin, bir sorununu çözmeye çalıştığını söyleyerek Tom'un ağ bağlantısının devre dışı bırakılmasını istemişti. Bobby çektiği numaranın bu aşamasının en aşılması zor bölüm olduğunu biliyordu; pek çok şirkette yardım masası çalışanları AHM'yle yakın temas içinde çalışırlar; hattâ, yardım masası çoğu zaman bilgi işlem biriminin bir parçasıdır. Ancak konuştuğu vurdum duymaz AHM görevlisi, olayı sıradan bir işlem yerine koyup bilgisayar ağı sorununu çözmekle uğraşan ve yardım masasında çalıştığını söyleyen kişiye adını sormadan hedefin bağlantı noktasını devre dışı bırakmayı kabul etmişti. İş tamamlandığında Tom şirketin intranetinden bütünüyle yalıtılmıştı. Sunucudaki dosyalara erişmesi olanaksız hale gelmişti. Mesai arkadaşlarıyla dosya alıp verememekte, e-postalarını okuyamamakta, hattâ yazıcıya bir çıktı bile gönderememekteydi. Bu durum, günümüz dünyasında mağarada yaşamak gibi bir şeydi.

Bobby'nin de tahmin ettiği üzere cep telefonunun çalması uzun sürmemişti. Doğal olarak sıkıntılı bir durumda olan bu zavallı "mesai arka-

daşına" yardımcı olmak konusunda hevesli görünüp sonra AHM'yi arayarak adamın ağ bağlantısını yeniden açtırmıştı. Kurbanı tekrar arayarak onu bir kez daha kandırmıştı. Bu kez, Bobby ona yardım ettikten sonra "hayır" dediği için Tom'un kendini suçlu hissetmesini sağlamıştı. Bunun üzerine Tom, bilgisayarına bir yazılım indirme önerisini kabul etmişti.

Doğal olarak, yapmayı kabul ettiği şey tam olarak göründüğü şey değildi. Tom'un ağ bağlantısını çökmekten koruyacağı söylenen yazılım aslında bir Truva Atı'ydı. Bobby, Yunanların Truvalılara yaptığını Tom'un bilgisayarına yapmıştı; yani düşmanı kalenin içine sokmuştu. Tom yazılım simgesine çift tıkladığında hiçbir şey olmadığını söylemişti. Zaten küçük program, tasarımı gereği, bilgisayara erişime izin verecek gizli bir yazılım yüklerken bile herhangi birşey olduğunu göstermezdi.

Program, Bobby'nin uzaktan erişimle Tom'un bilgisayarı üzerinde tam bir hakimiyet kurmasını sağlamıştı. Bobby Tom'un bilgisayarına girdiğinde onu ilgilendirebilecek muhasabe kayıtlarını arayabilir ve onları kendine kopyalayabilirdi. Sonra canı istediği zaman müşterilerinin aradığı bilgiyi bulabilmek için dosyalara bakabilirdi.

Her şey bununla da bitmiyordu. Her zaman geri dönüp, ilginç bilgiler sunabilecek anahtar sözcükleri kullanarak bir metin araması yapıp, şirket yöneticilerinin elektronik mesajlarını ve özel notlarını tarayabilirdi.

Hedefini Truva Atı yazılımını yüklemesi için kandırdığı günün akşamı Bobby cep telefonunu bir çöp bidonuna attı. Elbette, atmadan önce hafızasını temizledi ve bataryasını çıkardı. İsteyebileceği en son şey birinin cep telefonunu yanlışlıkla araması ve telefonun çalmaya başlamasıydı!

Aldatmacanın İncelenmesi

Saldırgan, hedefini, aslında var olmayan bir sorunu olduğuna inandırarak kendi ağına düşürür. Sorun, bu olayda olduğu gibi, henüz gerçekleşmemiş ama saldırganın gerçekleşeceğini bildiği çünkü kendisinin neden olacağı bir sorun da olabilir. Sonra da kendisini sorunu çözebilecek kişi olarak tanıtır.

Bu tarz saldırıda kullanılan düzen, saldırganın özellikle işine gelir, çünkü önceden ekilen tohum sayesinde hedef, bir sorunu olduğunu anladığında yardım istemek için kendi ayağıyla gelir. Saldırgan yalnızca

Mitnick Mesajı:

Eğer tanımadığınız biri size bir iyilik yapıyorsa ve sonra da karşılığında sizden bir iyilik bekliyorsa, istenen şeyin ne olduğu üzerinde dikkatle düşünmeden karşılık vermeyin.

Terimler

UZAKTAN ERİŞİMLİ KOMUT KABUĞU: Belirli işlevleri gerçekleştirmek ya da programları çalıştırmak için metin tabanlı komutlar kabul eden grafik içerikli olmayan bir arayüzdür. Teknik açıkları sömürebilen ya da kurbanın bilgisayarına bir Truva Atı yükleyebilen bir saldırgan bir komut kabuğuna uzaktan erişim sağlayabilir.

TERS TOPLUM MÜHENDİSLİĞİ: Kurbanın bir sorunla karşılaştığı ve yardım için saldırganı aradığı şeklinde gelişen toplum mühendisliği saldırısı.

Ters toplum mühendisliğinin başka bir türü de saldırganın aleyhinde olamdır. Hedef, bir saldırı yapıldığını anlar ve işletmenin varlıklarını güvenceye alabilmek için psikolojik etkileme unsurları kullanarak saldırgandan mümkün olduğu kadar çok bilgi almaya çalışır.

oturup telefonun çalmasını bekler. Bu yönteme, meslekte büyük bir sevecenlikle *ters toplum mühendisliği* denmiştir. Hedefin kendisini aramasını sağlayan saldırgan, anında inanılırlık kazanır. Yani eğer ben yardım masasında çalıştığını düşündüğüm birini ararsam ondan kimliğini kanıtlamasını istemem. İşte o zaman saldırgan başarmış demektir.

Böyle bir dolap çevirirken toplum mühendisi bilgisayarlarla ilgili sınırlı bilgiye sahip olan bir hedef seçmeye çalışır. Hedef ne kadar çok bilirse şüphelenme olasılığı o kadar çoktur; ya da onunla oyun oynandığını hemen anlayabilir. Zaman zaman bilgisayarla savaşan çalışanlar olarak söz ettiğim, teknoloji ve süreçleriyle ilgili konularda az bilgili olan kişiler her söylenene inanmaya daha eğilimlidirler. Bir yazılımın verebileceği zararla ilgili olarak hiçbir fikirleri olmadığı için "şu küçük programı yükleyiver," gibi bir hileyi yutma olasılıkları da yüksektir. Dahası, bilgisayar ağı üzerinden tehlikeye soktukları bilginin değeri konusunda fikir sahibi olma olasılıkları da azdır.

Yeni Başlayan Kıza Küçük Bir Yardım

Yeni işe başlayanlar, saldırganlar için en iyi hedeflerdir. Henüz çok insan tanımazlar, şirketin süreçlerini, yapılması ve yapılmaması gereken şeyleri bilmezler. Ve iyi bir izlenim bırakmak adına ne kadar yardımsever ve hızlı olduklarını göstermek için de heveslidirler.

Yardımsever Andrea

- *İnsan Kaynakları, Andrea Calhoun.*
- *Andrea, merhaba, ben Alex; Şirket Güvenliği'nden .*
- *Evet?*
- *Bugün işler nasıl?*

- İyi. Sizin için ne yapabilirim?

- Yeni başlayanlar için bir güvenlik semineri düzenliyoruz ve deneme için birkaç kişiyi biraraya getirmemiz gerekiyor. Geçen ay işe başlayan herkesin adlarına ve telefon numaralarına ihtiyacım var. Bana bu konuda yardımcı olabilir misin?

- Ancak öğleden sonra çıkarmam mümkün olabilir. Bu uygun mu? Dahili numaran nedir?

- Elbette olur, dahilim 52... aalı, günün çoğunda toplantıda olacağım. Ofise döndükten sonra seni ararım, bu herhalde dörtten sonra olur.

Alex 16:30'da aradığında Andrea listeyi hazırlamıştı ve adları ve dahili numaraları ona okudu.

Rosemary'e Bir Mesaj

Rosemary Morgan yeni işinden çok memnundu. Daha önce hiçbir dergi için çalışmamıştı ve insanları beklediğinden daha arkadaş canlısı bulmuştu. Her ay sonunda bitmesi gereken bir başka sayıyı çıkarabilmek için çalışanların çoğunun bitmek bilmeyen bir baskı altında oldukları düşünülünce bu şaşırtıcı bir durumdu. Bir Perşembe sabahı aldığı telefon bu dostça izlenimi pekiştirdi

- Rosemary Morgan'la mı görüşüyorum?

- Evet.

- Merhaba Rosemary. Ben Bill Jorday; Bilgi Güvenliği Grubu'ndan.

- Evet?

- Bizim birimden kimse sizinle güvenlik uygulamaları hakkında görüştü mü?

- Sanmıyorum.

- Peki. Bakalım. Öncelikle kimsenin şirket dışından getirdiği programları yüklemesine izin vermiyoruz. Bunun nedeni lisanslı olmayan yazılım kullanımından sorumlu olmak istememeniz ve solucan ya da virüs içeren yazılımların çıkarabileceği sorunlardan uzak durmak.

- Tamam.

- E-posta uygulamanızdan haberdar mısınız?

- Hayır.

- Şu anda kullandığınız e-posta adresi nedir?

- Rosemary@ttrzine.net.

- Kullanıcı adı olarak Rosemary'i mi kullanıyorsunuz?

- Hayır, R altçizgi Morgan'ı kullanıyorum.

- Tamam. Tüm yeni çalışanlarımızı beklemedikleri e-posta eklerini açmalarının oluşturacağı tehlikelere karşı uyarmak istiyoruz. Pek çok solucan ve virüsler ortalıkta geziniyor ve tanıdığınız insanlardan geliyor gibi görünen e-posta eklerinde geliyorlar. Bu yüzden beklemedi-

ğiniz bir ekli e-posta alırsanız, gönderici olarak görünen kişinin mesajı size gerçekten gönderip göndermediğini her zaman kontrol edip emin olmalısınız. Anlıyor musunuz?

- Evet. Bunu duymuştum.

- İyi. Uygulama her doksan günde bir parolanızı değiştirmeniz şeklinde. Parolanızı en son ne zaman değiştirdiniz?

- Yalnızca üç haftadır burada çalışıyorum ve daha ilk aldığım şifreyi kullanıyorum.

- Tamam, bu iyi. Doksan gün dolana kadar bekleyebilirsin. Ama insanların, tahmin edilmesi kolay olmayan şifreler kullandığından da emin olmak istiyoruz. Hem sayı hem de harf içeren bir şifre mi kullanıyorsunuz?

- Hayır.

- Bunu düzeltmeliyiz. Şu anda kullandığınız şifre nedir?

- Kızının adı, Annette.

- Bu çok güvenli bir şifre değil. Hiçbir zaman aile bilgilerinize dayanan şifreler seçmemelisiniz. Peki... benim yaptığımın aynısını yapabilirsiniz. Şifrenizin bir parçası olarak şu anda kullandığınızı kullanmanın bir sakıncası yok ama her değiştirdiğinizde içinde bulunduğunuz ayın sayısını ekleyin.

- Bunu şimdi yaparsam, yani Mart için, üç mü kullanmalıyım, sıfır-üç mü?

- Nasıl isterseniz. Hangisi sizin için daha rahat olur?

- Sanırım Annette-üç.

- İyi. Değişikliğin nasıl yapılacağı konusunda size yardımcı olmamı ister misiniz?

- Hayır, nasıl yapılacağını biliyorum.

- Güzel. Söylemem gereken birşey daha var. Bilgisayarınızda bir virüs koruma yazılımı var ve onu güncel tutmanız önemli. Arada bir bilgisayarınız yavaşladığında bile otomatik güncellemeyi devre dışı bırakmamalısınız. Tamam mı?

- Elbette.

- Çok iyi. Bilgisayarla ilgili bir sorununuz olduğunda aramanız için bunun telefon numarası sizde var mı?

Yoktu. Adam ona numarayı verdi, kadın özenle not aldı ve bir kez daha ona ne kadar iyi baktıklarını düşünerek işine geri döndü.

Aldatmacanın İncelenmesi

Bu öykü, elinizdeki kitabın temelinde yatan anafikri güçlendiriyor. Asıl amacından bağımsız olarak bir toplum mühendisinin bir çalışandan isteyeceği en temel bilgiler, hedefin tanımlama verileridir. Şirketin doğ-

Mitnick Mesajı:

Yeni işe başlayanların, şirket bilgisayar sistemlerine girişlerine izin verilmeden önce, özellikle şifrelerini başkalarına kesinlikle söylememekle ilgili olan güvenlik uygulamaları konusunda eğitilmeleri gerekir.

ru bölümünden tek bir çalışana ait kullanıcı adı ve şifre varsa saldırganın içeri girebilmek için ve peşinde olduğu herhangi bir bilgiye ulaşmak için ihtiyacı olan her şeyi vardır. Bu bilgiyi edinmek, krallığın anahtarını bulmak gibidir. Onlar elindeyken şirket bünyesinde özgürce dolaşabilir ve aradığı hazineyi bulabilir.

Düşündüğünüz Kadar Güvenli Değil

"Hassas bilgilerini korumak için çaba göstermeyen bir şirket düpedüz ihmalcidir." Pek çok insan bu görüşe katılacaktır. Gerçek şu ki gizli bilgilerini korumaya yönelik çaba gösteren şirketler bile ciddi bir tehlike altında olabilirler.

İşte size şirketlerin, deneyimli ve başarılı profesyoneller tarafından tasarlanmış güvenlik uygulamalarının aşılamayacağını düşünerek her gün kendi kendilerini nasıl kandırdıklarını gösteren bir öykü daha.

Steve Cramer'in öyküsü

Steve'in pahalı tohumlarla çimlendirilmiş ve herkesin gıptayla baktığı bir bahçesi yoktu. Çimleri biçmek için büyük bir makine da gerekmiyordu. Zaten böyle bir makine olsa bile kullanmazdı. Çünkü bu küçük çim biçme makinesiyle işinin daha uzun sürmesi sayesinde Anna'nın çalıştığı bankadaki insanlarla ilgili hikâyeler anlatmasından ya da ona yaptıkları işleri açıklamasından kurtulup kendi düşüncelerine odaklanabiliyordu. Hafta sonlarının ayrılmaz bir parçası haline gelen 'sevgilim şunu da yapar mısın?' listelerinden nefret ediyordu.

Bazıları Steve'in GeminiMed Tıbbî Cihazlar Şirketi için yeni cihazlar tasarlama işinin sıkıcı olduğunu düşünebilirdi. Ancak Steve hayat kurtardığını biliyordu. İşinin yaratıcı olduğunu düşünüyordu. Sanatçılar, besteciler, mühendisler de Steve'in yaptığına benzer işler yapıyorlar ve daha önce kimsenin yapmadığı bir şeyler yaratıyorlardı. Son yaptığı ve oldukça zekice tasarlanmış yeni bir çeşit kalp stenti şu ana dek en gurur duyduğu eseriydi.

O cumartesi, saat neredeyse 11:30 olmuştu. Steve çim biçme işini daha bitiremediği ve kalp stentinin tamamlanmasında son engel olan güç gereksiniminin düşürülmesi sorununa ciddi bir çözüm bulamadığı için huzursuzdu. Çim biçerken üzerinde düşünmek için harika bir konuydu ama hiçbir çözüm üretememişti.

Anna kapıda belirdi; saçını her zaman toz alırken takdığı kırmızı desenli kovboy eşarbıyla örtmüştü. *"Telefon"* diye bağırdı. *"İşten arıyorlar."*

"Kim?" diye geri bağırdı Steve.

"Ralph diye biri sanırım."

"Ralph mı?" Steve GeminiMed'de çalışan ve onu hafta sonu arayabilecek Ralph isimli birini tanımıyordu. Anna adı yanlış anlamış olmalıydı. Steve bunları düşünerek telefona gitti

"Steve, ben Teknik Destek'ten Ramon Perez." Steve, Anna'nın Ramon gibi bir İspanyol adını Ralph'a nasıl çevirdiğini merak etti.

"Bu nezaket icabı yapılan bir arama" diyordu Ramon. *"Sunucılardan üçü çöktü. Bir solucandan şüpheleniyoruz ve diskleri temizleyip yedekleri yükleyeceğiz. Çarşamba ya da Perşembe'ye kadar dosyalarınızı yükleyip çalıştırılabilir duruma getiririz. Yani her şey yolunda giderse."*

"Bu kesinlikle mümkün değil" dedi Steve sert bir şekilde ve sıkıntısını belli etmeye çalışarak. Bu insanlar nasıl bu kadar aptal olabiliyorlardı? Tüm haftasonu ve gelecek haftanın çoğunda dosyalarına erişemeden iş yapamayacağı akıllarına gelmiyor muydu? *"Olmaz. İki saate kadar evdeki bilgisayarımın başına oturacağım ve dosyalarıma erişmem gerekecek. Bilmem anlatabiliyor muyum?"*

"Evet, tabi, şimdiye kadar aradığım herkes listenin başında olmak istiyor. Buraya gelip bunun üstünde çalışmak için hafta sonumu harcıyorum ve konuştuğum herkesin bana püskürmesi hiç hoş olmuyor."

"Teslim tarihim yaklaşıyor ve şirket çıkacak ürüne çok güveniyor. Benim bu işi bu öğleden sonra bitirmem lâzım. Bunu kafana sok."

"Başlamadan önce aramam gereken daha bir sürü insan var." dedi Ramon. *"Dosyalarınızı salı'ya kadar hazır etsek nasıl olur?"*

"Salı değil, çarşamba değil. ŞİMDİ!" dedi Steve. Bu kalın kafalı adam durumun önemini anlayamazsa mutlaka başka birini araması gerekecekti.

"Tamam, tamam" dedi Ramon ve Steve onun asabi bir şekilde iç geçirdiğini duydu. *"Senin işini görebilmek için neler yapmam gerektiğine bir bakayım. RM22 sunucusunu kullanıyorsun, değil mi?"*

"RM22 ve GM16. Her ikisini de."

"Peki. Tamam, bazı işleri kısa yoldan yapıp zaman kazanabilirim. Kullanıcı adına ve parolana ihtiyacım olacak."

Eyvah, diye düşündü Steve. Ne demek oluyor bu? Benim parolama neden ihtiyaç duysun ki? Herkes bir tarafa sistem sorumluları neden sorsun ki bunu?

"Soyadın ne demiştin? Ve müdürün kim?"

"Ramon Perez. Bak sana ne diyeceğim, ilk işe başladığımda kullanıcı adı alırken doldurduğum bir form vardı ve oraya parolamı da yazmış-

tın. O parolayı bulup dosyaların burada olduğunu sana gösterebilirim. Olur mu?"

Steve bunun üzerinde birkaç saniye düşündü sonra da kabul etti. Ramon dosya dolabından formları almaya giderken, o artan bir sabırsızlıkla telefonun öbür ucunda bekledi. Steve Ramon'un bir kağıt yığınını karıştırdığını duyuyordu.

"İşte burada" dedi Ramon sonunda. *"Janice diye bir şifre koymuşsun."*

"Janice", diye düşündü Steve. Annesinin adıydı ve gerçekten de onu bazen şifre olarak kullanırdı. İşe girme belgelerini doldururken bu şifreyi pekala koymuş olabilirdi.

"Evet, bu doğru" diyerek onayladı.

"Tamam, zaman kaybediyoruz. Gerçek olduğunu biliyorsun. Kısa yolu kullanıp en çabuk şekilde dosyalarını kurtarmamı istiyorsan bana yardım etmen gerekecek."

"Kullanıcı adım s, d, altçizgi, cramer C-R-A-M-E-R. Şifre: pelikan1."

"Hemen işe koyulacağım" dedi Ramon; sonunda sesi yardımcı olabilecekmiş gibi geliyordu. *"Bana birkaç saat ver."*

Steve çim biçme işini bitirdi. öğle yemeğini yedi ve bilgisayarının başına geçtiğinde dosyalarının geri yüklenmiş olduklarını gördü. O huysuz sistem sorumlusunu bağırarak yola getirdiği için kendiyle gurur duydu ve Anna'nın da ne kadar sert konuştuğunu duymuş olmasını diledi. Adama ya da patronuna teşekkür etmek iyi olurdu ama böyle şeyleri yapacak biri olmadığının da farkındaydı.

Craig Cogburne'ün Öyküsü

Craig Cogburne yüksek teknoloji ürünleri üreten bir şirkette pazarlamacı olarak çalışıyordu ve işinde de oldukça iyiydi. Bir süre sonra müşteriyi okumak konusunda bir becerisi olduğunu fark etti. Kişinin hangi konularda dirençli olduğunu, satışı kapatmayı kolaylaştıracak bazı zayıflıklarını ve açıklarını görebiliyordu. Yeteneğini kullanmanın başka yollarını bulmaya çalıştı ve izlediği yol onu sonuç olarak daha kazançlı bir alana götürdü: sanayi casusluğu. Kendi ağzından dinleyelim:

Bu seferki çok sıkı bir işti. Çok fazla zamanımı almadı ve Hawaii'ye hattâ belki Tahiti'ye bir gezi yapacak kadar da çok kazanç sağladım.

Beni tutan adam, doğal olarak bana müşterinin kim olduğunu söylemedi; ama atılacak hızlı, büyük ve kolay bir adımla rekabeti yakalamak isteyen bir şirket olduğunu anladım. Tüm yapmam gereken kalp stenti denen yeni bir zamazingoya ait ürün özelliklerini ve tasarımlarını ele geçirmekti. Bunun ne olduğu konusunda hiçbir fikrim yoktu. Şirketin adı GeminiMed'di. Bu adı hiç duymamıştım ama yarın düzine yerde ofisleri olan Fortune 500 şirketlerinden biriydi; bu da işi küçük bir şirkete göre daha kolay kılıyordu çünkü küçük şirkette konuştuğun kişi-

nin olduğunu iddia ettiğin ve aslında olmadığın adamı tanıma şansı oldukça yüksek oluyordu.

Müşterim bana bir faks yolladı. Gönderilen bir doktor dergisinden alınmıştı ve GeminiMed'in farklı ve yeni bir tasarımı olan bir stent üzerinde çalıştığını, adının da STH-100 olduğunu yazıyordu. Doğruyu söylemek gerekirse bir gazeteci benim için büyük bir ayak işini halletmişti. İşe koyulmadan önce ihtiyacım olan tek bir şey vardı ve o da yeni ürünün adıydı.

Birinci sorun: Şirkette STH-100 üzerinde çalışan kişilerin ya da tasarımları görme yetkisine sahip insanların adlarını öğren. Santralı aradım ve, *"Mühendislik ekibinizden biriyle bağlantı kuracağıma söz vermiştim ve soyadını hatırlamıyorum, ama adı S'yle başlıyordu,"* dedim. Ve santraldaki kız dedi ki, *"Scott Archer ve Sam Davidson adında birileri var."* Hangisi STH-100 ekibinde çalışıyor bilmiyordu; bu yüzden rastgele Scott Archer'i seçtim, kız beni ona bağladı.

Adam telefonu açtığında, *"Merhaba, ben Mike, posta odasından. Elimizde STH-100 Kalp Stenti proje ekibine gelmiş bir kargo paketi var. Bunun kime gideceği konusunda bir fikriniz var mı?"* diye sordum. Bana ekip liderinin adını verdi, Jerry Mendel. Benim için Mendel'in numarasını bulmasını bile sağladım.

Aradım. Mendel yerinde yoktu ama telesekreterindeki mesaj ayın on üçüne kadar tatilde olacağını söylüyordu. Bu, kayağa mı, her neye gittiyse bir hafta daha yerinde olmayacağı anlamına geliyordu ve bu süre zarfından birilerinin birşeye ihtiyacı olursa 9137'den Michelle'i aramaları gerektiğini söylüyordu. Bu insanlar çok yardımsever oluyorlardı. Hem de çok.

Telefonu kapattım ve Michelle'i aradım. Telefonu açtığında ona dedim ki, *"Ben Bill Thomas. Jerry bana şartnameyi bitirdiğimde ekibindekilerin inceleyebilmesi için sizi aramam gerektiğini söylemişti. Kalp stenti üzerinde çalışıyorsunuz, öyle değil mi?"* Kadın öyle olduğunu söyledi.

Şimdi oyunun en zorlu kısmına gelmiştik. Eğer kadın kuşkulanır gibi olursa, Jerry'nin benden yapmamı rica ettiği bir iyiliği yerine getirmeye çalıştığımla ilgili kozumu oynamaya hazırdım. *"Hangi sisteme bağlısınız?"* diye sordum.

"Sistem?"

"Ekibiniz hangi bilgisayar sunucularını kullanıyor?"

"Oh," dedi kadın, *"RM22. Ekibin bazıları da GM16'yı kullanıyorlar."*

Buna ihtiyacım vardı ve bu onu kuşkulandırmadan alabileceğim bir bilgiydi. Elimden geldiği ölçüde olağan bir tavır takınmış ve bir sonraki adım için onu biraz yumuşamıştım. *"Jerry bana geliştirme ekibinde çalışanların e-posta adreslerini verebileceğinizi söylemişti"* dedim ve nefesimi tuttum.

"Elbette. Evrak dağıtım listesi, okumak için çok uzun; size onu e-posta'yla gönderebilir miyim?"

Eyvah. Sonu GeminiMed.com'la bitmeyen herhangi bir e-posta adresi işleri yokuşa sürerdi. *"Bana listeyi fakslasanız nasıl olur?"* dedim.

Bunu yapabileceğini söyledi.

"Faks makinenizin ışığı yanıp sönüyor. Başka bir tanesinin numarasını almam gerekecek. Sizi biraz sonra ararım." dedim ve telefonu kapattım.

Bu noktada tatsız bir durumda kaldığını düşünebilirsiniz ama bu da işin bir parçası. Danışmada oturan kadına sesim tanıdık gelmesin diye bir süre bekledim sonra da onu arayıp, *"Merhaba, ben Bill Thomas, buradaki faks makinemiz çalışmıyor, sizin makinenize benim için bir faks gönderebilirler mi?"* dedim. Mümkün olduğunu söyledi ve bana numarayı verdi.

Sonra da oraya gidip faksı alacaktım, öyle mi? Tabi ki hayır! Birinci kural: Çok gerekmedikçe mekâna asla girme. Yalnızca telefondaki bir ses olarak kalırsan senin kimliğini belirlemeleri çok daha güç olur. Ve eğer senin kimliğini belirleyemezlerse, seni tutuklayamazlar. Bir sese kelepçe takmak kolay değildir. Bu yüzden bir süre sonra danışmayı yeniden aradım ve kıza faksımın gelip gelmediğini sordum. *"Evet,"* diye yanıtladı.

"Peki" dedim ona, *"Onu birlikte çalıştığımız bir danışmana vermem gerekiyor. Benim için gönderebilir misin?"* Sorun olmayacağını söyledi. Hem neden sorun olsundu ki; danışmada çalışan birinin neyin hassas bilgi olduğunu bilmesi beklenemezdi. Danışma görevlisi "danışmana" faksı gönderirken, ben de vitrininde "Faks Gönderilir/Alınır" yazan yakınlardaki bir kırtasiyeye doğru yürüyerek günlük sporumu yaptım. Faksın benden önce oraya gelmiş olması gerekiyordu ve beklediğim gibi içeri girdiğimde beni bekliyordu. Altı sayfaya 1.75 dolar verdim. Bir dolarlık bir banknot ve biraz bozukluk karşılığında tüm ekibin adlarına ve e-posta adreslerine sahip olmuştum.

İçeri Girmek

Peki, birkaç saat içinde üç ya da dört kişiyle konuştum ve şirket bilgisayarlarına girebilmek için dev bir adım attım. Ama olayı kalbinden vurmak için birkaç parça bilgiye daha ihtiyacım vardı.

Birincisi, mühendislik sunucusuna dışardan bağlanmak için gerekli telefon numarasıydı. GeminiMed'i tekrar aradım ve santral memurundan Bilgi İşlem Birimi'ni bağlamasını istedim. Telefona çıkan adama bilgisayarlar konusunda yardımcı olabilecek biriyle görüşmek istediğimi söyledim. Beni aktardı ve teknik konularla ilgili olarak kafam karışmış, biraz da aptalmış gibi davrandım. *"Evdeyim, yeni bir dizüstü bilgisayar aldım ve dışardan bağlanabilecek şekilde onu ayarlamak istiyorum."*

Süreç çok açıktı ama bağlantı için gerekli telefon numarasına gelene kadar her şeyi bana tek tek anlatmasına izin verdim. Numarayı bana herhangi bir önemsiz bilgiymiş gibi verdi. Sonra numarayı denerken onu beklettim. Her şey yolundaydı.

Ağa bağlanma engelini aşmıştım. Numarayı çevirdim ve arayanın dahili ağ üzerindeki bilgisayarlara bağlanmasına izin veren bir uçbirim sunucusuyla donanmış olduğunu gördüm. Birkaç denemeden sonra parolasız konuk hesabı olan bir bilgisayara denk geldim. Bazı işletim sistemleri ilk kurulduklarında kullanıcıyı bir kullanıcı adı ve parola belirlemesi için yönlendirirler, ancak aynı zamanda bir de konuk hesabı açarlar. Kullanıcının konuk hesabı için ya bir parola belirlemesi ya da hesabı bütünüyle kapatması gerekir ama çoğu insan bunu bilmez ya da umursamaz. Bu sistem büyük olasılıkla yeni kurulmuştu ve sahibi konuk hesabını kapatmakla uğraşmamıştı.

Çok şükür bir konuk hesabı varmış ki, şu anda UNIX işletim sisteminin eski bir sürümünü çalıştıran bir bilgisayara erişimim var. UNIX altındaki işletim sistemi, o bilgisayara giriş hakkı olan herkesin şifrelenmiş parolalarını bir parola dosyasında saklar. Parola dosyası her kullanıcının tek yönlü karıştırılmış (bu geri döndürülemez bir çeşit şifreleme yöntemidir) parolalarını içerir. Tek yönlü bir karıştırma sonucunda "haydiyap" gibi bir parola şifrelenmiş bir karmaşayla temsil edilir. Bu durumda parola UNIX tarafından on üç alfanümerik simgeden oluşan bir karışıma dönüştürülecektir.

Bir kişi bir bilgisayara dosya aktarmak isterse, bir kullanıcı adı ve parola girerek kendini tanıtması istenir. Tanıtım bilgilerini kontrol eden sistem yazılımı girilen parolayı şifreler sonra da sonucu, parola dosyasındaki şifrelenmiş parolayla (yani karışımla) karşılaştırır. Eğer ikisi aynıysa, kullanıcıya erişim hakkı verilir.

Dosyada yazılı parolalar şifreli oldukları için dosya, şifreleri çözmenin bilinen bir yolu olmadığı gerekçesine dayanarak tüm kullanıcılara açıktır. Çok saçma! Dosyayı indirdim ve üzerinde bir sözlük saldırısı yaptım (Bu yöntemle ilgili bilgi için 12. bölüme bakınız) ve geliştirme ekibindeki mühendislerden biri, Steven Cramer adında bir adamın bilgisayarda parolası "Janice" olan bir hesabı olduğunu öğrendim. Şansımı deneyip bu parolayı kullanarak adamın geliştirme sunucularından birindeki hesabına girmeye çalıştım. İşe yarasaydı, bana biraz zaman kazandırır ve başka bir risk daha alınama gerek kalmazdı. Ama olmadı.

Bu, adamı bana kullanıcı adını ve parolasını vermesi için kandırmam gerektiği anlamına

Terimler

PAROLA KARMAŞASI: Bir parolayı tek yönlü bir şifreleme sürecinden geçirdikten sonra ortaya çıkan anlamsız harf dizilimi. Bu sürecin güya geri döndürülemez bir süreç olduğu, yani karışımdan tekrar parolayı elde etmenin mümkün olmadığı düşünülür.

geliyordu. Bunun için haftasonunu bekleyecektim.

Kalanı zaten biliyorsunuz. Cumartesi günü Cramer'i aradım ve şüphelerini yenmek için bir solucanla ve sunucuların yedekten geri yüklenmesi gerektiğiyle ilgili bir hikâye uydurdum.

Ya ona anlattığım işe giriş formlarında parolasının yazdığıyla ilgili öykü tutmasaydı? İşe girerken doldurduğu formlarla ilgili bir şey hatırlamayacağından emindim. Yeni işe giren biri o kadar çok form doldurur ki yıllar sonra bu formların neler olduğunu kim hatırlayabilir? Ne olursa olsun, eğer onda çuvallasaydım, elimde kullanabileceğim uzun bir isim listesi vardı.

Terimler

ÖLÜ NOKTA: Bilginin bırakılabileceği ve başkaları tarafından bulunma olasılığının düşük olduğu yer. Geleneksel casusların olduğu bir dünyada bu, duvarda yerinde oynamış bir taşın arkası olurdu; bilgisayar korsanlarının dünyasında bu çoğunlukla uzak bir ülkedeki bir internet sitesidir.

Cramer'in kullanıcı adını ve parolasını kullanarak sunucuya girdim, biraz ortalığa bakındım ve sonunda STH-100'ün tasarım dosyalarını buldum. Hangilerinin anahtar dosyalar olduklarını bilmiyordum, bu yüzden tüm dosyaları bir ölü noktaya, kimseyi kuşkulandırmadan durabilecekleri Çin'deki ücretsiz bir FTP sitesine aktardım. Ivır zıvırın içinden neye ihtiyacı varsa müşteri kendi arayıp bulsun.

Aldatmacanın İncelenmesi

Hırsızlık gibi olan ama her zaman yasadışı olmayan toplum mühendisliği sanatında, kendisine Craig Cogburne dediğimiz adam ya da en az onun kadar becerikli bir kişi için burada anlatılan zorluklar neredeyse sıradan şeylerdir. Bu adamın amacı, güvenlik duvarlarıyla ve olağan güvenlik teknolojileriyle korunan bir şirket bilgisayarında duran gizli dosyaları bulup indirmekti.

İşin çoğu çocuk oyuncağıydı. İşe posta odasından biri gibi davranarak başladı ve teslim edilmeyi bekleyen bir kargo paketi olduğunu söyleyerek konuya biraz aciliyet kattı. Bu kandırmaca, kalp stenti geliştirme ekibinin tatilde olan liderinin adını öğrenmesini sağladı ama ekip lideri düşünceli davranmış ve bilgi çalmaya çalışan toplum mühendislerinin işini kolaylaştırmak için yardımcısının adını ve telefon numarasını bırakmıştı. Craig ekip liderinin yardımcısı olan kadını aramış ve ekip liderinin isteği üzerine aradığını söyleyerek bütün şüpheleri ortadan kaldırmıştı. Ekip lideri şehir dışındayken Michelle'in söylenenleri doğrulamasına da olanak yoktu. Bunu gerçek olarak kabul etti ve ekip üyelerinin bir listesini vermek konusunda tereddüt etmedi. Craig için bu oldukça önemli ve değerli bir bilgiydi.

Craig listeyi, genellikle her iki taraf için de daha kullanışlı olan e-posta yerine faksla göndermesini istediğinde bile kuşkulanmadı. Kadın neden bu kadar kolay kanmıştı? Pek çok çalışan gibi, patronunun işe dönüp de yapılmasını istediği bir işi yapmaya çalışan birinin engellerle karşılaştığını duymasını istememişti. Dahası, arayanın söylediğine göre patronu yalnızca adamın isteklerini onaylamakla kalmamış, aynı zamanda ondan yardım da istemişti. Bir kez daha, çoğu insanı kandırılmaya açık hale getiren, takım oyuncusu olma isteğiyle dolup taşan biriyle karşı karşıyayız.

Craig, danışmadaki kızın yardımcı olacağını bilerek faksın danışmaya gönderilmesini sağlamış ve böylece binaya girme gereğinden de kurtulmuştu. Ne de olsa danışma görevlileri etkileyici kişilikleri ve iyi bir izlenim yaratmadaki becerileri nedeniyle seçilirler. Faks alıp göndermek gibi küçük iyilikleri yapmak danışmada çalışan birinin görev alanına girer ve Craig de bundan nasıl yararlanacağını biliyordu. Kızın dışarı gönderdiği şey, o bilginin ne kadar değerli olduğunu bilen biri için alarm zillerinin çalmasına neden olabilirdi; ama danışmada çalışan birinin hangi bilginin hassas, hangi bilginin sıradan olduğunu bilmesi nasıl beklenebilir ki?

Farklı bir yönlendirme kullanan Craig, şirketin uçbirim sunucusuna, yani dahili ağ üzerinde diğer bilgisayar sistemlerine erişim sağlayan donanıma bağlanmak için kullanılan telefon numarasını vermesi için bilgi işlemdeki adamı ikna etmek amacıyla saf ve şaşkın davranmıştı.

Craig, hiç değiştirilmemiş ve güvenlik duvarıyla korunan pek çok dahili ağda var olup doğrudan göz önündeki açıklardan birini, yani varsayılan parolalardan birini deneyerek kolaylıkla bağlanmayı başardı. Aslında pek çok işletim sisteminin, yönlendiricinin ve başka benzer ürünün, hattâ özel santralların varsayılan parolaları çevrimiçi olarak bulunabilir. Herhangi bir toplum mühendisi, bilgisayar korsanı ya da sanayi casusunun yanısıra yalnızca konuya meraklı olanlar bile listeyi http://www.phenoelit.de/dpl/dpl.html adresinden bulabilirler. (Nereye bakması gerektiğini bilenler için internetin yaşamı bu kadar kolaylaştırması inanılmaz. Artık siz de nereye bakmanız gerektiğini biliyorsunuz.)

Daha sonra Cogburne, kalp stenti geliştirme ekibinin kullandığı sunucuya girebilmek için, dikkatli ve şüpheci bir adamı bile ("Soyadın ne demiştin? Ve müdürün kim?") kullanıcı adını ve parolasını vermeye ikna etti.

Mitnick Mesajı:

Çalışan herkesin birinci önceliği eldeki işi bitirmektir. Böyle bir baskı altında, güvenlik uygulamaları sık sık ikinci sıraya düşer veya gözden kaçar. Toplum mühendisleri, işlerini yaparken buna güvenirler.

Bu, Craig'in şirketin en iyi korunan sırlarını karıştırması ve yeni ürün tasarımlarını indirmesi için kapıyı açık bırakmak gibi bir şeydi.

Ya Steve Cramer şüphelenmeyi sürdürseydi? Pazartesi sabahı işe gidene kadar kuşkularını dile getirmek adına birşey yapma olasılığı düşüktü, o zaman da zaten saldırıyı engelleyebilmek için çok geç kalmış olacaktı.

Oynanan son oyunun kilit kısmı şuydu: Craig ilk başta Steve'in endişelerine karşı gayretsiz ve ilgisiz bir rol takınmış, sonra da ses tonunu değiştirip Steve'in işini bitirebilmesi için ona yardım etmeye çalışıyormuş gibi bir hava yaratmıştı. Çoğu zaman kurban, ona yardım ettiğinize ya da bir iyilik yapmaya çalıştığınıza inanırsa, başka zamanlarda özenle koruyacağı gizli bilgileri sizinle paylaşacaktır.

Aldatmacanın Engellenmesi

Toplum mühendisinin kullandığı en güçlü numaralardan biri olayların gidişini değiştirmektir. Bu bölüm kapsamında gördüğünüz şey budur. Toplum mühendisi sorunu yaratır, sonra da mucizevi bir şekilde sorunu çözerek kurbanı şirketin en gizli bilgilerine erişim sağlamakta kendisine yardımcı olması için kandırır. Sizin çalışanlarınız da böyle bir oyuna gelirler miydi? Bunu önlemek için belirli güvenlik kurallarını bir kâğıda döküp dağıtmayı hiç denediniz mi?

Eğitim, Eğitim, Eğitim...

New York'u görmeye gelmiş bir adamla ilgili eski bir fıkra vardır. Adam yoldan birini çevirir ve sorar, "Carnegie Hall'a nasıl ulaşabilirim?" Öteki cevap verir, "Çalışarak, çalışarak, çalışarak." Toplum mühendisliği saldırılarına herkes o kadar açıktır ki, bir şirketin tek etkili savunması çalışanlarını eğitmek, bilgilendirmek ve bir toplum mühendisini tanımak için gerekli altyapıyı onlara vermektir. Sonra da insanlara sürekli olarak eğitim sırasında öğrendikleri hatırlatılmalıdır ama bunların hepsi unutlur.

Kuruluştaki herkes, şahsen tanımadığı biriyle görüştüğü zamanlarda -özellikle de bu kişi bir bilgisayara ya da ağa nasıl erişileceğini soruyorsa- makul düzeyde şüpheci ve dikkatli olmak konusunda eğitilmelidir. Başkalarına inanmayı istemek insan yaratılışında vardır ama Japonların dediği gibi, iş dünyası bir savaş alanıdır. İşiniz savunmadaki bir boşluktan büyük zarar görebilir. Şirket güvenlik kuralları uygun olan ve olmayan davranışları açıkça tanımlamalıdır.

Güvenliğin herkese uygun tek bir kalıbı yoktur. Çalışanların çoğunlukla farklı görevleri ve sorumlulukları, her şirket içi konumun da kendine özgü açık noktaları vardır. Şirketteki herkesin tamamlamakla yükümlü olduğu bir temel eğitim olmalıdır. Daha sonra insanlar sorunun bir

parçası olma olasılıklarını düşürecek belirli süreçlere bağlı kalabilmeleri için iş profillerine göre de eğitim görmelidirler. Hassas bilgileri kullanan ya da sorumluk gerektiren konumlardaki kişilere ayrıca özel eğitim verilmelidir.

Hassas Bilgileri Emniyete Almak

Bu bölümdeki öykülerde de gördüğünüz gibi, biri yanlarına gelip yardım etmeyi teklif ettiğinde insanların, iş gereklerine, büyüklüğe ve şirket kültürüne uygun olarak tasarlanmış şirket güvenlik kurallarına başvurmaları gerekir.

Sizden bir bilgiyi taramanızı, bilgisayarınıza bilmediğiniz komutlar girmenizi, yazılım ayarlarınızı değiştirmenizi ve -hepsinin arasında en tehlikeli olanı- bir e-posta ekini açmanızı ya da kaynağı belirsiz bir yazılımı indirmenizi isteyen bir yabancıyla hiçbir zaman işbirliği yapmayın. Hiçbir şey yapmıyormuş gibi görünse bile herhangi bir yazılım programı göründüğü kadar masum olmayabilir.

Eğitiminiz ne kadar iyi olursa olsun zaman içinde uygulamakta dikkatsiz davrandığımız belirli süreçler vardır. Sıkışık bir zamanda, tam da ona ihtiyacımız olduğu anda eğitimi unutuveririz. Kullanıcı adını ve parolayı vermemenin, neredeyse herkesin bildiği (ya da bilmesi gerektiği) ve hatırlatılmasına pek de gerek olmayan bir şey olduğunu düşünebilirsiniz. Mantıklı olan budur. Ama aslında her çalışana ofis bilgisayarlarında, ev bilgisayarlarında, hattâ posta odasındaki sayılandırma makinasında kullandıkları kullanıcı adını ve parolayı dışarıya vermelerinin, ATM kartlarının şifresini vermekle eş değer olduğu sık sık hatırlatılmalıdır.

Bazen -ama çok ender olarak- gizli bilgileri bir başkasına vermenin zorunlu hattâ önemli olduğu durumlar söz konusu olabilir. Bu nedenle "hiçbir zaman" konusunda katı kurallar oluşturmak, yerinde olmayacaktır. Yine de güvenlik kurallarınız ve süreçlerinizde, bir çalışanın parolasını başkasına verebileceği durumların ve -daha da önemlisi- bu bilgiyi kimin sormaya yetkili olduğunun açıkça belirtilmesi gerekmektedir.

Kaynağın Değerlendirilmesi

Pek çok kuruluşta, kural, şirkete ya da başka bir çalışana zarar verebilecek bilgilerin yalnızca yüz yüze bilinen kişilere ya da kuşkuya yer bırakmadan sesinin tanınabildiği kişilere verilebileceği şeklinde olmalıdır.

Üst düzey güvenlik gerektiren durumlarda, sadece kişisel olarak getirilen ya da güvenilir bir yetkilendirmeyle -örneğin önceden kararlaştırılmış gizli bir şifreyle ve zaman ayarlı kartlar gibi iki farklı unsur kullanılarak- gelen talepler değerlendirilmelidir.

Veri koruması süreçleri, şirketin hassas işlevleri olan bir bölümün-

Not: *Şahsen hiç bir işletmede parola değiştokuşuna izin verilmesi gerektiğine inanmıyorum. Çalışanların kişisel parolalarını değiştokuş etmesini ya da paylaşmasını yasaklayan katı bir kural yerleştirmek çok daha kolaydır. Üstelik de çok daha güvenlidir. Ancak her işletmenin bu kararı verirken, kendi kültürünü ve güvenlik yaklaşımlarını göz önünde bulundurması gerekmektedir.*

den kişisel olarak tanınmayan ya da herhangi bir şekilde kefil olunmamış birine bilgi aktarılmamasını ifade etmelidir.

Bu durumda başka bir şirket çalışanından kulağa gerçek gibi gelen bir talebi, örneğin ekibinizdekilerin adlarının ve e-posta adreslerinin listesinin istendiği bir durumu nasıl ele alırsınız? Ya da bazı evrakların sadece şirket içinde dolaşabileceğini çalışanların kafasına nasıl sokarsınız? Çözümün önemli bir parçası, dışarı gönderilecek bilgileri değerlendirmek üzere her birimden birini görevlendirmek olabilir. Bu durumda, görevlendirilen çalışanlara izlemeleri gereken özel kontrol süreçlerinin anlatılacağı bir ileri güvenlik eğitimi verilmelidir.

Kimseyi Unutmayın

Hepimiz çalıştığımız şirketteki yüksek güvenlik gerektiren birimleri ezbere sayabiliriz. Ama çoğunlukla göz önünde olmayan, buna karşın saldırılara oldukça açık olan yerlere dikkat etmeyiz. Bu olaylardan birinde, şirket içindeki bir numaraya faks çekilmesi yeterince masum ve güvenli görünebilir; ancak saldırgan, bu güvenlik açığından yararlanabilir. Buradaki ders: Sekreterler ve idari memurlardan, şirket yöneticileri ve üst düzey idarecilere kadar herkesin bu tarz oyunlara karşı uyanık olmaları için özel güvenlik eğitimleri alması gerektiğidir. Ön kapıyı kollamayı da unutmayın: Danışma görevlileri de toplum mühendislerinin öncelikli hedefleri arasındadır ve bazı ziyaretçiler ve arayanlar tarafından kullanılabilecek aldatma yöntemlerine karşı uyarılmaları gerekir.

Şirket güvenliği tarafından, bir toplum mühendisliği oyununa hedef olduğunu düşünen çalışanlar için bir çeşit bilgi birikim merkezi niteliğinde tek bir iletişim noktası oluşturulması gerekmektedir. Güvenlik olaylarının bildirileceği tek bir noktanın olması, planlı bir saldırı sırasında saldırının ortaya çıkması için etkili bir ön uyarı sistemi oluşmasını sağlayacak, böylece zaman kaybedilmeden durum kontrol altına alınabilecektir.

Not: *Şaşılacak bir şekilde, arayanın adını ve telefon numarasını şirket çalışanları veri tabanından kontrol etmek ve geri aramak bile kesin bir çözüm değil. Toplum mühendisleri şirket veritabanına ad eklemenin ya da telefon aramalarını yönlendirmenin yollarını bilirler.*

6 BANA YARDIMCI OLABİLİR MİSİNİZ?

Yardım teklif ederek toplum mühendislerinin insanları nasıl kandırdıklarını gördünüz. Başka bir sevilen yöntemde ise roller değişir ve toplum mühendisi karşı tarafın yardımına ihtiyacı olduğunu söyleyerek yönlendirme yapar. Zor durumda olan insanlara hep acımışızdır; bu yüzden bu yaklaşım toplum mühendisinin amacına ulaşmasında etkili olduğunu tekrar tekrar kanıtlamıştır.

Ziyaretçi

Üçüncü bölümde anlatılan öykülerden biri, bir saldırganın Sosyal Güvenlik Numarası'nı elde edebilmek için kurbanını nasıl kandırdığından söz ediyordu. Bu seferki toplum mühendisimiz aynı sonucu elde etmek için farklı bir yol izliyor ve sonra da bu bilgiyi kullanıyor.

Jones'ların Çetelesini Tutmak

Silikon Vadisi'nde, adını vermeyeceğimiz bir uluslararası şirket var. Dünyanın her tarafına dağılmış satış bürolarının ve diğer tesislerinin hepsi de bir geniş alan ağı (WAN-Wide Area Network) aracılığıyla şirketin genel müdürlüğüne bağlı. Brian Atterby adında, zeki, kıpır kıpır bir saldırgan, bu tip bir ağa, güvenliğin, genel müdürlüğe göre daha gevşek olduğu en uç noktalarından birinden girmenin daha kolay olduğunu biliyordu.

Saldırgan, Chicago bürosunu aradı ve Bay Jones'la görüşmek istediğini söyledi. Danışmadaki kız ona Bay Jones'un ilk adını bilip bilmediğini sordu; o da, *"Bir yere yazmıştım, bulmaya çalışıyorum. Orada Jones adlı kaç kişi çalışıyor?"* diye sordu. Kız, *"Üç,"* diye yanıtladı. *"Hangi bölümde çalışıyor?"*

"Adları okursanız belki hatırlayabilirim", dedi adam ve kız adları okudu, *"Barry, Joseph ve Gordon."*

"Joseph. Evet adının bu olduğuna eminim" dedi adam. *"Ve şeydeydi... hangi bölümdeydi?"*

"İş geliştirme."

"Hah işte o. Beni ona bağlayabilir misiniz?"

Kız telefonu aktardı. Jones telefonu açtığında saldırgan, *"Bay Jones? Merhaba ben bordro servisinden Tony. Maaş çekinizin doğrudan vakıf hesabınıza yatırılmasıyla ilgili talebinizi az önce yerine getirdik"* dedi.

"NE? Şaka yapıyor olmalısınız. Ben öyle bir talepte bulunmadım. Vakıfta hesabım bile yok."

"Ama... aktarma işlemini tamamladım bile."

Jones maaş çekinin başka birinin hesabına yatabileceği düşüncesine oldukça bozulmuştu ve telefonun diğer ucundaki adamın kafasının biraz yavaş çalıştığını düşünmeye başlamıştı. Jones daha yanıt bile veremeden saldırgan lafa girdi. *"Ne olduğunu kontrol etsem iyi olacak galiba. Maaş bordrosu değişiklikleri Sosyal Güvenlik Numarası'ndan takip ediliyor. Sizin Sosyal Güvenlik Numaranız nedir?"*

Jones numarayı verdi. Arayan, *"Hayır; haklısınız, talep sizden değilmiş"*, dedi. Her yıl daha da aptallaşıyorlar diye düşündü Jones.

"Tamam. Her şeyin düzelmesini sağlayacağım. Hemen bir değişiklik giriyorum. Endişelenmeyin, maaş çekiniz istediğiniz gibi elinize geçecek" dedi adam güven vererek.

Bir İş Gezisi

Bu olaydan kısa bir zaman sonra şirketin Austin-Teksas satış bürosunun sistem yöneticisine bir telefon geldi. *"Ben Joseph Jones"* dedi arayan. *"Genel Müdürlük İş Geliştirme'de çalışıyorum. Bu hafta Austin'de Driskill otelinde kalıyor olacağım. Şehirlerarası telefon bağlantısı kurmama gerek kalmadan e-postalarımı görebilmem için bana geçici bir hesap açmanızı rica edecektim."*

"İsminizi bir kez daha alayım, ayrıca Sosyal Güvenlik Numaranız da gerekiyor" dedi sistem yöneticisi. Sahte Jones numarayı verdi ve sürdürdü, *"Bağlantı hızı yüksek hatlarınız var mı?"*

"Bir dakika dostum. Veri tabanında olup olmadığına bakmam gerek." Kısa bir süre sonra, *"Evet, Joe. Bina numarası söyler misin?"* diye sordu adam. Saldırgan ödevini yapmıştı ve oda numarasını söyledi.

"Tamam" dedi sistem yöneticisi.

İş bu kadar kolaydı. Sistem yöneticisi, Joseph Jones adına, birimine ve özlük numarasına veri tabanından bakmış ve "Joe" da kontrol sorusuna doğru yanıtı vermişti. *"Kullanıcı adın şirket kullanıcı adınla aynı olacak, jbjones"* dedi sistem yöneticisi, *"ve başlangıç olarak giriş parolan 'degistirbeni' olacak."*

Mitnick Mesajı:

Bilgilerinizi korumak için güvenlik duvarlarına ve başka koruyucu unsurlara bel bağlamayın. En zayıf noktanıza bakın. Bu açığın çoğunlukla çalışanlarınızda olduğunu göreceksiniz.

Aldatmacanın İncelenmesi

On beş dakikalık bir zaman içinde yapılan birkaç telefon konuşması sonucunda saldırgan, şirketin ağına erişim elde etti. Bu şirket de pek çokları gibi *draje güvenlik* olarak söz edeceğim bir güvenlik sistemine sahipti. Bu deyim ilk olarak, Steve Bellovin ve Steven Cheswick adındaki iki Bell Laboratuvarları araştırmacısı tarafından kullanılmış. Bu tarz güvenlik sistemlerini, "dışı sert, içi ise yumuşak" olarak bir çikolata drajesine benzeterek açıklamışlar. Bellovin ve Cheswick'e göre dış kabuk, yani güvenlik duvarı, yeterli koruma sağlamaz; çünkü saldırgan onu bir kez aşmayı başardıktan sonra dahili bilgisayar ağlarının yumuşak, kolay çiğnenebilir güvenlik sistemleriyle karşılaşır. Çoğu zaman bunların sağladığı koruma da yetersizdir.

Terimler

DRAJE GÜVENLİK: Bell Laboratuvarları'ndan Bellovin ve Cheswick tarafından güvenlik duvarı gibi bir dış çeperin kuvvetli olduğu ama arkasındaki yapının zayıf kaldığı güvenlik senaryolarını açıklamak için kullanılmış. Bu deyimde sert kabuklu ve içi yumuşak M&M drajelerinden esinlenilmiş.

Bu öykü tanıma uyuyor. Bir arama numarası bir de geçici hesapla, saldırgan, bir internet güvenlik duvarını yıkma işiyle bile uğraşmaz ve içeri girdikten sonra dahili ağdaki bilgisayar sistemlerinin çoğuna erişebilir.

Kaynaklarımdan öğrendiğim kadarıyla bu oyun dünyanın en büyük yazılım şirketlerinden biri üzerinde tam anlamıyla oynanmış. Böyle bir şirketin sistem yöneticilerinin bunun gibi bir oyuna düşmeyecek şekilde eğitimli olduklarını düşünürsünüz. Ama benim deneyimlerime göre, toplum mühendisi yeterince akıllı ve ikna edici olduğu takdirde hiç kimse tam olarak güvende değildir.

Beni Şu Gönderdi Tarzı Güvenlik

Eski 'Beni şu gönderdi' barları zamanında -yani, içki yasağı döneminde, küvette yapılmış içkilerin su gibi aktığı gece klüplerinde- yeni gelen müşterinin içeri alınması için kapıya kadar gelip kapıyı çalması gerekirdi. Birkaç saniye sonra kapının üzerinde küçük bir yer açılır ve sert, tehditkâr bakışlı bir yüz oradan dışarı bakardı. Eğer müşteri, olan bitenden haberdarsa, bu bara sık gelen birinin adını söyler ("Beni Joe gönderdi" demek çoğu zaman yeterli olurdu) ve içerideki fedai, kapıyı açıp onu içeri alırdı.

Asıl numara "beni şu gönderdi" barının yerini öğrenmekti, çünkü kapıda herhangi bir işaret yoktu ve barın sahipleri varlıklarını duyurmak

Terimler

"BENİ ŞU GÖNDERDİ" TARZI GÜVENLİK: Bilginin nerede olduğunu bilmeye ve o bilgiye ya da bilgisayar sistemine erişmek için bir kelime ya da ad kullanmaya dayanan güvenlik şeklidir.

için dışarı neon tabelalar asmıyorlardı. Doğru yerde bulunmak çoğunlukla içeri girebilmek için yeterliydi. Benzer bir güvenlik yöntemi, şirket dünyasında da ne yazık ki sıkça kullanılıyor ve 'beni-şu-gönderdi' tarzı güvenlik adını vereceğim, işe yaramaz bir koruma sağlıyor.

Filmlerde Gördüm

İşte size pek çok insanın hatırlayacağı güzel bir filmden bir örnek. Akbabanın'ın Üç Günü'nde (Three Days of the Condor) Robert Redford'un oynadığı baş karakter Turner, CIA adına iş yapan küçük bir araştırma şirketinde çalışmaktadır. Bir gün öğle yemeğinden döndüğünde tüm arkadaşlarını vurularak öldürülmüş bulur. Kim olduklarını bilmediği kötü adamların kendisini aradıklarını bilerek bu olayı kimin ve neden yaptığını bulmaya çalışır.

Hikâyenin ilerisinde Turner kötü adamlardan birinin telefon numarasını öğrenmeyi başarır. Ancak bu adam kimdir ve Turner onun nerede olduğunu nasıl bulabilir? Turner'ın şansı yaver gider, çünkü senaryo yazarı David Rayfiel, Turner'ın geçmişine muhabere bölüğünde telefon hattı teknisyeni olarak eğitim almış olma özelliğini koymuş, böylece onu telefon şirketinin yöntemleri ve uygulamaları hakkında bilgili kılmıştı. Turner, kötü adamın telefon numarasıyla ne yapması gerektiğini gayet iyi biliyordu. Senaryo metninde sahne şöyle anlatılır:

TURNER YENİDEN BAĞLANIR ve BAŞKA BİR NUMARA ÇEVİRİR.

ZIRR! ZIRR! Sonra:

KADIN SESİ (FİLTRELENMİŞ)

MAA, Bayan Coleman konuşuyor.

TURNER (ahizeye konuşur)

Ben Harold Thomas, Bayan Coleman. Müşteri Hizmetleri. 202-555-7389 için MAA lütfen.

KADIN SESİ (FİLTRELENMİŞ)

Bir dakika lütfen.

(hemen sonra)

Leonard Atwood, 765 MacKensie Yolu, Chevy Chase, Maryland

Senaryo yazarının bir Maryland adresi için yanlışlıkla bir Washington alan kodu kullanıyor olması dışında burada ne olduğunu anlayabildiniz mi?

Mitnick Mesajı:

Gizlilik üzerinden güvenlik sistemleri toplum mühendisliği saldırılarını engellemekte etkisizdirler. Dünyadaki herhangi bir bilgisayar sistemini kullanan en az bir insan vardır. Bu yüzden, eğer saldırgan, sistemleri kullanan insanları etkileyebilirse, sistemin gizliliği anlamsız olacaktır.

Aldığı telefon hattı teknisyenliği eğitimi nedeniyle Turner, bir telefon şirketinin MAA (Müşteri Ad ve Adresi) bürosuna ulaşmak için hangi numarayı çevirmesi gerektiğini biliyordu. MAA, tesisatçılar ve diğer yetkili telefon şirketi çalışanlarına kolaylık sağlaması için kurulmuştu. Bir tesisatçı MAA'yı arar ve telefon numarasını verirdi. MAA memuru ise telefon numarasının ait olduğu kişinin adını ve adresini bulup tesisatçıya verirdi.

Telefon Şirketini Kandırmak

Gerçek dünyada MAA'nın telefon numarası çok iyi saklanan bir sırdır. Her ne kadar telefon şirketleri şimdilerde işi sıkıya almış ve bilgi vermek konusunda pek cömert davranmıyor olsalar da, o zamanlar güvenlik uzmanlarının gizlilik üzerinden güvenlik adını verdikleri bir çeşit 'beni şu gönderdi' tarzı güvenlik uygulaması kullanıyorlardı. MAA'yı arayan ve terminolojiyi bilen herhangi birinin ("Müşteri Hizmetleri. 555-1234'le ilgili MAA lütfen" gibi) bilgi almak için yetkili olduğunu varsayıyorlardı.

Ne kendinizi tanıtmaya, ne kimliğinizi kanıtlamaya, ne Sosyal Güvenlik Numaranızı vermeye, ne de hergün değişen bir parola girmeye gerek yoktu. Eğer aramanız gereken numarayı biliyorsanız ve sesiniz inandırıcı geliyorsa, o zaman bu bilgiyi almaya hakkınız var demekti.

Bu, telefon şirketi açısından çok yerinde bir varsayım değildi. Güvenliği sağlamak yolundaki tek çabaları yılda bir kereden az olmamak üzere dönem dönem telefon numarasını değiştirmekti. Buna rağmen bu numaralar hangi dönemde olursa olsun bu kullanışlı bilgi kaynağından yararlanmaktan ve başka beleşçi arkadaşlarıyla yaptıklarını paylaşmaktan hoşlanan telefon beleşçileri arasında yaygın olarak bilinen numaralardı. MAA bürosu dalaveresi, gençliğimde hobi olarak telefon beleşçiliği yaptığım zamanlarda ilk öğrendiğim şeylerden biriydi.

Terimler

GİZLİLİK ÜZERİNDEN GÜVENLİK: Sistemin (protokollerin, algoritmaların ve dahili sistemlerin) çalışma bilgileriyle ilgili ayrıntıları gizli tutmaya dayanan etkisiz bir bilgisayar güvenlik yöntemidir. Gizlilik üzerinden güvenlik, güvenilir bir grup insan dışında kimsenin sisteme giremeyeceği gibi bir yanlış inanışa dayanır.

İş dünyasında ve devlet dairelerinde 'beni şu gönderdi' tarzı güvenlik sistemleri kullanılmaya devam edilmektedir. Şirketinizin birimleri, çalışanları ve terminolojisiyle ilgili yeterli bilgiyi toplamış o kadar da becerikli olmayan herhangi bir saldırganın kendini yetkili biri olarak tanıtması olasıdır. Bazen daha azı bile yeterli olur. Tüm gereken şey dahili bir telefon numarasıdır.

Dikkatsiz Bilgisayar Yöneticisi

Her ne kadar şirketlerde çalışan pek çok kişi güvenlik açıklarına karşı ihmalkâr, ilgisiz ve dikkatsiz olsa da, Fortune 500 şirketleri arasında bulunan bir bilgisayar merkezinde yönetici ünvanıyla bulunan birinin en iyi güvenlik uygulamaları konusunda bilgili olmasını beklersiniz, öyle değil mi?

Şirketinin Bilişim Teknolojileri birimine bağlı olarak çalışan bir bilgisayar merkezi yöneticisinin basit ve bariz bir toplum mühendisliği dalaveresine kurban gideceği aklınızın ucundan bile geçmez. Özellikle de toplum mühendisi ergenlik çağından yeni çıkmış, hâlâ çocuk sayılabilecek biriyse. Ancak bazen beklentilerimizde yanılabiliriz.

Kanalı Ayarlamak

Yıllar önce radyoları yerel polis ya da itfaiye telsiz konuşmalarını dinleyecek şekilde ayarlamak ve her zaman rastlanmayan türden oldukça heyecanlı bir banka soygununu, bir işyeri yangınını ya da süratli bir kovalamacayı daha olaylar olurken dinlemek, vakit geçirmenin eğlenceli yollarından biriydi. Polis teşkilatının ve itfaiyenin kullandığı radyo frekansları köşedeki kitapçıdan alabileceğiniz kitapçıklarda bile bulunuyordu; bugün ise internet üzerinde listeler halinde duruyorlar ve bir kitapçıdan alabileceğiniz kitaplardan, yerel teşkilatların, ilçe, eyalet ve hattâ bazı durumlarda federal büroların bile radyo frekanslarını bulabilirsiniz.

Bunları dinleyenler doğal olarak yalnızca meraklılar değildi. Gecenin bir yarısında market soyan hırsızlar o tarafa doğru bir polis arabasının gelip gelmediğini öğrenmek için polis kanalını dinlerlerdi. Uyuşturucu kaçakçıları Uyuşturucu Masası polislerinin yerel hareketlerini buralardan öğrenirlerdi. Bir kundakçı, önce bir kibrit çakıp sonra da itfaiyeciler söndürmeye çabalarken tüm radyo konuşmalarını dinleyerek hasta zevkini tatmin edebilirdi.

Günümüzde bilgisayar teknolojisindeki gelişmeler ses mesajlarını şifreleme olanağı sağladı. Mühendisler tek bir mikroyongaya daha fazla işlem gücü tıkmanın yollarını bulurlarken, bir yandan da kötü adamlar ve meraklıların dinlememesi için polis kuvvetlerine yönelik küçük, şifreli telsizler üretmeye başladılar.

Kulak Misafiri Danny

Adına Danny diyeceğimiz anten meraklısı ve yetenekli bir bilgisayar korsanı, bu tür telsiz sistemleri üreten büyük firmaların birinden, gizli şifreleme yazılımının kaynak kodunu ele geçirmenin bir yolunu bulup bulamayacağını denemeye karar verdi. Kodu incelemenin, polis teşkilatını dinleyebilmesine olanak sağlayacağını ve belki de, en gelişmiş teknolojiye sahip devlet kurumlarının bile arkadaşlarıyla yaptığı konuşmaları dinlemesini güçleştirecek şekilde teknolojiyi kullanabileceğini umuyordu.

Bilgisayar korsanlarının karanlık dünyanın Danny'leri yalnızca meraklı -ve tamamıyla- zararsız türden adamlarla tehlikeli adamlar arasında özel bir sınıflandırmaya tâbidirler. Danny'ler, sunduğu heyecan için sistemlere ve ağlara giren ve teknolojinin nasıl çalıştığını görmenin keyfini çıkaran muzip bir korsanın merakının yanı sıra bir uzmanın bilgisine de sahiptirler. Ancak onların elektronik ortamları kırma ve o alana girme maceraları gerçekten de yalnızca bir maceradır. Bu adamlar, bu zararsız korsanlar, zevk için sitelere yasadışı giriş yaparlar. Yaptıklarından para kazanmazlar; dosyalara zarar vermezler, ağ bağlantılarını bozmazlar ya da bilgisayar sistemlerini çökertmezler. Onların yalnızca orada olup, güvenlik ve sistem yöneticilerinin sırtı dönükken dosyaları kopyalaması ve parolaları öğrenmek için e-postaları taraması, kendileri gibi davetsiz misafirleri dışarda tutmakla sorumlu adamların kulaklarını bükmektedir. İşin en keyifli yanı karşı tarafa üstünlük sağlamaktır.

Bu tanımlara uygun olarak bizim Danny'miz, yalnızca kendi bastırılamaz merakını tatmin etmek ve üreticinin bulduğu akıllıca yenilikleri takdir etmek için, hedef şirketin en iyi korunan ürününün ayrıntılarını incelemek istiyordu.

Bilindiği üzere, ürün tasarımları şirketin elindeki herhangi bir şey kadar değerli, korunması gereken ve özenle saklanan ticari sırlardır. Danny bunu biliyordu ama zerre kadar umurunda değildi. Ne de olsa, hedefteki, sadece büyük ve isimsiz bir şirketti.

Ancak yazılım kaynak kodunu nasıl elde edecekti? İşlerin gidişine bakılırsa, şirketin Güvenli İletişim Grubu'na ait "kraliyet mücevherlerini" ele geçirmek oldukça kolay olmuştu. Üstelik şirket, insanların kendilerini tanıtmaları için bir yerine iki ayrı anahtar gerektiren iki basamaklı bir kimlik belirleme sistemi kullanıyordu.

İşte size, büyük olasılıkla artık aşina

Terimler

İKİ BASAMAKLI TANIMLAMA: Kimliği belirlemek için iki farklı tanımlama şekli kullanılmasıdır. Örneğin, bir kişinin kendini tanıtabilmek için belirli, tanımlanabilir bir noktadan ve parolayı bilerek araması gerekebilir.

olduğunuz bir örnek. Yeni kredi kartınız geldiğinde, kartın doğru kişinin elinde olduğundan ve birilerinin zarfı posta kutusundan çalmadığından emin olmak için kartı veren şirket onları aramanızı ister. Şu sıralar kartla birlikte gelen talimatlar genellikle evden aramanızı öneriyor. Aradığınızda, kredi kartı şirketindeki yazılım, şirketin ödediği ücretsiz aramaların yapıldığı santralın sağladığı ONT'yi (Otomatik Numara Tanımlayıcısı'nı) çözümlüyor.

Kredi kartı şirketindeki bir bilgisayar, arayan tarafın numarasını şirketin kart sahipleri veri tabanında bulunan numarayla karşılaştırır. Görevli, telefonu açana kadar müşterinin veri tabanından çekilen bilgiler ekranda görünür. Böylece görevli, bilgileri gördüğü anda, aramanın bir müşterinin evinden yapıldığını anlar. Bu, kimlik belirlemenin bir basamağıdır.

Sonra görevli sizinle ilgili önüne çıkan bilgilerden birini seçer -bu çoğunlukla Sosyal Güvenlik Numarası, doğum tarihi ya da annenin kızlık soyadı olur- ve bu bilgiyi doğrulamak için size soru sorar. Eğer doğru yanıtı verirseniz, bu da kimlik belirlemenin, sizin bildiğiniz bir şeye dayanan ikinci basamağını oluşturur.

Hikâyemizde geçen güvenli telsiz sistemlerini üreten şirketin her çalışanının bilgisayara girmek için kullandığı kullanıcı adı ve parolanın yanı sıra bir de *Güvenli Kimlik* dedikleri küçük bir elektronik cihazı vardır. Buna *zaman tabanlı anahtar* denir. Bu cihazlar iki çeşittir: Biri bir kredi kartının yarısı boyutundadır ama biraz daha kalındır; diğeri ise insanların anahtarlıklarına takabilecekleri kadar küçüktür.

Şifreleme dünyasının bir eseri olan bu aletin üzerinde altı basamaklı bir sayı gösteren küçük bir ekran vardır. Her altmış saniyede bir ekranda farklı bir altı basamaklı sayı görünür. Yetkili bir kişinin, dışarıdan ağa gireceği zaman, önce gizli bir kişisel kimlik numarası sonra da anahtar cihazında görünen sayıları girerek kendini yetkili biri olarak tanıtması gerekir. Dahili sistem tarafından tanındıktan sonra kullanıcı adını ve parolasını yazarak girişi gerçekleştirir.

Genç korsan Danny'nin istediği kaynak kodunu alabilmesi için yalnızca bir çalışanın kullanıcı adını ve parolasını bulması yetmiyor (ki bu, deneyimli bir toplum mühendisi için çok zor bir iş değildir), aynı zamanda zaman tabanlı anahtar kontrolünü de atlatması gerekiyordu.

Gizli kişisel kimlik numarasıyla birleşmiş zaman tabanlı anahtar kullanılan iki basamaklı bir kimlik belirleme sistemini alt etmek kulağa tam Görevimiz Tehlike'den fırlamış bir iş gibi geliyor. Ama toplum mühendisi için böyle bir işte karşılaşacağı zorluk, özel bir beceriye sahip bir poker oyuncusunun rakiplerinin yüzlerini okumada karşılaştığı zorlukla benzerdir. Şansı yaver giderse, oturduğu masadan, diğer insanlardan aldığı tomarla parayla birlikte kalkabileceğini bilir.

Kaleyi Fethetmek

Danny hazırlıklarını yapmaya başladı. Çok geçmeden gerçek bir çalışan rolünü oynayacak kadar bilgi toplamıştı. Elinde bir çalışanın adı, bölümü, telefon numarası ve Sosyal Güvenlik Numarası'nın yanı sıra yöneticisinin adı ve telefon numarası da vardı.

O anda kelimenin tam anlamıyla fırtına öncesi sessizlik hakimdi. Yaptığı planı uygulayarak bir sonraki adımı atmadan önce Danny'nin yapması gereken birşey daha kalmıştı. Bu, kendi çabalarıyla yapamayacağı bir şeydi. Bir kar fırtınasına ihtiyacı vardı. Danny'nin, çalışanların ofislerine ulaşmasını engelleyecek kadar kötü bir hava için Tabiat Ana'dan küçük bir yardım alması gerekiyordu.

Söz konusu fabrikanın bulunduğu Güney Dakota'da kış mevsiminde kötü hava dileyen birinin çok beklemesi gerekmez. Cuma gecesi fırtına koptu. Kar şeklinde başlayan yağış, soğuk bir yağmura dönüştü ve böylece sabaha kadar tüm yollar kaygan ve tehlikeli bir buz tabakasıyla kaplandı. Danny için bu harika bir fırsattı.

Fabrikayı arayıp, bilgisayar odasını bağlattırdı ve bilgi işlemin işçi arılarından birine, kendini Roger Kowalski olarak tanıtan bir bilgisayar operatörüne ulaştı.

Danny, ele geçirdiği ve gerçek bir çalışana ait olan adı vererek konuştu. "Ben Bob Billings. Güvenli İletişim Grubu'nda çalışıyorum. Şu anda evdeyim ve fırtına yüzünden işe gelemiyorum. Bilgisayarıma ve sunucuya evden ulaşmam gerekiyor ama Güvenli Kimlik Kartı'mı masamda unutmuşum. Onu benim için alır mısınız? Ya da başka biri de alabilir. Sonra ağa girmem gerektiğinde ekranında yazanı bana okuyabilirsiniz. Ekibimin yetiştirmesi gereken önemli bir teslimat var ve bu durumda işi bitirmem mümkün değil. Ofise gelemiyorum, bu taraflardaki yollar çok tehlikeli bir hale geldi."

"Ben Bilgisayar Merkezi'nden ayrılamam" dedi bilgisayar işletmeni.

Danny hemen atladı, "Sizin bir Güvenli Kimlik Kartınız var mı?

"Bilgisayar Merkezi'nde bir tane var," dedi işletmen. "Acil bir durumda işletmenlerin kullanması için."

"Tamam" dedi Danny. "Bana büyük bir iyilik yapabilir misin? Ağa girmem gerektiği zaman Güvenli Kimlik Kartı'nı kullanabilir miyim? Yalnızca yollar düzelene kadar."

"Adınız ne demiştiniz?" diye sordu Kowalski

"Bob Billings."

"Kimle çalışıyorsunuz?"

"Ed Trenton'la."

Zor bir durumda kalma tehlikesi varsa, iyi bir toplum mühendisi, yapılması gerekenden daha fazla araştırma yapar. "İkinci kattayım" diye devam etti Danny. "Roy Tucker'in yanında oturuyorum."

Adam bu adı da biliyordu. Danny onu işlemeye devam etti. "Masama gidip Güvenli Kimlik Kartı'mı alıp gelirseniz çok daha kolay olabilir."

Danny adamın bunu yapmayacağından oldukça emindi. Her şeyden önce mesaisinin ortasında işi bırakıp koridorlardan geçip merdivenlerden çıkıp binanın öbür köşesine gitmek istemeyecekti. Ayrıca başka birinin masasının başına geçip özel eşyalarını karıştırır gibi bir durumda kalmak da istemezdi. Evet, bunu yapmayacağı üstüne oynamak yerinde olacaktı.

Kowalski yardıma ihtiyacı olan birine hayır demek istemiyordu ama evet deyip başını belaya sokmak da istemiyordu. Bu yüzden karar vermekten çekinerek yana adım attı. "Müdürüme sormam gerekecek. Biraz bekler misiniz?" Telefonu bıraktı ve Danny onun başka bir telefonu alıp, bir numara çevirdiğini sonra da isteğini birine anlattığını duydu. O anda Kowalski açıklaması güç birşey yaptı. Bob Billings adını kullanan adama kefil olmuştu. "Onu tanıyorum" dedi yöneticisine. "Ed Trenton için çalışıyor. Bilgisayar Merkezindeki Güvenli Kimlik Kartı'nı kullanmasına izin verebilir miyiz?" Danny telefon elinde amacına verilen bu olağanüstü ve beklenmedik destek karşısında şaşırıp kalmıştı. Ne şansına ne de kulaklarına inanamıyordu.

Birkaç dakika sonra Kowalski telefonu yeniden eline aldı. "Müdürüm sizinle şahsen konuşmak istiyor" dedi ve ona müdürünün adını ve cep telefonu numarasını verdi.

Danny müdürü aradı ve üzerinde çalıştığı projenin ayrıntılarını ve ekibinin önemli bir teslimatı yetiştirmesi gerektiğini de ekleyerek tüm hikâyeyi bir kez daha anlattı. "Biri gidip kartımı alabilirse daha kolay olur" dedi. "Masamın kilitli olduğunu sanmıyorum, sol üst çekmecede olmalı."

"Peki" dedi müdür, " Yalnızca hafta sonu için olmak kaydıyla sanırım Bilgisayar Merkezi'ndekini kullanmanıza izin verebiliriz. Görevli arkadaşlara aradığınızda erişim şifresini size okumalarını söyleyeceğim" dedi ve onunla birlikte kullanılacak kişisel tanıtım numarasını da verdi.

Tüm hafta sonu boyunca şirket bilgisayarına girmek istediği zaman Danny'nin yaptığı tek şey Bilgisayar Merkezi'ni aramak ve Güvenli Kimlik Kartı'nda yazan altı basamaklı sayıyı okumalarını rica etmek oldu.

İşi İçerden Bitirmek

Şirketin bilgisayar sistemine girdikten sonra ne olacaktı? Danny aradığı yazılımın bulunduğu sunucuya girmenin yolunu nasıl bulacaktı?

Bunun için zaten hazırlıklıydı.

Bilgisayar kullanıcılarının çoğu tartışma guruplarını bilirler. Bunlar, insanların yanıt aradıkları sorularını koydukları ya da müzik, bilgisayar ve daha yüzlerce başka konuda sanal arkadaşlar edinmek için kullandıkları elektronik bülten panolarıdır.

Bir tartışma gurubu sitesine mesaj bıraktıklarında, mesajlarının yıllarca çevrimiçi ve erişilebilir kalacağını pek az kişi bilir. Örneğin Google'ın, bazılarının tarihi yirmi yıl öncesine dayanan yedi yüz milyon mesajlık bir arşivi vardır! Danny işe http://groups.google.com adresine girmekle başladı.

Arama metni olarak "şifreli telsiz iletişimi" ve şirketin adını girip bir çalışana ait yıllar öncesinden kalmış bir mesaj buldu. Şirketin bu ürünü geliştirmeye başladığı yıllarda, herhalde polis teşkilatlarının ve federal büroların telsiz sinyallerini karıştırmayı düşünmelerinden çok önce bırakılmış bir mesajdı.

Mesajda gönderenin adı da bulunuyordu. Yalnızca adı değil, telefon numarası ve hattâ çalıştığı grubun adını vardı; Güvenli İletişim Grubu.

Danny telefonu açıp numarayı çevirdi. Yaptığı çok uzun bir atış gibi görünüyordu. Adam, yıllar sonra da aynı kuruluş için çalışmaya devam ediyor muydu? Böyle fırtınalı bir hafta sonunda iş yerinde olabilir miydi? Telefon bir kez, iki kez, üç kez çaldı ve sonunda açıldı. Açan kişi, "Ben Scott" dedi.

Danny, şirketin Bilgi İşlem Bölümü'nden olduğunu söyleyerek geliştirme işleri için kullanılan sunucuların adını vermeye (önceki bölümlerden artık aşina olduğunuz yollardan birini kullanarak) Scott'u ikna etti. Bu sunucularda, şifreli telsizlerde kullanılan, şirkete özgü algoritmaların ve yazılımların kaynak kodlarının bulunduğunu düşünüyordu.

Danny gittikçe yaklaşıyor ve heyecanı da giderek artıyordu. Çok az insanın başarabileceğini bildiği bir şeyi başardığında hissedeceği heyecanın ve büyük coşkunun beklentisi içindeydi.

Yine de henüz hedefine ulaşmamıştı. Yardımsever bilgisayar merkezi müdürü sayesinde tüm hafta sonu boyunca şirketin ağına istediği zaman girebiliyordu. Ayrıca hangi sunuculara erişmesi gerektiğini de biliyordu. Ancak bağlanmaya çalıştığında, oturum açtığı uçbirim sunucusu Güvenli İletişim Grubu geliştirme sistemlerine girmesine izin vermedi. O grubun bilgisayar sistemlerini koruyan bir iç güvenlik duvarı ya da yönlendirici olmalıydı. Girmek için başka bir yol bulması gerekiyordu.

Bir sonraki adım gözünü karartmasını gerektirmişti. Danny, Bilgisayar Merkezi'nde çalışan Kowalski'yi aradı ve, "Sunucum bağlanmama izin vermiyor" diye şikâyet etti. "Telnet kullanarak kendi sistemime bağlanabilmem için sizin bölümün bilgisayarlarında benim için bir hesap açabilir misiniz?"

Müdür zaten zaman tabanlı anahtarın sağladığı erişim şifresinin verilmesini onaylamıştı, bu yüzden böyle bir istek tuhaf karşılanmadı. Kowalski, Bilgisayar Merkezi bilgisayarlarından birinde geçici bir hesap açtı ve bir de parola verdi. Danny'e de, "İhtiyacınız kalmadığı zaman haber verirseniz, hesabı kaparım." dedi.

Geçici hesaba girdikten sonra Danny, ağ üzerinden Güvenli İletişim Grubu'nun bilgisayar sistemlerine bağlanmayı başardı. Ana geliştirme sunucusuna bağlanabilmek amacıyla teknik bir açık bulabilmek için bir saat boyunca çevrimiçi arama yaptı ve sonunda turnayı gözünden vurdu. Görünüşe göre sistem ya da ağ yöneticileri işletim sistemlerinde uzaktan erişime izin veren güvenlik hatalarıyla ilgili gelişmelerden haberdar değillerdi. Ama Danny haberdardı.

Kısa süre içerisinde, aradığı kaynak kodlarını buldu ve ücretsiz saklama alanı veren bir e-ticaret sitesine aktardı. Dosyalar bulunsa bile bu siteden kimse onun izini süremezdi.

Açtığı oturumu kapatmadan önce atması gereken bir adım daha vardı: Bıraktığı izleri dikkatle temizlemesi gerekiyordu. Cumartesi gecesi Jay Leno'nun programı bittiğinde o da kendi işini bitirdi. Danny bunun çok verimli bir hafta sonu olduğuna karar verdi. Üstelik de kendini hiç riske atması gerekmemişti. Baş döndürücü bir heyecandı, hattâ kayak sörfünden (snowboard) ve serbest atlayıştan (sky diving) bile daha heyecan vericiydi.

Danny o gece sarhoş oldu ama viski, cin, bira ya da sake içerek değil. Aşırdığı dosyalara bakarken, parmaklarının arasından kaymaya çalışan son derece gizli telsiz yazılımına yaklaşmanın verdiği güç ve başarı duygusuyla sarhoş olmuştu.

Aldatmacanın İncelenmesi

Bir önceki öyküde olduğu gibi, bu oyunun da işe yaramasının tek nedeni, bir şirket çalışanının, arayan kişinin söylediği kişi olduğunu, sorgulamadan kabullenmesidir. Sorunu olan bir mesai arkadaşına yardım etmek sanayi tekerinin dönmesini sağlayan ve bazı şirketlerin personeliyle çalışmayı diğerlerine göre daha keyifli hale getiren bir unsurdur. Öte yandan bu yardımseverlik, bir toplum mühendisinin sömürebileceği önemli bir zaaf da olabilir.

Danny'nin kullandığı başka bir yöntem ise nefisti. Birinin masasından Güvenli Kimlik Kartı'nı alıp gelmesi talebinde bulunurken sürekli

Mitnick Mesajı:

Bu öyküde anlatılanlar zaman tabanlı analizlerin ve benzer tanımlama yöntemlerinin kurnaz bir toplum mühendisine karşı koruma sağlamadıklarını bize gösteriyor. Tek savunma, güvenlik politikalarını bilen ve başkalarının kötü niyetle davranışlarını etkileyebileceğinin farkında olan sağduyulu bir çalışandır.

olarak emreder gibi konuşuyordu. Kimse emir almaktan hoşlanmaz. Bu tavrıyla Danny o isteğinin geri çevrilmesini sağladı ve başka bir çözüm önerisini kabul etti. Bu da tam istediği şeydi.

Bilgisayar Merkezi işletmeni Kowalski, Danny'nin adlarını verdiği kişileri tanıması nedeniyle tuzağa düşmüştü. Ama neden Kowalski'nin müdürü, hem de bir bilgi işlem yöneticisi, tanımadığı birinin şirketin dahili ağına girmesine izin verdi? Çünkü toplum mühendisinin araçları arasında yardım talebi en güçlü silahlardan biridir.

Böyle bir şey sizin şirketinizde de olabilir mi? Yoksa çoktan oldu mu?

Aldatmacanın Engellenmesi

Yardımcı olan kişinin, arayanın gerçek bir çalışan olup olmadığını kontrol etmeden ve gerekli önlemleri almadan saldırgana şirket ağına dışarıdan girebilme hakkını tanıması bu öykülerde sık sık tekrarlanan bir konu gibi görünüyor. Neden bu konuya bu kadar fazla değiniyorum dersiniz? Çünkü bu, pek çok toplum mühendisliği saldırısının en önemli unsuru, bir toplum mühendisinin amacına ulaşmasının en kolay yoludur. Neden bir saldırgan basit bir telefon konuşmasıyla bu işi halledebilecekken saatlerce güvenlik duvarlarını (firewall) kırmaya uğraşsın?

Toplum mühendisinin bu tarz bir saldırıyı gerçekleştirmek için kullandığı en güçlü yöntemlerden biri, saldırganlar tarafından sıkça kullanılan, yardıma ihtiyacı olduğu oyununu oynamaktır. Çalışanlarınızın müşterilere ve mesai arkadaşlarına yardımcı olmalarını engellemek istemeyeceğinize göre onları, bilgisayar erişimi ya da gizli bilgiler talep eden kişilere karşı kullanmaları için özel kontrol süreçleriyle donatmanız gerekmektedir.

Şirket güvenliği süreçleri, çeşitli durumlarda ne tür kontrol mekanizmalarının kullanılacağını ayrıntılı olarak anlatmalıdır. On yedinci bölümde süreçlerin ayrıntılı bir listesini bulabilirsiniz, ancak işte size göz önünde bulundurulabilecek bir takım kurallar:

- İstekte bulunan kişinin kimliğini kontrol etmek için kullanılabilecek en iyi yollardan biri o kişinin şirket rehberindeki telefonunu

aramaktır. Eğer kişi bir saldırgansa, o zaman kontrol telefonu ya sahte çalışan diğer hattâ beklerken gerçek kişiyle konuşmanızı ya da çalışanın bıraktığı sesli mesaja ulaşıp çalışanın sesini saldırganın sesiyle karşılaştırmanızı sağlar.

- Eğer kimlik kontrolü için şirketinizde Sosyal Güvenlik Numarası kullanılıyorsa, bu durumda bu numaraların hassas bilgi sayılması ve özenle korunup yabancılara verilmemesi gerekmektedir. Aynı şey dahili telefon numaraları, birim fatura bilgileri, hattâ e-posta adresleri gibi her türlü dahili tanımlayıcı için de geçerlidir.

- Şirket eğitimleri herkesin dikkatini, yetkili ve bilgili göründükleri için bilinmeyen kişilerin şirket çalışanı varsayılmaları uygulamasına çekmelidir. Bir kişinin şirket uygulamalarını bilmesi ya da şirket içi terimleri kullanması kimliğinin kontrol edilmemesi için yeterli neden değildir.

- Güvenlik görevlileri ve sistem yöneticileri sadece herkesin güvenlik kurallarına ne kadar uyduğunu görecek şekilde konuya odaklanmamalıdırlar. Aynı kurallara, süreçlere ve uygulamalara kendilerinin uyduğundan da emin olmalıdırlar.

- Parola ve benzeri şeyler, doğal olarak, hiçbir zaman başkasına verilmemelidir. Başkalarına verilmeyle ilgili kural, zaman tabanlı anahtarlar ve diğer tanımlama yöntemleri söz konusu olduğunda daha da önemli olmaktadır. Bu unsurlardan herhangi birinin başkalarına verilmesinin, şirketin bu sistemleri kurma amacına bütünüyle aykırı olduğunun herkesçe bilinmesi gerekmektedir. Başkalarına verilmesi, izinin sürülemeyeceği anlamına gelir. Eğer bir güvenlik sorunu yaşanırsa ya da bir şeyler ters giderse, kimin sorumlu olduğunu bulamazsınız.

- Bu kitapta hep vurguladığım gibi, çalışanların kendilerine gelen talepleri dikkatle değerlendirebilmeleri için toplum mühendisliği hilelerinin ve tekniklerinin bilincinde olmaları gerekmektedir. Güvenlik eğitiminin bir parçası olarak rol yapma eğitimlerini de göz önüne alabilirsiniz, böylece çalışanlarınız toplum mühendisinin nasıl çalıştığını daha iyi anlayabilirler.

7 DÜZMECE SİTELER VE TEHLİKELİ EKLER

"Karşılıksız hiçbir şey olmaz" diye eski bir söz vardır. Buna karşın bedava bir şeyler sunma tuzakları hem yasal ("Ama durun-dahası var! Hemen arayın ve yanında bir bıçak seti bir de mısır patlatma makinası verelim!") hem de o kadar da yasal olmayan ("Florida'da bir dönüm bataklık arazisi alın, ikinci dönüm bedavaya gelsin!") işler için önemli bir ilgi çekme yolu olmayı sürdürüyor.

Pek çoğumuz bedava birşeyler elde etmeye o kadar hevesliyiz ki yapılan öneri ya da verilen söz üzerinde mantıklı düşünemeyecek durumda olabiliyoruz. Şu yaygın uyarıyı hepimiz biliyoruz; "müşterilerin dikkatine"; ama artık başka bir uyarıyı daha dikkate almanın zamanı geldi: Bedava yazılımlara ve "hadi tıkla" diyen e-posta eklerine dikkat. Bilinçli bir saldırgan, bir şirket ağına girebilmek için bedava bir hediyeye karşı duyduğumuz doğal dürtüye hitap etmek dahil, neredeyse her yolu kullanacaktır. İşte birkaç örnek.

Bedava Bir (Boşluk) İstemez Miydiniz?

Tıpkı virüslerin zamanın başlangıcından bu yana insanoğlunun ve tıp uzmanlarının başına bela olmaları gibi, çok isabetli biçimde adlandırılmış bilgisayar virüsleri de teknoloji kullanıcılarının başına benzer bir bela açmışlardır. En çok zarar veren virüsler, -hiç de tesadüf olmayan bir biçimde- en çok ilgiyi toplayan ve göz önünde bulunanlar olmuştur. Bunlar bilgisayar *vandallarının* ürünleridir.

Kötü huylu bilgisayar vandallarına dönüşen bilgisayar hastaları, ne kadar zeki olduklarını gösterebilmek için uğraşıp didinirler. Bazen yaptıklarıyla bir kabul törenindeymiş gibi daha yaşlı ve deneyimli bilgisayar korsanlarını etkilemek amacındadırlar. Bu insanlar, zarar vermek üzere tasarlanmış bir virüs ya da solucan yaratmaya güdülenmişlerdir. Eğer yaptıkları iş dosyaları yok edip, sabit sürücüleri göçertiyorsa ve kendini gizlice binlerce insana gönderebiliyorsa, vandallar başarıları karşısında gururla kabarırlar. Eğer virüs, gazetelerin yazacağı kadar ve ana haberlerde ona karşı uyarılar yayınlanacak kadar kargaşa yarattıysa daha da iyi olur.

Vandallar ve virüsleriyle ilgili pek çok şey yazıldı; kitaplar: yazılımlar; ayrıca koruma sağlamak için şirketler kuruldu ama biz burada onların teknik saldırılarına karşı savunmalardan sözetmeyeceğiz. Bizim şu anki ilgi noktamız vandalın yıkıcı hareketlerinden çok onun uzaktan akrabası olan toplum mühendisinin maksatlı çabaları üzerinde olacak.

E-postayla Geldi

Her gün reklam mesajları içeren ya da ne istediğiniz, ne de ihtiyacınız olan birşeyleri bedava olarak sunan istenmeyen e-postalar alıyorsunuzdur. Nasıl şeyler olduklarını biliyorsunuz. Yatırım danışmanlığı, bilgisayarlar, televizyonlar, kameralar, vitaminler ya da seyahatler için indirimler; ihtiyacınız olmayan kredi kartları için fırsatlar; ücretli televizyon kanallarını bedava seyretmenizi sağlayacak bir cihaz; sağlığınızı ya da seks gücünüzü artırmanın yolları ve daha neler neler.

Ama arada bir, elektronik posta kutunuzda sizin de ilginizi çeken bir teklif gözünüze ilişebilir. Belki bedava bir oyundur, en sevdiğiniz yıldızın 94 fotoğraflık albümüdür, bedava bir takvim programıdır ya da bilgisayarınızı virüslere karşı koruyacak çok uygun fiyatlı bir paylaşım yazılımıdır. Sunulan herneyse, denemeniz için sizi ikna etmeye çalıştığı dosyayı indirmeniz için sizi yönlendirir.

Ya da belki konu satırında "Dan, seni özledim" ya da "Anna, neden bana yazmadın" ya da "Selam Tom, işte sana söz verdiğim seksi fotoğraf" gibi şeyler yazan mesajlar alırsınız. Böylece fotoğrafa bakmak ya da mesajı okumak için eki açarsınız.

Tüm bu hareketler -reklam e-postalarından öğrendiğiniz yazılımları indirmek, sizi daha önce duymadığınız bir siteye yönlendirecek bir bağlantıya tıklamak, tanımadığınız birinden gelen bir eki açmak- belaya davetiye çıkarmaktır. Şu da var ki, çoğu zaman ne bekliyorsanız tam olarak onu görürsünüz ya da daha kötüsü ümitleriniz boşa çıkar ya da sevimsiz şeylerle karşılaşırsınız ama bunlar zararsızdır. Ama bazen, karşınıza çıkan şey bir vandalın eseridir.

Bilgisayarınıza kötü huylu bir kod göndermek saldırının yalnızca küçük bir parçasıdır. Saldırının başarılı olabilmesi için saldırganın sizi eki indirmeye ikna etmesi gerekir.

En çok zarar veren kötü huylu solucanların birkaçını belirtmek gerekirse, Love Letter, SirCam ve Anna Kournikova gibi, hepsi de yayılabilmek için toplum mühendisliği aldatma tekniklerine dayanmışlar ve birşeyleri karşılıksız elde etme isteğimizden yararlanmışlardı. Solucan, gizli bilgiler ve bedava porno gibi ilgi çekici bir şey sunan ya da çok zekice bir hileyle, sizin güya sipariş etmiş olduğunuz çok pahalı bir eşyanın faturasının ekte olduğunu söyleyen bir mesaj içeren bir

NOT: *Bilgisayar dünyasında Uzaktan Erişimli Truva Atı (Remote Access Trojan) olarak bilinen bir çeşit program, saldırganın bilgisayarınız üzerinde tam bir kontol kurmasını sağlar, tıpkı sizin klavyenizin başında oturuyormuş gibi!*

e-postanın eki olarak gelir. Bu son tuzak kredi kartınızdan sipariş etmediğiniz bir ürünün parasının çekildiği endişesiyle sizi eki açmaya yönlendirir.

Ne kadar çok insanın bu tuzaklara düştüğünü bilmek şaşırtıcıdır; e-posta eklerini açmanın tehlikeleri konusunda tekrar tekrar uyarılmamıza rağmen tehlikeye karşı duyarlılığımız zaman içinde azalır ve her birimizi savunmasız bırakır.

Terimler

MALWARE (Kötü huylu yazılımın argo karşılığı) bir virüs, solucan ya da Truva Atı gibi zarar verici işlemler yapan bilgisayar programı.

Zararlı Yazılımların Belirlenmesi

Başka türlü bir *zararlı yazılım* (malware-malicious software) ise sizin bilginiz ya da onayınız dışında çalışan ve siz farkında olmadan görevini yerine getiren bir programı bilgisayarınıza yükler. Zararlı yazılımlar başta oldukça masum görünebilir hattâ bir Word™ dökümanı ya da Powerpoint™ sunumu ya da makro işlevleri olan herhangi bir program olabilir ama bunlar başka bir programı gizlice yükleyeceklerdir. Örneğin, zararlı yazılım, Bölüm 6'da sözü edilen Truva Atı'nın bir çeşidi olabilir. Bu yazılım makinanıza bir kez kuruldu mu, yazdığınız her karakteri -tüm parolalarınız ve kredi kartı numaralarınız dahil- saldırgana bildirir.

Şok edici bulabileceğiniz başka iki tür zararlı yazılım daha var. Bir tanesi saldırgana bilgisayar mikrofonunuzun civarında konuştuğunuz her kelimeyi bildirir (mikrofonunuzun kapalı olduğunu düşündüğünüz zaman bile). Daha da kötüsü, bilgisayarınıza bağlı bir kameranız varsa, bir saldırgan, benzer bir teknik kullanarak terminalinizin önünde olup biten her şeyi, kameranın kapalı olduğunu düşündüğünüz zaman bile, gece ya da gündüz, seyredebilir.

Kötü bir şaka anlayışı olan bir korsan, hınzırlıklarıyla rahatsız edici olmak üzere tasarlanmış küçük bir programı bilgisayarınıza kurmaya çalışabilir. Örneğin CD sürücünüzü ansızın açabilir ya da üzerinde çalıştığınız dosyayı sürekli simge durumuna küçültebilir. Ya da gecenin ortasında çığlık yüklü bir ses dosyasının en yüksek sesle çalmasına neden olabilir. Uyumaya ya da iş yapmaya çalışırken bunların hiçbiri eğlenceli gelmeyecektir... ama en azından kalıcı zarar vermezler.

Mitnick Mesajı:

Hediye veren saçmalıklara dikkat edin, yoksa şirketinizin başına Truva kentinin başına gelenler gelebilir. Ne yapmanız gerektiğini bilemiyorsanız, bir şeylerin bulaşmasını engellemek için koruma kullanın.

Bir Arkadaştan Mesaj

Aldığınız önlemlere karşın senaryolar daha da vahimleşebilir. Düşünün: Şansınızı hiç zorlamamaya karar verdiniz. Artık bildiğiniz ve güvendiğiniz, SecurityFocus.com ya da Amazon.com gibi, güvenlikli siteler dışında hiçbir yerden dosya indirmemeye karar verdiniz. Bilinmeyen kaynaklardan gelen e-postalardaki bağlantılara artık tıklamıyorsunuz. Beklemediğiniz hiçbir e-postadaki eki açmamaya karar verdiniz. Ve e-ticaret işlemleri yapmak ya da kişisel bilgiler alıp vermek için girdiğiniz sitelerde güvenli site simgesi olduğundan emin olmak için internet tarayıcınızı kontrol ediyorsunuz.

Ve bir gün bir dostunuzdan ya da iş arkadaşınızdan, eki olan bir e-posta alıyorsunuz. İyi tanıdığınız birinden geliyorsa zararlı bir şey olamaz, değil mi? Özellikle de bilgisayar verileriniz zarar görürse kimi suçlayacağınızı bildiğiniz sürece.

Eki açıyorsunuz ve... GÜÜM! Az önce bir solucan ya da Truva Atı tarafından vuruldunuz. Tanıdığınız biri neden size bunu yapsın? Çünkü herşey göründüğü gibi değildir. Şunu okumuştunuz: Birinin bilgisayarına giren ve sonra da kendini o kişinin adres listesindeki herkese postalayan solucan. Tüm bu insanlar da bildikleri ve güvendikleri birinden bir e-posta almışlardı ve bu güvenilir e-postaların her birinde, durgun bir göle atılmış bir taşın yarattığı halkalar gibi kendi kendini dağıtan solucanlar da vardı.

Bu tekniğin bu kadar etkili olmasının nedeni bir taşla iki kuş vurma kuramına dayanır: Diğer kuşkulanmayan kurbanlara yayılma becerisi ve güvenilir birinden geliyormuş gibi görünmesi.

Teknolojinin bugünkü seviyesinde, yakın birinden gelen bir e-postanın bile güvenli olup olmayacağını düşünüyor olmanız yaşamın üzücü bir gerçeğidir.

Konu Üzerine Çeşitlemeler

İçinde bulunduğumuz bilgi çağında, görmeyi beklemediğiniz bir internet sitesine yönlendirilmeyi de içeren bir dolandırıcılık çeşidi daha var. Bu sık sık olur ve değişik şekillerde karşımıza çıkar. Aşağıdaki örnek, internet'te dolaşan gerçek bir dümene dayanan tipik bir örnektir.

Mitnick Mesajı:

İnsan, dünyayı ve kendi yaşam tarzını değiştiren pek çok harika şey keşfetmiştir. Ancak teknolojinin her iyi kullanımı için, ister bilgisayar, ister telefon ya da internet olsun, birileri her zaman bunu kendi çıkarları için kötüye kullanmanın yolunu bulurlar.

Mutlu Noeller . . .

Edgar adında emekli bir sigorta satıcısı bir gün PayPal'dan bir e-posta alır. PayPal, hızlı ve elverişli koşullarla çevrim içi ödeme olanakları sunan bir şirkettir ve bu tarz bir hizmet, özellikle ülkenin (hattâ dünyanın) herhangi bir yerinde oturan biri, tanımadığı birinden bir mal satın alırken kullanışlıdır. PayPal, alıcının kredi kartından tutarı çeker ve parayı doğrudan satıcının hesabına aktarır.

Bir antika cam kavanoz koleksiyoncusu olarak Edgar çevrim içi müzayede şirketi olan eBay aracılığıyla birçok kez iş yapmıştır. PayPal'ı sık sık kullanır, bazen haftada birkaç kere de kullandığı olur. Bu yüzden 2001 tatil döneminde aldığı, PayPal'dan geliyor gibi görünen ve PayPal hesabını güncellemesi karşılığında bir ödül sunan bir e-posta Edgar'ın ilgisini çeker. Mesaj şöyledir:

> Mutlu Yıllar Değerli PayPal Müşterisi;
>
> Yeni yıl yaklaşırken ve hepimiz bir yıl daha ilerlerken PayPal size hesabınıza 5 dolar kredi eklemek istiyor!
>
> 5 dolarlık ödülünüzü alabilmeniz için tüm yapmanız gereken, 1 Ocak 2002 tarihine kadar bilgilerinizi güvenli Pay Pal sitemizden güncellemektir. Bizdeki bilgilerinizi güncelleyerek siz değerli müşteri hizmetlerimize mükemmel bir hizmet verme olanağı tanımış ve bu sırada kayıtlarımızı doğru tutmamızı sağlamış olacaksınız!
>
> Bilgilerinizi şimdi güncellemek ve PayPal hesabınıza 5 dolar eklemek için bu bağlantıyı tıklayınız: http://www.paypal-secure.com/cgi-bin.
>
> PayPal.com sitesini kullandığınız ve bize türümüzün en büyüğü olmada yardımcı olduğunuz için teşekkür ederiz!
>
> En içten dileklerimizle çok "Mutlu Noeller ve Mutlu Yıllar,"
>
> PayPal Ekibi

Edgar e-postayla ilgili birşeylerin ters olduğunu gösteren hatalı ayrıntıları da farketmemişti (örneğin, selamlama cümlesinden sonraki noktalı virgül ve "değerli müşteri hizmetlerimize mükemmel bir hizmet" diyen bozuk cümle gibi). Linki tıkladı, istenen bilgileri -ad, adres, telefon numarası ve kredi kartı bilgileri- girdi ve beş dolarlık kredisini bir sonraki kredi kartı ekstresinde görmek için oturup beklemeye başladı. Onun yerine gördüğü, hiçbir zaman almadığı eşyalara ait bir ödeme listesiydi.

E-Ticaret Siteleriyle İlgili Bir Not

Çevrim içi alışveriş yapmaya yanaşmayan, Amazon ve eBay gibi adı marka olmuş şirketlerden ya da Old Navy, Target ya da Nike gibi Ağ sitelerinden bile uzak duran insanlar tanıyorsunuzdur. Bir ta-

raftan bakınca kuşkulanmakta haklılar. Eğer İnternet tarayıcınız bugünün standardı olan 128-bit şifreleme kullanıyorsa, güvenli bir siteye gönderdiğiniz bilgiler bilgisayarınızdan şifreli olarak çıkıyordur. Bu veriler büyük bir çaba sarfedilerek deşifre edilebilirler ama büyük olasılıkla makul bir süre içerisinde kırılamazlar; bunu belki bir tek Ulusal Güvenlik Ajansı (NSA) başarabilir (ve bildiğimiz kadarıyla, NSA'nın ne Amerikan vatandaşlarının kredi kart numaralarını çalmaya, ne de kimlerin pornografik video kasetler ya da fantezi iç çamaşırları aldığını bulmaya yönelik bir ilgisi vardır).

Bu şifreli dosyalar, aslında yeterince zamanı ve kaynağı olan herhangi biri tarafından kırılabilir. Ama gerçekte hangi aptal, bir kredi kartı numarası çalmak için tüm bu emeği sarfeder; hele de pek çok e-ticaret şirketi, müşterilerinin finansal bilgilerini şifrelenmemiş veritabanlarında saklama hatasını yaparken? Daha da kötüsü, belli bir SQL veritabanı kullanan bazı e-ticaret şirketleri sorunu, fena halde genişletirler: Programın imalattan gelen sistem yöneticisi şifresini hiç değiştirmemişlerdir. Yazılımı kutusundan çıkardıklarında, şifresi "boşluk"tur ve bugün de "boşluk" olarak kalmaya devam eder. Bu nedenle veritabanının içeriği veritabanı sunucusuna bağlanmayı denemeye karar vermiş internet'teki herkese açıktır. Bu siteler her zaman saldırı altındadır ve bilgiler gerçekten de çalınır, hem de kimsenin ruhu duymadan.

Öte yandan, kredi kartı bilgilerinin çalınacağı korkusuyla internetten alışveriş yapmayan aynı insanlar, kredi kartlarını tuğla ve betondan yapılmış bir dükkândan alışveriş ederken kullanmakta ya da öğle yemeği, akşam yemeği veya içkilerini ödemek için annelerini bile götürmeyecekleri arka sokak barlarında ve lokantalarında kullanmakta bir sakınca görmezler. Kredi kartı slipleri bu tarz yerlerden sürekli çalınır ya da arka sokaktaki çöp kutularından araklanır. Ve herhangi bir ahlaksız kasiyer ya da garson, adınızı ve kredi kartı bilgilerinizi bir kenara not edebilir ya da içinden geçirilen herhangi bir kredi kartına ait bilgileri sonradan rahatça kullanılmak üzere saklayan ve internette kolayca bulunabilen bir kart tokatlama aleti kullanabilir.

Çevrim içi alışveriş etmenin tehlikeleri vardır ama büyük olasılıkla tuğla ve betondan yapılmış bir dükkândan alışveriş yapmak kadar güvenlidirler. Ve kredi kartı şirketleri, kartınızı çevrim içi kullanırken de size aynı korumayı sağlarlar -eğer hesabınızdan size ait olmayan harcamalar yapılmışsa bunun yalnızca ilk 50 dolarlık kısmından sorumlu olursunuz.

Bu yüzden benim görüşüme göre çevrim içi alışveriş yapmaktan çekinmek bir kuruntu olmaktan öteye gitmez.

Mitnick Mesajı:

Tam anlamıyla mükemmel bir gösterge olmasa da, her ne zaman bir site sizden özel olduğunu düşündüğünüz bir bilgi istiyorsa, bağlantının belgeli ve şifreli olduğundan mutlaka emin olun. Ve daha da önemlisi, geçersiz, süresi dolmuş ya da iptal edilmiş dijital sertifikalar gibi, bir güvenlik sorunu gösteren herhangi bir iletişim kutusunda hemen Evet'i tıklamayın.

Aldatmacanın İncelenmesi

Edgar yaygın kullanılan bir internet dümenine yakalanmıştı. Bu, çeşitli şekilerde karşımıza çıkan bir dolandırıcılık türü. Dokuzuncu bölümde anlatılan bir tanesi tıpkı aslı gibi olup, saldırgan tarafından yem olarak yaratılmış bir bağlanma sayfasını içerir. Farkı, sahte sayfanın, kullanıcının ulaşmak istediği bilgisayar sistemine erişim sağlamamasıdır; bunun yerine kullanıcı, adını ve parolasını bilgisayar korsanına vermiş olur.

Edgar, haydutların "paypal-secure.com" adında -yasal PayPal sitesine ait, güvenli bir sayfa olması gerekirmiş gibi görünen ama öyle olmayan- bir internet adresi satın aldığı bir dümene yakalanmıştır. Bilgileri o siteye girdiğinde, saldırganlara tam istedikleri şeyi vermiştir.

Çeşitleme Üzerine Çeşitlemeler

Bilgisayar kullanıcılarını gizli bilgilerini girebilecekleri düzmece internet sitelerine gitmeleri için kandırmanın kaç değişik yolu olabilir? Kimsenin geçerli, kesin bir yanıtı olduğunu sanmıyorum ancak "çok ama çok" diye bir cevap verebiliriz.

Kayıp Bağlantı

Bir hile sürekli karşımıza çıkar: Bir siteyi ziyaret etmek için çekici bir neden sunan bir e-posta gönderip doğrudan oraya yönlendiren bir bağlantı sağlamak. Farklı olarak, bağlantı sizi gittiğinizi düşündüğünüz siteye götürmez çünkü bağlantı aslında gerçek site için olan bağlantıyı taklit eder. İşte internet'te gerçekten kullanılmış başka bir örnek, yine çok suistimal edilen PayPal'ın adını kullanmaktadır:

www.PayPai.com

Hemen bakıldığında burada PayPal yazıyormuş gibi görünüyor. Kurban farketse bile yazıdaki küçük bir hatanın " l " harfini " i " gibi gösterdiğini düşünebilir. Ve kim, bakar bakmaz aşağıdaki linkte küçük harf L yerine 1 sayısının kullanıldığını farkedebilir?

www.PayPa1.com

Bu dalavereyi kredi kartı haydutları arasında sürekli popüler kılacak kadar çok yanlış yazımları ve hatalı yönlendirmeleri doğruymuş gibi kabullenecek insan var. İnsanlar düzmece siteye gittiklerinde, orası gitmeyi umdukları yer gibi görünür ve kredi kartı bilgilerini huzur içinde girerler. Bu dalaverelerden birini kurmak için saldırganın tek yapması gereken, düzmece bir site adı almak, e-postalarını göndermek ve enayilerin dolandırılmak için siteye girmelerini beklemektir.

2002'nin ortalarında bir e-posta aldım; görünüşe göre "ebay@ebay.com"dan, bir defada pek çok adrese gönderilmişti. Mesaj Şekil 7.1'de sunulmuştur.

Bağlantıyı tıklayarı kurbanlar eBay sayfasına çok benzeyen bir web sayfasına gittiler. Aslında sayfa, özgün eBay amblemi ve "Ara", "Sat" gibi, tıklandığında ziyaretçiyi gerçek eBay sayfasına götüren diğer gezinme bağlantılarıyla iyi tasarlanmıştı. Sağ alt köşede bir güvenlik simgesi de bulunmaktaydı. Bilgisiz kurbanı kandırmak amacıyla tasarımcı, kullanıcının sağladığı bilgilerin nereye gönderildiğini gizlemek için HTML şifrelemesi bile kullanmıştı.

Kötü niyetli, bilgisayar tabanlı toplum mühendisliği saldırısının mükemmel bir örneğiydi. Yine de kusursuz değildi.

E-posta mesajı çok iyi yazılmamıştı; özellikle de "Bu duyuruyu eBay'den aldınız"la başlayan paragraf acemice ve saçmaydı (bu oyunlardan sorumlu kişiler yazdıklarını kontrol etmesi için hiçbir zaman deneyimli birini tutmazlar ve bu hemen farkedilir). Ayrıca dikkatli biri eBay'in ziyaretçine PayPal bilgilerini sormasından kuşkulanırdı; eBay'ın müşterisine başka bir şirketle ilgili özel bilgilerini sorması için hiçbir neden olamaz.

Ve internet konusunda bilgili herhangi biri bağlantının eBay sayfasına değil, ücretsiz bir internet hizmet sağlayıcısı olan tripod.com sayfasına yönlendirildiğini anlayacaktır. Bu, e-postanın yasal olmadığının tam bir göstergesidir. Yine de eminim pek çok insan, kredi kartı numaraları dahil, istenen bilgileri bu sayfaya girmişlerdir.

NOT: *Neden insanların yanıltıcı veya uygunsuz alan adları almalarına izin veriliyor? Çünkü geçerli kanun ve çevrimiçi çalışma kuralları uyarınca, isteyen, kullanımda olmayan bir site adını alabilir. Şirketler taklit adreslerin kullanımıyla mücadele etmeye çalışıyorlar ama neye karşı olduklarını bir de siz düşünün. General Motors, f**kgeneralmotors.com adresini (yıldızlar olmadan) alıp URL'yi General Motors'un internet sitesine yönlendiren bir şirkete dava açtı. G.M. kaybetti.*

msj: Sevgili eBay Kullanıcısı,

Başka şahıslarıneBay hesabınızı uygunsuz olarak kullandıkları oldukça fark edilir bir hal almıştır ve Kullanıcı Anlaşması'nın şu maddesi ihlal edilmiştir:

4. Fiyat Verme ve Satın Alma

Sabit fiyatlı düzenlemelerimizden biri aracılığıyla bir mal aldığınız veya aşağıda açıklandığı üzere en yüksek fiyatı verdiğiniz takdirde satıcıyla aranızdaki işlemi tamamlamanız gerekmektedir. Eğer bir açık artırma sonunda en yüksek fiyatı vermişseniz (geçerli en düşük fiyat ve ihtiyat yükümlülüklerini karşılamak kaydıyla) ve verdiğiniz fiyat satıcı tarafından kabul edilmişse, satıcıyla işleminizi tamamlamanız gerekmektedir. Aksi halde, işlem kanunen veya bu Anlaşma gereğince yasaklanır.

Bu duyuruyu eBay'den aldınız çünkü şu anki hesabınızın diğer eBay üyeleriyle uyuşmazlıklar yaratması dikkatimizi çekti ve eBay, hesabınızın en kısa sürede onaylanmasını gerekli bulmaktadır. Lütfen hesabınızı onaylayınız aksi halde hesap iptal edilebilecektir. Hesabınızı Onaylamak İçin Burayı Tıklayınız - http://error_ebay tripod.com

****

Belirtilen ticari markalar ve işaretler sahiplerine aittir. eBay ve eBay amblemi eBay Inc.'e ait ticari markalardır.

Şekil 7.1 Bu ve benzeri e-postalardaki bağlantılar dikkatle kullanılmalıdır.

Uyanık Olun

İnternetin bireysel kullanıcıları olarak hepimizin uyanık olmamız; kişisel bilgilerin, şifrelerin, hesap numaralarının, PIN'lerin ve bunun gibi şeylerin ne zaman girileceğine bilinçli bir şekilde karar vermemiz gerekir.

Baktıkları belli bir internet sayfasının, güvenli bir sayfanın taşıması gereken şartlara uyup uymadığını söyleyebilecek kaç kişi tanıyorsunuz? Şirketinizin kaç çalışanı neye bakması gerektiğini biliyor?

İnternet kullanan herkes genellikle sitelerin bir yerlerinde beliren ve bir asma kilide benzeyen ufak şeklin ne olduğunu bilmeli. Kilit kapalı olduğunda sitenin güvenli olarak sertifikalandığını anlamalıdır. Kilit açık olduğu zaman ya da kilit gözükmediğinde site özgün bir site olarak belgelenmemiştir ve gönderilen herhangi bir bilgi açıktadır; yani, şifrelenmemiştir.

Terimler

ARKA KAPI: Kullanıcının bilgisi dışında bilgisayara gizli bir yol sağlayan üstü kapalı bir giriş noktası. Bir yazılım programı geliştirirken programcılar tarafından da kullanılır, böylece sorunları çözmek için programa girebilirler.

Her şeye karşın bir şirket bilgisayarının yönetimsel ayrıcalıklarını elde etmeyi başarmış bir saldırgan, kullanıcının gerçekte ne olduğu doğrultusundaki görüşünü değiştirmek için işletim sistemi koduna yamalar yapabilir ya da üzerinde oynayabilir. Örneğin, bir internet sitesinin dijital sertifikasının geçersiz olduğunu belirleyen internet tarayıcısı yazılımındaki program kodlarını, kontrolü aşabilmek için değiştirilebilir. Ya da sistem kök donanımı adı verilen birşeyle değiştirebilir; işletim sistemi düzeyinde bir ya da daha fazla, bulunması daha güç *arka kapı* yükleyebilir.

Güvenli bir bağlantı, siteyi özgün olarak tanımlar ve iletilen bilgiyi şifreler, böylece bir saldırgan elde ettiği verileri kullanamaz. Bir internet sitesine, hattâ güvenli bağlantı kullanan birisine güvenebilir misiniz? Hayır, çünkü site sahibi gerekli tüm güvenlik yamalarını uygulamakta ya da kullanıcıları ve yöneticileri doğru şifre uygulamaları konusunda zorlamakta yetersiz kalabilir. Bu yüzden güvenli görünen bir sitenin saldırıya açık olmadığını varsayamazsınız.

Güvenli HTTP (hypertext transfer protocol) veya SSL (secure sockets layer) dijital sertifikaları yalnızca uzaktaki siteye gönderilen bilgiyi şifrelemekte kullanılmaz, aynı zamanda belgeleme yapmak için de (doğru internet sitesiyle iletişim kurduğunuzu doğrulamak amacıyla) otomatik bir mekanizma sağlar. Ancak bu koruma mekanizması, adres çubuğunda görünen site adının, gerçekten de ulaşmak istediği site olup olmadığına dikkat etmeyen kullanıcılar söz konusu olduğunda işe yarayamaz.

Genellikle göz ardı edilen başka bir güvenlik konusu, karşımıza şunun gibi bir uyarı mesajıyla çıkar "Bu site güvenli değil ya da güvenlik sertifikasının süresi dolmuş. Yine de devam etmek istiyor musunuz?" Pek çok internet kullanıcısı mesajı anlamaz ve ortaya çıktığında hemen "Tamam" ya da "Evet"e tıklayarak, bir batağın içinde olabileceğinin farkında olmadan işine devam eder. Dikkat edin; güvenlik protokolü kullanmayan bir internet sitesinde adresiniz, telefon numaranız, kredi kartı veya banka hesap numaranız gibi kişisel bilgilerinizi ya da özel kalmasını istediğiniz herhangi bir şeyleri kesinlikle girmemelisiniz.

Thomas Jefferson özgürlüğümüzü sürekli tutmanın "her zaman tetikte" olmaktan geçtiğini söylemiştir. Bilgiyi değiştokuş aracı olarak kullanan bir toplumda özel yaşamı korumak ve güvenliği sağlamak da bir o kadar özen gerektirir.

Virüslere Duyarlı Olmak

Virüs yazılımlarıyla ilgili özel bir not: Virüs yazılımları şirket intraneti için önemlidir ama aynı zamanda bilgisayar kullanan her çalışan için de önemlidir. Makinalarına virüs koruma yazılımı yüklemiş olmak bir yana, kullanıcıların yazılımı açık tutmaları da gerekir (bu pek çok insanın sevmediği bir şeydir çünkü bilgisayarın bazı işlevlerini kaçınılmaz olarak yavaşlatır).

Virüs koruma yazılımlarıyla ilgili akılda tutulması gereken bir başka önemli nokta daha vardır: Virüs tanımlarını güncel tutmak. Şirketiniz, yazılımı ya da güncellemelerini ağ üzerinden dağıtmak üzere yapılandırmadığı sürece, her birey en son virüs tanımları dosyasını kendi başına indirme sorumluluğunu taşımalıdır. Kendi kişisel önerim herkesin virüs yazılımı seçeneklerini ve virüs tanımlarını her gün güncellenecek şekilde ayarlamalarıdır.

Basitçe söylemek gerekirse, virüs tanımlarınız düzenli olarak güncellenmiyorsa savunmasızsınızdır. Böyleyken bile, virüs koruma yazılımı geliştiren şirketlerin henüz bilmediği ya da bir tanımlama modeli çıkarmadıkları virüs ve solucanlara karşı tam olarak korunuyor sayılmazsınız.

Evdeki bilgisayarları ya da dizüstü bilgisayarları üzerinden uzaktan erişim hakkı tanınmış tüm çalışanların bu makinalar üzerinde en azından güncellenmiş virüs yazılımı ve bir kişisel güvenlik duvarı bulundurması gerekir. İşini bilen bir saldırgan en zayıf noktayı bulmak için büyük resme bakıp oradan saldıracaktır. Uzaktan erişimleri olan kişilerin kişisel güvenlik duvarları ve güncellenmiş antivirüs yazılımının gerekleri konusunda düzenli olarak uyarılmaları bir şirket sorumluluğudur; çünkü BT müdürlüğünden uzak olan bireysel çalışanların, yöneticilerin, satış sorumlularının ve diğerlerinin bilgisayarlarını korumasız bırakmalarının getireceği tehlikeleri hatırlamalarını bekleyemezsiniz.

Bu adımların dışında, daha az yaygın ama daha az önemli olmayan, Truva Atı saldırılarına karşı koruma sağlayan yazılım paketlerinin, diğer adıyla anti-Trojan yazılımlarının kullanılmasını şiddetle öneririm. Bu kitap yazıldığı sırada iyi bilinen programlardan iki tanesi şunlardır: The Cleaner (www.moosoft.com) ve Trojan Defence Sweep (www.diamondcs.com.au).

Sonuç olarak, ağ geçitlerinde tehlikeli e-postalara karşı tarama yapmayan tüm şirketler için olabilecek en önemli güvenlik mesajı şu olabilir: Hepimiz unutma eğilimli olduğumuza veya işimizi yaparken kenarda kalan şeyleri ihmal ettiğimize göre, güvenilebilecek bir kişi ya da kuruluştan

Terimler

SSL (Güvenli Yuva Katmanı): Hem istemcinin hem de sunucunun internet üzerinden güvenli iletişimle belgelenmesini sağlayan Netscape tarafından geliştirilmiş bir protokol.

gelmediği sürece e-posta eklerini açmamaları konusunda çalışanların, farklı şekillerde, tekrar tekrar uyarılmaları gerekir. Yönetim, faal virüs koruma yazılımlarını ve içinde yıkıcı bir yük taşıyabilen, görünüşte güvenli e-postalara karşı değeri ölçülemez bir koruma sağlayan anti-Trojan yazılımlarını kullanmaları gerektiğini çalışanlarına hatırlatmalıdır.

8 ACINDIRMA, SUÇLULUK DUYURMA VE SİNDİRME TEKNİĞİ KULLANMAK

On beşinci bölümde de söz edileceği gibi, bir toplum mühendisi isteklerini yerine getirmesi için hedefini yönlendirmek amacıyla etkileme psikolojisini kullanır. Yetenekli toplum mühendisleri, korku, heyecan ya da suçluluk gibi duyguları uyandıracak bir yöntem bulma konusunda çok ustadırlar. Bunu, elde olan bilgileri derinlemesine incelemeden insanları isteklerini yerine getirmeye yönlendiren istemsiz mekanizmalar olan psikolojik tetikleyicileri kullanarak yaparlar.

Hem kendimiz hem de başkaları adına zor durumlardan kaçınma eğilimindeyizdir. Bu olumlu dürtüden yola çıkarak, saldırgan, kişinin acıma duygusuyla oynayabilir; onun kendini suçlu hissetmesini sağlayabilir ya da silah olarak sindirmeyi kullanabilir.

İşte size, duygularla oynama konusunda en sevilen manevralarla ilgili birkaç üst düzey ders.

Stüdyo Ziyareti

Bazı insanların bir toplantının, özel bir eğlencenin ya da bir kitap tanıtım kokteylinin yapıldığı bir otelin balo salonunun kapısında duran görevliye gittiklerini, sonra da bilet ya da davetiye sorulmadan adamın yanından geçtiklerini hiç gördünüz mü?

Çok benzer bir şekilde bir toplum mühendisi de lafazanlıkla, girilmesi mümkün değilmiş gibi görünen yerlere girebilir. Tıpkı aşağıdaki, film endüstrisiyle ilgili öyküde anlatıldığı gibi.

Telefon Görüşmesi

- Ron Hillyard'ın bürosu, ben Dorothy.

- Merhaba Dorothy. Benim adım Kyle Bellamy. Canlandırma Tasarım'da Brian Glassman'ın ekibinde işe başladım. Sizler burada işleri kesinlikle farklı yürütüyorsunuz.

- Sanırım. Daha önce başka bir film şirketinde çalışmadığım için pek bilemiyorum. Sana nasıl yardımcı olabilirim?

- Doğruyu söylemek gerekirse kendimi biraz aptal gibi hissediyorum. Öğleden sonra fikir alışverişi için bir yazar gelecek ve ben onu içeri almak için kiminle konuşmam gerektiğini bilmiyorum. Burada, Brian'ın ofisinde çalışanlar çok iyiler ama onları çok sıkboğaz ediyormuşum gibi geliyor, şunu nasıl yaparım, bunu nasıl yaparım... Sanki yeni okula başlamışım da tuvaletin nerede olduğunu bilmiyormuşum

gibi. Durumumu anlatabiliyor muyum?

Dorothy güldü.

- Sen güvenlikle konuşmak istiyorsun. Önce 7'yi, sonra da 6138'i çevir. Eğer telefonu Lauren açarsa, ona, sana iyi bakması gerektiğini söylediğimi ilet.

- Teşekkürler, Dorothy. Ve eğer erkekler tuvaletini bulamazsam, seni yine arayabilirim!

Bu fikre birlikte güldüler ve telefonu kapattılar.

David Harold'un Hikâyesi

Film seyretmeye bayılırım ve Los Angeles'a taşındığımda film endüstrisinde çalışan bir yığın insanla tanışacağımı ve onların beni partilere götüreceğini ya da film stüdyolarında öğle yemeği yiyeceğimizi falan düşünmüştüm. Neyse, Los Angeles'ta bir yıl kaldım, yirmi altı yaşımı doldurmak üzereydim ve film dünyasıyla en büyük yakınlaşmam Pheonix ve Cleveland'dan gelen cici insanlarla birlikte yaptığım Universal Stüdios turu oldu. Sonunda, işleri, beklediğim gibi kendi elime almam gerektiğini anladım. Eğer onlar beni davet etmezlerse, ben kendimi davet edecektim. Yaptığım da bu oldu.

Bir Los Angeles Times aldım ve birkaç gün boyunca sinema sayfasını okuyup farklı stüdyolardan bazı yapımcıların adlarını not ettim. Önce büyük stüdyolardan birini vurmaya karar verdim.

Santralı aradım ve gazetede okuduğum bu yapımcının ofisine bağlanmak istediğimi söyledim. Telefonu açan sekreter anaç birine benziyordu. Şanslı olduğumu düşündüm, çünkü eğer oradaki keşfedilmek için bekleyen genç bir kız olsaydı büyük olasılıkla bana saatin kaç olduğunu bile söylemezdi.

Ama Dorothy öyle değildi, sokakta kalmış bir kedi yavrusunu evine alacak birine benziyordu. Yeni işinde kendini biraz mahcup hisseden yeni çocuğa acıyacak biriydi. Ben de kesinlikle doğru noktasına dokunmuştum. Birilerini kandırmaya çalışırken, onların size istediğinizden daha fazlasını vermeleri dürumu her gün başınıza gelmez. Bana acıyıp yalnızca güvenlikte çalışan insanlardan birinin adını vermekle kalmadı, aynı zamanda o hanıma, bana iyi bakması gerektiğini tembihlediğini de söylememi istedi.

Dorothy'nin adını kullanmayı zaten planlamıştım. Bu, işi daha da kolaylaştırdı. Lauren hemen açıldı ve verdiğim adın çalışan veritabanında olup olmadığına bakmaya bile yeltenmedi.

Öğleden sonra kapıya gittiğimde adımı ziyaretçi listesine eklemekle kalmamışlar benim için bir park yeri bile ayırmışlardı. Film stüdyosu kantininde geç bir öğle yemeği yedim ve akşama kadar etrafı gezdim. Hattâ birkaç ses stüdyosuna bile girdim ve film çekimlerini seyrettim. Saat 7'ye kadar oradan ayrılmadım. Geçirdiğim en heyecan verici günlerden biriydi.

Aldatmacanın İncelenmesi

Herkes bir zamanlar yeniydi. Hepimizin, özellikle genç ve deneyimsiz olduğumuz zamanlardan kalan ilk günlerle ilgili anılarımız vardır. Bu yüzden yeni bir çalışan yardım istediğinde pek çok insanın -özellikle de işe gireli çok olmamış olanların- kendi yeni yetmelik duygularını hatırlamalarını ve yardımcı olmak için her işi bir kenara bırakmalarını bekleyebilirsiniz. Toplum mühendisi bunu bilir ve kurbanlarının acıma duygularıyla oynamak için bunu kullanabileceğinin farkındadır.

Tanımadığımız insanların şirketimizin binalarına ve bürolarına dalavere yapıp girmelerini çok kolaylaştırıyoruz. Girişte güvenlik görevlileri olsa ve çalışan olmayan herhangi biri için içeri alınma işlemleri yapılsa bile, bu öyküde anlatılan oyunun çeşitli şekillerde kullanılması saldırganın bir ziyaretçi kartı almasını ve içeri girmesini sağlayacaktır. Ya şirketiniz ziyaretçilere eşlik edilmesi şartını koymuşsa? Bu iyi bir kural; ancak sadece, çalışanlarınız, ziyaretçi kartı olsun olmasın, tek başına gelen herkesi durdurup ona sorular sorma konusunda gerçekten bilinçliyse etkili olur. Eğer alınan yanıtlar tatmin edici olmazsa, çalışanlarınız güvenliğe haber vermek konusunda da istekli olmalıdırlar.

Dışardan gelenlerin lafazanlıkla tesislerinize girmesi şirketinizin hassas bilgilerini tehlikeye sokar. Bugünün ortamında, toplumumuzun üzerinde gezinen terör tehdidiyle birlikte, bilgiden çok daha fazlası tehlike altında olabilir.

"Şimdi Yap"

Toplum mühendisliği teknikleri kullanan herkes gerçek bir toplum mühendisi olmak zorunda değildir. Belli bir şirketin iç işlerini bilen herhangi biri de bir tehdit oluşturabilir. Dosyalarında ve veritabanlarında eleman bilgilerinin tümünü tutan şirketler için tehlike daha da büyüktür. Tahmin edeceğiniz gibi, çoğu şirket de böyle yapar.

Çalışanlar toplum mühendisliği saldırılarını fark edecek şekilde eğitilmediği ve yetiştirilmediği sürece, aşağıdaki öyküde geçen terkedilmiş kadın gibi kararlı insanlar, pek çok dürüst insanın olanaksız olduğunu düşündüğü şeyleri yapabilirler.

Doug'ın Hikâyesi

Linda'yla işler zaten iyi gitmiyordu ve Erin'le tanıştığım anda onun benim için yaratıldığını anladım. Linda, biraz, nasıl desem, tam olarak dengesiz sayılmasa da kafası bozulduğu zaman ipin ucunu kaçırabilen biri.

Mümkün olduğu kadar nazik bir şekilde artık taşınması gerektiğini ona söyledim ve eşyalarını toplanmasına yardım ettim. Hattâ aslında

benim olan birkaç Queensryche CD'sini almasına bile izin verdim. O gider gitmez anahtarcıya gidip ön kapı için yeni bir kilit aldım ve hemen o gece takdırdım. Ertesi sabah telefon şirketini aradım ve numaramı değiştirtip kayıtlarda görünmemesini istedim.

Artık Erin'in peşinden gitmek için özgürdüm.

Linda'nın Hikâyesi

Zaten ayrılmaya hazırdım, sadece daha karar vermemiştim. Ama kimse geri çevrilmekten hoşlanmaz. Bu durumda iş, "ne kadar iğrenç biri olduğunu ona nasıl gösterebilirim"e geldi.

Bulmam çok uzun sürmedi. Başka bir kız olmalıydı, yoksa beni bu kadar alelacele başından atmazdı. Böylece bir süre daha bekleyecek, sonra da gece geç saatlerde onu arayacaktım. Tam da en az aranmak istedikleri saatlerde.

Ertesi hafta sonuna kadar bekledim ve Cumartesi gecesi saat 11 gibi aradım. Numarasını değiştirmişti ve yeni numara kayıtlarda yoktu. Bu da onun ne kadar adi biri olduğunu gösteriyordu.

Bu çok da büyük bir engel değildi. Telefon şirketindeki işimden ayrılmadan önce eve getirdiğim evrakları karıştırmaya başladım. Ve işte buradaydı; Doug'ın telefon hattında oluşan bir arızadan kalan tamir makbuzunu saklamıştım ve makbuzun üzerinde telefona ait kablo ve çift numaraları yazıyordu. Telefon numaranızı istediğiniz kadar değiştirin, aynı bakır tel çifti evinizden çıkıp telefon şirketinin merkez ofis ya da MO denen ana santralına bağlanır. Her evden ve daireden çıkan bakır teller kablo ve çift adı verilen sayılarla tanımlanır. Eğer telefon şirketinin işleri nasıl yürüttüğünü bilirseniz, ki ben biliyorum, hedefin kablo ve çift sayılarını bilmek telefon numarasını bulmak için gerekli olan tek şeydir.

Kentteki tüm merkez ofislerin adresleri ve telefon numaralarının birlikte bir listesi elimde vardı. İğrenç Doug'la yaşadığım yerin yakınlarındaki bir MO'nun numarasını buldum ve aradım ama doğal olarak kimse açmadı. Tam da ihtiyacınız olduğu anda bu santral görevlisi nerededir? Yeni bir plan yapmak yaklaşık yirmi saniyemi aldı. Diğer merkez ofisleri aramaya başladım ve sonunda birini buldum. Ama kilometrelerce ötedeydi ve görevli büyük olasılıkla ayaklarını uzatmış oturuyordu. Yapmasını istediğim şeyi yapmak istemeyecekti. Planım hazırdı.

"Ben Linda, onarım merkezinden," dedim. "Acil bir durum var. Hastane acil servisinin telefonu arızalanmış. Bir teknisyen onarmaya çalışıyor ama sorunun nerede olduğunu bulamıyor. Hemen Webster Merkez Ofisi'ne gidip MO'dan ayrılan hattâ çevir sesi olup olmadığına bakılması gerek."

Sonra ona, "Oraya vardığında seni ararım" dedim. Çünkü onarım merkezini arayıp beni sormasını istemiyordum.

Mitnick Mesajı:

Hedef şirkette işlerin nasıl yürüdüğünü öğrendikten sonra, toplum mühendisinin bu bilgiyi kullanarak gerçek çalışanlarla ahbaplık kurması kolaylaşır. Şirketlerin kendilerine diş bileyen eski ve yeni çalışanlarından gelebilecek toplum mühendisliği saldırılarına karşı hazırlıklı olmaları gerekir. Kişilerin geçmişini taramak, bu tarz davranışlara eğilimi olan şahısları belirlemeye yardımcı olabilir. Ancak çoğu durumda bu insanları tespit etmek oldukça zordur. Böyle durumlarda en uygun koruma, şirkette çalışıp çalışmadıkları şahsen bilinmeyen kişilere bilgi vermeden önce aralarında kişinin iş durumunun kontrolü de olmak üzere kimlik belirleme işlemlerini denetlemek ve sıkılaştırmaktır.

Merkez ofisin rahat ortamından çıkıp arabasının ön camından buzu kazıyıp gecenin bir yarısı ıslak sokaklarda gezinmek istemeyeceğinin farkındaydım. Ama acil bir durum vardı ve bu yüzden ne kadar meşgul olduğuyla ilgili bir şey söyleyemedi.

Kırk beş dakika sonra onu Webster Merkez Ofisi'nden aradığımda, ona 29 numaralı kabloyu ve 2481 numaralı çifti kontrol etmesini söyledim. Kutuya gitti, kontrol etti ve evet, çevir sesi geliyordu. Ben bunu zaten biliyordum.

Sonra ona, "Tamam, şimdi bir HK yapmanı istiyorum," dedim. Bu hat kontrolü ve aynı zamanda telefon numarasını tespit etmesi anlamına geliyordu. Bunu, aradığı numarayı geri bildiren özel bir numarayı arayarak yapıyordu. Numaranın kayıtsız bir numara olduğunu ya da daha yeni değiştiğini falan bilmiyordu, bu yüzden istediğimi yaptı ve numaranın okunduğunu duydum. Harika. Her şey tıkır tıkır yürümüştü.

Ona, sanki numarayı biliyormuşum gibi "Sorun herhalde arada bir yerde" dedim. Adama teşekkür ettim ve bunun üzerinde çalışmaya devam edeceğimizi söyleyip iyi geceler diledim.

Doug'ın kayıtlarda gözükmeyen bir telefon numarasının arkasına saklanarak benden kaçmaya çalışması buraya kadardı. Eğlence başlamak üzereydi.

Aldatmacanın İncelenmesi

Bu öyküdeki genç hanım intikam almak için istediği bilgiyi elde etmeyi başarmıştı, çünkü işlerin işleyişiyle ilgili bilgisi vardı, telefon numaralarını, süreçleri ve telefon şirketinde kullanılan terimleri biliyordu. Bu bilgileri kullanarak yalnızca istediği numarayı elde etmekle kalmamış, bunu soğuk bir kış gecesi bir santral görevlisini şehrin diğer ucundan işini görmesi için getirterek yapmıştı.

"Bay Bigg Böyle Yapılmasını İstiyor"

Oldukça etkili ve popüler bir sindirme şekli -popülerliği basit olmasından kaynaklanır- yetki kullanarak insan davranışlarını etkilemeye dayanır.

Genel müdür asistanının adı bile çok iş görebilir. Özel dedektifler ve hattâ insan avcıları bunu her zaman yaparlar. Santralı ararlar ve genel müdürle görüşmek istediklerini söylerler. Sekreter ya da asistan telefonu açtığında genel müdür için bir evrak veya paket geldiğini söylerler ya da bir elektronik posta eki gönderdiklerini ve onu basıp basamayacağını sorarlar. Ya da faks numarasını öğrenmek isterler. Bu arada adınız neydi diye de sorarlar.

Sonra bir sonraki adamı ararlar ve: "Bay Bigg'in ofisinden Jeannie sizi aramamı ve bana bir konuda yardımcı olabileceğinizi söyledi."

Bu yönteme *ad düşürme* denir ve genellikle saldırganın üst düzey biriyle bağlantısı olduğuna hedefi inandırarak hızlı bir ahbaplık kurulması için kullanılan bir taktiktir. Kurban, ortak tanıdıkları olan birine daha çok yardım etme eğilimindedir.

Eğer saldırgan oldukça hassas bilgilere göz koyduysa, kurbanda, müdürleriyle başının derde girmesi korkusu gibi işe yarar duygular uyandırmak için böyle bir yaklaşıma başvurabilir. İşte bir örnek.

Scott'un Öyküsü

"Buyrun ben Scott Abrams."

"Scott, ben Christopher Dalbridge. Az önce Bay Biggley'le konuştum ve sesi biraz kızgın geliyordu. Tüm pazar payı araştırma raporlarının birer kopyasını incelenmemiz için bize göndermeniz doğrultusunda on gün önce size bir talimat vermiş. Elimize hiçbir şey geçmedi."

"Pazar payı araştırmaları mı? Bana kimse bununla ilgili bir şey söylemedi. Siz hangi birimdesiniz?"

"Biz danışmanlık firmasıyız ve şimdiden takvimin oldukça gerisindeyiz."

"Dinle, şu anda bir toplantıya girmek üzereyim. Bana telefon numaranızı verin ve..."

O anda saldırgan iyice canı sıkılmış gibi konuşur. *"Bay Biggley'e böyle mi söylememi istiyorsunuz? Bakın, analizlerimizi yarın sabah görmek istiyor ve bu gece onlar üstünde çalışmamız gerek. Şimdi, raporları sizden alamadığımız için yapamadığımızı ona ben mi söyleyeyim yoksa bunu kendiniz mi söylemek istersiniz?"*

Öfkeli bir genel müdür bütün haftanızı mahvedebilir. Hedef büyük olasılıkla toplantıya gitmeden önce bu işin halledilmesi gerektiğine karar verecektir. Toplum mühendisi bir kez daha istediği yanıtı almak için doğru düğmeye basmıştır.

Aldatmacanın İncelenmesi

Üst düzey yöneticilerin adını kullanarak sindirme numarası özellikle karşı taraf, şirkette oldukça alt seviyelerdeyse çok işe yarar. Önemli birinin adının geçmesi yalnızca olağan isteksizliğin ya da şüpheciliğin üstesinden gelmekle kalmaz, kişiyi yardımcı olmak için daha istekli yapar: Yardım ettiğiniz kişinin önemli ya da etkili biri olduğunu düşünüyorsanız, var olan yardımcı olma güdünüz doğal olarak katlanacaktır.

Ancak toplum mühendisi bu oyunu oynarken, kişinin kendi patronunun adını kullanmak yerine daha üst düzey birinin adını kullanmanın en iyisi olduğunu bilir. Ayrıca bu yöntemin küçük bir kuruluşta uygulanması çok güçtür. Saldırgan, kurbanının kazara pazarlama genel müdür yardımcısıyla karşılaşıp ona, "Beni aramasını söylediğiniz adama ürün pazarlama planlarını gönderdim" deyivermesini istemez. Böyle bir cümle rahatlıkla, "Ne pazarlama planı? Hangi adam?" gibi bir tepki doğurabilir. Bu da şirketin bir oyuna kurban gittiğinin anlaşılmasına neden olabilir.

Sosyal Güvenlik İdaresi Sizinle İlgili Ne Biliyor

Ellerinde bizlerle ilgili dosyalar olan devlet dairelerinin, görmeye yetkili olmayan insanlardan uzak tutmak için bilgilerimizi kilit altında tuttuklarını düşünmek isteriz. Gerçek şu ki, federal hükümet bile saldırılara karşı, hayal ettiğimiz kadar güvende değildir.

May Linn'in Telefonu

Yer: Sosyal Güvenlik İdaresi'nin bölge ofislerinden biri.
Zaman: Perşembe, sabah 10:18.

Mitnick Mesajı:

Sindirme yöntemi, bir cezalandırılma korkusu yaratarak insanları iş birliği yapmaya zorlar. Sindirme aynı zamanda küçük düşme korkusunu ya da bir sonraki ikramiye için yetersiz görülme gibi korkuları da uyandırır.

İnsanlar, söz konusu güvenlik olduğunda yetkiyi sorgulamanın kabul edilebilir, hattâ beklenen bir hareket olduğu doğrultusunda yetiştirilmelidirler. Bilgi güvenliği eğitimleri, ilişkileri zedelemeden, müşteri memnuniyeti yöntemlerini kullanarak yetkinin nasıl sorgulanması gerektiğini de vermelidir. Dahası bu beklenti yukarıdan aşağıya doğru da desteklenmelidir. Eğer konumlarına bakmadan insanları sorgulayan bir çalışanın arkasında durulmuyorsa, oluşacak tepki, sorgulamanın durması, yani olmasını istediğiniz şeyin tam tersi olacaktır.

- Mod üç. Ben May Linn Wang."

Telefonun diğer tarafındaki ses çekingen, neredeyse utangaç geliyordu.

- Bayan Wang, ben Artlur Arondale, Genel Müfettişlik makamından. Size 'May' diyebilir miyim?"

- May Linn lütfen, dedi kadın.

- Durum şu May Linn. Burada, henüz bilgisayarı olmayan yeni bir arkadaşımız var ve şu anda önemli bir projede çalıştığı için benim bilgisayarımı kullanıyor. Şu işe bakar mısın, bir Birleşik Devletler devlet dairesiyiz ve bu adamın kullanması için bir bilgisayar alacak kadar bütçede para olmadığını söylüyorlar. Şimdi de müdürüm işimde geri kaldığımı düşünüyor ve bahane duymak istemediğini söylüyor. Anlatabiliyor muyum?

- Demek istediğini çok iyi anlıyorum.

- MCS üzerinde bir küçük arama yapmada bana yardımcı olabilir misin, diye sordu adam, vergi mükelleflerinin bilgilerinin tutulduğu bilgisayar sisteminin adını kullanarak.

- Elbette. Ne gerekiyor?

- İlk önce Joseph Johnson, doğum tarihi 4/7/69 adıyla bir harf taraması yapmanı istiyorum." (Harf taraması bilgisayara vergi mükelleflerinin adlarına göre hesap aratmaktır. Arama doğum tarihiyle genişletilir.)

May Linn kısa bir duraksamadan sonra sordu:

- Ne öğrenmek istiyorsun?"

- Hesap numarası nedir, dedi adam, Sosyal Güvenlik Numarası için kurum içinde kullanılan terimi kullanarak. Kadın numarayı okudu.

- Tamam. Bu hesapla ilgili bir de sayı taraması yapmanı isteyeceğim, dedi arayan.

Bu, temel vergi mükellefi bilgilerini okumasını istediği anlamına geliyordu ve May Linn vergi mükellefinin doğum yerini, annesinin kızlık soyadını ve baba adını verdi. Kadın kartın veriliş ay ve yılını ve hangi bölge bürosu tarafından verildiğini söylerken arayan sabırla dinledi.

Sonra bir AKAS yapmasını istedi. ("ayrıntılı kazanç sorgusu"nun kısaltılmışı.)

AKAS taraması şu soruyu getirdi:

- Hangi yıl?

Arayan cevap verdi,

- 2001 yılı.

- Miktar 190.286 dolar; yatıran Johnson MicroTech, dedi May Linn.

- Başka ücret var mı?

- Hayır?

- *Teşekkürler, çok yardımcı oldun,* dedi adam.

Sonra bilgiye ihtiyacı olduğunda ve bilgisayarını kullanamadığında yeniden arayabilmek için ondan izin aldı. Yine toplum mühendislerinin en sevdiği numaralardan birini, her seferinde yeni bir hedef bulmakla uğraşmayıp sürekli aynı kişiyle görüşebilmek için bir bağlantı kurmaya çalışma yöntemini kullanmıştı.

- *Önümüzdeki hafta arayamazsın",* dedi kadın; çünkü Kentucky'ye kızkardeşinin düğününe gidiyordu. Başka ne zaman isterse elinden geleni yapacaktı.

Telefonu kapadığında May Linn, kendi gibi değeri bilinmeyen başka bir devlet memuruna biraz olsun yardım edebildiği için kendini iyi hissediyordu.

Keith Carter'in Öyküsü

Filmlere ve çok satan polisiye romanlara bakılacak olursa, özel dedektifler, etik konusunda eksikleri, insanlardan istediklerini almak konusunda da fazlaları olan kişiler. İşlerini tamamen yasadışı yöntemler kullanarak yürütüyorlar ve yakalanmaktan kıl payı sıyrılıyorlar. Aslında özel dedektiflerin büyük bir kısmı tamamen yasal işler yürütürler. Pek çoğu iş yaşamlarına yeminli polis memurları olarak başladıkları için neyin yasal olup neyin olmadığını gayet iyi bilirler ve pek çoğu çizgiyi aşmaya hevesli değillerdir.

Ancak istisnalar da vardır. Bazı özel dedektifler -hem de sayıları azımsanmayacak kadar çok- polisiye öykülerde çizilen karakterlere tıpatıp uyarlar. Meslekte bu adamlara *bilgi simsarları* denir. Kuralları çiğnemeye istekli insanlar için kullanılan nazik bir deyimdir. Bazı kısayollara başvurduklarında işlerini daha hızlı ve daha kolay yapabileceklerini bilirler. Bu kısayolların, onları birkaç yıl parmaklıkların arkasına tıkacak suçlar olması, en ahlaksız olanlarını caydırmamaktadır.

Yüksek gelirli özel dedektifler -kentin kiraların yüksek olduğu bir semtinde havalı bir apartman dairesinde çalışanlar- bu tarz işleri kendileri yapmazlar. Bu işleri yapması için bilgi simsarlarını tutmakla yetinirler.

Kendisine Keith Carter diyeceğimiz kişi etikle kendini yormayan türden bir özel dedektifti.

Elindeki iş tam bir "Kocam parayı nerede saklıyor?" işiydi. Ya da arada bir olduğu şekliyle, "Karım parayı nerede saklıyor?". Bazen zengin bir kadın gelir ve kendisine ait paraları kocasının nereye sakladığını öğrenmek ister (paralı bir kadının neden parasız bir adamla evlendiği bilmecesi Keith Carter'ın zaman zaman aklını kurcalasa da, buna hiçbir zaman iyi bir yanıt bulamamıştır).

Bu olayda adı Joe Johnson olan koca, paranın üstüne oturan taraftı. Karısının ailesinden borç aldığı on bin dolarla yüksek teknoloji şirketi ku-

ran ve bunu yüz milyon dolarlık bir şirkete dönüştüren akıllı bir adamdı. Kadının boşanma avukatına göre adam mallarını saklamak konusunda muazzam bir iş yapmış ve avukat mal varlığı beyanı talep etmişti.

Keith başlangıç noktasının Sosyal Güvenlik İdaresi olmasına karar vermişti. Böyle bir durumda Johnson'la ilgili, işe yarayacak bilgilerle dolu olabilecek dosyaları hedefliyordu. Bu bilgiyle donanmış olarak Keith kendini hedef olarak tanıtabilir ve bankaların, komisyoncu firmaların ve off-shore bankacılığı yapan kurumların ona her şeyi anlatmasını sağlayabilirdi.

İlk olarak, yerel bir ilçe bürosunu, herhangi birinin şehir telefon rehberinde bulabileceği 800'lü numarayı kullanarak aradı. Telefona çıkan memura istihkak şubesinden biriyle görüşmek istediğini söyledi. Biraz bekledi sonra telefon açıldı. O anda Keith vites değiştirdi ve "Merhaba" diyerek söze girişti. "Ben Gregory Adams, 329 numaralı Bölge Bürosu'ndan. Sonu 6363'le biten bir hesapla ilgilenen bir tasfiye memuruna ulaşmaya çalışıyorum. Bendeki numarayı çevirdiğimde faks çıkıyor."

"O Mod İki", dedi adam. Telefon numarasına baktı ve Keith'e verdi.

Keith sonra Mod İki'yi aradı. Telefonu May Linn açtığında yine tarz değiştirdi ve Genel Müfettişlik makamından aradığı ve başka birinin kendi bilgisayarını kullandığıyla ilgili sıradan oyununu oynadı. Kadın ona istediği bilgiyi verdi ve gelecekte yardıma ihtiyacı olursa elinden geleni yapacağını söyledi.

Aldatmacanın İncelenmesi

Bu yaklaşımı etkili kılan şey, başka birinin bilgisayarını kullanması ve "müdürüm benden memnun değil" hikâyesini kullanarak çalışanın duygularıyla oynaması oldu. İş yerinde insanlar duygularını pek sık açığa vurmazlar, vurduklarındaysa birilerinin toplum mühendisliğine karşı koyduğu savunmaların üstünden aşıverirler. "Çok zor durumdayım, bana yardım eder misin?" gibi duygusal bir hile, kazançlı çıkmak için yapılan tek şeydi.

Saldırgan, bu bilgiyi halktan gelen telefonlara bakan bir memurdan alamazdı. Keith'in kullandığı tarzda bir saldırı yalnızca karşı tarafta telefonu halka açık olmayan ve dolayısıyla arayanın içerden biri olduğu beklentisi içinde olan biri varsa geçerlidir. Bu da "beni şu gönderdi" tarzı güvenliğe başka bir örnektir.

Bu saldırının işe yaramasına yardımcı olan unsurlar arasında şunlar vardı:

- Mod'un telefon numarasının bilinmesi.
- Kullanılan terimlerin bilinmesi; sayı tarama, harf tarama ve AKAS.
- Genel Müfettişlik makamından olduğunu söylemek. Her federal hükümet çalışanı oranın geniş yetkilere sahip hükümet çapında bir kurum olduğunu bilir ve bu, saldırgana itibarlı bir hava verir.

Başka bir ilginç ayrıntı ise -mantıksal olarak bakıldığında tamamen farklı bir bölümden bambaşka biriyle görüşülseydi çok daha uygun ola-

Sosyal Güvensizlik

İlginç bir şekilde, Sosyal Güvenlik İdaresi, kendi çalışanları için yararlı bilgilerle dolu ancak aynı zamanda toplum mühendisleri için de oldukça değerli olan İdari İşlemler Talimatnamesi'nin bir kopyasını internete koydu. Bu öyküde geçtiği şekliyle kısaltmalar, terimler ve istenilen şeyin nasıl dile getirileceği orada açıkça anlatılıyor.

Sosyal Güvenlik İdaresi'yle ilgili daha çok şey mi öğrenmek istiyorsunuz? Google'da aratmanız ya da aşağıdaki adresi tarayıcınıza girmeniz yeterli: http://policy.ssa.gov/poms.nsf/. Eğer idare bu öyküyü okumuş ve siz bunu okuyana kadar talimatnameyi kaldırmamışsa, bir SGİ memurunun emniyet teşkilatına verebileceği bilgilerin neler olduğuyla ilgili ayrıntılı bilgiler de dahil olmak üzere birçok çevrimiçi açıklama bulacaksınız. Kullanım açısından bakılacak olursa, teşkilat kavramı, bir SGİ memurunu emniyet teşkilatından olduğuna ikna edebilecek toplum mühendislerini de kapsıyor.

cak bir durumda bile- toplum mühendislerinin kimseyi, "Neden beni arıyor?" diye düşündürmeyecek şekilde isteklerini sunuyor olmaları. Belki de arayana yardım etmek günlük döngünün sıradanlığında bir değişiklik yarattığı için kurban isteğin ne kadar olağandışı olduğuna dikkat etmiyordur.

Sonuç olarak bu olaydaki saldırgan, elde olan işe yetecek kadar bilgi toplamakla yetinmeyerek sürekli başvurabileceği bir bağlantı kurmak da istedi. Acındırma saldırısı için, "klavyeme kahve döktüm" gibi sıradan bir hile de kullanabilirdi. Ancak klavye bir günde değiştirilebileceği için, burada işe yaramazdı. Bu nedenle başka birinin kendi bilgisayarını kullandığıyla ilgili öyküyü yazdı. Bunu haftalarca sürdürebilirdi: "Evet, bilgisayarın dün geleceğini sanmıştım. Bir tane geldi ama başka biri bir numara çekip aleti kendine almış. Bu yüzden bu soytarı yine benim odamda bitiverdi." Ve bu iş böyle devam edebilir.

"Zavallı ben, yardıma ihtiyacım var," çok iyi iş görür.

Basit Bir Telefon

Bir saldırganın başlıca enstrümanlarından biri, isteğini makul bir şekilde sunmaktır. Kurbanın günlük işlerinin arasında gelen isteklere benzeyen, kurbanı fazlaca zorlamayacak türden bir şey olmalıdır. Yaşamda, pek çok başka şeyde olduğu gibi, bir gün bir isteği mantıklı bir şekilde sunmak zorken, başka bir gün bu iş çocuk oyuncağı olur.

Mary H'nin Telefonu

Tarih/Saat: 23 Kasım, Pazartesi, sabah 7:49.
Yer: Mauersby & Storch Müşavirlik, New York.

Pek çok insan için muhasebe işi sayılarla boğuşmaktan ve fasulye saymaktan ibarettir ve genellikle kanal tedavisi kadar eğlenceli (!) olduğu düşünülür. Neyse ki herkes işi böyle görmez. Örneğin Mary Harris; kıdemli muhasebecilik görevini ilgi çekici bulan biridir ve çalıştığı firmada konuya en hakim muhasebecilerinden biri olmasının nedenlerinden biri de budur.

O pazartesi sabahı Mary uzun bir gün olmasını beklediği için işe bir an önce başlamak amacıyla ofise erken geldi. O saatte telefonunun çaldığını duyunca şaşırdı. Ahizeyi kaldırdı:

"Merhaba, ben Peter Sheppard. Arbuckle Destek Hizmetleri'nde çalışıyorum, şirketinize teknik destek veriyoruz. Hafta sonunda bilgisayarlarında sorun olan insanlardan birkaç şikâyet aldık. Bu sabah herkes işe gelmeden önce kontrol etmek istedim. Bilgisayarınızı kullanırken ya da ağa bağlanırken sorun yaşıyor musunuz?"

Mary hünüz böyle bir sorunla karşılaşmadığını söyledi. Bilgisayarını açtı ve önyükleme yapılırken Peter ne yapmak istediğini ona anlatmaya başladı.

"Birkaç test yapmak istiyorum", dedi. "Bastığınız tuşları kendi ekranımda görebiliyorum ve ağ üzerinden doğru aktarıldığından emin olmak istiyorum. Her tuşa basışınızda bana onun ne olduğunu söylemenizi istiyorum, böylece burada da aynı harf ya da sayının görünüp görünmediğine bakabilirim. Tamam mı?"

Bilgisayarının çalışmamasıyla ve hiçbir işin bitmediği sıkıcı bir günle ilgili kâbusları olan biri olarak Mary bu adamın kendisine yardımcı olmasından fazlasıyla memnun kalmıştı. Biraz sonra ona, "Giriş ekranındayım ve kullanıcı adımı gireceğim. Şimdi giriyorum, M..A..R...Y..D."

"Şimdiye kadar gayet iyi" dedi Peter. "Onu burada görebiliyorum. Şimdi parolanı gir ama ne olduğunu bana söyleme. Hiç kimseye parolanı söylememelisin, teknik servise bile. Parolan korumalı olduğu için burada yıldızlar çıkacak, yani parolanı göremem." Bunların hiçbiri doğru değildi ama Mary'nin aklına yattı. Sonra Peter, "Bilgisayarın açıldığında haberim olsun" dedi.

Mary açıldığını söylediğinde Peter ona uygulamalardan iki tanesini açmasını söyledi. Kadın her ikisinin de gayet iyi çalıştıklarını haber verdi.

Mary her şeyin doğru bir şekilde çalışmasından memnun olmuştu. "Bilgisayarının sağlam olup olmadığını kontrol edebildiğim iyi oldu. Birşey daha var" dedi Peter ve devam etti, "Çalışanların parolalarını değiş-

tirebilmesi için bir güncelleme yaptık. Bana birkaç dakikanı ayırıp doğru çalışıp çalışmadığını görmeme yardımcı olabilir misin?"

Mary, yardım etmesinden dolayı adama müteşekkirdi ve hemen kabul etti. Peter ona, kullanıcıların parolalarını değiştirebilmesini sağlayan uygulamayı çalıştırmak için yapması gerekenleri adım adım anlattı. Parola değiştirme aslında Windows 2000 işletim sisteminin sıradan unsurlarından biridir. "Hadi şimdi parolanı gir", dedi kadına. "Sesli bir şekilde söylememen gerektiğini unutma."

Kadın bunu da yaptığında, Peter, "Hızlı bir deneme yapmak için, sana yeni parolanı sorduğunda, 'test123' gir. Sonra doğrulama kutucuğuna bir kez daha gir ve ENTER'e bas", dedi.

Sunucu bağlantısını çözme işleminde Mary'e yardımcı oldu. Sonra birkaç dakika bekletip, yeni parolasını deneyerek yeniden bağlanmasını istedi. Her şey saat gibi işliyordu, Peter çok memnun kalmıştı ve -kadını bir kez daha parolasını açıkça söylememesi için uyararak- Mary'nin eski parolasına dönmesi ya da yeni bir tane seçmesi konusunda yardımcı oldu.

"Çok iyi, Mary", dedi Peter. "Hiçbir sorun çıkmadı, bu çok iyi. Dinle, eğer herhangi bir sorun çıkarsa Arbuckle'dan bizi ara. Ben çoğunlukla özel projelerde çalışıyorum ama burada telefonu açan herkes sana yardımcı olabilir." Mary ona teşekkür etti ve vedalaştılar.

Peter'in Öyküsü

Peter'le ilgili söylentiler alıp başını gitmişti. Mahallesinde onunla birlikte okula giden birileri, başkalarının bulamadığı şeyleri bulabilen zeki bir bilgisayar manyağı olduğunu duymuşlardı. Alice Conrad ondan bir konuda yardım istediğinde önce hayır dedi. Neden yardım edecekti ki? Bir keresinde o kızla bir yerlerde karşılaştığında ona çıkma teklif etmiş, kız da onu geri çevirmişti.

Ancak yardım etmeyi reddetmesi kızı şaşırtmış gibi görünmüyordu. Zaten Peter'in yapabileceği birşey olduğunu düşünmediğini söyledi. Bu bir meydan okumaydı, çünkü yapabileceğinden emindi. Böylece Peter işi yapmayı kabul etti.

Alice'e bir pazarlama şirketine danışmanlık yapması için sözleşme teklif edilmişti ama sözleşme koşulları çok iyi değildi. Daha iyi koşullar talep etmeden önce diğer danışmanların sözleşmelerinin ne tür koşulları içerdiğini öğrenmek istiyordu.

Peter'in anlattığı şekliyle hikâye şöyle:

Alice için bunu söyleyemem ama yapabileceğimi düşünmedikleri birşeyi yapmamı isteyen insanlardan yaka silkmiştim. Üstelik de ben işin kolay olduğunu bilirken. Peki, o kadar da kolay değildi, en azından bu sefer. Biraz çaba gerektirecekti ama sorun olmayacaktı.

Ona akıllının ne demek olduğunu gösterecektim.

Pazartesi sabahı 7:30'u biraz geçe pazarlama şirketinin bürosunu aradım ve danışmayla görüşüp onlara muhasabeden biriyle konuşmam gerektiğini söyledim. Muhasebeden kimsenin gelip gelmediğini biliyor muydu acaba? Danışma görevlisi bana, "Sanırım birkaç dakika önce Mary'nin geldiğini gördüm, sizi ona bağlamaya çalışayım" dedi.

Mary telefonu açtığında ona bilgisayar sorunlarıyla ilgili küçük hikâyemi anlattım. Hikâye tüyleri diken diken etmek üzere tasarlanmıştı. Böylece bana büyük bir memnuniyetle yardımcı olacaktı. Parolasını değiştirmesine yardımcı olur olmaz kullanmasını istediğim geçici parola olan "test123"le hemen sisteme girdim.

Ustalık burada işin içine giriyordu; şirketin bilgisayar sistemine istediğim zaman kendime ait gizli bir parolayla girmemi sağlayacak küçük bir program yükledim. Mary'le konuşmam bittikten sonra, ilk işim sisteme girdiğimi kimsenin anlamaması için denetim tarihçesini silmek oldu. Bu kolay bir şeydi. Sistem yetkilerimi artırdıktan sonra güvenlikle ilgili www.ntsecurity.nu adlı bir internet sayfasında bulduğum *clearlogs* adında bedava bir programı indirdim.

Asıl işe sıra gelmişti. Dosya adında "sözleşme" kelimesi geçen belgeleri arattırdım ve dosyaları indirdim. Sonra biraz daha arama yaptım ve ana damarı, danışman ücret bilgilerinin olduğu klasörü buldum. Böylece tüm sözleşme dosyalarını biraraya getirdim ve bir ödemeler listesi yaptım.

Alice sözleşmelere bakabilir ve diğer danışmanlara ne kadar verdiklerini görebilirdi. Tüm bu dosyaları arama hamallığını kendisi yapsın. Ben onun benden istediği şeyi yapmıştım.

Verileri kaydettiğim disketlerden, kanıtları Alice'e gösterebilmek için birkaç dosyanın çıktısını aldım. Onu benimle buluşmaya ve akşam yemeğe çıkmaya zorladım. Kâğıtları karıştırırken yüzünün aldığı şekli görmeliydiniz. "Olamaz" dedi. "Olamaz."

Disketleri yanımda getirmemiştim. Onlar yemdi. Disketleri almak için bana gelmesi gerektiğini söyledim; ona yaptığım iyilikten dolayı bana duyduğu minneti göstereceğini umuyordum.

Aldatmacanın İncelenmesi

Peter'in pazarlama şirketini araması en temel toplum mühendisliği şekline bir örnektir. Çok az hazırlık gerektiren, ilk denemede işleyen ve birkaç dakikada başarılı olan basit bir girişimdir.

Daha da iyisi, kurban Mary'nin bir oyuna ya da bir hileye kurban gittiğini düşünmesi, durumu bir yerlere bildirmesi ya da yaygara koparması için hiçbir neden yoktu.

Mitnick Mesajı:

İsteğini dile getirme şekline bağlı olarak bir toplum mühendisinin insanlara bir şeyler yaptırmasının ne kadar kolay olduğunu görmek şaşırtıcı. Temel şart, psikolojik kurallara dayalı istemsiz bir tepkiyi tetiklemek ve arayanı bir müttefik olarak gördükleri zaman insanların zihinlerinde oluşan kısayollara güvenmektir.

Plan, Peter'in üç toplum mühendisliği taktiğini kullanması üstüne kuruluydu. Önce korku uyandırıp -bilgisayarının çalışmayabileceğini düşündürerek- Mary'nin işbirliği yapmasını sağladı. Sonra kadının kullandığı uygulamalardan ikisini çalıştırmasını bekledi, böylece kadın onların çalıştığından emin olacaktı ve ikisinin arasındaki ilişkiyi güçlendirecek, bir müttefiklik duygusu uyandıracaktı. En sonunda, bilgisayarının sağlam olduğundan emin olmak için gösterdiği yardımdan duyduğu minnettarlıkla oynayarak işinin en önemli kısmını gerçekleştirmek için biraz daha yardım etmesini sağladı.

Ona parolasını kendisine bile açıklamamasını söyleyerek Peter kusursuz bir ustalıkla şirket dosyalarının güvenliğiyle ilgili endişesi konusunda Mary'i ikna etti. Bu davranışı da, şirketi ve kendisini koruduğu için Peter'in bir sahtekâr olmadığı yolundaki güvenini artırdı.

Polis Baskını

Şöyle bir sahne hayal edin: Polis, internet üzerinden bedava film dağıtan Arturo Sanchez adında birini kapana kıstırmak ister. Hollywood stüdyoları adamın telif haklarını ihlal ettiğini söylemektedir, adam ise kaçınılmaz olarak girecekleri bir pazarı görmeleri ve yeni filmleri indirilebilir şekle sokmak için bir şeyler yapmaya başlamaları için onları dürtmeye çalışmaktadır. Arturo bunun stüdyolar için, tamamen göz ardı edilen, büyük bir gelir kaynağı olacağına (haklı olarak) parmak basmaya uğraşmaktadır.

Arama İzni Lütfen

Bir gece geç saatte eve döndüğünde yolun karşısından evinin pencerelerine bakar ve tüm ışıkların sönük olduğunu fark eder. Halbuki dışarı çıkarken birini hep açık bırakmaktadır.

Kapısını çalarak komşusunu uyandırır ve binaya bir polis baskını yapıldığını öğrenir. Ancak herkesi aşağıda bekletmişlerdir ve komşusu polislerin hangi evi aradıklarından emin değildir. Tek bildiği, ellerinde bazı ağır şeylerle dışarı çıktıklarıdır, ancak her şey sarılı olduğu için ne olduklarını anlayamamıştır ve kimseyi kelepçeleyip götürmemişlerdir.

Arturo oturduğu daireyi kontrol eder. Kötü haber: polislerin bıraktığı ve üç gün içerisinde arayıp bir randevu alması gerektiğini söyleyen bir kâğıt bulur. En kötü haber ise: bilgisayarlarını götürmüşlerdir.

Arturo ortalıktan kaybolur ve bir arkadaşının yanında kalmaya başlar. Ama belirsizlik içini kemirmektedir. Polis ne bilmektedir? Sonunda onu yakalamışlar ama kaçması için de bir fırsat mı tanımışlardır? Yoksa bu, kenti terk etmesine gerek kalmadan çözebileceği, tamamen farklı bir konu mudur?

Devam etmeden önce bir an durup düşünün: Polisin sizinle ilgili neler bildiğini öğrenmenin bir yolunu hayal edebiliyor musunuz? Politikacı tanıdıklarınız, Emniyet Müdürlüğü'nde arkadaşlarınız ya da savıcılıkta dostlarınız olmadığını varsayarsak, sıradan bir vatandaş olarak sizin bu bilgiyi elde edebilmeniz için bir yol olabilir mi? Ya da toplum mühendisliği becerileri olan biri böyle bir şeyi başarabilir mi?

Polisi Oyuna Getirmek

Arturo bilgilenme isteğini şöyle tatmin eder: Başlangıç olarak yakınlardaki bir fotokopi dükkânının telefon numarasını bulur, onları arar ve faks numaralarını ister.

Sonra bölge savcılığını arar ve evrak bölümünü ister. Evrak bürosuna bağlandığında kendini Lake Bölgesi'nden gelen bir dedektif olarak tanıtır ve halihazırda geçerli arama emirlerini takip eden memurla görüşmek istediğini söyler.

"Ben ilgileniyorum" der kadın. "Çok iyi", diye karşılık verir Arturo. "Dün gece bir suçluya baskın yaptık, baskının yazılı beyanına ulaşmaya çalışıyorum."

"Adreslere göre tutuyoruz", der kadın.

Adresi verir. Kadının sesi oldukça heyecanlı gelmiştir. "Ah, evet", der kadın coşkuyla. "Biliyorum bunu. Telif suçlusu."

"Tamam, o", der Arturo. "Yazılı beyanın ve arama emrinin bir kopyasına ihtiyacım var."

"Burada, önümde."

"Çok iyi", der adam. "Şu anda dışarıdayım ve bu konuyla ilgili on beş dakika sonra Gizli Servis'le bir toplantıya gireceğim. Bugünlerde biraz dalgınım, dosyayı evde unutmuşum ve gidip almaya kalkarsam yetişemeyeceğim. Sizden bir kopyasını alabilir miyim?"

"Elbette, sorun olmaz. Fotokopilerini çekerim, buraya gelip alabilirsiniz."

"Harika", der Arturo. "Çok iyi oldu ama şu anda şehrin diğer ucundayım. Bana fakslamanız mümkün mü?"

Bu biraz sorun yaratır ama aşılamaz birşey değildir. "Evrak bürosunda faksımız yok", der kadın. "Ama aşağıda sekreter odasında bir tane var. Kullanmama izin verebilirler."

"Ben sekreter odasını arayıp, gerekli ayarlamaları yaparım", der adam.

Sekreter odasındaki kadın bu işle memnuniyetle ilgilenecektir ama bunu kimin ödeyeceğini bilmek istemektedir. Bir fatura numarasına ihtiyacı vardır.

"Ben numarayı alıp, sizi yine ararım", der kadına.

Sonra bölge savcılığını arar, yine kendini bir polis memuru olarak tanıtır ve danışmadaki görevliye soruverir: "Bölge savcılığının fatura numarası nedir?" Görevli duraksamadan numarayı söyler.

Sekreter odasını geri arayıp fatura numarasını verir.

Fatura numarasını vermek için sekreter odasını geri araması o hanımı biraz daha işlemek için bahane olur. Kadını yukarı çıkıp fakslanacak evrakları almaya ikna eder.

İzlerini Örtmek

Arturo'nun birkaç adım daha atması gereklidir. Her zaman birilerinin birşeylerden kuşkulanması olasılığı vardır ve fotokopi mağazasına gidip belli bir faksı almak üzere birinin gelmesini bekleyen, sıradan giyimli birkaç polis memuruyla karşılaşabilecektir. Biraz bekler, sonra da faksın gönderilip gönderilmediğini kontrol etmek için sekreter odasına telefon eder. Şimdiye dek her şey yolunda gitmiştir.

Aynı mağaza zincirine bağlı, şehrin diğer tarafındaki başka bir fotokopi mağazasını arar ve işlerinin görülmesinden ne kadar memnun kaldığını ve müdüre bir teşekkür mektubu yazmak istediğini söyleyip müdürün adını sorar. Bu önemli bilgiyi kullanarak ilk fotokopi mağazasına telefon eder ve müdürle konuşmak istediğini söyler. Karşı taraf telefonu açtığında Arturo, "Merhaba, ben 628 Hartfield mağazasından Edward. Müdürüm. Anna sizi aramamı söyledi. Biraz kızgın bir müşterimiz var; biri ona yanlış mağazanın faks numarasını vermiş. Burada önemli bir faks bekliyor ve ona verilen faks sizin mağazanın numarası." Müdür, mağaza çalışanlarından birine faksı buldurup hemen Hartfield mağazasına gönderteceğine söz verir.

Faks ikinci mağazaya geldiğinde Arturo orada beklemektedir. Belgeleri aldıktan sonra sekreter odasındaki hanıma teşekkür etmek için arar ve "Elinizdeki kopyaları yukarı çıkarmanıza gerek yok, onları atabilirsiniz." der. Sonra ilk mağazanın müdürüne de telefon eder ve ona da ellerindeki faksı atabileceklerini söyler. Böylece birilerinin gelip sorular sorması olasılığına karşı, olan bitenle ilgili ortalıkta hiçbir iz kalmayacaktır. Toplum mühendisleri tedbirin elden bırakılmaması gerektiğini iyi bilirler.

Böyle bir düzmeceyle Arturo ilk fotokopi mağazasına gelen faks için

ve ikinci mağazaya faks göndermek için para vermek zorunda kalmamıştır. Eğer polis ilk mağazaya gelmiş olsaydı, ikinci noktaya adam gönderene kadar o çoktan gitmiş olurdu.

Öykünün sonu: Yazılı beyan ve arama emrinde yazdığına göre, polisin elinde Arturo'nun film kopyalama faaliyetleriyle ilgili belgelenmiş deliller vardır. Arturo'nun bilmek istediği şey budur. Geceyarısı olmadan eyalet sınırını geçer. Arturo yeni bir yaşama başlamak üzere yola çıkmıştır ve başka bir yerde yeni bir kimlikle işine yeniden başlamaya hazırdır.

Aldatmacanın İncelenmesi

Bölge savcılığında çalışan insanlar sürekli emniyet teşkilatı mensuplarıyla temas halindedirler; sorular sorarlar, düzenlemeler yaparlar, mesajlar alırlar. Telefonu açıp da kendine polis memuru, komiser yardımcısı ya da başka birşey deme cesareti olan herkesin sözüne güvenilir. Kullanılan terimleri bilmemesi, gergin olması, söylediklerini karıştırması ya da sesinde bir terslik olması gibi durumlar yoksa kimliğini doğrulaması için ona tek bir soru bile sorulmaz. Burada, iki farklı memurla yaşanan da tam olarak budur.

Eksik fatura numarası tek bir telefonla halledilmişti. Sonra Artura "On beş dakika sonra Gizli Servis'le bir toplantıya gireceğim, bugünlerde biraz dalgınım ve dosyayı evde unutmuşum", gibi bir öyküyle acındırma kartını oynamıştı. Kadın doğal olarak ona acımış ve işini gücünü bırakıp ona yardım etmişti.

Daha sonra Arturo bir değil iki fotokopi mağazası kullanarak faks almak konusunda kendini sağlama almıştı. Bunun üzerinde bir çeşitleme yapmak faksın izlenmesini daha da zorlaştırırdı: Saldırgan belgeyi başka bir fotokopi mağazasına göndermek yerine, faks numarası gibi gözüken ama aslında sizin adınıza faksları alan ve e-posta adresinize gönderen ücretsiz bir internet hizmetini kullanabilirdi. Böylece belge doğrudan saldırganın bilgisayarına indirilir, saldırganın yüzünü göstermesi hiç gerekmezdi. İş tamamlanır tamamlanmaz da e-posta adresi ve elektronik faks numarası terk edilirdi.

Rollerin Değişmesi

Kendisine Michael Parker diyeceğimiz genç bir adam yüksek gelirli işlerin üniversite mezunlarına gittiğini geç anlayan insanlardan biriydi.

NOT: *Nasıl oluyor da bir toplum mühendisi emniyet müdürlükleri, savcılıklar, telefon şirketleri uygulamaları, saldırılarında işine yarayacak iletişim ve bilgisayar şirketlerinin yapıları gibi, bu kadar çok işleme yönelik ayrıntıyı bilebiliyor? Çünkü bu onun işi. Bu bilgiler toplum mühendisinin sermayesidirler ve kandırma çabalarında ona yardımcı olurlar.*

Mitnick Mesajı:

İşin gerçeği, kimsenin iyi bir toplum mühendisi tarafından kandırılmaya karşı bağışıklığı yoktur. Günlük yaşamın lüzı nedeniyle, bizim için önemli olan konularda bile, her zaman üzerinde düşünülmüş kararlar veremeyiz. Karışık durumlar, zaman kısıtlamaları, ruh hali ya da zihin yorgunluğu dikkatimizin dağılmasına neden olabilir. Bu yüzden zihinsel kısayollar oluşturur, bilgiyi tam ve özenle incelemeden kararlarımızı veririz. Bu zihinsel sürece otomatik tepki verme denir. Tüm federal, eyalet ve yerel emniyet görevlileri için bile geçerlidir. Hepimiz insanız.

Yarım burs artı eğitim kredileriyle yerel bir üniversiteye gitme olanağı vardı ama bu, kirayı, yemeği, benzini ve araba sigortasını ödemek için geceleri ve hafta sonları çalışması anlamına geliyordu. Her zaman kısayolları bulmayı seven Michael, daha hızlı olan ve daha az çabayla sonuç veren başka bir yol olabileceğini düşündü. On yaşında ilk kez bir bilgisayarla oynadığından beri bu aletlerle ilgili pek çok şey öğrenmiş ve nasıl çalıştıkları konusuna kafayı takmıştı. Hızlandırılmış bir bilgisayar bilimleri lisans diploması yaratmayı denemeye karar verdi.

Üstün Başarısız Mezuniyet

Eyalet üniversitesinin bilgisayar sistemlerine girip, temiz bir B+ ya da A- ortalamayla mezun olmuş birinin kayıtlarını bulabilir, kayıtları kopyalar, adını değiştirir ve o yılın mezuniyet sınıfı listesine ekleyebilirdi. Düşününce bu fikirden rahatsız oldu. Kampüste bulunan bir öğrenciye ait başka kayıtların da olması gerektiğine karar verdi; harç ödeme kayıtları, yurtlar ofisi ve daha kim bilir başka neler. Yalnızca derslerin ve notların kaydını çıkarmak çok fazla açık oluşmasına neden olacaktı.

Düşünüp üzerinde kurdukça aklına uygun bir geçmişte bilgisayar bilimlerinden mezun kendiyle aynı adı taşıyan biri olup olmadığına bakmak geldi. Eğer varsa, iş başvuru formlarına onun Sosyal Güvenlik Numarası'nı girebilirdi, böylece adını ve sosyal güvenlik numarasını üniversiteden kontrol etmek isteyen biri, "Evet, söz konusu diplomayı almıştır", yanıtını alırdı. (Kendinin bildiği ama çoğu insanın farketmeyeceği birşey yapıp, işe başvururken diğer Parker'in Sosyal Güvenlik Numarası'nı girip sonra işe alınırsa, başlama formlarına kendi gerçek numarasını yazabilirdi. Çoğu şirket, yeni işe giren birinin iş başvurusunda farklı bir numara kullanıp kullanmadığını kontrol etmeyi akıl etmezdi.)

Belaya Bağlanmak

Üniversite kayıtlarında Michael Parker'i nasıl bulacaktı? Şöyle bir şey yaptı:

Üniversitenin ana kütüphanesine giderek bir bilgisayar uçbiriminin başına oturdu, üniversitenin internet sitesine girdi. Sonra Öğrenci İşleri'ni aradı. Telefona çıkan kişiye artık iyice aşina olduğunuz toplum mühendisliği taktiklerinden birini uyguladı. "Bilgi İşlem Merkezi'nden arıyorum. Ağ yapılandırmasında değişiklikler yapıyoruz ve erişiminizi engellemediğimizden emin olmak istiyoruz. Hangi sunucuya bağlısınız?"

"Sunucuyla ne demek istiyorsunuz?" diye sordu karşı taraf.

"Öğrenci akademik verilerine ulaşmak istediğinizde hangi bilgisayara bağlanıyorsunuz?"

Aldığı yanıt, admin.rnu.edu oldu. Konuştuğu kişi öğrenci kayıtlarının tutulduğu bilgisayarın adını ona vermişti. Bu, bulmacanın ilk parçasıydı. Artık hangi makineyi hedef alacağını biliyordu.

Adresi bilgisayara girdi ve bir yanıt alamadı. Bu, beklediği bir durumdu, erişimi engelleyen bir güvenlik duvarı vardı. O bilgisayar üzerinde çalışan hizmetlerden herhangi birine bağlanıp bağlanmadığını kontrol etmek için bir program çalıştırdı ve bir bilgisayarın uzaktan başka bir bilgisayara bağlanmasını ve ona bir basit uçbirim olarak erişmesini sağlayan bir Telnet servisinin çalıştığı açık bir bağlantı noktası buldu. Oraya girmek için ihtiyacı olan tek şey standart bir kullanıcı adı ve parolaydı.

Öğrenci İşleri'ni tekrar aradı ve bu kez farklı biriyle konuştuğundan emin olmak için önce dikkatle dinledi. Bir kadın çıktı ve ona yine üniversite Bilgi İşlem Merkezi'nden olduğunu söyledi. İdari kayıtlar için yeni bir işletim sistemi yüklediklerini anlattı. Bir ayrıcalık yapıp, deneme kipinde olan yeni sisteme onun bağlanmasını ve öğrenci akademik kayıtlarına erişip erişemediğine bakmasını istedi. Bağlanacağı adresin IP numarasını verdi ve ona neler yapması gerektiğini anlattı.

Aslında IP adresi kadını Michael'ın kütüphanede önünde oturduğu bilgisayara yönlendirmişti. Sekizinci bölümde açıklanan sürecin aynısını kullanarak, öğrenci kayıtlarına bakmak için girdiği sistemde görmeye alışık olduğunun tıpatıp aynısı bir giriş benzetimcisi, yani sahte bir giriş ekranı yaratmıştı. "Çalışmıyor" dedi kadın. "Sürekli 'Giriş Hatalı' mesajı veriyor."

Giriş benzetimcisi, kullanıcı adı ve parola girilirken kullanılan tuşları çoktan Michael'in uçbirimine kaydetmişti bile. Kadına, "Bazı hesaplar henüz bu makinaya aktarılmadı. Size bir hesap açayım, sonra yine ararım" dedi. Her yetenekli toplum mühendisi gibi açık uçları bağlamak konusuna dikkat ederek, kadını aramayı unutmamayı bir kenara not etti. Telefon edip test sisteminin henüz tam olarak çalışmadığını ve eğer onun için bir sorun olmayacaksa sorunun nereden kaynaklandığını bulduklarında arkadaşlarının onu arayacaklarını söyleyecekti.

Yardımsever Memur

Artık Michael hangi bilgisayar sistemine bağlanması gerektiğini bili-

Terimler

BASİT UÇBİRİM: Kendi mikroişlemcisi olmayan uçbirim. Basit uçbirimler yalnızca basit komutlar kabul ederler ve sadece harf ve sayıları gösterebilirler.

yordu ve elinde bir kullanıcı adı ve parola vardı. Ancak doğru ad ve mezuniyet tarihine sahip bir bilgisayar bilimleri mezununu aratabilmek için hangi komutlara gereksinimi olacaktı? Öğrenci veri tabanı bunun için çok uygundu. Üniversitenin ve öğrenci işlerinin ihtiyaçlarına göre hazırlanmıştı ve veri tabanına erişim için kendine özgü bir kullanımı vardı.

İlk adım bu son engeli kaldırmaktı: Öğrenci veri tabanını taramanın gizemleri konusunda ona kimin yol gösterebileceğini bulmalıydı. Öğrenci işlerini tekrar aradı ve yine başka biriyle konuştu. Kadına, Mühendislik Fakültesi Dekanlığı'ndan aradığını söyledi ve, "Öğrenci akademik dosyalarına ulaşmakta sorun yaşadığımız zaman kimi aramamız gerekiyordu?" diye sordu.

Bir süre sonra üniversitenin veri tabanı yöneticisiyle telefonda görüşüyor, ona bir acındırma numarası çekiyordu: "Ben Mark Sellers, öğrenci işlerinden. Yeni işe başlayan birine yardım eder misin? Seni aradığım için özür dilerim ama şu anda herkes toplantıda ve etrafta bana yardım edebilecek kimse yok. 1990 ve 2000 yılları arasındaki bilgisayar bilimleri mezunlarının listesine ihtiyacım var. Bu akşama kadar istiyorlar ve bunu onlara veremezsem, bu işte uzun süre kalamayabilirim. Başı dertte olan birine yardım etmek ister misin?" İnsanlara yardım etmek bu veri tabanı yöneticisinin işinin bir parçası olduğu için Michael'a yapması gerekenleri adım adım anlatırken iki kat fazla sabır göstermişti.

Konuşmaları bitene kadar Michael o yıllara ait tüm bilgisayar bilimleri mezunlarını içeren listeyi indirmişti. Birkaç dakika içinde bir arama yapmış ve iki Michael Parker birden bulmuştu. Bir tanesini seçti ve adamın Sosyal Güvenlik Numarası'nın yanı sıra veri tabanında bulunan başka işe yarar bilgileri de aldı.

Az önce, "Michael Parker, Bilgisayar Bilimleri Lisans Derecesi'ni 1998 yılında üstün başarı ile tamamlamıştır" unvanını almıştı. Bu durumda 'Lisans Derecesi' sahibi olması çok yerinde bir sonuç olmuştu.

Aldatmacanın İncelenmesi

Bu saldırıda daha önce sözünü etmediğim bir yöntem kullanıldı: Saldırganın, kuruluşun veri tabanı yöneticisine nasıl işleyeceğini bilmediği bir bilgisayar sürecinin adımlarını tek tek anlattırması. Rollerin güçlü ve etkili bir şekilde değiştirilmesi. Bu, raflarından mal arakladığınız dükkânın sahibinden kutuyu arabanıza kadar taşımanıza yardım etmesini istemek gibi bir şey.

Aldatmacanın Engellenmesi

Acındırma, suçluluk duyurma ve sindirme, toplum mühendilerinin en çok kullandığı üç·psikolojik yöntemdir ve bu öyküler bu taktiklerin kullanım şeklini göstermiştir. Siz ve bilgisayarınız bu tarz saldırılardan kaçınmak için neler yapabilirsiniz, biliyor musunuz?

Verilerin Korunması

Bu bölüm kapsamında anlatılan bazı öyküler, kişi şirketinizde çalışıyor (ya da öyle görünüyor) ve belge, şirket içi bir elektronik postaya ya da faks makinasına gönderiliyor olsa da tanımadığınız birine bir dosya göndermenin tehlikelerini vurguluyor.

Şirket güvenlik kuralları, göndericinin şahsen tanımadığı birine önemli bilgileri teslim etmesiyle ilgili son derece net olmalıdır. Hassas bilgiler içeren dosyaların aktarılmasına yönelik zorunlu süreçler belirlenmelidir. Şahsen tanınmayan birinden gelen bir talep durumunda, kontrol etmek için tanımlanmış açık adımlar olmalıdır ve bunları bilginin hassaslığına göre farklı düzeylerde yetkiler gerektirmelidir.

İşte göz önüne alınacak birkaç teknik:

- Bilginin neden istendiğini öğrenin (tanımlı bilgi sahibinden yetki alınmasını gerektirebilir).
- Bu işlemlere ait kişisel ya da birim içi günlük tutun.
- Süreçler konusunda eğitilmiş ve hassas bilgileri dışarı vermek üzere yetkilendirilmiş kişilerin bir listesini bulundurun. Çalışma grubunun dışına gönderilecek bilgilerin yalnızca bu kişiler tarafından gönderilmesini zorunlu kılın.
- Eğer istek yazılı olarak yapılmışsa (e-posta, faks ya da posta), isteğin, gönderdiğini düşündüğünüz kişiden geldiğinden emin olmak için gerekli önlemleri alın.

Parolalara İlişkin

Hassas bilgiye erişimi olan tüm çalışanların -bugün bu neredeyse

Mitnick Mesajı:

Bilgisayar kullanıcıları bu teknolojik dünyada var olan toplum mühendisliğine ilişkin tehditler ve zayıflıklardan bazen büsbütün habersiz oluyorlar. Bilgiye erişimleri var, ancak yine de neyin bir güvenlik tehdidi olabileceğiyle ilgili ayrıntılı bilgileri yok. Toplum mühendisi, aradığı bilginin değerini tam olarak bilmeyen bir çalışanı hedefleyecektir; böylece hedef, tanımadığı birinin isteğini yerine getirmeye daha meyilli olacaktır.

bilgisayarla çalışan herkes anlamına geliyor- parola değiştirmek gibi basit işleri birkaç saniyeliğine bile olsa yapmalarının büyük güvenlik açıklarına neden olabileceğini bilmeleri gerekiyor.

Güvenlik eğitimleri parola konusunu da içermelidir ve konu, parolanın ne zaman ve nasıl değiştirilebileceği, nelerin geçerli parolalar olacağı ve bu sürece başkalarını da katmanın oluşturabileceği tehlikelere odaklanmalıdır. Eğitim, tüm çalışanlara, özellikle parolalarının sorulduğu isteklere karşı şüpheyle yaklaşmaları gerektiğini vurgulamalıdır.

Dışarıdan bakıldığında bunun çalışanlara aktarmak için çok basit bir mesaj olduğu düşünülebilir. Öyle değildir. Böyle bir fikri takdir etmeleri için çalışanların, parolanın değiştirilmesi gibi basit bir işin nasıl güvenlik açıklarına yol açacağını anlamış olmaları gerekir. Bir çocuğa, "Karşıdan karşıya geçerken her iki yöne de bak" diyebilirsiniz ama çocuk bunun neden önemli olduğunu anlayana kadar olaya at gözlükleriyle bakmasına göz yummanız gerekir. At gözlükleriyle bakılan kurallar ya göz ardı edilir ya da unutulur.

Merkezî Bir Bildirim Noktası

Güvenlik politikanız, kuruluşunuza girme teşebbüsleri gibi görünen şüpheli faaliyetlerin bildirileceği bir kişi ya da guruptan oluşan merkezî bir nokta da oluşturmalıdır. Tüm çalışanlar elektronik ya da fiziksel bir müdahaleden kuşkulandıklarında kimi aramaları gerektiğini bilmelidirler. Bildirimin yapılması gereken noktanın telefon numarası her zaman el atında olmalıdır; böylece çalışanlar bir saldırı gerçekleştiğinden şüphelenirlerse numarayı bulmaya çalışmak zorunda kalmazlar.

Bilgisayar Ağını Koruyun

Çalışanlar bir bilgisayar sunucusu ya da ağ adının önemsiz bir bilgi olmadığını bilmelidirler. Aksine, güven uyandırabilmesi ya da istediği bilginin yerini öğrenmesi için saldırgana önemli bir kaynak oluşturabilirler.

Özellikle veri tabanı yöneticileri gibi, yazılımlarla çalışan kişiler teknik uzmanlığı olanlar grubuna girerler ve onların, kendilerinden bilgi ve tavsiye isteyen kişilerin kimliklerini doğrulamak konusunda çok katı ve özel kurallar çerçevesinde çalışmaları gereklidir.

Sürekli olarak bilgisayar desteği veren kişiler, ne tür isteklerin kırmı-

NOT: *Parolalar toplum mühendisliği saldırılarının o kadar önemli bir odak noktasıdır ki on altıncı bölümü tamamıyla buna ayırdık. Orada parolaların yönetilmesiyle ilgili önerilen kuralları bulabileceksiniz.*

zı ışık yaktığını, diğer bir deyişle, arayanın bir toplum mühendisliği saldırısı gerçekleştirdiğini gösteren durumlara karşı çok iyi bir eğitimden geçirilmelidirler.

Bu bölümün en son öyküsünde veri tabanı yöneticisinin bakış açısından, arayanın gerçek birinin kıstaslarına uyduğunu da belirtmeden geçemeyeceğim. Kampüsten arıyordu ve içinde bulunduğu site kesinlikle kullanıcı adı ve parola gerektiren bir siteydi. Bilgi talep eden birinin kimliğini doğrulamak için standart süreçlerin olmasının önemini bu durum bir kez daha vurguluyor. Özellikle de, arayanın gizli kayıtlara ulaşmak konusunda yardım istediği böyle bir olayda.

Tüm bu öneriler, üniversiteler ve yüksekokullar için ikiye katlanıyor. Bilgisayar korsanlığının pek çok üniversite öğrencisinin en sevdiği uğraş olduğu yeni bir haber sayılmaz ve öğrenci kayıtlarının ve bazen de fakülte kayıtlarının çekici hedefler teşkil etmeleri de şaşırtıcı değildir. Bu sömürü o kadar büyük boyutlardadır ki bazı şirketler kampüsleri tehlikeli bölgeler olarak değerlendirirler ve sonu .edu ile biten öğretim kurumlarının erişimini engellemek için güvenlik duvarları oluştururlar.

Uzun lafın kısası her türlü öğrenci ve personel kayıtları başlıca hedefler olarak görülmeli ve hassas bilgi kapsamında çok iyi korunmalıdır.

Eğitim İpuçları

Çoğu toplum mühendisliği saldırıları -nereye bakacağını bilenler için- savunulması komik olacak kadar kolay şeylerdir.

Şirket bakış açısından baktığımızda iyi bir eğitim verilmesi için önemli bir gereksinim vardır. Ancak aynı zamanda, insanlara öğrendiklerini hatırlatacak çeşitli yollar da olmalıdır.

Kullanıcının bilgisayarı açılırken her gün başka bir mesaj içeren bir ekran çıkabilir. Mesaj öyle tasarlanmış olmalıdır ki, kendiliğinden kaybolmamalı ve kullanıcının okuduğuna dair bir çeşit onay kutucuğuna tıklamasını gerektirmelidir.

Önerebileceğim bir başka yaklaşım ise bir dizi güvenlik mesajıdır. Sık sık görülen hatırlatma mesajları önemlidir çünkü bir bilinçlilik programı sürekli ve sonsuz olmalıdır. İçerikleri sunarken mesajlar her seferinde aynı şekilde dile getirilmemelidir. Araştırmalara göre farklı bir cümleyle sunulduğunda ya da farklı örnekler kullanıldığında bu mesajlar daha etkili olmaktadır.

Bir diğer kusursuz yaklaşım ise şirket bültenine kısa ilanlar vermektir. Her ne kadar bir güvenlik köşesi çok yerinde olacaksa da bu ilanlar tam bir köşe oluşturmamalıdır. Onun yerine, okuduğunuz gazetedeki küçük ilanlar gibi, iki ya da üç sütun genişliğinde bir ilan kutusu tasarlanabilir. Bültenin her baskısında, bu kısa ve dikkat çekici yöntemle yeni bir güvenlik unsuru hatırlatılabilir.

9 TERS DALAVERE

Bu kitabın başka bir yerinde de sözü edilen Belalılar (The Sting) filmi -ki bana göre dolandırıcılıkla ilgili yapılmış herhalde en iyi filmdir- zorlu bir kumpası büyüleyici bir ayrıntılandırmayla anlatır. Fimdeki dalavere, "büyük dalavereler" olarak bilinen üç büyük dolandırıcılık çeşidinden biri olan "*telleme*" işinin nasıl yürütüldüğünün açık bir örneğidir. Profesyonel bir ekibin bir oyun çevirip bir gecede nasıl büyük paralar hortumladığını öğrenmek istiyorsanız bundan iyi bir ders kitabı yoktur.

Ancak geleneksel dolandırıcılıklar, ne tür bir ayak oyunu kullanırlarsa kullansınlar, belli bir yol izlerler. Bazen oyun ters yönde oynanır, buna da ters dalavere denir. Saldırganın, kurbanın yardım için saldırganı arayacağı ya da kurbanın bir mesai arkadaşının isteğine saldırganın yanıt vereceği şekilde ortamı düzenlediği karmaşık bir dolaptır.

Bu iş nasıl mı yapılır? Şimdi göreceksiniz.

Tatlı Dille İkna Sanatı

Sıradan biri bir bilgisayar korsanını gözünde canlandırdığında çoğunlukla ilk akla gelen, en iyi arkadaşı bilgisayar olan ve anlık mesajlar dışında konuşma özürlü olan, yalnız, içine kapanık bir gerzeğin sevimsiz görüntüsüdür. Genellikle bilgisayar korsanlığı becerileri de olan toplum mühendisinin öbür cebinde insanî becerileri de vardır. İnsanları kullanıp yönlendirerek kesinlikle aklınıza gelmeyecek yollarla bilgi toplamasını sağlayacak iyi geliştirilmiş yeteneklere sahiptir.

Angela'yı Arayan Kişi

Yer: Federal Sanayi Bankası, Valley Şubesi.

Zaman: Sabah 11:27.

Angela Wisnowski, kendisine büyük bir miras kalmak üzere olduğunu ve tasarruf hesapları, mevduat sertifikaları ve önerebileceği güvenli ama iyi faiz veren başka yatırım araçları olup olmadığı konusunda bilgi almak istediğini söyleyen bir adamdan bir telefon aldı. Angela adama oldukça çok seçenek olduğunu ve bankaya kadar gelip karşılıklı görüşmek isteyip istemeyeceğini sordu. Adam para eline geçer geç-

Terimler

TERS DALAVERE: Saldırıya uğrayan kişinin saldırgandan yardım istediği bir dolandırıcılık şekli.

mez bir yolculuğa çıkacağını ve yapması gereken birçok hazırlık olduğunu söyledi. Böylece kadın bazı olasılıkları anlatmaya ve faiz oranlarıyla ilgili ayrıntılardan, bir mevduat sertifikasını erken satarsan ne olur gibi şeylerden söz etmeye başladı. Bir yandan da adamın yatırım hedeflerinin ne olduğunu anlamaya çalışıyordu.

Kadın tam ilerleme kaydediyor gibiydi ki, adam, "Çok özür dilerim. Diğer hattı açmam gerekiyor. Bu görüşmeye ne zaman devam edebiliriz. Böylece ben de üzerinde biraz düşünebilirim? Saat kaçta öğle tatiline çıkıyorsunuz?" diye sordu. Angela ona 12:30'da çıktığını söyledi ve adam o saatten önce ya da ertesi gün aramaya çalışacağına söz verdi.

Louis'i Arayan Kişi

Büyük bankalar her gün değişen dahili güvenlik şifreleri kullanırlar. Bir şubede çalışan biri başka bir şubeden bir bilgi istediğinde o günün şifresini vererek o bilgiyi istemeye yetkilili olduğunu gösterir. Ek bir güvenlik ve esneklik sağlaması için bazı büyük bankalar günde birkaç şifre birden çıkarırlar. Adına Federal Sanayi Bankası diyeceğim bir Batı Yakası şirketinin her çalışanı her sabah bilgisayarında o gün için belirlenmiş ve A'dan E'ye doğru kodlanmış beş şifrelik bir liste bulur.

Yer: Aynı.
Zaman: Aynı gün, öğleden sonra 12:48.

Louis Halpburn o gün öğleden sonra gelen ve bir hafta boyunca onun gibi bir sürüsüyle uğraştığı telefonun üzerinde pek durmamıştı.

- *Merhaba,* dedi arayan. *Ben Neil Webster. Boston 3182 nolu şubeden arıyorum. Angela Wisnowski'yle görüşebilir miyim?*

- *Yemeğe çıkmıştı. Ben yardımcı olabilir miyim?*

- *Müşterilerimizden birine bazı bilgileri fakslamamız için bize bir not bıraknuş.*

Telefondaki adamın sesi pek iyi gelmiyordu.

- *Bu tarz istekleri yerine getiren arkadaş bugün hasta olduğu için gelmedi"* dedi adam. *Elimde gönderilmesi gereken bir yığın şey var, saat neredeyse dört oldu ve doktorla randevuma yetişmek için yarım saat içinde çıkmış olmam gerek.*

Karşı tarafın acımasını sağlamak için tüm nedenleri sıralayarak yapılan konuşma, hedefi yumuşatmanın bir parçasıdır. Sonra devam etti,

- *Notu kim aldıysa, faks numarası okunmuyor. 213-birşey. Devamı nedir?"*

Louis faks numarasını okudu ve arayan,

- *Teşekkürler. Bunu göndermeden önce, size B şifresinin ne olduğunu sormam gerek."*

- *Ama siz burayı aradınız,* dedi Louis, Boston'dan arayan adamın ne demek istediğini anlayabileceği bir soğuklukla.

Bu iyi diye düşündü arayan. İnsanların en küçük bir dürtmeyle düşüvermemeleri iyi oluyor. Eğer biraz direnmezlerse iş çok kolaylaşıyor ve ben tembelleşmeye başlıyorum.

- Dışarıya birşey göndermeden önce onay almamız konusunda kafayı işütmüş bir şube müdürüm var, hepsi bu. Ama bilgiyi fakslamamızı istemiyorsanız önemli değil. Onaya gerek yok.

- Angela yarım saat kadar sonra burada olur. Ona seni aramasını söyleyebilirim, dedi Louis.

- Şifreyi vererek bunun geçerli bir istek olduğunu gösteremediğiniz için ona bugün gönderemediğimi söylerim. Eğer yarın doktor bana rapor vermezse, onu yeniden ararım.

- Tamam, olur.

- Mesaj, acil, diyordu. Neyse boş ver, onay olmadan elim kolum bağlı. Ona göndermeye çalıştığını ama senin şifreyi veremediğini söylersin değil mi?

Louis sonunda baskıya dayanamadı. Ahizeden sıkıntılı bir iç geçirme duyuldu.

- Peki, dedi. *Biraz bekle, bilgisayarıma kadar gitmem gerekiyor. Hangi şifreyi istiyorsun?*

- B, dedi arayan.

Louis aramayı beklemeye aldı, biraz sonra yeniden açtı.

- 3184.

- Bu doğru şifre değil.

- Bu doğru. B şifresi 3184.

- Ben B demedim, E dedim.

- Kahretsin. Bir dakika bekle.

Louis yeniden şifrelere bakarken biraz daha bekledi.

- E şifresi 9697.

- 9697, tamam. Faksı hemen gönderiyorum. Tamam mı?

- Tamam. Teşekkürler.

Walter'ı Arayan Kişi

- Federal Sanayi Bankası, ben Walter.

- Merhaba, Walter, ben Studio City 38 nolu şubeden Bob Grabowski, dedi arayan. *Bir müşteri hesabına ait imza kartonuna ihtiyacım var, bana onu fakslayabilir misin?*

İmza kartonu yalnızca müşterinin imzasını içermez, sosyal güvenlik numarası, doğum tarihi, annesinin kızlık soyadı ve bazen de ehliyet numarasına gibi diğer tanımlayıcı bilgileri de içerir. Bir toplum mühendisi için çok kullanışlıdır.

- *Elbette. C şifresi nedir?*

- *Şu anda bilgisayarımı başka biri kullanıyor,* dedi arayan. *Ama az önce B'yi ve E'yi kullanmıştım ve onları hatırlıyorum. Onlardan birini sorabilirsin.*

- *Tamam, E şifresi nedir?*

- *E şifresi 9697.*

Birkaç dakika sonra Walter istenen imza kartonunu fakslar.

Donna Plaice'i Arayan Kişi

- *Merhaba, ben Bay Anselmo.*

- *Size bugün nasıl yardımcı olabilirim?*

- *Hesabıma para yattığını öğrenebilmek için aramam gereken 800'lü numara hangisiydi?*

- *Bankanın bir müşterisi misiniz?*

- *Evet, ama numarayı uzun süredir kullanmadım ve şimdi de nereye yazdığımı hatırlamıyorum.*

- *Numara 800-555-8600.*

- *Tamam, teşekkürler.*

Vince Capelli'nin Öyküsü

Spokane'li bir polis memurunun oğlu olan Vince, saatlerce köle gibi çalışıp, asgarî ücret alabilmek için kelleyi koltuğa almayacağını erken yaşlardan beri biliyordu. Yaşamının iki temel amacı Spokane'den ayrılmak ve kendi işini kurmak oldu. Okul yılları boyunca arkadaşlarının onunla alay etmesi onu daha da kızıştırmıştı. Kendi işini kurmaya hevesli olması ama bir işin nasıl yürütüleceğiyle ilgili hiçbir fikri olmaması onlara gülünç geliyordu.

İçten içe Vince arkadaşlarının haklı olduğunu da biliyordu. İyi olduğu tek şey okulun beyzbol takımının tutucusu olarak yaptığı işti. Ama bunda da burs kazanacak ya da profesyonel beyzbol oynayacak kadar iyi değildi. O zaman nasıl bir işe girişecekti?

Vince'in grubundaki arkadaşları bir şeyi tam olarak anlamamışlardı: Aralarında birinin olan bir şey -yeni bir sustalı çakı, şık bir çift sıcak tutan eldiven, çekici bir kız arkadaş- eğer Vince'in hoşuna gitmişse çok geçmeden onun oluyordu. Ne çalıyor ne de birilerini arkadan vuruyordu, bunu yapmasına gerek yoktu. Çocuklar ellerindekileri isteyerek veriyorlardı ve sonra da bunun nasıl olduğunu düşünüyorlardı. Vince'e sormak da bir işe yaramıyordu, çünkü kendi de bilmiyordu. Görünüşe göre her ne isterse insanlar ona bunları veriyordu.

Vince Capelli, bu adı hiç duymamış olsa bile, erken yaşlardan beri bir toplum mühendisiydi.

Okul diplomalarını ellerine aldıktan sonra arkadaşları gülmeyi kestiler. Diğerleri, şehirde dolaşıp "Yanında patates kızartması ister misiniz?" diye sormak zorunda kalmayacakları bir iş bulmaya çalışırlarken Vince'in babası, teşkilattan ayrılıp kendi özel dedektiflik işini kuran eski bir polis arkadaşıyla konuşması için onu San Francisco'ya göndermişti. Adam, Vince'in bu işe çok uygun olan yeteneğini görmüş ve hemen onu işe almıştı.

Bu altı yıl önceydi. İşin, oturup beklemeyi gerektiren can sıkıcı saatlerle dolu sadakatsiz eşlerle ilgili bilgi toplama kısmından nefret ediyordu, ancak zavallı bir müteveffanın dava açılacak kadar zengin olup olmadığını öğrenmeye çalışan avukatların verdiği mal varlıklarını öğrenme işlerini her zaman heyecan verici buluyordu. Bu tarz işler ona aklını kullanması için pek çok fırsat sunuyordu.

Tıpkı Joe Markowitz adında bir adamın banka hesaplarına bakması gerektiği zaman olduğu gibi. Joe'nun eski bir arkadaşını dolandırmış gibi bir durumu vardı ve şu anda arkadaşı, dava açarsa para alabilecek kadar Markowitz'in yüklü olup olmadığını öğrenmek istiyordu.

Vince'in ilk adımı bankanın güvenlik şifrelerinden en az bir, ama tercihen iki tanesini ele geçirmekti. Bu kulağa neredeyse imkânsız bir işmiş gibi geliyor. Nasıl bir numara bir banka çalışanını şifreleri vermesi konusunda ikna edebilirdi ki? Kendi kendinize sorun; eğer siz bu işi yapmak istiyor olsaydınız, bunu nasıl yapacağınızla ilgili bir fikriniz olur muydu?

Vince gibi insanlar için bu iş çok kolaydır.

İşlerinde ve şirketlerinde kullandıkları terimleri biliyorsanız insanlar size güvenirler. Yakın çevrelerinin bir parçasıymış gibi görünürsünüz. Gizli bir tokalaşma gibidir. Vince'den dinleyelim:

Böyle bir iş için o kadar çok şeye ihtiyacım yoktu. Bu iş beyin cerrahisi değil. İşe başlamak için tek gereken şey bir şube numarasıydı. Buffalo Beacon Street şubesini aradığımda telefona çıkan adamın sesi bir gişe görevlisi gibi geliyordu.

"Ben Tim Ackerman" dedim. Herhangi bir ad olurdu, nasıl olsa bir yerlere yazmayacaktı. *"O şubenin numarası nedir?"*

"Telefon numarası mı, şube numarası mı?" diye bilmek istedi ama bu oldukça aptalcaydı, çünkü zaten telefon ediyordum, değil mi?

"Şube numarası."

"3182", dedi adam hiç duraksamadan. Ne, *"Neden bilmek istiyorsunuz?"* diye sordu, ne de başka bir şey. Hassas bilgi olmadığı için, kullandıkları her kâğıt parçasının üstünde yazılıydı.

İkinci adım hedefimin çalıştığı şubeyi aramak, orada çalışanlardan birinin adını ve onun ne zaman öğle yemeğine çıkacağını öğrenmekti. Angela 12:30'da yemeğe çıkıyordu. Her şey oldukça iyi gidiyordu.

Üçüncü adımda Angela öğle tatilindeyken aynı şubeyi tekrar arayacak, Boston'daki şu ve şu numaralı şubeden aradığımı söyleyecek, Angela'nın

bu bilginin fakslanmasını istediğini belirterek günlük şifreyi alacaktım. En zorlu kısım buydu, tekerler dönmeye buradan başlayacaktı. Eğer toplum mühendisliği becerisini sınayacak bir sınav yapıyor olsaydım, kurbanın haklı olarak kuşkulandığı benzer bir durum koyardım ve onu kırıp istediğiniz bilgiyi alana kadar orada kalmak zorunda kalırdınız. Bunu bir senaryodaki satırları tekrarlayarak ya da belli kalıpları ezberleyerek yapamazsınız; kurbanınızı okumanız, ne hissettiğini anlamanız, oltayı suya atıp çekerek bir balığı yakalıyormuş gibi onunla oynamanız gerekir. Ta ki zokayı yutturup, onu kayığa çekene kadar.

Böylece onu ağıma düşürdüm ve günlük şifrelerden birini aldım. Çoğu bankada yalnızca tek bir tane kullanırlar, öyle olsaydı işim bitmiş sayılırdı. Federal Sanayi Bankası'nda beş tane kullanıyorlar ve beşinden birini bilmek işi çok fazla şansa bırakmak olurdu. Beşte iki olursa bu küçük oyunun bir sonraki sahnesini tamamlamak için daha fazla şansım olacaktı. *"B demedim, E dedim,"* kısmına bayılıyorum. İşe yaradığı zaman harika oluyor. Ve çoğu zaman da işe yarıyor.

Üçüncü bir tane almak daha da iyi olurdu. Tek bir aramada üç tane birden almayı başarmışlığım da vardır. B, D ve E'nin okunuşları sizi yanlış anladıklarını iddia edebileceğiniz kadar birbirlerine benzerler. Ama gerçek bir şaşkınla konuşuyor olmanız gerekir. Bu kadın öyle değildi. İki taneyle yetinecektim.

Günlük şifreler imza kartonunu almak için benim kozum olacaklar. Arıyorum ve adam benden bir şifre istiyor. C'yi istiyor ve ben de yalnızca B ve E var. Ama bu dünyanın sonu değil. Böyle anlarda sakin olmalısınız, kendinize güvenmeli ve işinize devam etmelisiniz. Hiç istifimi bozmadan ona, *"Biri benim bilgisayarımı kullanıyor, bana diğerlerinden birini sor"* oyununu oynadım.

"Hepimiz aynı şirketin çalışanlarıyız, hepimiz bu işin içindeyiz; adamı yokuşa sürme". Böyle bir anda kurbanınızın bu şekilde düşündüğünü ümit edersiniz. Adam tam kitabına göre oynadı. Sunduğum seçeneklerden birini sordu, ona doğru yanıtı verdim ve imza kartonunu faksladı.

İş neredeyse bitmişti. Bir görüşme daha yapıp elektronik bir sesin istediğiniz bilgiyi okuduğu ve müşterilerin otomatik hizmet için kullandıkları 800'lü numarayı buldum. İmza kartonunda hedefimin tüm hesap numaraları ve kişisel kimlik numarası vardı, çünkü bu banka Sosyal Güvenlik Numarası'nın son dört ya da beş basamağını kullanıyordu. Elimde kalem 800'lü numarayı çevirdim ve birkaç dakikamı tuşlara basarak geçirerek adamın dört hesabının birden son durumlarını öğrendim. İşi sağlama almak için her birine en son yatırdığı ve çektiği paraları da bir kenara not ettim.

Müşterimin aradığı her şey fazlasıyla tamamdı. Her olasılığa karşı her zaman biraz fazla bilgi vermek hoşuma gider. Müşteri velinimetimizdir. Ne de olsa sürekli gelen işler işletmenin varlığını sürdürmesini sağlayan şeylerdir, öyle değil mi?

Aldatmacanın İncelenmesi

Tüm bu olayın kilit noktası o çok önemli günlük şifreleri almaktı ve bunu yapmak için saldırgan, yani Vince, pek çok farklı teknik kullandı.

Biraz laf ebeliği yaparak işe başlamıştı ki Louis ona şifreyi vermekte isteksiz davrandı. Louis şüphelenmekte haklıydı, şifreler diğer yönde kullanılmak üzere tasarlanmışlardı. İşlerin olağan sürecinde onu arayan, tanımadığı kişinin güvenlik kodunu vermesi gerekirdi. Bu Vince için çok kritik bir andı, tüm çabalarının başarıya ulaşıp ulaşmaması buna bağlıydı.

Louis'in şüphesi karşısında Vince adamı etkileme çabasını artırarak acındırma ("doktora gitme"), baskı ("yapacak yığınla işim var ve saat neredeyse dört oldu") ve etkileme ("ona bana şifreyi vermediğini söyle") yöntemlerine başvurdu. Akıllılık edip Vince aslında hiç tehdit kullanmadı, yalnızca ima etti: Eğer bana güvenlik şifresini vermezsen arkadaşının ihtiyacı olan müşteri bilgilerini gönderemem ve ona aslında gönderebilecek durumda olduğumu fakat senin işbirliği yapmadığını söylerim.

Yine de kabahati Louis'e atmakta acele etmeyelim. Ne de olsa telefondaki kişi, arkadaşı Angela'nın bir faks beklediğini biliyordu; en azından biliyormuş gibi görünüyordu. Arayan, güvenlik şifrelerinden de haberdardı ve onlara atanmış harflerle tanımlandıklarını biliyordu. Arayan, şube müdürünün daha fazla güvenlik için bunun yapılmasını istediğini söylemişti. İstediği doğrulamayı ona vermemek için ortalıkta bir neden görünmüyordu.

Louis yalnız değildi. Banka çalışanları neredeyse her gün güvenlik şifrelerini toplum mühendislerine verirler. İnanılmaz ama gerçek.

Özel bir dedektifin kullandığı yöntemlerin yasal olmaktan çıkıp yasadışı olmaya başladığı ince bir çizgi vardır. Şube numarasını aldığında Vince henüz yasadışı değildi. Louis'i günlük güvenlik şifrelerinden ikisini vermeye kandırdığında da yasadışı birşey yapmamıştı. Bir banka müşterisinin bilgilerini kendisine fakslanmasını istediği anda çizgiyi aştı.

Ama Vince ve patronu için bu düşük riskli bir suçtu. Para ya da mal çaldığınızda birileri onun kaybolduğunu anlarlar. Bilgi çaldığınızda çoğu zaman bunu kimse fark etmez, çünkü bilgi hâlâ ellerindedir.

Mitnick Mesajı:

Sözel güvenlik şifreleri, verilerin korunması için elverişli ve güvenilir bir yöntem sunmada parolalara denktirler. Ancak çalışanların toplum mühendislerinin kullandığı dalavereler konusunda bilgili olmaları ve krallığın anahtarlarını teslim etmemek üzere yetiştirilmeleri gerekir.

Dalavereye Alet Olan Polisler

Hilebaz bir özel dedektif ya da toplum mühendisi için birinin ehliyet numarasını bilmesinin gerektiği durumlar sık sık ortaya çıkar. Örneğin, birinin banka hesaplarıyla ilgili bilgi almak için onun kimliğine bürünmek istiyorsanız.

Birinin cüzdanını yürütmek ya da uygun bir anda omuzunun üzerinden göz ucuyla bakmak dışında ehliyet numarasını öğrenmek olanaksıza yakın olmalıdır. Ancak çok fazla toplum mühendisliği becerilerine sahip olmayan biri için bile bu pek zor bir iş sayılmaz.

Düzenli olarak ehliyet numaraları ve araç plaka numaraları öğrenmesi gereken -kendisine Eric Mantini diyeceğim- bir toplum mühendisi var. Eric, Motorlu Taşıtlar Müdürlüğü'nü aramanın ve bilgi alması gerektiğinde hep aynı oyunu oynamanın, içinde bulunduğu tehlikeyi gereksiz ölçüde artırdığına karar verdi ve bu süreci kolaylaştırmanın bir yolunun bulunup bulunmadığını araştırdı.

Büyük olasılıkla daha önce kimse düşünmemişti ama istediği anda bu bilgiyi almanın bir yolunu buldu. Bu işi Bölge Motorlu Taşıtlar Müdürlüğü'nün yürürlüğe koyduğu bir hizmetten yararlanarak yaptı. Pek çok bölge müdürlüğü, ayrıcalıklı bilgiler olmadıkları sürece, vatandaşlarla ilgili bilgileri sigorta kurumlarına, özel dedektiflere ve eyalet yasaları uyarınca ticaretin ve genel toplumun lehine olmak kaydıyla paylaşmanın uygun olduğu belli başka kuruluşlara açmışlardı.

Motorlu Taşıtlar Müdürlüğü'nün, doğal olarak, hangi tür verilerin verileceğine ilişkin uygun kısıtlamaları vardır. Sigorta sektörü dosyalardan belli tür bilgiler alabilir ama diğerleri alamaz. Özel dedektifler için farklı sınırlamalar geçerlidir ve bu böyle gider.

Emniyet teşkilatı mensupları için de farklı bir kural geçerlidir. Motorlu Taşıtlar Müdürlüğü, kendini uygun şekilde tanıtan yeminli bir polis memuruna kayıtlarındaki tüm bilgileri açacaktır. Eric'in yaşadığı eyalette Motorlu Taşıtlar Müdürlüğü'nün bir emniyet görevlisinden istediği tanımlamalar Talep Kodu ve memurun ehliyet numarasıydı. MTM çalışanı, bilgi vermeden önce her zaman memurun adını ehliyet numarasıyla ve başka bir bilgiyle -genellikle doğum tarihiyle- karşılaştıracaktı.

Toplum mühendisi Eric'in yapmak istediği, kendini bir emniyet teşkilatı mensubunun kimliğine büründürmekten başka birşey değildi. Bunu nasıl başaracaktı? Polislere bir ters dalavere uygulayarak!

Eric'in Dalaveresi

Önce bilinmeyen numaraları aradı ve eyalet başkentindeki Motorlu Taşıtlar Genel Müdürlüğü'nün telefon numarasını istedi. Aldığı numara

503-555-5000'di ve doğal olarak, vatandaşın araması için ayrılmış telefondu. Sonra yakınlardaki bir karakolu arayarak haberleşme bürosunu -diğer emniyet teşkilatı birimleriyle, ulusal suç veri tabanıyla, yerel yetkililerle ve benzeri yerlerle iletişimin kurulduğu birimi- istedi. Haberleşme bürosunda telefona çıkan memura Eyalet Motorlu Taşıtlar Genel Müdürlüğü'nün emniyet teşkilatını araması için ayrılmış numarayı öğrenmek istediğini söyledi.

"Sen kimsin?" diye sordu haberleşmedeki polis.

"Ben Al. 503-555-5753'ü arıyordum" dedi Eric. Bu yarı yarıya varsayım ve yarı yarıya uydurulmuş bir numaraydı. Emniyet teşkilatından gelecek telefonlar için MTM'de kurulan özel büro numarasının halka açık numarayla aynı bölge koduna sahip olması gerekirdi ve sonraki üç basamağın da aynı olacağı neredeyse kesindi. Tüm bilmesi gereken son dört basamaktı.

Karakol haberleşme bürolarına dışardan telefon gelmezdi ve arayan kişi numaranın çoğunu biliyordu. Teşkilattan biri olduğu açıktı.

"Numara 503-555-6127" dedi memur.

Artık Eric'in elinde emniyet teşkilatı mensuplarının kullanımına özel MTM numarası vardı. Ama yalnızca telefon numarası onun işini görmüyordu; o büronun birden fazla telefon hattı olmalıydı ve Eric'in kaç hat olduğunu ve her birinin numarasını öğrenmesi gerekiyordu.

Santral

Planını uygulamaya koymak için, emniyet teşkilatından arayanların aramalarını yönlendiren MTM santralına erişmesi gerekiyordu. Telekomünikasyon Müdürlüğü'nü aradı ve en çok kullanılan ticari telefon santrallerinden biri olan DMS-100'leri üreten Nortel'den aradığını söyledi. *"DMS-100 üzerinde çalışan santral teknisyenlerinden biriyle görüşebilir miyim?"*

Teknisyen telefonu açtığında, Teksas Nortel Teknik Destek Merkezi'nden aradığını ve tüm santralları en son yazılımla güncelleyebilmek için merkezî bir veri tabanı oluşturduklarını anlattı. Her şey uzaktan yapılacaktı ve santral teknisyenlerinin müdahalesine gerek olmayacaktı. Ancak santralın bilgisayar bağlantı numarasına ihtiyaçları vardı, böylece güncellemeleri doğrudan Destek Merkezi'nden yapabileceklerdi.

Oldukça akla yatkın görünüyordu ve teknisyen, Eric'e telefon numarasını verdi. Artık eyaletin telefon santrallarından birine doğrudan bağlanabilecekti.

Tıpkı her şirket bilgisayar ağında olduğu gibi saldırganlara karşı korunmak için bu tarz ticari santraller de parola korumalıdır. Telefon beleşçiliği geçmişi olan her iyi toplum mühendisinin bildiği üzere Nortel santrallerin yazılım güncellemeleri için kullandığı standart bir kullanıcı adı vardı: NTD (Nortel Teknik Destek'in baş harfleri, yani çok gizli

bir şey değil). Peki ya parola? Eric pek çok kez bağlanmaya çalışarak, her seferinde bariz ve sık kullanılan olasılıkları denedi. Kullanıcı adıyla aynı harfleri, NTD, girmek de işe yaramadı. "Yardımcı" kelimesi de olmadı, "yama" da.

Sonra "güncelleme"yi denedi... ve girdi. Başka ne beklenirdi ki! Bariz, kolayca tahmin edilebilen bir parola kullanılması, hiç parola olmamasından yalnızca bir nebze daha iyidir.

Konunuzda bilgili olmak iyidir. Eric'in o santralin nasıl programlandığı ve sorunların nasıl çözüldüğü hakkında büyük olasılıkla o teknisyen kadar bilgisi vardı. Yetkili bir kullanıcı olarak santrale eriştikten sonra hedefi olan telefon hatları üzerinde tam kontrol sağlayabilecekti. Emniyet teşkilatı mensuplarının MTM'yi aramak için kullandıkları numarayı, 555-6127, bilgisayarından arattırdı. Aynı müdürlükte on dokuz tane daha hat olduğunu gördü. Görünüşe göre arayanları çoktu.

Her gelen aramada santral meşgul olmayan birini bulana kadar yirmi hattı taramaya programlanmıştı.

Sıradaki on sekiz numaralı hattı seçti ve bu hattan aramaları başka bir telefona yönlendirecek şifreyi girdi. Yönlendirilen telefon numarası olarak da yeni ve ucuz, hazır kartlı cep telefonu numarasını kullandı. Bunlar, iş bittikten sonra atacak kadar ucuz oldukları için uyuşturucu kaçakçılarının tercih ettiği türden telefonlardı.

On sekizinci hattâ arama yönlendirme çalışır durumdayken, büronun ardarda gelen on yedi telefonla uğraştığı bir sırada bir sonraki telefon MTM bürosunda çalmayacak onun yerine Eric'in cep telefonuna yönlendirilecekti. Arkasına yaslandı ve beklemeye başladı.

MTM'ye gelen arama

O sabah saat sekizden biraz önce telefon çaldı. Bu işin en iyi ve en keyifli bölümüydü. Toplum mühendisi Eric oturmuş, onu gelip tutuklamaya yetkili ya da bir arama emri çıkarıp aleyhine delil toplamak için baskın yapabilecek bir polisle konuşuyordu.

Ve yalnızca tek bir polis aramayacaktı, bir biri ardına bir sürü polis arayacaktı. Bir keresinde Eric bir lokantada arkadaşlarıyla öğle yemeği yerken her beş dakikada bir telefon gelmiş, ödünç aldığı bir kalemle bilgileri bir kağıt peçetenin üstüne yazmıştı. Buna hâlâ durup durup güler.

Ancak polis memurlarıyla konuşmak iyi bir toplum mühendisine hiç sıkıntı vermez. Aslında emniyet teşkilatı birimlerini kandırmanın heyecanı Eric'in oynadığı oyunu büyük olasılıkla daha eğlenceli kılmıştır.

Eric'in anlattığı kadarıyla görüşmeler şöyle geçiyordu:

"MTM, yardımcı olabilir miyim?"

"Ben Dedektif Andrew Cole."

"Merhaba dedektif. Bugün sizin için ne yapabilirim?"

Emniyet teşkilatında fotoğraf istemek için kullanılan terimi kullanarak *"005602789 nolu ehliyet için soundex gerekiyor"* diyebilirdi. Bu, işe yarar bir şeydi; örneğin polisler bir şüpheliyi tutuklamaya giderlerken adamın neye benzediğini görmek için kullanırlardı.

"Elbette, hemen kayıtlara bakayım" diyordu Eric. *"Detektif Cole, bağlı olduğunuz yer neresi?"*

"Jefferson Bölgesi." Sonra Eric asıl soruları sormaya başlıyordu: *"Dedektif, talepkodunuz nedir?"*, *"Ehliyet numaranız?"*, *"Doğum tarihiniz?"*

Arayan, kişisel tanımlama bilgilerini veriyordu. Eric bilgileri doğrulamakla uğraşıyormuş gibi yapıp, sonra da arayana bilgilerinin doğrulandığını söylüyordu. En sonunda arayanın MTM'den istediği şeylerin ayrıntılarını soruyordu. İstenen adı arıyormuş gibi yapıp, arayanın tuşların tıklamasını duymasını sağlıyor sonra da şöyle bir şey diyordu. *"Kahretsin, bilgisayarım yine çöktü. Kusura bakma, dedektif, bilgisayarım bu hafta hep gidip geliyor. Tekrar arayıp başka bir görevlinin size yardımcı olmasını isteyebilir misiniz?"*

Böylece neden isteğinde yardımcı olamadığıyla ilgili memur beyde herhangi bir şüphe uyandırmadan açık uçları bağlıyordu. Bu arada Eric bir kimlik çalmıştı. Bunlar, ihtiyacı olduğu zaman gizli MTM bilgilerini almakta kullanabileceği ayrıntılardı.

Eric birkaç saat telefonlara yanıt verip düzinelerce talep kodu elde ettikten sonra santrale bağlandı ve yönlendirme işlemini iptal etti.

Sonraki aylarda, bilgiyi nasıl aldığını bilmek istemeyen yasal özel dedektiflik firmalarının ona verdiği işleri yapmayı sürdürdü. Gerektiği zaman yeniden santrala bağlanıyor, yönlendirmeyi açıyor ve bir yığın polis memuru bilgisi daha topluyordu.

Aldatmacanın İncelenmesi

Eric'in bu dalavereyi yapmak için bir dizi insan üstünde oynadığı oyunları bir gözden geçirelim. İlk başarılı adımda haberleşme bürosundaki bir memurun, karşısındakini başka bir polis memuru varsayıp, hiçbir kimlik tespiti yapmadan tamamıyla yabancı birine gizli MTM telefon numarasını vermesini sağladı.

Sonra Eyalet Telekomünikasyon Müdürlüğü'ndeki kişi de aynı şeyi yaptı. Eric'in santral üreticisi firmada çalıştığı iddiasını olduğu gibi kabul etti ve MTM'ye hizmet veren telefon santralının dışarıdan bağlanma numarasını bir yabancıya verdi.

Eric'in santrala erişebilmesinin nedeni, büyük ölçüde, santral üreticisinin tüm santrallarında aynı kullanıcı adını kullanmasından kaynaklanan zayıf güvenlik uygulamasıydı. Bu dikkatsizlik, toplum mühendisinin parolayı tahmin etmesini kolaylaştırdı, çünkü santral teknisyenlerinin herkes gibi hatırlaması kolay olacak parolalar seçeceğini biliyordu.

Santrala eriştikten sonra MTM'nin emniyet teşkilatı telefon hatlarından birini kendi cep telefonuna yönlendirdi.

Hepsinin üstüne en cüretkâr kısım olarak, birbiri ardına polis memurlarını kandırıp yalnızca talep kodlarını almakla kalmadı, aynı zamanda onların kendi kişisel bilgilerini vermelerini de sağladı. Böylece Eric onların kimliğine bürünebilecekti.

Bu dolabı çevirmek için her ne kadar teknik bilgi gerekse de, bir sahtekârla konuştuklarını bilmeyen bir grup insanın yardımı olmasaydı bu dolap işe yaramazdı.

Bu öykü, insanların, "Neden ben?" diye sormadıkları bir durumun bir başka örneği. Haberleşme bürosu memuru neden tanımadığı bir polis memuruna -ya da bu durumda olduğu gibi kendini polis memuru olarak tanıtan birine- bu bilgiyi versin ki? Bilgiyi kendi mesai arkadaşlarından ya da amirinden almasını da söyleyebilirdi. Verebileceğim tek yanıt, insanların bu soruyu kendilerine sık sık sormamaları şeklinde olur. Sormak akıllarına gelmiyor mu? Meydan okuyan ya da yardım etmeye isteksiz biri gibi gözükmek mi istemiyorlar? Belki de. Diğer açıklamalar tahminden öteye gitmez. Ama toplum mühendisleri nedenlerle ilgilenmezler; yalnızca bu küçük gerçeğin, aksi durumda alınması zor olacak bilgileri almalarını kolaylaştırmasıyla ilgilenirler.

Aldatmacanın Engellenmesi

Doğru kullanıldığı takdirde bir şifre çok önemli bir güvenlik önlemidir. Yanlış kullanılan bir güvenlik şifresi, hiç olmaması kadar kötü olabilir; çünkü aslında var olmayan sahte bir güven hissi uyandırır. Eğer çalışanlarınız onları gizli tutamıyorlarsa şifrelerin ne anlamı var?

Sözel güvenlik şifreleri kullanması gereken herhangi bir şirketin, çalışanlarına bu şifreleri ne zaman ve nasıl kullanacaklarını açıkça anlatması gerekmektedir. İyi bir eğitimle, bu bölümün ilk öyküsünde geçen karakter, yabancı birine güvenlik şifresi vermesi istendiğinde, kolaylıkla aşılabilen içgüdülerini dinlemek zorunda kalmazdı. Bu koşullar altında bu bilginin ona sorulmaması gerektiğini hissetti ama açık bir güvenlik politikasının olmaması -ve güçlü bir sağduyu- yelkenleri suya indirmesine neden oldu.

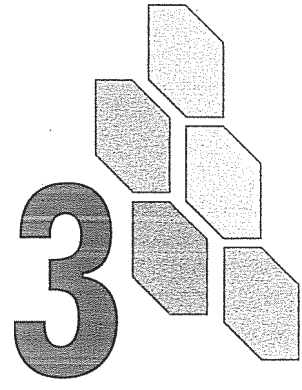
Mitnick Mesajı:

Şirketinizde bir telefon santralı olsaydı, sorumlu kişi satıcıdan gelen ve bağlantı numarasını isteyen bir telefon karşısında ne yapardı? Ve bu arada, bu kişi santralın standart parolasını hiç değiştirmiş miydi? O parola herhangi bir sözlükte bulunabilecek, kolay tahmin edilebilir bir parola mıydı?

Güvenlik süreçlerinde, bir çalışanın doğru olmayan bir güvenlik şifresi talebinde bulunduğu durumları da içeren adımlar olmalıdır. Tüm çalışanlar, günlük şifre ya da parola gibi tanımlama bilgileriyle ilgili gelen şüpheli talepleri hemen bildirecek şekilde eğitilmelidirler. Ayrıca istekte bulunan kişinin kimliğinin onaylanmadığı durumları da haber vermelidirler.

En azından, çalışan, arayanın adını, telefon numarasını, ofis ya da birimini not etmeli, sonra telefonu kapatmalıdır. Geri aramadan önce şirkette o isimde çalışan birinin olup olmadığını ve arayacağı telefonun çevrimiçi ya da basılı rehberdeki numarayla uyuşup uyuşmadığını kontrol etmelidir. Çoğu zaman bu basit yöntem bile arayanın söylediği kişi olup olmadığını anlamak için yeterlidir.

Şirketin çevrimiçi bir rehber yerine basılı bir telefon rehberi varsa kimlik tespiti işlemi biraz güçleşir. İşe yeni başlayanlar olur; işten ayrılanlar; insanların birimleri, konumları ve telefon numaraları değişebilir. Basılı rehberler basıldıkları gün, hattâ daha dağıtılmadan önce güncelliklerini yitirirler. Çevrimiçi rehberler bile her zaman güvenilir değillerdir, çünkü toplum mühendisleri onlarla nasıl oynayacaklarını bilirler. Eğer bir çalışan, bağımsız bir kaynaktan telefon numarasını doğrulayamıyorsa, ona, ilgili kişinin yöneticisini aramak gibi farklı bir yol kullanması konusunda talimatlar da verilmelidir.



Davetsiz Misafirlere Dikkat!

10 İÇERİYE GİRMEK

Dışarıdan birinin bir şirket çalışanının kimliğine bürünmesi ve güvenlik konusunda en duyarlı olanları bile inandıracak kadar başarılı bir taklit yapması neden bu kadar kolaydır? Peki, güvenlik süreçlerini çok iyi bilen, tanımadıkları insanlara şüpheyle bakan ve şirketlerinin çıkarlarını korumak konusunda titiz davranan kişileri kandırmak neden bu kadar kolaydır?

Bu bölümde anlatılan öyküleri okurken bu soruları aklınızda tutun.

Mahcup Olmuş Güvenlik Görevlisi

Gün/Saat: 17 Ekim, Salı, sabah 02:16.
Yer: Skywatcher Havacılık Şirketi'nin Tucson-Arizona dışındaki fabrikası.

Güvenlik Görevlisinin Öyküsü

Deri ayakkabılarının topuklarının, içinde neredeyse hiç kimsenin bulunmadığı fabrikanın zemininde tıklayışını duymak Leroy Greene'e gece saatlerini güvenlik odasında video monitörlerini seyrederek geçirmekten daha iyi gelmişti. Orada ekranlara bakmaktan başka bir şey yapmasına, hattâ bir dergi ya da ciltli İncil'ini okumasına dahi izin verilmiyordu. Oturup hiçbir şeyin hareket etmediği sabit görüntülere bakması gerekiyordu.

Ama koridorlarda gezinirken en azından bacaklarını açıyor ve işin içine kollarını ve omuzlarını da kattığı zaman biraz egzersiz yapmış oluyordu. Lise Amerikan futbolu takımında şehir şampiyonasında sağ kanat oynamış biri için bu pek de bir egzersiz sayılmazdı. Yine de iş iştir, diye düşündü.

Güneybatı köşesini döndü ve bir kilometre uzunluğundaki üretim alanına bakan köprüden yürümeye başladı. Aşağıya baktı ve iki kişinin, yapımı tamamlanmamış helikopterlerin üretim hattının yanından geçtiklerini gördü. Gecenin bu saati için tuhaf bir görüntüydü. *"Kontrol etsem iyi olacak"* diye düşündü.

Leroy, onu üretim alanında ikilinin arkasına çıkaracak merdivenlere doğru yöneldi ve o tam yanlarına gelene kadar adamlar onun geldiğini hissetmediler. *"Günaydın. Güvenlik kartlarınızı görebilir miyim lütfen"* dedi. Leroy böyle anlarda hep sesini yumuşak tutmaya çalışırdı; sadece cüssesinin bile ürkütücü gözükebileceğini biliyordu.

"Merhaba Leroy", dedi bir tanesi, yaka kartından adını okuyarak. *"Ben Tom Stilton, Phoenix'deki Genel Müdürlük pazarlama bölümünden. Toplantı için şehre geldim ve arkadaşıma dünyanın en iyi helikopterlerinin yapıldığı yeri göstermek istedim."*

"Evet. Kartınız lütfen" dedi Leroy. Ne kadar genç oldukları gözünden kaçmamıştı. Pazarlamada olduğunu söyleyen, liseyi yeni bitirmiş gibi duruyordu, diğerinin saçları omuzlarına kadar iniyor ve on beş yaşlarında görünüyordu.

Kısa saçlı olan, kartını çıkarmak için elini cebine attı sonra tüm ceplerini yoklamaya başladı. Leroy birdenbire bu işle ilgili kötü bir hisse kapıldı. *"Kahretsin"* dedi adam. *"Arabada bırakmış olmalıyım. Gidip alabilirim; park yerine gidip gelmem on dakika sürmez."*

Leroy bu arada not defterini çıkarmıştı. *"Adınız ne demiştiniz?"* diye sordu ve aldığı cevabı dikkatle not etti. Sonra da Güvenlik Ofisi'ne kadar onunla gelmelerini rica etti. Tom, asansörde altı aydır şirkette çalıştığını ve bu yüzden başının belaya girmesini istemediğini söyledi.

Güvenlik odasında Leroy ikiliyi sorgularken gece devriyesinden iki kişi daha onlara katıldı. Stilton kendi telefon numarasını verdi ve müdürünün Judy Underwood olduğunu söyleyerek onun telefon numarasını da verdi. Bilgiler bilgisayardaki verilerle uyuyordu. Leroy diğer iki güvenlik görevlisini bir kenara çekti ve aralarında ne yapmaları gerektiğini konuştular. Kimse bu işte yanlış birşey yapmak istemiyordu. Üçü de, kadını gecenin bir yarısında yatağından kaldırmak anlamına gelse de müdürü aramanın en iyisi olduğunu düşünüyorlardı.

Leroy Bayan Underwood'u kendisi aradı, kim olduğunu anlattı ve kendisiyle birlikte çalışan Tom Stilton adlı birinin olup olmadığını sordu. Kadının sesi yarı uykulu geliyordu. *"Evet"* dedi.

"Sabah 2:30'da onu üzerinde kimlik kartı olmadan üretim hatlarının bulunduğu alanda bulduk."

"Onunla konuşayım" dedi Bayan Underwood.

Stilton telefona çıktı ve *"Judy, gecenin ortasında bu adamlar seni uyandırdığı için çok üzgünüm. Umarım bu benim aleyhime bir durum olmaz."* dedi.

Adam dinledi ve sonra devam etti. *"Yeni basın açıklamasıyla ilgili toplantı için zaten sabah erkenden burada olmam gerekiyordu. Her neyse, Thompson anlaşmasıyla ilgili e-postayı aldın mı? Bu işi kaybetmemek için Pazartesi sabahı Jim'le görüşmemiz gerekiyor. Ve salı günkü öğle yemeği planımız hâlâ geçerli, değil mi?"*

Biraz daha dinledi, hoşçakal dedi ve telefonu kapattı.

Bu Leroy'u şaşırttı; kadının her şeyin yolunda olduğunu kendisine de söylemesi için telefonu geri alacağını düşünüyordu. Müdürü tekrar arayıp ona bunu sorup sormaması gerektiğini düşündü ama sonra vazgeç-

ti. Gecenin ortasında onu zaten bir kere rahatsız etmişti, ikinci bir kere arayacak olursa sinirlenebilir ve kendisini müdürüne şikayet edebilirdi. *"Ortalığı karıştırmaya ne gerek var?"* diye düşündü.

Stilton, *"Üretim hattının kalanını arkadaşıma göstermemde bir sakınca var mı?"* diye sordu Leroy'a. *"Bizimle gelip yanımızda durmak ister misiniz?"*

"Gidebilirsiniz" dedi Leroy. *"Gezin ama bir dahaki sefere kartınızı unutmayın. Ve mesai saatleri dışında fabrikada kalacaksanız güvenliği haberdar edin. Kural böyle."*

"Bunu unutmam Leroy", dedi Stilton ve gittiler.

Daha on dakika geçmemişti ki Güvenlik Ofisi'ndeki telefon çaldı. Arayan Bayan Underwood'du. *"O adam kimdi?"*, diye sordu. Sürekli soru sormaya çalıştığını ama adamın konuşmasını kesmeyip öğlen yemeğe çıkmaktan falan söz ettiğini anlattı ve kadın onun kim olduğunu bilmiyordu.

Güvenlik görevlileri danışmayı ve park yeri girişinde görevli bekçiyi aradılar. Her ikisi de birkaç dakika önce iki genç adamın çıktığını söylediler.

Sonradan öyküyü anlatırken Leroy her zaman şöyle bitiriyordu; *"Tanrı biliyor patron beni baştan aşağı fırçaladı. Hâlâ bir işim olduğu için çok şanslıyım."*

Joe Harper'ın Öyküsü

On yedi yaşındaki Joe Harper yalnızca neler bulabileceğini merak ettiği için bir yıldan uzun süredir, bazen gece bazen gündüz binalara giriyordu. Her ikisi de gece çalışan, müzisyen bir babanın ve kokteyl garsonu bir annenin oğlu olarak Joe'nun kendi başına geçirecek çok zamanı vardı. Aynı olaya ait kendi öyküsü her şeyin nasıl geliştiğine eğitici bir ışık tutmaktadır:

> Helikopter pilotu olmak isteyen Kenny adında bir arkadaşım var. Helikopterleri yaptıkları üretim alanını görmek için onu Skywatcher fabrikasına sokup sokamayacağımı sordu. Daha önce başka yerlere girdiğimi biliyordu. Girmemem gereken yerlere girmeye çalışmak benim için tam bir heyecan fırtınasıdır.
>
> Ancak bir fabrikaya ya da ofis binasına elini kolunu sallayarak giremezsin. Üzerinde düşünmeli, planlar ve hedefle ilgili tam bir keşif yapmalısın. Adlar, unvanlar, raporlama yapısı ve telefon numaraları için şirketin internet sayfasına bakar, gazete küpürlerini ve dergi yazılarını okursun. Benim güvenlik anlayışımı titiz bir araştırma oluşturur; bu yüzden bana meydan okuyan herkesle, bir çalışan kadar bilgili bir şekilde konuşabilirim.
>
> Bu durumda nereden başlayacaktım? Önce internetten şirketin nerelerde bürolarının olduğuna baktım ve şirket Genel Müdürlüğü'nün Pho-

enix'de olduğunu öğrendim. Mükemmel. Arayıp pazarlama bölümünü istedim; her şirketin bir pazarlama bölümü vardır. Telefonu bir hanım açtı ve ona Blue Pencil Graphics'den aradığımı söyleyerek, hizmetlerimizden yararlanmak isteyip istemeyeceklerini öğrenmek için kiminle konuşmam gerektiğini sordum. İlgilinin Tom Stilton olduğunu söyledi. Telefon numarasını istedim ama kadın bana bu bilgiyi dışarı vermediklerini ancak beni ona bağlayabileceğini söyledi. Stilton'ın telefonunu telesekreter açtı ve sesli mesaj şöyle dedi, *"Ben Grafik Bölümü'nden Tom Stilton, dahili 3147, lütfen mesaj bırakınız."* Dışarı dahili numara vermiyorlardı ama bu adam bıraktığı sesli mesajda kendisinkini veriyordu. Bu iyiydi. Artık elimde bir ad ve bir dahili numara vardı.

Aynı ofisi bir kez daha aradım. *"Merhaba, Tom Stilton'u arıyordum ama yerinde yok. Müdürüne birkaç küçük soru sormak istiyordum."* Müdürü de dışardaydı, ama işim bittiğinde müdürünün de adını öğrenmiştim. Ve o da nazik bir şekilde sesli mesajında dahili numarasını bırakmıştı.

Herhalde danışma görevlisinden zorlanmadan geçebilirdim ama fabrikanın oradan arabayla geçmiştim ve park yerinin çevresinde tel çit olduğunu hatırlıyordum. Çit demek, içeri girmeye çalıştığınızda sizi kontrol etmek isteyen bir bekçi demektir. Geceleri plakaları not ediyor olabilirlerdi; bu yüzden bit pazarından eski bir plaka almak zorunda kaldım.

Ama önce bekçi kulübesinin telefon numarasını bulmam gerekiyordu. Yeniden aradığımda aynı santral memuru çıkarsa beni tanımaması için biraz bekledim. Sonra aradım ve dedim ki, *"Ridge Caddesi bekçi kulübesindeki telefonun sürekli gidip geldiği yolunda bir şikâyet almıştık; sorun devam ediyor mu?"* Santral memuru kadın bilmediğini söyledi ama beni oraya bağlayacaktı.

Telefonu bir adam açtı. *"Ridge Caddesi kapısı, ben Ryan."* *"Merhaba Ryan, adım John."* dedim. *"Orada telefonlarla ilgili bir sorun yaşıyor musunuz?"* Adam yalnızca düşük ücretli bir güvenlik görevlisiydi ama sanırım biraz eğitim almıştı; çünkü hemen, *"Adınız John muydu? Soyadınız neydi?"* diye sordu. Sanki onu duymamış gibi konuşmayı sürdürdüm. *"Daha önce biri arayıp bir sorun olduğunu söylemişti".*

Telefonu ağzından uzakta tutup bağırdığını duyabiliyordum. *"Hey, Bruce, Roger. Bu telefonda bir sorun olmuş muydu?"* Tekrar ahizeyi kulağına götürdü ve *"Hayır, bildiğimiz kadarıyla hiç sorun çıkmamış."* dedi.

"Orada kaç hat var?"

Adımla ilgilenmeyi tamamen bırakmıştı. *"İki"* dedi.

"Şu anda hangisini kullanıyorsun?"

"3140."

Yakaladım! *"Her ikisi de çalışıyor mu?"*

"Öyle görünüyor."

"Tamam" dedim. *"Tom, eğer herhangi bir sorunla karşılaşırsanız, teknik servisi aramanız yeterli. Seve seve yardımcı oluruz."*

Arkadaşım ve ben hemen ertesi gece fabrikayı ziyaret etmeye karar verdik. Akşamüstüne doğru pazarlamadaki adamın adını kullanarak nöbetçi kulübesini aradım. "Merhaba, ben Grafik bölümünden Tom Stilton. Zorlu bir teslim tarihi yaklaşıyor ve bize yardım etmek için şehre gelecek birkaç arkadaş var. Büyük olasılıkla sabah birden ikiden önce orada olmazlar. O saatte vardiyanız devam ediyor mu?"

Hayır dediği için mutluydu; gece yarısı çıkıyordu.

"Bir sonraki adam için bir not bırak" dedim. *"İki kişi gelip de Tom Stilton'u görmek istediklerini söylerlerse, onları içeri alsın, olur mu?"*

Evet, dedi adam sorun olmazdı. Adımı. bölümümü ve dahili numaramı aldı ve ilgileneceğini söyledi.

İkiyi biraz geçe arabayla kapıya gittik, Tom Stilton'ın adını verdim ve uykulu bir bekçi içeri girmemiz gereken kapıyı işaret etti ve nereye park etmemiz gerektiğini gösterdi.

Binaya girdiğimizde, danışmada, her zamanki mesai saatleri dışı imzalarının atıldığı bir güvenlik noktası daha vardı. Görevliye sabaha bitirmem gereken bir rapor olduğunu ve bu arkadaşımın fabrikayı görmek istediğini söyledim. *"Helikopterlere bayılır"* dedim *"Sanırım helikopter kullanmayı öğrenmek istiyor."* Benden kartımı istedi. Elimi cebime attım sonra üstümü yokladım ve arabada bırakmış olabileceğimi söyledim. *"Gidip alayım"* dedim. *"On dakika sürer."* Adam ise, *"Boş ver, sorun yok, imzalaman yeterli."* dedi.

Üretim hattı boyunca yürümek çok iyiydi. Ta ki o çam yarması Leroy bizi durdurana kadar.

Güvenlik ofisinde, şirket çalışanı olmayan birinin çok sinirli ve korkmuş davranacağını anladım. İşler iyice karıştığında gerçekten kızmış gibi davrandım. Sanki gerçekten söylediğim kişiymişim de bana inanmamalarına bozulmuşum gibi.

Müdürüm olduğunu söylediğim kadını arayıp aramayacaklarına karar vermeye ve ev numarasını bilgisayardan bulmaya çalışırlarken bir an için, *"Tabana kuvvet kaçmanın tam zamanı"* diye düşündüm. Ama işin içinde park yeri kapısı vardı, binadan çıkmayı başarsak bile, kapıyı kapatırlardı ve biz hepten içerde kalırdık.

Leroy, Stilton'un müdürü olan kadını arayıp sonrasında telefonu bana verdiğinde kadın bana bağırmaya başladı. *"Kimsiniz, kiminle konuşuyorum?"* dedi ama ben de sanki tatlı bir sohbet ediyormuşcasına konuşmaya devam ettim, sonra da telefonu kapattım.

Gecenin ortasında şirket numarasını verebilecek birini bulmak ne kadar zaman alır? Kadın güvenlik ofisini arayıp adamları uyarmadan önce buradan çıkmak için on beş dakikadan az zamanımız olduğuna karar verdim.

Çok acelemiz varmış gibi görünmeden oradan çıkabildiğimiz kadar hızlı çıktık. Kapıdaki bekçi bize el sallamakla yetindiğinde kesinlikle çok ferahlamıştık.

Aldatmacanın İncelenmesi

Bu hikâyenin dayandığı gerçek olayda saldırganların gerçekten ergenlik çağında gençler olduklarını vurgulamakta yarar var. İçeri girme girişimi bu işten sıyrılıp sıyrılmayacaklarını görmek için yaptıkları bir eğlenceydi. Ama bir çift genç için bu kadar kolay olduysa yetişkin hırsızlar, sanayi casusları ya da teröristler için çok daha kolay olurdu.

Üç deneyimli güvenlik görevlisi bir çift davetsiz misafirin ellerini kollarını sallayarak gitmelerine nasıl izin verdiler? Üstelik bunlar herhangi iki kişi değil, makul birini kuşkuya düşürecek kadar genç bir ikiliyken.

Leroy önceleri doğru bir hareket yapıp şüphelenmişti. Onları Güvenlik Ofisi'ne götürmekte ve adının Tom Stilton olduğunu söyleyen adamı sorgulayarak, verdiği adları ve telefon numaralarını kontrol etmekte haklıydı. Yöneticisine telefon etmek konusundaki kararı da son derece yerindeydi.

Ama sonunda genç adamın kendine güvenine ve öfkesine aldandı. Bir hırsız ya da içeri zorla girmeye çalışan birinden beklenecek türden bir davranış değildi; yalnızca bir çalışan böyle davranabilirdi... Ya da Leroy öyle olacağını varsaymıştı. Leroy hislerine değil, sağlam kimlik tespitine inanacak şekilde eğitilmeliydi.

Genç adam telefonu, kendisine vermeden kapattığında neden daha fazla kuşkulanmamıştı? Böylece Leroy, kimliğin doğrulunu doğrudan Judy Underwood'dan öğrenebilir ve çocuğun gece geç saatte fabrikada bulunmasının bir nedeni olduğuna dair ondan güvence alabilirdi.

Mitnick Mesajı:

Etkileyici insanların çoğu zaman çekici kişilikleri vardır. Genellikle hızlı harekete geçerler ve oldukça konuşkandırlar. Toplum mühendisleri de işbirliği yaptıracak şekilde insanların düşünce süreçlerini bozmakta ustadırlar. Herhangi birinin bu tarz bir etkilemeye açık olmadığını düşünmek toplum mühendisinin becerilerini ve avlanma güdüsünü hafife almak olur.

Öte yandan iyi bir toplum mühendisi hiç bir zaman hasmını hafife almaz.

Leroy öyle cüretkâr bir dalavereye gelmişti ki durumu şak diye görmesi gerekirdi. Ama bir de onun bakış açısından bakalım: Bir lise mezunu, iş endişesi, gecenin ortasında bir şirket yöneticisini ikinci kez rahatsız etmenin kendi başını derde sokup sokmayacağı düşüncesinin getirdiği kararsızlık. Eğer siz onun yerinde olsaydınız, ikinci aramayı yapar mıydınız?"

Ancak doğal olarak ikinci arama tek olası hareket değildi. Güvenlik görevlisi başka ne yapabilirdi?

Müdüre telefon etmeden önce ikiliden resimli kimlik belgeleri göstermelerini isteyebilirdi. Fabrikaya arabayla gelmişlerdi, yani en azından birinin sürücü ehliyeti vardı. İşin başında sahte isim verdikleri hemen ortaya çıkardı (profesyonel biri elinde sahte bir kimlikle gelebilirdi ama bu gençler öyle bir önlem almamışlardı). Her koşulda Leroy kimlik belgelerini inceleyip bilgiyi not etmeliydi. İkisi de üzerlerinde kimlik olmadığını söyleyecek olsalardı, bu durumda onları arabaya kadar götürüp "Tom Stilton"un orada bıraktığını söylediği şirket kimlik kartını alacaklardı.

Telefon görüşmesinin ardından, güvenlik ekibinden biri, binadan ayrılana kadar ikisiyle birlikte kalmalıydı. Sonra arabalarına kadar onlarla birlikte gitmeli ve plakalarını not etmeliydi. Eğer yeterince dikkatli biriyse (saldırganın bit pazarından aldığı) plakanın geçerli bir kayıt puluna sahip olmadığını görürdü. Bu da durumu daha derinlemesine incelemek üzere ikisini alıkoymak için yeterli bir nedendi.

Çöp Dalışı

Çöp dalışı terimi, işe yarar bilgiler bulmak için hedefin çöpünü karıştırma işi için kullanılır. Bu yöntemi kullanarak bir hedefle ilgili elde edebileceğiniz bilgi miktarı şaşırtıcıdır.

Çoğu insan neleri attığına pek dikkat etmez: telefon faturaları, kredi kartı ekstreleri, reçeteli ilaç kutuları, banka faturaları, işle ilgili belgeler ve daha neler neler.

İş yerlerinde çalışanlar, birilerinin, işlerine yarayacak bilgileri bulmak için çöpleri karıştırdıkları konusunda uyarılmalıdırlar.

Lise yıllarımda yerel telefon şirketi binalarının arkasındaki çöpleri karıştırmaya giderdim. Genellikle yalnız olurdum ama arada bir telefon şirketlerine benzer bir ilgi duyan başka arkadaşlarla da gittiğim olurdu. Çöp dalışında bir kere ustalaştınız mı, birkaç numara kapıyordunuz; örneğin tuvaletlerden gelen çöp torbalarından uzak durmak için özen göstermeyi ve eldiven giymenin önemini kavramak gibi.

Çöp dalışı eğlenceli değildir, ama getirisi inanılmazdır -şirketin dahili telefon rehberleri, bilgisayar kullanım kılavuzları, çalışan listeleri, santral

Terimler

ÇÖP DALIŞI: Ya kendi başına değerli olan ya da dahili telefon numaraları ve unvanlar gibi toplum mühendisliği sırasında kullanılabilecek araçlar olan atılmış bilgileri bir şirketin çöpünden (genellikle dışarıda ve korumasız olan bir çöplükten) toplama işi.

cihazlarının nasıl programlandığını gösteren atılmış çıktılar ve daha fazlası- hepsi orada durmuş alınmayı beklerler.

Yeni rehberlerin çıktığı akşamlarda çöp ziyaretleri yapardım, çünkü çöp bidonlarında düşünmeden atılmış yığınla eski rehber olurdu. Başka tuhaf zamanlarda da bazı ilginç bilgi cevherleri içerebilecek not kâğıtları, mektuplar, raporlar gibi şeyler bulmak için giderdim.

Gittiğimde önce muavvakutular bulur, bunları çekip çıkarır, bir kenara koyardım. Biri bana ne yaptığımı soracak olursa, ki bu arada sırada olurdu, bir arkadaşımın taşındığını ve ona yardımcı olmak için kutu topladığımı söylerdim. Bekçiler, götürmek için kutulara koyduğum belgeleri hiçbir zaman fark etmezdi. Bazı durumlarda bana çekip gitmemi söylerlerdi, ben de başka bir telefon şirketinin merkez binasına giderdim.

Bugün nasıl bilmiyorum ama o zamanlar hangi torbalarda ilginç bir şeylerin olabileceğini anlamak kolaydı. Yerden süpürülen tozlar ve kantin çöpleri doğrudan büyük torbalara koyulurken, ofis çöp kutularında temizlikçilerin bir bir çıkarıp ağızlarını bağladıkları beyaz, tek kullanımlık çöp torbaları kullanılırdı.

Bir keresinde, arkadaşlarla birlikte karıştırırken elle yırtılmış kağıtlar bulduk. Sadece yırtılmakla kalmamış, birileri üşenmeyip kağıtları küçük parçalara da ayırmıştı. Hepsi birden, kullanışlı bir şekilde tek bir yirmi litrelik çöp torbasına doldurulmuştu. Torbayı civardaki çörek dükkânlarından birine götürdük, parçaları bir masaya yaydık ve hepsini tek tek birleştirmeye başladık.

Hepimiz yapboz yapan kişilerdik, o yüzden bu bize dev bir yapbozun heyecan verici meydan okumasını yaşatıyordu... Ama sonucuna bakılırsa, çocuksu bir heyecandan daha fazlasını içeriyordu. Tamamlandığında, şirketin kritik bilgisayar sistemlerinden birine ait tüm kullanıcı adları ve parolalarının bulunduğu bir liste ortaya çıkmıştı.

Çöp dalışı maceralarımız gösterdiğimiz çabaya ve aldığımız riske değer miydi? Kesinlikle değerdi. Düşündüğünüzden daha da fazlasına değerdi, çünkü bu işin tehlikesi sıfırdı. O zamanlar böyleydi, bugün de böyle. Arazilerine izinsiz girmediğiniz sürece başkalarının çöpünü karıştırmak yüzde yüz yasaldır.

Doğal olarak kafalarını çöpe sokanlar bir tek telefon beleşçileri ve bilgisayar korsanları değildir. Ülkedeki tüm polis kuvvetleri, düzenli aralıklarla çöplerden bilgi toplarlar ve mafya babalarından tutun da basit

hırsızlara kadar bir yığın insan çöplerden toplanan kanıtlara dayandırılarak hüküm giymiştir. Bizimki de dahil, istihbarat örgütleri bu yola yıllardır başvurmaktadırlar.

James Bond için aşağılık bir yöntem olabilir. Sinemaseverler onu dizlerinin üstünde çöp karıştırırken değil de kurnazca düşmanını alt edip bir fıstığı yatağa atarken görmeyi tercih edeceklerdir. Değerli bir şey muz kabuklarının ve kahve artıklarının arasından çıkarılabildiğinde gerçek casuslar o kadar müşkülpesent değildirler. Özellikle çöpten bilgi toplamak tehlikeye atılmalarını önleyecekse.

Çöp Karşılığı Para

Şirketler de çöp dalışı oyununu oynarlar. Gazetelerin Haziran 2000'de bayram ettikleri bir gün vardı, Oracle şirketinin (Oracle Genel Müdürü Larry Ellison herhalde ülkenin en lafını esirgemeyen Microsoft karşıtıydı) bir araştırma şirketi tuttuğunu ve araştırma şirketinin suçüstü yakalandığını yazıyorlardı. Görünüşe göre, araştırmacılar, Microsoft'un desteklediği ACT adlı bir halkla ilişkiler şirketinin çöpünü istiyorlardı ama yakalanma tehlikesini göze alamadılar. Basında çıkanlara göre araştırma şirketi bir kadın göndermiş ve kadın ACT çöpü karşılığında kapıcılara 60 dolar teklif etmişti. Kapıcılar teklifi geri çevirmişlerdi. Ertesi gece kadın yine gelmiş ve teklifini 500 dolara çıkarmış, başlarındaki adama da 200 dolar teklif etmişti.

Kapıcılar kadına "hayır" demişler, sonra da polise haber vermişlerdi.

Önde gelen internet gazetecilerinden Declan McCullah, edebiyattan esinlenerek, konuyla ilgili Wired News yazısının başlığını şöyle atmıştı, "MS'yi Gözetleyen Oracle Olmasın?" Time dergisi doğrudan Oracle Genel Müdürü Ellison'u mimleyip, yazısını başlığını basitçe, "Dikizci Larry," şeklinde belirlemişti.

Aldatmacanın İncelenmesi

Benim yaşadıklarıma ve Oracle'ın yaptığına bakarak neden birilerinin başkalarının çöpünü çalmak isteyeceğini merak edebilirsiniz.

Yanıt, sanırım, tehlike boyutunun sıfır ama kazancın hatırı sayılır olması olurdu. Tamam, belki kapıcılara rüşvet vermek sonuçların istendiği gibi olma olasılığını artırır ama biraz kirlenmeyi göze alan biri için rüşvet gerekli değildir.

Bir toplum mühendisi için çöp dalışlarının kendi faydaları da vardır. Hedef şirkete yapacağı saldırıyı yönlendirebilecek kadar isim, bölümler, unvanlar, telefon numaraları ve proje görevlendirmeleri gibi bilgileri bulabileceği, aralarında not defterleri, ajandalar, mektuplar ve benzeri şeyler olan eşyalar toplayabilir. Çöplerden, şirket kuruluş şemaları, şirket

Mitnick Mesajı:

Sizin çöpünüz düşmanımızın hazinesi olabilir. Özel yaşamımızda attığımız eşyaları çok üzerinde durmayız; o zamanı neden iş yerindeki insanların farklı bir yaklaşımı olması gerektiğine inanıyoruz? Her şey işgücünü tehlikeler (değerli bilgiler arayan alıklaksızlar) ve verilen açıklara (öğütücüden geçirilmemiş ya da doğru dürüst silinmemiş hassas bilgiler) konusunda eğitmekte bitiyor.

yapısıyla ilgili notlar, yolculuk tarihleri ve bunun gibi bilgiler çıkabilir. Tüm bu ayrıntılar içeriden birine önemsiz gibi görünebilir, ancak bir saldırgan için fazlasıyla değerli bilgiler olabilir.

Mark Joseph Edwards, *Internet Security with Windows NT* adlı kitabında kimilerine sadece çöp gibi görünen materyallerden "yazım hataları yüzünden atılmış raporlar, kâğıt parçalarına yazılmış parolalar, üzerlerinde telefon numarası olan 'seni şurdan aradılar' gibi notlar, içinde hâlâ evrak olan klasörler, silinmemiş ya da imha edilmemiş disketler ve bantlar; hepsi de olası bir saldırgana yardımcı olacak şeylerdir." diye bahseder.

Yazar devam eder ve şu soruyu sorar: "... temizlikçi olarak çalışan kişiler kimlerdir? Temizlikçilerin bilgisayar odasına girmemesine karar vermişsinizdir; ama unutmayın ki bu insanlar çöp kutularına bakabilir. Eğer federal kurumlar çöp kutularına ve kâğıt öğütücülerine erişimi olan insanlara sicil soruşturması yapmayı gerekli görüyorlarsa, belki siz de bunu yapmalısınız."

Küçük Düşen Müdür

Harlan Fortis her zamanki gibi Bölge Otoyol Dairesi'ndeki işine geldiği zaman kimse bir tuhaflık olduğunu düşünmemişti. Evden aceleyle çıktığını ve kartını unuttuğunu söyledi. Güvenlik görevlisi, burada çalıştığı iki yıllık süre boyunca Harlan'ın hafta içi her gün ofise girip çıktığını görmüştü. Geçici bir çalışan kartı vererek bir imza attırdı ve adam işinin başına gitti.

İki gün sonra işler karışmaya başladı. Hikâye tüm bölüme saman alevi gibi yayıldı. Duyan insanların yarısı olayın doğru olamayacağını düşünüyordu. Kalanlar ise kahkahalarla gülsünler mi yoksa zavallı adama acısınlar mı bilemiyorlardı.

Ne de olsa George Adamson nazik ve sevecen biri ve başlarına gelen en iyi bölüm yöneticisiydi. Yaşadıklarını hak etmemişti. Yani hikâyenin gerçek olduğu düşünülürse.

Sorun, George'un bir cuma günü geç saatte Harlan'ı odasına çağı-

rıp, elinden geldiği kadar nazik bir şekilde pazartesi günü yeni birimine gitmesinin gerektiğini söylemesiyle başladı; Sağlık Hizmetleri Dairesi'ne. Harlan için bu işten atılmak gibi değildi. Daha da kötüydü; küçük düşürücüydü. Sesini kısıp bunu sineye çekmeyecekti.

Aynı akşam, sundurmasında oturmuş, evlerine dönen insanları seyrediyordu. Sonunda aynı mahallede oturan David adındaki çocuğu gördü. Okuldan mobiletiyle eve dönen o çocuğa herkes "Savaş Oyunlarındaki Çocuk" diyordu. David'i durdurdu; bu amaç için aldığı Mountain Dew Code Red içeceğini verdi ve ona bir iş teklif etti: Bilgisayarlarla ilgili yardım ve ağzını sıkı tutması karşılığında en yeni video oyun konsolu ve altı yeni oyun.

Harlan -şüphe uyandırabilecek ayrıntılara girmeden- projesini anlattıktan sonra David yardım etmeyi kabul etti. Harlan'a ne yapması gerektiğini açıkladı. Bir modem satın alacak, ofise gidecek, fazladan bir telefon girişi olan birinin bilgisayarına modemi bağlayacaktı. Cihazı kimsenin göremeyeceği bir şekilde masanın altına saklayacaktı. Sonra tehlikeli kısım geliyordu. Harlan'ın, bilgisayarın başına oturup, bir uzaktan erişim yazılım paketini indirip çalıştırması gerekiyordu. Her an masanın sahibi geri gelebilir ya da başka biri geçerken Harlan'ı adamın ofisinde görebilirdi. O kadar huzursuzdu ki çocuğun onun için yazdığı listeden yapması gerekenleri güçlükle okuyabiliyordu. Ama işi bitirdi ve farkedilmeden binadan çıktı.

Bombayı Yerleştirmek

David o gece yemekten sonra ona uğradı. İkisi birlikte Harlan'ın bilgisayarının başına oturdular ve oğlan birkaç dakika içinde modeme bağlanıp erişim sağlayarak George Adamson'ın makinasına ulaştı. Çok zor olmamıştı, çünkü George parolasını değiştirmek gibi emniyet önlemlerini hiçbir zaman almazdı ve sürekli birilerinden bir dosyayı indirmesini ya da elektronik postayla göndermesini isterdi. Zaman içinde ofisteki herkes adamın parolasını öğrenmişti.

David biraz gezindikten sonra bilgisayarda BütçeSlaytları2002.ppt dosyasını buldu ve onu Harlan'ın bilgisayarına indirdi. Harlan sonra çocuğa eve gitmesini ve birkaç saat sonra geri gelmesini söyledi.

David geri geldiğinde, Harlan ondan Otoyol Dairesi'nin bilgisayar sistemine bağlanmasını ve aynı dosyayı, eskisini silerek, buldukları yere koymasını istedi. Harlan David'e video oyun konsolunu gösterdi ve her şey yolunda giderse aletin yarın onun olacağına söz verdi.

George'u Şaşırtmak

Bütçe görüşmeleri gibi kulağa sıkıcı gelen bir şeyin pek kimsenin ilgisini çekeceğini düşünmezsiniz ama Bölge Konseyi'nin toplantı odası, gazeteciler, özel ilgi guruplarının temsilcileri, halktan insanlar ve hattâ iki televizyon haber ekibiyle tıkabasa dolmuştu.

George bu görüşmelerde her zaman çok şeyin risk altında olduğunu düşünmüştü. Kesenin ağzını açacak olan İlçe Konseyi'ydi ve George ikna edici bir sunum yapmazsa Otoyol Bütçesi kısalacaktı. Sonra da herkes yollardaki çukurlardan, çalışmayan trafik lambalarından ve tehlikeli dörtyol ağızlarından şikâyetçi olmaya başlayacak ve onu suçlayacaktı. Ertesi yıl yaşam daha da sefil bir hal alacaktı. Kürsüye çıkacak kişi olarak tanıtıldığında kendine güveniyordu. Bu sunum üzerinde altı hafta çalışmıştı ve PowerPoint slaytlarını karısına, diğer yöneticilere ve bazı yakın arkadaşlarına göstermişti. Herkes bunun şimdiye kadar yaptığı en iyi sunum olduğunda hemfikirdi.

İlk üç slayt çok iyi gitti. Her zamankinden farklı olarak bütün Konsey üyeleri dikkatlerini ona vermiş gibiydiler. Vurgulamak istediği noktaları etkili bir şekilde belirtiyordu.

Ve sonra birden her şey ters gitmeye başladı. Dördüncü slaytta geçen yıl açılan yeni otoyolun günbatımında çekilmiş bir fotoğrafının olması gerekiyordu. Onun yerine başka bir şey vardı, fazlasıyla küçük düşürücü bir şey: Penthouse ya da Hustler türü bir dergiden alınma bir resim. Dinleyicilerin hayret dolu seslerini duydu ve bir sonraki slayta geçmek için hemen dizüstü bilgisayarının düğmesine bastı.

Bu daha da kötüydü. Hayal gücüne hiçbir şey bırakılmamıştı.

Tıklayarak bir sonraki slayta geçmeye çalışıyordu ki dinleyicilerden biri projektörün fişini çekti ve bu sırada toplantı başkanı tokmağını sertçe vurarak gürültünün içinde toplantının ertelendiğini duyurdu.

Aldatmacanın İncelenmesi

Bu tepesi atmış çalışan, genç bir bilgisayar korsanının bilgilerini kullanarak, daire yöneticisinin bilgisayarına girmeyi başarmış, önemli bir PowerPoint sunumunu indirmiş ve bazı slaytları kesinlikle küçük düşürücü başka resimlerle değiştirmişti. Sonra da sunumu adamın bilgisayarına geri koymuştu.

Modem bir fişe takılı ve ofis bilgisayarlarından birine bağlıyken genç korsan telefon hattını kullanarak dışarıdan bağlanabilmişti. Çocuk, uzaktan erişim yazılımını önceden kurmuştu, böylece bilgisayara bağlandıktan sonra sistemde duran her dosyaya tam erişim sağlayabilecekti. Bilgisayar, kuruluşun ağına bağlı olduğu ve çocuk müdürün kullanıcı adını ve parolasını bildiği için kolaylıkla müdürün dosyalarına erişebilirdi.

Dergi resimlerini tarayıcıdan geçirmek de dahil, tüm iş yalnızca birkaç saat sürmüştü. Sonuç olarak iyi bir adamın şerefine sürülen leke ise akıl almaz bir büyüklüktedir.

Mitnick Mesajı:

İşten atılan, başka bir birime aktarılan ya da küçülme nedeniyle işine son verilen çalışanların büyük bölümü hiç sorun yaratmazlar. Ancak bir şirketin felaketi önlemek için ne gibi önlemler alabileceğini anlaması için bir tane sorun çıkması yeter.

Deneyimlerin ve istatistiklerin açıkça gösterdiğine göre şirkete en büyük tehlike içerden gelmektedir. Değerli bilgilerin nerede durduğuyla ilgili ayrıntılı bilgiyi ve şirketi nereden vurmanın en büyük zararı vereceğini ancak içerdekiler bilebilirler.

Terfi İsteyen Biri

Güzel bir sonbahar günü öğleden önce Peter Milton, Honorable Oto Yedek Parçaları'nın Denver'daki bölge ofisi binasının lobisine girdi. Bu şirket, araba piyasası için ulusal boyutta bir yedek parça toptancısıdır. Peter danışmada beklediği sırada danışma görevlisi genç hanım onu ziyaretçi olarak kaydetti, arayan birine arabayla geliş yolunu anlattı ve kargo şirketinden gelen bir adamla ilgilendi. Bunların hepsi aşağı yukarı aynı zamanda oldu.

Kadın ona yardımcı olmak için zaman bulunca, "Bu kadar çok şeyi bir arada yapmayı nasıl öğrendiniz?", diye sordu Peter. Kadın gülümsedi; görünüşe göre bunu farketmesinden memnun olmuştu. Ona Dallas Bürosu pazarlamadan olduğunu ve Atlanta bölge satışları sorumlusu Mike Talbott'un kendisiyle görüşeceğini söyledi. "Bugün ziyaret edeceğimiz bir müşterimiz var" dedi. "Burada, lobide bekleyeceğim."

"Pazarlama", dedi genç kadın neredeyse arzu dolu bir şekilde ve Peter ona gülümsedi. Ardından ne geleceğini duymak istiyordu. "Üniversiteye gitseydim, bu konuda eğitim alırdım." dedi. "Pazarlamada çalışmayı çok isterdim."

Peter yeniden gülümsedi. "Kaila", dedi, masanın üstündeki levhadan kadının adını okuyarak. "Dallas büromuzda eskiden sekreter olan bir hanım vardı. Kendini üç yıl önce pazarlamaya aldırdı. Şimdi pazarlama müdür yardımcısı ve eskiden kazandığının iki katını kazanıyor."

Kaila ışıltılı gözlerle baktı. Adam devam etti, "Bilgisayar kullanabilir misin?"

"Elbette", dedi kadın.

"Pazarlamada bir sekreterlik işi için yukardakilere seni önermeme ne dersin?"

Birden yüzü aydınlandı. "Bunun için Dallas'a bile giderim."

"Dallas'a bayılacaksın." dedi adam. "Şu anda bir açık olup olmadığına dair birşey söyleyemem ama elimden geleni yapacağım."

Kaila, takım elbiseli, kravatlı, düzgün kesimli ve iyi taralı saçları olan bu cici adamın iş yaşamında büyük bir değişiklik yaratabileceğini düşündü.

Peter lobide oturdu, dizüstü bilgisayarını açtı ve iş yapmaya başladı. On-on beş dakika sonra yeniden masaya geldi. "Görünüşe göre Mike'in işi uzadı. Beklerken e-postalarıma bakabileceğim bir konferans salonu var mı?"

Kaila konferans salonlarının kullanım saatlerini ayarlayan adamı aradı ve Peter'in ayırtılmamış bir tanesini kullanabilmesi için gerekli ayarlamaları yaptı. Silikon Vadisi şirketlerinden gelen bir geleneği sürdürerek (Apple herhalde bu uygulamayı ilk başlatandır), bazı konferans salonlarına çizgi film kahramanlarının, lokanta zincirlerinin, film yıldızlarının ya da çizgi roman kahramanlarının isimleri verilmişti. Fare Minnie salonunu bulması söylendi. Kadın giriş işlemlerini yaptı ve Fare Minnie salonuna nasıl gideceğini anlattı.

Peter odayı buldu, içeri yerleşti ve bilgisayarını ethernet girişini kullanarak ağa bağladı.

Neler olup bittiğini anlayabildiniz mi?

Doğru; saldırgan şirketin güvenlik duvarının arkasına geçerek şirket ağına bağlanmıştı.

Anthony'nin Öyküsü

Sanırım Anthony Lake'in tembel bir işadamı olduğu söylenebilirdi. Ya da belki "düzenbaz" demek daha yerinde olabilir.

Başka insanlar için çalışmak yerine kendi işini kurmak istemişti; hayali sabit bir yerde duracağı ve tüm ülkede koşturup durmasını gerektirmeyecek bir dükkân açmaktı. Ancak para getireceğinden emin olduğu bir iş yapmak istiyordu.

Ne tür bir dükkân olabilirdi acaba? Bulması uzun sürmedi. Araba tamiratından anlıyordu, böylece araba yedek parçaları dükkânında karar kıldı.

Başarılı olmayı nasıl garantiye alabilirdi? Yanıt aklına şimşek gibi geldi: Honorable Oto Yedek Parça Toptancısı'nı tüm mallarını kendisine maliyetine satmaya ikna etmek.

Doğal olarak böyle bir şeyi isteyerek yapmazlardı. Ancak Anthony insanları nasıl kandıracağını, arkadaşı Mickey ise başkalarının bilgisayarlarına nasıl gireceğini biliyordu. İkisi birlikte zekice bir plan yaptılar.

Mitnick Mesajı:

Çalışanlarınızı, bir kitabı yalnızca kapağına bakarak değerlendirmemeleri konusunda eğitin. Bir kişiye, yalnızca iyi giyimli olduğu ve saçı başı yapılı olduğu için inanılmamalı.

O sonbahar günü kendini inandırıcı bir şekilde Peter Milton adında bir çalışan olarak tanıttı ve çalışanları dalavereye getirip Honorable Oto Yedek Parça binasına girerek, dizüstü bilgisayarını ağa bağladı. Şimdiye kadar her şey yolunda gitmişti. Bundan sonra yapması gerekenler kolay olmayacaktı, özellikle de Anthony kendine on beş dakikalık bir limit belirlemişken. Daha uzun sürerse farkedilme tehlikesinin giderek artacağını düşünüyordu.

Bilgisayar aldıkları şirkete bağlı bir destek personeli gibi davranarak daha önce yaptığı bir telefon görüşmesinde onlara uzun bir terane okumuştu. "Şirketinizin bizimle iki yıllık bir destek kontratı var, bu yüzden sizi veri tabanımıza ekliyoruz böylece kullandığınız bir yazılım için bir yama ya da yeni bir yükseltilmiş sürüm çıktığında haberiniz olacak. Hangi uygulamaları kullandığınızı öğrenebilir miyim?" Gelen yanıt bir program listesi şeklindeydi ve muhasebeci bir arkadaş MAS 90 adlı programın aradıkları -perakende dükkânların listesi ve her birine verilen indirimler ve ödeme koşullarını içeren- program olduğunu söyledi.

Bu kilit bilgiden yararlanarak, ağdaki tüm geçerli terminalleri tanımlayan bir yazılım kullandı ve muhasebe bölümünün kullandığı doğru sunucuyu bulması çok zamanını almadı. Dizüstü bilgisayarına yüklü korsanlık araçları takımından bir program çalıştırdı ve onu hedef sunucuda bulunan yetkili kullanıcıları belirlemek için kullandı. Başka bir programla, "boşluk" ve "parola" gibi sık kullanılan parolaları denemeye başladı. "Parola" işe yaradı. Şaşılacak bir durum değildi. İş parola seçmeye gelince insanlar tüm yaratıcılıklarını kaybediyorlardı.

Yalnızca altı dakika geçmişti ve oyunun yarısı bitmiş, içeri girmişti.

Bir üç dakikayı da yeni şirket adını, adresini, telefon numarasını ve bağlantı numarasını dikkatle müşteri listesine eklemekle geçirdi. Ve sıra en kritik, her şeyin temel amacı olan değişikliğe geldi. Bu, tüm Honorable Oto Yedek Parçaları'nın ona %1 kazançla satılacağını belirleyen değişiklikti.

Yaklaşık on dakika içinde işi bitmişti. Kaila'ya teşekkür edip e-postalarını okuma işini bitirdiğini söyleyecek kadar oyalandı. Ayrıca Mike Talbot'un kendisine ulaştığını, planda bir değişiklik olduğunu ve müşterinin ofisinde buluşacaklarını söyledi. Kaila'ya onu pazarlamadaki o iş için önereceğini söylemeyi de ihmal etmedi ekledi.

Aldatmacanın İncelenmesi

Kendini Peter Milton olarak adlandıran saldırgan iki psikolojik tahrip tekniği kullanmıştı; biri planlıydı diğeri de o anda uydurulmuştu.

İyi para kazanan bir yönetici gibi giyinmişti. Kravat, ceket, düzgün kesimli saçlar; bunlar küçük ayrıntılar gibi görünebilirler ama kesinlikle bir etki bırakırlardı. Bunu ben istemeden keşfetmiştim. GTE Kaliforniya ofisinde -artık var olmayan büyük bir telefon şirketinde- çalıştığım kısa süre içerisinde kartım olmadan rahat ama düzgün giyimli -örneğin, spor bir gömlek, pilisiz pantolon ve Dockers ayakkabılarla- bir şekilde işe gelirsem durdurulup sorguya çekilirdim. Kartın nerede, kimsin, nerede çalışıyorsun? Başka bir gün ise, yine kartsız ama takım elbise ve kravat takıp iş adamı gibi giderdim. Eskiden kalma, hemen arkasından geçme yönteminin bir türünü kullanıp, binanın içine ya da güvenlikli bir girişe doğru yürüyen insan kalabalığının arasına karışırdım. Ana girişe yaklaşırlarken bazı insanlara takılıp onlardan biriymiş gibi sohbet ede ede yürürdüm. Kapıdan geçerdim ve güvenlik görevlileri kartımın olmadığını anlasalar bile yönetici gibi gözüktüğüm ve kartları olan insanlarla birlikte yürüdüğüm için bana birşey demezlerdi.

Bu deneyimim sayesinde güvenlik görevlilerinin davranışlarının ne kadar tahmin edilebilir olduğunu öğrendim. Onlar da hepimiz gibi görünüşe bakıp karar veriyorlardı. Bu da toplum mühendislerinin kullanmayı öğrendikleri ciddi bir zayıflıktı.

Saldırganın ikinci psikolojik silahı danışmada görevli kızın gösterdiği olağanüstü çabayı görmesiyle devreye girdi. Pek çok işi aynı anda yaparak, telaşa kapılmadan, herkese tüm dikkatini verdiği hissini yaratıyordu. Peter, kızın, kendini kanıtlamaya çalışan, yükselmek isteyen biri olduğu kanısına vardı. Pazarlama bölümünde çalıştığını söyleyince kızın tepkisine bakıp onunla bir yakınlık kurup kuramayacağına dair ipuçları aradı. Saldırgan için bu, daha iyi bir işe kaydınlması için yardım etmeye çalışacağına söz vererek etkileyebileceği insanlar listesine birinin daha eklenmesi anlamına geliyordu. (Eğer Muhasebe bölümüne gitmek istediğini söylemiş olsaydı, doğal olarak Peter da orada bir iş bulmasında yardımcı olabilecek bağlantılarının olduğunu söyleyecekti.)

Saldırganlar bu öyküde kullanılan başka bir psikolojik silahı daha kullanmayı çok severler: İki kademeli bir saldırıyla güven yaratmak. Önce pazarlamadaki işle ilgili biraz sohbet etti ve sonra da gerçek birinin "ismini bırakma" -başka bir çalışanın adını verme- tekniğini kullandı. Sırası gelmişken, kendi kullandığı ad da gerçek bir çalışana aitti.

Açılış sohbetinden sonra konferans salonuna geçmeyi hemen isteyebilirdi. Ama onun yerine biraz oturup çalışırmış gibi yaptı; güya bir arkadaşını bekliyordu. Olası şüpheleri bastırmanın başka bir yolu da buydu, çünkü saldırganlar ortalıkta fazla dolaşmazlardı. Yine de ortalıkta

Mitnick Mesajı:

Yabancı birinin şirket ağına dizüstü bilgisayarını bağlayabileceği bir yere girmesine izin vermek güvenlik sorunları oluşma tehlikesini artırır. Bir çalışanın, özellikle de şehir dışından gelmiş birinin, konferans salonundan e-postalarına bakması son derece makuldur. Ama ziyaretçi güvenilir bir çalışan değilse ya da ağ, yetkisiz bağlantıları engelleyecek şekilde yapılandırılmamışsa, bu durum şirket dosyalarının tehlikeye girmesine olanak tanıyan zayıf halka olabilir.

fazla dolaşmadı; toplum mühendisleri suç mahalinde gereğinden uzun kalmanın doğru birşey olmadığını bilirler.

Şunu da eklemek gerekir ki: Bu yazının hazırlandığı dönemdeki yasalara göre Anthony lobiye girerek bir suç işlememiştir. Gerçek bir çalışanın adını kullandığı zaman da suç işlememiştir. Ayrıca konferans salonunu kendisi için açmalarını sağlamasında da bir suç unsuru bulunmamaktadır. Şirket ağına bağlandığında ve hedef bilgisayarı aradığında da henüz bir suç işlememiştir.

Bilgisayar sistemini kırana kadar herhangi bir suç işlememiştir.

Kevin'i Merak Edenler

Yıllar önce küçük bir işte çalışırken, bilgi işlem bölümünü oluşturan diğer üç bilgisayarcıyla birlikte oturduğum ofise ne zaman girsem, adamlardan biri (burada ona Joe diyeceğim) bilgisayarındaki görüntüyü hızla değiştiriyordu. Bunun şüpheli bir durum olduğunu hemen anladım. Aynı gün içerisinde bu olay iki kere daha tekrarlanınca, bilmem gereken bir şeyler olduğundan emin olmuştum. Bu adam benim görmemi istemediği nasıl bir iş yapıyor olabilirdi?

Joe'nun bilgisayarı şirketin minibilgisayarlarına erişimi olan bir uçbirim gibi çalışıyordu, böylece neler yaptığını izleyebileceğim bir takip programı yükledim. Program omuzunun üstünden bakan bir televizyon kamerası gibi çalışıyor, bilgisayarında ne görüyorsa aynısını bana da gösteriyordu.

Benim masam Joe'nun masasının yanındaydı; görmesini zorlaştırmak için kendi monitörümü mümkün olduğunca döndürdüm ama her an bakabilir ve onun yaptıklarını izlediğimi anlayabilirdi. Ancak bu sorun olmayacaktı, çünkü yaptığı işe kendini fazlasıyla kaptırmıştı.

Gördüğüm şey karşısında çok şaşırdım. Alçak herifin benim bordro bilgilerimi karıştırdığını görünce ağzım açık kaldı. Adam benim maaşıma bakıyordu!

O sırada orada üç aylıktım ve Joe'nun ondan daha fazla maaş aldığım fikrine dayanamadığını düşündüm.

Birkaç dakika sonra, programlama bilgisi olmayan deneyimsiz bilgisayar korsanlarının kullandığı türden araçlar indirdiğini gördüm. Demek Joe dünyadan habersizdi ve Amerika'nın en deneyimli bilgisayar korsanlarından birinin yanında oturduğu konusunda en küçük bir fikri yoktu. Bu çok gülünç bir durumdu.

Maaşımla ilgili bilgileri çoktan almıştı, bu yüzden onu durdurmak için çok geçti. Ayrıca vergi dairesinde ya da Sosyal Güvenlik Dairesi'nde çalışan ve bilgisayar erişimi olan herhangi biri de maaşınıza bakabilirdi. Ne işler karıştırdığını bildiğimi söyleyerek elimdeki kozu kaybetmek istemiyordum. O zamanlar en büyük amacım fazla su yüzüne çıkmamaktı. İyi bir toplum mühendisi, becerilerinin ve bilgisinin reklamını yapmaz. İnsanların her zaman sizi hafife almalarını istersiniz, tehlike olarak görmelerini değil.

Böylece olayın üstünde durmadım ve Joe benimle ilgili bir sır bildiğini sanırken ben kendi kendime güldüm, halbuki her şey tam tersiydi. Onun neler karıştırdığını bilerek kozları ben elimde tutuyordum.

Zamanla, Bilgi İşlem grubunda çalıştığımız üç mesai arkadaşımın hepsinin de -ekipteki tek kız için de geçerli olmak üzere- gördükleri şu ya da bu şirin sekreterin ya da yakışıklı bir oğlanın eve götürdükleri maaşlarına bakıp eğlendiklerini keşfettim. Merak ettikleri herkesin maaşına ve primlerine bakıyorlardı. Bunların arasında üst düzey yöneticiler de vardı.

Aldatmacanın İncelenmesi

Bu öykü ilginç bir sorunu yansıtmaktadır. Bordro dosyaları şirketin bilgisayar sisteminin yönetiminden sorumlu kişiler tarafından erişilebilecek bir konumdadırlar. İş yine bir personel sorunu durumuna gelir: kimin güvenilir olduğuna karar vermek. Bazı durumlarda Bİ çalışanları sağa sola göz atmak fikrini çekici bulurlar. Bunu yapacak olanakları da vardır çünkü bu dosyalara erişimi kısıtlayan kontrolleri aşmak için özel haklara sahiptirler.

Alınacak bir önlem, bordro dosyaları gibi özellikle hassas dosyalara erişimi denetlemek olabilir. Gerekli haklara sahip herhangi biri denetimi kaldırabilir ya da takip edilmelerini sağlayacak yerleri temizleyebilir, ancak atılacak her adım ahlâksız bir çalışanın izlerini saklayabilmesi için daha fazla çaba harcamasını gerektirecektir.

Aldatmacanın Engellenmesi

Toplum mühendisleri, çöpleri karıştırmaktan tutun da bir güvenlik görevlisini ya da danışma memurunu kandırmaya kadar çeşitli yöntemlerle şirket alanınıza girebilirler. Ama bunlara karşı da alabileceğiniz önlemler olduğunu duymak hoşunuza gidecektir.

Mesai Saatleri Dışında Güvenlik

İşyerine kartları olmadan gelen tüm çalışanların, lobide ya da güvenlik ofisinde, o gün için geçici bir kart vermek amacıyla durdurulmaları gerekir. Personel kartı yanında olmayan biriyle karşılaştıklarında şirket güvenlik görevlilerinin izleyecekleri belirli adımlar olsaydı, bu bölümde anlatılan ilk olay çok daha farklı bir şekilde sonuçlanabilirdi.

Güvenliğin öncelik taşımadığı şirketlerde ya da şirket içi alanlarda herkesin kartını görünür bir yerde taşımasında ısrar etmek önemli olmayabilir. Ama hassas bölgelere sahip alanlarda bu kural, katı bir şekilde uygulanan, standart bir kural olmalıdır. Çalışanlar kart göstermeyen kişileri durdurmak konusunda eğitilmeli ve teşvik edilmelidirler. Üst düzey çalışanlara da kendisini durduran kişiyi küçük düşürmeden bu tarz kontrolleri kabullenmeleri öğretilmelidir.

Şirket kuralları, sürekli kartını takmayı unutan kişilere verilecek cezalar konusunda çalışanları uyarmalıdır. Cezaların arasında çalışanın bir günlüğüne ücretsiz uzaklaştırılması ya da siciline geçecek bir uyarının verilmesi olabilir. Bazı şirketler giderek artan sert cezaları yürürlüğe koymuşlardır. Bu cezalar, kişinin müdürüne durumun iletilemesi, sonra da resmî bir ihtar şeklinde olabilir.

Ek olarak, korunması gereken hassas bilgilerin olduğu yerlerde, mesai saatleri dışında işe gelecek kişilere izin verilebilmesi için gerekli süreçler oturtulmalıdır. Bir çözüm, bu ziyaretlerin şirket güvenliği ya da bu işe bakan birim aracılığıyla yapılması olabilir. Bu birim mesai dışı çalışma talebiyle arayan herhangi bir çalışanın kimliğini kişinin müdürünü arayarak ya da başka makul bir güvenlik yöntemi izleyerek düzenli olarak kontrol edebilir.

Çöplere Saygılı Olmak

Çöp dalışı öyküsü, şirket atıklarınızın olası kötüye kullanım yollarının üstünde durdu. İşte çöpler konusunda akıllı olmanın sekiz anahtarı:

- Tüm hassas bilgileri hassaslık derecesine göre sınıflandırın.
- Hassas bilgilerin atılmasına yönelik olarak şirket çapında iş süreçleri oluşturun.
- Atılacak tüm hassas bilgilerin önce kâğıt öğütücüden geçirilmesi konusunda ısrarlı davranın ve öğütücüden geçmeyecek kadar küçük olup önemli bilgiler içeren kağıt parçalarından kurtulmak üzere güvenli bir yöntem belirleyin. Kâğıt öğütücüler, kararlı bir saldırganın biraz sabırla bir araya getirebileceği kâğıt şeritleri çıkaran ucuz makinelerden olmamalıdırlar. Onlar yerine çapraz öğütücü denen türler ya da çıktıyı işe yaramaz bir küspeye dönüştüren makineler kullanılmalıdır.

- Atılmadan önce veri kayıt ortamlarını -disketler, sıkıştırılmış diskler, dosya saklamak için kullanılan CD'ler ve DVD'ler, bantlar, eski sabit sürücüler ve diğerlerini- tamamen silecek ya da kullanılmaz hale getirecek bir yöntem oluşturulmasını sağlayın. Dosyaları silmenin onları gerçek anlamda ortadan kaldırmadığını, silinen dosyaların yeniden kurtarılabildiklerini unutmayın. Enron yöneticileri ve pek çok başkaları bunu acı bir şekilde öğrendiler. Kaydedilebilir ortamları yalnızca çöpe atmak mahallenizin arkadaş canlısı çöp dalıcısına davetiye çıkarmaktır. (Kaydedilebilir ortamların ve araçların atılmasına yönelik belirli kurallar için 16. bölüme bakınız.)
- Temizlik ekiplerinizin seçiminde uygun ölçüde bir kontrol sağlayın, gerekirse sicillerine bakın.
- Çalışanlarınızı, çöpe attıkları şeyin içeriğine dikkat etmeleri konusunda düzenli olarak uyarın.
- Büyük çöp bidonlarını kilitleyin.
- Hassas malzemeler için farklı atık varilleri kullanın ve bu tarz işlerde uzmanlaşmış bir şirketle anlaşarak malzemelerin imhasını sağlayın.

Çalışanlara Güle Güle Derken

Hassas bilgilere, parolalara, dışarıdan erişim numaralarına ve benzer şeylere erişimi olan bir çalışan işten ayrılırken uyulması gereken katı kurallar olması gerektiği bu sayfalarda daha önce vurgulanmıştı. Güvenlik süreçleriniz kimlerin hangi sistemlerde yetkili olduğunu takip edecek yollar içermelidir. Kararlı bir toplum mühendisinin güvenlik bariyerlerinizden geçmesini engellemek zor bir iştir ama eski çalışanlarınız için de bunun kolay olmaması gerekir.

Kolaylıkla göz ardı edilebilen başka bir ayrıntı ise arşivden yedekleme bantlarını almaya yetkili bir çalışan işten ayrıldığında görülür. Kâğıda dökülmüş bir kurallar bütünü, kişinin adının yetki listesinden silinmesi için hemen arşivleme şirketinin aranması gerektiğini vurgulamalıdır.

Kitabın on altıncı bölümünde bu önemli konuyla ilgili ayrıntılı bilgi verilmektedir, ancak bu öyküde de görüldüğü üzere, yerleştirilmesi gereken bazı kilit güvenlik önlemlerini burada belirtmek yerinde olacaktır:

- Bir çalışan ayrıldığında atılacak adımların tam ve ayrıntılı bir kontrol listesi tutulmalıdır ve hassas bilgilere erişimi olan çalışanlar için özel maddeler bulunmalıdır.
- Çalışanın bilgisayar erişiminin zaman kaybetmeden -hattâ kişi daha binayı terk etmeden önce- kapatılmasına yönelik bir kural belirlenmelidir.

- Kişinin tanıtım kartının ve eğer varsa, anahtarların ve elektronik erişim cihazlarının geri alınmasıyla ilgili bir süreç oluşturulmalıdır.
- Güvenlik görevlilerinin giriş kartı olmayan çalışanları içeri almadan önce resimli bir kimlik kartı görmeleri ve kişinin şirkette çalışıp çalışmadığının bir listeden kontrol edilmesi kurallarını getiren maddeler olmalıdır.

Bazı adımlar kimi şirketler için aşırı ya da daha pahalı olabilirken başkaları için uygun olabilir. Bu tarz katı güvenlik önlemleri arasında aşağıdakiler bulunabilir:

- Elektronik kimlik kartlarıyla çalışan manyetik giriş kapıları bulunmalıdır. Kişinin şirket personeli olduğunun ve binaya girmeye yetkili olup olmadığının elektronik olarak anında belirlenebilmesi için her çalışan, kartını tarayıcıdan geçirir. (Şu da unutulmamalıdır ki, her şeye karşın güvenlik görevlileri hemen arkasından geçmelere -yetkisiz birinin gerçek bir çalışanın hemen arkasından içeriye sızmasına- karşı uyanık olacak şekilde eğitilmelidir.)
- Ayrılan kişiyle (özellikle bu kişi işten atılmışsa) aynı iş ekibinde çalışan herkese parolalarını değiştirme zorunluluğu getirilmelidir. (Bu çok abartılı gibi mi görünüyor? General Telephone şirketindeki kısa süreli hizmetimden uzun yıllar sonra, Pacific Bell güvenlik sorumlularının General Telephone'un beni işe aldığını öğrendiklerinde "gülmekten kırıldıklarını" duydum. Bu General Telephone'un yararına oldu, çünkü beni işten çıkardıktan sonra ünlü bir bilgisayar korsanın onlarla çalışmış olduğunu öğrendiklerinde, şirketteki herkesin parolalarını değiştirmesini zorunlu kılmışlar!)

Binalarınızın hapishane gibi olmasını istemezsiniz ama aynı zamanda dün işten atılıp bugün zarar vermeye niyetli olarak geri gelen birine karşı da korunmanız gerekir.

Kimseyi Unutmayın

Güvenlik politikaları işe yeni girmiş çalışanları ve hassas bilgiyle haşır neşir olmayan, danışma görevlisi gibi kişileri göz ardı etme eğilimindedirler. Daha önce gördüğümüz gibi, danışma görevlileri saldırganlar için elverişli hedeflerdir ve araba yedek parçaları şirketine girişi anlatan öykü de bu konuda örnek oluşturuyor. Şirketin farklı bir tesisinde çalıştığını söyleyen ve bir profesyonel gibi giyinmiş arkadaş canlısı bir kişi göründüğü gibi olmayabilir. Danışma görevlileri yeri geldiğinde şirket kimliğini nazikçe soracak şekilde eğitilmiş olmalıdırlar ve bu eğitim yalnızca ana girişte duran danışma görevlisine değil, öğle saatlerinde ya da kahve molalarında onların yerine bakan kişilere de verilmelidir.

Şirket dışından gelen ziyaretçiler için güvenlik kuralları resimli bir

kimlik gösterilmesini ve bilginin kaydedilmesini zorunlu tutmalıdır. Sahte kimlik üretmek zor değildir, ancak kimliğin gösterilmesi olası saldırganlar için bahane üretme işini bir derece zorlaştırmaktadır.

Ba ı şirketlerde ziyaretçilerin lobiden alınıp toplantıdan toplantıya giderken kendilerine eşlik edilmesi zorunluluğu getiren bir kural uygulamak mantıklı olabilir. Eşlik eden görevlinin ziyaretçiyi ilk toplantısına götürdüğünde bu kişinin binaya çalışan olarak mı yoksa dışardan bir ziyaretçi olarak mı girdiğini açıkça belirtme koşulu olmalıdır. Neden bu önemlidir? Çünkü, daha önceki hikâyelerde de gördüğümüz gibi, bir saldırgan sık sık ilk karşılaştığı kişiye kendini belirli bir kişi olarak tanıtırken ikinci karşılaştığına tamamen farklı biri olarak tanıtmaktadır. Bir saldırganın lobide kendini göstermesi, danışma görevlisini bir mühendisle randevusu olduğuna inandırması... sonra mühendisin odasına kadar götürülmesi ve orada kendini şirkete bir ürün satmak isteyen bir satış temsilcisi olarak tanıtması... ve en sonunda da mühendisle görüşmesi bittiğinde binada serbestçe gezinme fırsatı bulması son derece kolaydır.

Başka bir ofisten gelen bir çalışanı içeri almadan önce kişinin gerçekten bir çalışan olup olmadığının tespiti için uygun süreçler bulunmalıdır. Danışma ve güvenlik görevlileri, saldırganların şirket binalarına girebilmek için kullandıkları, bir çalışanın kimliğine bürünme yöntemlerinin bilincinde olmalıdırlar.

Binanın içine girmeyi başaran ve dizüstü bilgisayarını şirket güvenlik duvarının arkasından ağa bağlayan bir saldırgana karşı korunmak için ne yapılabilir? Bugünün teknolojileri göz önüne alındığında bu güç bir iştir. Konferans salonları, eğitim odaları ve benzeri yerlerde kilit altına alınmamış ağ girişleri bulunmamalıdır; ya da en azından, bu girişler güvenlik duvarları ya da routerlarla koruma altına alınmış olmalıdırlar. Ama en iyi koruma, ağa bağlanan herkesin kendini tanıtması için güvenli bir yol oluşturmaktır.

Bilgiyi Sağlama Alın!

Küçük bir uyarı: Şirketinizin her Bİ çalışanı ne kadar maaş aldığınızı, genel müdürün ne kadar para aldığını ve kayak tatiline giderken kimin şirket jetini kullandığını büyük olasılıkla biliyordur ya da çok geçmeden öğrenecektir.

Bazı şirketlerde Bilgi İşlem ya da muhasebe çalışanlarının kendi maaşlarını yükseltmeleri, sahte bir satıcıya ödeme yapmaları, insan kaynakları kayıtlarından olumsuz sicilleri silmeleri ve bunun gibi şeyler yapmaları bile mümkündür. Bazen yalnızca yakalanma korkusu onları dürüst olmaya iter... sonunda bir gün gelir ve adamın açgözlülüğü ya da ahlâksız ruhu tehlikeyi bir kenara iterek, götürebildiği kadar para götürmesine neden olur.

Elbette buna karşı da çözümler vardır. Hassas dosyalara, uygun erişim kontrolleri yerleştirilerek yalnızca yetkili kişilerin onları açması sağlanabilir. Bazı işletim sistemleri belli olayları, örneğin başarılı olsun olmasın korumalı bir dosyaya ulaşmaya çalışan herkesi, kaydedecek şekilde ayarlanabilen denetim kontrolleri içerir.

Eğer şirketiniz konunun bilincindeyse ve hassas dosyaları koruyan uygun denetim mekanizmaları ve erişim sınırlamaları yerleştirmişse, doğru yönde güçlü adımlar atıyorsunuz demektir.

11 TEKNOLOJİYİ VE TOPLUM MÜHENDİSLİĞİNİ BİRLEŞTİRMEK

Bir toplum mühendisi, amacına ulaşmasına yardımcı olması için insanları birşeyler yapmaya yönlendirebilme yeteneğiyle yaşar; ancak başarılı olabilmek için, çoğu zaman hatırı sayılır bir bilgi birikimine sahip olmasının yanısıra bilgisayar ve telefon sistemleriyle haşır neşir olması da gerekir.

İşte size teknolojinin önemli bir rol oynadığı özgün toplum mühendisliği dolaplarından bir örnek.

Parmaklıkların arasından korsanlık

Fiziksel, iletişimsel ya da elektronik olarak zorla içeri girmelere karşı korunan en güvenli yerler arasında sizce nereler vardır? Pentagon mu? Doğru. Beyaz Saray mı? Kesinlikle. Bir dağın altına gömülü Kuzey Amerika Hava Savunma Üssü, NORAD mı? Şüphesiz.

Ya hapishaneler ve tutukevlerine ne dersiniz? Ülkedeki herhangi bir yerden daha korunaklı olmalılar, öyle değil mi? İnsanlar ender olarak kaçarlar, kaçtıklarında da genellikle kısa sürede yakalanırlar. Federal bir tesisin toplum mühendisliği saldırılarına karşı dayanıklı olacağını düşünürsünüz. Ancak yanılırsınız, hiçbir yerde kusursuz güvenlik diye birşey yoktur.

Birkaç yıl önce bir çift düzenbaz (aslında profesyonel dolandırıcılar) bir sorunla karşılaştılar. En son kaldırdıkları yüklü paranın bir bölge yargıcına ait olduğu ortaya çıktı. İkilinin geçen yıllarda zaman zaman yasayla başları derde girmişti ama bu kez federal yetkililer durumla daha çok ilgilendiler. Düzenbazlardan birini, Charles Gondorff'u enselediler ve onu San Diego yakınlarındaki bir tutukevine attılar. Federal sulh hakimi, kaçma olasılığı olduğu ve topluma zararlı olduğu gerekçesiyle Gondorff'un göz altına alınmasına karar verdi.

Arkadaşı Johnny Hooker, Charlie'nin bir savunma avukatına ihtiyacı olacağını biliyordu. Ama parayı nereden bulacaktı? Pek çok dolandırıcı gibi o da paraları güzel giysilere, havalı kameralara ve kadınlara yatırmış, böylece para, geldiği kadar hızla suyunu çekmişti. Johnny'nin, üzerinde, yaşamasına yetecek kadar para nadiren bulunurdu.

İyi bir avukat tutacak kadar parayı başka bir dolap çevirerek bulması gerekiyordu. Johnny bunu tek başına başaramazdı. Oynadıkları oyunların arkasındaki adam hep Charlie Gondorff olmuştu. Ama Johnny,

Terimler

DOĞRUDAN BAĞLANTI HİZMETİ: Alıcı kaldırıldığında doğrudan sabit bir numaraya bağlanan telefonlar için telefon şirketlerinde kullanılan bir terim.

REDDET-KES: Belirli bir telefon numarasında gelen aramaların engellenmesi şeklinde gerekli ayarlamalar yapılarak sunulan bir telefon şirketi hizmet seçeneği.

Federaller işin içinde iki kişinin olduğunu bilirken ve diğerini de yakalamak için bu kadar heveslilerken ne yapacağını sormak için tutukevine gitmeye cesaret edemezdi. Yalnızca ailesinin ziyaret etmesine izin veriliyordu, bu da sahte kimlik belgesi gösterip ailenin bir ferdi olduğunu öne sürmesi gerekecek demekti. Federal bir hapishanede sahte kimlik kullanmaya çalışmak pek iyi bir fikir gibi gelmedi.

Hayır, Gondorff'la bağlantı kurmak için başka bir yol bulması gerekecekti.

Kolay olmayacaktı. Herhangi bir federal, eyalet ya da yerel hapishanede tutuklu bulunan birinin gelen telefonlara çıkmasına izin verilmezdi. Federal bir tutukevinde her tutuklu telefonunun yanında asılı duran levhada şöyle bir şey yazılıdır: "Bu levha buraya, bu telefondan yapılan tüm görüşmelerin dinlendiğini ve telefonu kullanmanın konuşmanın dinleneceğinin kabul edilmesi anlamına geldiğini hatırlatmak için koyulmuştur." Eğer suç işlemek gibi bir planınız varsa, devlet görevlilerinin telefonu dinlemesinin tek bir sonucu vardır: Hapishanedeki tatilinizin süresinin biraz daha uzaması.

Ancak Johnny belli aramaların dinlenmediğini biliyordu. Örneğin müvekkil-avukat görüşmesi gibi. Aslında Gondorff'un tutulduğu yerde doğrudan Federal Kamu Savunma Bürosu'na (KSB) bağlı telefonlar vardı. O telefonlardan birini kaldırıyordun ve KSB'deki bağlı olduğu telefona doğrudan ulaşıyordun. Telefon şirketleri buna Doğrudan Bağlantı Hizmeti adını verir. Hiçbir şeyden kuşkulanmayan yetkililer bu hizmetin güvenli ve kurcalanmaya dayanıklı olduğunu varsayıyorlardı, çünkü dışarıya yapılan aramalar yalnızca KSB'ye gidiyor, gelen aramalar ise engelleniyordu. Biri telefon numaralarını bulmayı başarsa bile numaralar telefon şirketindeki santralda reddet-kes şeklinde programlanmışlardı.

Johnny bu sorunu çözmenin bir yolu olması gerektiğine karar verdi. Gondorff zaten içerden, KSB telefonlarından birini kaldırıp şunu söylemeyi de denemişti: "Ben Tom, telefon şirketi onarım bölümünden. Bu hat üstünde bir test yapıyoruz, önce dokuz sonra da sıfır sıfır tuşlamanız gerekiyor." Dokuz dış hattâ erişimi sağlayacak, sıfır sıfır da şehirlerarası santrale bağlayacaktı. İşe yaramadı. KSB'de telefonu açan kişi bu numarayı zaten biliyordu.

Johnny'nin işleri daha iyi gidiyordu. Tutukevinde on hücre birimi bu-

lunduğunu ve bunların her birinin Kamu Savunma Bürosu'yla doğrudan bağlantılı olduğunu kolaylıkla öğrenmişti. Bazı engellerle karşılaşıyordu ama iyi bir toplum mühendisi olarak ayağa takılıp duran bu can sıkıcı taşların çevresinden dolaşmanın yollarını da buluyordu. Acaba Gondorff hangi birimdeydi? O hücre biriminde bulunan doğrudan bağlantı hattının telefon numarası neydi? Ve hapishane yetkilileri tarafından engellenmeden ilk mesajı Gondorff'a nasıl ulaştıracaktı?

Federal kurumlarda bulunan gizli telefonların numaralarını elde etmek, sıradan insanlara olanaksız gibi görünen bir şey iken, bir dalavereci için çoğunlukla birkaç telefon görüşmesiyle ele geçirebilecek bir bilgidir. Kafasında oluşturduğu planı birkaç gece yatağında dönerek gözden geçirdikten sonra Johnny bir sabah her şey kafasında beş adım olarak planlanmış bir şekilde uyandı.

Önce, KSB'ye doğrudan bağlı on telefonun numaralarını öğrenecekti.

On telefonu birden gelen aramaları alacak şekilde değiştirecekti.

Gondorff'un hangi hücre biriminde olduğunu bulacaktı.

Sonra hangi telefonun bu birime bağlı olduğunu öğrenecekti.

En sonunda, yetkileri kuşkulandırmadan Gondorff'la bir telefon görüşmesi ayarlayacaktı.

Çocuk oyuncağı, diye düşündü.

Bell Ana'yı Arıyor...

Johnny, federal hükümet adına mal ve hizmet satın alan Genel Hizmet İdaresi'nden arıyormuş numarası yaparak telefon şirketi müdürlüğünü aramakla işe başladı. Bir ek hizmet sözleşmesi üzerinde çalıştığını ve kullanılan doğrudan bağlantı hizmetlerinin fatura bilgilerine ihtiyacı olduğunu söyledi. Bu listeye San Diego tutukevinin telefon numaralarının ve aylık giderlerinin de dahil olması gerektiğini ekledi. Karşıdaki hanım yardımcı olmaktan memnun olacaktı.

Numaraları elde ettikten sonra emin olmak için bu hatlardan birini çevirdi ve karşılığında duyduğu şey tipik bir kaydı oldu. "Bu hattın bağlantısı kesilmiştir ya da hat hizmet dışıdır." İşin aslının bu kayıtta söylenenle uzaktan yakından bir ilgisi olmadığını biliyordu, tam beklediği gibi, hat, gelen aramaları engellemek üzere programlanmıştı.

Telefon şirketinin çalışma şekilleri ve süreçleriyle ilgili geniş bilgisi sayesinde RCMAC, Recent Change Memory Authorization Center (Kısa Süreli Hafıza Değişim Yetki Merkezi - bu adları kimin uydurduğunu hep merak etmişimdir!) adında bir bölüme ulaşması gerektiğini biliyordu. Telefon şirketinin İşlemler Ofisi'ni aramakla işe başladı ve onarımdan aradığını söyleyip, verdiği alan kodu ve önekin ait olduğu bölgeye

bakan RCMAC'nin telefon numarasını istedi. Tutukevindeki tüm telefon hattı hizmetleri aynı merkez ofisten veriliyordu. Bu, onarıma gitmiş ve yardıma ihtiyacı olan teknisyenlerin her zaman yaptığı türden, sıradan bir istekti ve memur ona numarayı vermekte tereddüt etmedi.

RCMAC'yi aradı, sahte bir ad verdi ve yine onarım bölümünde çalıştığını söyledi. Telefonu açan kadından, daha önce işlemler ofisinden aldığı numaralardan birine ulaşmasını istedi. Kadın numarayı bulduğunda Johnny sordu: "Numara reddet-kes olarak mı ayarlanmış?"

"Evet", dedi kadın.

"Eh, bu, müşteriye neden hiç telefon gelmediğini açıklıyor!", dedi Johnny. "Bana bir iyilik yapabilir misin? Hat sınıf numarasını değiştirmeni ya da reddet-kes özelliğini kaldırmanı isteyeceğim, olur mu?" Kadın, değişimi gerçekleştirebilmek için bir hizmet emri gerekip gerekmediğini kontrol etmek için başka bir bilgisayar sistemine bakarken kısa bir sessizlik oldu. "Bu numaranın yalnızca arama yapmaya açık olması gerekiyor. Değişiklik yapmak için hizmet emri yok."

"Doğru, bir yanlışlık oldu. Emri dün çıkarmamız gerekiyordu ama bu müşteriyle her zaman ilgilenen abone temsilcisi hastalanıp eve gitti ve bu işi yapmayı başkasına söylemeyi de unuttu. Bu yüzden müşteri şu anda küplere binmiş durumda."

Kadın bir an duralayıp, standart çalışma şekline aykırı ve olağan dışı bu isteği değerlendirdi, sonra da, "Tamam", dedi. Kadının değişikliği girmek için tuşlara bastığını duyabiliyordu. Birkaç saniye sonra iş bitmişti.

Buzlar çözülmüş, aralarında bir çeşit yakınlaşma oluşmuştu. Kadının tavırlarını ve yardım etme isteğini tartarak, Johnny hepsini yaptırmakta tereddüt etmedi. "Bana yardım edebileceğiniz birkaç dakikanız daha var mı?" diye sordu.

"Var", diye yanıtladı kadın. "Ne gerekiyordu?"

"Aynı müşteriye ait başka numaralar da var ve hepsinde de aynı sorun mevcut. Ben numaraları size okursam, siz de reddet-kes ayarlarını düzeltebilir misiniz?" Kadın bunun sorun olmayacağını söyledi.

Birkaç dakika sonra telefon hatlarının hepsi de gelen aramaları alacak şekilde "düzeltilmişti."

Gondorff'un bulunması

Bir sonraki adım Gondorff'un hangi hücre biriminde olduğunu bulmaktı. Hapishane ve tutukevlerini yönetenler bu bilgiyi dışarıdan birilerinin öğrenmesini kesinlikle istemezler. Johnny'nin bir kez daha toplum mühendisliği becerilerine güvenmesi gerekiyordu.

Başka bir şehirdeki bir federal hapishaneyi aradı; Johnny Miami'yi aramıştı -ama başka herhangi bir yer de iş görürdü- ve New York'taki tutukevinden aradığını söyledi. Müdürlüğün tutuklu bilgisayarında çalışan biriyle konuşmak istedi. Tutuklu bilgisayarı, ülkenin herhangi bir yerinde Hapishaneler Müdürlüğü'ne bağlı tesislerde tutulan mahkûmlarla ilgili bilgilerin saklandığı bilgisayar sistemiydi.

İlgili kişi telefona çıktığında Johnny, Brooklyn aksanıyla konuşmaya başladı. "Merhaba," dedi. Ben New York Federal Tutukevi'nden Thomas. Tutuklu bilgisayarıyla bağlantımız gidip geliyor, bir tutuklunun yerini bulmama yardımcı olabilir misin, sanırım sizin orada tutuluyor" ve Gondorff'un adını ve kayıt numarasını verdi.

"Hayır, burada değil", dedi adam birkaç saniye sonra. "San Diego'daki tutukevinde."

Johnny şaşırmış gibi yaptı. "San Diego mu? Geçen hafta korumalı bir uçakla Miami'ye aktarılması gerekiyordu! Aynı adamdan mı söz ediyoruz? Adamın doğum tarihi nedir?"

"3/12/60", dedi adam ekrandan okuyarak.

"Evet, aynı adam. Hangi hücre biriminde tutuluyor?"

"Hücre On Kuzey", dedi adam. Her ne kadar New York'taki bir hapishane görevlisinin böyle bir şeyi öğrenmek istemesinin anlaşılır bir nedeni olmasa da soruyu neşeyle yanıtlamıştı.

Johnny tüm telefonları gelen aramalar için açtırmış ve Gondorff'un hangi hücre biriminde olduğunu da öğrenmişti. Bir sonraki adım hangi telefon numarasının *Hücre On Kuzey* olduğunu bulmaktı.

Bu biraz zor olacaktı. Johnny numaralardan birini aradı. Telefon zili kapalı olacağı için kimsenin telefonun çaldığını anlamayacağını biliyordu. Oturdu ve Fodor'un Avrupa'nın Büyük Kentleri adlı gezi rehberine göz gezdirirken bir yandan da ahizeden çalma sesini dinliyordu. Sonunda biri telefonu açtı. Diğer uçtaki tutuklu doğal olarak mahkemece belirlenmiş avukatına ulaşmaya çalışıyordu. Johnny karşı tarafın beklentisine karşılık verecek yanıtı hazırlamıştı. "Kamu Savunma Bürosu", dedi.

Adam avukatıyla görüşmek istediğini söylediğinde, Johnny, "Burada olup olmadığını bakayım, hangi hücre biriminden arıyorsun?" dedi. Adamın yanıtını not etti, bekletme düğmesine bastı, otuz saniye sonra yeniden açtı ve, "Mahkemedeymiş, daha sonra araman gerekecek", diyerek kapattı.

Sabahının çoğunu bunu yaparak geçirdi ama daha kötüsü de olabilirdi. Dördüncü denemesinde *Hücre On Kuzey*'i buldu. Böylece Johnny artık Gondorff'un birimine ait KSB numarasını biliyordu.

Saatlerinizi ayarlayın

Şimdi iş Gondorff'a tutukluları doğrudan Kamu Savunma Bürosu'yla görüştüren telefonu ne zaman açacağını söyleyen bir mesaj göndermeye kalıyordu. Bu göründüğünden daha kolay bir işti.

Johnny tutukevini arayarak, en resmi sesiyle kendini bir çalışan olarak tanıttı ve Hücre On Kuzey'le görüşmek istediğini söyledi. Arama hemen aktarıldı. İnfaz koruma memuru telefonu açtığında Johnny, yeni tutukluların giriş ve çıkışlarını düzenleyen Dağıtım ve Tahliye Birimi'nin iç görüşmelerde kullanılan kısaltmasını kullanarak memuru kandırdı. "Ben DT'den Tyson", dedi. "Tutuklu Gondorff'la görüşmem gerek. Göndermemiz gereken ona ait eşyalar var, nereye gönderilmesini istiyorsa oranın adresini vermesi gerekiyor. Onu telefona çağırabilir misiniz?"

Johnny memurun oturma salonuna bağırdığını duydu. Birkaç dakikalık sabırsız bir bekleyişten sonra, telefona tanıdık bir ses çıktı.

Johnny ona, "Konuşmam bitene kadar sakın sesini çıkarma", dedi. Eşyaların nereye gönderilmesini istediğini konuşuyorlarmış gibi görünmesi için Johnny ona söylemesi gerekenleri anlattı, sonra da, "Bugün öğleden sonra saat birde Kamu Savunma Bürosu telefonunun başında olabileceksen, yanıt verme. Olamayacaksan, o zaman orada olabileceğin bir saati söyle", dedi. Gondorff yanıt vermedi. Johnny devam etti. "İyi. Saat birde orada ol. Seni arayacağım. Ahizeyi kaldır. Eğer telefon otomatik olarak Kamu Savunma Bürosu'nu aramaya başlarsa her yirmi saniyede bir telefonun düğmesine bas. Sesimi duyana kadar bunu yapmayı sürdür."

Saat birde Gondorff telefonu açtı ve Johnny orada onu bekliyordu. Sohbet eder gibi, aceleye getirmeden, keyifle konuştular ve benzer görüşmeler Gondorff'un mahkeme masraflarını karşılamak için çevirecekleri dolabın ayrıntılarını konuşmak amacıyla birkaç kere daha tekrarlandı. Hepsi de devlet gözetiminin dışında gerçekleşmişti.

Aldatmacanın incelenmesi

Bu olay, bir toplum mühendisinin, her biri tek başına önemsiz gibi duran işleri yapmaları için farklı insanları kandırarak, olanaksız zannedilen bir işi nasıl başardığını gösteren çarpıcı bir örnektir. Aslında, yapılan her hareket, dalavere tamamlanana kadar bulmacanın bir parçasını oluşturur.

İlk telefon şirketi çalışanı, federal hükümete bağlı Genel Hizmetler İdaresi'nden birine bilgi verdiğini düşünüyordu.

Bir sonraki telefon şirketi çalışanı, telefon hizmet sınıfını bir hizmet emri olmadan değiştirmemesi gerektiğini biliyordu ama yine de sevimli adama yardımcı oldu. Böylece tutukevindeki Kamu Savunma Bürosu telefonlarının tümü dışarıdan aranabilir duruma geldi.

Miami tutukevindeki adam için başka bir federal merkezde çalışan ve bilgisayarla sorun yaşayan birine yardım etmek gayet mantıklıydı. Her ne kadar hücre birimini öğrenmek istemesi için bir neden yokmuş gibi gözükse de, soruya yanıt vermemesi için de bir neden yoktu, öyle değil mi?

Ve arayanın aynı tesis içinden biri olduğunu sanan *Hücre On Kuzey*'de görevli memur, adamın resmi bir iş için aradığını düşünüyordu. İstediği oldukça mantıklıydı, bu yüzden Gondorff isimli tutukluyu telefona çağırdı. Sorun olmadı.

Bir dizi iyi planlanmış adımı bir araya getirip dalavereyi tamamlamışlardı.

Hızlı dosya indirme

Hukuk fakültesini bitirmelerinden on yıl sonra Ned Racine hâlâ, faturasını ödeyecek kadar parası olmayan insanların kıytırık işleriyle uğraşırken, sınıf arkadaşları, bahçeleri olan güzel evlerde yaşıyor, şehir klüplerine üye oluyor, haftada bir-iki kez golf oynuyorlardı. Sonunda bir gün Ned'in canına tak etti.

Şimdiye kadar elde ettiği tek iyi müşterisi, şirket birleşmeleri ve devirler konusunda uzmanlaşmış, küçük ama oldukça başarılı bir muhasebe şirketiydi. Uzun süredir Ned'le iş yapmıyorlardı. Ned müşterilerinin, gazetelerde çıkması halinde birkaç halka açık şirketin hisse senedi fiyatlarını etkileyebilecek bazı işlere karıştıklarını anlamıştı. Önemsiz, doğrudan işlem görmeyen hisselerdi ama bazı açılardan bu daha iyiydi; fiyatlardaki küçük bir fırlama yatırımlardan elde edilen büyük yüzdeli bir getiri anlamına geliyordu. Adamların dosyalarına ulaşıp neyle uğraştıklarını bir bulabilirse iş tamam olacaktı.

Alışılmadık yöntemler konusunda akıllı birini tanıyan bir arkadaşı vardı. Adam planı dinledi, gaza geldi ve yardım etmeyi kabul etti. Ned'in portföyündeki hisse senetleri yüzdesine bakıp her zaman aldığından daha küçük bir ücret karşılığında Ned'e ne yapması gerektiğini anlattı. Ayrıca ona piyasaya çıkalı çok az zaman olmuş küçük ve kullanışlı bir alet de verdi.

Birkaç gün boyunca Ned, muhasebe şirketinin gösterişsiz, mağaza vitrinine benzeyen bürosunun bulunduğu küçük iş hanının araba park

Mitnick Mesajı:

Sanayi casusları ve bilgisayarlara giren kişiler, hedef işletmelere bazen fiziksel olarak da girerler. İçeri girmek için bir demir sopa kullanmak yerine, toplum mühendisi kapının diğer tarafındaki insanı etkilemek için aldatma sanatını kullanır.

yerini gözetledi. Çoğu insan beş buçuk, altı gibi çıkıyordu. Yediye doğru park yeri tamamen boşalıyordu. Temizlikçiler yedi buçuk gibi geliyorlardı. Mükemmel.

Ertesi gece, sekize birkaç dakika kala, Ned otoparkın kaşısındaki yola arabasını park etti. Beklediği gibi temizlik hizmetleri şirketinin kamyonu sayılmazsa park yeri boştu. Ned kapıya kulağını koydu ve elektrikli süpürgenin gürültüsünü duydu. Sertçe kapıyı çaldı ve beklemeye başladı. Takım elbise giymiş, kravat takmıştı ve elinde yıpranmış çantasını taşıyordu. Yanıt gelmedi ama o sabırlıydı. Bir daha çaldı. Sonunda kapıda temizlikçilerden biri belirdi. "Merhaba", dedi Ned, cam kapının arkasından bağırarak ve daha önce şirket ortaklarından birinden aldığı kartviziti göstererek. "Anahtarlarımı arabama kilitlemişim, masama gitmem gerekiyor."

Adam kapıyı açtı, sonra Ned'in arkasından tekrar kilitledi ve koridora giderek Ned'in gittiği yeri görebilmesi için ışıkları açtı. Neden olmasın; ekmeğini kazanmasını sağlayan insanlardan birine yardımcı olmaya çalışıyordu. Böyle düşünmesi için her nedeni vardı.

Ned ortaklardan birinin bilgisayarının başına oturdu ve makinayı açtı. Bilgisayar açılırken ona verilen küçük aleti bilgisayarın USB girişine taktı. Bir anahtarlıkta taşınabilecek kadar küçük bir aletti, ancak yine de 120 megabayt veri taşıyabiliyordu. Ortağın sekreterinin bir Post-it kâğıda yazıp ekrana yapıştırdığı kullanıcı adını ve parolasını kullanarak ağa girdi. Beş dakikadan az bir sürede bilgisayarda ve ortakların ağ klasöründe yüklü tüm çizelge ve belge dosyalarını indirmiş evine gidiyordu.

Kolay para

Lisede ilk defa bilgisayarlarla tanıştığımda, Los Angeles'taki tüm okulların paylaştığı merkezi bir DEC PDP 11 minibilgisayarına modem aracılığıyla bağlanıyorduk. O bilgisayarda kurulu işletim sisteminin adı RSTS/E'ydi ve ilk kullanmayı öğrendiğim işletim sistemiydi.

O zamanlar, yani 1981'de DEC firması ürün kullanıcıları için yıllık bir konferans düzenliyordu ve bir yerde konferanslardan birinin Los Angeles'ta düzenleneceğini okudum. Bu işletim sisteminin kullanıcıları için hazırlanan tanınmış bir dergide LOCK-11 adlı yeni bir güvenlik ürününün duyurusu vardı. Ürün akıllıca hazırlanmış bir reklam kampanyasıyla sunuluyordu. "Saat sabah 3:30 ve sokağın ilersinde oturan Johnny sizin bağlantı numaranızı 336. denemesinde bulmuş, 555-0336. O içeri girmiş, sizi de dışarı sepetlemiş. Sizin de bir LOCK-11'iniz olsun." Reklamın anlattığına göre ürün bilgisayar korsanlarına karşı tam koruma sağlıyordu. Ve konferansta tanıtılıyor olacaktı.

Ürünü görmeyi ben de çok istiyordum. Yıllardır birlikte korsanlık yaptığımız, liseden sınıf arkadaşım ve dostum ama sonradan bana kar-

şı çalışan bir federal ihbarcı olan Vinny, yeni DEC ürününe yönelik ilgimi paylaşıyordu ve konferansa onunla birlikte gitmem için ısrar etti.

Peşin para

Ürün tanıtımına gittiğimizde LOCK-11'in çevresindeki kalabalıkta bir çalkalanma vardı. Görünüşe göre tasarımcılar kimsenin ürünlerini kıramayacağına dair anında ödeme yapacakları bir bahis oluşturmuşlardı. Bu reddedemeyeceğim bir meydan okumaydı.

Doğrudan LOCK-11'in tanıtım masasına gittik ve başında ürünün tasarımcıları olan üç adamın durduğunu gördük. Onları tanımıştım ve onlar da beni tanımışlardı; yetkililerle yaşadığım ilk gençlik sürtüşmelerimle ilgili Los Angeles Times gazetesinde çıkan büyük bir yazı nedeniyle, gençliğimde bile bir telefon beleşçisi ve bilgisayar korsanı olarak belli bir ünüm vardı. Yazıda anlatıldığına göre, gecenin bir yarısında Pasifik Telefon şirketi binasına girebilmek için kapıdakileri ikna etmiş ve güvenlik görevlilerinin burunlarının dibinden elimde bilgisayar kullanım kılavuzlarıyla çıkıp gitmiştim. (Görünüşe göre Los Angeles Times çarpıcı bir öykü çıkarmak istemişti ve adımı yayınlamak işlerine yaramıştı. Daha ergenlik çağında olduğum için, yazı, suç işleyen çocukların isimlerinin saklanması yasasını çiğnediğinden geleneklere aykırıydı.)

Vinny ve ben oraya gittiğimizde, bu her iki tarafta da bir ilgi uyandı. Karşı tarafta bir ilgi uyandırmıştı, çünkü benim gazetede okudukları korsan olduğumu anlamışlardı ve beni gördüklerine biraz şaşırmışlardı. Bizim tarafta da şaşkınlık yaratmıştı, çünkü tasarımcılardan her birinin yaka kartının arkasına bir 100 dolarlık banknot sıkıştırılmıştı. Sistemlerini kırabilecek kişiye verecekleri ödül 300 dolardı. Bu, bir çift okul çocuğu için çok para gibi görünüyordu. İşe koyulmak için sabırsızlanıyorduk.

LOCK-11 iki kademeli güvenliğe dayanan bilindik bir yöntemle tasarlanmıştı. Her zamanki gibi kullanıcının geçerli bir kimliği ve parolası olmalıydı ama buna ek olarak kimlik ve parola yalnızca yetkili uçbirimlerden girildiğinde işe yarıyordu. Bu yaklaşıma *uçbirim tabanlı güvenlik* deniyordu. Sistemi kırabilmek için bir korsanın yalnızca kimlik ve parolayı bilmesi yeterli değildi, bilgiyi doğru uçbirimden giriyor olması da gerekiyordu. İyi kurulmuş bir sistemdi ve LOCK-11'in yaratıcıları kötü adamları dışarıda tutacaklarından emindiler. Onlara bir ders verecek ve üstüne üstlük üç yüz dolar kazanacaktık.

Terimler

UÇBİRİM TABANLI GÜVENLİK: Kısmen belirli bir uçbirimin tanımlanmasına bağlı olarak kullanılan güvenlik; bu güvenlik yöntemi özellikle IBM'in büyük bilgisayarlarında çok kullanılırdı.

RSTS/E üstadı olarak bilinen ve benim de tanıdığım adamlardan biri bizden önce tanıtım masasına gelmişti. Yıllar ön-

Mitnick Mesajı:

İşte, akıllı insanların rakiplerini hafife almalarına bir örnek daha. Siz ne dersiniz? Siz de şirketinizin güvenlik önlemlerine, üzerlerine 300 dolar bahse girecek kadar güveniyor musunuz? Bazen teknolojik bir güvenlik önleminin çevresinden dolaşmanın tek yolu sizin düşündüğünüz şekilde değildir.

ce kendi arkadaşları beni geri çevirdikten sonra DEC dahili geliştirme bilgisayarına girmem konusunda bana meydan okuyan adamlardan biriydi. O günden bu yana saygın bir programcı olmuştu. Biz gelmeden önce LOCK-11'i kırmayı denediğini fakat başaramadığını öğrendik. Bu olayı tasarımcılara, ürünlerinin gerçekten sağlam olduğu konusunda büyük güven vermişti.

Yarışma çok basitti: Kırıyordun, parayı alıyordun. İyi bir tanıtım gösterisiydi; biri onları küçük düşürüp parayı almadığı sürece. Ürünlerinden o kadar eminlerdi ki tanıtım masasına sistemdeki bazı hesaplara ait kullanıcı adı ve parolaları içeren bir liste asma cüretini bile göstermişlerdi. Hiçbiri de öyle sıradan hesaplar değildi; yetkilerle donatılmış ayrıcalıklı hesaplardı.

Bu aslında kulağa geldiği kadar çarpıcı birşey değildi. Böyle bir düzenekte, her uçbirimin doğrudan bilgisayarın üstündeki girişlerden birine bağlandığını biliyordum. Konferans salonuna bir ziyaretçinin yalnızca ayrıcalıkları olmayan bir kullanıcı olarak bağlanabilmesine izin veren beş uçbirim kurduklarını anlamak için dâhi olmaya gerek yoktu. Diğer bir deyişle bu uçbirimlerden bağlanmak yalnızca sistem yöneticisi olmayan hesaplarla mümkündü. İki yol varmış gibi görünüyordu: Ya güvenlik yazılımını olduğu gibi bertaraf edecektik -ki bu LOCK-11'in tasarlanış amacıydı- ya da bir şekilde tasarımcıların düşünmediği bir şekilde yazılımın çevresinden dolaşacaktık.

Meydan okumaya karşılık vermek

Vinny ve ben oradan uzaklaşıp bahsi konuşmaya başladık ve benim aklıma bir plan geldi. Masum masum ortalıkta gezinip uzaktan tanıtım masasını gözlüyorduk. Öğlen olduğunda ve kalabalık azaldığında üç tasarımcı verilen aradan yararlanıp birlikte yemeğe gittiler ve geride aralarından birinin karısı ya da kız arkadaşı olabilecek bir kadın bıraktılar. Tekrar geri gittik ve ondan bundan konuşarak ben kadını oyalamaya başladım. "Ne kadar zamandır şirkette çalışıyorsunuz? Şirketinizin pazarda başka hangi ürünleri var?" gibi şeyler.

Bu sırada Vinny kadının görebileceği alanın dışında işe koyulmuş, her ikimizin de geliştirdiği bir becerisini kullanıyordu. Bilgisayarlara gir-

me çılgınlığımız ve sihirbazlığa duyduğum kendi ilgim dışında, ikimiz de kilit açmakla çok ilgileniyorduk. Küçükken San Fernando Vadisi'nde, kilit açma, kelepçelerden kurtulma, sahte kimlik yaratma gibi konulardabir çocuğun bilmemesi gereken her şeyle ilgili aykırı kitapların bulunduğu bir kitapçının raflarını didik didik etmiştim.

Vinny de benim gibi hırdavatçıdan alınmış herhangi bir sıradan kilidi açmak konusunda oldukça iyi olana kadar çalışmıştı. Bir ara kilitlerle ilgili şakalar yapmaya bayılırdım. Örneğin daha güvenli olsun diye iki kilit birden kullanan birini görürsem iki kilidi de açar, yerlerini değiştirirdim, bu da her birini yanlış anahtarla açmaya çalışan kilit sahibinin kafasını karıştırıp canını sıkardı.

Sergi salonunda ben genç kadını oyalarken Vinny masanın gerisinde görülmeyecek şekilde yere çökmüş, LOCK-11 minibilgisayarlarının ve kablo sonlarının durduğu dolabın kilidini açıyordu. Dolabın kilitli olduğunu düşünmeleri şaka gibiydi. Çilingirlerin gofret kilit dedikleri, bizim gibi oldukça acemi kilit açıcılar tarafından bile anahtarsız açması çok kolay olan kilitler kullanıyorlardı.

Vinny'nin kilidi açması bir dakika kadar sürdü. Dolabın içinde tam aradığı şeyi bulmuştu. Kullanıcı uçbirimlerini bağlamak için bir dizi bağlantı noktasının yanı sıra konsol uçbirimi için de ayrı bir bağlantı noktası vardı. Bu uçbirim, bilgisayarı işletmek ya da sistem yöneticisinin tüm bilgisayarları yönetmesi için kullanılıyordu. Vinny konsol bağlantısından çıkan bir kabloyu tanıtım masasındaki monitörlerden birine taktı.

Bu yaptığı, söz konusu uçbirimin artık bir konsol monitörü olarak tanınacağı anlamına geliyordu. Yeni bir kablo takılmış makinanın başına oturdum ve tasarımcıların korkusuzca verdikleri parolalardan birini kullanarak sisteme girdim. LOCK-11 yazılımı artık beni yetkili bir uçbirimden bağlanıyor olarak gördüğü için bana giriş izni vermişti ve bir sistem yöneticisinin yetkileriyle bağlanmıştım. Buradaki tüm uçbirimlerden ayrıcalıklı kullanıcı olarak bağlanmamı sağlayacak şekilde değiştirerek işletim sistemini yamaladım.

Gizli yamam yüklendikten sonra Vinny uçbirim kablosunu çıkarıp ilk takılı olduğu yere geri takma işini yaptı. Sonra kilidi yeniden kurcalayıp bu sefer dolabın kapısını kilitledi.

Bilgisayarda hangi dosyaların olduğunu görmek için bir dizin dökümü aldım. LOCK-11'in programına ve ilgili dosyalara bakarken çok şaşırtıcı bulduğum bir şeyle, bu bilgisayarda bulunmaması gereken bir dizinle karşılaştım. Tasarımcılar kendilerinden ve yazılımlarının aşılamaz olduğundan o kadar eminlerdi ki, yeni ürünlerinin kaynak kodlarını kaldırmaya bile yeltenmemişlerdi. Hemen yanındaki çıktı alma uçbirimine geçerek, kaynak kodunun parçalarını, o zamanlar kullanılan yeşil şeritli sürekli formlara bastırmaya başladım.

Vinny kilidi kapamayı yeni bitirmiş ve yanıma gelmişti ki adamlar öğle yemeğinden dönüyorlardı. Yazıcı yazmasını sürdürürken, beni bilgisayarın klavyesine birşeyler girerken buldular. "Ne yapıyorsun, Kevin?" diye sordu bir tanesi.

"Sadece kaynak kodlarınızın çıktısını aldırıyorum" dedim. Doğal olarak şaka yaptığımı düşündüler. Ta ki yazıcıya bakıp çıktıların gerçekten titizlikle korudukları ürünlerinin kaynak kodu olduğunu görünceye kadar.

Ayrıcalıklı kullanıcı olarak girdiğime inanamadılar. "Bir Kontrol-T gir", dedi tasarımcılardan biri. Girdim. Ekranda çıkan görüntü söylediklerimi doğruluyordu. Vinny, "Üç yüz dolar, lütfen", derken adam alnına vuruyordu.

Adamlar parayı ödediler. Günün kalanında Vinny ve ben konferans kartlarımıza taktığımız yüz dolarlık banknotlarla dolaştık. Herkes paraların ne anlama geldiğini biliyordu.

Vinny ve ben, doğal olarak, yazılımı yenmiştik ve eğer tasarım ekibi yarışma için daha iyi kurallar belirleselerdi ya da daha iyi bir kilit kullansalardı ya da teçhizatlarının başında dursalardı, o gün bir çift çocuğun elinden çektiklerini çekmeyeceklerdi.

Sonradan öğrendim ki tasarım ekibi para çekmek için bankaya uğramak zorunda kalmış. Bize verdikleri yüz dolarlık banknotlar yanlarında getirdikleri tüm paraymış.

Bir saldırı aracı olarak sözlük

Eğer biri parolanızı ele geçirirse sisteminizi işgal edebilir. Çoğu durumda neyin ters gittiğini bile anlamazsınız.

Adına İvan Peters diyeceğim genç bir saldırganın yeni bir oyunun kaynak kodunu ele geçirmek gibi bir hedefi vardı. Şirketin geniş alan ağına (WAN) girmekte zorlanmamıştı, çünkü bilgisayar korsanı arkadaşlarından biri şirketin internet sunucularından birini çoktan aşmıştı. Arkadaşı intranet yazılımında güncellenmemiş bir açık bulduktan sonra sistemin iki yönlü sunucu olarak kurulduğunu anlayınca neredeyse küçük dilini yutmuştu. Yani dahili ağa girmek için de bir giriş noktası bulunuyordu.

Ama İvan bağlandıktan sonra, Louvre müzesine girmek ve Mona Lisa'yı bulmaya çalışmakla eş değer bir zorlukla karşılaşmıştı. Müze haritası elinizde yoksa orada haftalarca gezinebilirdiniz. Şirket, yüzlerce ofisi ve binlerce bilgisayar sunucusu olan dünya çapında bir şirketti ve tam olarak geliştirme sistemlerine ait bir dizin sunmuyor ya da onu doğru yere götürecek bir tur rehberi de sağlamıyordu.

Hedeflediği sunucuyu bulmak için teknik bir yaklaşım kullanmak ye-

rine İvan bir toplum mühendisliği yaklaşımı kullandı. Bu kitapta açıklanan yöntemlere dayanan telefon görüşmeleri yaptı. Önce, Bilgi İşlem teknik destek servisini arayarak ekibiyle tasarladıkları üründe arayüz sorunu yaşayan bir şirket çalışanı olduğunu söyledi ve oyun geliştirme ekibinin proje liderinin telefon numarasını istedi.

Sonra kendisine verilen adı, Bilgi İşlemden biri gibi davranarak aradı. "Bu gece geç saatlerde bir yönlendiriciyi değiştireceğiz ve ekibinizin sunucuyla bağlantısının kopmayacağından emin olmak istiyoruz. Bunun için ekibinizin hangi sunucuyu kullandığını bilmemiz gerekiyor." Ağ sürekli yenileniyordu ve sunucunun adını vermenin hiçbir zararı olmazdı, öyle değil mi? Sunucu parola korumalı olduğuna göre yalnızca adını bilmek içeri girmeye çalışan birinin işine yaramazdı. Böylece adam saldırgana sunucunun adını verdi. Arayanın anlattıklarının doğru olup olmadığını kontrol etmeye ya da adamın adını soyadı ve telefonunu almaya yeltenmedi bile. Yalnızca sunucu adlarını verdi; ATM5 ve ATM6.

Parola saldırısı

Bu noktada İvan tanımlama bilgilerini almak için teknik bir yaklaşım kullandı. Uzaktan erişim kabiliyeti sunan sistemlere yapılan teknik saldırıların çoğunda ilk adım sisteme ilk giriş noktasını oluşturacak zayıf parolalı bir hesap bulmaktır.

Bir saldırgan parolaları uzaktan tanımlayacak korsanlık araçları kullanmaya kalkarsa, bu çabası onun şirketin ağına saatlerce bağlı kalmasını gerektirebilirdi. Açıkçası bunu yapması pek akıllıca olmazdı, çünkü ne kadar uzun süre bağlı kalırsa farkedilme ve yakalanma riski de o kadar artardı.

Hazırlık adımı olarak İvan hedef sistemin ayrıntılarını gösteren bir sayım yapacaktı. Bir kez daha internet bu amaç için gerekli yazılımı kolayca sağlıyordu (http://ntsleuth.0catch.com; "catch" kelimesinin başındaki sıfır). İvan, internet'te sayım sürecini otomatikleştiren ve herkese açık pek çok korsanlık aracı buldu. Kuruluşun çoğunlukla Windows tabanlı sunucular kullandığını bilerek, bir NetBIOS (temel giriş/çıkış sistemi) sayım programı olan NBTE'nin yazılımını indirdi. ATM5 sunucusunun IP adresini girdi ve programı çalıştırmaya başladı. Sayım programı sunucuda tanımlı pek çok hesap bulmuştu.

Terimler

SAYIM: Hedef sistemde sunulan hizmetleri, işletim sistemi tabanını ve sisteme erişimi olan kullanıcıların hesap adlarının listesini veren bir süreç.

Var olan hesaplar belirlendikten sonra, aynı sayım aracının bilgisayar sistemine sözlük saldırısı yapma özelliği kullanılabilirdi. Sözlük saldırısı çoğu bilgisayar güvenliği çalışanının ve saldırganların oldukça yakından bildikleri bir şeydir ama pek çok kişi bunun mümkün ol-

duğunu duyunca herhalde şaşkına uğrayacaktır. Bu tarz bir saldırı, sistemdeki her kullanıcının parolasını sıkça kullanılan kelimeleri tarayarak ortaya çıkarmaya yöneliktir.

Bazı şeyleri yapmak konusunda tembellik edebiliyoruz ama parolalarını seçerlerken insanların yaratıcılıklarının ve hayal güçlerinin kaybolduğunu görmek beni hep hayrete düşürmüştür. Çoğumuz bize koruma sağlayan bir parola isteriz ama aynı zamanda kolay hatırlanmasını da isteriz ve bu genellikle kendimize yakın şeyler olması anlamına gelir. Adımızın baş harfleri, göbek adımız, lâkabımız, eşimizin adı, en sevdiğimiz şarkı, film ya da yemek olabilir. Oturduğumuz sokağın adı ya da yaşadığımız şehrin adı, kullandığımız arabanın markası, Hawai'de kalmak istediğimiz sahildeki tatil köyünün adı ya da en iyi alabalıkları avladığımız en sevdiğimiz akarsuyun adı. Burada çıkan deseni gördünüz mü? Bunlar çoğunlukla kişi adları, yer adları ya da sözlükte bulunabilecek sözcükler. Bir sözlük saldırısı, sık kullanılan kelimeleri hızlı bir şekilde girerek her birinin bir ya da daha fazla kullanıcı hesabının parolası olup olmadığına bakar.

İvan sözlük saldırısını üç basamakta çalıştırdı. İlkinde yaklaşık 800 kelimelik en sık kullanılan parolalardan oluşan basit bir liste kullandı. Bu listede gizli, iş ve parola kelimeleri de vardı. Program ayrıca sözlük kelimelerinin yanına sayı ekleyerek ya da içinde bulunan ayın sayısını girerek sıra değişiklikleri de yapıyordu. Program her kelimeyi belirlenmiş tüm kullanıcı hesaplarında deniyordu. İşe yaramadı.

Sonraki denemesinde İvan, Google arama motoruna gitti ve "sözcük listeleri sözlükler" anahtar kelimeleriyle arama yaptı. İngilizce ve pek çok yabancı dil için kapsamlı sözcük listeleri ve sözlükler bulunan binlerce site buldu. Bir İngilizce sözlüğün tümünü indirdi. Sonra Google'da bulduğu bazı sözcük listelerini de indirerek elindekileri zenginleştirdi. İvan www.outpost9.com/files/WordLists.html sitesini seçmişti.

Bu site ona, aralarında soyadların, adların, kongre üyelerinin adlarının ve ilgili kelimelerin, oyuncuların adlarının, İncil'den kelimelerin ve adların olduğu, indirilebilecek (hepsi de ücretsiz) bir dizi dosya sunuyordu.

Sözcük listeleri sunan pek çok siteden biri de aslında Oxford Üniversitesinin sitesiydi; ftp://ftp.ox.ac.uk/pub/wordlists.

Diğer siteler çizgi film karakterlerini, Shakespeare'in kullandığı sözcükleri, Odyssea'da geçen kelimeleri, Tolkien ve Uzay Yolu dizisinin yanı sıra bilim ve dinle ilgili olanları da içeren başka listeler de sunuyorlardı. (Bir şirket 4,4 milyon sözcük içeren bir listeyi yalnızca 20 dolara satmakta.) Saldırı programı sözlükteki kelimelerin anagramlarını -pek çok bilgisayar kullanıcısının güvenliklerini artırdığını düşündüğü, sevilen bir yöntemdir- deneyecek şekilde de programlanabilir.

Düşündüğünden daha hızlı

İvan hangi sözcük listesini kullanacağına karar verdikten sonra saldırıya geçti. Yazılım otomatik olarak çalışıyordu ve İvan dikkatini başka şeylere verebilirdi. İşin inanılmaz tarafı ise şuydu: Böyle bir saldırı sırasında bilgisayar korsanının Rip van Winkle gibi uykuya dalacağını ve uyandığında yazılımın daha küçücük bir yol katetmiş olacağını düşünebilirsiniz. Aslında, saldırılan işletim sistemi tabanına, sistemin güvenlik ayarlarına ve ağ bağlantısına bakılarak İngilizce sözlükte bulunan bütün sözcükler -şaşılacak şekilde- otuz dakikadan az bir süre içerisinde denenebilir!

Bu saldırı sürerken İvan başka bir bilgisayardan geliştirme grubunun kullandığı diğer sunucu olan ATM6'ya benzer bir saldırı başlattı. Yirmi dakika sonra saldırı yazılımı hiçbir şeyin farkında olmayan kullanıcıların çoğunun olanaksız olduğunu düşündüğü bir işi başardı. Yazılım kullanıcılardan birinin, Yüzüklerin Efendisi kitabındaki Hobbitlerden birinin adı olan "Frodo" kelimesini parola olarak kullandığını bulmuştu.

İvan, elinde bu parolayla bu kullanıcının hesabından ATM6 sunucusuna bağlandı.

Saldırganımız için hem iyi hem de kötü haberler vardı. İyi haber, kırdığı hesabın, bir sonraki adımda önemli olacak yönetici özellikleri olmasıydı. Kötü haber ise oyunun kaynak kodu hiçbir yerde yoktu. O zaman diğer makinada, sözlük saldırısına karşı dirençli olduğunu anladığı ATM5'te olmalıydı. Ama İvan'ın vazgeçmeye niyeti yoktu, denemediği birkaç numarası daha vardı.

Bazı Windows ve Unix işletim sistemlerinde şifrelenmiş parolalar, yüklü oldukları bilgisayara erişimi olan herkese açıktır. Bunun nedeni şifreli parolaların kırılamaması ve bu yüzden korumaya gerek olmamasıdır. Bu kuram yanlıştır. Yine internette bulunabilen pwdump3 adlı başka bir araçla İvan, ATM6 makinasındaki şifrelenmiş parolaları bulup indirdi.

Tipik bir şifrelenmiş parola dosyası aşağıdaki gibidir:

```
Administrator:500:95E4321A38AD8D6AB75EOC8D76954A50:
2E48927AOBO4F3BFB341E26F6D6E9A97:::

akasper:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393C
E7F90A8357F157873D72D0490821: : :

digger:1111:5D15COD58DD216C525AD3B83FA6627C7:17AD
564144308B42B8403DOIAE256558: : :

ellgan:1112:2017D4A5D8D1383EFF17365FAFIFFE89:O7AEC9
50C22CBB9C2C734EB89320DB13: : :

tabeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1FO11
5A728447212FCO5EID2D820B35B: : :
```

vkantar:1116:81A6A5DO35596E7DAAD3B435B51404EE:B93
3D36DD12258946FCC7BD153F1CD6E : : :

vwallwick:1119:25904EC665BA30F4449AF42E1054F192:15B
2B7953FB632907455D2706A432469 : : :

mmcdonald:1121:A4AEDO98D29A3217AAD3B435B51404EE:
E40670F936B79C2ED522F5ECA9398A27 : : :

kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DE
C8E827A121273EFO84CDBF5FD1925C : : :

İvan bilgisayarına indirdiği şifrelenmiş parolalara, başka bir araç kullanarak kaba kuvvet *(brute force)* olarak bilinen farklı bir parola saldırısı yaptı. Bu tarz saldırılar alfanümerik karakterlerin ve çoğu özel simgenin kombinasyonlarını dener.

İvan, L0phtcrack3 adlı bir yazılım kullandı. ("loft-krak şeklinde okunur ve www.atstake.com sitesinde bulunabilir; bazı mükemmel parola ele geçirme araçları için başka bir kaynak da www.elcomsoft.com 'dur.) Sistem yöneticileri L0phtcrack3 yazılımını zayıf parolaları denetlemek için, saldırganlar ise parolaları kırmak için kullanırlar. LC3 harf, sayı ve aralarında !@#$%^& gibi simgelerin de bulunduğu karakter kombinasyonlarıyla parolaları yoklar (Ancak, dikkat edilmelidir ki, yazıcıdan bastırılamayacak karakterler kullanıldığında LC3 parolayı bulmayı başaramaz).

Programın neredeyse inanılmaza yakın bir hızı vardır. İşlemcisi 1 GHz olan bir makinada hızı saniyede 2,8 milyon denemeye kadar çıkabilmektedir. Bu hızda bile, eğer sistem yöneticisi Windows işletim sisteminde doğru ayarlamaları yaptıysa (LANMAN şifreli parolalarının kullanılmasını iptal etmek gibi), bir parolanın kırılması yine de oldukça uzun bir zaman alabilir.

Bu nedenle saldırgan sık sık parola dosyalarını indirir ve hedef şirketin ağına bağlı kalıp farkedilme riskini artırmaktansa çözümlemeyi kendi bilgisayarında ya da başka bir bilgisayarda yapar.

İvan için, bekleyiş o kadar uzun sürmedi. Birkaç saat sonra, kullandığı yazılım, geliştirme ekibi üyelerinin her birine ait parolaları verdi. Ama bunlar ATM6 makinasının kullanıcılarının parolalarıydı ve İvan peşinde olduğu kaynak kodlarının bu sunucuda olmadığını zaten biliyordu.

Şimdi ne olacaktı? Daha ATM5 makinesinde bulunan bir hesabın parolasını bulmayı başaramamıştı. Bilgisayar kor-

Terimler

KABA KUVVET SALDIRISI: Alfanümerik karakterlerin ve özel simgelerin mümkün olan her kombinasyonunu deneyen bir parola belirleme stratejisi.

sanlarına özgü düşünme şeklini kullanarak ve sıradan kullanıcıların zayıf güvenlik alışkanlıklarını anlamış biri olarak, ekip üyelerinden birinin her iki makina için de aynı parolayı kullanıyor olabileceğini düşündü.

Tam tahmin ettiği gibiydi. Ekip üyelerinden biri "oyuncular" olan parolasını hem ATM5'de hem de ATM6'da kullanıyordu.

Aradığı programları bulabilmesi için kapı ardına kadar açılmıştı. Kaynak kodu klasörünü bulduktan ve onu zevkle indirdikten sonra sistem kıranlara özgü bir adım daha attı. İleride yazılımın güncellenmiş sürümünü almak isteyebileceğini düşünerek yönetici hakları olan ama kullanılmayan bir hesabın parolasını değiştirdi.

Aldatmacanın incelenmesi

Hem teknik hem de insan kaynaklı açıklardan faydalanan bu saldırıda saldırgan, tescilli bilgileri tutan geliştirme sunucularının adlarını ve yerlerini öğrenmek için sahte bir telefon görüşmesi yapmıştı.

Sonra, geliştirme sunucusunda hesabı olan herkesin geçerli hesap adlarını belirlemek için bir yazılım kullandı. Sonra da birbiri ardına iki parola saldırısı gerçekleştirdi. Bunların arasında, bir İngilizce sözlükte bulunan tüm kelimeleri deneyerek sıkça kullanılan parolaları arayan sözlük saldırısı da vardı. Bazen bu sözlük, adlar, yerler ve özel ilgi alanları içeren pek çok başka sözcük listesiyle desteklenebilir.

Hem ticari hem de halka açık korsanlık araçları, akla gelen herhangi bir amaç için kullanabilmek üzere herkes tarafından elde edilebildiklerinden, yatırımlarınız olan bilgisayar sistemlerini ve ağ altyapınızı kororken uyanık davranmanız oldukça önemlidir.

Bu tehlikenin boyutu abartılmış değildir. Computer World dergisine göre, New York merkezli Oppenheimer Fonları'nın incelenmesinden şaşırtıcı bir bulgu elde edilmiştir. Şirketin Ağ Güvenliğinden Sorumlu Genel Müdür Yardımcısı, standart yazılım paketleri kullanarak şirket çalışanlarına bir parola saldırısı yapmıştır. Dergideki yazıya göre üç dakika içerisinde 800 çalışanın parolası kırılmıştır.

Mitnick Mesajı:

Monopol oyununun terimleri gibi, parolanız için sözlükten aldığınız bir kelime kullanırsanız sonuç, Hemen Hapse Git; Başlangıçtan Geçme, 200 Dolar Alma şeklinde olur. Çalışanlarınızı, varlıklarınızı gerçekten koruyacak parolalar seçmeleri konusunda eğitmelisiniz.

Aldatmacanın engellenmesi

Toplum mühendisliği saldırıları teknolojik bir unsur eklendiğinde daha tehlikeli bir hal alabilmektedir. Bu tarz bir saldırıyı engellemek, genellikle hem insan boyutunda hem de teknik boyutta önlem almayı gerektirir.

Hayır demeyi öğrenin

Buradaki ilk öyküde telefon şirketinin RCMAC memuru, değişimi onaylayan hizmet emirleri yokken on telefon hattının reddet-kes durumunu kaldırmamalıydı. Çalışanların güvenlik kurallarını ve süreçlerini bilmeleri yeterli değildir; bu kuralların, zararın oluşmasını engellemek için ne kadar önemli olduğunu da anlamış olmaları gerekir.

Güvenlik kuralları süreçlerinin uygulanması bir ödül-ceza sistemi içerisinde teşvik edilmelidir. Doğal olarak kurallar esnek olmalı ancak göz ardı edilme olasılıkları yüksek, sorumluluk gerektiren adımları atma işini çalışanlara bırakmamalıdır. Ayrıca bir güvenlik bilinci programı, güvenlik süreçlerinin çevresinden dolaşan kısayollar kullanmanın -her ne kadar alınan işleri zamanında tamamlamak önemli olsa da- şirket ve çalışanlar için yıkıcı olabileceği konusunda ikna edici olmalıdır.

Aynı dikkat telefonda yabancı birine bilgi verirken de gösterilmelidir. Arayan kendini ne kadar ikna edici bir tarzda tanıtırsa tanıtsın, şirketteki deneyiminden ve konumundan bağımsız olarak, kimliği onaylanana kadar, ona herkese açık olarak belirlenmiş bilgiler dışında bilgi verilmemelidir. Eğer bu kurala sıkı bir şekilde uyulsaydı, bu öyküde geçen toplum mühendisliği oyunu başarısız olur ve federal tutuklu Gondorff bir daha arkadaşı Johnny'le birlikte kimseye yeni bir oyun oynayamazdı.

Şu husus o kadar önemli ki bu kitapta bunu sürekli yineliyorum: Kontrol, kontrol, kontrol. Yüzyüze yapılmamış herhangi bir istek, istek sahibinin kimliğini kontrol etmeden yerine getirilmemelidir; nokta.

Temizlik

Yirmi dört saat çalışan güvenlik görevlileri olmayan şirketler için saldırganın mesai saatlerinden sonra ofise girmesi ciddi bir sorundur. Temizlikçiler, şirketten gibi görünen ve bir tuhaflık görmedikleri herkese çoğunlukla saygıyla davranırlar. Ne de olsa bu kişi onların başını belaya sokabilecek ya da onları işten attırabilecek biridir. Bu yüzden ister şirket elemanı olsunlar, ister taşeron bir temizlik şirketinden geliyor olsunlar, temizlik ekipleri fiziksel güvenlik konularında eğitilmelidirler.

Temizlik işinin üniversite diploması gerektirdiği söylenemez, hattâ İngilizce konuşmayı bile gerektirmez ve verilen eğitimler, eğer varsa, farklı işler için ne tür temizlik malzemeleri kullanılacağı gibi güvenlikle il-

gisi olmayan konularda olurlar. Genellikle bu insanlar, "Eğer mesai saatleri dışında kendisini içeri almanızı isteyen biri olursa, şirket kimlik kartını göstermesi şarttır. Sonra sizin temizlik şirketini arayıp, durumu anlatmanız ve karşı tarafın size izin vermesini beklemeniz gerekir", gibi talimatlar almazlar.

Bir kuruluşun -başına gelmeden önce- bu bölümde anlatılan durumlara karşı hazırlıklı olması ve çalışanlarını ona göre eğitmesi gerekir. Gördüğüm kadarıyla, hepsi olmasa da, özel sektör işletmelerinin çoğu fiziksel güvenliğin bu boyutu konusunda fazlasıyla gevşek davranıyorlar. Soruna diğer yönden yaklaşıp sorumluluğu şirketin kendi çalışanlarına da yükleyebilirsiniz. Yirmi dört saat güvenlik hizmeti olmayan bir şirket, mesai saatleri dışında iş yerine gelen çalışanlarına kendi anahtarlarını ve manyetik giriş kartlarını getirmelerini şart koşabilir. Temizlik görevlilerine hiçbir zaman birini içeri almamaları konusunda kesin talimatlar verebilir. Temizlik şirketine de içeriye kimseyi almamaları konusunda çalışanlarının her zaman eğitimli olmaları gerektiğini hatırlatabilirsiniz. Şu basit bir kuraldır: Kapıyı kimseye açmayın. Eğer bu uygunsa, temizlik şirketi sözleşmesinin maddelerinden biri olarak yazıya dökülebilir.

Temizlik ekipleri aynı zamanda birinin arkasından geçme teknikleriyle ilgili de eğitilmelidirler. Ayrıca birinin, bir şirket çalışanına benziyor diye, hemen peşlerinden binaya girmeye çalışmasına izin vermeyecek şekilde de bilgilendirilmeliler.

Arada bir -örneğin yılda üç ya da dört kere- içeri girme testleri ve açıklık değerlendirmeleri yapın. Temizlik ekibi çalışırken kapıya birini gönderin ve o kişi temizlikçileri ikna ederek içeri girmeye çalışsın. Bu iş için kendi çalışanlarınızı kullanmaktansa bu tarz içeri girme testlerinde uzmanlaşmış şirketlerle çalışmayı tercih edin.

Kulaktan kulağa: Parolalarınızı gizli tutun

Giderek daha çok şirket teknik yöntemlere dayanan güvenlik kurallarını uygulamaya geçiriyor. Örneğin, parola kurallarını denetleyecek şekilde işletim sistemi ayarlanabilir ve hesabı kilitlemeden önce başarısız parola giriş denemelerinin sayısı sınırlandırılabilir. Aslında Microsoft Windows'un işletmelere yönelik sürüm paketlerine bu özellik genellikle mevcuttur. Ancak daha fazla çaba gerektiren özelliklerden müşterilerin ne kadar çabuk sıkıldığı görülünce, ürünler güvenlik ayarları kapalı olarak sunulmaya başlandı. Yazılım şirketlerinin -tam tersi olması gerekirken- ürünlerini güvenlik ayarları kapatılmış olarak teslim etmeyi durdurmasının tam zamanıymış gibi görünüyor. (Sanırım yakında bunu kendileri de anlayacaklar.)

Şirket güvenlik kurallarının, kolay yanılabilen insanlara gereğinden fazla bel bağlamamak amacıyla, mümkün olduğunca teknolojik güven-

lik unsurlarını uygulamaları konusunda sistem yöneticilerine dayatmada bulunması son derece doğaldır. Örneğin belirli bir hesapta birbiri ardına yapılan başarısız giriş denemelerinin sayısını sınırlamanın bir saldırganın işini oldukça zorlaştıracağını görmek çok fazla kafa yormayı gerektirmez.

Her kuruluş, sağlam güvenlik ve çalışan üretkenliği arasındaki hassas dengeyi korumak zorundadır. Bu, bazı çalışanların güvenliği hiçe saymalarına, alınan önlemlerin hassas şirket bilgilerini korumada ne kadar önemli olduğunu görememelerine neden olur.

Eğer şirket kurallarının değinmediği bazı konular varsa, çalışanlar en az zorluk çekecekleri yoldan, işlerini kolaylaştıracak en uygun hareketi yaparak görevlerini yerine getirebilirler. Bazı çalışanlar değişime direnç gösterebilir ve doğru güvenlik alışkanlıklarını açık açık hiçe sayabilir. Basit olmayan ve uzun parola kurallarına uyan ama sonra da parolasını bir not kâğıdına yazıp meydan okurcasına bilgisayarının ekranına yapıştıran çalışanlarla karşılaşmışsınızdır.

Şirketinizi korumanın en etkili yollarından biri, teknik altyapınızda, güçlü güvenlik ayarlarının yanı sıra keşfedilmesi zor parolalar kullanmaktır.

Parola kurallarıyla ilgili ayrıntılı değerlendirmeleri 16. bölümde bulabilirsiniz.

12 İŞE YENİ GİRENLERE SALDIRILAR

Burada anlatılan öykülerin çoğunun da gösterdiği gibi becerikli bir toplum mühendisi çoğunlukla kurum içi yetki sıralamasında alt seviyede olan çalışanları hedefler. Bu insanları, hassas şirket bilgilerine saldırganı bir adım daha yaklaştıracak, zararsız gibi görünen bilgileri vermeleri doğrultusunda yönlendirmek kolaydır.

Bir saldırganın işe yeni başlamış çalışanlara saldırmasının nedeni, onların çoğu zaman belirli şirket bilgilerinin ya da bazı hareketlerin olası sonuçlarının farkında olmamalarıdır. Ayrıca en bilinen toplum mühendisliği tekniklerinden bazılarıyla kolayca etki altına girme eğilimindedirler; yetkili kişi izlenimi uyandıran biri, arkadaş canlısı ve sevimli duran biri, şirkette kurbanın da tanıdığı kişileri tanıyan biri, saldırganın isteklerinin çok acil olduğuyla ilgili bir talep ya da kurbanın bir yardım göreceğine ya da göze gireceğine yönelik edindiği bir kanı gibi.

Şimdi de iş başındaki alt seviye çalışanlara yapılan saldırılara bazı örnekler verelim.

Yardımsever Güvenlik Görevlisi

Dolandırıcılar açgözlü birini bulmaya çalışırlar çünkü dolandırılma olasılıkları yüksek olanlar onlardır. Toplum mühendisleri temizlik ekibinden ya da güvenlik görevlilerinden birini seçerken iyi huylu, arkadaş canlısı ve güvenilir birini bulmayı umarlar. Çünkü en büyük olasılıkla yardım etmeyi isteyebilecekler onlardır. Aşağıda anlatılan öyküde saldırganın aklından geçen de tam böyle bir şeydir.

Elliot'un Bakış Açısı

Gün/Saat: Şubat 1998, Salı, sabah 03:26.
Yer: Marchand Mikrosistemler tesisi, Nashua-New Hampshire

Elliot Stanley saat başı çıkması gereken devriyeler dışında yerinden ayrılmaması gerektiğini biliyordu. Ama gecenin bir yarısı olmuştu ve mesaisi başladığından beri tek bir kişi bile görmemişti. Telefondaki zavallı adamın sesi gerçekten yardıma ihtiyacı varmış gibi geliyordu. Ve birilerine küçük bir iyilik yapmak insanın her zaman kendini daha iyi hissetmesini sağlıyordu.

Bill'in Öyküsü

Bill Goodrock'un çok basit, hiç değişmeden on iki yaşından beri bağlandığı tek bir amacı vardı: Yirmi dört yaşına gelmeden ve kendi birikimlerinin tek kuruşuna dokunmadan emekli olmak. Kendi başına da başarılı olabileceğini, her şeye kâdir, huysuz babasına gösterecekti.

İki yıl kalmıştı ve gelecek yirmi dört ayda başarılı bir iş adamı ve zeki bir yatırımcı olarak zengin olamayacağı oldukça açıktı. Bir ara silahla banka soymayı da düşünmüş ama bunun hikâyelerde kalması gerektiğine ve tehlike-kazanç dengesinin berbat olduğuna karar vermişti. Onun yerine, Rifkin gibi, bir bankayı elektronik olarak soymanın hayallerini kuruyordu.

Bill en son ailesiyle birlikte Avrupa'ya gittiğinde Monaco'da 100 franklık bir banka hesabı açtırdı. Yüz frank orada duruyordu ama o paranın bir anda yedi basamaklı olmasını sağlayacak bir planı vardı. Eğer şansı yaver giderse bu miktar sekiz basamaklı bile olabilirdi.

Bill'in kız arkadaşı Annemarie büyük bir Boston bankasında birleşme ve devirler bölümünde çalışıyordu. Bir gün kız arkadaşının ofisinde, onun geç saatlere kalmış bir toplantıdan çıkmasını beklerken, merakını yenemedi ve kendi dizüstü bilgisayarını, içinde beklediği konferans salonundaki ethernet girişine bağladı. İşte! Dahili ağa, bankanın ağına bağlanmıştı... hem de güvenlik duvarının arkasından. Aklına bir fikir geldi.

Başarılı bir bilgisayar mühendisliği doktorası yapmakta olan ve Marchand Microsystems'da staj yapan Julia adında genç bir kadını tanıyan bir sınıf arkadaşıyla yeteneklerini bir araya getirdiler. Julia içerden önemli bilgiler edinmek için iyi bir kaynak gibi görünüyordu. Kadına bir film senaryosu yazdıklarını söylediler ve Julia onlara inandı. Onlarla bir öykü yazmanın eğlenceli olduğunu düşünüyordu ve anlattıkları dümenin nasıl çevrileceğiyle ilgili tüm ayrıntıları onlara anlattı. Fikrin çok iyi olduğunu düşünüyor ve film yazılarında adının geçmesi için sürekli kafalarını ütülüyordu. Onu senaryoların nasıl sık sık çalındığıyla ilgili uyardılar ve bunları kimseyi anlatmaması için yemin ettirdiler.

Julia tarafından iyi yetiştirilmiş olarak işin tehlikeli kısmını Bill kendi yaptı ve işi kotarabileceğinden hiç kuşku duymadı. Kendi ağzından dinleyelim:

Öğleden sonra telefon ettim ve gece güvenlik amirinin adının İsaiah Adams olduğunu öğrenmeyi başardım. Gece 21:30'da binayı aradım ve giriş güvenlik masasında duran bekçiyle konuştum. Hikâyem tamamen aciliyete dayalıydı ve biraz telaşa kapılmış gibi konuştum. "Arabamla ilgili bir sorun çıktı ve tesise gelemiyorum" dedim. "Acil bir durum var ve gerçekten yardıma ihtiyacım var. Güvenlik amiri İsaiah'ı aramayı denedim ama evde değil. Bana bir kerelik yardımcı olabilir misiniz, çok makbule geçecek."

Geniş tesisteki odaların her biri numaralıydı, böylece adama bilgisayar laboratuvarının numarasını verdim ve yerini bilip bilmediğini sordum. Bildiğini söyledi ve benim için oraya gitmeyi kabul etti. Odaya gitmesi birkaç dakikasını alacaktı. Tek bir telefon hattım olduğunu ve onu da sorunu çözmek için ağa bağlanmakta kullandığım gibi bir bahaneyi öne sürerek onu laboratuvardan arayacağımı söyledim.

Aradığımda oraya varmış beni bekliyordu. Ona üzerinde "elmer" yazan bir etiket olan uçbirimi nerede bulacağını açıkladım. Bu, Julia'nın anlattığına göre, şirketin pazarladığı işletim sistemlerinin piyasa sürümlerinin yapıldığı ana bilgisayardı. Bekçi bilgisayarı bulduğunu söylediğinde Julia'nın bize doğru bilgi verdiğini anladım ve içim bir hoş oldu. Birkaç kere Enter tuşuna basmasını söyledim, o da bana ekrana pound (£) işaretlerinin çıktığını söyledi. Bu işaret, sunucuya tüm sistem yetkilerinin olduğu süper-kullanıcı hesabından girildiğini gösteriyordu. Bekçi, klavyede tek parmak yazıyordu ve ben ona, biraz zorlu olan bir sonraki komutu söylerken kan ter içinde kaldı.

```
echo 'fix:x:0:0::/:/bin/sh' >> /etc/passwd
```

Sonunda doğru girmeyi başardı ve böylece hesaplardan birinin adını değiştirdik. Sonra ona şu komutu girmesini söyledim:

```
echo 'fix: :10300:0:0' 55 /etc/shadow
```

Bu komut, iki nokta üst üstelerin arasındaki şifreli parolayı oluşturdu. İki nokta üstüstelerin arasına hiçbir şey koymamak parolanın olmayacağı anlamına gelir. Bu yüzden, hesaptaki düzeltmeyi boş bir parola kullanarak parola dosyasına eklemek için bu iki komut yetmişti. Daha da iyisi, bu hesap da süper-kullanıcı yetkilerine sahip olacaktı.

Bunun ardından ondan yapmasını istediğim şey, dosya adlarının uzun bir listesini çıkaran tekrarlanan bir dizin komutu oldu. Sonra kâğıdı ileri doğru beslemesini, yırtmasını ve yanına alıp bekçi kulübesine dönmesini söyledim, çünkü daha sonra oradan bana birşeyler okumasını isteyebilirdim.

İşin güzel yanı bekçinin yeni bir hesap açtığından haberi yoktu. Ona dizinlere göre dosya adlarını bastırtmıştım, çünkü daha önce yazdığı

NOT: *Burada kullanılan arka kapı, işletim sistemi giriş programını değiştiren türden değil. Daha doğrusu giriş programının kullandığı dinamik kitaplıktaki belirli bir işlev, gizli bir giriş noktasını yaratacak şekilde değiştiriliyor. Sıradan saldırılarda saldırganlar çoğunlukla ya giriş programını değiştirirler ya da doğrudan ona yama yaparlar ama dikkatli sistem yöneticileri programı yükleme cd'sinde ya da başka dağıtım ortamlarında bulunan şekliyle karşılaştırarak değişikliği fark edebilirler.*

Terimler

YAMA: Çalıştırılabilir bir programa yerleştirildiğinde, var olan sorunu çözen bir program parçacığı.

komutların bilgisayar odasından onunla birlikte çıkmasını istiyordum. Böylece sistem yöneticisi ya da işletmeni ertesi sabah bir güvenlik ihlali olduğuna dair hiçbir şey fark etmeyecekti.

Artık bir hesabım, parolam ve tam yetkim vardı. Geceyarısından az önce sisteme telefonla bağlandım ve Julia'nın "film senaryosu için" özenle yazdığı komutları girmeye başladım. Göz açıp kapayıncaya kadar şirketin işletim sistemi yazılımının yeni sürümünün kaynak kodunun ana kopyasının durduğu geliştirme sistemine erişmiştim.

Julia'nın yazdığı ve işletim sistemi kitaplıklarından birindeki bir altprogramı değiştirdiğini söylediği yamayı yükledim. Aslında bu yama, sisteme gizli bir parola kullanarak uzaktan erişim sağlayacak bir arka kapı oluşturuyordu.

Julia'nın benim için yazdığı talimatları özenle uygulayarak, önce yamayı yükledim; sonra da, yaptıklarımdan geriye hiçbir iz kalmayacak şekilde düzeltme hesabını kaldıran ve tüm denetleme günlüklerini tertemiz eden adımlar atıp etkili bir şekilde izlerimi yokettim.

Yakında şirket yeni işletim sistemi güncellemelerini, dünya çapında finansal kuruluşlar olan müşterilerine göndermeye başlayacaktı. Ve gönderdikleri her kopya, gönderilmeden önce ana dağıtım sürümüne yerleştirdiğim arka kapıyı içerecekti. Böylece güncellemeyi yükleyen her bankanın ve menkul değerler şirketinin bilgisayar sistemine erişmemi sağlayacaktı.

Henüz tam olarak hedefime varmamıştım, yapacak daha çok işim vardı. "Ziyaret" etmek istediğim her finansal kurumun dahili ağına girmem gerekiyordu. Sonra hangi bilgisayarlarını para havaleleri için kullandıklarını bulmam ve yaptıkları işlemlerin ayrıntılarını ve parayı tam olarak nasıl havale ettiklerini öğrenebilmek için gözetleme yazılımları yüklemem gerekecekti.

Bunları tümünü uzaktan, herhangi bir yerdeki bir bilgisayardan yapabilirdim. Örneğin bir deniz kıyısından. Bekle beni Tahiti, geliyorum.

Yeniden bekçiyi aradım, yardımları için teşekkür ettim ve ona dökümü çöpe atabileceğini söyledim.

Aldatmacanın İncelenmesi

Güvenlik görevlisinin görevleriyle ilgili aldığı talimatlar vardı ama ne kadar ayrıntılı ve iyi düşünülmüş de olsalar bu talimatlar her olası durumu öngörmüyordu. Şirket çalışanı olduğunu düşündüğü biri için bir bilgisayara birkaç komut girmesinin yaratabileceği zarardan kimse ona söz etmemişti.

Mitnick Mesajı:

Bir saldırgan bir bilgisayar sistemine ya da ağına kendi ulaşamıyorsa, bunu yapması için başka birisini bulmaya çalışacaktır. Planın yürütmesi için fiziksel girişlerin zorunlu olduğu durumlarda kurbanı aracı olarak kullanmak, işi kendisinin yapmasından daha iyi bile olabilir, çünkü saldırgan böylece farkedilme ve yakalanma tehlikesini oldukça azaltabilir.

Her ne kadar güvenli bir laboratuvarın kilitli kapısının arkasında da olsa, bekçinin de işbirliğiyle, dağıtım kopyasınının saklandığı kritik sisteme erişim oldukça kolay olmuştu. Bekçinin elinde, doğal olarak, tüm kilitli kapıların anahtarları vardı.

Aslında dürüst olan bir çalışan bile (hikâyemizde doktora öğrencisi ve şirket stajyeri olan Julia) bir toplum mühendisliği saldırısı için can alıcı öneme sahip bilgileri vermesi için kandırılabilir ya da bunu yapması için ona para yedirilebilir. Örneğin hedef bilgisayar sisteminin nerede olduğu ve -bu saldırının başarısı için çok önemli olan- yazılımın yeni sürümünün ne zaman dağıtıma çıkacağı gibi bilgileri verebilirler. İşletim sisteminin temiz bir kaynaktan yeniden yapılandırıldığı durumda, bu tarz bir değişikliğin çok erken yapılması, fark edilme ya da geçersiz olma tehlikesini getirdiği için zamanı bilmek önemlidir.

Bekçinin çıktıyı girişteki masasına götürmesini sağlamanın, sonra da onu orada çöpe attırmanın altındaki nedeni görebildiniz mi? Bu önemli bir adımdı. Bir sonraki iş gününde bilgisayar işletmenleri işe geldiklerinde, saldırgan, çıktı alma uçbiriminde ya da laboratuvarın çöpünde onların bu kanıtı görmelerini istemiyordu. Bekçiye akla yatkın bir açıklama yaparak dökümü yanında götürmesini sağlaması bu riskten kurtulmasına yetmişti.

Acil Yama

Teknik destek biriminde çalışan birinin dışardan birine bilgisayar ağına giriş hakkı tanımanın doğuracağı sakıncaların bilincinde olmasını beklersiniz. Ancak bu dışardan biri, yardımsever bir yazılım satıcısı gibi davranan akıllı bir toplum mühendisi ise, sonuçlar pek beklediğiniz gibi çıkmayabilir.

Faydalı Bir Telefon Görüşmesi

Arayan, orada bilgisayarlardan kimin sorumlu olduğunu bilmek istiyordu ve santral memuru onu teknik destek sorumlusu Paul Ahearn'a bağladı.

Arayan, kendini Edward olarak tanıtarak, veritabanı satıcısı SeerWare'dan aradığını söyledi. "Görünüşe göre bazı müşterilerimiz acil güncellemeyle ilgili e-postamızı almamışlar, bu yüzden yamanın yüklenmesinde sorun çıkıp çıkmadığını kontrol etmek için bazılarını arıyoruz. Yeni güncellemeyi yükleyebildiniz mi?"

Paul öyle birşey görmediğinden oldukça emin olduğunu söyledi.

Edward, "Program zaman zaman büyük veri kayıplarına neden olabilir, bu nedenle en kısa sürede yüklemenizi öneririz" dedi. "Evet" dedi Paul, bu kesinlikle yapmak isteyeceği bir şey olurdu. "Tamam" diye karşılık verdi arayan. "Size yamayı bir bant ya da CD'ye yüklenmiş olarak gönderebiliriz ve şunu da eklemek isterim ki bu gerçekten önemli çünkü iki şirket, şimdiden pek çok güne ait verilerini kaybettiler. Bu yüzden, bu olay sizin de başınıza gelmeden, elinize geçer geçmez yamayı yüklemelisiniz."

"İnternet sitenizden indirmem mümkün değil mi?" diye sordu Paul.

"Yakında hazır olacağını sanıyorum; teknik ekip hasarı düzeltmeye çalışmakla meşgul. İsterseniz müşteri destek hizmetlerinin yamayı uzaktan yüklemesini sağlayabiliriz. Sisteminize bağlanmak için telefon hattını kullanabilir ya da, destekliyorsanız, Telnet'i deneyebiliriz."

"Özellikle internetten Telnet'e izin vermiyoruz; güvenli değil" diye karşılık verdi Paul. "Eğer SSH kullanabilirseniz, bu olabilir".

"Evet, SSH'imiz var. IP adresiniz nedir?"

Paul ona IP adresini verdi ve Edward hangi kullanıcı adını ve parolayı kullanabileceğini sordu. Paul ona bu bilgileri de verdi.

Aldatmacanın İncelenmesi

Bu telefon gerçekten de veritabanı üreticisinden gelmiş olabilirdi. Ancak o zaman bu öykü bu kitapta yer almazdı.

Toplum mühendisi kritik verilerin yok olabileceği gibi bir korku uyandırarak kurbanını etkiledi ve sorunu halledecek hızlı bir çözüm önerdi.

Ayrıca bir toplum mühendisinin, bilginin değerini bilen birini hedeflediği zaman, uzaktan erişim elde edebilmek için çok inandırıcı ve ikna edici nedenler bulması gerekir. Bazen işin içine aciliyet katarak kurbanını hızlı hareket etmeye zorlayıp konuyu fazla düşünmesine izin vermeden isteğini kabul etmesini sağlar.

Yeni Kız

Bir saldırgan, şirketinizin dosyalarında duran hangi tür bilgiye ulaşmak isteyebilir? Bazen hiç korumaya ihtiyacınız olmadığını düşündüğünüz bir şey olabilir.

Sarah'ya Gelen Telefon

- *İnsan Kaynakları, ben Sarah.*

- *Merhaba Sarah. Ben George, şirket otoparkında görevliyim. Asansörlere binmek ve otoparka girmek için kullandığınız erişim kartlarını hatırlıyor musun? Bir sorun çıktı ve son on beş gün içinde yeni girenler için açtığınız bütün kartları yeniden programlamamız gerekiyor.*

- *Adlarına mı ihtiyacınız var?*

- *Ve telefon numaralarına.*

- *Yeni işe alınanlar listesine bakıp seni geri arayabilirim. Telefon numaran nedir?*

- *73... Ah, az sonra kahve molasına çıkacağım, yarım saat sonra ben seni arasam nasıl olur?*

- *Tamam, olur.*

Adam geri aradığında, kız:

- *Evet, yalnızca iki kişi var. Finans bölümünden Anna Myrtle, sekreter, ve yeni genel müdür yardımcısı Bay Underwood,* dedi.

- *Telefon numaraları?*

- *Evet, tamam. Bay Underwood 6973. Anna Myrtle 2127.*

- *Çok yardımcı oldun, teşekkürler.*

Anna'ya Gelen Telefon

- *Finans bölümü, Anna'yla görüşüyorsunuz.*

- *Geç saatlere kadar çalışan birini bulabildiğim için çok memnunum. Ben Ron Vittaro. Ticaret bölümünün ağ sorumlusuyum. Sanırım henüz tanıştırılmadık. Şirkete hoşgeldin.*

- *Teşekkür ederim.*

- *Anna, Los Angeles'tayım ve bir krizi çözmeye çalışıyorum. Bana ayırabileceğin bir on dakikan var mı?*

- *Elbette. Ne yapmam gerekiyor?*

- *Ofisime çık. Nerede olduğunu biliyor musun?*

- *Hayır.*

- *Peki, on beşinci katta köşedeki oda; oda numarası 1502. Birkaç dakika içinde seni oradan ararım. Ofise gittiğinde aramanın doğrudan sesli mesaja bağlanmaması için ileri tuşuna basman gerekecek.*

- *Tamam, şimdi gidiyorum.*

On dakika sonra Ron'un odasına varmış, arama aktarma işlevini iptal etmiş bekliyordu ki telefon çaldı. Adam, kıza oturmasını ve internet tarayıcısını çalıştırmasını söyledi. Açıldığında yazması için www.geocities.com/ron-insen/eser.doc.exe adresini verdi.

Bir iletişim kutusu çıktı ve adam "Aç" düğmesini tıklamasını söyledi. Bilgisayar yazıyı indiriyormuş gibi gözüktü ama sonra ekran kararda. Anna birşeylerin ters gidiyor gibi göründüğünü söylediğinde adam karşılık verdi:

- Ah, hayır. Sürekli o web sitesinden bir şeyler indirmekte güçlük çekiyorum ama düzeltildiğini sanmıştım. Peki, boş ver o zaman, dosyayı daha sonra başka bir şekilde indiririm.

Oluşan sorundan sonra bilgisayarının düzgün çalışıp çalışmadığından emin olmak için Anna'dan bilgisayarını yeniden başlatmasını istedi. Yeniden başlatması için gerekli adımları kıza anlattı.

Bilgisayar yeniden düzgün bir şekilde çalışmaya başladığında, ona içtenlikle teşekkür etti ve telefonu kapattı. Anna üzerinde çalıştığı işi bitirmek için finans bölümüne geri döndü.

Kurt Dillon'un Öyküsü

Millard-Fenton yayıncılık, iş yapmak üzere oldukları yeni yazarları konusunda oldukça heyecanlıydılar. Bu yazar, bir Fortune 500 şirketinin, anlatacak ilginç öyküleri olan emekli genel müdürüydü. Biri, görüşmeleri ayarlaması için adamı bir yazar manajerine yönlendirmişti. Menajer, yayınevi sözleşmelerinin nasıl yapıldığıyla ilgili hiçbir şey bilmediğini itiraf etmek istemiyordu; bu nedenle, bilmesi gerekenleri öğrenmesine yardımcı olması için eski bir arkadaşını tutmuştu. Bu eski arkadaş, ne yazık ki, pek iyi bir seçim değildi. Kurt Dillon araştırmalarında olağandışı olarak adlandırabileceğimiz, pek de etik olmayan yöntemler kullanırdı.

Terimler

CASUS YAZILIM: Hedefin bilgisayar faaliyetlerini gizlice izlemesi için özel olarak yapılmış program. Bunun bir çeşidi de, çevrimiçi reklamların internette gezinme alışkanlıklarına göre tasarlanabilmesi için internetten alışveriş edenlerin ziyaret ettikleri siteleri takip etmek için kullanılır. Yazılım, kullanıcının, aralarında girilen parolalar ve klavyeden yazdığı yazılar, e-postalar, sohbetler, anında mesajlar, ziyaret edilen tüm ağ sayfaları ve ekran resimleri olan tüm faaliyetlerini yakalar.

Kurt, Ron Vittaro adıyla Geocities'den ücretsiz bir site aldı ve yeni siteye bir casus yazılım yükledi. Yazılımın adını *eser.doc.exe* olarak değiştirdi, böylece dosya bir Word belgesi olarak gözükecek ve kuşku uyandırmayacaktı. Aslında işler Kurt'un beklediğinden daha iyi yürümüştü, çünkü gerçek Vittaro, Windows işletim sistemindeki "Bilinen dosya türleri için dosya uzantılarını gizle" seçeneğinin varsayılan ayarını hiç değiştirmemişti. Bu ayar yüzünden dosyanın adı zaten *eser.doc* olarak çıkmıştı.

Sonra hanım arkadaşlarından birinin Vittaro'nun sekreterini aramasını sağla-

dı. Dillon'un yönlendirmeleriyle kadın Vittaro'nun sekreteriyle konuştu. "Ultimate Kitabevleri, Toronto'nun başkanı Paul Spadone'un yönetici asistanıyım. Bay Vittaro patronumla bir süre önce bir kitap fuarında tanışmış ve ortak yürütülebilecek bir projeyle ilgili konuşmak için aramasını istemiş. Bay Spadone sürekli seyahatlerde, bu yüzden benden Bay Vittaro'nun ne zaman ofisinde olacağını öğrenmemi istedi."

Terimler

SESSİZ YÜKLEME: Bilgisayar kullanıcısının ya da işletmeninin fark etmeyeceği şekilde bir yazılım uygulaması yükleme yöntemi.

İkisi ajandaları karşılaştırmayı bitirdiklerinde, Kurt'un bayan arkadaşı Bay Vittaro'nun ofisinde olacağı tarihlerle ilgili saldırgana yeterince bilgi sağlamıştı. Bu aynı zamanda Vittaro'nun yerinde olmayacağı tarihleri de bildirdiği anlamına geliyordu. Vittaro'nun sekreterinin de onun yokluğundan faydalanıp biraz kayak yapmaya gideceğini öğrenmek için de uzun uzun sohbet etmesi gerekmemişti. Kısa bir süre için ikisi de ofiste olmayacaklardı. Mükemmel.

İkisinin birden olmadıkları ilk gün, emin olmak için uyduruk, acil bir mesajla telefon ettiğinde danışma görevlisi ona, "Bay Vittaro ofisinde değil, sekreteri de bugün yok. İkisi de bugün, yarın ve sonraki gün burada olmayacaklar" dedi.

Yeni bir çalışanı oyununa alet etme konusunda ilk denemesinde başarılı olmuştu ve aslında herkesçe bilinen, ticari olarak bulunabilen ve saldırganın sessiz yükleme için üzerinde oynadığı bir casus yazılım olan bir "eseri" indirmesini istediğinde kız gözünü kırpmadan indirmişti. Sessiz yükleme yöntemiyle kurulum hiçbir virüs koruma yazılımı tarafından farkedilmez. Tuhaf bir nedenden ötürü virüs koruma programları yapan üreticiler halihazırda varolan casus yazılımları bulacak bir ürünü pazara sürmüyorlar.

Genç kadının, yazılımı Vittaro'nun bilgisayarına yüklemesinin hemen ardından, Kurt, Geocities sitesine geri gitti ve doc.exe dosyasını internette bulduğu bir kitapla değiştirdi. Birileri oyunu farkeder ve ne olduğunu anlamak için siteye gelip bakacak olurlarsa tüm bulabilecekleri zararsız, acemice yazılmış, basılamaz bir kitap metninden ibaret olacaktı.

Program, yüklendikten ve bilgisayar yeniden başlatıldıktan sonra hemen harekete geçmek üzere ayarlanmıştı. Ron Vittaro birkaç gün içinde dönecek, işe başlayacak ve casus yazılım klavyeden bilgisayarına girdiği her şeyi, gönderdiği e-postaları ve o anda ekranından gördüklerinin bir resmini ona iletecekti. Hepsi düzenli aralıklarla Ukrayna'daki ücretsiz elektronik posta hizmeti veren bir siteye gönderilecekti.

Vittaro'nun dönüşünden birkaç gün sonra Kurt, Ukrayna'daki posta kutusuna birikmiş günlük dosyalarını karıştırıyordu ve çok geçmeden

Millard-Fenton Yayıncılığın o yazarla anlaşmak için tam olarak nereye kadar gitmek istediğini anlatan gizli e-postalar buldu. Bu bilgiyle donanarak yazarın menajerinin anlaşmayı bütünüyle kaybetme riski oluşmadan, ilk teklif edilenden çok daha iyi koşullar için pazarlık etmesi kolay olacaktı. Bu da doğal olarak menajer için daha dolgun bir komisyon anlamına geliyordu.

Aldatmacanın İncelenmesi

Bu oyunda saldırgan, aracı olarak yeni bir çalışan seçerek, onun işbirliği yapma ve iyi bir takım oyuncusu olma isteğine güvendi ve başarı şansını artırdı. Yeni elemanın şirket, çalışanlar ve dalavere teşebbüsünü aksatacak güvenlik uygulamaları konusunda daha az bilgili olma olasılığı vardı.

Kurt, finans bölümünde bir memur olan Anna'yla görüşmesinde genel müdür yardımcısı gibi davrandığı için, kızın, kendisinin yetkisini sorgulama olasılığının çok düşük olduğunu biliyordu. Aksine, bir genel müdür yardımcısına hizmet ederek göze girebileceğini de düşünebilirdi.

Anna'ya adım adım anlattığı, casus yazılım kurmaya yönelik süreç dışarıdan bakıldığında zararsız görünüyordu. Anna'nın, zararsız gibi görünen davranışlarının bir saldırgana şirketin çıkarlarıyla ters yönde kullanılabilecek değerli bilgiler sağladığı konusunda en küçük bir fikri yoktu.

Ve neden genel müdür yardımcısının mesajlarını Ukrayna'daki bir e-posta adresine göndermeyi seçmişti? Pek çok nedenden ötürü uzak yerler bir saldırganın izinin sürülmesi ya da ona karşı harekete geçilmesi şansını azaltır. Bunun gibi ülkelerde bu tarz suçlar genellikle düşük önceliklidirler ve internet üzerinden işlenen bir suç kaydadeğer bir suç değildir. Bu yüzden Amerikan emniyet birimiyle işbirliği yapma olasılığı düşük olan ülkelerden e-posta adresleri almak çekici bir stratejidir.

Aldatmacanın Engellenmesi

Bir toplum mühendisi, her zaman isteklerinde yanlış bir şeyler olduğunu anlama şansı düşük çalışanları hedeflemeyi tercih eder. Bu, işini kolaylaştırmakla kalmaz, bu bölümde anlatılan öykülerde olduğu gibi tehlikeyi de azaltır.

Gafili Kandırmak

Daha önce bir yabancının talimatlarını yerine getirmeye ikna olmamaları için çalışanların yoğun bir şekilde eğitilmeleri gerektiğini vurgulamıştım. Tüm çalışanlar ayrıca bir isteği, başka birinin bilgisayarında yerine getirmenin tehlikesini de anlamak zorundadırlar. Şirket kuralları,

Mitnick Mesajı:

Mesai arkadaşınızdan ya da bir astınızdan yardım istemek olağan bir durumdur. Toplum mühendisleri insanların yardım etmeye ve iyi bir takım oyuncusu olmaya yönelik isteklerini sömürmeyi bilirler. Saldırgan, amacına yaklaşabilmek için hiç bir şeyin farkında olmayan çalışanları kandırıp çeşitli işleri yaptırmalarını sağlayarak bu olumlu ve insanî niteliği kullanır. Birilerinin sizi kandırmaya çalışıp çalışmadığını anlayabilmeniz için bu basit noktayı anlamış olmanız gereklidir.

yöneticiler tarafından özellikle onaylanmadığı sürece bunu yasaklamalıdırlar. Mümkün olabileceği durumlar arasında şunlar olabilir:

- İstek iyi tanıdığınız birinden geldiyse, yüz yüze bir görüşmede dile getirildiyse ya da arayanın sesini tanıdığınızdan emin olduğunuz bir telefon görüşmesi sırasında alındıysa;
- Denenmiş yöntemler kullanarak istek sahibinin kimlik tespiti olumlu bir şekilde yapılmışsa;
- Yapılacak işlem, istek sahibini şahsen tanıyan bir yönetici ya da benzeri bir yetkili tarafından onaylandıysa.

Bir şeyler isteyen kişi üst düzey bir yönetici olduğunu iddia etse bile çalışanlar şahsen tanımadıkları kişilere yardım etmemeleri konusunda eğitilmelidirler. Kimlik tespitiyle ilgili güvenlik süreçleri yürürlüğe konduktan sonra yönetim, bir kuralı bertaraf etmesini isteyen üst düzey bir yöneticiye meydan okuması anlamına gelse bile çalışanların bu kurallara uymalarını desteklemelidir.

Her şirketin, bilgisayarlar ya da bilgisayar donanımlarıyla ilgili taleplere yanıt vermek konusunda çalışanlara yol gösterecek kural ve süreçleri olmalıdır. Yayıncılık şirketiyle ilgili öyküde toplum mühendisi bilgi güvenliği kuralları ve süreçleriyle ilgili bir eğitim almamış yeni bir çalışanı seçti. Bu tarz bir saldırının önüne geçmek için yeni ya da eski her çalışanın basit bir kurala uyması sağlanmalıdır: Tanımadığınız birinin isteğini yerine getirmek için bilgisayar sistemini kullanmayınız. Nokta.

Bir bilgisayara ya da bilgisayarla ilgili bir donanıma fiziksel ya da elektronik erişimi olan bir çalışanın bir saldırgan adına zararlı hareketler yapmak üzere yönlendirilmeye açık olduğunu unutmayınız.

Çalışanlar ve özellikle Bilgi İşlem elemanları, dışarıdan birinin bilgisayar ağına erişmesine izin vermenin, banka hesap numarasını telefonla satış yapan birine vermekle ya da telefon kartı kodunu hapisteki bir yabancıya vermekle arasında bir fark olmadığının bilincinde olmalıdırlar. Çalışanlar bir isteği yerine getirmenin, hassas bilgilerin açığa çıkmasına ya da şirket bilgisayar sisteminin paylaşıma açılmasına neden olup olmadığı konusu dikkatle tartmalıdırlar.

Bilgi İşlem personeli de satıcı gibi arayan tanımadıkları kişilere karşı tetikte olmalıdırlar. Genel olarak bir şirket her teknoloji satıcısının bağlantı kuracağı belli kişiler görevlendirmeli ve diğer çalışanların telefon ya da bilgisayar donanımlarına yönelik satıcılardan gelen bilgi ya da değişiklik taleplerine yanıt vermemesi için bir kural koymalıdır. Bu yolla belirlenen kişiler, arayan ya da ziyaret eden satıcılara aşina olurlar ve sahtekâr tarafından kandırılma olasılıkları düşer. Şirketin destek sözleşmesinin olmadığı bir satıcı aradığında bile buna kuşkuyla bakılmalıdır.

Kuruluştaki herkesin, bilgi güvenliğinin zayıflıkları ve gelebilecek tehditler konusunda uyarılmaları gerekmektedir. Güvenlik görevlileri ve benzer çalışanlara yalnızca güvenlik eğitiminin değil aynı zamanda bilgi güvenliği eğitiminin de verilmesi gerektiği unutulmamalıdır. Güvenlik görevlileri, tüm tesise fiziksel erişimleri olduğu için, kendilerine karşı kullanılabilecek toplum mühendisliği tekniklerini tanıyabilmelidirler.

Casus Yazılımlara Dikkat

Casus yazılımlar bir zamanlar çoğunlukla çocuklarının internette ne yaptığını merak eden ana-babalar tarafından ya da hangi çalışanların internette gezerek işten kaytardığını belirlemeye çalışan işverenler tarafından kullanılırdı. Daha ciddi bir kullanımı bilgi varlıklarına karşı olası hırsızlıkları ya da sanayi casusluğunu belirlemeye yönelikti. Tasarımcılar casus yazılımlarını çocukları korumak için bir araç olduğunu söyleyerek pazarlarlar ama asıl müşterileri başkalarını gözetlemek isteyen insanlardır. Bugünlerde, casus yazılım satışları insanların eşlerinin ya da benzer önemli kişilerin kendilerini aldatıp aldatmadıklarını öğrenmek istemeleriyle büyük ölçüde artmıştır.

Bu kitaptaki casus yazılım öyküsünü yazmaya başlamadan kısa bir süre önce, benim adıma e-postalarıma bakan kişi (internet kullanmam yasak olduğundan) bir dizi casus yazılımın reklamını yapan bir spam e-posta bulmuş. Reklamı yapılan programlardan biri şöyle birşey:

> **EN ÇOK İSTEYECEĞİNİZ ŞEY:** Bu güçlü gözetleme ve casus programı, geri planda kendisini farkettirmeden çalışırken tüm klavye girişlerini ve tüm açık pencerelerin zaman ve başlıklarını gizlice kaydeder. Günlükler şifrelenip sizin belirlediğiniz bir e-posta adresine otomatik olarak gönderilebilir ya da sabit diske kaydedilebilirler. Programa erişim parola korumalıdır ve CTRL+ALT+DEL menüsünde gözükmesi engellenebilir.
>
> Yazılan internet adreslerini görmek, sohbet oturumlarını, e-postaları ve pek çok başka şeyi (hattâ parolaları ;-)) izlemek için kullanabilirsiniz.
>
> **Farkedilmeden HERHANGİ BİR PC'ye yükleyin ve günlükleri kendinize göndertin!!!**

Virüs Koruma Boşluğu

Virüs koruma yazılımları ticarî casus yazılımları bulamazlar ve böylece amacı başkalarını gözetlemek bile olsa yazılıma kötü huylu bir yazılım değilmiş gibi yaklaşmış olurlar. Böylece telefon dinlemenin bilgisayar karşılığı farkedilmez ve hepimiz için sürekli yasadışı bir gözlem altında olma riskini yaratır. Virüs koruma programları üreticileri, doğal olarak, casus yazılımların yasal amaçlar için de kullanıldığını ve bu nedenle kötü huylu olarak nitelendirilmemesi gerektiğini öne sürebilirler. Ancak, bir zamanlar bilgisayar korsanları tarafından kullanılmış araçların, artık serbestçe dağıtılan ya da güvenliğe yönelik yazılım olarak satılan gelişmiş şekilleri yine de kötü huylu yazılım olarak muamele görebiliyor. Burada bir çifte standart var ve ben bunun nedenini merak ediyorum.

Aynı e-postada tanıtılan başka bir ürün, kullanıcının bilgisayarından, tıpkı kullanıcının omuzunun üzerinden bakan bir video kamera gibi ekran resimleri alabileceğini söylüyordu. Bu yazılımlardan bazıları kurbanın bilgisayarına fiziksel erişim sağlamayı bile gerektirmez. Kur, programı uzaktan ayarla ve anında bilgisayarı dinleyebilir duruma geç! FBI bu teknolojiye bayılıyor olmalı.

Casus yazılımlar bu kadar kolay bulunurken, şirketinizin iki koruma düzeyi oluşturması gerekmektedir. Tüm bilgisayarlara SpyCop gibi (www.spycop.com adresinden sağlanabilir) casus yazılımları tespit eden bir program yüklemeli ve çalışanlarınızın düzenli olarak tarama yaptırmalarını sağlamalısınız. Buna ek olarak, çalışanlarınızı bir program indirmeye ya da kötü huylu bir yazılım kurabilecek bir e-posta eki açmaya yöneltecek dalaverelerin oluşturduğu tehlikelere karşı eğitmeniz de gerekir.

Bir çalışanın kahve molası, öğle yemeği ya da bir toplantı için masasında bulunmadığı durumlarda casus yazılımların yüklenmesini engellemek için alınacak önlemlere ek olarak, tüm çalışanların bilgisayar sistemlerini şifreli bir ekran koruyucu ya da benzer bir yöntemle kilitlemeleri de yetkisiz birinin çalışanın bilgisayarına erişmesi tehlikesini büyük ölçüde azaltacaktır. Kişinin odasına ya da bölmesine sızan hiç kimse dosyalarına erişip, e-postalarını okuyup casus yazılımlar ve kötü huylu programlar yükleyemeyecektir. Ekran koruyucu parolasını devreye sokmak için gerekli kaynak yok denecek kadar az, çalışanların bilgisayarlarını korumada sağladığı kazançsa muazzam ölçüde büyüktür. Bu koşullarda faydamaliyet analizini yapmak için çok kafa yormaya gerek yoktur.

ZEKİCE OYNANMIŞ OYUNLAR

Hassas bilgiler talep eden ya da bir saldırganın işine yarayabilecek bir şeyler isteyen yabancı biri aradığında, telefonu açan kişinin, arayanın telefon numarasını alacak ve kişinin gerçekten söylediği kişi -şirket çalışanı ya da ortak çalışılan bir firma personeli ya da satıcılardan birinden gelen bir teknik destek görevlisi- olup olmadığını kontrol etmek için onu geri arayacak şekilde eğitilmesi gerektiğini artık iyice görmüş olmalısınız.

Arayanların kimliğinin tespiti için şirket çalışanlarının özenle izlemesi gereken oturmuş bir süreç olsa bile, çok yönlü saldırganlar kurbanlarını söyledikleri kişiler olduklarına inandırmak için yine de çeşitli oyunlar oynayabilirler. Aşağıda anlatıldığı gibi, güvenlik bilinci yerleşmiş çalışanlar bile bu tarz yöntemlerle tuzağa düşürülebilirler.

Yanıltıcı Arayan Kimliği

Cep telefonuna arama gelen herkes, arayan kimliği olarak bilinen, arayanın numarasını görme özelliğini bilir. İş dünyasında, aramanın şirket içinden mi yoksa dışından mı geldiğini bir bakışta anlamak gibi de bir faydası vardır.

Yıllar önce, telefon şirketlerinin bu hizmeti halka sunmalarına izin verilmediği zamanlarda bazı hırslı telefon beleşçileri arayan numarayı görmenin sağladığı olanaklarla tanışmışlardı. Daha arayan kişi bir şey söyleyemeden onu adıyla selamlayıp insanları hayrete düşürerek eğleniyorlardı.

Güvende olduğunuzu düşündüğünüz bir anda, gördüğünüze güvenerek -yani telefonun ekranında, arayanın numarasını görerek- kimlik tespiti uygulaması, aslında saldırganın tam da yapmanızı istediği şey olabilir.

Linda'nın Telefon Görüşmesi

Gün/Saat: 23 Temmuz, Salı, saat 15:12
Yer: Starbeat Havacılık, Finans Dairesi

Tam patronuna bir not yazarken Linda Hill'in telefonu çaldı. Arayanın numarasına baktığında aramanın New York Genel Müdürlük binasından, Victor Martin adlı birinden geldiğini gördü. Bu tanıdığı bir isim değildi.

Yazdığı notla ilgili düşünce akışını kaybetmemek için aramayı telesekretere bırakmayı düşündü. Ama merakına yenildi ve telefonu açtı. Arayan kendini tanıttı ve Ürün Araştırma'dan olduğunu, Genel Müdür'ün istediği bir şeyler üzerinde çalıştığını söyledi. "Bazı bankacılarla toplantı için Boston'a gidiyor. İçinde bulunduğumuz üç aylık döneme ait başlıca finansal verilere ihtiyacı var," dedi. "Ve bir şey daha. Apache projesiyle ilgili finansal tahminlere de gereksinimi var," diye ekledi Victor, şirketin baharda piyasaya süreceği önemli ürünlerden birinin kod adını kullanarak.

Kadın ona e-posta adresini sordu ama adam e-posta almakla ilgili bir sorunu olduğunu, teknik servisin bunun üzerinde çalıştığını söyledi ve bu yüzden verileri fakslayıp fakslayamayacağını sordu. Kadın bunun sorun olmayacağını söyledi ve Victor ona dahili faks numarasını verdi.

Birkaç dakika sonra Linda ona faksı yolladı.

Ama Victor, Ürün Araştırma'da çalışmıyordu. Aslında o şirkette bile çalışmıyordu.

Jack'ın Öyküsü

Jack Dawkins profesyonel yaşamına erken yaşlarda Yankee Stadyumu'nda oynanan maçlarda, kalabalık metro istasyonlarında ve Times Meydanı'na gece gelen turist kalabalığının arasında yankesicilik yaparak başladı. O kadar çevik ve becerikliydi ki adama fark ettirmeden kolundan saatini bile alabilirdi. Ama sarsak ergenlik çağında hantallaşmış ve yakalanmıştı. Islahevinde, yakalanma tehlikesi çok daha düşük olan yeni bir meslek edinmişti.

Şu anki işi, bir şirketin üç aylık kâr-zarar durumunu ve nakit akım bilgilerini, veriler ABD Sermaye Piyasası Kurulu'na verilmeden ve halka açılmadan önce ele geçirmesini gerektiriyordu. Müşterisi, bu bilgileri neden istediğini söylemeyen bir diş hekimiydi. Jack'e kalırsa adamın gizliliği komikti. Böylelerini daha önce de görmüştü; adamın büyük olasılıkla bir kumar sorunu vardı ya da daha karısının bilmediği masraflı bir kız arkadaşa sahipti. Ya da belki hisse senetleriyle oynamada ne kadar akıllı olduğuyla ilgili karısına hava atarken bir tomar para kaybetmiş ve çeyrek dönemlik sonuçlarını açıkladıklarında şirket hisse senetlerinin ne yöne gideceğini öğrenenerek, kesin bir şeye büyük oynayıp çok kazanmak istiyordu.

İnsanlar, dikkatli bir toplum mühendisinin daha önce karşılaşmadığı bir durumu çözmek için ne kadar az zamana ihtiyacı olduğunu öğrendiklerinde şaşırıyorlar. Jack diş hekimiyle yaptığı toplantıdan eve dönene kadar çoktan bir plan yapmıştı. Arkadaşı Charles Bates kendi telefon santralı, diğer bir deyişle PBX'i olan Panda İthalat adlı bir şirkette çalışıyordu.

Telefon sistemleri konusunda bilgili insanların aşina olduğu terimler-

le ifade edersek, PBX, T1 olarak bilinen bir dijital telefon hizmetine bağlıydı ve PRI ISDN olarak ayarlıydı. Bu, Panda'dan yapılan her aramada kurulum ve diğer görüşme bilgileri veri kanalından telefon şirketi santralına gidiyor anlamına geliyordu. Bu bilgiler arasında (eğer engellenmemişse) alıcı uçta numara görüntüleme arayüzüne aktarılan, arayanın telefon numarası da vardı.

Jack'in arkadaşı, aranan kişinin arayan numarayı görebileceği şekilde santralı nasıl programlayacağını biliyordu. Üstelik Panda ofisinden kullanılan gerçek telefon numarasını değil, santrala her ne telefon numarası programlandıysa karşı tarafın onu görmesini sağlayabiliyordu. Bu dümenin işlemesinin nedeni, yerel telefon şirketlerinin müşterinin kullandığı telefon numarasıyla müşterinin parasını ödediği telefon numarasını karşılaştırmaya yanaşmamasıydı.

Jack Dawkins'in ihtiyacı olan tek şey böyle bir telefon hizmetini kullanabilmekti. Neyseki arkadaşı ve kısa bir süre için suç ortağı olan Charles Bates küçük bir ücret karşılığında her zaman yardım etmeye hazırdı. Bu durumda Jack ve Charles şirket telefon santralını geçici olarak programlamışlardı. Böylece Panda şirketinin içindeki belli bir telefondan arandığında Victor Martin'in telefon numarasını gösterecek ve arama Starbeat Havacılık'tan geliyor gibi görünecekti.

Görünen numaranın istediğiniz numarayla değiştirilebileceği fikri o kadar az bilinir ki bu yüzden çok az sorgulanır. Bu olayda Linda, Ürün Araştırma'dan olduğunu düşündüğü kişiye istediği faksı memnuniyetle gönderdi.

Jack telefonu kapattığında Charles şirket telefon santralını yeniden programlayıp telefon numarasını asıl ayarlarına geri döndürdü.

Aldatmacanın İncelenmesi

Bazı şirketler müşterilerinin ya da mal aldıkları şirketlerin çalışanlarının telefon numaralarını bilmelerini istemez. Örneğin, Ford firması Müşteri Destek Merkezi'nden arayan her müşteri temsilcisinin doğrudan telefon numarasını görmek yerine, Merkezden gelen tüm aramaların Merkezin 800'lü numarasını ve "Ford Destek" gibi bir bilgi göstermesini isteyebilir. Microsoft, çalışanlarının aradığı herkesin arayan numaraya bakıp dahili numaraları öğrenmemesi için, çalışanlarına telefon numaralarını yalnızca kendi seçtikleri muhataplarına verme seçeneğini tanıyabilir. Bu yolla şirket dahili numaralarının gizliliğini koruyabilir.

Ancak bu yeniden programlanma özelliği, şakacılar, fatura tahsildarları, telefonla satış yapanlar ve tabii, toplum mühendisleri için çok kullanışlı bir araç oluşturmaktadır.

Çeşitleme: Amerika Birleşik Devletleri Başkanı Arıyor

Los Angeles, KFI Talk Radio adındaki bir radyoda "İnternetin Karanlık Yüzü" adlı bir programın ikinci sunucusu olarak radyonun program yönetmeniyle birlikte çalışıyordum. Tanıdığım en işine bağlı ve çalışkan insanlardan biri olan David, çok meşgul olduğu için telefonla ulaşılması zor biriydi. Arayan numara göstergesine bakıp konuşmak istediği biri değilse telefonu açmayan insanlardandı.

Cep telefonumda arama engeli olduğu için ben aradığımda kimin aradığını göremiyor ve telefonu açmıyordu. Telesekreter devreye giriyordu ve bu benim için çok can sıkıcı oluyordu.

Yüksek teknoloji şirketlerine ofis bulan bir emlak şirketinin sahibi olan eski bir arkadaşımla bu konuda ne yapılabileceğini görüştüm. Birlikte bir plan yaptık. Şirketine ait bir Meridian telefon santralına erişimi vardı ve bir önceki öyküde anlatıldığı gibi, arayan tarafın numarasını yeniden programlayabiliyordu. Ne zaman program yönetmeniyle konuşmam gerekse ve ona ulaşamazsam, arkadaşımdan, seçtiğim bir numaranın arayan numara olarak gözükmesi için gerekli programlamayı yapmasını rica ederdim. Bazen aramayı David'in yardımcısından ya da radyo istasyonunun sahibi olan holdingden geliyormuş gibi göstermesini isterdim.

Ama en sevdiğim, aramayı David'in kendi evinden geliyormuş gibi göstermekti. Böyle olduğu zaman telefonu hep açıyordu. Ancak adama hakkını vermek lâzım. Telefonu açıp onu bir kez daha kandırdığımı görünce olayı şaka yollu karşılamayı biliyordu. Bunun en iyi tarafı ise istediğim şeyin ne olduğunu anlayıp sorunu çözene kadar telefonda kalmasıydı.

Bu küçük numarayı Art Bell Show'da gösterdiğimde, arayan kimliğimi FBI Los Angeles genel merkezinin adı ve numarası olarak değiştirdim. Art tüm bu olanlara oldukça şaşırdı ve yasadışı bir şey yaptığım konusunda beni uyardı. Sahtecilik yapmadığım sürece bunun tamamıyla yasal olduğunu ona anlattım. Programdan sonra bunu nasıl yaptığımı soran yüzlerce e-posta aldım. Artık siz biliyorsunuz.

Toplum mühendisinin inanılırlığını artırması için bu kusursuz bir araçtır. Örneğin, toplum mühendisliği saldırı sürecinin araştırma aşamasında hedefin arayan numaraları görebildiği anlaşılırsa, saldırgan kendi numarasını güvenilir bir şirketten ya da çalışandan geliyormuş gibi gösterebilir. Bir fatura tahsildarı, yaptığı aramaları işyerinizden geliyor gibi gösterebilir.

Ama durup bunun etkilerini düşünmek gerek. Bir bilgisayar saldırganı, şirketinizin Bilgi İşlem biriminden olduğunu söyleyerek sizi evinizden arayabilir. Telefondaki kişi, çöken bir sunucudan dosyalarınızı kur-

Mitnick Mesajı:

Bir daha size bir telefon geldiğinde ve telefonun göstergesine bakıp arayanın sevgili anneniz olduğunu gördüğünüzde, hiç belli olmaz, sevimli, yaşlı bir toplum mühendisiyle karşılaşabilirsiniz.

tarmak için acilen parolanıza ihtiyaç duymaktadır. Ya da arayan numara olarak bankanızın veya menkul kıymet danışmanınızın adı ve numarası gözükebilir ve o tatlı sesli kız hesap numaralarınızı ve annenizin kızlık soyadını kontrol etmesi gerektiğini söylemektedir. İşi sağlama almak için sistemde oluşan bir sorun nedeniyle ATM kart numaranızı da elindeki bilgiyle karşılaştırması gerekmektedir. Şüpheli hisse senetlerinin alınıp satıldığı bir yer, aramalarını Merrill Lynch ya da Citibank'tan yapılıyormuş gibi gösterebilir. Kimlik bilgilerinizi çalmaya çalışan biri Visa'dan arıyormuş gibi görünüp, sizi kredi kartı numaranızı vermeye kandırabilir. Size diş bileyen biri, arayıp vergi dairesinden ya da FBI'dan olduğunu söyleyebilir.

Bir PRI'ya bağlı bir telefon sistemine erişiminiz ve satıcı şirketin internet sayfasından edinebileceğiniz küçük bir programlama bilginiz varsa, bu taktiği arkadaşlarınıza sıkı oyunlar oynamak için kullanabilirsiniz. Tanıdığınız abartılı politik eğilimleri olan biri var mı? Gösterilecek numarayı 202 456-1414 programlayıp, arayan numaralarda gösterilen arayan kimliğini "BEYAZ SARAY" olarak değiştirebilirsiniz.

Başkanın onu aradığını düşünecektir!

Hikâyenin ana fikri basittir: Dahili aramaları gördüğünüz durumlar dışında arayan kimliğine güvenilmez. Hem işte hem de evde, herkes arayan numara üçkâğıdının farkında olmalı ve telefonda gözüken adın ve numaranın kimlik tespiti için güvenilir bir veri olmadığının bilincinde olmalıdır.

Görünmez Çalışan

Shirley Cutlass hızlı para kazanmanın yeni ve heyecanlı bir yolunu bulmuştu. Artık para kazanmak için yırtınma devri kapanmıştı. Son yılların en sık işlenen suçunu işleyen yüzlerce dalavereciden biri olmuştu. Shirley bir kimlik hırsızıydı.

Bugün gözünü bir kredi kartı şirketinin müşteri hizmetleri bölümünden gizli bilgi almaya dikmişti. Her zamanki ödevlerini yerine getirdikten sonra, hedef şirketi aradı ve telefonu açan santral memuruna Telekomünikasyon birimine bağlanmak istediğini söyledi. Telekomünikasyona bağlandığında sesli mesaj yöneticisiyle konuşmak istedi.

Araştırmalarından edindiği bilgileri kullanarak adının Norma Todd olduğunu ve Cleveland bürosundan aradığını söyledi. Artık size de tanıdık gelen bir kılıf uydurarak bir haftalığına şirket genel müdürlüğüne geleceğini ve şehirlerarası telefon görüşmesi yapmadan sesli mesajlarını kontrol etmek için orada bir sesli mesaj kutusuna ihtiyacı olduğunu anlattı. Adam konuyla ilgileneceğini ve gerekli düzenlemeleri yaptıktan sonra ihtiyacı olan bilgileri vermek için onu arayacağını söyledi.

Şuh bir ses tonuyla kadın, "Şu anda bir toplantıya gidiyorum, sizi bir saat sonra yeniden arayabilir miyim?" diye sordu.

Tekrar aradığında adam her şeyin ayarlandığını söyledi ve ona dahili numara ve geçici paroladan oluşan bilgiyi verdi. Adam, sesli mesaj parolasını nasıl değiştireceğini bilip bilmediğini sordu ve kadın yapılması gerekenleri adam kadar iyi bilse de yine de anlatmasına izin verdi.

"Ha, bir de", dedi kadın ve sordu, "mesajlarımı otelden kontrol etmek için hangi numarayı çevirmem gerekiyor?" Adam ona numarayı verdi.

Shirley o numarayı aradı, parolayı değiştirdi ve arayanlar için yeni bir selamlama mesajı kaydetti.

Shirley Saldırır

Şimdiye kadar yaptığı, altyapıyı oluşturmaktan ibaretti. Artık aldatma sanatını kullanmaya hazırdı.

Şirketin müşteri hizmetleri bölümünü aradı. "Cleveland bürosu, Tahsilatta çalışıyorum" dedi ve artık aşina olduğunuz bahanenin bir başka çeşidini anlatmaya girişti. "Teknik destek ekibi bilgisayarımı tamir etmeye uğraşıyor, bu yüzden bir bilgiyi bulmak için yardımınıza ihtiyacım var." Ve kimliğini çalmaya niyetli olduğu kişinin adını ve doğum tarihini verdi. Sonra istediği bilgileri sıraladı: Adresi, annesinin kızlık soyadı, kart numarası, kredi limiti, kullanabileceği kredi miktarı ve geçmiş ödemeleri. "Beni bu numaradan arayabilirsiniz", diyerek ses mesajı yöneticisinin onun için ayırdığı dahili numarayı verdi. "Eğer yerimde yoksam, bilgiyi sesli mesaj olarak bırakabilirsiniz."

Sabah başka işlerle uğraşmayı sürdürdü ve öğleden sonra sesli mesajını kontrol etti. İstediği her şey oradaydı. Telefonu kapamadan önce kendi selamlama mesajını sildi. Geride sesinin kaydını bırakmak dikkatsiz bir hareket olacaktı.

Amerika'nın en hızlı artan, yeni yüzyılın en popüler suçu olan kimlik hırsızlığına bir kurban daha verilmişti. Shirley az önce ele geçirdiği kredi kartını ve kimlik bilgilerini kullanarak kurbanın kartından harcama yapmaya başlamıştı bile.

Mitnick Mesajı:

Arada bir kendi sesli mesaj kutunuzu aramayı deneyin; eğer size ait olmayan bir selamlama mesajı duyarsanız, hayatınızın ilk toplum mühendisiyle karşılaşmış demektir.

Aldatmacanın İncelenmesi

Çevirilen bu dalaverede saldırgan önce şirketin sesli mesaj yöneticisini, geçici bir sesli mesaj kutusu açması için bir şirket çalışanı olduğu yolunda kandırdı. Eğer adam kimlik tespiti yapacak olsaydı, kadının verdiği adın ve telefon numarasının şirket çalışanları veri tabanındaki listelerle uyuştuğunu görecekti.

Geriye kalan, yalnızca bilgisayar sorunuyla ilgili geçerli bir mazeret vermek, ihtiyacı olan bilgileri karşı taraftan istemek ve bilgilerin sesli mesaja bırakılmasını rica etmekten ibaretti. Neden bir çalışan başka bir şirket mensubuna yardım etmesin ki? Shirley'nin verdiği numaranın dahili bir numara olduğu açık bir şekilde görülürken kuşkulanmak için hiçbir neden yoktu.

Yardımsever Sekreter

Robert Jorday adındaki bilgisayar korsanı küresel bir şirket olan Rudolfo Gemicilik Inc.'in bilgisayar sistemlerine düzenli olarak giriyordu. Şirket, sonunda birilerinin uçbirim sunucularına bağlandığını ve bu sunucular üzerinden kullanıcının şirketteki herhangi bir bilgisayara girebildiğini anladı. Şirket ağını korumak için, her uçbirim sunucusuna telefon hatlı modem takılmasına karar verildi.

Robert, Ağ Hizmetleri Merkezi'ni, Hukuk İşleri'nden arayan bir avukatmış gibi aradı ve ağa bağlanmakta güçlük çektiğini söyledi. Konuştuğu ağ yöneticisi ona birkaç güvenlik sorunu yaşadıklarını bu yüzden tüm telefon bağlantılı kullanıcıların aylık parolayı yöneticilerinden alması gerektiğini belirtti. Robert her ayın parolasının yöneticilere nasıl aktarıldığını ve parolayı nasıl ele geçirebileceğini düşündü. Öğrendiği kadarıyla aradığı yanıt, bir sonraki ayın parolasının ofis postası aracılığıyla bir not olarak her şirket yöneticisine iletilmesinde yatıyordu.

Bu, işleri kolaylaştırmıştı. Robert küçük bir araştırma yaptı, hemen ayın birinden sonra şirketi aradı ve yöneticilerden birinin, adının Janet olduğunu söylediği sekreteriyle görüştü. "Merhaba, Janet. Ben Araştırma ve Geliştirme'den Randy Goldstein. Şirket dışından uçbirim sunucusuna bağlanmak için kullanılan yeni parola notunu aldığıma emin gibiyim ama hiçbir yerde bulamıyorum. Bu ayın notunu siz aldınız mı?"

Evet, dedi kadın, almışlardı.

Mitnick Mesajı:

Becerikli toplum mühendisi, insanları etkileyerek kendisine iyilik yapmalarını sağlamak konusunda çok akıllıdır. Bir faks alıp sonra onu başka bir yere göndermek o kadar zararsız görünür ki bir danışma görevlisini ya da başka birini bunu yapmaya ikna etmek çok kolaydır. Biri sizden bilgi talep ederek bir iyilik yapmanızı istiyorsa ve siz o kişiyi tanımıyor ya da kimliğini kontrol edemiyorsanız, "hayır" deyin.

Onu kendisine fakslayıp fakslayamayacağını sordu ve kız kabul etti. Ona şirket alanında başka bir binanın danışma faks numarasını verdi. Burada faksların kendisi adına bekletilmesi için gerekli düzenlemeleri çoktan yapmıştı. Daha sonra da parola faksının kendisine yönlendirilmesini sağlayacaktı. Ancak bu kez Robert farklı bir faks yönlendirme yöntemi kullandı. Danışma görevlisine bir çevrimiçi faks hizmetinin numarasını vermişti. Bu numaraya faks gönderdiğinizde sistem onu abonenin e-posta adresine gönderiyordu.

Yeni parola Robert'ın Çin'deki bir ücretsiz e-posta hizmetinden aldığı e-postaya geldi. Faksın nereye gittiği izlenecek olursa, soruşturmayı yürüten kişi Çinli yetkililerle işbirliği sağlayabilmek için saçını başını yolacaktı. Böyle konularda Çinlilerin pek yardımcı olmayacaklarını Robert biliyordu. En güzeli ise faks makinasının başında hiç bulunmamış olmasıydı.

Trafik Mahkemesi

Aşırı hız cezası kesilen herkes herhalde cezadan sıyrılmanın bir yolunu bulmayı hayal etmiştir. Ehliyet kursuna giderek, cezayı ödeyerek ya da yargıcı polis hızölçerinin ya da radar cihazının en son ne zaman bakımdan geçtiğini değerlendirmeye ikna etmeye çalışarak bu iş olmaz. Hayır, en güzel senaryo sistemi alt ederek ceza makbuzundan kurtulmaktır.

Dalavere

Her ne kadar bir trafik cezasından kurtulmak için bu yöntemi önermesem de (her zaman söylendiği üzere, bunu kendiniz yapmayı denemeyin), toplum mühendislerinin aldatma sanatını kullanmalarına iyi bir örnek oluşturmaktadır.

Bu trafik ihlalcisinin adı Paul Durea olsun.

İlk Adımlar

- *Los Angeles Emniyet Müdürlüğü, Hollenbeck birimi.*
- *Merhaba, Celp Bürosu'ndan biriyle görüşmek istemiştim.*

- Mahkeme celplerine ben bakıyorum.

- Çok iyi. Ben avukat John Leland: Meecham, Meecham ve Talbott Avukatlık Bürosu'ndan. Bir memuru bir davaya çağırmam gerekiyor.

- Peki, hangi memuru?

- Büronuzda Memur Kendall adında biri var mı?

- Sicil numarası nedir?

- 21349

- Evet, var. Ne zaman ihtiyacınız var?

- Gelecek ay bir ara ama bu dava için başka tanıklar da davet etmem ve sonra da mahkemeye hangi günlerin bizim için daha uygun olduğunu söylemem gerekiyor. Gelecek ay Memur Kendall'ın müsait olabileceği günler hangileri?

- Bakalım...Yirmisinden yirmi üçüne kadar tatilde ve sekiziyle on altısı arasında da eğitimde olacak.

- Teşekkürler. Öğrenmek istediğim buydu. Mahkeme tarihi belli olduğu zaman sizi yine ararım.

Bölge Mahkemesi, Kâtip Masası

Paul: Bu trafik cezası için bir mahkeme tarihi belirlemek istiyorum.

Kâtip: Tamam. Size, gelecek ayın yirmi altısını verebilirim.

- Bir tebligat ayarlamak istiyordum.

- Trafik cezası için tebligat mı istiyorsunuz?

- Evet.

- Tamam. Tebligatı yarın sabah ya da öğleden sonra yapabiliriz. Hangisini tercih edersiniz?

- Öğleden sonra.

- Tebligat yarın öğleden sonra 13:30'da 6 numaralı mahkeme salonunda.

- Teşekkürler, orada olacağım.

Bölge Mahkemesi, Altı Numaralı Mahkeme

Tarih: Perşembe, öğleden sonra 13:45

Katip: Bay Durea, lütfen kürsüye yaklaşın.

Yargıç: Bay Durea, bugün öğleden sonra size açıklanan seçenekleri anladınız mı?

Paul: Evet, sayın yargıç.

Yargıç: Trafik okuluna gitme seçeneğini kullanmak ister misiniz? Sekiz saatlik bir kursu başarıyla tamamladıktan sonra davanız düşecektir. Kayıtlarınızı inceledim ve şu anda gerekli niteliklere sahip görünüyorsunuz.

Paul: Hayır, sayın yargıç. Davamın görülmesini talep ediyorum. Bir şey daha var sayın yargıç, ülke dışına çıkmam gerekiyor ama ayın sekizinde ve dokuzunda uygun olacağım. Davamın o günlerden birinde görülmesi mümkün olabilir mi? Yarın Avrupa'ya iş gezisine gidiyorum ve dört hafta sonra döneceğim.

Yargıç: Pekala. Dava 8 Haziran, sabah 08:30'de dört numaralı mahkeme salonunda görülecektir.

Paul: Teşekkürler, sayın yargıç.

Bölge Mahkemesi, Dört Numaralı Mahkeme

Paul ayın sekizinde mahkemeye erken geldi. Yargıç geldiğinde katip ona polis memurlarının gelmediği davaların bir listesini verdi. Yargıç, aralarında Paul'ün de olduğu davalıları çağırdı ve onlara davalarının düştüğünü söyledi.

Aldatmacanın İncelenmesi

Polis ceza kestiği zaman ceza makbuzunun üzerine adını ve sicil numarasını da yazar (ya da çalıştığı kurumda bu kişiye özgü numaraya ne ad veriliyorsa onu yazar). Görevli olduğu karakolu bulmak çok kolay olur. Bilinmeyen numaraları arayıp makbuzun üstünde yazan emniyet müdürlüğü karakolunun adını (otoyol devriyesi, bölge şerifi ya da herneyse) vermeniz ayağınızı kapıdan içeri sokmanız için yeterlidir. Karakolu aradıktan sonra, trafik cezasının kesildiği bölgeyle ilgili mahkeme celplerine bakan memura sizi yönlendirebilirler.

Emniyet mensupları düzenli olarak mahkemelere çağırılırlar; bu, yaptıkları işin bir parçasıdır. Bir bölge savcısı ya da savunma avukatı bir polis memurunun tanıklığına ihtiyaç duyarsa ve sistemin nasıl işlediğini biliyorsa, önce memurun ne zaman uygun olduğunu öğrenir. Bunu yapmak kolaydır, karakoldaki celp memurunu aramak yeterli olur.

Çoğunlukla bu görüşmelerde avukat memurun şu ve şu tarihlerde uygun olup olmadığını sorar. Bu oyunu oynayabilmek için Paul'un duruma göre davranması, celp görevlisinin polis memurunun dolu olduğu zamanları vermesi için elle tutulur bir neden bulması gerekiyordu.

Mahkeme binasına gittiğinde neden Paul kâtibe doğrudan istediği şeyi söylemedi? Basit; anladığım kadarıyla çoğu yerde trafik mahkemesi kâtipleri halkın mahkeme tarihi seçmesine izin vermezler. Eğer kâtibin önerdiği bir tarih kişiye uymuyorsa, kâtip bir iki tarih önerisinde daha bulunur ama daha fazlasını yapmaz. Öte yandan tebligatta kendini gösterecek zamanı ayırabilmiş birinin şansı daha yüksektir.

Paul bir tebligat hakkı olduğunu biliyordu. Yargıçların gün taleplerine çoğunlukla olumlu baktığını da biliyordu. Polis memurunun eğitim günlerine denk gelen günleri özellikle seçti. Polisin durumu göz önüne alındığın-

Mitnick Mesajı:

İnsan aklı muhteşem bir eser. Biçimsiz bir durumdan sıyrılmak ya da istediklerini elde etmek için dolambaçlı yollar üretmekte insanların ne kadar yaratıcı olduğunu görmek ilginç. Kamu ve özel sektörde bilgi ve bilgisayar sistemlerini korumak için sizin de aynı yaratıcılığı ve hayal gücünü göstermeniz gerekir. Bu yüzden dostlarım, şirketinizin güvenlik politikalarını oluştururken yaratıcı olun ve olaylara dışardan bakın.

da eğitime gitmek bir trafik mahkemesinde bulunmaktan daha önemli olacaktı.

Trafik mahkemelerinde, polis memuru mahkemeye gelmezse dava düşer. Ne para cezası, ne trafik okulu, ne ceza puanı... hiçbir şey olmaz. Daha da iyisi trafik suçu kayda da geçmez!

Tahminime göre bazı polis yetkilileri, mahkeme görevlileri, bölge savcıları ve benzeri kişiler bu öyküyü okuyacaklar ve bu numaranın işlediğini bildikleri için başlarını sallayacaklar. Ama baş sallamakla kalacaklar ve hiçbir şey değişmeyecek. Bu konuda bahse girebilirim. 1992'de çıkan *Sneakers* adlı filmdeki Cosmo karakterinin de söylediği gibi, "Her şey ya birdir ya sıfırdır", yani sonuç olarak her şey bilgiye dayanıyor.

Emniyet müdürlüğü birimleri bir polis memurunun aylık programını, arayan neredeyse herkese vermeye istekli oldukları sürece trafik cezalarından kurtulmak her zaman mümkün olacaktır. Şirketinizin ya da kurumunuzun yaptığı işlemlerde de akıllı bir toplum mühendisinin almalarını pek de istemeyeceğiniz bilgileri almak için kullanabileceği benzer açıklar var mı?

Samantha'nın İntikamı

Samantha Gregson kızgındı.

Üniversiteden işletme diploması alabilmek için çok çalışmış ve bunu başarmak için bir yığın öğrenci kredisi almıştı. Büyük paralar kazanabileceği bir kariyer sahibi olmak için üniversite diploması gerektiği her zaman beynine kazınmıştı. Sonunda mezun olmuş ama hiçbir yerde eli yüzü düzgün bir iş bulamamıştı.

Lambeck İmalat'taki işe girebildiği için çok memnun olmuştu. Sekreterlik işi yapmak küçük düşürücü olabilirdi ama Bay Cartright onu işe almaktan ne kadar memnun olduklarını ve şu anda işe sekreterlikle başlamasının, açılacak ilk idari olmayan konuma onun gelmesini sağlayacağını söylemişti.

İki ay sonra Cartright'ın en alttaki ürün yöneticilerinden birinin ayrılacağını duydu. O gece gözünü kırpmadı ve kendini beşinci katta, kapı-

sı olan bir odada, toplantılara katılıp kararlar alırken hayal etti.

Ertesi sabah ilk iş olarak Bay Cartright'ın odasına gitti. Cartright ona, profesyonel bir konuma geçmeden önce yaptıkları işin piyasasını daha iyi öğrenmesi gerektiğini düşündüklerini söyledi. Sonra da gidip, piyasayı ondan çok daha az tanıyan şirket dışından bir amatörü işe aldılar.

O zaman yavaş yavaş anlamaya başladı. Şirkette çalışan pek çok kadın vardı ama neredeyse hepsi de sekreter konumundaydılar. Ona yöneticilik görevi vermeyeceklerdi. Hiçbir zaman.

Ödeşme

Onlara bunu nasıl ödeteceğini planlaması neredeyse bir haftasını aldı. Bir ay kadar önce yeni bir ürün tanıtımı için bir ticaret dergisinden gelen adam ona asılmıştı. Birkaç hafta sonra adam Samantha'yı işten aramış ve Cobra 273 ürünüyle ilgili biraz ön bilgi verebilirse ona çiçek göndereceğini ve gerçekten çok sıkı bir bilgi olursa onu yemeğe çıkarmak için Şikago'dan kalkıp geleceğini söylemişti.

Bu konuşmadan kısa bir süre sonra şirket ağına bağlanmaya çalışan genç Bay Johannson'un yanında durmuştu. Hiç düşünmeden adamın parmaklarını seyretti (buna omuz gezintisi de denir). Parola olarak "marty63" girmişti.

Planı oluşmaya başlıyordu. Şirkete geldikten sonra yazdığı bir notu hatırladı. Dosyaların arasında bir kopyasını buldu ve ilkinin tarzını kullanarak yeni bir tane daha yazdı. Şöyle bir şey olmuştu:

> KİME: C. Pelton, Bilgi İşlem Bölümü
>
> KİMDEN: L. Cartright, Geliştirme
>
> Martin Johansson, bölümümdeki bir özel projeler ekibiyle birlikte çalışacaktır.
>
> Bu nedenle kendisine, mühendislik grubunun tüm sunucularına erişmek üzere yetki vermiş bulunuyorum. Bay Johansson'un güvenlik profilinin bir ürün geliştiricisiyle aynı haklara sahip olacak şekilde güncellenmesi gerekecektir.
>
> Louis Cartright

Herkes yemeğe çıktıktan sonra Bay Cartright'ın imzasını ilk nottan kesip yenisine yapıştırdı ve kenarlarını daksilledi. Elde ettiği şeyin bir fotokopisini çekti ve sonra fotokopinin fotokopisini çekti. İmzanın çevresindeki kâğıt kenar izleri güçlükle seçilebiliyordu.

Bay Cartrigth'ın odasının yakınındaki makinadan faks çekti.

Üç gün sonra mesaiye kaldı ve herkes gidene kadar bekledi. Johannson'un odasına girdi ve ağa adamın kullanıcı adını ve parolasını, marty63'ü, girerek bağlanmayı denedi. İşe yaradı.

Dakikalar içerisinde Cobra 273'ün ürün özelliklerini içeren dosyayı buldu ve onları sıkıştırarak bir disketin içine kaydetti.

Serin gece esintisinde park yerine doğru yürürken disket güvenli bir şekilde çantasında duruyordu. Disketi o gece dergi muhabirine yollayacaktı.

Terimler

OMUZ GEZİNTİSİ: Klavyeye bilgi giren birini, parolasını ya da başka kullanıcı bilgilerini görüp çalmak amacıyla seyretmek.

Aldatmacanın İncelenmesi

Canı sıkılmış bir çalışan, dosyaları tarar, hızlı bir kes-yapıştır ve daksilleme işleminin ardından biraz yaratıcı bir fotokopicilik yapar ve ardından faks gider. Ve bingo! Gizli pazarlama ve ürün bilgilerini dışarı çıkarmıştır.

Birkaç gün sonra bir ekonomi dergisi muhabiri çok yeni bir ürünün özellikleri ve pazarlama planlarıyla ilgili büyük bir haber patlatır. Bu haberi içeren dergi, ürünün piyasaya sürülmesinden aylar önce piyasadaki dergi abonelerinin elinde olacaktır. Rekabetçi firmalar aylar öncesinden benzer ürünler geliştirmeye başlayacaklar ve Cobra 273'ü köstekleyecek reklam kampanyaları hazırlayacaklardır.

Doğal olarak dergi hiçbir zaman haber kaynağını açıklamayacaktır.

Aldatmacanın Engellenmesi

Rekabetçi bir şirketin ya da başkalarının işlerine yarayabilecek değerli, hassas ve önemli bilgiler istendiğinde, çalışanlar, arayan numaraya bakmanın kabul edilebilir bir kimlik tespit yöntemi olmadığının bilince olmalıdırlar. Talebin geçerliliğinin ve arayanın bu bilgiyi almaya yetkili olup olmadığının, kişinin yöneticisine sorularak doğrulanması gibi farklı kontrol yöntemleri de kullanılmalıdır.

Kontrol süreci her şirketin kendisi için tanımlaması gereken bir denge unsuru içerir: Güvenlik-Üretkenlik dengesi. Bağlayıcı güvenlik önlemlerine hangi öncelikler tanınacaktır? Çalışanlar güvenlik işlemlerini uygulamaya direnecekler ve hattâ iş yükümlülüklerini yerine getirebilmek için güvenliği bir kenara mı bırakacaklardır? Çalışanlar güvenliğin kendileri ve şirketleri için taşıdığı önemin farkındalar mıdır? Şirket kültürüne ve ticari gereksinimlere göre geliştirilecek bir güvenlik politikasının bu soruları yanıtlaması gerekmektedir.

Çoğu insan, işlerini yapmalarını geciktiren şeylere kaçınılmaz olarak sıkıntı gözüyle bakar ve zaman kaybı gibi görünen herhangi bir güvenlik önlemini ciddiye almayabilir. Bu işte kilit unsur, güvenliğin günlük sorumluluklarının bir parçası olduğu konusunda çalışanları eğitimlerle teşvik etmektir.

Arayan kimliği hizmeti, şirket dışından gelen sesli aramaları tanımlamak için hiçbir zaman kullanılmasa da ONT (otomatik numara tanımlayıcısı) yöntemi kullanılabilir. Gelen tüm aramaların ücretinin şirket tarafından ödendiği bir ücretsiz arama hizmetine abone olunursa ONT hizmeti şirkete verilir ve bu, kimlik tespiti için güvenilir bir araç oluşturur. Arayan kimliğinin aksine telefon şirketi santralı arayan numarayı verirken müşterinin gönderdiği bilgiyi kullanmaz. ONT tarafından aktarılan numara arayan tarafa ait fatura numarasıdır.

Pek çok modem üreticisinin ürünlerine arayan kimliği görme özelliği eklediklerine de dikkat ediniz, böylece yalnızca önceden yetkilendirilmiş bir telefon numarası listesine uzaktan erişim hakkı tanıyarak şirket ağını korumaktadırlar. Arayan numarayı tanıyan modemler düşük güvenlikli bir ortamda kabul edilebilir tanımlama yöntemleridir, ancak şu ana kadar da açıkça görülebildiği üzere, görünen numarayı değiştirmek bilgisayar kırıcıları için nispeten kolay bir tekniktir ve bu nedenle yüksek güvenlikli bir ortamda arayanın kimliğini ve aradığı yeri tanımlamak konusunda güvenilir değildir.

Şirket telefon sisteminde bir sesli mesaj kutusu oluşturması için sistem yöneticisinin kandırıldığı hikâyedeki şekliyle kimlik hırsızlığı olayını çözmek için tüm telefon hizmetlerinin, tüm sesli mesaj kutularının ve gerek basılı gerekse çevrimiçi şirket rehberinde geçen tüm numaraların bu amaç için hazırlanmış bir form doldurularak yazılı talep edilmesini zorunlu tutun. Çalışanın yöneticisi talebi imzalamalı ve sesli mesaj yöneticisi imzayı kontrol etmelidir.

Şirket güvenlik kuralları, yeni bilgisayar hesaplarının açılmasının ya da yetkilerin artırılmasının sadece talepte bulunan kişinin olumlu onayının alınmasından sonra gerçekleştirilmesini zorunlu kılmalıdır. Talep onayı, sistem yöneticisini ya da onun yerine bakan kişiyi basılı ya da çevrimiçi şirket rehberinde geçen numarasından aramak şeklinde olabilir. Eğer şirket, çalışanların dijital olarak mesajlarını imzalayabildikleri güvenli e-posta sistemi kullanıyorsa, bu tanımlama yöntemi de geçerli bir yöntem olarak kullanılabilir.

Şirket bilgisayar sistemlerine erişimi olsun olmasın, her çalışanın bir toplum mühendisi tarafından kandırılabileceğini unutmayın. Güvenlik bilinci eğitimlerine herkesin katılmasını sağlayın. İdari yardımcılar, danışma görevlileri, santral memurları ve güvenlik görevlileri kendilerine yöneltilebilecek toplum mühendisliği saldırı tekniklerinin bilincinde olmalıdırlar. Böylece bu saldırılara karşı kendilerini savunmaya hazır olabilirler.

SANAYİ CASUSLUĞU

Devlete, şirketlere ve üniversite sistemlerine karşı oldukça yoğun bir bilgi saldırısı tehdidi vardır. Basın neredeyse her gün, yeni bir bilgisayar virüsünden, "hizmet dışıdır (denial of service)" saldırısından ya da internetteki bir e-ticaret sitesinden kredi kartı bilgilerinin çalınmasından söz etmektedir.

Borland'ın Symantec'i ticari sırlarını çalmakla suçlaması, Cadence Tasarım Sistemleri'nin bir rakibini kaynak kodlarını çalmakla suçlayarak dava açması gibi sanayi casusluğu olaylarını basında görüyoruz.

Bunlar her gün oluyor.

Bir Dalavere Üzerine Çeşitleme

Aşağıdaki öyküde anlatılan dalavere, her ne kadar Köstebek (The Insider) gibi bir Hollywood filminden ya da John Grisham'ın bir romanından fırlamış gibiyse de herhalde birçok kereler başarıyla uygulanmıştır.

Toplu Dava

Önemli bir eczacılık şirketi olan Pharmomedic'e karşı açılmış büyük bir toplu dava hayal edin. Davanın konusu, şirketin çok kullanılan ilaçlarından birinin, ancak bir hastanın ilacı yıllarca kullanmasıyla ortaya çıkabilecek, yıkıcı bir yan etkisi olduğunun şirket tarafından bilinmesidir. İddiaya göre bu tehlikenin varlığını gösteren çeşitli araştırma sonuçları şirketin elinde vardır ama bu kanıtlar saklanmış ve olması gerektiği gibi FDA'ya (Food and Drug Administration - Gıda ve İlaç İdaresi) teslim edilmemiştir.

Toplu davayı açan New York hukuk firmasının başındaki yetkili avukat William ("Billy") Chaney'in elinde iddiayı destekleyen iki Pharmomedic doktoruna ait görevden alınma belgeleri vardır. Ancak her iki doktor da emekli olmuş ve ne ellerinde dosya ya da belge vardır, ne de güçlü ve ikna edici bir şekilde tanıklık yapacak konumdadırlar. Billy durumunun sallantıda olduğunun farkındadır. Sonuç raporlarından birinin bir kopyasını ya da yöneticiler arasında gidip gelmiş bir yazışma ya da bilgi notunu elde edemezse, dava düşecektir.

Böylece, daha önce de kendilerine iş verdiği, Andreeson ve Oğulları özel dedektiflik acentasına yeni bir işle gider. Billy, Pete ve adamlarının o bilgileri nasıl elde ettiklerini bilmez, bilmek de istemez. Tek bildiği, Pete Andreeson'un iyi bir dedektif olduğudur.

Andreeson için bu tarz bir görev, kendisinin karanlık işler dediği türden bir iştir. Birinci kural, onu tutan şirketler ve hukuk firmaları hiçbir zaman bilgiyi nasıl elde ettiğini öğrenemeyeceklerdir ve böylece her zaman tam ve akla yatkın bir inkâr nedenleri olacaktır. Eğer elini taşın altına sokacak biri varsa bu da Pete'tir ve büyük işlerde aldığı ücretlere bakılırsa bu tehlikeye girdiğine değer gibi görünmektedir. Ayrıca insanları tongaya düşürmekten de kişisel bir zevk almaktadır.

Eğer Chaney'in bulmasını istediği dosyalar gerçekten varlarsa ve imha edilmemişlerse, Pharmomedic'in dosyaları arasında bir yerlerde olmaları gerekir. Ama onları koca şirketin dev dosya yığınının arasında bulmak büyük bir iş olacaktır. Öte yandan dosyaların kopyalarını kendi hukukçularına, Jenkins ve Petry'e de vermiş olabilirler. Eğer savunma avukatları bu belgelerin varlığından haberdarlarsa ve araştırma safhasında onları geri çevirmedilerse, o zaman hukukçuluk mesleğinin etiğine aykırı davranmışlar ve yasaları çiğnemişlerdir. Pete'in kitabında, böyle bir durum her saldırıyı mübah kılmaktadır.

Pete'in Saldırısı

Pete adamlarından bazılarını bu konuyu araştırmaları için görevlendirir ve birkaç gün içinde Jenkins ve Petry'nin kendi bünyelerinde tutmadıkları yedeklemelerini hangi şirkette sakladıklarını öğrenir. Ayrıca saklama şirketinin elinde, hukuk firmasının bantları almak için yetkilendirdiği kişilere ait bir liste olduğunu da öğrenir. Bu insanların her birinin kendilerine ait parolaları olduğu da bilinen şeyler arasındadır. Pete, adamlarından ikisini karanlık bir iş yapmaları için yollar.

Adamlar internette www.southord.com adresinden sipariş edilebilecek bir maymuncukla kilidi açarlar. Birkaç dakika içinde, sabaha karşı üç sularında saklama şirketinin bürolarına sızarlar ve bir bilgisayarı açarlar. Windows 98 logosunu görmek hoşlarına gider, çünkü bu, işin çok kolay olacağı anlamına gelmektedir. Windows 98 kendini tanıtmanı gerektirmez. Kısa bir aramadan sonra saklama şirketi müşterilerinden her birinin, bantları alması için yetkilendirdiği insanların adlarının bulunduğu bir Microsoft Access veritabanı bulurlar. Jenkins ve Petry yetki listesine sahte bir ad eklerler. Bu ad, adamlardan birinin bulduğu sahte ehliyetlerden birindeki adla aynıdır. (Kilitli depo bölgesine zorla girip müşterinin istediği bantları da o anda bulabilirler miydi? Kesinlikle; ama o zaman, aralarında hukuk firmasının da olduğu tüm müşteriler şirkete girildiğini öğrenirler ve saldırganlar üstünlüklerini kaybederlerdi. Profesyoneller "gerekirse" diye her zaman gelecekte ulaşabilecekleri açık bir kapı bırakırlar.)

Sanayi casuslarının gelecekte kullanmak üzere arka cepte tutma uygulamasını uyarak, her ihtimale karşı, yetkilendirme listesinin olduğu dosyayı bir diskete kopyalarlar. Hiçbirinin bunun nerede işe yarayabileceği konusunda bir fikri yoktur ama bu da arada bir işe yarayan, "Hazır gelmişken şunu da alsak", türünden bir bilgidir.

Mitnick Mesajı:

Değerli bilgiler ne şekilde olurlarsa olsunlar ya da nerede dururlarsa dursunlar korunmalıdırlar. Bir kuruluşun müşteri listesi kâğıt üzerinde ya da elektronik dosya olarak ofisinizde veya bir kasada dursa da aynı değere sahiptir. Toplum mühendisleri, çevresinden en kolay dolaşacakları ve en az korunan saldırı noktasını her zaman tercih ederler. Bir şirketin şirket dışı yedekleme bantlarını sakladığı yer, farkedilme ya da yakalanma tehlikesinin düşük olduğu bir nokta olarak görülmüştü. Değerli, hassas ve önemli verilerini üçüncü şahıslara emanet eden her kuruluş gizliliğini korumak için verilerini şifremelidir.

Ertesi gün adamlardan biri saklama şirketini arayarak, yetki listesine ekledikleri adı ve ada ait parolayı verir. Geçen aya ait tüm Jenkins ve Petry bantlarını ister ve paketi bir kurye servisinin gelip alacağını söyler. İkindi vaktinde bantlar Andreeson'un elindedir. Adamları, istedikleri zaman tarama yapacak şekilde, tüm verileri kendi bilgisayar sistemlerine aktarmışlardır. Pek çok başka şirket gibi, hukuk firmasının da yedeklenmiş verilerini şifrelemeyle uğraşmaması Andreeson'u memnun eder.

Bantlar ertesi gün saklama şirketine teslim edilir ve kimsenin operasyondan haberi olmaz.

Aldatmacanın İncelenmesi

Gevşek fiziksel güvenlik nedeniyle, kötü adamlar saklama şirketinin kilidini kolaylıkla açmışlar, bilgisayarına ulaşmışlar ve saklama deposuna ulaşmaya yetkili kişilerin listesinin bulunduğu veri tabanıyla oynamışlardır. Listeye bir ad eklemek sahtekârların, şirketin saklama deposuna zorla girmelerine gerek bırakmadan istedikleri yedekleme bantlarını elde etmelerini sağlamıştır. Çoğu şirket, yedekleme dosyalarını şifrelemediğinden, bilgi olduğu gibi orada durmaktadır.

Bu olay, geçerli güvenlik önlemleri almayan bir hizmet şirketinin, saldırganların müşterisinin bilgi varlıklarına ulaşmasını nasıl kolaylaştırdığına bir örnek daha oluşturuyor.

Yeni İş Ortağı

Toplum mühendislerinin sıradan dolandırıcılara ve üçkâğıtçılara göre bir üstünlüğü vardır, bu da uzaklıktır. Bir üçkâğıtçı, yalnızca yanınızdayken sizi kandırabilir ve eğer oyuna geldiğinizi yeterince erken anlarsanız, onu iyice tarif edebilir hattâ polisleri zamanında çağırabilirsiniz.

Toplum mühendisleri çoğunlukla bu tehlikeden hastalıkmış gibi uzak dururlar. Ancak bazen bu tehlikeye de girmek gerekir.

Jessica'nın Öyküsü

Jessica Andover gösterişli bir robotik şirketinde çalıştığı için çok mutluydu. Yalnızca yeni nesil bir teknoloji şirketiydi ve pek de iyi para vermiyor olabilirdi ama küçüktü ve çalışanları arkadaş canlısıydı. Ayrıca kendisine verilen şirket hisse senetlerinin her an onu zengin edebileceğini bilmenin heyecanı da vardı. Belki şirket kurucuları gibi milyoner olmazdı ama yeterince zengin olurdu.

Ağustos'ta bir Salı sabahı lobiden girdiğinde Rick Daggot'un ışıl ışıl gülümsemesine neden olan şey de aynen buydu. Pahalı görünümlü takım elbisesi (Armani), ağır altın kol saati (Rolex President) ve kusursuz saç kesimiyle, lise yıllarında Jessica gibi kızları çılgına çeviren türden, erkeksi, kendine güvenli bir havaya sahipti.

"Merhaba", dedi adam. "Ben Rick Daggot. Larry'yle randevum vardı."

Jessica'nın gülümsemesi birden kayboldu. "Larry mi?" deyiverdi. "Larry bu hafta tatilde."

Rick, elektronik ajandasını çıkarıp açtıktan sonra ona göstererek, "Saat birde onunla randevum var. Onunla buluşmak için Louisville'den buraya uçtum", dedi. Jessica ona baktı ve başını olumsuz bir şekilde iki yana salladı. "Yirmisi" dedi. "Bu gelecek hafta." Adam avuç içi bilgisayarını kendine çevirip baktı. "Ah, hayır!" diye inledi. "Yaptığım aptallığa inanamıyorum."

"En azından sizin için dönüş biletinizi ayarlayabilir miyim?" diye sordu kız, adam için üzülerek.

Kız telefon görüşmesini yaparken Rick, Larry'yle birlikte bir stratejik pazarlama ortaklığı kurmayı tasarladıklarını itiraf etti. Rick'in şirketi üretim ve montaj bandı için ürünler üretiyordu. Bu parçalar yeni ürünleri C2Alpha'yı mükemmel bir şekilde tamamlayacaktı. Rick'in ürünleri ve C2Alpha birlikte, her iki şirket için de önemli sanayi pazarları açacak güçlü bir çözüm oluşturacaktı.

Jessica öğleden sonra geç bir saate uçak reservasyonunu yapmayı bitirdiğinde, Rick, "En azından, eğer buradaysa Steve'le görüşebilirim", dedi. Ama şirketin genel müdür yardımcısı ve kurucularından biri olan Steve de ofis dışındaydı.

Jessica'ya çok iyi davranan ve biraz da asılan Rick, burada olduğuna ve öğleden sonra geç saatlere kadar eve dönemeyeceğine göre bazı kilit kişileri öğle yemeğine götürmek istediğini söyledi. Sonra da ekledi, "Sen de tabii; öğle saatinde yerine bakabilecek biri var mı?"

Kendisinin de aralarına katılacağı düşüncesiyle mahcup olan Jessica sordu, "Kimlerin gelmesini istiyorsun?" Adam, yeniden avuç içi bilgisayarına baktı ve birkaç kişinin -AR-GE'den iki mühendisin, yeni satış ve

pazarlama sorumlusunun ve projeye atanan finans müdürünün- adını verdi. Rick, Jessica'ya şirketle olan ilişkisini onlara anlatmasını önerdi ve kendini onlara tanıtmak istediğini söyledi. Jessica'nın her zaman gitmek istediği, çevredeki en iyi lokantaya gideceklerini ve saat 12:30 için bir masa ayırtacağını da ekledi. Her şeyin yolunda olup olmadığından emin olmak için öğleden önce arayacaktı.

Lokantada buluştuklarında -dördü ve Jessica- masa henüz hazır değildi, böylece bara oturdular ve Rick içkileri ve yemeği kendisinin ödeyeceğini bir kez daha vurguladı. Rick, tarzı ve kalitesi olan bir adamdı. İlk tanıştığınız andan itibaren onun yanında kendinizi yıllardır tanıdığınız birinin yanında olduğunuz kadar rahat hissediyordunuz. Her zaman ne söylemesi gerektiğini iyi biliyormuş gibi görünüyor, sohbet durulduğunda neşeli ya da komik bir yorum yapabiliyor ve onun yakınlarında olduğunuz için kendinizi iyi hissetmenizi sağlıyordu.

Kurmakta çok hevesli göründüğü ortak pazarlama çözümünü hepsinin gözlerinde canlandırmasına yetecek kadar, kendi şirketinin ürünleriyle ilgili de yeterince ayrıntı anlatmıştı. Şirketinin satış yapmakta olduğu pek çok Fortune 500 şirketinin adını da vermiş, masadaki herkese, fabrikadan çıktığı andan itibaren, ürünlerinin çok iyi iş yapacağı hayalini kurdurmayı başarmıştı.

Sonra Rick mühendislerden biri olan Brian'ın yanına geçti. Diğerleri kendi aralarında sohbet ederlerken, Rick bazı fikirlerini Brian'la özel olarak paylaştı ve ondan C2Alpha'nın kendine özgü nitelikleri ve onu piyasadaki benzerlerinden neyin ayırdığı gibi bilgiler aldı. Brian'ın gurur duyduğu ve çok "sıkı" olduğunu düşündüğü bir iki özelliği şirketin önemsizmiş gibi göstermeye çalıştığını da öğrendi.

Rick, tarzını sürdürüp her biriyle küçük sohbetler etti. Pazarlama sorumlusu, piyasaya sürüm tarihi ve pazarlama planlarından bahsetme olanağı bulduğu için mutluydu. Cebinden bir zarf çıkardı. Malzeme ve imalat maliyetlerinin ayrıntılarını, fiyat noktası ile beklenen kâr payını, adlarını sıraladığı satıcılarla ne tür anlaşmalar yaptığını bir bir anlattı.

Masaları hazır olduğunda Rick herkesle görüş alışverişinde bulunmuş ve herkesi kendine hayran bırakmıştı. Yemeğin sonunda hepsi Rick'le tokalaşıp teşekkür ettiler. Rick her biriyle kartvizit alıp verdikten sonra, mühendis olan Brian'a Larry döner dönmez daha uzun bir görüşme yapmak istediğini de söyledi.

Ertesi gün Brian telefonu açtığında arayanın Rick olduğunu görmüştü. Rick az önce Larry'le konuştuğunu söylüyordu. "Bazı özellikleri görüşmek için Pazartesi geri geleceğim", dedi. "Sizin ürünle ilgili en kısa sürede bilgi sahibi olmamı istiyor. En son tasarımları ve özellikleri ona e-postalamanı istediğini söyledi. Bilmemi istediği kısımları çıkarıp, bana yollayacak."

Mühendis bunun uygun olacağını söyledi. "İyi", diye karşılık verdi Rick. Sonra sürdürdü, "Larry e-postasına ulaşmakta bir sorun yaşıyormuş. Otelin iş merkezinden kendisine bir Yahoo adresi almalarını rica etmiş. Belgeleri onun her zaman kullandığı e-posta adresine göndermek yerine dosyaları larryrobotics@yahoo.com adresine göndermen gerekiyormuş."

Ertesi Pazartesi sabahı Larry güneşten yanmış ve rahatlamış olarak girdiğinde Jessica ilk haberi vermek ve Rick'i öve öve anlatmak için çok heyecanlıydı. "Ne müthiş bir adam. Bazılarımızı yemeğe götürdü, beni bile." Larry anlamamış gibi duruyordu. "Rick mi? Rick de kim ya?"

"Neden söz ediyorsun? Yeni iş ortağın."

"Ne!!!???"

"Sorduğu sorulardan herkes çok etkilendi."

"Rick diye birini tanımıyorum ..."

"Senin neyin var? Şaka mı bu, Larry? Benimle dalga geçiyorsun değil mi?"

"Yöneticileri konferans salonuna topla. Hemen şimdi. Ne işleri varsa bırakıp gelsinler. O gün öğle yemeğine gelenleri de çağır. Sen de dahil."

Kasvetli bir havada, pek konuşmadan masanın çevresine toplandılar. Larry içeri girip oturdu ve konuşmaya başladı. "Rick adında kimseyi tanımıyorum. Sizden sakladığım bir iş ortağım da yok. Bunun en azından açık olduğunu düşünüyordum. Eğer aramızda şaka yapmaktan hoşlanan biri varsa, şimdi ortaya çıkmasını istiyorum."

Hiç ses çıkmadı. Her an oda daha kararıyormuş gibiydi.

Sonunda Brian konuştu. "Ekinde ürün özellikleri ve kaynak kodu olan e-postayı sana gönderdiğimde neden birşey söylemedin?"

"Ne e-postası?!"

Brian gerildi. "Ah ... hayır!"

Cliff, diğer mühendis, araya girdi. "Hepimize kartvizitini verdi. Tek yapmamız gereken onu arayıp neler olup bittiğini öğrenmek."

Brian avuç içi bilgisayarını çıkardı, bir bilgiye baktı ve aleti masanın üstünden kaydırarak Larry'e doğru itti. Ümitlerini kesmeden hepsi hipnotize gibi Larry'nın telefonu çevirişini seyrediyorlardı. Bir an sonra telefonun hoperlörünü açan düğmeye bastı ve hepsi meşgul sesini duydular. Yirmi dakika boyunca numarayı defalarca çevirdikten sonra, canı iyice sıkılmış Larry acil bir kesinti yaratmasını rica etmek için santralı aradı.

Biraz sonra santral yeniden hattâ geldi. Meydan okur bir tonda, "Beyefendi bu numarayı nereden buldunuz?" diye sordu. Larry acilen gö-

rüşmesi gereken bir adamın kartvizitinden aldığını söyledi. Santral, "Üzgünüm", dedi. "O bir telefon şirketi test numarası. Her zaman meşgul çalar."

Larry, Rick'le paylaşılan bilgilerin bir listesini çıkarmaya başladı. Görüntü hiç iyi değildi.

İki polis dedektifi gelip tutanak tuttular. Hikâyeyi dinledikten sonra, eyalet kanunlarına göre herhangi bir suç işlenmediğini ve yapabilecekleri bir şey olmadığını söylediler. Larry'e FBI'la görüşmesini önerdiler, çünkü eyaletler arası ticaretle ilgili suçlar onların yetki alanına giriyordu. Rick Daggot kendini farklı tanıtarak mühendisten test sonuçlarını göndermesini istediğinde federal bir suç işlemiş olabilirdi ama bunu öğrenmek için FBI'la konuşması gerekiyordu.

Üç ay sonra Larry mutfakta oturmuş, kahvaltı edip gazetesini okurken az kalsın kahvesini döküyordu. "Rick" adını ilk duyduğu andan beri olmasından korktuğu şey, en büyük kâbusu gerçekleşmişti. Ekonomi sayfasında büyük puntolarla verilen haberde, daha önce adını hiç duymadığı bir şirketin, geçen iki yıldır kendi şirketinin geliştirdiği C2Alpha'nın tıpatıp aynısı gibi görünen yeni ürününü piyasaya sürdüğünü duyuruyordu.

Kandırmaca yoluyla o insanlar pazarda öne geçmişlerdi. Rüyaları yıkılmıştı. Araştırmaya ve geliştirmeye yatırılan milyonlarca dolar ziyan olmuştu. Ve onlara karşı tek bir kanıtı bile yoktu.

Sammy Sanford'un Öyküsü

Düzgün bir işte çalışıp büyük paralar kazanacak kadar akıllı ama bir dolandırıcı olarak hayatını kazanmayı tercih edecek kadar da sahtekâr bir adam olan Sammy Sanford kendini çok iyi idare ediyordu. Zamanında içki sorunu olduğu için erken emekliliğe zorlanmış bir casusun dikkatini çekmişti. Adam kızgın ve intikam doluydu ve devletin onu uzmanlaştırdığı yetenekleri satmanın bir yolunu bulmuştu. Her zaman kullanabileceği insanlara karşı gözü açıktı ve ilk karşılaştıklarında Sammy'nin yeteneğini görmüştü. Sammy bu işi kolay bulmuş ve ilgi noktasını insanların paralarını çarpmaktan şirket sırlarını çarpmaya doğru çevirmenin oldukça kazançlı olduğunu da görmüştü. Devamını kendisinden dinleyelim:

Çoğu insanın benim yaptığım işleri yapacak cesareti yoktur. İnsanları telefondan ya da internet üzerinden kandırmaya çalışırsınız ve kimse sizi görmez. Ama eski usul, yüz yüze türünden iyi bir dolandırıcı (ve onlardan, ortalıkta düşündüğünüzden daha çok var) gözünüzün içine bakıp kuyruklu bir yalan söyler ve siz ona inanırsınız. Bunun suç olduğunu düşünen bir iki savcı biliyorum. Ben buna yetenek derdim.

Ama gözünüzü kapatıp işe dalamazsınız, önce ortalığı yoklamanız

gerekir. Sokakta tavcılık yaparken dostça bir sohbetle ve dikkatle kurulmuş cümlelerle adamın nabzını yoklayabilirsiniz. Doğru yanıtları alırsınız ve şak!.. kuşu kafese alırsınız.

Şirket işi, büyük dalavere dediğimiz türden bir iştir. Önden hazırlık yapmanız gerekir. Hassas noktalarının ne olduğunu, ne bilmek istediklerini, neye ihtiyaçları olduğunu bilmelisiniz. Bir saldırı planlayın, sabırlı olun, ödevinizi yapın. Oynayacağınız rolü belirleyin ve ne söyleyeceğinizi iyi çalışın. Hazır olana kadar kapılarına gitmeyin.

Bu iş için hız kazanana kadar üç haftadan fazla zaman harcadım. Müşteri, "şirketimin" ne yaptığını ve bunun neden iyi bir pazarlama ortaklığı olacağını nasıl anlatacağımı bana iki günde öğretti.

Sonra şansım yaver gitti. Şirketi aradım ve bir girişim sermayesi şirketinden aradığımı, bir toplantı ayarlamak istediğimizi söyledim. Önümüzdeki bir iki ay içinde tüm ortaklarımızın bulunabileceği bir zaman ayarlamaya çalışıyorum. Uzak durmam gereken, Larry'nin şehirde olmayacağı herhangi bir zaman aralığı var mıydı acaba? Ve kadın "evet" dedi. Şirketi kurduğundan beri iki yıldır hiç tatil yapmamıştı; ancak kararı Ağustos'un ilk haftasında onu bir golf tatiline sürüklüyordu.

Yalnızca iki hafta sonraydı. Bekleyebilirdim.

Bu sırada bir ekonomi dergisinden, şirketin halkla ilişkilerini yürüten firmanın adını buldum. Robotik şirketi müşterileri için topladıkları ilginin hoşuma gittiğini ve onların işini kim görüyorsa kendi şirketimle ilgili olarak onunla konuşmak istediğimi belirttim. Yeni bir müşteri kazanma fikrinden hoşlanan cıvıl cıvıl genç bir hanım olduğu ortaya çıktı. Pahalı bir öğle yemeğinde, niyetlendiğinden bir kadeh fazla içti ve "müşterilerinin sorunlarını anlamakta ve doğru halkla ilişkiler çözümleri bulmakta ah ne kadar iyi" olduklarına beni ikna etmek için elinden geleni yaptı. İkna edilmesi güç birini oynuyordum. Bazı ayrıntılara ihtiyacım vardı. Biraz dürtüklemenin ardından masa temizlenene kadar bana yeni ürün ve şirketin karşılaştığı sorunlar hakkında beklediğimden daha çok şey anlatmıştı.

Her şey tıkır tıkır yürüdü. Buluşmanın gelecek hafta olmasıyla ilgili çok mahcup olduğum ama gelmişken ekiple tanışabileceğim öyküsünü danışma görevlisi olduğu gibi yutmuştu. Hattâ arada bana acımıştı bile. Öğle yemeği, bahşiş dahil, bana 150 dolara mal oldu ve istediğimi aldım. Telefon numaraları, unvanlar ve söylediğim kişi olduğuma inanan kilit bir mühendis.

Brian'ın beni şaşırttığını itiraf etmeliyim. Ne istesem gönderecek türden bir adama benziyordu. Konuyu açtığımda, bir şeyleri söylemiyormuş gibi gelmişti. Beklenmeyeni beklemek her zaman işe yarar. Larry adına alınmış e-posta adresi, her olasılığa karşı arka cebimde duruyordu. Yahoo güvenlik sorumluları, izleyebilmeleri için adresi birinin kullan-

masını herhalde hâlâ bekliyorlardır. Daha çok bekleyecekler. İş işten geçmişti. Ben yeni bir projeye atılmıştım bile.

Aldatmacanın İncelenmesi

Yüz yüze dalavere çeviren kişi kendini hedefe kabul ettirebilecek bir şekilde göstermelidir. Yarışlara giderken kendini başka bir şekle sokarken, mahallenin barına giderken başka, havalı bir otelin şık barına giderken daha başka görünecektir.

Sanayi casusluğunda da aynı şekildedir. Eğer casus, oturmuş bir firmanın yöneticisi, bir danışman ya da satış sorumlusu kılığına girecekse yapacağı saldırı ceket giyip kravat takmayı ve pahalı bir çanta taşımayı gerektirebilir. Bir yazılım mühendisi, teknik eleman ya da posta odasından biri gibi davranacağı başka bir işte giysiler, üniforma, her şey farklı görünmelidir.

Şirkete sızabilmek için kendini Rick Daggot olarak tanıtan kişinin şirketin ürünü ve piyasayla ilgili ayrıntılı bilgiyle donanmış, bir güven ve başarı görüntüsü oluşturması gerekiyordu.

Önceden bilmesi gereken bilgiyi edinmekte çok güçlük çekmemişti. Genel müdürün ne zaman yerinde olmayacağını öğrenmek için basit bir oyun oynamıştı. Çok zor olmasa da, biraz dikkat gerektiren konu, yaptıklarıyla ilgili "konuya hakim" görünecek kadar projeye yönelik bilgi toplamaktı. Bu tarz bilgiler çoğu zaman mal aldıkları şirketlerin, yatırımcıların, para toplamak için konuştukları girişim sermayecilerinin, çalıştıkları bankanın ve hukuk şirketinin bildikleri şeylerdi. Ancak saldırgan dikkatli olmalıydı. Şirket içi bilgileri paylaşabilecek birini bulmak zor bir işti ve bilgi alınabilecek birini bulmak için iki ya da üç kaynağı yoklamak

Mitnick Mesajı:

Her ne kadar çoğu toplum mühendisliği saldırısı telefon ya da e-posta üzerinden gerçekleşse de gözükara bir saldırganın işyerinizde şahsen belirmeyeceğini düşünmemelisiniz. Çoğu zaman sahtekâr, Photoshop gibi kolayca bulunabilen bir yazılımı kullanarak bir personel kartının sahtesini hazırladıktan sonra şirket binasına girebilmek için bazı toplum mühendisliği tekniklerini kullanır. Ya telefon şirketinin test numarasının yazılı olduğu kartvizitlere ne demeli? Bir özel dedektiflik dizisi olan Rockford Dosyaları adlı televizyon programında akıllıca ve eğlenceli sayılabilecek bir teknik gösterilmişti. Aktör James Garner'ın oynadığı Rockford karakterinin arabasında, gerektiği hallerde uygun kartı basmak için kullandığı, taşınabilir bir kartvizit basma makinası vardı. Bu günlerde toplum mühendisleri kartvizitlerini bir saat içinde bir fotokopicide bastırabilir ya da bir lazer yazıcıdan çıktı alabilirler.

NOT: *Soğuktan Gelen Casus, Son Casus ve daha pek çok dikkate değer romanın yazarı olan John Le Carre, itinalı, yaşam boyu dolandırıcılıkla uğraşmış bir babanın oğlu olarak büyüdü. Daha Le Carre bir çocukken, babasını başkalarını kandırmakta başarılı olmasına rağmen, alınmak durumuna düşüp başka bir dolandırıcının kurbanı olduğunu öğrendiğinde çok şaşırmıştı. Bu da herkesin, hattâ bir toplum mühendisinin bile, başka bir toplum mühendisi tarafından avlanabileceğini bize gösteriyor.*

insanların oynanan oyunu farketmelerine neden olabilirdi. O taraf tehlikeliydi. Dünyadaki Rick Daggot'lar seçimlerini dikkatle yapmalı ve her bilgi patikasından bir kez geçmelidirler.

Öğle yemeği de başka bir zorlu girişimdi. Öncelikle her şeyi öyle ayarlamalıydı ki, diğerlerine duyurmadan herkesle birkaç dakika yalnız kalabilmeliydi. Jessica'ya 12:30 dedi ama masayı saat 13:00 için ayırttı. Yemek yiyecekleri yer, hesabı şirket masraflarına ekleyebileceğiniz türden, şık bir lokantaydı. Saat oynamasının birer içki için bara oturmalarını gerektireceğini umuyordu, tam da böyle olmuştu. Tek tek herkesin yanlarına gidip sohbet etmek için kusursuz bir fırsattı.

Yine de Rick'in bir sahtekâr olduğunu ortaya çıkaracak, atabileceği bir sürü yanlış adım vardı. Ancak kendine fazlasıyla güvenen ve kurnaz bir sanayi casusu kendini böyle bir tehlikeye maruz bırakırdı. Ama yıllarca sokaklarda tavcı olarak çalışmak Rick'in yeteneklerini geliştirmiş ve dili sürçse de tüm kuşkuları yatıştıracak kadar iyi bir şekilde olayı kapatabileceğine dair kendine güvenmesini sağlamıştı. Burası tüm sürecin en zorlu ve en tehlikeli kısmıydı ve böyle bir dalavereyi çevirirken duyduğu kıvanç neden hızlı arabalar kullanmadığı, gök dalışı (skydiving) yapmadığı ya da karısını aldatmadığını anlamasını sağlamıştı. İşini yaparken yeterince heyecanlanıyordu. Kaç kişi, diye merak etti, kaç kişi bu kadar şanslı olabilirdi ki?

Aklı başında bir avuç kadın ve erkeğin aralarına bir sahtekârı almalarının nedeni ne olabilir? Oluşan bir durumu hem aklımızla hem de içgüdülerimizle tartarız. Eğer anlattığı hikâye tutarlıysa -bu, akılla yapılan kısımdır- ve dolandırıcı inanılır bir görüntü çizdiyse çoğu zaman yelkenleri suya indiririz. Başarılı bir dolandırıcıyı ya da toplum mühendisini parmaklıkların arkasına düşenlerden ayıran unsur inanılır görüntüdür.

Kendi kendinize sorun: Rick'in anlattığı gibi bir öyküyü asla yutmayacağımdan ne kadar eminim? Eğer yutmayacağınızdan eminseniz, o zaman kendinize birinin size böyle bir numara yapmaya kalkıp kalkmadığını sorun. Eğer ikinci soruya verdiğiniz yanıt evetse, büyük olasılıkla birinci sorunun doğru yanıtı da bu olacaktır.

Birdirbir

Size bir soru: Aşağıdaki öyküde sanayi casusluğuyla ilgili bir şey yoktur. Okurken, bakın bakalım, neden bu öyküyü bu bölümde anlattığımı anlayabilecek misiniz!

Harry Tardy evine dönmüştü ve canı sıkkındı. Askere yazılmak, acemi birliğinden atılana kadar, çok iyi bir fikir gibi gelmişti. Şimdi nefret ettiği bu yere geri dönmüş yerel yüksekokulda bilgisayar dersleri alıyor ve dünyaya bir tokat patlatmanın yollarını arıyordu.

Sonunda bir plan yaptı. Sınıfındaki adamlardan biriyle bir kadeh bir şey içerlerken, herkesi küçümseyen, çok bilmiş bir herif olan hocalarından şikâyet ediyorlardı. Birlikte adamı yakacak kurnaz bir plan yaptılar. Çok kullanılan bir PDA'nın (personal digital asistant - kişisel dijital yardımcı) kaynak kodunu ele geçirecekler ve şirketin, kötü adamın bilgisayar hocası olduğunu düşüneceği şekilde geride iz bırakarak, hocanın bilgisayarına göndereceklerdi.

Yeni arkadaş Karl Alexander, birkaç numara bildiğini söylemişti ve bu işin nasıl kotarılacağını Harry'ye gösterecekti. Tabii, yakalanmadan.

Ödevlerini Yapıyorlar

Yaptığı ilk araştırmada Harry, ürünün, PDA üreticisinin deniz aşırı bir yerdeki Genel Müdürlüğü'ne bağlı Geliştirme Merkezi'nde yapıldığını öğrenmişti. Ama Birleşik Devletler'de de bir Ar-Ge merkezi vardı. Karl'ın söylediğine göre bu iyi bir şeydi, çünkü yaptıkları işin yürümesi için Birleşik Devletler'de de kaynak koduna ihtiyaç duyan bir şirkete ait bir tesis olması gerekiyordu.

Bu noktada Harry deniz aşırı Geliştirme Merkezi'ni aramaya hazırdı. Burada devreye kendini acındırma girecekti. "Aman tanrım, başım dertte, yardıma ihtiyacım var, lütfen, lütfen bana yardım edin." Yapacakları acındırma doğal olarak bundan daha üstü kapalı olacaktı. Karl bir metin yazdı ama Harry onu okumaya çalışırken sahte olduğu çıkardığı her sesten belli oluyordu. Sonuç olarak söylemek istediğini sohbet eder gibi söyleyebilmesi için Karl'la oturup çalıştılar.

Sonunda, Karl yanında otururken, Harry'nin söylediği şey aşağıdaki gibiydi.

"Minneapolis Ar-Ge'den arıyorum. Sunucumuza tüm bölümü etkileyen bir solucan girdi. İşletim sistemini yeniden yüklememiz gerekti ve yedekleri geri yükleyeceğimiz zaman yedeklemelerden hiçbirinin sağlam olmadığını gördük. Bilin baka-

Terimler

GZIP: Bir Linux GNU uygulaması kullanarak dosyaların tek bir sıkıştırılmış dosyada toplanması.

Terimler

HERKESE AÇIK FTP: FTP (file transfer protocol - dosya aktarım protokolü) kullanıcı adı bile olmaksızın herkesin ulaşıp dosya yerleştirebileceği ve görebileceği veri saklama alanlarıdır. Her ne kadar herkese açık FTP'lere parolasız erişim mümkünse de genellikle belli kalsörlerin kullanıcı hakları sınırlandırılmıştır.

lım yedeklerin sağlamlığını kimin kontrol etmesi gerekiyor? Bendenizin. Bu yüzden patronumdan bir araba dolusu fırça yedim ve yöneticiler veri kaybettik diye veryansın ettiler. Mümkün olduğu kadar hızlı, kaynak kodu klasörünün en son haline ihtiyacım var. Ne kadar hızlı gönderebilirseniz o kadar iyi. Kaynak kodunu zip'leyip bana göndermenizi rica ediyorum."

Bu aşamada Karl bir kâğıda bir not yazıp verdi ve Harry telefonun diğer ucundaki adama dosyayı dahili olarak Minneapolis Ar-Ge'ye yollamasını istediğini söyledi. Bu önemli bir ayrıntıydı. Telefonun ucundaki adam, dosyanın şirketin başka bir bölümüne gönderilmesinin istendiğinden emin olunca, rahatlamıştı; bunda ne terslik olabilirdi ki?

Adam dosyaları zip'leyip göndermeyi kabul etti. Karl yanındayken Harry, büyük kaynak kodunu tek bir dosyaya sığdırmak için yapması gerekenleri adama adım adım anlattı. Ayrıca sıkıştırılmış dosyada kullanması için bir dosya ismi verdi: "yeniveri". Bunun eski, bozuk dosyalarla karışmaması için gerekli olduğunu da anlattı.

Bir sonraki adımı Harry'nin anlaması için Karl'ın iki kere anlatması gerekmişti ama Karl'ın hayalini kurduğu küçük birdirbir oyunu için bu önemliydi. Harry Minneapolis Ar-Ge'yi arayacak ve oradaki birineşöyle diyecekti: "Size bir dosya göndermek istiyorum ve sonra bu dosyayı benim için başka bir yere göndermenizi rica ediyorum." Bu talep doğal olarak kulağa akla yatkın gelen her türlü nedenle süslenip püslenmişti. Harry'nin kafasını karıştıran şey şuydu: "Size bir dosya göndereceğim", demesi gerekiyordu ancak dosyayı gönderecek kişi kendisi değildi. Ar-Ge bölümünde konuştuğu adamın dosyanın kendisinden geldiğini düşünmesini istiyordu. Aslında merkeze gelecek dosya Avrupa'dan gelen tescilli kaynak kodu dosyasıydı. "Başka bir kıtadan gelen bir şey için neden ben gönderdim diyorum?" Harry bunun nedenini bilmek istiyordu.

"Ar-Ge Merkezi'ndeki adam kilit kişi", diye açıkladı Karl. "Amerika'daki bir başka çalışana bir iyilik yaptığını düşünüyor olması gerek, senden bir dosya alacak sonra senin için o dosyayı başka birine iletecek."

Harry sonunda anlamıştı. Ar-Ge Merkezini aradı, Bilgisayar Merkezi'yle görüşmek istediğini söyledi, orada da bir bilgisayar operatörüyle konuşmak istedi. Sesi Harry kadar genç gelen biri çıktı telefona. Harry ona "merhaba" dedi ve şirketin Chicago üretim bölümünden aradığını ve birlikte bir projede çalıştıkları bir dosyayı ortaklarından birine gönder-

meye çalıştığını açıkladı. "Ancak", dedi ve ekledi, "Yönlendiricide bir sorun var ve onların ağına ulaşamıyor. Dosyayı size göndermek istiyorum. Dosyayı gönderdikten sonra sizi arayıp onu ortağın bilgisayarına aktarmanız için gerekli adımları anlatırım."

Şimdilik her şey yolundaydı. Sonra Harry adama bilgisayar merkezinin herkese açık bir FTP hesabının olup olmadığını sordu. Bu, bir dizine dosya yüklemek ya da bir dizinden dosya almak için kullanılan parolasız bir alandı. Evet, herkese açık FTP vardı ve adam oraya ulaşmak için gerekli olan IP adresini Harry'e verdi.

Eldeki bu bilgilerle Harry denizaşırı Geliştirme Merkezi'ni yine aradı. Sıkıştırılmış dosya hazırdı ve Harry herkese açık FTP sitesine dosyayı aktarmak için gerekli açıklamaları yaptı. Beş dakikadan kısa bir süre içinde sıkıştırılmış kaynak kodu dosyası Ar-Ge Merkezi'ndeki çocuğa gönderilmişti.

Kurbanı Tuzağa Düşürmek

Hedeflerine giden yolu yarılamışlardı. Şimdi, devam etmeden önce dosyanın geldiğinden emin olmak için Harry ve Karl'ın beklemeleri gerekiyordu. Beklerken, odanın diğer tarafında duran, hocanın masasına gittiler ve atılması gereken iki önemli adımla ilgilendiler. İlk adım bu makinada da bir herkese açık FTP sunucusu oluşturmaktı, böylece oyunlarının son ayağında dosyanın gelebileceği bir yer olacaktı.

İkinci adım zorlu olabiliecek bir soruna çözüm bulmaya yönelikti. Ar-Ge Merkezi'ndeki adamdan dosyayı warren@rms.ca.edu gibi bir adrese göndermelerini açıkçası isteyemezlerdi. Alan adının ".edu" olması büyük bir açık vermek demekti. Yarı uyanık bir bilgisayarcı bile bunun bir okulun adresini olduğunu anlar, anında tüm harekâtı sona erdirirdi. Bundan kaçınmak için hocanın bilgisayarındaki Windows'a girdiler ve dosyanın gönderileceği adres olarak verecekleri makinanın IP numarasına baktılar.

O sırada Ar-Ge Merkezi'ndeki bilgisayar uzmanını arama zamanı gelmişti. Harry telefonla ona ulaştı ve, "Söz ettiğim dosyayı az önce gönderdim. Gelip gelmediğine bir bakabilir misin?" diye sordu. Evet, gelmişti. Harry dosyayı başka bir yere iletmesini rica etti ve ona IP adresini verdi. Genç adam bağlantıyı kurup dosyayı göndermeye başlayana kadar telefonda bekledi ve hocanın bilgisayarındaki -dosyayı almakla meşgul- sabit sürücünün ışığı yanıp sönmeye başlayınca ikisinin de suratında kocaman birer gülümseme belirdi.

Harry ve adam, bir gün bilgisayarların ve ara birimlerinin nasıl daha güvenilir olacağıyla ilgili biraz sohbet ettiler ve sonra Harry teşekkür ederek veda etti.

İkisi, dosyayı hocanın bilgisayarından bir çift diskete kopyaladılar. Daha sonra bakmak için her biri birer kopya almıştı, doya doya bakabileceğin bir tabloyu müzeden çalıp kimseye birşey söyleyememek gibi bir şeydi bu. Ancak bu durumda daha çok onlar gerçek tablonun birer kopyasını almış gibiydiler ve gerçek olan hâlâ müzede duruyordu.

Sonra Karl, Harry'e hocanın makinasından FTP sunucusunu kaldırmanın adımlarını ve yaptıklarından geriye birşey kalmaması için denetleme izlerini nasıl sileceğini anlattı. Geriye bir tek, kolayca bulunabilecek bir yerde duran çalıntı bir dosya kalmıştı.

Son bir adım olarak kaynak kodunun bir parçasını doğrudan hocanın bilgisayarından Usenet'e koydular. Yalnızca küçük bir parçaydı, böylece şirkete büyük bir zarar vermemiş olacaklar ama hocaya kadar takip edilebilecek açık izler bırakmış olacaklardı. Adam bazı şeyleri açıklamakta çok zorlanacaktı.

Aldatmacanın İncelenmesi

Bu dalaverenin yürümesi için birkaç unsur bir araya getirilmiş olsa da kendini acındırıp yardım isteyen -patronumdan fırça yedim, yöneticiler veryansın ettiler, gibi- iyi bir rol yapma olmadan bu iş başarılamazdı. Bu ve telefonun diğer ucundaki adama sorunu nasıl çözeceğini anlatan ayrıntılı bir açıklama oldukça inandırıcı bir dalavere olarak kendini gösterdi. Bu noktada ve pek çok başka zamanda da işe yaramıştı.

İkinci önemli nokta, dosyanın değerini anlayacak adamdan dosyayı şirket içi bir adrese göndermesini istemişlerdi.

Bulmacanın üçüncü parçası ise bilgisayar işletmeninin dosyanın şirket içinden gönderildiğini görmesiydi. Bu da yalnızca, dosyayı ona gönderen adamın eğer dış ağ bağlantısı çalışıyor olsaydı bunu kendisinin de gönderebileceği anlamına gelebilirdi ya da en azından öyle gibi görünürdü. Dosyayı onun adına göndermekte ne gibi bir sakınca olabilirdi ki?

Sıkıştırılmış dosyaya farklı bir ad verilmesine ne dersiniz? Küçük gibi görünse de önemli bir ayrıntı. Saldırgan, dosyanın içinde bir kaynak kod olduğunu gösteren ya da ürünle ilgili bir adla görülmesi riskini göze alamazdı. Böyle bir ada sahip bir dosyayı şirket dışına gönderme ta-

Mitnick Mesajı:

Her çalışanın beynine kazınmış temel bir kural olmalıdır: Yönetimin onayı olmadığı sürece, göndereceğiniz yer şirketinizin dahili ağındaymış gibi gözükse de, şahsen tanımadığınız kişilere dosya göndermeyin.

lebi alarm zillerini çaldırabilirdi. Dosyanın zararsız görünümlü bir adla yeniden adlandırılması önemliydi. Saldırganların da öngördüğü üzere ikinci genç adamın dosyayı şirket dışına göndermekle ilgili hiçbir çekincesi olmadı. Bilginin gerçekte ne olduğuyla ilgili hiçbir ipucu vermeyen "yeniveri" gibi bir adı olan bir dosya zaten onu pek kuşkulandırmazdı.

Sonuç olarak bu öykünün sanayi casusluğuyla ilgili bir bölümde ne aradığını çözebildiniz mi? Çözemediyseniz, işte yanıtı: Bu iki öğrencinin haince bir şaka olarak yaptıkları şey, rakip bir firmanın ya da yabancı bir ülkenin tuttuğu profesyonel bir sanayi casusu tarafından kolaylıkla yapılabilirdi. Her koşulda da şirketin zararı korkunç olur, rakip firmanın ürünü piyasaya çıktığı zaman yeni ürünlerinin satışlarına ciddi bir darbe vurulmuş olurdu.

Benzer bir saldırı sizin şirketinize karşı kolayca gerçekleştirilebilir mi?

Aldatmacanın Engellenmesi

Uzun süredir şirketlere sorun oluşturan sanayi casusluğu, Soğuk Savaş'ın da sona ermesiyle ücret karşılığı şirket sırlarını ele geçirmeye odaklanmış geleneksel casusların ekmek kapısı oldu. Yabancı hükümetler ve şirketler serbest çalışan sanayi casuslarını bilgi çalmaları için tutuyorlar. Yerel şirketler de, rekabetçi bilgiler elde etme çabalarında çizgiyi aşan bilgi simsarlarına başvuruyorlar. Çoğu zaman eski askerî casuslar, kuruluşları kolaylıkla sömürmek için gerekli ön bilgiye ve deneyime sahip endüstriyel bilgi simsarlarına dönüşüyorlardı. Özellikle bilgilerini korumak ve çalışanlarını eğitmek konusunda gerekli önlemleri almayı başaramamış kuruluşlar başlıca hedeflerdi.

Güvenli Saklama Şirketi

Bilgilerini farklı bir yerde tutan bir şirketin yaşadığı sorunlara ne çözüm getirebilirdi? Şirket, verilerini şifrelemiş olsaydı buradaki tehlike önlenebilirdi. Evet, şifreleme daha fazla zaman ve harcama gerektirir ama harcanan çabalara değer. Şifreli dosyaların şifreleme/deşifreleme sistemlerinin düzgün çalışıp çalışmadığı düzenli olarak kontrol edilmelidir.

Her zaman şifre anahtarının kaybolması ya da anahtarı bilen tek kişiye otobüs çarpması gibi tehlikeler vardır. Ama yaşanabilecek can sıkıntısı, bu şekilde asgarî düzeye indirilir ve hassas bilgilerini kendi bünyesi dışında ticarî bir firmada tutan ve şifreleme kullanmayan herhangi biri, açık sözlülüğümü bağışlayın ama, salaktır. Kötü bir mahallede cebinizden yirmi dolarlık banknotları sarkıtarak yürümek, esasen soyulmaya davetiye çıkarmak gibi bir şeydir.

Yedekleme ortamlarını birilerinin alıp götürebileceği bir yerde bırakmak sık görülen bir güvenlik açığıdır. Yıllar önce müşteri bilgilerini koru-

mak için daha iyi önlemler alabilecek bir şirkette çalışıyordum. Yedekleme sorumluları şirketin yedekleme bantlarını her gün bir kuryenin gelip alması için kilitli bilgisayar odasının dışına bırakıyorlardı. Herhangi biri, şirketin şifrelenmemiş metinler içeren tüm belgelerinin bulunduğu bu bantları alıp gidebilirdi. Eğer yedekleme verileri şifrelenmiş olsalardı, malzeme kaybı sadece biraz baş ağrıtırdı. Eğer şifrelenmemiş olsalardı; şirket üstündeki böyle bir etkiyi benden daha iyi gözünüzde canlandırabilirsiniz.

Büyük şirketler için, verileri bünyeleri dışında saklama gereksinimi kaçınılmazdır. Ancak şirketinizin güvenlik süreçlerinin arasında, saklama şirketinin kendi güvenlik kuralları ve uygulamaları konusunda ne kadar sağduyulu davrandığını kontrol etme zorunluluğu da olmalıdır. Eğer sizin şirketiniz kadar kararlı değillerse, tüm güvenlik çabalarınız boşa gidebilir.

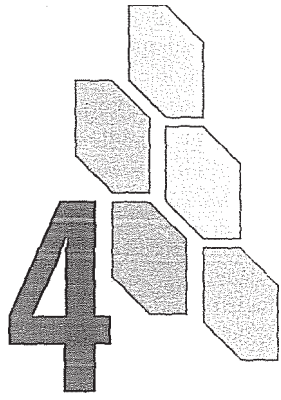
Küçük şirketlerin yedekleme için iyi bir seçenekleri daha vardır. Yeni ve değiştirilmiş dosyalarını her gece çevrimiçi saklama ortamı sunan şirketlerden birine gönderebilirler. Yine verilerin şifrelenmesi önemlidir. Aksi durumda bilgiler, yoldan çıkmış bir saklama şirketi çalışanının yanısıra çevrimiçi saklama şirketinin bilgisayar sistemlerine ya da ağına girebilecek her bilgisayar korsanına da açık olur.

Tabii ki, yedekleme dosyalarınızın güvenliğini korumak için bir şifreleme sistemi kurduğunuz gibi, şifre anahtarlarını ya da parolaları saklamak için de üstün bir güvenlik süreci oluşturmanız gerekmektedir. Verileri şifrelemek için kullanılan anahtarlar bir kasada ya da kilit altında tutulmalıdır. Sıradan şirket uygulamaları bu verilerle ilgilenen çalışanın aniden ayrılabileceği, ölebileceği ya da başka bir işe geçebileceği olasılıklarına karşı alınacak önlemleri de kapsamalıdır. Saklama yerini ve şifreleme/deşifreleme adımlarının yanısıra anahtarların nasıl değiştirildiğiyle ilgili kuralları da bilen her zaman en az iki kişi olmalıdır. Kurallar ayrıca şifreleme anahtarlarına erişimi olan çalışanın ayrılması durumunda şifrelerin hemen değiştirilmesini de zorunlu kılmalıdır.

O Da Kim?

Bu bölümde anlatılan, bilgi paylaşmaları için çalışanları kandırmak amacıyla etkileyiciliğini kullanan kurnaz dolandırıcı örneği, kimlik tespitinin önemini bir kez daha vurgular. Kaynak kodunun bir FTP sitesine yönlendirilmesi talebi de talep sahibini tanımanın önemine işaret eder.

On altıncı bölümde, bilgi ya da bir işlemin yapılması talebiyle gelen herhangi bir yabancının kimlik tespitini yapmak için belirli kurallar bulacaksınız. Kimlik tespitinin öneminden kitabın her yerinde söz ettik; 16. bölümde bunun nasıl yapılması gerektiğinin ayrıntılarını göreceksiniz.



Çıtayı Yükseltmek

BİLGİ GÜVENLİĞİNİN ÖNEMİNİ BİLMEK VE EĞİTİM

Bir toplum mühendisine, iki ay içinde piyasaya çıkaracağınız çok sıkı yeni ürününüzün planlarını ele geçirme görevi verilmiş. Onu ne durduracak?

Güvenlik duvarınız mı? Hayır.

Güçlü kimlik tespit cihazları mı? Hayır.

Hırsız uyarı sistemleri mi? Hayır.

Şifreleme mi? Hayır.

Telefon hattı kullanan aramalı modemler için sınırlı numara kullanımı mı? Hayır.

Dışarıdan birinin hangi sunucunun ürün planlarını içerdiğini bulmasını zorlaştırmak için sunuculara şifreli adlar vermek mi? Hayır.

Gerçek şu ki, dünyada bir toplum mühendisliği saldırısını engelleyebilecek bir teknoloji yok.

Teknoloji, Eğitim ve Süreçler Üzerine Güvenlik

Güvenlik delme testleri yapan şirketlerin raporlarına göre toplum mühendisliği yöntemleri kullanılarak müşteri şirketin bilgisayar sistemlerine girme denemeleri neredeyse yüzde 100 başarılı oluyor. Güvenlik teknolojileri insanları karar verme sürecinin dışında tutarak bu tarz saldırıları daha güçleştiriyor. Ancak toplum mühendisliği tehdidini azaltmanın aslında en etkili yolu, güvenlik teknolojileriyle birlikte, çalışan davranışlarına ve alınacak eğitimlere bazı temel şartlar getiren güvenlik süreçlerinin ortak kullanımından geçmektedir.

Ürün planlarını korumanın yalnızca tek bir yolu vardır ve bu da eğitimli, bilinçli ve sağduyulu bir iş gücüdür. Bunlar, süreçler ve kurallar konusundaki eğitimlerin yanı sıra -belki de daha önemli olan- sürekli bir bilinçlilik programı da içerir. Bazı yetkililer bir şirketin toplam güvenlik bütçesinin yüzde 40'ının bilinçlilik eğitimlerine ayırılmasını önermektedirler.

İlk adım, psikolojik olarak onları etkilemek isteyecek tekinsiz insanların bulunduğuna dair, kuruluştaki herkesi bilinçlendirmektir. Çalışanlar

hangi bilgilerin korunması gerektiği ve bunların nasıl korunacağı konusunda eğitilmelidirler. İnsanların nasıl etki altında kalabilecekleriyle ilgili bilgileri olursa, gelişmekte olan bir saldırıyı görebilmek için çok daha iyi bir konumda olacaklardır.

Güvenlik bilinci, aynı zamanda şirketteki herkesi şirket güvenlik kuralları ve süreçleriyle ilgili olarak eğitmek anlamına da gelir. 17. bölümde de anlatıldığı gibi, politikalar, şirket bilgi sistemlerini ve hassas bilgileri koruma doğrultusunda, çalışan davranışlarını yönlendirmesi için hazırlanmış önemli kurallardır.

Bu bölüm ve bir sonraki, sizi maliyetli olabilecek saldırılardan koruyabilecek bir güvenlik tasarımı ortaya koymaktadır. Eğer iyi düşünülmüş süreçleri takip eden, eğitimli ve dikkatli çalışanlarınız yoksa bu iş olasılık olmaktan çıkıp değerli bilgilerinizi ne zaman bir toplum mühendisine kaptıracağınız şekline bürünerek kesinlik kazanır. Bu kuralları yerleştirmeden önce bir saldırının gerçekleşmesini beklemeyin. İşinizin ve çalışanlarınızın rahatlığı açısından bu çok yıkıcı olabilir.

Saldırganların İnsan Yaradılışından Nasıl Faydalandıklarının Anlaşılması

Başarılı bir eğitim programı geliştirmek için, öncelikle insanların neden saldırılara karşı açık olduğunu anlamanız gerekir. Eğitimlerinizde bu eğilimleri tanımlayarak -örneğin rol yapma görüşmelerinde dikkati buna çekebilirsiniz- neden hepimizin toplum mühendislerinin etkisi altında kalabileceğimizi anlamaları için çalışanlarınıza yardımcı olabilirsiniz.

Etkileme, toplum bilimcilerin en azından elli yıldır üzerinde çalıştıkları bir konudur. Robert B. Cialdini, Scientific American'da (Şubat 2001) araştırmasını özetleyerek, bir isteğe olumlu yanıt alma girişiminde kullanılan "insan yaradılışının altı eğilimi"ni sundu.

Bu altı eğilim, toplum mühendislerinin (bazen bilinçli, çoğu zaman da bilinçsiz olarak) etkileme denemelerini dayandırdıkları eğilimlerle aynıdır.

Yetki

Yetkili biri bir talepte bulunduğu zaman insanların bu talebi yerine getirme eğilimi vardır. Bu sayfalarda daha önce de söz edildiği üzere, bir kişi, talepte bulunan kişinin yetkili olduğuna ya da böyle bir talepte bulunabilmek için yetkilendirilmiş olduğuna inanırsa isteği yerine getirmeye ikna edilebilir.

Dr. Cialdini "Etki" adlı kitabında ABD'nin orta batı kesimindeki üç hastanede yapılan bir araştırmayı yazmaktadır. Yirmi iki ayrı hemşire kendi-

ni hastane doktorlarından biri olarak tanıtan biri tarafından aranır ve kendilerine koğuştaki bir hastaya bir ilaç vermeleri konusunda talimatlar verilir. Bu talimatları alan hemşireler arayanı tanımıyorlardır ve gerçek bir doktor olup olmadığını (ki değildir) bilmiyorlardır. İlaçla ilgili talimat telefonla verilmektedir ve bu da hastane kurallarına aykırıdır. Ayrıca verilmesi istenen ilacın koğuşlarda kullanılmasına izin verilmemektedir ve uygulanması istenen doz günlük dozun iki katıdır. Bu yüzden hastanın yaşamını tehlikeye atma olasılığı vardır. Ancak olayların yüzde 95'inde Cialdini'nin anlattığına göre "hemşire, koğuş ilaç dolabından istenen dozu alır ve ilacı vermek üzere hastanın odasına doğru giderken", bir gözlemci tarafından durdurulur ve kendisine deneyden bahsedilir.

> **Saldırı örnekleri:** Bir toplum mühendisi, bilgi-işlem biriminden aradığını ya da yönetici olduğunu veya bir şirket yöneticisinin yanından aradığını söyleyerek kendini yetkili biriymiş gibi göstermeye çalışır.

Sevme

İstekte bulunan kişi kendini sevimli ya da kurbanla ortak ilgi alanları, inançları ve tavırları olan biri olarak gösterebilirse, insanlarda isteği yerine getirme eğilimi ortaya çıkar.

> **Saldırı örnekleri:** Sohbet aracılığıyla saldırgan, kurbanın bir hobisini ya da ilgi alanını öğrenmeyi başarır ve aynı hobi ya da ilgi alanına benzer bir ilgi ve hayranlık duyduğunu söyler. Aynı eyaletten ya da aynı okuldan olduklarını veya benzer hedefleri paylaştıklarını iddia edebilir. Toplum mühendisi, benzerlik görüntüsünü yaratabilmek için hedefinin davranışlarını taklit etme yoluna da gidecektir.

Karşılık Bekleme

Bize değerli bir şey verilir ya da verileceği taahüdünde bulunulursa hiç düşünmeden isteği yerine getiririz. Armağan, bir maddi cisim, tavsiye ya da yardım olabilir. Biri sizin için bir şey yaptığı zaman, karşılık verme eğilimi hissedersiniz. Bu karşılık vermeye yönelik güçlü eğilim armağanı alacak olan kişinin onu talep etmediği durumlarda bile kendini gösterir. İnsanları bize bir "iyilik" yapmaları (isteğimizi yerine getirmeleri) konusunda etkilemenin en etkili yollarından biri ona bir hediye vererek ya da yardım ederek bir zorunluluk duymalarını sağlamaktır.

Hare Krişna dini tarikatının üyeleri, önce insanlara hediye olarak bir kitap ya da çiçek vererek insanları amaçları için bağışta bulunmaları konusunda etkilemekte çok başarılıdırlar. Eğer kişi, hediyeyi geri vermeyi denerse, veren kişi, "O bizim size armağanımız", diyerek geri çevirir. Karşılık vermeye yönelik davranışsal kural Krişnalar tarafından bağışları büyük ölçüde artırmak için kullanılmıştır.

Saldırı örnekleri: Bir çalışan, Bilgi İşlem biriminden aradığını söyleyen birinden bir telefon alır. Arayan, bazı şirket bilgisayarlarına virüs koruma yazılımının tanımadığı, bilgisayardaki tüm dosyaları yok edebilecek bir virüs bulaştığını ve oluşabilecek sorunları engellemek için bazı yöntemleri anlatmak istediğini söyler. Bunun ardından arayan kişinin yeni güncellenmiş ve kullanıcıların parolalarını değiştirebilmelerini sağlayan bir yazılımı denemesini rica eder. Çalışan bu ricayı geri çeviremez çünkü arayan az önce onu güya bir virüsten koruyarak yardım etmiştir. Arayanın isteğini yerine getirerek karşılık verir.

Tutarlılık

Herkesin içinde bir amaca destek ya da bir söz verdikten sonra insanların isteklerini yerine getirme eğilimleri depreşir. Bir kez birşeyi yapacağımıza dair bir söz verdik mi, güvenilmeyen ya da istenmeyen biri olarak görünmek istemeyiz ve verdiğimiz sözle ya da yaptığımız açıklamayla ters düşmemek için işi tamamlama eğilimine gireriz.

Saldırı örneği: Saldırgan, işinde yeni sayılabilecek bir çalışanla bağlantı kurar ve şirketin bilgi sistemlerini kullanmasına izin verilebilmesinin bir şartı olarak belirli güvenlik kurallarına ve süreçlerine uyması gerektiğini hatırlatır. Birkaç güvenlik uygulamasından söz ettikten sonra arayan, kullanıcıdan, tahmin etmesi güç bir parola seçilmesi kuralı uyarınca "uyumluluk kontrolü" için parolasını söylemesini ister. Kullanıcı parolasını açıkladıktan sonra arayan gelecekte parolaları öyle bir yöntemle oluşturmasını önerir ki böylece saldırgan parolayı tahmin edebilecektir. Kurban, şirket kurallarına uymak üzere daha önce verdiği taahhüt doğrultusunda ve arayanın yalnızca kurallara uyulup uyulmadığını kontrol ettiği varsayımıyla isteği yerine getirir.

Toplum İçinde Kabul Görme

İnsanlar, davranışlarının başkalarının davranışlarıyla aynı olduğunu bilirlerse istekleri yerine getirme eğilimleri daha da artar. Başkalarının hareketleri, söz konusu davranışın doğru ve yerinde bir hareket olduğunun onayı olarak görülür.

Saldırı örneği: Arayan, bir araştırma yaptığını anlatır ve birimde kendisine yardımcı olduğunu iddia ettiği diğer insanların adlarını verir. Kurban diğerlerinin katılımının, isteğin geçerliliğini gösterdiğini düşünerek yardımcı olmayı kabul eder. Arayan, aralarında kurbanın bilgisayar kullanıcı adını ve parolasını açıklamaya yönelten soruların da bulunduğu bir dizi soru sorar.

Kıtlık

Aranan nesnenin miktarı azsa ve onu elde etmek için bir rekabet varsa ya da yalnızca kısa bir süre için orada olacaksa insanlar istekleri yerine getirme eğilimine girerler.

> **Saldırı örneği:** Saldırgan, şirketin yeni internet sitesine kayıt olan ilk 500 kişinin en yeni filmlere bedava bilet kazanacağını söyleyen e-postalar yollar. Hiçbir şeyin farkında olmayan bir çalışan, siteye kaydolurken ondan şirket e-posta adresi ve bir parola seçmesi istenir. Pek çok insanın, kolaylık olsun diye, kullandıkları her bilgisayar sisteminde aynı ya da benzer parolaları kullanma eğilimi vardır. Saldırgan bundan yararlanarak internet sitesi kayıt işlemlerinde girilen kullanıcı adı ve parolayı kullanıp hedefin ev ya da iş bilgisayar sistemlerine girmeye çalışır.

Eğitim ve Bilinçlendirme Programları Hazırlamak

Bir güvenlik kuralları kitapçığı çıkarmak ya da çalışanları güvenlik kurallarını ayrıntılı olarak anlatan bir intranet sayfasına yönlendirmek riski tek başına azaltmaz. Her işletme yalnızca kuralları yazılı olarak belirlemekle kalmamalı, aynı zamanda şirket bilgi ya da bilgisayar sistemleriyle çalışan herkesi kuralları öğrenmeye ve uygulamaya yönlendirmek için gerekli çabayı da göstermelidir. Ayrıca, insanların kolaylık olsun diye kuralın etrafından dolaşmamaları için, her kuralın altında yatan nedenlerin herkes tarafından anlaşıldığından emin olmalısınız. Aksi halde bilgisizlik her zaman çalışanın bahanesi olur ve toplum mühendisleri bu açığı hep sömürürler.

Herhangi bir güvenlik bilinçlendirme programının temel amacı, kuruluşun bilgi varlıklarını korumak için her çalışanın katkıda bulunmasını teşvik edip, insanların davranış ve tavırlarını değiştirmek amacıyla onları etkilemektir. Bu noktada en büyük teşvik edici unsur, katkılarının yalnızca şirkete değil aynı zamanda tek tek her çalışana getireceği kazançtan söz etmek olacaktır. Şirket her çalışanla ilgili belli özel bilgilere sahip olduğuna göre, çalışanlar bilgi ve bilgi sistemlerini korumak için paylarına düşeni yaptıklarında, aslında kendi bilgilerini de koruyor olacaklardır.

Bir güvenlik eğitim programı büyük bir desteğe ihtiyaç duyar. Eğitim girişiminin hassas bilgilere ya da şirket bilgisayar sistemlerine erişimi olan herkese ulaşması, sürekli olması ve çalışanları yeni tehditlere ve açıklara karşı uyarabilmek için düzenli olarak güncellenmesi gerekir. Çalışanlar, üst yönetimin programa tamamen bağlı olduğunu görmelidirler. Bu bağlılık gerçek bir bağlılık olmalıdır ve sadece mühürlü bir "Tam destek veriyoruz", notundan ibaret olmamalıdır. Program, onu ge-

liştirmeye, duyurmaya, denemeye ve başarısını ölçmeye yetecek kadar da kaynağa sahip olmalıdır.

Hedefler

Bir bilgi güvenliği eğitimi ve bilinçlendirme programının geliştirilmesinde akılda tutulması gereken en önemli yol gösterici, programın şirketlerinin her an bir saldırıya uğrayabileceği bilincini tüm çalışanlarda uyandırmaya odaklanması olmalıdır. Bilgisayar sistemlerine girmeye ya da hassas bilgileri çalmaya yönelik girişimlere karşı yapılan her savunmada çalışanların tümünün birer rolü olduğunu öğrenmeleri şarttır.

Bilgi güvenliğinin pek çok şekli teknoloji içerdiği için, çalışanların, sorunun güvenlik duvarları ve diğer güvenlik teknolojileriyle çözüldüğünü düşünmeleri çok kolaydır. Eğitimin başlıca hedeflerinden biri, her çalışanın, kuruluşun genel güvenliğinin en ön saflarında durduğunun farkına varmasını sağlamak olmalıdır.

Güvenlik eğitimlerinin kuralları aktarmaktan öte daha önemli bir amacı olmalıdır. Eğitim programı tasarımcısı, işlerini bitirme baskısıyla güvenlik yükümlülüklerini uygulamama ya da göz ardı etme şeklinde görülen, çalışan tarafındaki güçlü tahrikleri görebilmelidir. Toplum mühendisliği taktikleriyle ilgili bilgi ve saldırılara karşı nasıl savunma yapılacağı önemlidir ama bu sadece eğitim ağırlıklı olarak çalışanları bilgiyi kullanmaya teşvik etmek üzere tasarlanmışsa işe yarar.

Eğer eğitimi tamamlayan herkes, bilgi güvenliğinin işinin bir parçası olduğu gerçeğine inanmış ve harekete geçmişse şirket o zaman programının ana hedefine ulaştığını varsayabilir.

Çalışanlar, toplum mühendisliği saldırıları tehdidinin gerçek olduğunu ve ciddi bir hassas bilgi kaybının şirketi olduğu kadar kendi kişisel bilgilerini ve işlerini de tehlikeye sokabileceğini kabul edip anlamalıdırlar. İşteki bilgi güvenliği konusunda dikkatsiz davranmakla, ATM ya da kredi kartı numarası konusunda dikkatsiz davranmak bir bakıma aynıdır. Güvenlik uygulamaları konusunda istek uyandırmak için bu çok yerinde bir benzetme olabilir.

Eğitim ve Bilinçlendirme Programını Oluşturmak

Bilgi güvenliği programını tasarlamakla yükümlü kişi bunun tek beden bir proje olmadığını bilmelidir. Eğitim daha çok şirket içindeki farklı grupların belirli gereksinimlerini karşılayacak şekilde tasarlanmalıdır. 16. bölümde dış çerçevesi verilen güvenlik kurallarının çoğu tüm çalışanlar için uygun olsa da, diğer pek çokları da özgündür. En azından çoğu şirket şu belirgin gruplar için eğitim programlarına ihtiyaç duya-

NOT: *Özgün bir program geliştirmek için yeterli kaynağı olmayan işletmeler için güvenlik bilinçlendirme eğitimi hizmeti veren pek çok eğitim şirketi bulunmaktadır. Güvenli Dünya Fuarı (www.secureworldexpo.com) gibi fuarlar bu şirketlerin bir araya gelme yerleridir.*

caktır: Yöneticiler, bilgi-işlem personeli, bilgisayar kullanıcıları, teknik olmayan personel, idarî yardımcılar, danışma görevlileri ve güvenlik görevlileri (16. bölümde görevlere göre kural dağılımına bakınız.).

Bir şirketin güvenlik görevlileri, bilgisayar konusunda bilgilerinin olması beklenmediği için ve belki çok sınırlı kullanımlar dışında, şirket bilgisayarlarıyla haşır neşir olmadıklarından, bu tarz eğitimler geliştirilirken göz önüne alınmazlar. Ancak toplum mühendisleri güvenlik görevlilerini ya da başka insanları binaya ya da ofise girmelerine izin vermeleri için ya da bilgisayar güvenlik ihlallerine neden olacak bir davranışta bulunmaları doğrultusunda kandırabilirler. Her ne kadar güvenlik güçleri bilgisayarla çalışan personele verilen eğitimin tümünü almak zorunda değilse de güvenlik bilinçlendirme programlarında da göz ardı edilmemelidir.

İş dünyasında, tüm çalışanların eğitilmesinin gerektiği ve güvenlik kadar herhalde aynı anda hem önemli hem de sıkıcı çok az konu vardır. İyi tasarlanmış güvenlik eğitimi programları, öğrenenlerin hem ilgisini çekmeli hem de onları heveslendirmelidir.

Amaç, bilgi güvenliği bilinçlendirme eğitimlerini çekici ve karşılıklı etkileşimli yapmak olmalıdır. Kullanılabilecek yöntemler arasında, toplum mühendisliği tekniklerini rol yapma oyunlarıyla göstermek; daha az şanslı olan diğer işletmelere yakın zamanda yapılan saldırılarla ilgili basın haberlerini incelemek ve şirketlerin kayıpları önleme yollarını tartışmak ya da aynı anda hem eğlenceli hem de eğitici olması açısından güvenlik videolarını göstermek olabilir. Videolar ve ilgili malzemeleri pazarlayan pek çok güvenlik bilinçlendirme şirketi bulunmaktadır.

Bu kitaptaki öyküler, tehlikeye karşı uyarmak ve insan davranışlarının açıklarını göstermek amacıyla toplum mühendisliği teknik ve yöntemleriyle ilgili pek çok bilgi sunmaktadır. Oradaki senaryoları, rol yapma faaliyetlerine temel olacak şekilde kullanabilirsiniz. Öyküler aynı zamanda, saldırının başarılı olmasını engellemek için kurbanların nasıl davranması gerektiğiyle ilgili renkli tartışmalar yapabilme fırsatı da sunmaktadır.

Becerikli bir program geliştiricisi ve becerikli eğiticiler, sınıfın havasını canlı tutmak ve bu sırada insanları çözümün parçası olmaya teşvik etmek içiri çözülecek bir sürü sorunun yanı sıra pek çok başka fırsat da bulacaklardır.

Eğitimin Yapısı

Temel bir güvenlik bilinçlendirme eğitim programı tüm çalışanların katılacağı şekilde geliştirilmelidir. Yeni işe girenlerin intibak eğitimlerinin bir parçası olarak bu eğitimi alma zorunlulukları olmalıdır. Hiçbir çalışana temel bir güvenlik bilinçlendirme oturumuna katılmadan bilgisayar erişimi verilmemesini öneririm.

İlk bilinçlendirme eğitimi için dikkatleri çekmeye odaklanmış ve önemli mesajların hatırlanacağı kadar kısa bir oturum uygun olabilir. Üzerinde durduğumuz konuların miktarı kesinlikle daha uzun bir eğitim gerektirse de, makul sayıda, önemli mesajlarla birlikte verilmiş bir bilinç ve istek oluşturmanın önemi, benim görüşüme göre, insanları çok fazla bilgiyle buluşturan yarım günlük ya da tam günlük eğitimlerden çok daha fazladır.

Bu oturumların üzerinde durulması, tüm çalışanların sıkı sıkıya uyduğu güvenlik alışkanlıkları olmadığı durumda şirkete ve bireysel olarak çalışanlara gelebilecek zararların değerlendirildiğini göstermektedir. Belirli güvenlik uygulamalarını öğrenmekten daha da önemlisi; çalışanların, güvenlik adına kişisel sorumluluk almaları konusunda teşvik edilmeleridir.

Çalışanların rahatlıkla sınıflarda toplanamadığı durumlarda şirket, videolar, bilgisayar tabanlı eğitimler, çevrimiçi dersler ya da basılı malzemeler gibi farklı bilgilendirme yöntemleri kullanarak bilinçlendirme eğitimleri geliştirmeyi de göz önünde tutmalıdır.

İlk kısa oturumdan sonra, belirli açıklar ve şirketteki konumlarına göre saldırı teknikleri konusunda çalışanları eğitecek daha uzun oturumlar geliştirilmelidir. Hatırlatma eğitimleri yılda en az bir kez zorunlu olmalıdır. Tehdidin boyutu ve insanları sömürmek için kullanılan yöntemler sürekli değişmektedir, bu yüzden programın içeriği de sürekli güncellenmelidir. Dahası, insanların bilinçliliği ve uyanıklığı zaman içinde azalır; bu nedenle güvenlik ilkelerini vurgulamak için eğitimin düzenli aralıklarla tekrarlanması gerekir. Bu noktada dikkatler yine, belirli tehditlerin ve toplum mühendisliği yöntemlerinin üzerinde olduğu kadar, çalışanları güvenlik kurallarının önemine inandırmak ve kurallara bağlı kalmaya teşvik etmek üzerinde de olmalıdır.

Yöneticiler altlarında çalışanlara güvenlik kuralları ve süreçlerine aşina olmaları ve güvenlik bilinçlendirme programına katılmaları için yeterince zaman tanımalıdırlar. Çalışanların kendi istedikleri zaman güvenlik kurallarını öğrenmeleri ya da eğitimlere katılmaları beklenemez. Yeni işe girenlere ise iş sorumluluklarını almadan önce güvenlik kurallarını ve basılı güvenlik uygulamalarını gözden geçirmek için yeterli zaman verilmelidir.

Kurum içinde konumları değişerek hassas bilgilere ya da bilgisayar

sistemlerine erişimi gerektiren bir işe geçen çalışanların, doğal olarak, yeni sorumluluklarına uygun olarak tasarlanmış güvenlik eğitimi programını tamamlamaları gerekir. Örneğin, bir bilgisayar işletmeni sistem yöneticisi olursa ya da bir danışma görevlisi, idarî yardımcı olursa ona yeniden eğitim verilmesi şarttır.

Eğitimin İçeriği

Temele indirgendiklerinde tüm toplum mühendisliği saldırıları aynı unsuru kullanırlar: Aldatma. Saldırganın bir çalışan ya da hassas bilgilere ulaşmaya veya bilgisayarlar ve bilgisayar donanımları kullanılarak yapılan işler konusunda kurbana talimat vermeye yetkili başka bir kişi olduğuna kurban inandırılır. Bu saldırıların hemen hepsi hedef olan çalışanın iki şey yapmasıyla boşa çıkarılabilir:

- İstekte bulunan kişinin kimliğini kontrol etmekle: Bu kişi gerçekten olduğunu söylediği kişi mi?
- Kişinin yetkili olup olmadığını kontrol etmekle: Kişinin bu bilgiyi öğrenmeye ihtiyacı var mı ya da böyle bir istekte bulunmak için yetkili mi?

Eğer bilinçlendirme eğitimi programları, her çalışanın davranışlarını bu kriterlere aykırı olan tüm istekleri sorgulamak konusunda tutarlı olacak şekilde değiştirebilirse, o zaman toplum mühendisliği saldırılarıyla ilişkilendirilebilecek risk büyük ölçüde azaltmış olur.

İnsan davranışlarına ve toplum mühendisliği tekniklerine odaklanan güvenlik bilinçlendirme ve eğitim programlarında bulunabilecek kullanışlı bilgiler arasında şunlar yer alabilir:

- Saldırganların insanları aldatmak için toplum mühendisliği becerilerini nasıl kullandıklarının bir açıklaması;
- Toplum mühendislerinin amaçlarına ulaşmak için kullandıkları yöntemler;
- Olası bir toplum mühendisliği saldırısının nasıl farkedileceği;
- Şüpheli bir isteği değerlendirme süreçleri;
- Toplum mühendisliği girişimlerinin ya da başarılı saldırıların nereye haber verileceği;

NOT: *Güvenlik bilinci ve eğitimi hiç bir zaman kusursuz olmayacağı için derinlemesine bir savunma oluşturabilmek için mümkün olduğu kadar güvenlik teknolojisi kullanmaya çalışın. Bu, güvenlik önlemlerinin çalışanlardan çok, teknoloji tarafından alınmasıdır. Örneğin, işletim sistemi, çalışanların internetten dosya indirmesini ya da kısa ve kolay parolalar seçmesini engelleyecek şekilde ayarlanabilir.*

- Kişinin sahip olduğunu iddia ettiği konumuna ve önemine bakmaksızın şüpheli bir istekte bulunan herkesi sorgulamanın önemi;
- İçlerindeki dürtü karşı tarafa yardımcı olmaları gerektiğini söylese de, düzgün bir kimlik tespiti olmadan gözü kapalı kimseye güvenmemeleri gerektiği gerçeği;
- Bir bilgi ya da işlem talebinde bulunan herhangi birinin kimliğini ve yetkisini kontrol etmenin önemi (Kimlik tespiti yöntemleri için bakınız "Onay ve Yetkilendirme Süreçleri", 16. Bölüm);
- Her türlü veri sınıflandırma sistemiyle ilgili bilginin yanısıra hassas bilgileri koruma süreçleri;
- Şirketin güvenlik kurallarının ve süreçlerinin yeri ile bilgi ve şirket bilgi sistemlerini korumadaki önemleri;
- Kilit güvenlik kuralları ve anlamlarına ilişkin bir özet. Örneğin, her çalışanın tahmini güç bir parolayı nasıl oluşturacağına ilişkin bilgilendirilmesi.

Tanım itibarıyla toplum mühendisliği, insanlar arası bir çeşit etkileşim yöntemidir. Bir saldırgan hedefine ulaşmak için çeşitli iletişim yöntemleri ve teknolojilerini sık sık kullanacaktır. Bu nedenle iyi tasarlanmış bir bilinçlendirme programının aşağıdakilerin tümünü ya da bir kısmını içermesi gerekmektedir:

- Bilgisayar ve sesli mesaj parolalarıyla ilgili güvenlik süreçleri;
- Hassas bilgilerin ya da malzemelerin verilmesine yönelik süreç;
- Aralarında virüslerin, solucanların ve Truva Atlarının da olduğu kötü huylu yazılımlara karşı alınacak önlemleri de içerecek şekilde e-posta kullanımı kuralları;
- Yaka kartı takmak gibi fiziksel güvenlik zorunlulukları;
- Binada kart takmayan kişileri sorgulama yükümlülüğü;
- Sesli mesaj kullanımı için en doğru güvenlik uygulamaları;
- Bilgilerin sınıflandırmasının nasıl yapılacağı ve hassas bilgileri korumak için alınacak önlemler;
- Hassas belgelerin ve gizli dosyalar içeren ya da bir zamanlar içermiş bilgisayar taşınabilir ortamlarınının doğru bir şekilde silinmesi.

Eğer şirket, toplum mühendisliği saldırılarına karşı savunmasının etkinliğini ölçmek için delme testi yapmayı planlıyorsa, çalışanları bu uygulamadan haberdar eden bir uyarı yapmalıdır. Böyle bir testin parçası olarak saldırganların yöntemlerini kullanan birinin telefon ya da başka

bir araç kullanarak iletişime geçebileceğini çalışanlarınızın bilmesini sağlayın. Bu testlerin sonuçlarını, çalışanları cezalandırmak için değil, bazı alanlardaki ek eğitim ihtiyacını belirlemek için kullanın.

Yukarıdaki tüm maddelerle ilgili ayrıntıları 16. bölümde bulabilirsiniz.

Ölçüm

Şirketiniz, bilgisayar sistemine erişim hakkı tanımadan önce çalışanların güvenlik bilinçlendirme eğitiminde sunulan bilgilere hakimiyetini ölçmek isteyebilir. Eğer çevrimiçi yapılacak testler tasarlarsanız, pek çok sınav değerlendirme yazılımı, güçlendirilmesi gereken eğitim alanlarını belirlemek için test sonuçlarını çabucak değerlendirebilir.

Şirketiniz bir ödül ve çalışanını teşvik amacıyla güvenlik eğitimini tamamladığını gösteren bir sertifika sunmayı da düşünebilir.

Programı tamamlamanın kalıplaşmış bir sonucu olarak, programda öğretilen güvenlik kurallarına ve ilkelerine uyacağına dair her çalışandan bir taahhüt belgesini imzalamasının istenmesini öneririm. Araştırmalara göre, böyle bir belge imzalayarak bağlılığını gösteren kişi, süreçlere uymak konusunda daha çok çaba gösterebiliyor.

Sürekli Bilinç

Pek çok insan bilir ki, önemli konularda bile, öğrenilenler, düzenli olarak tekrarlanmadıkları sürece yok olma eğilimindedirler. Çalışanların toplum mühendisliği saldırılarına karşı korunmak konusunda hızlarını kaybetmemeleri için bir sürekli bilinç programı önemlidir.

Güvenliği, çalışan düşünce zincirinin en önünde tutan yöntemlerden biri de bilgi güvenliğini her şirket çalışanı için bir iş sorumluluğu olarak tanımlamaktır. Bu, çalışanların şirketin genel güvenliğindeki can alıcı rollerini anlamalarına yardımcı olacaktır. Aksi takdirde "güvenlik benim işim değil" türünden güçlü bir eğilim oluşacaktır.

Bir bilgi güvenliği programının genel sorumluluğu çoğunlukla güvenlik birimindeki ya da bilgi işlem birimindeki birine verilse de, bir bilgi güvenliği bilinçlendirme programının geliştirilmesi işi, büyük olasılıkla eğitim biriminin ortak bir projesi olarak en iyi şekilde yapılandırılmış olacaktır.

Sürekli bilinç programının yaratıcı olması gerekir ve iyi güvenlik alışkanlıkları konusunda çalışanlara sürekli hatırlatıcı güvenlik mesajları iletmek için mümkün olan her kanalı kullanmalıdır. Yöntemler, programı geliştirip uygulamaya koyacak insanların hayal edebildiği ölçüde yeni kanalların yanı sıra her türlü geleneksel kanaldan da yararlanmalıdırlar. Geleneksel reklamcılıkta olduğu gibi eğlenceli ve akıllıca olmaları işe

yarar. Mesajlardaki söz sıralarının değiştirilmesi de aşinalık yaratıp göz ardı edilmelerini engeller.

Bir sürekli bilinç programının içeriğinde bulunabilecekler şunlar olabilir:

- Bu kitabın birer kopyasını tüm çalışanlara vermek.
- Şirket bültenine bilgi sağlayıcı unsurlar koymak: Makaleler, kutu içine yazılmış hatırlatmalar (tercihen kısa, dikkat çekici noktalar şeklinde) ya da karikatürler olabilir.
- Ayın Güvenlik Çalışanı'nın bir resmini koymak.
- Çalışanların gittikleri yerlere posterler asmak.
- Bülten panolarına duyurular asmak.
- Maaş bordro zarflarına broşürler koymak.
- Hatırlatma amaçlı e-postalar göndermek.
- Güvenlikle ilişkili ekran koruyucular kullanmak.
- Sesli mesaj sistemi aracılığıyla güvenliği hatırlatan duyurular yapmak.
- Üzerinde, "Sizi arayan gerçekten olduğunu iddia ettiği kişi mi?" gibi şeyler yazan yapışkanlı etiketler bastırmak.
- Bilgisayara bağlanırken, "Eğer e-postayla gizli bilgiler gönderiyorsanız, mutlaka şifre koyun", gibi hatırlatma mesajlarının çıkması için ayarlamalar yapmak.
- Güvenlik bilincini çalışan performans raporlarının ve yıllık değerlendirmelerin ayrılmaz bir parçası durumuna getirmek.
- İntranete, çalışanların ilgisini çekecek karikatürler, fıkralar ya da başka şeyler biçiminde güvenlik bilinci hatırlatıcıları koymak.
- Kafeteryada sık sık farklı bir güvenlik unsurunu hatırlatan bir elektronik mesaj tahtası kullanmak.
- Dosyalar ve broşürler dağıtmak.
- Dikkat çekici ayrıntılar düşünülebilir, örneğin kafeteryada ücretsiz fal kurabiyeleri dağıtılabilir ve her birinde fal yerine bir güvenlik hatırlatıcısı olabilir.

Tehlike her zaman var; hatırlatıcıların da her zaman var olması gerekir.

Benim Bundan Çıkarım Ne?

Güvenlik bilinçlendirme ve eğitim programlarına ek olarak, işleyen ve iyi tanıtılmış bir ödüllendirme sistemini de ciddi şekilde öneririm. Bir

toplum mühendisliği saldırısını tespit edip önlemiş ya da bilgi güvenliği programının başarısına büyük bir katkıda bulunmuş çalışanlarınıza teşekkür etmelisiniz. Ödül programının varlığı güvenlik bilinçlendirme oturumlarında tüm çalışanlara anlatılmalı ve güvenlik ihlalleri tüm kuruluşa geniş bir şekilde duyurulmalıdır.

İşin diğer yüzünde insanlar, ister dikkatsizlikten ister direnmekten olsun, bilgi güvenliği kurallarına uymamanın sonuçlarının da farkında olmalıdırlar. Her ne kadar hepimiz hata yapsak da güvenlik kurallarının sürekli ihlali de hoş karşılanmamalıdır.

ŞİRKET BİLGİ GÜVENLİĞİ KURALLARI ÖNERİLERİ

FBI'in yaptığı ve Associated Press'in Nisan 2002'de yayınladığı bir araştırmanın sonuçlarına bakılırsa, büyük şirketlerin ve devlet kurumlarının onda dokuzu bilgisayar kırıcılarının saldırısına uğramış. İlginç bir şekilde araştırma her üç şirketten yalnızca birinin saldırıları bildirdiğini ya da kamuoyuna açıkladığını ortaya çıkarmış. Bir saldırıya kurban gittikleri konusunda suskun kalmaları mantıklı olabilir. Müşterilerinin güvenini yitirmemek ve şirketin açıklarının olabileceğini öğrenen saldırganların yeni saldırılarını engellemek için çoğu işletme, bilgisayar güvenliğine yönelik saldırıları kamuoyuna açıklamazlar olaylarını açık bir şekilde rapor etmezler.

Görünüşe göre, toplum mühendisliği saldırılarıyla ilgili hiç istatistik yok; olsaydı da sayılar oldukça güvenilmez olurdu. Çoğu durumda, bir şirket, bir toplum mühendisinin bilgiyi ne zaman çaldığını hiçbir zaman bilemez ve bu yüzden pek çok saldırı fark edilmez ve rapor edilmeden kalır.

Toplum mühendisliği saldırılarının çoğuna karşı etkili önlemler alınabilir. Doğruyu söylemek gerekirse kuruluştaki herkes güvenliğin önemini anlamadığı ve şirket güvenlik kurallarına uyup bunu işinin bir parçası olarak kabul etmediği sürece, toplum mühendisliği saldırıları her zaman şirketler için büyük bir tehlike olmaya devam edeceklerdir.

Aslında, güvenlik açıklarını kapamak için teknolojik silahların gelişmesi, tescilli şirket bilgilerine ulaşmak ya da şirket ağına girmek için insanları kullanan toplum mühendisliği saldırılarını kesinlikle ciddi ölçüde sıklaştıracak ve ortam, bilgi hırsızları için daha çekici bir hal alacaktır. Bir sanayi casusu doğal olarak amacına ulaşma işini en kolay ve en düşük fark edilme tehlikesi olan yoldan yapacaktır. İşin doğrusu, bilgisayar sistemlerini ve ağını en son çıkan güvenlik teknolojilerini kullanarak koruyan bir şirket, hedeflerine ulaşmak için toplum mühendisliği stratejilerini, yöntemlerini ve taktiklerini kullanan saldırganlardan gelecek saldırılara daha çok maruz kalma tehlikesiyle karşı karşıya kalacaktır.

Bu bölüm, toplum mühendisliği saldırı riskini en aza indirgeyecek şekilde tasarlanmış belli kurallar sunmaktadır. Kurallar tam olarak sadece teknik açıkları sömürmeye yönelik saldırılara hitap etmemektedirler. Güvenilir bir çalışanı, saldırganın hassas şirket bilgilerine ya da bilgisayar sistem ve ağlarına erişebilmesini sağlayan bilgiler vermeye ya da bir iş yapmaya kandırabilmek için oynanan oyunları ya da öne sürülen bahaneleri de kapsamaktadırlar.

Güvenlik Kuralı Nedir?

Güvenlik kuralları, bilgiyi korumak amacıyla, çalışan davranışları için yön göstericidir ve olası güvenlik tehditlerini bertaraf etmek için etkili kontroller geliştirilmesinin temel taşıdır. Bu kurallar, iş toplum mühendisliği saldırılarını tespit etmeye ve önlemeye gelince daha da önemli olmaktadırlar.

Etkili güvenlik kontrolleri, iyi düzenlenmiş kurallar ve süreçlerle çalışanları eğiterek yerleştirilir. Ancak şunu da vurgulamak gerekir ki, tüm çalışanlar tarafından sadakatle uygulansa da güvenlik kuralları her toplum mühendisliği saldırısının engelleneceğini garanti etmezler. Amaç, daha çok, riski kabul edilebilir düzeye indirebilmektir.

Burada sunulan kurallar, tam anlamıyla toplum mühendisliği konularıyla ilgili olmasa da toplum mühendisliği saldırılarında çoğunlukla kullanılan teknikleri de içermektedirler. Örneğin e-postaları açmakla ilgili kurallar bilgisayar kırıcılarının sık sık kullandığı bir yöntemle ilgilidir. Saldırgan, kurbanın bilgisayarında kontrolü ele geçirmesini sağlayan kötü huylu Truva Atı yazılımlarını e-posta aracılığıyla yükleyebilir.

Bir Program Oluşturmanın Adımları

Kapsamlı bir bilgi güvenliği programı, işe genellikle üç şeyi belirleyip risk ölçümü yaparak başlar:

- Kurumun bilgi varlıklarından hangilerinin korunması gerekir?
- Bu varlıklara karşı ne gibi tehditler vardır?
- Bu olası tehditler gerçekleştiği durumda kuruma ne gibi zararlar gelebilir?

Risk değerlendirmenin öncelikli amacı hangi bilgi varlıklarının acilen korunmaları gerektiğini belirlemek ve maliyet-kâr analizi yaparak önlem almanın uygun maliyetli olup olmadığına bakmaktır. Daha açık ifade etmek gerekirse, hangi varlıklar en önce koruma altına alınacak ve bu varlıkları korumak için ne kadar zaman harcanacaktır?

Üst yönetimin güvenlik kuralları ve bilgi güvenliği programı geliştirmenin önemini güçlü bir şekilde desteklemesi ve bu görüşü paylaşması önemlidir. Diğer herhangi bir şirket programında olduğu gibi, eğer güvenlik programı başarılı olacaksa, yönetim yalnızca bir onay imzası atmakla kalmamalı, şahsen örnek olarak bağlılığını göstermelidir. Çalışanlar, bilgi güvenliğinin şirket faaliyetleri açısından can alıcı olduğu, şirket içi bilgilerin korunmasının şirket varlığının korunması için önemli olduğu ve çalışanların işlerinin programın başarısına bağlı olabileceği gerçeklerine yönetimin güçlü bir şekilde bağlı olduğunun bilincinde olmalıdırlar.

Bilgi güvenliği kurallarını temize çekmekle görevlendirilmiş personelin, kuralların teknik terimler kullanılmadan yazılması ve teknik olmayan çalışanlar tarafından rahatça anlaşılabilmesi gerektiğini anlamış olması şarttır. Belgenin, her kuralın neden önemli olduğunu da açıklaması gerekir; aksi halde, çalışanlar, kuralları zaman kaybı olarak görerek bir kenara itebilirler. Kurallar büyük olasılıkla onları yerleştirmeye yarayan süreçlerden daha az sıklıkta değişeceğinden kuralları kaleme alan kişi, kuralları tanıtan bir belge oluşturmalı ve süreçler için de ayrı bir belge açmalıdır.

Ek olarak, kuralları yazan kişi, güvenlik teknolojilerinin iyi bilgi güvenliği uygulamalarını oturtmakta kullanılabileceğini de bilmelidir. Örneğin, çoğu işletim sistemi, kullanıcı parolalarının uzunluk gibi bazı özelliklere uyup uymadıklarını kontrol edecek şekilde ayarlanabilmektedir. Bazı şirketlerde kullanıcıların program indirmesi işletim sistemindeki yerel ya da genel ayarlar aracılığıyla denetlenebilir. Kurallar, insan kaynaklı karar alma mekanizmalarını devre dışı bırakmaya kıyasla daha uygun maliyetli olduğu koşullarda, güvenlik teknolojileri kullanma zorunluluğunu da getirmelidir.

Çalışanlar, güvenlik kuralarına ve süreçlerine uymadıkları takdirde oluşabilecek sonuçlar hakkında da uyarılmalıdırlar. Kurallara uymamanın karşılığı olarak bir takım uygun cezalar yerleştirilmeli ve herkese duyurulmalıdır. Aynı zamanda, güvenlik uygulamaları konusunda başarılı ya da bir güvenlik olayını farkedip bildirmiş çalışanlar için de bir ödül sistemi oluşturulmalıdır. Ne zaman bir çalışan bir güvenlik ihlalini engellemekten ödül alırsa, bu, tüm şirket içinde -şirket bülteninde çıkan bir makale şeklinde bile olsa- duyurulmalıdır.

Güvenlik bilinçlendirme programının bir amacı, güvenlik kurallarının önemini ve bu kurallara uymamaktan doğabilecek zararı anlatmaktır. İnsan yaradılışı gereği, çalışanlar zaman zaman makul gözükmeyen ya da zaman alıcı gibi görünen kuralları göz ardı edecek ya da boşluklarından yararlanacaktır. Çalışanların, kuralları çevrelerinden dolaşılacak birer engel gibi görmek yerine, kuralların önemini anlamaları ve uymaya istekli olmalarını sağlamak yönetimin sorumlulukları arasındadır.

Bilgi güvenliği kurallarının değişmez kurallar olmadığını belirtmekte yarar vardır. İş ortamları değiştikçe, piyasaya yeni güvenlik teknolojileri çıktıkça ve güvenlik açıkları evrimleştikçe kuralların değiştirilmesi ya da desteklenmesi gerekebilir. Düzenli bir gözden geçirme ve güncelleme süreci devreye alınmalıdır. Şirket güvenlik kurallarını ve süreçlerini intranet üzerinden herkese açın ya da bu tarz kuralları herkesin ulaşabileceği bir klasöre koyun. Bu hareket, kuralların ve süreçlerin daha sık okunma olasılığını artırır ve çalışanların bilgi güvenliğiyle ilgili sorularına daha hızlı yanıt bulmaları açısından etkili bir yöntem olur.

Sonuç olarak, eğitimlerdeki açıkları ya da şirket kural ve süreçlerine

uyumdaki eksikliği ortaya çıkarmak amacıyla, toplum mühendisliği yöntem ve taktikleri kullanılarak düzenli delme testleri ve açık değerlendirmeleri yapılmalıdır. Aldatıcı delme testleri uygulanmadan önce bu tarz testlerin zaman zaman yapılacağı çalışanlara duyurulmalıdır.

Bu Kurallar Nasıl Kullanılır?

Bu bölümde aytıntılarıyla anlatılan kurallar, tüm güvenlik risklerini azaltması için önemli olduğuna inandığım bilgi güvenliği kurallarının yalnızca küçük bir parçasıdır. Buna göre, burada sözü geçen kuralların kapsamlı bir bilgi güvenliği kural listesi olduğu düşünülmemelidir. Bu kurallar, daha çok, şirketinizin belirli ihtiyaçlarına uygun olabilecek kapsamlı bir güvenlik kuralları bütünü oluşturabilmek için bir temeldir.

Kuralları hazırlayanlar, şirketlerine özgü, çevrelerine ve iş hedeflerine uygun kurallar seçmelidirler. Her kuruluş, iş gereksinimleri, yasal yükümlülükleri, kurum kültürü ve kullandığı bilgi sistemlerine göre aşağıda anlatılan kurallardan ihtiyacı olanı alabilir, diğerlerini bir kenara bırakabilir.

Her veri sınıfındaki kuralların ne kadar katı olacağıyla ilgili de verilecek kararlar vardır. Tek bir binaya sığan ve çalışanların çoğunun birbirini tanıdığı küçük bir şirketin, telefon edip o şirkette çalıştığını söyleyen bir saldırgandan korkmasına gerek yoktur (ancak saldırgan, bir satıcı firmadan aradığı ayağına da yatabilir). Ayrıca artan risklere karşın rahat bir kurum kültürüne sahip bir şirket, güvenlik hedeflerine ulaşmak için önerilen kuralların yalnızca küçük bir bölümünü kullanmak isteyebilir.

Veri Sınıflandırma

Bir veri sınıflandırma politikası kuruluşun bilgi varlıklarını korumak için önemlidir ve hassas bilgilerin yayılmasını denetleyen bir sınıflandırma sistemi getirir. Bu politika, tüm çalışanları her bilgi parçasının hassaslık derecesi konusunda bilinçlendirerek şirket bilgilerini korumak için bir çerçeve oluşturur.

Veri sınıflandırma politikası olmadan çalışmak -bu, artık günümüzde pek çok şirketin olmazsa olmazıdır- kararların çoğunu bireysel düzeyde çalışanlara bırakır. Doğal olarak çalışan kararları, bilginin hassaslığı, önemi ve değerinden çok büyük ölçüde öznel unsurlara dayanır. Çalışanlar bir bilgi talebine karşılık vererek, bilgiyi bir saldırganın ellerine teslim edebilecekleri olasılığından habersiz oldukları için de bilgi duyurulur.

Veri sınıflandırma politikası pek çok düzeyden birinde değerli bilgilerin sınıflandırılması için yol göstericidir. Her bilgi parçasının sınıflandırılmasıyla çalışanlar, hassas bilgilerin kasıtsız olarak şirketten dışarı çık-

masını önleyecek bir veri kullanım sürecine uyabileceklerdir. Bu süreçler çalışanların hassas bilgileri yetkisiz kişilere vermek için kandırılmaları olasılığını azaltacaktır.

Her çalışan (normal olarak bilgisayar ya da şirket iletişim ağlarını kullanmayanlar da dahil) şirketin veri sınıflandırma politikası konusunda eğitilmelidir. Şirket işgücünün -temizlikçiler, güvenlik görevlileri, fotokopicilerin yanısıra danışmanlar, taşeronlar ve hattâ stajyerler de aralarında olmak üzere- her üyesinin hassas bilgilere erişimi olabileceğinden, herkes bir saldırının hedefi olabilir.

Yönetim, şirket içinde halihazırda kullanımda olan her bilgi için bir *bilgi sahibi* belirlemelidir. Diğer şeylerin yanı sıra *bilgi sahibi* bilgi varlıklarının korunmasından sorumludur. Bilgiyi koruma gereksinimine göre hangi derece sınıflandırma yapılacağına o karar verir ve düzenli olarak sınıflandırma derecelerini yeniden değerlendirir ve uygun gördüğü değişiklikleri yapar. *Bilgi sahibi,* veri koruma görevini bir *vekile* ya da *sorumluya* da devredebilir.

Sınıflandırmalar ve Tanımlar

Bilgi, hassaslığına göre değişen sınıflandırma düzeylerine bölünmelidir. Bir sınıflandırma sistemi bir kez kurulduktan sonra bilgiyi yeniden sınıflandırmak zaman isteyen ve pahalı bir iş haline gelir. Örnek sınıflandırmamızda, orta-büyük ölçekli işletmelerin çoğu için uygun olacak dört sınıflandırma düzeyi seçtim. Hassas bilgilerin sayısı ve çeşidine göre işletmeler, belirli bilgi çeşitlerini de kapsamak için yeni sınıflandırmalar eklemek isteyebilirler. Daha küçük işletmelerde üç düzeyli bir sınıflandırma sistemi yeterli olacaktır.

Gizli: Bu bilgi sınıfı en hassas olanıdır. Gizli bilgiler yalnızca kurum içi kullanım içindir. Çoğu zaman kesinlikle bilmesi şart olan sınırlı sayıda insan tarafından bilinmelidir. Gizli bilgi, herhangi bir yetkisiz paylaşımın şirkete, hissedarlara ve/veya müşterilere ciddi zararlar verebileceği bir yapıdadır. Bu bilgiler genel olarak aşağıdaki gruplardan birine girerler:

- Ticari sırlar, tescilli kaynak kodları, teknik ya da işlevsel özellikler ya da bir rakibin işine yarayabilecek ürün bilgileri gibi bilgiler.
- Halka açılmamış finansal ya da pazarlamaya yönelik bilgiler.
- Gelecekteki iş stratejileri gibi şirketin işleri için önemli olan diğer bilgiler.

Özel: Bu sınıflandırma, kurum içinde kullanılması öngörülen kişisel nitelikteki bilgileri içerir. Özel bilginin yetkisiz dağıtımı çalışanların ya da yetkisiz kişilerin (özellikle toplum mühendislerinin) eline geçtiği zaman şirkete ciddi şekilde zarar verebilmektedir. Bu tarz bilgilerin arasında çalışanların tıbbî geçmişi, sağlık yardımları, banka hesap bilgileri, ücret geçmişi ya da halka açık olmayan diğer kişisel tanımlamalar bulunmaktadır.

NOT: *"Dahili" olarak sınıflandırılmış bilgiler, güvenlik personeli tarafından sık sık "Hassas" olarak da adlandırılırlar, Ben Dahili şeklinde kullanacağım çünkü terimin kendisi bilginin hitap ettiği kişileri tanımlıyor. Hassas terimini bir güvenlik sınıflandırması olarak değil de Gizli, Özel ve Dahili bilgilerinin tümünü anlatan bir terim olarak kullandım. Hassas, özellikle Genel olarak tanımlanmamış her türlü şirket bilgisine karşılık gelmektedir.*

Dahili: Bu bilgi sınıfı kurumda çalışan herkese rahatlıkla dağıtılabilir. Dahili bilginin yetkisiz dağıtımının çoğu zaman şirkete, hissedarlara, iş ortaklarına, müşterilere ya da çalışanlara ciddi bir zarar vermesi beklenmez. Buna karşın, toplum mühendisliği becerilerini kullanmakta usta olan kişiler bu bilgiyi kullanarak yetkili bir çalışan, taşeron ya da satıcı firma gibi davranıp hiçbir şeyden kuşkulanmayan personeli hassas bilgileri vermesi doğrultusunda kandırabilir ve bu, şirket bilgisayar sistemlerine yetkisiz bir erişim sağlanmasına neden olabilir.

Satıcı firmalara, taşeronlara, ortak şirketlere ve benzeri üçüncü şahıslara *dahili bilgi* verilmeden önce taraflar arasında bir gizlilik anlaşması imzalanmalıdır. Dahili bilgiler genellikle günlük işlerde kullanılan, dışarıya verilmemesi gereken şirket kuruluş şemaları, ağ bağlantı numaraları, dahili sistem adları, uzaktan erişim süreçleri, maliyet merkezi kodları ve bunun gibi herhangi bir bilgiyi içerebilir.

Genel: Özellikle kamuya duyurmak üzere belirlenmiş bilgilerdir. Basın açıklamaları, müşteri destek iletişim bilgileri ya da ürün broşürleri gibi bu tarz bilgiler herkese serbestçe dağıtılabilir. Genel olarak sınıflandırılmamış diğer tüm bilgilerin *hassas bilgi* olarak ele alınması gerektiği unutulmamalıdır.

Sınıflandırılmış Veri Terimleri

Sınıflandırmalarına göre veriler belli düzeylerdeki kişilere dağıtılmalıdırlar. Bu bölümde verilen bazı kurallar bilginin *onaylanmamış kişilere* verilmesiyle ilgilidir. Bu ifadeyi açmak gerekirse *onaylanmamış kişi*, şirkette halen çalışmakta ya da bilgiyi almak için doğru konumda olup olmadığının ya da güvenilir bir üçüncü şahsın ona kefil olup olmadığının çalışan tarafından bilinmediği kişidir.

Bunun tam tersi olan, *güvenilir kişi*, yüzyüze karşılaştığınız, bilgi erişimi için yeterli yetkiye sahip bir şirket çalışanı, müşteri ya da şirket danışmanı olarak tanıdığınız kişidir. *Güvenilir kişi* şirketinizle uzun süredir çalışan bir şirketin elemanı da olabilir (örneğin, bir müşteri, satıcı ya da sır saklama anlaşması imzalanmış bir stratejik iş ortağı gibi).

Üçüncü şahıs kefaletinde, bir *güvenilir kişi,* bir kişinin iş durumu ve kişinin bilgi ya da iş istemeye yetkili olup olmadığıyla ilgili kontrol verisi

sağlar. Bazı durumlarda bu kurallar, kefil oldukları birinden gelen bilgi ya da iş taleplerine karşılık vermeden önce *güvenilir kişinin* şirkette çalışmaya devam edip etmediğini de doğrulamanızı gerektirir.

Ayrıcalıklı hesap, temel kullanıcı hesabının ötesinde bilgisayar ya da benzeri bir ortama erişim izni soran, sistem yönetici hesabı türünden bir hesaptır. Ayrıcalıklı hesaplara sahip olan çalışanlar genellikle kullanıcı yetkilerini değiştirip, sistem işlevleri gerçekleştirebilirler.

Genel bölüm posta kutusu, bölüm adına genel bir mesajla açılan bir sesli mesaj kutusudur. Böyle bir kutu belirli bir bölümde çalışanların adlarını ve dahili numaralarını korumak amacıyla kullanılır.

Onay ve Yetkilendirme Süreçleri

Bilgi hırsızları, gizli şirket bilgilerine ulaşmak ve bu bilgileri ele geçirmek için çoğunlukla gerçek çalışanlar, taşeronlar, satıcılar ya da iş ortakları gibi davranarak aldatma taktikleri kullanırlar. Etkili bilgi güvenliğini sürekli kılmak için bir iş yapması ya da hassas bir bilgi vermesi istenen bir çalışan, arayanın kimliğini tespit etmeli ve bir istekte bulunma yetkisinin olup olmadığını onaylattırmalıdır.

Bu bölümde önerilen süreçler, herhangi bir iletişim aracıyla -telefon, faks ya da e-posta- kendisinden bir şey istenmiş bir çalışana, isteğin geçerli ve isteyenin de gerçek olup olmadığını belirlemekte yardımcı olmak üzere tasarlanmışlardır.

Güvenilir Kişiden Gelen İstekler

Bir güvenilir kişiden gelen iş ya da bilgi talebi durumunda şunların yapılması gerekebilir:

- Kişinin şirket bünyesinde çalıştığının ya da söz konusu sınıfa ait bilgilere erişim koşulunu da içeren bir ilişkinin varlığının kontrol edilmesi. Bunun amacı, ilişiği kesilmiş çalışanların, satıcıların, taşeronların ve benzer kişilerin kendilerini çalışıyor olarak göstermelerini önlemektir.
- Kişinin bilme gereksiniminin ve bir iş ya da bilgi talebinde bulunmaya yetkili olup olmadığının kontrol edilmesi.

Onaylanmamış Bir Kişiden Gelen İstekler

Onaylanmamış bir kişi bir istekte bulunduğu zaman, istekte bulunan kişinin bu talepte bulunmaya yetkili olup olmadığını belirlemek için uygun bir onay süreci kullanılmalıdır. Özellikle de istek, bilgisayarlar ya da bilgisayar donanımlarıyla ilgiliyse. Bu süreç, toplum mühendisliği saldırılarının başarılı olmasını engellemek için temel bir önlemdir. Eğer bu

onay süreçleri uygulanırsa, başarılı toplum mühendisliği saldırılarının sayısını büyük ölçüde azalacaktır.

Süreci maliyet artırıcı ya da çalışanların onu boşvereceği kadar hantal yapmamanız da önemlidir.

Aşağıda da belirtildiği gibi onay süreci üç adımdan oluşur:

- Kişinin olduğunu söylediği kişi olup olmadığının kontrol edilmesi.
- Talep sahibinin halen şirkette çalıştığının ya da şirketle bilme gereği oluşturabilecek bir ilişkisinin olduğunun belirlenmesi.
- Kişinin ilgili bilgiyi almaya ya da ilgili işi talep etmeye yetkili olup olmadığının belirlenmesi.

Birinci Adım: Kimlik Tespiti

Önerilen onay adımları, etkinliklerine göre aşağıda sıralanmışlardır; sayı ne kadar büyük olursa yöntem o kadar etkilidir. Her öğeyle birlikte, ilgili yöntemin zayıflığıyla ve bir toplum mühendisinin çalışanları kandırabilmek için bu yöntemi aşma ya da çevresinden dolaşma yoluyla ilgili bir açıklama bulunmaktadır.

1. **Arayan Kimliği** (bu özelliğin şirket telefon sisteminde var olduğunu varsayıyoruz): Arayan numaraya bakarak, aramanın şirket içinden mi yoksa dışından mı geldiği bulunabilir ve arayanın verdiği kimliğin görünen ad ve telefon numarasıyla uyuşup uyuşmadığına bakılır.

   Zayıflığı: Dışarıdan gelen aramaya ait arayan kimliği bilgileri, dijital telefon hizmetlerine bağlı bir PBX ya da telefon santralına erişimi olan herhangi biri tarafından sahte bilgilerle değiştirilebilir.

2. **Geri Arama:** İstek sahibi, şirket rehberinden bulunur ve rehberde geçen dahili numara aranarak istekte bulunan kişinin gerçekten şirkette çalışıp çalışmadığı kontrol edilir.

   Zayıflığı: Çalışan, listede geçen şirket dahili numarasını kontrol amaçlı olarak aradığı zaman, yeterli bilgiye sahip bir saldırgan, aramayı kendi dış hattına aktarılacak şekilde yönlendirebilir.

3. **Kefil Olunması:** İstek sahibine kefil olmuş bir *güvenilir kişi* istekte bulunan kişinin kimliğini onaylamış olur.

   Zayıflığı: Başka biri gibi davranan saldırganlar, farklı bir çalışanı kimliklerinin doğruluğuna çoğunlukla inandırabilirler ve o çalışanın kendilerine kefil olmasını sağlayabilirler.

4. **Gizli Ortak Bilgi:** Kurum çapında kullanılan, parola ya da günlük şifre gibi bir gizli ortak bilgi.

   Zayıflığı: Eğer gizli ortak bilgiyi çok kişi bilirse, saldırganın onu öğrenmesi daha kolay olur.

5. **Çalışanın Yöneticisi/Müdürü:** Çalışanın bağlı olduğu yönetici aranır ve onay istenir.

   Zayıflığı: Eğer yöneticinin numaralarını istekte bulunan şahıs vermişse, çalışan o numarayı aradığında ulaştığı kişi gerçek yönetici değil aslında saldırganın suç ortağı olabilir.

6. **Güvenli e-posta:** Dijital olarak imzalı bir mesaj istenir.

   Zayıflığı: Eğer saldırgan zaten çalışanın bilgisayarına girmiş ve çalışanın imza parolasını alabilmek için tuş girişlerini kaydeden bir program yüklemişse, bu durumda çalışandan geliyormuş gibi görünen dijital imzalı bir e-posta gönderebilir.

7. **Sesi Şahsen Tanımak:** Kendisine istek gelen kişinin istek sahibiyle daha önceden çalışmış olması (tercihen yüz yüze), bir *güvenilir kişi* olduğundan emin olması ve kişinin sesini telefondan tanıyacak kadar kişiyi tanıması.

   Zayıflığı: Bu oldukça güvenli bir yöntemdir ve bir saldırgan tarafından kolay kolay aşılamaz, ancak kendisine istek gelen kişi arayanı tanımıyorsa ya da daha önce onunla hiç konuşmamışsa bu yöntem bir işe yaramaz.

8. **Değişken Parola Çözümü:** İstek sahibi *güvenli kimlik* gibi bir değişken parola çözümüyle kendini tanıtır.

   Zayıflığı: Bu yöntemi aşmak için saldırganın, hem değişken parola cihazlarından birini, hem de cihazın ait olduğu çalışanın kimlik numarasını ele geçirmesi gerekir ya da bir çalışanı cihazın üzerinden bilgiyi okuması ve kimlik numarasını vermesi için kandırabilir.

9. **Kimliğiyle Birlikte Gelen Kişi:** İstekte bulunan kişi şahsen gelir ve tercihen resimli personel kartını ya da başka uygun bir kimlik kartını gösterir.

   Zayıflığı: Saldırganlar sık sık bir çalışanın kartını çalabilir ya da gerçek gibi görünen bir sahtesini yapabilirler. Ancak saldırganlar çoğunlukla bu yaklaşımı kullanmazlar çünkü bir yere şahsen gitmek saldırganı büyük bir tanınma ve alıkonma tehlikesine sokar.

İkinci Adım: İş Durumunun Kontrolü

En büyük bilgi güvenliği tehdidi bir profesyonel toplum mühendisinden ya da becerikli bir bilgisayar korsanından gelmez. Çok daha yakındaki birinden, kısa süre önce işten atılmış, intikam almak isteyen ya da şirketten çaldığı bilgileri kullanarak kendi işini kurmayı ümit eden çalışandan gelir (Bu sürecin başka bir türünün, satıcı, danışman ya da sözleşmeli işçi gibi şirketinizle farklı bir iş ilişkisi olan kişiler için de kullanılabileceğini unutmayınız).

Başka birine Hassas bilgiler vermeden ya da bilgisayar ve bilgisayar donanımlarıyla ilgili başka birinin verdiği talimatlara uymadan önce konuştuğunuz kimsenin sizinle aynı şirkette çalışıp çalışmadığını şu yöntemlerden birini kullanarak kontrol edebilirsiniz.

Personel Telefon Rehberinden Kontrol: Eğer şirket, çalışanların listesinin titizlikle tutulduğu bir çevrimiçi telefon rehberi bulunduruyorsa, arayanın bu listede olduğundan emin olun.

Arayanın Yöneticisinden Kontrol: Arayanın yöneticisini, arayanın verdiği numaradan değil, şirket rehberinde geçen numarasından arayın.

Arayanın Birim ya da İş Gurubundan Kontrol: Arayanın birimini ya da iş grubunu arayın ve orada çalışan herhangi birinden söz konusu kişinin orada çalışmakta olup olmadığını öğrenin.

Üçüncü Adım: Bilme Gereğinin Kontrolü

İstekte bulunan kişinin halen şirkette çalışıp çalışmadığını ya da şirketinizle bir ilişkisi kalıp kalmadığını kontrol etmenin yanısıra, bir de, istek sahibinin istediği bilgiyi talep etmeye ya da bilgisayarları veya bilgisayar donanımlarını etkileyecek belirli işlemleri talep etmeye yetkili olup olmadığı konusu vardır.

Bunun kontrolü şu yöntemlerden biri kullanılarak yapılabilir:

İşyeri Unvan/İş Gurubu/Sorumluluklar Listelerine Başvurun: Bir şirket hangi çalışanların ne tür bilgileri almaya yetkili olduğunu içeren listeler çıkararak yetkilendirme bilgilerine hızlı erişim sağlayabilir. Bu listeler çalışan unvanına, birimine ve iş gurubuna, sorumluluklara ya da başka verilere göre sıralanmış olabilir. Bu tarz listelerin çevrimiçi tutulması ve sürekli güncellenerek yetkilendirme bilgilerine hızlı erişim sağlaması gerekir. Çoğunlukla *bilgi sahipleri*, denetimleri altında olan bilgilere erişilebilmesi için listelerin oluşturulmasından ve güncellenmesinden sorumludurlar.

Bir Yöneticiden Onay Alın: Bir çalışan, isteği yerine getirmek üzere onay almak için kendi yöneticisiyle ya da istek sahibinin yöneticisiyle bağlantıya geçer.

NOT: *Bu tarz listelerin toplum mühendisine davetiye çıkarmak olduğu da göz önünde bulundurulmalıdır. Düşünün: Eğer bir şirketi hedefleyen bir saldırgan şirketin böyle listeler tuttuğunu öğrenecek olursa bir tanesini ele geçirmek için bir nedeni olacaktır. Ele geçirdikten sonra da bu tarz listeler saldırgana pek çok kapı açarlar ve şirket için ciddi bir tehlike oluştururlar.*

Bilgi Sahibinden ya da Sorumlusundan Onay Alın: Belirli bir kişinin bilgiye erişimi olup olmayacağıyla ilgili son söz hakkı *bilgi sahibinindir*. Bilgisayar tabanlı erişim kontrol süreci, var olan iş tanımlarına uygun bilgilere erişme talebinin onayı için çalışanın kendi yöneticisini aramasıdır. Eğer böyle bir tanım yoksa, ilgili *bilgi sahibini* arayıp izin istemek yöneticinin sorumluluğudur. Bu emir-komuta zincirine uyulması gerekir, yoksa *bilgi sahipleri* sık sık gelen bir talep akınına uğrarlar.

Tescilli Bir Yazılım Paketi Aracılığıyla Onay Alın: Rekabetçi bir ortamda çalışan büyük bir şirketin bilme gereği yetkilerini veren tescilli bir yazılım paketi geliştirmesi kullanışlı olabilir. Böyle bir veritabanı, çalışan adlarını ve gizli bilgilere erişim yetkilerini tutar. Kullanıcılar her çalışanın erişim yetkilerini göremezler ama onun yerine istekte bulunan kişinin adını ve istenen bilginin tanımlayıcısını girebilirler. Daha sonra yazılım, aranan kişinin ilgili bilgileri almaya yetkili olup olmadığına dair bir sonuç çıkarır. Bu seçenek, değerli, önemli ya da hassas bilgilere erişim yetkisine sahip personel listelerinin çalınma tehlikesini bertaraf eder.

Yönetim Kuralları

Aşağıdaki kurallar yönetici seviyesindeki çalışanlarla ilgilidir. Veri Sınıflandırılması, Bilgi Verilmesi, Telefon İdaresi ve Çeşitli Kurallar gibi konulara bölünmüşlerdir. Her kural sınıfı kuralların rahat tanımlanabilmeleri için kendine özgü bir sayılandırma içermektedir.

Veri Sınıflandırma Kuralları

Veri Sınıflandırma, şirketinizin hassas verilerinin nasıl sınıflandırıldığına ve bu bilgilere kimlerin erişim yetkisinin olması gerektiğine değinir.

1-1 Veri sınıflandırması yapın

Kural: Tüm değerli, hassas ya da önemli iş bilgileri ilgili *bilgi sahibi* ya da *vekili* tarafından bir sınıflandırmaya tutulmalıdır.

Açıklamalar/Notlar: İlgili *bilgi sahibi* ya da *vekili* iş hedeflerine ulaşmak için düzenli olarak kullanılan herhangi bir bilgiyi uygun veri sınıfına yerleştirecektir. *Bilgi sahibi,* bu tarz bilgilere kimlerin erişebileceğini ve bu bilgilerle neler yapılabileceğini denetler. *Bilgi sahibi,* sınıflandırmayı yeniden yapabilir ve düzenli olarak sınıflandırmanın yenilenmesi için bir zaman belirleyebilir.

Başka bir şekilde sınıflandırılmamış her bilgi *hassas* olarak sınıflandırılmalıdır.

1-2 Sınıflara göre kullanma süreçleri çıkarın

Kural: Şirket her sınıf bilginin verilmesine yönelik süreçler oluşturmalıdır.

Açıklamalar/Notlar: Sınıflandırmalar yapıldıktan sonra, bilginin çalışanlara ve dışardan kişilere verilmesiyle ilgili, daha önce bu bölümde Onay ve Yetkilendirme konusunda anlatıldığı gibi süreçler oluşturulmalıdır.

1-3 Tüm öğeleri işaretleyin

Kural: Gizli, özel ya da dahili bilgi içeren hem basılı malzemeleri, hem de bilgisayar saklama ortamlarını ilgili veri sınıflandırmasını gösterecek açık bir şekilde işaretleyin.

Açıklamalar/Notlar: Basılı belgelerin, üstünde göze çarpan bir veri sınıfı işareti olan bir kapak sayfası olmalıdır ve veri sınıfı, belge açıldığında da görülecek şekilde her sayfada bulunmalıdır.

İlgili veri sınıflarıyla kolaylıkla işaretlenemeyen tüm elektronik dosyalar, (veritabanı ya da ham veri dosyaları), uygunsuz bir şekilde dağıtılmasını, değiştirilmesini, yok edilmesini ya da erişilemez duruma getirilmesini önlemek için erişim denetimleriyle korunmalıdırlar.

Disketler, bantlar ve CD-ROM'lar gibi tüm veri taşıma ortamları, içlerindeki en üst düzey güvenlik seviyesine göre sınıflandırılmalıdırlar.

Bilginin Verilmesi

Bilgi verilmesi, kim olduklarına ve bilme gereklerine bakılarak bilginin çeşitli şahıslara verilmesini kapsar.

2-1 Çalışan kimliğinin tespiti süreci

Kural: Gizli ya da hassas bilgilerin verilmesini ya da herhangi bir bilgisayar donanımının ya da yazılımının kullanılmasını içeren bir işin yapılmasından önce kişinin kimliğinin, iş durumunun ve yetkilerinin kontrol edilebilmesi için çalışanların kullanabileceği kapsamlı süreçler şirket tarafından oluşturulmalıdır.

Açıklamalar/Notlar: Şirketin büyüklüğü ve güvenlik ihtiyaçlarına uygun olarak, kimlik tespiti için, gelişmiş güvenlik teknolojileri kullanılmalıdır. En iyi güvenlik uygulaması, tanımlama anahtarını gizli ortak bilgiyle birlikte kullanarak istekte bulunan kişileri doğru bir şekilde tanımlamaktır. Bu uygulama, riski büyük ölçüde azaltsa da bazı işletmeler için maliyeti çok yüksek olabilir. Bu koşullarda şirket, günlük bir parola ya da şifre gibi tüm şirket çapında geçerli bir gizli ortak bilgi kullanabilir.

2-2 Bilginin üçüncü şahıslara verilmesi

Kural: Bir dizi kendini kanıtlamış bilgi verme süreci yürürlüğe konmalı ve tüm çalışanlar bu süreçleri izlemeleri konusunda eğitilmelidirler.

Açıklamalar/Notlar: Dağıtım süreçlerinin genel olarak şunlar için oluşturulması gerekir:

- Şirket içine verilecek bilgiler;
- Danışmanlara, geçici işçilere, stajyerlere, şirketle alıcı-satıcı ilişkisi ya da stratejik ortaklık anlaşması olan kuruluşların çalışanlarına ve bunun gibi, şirketle oturmuş bir ilişkisi olan kuruluşların çalışanlarına bilginin verilmesi;
- Şirket dışına verilecek bilgiler;
- Bilgi şahsen, telefonla, e-postayla, faksla, sesli mesajla, posta aracılığıyla, imzalı kuryeyle ve elektronik aktarımla veriliyorsa her veri sınıfıyla ilgili bilgiler.

2-3 Gizli bilgilerin dağıtımı

Kural: Yetkisiz kişilerin eline geçtiğinde büyük zararlara neden olabilecek şirket bilgileri olan *gizli* bilgiler ancak almaya yetkili bir *güvenilir kişiye* verilebilir.

Açıklamalar/Notlar: Fiziksel (yani basılı ya da taşınabilir saklama ortamı) olarak gizli bilgiler şu şekilde teslim edilebilir:

- Şahsen;
- Mühürlü ve gizli damgası vurulmuş olarak dahili kuryeyle;
- Şirket dışına itibarlı bir kurye şirketinin hizmetiyle ya da taahhütlü veya onaylı posta hizmeti kullanarak.

Elektronik (bilgisayar dosyaları, veritabanı dosyaları, e-posta) olarak gizli bilgiler şu şekilde teslim edilebilir:

- Şifreli e-posta içeriğinde;
- Şifreli bir dosya olarak e-posta ekinde;
- Şirket dahili ağındaki bir sunucuya elektronik aktarımla;
- Bir faks programı kullanarak bilgisayardan. Ancak karşı makinayı ilgili kişinin kullandığından ya da faks gönderilirken ilgili kişinin makinanın başında beklediğinden emin olunması gerekir. Diğer bir seçenek ise, şifreli bir telefon hattından parola korumalı bir faks sunucusundan gönderilmesi durumunda, faksın alıcı olmadan gönderilmesi mümkündür.

Gizli bilgiler, karşılıklı, şirket içi telefonla, şirket dışından şifreli telefonla, şifreli uydu aktarımıyla, şifreli videokonferans bağlantısıyla ve şifreli İnternet Protokolü üzerinden ses geçidiyle (VoIP) yapılan karşılıklı görüşmelerle de iletilebilirler.

Faksla gönderimlerde önerilen yöntem, gönderenin bir kapak say-

fası göndermesini, alıcının sayfayı alması üzerinde karşılık olarak başka bir sayfa göndererek faks makinasının başında olduğunu göstermesini içermektedir. Gönderen, daha sonra faksın tümünü gönderir.

Şu iletişim kanalları ise gizli bilgilerin görüşülmesi ya da dağıtılması için kabul edilebilir yöntemler değillerdir: Şifresiz e-postalar, sesli mesajlar, posta hizmetleri ya da herhangi bir telsiz iletişim yöntemi (cep telefonları, kısa mesaj hizmetleri ya da telsiz telefonlar)

2-4 Özel bilgilerin dağıtımı

Kural: Açığa çıktıkları takdirde çalışanlara ya da şirkete zarar vermek üzere kullanılabilecek, çalışan ya da çalışanlarla ilgili kişisel bilgileri ifade eden özel bilgiler, yalnızca onu almaya yetkili bir *güvenilir kişiye* teslim edilebilir.

Açıklamalar/Notlar: Fiziksel (yani basılı ya da taşınabilir saklama ortamı) olarak özel bilgiler şu şekilde teslim edilebilir:

- Şahsen;
- Mühürlü ve özel damgası vurulmuş olarak dahili kuryeyle;
- Posta hizmetiyle.

Elektronik (bilgisayar dosyaları, veritabanı dosyaları, e-posta) olarak özel bilgiler şu şekilde teslim edilebilir:

- Dahili e-postayla;
- Şirket dahili ağındaki bir sunucuya elektronik aktarımla;
- Bir faks programı kullanarak bilgisayardan, ancak karşı makinayı ilgili kişinin kullandığından ya da faks gönderilirken ilgili kişinin makinanın başında beklediğinden emin olunması gerekir. Diğer bir seçenek ise, şifreli bir telefon hattından parola korumalı bir faks sunucusuna gönderilmesi durumunda, faksın alıcı olmadan gönderilmesi mümkündür.

Özel bilgiler, karşılıklı, şirket içi telefonla, uydu aktarımıyla, videokonferans bağlantısıyla ve şifreli İnternet Protokolü izerinden ses geçidiyle (VoIP) yapılan karşılıklı görüşmelerle de iletilebilirler.

Şu iletişim kanalları ise özel bilgilerin görüşülmesi ya da dağıtılması için kabul edilebilir yöntemler değillerdir: Şifresiz e-postalar, sesli mesajlar, posta hizmetleri ya da herhangi bir telsiz iletişim yöntemi (cep telefonları, kısa mesaj hizmetleri ya da telsiz telefonlar)

2-5 Dahili bilgilerin dağıtımı

Kural: Dahili bilgiler, yalnızca şirket içinde dağıtılabilecek ya da gizlilik anlaşması imzalamış *güvenilir kişilere* verilebilecek bilgilerdir. Dahili bilginin dağıtımına yönelik yönergeler hazırlamanız gerekir.

Açıklamalar/Notlar: Dahili bilgiler, aralarında dahili e-posta da olmak üzere her yolla iletilebilirler, ancak şifreli olmadıkları sürece e-postayla şirket dışına gönderilemezler.

2-6 Hassas bilgilerin telefon üzerinden görüşülmesi

Kural: Genel sınıfında tanımlanmamış herhangi bir bilgiyi telefon üzerinde görüşmeden önce, bilgiyi verecek kişinin, karşı tarafın sesini daha önceden şahsen duymuş olması ya da şirket telefon sisteminin aramanın istek sahibine ait dahili bir numaradan yapıldığını tespit etmiş olması gerekmektedir.

Açıklamalar/Notlar: Eğer istekte bulunan kişinin sesi tanınmıyorsa, kayıtlı bir ses mesajından sesleri karşılaştırabilmek için arayanın dahili numarasını arayın ya da arayanın yöneticisine kimliğini ve bilme gereğini onaylattırın.

2-7 Girişte ya da danışmada görevli personel süreçleri.

Kural: Giriş görevlileri, şirkette çalışıp çalışmadığını bilmedikleri herhangi birine herhangi bir paketi verirlerken resimli kimlik kontrolü yapmalıdırlar. Kişinin adının, ehliyet numarasının, doğum tarihinin, alınan paketin ve alımın gerçekleştiği gün ve saatin işlendiği bir kayıt defteri tutulmalıdır.

Açıklamalar/Notlar: Bu kural dışarı gönderilen paketlerin taşıyıcılara ya da kurye hizmeti veren şirketlere teslim edilmesinde de geçerlidir. Bu şirketler, çalışanların kimliklerinin kontrol edilebileceği kimlik kartları çıkarırlar.

2-8 Üçüncü şahıslara yazılım aktarımı

Kural: Herhangi bir yazılım, program ya da bilgisayar açıklamalarının verilmesinden ya da aktarılmasından önce istek sahibinin doğru kişi olduğu belirlenmeli ve bu aktarımın, söz konusu bilginin veri sınıfıyla tutarlı olup olmadığı kesinleştirilmelidir. Şirket bünyesinde kaynak kodu biçiminde yapılmış yazılımlar çoğunlukla şirket mülkü sayılır ve gizli olarak sınıflandırılırlar.

Açıklamalar/Kurallar: Yetki belirlenmesi genellikle istekte bulunan kişinin işini yapmak için yazılım erişimine ihtiyacı olup olmadığına göre yapılır.

2-9 Satış ve pazarlamanın müşteri önerilerinin incelemesi

Kural: Satış ve pazarlama personeli, dahili geri arama numaralarını, ürün planlarını, ürün grubu iletişim sorumlularını ya da diğer hassas bilgileri olası bir müşteriye vermeden önce verilen önerileri incelemelidir.

Açıklamalar/Notlar: Satış ve pazarlama temsilcisiyle bağlantı ku-

rup, onu ufukta büyük bir alımın olacağına inandırmak, sanayi casuslarının sık kullandıkları yöntemler arasındadır. Satış fırsatından yararlanma çabasıyla satış ve pazarlama temsilcileri, saldırgan tarafından hassas bilgilere ulaşmak için poker markası olarak kullanılabilecek bilgileri sık sık verirler.

2-10 Dosya ve verilerin aktarımı

Kural: İstek sahibi, kimliği belirlenmiş ve veriyi ilgili taşınabilir ortamda alması gerektiği anlaşılmış bir *güvenilir kişi* olmadığı sürece dosyalar ya da diğer elektronik veriler hiçbir taşınabilir ortama aktarılmamalıdır.

Açıklamalar/Notlar: Bir toplum mühendisi hassas bilgilerin bir banda, diskete ya da diğer taşınabilir ortamlara kopyalanmış olarak kendine gönderilmesini ya da birinin gelip alması için girişte bekletilmesini istemek için akla yatkın bir gerekçe sunarak çalışanı kandırabilir.

Telefon İdaresi

Telefon idaresi kuralları, çalışanların, arayan kimliğini kontrol edebilmelerini ve şirketi arayan kişilere karşı kendi iletişim bilgilerini korumalarını sağlar.

3-1 Bilgisayar bağlantısı ya da faks numaralarında aramaların yönlendirilmesi

Kural: Aramaları dış hat telefon numaralarına yönlendiren arama yönlendirme hizmetleri şirket içindeki herhangi bir modem ya da faks numarasına sağlanmamalıdır.

Açıklamalar/Notlar: Çok yönlü saldırganlar, dahili numaraları saldırganın kontrolü altındaki bir dış hat telefonuna yönlendirmeleri konusunda telefon şirketi personelini ya da dahili telekomünikasyon çalışanlarını kandırmaya çalışabilirler. Bu saldırı, saldırganın, fakslara müdahale edebilmesine, gizli bilgilerin şirket içine fakslanmalarını isteyebilmesine (çalışanlar kurum içine birşey fakslamanın emin olduğunu varsayarlar) ya da bağlantı hatlarını giriş sürecinin aynısını taklit eden tuzak bir bilgisayara yönlendirerek modemle bağlanan kullanıcıların parolalarını ele geçirmesine yol açacaktır.

Şirket içinde kullanılan telefon hizmetine göre arama yönlendirme özelliği, telekomünikasyon bölümünden çok, iletişim hizmeti sağlayıcısının kontrolü altında olabilir. Bu durumda arama yönlendirme özelliğinin bağlantı ve faksa ayrılmış telefon numaralarında bulunmamasını isteyen bir taleple iletişim hizmet sağlayıcısına gidilmesi gerekecektir.

3-2 Arayan kimliği

Kural: Şirket telefon sistemi, tüm dahili telefonlara arayan hat tanımlama (arayan kimliği) hizmetini sağlamalıdır ve eğer münkünse, dışarıdan gelen aramalarda farklı bir çalma sesi kullanılmalıdır.

Açıklamalar/Notlar: Eğer çalışanlar, şirket dışından gelen aramaların kimden geldiğini görebilirlerse, bu onların bir saldırıyı engellemelerine ya da ilgili güvenlik sorumlusuna saldırganı tarif etmelerine yardımcı olabilir.

3-3 Nezaket telefonları

Kural: Ziyaretçilerin şirket çalışanı gibi davranmalarını önlemek için her nezaket telefonunun nereden edildiği (örneğin, "Danışma") aranan ın telefon göstergesinde açıkça görülebilmelidir.

Açıklamalar/Notlar: Eğer dahili aramaların arayan kimlikleri yalnızca dahili numarayı gösteriyorsa, danışma ve diğer herkese açık yerlerdeki şirket telefonlarından yapılan aramalara yönelik uygun önlemler alınmalıdır. Bir saldırganın bu telefonlardan birinden arama yapması ve aramanın herhangi bir başka çalışanın telefonundan yapıldığı doğrultusunda aradığı kişiyi kandırmasının mümkün olmaması gerekmektedir.

3-4 Telefon sistemleri ile gelen üretici parolaları

Kural: Sesli mesaj yöneticisi, şirket çalışanları tarafından kullanılmadan önce telefon sistemiyle birlikte gelen parolalar değiştirilmelidir.

Açıklamalar/Notlar: Toplum mühendisleri, üreticilerden ilk parola listelerini edinebilir ve bunları yönetici hesaplarına erişmek için kullanabilirler.

3-5 Bölüm sesli mesaj kutuları

Kural: Dışarıyla bağlantısı olabilecek her bölüme için bir sesli mesaj kutusu oluşturun.

Açıklamalar/Notlar: Toplum mühendisliğinin ilk adımı hedef şirket ve çalışanları hakkında bilgi toplamaktır. Şirket, çalışanların ad ve telefon numaralarına erişimi sınırlayarak, toplum mühendisinin şirket içinden hedef belirlemesini ya da çalışanları kandırmak için başkalarının adlarını kullanmasını güçleştirebilir.

3-6 Telefon sistem satıcısının onaylanması

Kural: Satıcı firmadan gelen hizmet teknisyenlerinden hiçbirine, satıcı firma bilgileri ve gelenlerin yetkileri onaylanmadan, şirket telefon sistemine uzaktan erişim hakkı tanınmamalıdır.

Açıklamalar/Notlar: Şirket telefon sistemlerine giren bilgisayar korsanları sesli mesaj kutusu yaratma, diğer kullanıcılara gelen mesajlara

müdahale etme ya da parasını şirketin ödediği telefon görüşmeleri yapabilme becerisini kazanırlar.

3-7 Telefon sisteminin ayarlanması

Kural: Sesli mesaj yöneticisi, telefon sisteminde ilgili güvenlik ayarlamalarını yaparak güvenlik gerekliliklerinin yerine getirilmesini sağlar.

Açıklamalar/Notlar: Telefon sistemleri sesli mesajlar için az ya da çok kapsamlı güvenlik düzeylerine göre ayarlanabilirler. Yönetici, şirket güvenlik anlayışının bilincinde olmalı ve sistemi hassas bilgileri korumak üzere ayarlamak için güvenlik sorumlularıyla birlikte çalışmalıdır.

3-8 Arama izleme özelliği

Kural: İletişim hizmetleri veren firmanın sınırlamalarına göre, çalışanların, arayanın saldırgan olduğundan kuşkulandıkları durumda kıstırıp kovalayan bu işlevi çalıştırabilmeleri sağlanabilecek şekilde, arama izleme özelliği devreye sokulmalıdır.

Açıklamalar/Notlar: Çalışanlar, arama izleme işlevinin kullanımı ve kullanılacağı durumlar konusunda eğitilmelidirler. Arayan kişi, açıkça, şirket bilgisayar sistemlerine yetkisiz girmeye ya da hassas bilgileri ele geçirmeye çalışıyorsa, bir arama izleme süreci başlatılmalıdır. Ne zaman bir çalışan arama izleme özelliğini çalıştırırsa, *Olay Bildirme Merkezi'ne* de hemen haber verilmelidir.

3-9 Otomatik telefon sistemleri

Kural: Eğer şirket otomatik bir yanıt verme sistemi kullanıyorsa, sistem bir çalışana ya da bölüme aramayı aktarırken dahili numarayı söylemeyecek şekilde programlanmalıdır.

Açıklamalar/Notlar: Saldırganlar bir şirketin otomatik telefon sistemini, çalışan adlarını dahili telefonlarla karşılaştırmak için kullanabilirler. Daha sonra saldırganlar bu dahili numara bilgilerini kullanarak aradıkları kişileri şirket içi bilgi almaya yetkili çalışanlar olduklarına inandırırlar.

3-10 Birbiri ardına başarısız girme denemesinden sonra sesli mesaj kutularının kapatılması

Kural: Peşpeşe belirli bir sayıda başarısız girme denemesi olduğunda sesli mesaj hesaplarını kilitleyecek şekilde şirket telefon sisteminin programlanması.

Açıklamalar/Notlar: Telekomünikasyon yöneticisi ardı ardına beş başarısız giriş denemesinden sonra sesli mesaj kutusunu kapatmalıdır. Yönetici daha sonra kilitli sesli mesaj kutularını tek tek kendisi açmalıdır.

3-11 Sınırlandırılmış dahili telefonlar

Kural: Çoğu zaman dışarıdan gelen aramaları kabul etmeyen bölüm ve iş gruplarına ait tüm dahili telefonlar (yardım masası, bilgisayar odası, çalışan teknik destek vb.) yalnızca diğer dahili telefonların ulaşabileceği şekilde programlanmalıdır. Diğer bir seçenek ise parola korumalı olması ve dışarıdan arayan çalışanların doğru parolayı girmeleridir.

Açıklamalar/Notlar: Her ne kadar bu kural amatör toplum mühendislerinin çoğu girişimlerini önleyebilse de, kararlı bir toplum mühendisinin bazen bir çalışanı sınırlı bir hattı aramaya ve karşı taraftan saldırganı geri aramaya ya da yalnızca sınırlı hattâ bir toplu görüşme oluşturmaya ikna edebileceği de unutulmamalıdır. Saldırgana yardımcı olacak şekilde çalışanların kandırılması yöntemi bu taktiklerle ilgili bilinci artırmak amacıyla güvenlik eğitimleri sırasında tartışılmalıdır.

Çeşitli

4-1 Personel kartı tasarımı

Kural: Personel kartları uzaktan tanınabilecek büyük bir fotoğraf içerecek şekilde tasarlanmalıdır.

Açıklamalar/Notlar: Sıradan tasarımlı şirket kimlik kartlarındaki fotoğraflar işe yaramazdan bir gömlek üstündür. Binaya giren biriyle, kimlik kontrolüne yetkili bir güvenlik ya da danışma görevlisi arasındaki uzaklık o kadar fazladır ki, kişi yürüyüp geçerken, resim, seçilemeyecek kadar küçük kalır. Böyle bir durumda fotoğrafın işe yarayabilmesi için kartın yeniden tasarlarması şarttır.

4-2 Konum ya da sorumluluk değiştirirken erişim haklarının gözden geçirilmesi

Kural: Ne zaman bir şirket çalışanının konumu değişir ya da sorumlulukları azalır veya çoğalırsa, çalışanın yöneticisi, gerekli güvenlik profilinin oluşturulması için değişimden Bilgi İşlem Merkezini haberdar eder.

Açıklamalar/Notlar: Çalışanların erişim yetkilerinin yönetimi, korunması gereken bilgilerin açığa çıkmasını kısıtlamak için şarttır. En düşük yetki kuralı geçerli olacaktır: Kullanıcılara verilen erişim yetkileri işlerini yapmalarında gerekli olan en düşük seviye olacaktır. Yükseltilmiş erişim yetkileriyle sonuçlanan değişim talepleri yükseltilmiş erişim yetkileri veren bir kuralla bağlantılı olmalıdır.

Hesap sahibinin erişim yetkilerini ihtiyaç doğrultusunda ayarlamaları için Bilgi İşlem birimine haber verme sorumluluğu, çalışanın yöneticisinin ya da insan kaynakları bölümünündür.

4-3 Şirket çalışanı olmayanlar için özel kimlik

Kural: Şirketiniz, düzenli olarak içeride işi olan ama şirket çalışanı olmayan kişiler ve güvenilir kuryeler için özel fotoğraflı şirket kartı çıkarmalıdır.

Açıklamalar/Notlar: Düzenli olarak binaya girmesi gereken şirket dışı kişiler (örneğin, kafeteryaya yiyecek ve içecek getirenler, fotokopi makinası tamircileri ya da telefon bağlamaya gelenler) şirketiniz için bir tehdit oluşturabilirler. Bu ziyaretçilere kart çıkarmaya ek olarak şirketlerin, çalışanlarına kartsız bir ziyaretçi gördüklerinde nasıl davranmaları gerektiği konusunda da eğitim verilmelidir.

4-4 Taşeronların bilgisayar hesaplarını kapatmak

Kural: Kendisine bir bilgisayar hesabı açılmış bir taşeron işini bitirdikten ya da sözleşmesi sona erdikten sonra, sorumlu yönetici derhal Bilgi İşlem bölümünü haberdar ederek uzaktan erişim için telefon bağlantısı ya da internet erişimleri ve veritabanı erişim hesapları da dahil olmak üzere taşeronun bilgisayar hesaplarını kapattıracaktır.

Açıklamalar/Notlar: Bir çalışanın işine son verildiğinde verilere ulaşmak için şirket sistemleri ve süreçleri bilgisini kullanma tehlikesi vardır. Eski çalışanın kullandığı ya da bildiği tüm bilgisayar hesapları hemen kapatılmalıdır. Bu hesapların arasında üretim veri tabanına erişim, uzaktan bağlantı ve bilgisayar bağlantılı donanımlara erişim için kullanılan diğer hesaplar da bulunmalıdır.

4-5 Olay bildirme merkezi

Kural: Bir olay bildirme merkezi kurulmalı ya da daha küçük şirketlerde, olası güvenlik olaylarına yönelik uyarıları alıp duyuracak bir olay bildirme sorumlusu ve yardımcısı seçilmelidir.

Açıklamalar/Notlar: Şüpheli güvenlik olaylarının bildirilmesi işlevini merkezîleştirerek daha önce fark edilemeyecek türden bir saldırının fark edilmesi sağlanabilir. Şirket çapında düzenli saldırılar görülür ve bunlar bildirilirse olay bildirme merkezi saldırganın neyi hedeflediğini bulabilir; böylece ilgili varlıkları korumak için özel bir çaba harcanabilir.

Olay raporlarını almakla görevlendirilmiş çalışanlar toplum mühendisliği yöntem ve taktiklerine aşina olmalıdırlar. Böylece raporları değerlendirip, devam eden bir saldırıyı görebilirler.

4-6 Olay bildirme hattı

Kural: Olay bildirme merkezine hatırlaması kolay bir dahili numarası olan bir hat açılabilir.

Açıklamalar/Notlar: Çalışanlar bir toplum mühendisliği saldırısının hedefi olduklarından şüphelendiklerinde hemen olay bildirme merkezi-

ni haberdar edebilmelidirler. Haberin zamanında verilebilmesi için ilgili numara, tüm şirket telefon santralı memurlarının ve danışma görevlilerinin önlerinde asılı olmalı ya da rahat ulaşabilecekleri bir yerde durmalıdır.

Şirket çapında bir erken uyarı sistemi, sürmekte olan bir saldırıyı tespit edip karşılık vermeye büyük ölçüde yardımcı olabilir. Yazılı tüzükler uyarınca, olay bildirme merkezi görevlileri, personelin dikkatli olması için bir saldırının söz konusu olduğu doğrultusunda hemen hedeflenen gruplara uyarı gönderirler. Uyarının zamanında yapılabilmesi için merkez numarasının şirket bünyesinde herkese dağıtılmış olması gerekir.

4-7 Hassas alanlar kapatılmalıdır

Kural: Bir güvenlik görevlisi hassas ya da güvenli alanları gözetim altında tutacak ve bu alanlara giriş iki kademeli tanıtım gerektirecektir.

Açıklamalar/Notlar: Kabul edilebilir tanıtım şekillerinden biri çalışanın kartını geçirip bir erişim şifresi girmesinin istendiği dijital elektronik kilittir. Hassas bölgeleri güvenlik altına almanın en emin yolu, kapıya kartlı girişi gözetleyecek bir güvenlik görevlisi yerleştirmektir. Bunun çok maliyetli olduğu kuruluşlarda kimlik kontrolü için iki kademeli tanıtım kullanılmalıdır. Riske ve maliyete göre biyometrik özellikli bir giriş kartı da önerilir.

4-8 Ağ ve telefon kutuları

Kural: Ağ kabloları, telefon kabloları ya da ağ erişim noktaları bulunan kutular, dolaplar ya da odalar her zaman kapalı tutulmalıdır.

Açıklamalar/Notlar: Yalnızca yetkili personelin telefon ve ağ kutularına, odalara ve dolaplara erişimine izin verilmelidir. Dışarıdan gelen onarım görevlileri ya da satıcı firma sorumlularının kimlikleri bilgi güvenliğinden sorumlu bölümün çıkardığı süreçler kullanılarak, kuşku bırakmayacak biçimde kontrol edilmelidirler. Telefon hatlarına, ağ bağlantı noktalarına, düğmelere, köprülere ya da diğer ilgili cihazlara erişim olması, bilgisayar ve ağ güvenliğini kırmak isteyen bir saldırgan tarafından kullanılabilir.

4-9 Şirket içi posta kutuları

Kural: Şirket içi posta kutuları herkese açık yerlere konmamalıdır.

Açıklamalar/Notlar: Şirket içi posta alım noktalarına erişimi olan sanayi casusları ya da bilgisayar kırıcıları, çalışanları gizli bilgi vermeye ya da saldırgana yardımcı olacak bir işlem yapmaya yetkilendiren sahte yetki mektuplarını ya da dahili formları rahatlıkla gönderebilirler. Ayrıca saldırgan, içinde bir yazılım güncellemesi yükleme ya da saldırganın amaçları doğrultusunda yerleştirilmiş makrolar içeren bir dosyayı açma

talimatları içeren elektronik ortamlar gönderebilir. Şirket içi postayla gelen herhangi bir paketin, doğal olarak, alıcılar tarafından güvenilir olduğu varsayılır.

4-10 Şirket bülten panosu

Kural: Şirket çalışanları yararına olan bülten panoları dışarıdan gelenlerin erişebileceği yerlere asılmamalıdırlar.

Açıklamalar/Notlar: Pek çok işletmede, herkesin okuyabilmesi için şirkete ya da çalışana ait özel bilgilerin asıldığı bülten panoları bulunur. Çalışan haberleri, çalışan listeleri, dahili mektuplar, ilanlarda adı geçen çalışanların ev telefon numaraları ve diğer benzeri bilgiler panoya asılırlar.

Bülten panoları, ziyaretçilerin giremeyeceği şirket kafeteryalarının yakınlarına, sigara ve kahve molası köşelerine yerleştirilebilir. Bu tarz bilgiler ziyaretçilerin ya da gelip geçenlerin ulaşabileceği yerlerde bulunmamalıdır.

4-11 Bilgisayar merkezi girişi

Kural: Bilgisayar odası ya da veri merkezi her zaman kilitli tutulmalı ve çalışanların içeri girerken kimlik göstermeleri zorunlu olmalıdır.

Açıklamalar/Notlar: Şirket güvenliği, tüm girişlerin elektronik olarak kayıtlarının tutulabilmesi ve denetlenebilmesi için elektronik kart ya da kart okuyucu kullanma seçeneğini de değerlendirmelidir.

4-12 Hizmet sağlayıcılardaki müşteri hesapları

Kural: Şirkete önemli hizmetler sağlayan satıcılara sipariş veren şirket çalışanları yetkisiz kişilerin şirket adına sipariş vermelerini önlemek için parolalı bir hesap açmalıdırlar.

Açıklamalar/Notlar: Siparişle çalışan şirketler ve pek çok başka firma, müşterilerinin parola koymalarına izin verirler. Şirket ise işe uygun hizmet alabilmek için tüm satıcılarında parola oluşturmalıdır. Bu kural özellikle telekomünikasyon ve internet hizmetleri için önemlidir. Kritik hizmetlerin etkilendiği durumlarda, arayanın sipariş vermek için yetkili olup olmadığını kontrol etmek için ortak bir bilgi kullanılması şarttır. Sosyal güvenlik numarası, şirket vergi numarası, annenin kızlık soyadı ya da benzeri tanımlayıcı bilgilerin kullanılmaması gerektiği de unutulmamalıdır.

Bir toplum mühendisi, örneğin telefon şirketini arayıp modem hatlarına yönlendirme eklenmesi için talimat verebilir ya da kullanıcılar ana bilgisayarı arattırdıklarında sahte bir IP numarası vermek için çeviri bilgilerinin değiştirilmesini İnternet Hizmet Sağlayıcısı'ndan isteyebilir.

4-13 Bölüm bağlantı sorumlusu

Kural: Şirketiniz, her bölümden ya da iş grubundan bir kişiye bağlantı kurulacak kişi sorumluluğunu verdiği bir program tesis edebilir. Böylece herhangi bir çalışan, o bölümden olduğunu iddia eden bilinmeyen kişilerin gerçekliğini kolaylıkla doğrulayabilir. Örneğin, yardım masası destek isteyen bir çalışanın kimliğini onaylatmak için ilgili bölümün bağlantı kişisini arayabilir.

Açıklamalar/Notlar: Kimliğin bu yöntemle tespiti, bu tarz çalışanlar parolaları yenilemek ya da bilgisayar hesabıyla ilişkili konularda destek almak istediğinde kendi bölümünden diğer çalışanlara kefil olacak çalışan sayısını da azaltır.

Toplum mühendisliği saldırılarının başarılı olmalarının bir nedeni de teknik destek çalışanlarının yeterli zamanlarının olmaması ve istek sahibinin kimlik tespitini doğru bir yöntemle yapmamalarıdır. Bağlantı kişisinin kefil olması, teknik destek ekibinin onay amacıyla şahsen görüşmeleri gereken kişi sayısını azaltır.

4-14 Müşteri parolaları

Kural: Müşteri hizmet temsilcilerinin müşteri hesap parolalarını alma yetkileri olmayacaktır.

Açıklamalar/Notlar: Toplum mühendisleri sık sık müşteri hizmetlerini arayıp parola ya da Sosyal Güvenlik Numarası gibi müşteri tanımlama bilgilerini elde etmeye çalışırlar. Bir toplum mühendisi bu bilgiyi kullanarak başka bir müşteri temsilcisini arayıp, müşteri gibi davranıp bilgi elde etmeye ya da sahte siparişler vermeye çalışabilir.

Bu denemelerin başarıya ulaşmasını engellemek için müşteri hizmet yazılımı yalnızca arayanın verdiği tanımlama bilgilerinin girilebileceği şekilde tasarlanmalıdır ve temsilci, sistemden sadece parolanın doğru olup olmadığını söyleyen bir mesaj almalıdır.

4-15 Açıklık testleri

Kural: Güvenlik bilinçlendirme ve çalışan intibak eğitimleri sırasında güvenlik açıklarını test etmek için şirketin toplum mühendisliği taktikleri kullanacağını bildirilmesi gerekmektedir.

Açıklamalar/Notlar: Toplum mühendisliği delme testleri önceden bildirilmeden yapılırsa diğer çalışanların ya da testi yapan şirket elemanlarının kendilerine karşı aldatıcı taktikler kullanması nedeniyle şirket çalışanlarında öfke, utanma ya da başka duygusal sarsıntılar oluşabilir.

4-16 Şirket Gizli bilgilerinin gösterilmesi

Kural: Halka açıklanması düşünülmeyen şirket bilgileri herkesin görebileceği yerlere asılmamalıdır.

Açıklamalar/Notlar: Gizli ürün ya da süreç bilgilerine ek olarak, dahili telefon numaraları veya çalışan listeleri gibi listeler ya da her bölümün yöneticilerinin listesini içeren bina görev çizelgeleri gibi dahili iletişim bilgilerinin de gözlerden uzak tutulmaları gerekmektedir.

4-17 Güvenlik bilinçlendirme eğitimi

Kural: Şirketin tüm çalışanları, çalışan intibak eğitimleri sırasında bir güvenlik bilinçlendirme eğitimini de tamamlamalıdırlar. Dahası, her çalışan, on iki ayı geçmemek koşuluyla güvenlik eğitimlerini yürüten bölümün belirlediği düzenli aralıklarla güvenlik bilincini tazeleme eğitimleri almalıdır.

Açıklamalar/Notlar: Pek çok kuruluş uç kullanıcı bilinçlendirme eğitimini tamamen göz ardı eder. 2001 Küresel Bilgi Güvenliği Araştırması'na göre, araştırmaya katılan kuruluşların yalnızca yüzde 30'u kullanıcılara yönelik bilinçlendirme eğitimlerine para ayırmaktadır. Bilinçlendirme eğitimi toplum mühendisliği teknikleri kullanılarak başarıya ulaşabilen güvenlik ihlallerinin sayısını azaltmaya yönelik önemli bir gerekliliktir.

4-18 Bilgisayar erişimi için güvenlik eğitimi dersleri

Kural: Çalışanlar herhangi bir şirkette, bilgisayar sistemine erişim hakkı elde etmeden önce bilgi güvenliği derslerini başarıyla tamamlamış olmalıdırlar.

Açıklamalar/Notlar: Toplum mühendisleri sık sık yeni işe girenleri hedef alırlar ve onların gurup olarak şirketin güvenlik kurallarını, veri sınıflandırma ve hassas bilgilerin kullanımına yönelik doğru süreçleri bilme olasılıklarının düşük olduğunu bilirler.

Eğitim, çalışanların güvenlik kurallarıyla ilgili olarak sorular sormalarına da olanak tanımalıdır. Eğitimin ardından hesap sahibinin güvenlik kurallarını anladığını ve kurallara uyacağını taahhüt eden bir belge imzalaması zorunlu olmalıdır.

4-19 Çalışan kartı renkli baskılı olmalıdır

Kural: Kimlik kartları, kart sahibinin çalışan, taşeron, geçici satıcı, danışman, ziyaretçi ya da stajyer olduğunu gösterecek şekilde renklendirilmiş olmalıdır.

Açıklamalar/Notlar: Kart rengi, kişinin konumunu uzaktan anlamak için çok iyi bir yoldur. Diğer bir seçenek ise kart sahibinin konumunu belirtmek için iri harfler kullanılmasıdır, ancak renkli bir tasarım olması hataya mahal vermez ve görmesi daha kolaydır.

Binanın içine girebilmek için toplum mühendislerinin sıkça kullandıkları bir yöntem de kurye ya da tamirci kılığına girmektir. İçeri girebildikten sonra saldırgan başka bir çalışan olarak davranabilir ya da hiçbir şeyin farkında olmayan çalışanların işbirliğini elde etmek için unva-

nıyla ilgili yalan söyleyebilir. Örneğin, binaya telefon tamircisi olarak giren bir kişi bir çalışan gibi davranamaz, çünkü kartının rengi onu ele verir.

Bilgi İşlem Teknolojileri Kuralları

Herhangi bir şirketin bilgi işlem teknolojileri bölümü kuruluşun bilgi varlıklarını korumada yardımcı olması için kurallara özel bir gereksinim duymaktadır. Bir kuruluştaki Bilgi İşlem Merkezinin özgün yapısını yansıtabilmek amacıyla, Bilgi İşlem yönergelerini Genel, Yardım Masası, Bilgisayar Yönetimi ve Bilgisayar İşlemleri olarak böldüm.

Genel

5-1 Bilgi İşlem bölümü çalışan iletişim bilgileri

Kural: Bilgi İşlem bölümü çalışanlarının telefon numaraları ve e-posta adresleri, bilme gereği olmayan herhangi birine verilmemelidir.

Açıklamalar/Notlar: Bu kuralın amacı, iletişim bilgilerinin toplum mühendisleri tarafından ele geçirilmesini engellemektir. Bilgi İşlem için yanızca genel bir iletişim numarası ya da e-posta adresi verilerek dışarıdan arayanların Bilgi İşlem bölümü çalışanlarına doğrudan ulaşması engellenecektir. Site yöneticisinin ve teknik hizmetlerin e-posta adresi yalnızca admin@companyname.com gibi genel adlardan oluşmalıdır. Verilen telefon numaraları bireysel çalışanlara değil, bölümün sesli mesaj kutusuna bağlanmalıdırlar.

Doğrudan iletişim bilgileri herkese açık olduğu zaman bir bilgisayar korsanının belirli Bilgi İşlem çalışanlarına ulaşması ve bir saldırıda kullanılabilecek bilgileri ya da Bilgi İşlem çalışanı gibi davranmak amacıyla adlarını ve iletişim bilgilerini vermeleri için onları kandırması kolaylaşacaktır.

5-2 Teknik destek talepleri

Kural: Tüm teknik destek talepleri bu tarz talepleri değerlendiren gruba yönlendirilmelidir.

Açıklamalar/Notlar: Toplum mühendisleri, genel olarak teknik destek konularıyla ilgilenmeyen ve bu tarz isteklere yanıt verebilmek için uygun güvenlik süreçlerinin farkında olmayan Bilgi İşlem çalışanlarını aramayı deneyebilirler. Buna göre Bilgi İşlem çalışanları bu istekleri geri çevirmek ve arayanı destek vermekle yükümlü gruba yönlendirmek üzere eğitilmelidirler.

Yardım Masası

6-1 Uzaktan erişim süreçleri

Kural: Yardım masası çalışanları, harici ağ erişim noktaları ya da

bağlantı numaraları da aralarında olmak üzere uzaktan erişimle ilgili bilgileri ve ayrıntıları açıklamamalıdırlar. Ancak, istek sahibi aşağıdaki koşullardan birine uyuyorsa durum değişebilir:

- Dahili bilgi alabileceğine dair yetkili olduğunun onaylanmış olması.
- Harici bir kullanıcı olarak şirket ağına bağlanmaya yetkili olduğunun onaylanmış olması. Kişi şahsen tanınmadığı sürece bu bölümde anlatılan Onay ve Yetkilendirme Süreçlerine uygun olarak istek sahibinin kimlik tespiti kuşku bırakmayacak şekilde yapılmalıdır.

Açıklamalar/Notlar: Hem işleri bilgisayarla ilgili konularda kullanıcılara destek vermek olduğu, hem de arttırılmış sistem yetkileri olduğu için şirket yardım masası sık sık toplum mühendisinin başlıca hedefi olur. Tüm yardım masası çalışanları, şirket kaynaklarına yetkisiz kişilerin ulaşmasına yol açabilecek yetkisiz bilgi aktarımlarını engelleyen bir insan güvenlik duvarı olacak şekilde yetiştirilmelidirler. En basit kural, kimlik tespitinin sonucu olumlu çıkmadan hiçbir zaman uzaktan erişim süreçlerini kimseye açıklamamaktır.

6-2 Parolaları ilk duruma döndürmek

Kural: Bir kullanıcı hesabına ait parola yalnızca hesap sahibinin isteği doğrultusunda yenilenebilir.

Açıklamalar/Notlar: Toplum mühendisleri tarafından en sık oynanan oyun, başka birinin hesabının parolasını ilk duruma döndürtmek ya da değiştirtmektir. Saldırgan, parolasını unutmuş ya da kaybetmiş bir çalışan gibi davranır. Bu tarz bir saldırının başarı şansını azaltabilmek için, parolayı ilk durumuna döndürmeye yönelik bir talep geldiğinde Bilgi İşlem çalışanı herhangi bir işlem yapmadan önce talebi veren çalışanı geri aramalıdır ve bu arama için çalışan telefon rehberindeki numarayı kullanmalıdır. Bu süreçle ilgili olarak Onay ve Yetkilendirme Süreçlerine bakınız.

6-3 Yetkilerin değişimi

Kural: Bir kullanıcının yetkilerini ya da erişim haklarını artırmaya yönelik tüm talepler hesap sahibinin yöneticisi tarafından yazılı olarak onaylanmış olmalıdır. Ayrıca bu tarz taleplerin Onay ve Yetkilendirme Süreçlerine uygun olarak geçerlilikleri onaylanmalıdır.

Açıklamalar/Notlar: Bir bilgisayar korsanı standart bir kullanıcı hesabına girdikten sonra bir sonraki adım saldırganın tüm sistem üzerinde tam kontrol sağlaması için yetkilerini artırması olur. Yetkilendirme süreciyle ilgili bilgisi olan bir saldırgan e-postayla, faksla ya da telefonla, yetkili gibi görünen bir talepte bulunabilir. Örneğin, saldırgan teknik destek ya da yardım masasını arayıp girebildiği hesaba ek erişim hak-

ları alabilmek için bir teknisyeni ikna etmeye çalışabilir.

6-4 Yeni hesap yetkisi

Kural: Çalışanlar, taşeronlar ya da diğer yetkili kişilerin kullanımı için açılacak yeni hesap talepleri çalışanın yöneticisi tarafından imzalanmış yazılı bir belgeyle ya da dijital olarak imzalanmış elektronik postayla yapılmalıdır. Bu istekler şirket içi posta aracılığıyla teyit edilmelidir.

Açıklamalar/Notlar: Parolalar ve diğer bilgiler bilgisayar sistemlerine girmek için faydalı olduklarından, bilgi hırsızlarının erişim sağlamada kullandıkları en öncelikli hedeflerdir ve özel önlemler alınması şarttır. Bu kuralın amacı bilgisayar kırıcılarının yetkili personel gibi davranmasını ya da yeni hesap taleplerinin sahtesini oluşturmasını önlemek içindir. Bu nedenle tüm bu tarz istekler Onay ve Yetkilendirme Süreçleri kullanılarak şüphe kalmayacak biçimde onaylanmalıdırlar.

6-5 Yeni parolaların teslimi

Kural: Yeni parolalar şirket gizli bilgileri olarak ele alınmalı ve şahsen, taahhütlü posta gibi imzalı teslimatla ya da güvenilir kargo şirketleri gibi güvenli yöntemler kullanarak teslim edilmelidirler (bkz. gizli bilgilerin dağıtımı ile ilgili kurallar).

Açıklamalar/Notlar: Şirket içi posta da kullanılabilir, ancak parolaların, içeriğini göstermeyen güvenli zarflarda gönderilmesi gerekir. Önerilen bir yöntem de her bölümden bir bilgisayar iletişim sorumlusu belirlemektir. Bu kişi yeni hesap ayrıntılarının dağıtımından ve parolalarını kaybeden ya da unutan çalışanlara kefil olmaktan sorumludur. Bu durumda, destek personeli her zaman şahsen tanıdığı küçük bir gurupla birlikte çalışıyor olacaktır.

6-6 Bir hesabın kapatılması

Kural: Bir kullanıcı hesabını kapatmadan önce talebin yetkili birinden geldiğinin doğrulanması gerekmektedir.

Açıklamalar/Notlar: Bu kuralın amacı, saldırganın bir hesabın kapatılmasını isteyip sonra da kullanıcının bilgisayar sistemine erişememesi sorununu çözmeye çalışıyor numarası yapması engellemek içindir. Toplum mühendisi kullanıcının sisteme girememesiyle ilgili önceden bilgisi olan bir teknisyen gibi davranarak kurbanı aradığında, kurban, yapılan kontroller sırasında parolası istendiğinde çoğu zaman bu bilgiyi verir.

6-7 Ağ bağlantı noktalarının ve araçlarının devre dışı bırakılması

Kural: Hiçbir çalışan kim olduğunu bilmedikleri bir teknik destek çalışanı için herhangi bir ağ aracını ya da bağlantı noktasını kapatmamalıdır.

Açıklamalar/Notlar: Bu kuralın amacı, bir saldırganın bir ağ bağlantısının kapatılmasını isteyip sonra da ağa erişim sorununu çözmek için çalışanı aramasını engellemektir. Yardımsever bir teknisyen kılığındaki toplum mühendisi, kullanıcının ağ sorununa ilişkin ön bilgisi varmış gibi davrandığında, kurban, yapılan kontroller sırasında parolası istendiğinde çoğu zaman bu bilgiyi verir.

6-8 Telsiz erişimi süreçlerinin açıklanması

Kural: Hiçbir çalışan telsiz ağına bağlanmaya yetkili olmayan kimselere telsiz ağı üzerinden şirket ağına bağlanma süreçlerini açıklamamalıdır.

Açıklamalar/Notlar: Telsiz erişim bilgilerini açıklamadan önce kişinin harici kullanıcı olarak şirket ağına bağlanmaya yetkili olup olmadığı her zaman önceden kontrol edilmelidir (bkz. Onay ve Yetkilendirme Süreçleri).

6-9 Kullanıcı gizliliği

Kural: Bilgisayarla ilgili sorun olduğunu bildiren çalışanların adları bilgi işlem bölümü dışından kimseye açıklanmamalıdır.

Açıklamalar/Notlar: Sıradan bir saldırıda toplum mühendisi yardım masasını arar ve yakın zamanda bilgisayarlarında sorun olduğunu bildiren çalışanların adlarını ister. Arayan çalışan, taşeron ya da telefon şirketi elemanı gibi davranabilir. Sorun olduğunu söyleyen kişilerin adlarını aldıktan sonra toplum mühendisi yardım masası ya da teknik destek personeli gibi davranır ve çalışanı arayarak sorunu çözmek için aradığını söyler. Arama sırasında saldırgan, kurbanı istediği bilgileri vermesi ya da saldırganı hedefine götürecek bir işlem yapması için kandırır.

6-10 Komut girmek ya da program çalıştırmak

Kural: Bilgi İşlem bölümünde ayrıcalıklı hesapları olan çalışanlar, şahsen tanımadıkları birinin isteği üzerine herhangi bir komut ya da progam çalıştırmamalıdırlar.

Açıklamalar/Notlar: Saldırganların bir Truva Atı ya da başka bir kötü huylu yazılım yüklemek için sıkça kullandıkları bir yöntem de var olan bir programın adını değiştirmek ve sonra da yardım masasını arayarak programı çalıştırmaya uğraşırken hata mesajı verdiğini söylemektir. Saldırgan, yardım masası teknisyenini programı çalıştırmaya ikna eder. Teknisyen programı çalıştırdığında kötü huylu yazılım çalıştıran kullanıcının yetkilerini görür ve saldırgana aynı yetkileri verdiği bir işlem gerçekleştirir. Bu, saldırganın şirket sistemini ele geçirmesini sağlar.

Bu kural destek personelinin bir isteğe bağlı olarak herhangi bir programı çalıştırmadan önce çalışan konumunun doğrulanmasını zorunlu tutarak yukarıda bahsedilen taktiğe karşı bir önlem getirmektedir.

Bilgisayar İdaresi

7-1 Genel erişim haklarının değiştirilmesi

Kural: Bir elektronik iş profiliyle ilgili genel erişim haklarını değiştirme talebi şirket ağında erişim haklarını yöneten gurup tarafından onaylanmalıdır.

Açıklamalar/Notlar: Yetkililer her değişim talebinin bilgi güvenliği için bir tehdit unsuru oluşturup oluşturmadığını değerlendireceklerdir. Eğer oluşturuyorsa, sorumlu kişi istek sahibini gerekli konularda uyaracak ve yapılacak değişiklikler konusunda ortak bir karara varacaklardır.

7-2 Uzaktan erişim talepleri

Kural: Uzaktan bilgisayar erişimi yalnızca şirket dışı noktalardan bilgisayar sistemlerine girme gerekliliği olduğunu gösteren çalışanlara verilecektir.

Açıklamalar/Notlar: Yetkili personel tarafından şirket ağına dışarıdan bağlanma ihtiyacına göre bu tarz erişimin yalnızca gerek duyanlara verilecek şekilde sınırlandırılması uzaktan erişimli kullanıcıların yönetimini ve oluşan riski büyük ölçüde azaltacaktır. Dışarıdan bağlanma yetkileri olan kişilerin sayısı ne kadar az olursa saldırganın hedef seçenekleri de o kadar az olacaktır. Saldırganın şirket ağına girmek için bağlantılarını çalmak ya da onların kimliğine bürünmek niyetiyle uzak kullanıcıları hedefleyebileceğini hiçbir zaman unutmayınız.

7-3 Ayrıcalıklı hesap parolalarının ilk duruma getirilmesi

Kural: Yetkili bir hesaba ait parolanın ilk durumuna getirilmesi talebi, hesabın bulunduğu bilgisayardan sorumlu sistem yöneticisi tarafından onaylanmalıdır. Yeni parola, şirket içi postayla gönderilmeli ya da şahsen iletilmelidir.

Açıklamalar/Notlar: Ayrıcalıklı hesapların tüm sistem kaynaklarına ve bilgisayar sistemindeki dosyalara erişimi vardır. Doğal olarak bu hesaplarda mümkün olan en güçlü koruma kullanılmalıdır.

7-4 Dışarıdan gelen destek personelinin uzaktan erişimi

Kural: Hiçbir dışarıdan destek personeline (yazılım ya da donanım satan firmadan gelen personel gibi) ilgili hizmetleri vermeye yetkili olup olmadıkları kontrol edilmeden ve kimlik tespiti yapılmadan şirket bilgisayar sistemlerine ya da ilgili araçlara uzaktan erişme hakkı ya da bilgisi verilmemelidir. Eğer destek hizmeti vermek üzere satıcı firma yetkili erişim talep ediyorsa, verilen hizmet sona erdiğinde satıcı firmanın kullandığı hesabın parolası zaman kaybetmeden değiştirilmelidir.

Açıklamalar/Notlar: Bilgisayar korsanları şirket bilgisayar ya da telekomünikasyon ağına girebilmek için satıcıymış gibi davranabilirler. Bu nedenle sistemde herhangi bir iş gerçekleştirme yetkilerinin yanısıra satıcının kimliğinin de onaylanması önemlidir. Ayrıca iş bittiğinde satıcının kullandığı hesap parolası değiştirilerek sistem kapıları kapatılmalıdır.

Hiçbir satıcı firmanın geçici olarak bile herhangi bir hesap için kendi istediği parolayı kullanmasına izin verilmemelidir. Bazı satıcıların farklı bilgisayar sistemlerinde aynı ya da benzer parolaları kullandıkları bilinmektedir. Örneğin, bir ağ güvenlik şirketi tüm müşteri bilgisayar sistemlerindeki hesaplarına aynı parola ile erişmektedir ve üstüne üstlük dışarıya Telnet erişimine de izin verilmiştir.

7-5 Şirket sistemlerine uzaktan erişim için güçlü tanımlama

Kural: Şirket ağına uzaktan erişim için kullanılan tüm bağlantı noktaları değişken parolalar ya da biyometrikler gibi güçlü tanımlama araçlarıyla korunmalıdırlar.

Açıklamalar/Notlar: Pek çok işletme, uzak kullanıcıları tanımlamanın tek yolu olarak sabit parolalara güvenirler. Bu uygulama sakıncalıdır çünkü güvensizdir. Bilgisayar korsanları kurbanın ağında olası en zayıf bağlantıyı oluşturabilecek uzaktan erişim noktasını hedeflerler. Başka birinin parolanızı öğrenip öğrenmediğini hiçbir zaman bilemezsiniz.

Bu nedenle uzaktan erişim noktaları, zaman tabanlı anahtarlar, akıllı kartlar ya da biyometrik araçlar gibi güçlü tanımlama araçlarıyla korunmalıdır, böylece araya girerek alınmış parolaların saldırgan için hiçbir değeri olmaz.

Değişken parolalara dayalı tanımlamalar kullanışsız olduklarından, bilgisayar kullanıcıları, tahmin edilmesi zor parola seçme kuralına sadakatle uymalıdırlar.

7-6 İşletim sistemi ayarları

Kural: Sistem yöneticileri mümkün olan her noktada işletim sistemlerinin tüm geçerli güvenlik kural ve süreçleriyle tutarlı bir şekilde ayarlanmış olduğundan emin olmalıdırlar.

Açıklamalar/Notlar: Güvenlik kurallarını hazırlamak ve dağıtmak tehlikeyi azaltmaya yönelik önemli bir adımdır ama çoğu durumda uyup uymamak ister istemez bireysel çalışana kalmıştır. Ancak bilgisayarla ilgili birçok kural, parolaların sahip olması gereken uzunluk gibi, işletim sistemi ayarları sayesinde zorunlu duruma getirilebilir. Güvenlik kurallarını işletim sistemi özelliklerini ayarlayarak otomatikleştirmek, kararları etkili bir şekilde insan unsurunun elinden alıp kuruluşun genel güvenliğini artırmaktadır.

7-7 Zorunlu süre aşımı

Kural: Tüm bilgisayar hesapları bir yıl içerisinde kapanmaya ayarlanmalıdır.

Açıklamalar/Notlar: Bu kuralın amacı, bilgisayar korsanları sık sık, kullanılmayan hesapları hedeflediklèri için, artık kullanılmayan bilgisayar hesaplarını ortadan kaldırmaktır. Bu süreç eski çalışanlara ya da taşeronlara ait ve kazara olduğu gibi bırakılmış herhangi bir bilgisayar hesabının otomatik olarak kaldırılacağını garantiler.

Yönetimin takdirine bağlı olarak yenileme zamanında çalışanların güvenlik tazeleme eğitimi almaları ya da bilgi güvenlik kurallarını gözden geçirip bunlara uyacaklarına dair bir taahhütname imzalamaları zorunlu tutulabilir.

7-8 Genel e-posta adresleri

Kural: Bilgi İşlem bölümü dışarıyla sürekli iletişimi olan her bölüm için genel bir e-posta adresi oluşturacaktır.

Açıklamalar/Notlar: Genel e-posta adresi santral memurları tarafından ya da şirketin internet sitesi aracılığıyla dışarıya verilebilir. Böylece her çalışan kendi şahsi e-posta adresini yalnızca bilmesi gereken kişilere verecektir.

Bir toplum mühendisliği saldırısının ilk aşamasında saldırgan genellikle çalışanların telefon numaralarını, adlarını ve unvanlarını öğrenmeye çalışır. Çoğu zaman bu bilgi şirket internet sitesinde bulunabilir ya da istendiğinde herkese verilebilir. Genel sesli mesaj kutularının ve/veya e-posta adreslerinin yaratılması çalışan adlarının belirli bölümler ya da sorumluluklarla bağdaştırılmasını zorlaştırmaktadır.

7-9 Alan tescilleri için iletişim bilgileri

Kural: İnternet adres alanları ya da alan adları almak için kayıt olurken sağlanan iletişim bilgileri idari, teknik ya da diğer çalışanların bireysel olarak adlarını vermemelidir. Onun yerine oraya genel bir e-posta adresi ve ana şirket telefon numarası girilmelidir.

Açıklamalar/Notlar: Bu kuralın amacı iletişim bilgilerinin bilgisayar korsanları tarafından kötüye kullanılmasını önlemektir. Bireylerin adları ve telefon numaraları verildiğinde bir saldırgan bu bilgileri kullanarak kişilerle bağlantı kurabilir ve onları sistem bilgileri vermeleri ya da saldırganın amacına uyan bir işlem yapmaları doğrultusunda kandırabilir. Toplum mühendisi diğer şirket çalışanlarını kandırabilmek için adı geçen çalışanlardan biri gibi davranabilir.

Belirli bir çalışanın e-posta adresi yerine, iletişim bilgisi administrator@company.com şeklinde olmalıdır. Telekomünikasyon bölümü çalışanları, idari ve teknik iletişim için genel bir sesli mesaj kutusu oluştura-

rak bir toplum mühendisliği saldırısında işe yarayabilecek bilgilerin gizliliğini korumuş olurlar.

7-10 Güvenlik ve işletim sistemi güncellemelerinin yüklenmesi

Kural: İşletim sistemi ve uygulama yazılımlarına yönelik tüm güvenlik yamaları, çıktıkları zaman en kısa sürede yüklenmelidirler. Eğer bu kural görev-kritik üretim sistemlerinin işleyişiyle çatışıyorsa bu tarz güncellemeler uygun oldukları zaman yapılmalıdırlar.

Açıklamalar/Notlar: Bir açık görüldüğünde bir yamanın ya da geçici bir çözümün var olup olmadığını öğrenmek için yazılım üreticisi zaman kaybetmeden aranmalıdır. Yamalanmamış bir bilgisayar sistemi kuruma en büyük güvenlik tehditlerinden birini oluşturur. Sistem yöneticileri gerekli çözümleri uygulamayı geciktirirlerse pencere o kadar açılır ki saldırgan tırmanıp içeri girebilir.

Bulunan düzinelerce güvenlik açığı haftalık olarak internette yayınlanmaktadır. Bilgi işlem çalışanları mümkün olan en kısa sürede güvenlik yamalarını ve çözümlerini yükleme çabaları konusunda uyanık davranana kadar, şirket ağı hep bir güvenlik ihlali yaşama tehlikesiyle karşı karşıya kalacaktır. İşletmede kullanılan uygulama programları ve işletim sisteminin zayıflıklarıyla ilgili yapılan açıklamalardan haberdar olmak oldukça önemlidir.

7-11 İnternet sayfalarındaki iletişim bilgileri

Kural: Şirketin harici internet sayfası, şirket yapısı ile ilgili hiçbir bilgi vermemeli ya da çalişanları isim isim göstermemelidir.

Açıklamalar/Notlar: Kuruluş şemaları, hiyerarşi şemaları, çalışan ya da bölüm listeleri, raporlama yapısı, adlar, unvanlar, dahili telefon numaraları, çalışan numaraları ya da şirket yapısına yönelik benzeri bilgiler internet sayfalarında genel erişime açık olmamalıdırlar.

Bilgisayar korsanları, yararlı bilgileri sık sık hedefin internet sayfasından bulurlar. Saldırgan, çevirdiği bir dolapta konuya hakim bir çalışan gibi görünmek için bu bilgiyi kullanır. Elinde bu bilgi varken toplum mühendisinin inandırıcı olma olasılığı daha fazladır. Dahası, saldırgan, bu bilgiyi inceleyerek değerli, hassas ya da önemli bilgilere erişimi olabilecek hedefleri bulabilir.

7-12 Ayrıcalıklı hesapların oluşturulması

Kural: Sistem yöneticisi tarafından onaylanmadığı sürece hiçbir ayrıcalıklı hesap açılmamalı ya da herhangi bir hesabın sistem yetkileri artırılmamalıdır.

Açıklamalar/Notlar: Bilgisayar korsanları sık sık donanım ya da yazılım satıcısı firma yetkilisi gibi davranarak teknik personeli onaylanma-

mış hesaplar açmaları doğrultusunda kandırmaya çalışabilirler. Bu kuralın amacı, ayrıcalıklı hesapların oluşurulması üzerine daha büyük bir denetim getirerek bu saldırıları engellemektir. Yüksek yetkilerle donatılmış bir hesap açma talebini sistem yöneticisi onaylamış olmalıdır.

7-13 Misafir hesapları

Kural: Herhangi bir bilgisayar sisteminde ya da ilgili ağ araçlarında bulunan misafir hesapları, yönetimin onayladığı adsız erişimli FTP (dosya aktarım protokolu) sunucusu hariç, devre dışı bırakılmalı ya da kaldırılmalıdır.

Açıklamalar/Notlar: Misafir hesabın amacı kendilerine ait bir hesap açılmasına gerek olmayan kişilere geçici erişim sağlamaktır. Pek çok işletim sistemi misafir hesaplar açılmış olarak gelir. Misafir hesaplar her zaman devre dışı bırakılmalıdır, çünkü varlıkları kullanıcı sorumluluğu ilkesine aykırıdır. Bilgi İşlem tüm bilgisayarlardaki faaliyeti denetleyebilmeli ve onları belirli bir kullanıcıyla bağdaştırabilmelidir.

Toplum mühendisleri ya doğrudan kullanıp ya da yetkili personeli bir misafir hesabı kullanmaya ikna edip yetkisiz erişim sağlamak için misafir hesaplarından kolaylıkla yararlanırlar.

7-14 Şirket dışında tutulan yedeklerin şifrelenmesi

Kural: Şirket dışında tutulan herhangi bir veri yetkisiz erişimi engellemek için şifrelenmelidir.

Açıklamalar/Kurallar: Herhangi bir bilginin yeniden yerine koyulması gerektiği durumlarda sorumlular tüm bilgilerin geri getirilebileceğinden emin olmalıdırlar. Bu da, verilerin geri getirilebileceğinden emin olmak için düzenli olarak şifreli dosyalardan rastgele bir örnekleme deneme deşifrelemesi yapılmasını gerektirir. Ayrıca verileri şifrelemek için kullanılan anahtar kaybolma ya da bulunamama olasılığına karşı güvenilir bir yöneticiye emanet edilmelidir.

7-15 Ağ bağlantılarına ziyaretçi erişimi

Kural: Herkese açık tüm ethernet erişim noktaları dahili ağa yetkisiz ulaşımı engellemek için parçalı ağda (segmented network) bulundurulmalıdır.

Açıklamalar/Notlar: Bu kuralın amacı, dışarıdan kişilerin şirket alanına girdiklerinde dahili ağa bağlanmalarını önlemektir. Konferans salonlarına, kafeteryaya, eğitim merkezlerine ya da ziyaretçilerin erişimi olabilecek başka yerlere yerleştirilen ethernet girişleri ziyaretçilerin şirket bilgisayar sistemlerine yetkisiz erişimini engellemek için filtrelenmelidir.

Ağ ya da güvenlik sorumlusu, bu noktalardan erişimi engelleyebilmek için, eğer varsa, sanal bir Yerel Ağ (LAN) anahtarı oluşturmayı seçebilir.

7-16 Bağlantı modemleri

Kural: Aramalara açık bağlantı modemleri uygun güvenlik duvarı uygulamalarıyla bağlanmalıdır.

Açıklamalar/Notlar: Savaş Oyunları (War Games) adlı filmde de anlatıldığı gibi korsanlar modem bağlı telefon hatlarını bulmak için savaş araması olarak bilinen bir teknik kullanırlar. Süreç, saldırganın şirketin bulunduğu bölgede kullanılan alan prefikslerini tanımlaması ile başlar. Bu prefiksle başlayan her numara, modem bağlı hatları bulmak için bir tarama programının da yardımıyla taranır. Modemin güvenlik duvarı uygulaması, bağlantı güvenli olarak kurulmadıkça veri trafiğine izin vermez. Süreci hızlandırmak için bu programlar bir sonraki numarayı denemeden önce modem yanıtını bir ya da iki çalış süresi kadar beklemek üzere ayarlanmışlardır. Bir şirket modem hattının otomatik yanıt seçeneğini en az dört çalış olarak ayarlarsa tarama programları modemli hatları bulamayacaklardır.

7-17 Virüs koruma yazılımları

Kural: Her bilgisayar sistemine virüs koruma yazılımlarının son sürümleri yüklenmeli ve çalıştırılmalıdır.

Açıklamalar/Notlar: Virüs koruma yazılımlarını ve şablon dosyalarını (yeni virüsleri bulmak için virüs yazılımlarına özgü şablonları tanıyan programlar) kullanıcı bilgisayarlarına kadar otomatik olarak indirememiş şirketlerde bireysel kullanıcılar, yazılımı, şirket ağına uzaktan erişmek için kullanılan bilgisayar sistemlerindekiler de dahil, kendi sistemlerine yükleme ve sürekli güncelleme sorumluluğunu almalıdırlar.

Eğer uygunsa bu yazılım virüs ve Truva Atı imzaları için her gece otomatik olarak güncellenecek şekilde ayarlanmalıdır. Şablon ya da imza dosyaları kullanıcı bilgisayarlarına kadar indirilmezse, kullanıcılar en azından haftada bir şablon dosyalarını güncelleme sorumluluğunu taşıyacaklardır.

Bu uygulamalar şirket bilgisayar sistemlerine bağlanan tüm masaüstü ve dizüstü makinalar için geçerlidir ve bilgisayarın şirkete ait ya da şahsa ait olup olmadığına göre de değişmez.

7-18 Gelen e-posta ekleri (yüksek güvenlik gereksinimi)

Kural: Yüksek güvenlik ihtiyaçları olan bir kuruluşta şirket güvenlik duvarı tüm e-posta eklerini eleyecek şekilde ayarlanmalıdır.

Açıklamalar/Notlar: Bu kural yalnızca yüksek güvenlik gereksinimleri olan ya da e-posta ekinde dosya almaya ihtiyacı olmayan işletmeler için geçerlidir.

7-19 Yazılım onayı

Kural: Tüm yeni yazılımlar, yazılım çözümleri ya da güncellemeleri,

ister fiziksel ortamda olsun, ister internet üzerinden elde edilmiş olsun yüklenmeden önce güvenilirlikleri doğrulanmalıdır. Bu kural, özellikle sistem yetkileri gerektiren yazılımlar yüklenirken bilgi işlem bölümünü ilgilendirir.

Açıklamalar/Notlar: Bu kuralda sözü edilen bilgisayar yazılımları işletim sistemi parçalarını, uygulamaları, yazılım çözümlerini, yamaları ya da herhangi bir yazılım güncellemesini içerir. Pek çok yazılım üreticisi, müşterinin dağıtımın içeriğini genellikle bir dijital imza kullanarak kontrol edebileceği yöntemler yerleştirmişlerdir. İçeriğin onaylanmadığı her durumda, yazılımın güvenilirliğini doğrulamak için üreticiye başvurulmalıdır.

Bilgisayar saldırganlarının yazılım üreticisinde yapılmış ve şirkete postalanmış gibi görünen bir paketle kurbana yazılım gönderdiği de bilinmektedir. Aldığınız her yazılımın, özellikle de talep etmediğiniz bir yazılımsa, şirket sistemine yüklemeden önce güvenilirliğini doğrulamanız önemlidir.

Becerikli bir saldırganın kurumunuzun bir üreticiden yazılım sipariş ettiğini öğrenebileceğini unutmayın. Elinde bu bilgi varken saldırgan, gerçek üreticiye verilen siparişi iptal edebilir ve siparişi kendi yerine getirebilir. O zaman yazılım, kötü huylu bir işlev gerçekleştirmek üzere değiştirilmiş olur ve şirketinize asıl paketinde, gerekirse vakumlanmış olarak gönderilir. Ürün yüklendikten sonra kontrol artık saldırganın eline geçer.

7-20 Varsayılan parolalar

Kural: Varsayılan bir parolaya sahip olan tüm işletim sistemi yazılımlarının ve donanımlarının şirket parola kuralları doğrultusunda parolaları değiştirilmelidir.

Açıklamalar/Notlar: Pek çok işletim sistemi ve bilgisayarla ilgili donanımlar varsayılan parolalarla gönderilirler; diğer bir deyişle satılan her parça aynı parolaya sahiptir. Varsayılan parolaların değiştirilmesi konusunu ihmal etmek, şirketi tehlikeye sokan ciddi bir hatadır.

Varsayılan parolalar herkesçe bilinirler ve internet sayfalarında bulunurlar. Bir saldırı sırasında saldırganın denediği ilk parola, üreticinin koyduğu varsayılan paroladır.

7-21 Başarısız erişim denemeleri sonucu kilitlenme (düşük orta düzey güvenlik)

Kural: Özellikle düşük ve orta düzey güvenlik gereksinimleri olan bir kurumda aynı hesaba birbiri ardına belirli bir sayıda girme girişimi olursa hesap bir süreliğine kilitlenmelidir.

Açıklamalar/Notlar: Tüm şirket bilgisayarları ve sunucularına birbiri ardına yapılan başarısız girme denemelerine bir sınır getirilmelidir. Bu

kural deneme yanılmayla parola tahmini, sözlük saldırısı ya da kaba kuvvetle yetkisiz erişim sağlama yöntemlerini engellemek için gereklidir.

Sistem yöneticisi güvenlik ayarlarını, peşpeşe başarısız bağlanma girişimi eşiğine gelindiğinde hesabı kilitleyecek şekilde yapmalıdır. Yedi başarısız denemeden sonra bir hesabın en az otuz dakika boyunca kilitlenmesi önerilir.

7-22 Başarısız erişim girişimleri sonucu hesabın kapatılması (yüksek güvenlik)

Kural: Yüksek güvenlik gereksinimleri olan bir kurumda aynı hesaba birbiri ardına belirli bir sayıda başarısız girme girişimi olursa hesap, desteği veren grup tarafından düzeltilene kadar kapatılmalıdır.

Açıklamalar/Notlar: Tüm şirket bilgisayarları ve sunucularına birbiri ardına yapılan başarısız girme denemelerine bir sınır getirilmelidir. Bu kural deneme yanılmayla parola tahmini, sözlük saldırısı ya da kaba kuvvetle yetkisiz erişim sağlama yöntemlerini engellemek için gereklidir.

Sistem yöneticisi, güvenlik ayarlarını, beş başarısız bağlanma girişiminden sonra hesabı kapayacak şekilde yapmalıdır. Böyle bir saldırının ardından hesap sahibinin hesabı açtırmak için teknik destek birimini ya da hesap desteğinden sorumlu grubu araması gerekir. Hesabı yeniden devreye sokmadan önce ilgili birimin Onay ve Yetkilendirme Süreçlerine uygun olarak hesap sahibi için kesinlikle bir kimlik tespiti yapması şarttır.

7-23 Ayrıcalıklı hesapların parolalarının düzenli olarak değiştirilmesi

Kural: Tüm ayrıcalıklı hesap sahiplerinin en çok otuz günde bir parolalarını değiştirmeleri zorunluluğu getirilecektir.

Açıklamalar/Notlar: İşletim sistemi sınırlamalarına bağlı olarak, sistem yöneticisi sistem yazılımının güvenlik özelliklerini ayarlayarak kullanıcıları bu kurala uymaya zorlayabilir.

7-24 Kullanıcı parolalarının düzenli olarak değişimi

Kural: Tüm hesap sahipleri en çok altmış günde bir parolalarını değiştirmelidirler.

Açıklamalar/Notlar: Bu özelliğe sahip işletim sistemleri kullanarak, sistem yöneticisi, yazılımın güvenlik özelliklerinin ayarlanmasıyla kullanıcıları bu kurala uymaya zorlayabilir.

7-25 Yeni hesap parolası oluşturmak

Kural: Yeni bilgisayar hesapları, süresi dolmuş bir parolayla oluşturulmalı, böylece hesap sahibine ilk kullanım için yeni bir parola belirleme zorunluluğu getirilmelidir.

Açıklamalar/Notlar: Bu zorunluluk kendi parolasını hesap sahibinden başka kimsenin bilmemesini sağlar.

7-26 Açılış parolaları

Kural: Tüm bilgisayar sistemleri açılışta parola isteyecek şekilde ayarlanmalıdırlar.

Açıklamalar/Notlar: Bilgisayarlar açıldıkları zaman işletim sistemi yüklenmeden önce parola soracak şekilde ayarlanmalıdırlar. Bu, yetkisiz kimselerin başka birinin bilgisayarını açıp kullanmasını engeller. Bu kural şirket içindeki tüm bilgisayarlar için geçerlidir.

7-27 Ayrıcalıklı hesaplar için parola zorunlulukları

Kural: Tüm ayrıcalıklı hesapların güçlü parolaları olmalıdır. Parola aşağıdaki özelliklere uymalıdır.

- Herhangi bir dildeki sözlüklerde bulunmamalıdır.
- Büyük ve küçük harflerden oluşmalı ve en az bir harf, bir simge ve bir sayı içermelidir.
- En az 12 karakter uzunluğunda olmalıdır.
- Şirkete ya da bireye herhangi bir nedenle verilmemelidir.

Açıklamalar/Notlar: Çoğu durumda bilgisayar korsanları sistem yetkileri elde etmek için belirli hesapları hedeflerler. Zaman zaman saldırgan, sistem üzerinde tam kontrol sağlamak için başka açıkları da sömürür.

Saldırganın deneyeceği ilk parolalar basit, sözlükte bulunan sık kullanılan kelimeler olacaktır. Güçlü parolaların seçilmesi, bir saldırganın deneme yanılma, sözlük saldırısı ya da kaba kuvvet saldırısı kullanarak parolayı bulma olasılığını azaltır ve güvenliği artırır.

7-28 Telsiz erişim noktaları

Kural: Bir telsiz ağına erişimi olan tüm kullanıcılar şirket ağlarını korumak için VPN (virtual private network - sanal özel ağ) teknolojisi kullanmalıdırlar.

Açıklamalar/Notlar: Telsiz ağlara, savaş sürüşü adı verilen yeni bir yöntemle saldırılıyor. Bu yöntem 802.11B NIC kartıyla donanmış bir dizüstü bilgisayarla telsiz ağı bulana kadar yürümek ya da arabayla dolaşmaktan ibaret.

Pek çok şirket telsiz bağlantısını şifreleyerek güvence altına alan WEP'i (wireless equivalency protokol - telsiz denklik protokolü) bile devreye sokmadan telsiz ağlarını kullanmaya başladılar. Açık olduğu zaman bile WEP'in geçerli sürümü (2002'nin ortalarında) yetersizdir. Kırılıp

ardına kadar açılmıştır ve pek çok internet sitesi açık telsiz sistemlerini bulmak için yöntemler üretmeye ve WEP özelliği açık telsiz erişim noktalarını kırmaya adanmıştır.

Bu yüzden, VPN teknolojisi kullanarak 802.11B protokolüne ek bir koruma sağlanması önemlidir.

7-29 Virüs şablon dosyalarının güncellenmesi

Kural: Her bilgisayar sistemi virüs koruma yazılımları için virüs/Truva Atı şablon dosyalarını otomatik olarak güncellemek üzere programlanmalıdır.

Açıklamalar/Notlar: Bu tarz güncellemeler en azından haftada bir yapılmalıdır. Çalışanların, bilgisayarlarını açık bıraktıkları işletmelerde şablon dosyalarının her gece güncellenmesi şiddetle önerilir.

Virüs koruma yazılımları yeni tür kötü huylu yazılımları görecek şekilde güncellenmezse etkisiz kalır. Desen dosyaları güncellenmediğinde virüs, solucan ve Truva Atı tehlikesi büyük ölçüde arttığı için virüs ya da kötü huylu yazılım koruma ürünlerinin güncel tutulması önemlidir.

Bilgisayar İşlemleri

8-1 Komut girmek ve program çalıştırmak

Kural: Bilgisayar işlemlerinden sorumlu personel, tanımadıkları birinden gelen talep üzerine komut girmemeli ve program çalıştırmamalıdır. Onaylanmamış bir kişinin istekte bulunmak için geçerli bir nedeni varmış gibi görünen durumlar ortaya çıkarsa öncelikle yöneticinin onayı alınmadan bu istek yerine getirilmemelidir.

Açıklamalar/Notlar: Bilgisayar işlemleri çalışanları, konumları gereği çoğunlukla ayrıcalıklı hesap erişimleri olduğu için toplum mühendislerinin çok kullandığı hedefler arasındadırlar ve saldırgan onların diğer Bilgi İşlem çalışanlarına göre şirket süreçleriyle ilgili olarak daha az bilgili ve daha az deneyimli olduklarını düşünür. Bu kuralın amacı, toplum mühendislerinin bilgisayar işlemleri çalışanlarını kandırmalarını önlemek amacıyla uygun bir kontrol ve denge unsuru oluşturmaktır.

8-2 Ayrıcalıklı hesabı olan çalışanlar

Kural: Ayrıcalıklı hesapları olan çalışanlar onaylanmamış kişilere destek ve bilgi vermemelidirler. Özellikle de bilgisayar yardımı (bir uygulamanın kullanımı konusunda eğitim gibi), herhangi bir şirket veritabanına erişim, yazılım indirme ya da uzaktan erişim yeteneğine sahip çalışanların adlarının açıklanması gibi durumlar söz konusu olduğunda bu geçerlidir.

Açıklamalar/Notlar: Toplum mühendisleri çoğunlukla ayrıcalıklı he-

sapları olan çalışanları hedeflerler. Bu kuralın amacı ayrıcalıklı hesaplara sahip Bilgi İşlem çalışanlarını toplum mühendisliği saldırısı olabilecek telefonları başarıyla ele almaları konusunda yönlendirmektir.

8-3 Dahili sistem bilgileri

Kural: Bilgisayar işlemleri personeli, istek sahibine kimlik tespiti yapmadan, şirket bilgisayar sistemleri ya da ilgili donanımlarla ilgili değerli bilgileri kesinlikle açıklamamalıdır.

Açıklamalar/Notlar: Bilgisayar korsanları sistem erişim süreçleri, harici uzaktan erişim noktaları ve telefon bağlantı numaraları gibi, saldırgan için önemli olabilecek değerli bilgileri elde edebilmek için sık sık bilgisayar işlemleri personeliyle iletişim kurarlar.

Teknik destek personeli ya da yardım masası olan şirketlerde, bilgisayar sistemleri ya da ilgili donanıma yönelik soruların bilgisayar işlemleri personeline gelmesi olağandışı bir durum olarak görülmelidir. Herhangi bir veri talebi, şirket veri sınıflandırma kuralları çerçevesinde istek sahibinin bu bilgiyi istemeye yetkili olup olmadığını belirlemek üzere incelenmelidir. Veri sınıfına karar verilemediğinde, istenen bilgi incelemeye alınmalıdır.

Bazı durumlarda satıcı firmadan gelen teknik destek sorumlularının, şirketin bilgisayar sistemine erişimi olan kişilerle iletişim kurmaları gerekir. Bu tarz firmaların, şirketlerin Bilgi İşlem bölümlerinde iletişim kurdukları belirli kişiler olması gerekir, böylece bu kişiler karşılıklı onay açısından birbirlerini tanıyor olurlar.

8-4 Parolaların açıklanması

Kural: Bilgisayar işlemleri personeli hiçbir zaman kendilerine ait olan ya da onlara emanet edilmiş parolaları bir bilgi işlem yöneticisinin onayı olmadan açıklamamalıdırlar.

Açıklamalar/Notlar: Genel olarak başka birine parola söylemek yasaktır. Kural, acil bir durumda bilgisayar işlemleri personelinin üçüncü şahıslara bir parolayı verebileceği durumunu göz önünde bulundurur. Herhangi bir parolanın açıklanmasını yasaklayan genel kurala gelen bu istisna, bir bilgi işlem yöneticisinin özel iznini gerektirir. Daha fazla önlem almak adına, tanımlama bilgilerini açıklama sorumluluğunun, onay süreçleriyle ilgili özel eğitim almış bir grup kişiyle sınırlandırılması da şarttır.

8-5 Elektronik ortam

Kural: Dışarı verilmek üzere sınıflandırılmamış bilgiler içeren tüm elektronik ortamlar fiziksel olarak güvenli bir yere kilitlenmelidirler.

Açıklamalar/Notlar: Bu kuralın amacı elektronik ortamlarda saklanmış hassas bilgilerin fiziksel olarak çalınmasını önlemektir.

8-7 Yedekleme ortamları

Kural: Bilgisayar işlemleri personeli yedekleme ortamlarını şirket kasasında ya da başka bir güvenli yerde saklamalıdır.

Açıklamalar/Notlar: Yedekleme ortamları bilgisayar korsanlarının başlıca hedeflerindendir. Zincirin zayıf halkası fiziksel olarak korunmayan yedekleme ortamları olabilecekken, bir saldırgan, bir bilgisayar sistemine girmeye çalışmak için zaman harcamayacaktır. Yedekleme ortamları çalındıktan sonra saldırgan, veriler şifreli olmadığı sürece, orada kayıtlı herhangi bir dosyaya erişebilecektir. Bu yüzden yedekleme ortamlarını fiziksel olarak güvence altına almak şirket bilgilerinin gizliliğini korumak için önemli bir süreç olacaktır.

Tüm Çalışanlar İçin Geçerli Kurallar

Bilgi işlem, insan kaynakları, muhasebe ya da destek hizmetleri; şirketin neresinde çalışıyor olurlarsa olsunlar her çalışanın bilmesi gereken belirli güvenlik kuralları vardır. Bu kurallar, genel, bilgisayar kullanımı, e-posta kullanımı, evden çalışanlara yönelik kurallar, telefon kullanımı, faks kullanımı, sesli mesaj kullanımı ve parolalar şeklinde sınıflandırılmıştır.

Genel

9-1 Şüpheli aramaların rapor edilmesi

Kural: Herhangi bir şüpheli bilgi ya da bilgisayar işlemi talebinde bulunulması durumu da dahil olmak üzere bir güvenlik ihlaline maruz kaldıklarından kuşkulanan çalışanlar hemen olayı şirketin olay bildirme grubuna bildirmelidirler.

Açıklamalar/Notlar: Toplum mühendisi, isteklerini yerine getirmeye hedefini ikna edemediği durumda, her zaman başka birini deneyecektir. Şüpheli bir aramayı ya da olayı bildiren çalışan, bir saldırı olduğu yolunda şirketi bilgilendirmek için ilk adımı atmış olur. Böylece, çalışanlar, toplum mühendisliği saldırılarına karşı ilk savunma hattını oluştururlar.

9-2 Şüpheli aramaları belgelemek

Kural: Bir toplum mühendisliği saldırısı gibi görünen şüpheli bir aramada, çalışan, uygun olduğu ölçüde, saldırganın ne başarmaya çalıştığını anlatacak kadar ayrıntı öğrenmeye çalışmalı ve belgeleme amacıyla bu ayrıntılarla ilgili notlar almalıdır.

Açıklamalar/Notlar: Bu tarz ayrıntılar, olay bildirme grubuna bildirildiğinde, saldırının yönünün ya da amacının bulunmasına yardımcı olur.

9-3 Bağlantı numaralarının verilmesi

Kural: Şirket çalışanları şirketin modem telefon numaralarını açıklamamalı ve bu tarz istekleri her zaman yardım masasına ya da teknik destek personeline yönlendirmelidir.

Açıklamalar/Notlar: Bağlantı telefon numaraları, yalnızca iş yükümlülüklerini yerine getirebilmek için bunun gibi bilgilere gereksinimi olan çalışanlara verilecek türden bir dahili bilgi olarak değerlendirilmelidir.

Toplum mühendisleri düzenli olarak bilgi taleplerine karşı daha az korumacı davranacak çalışanları ya da bölümleri hedeflerler. Örneğin saldırgan, bir faturalama sorununu çözmeye çalışan bir telefon şirketi çalışanı gibi kendini gösterip ödemeler bölümünü arayabilir. Saldırgan daha sonra sorunu çözebilmek için bildikleri başka faks ya da bağlantı numarası olup olmadığını sorar. Toplum mühendisi sık sık bu tarz bilgiyi vermenin oluşturduğu tehlikenin farkında olmayan ya da şirket bilgi verme kural ve süreçlerine yönelik yeterli eğitimi almamış bir çalışanı seçer.

9-4 Şirket kimlik kartları

Kural: İçinde bulundukları ofis bölgesi haricinde, üst ve orta yönetim de dahil, tüm şirket çalışanları her zaman personel kartlarını takmalıdırlar.

Açıklamalar/Notlar: Şirket yöneticileri de dahil tüm çalışanlar, halka açık yerler ya da kişinin kendi ofisi ya da çalışma alanı dışındaki her yerde, kimlik takmanın zorunlu olduğunu anlamaları için eğitilmeli ve teşvik edilmelidirler.

9-5 Kimlik kartı ihlallerinin sorgulanması

Kural: Tüm çalışanlar şirket kimlik kartı ya da ziyaretçi kartı takmayan tanımadıkları kişileri hemen sorgulamalıdırlar.

Açıklamalar/Notlar: Her ne kadar hiçbir şirket, açık göz çalışanların kimliksiz koridora çıkan başka çalışanları enselediği bir kültür yaratmak istemese de bilgilerini koruma endişesine sahip herhangi bir şirketin, bina içinde sorgulamadan dolaşan bir toplum mühendisi tehdidini de ciddiye alması gerekir. "Her zaman kartlı dolaş" kuralını yerleştirmek için gayretli olduğunu gösteren çalışanları teşvik etmek için şirket gazetesinde ya da bülten panosunda duyurulması, birkaç saatlik ücretli izin ya da şahsi dosyasına konacak bir tavsiye mektubu verilmesi gibi çeşitli uygulamalar kullanılabilir.

9-6 Peşpeşe geçmek (güvenlikli girişlerden geçişler)

Kural: Binaya giren çalışanlar, içeri girmek için manyetik kart gibi güvenli araçlar kullandıklarında tanımadıkları hiç kimsenin hemen arkalarından gelmesine izin vermemelidirler (peşpeşe geçmek).

Açıklamalar/Notlar: Çalışanlar, bir tesise ya da güvenli bir alana

girmeye çalışan tanımadıkları kişilerin kendilerini tanıtmalarını istemenin kabalık olmayacağını bilmelidirler.

Toplum mühendisleri peşpeşe geçme olarak bilinen bir teknik kullanırlar. Bu teknikte tesise ya da hassas bir alana giren birini beklerler ve onunla birlikte içeri giriverirler. Çoğu insan, büyük olasılıkla şirket çalışanı olduklarını varsaydığı diğer kişileri sorgulamaktan rahatsız olur. Başka bir peşpeşe geçme tekniği ise bir sürü kutuyu birden taşımaktır, böylece hiçbir şeyin farkında olmayan bir çalışan, yardım etmek için kapıyı açar ya da tutar.

9-7 Hassas belgelerin kâğıt öğütücüden geçirilmesi

Kural: Atılacak hassas belgeler çapraz öğütücüden geçirilmelidir. Herhangi bir zamanda hassas bilgiler ya da malzemeler içermiş olan sabit sürücüler de dahil tüm taşınabilir ortamlar bilgi güvenliğinden sorumlu grup tarafından belirlenen süreçler gereğince yok edilmelidir.

Açıklamalar/Notlar: Sıradan kâğıt öğütücüler belgeleri yeterli ölçüde parçalamazlar; çapraz-öğütücüler ise belgeleri tanınmaz duruma getirirler. En iyi güvenlik uygulaması, kuruluşun, başlıca rakiplerinin, atılmış malzemelerin arasında işlerine yarayacak bilgiler arayacaklarını varsaymasıdır.

Sanayi casusları ve bilgisayar sadırganları hassas bilgileri sürekli çöpe atılmış malzemelerden çıkarırlar. Bazı durumlarda rakip şirketlerin çöpleri vermeleri için temizlikçilere rüşvet vermeye teşebbüs ettikleri de bilinir. Yakın bir örnek, bir sermaye piyasası aracı kurumu çalışanı içeriden edinilen bilgiyle yapılan alım satımlara yönelik çöpte bir takım malzemeler bulmuştu.

9-8 Kişisel tanımlayıcılar

Kural: Kimlik numarası, Sosyal Güvenlik Numarası, ehliyet numarası, doğum tarihi ve yeri ve annenin kızlık soyadı gibi kişisel tanımlayıcılar kimlik tespiti amacıyla kullanılmamalıdırlar. Bu tanımlayıcılar sır değildir ve sayısız yöntemle elde edilebilirler.

Açıklamalar/Notlar: Bir toplum mühendisi başka insanların kişisel tanımlayıcılarını bir ücret karşılığında edinebilir. Aslında genel kanının aksine internet erişimi ve kredi kartı olan herhangi biri bu kişisel tanımlama bilgilerini ele geçirebilir. Açık tehlikeye karşın bankalar, hizmet şirketleri ve kredi kartı şirketleri sık sık bu tanımlayıcıları kullanmaktadırlar. Sadece bu nedenle kimlik hırsızlığı son on yılın en hızlı artan suçu olmuştur.

9-9 Kuruluş şemaları

Kural: Şirketin kuruluş şemasında gösterilen ayrıntılar şirket çalışanları dışında kimseye verilmemelidir.

Açıklamalar/Notlar: Şirket yapısı bilgileri kuruluş şemalarını, hiye-

rarşi şemalarını, bölüm çalışan listelerini, raporlama yapısını, çalışan adlarını, çalışan unvanlarını, dahili telefon numaralarını, kimlik numaralarını ya da benzeri bilgileri içerir.

Toplum mühendisliği saldırısının ilk aşamasında amaç şirketin iç yapısıyla ilgili bilgi toplamaktır. Sonra bu bilgiler bir saldırı planı yapmak için kullanılır. Saldırgan, hangi çalışanların aradığı bilgiye erişimi olabileceğine karar verebilmek için bu bilgiyi inceler. Saldırı sırasında bilgi, saldırganın işine hakim bir çalışan olarak görünmesini sağlar ve kurbanını iş birliği yapmaya ikna etme olasılığını artırır.

9-10 Çalışanlarla ilgili özel bilgiler

Kural: Çalışanların özel bilgilerine yönelik tüm talepler insan kaynaklarına yönlendirilmelidir.

Açıklamalar/Notlar: Bu kuralın bir istisnası, işle ilgili bir konuda bağlantı kurulması gereken ya da karşı taraftan telefon bekleyen bir çalışanın telefon numarasının verilmesi olabilir. Ancak numarayı isteyen kişinin telefon numarasının alınması ve çalışanın onu geri araması her zaman tercih edilmesi gereken yoldur.

Bilgisayar Kullanımı

10-1 Bilgisayara komut girmek

Kural: İstek sahibinin bilgi işlem bölümünün bir çalışanı olduğu onaylanmadığı sürece şirket çalışanları, başka birinin isteği üzerine bilgisayara ya da bilgisayarlarla ilgili donanıma hiçbir zaman komut girmemelidirler.

Açıklamalar/Notlar: Toplum mühendislerinin sıkça oynadığı bir oyun, çalışandan sistem ayarlarını değiştiren bir komut girmesini istemeleridir. Bu sayede saldırgan, kendini tanıtmadan kurbanın bilgisayarına girebilir ya da teknik bir saldırıda kullanılabilecek bilgilere erişebilir.

10-2 Dahili adlandırma standartları

Kural: İstek sahibinin şirkette çalıştığı onaylanmadan çalışanlar bilgisayar sistemlerinin ya da veri tabanlarının adlarını açıklamamalıdırlar.

Açıklamalar/Notlar: Toplum mühendisleri bazen şirket bilgisayar sistemlerinin adlarını elde etmeye çalışırlar. Adları öğrendikten sonra saldırgan, şirketi arar ve sistemleri kullanmakta sorun çeken bir çalışan gibi davranır. Toplum mühendisi o sisteme verilen dahili adı bilerek inandırıcılığını artırır.

10-3 Program çalıştırma talepleri

Kural: Şirket çalışanları, başka birinin isteği üzerine herhangi bir bilgisayar uygulamasını ya da programını çalıştırmamalıdırlar.

Açıklamalar/Notlar: Program veya uygulama çalıştırmaya ya da bilgisayarda herhangi bir işlem yapmaya yönelik talepler talep sahibinin bilgi işlem bölümü çalışanı olduğu onaylanana kadar reddedilmelidir. Eğer talep bir dosyadan ya da elektronik mesajdan, gizli bilgilerin çekilmesiyle ilgiliyse, talebe karşılık vermek, gizli bilgi verme süreçleriyle uyumlu olmalıdır (bkz. Bilgi Verme Kuralları).

Bilgisayar saldırganları sistemi ele geçirmelerini sağlayacak programları çalıştırmaları için insanları kandırırlar. Hiçbir şeyden kuşkulanmayan bir kullanıcı, saldırganın yerleştirdiği bir programı çalıştırdığında, ortaya çıkan sonuç, saldırganın, kurbanın bilgisayarına erişmesine neden olabilir. Bir toplum mühendisi zarar verebilecek bilgisayar komutlarını çalıştırması için birilerini kandırabilirken, teknik tabanlı bir saldırı, benzer bir zararı bilgisayar programlarını çalıştırması için bilgisayarın işletim sistemini kandırarak yapabilir.

10-4 Yazılım indirmek ya da yüklemek

Kural: İstek sahibinin bilgi işlem bölümünün bir çalışanı olduğu onaylanmadığı sürece şirket çalışanları başka birinin isteği doğrultusunda hiçbir zaman yazılım indirmemeli ya da yüklememelidir.

Açıklamalar/Notlar: Çalışanlar bilgisayarlarla ilgili donanıma yönelik herhangi bir olağandışı işlem talebine karşı her zaman uyanık olmalıdırlar.

Toplum mühendislerinin sıkça kullandığı taktiklerden birisi, hiçbir şeyden kuşkulanmayan kurbanlarını saldırgana bilgisayar ya da ağ güvenliğini aşma amacında yardımcı olacak bir program yüklemeye ya da indirmeye ikna etmektir. Bazı durumlarda program gizlice kullanıcıyı gözetleyebilir ya da gizli bir uzaktan kontrol yazılımıyla saldırganın bilgisayar sistemini ele geçirmesini sağlayabilir.

10-5 Düz metin parolalar ve e-posta

Kural: Şifreli olmadıkları sürece parolalar e-postayla gönderilmemelidirler.

Açıklamalar/Notlar: Her ne kadar önerilmese de bu kural aşağıdaki gibi sınırlı koşullarda e-ticaret sitelerinde de kullanılabilir:

- Siteye kaydolmuş müşterilere parolalarının gönderilmesi.
- Parolasını unutmuş ya da kaybetmiş müşterilere parolalarının gönderilmesi.

10-6 Güvenlikle ilgili yazılımlar

Kural: Şirket çalışanları hiçbir zaman virüs/Truva Atı koruma, güvenlik duvarı ya da diğer güvenlikle ilgili yazılımları bilgi işlem bölümünden alınmış bir onay olmadan devre dışı bırakmamalı ya da kaldırmamalıdırlar.

Açıklamalar/Notlar: Bilgisayar kullanıcıları bazen güvenlikle ilgili yazılımları, başka herhangi bir nedeni olmadan, bilgisayarlarının hızını artıracağını düşünerek kapatırlar.

Bir toplum mühendisi, güvenlikle ilgili tehditlerden şirketi korumak için gerekli olan bir yazılımı kaldırması ya da devre dışı bırakması için bir çalışanı kandırmaya çalışabilir.

10-7 Modemlerin yüklenmesi

Kural: Bilgi İşlem bölümünden onay alınmadan herhangi bir bilgisayara modem bağlanamaz.

Açıklamalar/Notlar: Çalışma ortamında masalarda ya da bilgisayarların üstünde duran modemlerin -özellikle de şirket ağına bağlılarsa- ciddi bir güvenlik tehdidi oluşturdukları bilinmelidir. Buna göre, bu kural modem bağlama süreçlerini düzenlemektedir.

Bilgisayar korsanları bir telefon silsilesine bağlı çalışan bir modem hattı olup olmadığını anlamak için savaş araması denen bir teknik kullanırlar. Aynı teknik, şirket içinde modemlere bağlı telefon numaralarını bulmak için de kullanılabilir. Eğer saldırgan, bilgisayar sisteminin, kolay tahmin edilebilir bir parolası olan ya da hiç parolası olmayan zayıf bir uzaktan erişim programı kullanan bir modeme bağlı olduğunu görürse, kolaylıkla şirket ağına girebilir.

10-8 Modemler ve otomatik yanıt verme ayarları

Kural: Birilerinin bilgisayar sistemine modem bağlantısından girmesini önlemek amacıyla Bilgi İşlem onaylı tüm bilgisayarların, modem otomatik yanıt verme özellikleri kapatılmalıdır.

Açıklamalar/Notlar: Bilgi işlem bölümü, uygun olduğu ölçüde, modem aracılığıyla harici bilgisayar sistemlerine bağlanması gereken çalışanlar için dış hat bağlantılarda kullanılacak bir iletişim alanı tahsis etmelidir.

10-9 Kırma araçları

Kural: Çalışanlar yazılım koruma mekanizmalarını alt etmek üzere tasarlanmış yazılım araçları indirmemeli ya da kullanmamalıdırlar.

Açıklama/Notlar: İnternette ticari yazılımları ve paylaşım yazılımlarını kırmak üzere tasarlanmış programlara adanmış düzinelerce site vardır. Bu araçların kullanımı yalnızca yazılım sahibinin telif haklarını çiğnemekle kalmamakta, aynı zamanda oldukça da büyük bir tehlike oluşturmaktadır. Bu programlar bilinmeyen kaynaklardan geldiği için kullanıcının bilgisayarına zarar verebilecek kötü huylu yazılımlar içerebilir ya da programı yazan kişinin, kullanıcının bilgisayarına erişebilmesi için bir Truva Atı yerleştirebilir.

10-10 Çevrimiçi şirket bilgileri

Kural: Çalışanlar herhangi bir herkese açık haber gurubuna, foruma ya da bültene şirkete ait donanım ya da yazılımlarla ilgili ayrıntılar yazmamalı ve kurallara uygun olanlar dışında iletişim bilgileri vermemelidirler.

Açıklamalar/Notlar: Usenet'e, çevrimiçi forumlara, bülten panolarına ya da yazışma listelerine bırakılmış herhangi bir mesaj, hedef şirket ya da hedef bireyle ilgili bilgi toplarken araştırılabilir. Bir toplum mühendisliği saldırısının araştırma aşamasında, saldırgan şirketle, ürünleriyle ve çalışanlarıyla ilgili yararlı bilgiler bulabilmek için internetteki mesaj grupları taranabilir.

Bazı mesajlar saldırganın saldırısını ilerletmek için kullanabileceği ufak tefek bilgiler de içerir. Örneğin, bir ağ yöneticisi belirli bir marka ve model güvenlik duvarı için güvenlik duvarı filtrelerinin ayarlanmasıyla ilgili bir soru mesajı bırakmış olabilir. Bu mesajı bulan bir saldırgan şirket ağına girebilmesi için çevresinden dolaşmasını sağlayacak, şirketin güvenlik duvarı ayarları ve türüyle ilgili değerli bilgiler elde edebilir.

Çalışanların haber gruplarına nereden geldiğinin anlaşılmayacağı adsız hesaplardan mesaj göndermelerine izin vererek bu sorun azaltılabilir ya da önüne geçilebilir. Kural, doğal olarak çalışanların şirketle ilişkilendirilebilecek herhangi bir iletişim bilgisi bırakmamaları şartını da getirmelidir.

10-11 Elektronik depolama ortamları

Kural: Eğer bilgisayar bilgilerini saklamak için kullanılan CD-ROM gibi ortamlar, çalışma alanında ya da çalışanın masasında bırakılmışsa ve bilinmeyen bir kaynaktan geliyorsa bilgisayar sistemine sokulmamalıdır.

Açıklamalar/Notlar: Saldırganların kötü huylu yazılım yüklemek için kullandıkları yöntemlerden biri programları bir CD-ROM'a koyup ilgi çekici bir şekilde etiketlemektir (örneğin, "Personel Maaş Verileri-Gizlidir"). Sonra bunun birkaç kopyasını çalışanların kullandıkları alanlara bırakırlar. Yalnızca biri bir bilgisayara girer ve içindeki dosyalar açılırsa, saldırganın kötü huylu yazılımı çalışmaya başlar. Bu, sisteme girilmesini sağlayacak bir arka kapı yaratabilir ya da ağa başka türlü zararlar verebilir.

10-12 Taşınabilir ortamların atılması

Kural: Bilgi silinmiş bile olsa herhangi bir zaman aralığında hassas şirket bilgilerinin tutulduğu bir elektronik ortamı çöpe atmadan önce ortam manyetik olarak silinmeli ya da kurtarılamayacak şekilde zarar görmüş olmalıdır.

Açıklamalar/Notlar: Basılı belgelerin öğütülmesi bugünlerde sıradan işlerden biri olduysa da, şirket çalışanları bir zamanlar hassas bilgiler içermiş bir elektronik ortamı çöpe atmanın yaratabileceği tehdidi gözardı edebilirler. Bilgisayar saldırganları, atılmış elektronik ortamlarda bulunan bilgileri geri getirmeye çalışırlar. Çalışanlar, dosyaları silerek, bu dosyaların geri getirilemeyeceğini varsayıyor olabilirler. Bu varsayım tamamen yanlıştır ve gizli iş bilgilerinin yanlış ellere düşmesine neden olabilir. Bu nedenle genel olarak sınıflandırılmamış bilgiler içermekte ya da bir zamanlar içermiş olan tüm elektronik ortamlar tamamen temizlenmeli ya da sorumlu grubun onayladığı yöntemler kullanılarak yok edilmelidir.

10-13 Parola korumalı ekran koruyucular

Kural: Tüm bilgisayar kullanıcıları bir ekran koruyucusu parolası oluşturmalı ve belli bir süre kullanılmadığı zaman bilgisayarı kilitleyen bir zaman aşımı süresi belirlemelidir.

Açıklamalar/Notlar: Tüm çalışanlar bir ekran koruyucu parolası ve on dakikadan fazla olmamak üzere bir zaman aşımı süresi ayarlamalıdırlar. Bu kuralın amacı yetkisiz kişilerin başka birinin bilgisayarını kullanmasını önlemektir. Bu nedenle bu kural şirket bilgisayar sistemlerini, dışarıdan binaya girebilen kişilere karşı korur.

10-14 Parola gizlilik taahhüdü

Kural: Yeni bir bilgisayar hesabı açılmadan önce çalışan ya da taşeron, parolaların hiçbir zaman herhangi birine açıklanmaması ya da paylaşılmaması gerektiğini ve bu kurallara uymayı kabul ettiğini gösteren yazılı bir beyan imzalamalıdır.

Açıklamalar/Notlar: Anlaşmada, bu tarz bir anlaşmaya uyulmadığı durumda bunun, cezası işten çıkarmaya kadar varan ciddi bir disiplin suçu teşkil edeceğini belirten bir madde de bulundurulmalıdır.

E-Posta Kullanımı

11-1 E-Posta ekleri

Kural: E-posta ekleri güvenilir bir kişiden gelmediği ya da işle ilgili olarak beklenmediği sürece açılmamalıdır.

Açıklamalar/Notlar: Tüm e-posta ekleri yakından izlenmelidir. Alıcı, eki açmadan önce güvenilir bir kişinin ekli bir e-posta gönderileceğine dair ön bilgi vermesini zorunlu tutabilirsiniz. Bu, saldırganların toplum mühendisliği taktikleri kullanarak insanları ekleri açmaları doğrultusunda kandırabilme riskini azaltacaktır.

Bir bilgisayar sistemine girmenin yöntemlerinden biri, saldırganın sisteme girebilmesini sağlayacak bir açık yaratan kötü huylu bir prog-

ramı çalıştırması için çalışanı kandırmaktır. Saldırgan, çalıştırılabilir bir kod ya da makro içeren bir e-posta eki göndererek kullanıcının bilgisayarının kontrolünü ele geçirebilir.

Bir toplum mühendisi kötü huylu e-posta ekleri gönderebilir, sonra da telefonla arayıp alıcıyı eki açmaya ikna etmeye çalışabilir.

11-2 Harici adreslere otomatik yönlendirme

Kural: Gelen e-postaların otomatik olarak harici bir e-posta adresine yönlendirilmesi yasaklanmalıdır.

Açıklamalar/Notlar: Bu kuralın amacı, dahili bir e-posta adresine gönderilmiş bir e-postayı dışarıdan birinin almasını önlemektir.

Çalışanlar, ofisten uzak olacakları zaman gelen e-postalarını bazen şirket dışından bir e-posta adresine yönlendirirler. Ya da bir saldırgan, bir çalışanı kandırarak e-postaları şirket dışından bir adrese postalayan bir dahili e-posta adresi oluşturtabilir. Saldırgan, daha sonra dahili e-posta adresi olan, içeriden biri gibi davranarak, insanların hassas bilgilerí harici bir adrese göndermelerini sağlayabilir.

11-3 E-postaların yönlendirilmesi

Kural: Onaylanmamış bir kişiden gelen herhangi bir başka onaylanmamış kişiye e-posta aktarma talebi, talep sahibine kimlik tespiti yapılmasını gerektirir.

11-4 E-postaların onaylanması

Kural: Genel olarak sınıflandırılmamış bir bilgi talebi içeren ya da bilgisayarlarla ilgili donanımlara yönelik bir işlem yapılmasını isteyen ve güvenilir bir kişiden geliyor gibi görünen bir e-posta mesajı için ek bir tanımlama şekli daha gereklidir (bkz. Onay ve Yetkilendirme Süreçleri).

Açıklamalar/Notlar: Bir saldırgan bir e-postayı ve başlığını kolaylıkla taklit ederek onu farklı bir e-posta adresinden geliyormuş gibi gösterebilir. Ayrıca girdiği bir bilgisayar sisteminden de e-posta gönderebilir. E-postanın başlığını inceleyerek bile müdahale edilmiş bir dahili sistemden gönderilip gönderilmediğini ayırt edemezsiniz.

Telefon Kullanımı

12-1 Telefon anketlerine katılmak

Kural: Çalışanlar, başka kuruluşların ya da kişilerin soru sorma yoluyla yaptığı anketlere katılamazlar. Bu tarz talepler halkla ilişkiler bölümüne ya da diğer sorumlu kişilere yönlendirilmelidir.

Açıklamalar/Notlar: Şirkete karşı kullanılabilecek değerli bilgileri elde edebilmek için toplum mühendislerinin kullandığı yöntemlerden biri

de çalışanı arayıp bir anket yaptığını söylemektir. Yasal bir araştırmaya katkıda bulunduklarına inandıkları zaman insanların şirket ya da kendileriyle ilgili yabancılara bilgi vermek konusunda ne kadar rahat olduklarına inanamazsınız. Saldırgan, zararsız görünümlü soruların arasına yanıtlarını bilmek istediği birkaç soruyu daha sıkıştırır. Sonuç olarak bu tarz bilgiler şirket ağına girmek için kullanılabilirler.

12-2 Dahili telefon numaralarının verilmesi

Kural: Eğer onaylanmamış bir kişi bir çalışana telefon numarasını sorarsa, çalışan, şirket işlerinin yönetilmesi ile ilgili olarak numarayı vermenin gerekli olup olmadığı doğrultusunda uygun bir karar verebilir.

Açıklamalar/Notlar: Bu kuralın amacı dahili telefon numaralarını vermenin gerekli olup olmadığı üzerinde düşünülmüş bir karar vermeye çalışanları yönlendirmektir. Numarayı öğrenmek için iyi bir nedenleri varmış gibi görünmeyen insanlarla uğraşırken en emin yol ana şirket telefonunu aramaları ve oradan aktarılmalarını söylemektir.

12-3 Sesli mesaj parolaları

Kural: Herhangi birinin sesli mesaj kutusuna parola bilgileri içeren mesajlar bırakmak yasaktır.

Açıklamalar/Notlar: Kolay tahmin edilebilir bir erişim koduyla yetersiz bir şekilde korundukları için bir toplum mühendisi sık sık bir çalışanın sesli mesaj kutusuna erişebilir. Saldırı türlerinden birinde, bilgili bir bilgisayar korsanı kendi sahte sesli mesaj kutusunu yaratabilir ve başka bir çalışanı parola bilgilerini içeren bir mesaj bırakmaya ikna edebilir. Bu kural bu tarz bir oyunun üstesinden gelmek içindir.

Faks Kullanımı

13-1 Faks gönderilmesi

Kural: İstek sahibinin kimlik tespiti yapılmadan kimseden faks alınamaz ve kimseye faks gönderilemez.

Açıklamalar/Notlar: Bilgi hırsızları, güvenilir çalışanları, şirket içindeki bir faks makinasına hassas bilgileri göndermeleri doğrultusunda kandırabilirler. Kurbana faks numarasını vermeden önce saldırgan, sekreter ya da idarî yardımcı gibi, hiçbir şeyden haberi olmayan bir çalışanı arar ve daha sonra alınması için kendilerine bir faks gönderilip gönderilemeyeceğini sorar. Ardından, masum çalışan faksı aldıktan sonra, saldırgan çalışanı arar ve faksın başka bir yere fakslanmasını rica eder. Arada, bunun acil bir toplantı için gerekli olduğunu söylemeyi de ihmal etmez. Faksı göndermesi istenen kişi, o bilginin değeri konusunda bir fikri olmadığı için isteği yerine getirir.

13-2 Faksla gönderilmiş talimatların onaylanması

Kural: Faksla gelen talimatları yerine getirmeden önce, gönderenin şirketin bir çalışanı ya da bir güvenilir kişi olduğu onaylanmalıdır.

Açıklamalar/Notlar: Faks aracılığıyla, bilgisayara komut girilmesi ya da bilgi istenmesi gibi olağandışı istekler gönderildiği zaman çalışanlar dikkatli olmalıdırlar. Fakslanmış belgelerin başlığında geçen bilgiler gönderici faks makinasının ayarlarıyla oynanarak değiştirilebilir. Bu yüzden faks başlığı yetki ya da kimlik tespiti için yeterli bir veri olarak kabul edilmemelidir.

13-3 Faksla hassas bilgilerin gönderilmesi

Kural: Başka çalışanların da erişebileceği bir yerde duran bir faks makinasına hassas bilgi göndermeden önce, gönderen, bir kapak sayfası göndermelidir. Alıcı, kapak sayfasını alır almaz karşılık olarak bir sayfa gönderir ve faks başında olduğunu gösterir. Gönderici, daha sonra faksın tümünü gönderir.

Açıklamalar/Notlar: Bu tokalaşma süreci, göndericinin, alıcının makinanın başında bulunduğundan emin olmasını sağlar. Bu süreç ayrıca, mesajı alacak faks numarasının başka bir numaraya yönlendirilmediğini de doğrular.

13-4 Parola fakslamak yasaktır

Kural: Parolalar hiçbir koşulda faks aracılığıyla gönderilmemelidir.

Açıklamalar/Notlar: Tanımlama bilgilerini faksla göndermek güvenli değildir. Çoğu faks makinası, çok sayıda çalışanın birden elinin altındadır. Dahası, fakslar genel telefon santralları ağına bağlıdırlar. Gönderilen faks başka bir numarada bulunan saldırgana gidecek şekilde arama yönlendirmesi yapılabilir.

Sesli Mesaj Kullanımı

14-1 Sesli mesaj parolaları

Kural: Sesli mesaj parolaları hiçbir nedenle başkalarına verilmemelidirler. Buna ek olarak sesli mesaj parolaları en çok doksan günde bir değiştirilmelidir.

Açıklamalar/Notlar: Gizli şirket bilgileri sesli mesaj kutularına bırakılabilir. Bu bilgiyi korumak için çalışanlar sesli mesaj parolalarını sık sık değiştirmeli ve bunları hiçbir zaman başkalarına vermemelidirler. Ayrıca, on iki aylık dönemler içerisinde sesli mesaj kullanıcıları aynı ya da benzer parolalar kullanmamalıdırlar.

14-2 Çoklu sistemlerde parolalar

Kural: Sesli mesaj kullanıcıları ister dahili isterse harici, telefon ya

da bilgisayar sistemlerinde kullandıkları parolayı kullanmamalıdırlar.

Açıklamalar/Notlar: Sesli mesaj ve bilgisayar gibi farklı ortamlarda aynı ya da benzer parolayı kullanmak, bir tanesini tespit ettikten sonra toplum mühendislerinin tüm parolaları tahmin etmelerini kolaylaştırır.

14-3 Sesli mesaj parolalarının ayarlanması

Kural: Sesli mesaj kullanıcıları ve yöneticiler tahmin edilmesi zor olan sesli mesaj parolaları kullanmalıdırlar. Parolalar herhangi bir şekilde kullanan kişiyle ya da şirketle ilişkilendirilmemeli ve tahmin edilme olasılığı olan öngörülebilir bir düzende olmamalıdır.

Açıklamalar/Notlar: Parolalar ardışık ya da tekrarlanan sayılar (örneğin, 1111, 1234, 1010) içermemelidir. Dahili telefon numaralarının aynısı ya da benzeri olmamalı, adres, posta kodu, doğum tarihi, araç plakası, telefon numarası, ağırlık, IQ ya da başka türlü tahmin edilebilir kişisel bilgilerle ilişkili olmamalıdırlar.

14-4 "Eski" olarak işaretlenmiş mesajlar

Kural: Dinlenmemiş sesli mesajlar yeni mesaj olarak işaretlenmediğinde sesli mesaj yöneticisi, olası bir güvenlik ihlaline karşı uyarılmalı ve sesli mesaj parolası hemen değiştirilmelidir.

Açıklamalar/Notlar: Toplum mühendisleri çeşitli yollarla sesli mesaj kutularına ulaşabilirler. Hiç dinlemediği mesajların yeni mesaj olarak geçmediği bir durumda, çalışan, birinin sesli mesaj kutusuna yetkisiz giriş yapıp mesajları dinlediğini varsaymalıdır.

14-5 Harici sesli mesaj açılış notları

Kural: Şirket çalışanları dışarıya yönelik sesli mesaj açılış notlarında verdikleri bilgiyi sınırlamalıdırlar. Genel olarak, çalışanın günlük işleri ya da yolculuk tarihleriyle ilgili bilgiler verilmemelidir.

Açıklamalar/Notlar: Dışarıya yönelik açılış notları, soyad, dahili telefon numarası ya da yerinde bulunmama nedenlerini (yolculuk, tatil tarihleri ya da günlük program gibi) içermemelidir. Bir saldırgan bu bilgiyi diğer çalışanları kandırmaya yönelik akla yatkın bir hikâye uydurabilmek için kullanır.

14-6 Sesli mesaj parola düzenleri

Kural: Sesli mesaj kullanıcıları bir bölümü sabit kalan, kalanı öngörülebilir bir şekilde değişen parolalar seçmemelidirler.

Açıklamalar/Notlar: Örneğin, son iki basamağın içinde bulunulan aya karşılık geldiği 743501, 743502, 743503 gibi parolalar kullanılmamalıdır.

14-7 Gizli ya da özel bilgiler

Kural: Gizli ya da özel bilgiler sesli mesajlarla aktarılmamalıdır.

Açıklamalar/Notlar: Şirket telefon sistemi çoğu zaman şirket bilgisayar sistemlerinden daha fazla saldırıya açıktır. Parolalar, bir saldırganın yaptığı tahminleri büyük ölçüde kolaylaştıran bir dizi sayıdan oluşur. Ayrıca bazı kuruluşlarda sesli mesaj parolaları yöneticileri adına mesaj alma sorumluluğu olan sekreterlere ya da yönetici asistanlarına verilebilmektedir. Yukarıdaki bilgilerin ışığında kimsenin sesli mesaj kutusuna hassas bilgiler bırakılmamalıdır.

Parolalar

15-1 Telefon güvenliği

Kural: Parolalar hiçbir zaman telefonda verilmemelidir.

Açıklamalar/Notlar: Saldırganlar, ya şahsen ya da teknolojik bir araç yardımıyla telefon görüşmelerini dinlemenin yollarını bulabilirler.

15-2 Bilgisayar parolalarının verilmesi

Kural: Bilgi işlem yöneticisinin yazılı onayı olmadan bilgisayar kullanıcıları hiçbir koşulda parolalarını başkalarına vermemelidirler.

Açıklamalar/Notlar: Pek çok toplum mühendisliği saldırısının amacı hiçbir şeyden kuşkulanmayan kişilerin hesap adlarını ve parolalarını açıklamaları doğrultusunda onları kandırmaktır. Bu kural şirkete karşı yapılan toplum mühendisliği saldırılarının başarı olasılığını azaltmak için önemli bir adımdır. Sonuç olarak, bu kurala şirket bünyesinde harfiyen uyulmalıdır.

15-3 İnternet parolaları

Kural: Çalışanlar, şirket sisteminde kullandıkları parolanın bir benzerini ya da aynısını internet sitelerinde de kullanmamalıdırlar.

Açıklamalar/Notlar: Kötü amaçlı internet sitesi sahipleri değerli bir şey sunan ya da bir ödül kazanma olasılığı olduğunu söyleyen bir site yapabilirler. Ziyaretçilerin kayıt olabilmek için bir e-posta adresi, kullanıcı adı ve parola girmeleri gerekir. Çoğu insan aynı ya da benzer kayıt bilgilerini tekrar tekrar kullandıkları için kötü amaçlı internet sitelerinin sahipleri kullanılan parolayı ve bu parolanın çeşitli şekillerini hedefin ev ya da iş bilgisayarına saldırmak için kullanabilirler. Ziyaretçinin iş bilgisayarı kayıt işlemi sırasında girdiği e-posta adresinden de bazen bulunabilir.

15-4 Çoklu sistemlerde parolalar

Kural: Şirket çalışanları aynı ya da benzeri bir parolayı birden fazla sistemde kullanmamalıdırlar. Bu kural çeşitli araçları (bilgisayar ya da

sesli mesaj); çeşitli konumları (ev ya da iş); çeşitli sistemleri, araçları (yönlendirici ya da güvenlik duvarı) ya da programları (veritabanı ya da uygulama) kapsayabilir.

Açıklamalar/Notlar: Saldırganlar bilgisayar sistemlerine ya da ağlarına girmek için insan doğasını kullanırlar. Çoğu insanın girdikleri her sistemde bir sürü parolayı akılda tutma keşmekeşinden kurtulmak için aynı ya da benzer parolalar kullandıklarını bilirler. Bu yüzden saldırgan, hedefin hesabının olduğu sistemlerden birinin parolasını öğrenmeye çalışır. Parolayı bir kez öğrendikten sonra aynı parolanın ya da bir benzerinin çalışanın kullandığı diğer sistemlere ve araçlara erişim sağlama olasılığı yüksektir.

15-5 Parolaların yeniden kullanılması

Kural: Hiçbir bilgisayar kullanıcısı on sekiz aylık süre içerisinde aynı ya da benzer bir parola kullanmamalıdır.

Açıklamalar/Notlar: Parolanın sık değiştirilmesi, bir sadırganın bir kullanıcının parolasını keşfetmesi durumunda oluşabilecek zararı en aza indirger. Yeni parolayı önceki parolalardan farklı yapmak saldırganın tahmin etmesini zorlaştırır.

15-6 Parola yapısı

Kural: Çalışanlar, bir bölümü sabit kalan diğer bölümü öngörülebilir bir şekilde değişen parolalar seçmemelidirler.

Açıklamalar/Notlar: Örneğin, son iki basamağın içinde bulunulan aya karşılık geldiği Kevin01, Kevin02, Kevin03 gibi parolalar kullanılmamalıdır.

15-7 Parola seçimi

Kural: Bilgisayar kullanıcıları aşağıdaki koşulları sağlayan bir parola yaratmalı ya da seçmelidir.

- Standart kullanıcı hesapları için en az sekiz karakter ve ayrıcalıklı hesaplar için en az on iki karakter uzunluğunda olmalıdır.
- En az bir sayı, bir simge ($, -, |, & gibi), bir küçük harf ve bir büyük harf (işletim sisteminde bulunan farklı yazı şekillerinin el verdiği ölçüde) içermelidir.
- Aşağıdakilerden herhangi birini içermemelidir: Herhangi bir dildeki sözlükte bulunabilecek bir kelime, çalışanın soyadı, hobileri, plaka numarası, Sosyal Güvenlik Numarası, adresi, telefon numarası, evcil hayvanının adı, doğum günü ya da bu kelimeleri içeren kelime grupları.
- Daha önce kullanılmış bir parolanın bir tarafı sabit bir tarafı değişmiş türden farklı bir şekli de olmamalıdır, kevin, kevin1, kevin2 ya da kevinocak, kevinşubat gibi.

Açıklamalar/Notlar: Yukarıda sıralanan özelliklerin kullanılması toplum mühendisinin tahmin etmesinin zor olacağı bir parola ortaya çıkaracaktır. Diğer bir seçenek ise sesli-sessiz harf yöntemidir. Bu yöntemle hatırlaması ve okuması kolay bir parola elde edilebilir. Böyle bir parola oluşturabilmek için "ABABABAB" şablonunda B harflerini sessiz harflerle, A harflerini ise sesli harflerler değiştirin. Örnek vermek gerekirse, MIKOFASO ya da KUSOCENA olabilir.

15-8 Parolaları not etmek

Kural: Çalışanlar parolalarını yalnızca bilgisayardan ya da başka parola korumalı donanımdan uzakta güvenli bir yere koyacaklarsa bir yere not edebilirler.

Açıklamalar/Notlar: Çalışanlara parolalarını hiçbir zaman bir yere yazmamaları salık verilmelidir. Ancak bazı koşullar altında bu gerekli olabilir. Örneğin, çalışanın farklı bilgisayar sistemlerinde birden fazla hesabı varsa. Herhangi bir yazılı parola bilgisayardan uzakta güvenli bir yere konmalıdır. Hiçbir koşulda parola klavyenin altına saklanmamalı ya da monitöre yapıştırılmamalıdır.

15-9 Bilgisayar dosyalarındaki şifrelenmemiş parolalar

Kural: Şifrelenmemiş parolalar herhangi bir bilgisayar dosyasında saklanmayacak ya da bir işlev tuşuyla çağırılabilecek şekilde programlanmayacaktır. Gerekli olduğu durumda parolalar, Bilgi İşlem bölümünün yetkisiz erişimleri engellemek için onayladığı bir şifreleme yazılımı kullanılarak saklanmalıdır.

Açıklamalar/Notlar: Parolalar şifrelenmemiş olarak tutuldukları bilgisayar veri dosyalarından, toplu komut dosyalarından, uçbirim işlev tuşlarından, giriş dosyalarından, makro ya da yazı programlarından veya FTP sitelerinin parolalarını içeren herhangi bir veri dosyasından bir saldırgan tarafından kolaylıkla bulunup çıkarılabilir.

Dışarıdan Çalışanlar İçin Kurallar

Dışarıdan çalışanlar, şirket güvenlik duvarının dışındadırlar ve bu nedenle saldırılara açıktırlar. Bu kurallar toplum mühendisinin dışarıdan çalışan personelinizi verilerinize açılan bir kapı olarak kullanmasını önlemenize yardımcı olacaktır.

16-1 Küçük istemciler

Kural: Uzaktan erişim yetkisine sahip tüm şirket çalışanları şirket ağına bağlanmak için küçük istemci kullanmalıdırlar.

Açıklamalar/Notlar: Bir saldırgan, saldırı stratejisini kurarken, dışarıdan şirket ağına erişimi olan kullanıcıları bulmaya çalışır. Bu nedenle dışarıdan çalışanlar başlıca hedefleri oluştururlar. Bu kişilerin bilgisayar-

larında sıkı güvenlik kontrollerinin olma olasılığı zayıftır ve bu, şirket ağına girebilecek açık bir nokta bırakır.

Güvenilir bir ağa bağlanan herhangi bir bilgisayar, klavye girişlerini kaydeden programlarla tuzaklanabilir ya da bağlantıları kaçırılabilir. Bir küçük istemci stratejisi sorunları çözmek için kullanılabilir. Küçük istemci, sürücüsü olmayan bir bilgisayar ya da bir monitör gibidir. Uçbirim gibi çalışan bu bilgisayarda gerekli saklama ortamları yoktur ancak buna karşılık işletim sistemi, uygulama programları ve tüm veriler şirket ağında durur. Küçük istemci üzerinden ağa erişilmesi, yamalanmamış sistemlerin, eskimiş işletim sistemlerinin ve kötü huylu programların oluşturduğu riski büyük ölçüde azaltmaktadır. Aynı zamanda dışarıdan çalışanların güvenliğini sağlamak da merkezi güvenlik kontrolleri sayesinde daha kolay ve etkili olur. Güvenlik konularıyla tam anlamıyla ilgilenmek konusunda işi deneyimsiz kullanıcılara bırakmaktansa bu tarz yükümlülükler eğitimli ağ ya da sistem yöneticilerine bırakılmalıdır.

16-2 Dışarıdan çalışanların bilgisayarları için güvenlik yazılımları

Kural: Şirket ağına bağlanmak için kullanılan herhangi bir harici bilgisayar sisteminde virüs ve Truva Atı koruma programları ve (donanımdan ya da yazılımdan gelen) kişisel bir güvenlik duvarı bulunmalıdır. Virüs ve Truva Atı tanım dosyaları en azından haftalık olarak yenilenmelidir.

Açıklamalar/Notlar: Genellikle dışarıdan ve evden çalışanlar güvenlik konularında bilgili değillerdir ve dikkatsizlik ya da ihmalkârlıkla bilgisayar sistemlerini ya da şirket ağlarını saldırıya açık bırakabilirler. Bu nedenle dışarıdan çalışanlar düzgün bir şekilde eğitilmezlerse ciddi bir güvenlik tehdidi oluşturmaktadırlar. Kötü huylu yazılımlara karşı korunmak için virüsten ve Truva Atından korunma programlarının yüklenmesine ek olarak, saldırganların çalışanlara sunulan herhangi bir hizmete dışarıdan erişebilmelerini engellemek için de bir güvenlik duvarı şarttır.

Microsoft'a yapılan bir saldırının da gösterdiği gibi, kötü huylu yazılımların çoğalmasına karşı en elzem güvenlik teknolojilerini kullanmamanın riski hafife alınmamalıdır. Dışarıdan çalışan bir Microsoft çalışanının bilgisayar sistemine bir Truva Atı bulaşır. Saldırgan ya da saldırganlar çalışanın güvenilir ağını kullanarak geliştirme kaynak kodlarını çalmak için Microsoft'un geliştirme ağına girebilmişlerdir.

İnsan Kaynakları Kuralları

İnsan kaynakları bölümlerinin, kendi çalışma ortamları aracılığıyla kişisel bilgileri elde etmeye çalışanlara karşı personeli korumak konusunda özel bir görevleri vardır. İnsan Kaynakları çalışanlarının aynı zamanda şirketlerini mutsuz eski çalışanlara karşı koruma sorumlulukları da vardır.

17-1 Ayrılan çalışanlar

Kural: Ne zaman bir çalışan şirketten ayrılır ya da ilişkisi kesilirse, insan kaynakları hemen aşağıdaki işlemleri yerine getirmelidir:

- Çevrimiçi telefon rehberinden kişinin adını çıkarmalı ve sesli mesajlarını iptal etmeli ya da yönlendirmelidir.
- Bina girişlerinde ya da şirket lobilerinde görevli personeli bilgilendirmelidir.
- Çalışanın adını ayrılan çalışanlar listesine eklemeli ve bu liste, sıklığı bir haftadan daha az olmayacak şekilde tüm çalışanlara gönderilmelidir.

Açıklamalar/Kurallar: Bina girişlerinde görevli çalışanlar eski bir çalışanın binaya yeniden girmesini önlemek üzere uyarılmalıdırlar. Ayrıca, diğer çalışanların da uyarılması eski çalışanın halen çalışıyormuş gibi davranarak başkalarını şirkete zarar verebilecek hareketlerde bulunmaları doğrultusunda kandırmasını önleyecektir.

Bazı koşullarda eski çalışanla aynı bölümde çalışan herkesin parolalarını değiştirmelerinin istenmesi gerekli olabilir. (Yalnızca bilgisayar korsanlığı konusundaki ünüm nedeniyle GTE'deki işime son verildiğinde şirket tüm çalışanların parolalarını değiştirmelerini zorunlu tutmuştu.)

17-2 Bilgi İşlem bölümünün uyarılması

Kural: Şirkette çalışan bir kişi işten ayrıldığında ya da işine son verildiğinde insan kaynakları, eski çalışanın, aralarında veri tabanı erişimi, uzaktan bağlantı ya da uzak noktalardan internet erişimi hesaplarının da bulunduğu tüm bilgisayar hesaplarını iptal etmesi için bilgi işlem bölümünü hemen haberdar etmelidir.

Açıklamalar/Notlar: Eski bir çalışanın işle ilişiği kesilir kesilmez tüm bilgisayar sistemlerine, ağ araçlarına, veritabanlarına ya da herhangi bir bilgisayar donanımına erişiminin derhal kesilmesi önemlidir. Aksi durumda şirket kin dolu bir çalışanın şirket bilgisayar sistemlerine girip ciddi zararlar verebilmesi için kapıyı ardına kadar açık bırakmış olur.

17-3 İşe alma sürecinde kullanılan gizli bilgiler

Kural: İlanlar ve iş boşluklarını doldurmak için uygun aday bulmaya yönelik diğer herkese açık davetler mümkün olduğu ölçüde şirketin kullandığı bilgisayar donanım ve yazılımları konusunda bilgi vermemelidir.

Açıklamalar/Notlar: Yöneticiler ve insan kaynakları personeli yalnızca nitelikli adayların özgeçmişlerini almaya yetecek kadar şirket bilgisayar donanım ve yazılımları hakkında bilgi vermelidirler.

Bilgisayar korsanları açık iş listelerini bulmak için gazeteleri ve şirket basın açıklamalarını okurlar, İnternet sayfalarına girerler. Çoğu zaman

şirketler, müstakbel çalışanları çekebilmek için kullandıkları donanım ve yazılımlarla ilgili çok fazla ayrıntı açıklamaktadırlar. Saldırgan, hedefinin Bilgi İşlem sistemleriyle ilgili bir bilgiyi bir kez ele geçirdi mi, saldırının bir sonraki adımı için hazır demektir. Örneğin, bir şirketin VMS işletim sistemi kullandığını öğrenen bir saldırgan sistemin hangi sürüm olduğunu öğrenmek için birkaç yeri arayabilir ve sonra da yazılım şirketinden geliyor gibi sahte bir acil güvenlik yaması gönderebilir. Yama bir kez yüklendikten sonra saldırgan sisteme girer.

17-4 Çalışanların kişisel bilgileri

Kural: İnsan kaynakları bölümü, çalışanın ya da insan kaynakları yöneticisinin yazılı onayı olmadan halen çalışan ya da çalışmayan hiçbir personel, taşeron, danışman, geçici işçi ya da stajyerin kişisel bilgilerini açıklamamalıdır.

Açıklamalar/Notlar: İnsan avcıları, özel dedektifler ve kimlik hırsızları, kimlik numaraları, doğum tarihleri, ücret bilgileri, aralarında banka hesap numaraları ve sağlık yardımları gibi bilgilerin de olduğu malî verileri içeren kişisel çalışan bilgilerini hedeflerler. Toplum mühendisi ilgili birey gibi davranabilmek amacıyla bu bilgileri elde edebilir. Ayrıca yeni işe başlayanların adlarının açıklanması da bilgi hırsızlarının çok işine yarayabilir. Yeni işe başlayanlar eski olduklarını, yetkili olduklarını ya da şirket güvenliğinden olduklarını iddia eden kişilerden gelen talepleri yerine getirmeye daha eğilimlidirler.

17-5 Sicil taramaları

Kural: Kendilerine bir iş önerilmeden ya da sözleşmeye dayanan bir iş ilişkisine girmeden önce tüm yeni işe başlayanlar, taşeronlar, danışmanlar, geçici işçiler ya da stajyerler için bir sicil taraması zorunlu olmalıdır.

Açıklamalar/Notlar: Maliyetler göz önüne alındığında sicil taramaları güven teşkil etmesi gereken belirli konumlarla sınırlı tutulabilir. Ancak şirket odalarına girme hakkı tanınmış herhangi birinin olası bir tehdit oluşturabileceği de unutulmamalıdır. Örneğin, temizlik ekiplerinin personel odalarına girme hakkı vardır ve bu onlara orada bulunan bilgisayar sistemlerine girme hakkını da verir. Fiziksel olarak bir bilgisayara erişim elde eden bir saldırgan parolaları yakalamak için bir dakikadan kısa bir süre içerisinde klavye girişlerini kaydeden bir programı bilgisayara yükleyebilir.

Bilgisayar korsanları hedef şirketin bilgisayar sistemlerine ve ağına girebilmek için şirkette iş bulma yoluna bile gidebilirler. Bir saldırgan, hedef şirketteki sorumlu kişiyi arayarak şirketin çalıştığı temizlik şirketinin adını kolaylıkla elde edebilir ve iş teklifiyle gelmiş bir temizlik firması olduğunu söyleyerek bu hizmeti vermekte olan şirketin adını öğrenir.

Fiziksel Güvenlik Kuralları

Her ne kadar toplum mühendisleri hedeflemek istedikleri bir işyerinde şahsen bulunmaktan kaçınsalar da zaman zaman bulunduğunuz mekâna da gireceklerdir. Bu kurallar fiziksel ortamınızı tehditlerden korumanıza yardımcı olacaktır.

18-1 Personel olmayanların kimlik tespiti

Kural: Kuryeler ve düzenli olarak şirket binalarına girmeleri gereken, şirket dışından kişilerin şirket güvenliğinin belirlediği kurallara uygun olarak düzenlenmiş özel yaka kartları ya da benzeri bir kimlikleri olmalıdır.

Açıklamalar/Notlar: Düzenli olarak binalara girmesi gereken personel olmayan kişilere (örneğin, kafeteryaya yiyecek ve içecek getirenlere, telefon bağlantılarını yapanlara ya da fotokopi makinalarını tamir edenlere) bu amaçla çıkarılmış özel bir şirket kimlik belgesi verilmelidir. Ara sıra girmesi gereken ya da bir kerelik işi olan kişiler ziyaretçi olarak değerlendirilmeli ve her zaman yanlarında bir refakatçi bulundurulmalıdır.

18-2 Ziyaretçi kimlik tespiti

Kural: Tüm ziyaretçiler içeri alınabilmeleri için geçerli bir sürücü ehliyeti ya da başka bir resimli kimlik belgesi göstermelidirler.

Açıklamalar/Notlar: Güvenlik görevlileri ya da danışma memuru ziyaretçi kartı vermeden önce kimlik belgesinin bir fotokopisini almalı ve bu kopya ziyaretçi defterinde saklanmalıdır. Diğer bir seçenek ise kimlik bilgilerinin danışma memuru ya da güvenlik görevlisi tarafından ziyaretçi defterine kaydedilmesidir. Ziyaretçilerin kimlik bilgilerini kendilerinin girmesine izin verilmemelidir.

Bir binaya girmeye çalışan toplum mühendisleri deftere her zaman yanlış bilgi gireceklerdir. Her ne kadar sahte bir kimlik elde etmek ve ziyaret edileceği söylenen kişinin adını öğrenmek zor olmasa da çalışanın girişleri kaydetmesini zorunlu tutmak güvenlik sürecini bir kademe daha artırmaktadır.

18-3 Ziyaretçilere eşlik edilmesi

Kural: Ziyaretçiler her zaman bir çalışanın eşliğinde olmalı ya da yanlarında refakatçi bulunmalıdır.

Açıklamalar/Notlar: Toplum mühendislerinin çevirmeyi sevdikleri dolaplardan biri de, bir şirket çalışanını ziyaret etmektir (örneğin, stratejik ortaklığın olduğu bir firmadan geldiğini söyleyerek ürün mühendisini ziyaret etmek gibi). İlk görüşmeye refakatçi eşliğinde gittikten sonra toplum mühendisi konuştuğu kişiyi kendi başına lobiye dönebileceği

konusunda ikna eder. Bu yöntemle binayı serbestçe dolaşma fırsatı elde eder ve büyük olasılıkla hassas bilgilere ulaşabilir.

18-4 Geçici kimlikler

Kural: Başka bir tesisten gelen ve yanlarında personel kartları bulunmayan şirket çalışanları geçerli bir sürücü ehliyeti ya da benzeri resimli bir kimlik göstermeli ve onlara geçici bir ziyaretçi kartı verilmelidir.

Açıklamalar/Notlar: Saldırganlar şirkete girebilmek için sık sık şirketin başka bir binasından ya da şubesinden gelen çalışanlar gibi davranırlar.

18-5 Acil tahliye

Kural: Acil bir durumda ya da bir talim sırasında güvenlik görevlileri herkesin binaları terkettiğinden emin olmalıdırlar.

Açıklamalar/Notlar: Güvenlik görevlileri tuvaletlerde ya da odalarda geride kalmış olabilecek kişiler olup olmadığını kontrol etmelidirler. İtfaiyenin ya da ortaya çıkan durumda yetkili olan diğer kurumların da belirttiği üzere güvenlik kuvvetleri tahliyeden çok sonra binayı terk eden kişilere karşı uyanık olmalıdırlar.

Sanayi casusları ya da deneyimli bilgisayar korsanları bir binaya ya da güvenli bir alana girebilmek için yanlış alarm verebilirler. Kullanılan hilelerden biri havaya 'Butil Merkaptan' adında zararsız bir gaz vermektir. Çalışanlar tahliye işlemine başladıktan sonra gözü kara saldırgan bu fırsatı ya bilgi çalmak için ya da şirket bilgisayar sistemine girmek için kullanır. Bilgi hırsızlarının kullandığı başka bir taktik de, bazen tuvalette bazen bir odada, tam tahliye taliminin başladığı saatte ya da acil tahliyeye neden olacak sis bombası ya da başka bir gereç kullandıktan sonra geride kalmaktır.

18-6 Posta odasında ziyaretçiler

Kural: Bir şirket çalışanının gözetiminde olmadan hiçbir ziyaretçinin posta odasına girmesine izin verilmemelidir.

Açıklamalar/Notlar: Bu kuralın amacı dışardan birinin şirket içi postaları karıştırmasını, göndermesini ya da çalmasını önlemektir.

18-7 Araç plaka numaraları

Kural: Eğer şirketin bekçili bir otoparkı varsa, güvenlik görevlileri bu alana giren tüm araçların plakalarını not etmelidirler.

18-8 Çöp bidonları

Kural: Çöp bidonları her zaman şirket alanın içinde bulunmalı ve dışarıdan erişilebilir olmamalıdır.

Açıklamalar/Notlar: Bilgisayar saldırganları ve sanayi casusları şirket çöplerinden değerli bilgiler elde edebilirler. Mahkemeler çöpleri yasal olarak terk edilmiş mal olarak değerlendirirler ve bu yüzden bidonlar herkese açık bir alanda durdukları sürece çöp dalışları tamamiyle yasaldır. Bu nedenle çöplerin, şirketin, bidonları ve içindekileri koruma hakkının olduğu şirket alanı içinde tutulmaları önemlidir.

Danışma Görevlileri İçin Kurallar

Danışma görevlileri, iş toplum mühendisleriyle uğraşmaya geldiğinde çoğu zaman ön cephededirler. Ancak onlara nadiren bir saldırganı fark edip durdurabilmelerini sağlayacak eğitimler verilir. Danışma görevlinizin şirketinizi ve verilerini daha iyi koruyabilmesi için bu kuralları yürürlüğe koyun.

19-1 Dahili telefon rehberi

Kural: Dahili telefon rehberinde açıklanan bilgilere yalnızca şirket çalışanları erişebilmelidir.

Açıklamalar/Notlar: Rehberde bulunan tüm unvanlar, adlar, telefon numaraları ve adresler dahili bilgi olarak değerlendirilmeli ve yalnızca veri sınıflandırma kuralları ve dahili bilgilere yönelik kurallar doğrultusunda verilmelidir.

Ayrıca arayan tarafın elinde, ulaşmaya çalıştığı kişinin adı ya da dahili numarası olmalıdır. Arayanın dahili numarayı bilmediği bir durumda her ne kadar danışma görevlisi gerekli bağlantıyı sağlasa da arayana dahili numarayı vermesi yasak olmalıdır (Örnek: İsteyen meraklılar, herhangi bir Birleşik Devletler devlet dairesini arayıp santral memuruna dahili numarayı sorarak bu süreci deneyebilirler.).

19-2 Belirli bölümlerin/grupların telefon numaraları

Kural: Çalışanlar, arayanın geçerli bir nedeni olup olmadığını kontrol etmeden, şirket yardım masasının, telekomünikasyon bölümünün, bilgi işlemin ya da sistem yöneticisinin dış hat telefon numaralarını vermemelidirler. Danışma görevlisi, bu gruplardan birine bir telefon aktarırken arayanın adını mutlaka açıklamalıdır.

Açıklamalar/Notlar: Bazı kuruluşlar bu kuralı fazla baskılayıcı bulsalar da, bu kural bir toplum mühendisinin çalışan gibi davranıp başkalarını kendi dahili numaralarından yönlendirme yapmaları için kandırmasını (bazı telefon sistemlerinde bu işlem, aramanın şirket içinden yapılıyormuş gibi görünmesini sağlar) ya da kendini kanıtlayabilmek için kurbanına bu numaraları bildiğini göstermesini güçleştirir.

19-3 Bilgi aktarımı

Kural: Santral memurları ve danışma görevlileri, çalışan olup olmadığını şahsen bilmedikleri kişiler adına not almamalı ya da bilgi aktarmamalıdır.

Açıklamalar/Notlar: Toplum mühendisleri, dikkatsizlik gösterip kendilerine kefil olmaları için çalışanları kandırmak konusunda ustadırlar. Toplum mühendisliği hilelerinden biri, danışmanın numarasını elde edip, danışma görevlisine kendisi için bırakılmış mesaj olup olmadığını sormaktır. Daha sonra kurbanını ararken saldırgan, bir çalışan gibi davranır ve hassas bir bilgi verilmesini ya da bir işlem yapılmasını isteyerek ana santral numarasını geri arama numarası olarak verir. En sonunda saldırgan danışma görevlisini arar ve hiçbir şeyden kuşkulanmayan kurbanın kendisi için bıraktığı mesajı alır.

19-4 Alınmak üzere bırakılmış malzemeler

Kural: Bir kuryeye ya da tanımlanmamış başka bir kişiye herhangi bir şey verirken, danışma görevlisi ya da güvenlik görevlisi resimli bir kimlik görmeli ve kimlik bilgilerini kuralların öngördüğü şekilde kayıt defterine işlemelidir.

Açıklamalar/Notlar: Toplum mühendisliği taktiklerinden biri de, hassas malzemeleri danışma görevlisine ya da danışma masasına bıraktırarak güya yetkili olan bir başka çalışana vermesi için bir çalışanı kandırmaktır. Danışma görevlisi ya da güvenlik görevlisi de, doğal olarak paketin alınmasının sakıncalı olmadığını düşünür. Toplum mühendisi ya kendisi gelir ya da paketi alması için bir kurye hizmetinden yararlanır.

Olay Bildirme Grubu İçin Kurallar

Her şirket, şirket güvenliğine yönelik herhangi bir saldırı fark edildiğinde aranmak üzere merkezi bir gurup oluşturmalıdır. Aşağıda bu grubun faaliyetlerinin düzenlenmesi ve yapılandırılmasına yönelik birkaç yol gösterici kural bulacaksınız.

20-1 Olay bildirme grubu

Kural: Bir kişi ya da gurup bu iş için görevlendirilmeli ve çalışanlar güvenlikle ilgili olayları onlara iletmek üzere bilgilendirilmelidir.

Açıklamalar/Notlar: Çalışanlar bir güvenlik tehdidini nasıl ayırt edeceklerini bilmeli ve oluşacak herhangi bir tehdidi ilgili olay bildirme grubuna bildirecek şekilde eğitilmelidir. Bir tehdit oluştuğunda böyle bir gurubun harekete geçebilmesi için kuruluşun belirli süreçler ve yetkiler belirlemesi de önemlidir.

20-2 Sürmekte olan saldırılar

Kural: Olay bildirme gurubuna, sürmekte olan bir toplum mühendisliği saldırısı bildirildiğinde gurup, hedeflenen bölümlerde görevli ve bu iş için belirlenmiş çalışanları uyarmak üzere süreçleri başlatacaktır.

Açıklamalar/Notlar: Olay bildirme gurubu ya da sorumlu yönetici, şirket çapında bir uyarı gönderilip gönderilmeyeceğine de karar vermelidir. Sorumlu kişi ya da gurubun, bir saldırının devam ettiğine inancı tamsa, şirket çalışanlarını tetikte olmaları konusunda uyararak zararı en aza indirmek başlıca öncelikleri olmalıdır.

BİR BAKIŞTA GÜVENLİK

Aşağıda verilen listeler ve şemalar ikinci bölümden on dördüncü bölümün sonuna kadar anlatılan toplum mühendisliği yöntemlerinin ve on altıncı bölümde ayrıntılandırılan onay süreçlerinin bir bakışta görülebileceği bir başvuru kılavuzu oluşturmaktadır. Bu bilgileri kurumunuza uyarlayın ve bir bilgi güvenliği sorunu ortaya çıktığı zaman çalışanlarınızın başvurabilmesi için herkese duyurun.

Bir Saldırının Belirlenmesi

Bu tablolar ve kontrol listeleri bir toplum mühendisliği saldırısını tespit etmenize yardımcı olacaklardır.

Toplum mühendisliği döngüsü

HAREKET	ACIKLAMA
Araştırma	Aralarında güvenlik delme testi kayıtları, yıllık raporlar, pazarlama broşürleri, patent uygulamaları, basın kupürleri, sektör dergileri, internet sayfası içeriği olabilir. Ayrıca çöp dalışları da olabilir.
Dostluk ve güven uyandırma	İçeriden gelen bilgilerin kullanılması, başkasının kimliğine bürünme, kurbanın tanıdığı kişilerin adlarının sıralanması, yardım isteği ya da otoriteye sahip olma.
Güveni kötüye kullanma	Kurbandan, bir bilgi vermesinin ya da bir işlem yapmasının istenmesi. Ters dalaverede kurban, saldırgandan yardım ister.
Bilgi kullanma	Eğer edinilen bilgi asıl amaçtan bir adım uzaktaysa, saldırgan, amacına ulaşana kadar döngüdeki önceki adımlara geri döner.

En Çok Kullanılan Toplum Mühendisliği Yöntemleri

- Bir çalışan gibi davranmak.
- Bir satıcı firmanın, ortak iş yürütülen bir şirketin ya da güvenlik güçlerinin bir personeli gibi davranmak.
- Yetkili biri gibi davranmak.

- Yardıma ihtiyacı olan, işe yeni girmiş biri gibi davranmak.
- Bir sistem yaması ya da güncellemesi sunmak için arayan bir satıcı ya da sistem üreticisi gibi davranmak.
- Sorun çıktığı takdirde yardım edebileceğini söyleyip sonra sorunu kendisi yaratmak ve böylece kurbanın yardım istemek için kendisini aramasını sağlamak.
- Kurbanın yüklemesi için bedava yazılım ya da yama göndermek.
- E-posta ekinde virüs ya da Truva Atı göndermek.
- Kullanıcının yeniden bağlanmasını ya da parola girmesini isteyen sahte bir pencere kullanmak.
- Gözden çıkarılmış bir bilgisayar sistemi ya da programıyla, kurbanın klavyeden yaptığı girişleri kaydetmek.
- İçinde kötü huylu yazılım bulunan CD'leri işyerinde görünür bir şekilde bırakmak.
- Güven kazanmak için şirket içi terimleri kullanmak.
- Şirket içi teslimata girmesi için posta odasına bir belge ya da dosya bırakmak.
- İçerden gönderildiği izlenimini verebilmek için faks makinasının başlığını değiştirmek.
- Danışma görevlisinden, alacağı faksı başka bir yere fakslamasını rica etmek.
- Bir dosyanın şirket içi gibi görünen bir yere gönderilmesini istemek.
- Geri aramalarda şirket mensubu gibi görünecek şekilde bir sesli mesaj kutusu oluşturmak.
- Şehir dışındaki bir ofisten geldiğini söyleyip bulunduğu yerden e-postalarını okuyabilmeyi istemek.

Bir Saldırının Uyarı Sinyalleri

- Bir geri arama numarası vermekten kaçınılması.
- Sıradışı taleplerde bulunulması.
- Yetkili olunduğunun öne sürülmesi.
- Aciliyetin üzerine vurgu yapılması.
- İsteğin yerine getirilmemesi durumunda kötü sonuçlar doğacağının söylenmesi.
- Soru sorulduğunda rahatsız olunması.
- Bilinen adların sıralanması.
- İltifat edilip pohpohlanma.
- Kur yapılması.

Saldırılarda en sık görülen hedefler

HEDEF TÜRÜ	ÖRNEKLER
Bilginin değerinden habersiz olanlar	Danışma görevlileri, santral memurları, idarî yardımcılar, güvenlik görevlileri.
Özel ayrıcalıklara sahip olanlar	Yardım masası ya da teknik destek, sistem yöneticileri, bilgisayar operatörleri, telefon sistemleri yöneticileri.
Üretici/Satıcı firmalar	Bilgisayar donanımı ve/veya yazılım üreticileri, sesli mesaj sistemleri satıcıları.
Belli bölümler	Muhasebe, insan kaynakları.

Şirketleri Saldırılara Açık Duruma Getiren Unsurlar

- Çok sayıda çalışan olması.
- Birden fazla tesis bulunması.
- Çalışanın nerede olduğuyla ilgili sesli mesajlarda bilgi verilmesi.
- Dahili telefon numarasının verilmesi.
- Güvenlik eğitimlerinin yetersizliği.
- Veri sınıflandırma sisteminin bulunmaması.
- Bir olay bildirme ya da karşı eylem planının yürürlükte olmaması.

Onaylama ve Veri Sınıflandırma

Bu tablolar ve şemalar toplum mühendisliği saldırısı olabilecek bilgi ya da işlem taleplerine karşılık vermenize yardımcı olacaklardır.

Kimlik Tespiti Yapılma Süreci

HAREKET	TANIM
Arayan kimliğinin belirlenmesi	Gelen aramanın dahili olup olmadığını ve görünen numaranın ya da adın, arayanın kimliğiyle uyuşup uyuşmadığını kontrol edin.
Geri arama	İstek sahibini şirket telefon rehberinden bulup, rehberde geçen numaradan onu geri arayın.
Kefil olma	Güvenilir bir çalışandan istek sahibine kefil olmasını isteyin.
Paylaşılan ortak anahtar	Bir parola ya da günlük şifre gibi şirket içinde kullanılan ortak anahtarı talep edin.

HAREKET	TANIM *(Tablonun devamı)*
Müdür ya da yönetici	Çalışanın bir üst yöneticisini arayın ve kimliğinin ve çalışma durumunun onaylanmasını isteyin.
Güvenli e-posta	Dijital olarak imzalanmış bir mesaj talep edin.
Kişisel ses tanımlama	Çalışanın tanıdığı biri arıyorsa sesinden tanımaya çalışın.
Değişken parolalar	Güvenli kimlik ya da başka bir güçlü tanımlama aracı kullanarak değişken parola çözümlerine başvurun.
Şahsen görme	İstek sahibinin personel kartıyla ya da başka bir kimlik belgesiyle şahsen gelmesini isteyin.

Çalışma Durumunun Onaylanma Süreci

HAREKET	ACIKLAMA
Şirket telefon rehberinden kontrol	Çevrimiçi rehberde istek sahibinin adının geçip geçmediğini kontrol edin.
İstek sahibinin yöneticisinin onayı	Şirket rehberinde geçen numarayı kullanarak istek sahibinin yöneticisini arayın.
İstek sahibinin bölümünün ya da iş grubunun onayı	İstek sahibinin bölümünü ya da iş grubunu arayarak kişinin halen şirkette çalışıp çalışmadığını kontrol edin.

Bilme Gereğini Kontrol Süreci

HAREKET	TANIM
Unvan/iş grubu/sorumluluklar listelerine başvurun	Belli gizli bilgilere hangi çalışanların erişim hakkı olduğunu öğrenmek için önceden yayınlanmış şirket içi listelere başvurun.
Yöneticiden yetki alın	Kendi yöneticinizi ya da istek sahibinin yöneticisini arayıp isteği yerine getirmek için onay isteyin.
Bilgi sahibinden ya da yedek sorumludan yetki alın	Bilgi sahibinden istekte bulunan kişinin bilme gereği olup olmadığını öğrenin.
Otomatik bir araç kullanarak yetki alın	Yetkili personel için tescilli yazılım veri tabanlarına bakın.

Şirket Çalışanı Olmayanları Belirlemek İçin Kriterler

KRİTER	HAREKET
İlişki	İstekte bulunan kişinin çalıştığı firmanın bir satıcı, stratejik ortak ya da başka bir iş ilişkisi olan firma olduğundan emin olun.
Kimlik	İstek sahibinin kimliğini ve iş durumunu satıcı/ortak firmadan öğrenin.
Açığa vurmama	İstek sahibinin yürürlükte olan bir açığa vurmama anlaşması imzaladığından emin olun.
Erişim	Bilgi, dahili veya daha üst derece olarak sınıflandırılmışsa talebi yönetime gönderin.

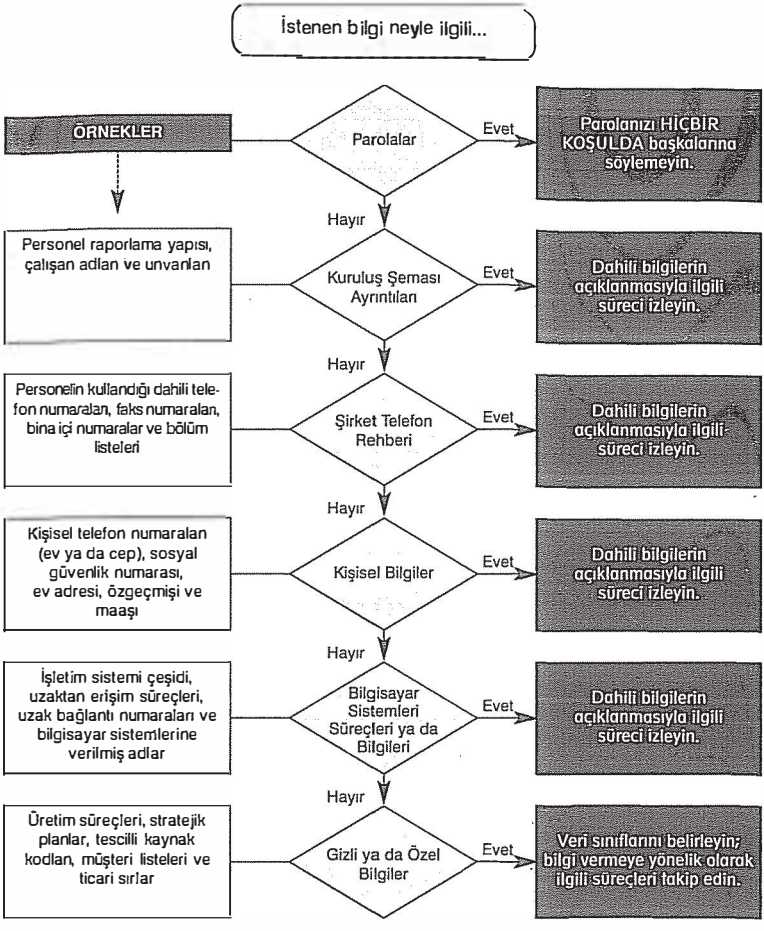
Veri Sınıflandırma

SINIFLANDIRMA	AÇIKLAMA	SÜREÇ
Genel	Herkese serbestçe verilebilir.	Onaylanmaya gerek yoktur.
Dahili	Şirket içi kullanım içindir.	Şirket çalışanlarının halen çalışıp çalışmadıklarının kontrolü ya da şirket çalışanı olmayanlar için yürürlükte bir açığa vurmama anlaşmasının olması ve yönetici onayının alınması.
Özel	Yalnızca kurum içinde kullanılmak üzere belirlenmiş kişisel nitelikli bilgiler.	İstek sahibinin faal bir çalışan ya da dışardan yetkili bir kişi olduğunun onaylanması. Yetkili çalışanlara ya da dışardan gelen taleplere özel bilgiler vermeden önce insan kaynaklarından kontrol edilmesi.
Gizli	Kurum içinde yalnızca kesinlikle bilmesi gereken kişilerce bilinen bilgiler.	İlgili bilgi sahibine istekte bulunan kişinin kimliğini ve bilme gereğini onaylatın. Yalnızca yöneticinin, bilgi sahibinin ya da sorumlusunun yazılı izniyle isteği yerine getirin. Yürürlükte olan bir açığa vurmama anlaşması olup olmadığını kontrol edin. Şirket mensubu olmayan kişilere yalnızca yöneticier açıklama yapabilir.

Bilgi Talebine Karşılık Vermek

Altın Sorular

Bu kişinin söylediği kişi olduğunu nasıl bilebilirim?
Bu kişinin böyle bir istekte bulunmak için yetkili olup olmadığını nasıl öğrenebilirim?

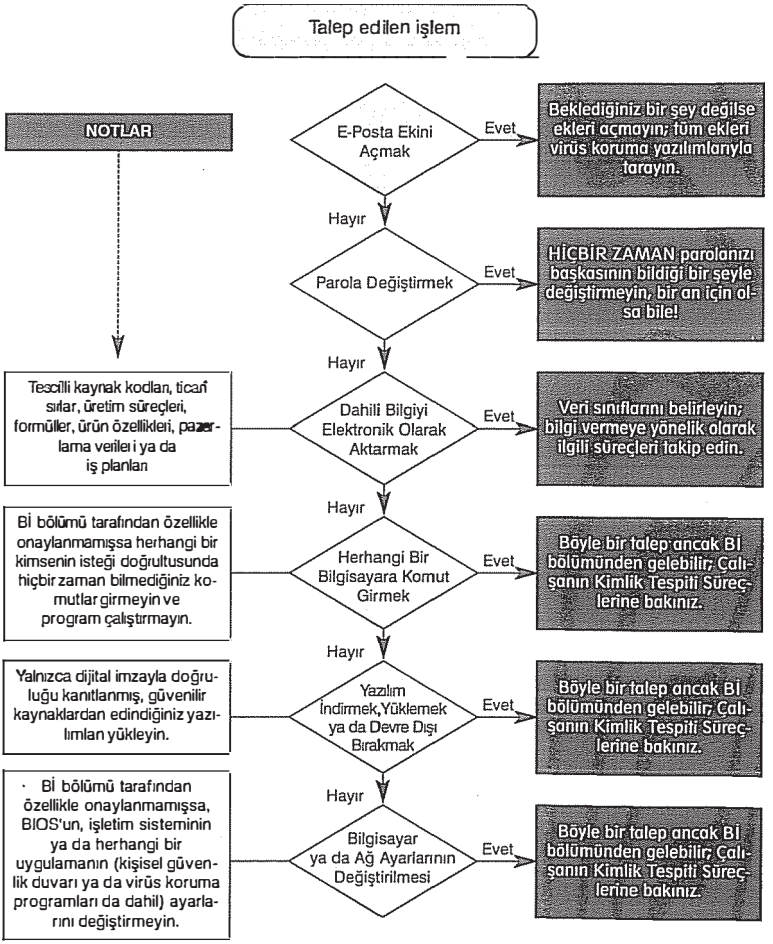


Genel olarak sınıflandırılmadığı sürece tüm bilgiler hassas olarak nitelendirilir.

İşlem Talebine Karşılık Vermek

Altın Kurallar

Kimlik tespiti yapılmadan kimseye güvenilmemelidir.
Gelen taleplerin sorgulanması teşvik edilmelidir.



Başkaları adına yaptığınız tüm hareketler şirket varlıklarını tehlikeye sokacak durumlar yaratabilir.
Daima kontrol edin, kontrol edin, kontrol edin.

KAYNAKLAR

1. Bölüm

BloomBecker, Buck. 1990. *Spectacular Computer Crimes: What They Are and How They Cost American Business Half a Billion Dollars a Year.* Irwin Professional Publishing.

Littman, Jonathan. 1997. *The Fugitive Game: Online with Kevin Mitnick.* Little Brown & Co.

Penenberg, Adam L. April 19, 1999. "The Demonizing of a Hacker." Forbes.

2. Bölüm

Stanley Rifkin'in öyküsü aşağıdaki açıklamalara dayandırılmıştır:

Bilgisayar Güvenliği Enstitüsü, Tarihsiz, "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar." Basın açıklaması.

Epstein, Edward Jay. Yayınlanmamış. "The Diamond Invention."

Holwick, Rev. David. Yayınlanmamış açıklaması.

Bay Rifkin, kendisiyle röportaj yapılması taleplerini geri çevirerek adını saklı tutma hakkını koruduğu için, yaptığı işle ilgili yapılan açıklamalarda farklılıklar olduğunu doğrulama nezaketini göstermiştir.

16. Bölüm

Cialdini, Robert B. 2000. *Influence: Science and Practice, 4th edition.* Allyn and Bacon.

Cialdini, Robert B. February 2001. "The Science of Persuasion." *Scientific American.* 284:2.

17. Bölüm

Bu bölümdeki bazı kurallar aşağıda adı geçen esere dayandırılmıştır:

Wood, Charles Cresson. 1999. "Information Security Policies Made Easy." Baseline Software.

TEŞEKKÜR

KEVIN MITNICK'TEN

Gerçek dostluk iki beden tek kafa olarak tanımlanır; pek çok insanın yaşamında gerçek dost diyebileceği biri yoktur. Jack Biello, ahlaksız gazetecilerin ve aşırı heyecanlı savcıların elinden çektiğim muazzam eziyete karşı çıkmış, sevgi dolu ve yardımsever bir insandı. "Kevin'e Özgürlük" hareketinin önde gelen isimlerindendi ve hükümetin bilinmesini istemediği bilgileri açığa çıkaran güçlü makaleler yazmakta sıradışı yeteneğe sahip bir yazardı. Jack her zaman korkusuzca yanımda oldu, konuşmaları ve yazıları hazırlarken hep benimle birlikte çalıştı ve bir noktada basın danışmanım olarak beni temsil etti.

Bu nedenle bu kitap, bu eseri bitirmek üzereyken yakın zamanda kanserden ölerek içimde büyük bir boşluk ve üzüntü yaratan sevgili dostum Jack Biello'ya adanmıştır.

Ailemin sevgisi ve desteği olmasaydı bu kitap gerçekleşmezdi. Annem Shelly Jaffe ve büyükannem Reba Vartanian tüm yaşamım boyunca benden koşulsuz sevgi ve desteklerini esirgemediler. En iyi arkadaşım olarak gördüğüm, böylesine iyi ve sadık bir anne tarafından yetiştirildiğim için çok şanslıyım. Büyükannem bana ikinci bir anne gibi olmuş ve yalnızca bir annenin gösterebileceği şefkat ve ilgiyi göstermişti. Yardımsever ve şefkatli insanlar oldukları için başkalarına yardım etmenin ve benden daha az şanslı olanlara destek olmanın ilkelerini bana öğretenler onlardı. Böylece vermek ve yardım etmek üzerine kurulu bir şemayı taklit ederek, bir bakıma onların yaşamları için çizdikleri yolu izlemiş oldum. Umarım bu kitabın yazılışı sırasında teslim tarihlerine yetiştirilmesi gereken işleri bahane ederek onları görme fırsatını kaçırdığım ve onları ikinci plana ittiğim için beni affedebilirler. Bu kitap her zaman kalbimde tutacağım kişilerin sürekli sevgisi ve desteği olmadan mümkün olmazdı.

Kitabın kitapçılarda satışa sunulduğu ilk gün babam Alan Mitnick'in ve kardeşim Adam Mitnick'in de benimle şampanya patlatacak kadar yaşamış olmalarını isterdim. Bir pazarlamacı ve iş adamı olarak babam bana hiçbir zaman unutmayacağım, yaşamın bazı ince noktalarını öğretti. Yaşamının son aylarında onun yanında olabildiğim için mutluyum, ancak bu, etkisini henüz üzerimden atamadığım çok zorlu bir deneyimdi.

Teyzem Chickie Leventhal'ın kalbimde her zaman çok özel bir yeri olacak. Yaptığım bazı aptalca hatalardan dolayı düş kırıklığına uğramış

olsa da, sevgi ve desteğini esirgemeyerek her zaman benim yanımda oldu. Kendimi bu kitabın yazılmasına adadığımdan, haftalık Sebt günü kutlamalarında kuzenim Mitch Leventhal ve erkek arkadaşı Dr. Robert Berkowitz'e katılma fırsatını kaçırdım.

Annemin erkek arkadaşı Steven Knittle'a, yanında olamadığım zamanlarda anneme gösterdiği sevgi ve destek için en içten teşekkürlerimi sunmalıyım.

Amcam ise en çok övgüyü hak eden kişidir. Toplum mühendisliği becerilerimi Mitchell amcamdan aldığım söylenebilir. Amcam, benim ustalaşmak bir tarafa, anlamaya bile yaklaşamayacağım bir şekilde tüm dünyayı ve üstünde yaşayan insanları nasıl yönlendireceğini bilirdi. Onun şansı, çekici kişiliğiyle istediğini etkileyebileceği yıllarda bendeki bilgisayar tutkusunun onda olmayışıydı. En yüce toplum mühendisi unvanını her zaman elinde tutacaktır.

Bu teşekkürleri yazarken, sevgilerini, dostluklarını ve desteklerini esirgemedikleri için teşekkür etmem ve minnettarlığımı dile getirmem gereken çok kişi olduğunu fark ettim. Son yıllarda tanıştığım iyi ve cömert insanların hepsinin adları bir anda aklıma gelmiyor ama hepsini bir yere sığdırabilmek için bir bilgisayara ihtiyacım olacağını söylemek yeterli olacaktır sanırım. Dünyanın her tarafından bana cesaret, övgü ve destek dolu sözler yazan pek çok insan oldu. Bu sözlerin benim için çok büyük anlamı vardı, özellikle de onlara en çok ihtiyaç duyduğum zamanlarda.

Yanımda olan ve değerli zamanlarını ve enerjilerini, bana yapılan haksız muameleye ve "Kevin Mitnick Efsanesi"nden kazanç sağlamak isteyenlerce ortaya atılan abartılı söylentilere karşı itirazlarını ve endişelerini dinleyecek herkese anlatarak harcayan tüm destekçilerime özellikle müteşekkirim.

Çok satan bir yazar olan Bill Simon'la bir ekip olarak çalışmak gibi olağanüstü bir fırsat elde ettim ve farklı çalışma zamanlarımıza karşın birlikte büyük bir gayretle çalıştık. Bill oldukça düzenli; erken kalkıyor ve amaçlarının bilincinde olarak, iyi planlanmış bir şekilde çalışıyor. Benim geceyarısı çalışma düzenime uyum sağladığı için Bill'e ayrıca teşekkür ederim. Bu projeye olan bağlılığım ve uzun çalışma saatlerim, Bill'in düzenli çalışma saatlerine ters düşecek şekilde beni sabahın erken saatlerine kadar ayakta tutmuştur.

Düşüncelerimi iyi bir okuyucuya layık cümlelere dökebilecek biriyle birlikte çalıştığım için çok şanslı olmamın yanı sıra, benim programcılara özgü ayrıntılara odaklanma huyuma karşı Bill (çoğu zaman) çok sabırlı davranan bir adamdı. Yine bu teşekkür bölümünde, benim ayrıntılara takılma eğilimim yüzünden uzun yazarlık kariyeri boyunca ilk ve tek olarak bir teslim tarihini geçirmesine neden olduğum için ondan özür

dilemek istiyorum. Onun, sonunda anlamayı ve paylaşmayı başardığım bir yazarlık onuru var; birlikte başka kitaplar da yazabilmeyi umuyoruz.

Rancho Santa Fe'de çalışmak için Simon ailesinin evinde bulunma mutluluğu ve Bill'in eşi Arynne tarafından şımartılmak, bu yazma projesinin en gözde zamanları arasında sayılabilir. Arynne'in sohbeti ve yemekleri hafızamdan asla silinmeyecek. Arynne, sıcaklık ve güzellik dolu bir yuva yaratmış, nitelikli, akıllı ve neşeli bir hanım. Aspartam'ın zararları konusunda bana verdiği nasihatler aklımın bir köşesinde çınlamadan sanırım bir daha diyet kola içemeyeceğim.

Stacey Kirkland benim için çok şey ifade ediyor. Zamanının çoğunu, düşüncelerime görsel destek sağlayacak şemaları ve grafikleri bilgisayarda tasarlamada bana yardım ederek geçirdi. Onun harika özelliklerini takdir ediyorum; yaşamdaki en iyi şeyleri hak eden, gerçekten iyi ve sevgi dolu biri. İlgili bir arkadaş olarak beni cesaretlendirdi. Kendisine çok değer veriyorum. Sağladığı tüm içten destek ve ihtiyacım olduğunda yanımda olduğu için ona teşekkür etmek istiyorum.

Nexspace'den Alex Kasper yalnızca en iyi arkadaşım değil, aynı zamanda iş ortağım ve meslektaşım. Los Angeles KFI AM 640 radyosunda Program Yönetmeni David G. Hall'ın becerikli rehberliğinde "İnternetin Karanlık Tarafı" adında internetle ilgili sevilen bir radyo programını birlikte yapmıştık. Alex, paha biçilmez yardım ve önerileriyle bu kitaba önemli katkılarda bulundu. Gece yarılarının da ötesine uzanan bir iyilik ve cömertlikle her zaman olumlu ve yardımsever bir etki bıraktı. Alex ve ben yakın zamanda işletmelerin çalışanlarını toplum mühendisliği saldırılarına karşı eğitmelerine yardımcı olacak bir film/video hazırladık.

Informed Decision şirketinden Paul Dryman bir aile dostundan çok daha öte biridir. Bu çok saygı duyulan ve güvenilir özel dedektif, arka plan araştırmaları yürütmedeki süreç ve eğilimleri anlamama katkıda bulundu. Paul'ün bilgisi ve deneyimi bu kitabın dördüncü bölümünde sözü edilen personel güvenlik konularını ifade etmemde de yardımcı oldu.

En iyi arkadaşlarımdan biri, Candi Layman sevgi ve desteğiyle sürekli arkamdaydı. Yaşamda en iyileri hak eden, gerçekten muhteşem bir insan. Hayatımın en acı günlerinde Candi her zaman beni cesaretlendirdi ve dostum olarak kaldı. Bu kadar harika, sevecen ve şefkatli bir insanla karşılaştığım için çok şanslıyım ve yanımda olduğu için ona teşekkür etmek istiyorum.

Aldığım ilk telif ücreti Erin Finn'le yaptığım konuşmalar karşılığında kesinlikle cep telefonu operatörüne gidecek. Hiç kuşkusuz Erin benim can yoldaşım. Bazı açılardan korkutucu bir şekilde birbirimize benziyoruz. İkimiz de teknolojiye aşığız; aynı yemek, müzik ve film zevklerini paylaşıyoruz. AT&T cep telefonu hizmetleri, onun Chicago'daki evini aramam için bana verdiği "bedava geceler ve haftasonları" tarifesinden

kesinlikle zarar ediyor olmalı. En azından artık Kevin Mitnick tarifesini kullanmıyorum. Erin'in bu kitaba yönelik inancı ve hevesi beni de heyecanlandırdı. Arkadaşım olduğu için çok şanslıyım.

Profesyonel yaşantımda bana yardımcı olan ve olağanüstü şekillerde kendilerini işlerine vermiş bazı kişilere teşekkür etmek için sabırsızlanıyorum. Konuşmalarımı (sevdiğim ve saydığım dürüst ve ilgili bir kişi olan) Amy Gray ayarlıyor; Waterside Yayıncılık'tan David Fugate telif hakları sözleşmesinin imzalanmasından önce ve sonra pek çok kere yardımıma koşan bir yayın menajeri; ve devlete karşı verdiğim, yıllar süren savaşta, savunma tarafında beni temsil eden ekipte bulunan Los Angeles'lı avukat Gregory Vinson. Ayrıntılara takılma huyuma karşı Bill kadar anlayışlı ve sabırlı olduğunu söylemekte eminim haklıyımdır. Adıma yazdığı yasal bilgilendirmelerle uğraşırken o da benzer deneyimler yaşadı.

Avukatlarla çok uğraştım ama adalet sistemiyle olumsuz ilişkilerimin olduğu yıllarda, çok ümitsiz bir durumdayken öne çıkıp bana yardım etmeyi teklif eden avukatlara teşekkürlerimi sunmak için bir fırsat kolluyordum. Tatlı sözlerden tutun da davamla yakından ilgilenmeye kadar, benmerkezli avukat tiplemesine uymayan pek çok avukatla tanıştım. O insanların bir karşılık beklemeden bana yaptıkları iyilikler ve cömert tutumlarına zamanla saygı duymaya, hayran kalmaya ve onları takdir etmeye başladım. Her biri de bir paragraf dolusu güzel sözle hatırlanmaya layıklar. Ama en azından hepsinin adını burada belirteceğim, çünkü her biri de şükranlarımla birlikte kalbimde yaşıyorlar: Greg Aclin, Bob Carmen, John Dusenbury, Sherman Ellison, Omar Figueroa, Carolyn Hagin, Rob Hale, Alvin Michaelson, Ralph Peretz, Vicki Podberesky, Donald C. Randolph, Dave Roberts, Alan Rubin, Steven Sadowski, Tony Serra, Richard Sherman, Skip Slates, Karen Smith, Richard Steingard, saygıdeğer hâkim Robert Talcott, Barry Tarlow, John Yzurdiaga ve Gregory Vinson.

Bana bu kitabı yazma fırsatını verdiği ve ilk kez kitap yazacak biri olarak bana güvendiği için John Wiley & Sons Yayıncılığa müteşekkirim. Bu hayalin gerçekleşmesine katkıda bulunmuş aşağıda adı geçen Wiley çalışanlarına teşekkür etmek istiyorum: Ellen Gerstein, Bob Ipsen, Carol Long (editörüm ve moda tasarımcım) ve Nancy Stevenson.

Destek verip önerilerde bulunan ve pek çok başka şekilde bana yardım eden diğer aile üyeleri, dostlar ve iş arkadaşları da hatırlanıp teşekkür edilmesi gereken kişiler arasındalar. Bu kişiler: J. J. Abrams, David Agger, Bob Arkow, Stephen Barnes, Dr. Robert Berkowitz, Dale Coddington, Eric Corley, Delin Cormeny, Ed Cummings, Art Davis, Michelle Delio, Sam Downing, John Draper, Paul Dryman, Nick Duva, Roy Eskapa, Alex Fielding, Lisa Flores, Brock Frank, Steve Gibson, Jerry Greenblatt, Greg Grunberg, Bill Handle, David G. Halt, Dave Harrison, Les-

lie Herman, Jim Hill, Dan Howard, Steve Hunt, Rez Johar, Steve Knittle, Gary Kremen, Barry Krugel, Earl Krugel, Adrian Lamo, Leo Laporte, Mitch Leventhal, Cynthia Levin, C.J. Little, Jonathan Littman, Mark Maifrett, Brian Martin, Forrest McDonald, Kerry McElwee, Alan McSwain, Elliott Moore, Michael Morris, Eddie Munoz, Patrick Norton, Shawn Nunley, Brenda Parker, Chris Pelton, Kevin Poulsen, Scott Press, Linda ve Art Pryor, Jennifer Reade, Israel ve Rachel Rosencrantz, Mark Ross, William Royer, Irv Rubin, Ryan Russell, Neil Saavedra, Wynn Schwartu, Pete Shipley, Joh Sift, Dan Sokol, Trudy Spector, Matt Spergel, Eliza Amadea Sultan, Douglas Thomas, Roy Tucker, Bryan Turbow, Ron Wetzel, Don David Wilson, Darci Wood, Kevin Wortman, Steve Wozniak ve Los Angeles W6NUT (147.435 MHz) vericisindeki tüm dostlarım.

Ve bağlı olduğum şartlı tahliye memuru Larry Hawley, bu kitabı yazarak güvenlikle ilgili konularda tavsiyeler vermem ve danışmanlık yapmam konusunda bana izin verdiği için çok özel bir teşekkürü hak ediyor.

En son olarak, emniyet teşkilatının mensuplarına teşekkür etmeliyim. İşlerini yapmaya çalışan bu insanlara karşı hiçbir kin beslemiyorum. Toplumun çıkarını kendi çıkarlarından üstün tutarak kendini toplum hizmetine adamanın saygı duyulacak bir şey olduğuna içtenlikle inanıyorum. Her ne kadar zaman zaman kibirli tavırlar sergiledimse de, bu ülkeyi sevdiğimi ve burayı dünyanın en güvenli yeri yapmak için elimden gelen her şeyi yapacağımı hepinizin bilmesini istiyorum. Zaten bu kitabı yazma amaçlarımdan biri de tam olarak bu.

BILL SIMON'DAN

Herkesin içinde doğru bir kişinin olduğuna dair bir kanım var; tek sorun bazı insanların kendi bay ya da bayan doğru'larını bulacak kadar şanslı olmamalarından kaynaklanıyor. Diğerleri ise şanslı olanlar. Tanrı'nın hazinelerinden biri, karım Arynne'le şimdiden pek çok güzel yıl geçirmiş biri olarak hayatımın erken bir döneminde şansımın yaver gittiğine inanıyorum. Ne kadar şanslı olduğumu unutacak olursam, ne kadar çok insanın onunla zaman geçirmek istediğine ve ona değer verdiğine bakmam yeterli olacaktır. Arynne, bu hayat yolunda benimle birlikte yürüdüğün için teşekkür ederim.

Bu kitabın yazılması sırasında, Kevin'in ve benim bu sıradışı kitapta gerçeklerle ilginçliği bir araya getirme amacımıza ulaştığımızdan emin olmamızı sağlayan sadık bir arkadaş grubunun yardımına güvendim. Bu kişilerden her biri dürüst ve sadık değerlere sahip insanlardır ve bir sonraki yazma projesinde kendilerine yeniden ihtiyaç duyabileceğimi bilirler. Bu kişiler alfabetik olarak: Jean Claude Beneventi, Linda Brown, Walt Brown, Korgeneral Don Johnson, Dorothy Ryan, Guri Stark, Chris Steep, Michael Steep ve John Votaw.

Arkadaşının arkadaşından gelen bir talebe zaman ayırmaktan çekinmeyen Network Security Group başkanı John Lucich'e ve hoş bir hareket yapıp Bilgi İşlem operasyonlarıyla ilgili pek çok yere telefon eden Gordon Garb'a buradan özel birer teşekkür.

Yaşamda bazen bir dostunuz, zamanla iyi bir dost olacak biriyle sizi tanıştırarak gözünüzde biraz daha yücelir. California, Cardiff'deki Waterside Yayıncılık'ta çalışan David Furgate bu kitabı yazma fikriyle ortaya çıkan ve beni, önce iş ortağım olup sonradan dostum olan Kevin'le tanıştıran kişiydi. Teşekkürler David. Ve birbiri ardına gelen kitap projeleriyle beni her zaman meşgul tutan Waterside başkanı, eşi bulunmaz Bill Gladstone'a da ayrıca teşekkürler; benim tarafımda olduğun için mutluyum.

Evimizde ve evimdeki ofisimde Arynne'e yardımcı olan becerikli bir ekibimiz var. Bunların arasında idarî asistan Jessica Dudgeon ve ev işlerimize bakan Josie Rodriguez de var.

Annem Marjorie Simon ve babam I.B. Simon'a da teşekkür ederim; keşke bir yazar olarak göstediğim başarıyı görebilmek için hayatta olsalardı. Kızım Victoria'ya da teşekkür ederim. Onunla beraber olduğumda ona ne kadar hayran olduğumu, ona ne kadar saygı duyduğumu ve onunla ne kadar gurur duyduğumu daha iyi anlıyorum.

DİZİN

A

açık,
  etkileyen unsurlar, 305
  değerlendirmesi, 178-179, 243
  testi, 263-264
ad düşürme, 102
adli sicil belgesi, 30
Ağ sayfaları
  kelime listesi, 173-174
  e-ticaret, 89-90
  sahte, 89-93
  güvenli bağlantılar, 94
aldatmaca
  güven unsuru, 7
  teröristler, 9
  anne-babalar, toplum mühendisliği, 10-11
araç plakası, eski, 140
arama
  engeli, 198
  izleme özelliği, 258
  yönlendirme, 256, 290, 130
arayan kimliği, 195, 198, 248, 257, 305
arka kapı, 94, 183, 184, 286
ARPANet (İleri Araştırma Projeleri Birimi Ağı), 8
asma kilit simgesi, Ağ sayfası, 93
ayrıcalıklı hesap, 170, 247, 268-269, 272, 276-279, 293

B

basit uçbirim, 116, 117
beleşçiler, telefon, 11, 31, 37, 75, 129, 144, 169, 195
belirleme kriterleri, şirket çalışanı olmayanlar, 307
"beni şu gönderdi" tarzı güvenlik, 73, 106
bilgi
  gizli değeri, 15
  poker markası olarak, 23
  zararsız gibi görünen bilgiye erişim, 181
bilgi işlem teknolojileri kuralları, 265
Bilgi Sahibi, 118, 245, 251, 306
bilgi simsarı, 34
bilgisayar idaresi kuralları, 269
bilgisayar işlemleri kuralları, 278
bilgisayar korsanları, 6, 7, 46, 85, 91, 120, 148, 154, 157, 169, 172, 175, 193, 201, 285, 296
bilgisayarvandalları, 85-86
bilinçlendirme programı, 231, 232, 237, 243
bilmegereğinin onaylanması, 250, 255, 306, 307
bordro dosyaları, erişim, 153-154
bülten panosu, şirket içi, 262, 281

C

casus yazılım, 188-190, 192
casusluk, şirket (sanayi), 167, 48, 61, 66, 142
Clearlogs adlı program, 110
CreditChex, 15

Ç

çalışan,
  işe yeni girenlere saldırılar, 181
  özel bilgiler, 283
  eskiden çalışmış ya da halen çalışmakta olan, 296
  işten ayrılma süreçleri, 296
  sicil taramaları, 297
çek, karşılıksız, 16
çöp dalışı, 143, 144, 145, 155
çöpler
  karıştırmak, 143
  kurallar, 299
  bilgeliğin sekiz anahtarı, 155-156

D

Dahilî veri sınıflandırması, 246
danışma görevlisi için, kurallar, 300
delme testi, 236, 303
Deneme Numaraları Rehberi, 31-32
denetim, tarihçenin silinmesi, 110
denetleme, günlükler, 189, 192
dışarıdan çalışanlar için kurallar, 294-295
dijital sertifika, ağ sayfası, 91, 93
dinlemek, radyo frekanslarını, 76
doğrudan bağlantı telefon hizmeti, 162
dolandırıcı, 215, 215
dosyaların aktarılması, 64
draje güvenlik, 73

E

eBay, 89, 92, 93
eğitim
  parola güvenliği üzerine, 119
  güvenlik hatırlatıcılarının kullanılması, 120
  temizlik elbiseleri, 178, 232
  güvenlik görevlileri, 192
  önemi, 227-228
  rol yapma, 228, 232-233
  çalışanları teşvik etmek, 231
  programlara destek, 231
  amaçlar, 231-232
  program oluşturmak, 232-233
  yapısı, 234-235
  programın içeriği, 235-237
  ölçüm, 237
  süregelen, 237-238
  hangi çalışanların eğitileceği, 32, 35, 67
  yeni işe başlayanlar, 59, 234
  iş profiline göre, 67, 232-235
  eğitim, 84, 190-192, 227-239 264-265
ekran koruyucu parolası, 287
emniyet güçleri

süreçlerin öğrenilmesi, 30
USBM klavuzu, 45
kulak misafiri olmak, 77
en düşük yetki, kuralı, 259
e-posta
adresin verilmesi, 42, 57, 62
uzak ülkelerden alınan, 190, 202
kullanımkurallan, 236, 242, 247, 249, 271, 280, 284, 287
bağlantılan, 85, 89
eki, 193, 288, 33, 68, 87, 88, 96, 274, 288, 304
erişim
kontrolü, 7
çalışan erişiminin kapatılması, 156
genel erişim haklarını değiştirilmesi, 269
erişimin kilitlenmesi, 275, 276
telsiz erişim noktalan, 277, 278
e-ticaret, 82, 88, 89, 90, 209, 284

F

faks
yönlendirilmesi, 202
kullanım kurallan, 280, 289
Federal Soruşturma Bürosu, FBI, 30, 45, 193
fiziksel güvenlik, kurallar, 298-300

G

geri arama, 248, 305
giriş benzetimcisi, 116
Gizli veri sınıflandırması, 244, 251
gizlilik, üzerinden güvenlik, 75
güven
kötüye kullanılması, 7-8
oluşturulması, 37-49
tanımadığınız kimselere, 43
ve inanılırlık, 46
akıllıca kullanımı, 48
Güvenilir Kişi, 247-248
güvenli HTTP, 94
güvenlik
draje, 73
üçbirim tabanlı, 169
"beni-şu-gönderdi" tarzı, 73, 106
şifreleri, 122, 127, 132
duvan, 66, 73, 81, 95, 116, 150, 158, 182, 274, 284, 293, 295
güvenli kimlik, 78-80
gzip, 219

H

haber gruplan, 286
hassas veri sınıflandırması, 251
hat çevirme telefon numarası, 31
hat kontrolü, 100
havaalanlan, güvenlik, 9
hesap
geçici, 73
ayrıcalıklı, 170, 247, 268, 269, 272, 273, 276, 277, 278
kapatma, 260
yetkilendirme, 267, 247, 266
süre aşımı, 269
misafir, 273
hükümet, internette bulunabilen bilgiler, 45

İ

içeriden gelen tehdit, 118, 190
iki basamaklı tanımlama, 77
iki yönlü sunucu, 172
ikna, tatlı dille, 121
imza kartı, banka, 123
insan avcılan, toplum mühendisliği, 102
insan kaynaklan, kurallar, 280, 283, 296
internet
hükümet bilgileri, 45
varsayılan parola listeleri, 66
düzmece siteler, 92
korsanlık araçlan, 173, 177
intikam, 101,215, 249
intranet, içerik, 49
iş durumu, kontrol, 101, 246, 252
işletim sistemi ayarlan, 176, 188, 243, 270, 272, 277, 293

K

kaba kuvvet saldırısı, 176, 276, 277
kablo ve çift sayısı, 100
kâğıt öğütücüler, 146, 282
karmaşa, parola, 64
kart
tasarımı, 259
elektronik kimlik kartı, 262
kurallar, 236, 260
kaynak kodlarının, elde edilmesi, 42, 77, 184, 214
kefil olma, 246, 248
kelime listesi, kullanımı, 173-174
kitlik, 231
kimlik
iki basamaklı tanımlama, 77, 78
hırsızlığı, 200, 208, 282
kontrolü, 84, 255, 259, 261
komut kabuğu, uzaktan erişim, 56
korsanlık araçlan, 151, 173
kurallar,
gözden geçirilmesi ve güncellenmesi, 234, 243
uymamanın sonuçlan, 243
veri sınıflandırma, 244, 251-252
onay ve yetkilendirme kurallan, 247
çalışan parolalan, 267, 269, 276-267
yönetim, 251-265
veri sınıflandırma, 251-252
bilgi verilmesi, 252-256
telefon idaresi, 256-259
yardım masası, 265-268
bilgi işlem teknolojileri, 265-280
bilgisayar idaresi, 269-278
bilgisayar işlemleri, 278-280
çalışanlar, genel, 280-283
çalışan, 280-294
bilgisayar kullanımı, 283-287
e-posta kullanımı, 287-288
telefon kullanımı, 288-289
faks kullanımı, 289-290
sesli mesaj kullanımı, 290-292
dışandan çalışanlar, 294-295
insan kaynaklan, 295-297
fiziksel güvenlik, 298-300
danışma görevlisi, 300-301

olay bildirme gurubu, 301-302
şemaları, kuruluş şemaları, 145, 246, 272, 282
küçük istemci, 294-295

L
LOphtcrack3 uygulaması, 176
LOCK-11, 168-171

M
MAA (Müşteri Ad ve Adresi) Bürosu, 74
maliyet merkezi kodu, 23, 25
MHBM (Mekanik Hat Belirleme Merkezi), 29
misafir hesabı, 273
modem, telefon hattı, 148, 168, 201, 256, 262, 274, 281
Motorlu Taşıtlar Müdürlüğü, bilgi alınması, 128
müşteriler, korunmaları, 48

O
olay bildirme, 258, 260, 280, 301
omuz gezintisi, 207
onay, üçüncü şahıs kefaleti, 247
onaylama
yöntemleri, 132
kuralları, 247-251
e-posta, 288
telefonla, 288
ipuçları, 84-84
Onaylanmamış Kişi, 246
ONT (Otomatik Numara Tanımlama), 78, 208
Oracle şirketi, 145

Ö
öğrenci kayıtları, hedef olarak, 116
ölü nokta, 65, 202
Öncelikli Hız Erişimi ISDN, 197
özel dedektif, 11-16, 102

P
parola
karmaşası, 64
sözlük saldırısı, 64, 173, 276
varsayılan, 66, 275
giriş benzetimcisi kullanarak bulunması, 116
korsanlık programı, 151, 173, 177
kaba kuvvet saldırısı, 176, 276
casus yazılımlarla ele geçirilmesi, 188, 192
omuz gezintisi, 207
geçersiz, 258, 275, 276
ilk durumuna döndürme, 266, 269
misafir hesabı, 273
kuralları, 275, 266, 267, 269, 275, 276, 277, 279, 284, 290, 291, 292, 293, 294, 305
açıklanması, 287, 279
ekran koruyucu, 287
seçimi, 293
PayPal, 89, 91
peşpeşe geçmek, 281
poker markası, bilgi, 39
posta deliği, 25
psikolojik tetikleyiciler, 97
pwdump3 aracı, 175

R
RCMAC (kısa süreli hafıza değişim yetki merkezi), 163, 178
reddet-kes telefon hizmeti, 162, 178
rehberler
çevrimiçi, 133
Deneme Numaraları Rehberi, 31-32
Rifkin, Stanley Mark (toplum mühendisi), 4-6
risk ölçümü, 242
rollerin değişmesi, 114-117
rüşvet, 145, 282

S
saflık, kurumsal, 8
saklama, çevrimiçi, 224
saklama şirketi, saldırı, 210
saldırı
doğrudan, 28
sözlük, 64, 172, 173, 175, 276
kaba kuvvet, 176, 276, 277
kimlik hırsızlığı, 200, 208, 282
satıcı talepleri, 185-186, 191, 257
sayım, 173
sayım yazılımı, 173
sesi tanımak, 249
sesli mesaj
telefon numarası bırakılması, 139
geçici bir hesap almak, 201
kuralları, 236, 289, 290-292
birime ait, 247
kapatma, 258
sessiz yükleme, 189
sicil taramaları, 297
sindirme, yetki kullanarak, 102
sistem yöneticisi yetkileri, 170-172
solucanlar, 85-86, 88
SosyalGüvenlikNumarası, 26, 47, 71, 104
sözlük saldırısı, 64, 172, 173, 175, 276
SpyCop, 193
SSL (Güvenli Yuva Katmanı), 94-95
sunucu
adının verilmesi, 27, 42, 46, 81, 116, 116
vekil, 49
bağlantı erişim numarası, 66
sürücü ehliyeti, 143, 299

Ş
şifreleme
parolayı, 64
ağ sayfası bilgisini, 94
yedeklenmiş ve saklanmış dosyaları, 211, 223
sesli mesajları, 254
anahtarları, 90
şirket rehberi, toplum mühendisi hedefi olarak, 24

T
takip programı, bilgisayar, 153
taklit etme, bir polis memurunu, 46, 128
taşeron, hesapları, 260
taşınabilir ortamlar, 236,256, 282, 286
Telefon İdaresi kuralları, 256-259
telefon numaraları
rehberde geçmeyenlerin elde edilmesi, 11, 29
ters sorgulama, 29
hat çevirme, 31
Deneme Numaraları Rehberi, 31

Müşteri Ad ve Adresi bürosu, 74
ONT (Otomatik Numara Tanımlama), 78, 208
kablo ve çift numarasının bulunması, 100
hat kontrolü, 101
dahili, açıklanması, 140, 143, 256, 258, 259, 282, 289, 300, 305
arayan kimliği, 195, 208, 248, 257
yeniden programlama, 197
telefon santralı, 131, 196, 248
telsiz erişim noktaları, 277-278
temizlik ekipleri, güvenlik eğitimi, 178, 179
terim/terimler, 30, 45, 75, 125
teröristler, aldatmaca, 9
ters dalavere, 121
ters sorgulama, 29
The Cleaner (Temizlikçi), 95
toplu dava, örnek olay, 209
toplum mühendisliği
teknolojiyle birleşen, 161
anne-babalar, 192
saldırıların başarı oranı, 227
ters, 56
teröristler, 9
toplum mühendisliği saldırıları
başarı oranı, 227
rehberde geçmeyen numaraların elde edilmesi, 11, 29
iş bulma acentaları tarafından yapılan, 21, 30
toplum mühendisliği saldırısı, 24, 83, 92, 35, 66, 75
emniyet güçleri süreçlerinin öğrenilmesi, 31, 46
müşteri bilgilerinin elde edilmesi, 33, 35, 48
kredi kartı numaralarının ele geçirilmesi, 39, 40, 41, 45, 48, 78, 87, 90, 199, 209
yeni işe başlayanların hedef olması, 57
internet dalavereleri örnek olayı, 85, 88, 89, 93
çalışanlardan gelen, 102, 153
döngüsü, 303
uyarı sinyalleri, 304
toplumda kabul görme, 230
trafik cezasından kurtulmak, 202
Trojan Defense Sweep (Truva Atı Savunma Süpürgesi), 95
Truva Atı, 55, 87, 88
tuş girişleri, takibi, 249, 11, 54, 116
tutukevi, örnek olay, 161

U

uçbirim, 117, 169, 170
USBM (Ulusal Suç Bilgileri Merkezi), 31, 45
uzaktan erişim, 55, 56, 82, 86, 95, 147, 173, 184, 208, 246, 260, 265, 269, 270
uzaktan erişimli komut kabuğu, 56
Uzaktan Erişimli Truva Atı, 86

Ü

üniversite kayıtları, hedef olarak, 115
Üye İşyeri Numarası, 16-21

V

vekil sunucu, 49
veri sınıflandırma
kurallar, 244
Gizli, 245
Özel, 245
Dahili, 246
Genel, 246
terimler, 246
video kiralama mağazası, örnek olay, 38-40
virüs, 85, 95-96, (bkz. virüs koruma yazılımları)
virüs koruma yazılımları
güncel tutulması, 58, 95
ve casus yazılımlar, 188, 192
kurallar, 272, 278, 284

Y

yabancı ülkelerden alınan e-postalar, 190, 202
yama, 171, 184, 185, 272
yardım masası kuralları, 265
yazılım
gözetleme, 184, 192
sessiz yükleme, 189
Truva Atı, 55, 87, 95, 242
virüs koruma, 58, 95, 186, 193, 230, 274, 278
kötü huylu yazılım (malware), 87
yazılımcı veletler, 6
yedekleme ortamları, 223, 280
yetki
sorgulanması, 40, 47, 103, 190, 236
sindirme amacıyla kullanılan, 103
yetkilendirme
uzaktan erişim için, 55, 56, 82, 86, 95, 147, 173, 184, 208, 246, 260, 265, 269, 270
süreçleri, 247, 266, 276
yükleme, sessiz, 189

Z

zararlı kod, zararlı kod, 54
zararlı yazılım (malware), 87
ziyaretçi kartı, ziyaretçi kartı, 281, 298, 299
ziyaretçiler, ziyaretçiler, 99, 157, 273, 298-300