ALDATMA SANATI

Bilgi Güvenliğinde İnsan Faktörünün Kontrolü

Kevin D. Mitnick
William L. Simon

THE ART OF DECEPTION

Originally Published by Wiley Publishing, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ALDATMA SANATI
Kevin D. Mitnick

ISBN 978-975-7064-91-6

ODTÜ Geliştirme Vakfı
Yayıncılık ve İletişim A.Ş. Yayınları

Yayın Yönetmeni
İlhami BUĞDAYCI

Çeviren
Nejat Eralp TEZCAN

Kapak Tasarımı
İnova Tasarım

Sayfa Düzeni
Emrullah ÖZ

7. Basım Kasım 2016
Ayrıntı Basım Yayım ve Mat. Hiz. San. Tic. Ltd. Şti.
İvedik Organize San. 770. Sokak Ostim-ANKARA
Tel: (312) 394 55 90 Faks: (312) 394 55 94
Sertifika no: 13987

ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim A.Ş.
Öveçler 1042. Cad. No: 57/1 Çankaya-ANKARA
Tel: 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

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 yapmalarını 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