TİDE Academia Research
Sayı 2 / 281-306 (2019)

HİLE RİSKİ AÇISINDAN SOSYAL MÜHENDİSLİK

Duygu ANIL KESKİN[1]
Samet GÖZENMAN[2]

Submitted/Başvuru: 09.12.2019
Revison/Düzeltme: 15.12.2019
Accepted/Kabul: 30.12.2019

Öz

İnsan sosyal bir varlıktır. İnsanlar, hayatın her anında dış çevre ile birebir ya da dolaylı yollardan etkileşim halindedir ve insanlığın doğuşundan itibaren dış çevreden gelebilecek tehlike ve tehditlerle her zaman karşı karşıyadır. Bu çalışma; güvenlik zincirinin en zayıf halkası ve oluşan bu tehditlerin ana kaynağının insan unsuru olduğu varsayımı altında, insanları birebir ya da dolaylı yollardan etkileyen insanları aldatma sanatı olarak adlandırılan sosyal mühendislik yöntemini farklı yönleriyle incelemektedir. Çalışmanın amacı, sosyal mühendislerin bireyler ve kurumlar açısından oluşturduğu tehditleri, bu tehditlerde kullanılan sosyal mühendislik yöntemlerini açıklamak ve bu bağlamda hile riskine karşı bireylerin ve kurumların kontrol ve güvenlik önlemleri almalarında ve hile karşıtı politikalar geliştirmelerinde sosyal mühendislik hakkında farkındalık yaratacak bilgi sağlamaktır.

Anahtar Kelimeler: Sosyal mühendislik, hile riski, dolandırıcılık, sosyal mühendislik yöntemleri, güvenlik önlemleri

JEL Sınıflandırması: M40, M41

1. Doç.Dr., İstanbul Üniversitesi İktisat Fakültesi İşletme Bölümü, Muhasebe Bilim Dalı, danil@istanbul.edu.tr, ORCID: 0000-0003-3069-0615

2. İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Yüksek Lisans Programı, sametgozenman@gmail.com, , ORCID: 0000-0001-5872-8684

To cite this article: Anıl-Keskin, D. & Gözenman, S.. (2019). Hile Riski Açısından Sosyal Mühendislik. TİDE AcademIA Research, 1(2), 281-306

SOCIAL ENGINEERING IN TERMS OF FRAUD RISK

Abstract

Human is a social entity. People are always interacting with the external environment in every moment of life, and are always encountered to the dangers and threats that may arise from the beginning of humanity. This work; under the assumption that it is the weakest link in the security chain and that the main source of these threats is the human element, it examines different aspects of the social engineering method called art of deceiving people who are influenced by individuals or indirect ways. The aim of this study is to explain the social engineering methods used in these threats and to provide information about social engineering in individuals and institutions to take control and security measures against anti-fraud risk and develop anti-fraud policies. It provides information by creating awareness about social engineering.

Keywords: Social engineering, fraud risk, fraud, social engineering methods, security measures

JEL Codes: M40, M41

1. Giriş

Birçok işletme ve kuruluşun süreç ve operasyonlarında bilgi sistemlerinden faydalanması, bu işletme ve kuruluşlara sağladığı teknolojik yeniliklerin ve yararların yanı sıra kendine özgü riskleri de beraberinde getirmektedir. (Kardeş Selimoğlu, Özbirecikli, & Uzay , 2017) İkibinli yılların başında yaşanan Enron ve WorldCom gibi muhasebe ve yönetim skandalları sonrasında 2002 yılında ABD'de yayınlanan Sarbanes-Oxley Kanunu ile halka açık şirketler ve finansal tablo denetimine tabi diğer tüm kuruluşlar için bilgi sistemlerine ilişkin kontrollerin denetimi zorunlu tutulmuştur. Bilgi teknolojileri denetimi, bu skandallar nedeniyle ortaya çıkan kamu ve toplum güveninin azalmasını önlemek ve finansal raporlamada dürüst resim ilkesini yerine getirmek adına kritik bir mekanizma haline gelmiştir.

Ekonomik ve stratejik anlamı olan her nitelikte bilginin günümüzde saldırı hedefinde olduğu bilinmektedir. Bu durum bilginin kullanılması dışında, korunması ve aktarılmasına ilişkin sorumlulukları da beraberinde getirmektedir. Günümüzde bilgi teknolojileri, güvenlik sisteminin en zayıf halkası insandan bağımsız düşünülmemelidir. (Bağcı, 2009) Geçmişten günümüze bazı insanlar veya insan grupları için çalışmak, çalışarak üretmek yerine, başkasının ürettiğini almak daha cazip olmuştur. İlk çağlardan beri insan davranışları ve doğal yaşamı incelendiğinde, başkasına ait olanı elde etme güdüsü; fiziki güç kullanarak, savaşlarla, yağmalamalarla, gasp ederek, soygun şeklinde ortaya çıkarken, diğer taraftan ikna etme, aldatma, kurnazlık, sahtekârlık, hile yapılarak dolandırıcılık şekliyle de görülmektedir. Kullanılan yöntemler gerek fiziki gerekse de fikri olsun bilgi birikimine dayanan, son derece zekice hazırlanmış, planlanan ve uygulanan bir süreçtir.

Bazı kişiler bu bağlamda insan zafiyetlerinden yararlanarak içinde bulundukları ortamları, durumları fırsata çevirerek çeşitli ikna ve kandırma yöntemleri ile çeşitli bilgileri ele geçirmeye ve amaçları doğrultusunda kullanmaya çalışmaktadırlar. Hacker olarak da adlandırılan bu kişiler, güvenliğin insan boyutunu manipüle ederek sosyal mühendisliğe yönelmekte ve tespit ettikleri güvenlik boşluklarını kendi çıkarları için kullanmaktadırlar. Kurumlar açısından bilgi güvenliği boşlukları çoğu zaman olay meydana geldikten sonra tespit edilmekte, bazı durumlarda ise aynı bilgi ağını kullanan birden fazla kurumun ol-

ması durumunda ise hangi kurumdaki güvenlik boşluklarından faydalanıldığı anlaşılamamaktadır. (Bağcı, 2009)

İnsanları aldatma sanatı olarak da tanımlanan sosyal mühendislik; insan ilişkilerine dayanarak, insan davranışlarındaki ön yargılardan beslenmektedir. Sosyal mühendisliğin çeşitleri değişen piyasa koşullarına ve teknolojiye bağlı olarak farklılaşmaktadır. İletişim ağlarının gelişmesi ve bilginin kolay elde edilebilmesi sosyal mühendisliğin dinamik bir şekilde çok yönlülüğe açık olması nedeniyle, teknolojinin getirmiş olduğu olanakları kullanarak zaman ve mekândan bağımsız gerçekleştirilebilmektedir.

Değişen ve küreselleşen dünya düzeninde sınırların kalkmasıyla, gelişen teknoloji hayatın her alanına girerek, bilgiye erişimi kolaylaştırmakta, iletişim ağlarının genişlemesine olanak tanıyarak, insanlar arası etkileşim kalıplarını dönüştürmektedir. İnsan ilişkilerinin manipüle edilmesi yoluyla gerçekleştirilen sosyal mühendislik saldırılarındaki temel hedef, kurumsal ve kişisel bilgilerin ele geçirilmesi, ele geçirilen bilgilerin kurumlar ve kişiler aleyhine kullanılması, kendi bilgilerine erişimin engellenmesi, kayıtlı bilgilerin silinmesi ve bilgilerin doğruluğunu etkileyecek değişiklikler yapılarak zarara uğratılması olabilmektedir. Bu makale çalışmasında, bilgiyi farklı yöntemler ile ele geçirmeyi amaçlayan sosyal mühendisliği detayları ile ele alıp, bireyler ve kurumlar açısından oluşturduğu tehditleri, bu tehditlerde kullanılan yöntemleri ve alınabilecek kontrol ve güvenlik önlemlerini incelenmektir. (Bağcı, 2009)

2. Sosyal Mühendislik

Sosyal mühendislik, kullanıcıların bilgi sistemlerini tehlikeye atan karanlık sanattır. Sosyal mühendislik, sanal topluluklarda ciddi bir tehdit olarak ortaya çıkan ve bilgi sistemlerine saldırmanın etkili bir yoludur. (Katharina Krombholz, 2015) Teknoloji aracılığıyla veya teknoloji kullanmaksızın normal şartlar altında sahip olunamayacak değerli bilgilere ve ağ sistemlerine, yasal kullanıcılar üzerinden erişim sağlama amacıyla düşük teknolojili ve insan zafiyetlerine dayalı yöntemler olarak da tanımlanmaktadır. Normal koşullarda insanların tanımadıkları biri için yapmayacaklarını yapmalarını sağlama sanatı olarak da tanımlanmaktadır. (Yavanoğlu, Sağıroğlu, & Çolak, 2012) Sosyal mühendislik, insan tutum ve davranışlarındaki önyargılar üzerine kurgulanan; etkileme, zorlama, aldatıcı ilişkiler

geliştirme, sorumluluğu, etik değerleri, dürüstlüğü ya da bağlılığı azaltma amacını güden yöntemler kullanarak kişileri gizli bilgi vermeleri veya erişim sağlamaları için aldatma sürecidir. (Bağcı, 2009) Sosyal mühendislik saldırıları, kişisel beceriye dayanan, basit ve etkili saldırılardır. (Hekim & Başıbüyük, 2013) İnsan odaklı ve teknoloji odaklı olarak hedef kişiye saldırıda bulunulabilmektedirler. Bilgisayar güvenliğinde sosyal mühendislik ise "bir bilişim korsanının ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar kullanarak, sisteme erişmek için gerekli bilgiyi elde etme tekniklerine verilen genel ad" olarak da tanımlanmaktadır (Yavanoğlu, Sağıroğlu, & Çolak, 2012) İngilizcede ''Social Engineering'' teriminden dilimize çevrilmiştir.

Sosyal mühendislik kavramı sosyal mühendisliğin oluşmasında ana unsurlar olan psikoloji, güvenlik, sahtecilik ve dolandırıcılık, internet ve bilgisayar korsanlığı konularından oluşmaktadır.

Sosyal mühendislik türlerinin sürekli değişen ve yenilenen bir yapısının olması, alınan güvenlik önlemlerine rağmen güvenlik boşluklarına yönelen, net tanımlanmayan ve savunmasız alanlara doğru yönelen sosyal mühendislere karşı mutlak bir başarı sağlamamaktadır. Bu sebeple, her sistemde olduğu gibi güvenlik sistemlerinin de periyodik olarak değerlendirilmesi ve geliştirilmesi gerekmektedir.

2.1 Sosyal Mühendislerin Ortak Özellikleri, Hedefleri ve Süreçleri

Sosyal mühendislerin kişilik yapısı, genel hal ve hareketleri, ortak özellikleri incelendiğinde farklı meziyetlere sahip oldukları görülmektedir. Sosyal mühendislik aldatma sanatıdır. Farklı teknik ve becerilerle, farklı senaryolar ile algı oluşturarak, insanların duygularına hitap ederek hal ve hareketlerindeki boşlukları fırsata çevirme eğilimindedir.

Sosyal mühendis yetkin bir araştırma bilgisine sahip istihbaratçı, toplumsal olayları ve eğilimleri irdeleyecek bir sosyolog, yaptığı işi sonuna kadar savunacak bir avukat, bankacılık sistemlerini ve süreçleri bilen iyi bir bankacı rolüne bürünebilir. Ya da karşısındaki kişinin hal ve hareketlerini inceleyen farklı tekniklerle karşısındaki ile etkin bir iletişim kuran bir psikolog, teknolojiyi çok iyi kullanan bilgisayar kullanım beceresi, teknik bilgisi üst düzeyde bir bilgisayar mühendisi, yazılımcı, satacağı ürünü en iyi şekilde sunan ve sizi almaya ikna eden usta bir pazarlamacı, etkin konuşma yetisine sahip bir çağrı merkezi çalışanı ve

en önemli özelliği hangi rol verilirse verilsin, verilen rolle bütünleşen usta bir oyuncudur. Daha birçok meslek grubunun özelliklerini taşımaktadır.

Sosyal mühendisler, her zaman güncel olayları takip ederek, kendini geliştirmekte, toplum yapısını eğilimleri gözeterek kendisine fırsat yaratmaya çalışmaktadır. Hedefindeki kişiye farklı psikolojik yöntemler ile yaklaşıp algı oluşturup; ses tonu, konuşmasının hızını konuştuğu kişiye göre seçmektedir. İnsan ilişkileri ve zaafları konusunda son derece bilgilidir. İlk amacı karşısındaki kişiye güven vermektir. Üstlendiği rolü (savcı, bankacı, polis vb.) en iyi şekilde oynayarak, mağdur kişiye teknik ve hukuksal terimler kullanarak güven vermektedir. Elinde kısıtlı bilgi mevcut ise karşısındaki kişiyi ikna etmek için bu bilgiyi kullanmaktadır. Karşısındakini konuşturarak konular arasında hızlı geçişler yaparak mağdurdan gelen bilgiler ile bağdaştırmaktadır. Masumca konuşmaların, soruların arasında anahtar sorular sorarak mağdur farkında olmadan istediği bilgiyi elde edebilmektedir.

Tercih edilen kimliklerde sosyal mühendisler kendilerini suni senaryolar oluşturarak; kamu görevlisi, firma yetkilisi, bir tanıdığı ya da tanıdığının yakını olarak tanıtmaktadırlar. Uygulanan psikolojik teknikleri, yöntem ve senaryoları ele alırsak bu nitelikteki hilekarlar ilk aşamada karşısındaki kişinin güvenini kazanmakta, yakınlık duygusu hisseden hedef kişi sosyal mühendisin istediklerini, yönlendirmelerini şüphe duymadan yapabilmektedirler. (Yılmaz, 2015)

Planladıkları senaryo dahilinde farklı teknikler uygulayan hilekarlar acil durum ve panik havası yaratarak, karşısındakini korkutarak, konuşmanın tıkandığı anlarda tehdide yönelmektedirler. Aynı zamanda rahat ve ısrarcıdırlar. Yardımcı olma arzusunda olduklarını karşısındakine hissettirirler, gerekirse belirtirler. Söylediklerinin yapılmaması durumunda karşısındaki kişinin zor durumda kalabileceğini söylerler. Vaatlerde bulunurlar. Ödül hediye kazandınız şeklinde fırsatlar ve teklifler sunabilmektedirler. İstek ve yönlendirmeler ile merak duygusu uyandırarak, mağdurun zayıf duyguları ve algılarına hitap ederek kendi ağına çekebilmektedirler.

Sosyal mühendisler kendilerini önemli bir kişi olarak göstermektedirler. Kurumlara ve kuruluşlara bağlı isimleri tanıdığını söyleyerek, isim vermekten çekinmezler. Gireceği ortama hemen uyum sağlarlar. Üstlendikleri rol neticesinde ikna kabiliyetleri yüksek, nazik, etki-

leyicidirler. Söz söyleme ve insanı aldatma sanatı konusunda başarılıdırlar. Her an mağdur potansiyeli olanların boşluğunu ararlar. Sorun çıkarıp sorun çözme eğilimindedirler. Hedefteki kişileri etkileyip, inandırmak için farklı söylemlerde bulunmaktadırlar.

Sosyal mühendislik farklı meslek dallarının ustalık becerilerini barındıran bir yapıdan oluşmaktadır. Bu faaliyet tek bir kişi tarafından gerçekleşebileceği gibi, bu amaçla kurulmuş merkez, aracılar ve ayakçılardan oluşan bir yapıdan da söz edilebilir.

Bir değere sahip her türlü bilgi, saldırı hedefi olabilmekte, bu nedenle kişi veya kurumlar hedef olabilmekte ve çeşitli risklerle karşı karşıya kalabilmektedir. Sisteme erişim hakkı olan yetki ve itibar elde etmeye çalışanlar, kendisine danışıldığı imajı yaratılan personeller, kuruma ya da kurum çalışanlarına bağlılığı zayıflamış zaafları ve açıkları olan personeller, alt kademelerde çalışan yardımcı olmaya istekli personeller, sisteme erişimi olmamasına rağmen güvenlik ve santral gibi destek hizmetlerinde çalışan personeller ilk aşamada hedef alınabilmektedir. (Bağcı, 2009) Sosyal mühendis birincil olarak ele geçirilmiş bir datadan, teknoloji temelli yöntemler kullanarak ağına takılmış bir veriden, iz sürdüğü bir kişilikten beslenebilmektedir.

İfade edildiği gibi hedef kitle herkes olabilmektedir. Yaş, cinsiyet, eğitim durumu, demografik bilgiler vb. sınıflandırmalar ayırt edilmeksizin büyük bir denize atılmış tek bir olta gibi gözükse de kullanılan kaynaklar ve hedef seçimi spesifik bir şekilde de gerçekleşebilmektedir.

Sosyal mühendislik uygularken ki süreçte, öncelikle mağdur hakkında araştırma yapılır, potansiyel mağdura karşı güveni sağlamak amaçlı hareket, davranış ve eylemlerde bulunulur. Elde ettiği bu bilgiyi kullanacağı amaç doğrultusunda denemektedir. Başarısız olması durumunda bilgi elde ettiği mağduru, yani kaynakla tekrar bağlantı sağlayarak elde ettiği bu bilgileri sosyal mühendislik yöntemleri ile doğrulatabilir. Ve veri kaynağına tekrar ulaşabilmek için açık kapı mutlaka bırakılmaktadır. (Gündüz & Daş, 2016)

Şekil 1. Sosyal Mühendislik Süreci (Gündüz & Daş, 2016)

2.2. Sosyal Mühendislikte Kullanılan Yaygın Yöntemler

Sosyal mühendislikte kullanılan genel yöntemler, teknoloji odaklı ve insan odaklı olmak üzere iki şekilde sınıflandırılabilir. Kullanılan yöntemleri her ne kadar insan odaklı ve teknoloji odaklı olarak ayırsak da hiçbir sistem insandan bağımsız değildir. Bu teknolojik ürünler, teknolojik gelişmeler insanlar tarafından yapılır ve geliştirilirler. Sistemlerden faydalanan ve sistemi kullananlar da yine insanlardır.

Sosyal mühendislikte kullanılan genel yöntemler, sosyal mühendislerin insanların algı, duygu, tutum ve davranışları üzerine geliştirdiği genel dolandırıcılık tipolojileri açısından incelenmektedir. Sosyal mühendislik vakalarının yaşanabileceği muhtemel ortamlar ise; insan-makine, makine-makine, insan-yazılım, yazılım-yazılım, korsan-karma (makine,yazılım, insan) arayüz ortamlarıdır. (Vural & Sağıroğlu, 2011)

2.2.1. Teknoloji Temelli Sosyal Mühendislik Yöntemleri

Temeli teknolojiye dayanan sosyal mühendislik yönteminde, kişiye ait bilgiler teknoloji kullanılarak elde edilmektedir. Artan bilgisayar ve internet kullanımı, özellikle bilişim sektöründe yaşanan gelişmeler dolandırıcılık olaylarında teknolojik yöntemlerin kullanıldığı daha karmaşık bir yapıya dönüşmektedir. Bilgisayar sistemi ve özellikleri akıllı cihazlara taşınmış, internet kullanımı artmış, insanların yaşamını kolaylaştıran teknolojinin etkisi kaçınılmaz bir hal almıştır. İnternet ve bilgisayar kullanımının artmasına bağlı olarak değişen alışkanlıklar ve bilinçsiz kullanımlar sosyal mühendislerin de dikkatini çekmiş ve

buna bağlı olarak farklı yöntemler geliştirmişlerdir. Normalmiş gibi gözüken ve girilen bir site, yüklenen bir uygulama, tıklanan bir link ve birçok farklı yöntem sosyal mühendislerin insanların kişisel bilgilerini elde etmesi için hazine değeri taşımaktadır. İnternet dolandırıcılığı her geçen gün daha fazla kullanılmaktadır. Yazılım şirketleri programlarını nasıl güçlendireceklerini öğrenirken, bilgisayar korsanları ve kötü niyetli sosyal mühendisler altyapının en zayıf kesimine, insanlara yönelmektedir. Kullanılan dokuz yaygın yöntem aşağıdaki gibidir. (TBB, 2015)

2.2.1.1. Virüsler, Solucanlar, Truva Yazılımları

Virüsler, solucanlar ve truva yazılımları; bilgisayar ve sistemlerin düzgün şekilde çalışmasını engelleyerek, kullanıcı kişinin izni ve bilgisi dışında sistemi yönlendirmesine sebebiyet veren, bilgisayar ve sistem içerisinde yer alan veri ve bilgilerin ele geçirilmesine olanak sağlayan kötü amaçlı yazılım çeşitleridir. Bu yazılımlar sistemin yavaşlamasına ve çökmesine sebebiyet vermektedir.

2.2.1.2. Tuş ve Ekran Kaydediciler

Hedef kişinin klavye hareketlerine ulaşmayı amaç edinen bir saldırı türüdür. Klavye ve ekran hareketleri kayıt altına alınarak edinilen bilgilerin kullanılması amaçlanmaktadır.

2.2.1.3. Phishing (Olta Saldırıları)

Hedef kişiyi, kişi ve kurumların internet sayfaları ve benzeri tasarlanmış sitelere yönlendirerek, bilgi girişi yaptırılması amaçlanmaktadır. Phishing (Voice Phishing) Olta Saldırıları ise ses ile aldatma yöntemidir. Phishing saldırıları, teknoloji temelli sosyal mühendislik olaylarında kullanılıp, hedefteki kişiden aranılarak bilgi edinilmesini amaçlamaktadır.

2.2.1.4. WI-FI Dolandırıcılığı

Sosyal mühendisler ortak kullanım alanlarında, mekanlarda şifresiz Wi-fi alanı yaratarak hedef kişinin bu ağa bağlanması ve bilgilerinin ele geçirilmesi planlanmaktadır.

2.2.1.5. Pop- Up Ekranlar

Hedefteki kişilerin cihazlarına ani bildirimler ileterek kişilerin bunları tıklaması amaçlanmaktadır. En çok karşılaşılan örnekler reklam, arıza, güncelleme bildirimleridir.

2.2.1.6. Spam E-Postalar ve Botnet

Genellikle istenmeyen mailler olarak isimlendirilen bu e-mailler, alıcı kişinin cihazına içerisinde taşıdıkları zararlı yazılımları bulaştırabilmekte, içerisinde virüs bulunan, zararlı yazılımlar barındıran sitelere de farklı senaryolar ile yönlendirme yapmaktadırlar. Bot terimi robotun kısaltmasıdır. Saldırganlar hedefteki kişilerin cihazlarına kötü amaçlı yazılımlar, programlar sızdırarak, cihazı kullanıcıdan habersiz olarak internette farklı görevlerde kullanmalarına olanak sağlamaktadır. Zombi olarak da bilinmektedirler.

2.2.1.7. Teknolojik Donanımlar

Hedefteki kişiye ait bilgileri ele geçirmeye yönelik teknolojinin veya teknolojik cihazların kullanılmasıdır. Kullanılan donanımlar, mağdurun dinlenmesine, yaptığı işlem hareketlerinin kaydedilmesine, kopyalanmasına, işlemlere müdahale edilmesine olanak sağlar.

2.2.1.8. Ortadaki Adam Saldırısı

Ortadaki adam saldırısı (Man-in-the-middle attack), bir network aracılığıyla hedef kişinin bilgisayarı ve diğer kullanılan ağ araçlarının (yönlendirici, switch, modem ya da server gibi) arasına sızıp, bilgilerini ele geçirmeye yönelik bir saldırı çeşididir. (terramedusa, 2019)

2.2.1.9. Tarayıcı Saldırıları

Tarayıcıdaki adam saldırısı (Man In The Browser Attack), hedef kişinin sistem şifrelerini ya da gireceği şifreleri ele geçirmek yerine, kullanılan internet tarayıcısı içerisine zararlı yazılım yerleştirip saldırıda bulunulmasıdır. Bu saldırıda ilgili işlemin yapılması için hedef kişinin internet bankacılığına girmesi ya da para transfer işlemi yapması beklenmektedir. Bu esnada zararlı yazılım içeren internet tarayıcısı eklentisi hedef kişinin kullanıcı bilgilerini, alıcı bilgilerini, transfer bilgilerini, miktarları değiştirebilmekte, kullanıcı adına transferler gerçekleştirebilmektedir. (terramedusa, 2019)

2.2.2. İnsan Temelli Sosyal Mühendislik Yöntemleri

Temeli insana dayanan sosyal mühendislik yönteminde sosyal mühendisler bilgi almak ya da istenilen işlemleri yaptırmak amacıyla hedefteki kişi ya da kişiler ile iletişime geçip, oluşturulan senaryo dahilinde, bir kimliğe bürünerek, güven vererek, etkileyerek ve ikna

ederek bilgilerinin ele geçirilmesi ve sosyal mühendisin amacı doğrultusunda kullanılması sürecine dayanmaktadır. Sosyal mühendisler ikna yoluyla dolandırıcılık yönteminde kişisel bilgileri ele geçirmek ve amaçları doğrultusunda kullanmak için birçok psikolojik teknik uygulayıp farklı yöntem ve senaryolar yaratmaktadırlar. Hedefteki kişilerin doğal eğilimleri, etkileşim ağları ve duyguları, sosyal mühendisin besleneceği ana kaynaklar arasındadır. (TBB, 2015)

2.2.2.1. İkna Yolu Dolandırıcılığı

Sosyal mühendisin hedef kişi ya da kişilerde güven oluşturarak, çeşitli senaryo ve psikolojik testler uygulaması yoluyla bilgilerini ele geçirme ve amaçları için kullanmasıdır. İkna yolu dolandırıcılığı yöntemleri arasında hedef kişiye yönelik olarak en sık kullanılanlar; çeşitli ortamlarda ve platformlarda vaat, ödül, imkan ve fırsat sunma, belirli ürün üzerinden satış ve pazarlama, yardım ve bağış toplama, durum psikolojisi oluşturarak korkutma ve endişe yaratma ve bilgilerini kontrol etme amacıyla yaklaşılmasıdır.

2.2.2.2. Çöp Kurcalama

Kurumların kullanmadıkları, değersiz olarak gördükleri ya da yok etmedikleri, üzerinde bilgi bulunan her türlü materyallerin atıldığı ve bu atıkların ve benzeri nesnelerin sosyal mühendisler tarafından gerekli bilgiye ulaşabilmek amacıyla iz sürülüp toplandığı yöntemdir. Hiç umursanmayacak bir çöp konteynerinde kuruma ait, kurumda çalışan ya da kurumun çalıştığı kişilere ait birçok bilgi ve belgeye ulaşılabilmektedir. Sosyal mühendisler bu atıklardan elde ettikleri bilgileri amaçları doğrultusunda kullanmaktadırlar.

2.2.2.3. Omuz Sörfü, Casusluk ve Kulak Misafirliği

Ustaca bir gözlemcilik yeteneği isteyen bu yöntemde, sosyal mühendis hedefindeki kişiyi gözlemleyerek amacı doğrultusunda gerekli bilgi ve ipucuna ulaşmaktadır. Gözlemlerinde dürbün, kamera, akıllı cihazlar, ses kayıt cihazı gibi çeşitli teknolojik nesnelerden de yararlanabilmektedirler. Aynı zamanda aynı ortam içerisinde hedef kişiye fark ettirmeden, hareketlerini izleyerek, kulak kabartarak gerekli bilgi ve ipuçlarını da elde edebilmektedirler. Gizli bilgilerin, evrakların, şifrelerin kötü amaçlı kişilerin eline geçmemesi için dikkatli ve tedbirli davranmak gerekmektedir. Risk teşkil eden belgelerin ortalık yerde bırakılmama-

sı, üçüncü kişilerin yanında şifre girişleri yapılırken izlenilmediğinden emin olarak giriş yapılması, çevre kontrolü güvenlik riskini azaltan yöntemler arasında sıralanabilmektedir.

2.3. Sosyal Mühendislikte Kullanılan Bazı Teknikler

Sosyal mühendisler hedef kişilerin bilgilerini ele geçirebilmek için çok farklı yöntemler denerken, bu yöntemler içerisinde de farklı tekniklerden yararlanmaktadırlar.

2.3.1. Medya Manipülasyonu

Bilgiye erişim konusunda kaynakların çeşitliliği buna bağlı olarak haber kaynaklarının internet üzerinden sosyal ağlar ile entegrasyonu, medya manipülasyonu doğrultusunda sosyal mühendislerin insanların dikkatini çekmek ve yönlendirmek amacı ile tercih ettiği yöntemlerden biri haline gelmiştir.

Dikkat çeken gündem haberleri, ünlü kişilere ait skandallar, ürünler ve lansmanlar, ölüm haberleri, tartışmalar, fotoğraflar, önemli gün ve tarihler, büyük etkinlikler, popüler spor haberleri ve olayları, insanları medya manipülasyonunda sosyal mühendislerin sıklıkla tercih ettiği haber kaynakları arasındadır. İnsanların bilgi edinmek için aradığı bir bilgi ya da olaydan, ya da bir sosyal ağ üzerinde insanlar üzerinde merak duygusu yaratarak yönlendirmelerde bulunulabilmektedir. Sosyal mühendis hedefteki kişiyi virüs bulaştıracak bir linke tıklamaya, bir uygulama ya da programı indirmeye, sahte siteler oluşturarak bilgilerini ve şifrelerini girmeye yönlendirerek amacı doğrultusunda bilgilere ulaşmaktadır. (trendmicro.com.tr, 2019)

2.3.2. Evet - Evet Tekniği

Hedef kişiyi ikna etmek için kullanılan tekniklerden biri de ''evet - evet'' tekniğidir. Hedefteki iletişim kurulan kişiye önce güven verip, ard arda evet cevabı verme olasılığı olan sorular yöneltip, asıl talep ile ilgili soru en sonda sorulmaktadır. Sosyal mühendis tarafından hedef üzerinde zihinde örüntü oluşturularak, son belirtilen talebi onaylamasına sebebiyet verecek ortam oluşturulmaktadır. Hedef ile iletişime geçilen konunun ve ürünün önemi ve gerekliliği vurgulanarak algı oluşturulmaktadır. Satış pazarlama, bilgi kontrol sosyal mühendislik yöntemleriyle beraber kullanılan, sıklıkla tercih edilen bir yöntemdir. (Karabulut Y. , 2010)

2.3.3. Rica Tekniği

Küçükten büyüğe rica tekniği ile; öncelikle hedefi zorlamayacak, yapabileceği şeyler hakkında talepte bulunmaktadır. Yavaş yavaş talepler büyütülerek karşındakine yapabiliyor duygusu, motivasyon ve ilişkisel bağı kaybetmemek için kabullendirme yöntemine gidilmektedir. Bu tekniğin tam tersi de büyükten küçüğe rica tekniğidir. Hedef kişiye bir talepte bulunulur. İlk talebe kişinin hayır diyeceği varsayımı altında, daha sonrasında küçük talepler ile asıl yaptırılmak istenilen kişiyi ruhsal, duygusal etkileyerek ve seçenek şansı azaltılarak kişiyi rica edinilen talebi yapma zorunluluğu hissi yaratılmaktadır. İş çevrelerinde sıkça karşılaşılan bir tekniktir.

2.3.4. Trafik Lambaları Tekniği

Trafik Lambaları Tekniği sosyal mühendislerin karşısındaki kişiler ile etkileşim hallerinde duygu kontrolü ve karşısındaki kişiye güven oluşturup, ikna etme aşamasında da kullanılan bir teknik türüdür. Ara verme tekniğinin trafik ışıklarına benzetilmesi ile adlandırılmıştır.

Bu yöntemde sosyal mühendis hedef kişi ile iletişimi esnasında amacı doğrultusunda ''Dur- düşün- eylemini yap'' üçlemini uygulamaktadır.

Trafik Işıkları Tekniği, adından da anlaşılacağı üzere ismini trafik ışıklarındaki renklerden almaktadır. Kırmızı ışık yani ilk evredir; iletişimde bulunan kişinin hareketlerine göre sosyal mühendis kendisini arka plana çekme evresidir. Sarı ışık, hazırlan hedefteki kişinin hareketleri ve tepkilerini gözlemleyerek, sosyal mühendis yapacaklarını düşünmekte ve içinde bulunduğu durumu lehine çevirebilmek için ortam aramakta, dinlemekte ve gözlemlemektedir. Yeşil ışık, geç; bu evrede sosyal mühendis kafasında çözüm yolunu bulmuş olarak farklı yöntemler ile hedefin üzerine gitmektedir. Kimi zaman bu etkili bir konuşma, kimi zaman farklı senaryolar üretme, kimi zaman da dış kaynaklardan yararlanma şeklinde olabilmektedir.

2.3.5. Ay Işığı Tekniği

Sosyal mühendisin hedefteki kişiye güven vererek, kendisine bağlı hale getirmesini, durumu olağanlaştırıp, amacına ulaşarak ortadan kaybolmasını açıklayan bir tekniktir. Belirli bir söylemi karşısındakine itiraf ettirmeye, sosyal mühendisin yaptıklarının hedef tarafın-

dan sorgulatılmamasına ve bu esnada hedef kişi hakkında bilgi alınmaya ve amacı doğrultusunda kullanılmaya çalışılmaktadır. Etkileşim sırasında hedef kişinin algılarını kapatarak, direkt sosyal mühendise odaklanması ve bu süreçte istenilenlerin yaptırılmasına çalışılır. Sonucunda hedef kişiyle yavaş yavaş iletişim kesilerek fark ettirilmeden ortadan kaybolunmaktadır. (Karabulut Y. , 2010)

2.3.6. Önce Ver, Sonra Geri Al Tekniği

Bu yöntemde hedefteki kişi ya da kişilere görüşler sunularak, cazip fırsatlar, koşullar, vaatler verilmektedir. Karşı taraf tarafından verilen görüşe, ürüne, sunuya hedef kişinin özümsemesi, tutumunun değişerek, bağlılığının artması amaçlanmaktadır.

2.3.7. Saadet Zinciri

Piramit şekline benzeyen bu yapı Charles Ponzi tarafından 1920'li yıllarda ortaya çıkmıştır. Piramit yapı sisteminin bilinen adı saadet zinciridir. Ponzi hilesi, eski ve karlı bir yöntemdir. Günümüzde pazarlama stratejilerinde kullanılan bu yöntem, piramidin en üstündekilerin kazandığı sistemde, sisteme dahil olan her kişinin altındaki kişi ve onun bağlantıları sayesinde işi kendine döndürdüğü bir bağlantı sistemidir. Sosyal mühendis, öncelikle az sayıda kişiyi yüksek getiri vaadiyle sisteme dahil etmeye ikna etmektedir. Sisteme girenler belirli bir para öderler. Gerçekten de sisteme ilk girenler, yüksek getiri elde edip bunu çevreleriyle paylaşarak, kaçırılmaması gereken bir fırsat olarak anlatırlar. Sistem, ilk kuranın paralarla birlikte aniden ortadan kaybolmasıyla ve sistemdekilerin hepsinin aynı anda paralarını geri istemeleriyle çökmektedir. (Mengi vd., 2013)

2.3.8. Seçenek ve Alternatif Çözüm Sunma

Hedefe belirli konuda kısıtlanmış seçenekler sunularak, hedef kişiye zorunlu seçenek yapması hususunda baskı yapılmaktadır. Sonuca ulaşılamamış ise, sonraki aşamasında hedef kişinin iyiliğine daha iyi seçenekler sunma varsayımı altında alternatif çözüm sunularak esasında başta kafada oluşturulmuş talepler, durumlar, ürünler iletilir. "Hangisi?" sorusuyla tercih yapmak zorunda bırakılmaktadır.

2.3.9. Bağımlık Oluşturma ve Yer Etme

Hedefin bir kişiye, ürüne, kuruma uzun süre bağlılığının oluşturulması alıştırılması sonucunda; mevcut alışkanlıklarından, değişime kapalılığından, sorgulayıcı yönünün zayıflamasından faydalanılmaktadır. Her şeyi olağan ve en iyi seçimin kendisi olduğunu göstererek mevcut durumu sürdürme aidiyetini arttırma ve karşı tarafa belli etmeden zaman zaman zihinsel hatırlatıcı, uyarıcı mesajları vererek kendisini hatırlatarak taleplerde bulunulmasıdır. Hedefi borca sokarak kendisine bağlama da en çok kullanılan yöntemlerden biridir.

2.3.10. Soruya Soruyla Yanıt Verme

Hedef kişiye durmadan soru sorarak, sorunlarına ya da taleplerine ayrı sorular yönelterek cevap vererek hedef kişinin kafasının karıştırılmasıdır. Yeri geldiğinde hızlı konuşarak, konuyu başka yönlere çekerek, zaman kazanarak sonuca varılmaya çalışılmasıdır.

3. Sosyal Mühendisliğin Mağdurlar Üzerindeki Etkileri

Sosyal mühendislik olaylarının kurum üzerindeki etkilerine bakıldığında sadece kurumun değil doğrudan kişilerin de bilgilerinin ele geçmesine sebebiyet verebilmektedir. Sosyal mühendislik olayına maruz kalmış bir kurumda müşteri ve itibar kaybı en hassas konuların başında yer almaktadır. Güveni kaybolan bir birey asla inanmadığı bir kurum ile çalışmak istemez. Bilgilerin ele geçirilmesi, şirket stratejisini, şirket yapısını olumsuz yönde etkileyerek çok büyük finansal kayıplara yol açabilmektedir. Denetim ve kontrol süreçlerinin özenle yapılması, güvenliğe yönelik gereken yatırımın yapılması, uygulanması kurumların daha büyük risklerin altında kalmasını engelleyecektir.

Sosyal mühendislik saldırıları kişileri ve kurumları hedef almaktadır. Saldırıların bireyler ve kurumlar üzerinde farklı etkileri bulunmaktadır. Kurumsal bilgi sistemlerinin güvenliği sadece teknik önlemlerin alınmasıyla sağlanmamaktadır. Teknoloji temelli olmayan sebeplerden de bilgi sistemlerinin güvenliği tehdit altındadır. İşletme yönetimi açısından hile riski olarak tanımlanan bu tehditlerin öncelikle tespit edilmesi ardında da değerlendirilmesi gerekmektedir. Bilgi sistemleri teknik (bilişim sistemleri, doküman yönetim sistemleri, süreç analizleri, vb.) ve teknik olmayan (çalışanların bilinci, kurum

kültürü, yönetimsel prosedürler, fiziksel güvenlik vb.) unsurları açısından güvenlik testleriyle değerlendirilmelidir. Kurumların bilgi güvenliğini sağlama sürecinde kullandıkları bilgi sistemlerinin boşluklarının erken teşhisini yapması ve boşlukların kısa sürede giderilmesi önemlidir. Buradaki kritik nokta saldırı gelmeden önce güvenlik boşluklarını tespit ederek önleyici tedbirler alınmasını sağlayan güvenlik testleri kurumsal bilgi güvenliğinin sağlanmasında büyük önem taşımaktadır. Güvenlik testleri; bilgisayar ağlarının güvenliğini artırmak, ağ ve ağ kaynaklarındaki kontrol boşluklarının tespit edilerek bilgi sistemlerinin (etik amaçlı saldırılar-ethical hacking) güvenlik seviyesini değerlendirmek bir başka değişle açık kapıyı bulmak için uygulanan testlerdir. (Vural & Sağıroğlu, 2011)

Sürekli gelişen ve değişen bir yapıya sahip bilgi teknolojileri sisteminde bilgi güvenliğinin bir defalık sağlanması veya yapılandırılması yeterli değildir. Bu nedenle işletme yönetimi tarafından kurulan bilgi teknolojileri sistemlerinin mevcut ihtiyacı karşılaması, sistemin belirlenen politikalar ve prosedürlere uygun olarak çalışıp çalışmadığının kontrolü, güvenlik boşluklarının tespiti, açık kapıların bulunması amacıyla ve sürekli değişen yapısı nedeniyle periyodik olarak gözden geçirilmesi ve güncellenmesi, yönetici ve personele sistemle ilgili eğitim verilmesi oluşabilecek yeni riskler karşısında hemen aksiyon almayı sağlamaktadır. Güvenlik testleri planlama, bilgi toplama, güvenlik boşluklarının bulunması, boşlukların kullanılması ve raporlama süreçlerinden oluşmaktadır. "Planlama; kapsam tespiti, test türleri, zaman dilimleri, riskler, araçlar, personel, işin süresi, maliyet, etik, bilgi değişimi ve gizlilik anlaşmaları konularını içeren başlangıç aşamasıdır. Planlama tamamlandığında; kurumsal bilgi varlıklarının tespit edildiği, tespit edilen bilgi varlıklarının sınıflandırıldığı ve güvenlik testinin omurgasının oluşturulduğu bilgi toplama aşamasına geçilmektedir. Bu süreçte, sosyal mühendislik testleriyle kurum veya kuruluşlar hakkında detaylı bilgiler toplanır. Telefon Yoluyla Taklit ve İkna; E-posta Yoluyla Kandırmaca; Çöplük Karıştırma; Masaüstü Testleri ve Fiziksel Erişim, sosyal mühendisler tarafından bilgi toplama araçlarıdır. Güvenlik boşlukları, sosyal mühendislerin sömürebileceği hatalardır. Bilgi kaynakları (insan, haberleşme, bilgisayar ağları, bilgisayar, vb.) üzerinde var olan ve istismar edilebilecek güvenlik boşluklarının tespit edilmesi, tanımlanması ve sınıflandırılması süreci güvenlik boşluğu analizi olarak adlandırılmaktadır Bilgisayarlar ve ağlar üzerindeki zafiyetlere ek olarak bu sistemlerin işletilmesiyle ilgili politika ve prosedürlerden kaynaklanan güvenlik boşlukları da tanımlanmaktadır. (Vural & Sağıroğlu, 2011)

Kurumların bilgi güvenlik politika ve prosedürlerinin oluşturulmasında, kurumsal bilgi sistemlerinin güvenliğini tehdit eden durumlar güvenlik testleriyle tespit edilerek, risk değerlendirmeleri ve risk analizleri yapılmaktadır. Risk analiz sonuçları kurumsal bilgi güvenliği sistemi çerçevesinde belirlenen politika ve prosedürleri oluşturmaktadır. Bu testler ve sistemin etkinliğinin belirli düzeyde sağlanması güvenlik sertifikalarının alınması için gerekmektedir. (Vural & Sağıroğlu, 2011) Kurumlar bu saldırılardan korunmak için çeşitli önlemler almaktadırlar.

Kurumlardaki çeşitli kullanıcı profillerinin sisteme erişim imkânları göz önüne alınarak, kullanıcı güvenlik politikalarındaki sıkılaştırmalara önem verilmeli, tüm kullanıcı profillerinin yetkileri prosedürler ile belirlenmelidir. Çöpe atılacak belge veya dokümanlar, kırpıcılardan geçirilmeli veya okunamayacak şekilde yırtılmalıdır.

Güçlü güvenlik politikaları yaratırken çalışanlara yeterince güvenilmemesi durumunda çalışanların kuruma bağlılığı zayıflayacak, gereğinden fazla güven duyulması durumunda ise çalışanlardan ya da çalışanlar üzerinden gelecek saldırılara karşı sistem savunmasız bırakılmış olacaktır.

Çalışanlar iş ve özel hayat dengesini iyi ayarlamalı müşteri ilişkileri konusunda hassas davranılmalıdır. Kurumdaki kişiler sorgulayıcı, şüpheci olmalıdır. Hedef ve kâr amacı doğrultusunda oluşabilecek risklere karşı müşteri edinimine dikkat edilmelidir. Referans kişiler ile çalışılması hem müşteri hem kurum açısından güven telkin etmektedir. Kurumdaki çalışanlar için temiz masa / temiz ekran politikası uygulanmalıdır. Kurumda işten ayrılan personeller için uyulması gereken prosedürler hazırlanmalıdır. Kurumdan ayrılan personellerin kullandıkları sistem parolaları ve bilgileri pasif hale getirilmelidir.

Kuruma ziyaretçi geldiğinde, kişi ya da kişilerden kimlik istenmeli, kurum içerisinde bulunan bir çalışan gelen kişiye refakat etmelidir. Kurumlar için önem arz eden bölgelere 24 saat aktif çalışan güvenlik kameraları yerleştirilmelidir.

Şifre girişleri yapılırken, giriş yapan kişinin fark edilmeden izlenmesi anlamında kullanılan omuz sörfüne karşı dikkatli olunmalıdır. Kurumlar için önem arz eden bölgelere 24 saat aktif çalışan güvenlik kameraları yerleştirilmelidir. Çalışanlar tanımadıkları kişilerden gelen istekler, bildirimler, erişimler karşısında daha dikkatli olmalıdır. Kurumda çalışan

tüm personellere periyodik olarak bilgi güvenliği eğitimleri verilmeli, güncel olaylar, oluşabilecek riskler anlatılmalı farkındalıkları arttırılmalıdır.

Siber saldırılara karşı güvenlik önlemleri alınmalı, olası sızıntılara karşı gerekli denetim süreçleri yapılandırılmalıdır. İş sürekliliği planlarında kurumun karşılaşabileceği risklere karşı bilgi güvenliği konuları da kapsama alınmalıdır. (Basaran, 2016)

Bir kurum sosyal mühendislik kapsamında bilgilerinin ele geçmesi halinde kurum zafiyetlerine yönelik denetim cezaları, hukuki yaptırımlar ile karşı karşıya kalabilmektedir. Kaçınılan yatırım maliyeti büyük sorunları beraberinde getirebilmekte, ele geçirilen sistem ve kaynaklar, başka kurumlardaki verilerine zarar verilmesi ya da ele geçirilmesi için de kullanılabilmektedir. Büyük ölçekli kurumlar, bu bilinçle siber saldırılara ve sosyal mühendislik olaylarına karşı dikkatli olmalı, gerekli yatırımı yapıp, gerekli önlemleri almalıdırlar.

İnsanlar, değişen dünya düzeninde, mevcut sistemde her gün farklı insan ve kaynaklarla sayısız etkileşim halindedir. İşletme yönetimi, sosyal mühendislik gibi insan temelli saldırıların riskini azaltmak için çalışanların siber güvenliğe ilişkin konularda eğitilmeleri ve bilinçlendirilmeleri gerekmektedir. (Mengi, 2012)(Hekim, 2013)

4. Hile Riski Açısından Sosyal Mühendislik

Bu başlık altında konu iki boyuttan ele alınacaktır. 1) Denetlenen işletme personelinin kendisinin sosyal mühendis olması ve 2) Denetlenen işletmenin sosyal mühendislik uygulamalarına maruz kalması. Her iki boyut denetçi açısından bir risk unsurudur fakat birinci durum denetçi açısından çok daha ciddi bir risk olarak değerlendirilebilir. Çünkü birinci durumda, personelin çalıştığı işletmede de sosyal mühendislik uygulamasına yönelmesi söz konusu olabilecektir.

Risk, gelecekte karşılaşılması muhtemel olaylardır. İşletme yönetiminin, işletmenin stratejik amaçlarına ulaşmasını sağlayacak veya engelleyecek muhtemel olayları belirlemesi gerekmektedir. İşletmelerin amaçlarına ulaşmayı engelleyecek unsurlardan biri hile riskidir. Hile riski; "yasal olmayan bir avantaj veya haksız bir kazanç sağlamak için aldatma dahil, yönetici, çalışan veya üçüncü kişiler arasından bir veya birkaç kişinin kasıtlı bir eylem gerçekleştirme olasılığıdır." (Kardeş Selimoğlu, Özbirecikli, & Uzay , 2017) Hile riski,

denetim teorisi açısından bir yapısal risk bileşenidir. Yönetsel süreçler içerisinde yönetimin çalışanlar veya yöneticiler tarafından yapılan riskleri tespit etmeye, önlemeye, analiz etmeye ve yönetmeye gereksinimi vardır. Hilenin dört unsuru vardır. Baskı; fırsat; haklı gösterme ve yetkinliktir. Kişiler veya kurumlar farklı baskı veya ihtiyaç durumları karşısında usulsüzlük yapma eğilimindedirler. Fırsat ise kurumdaki gerek kontrol gerekse de güvenlik boşlukları ve eksiklikleri nedeniyle olanaklı hale gelmektedir. Ancak gerek işletme için de gerekse de işletme dışındaki kişinin veya kurumun bu fırsatı fark edebilmesi ve bu fırsatı zaman içerisinde defalarca değerlendirebilmesi ancak yetkinliğine bağlıdır. Yetkinliğe sahip sosyal mühendisler, işletme içindeki fırsatları değerlendirerek eylemleri gerçekleştirmektedirler. İşletme yönetimi açısından işletmenin hile riskinin analizi yapılırken yetkinliklerin de göz önünde bulundurulması gereklidir. (Mengi, 2012)

İşletme yönetimi, sosyal mühendislere yönelik etkin bir bilgi yönetimi sistemi kurmalıdır. Özellikle sosyal mühendisliğin kullanıldığı alanlara yönelik geliştirilecek bir sistemin sağlayacağı yarar tartışılmazdır. Özellikle büyük verinin kullanılması, korunması ve aktarılmasına yönelik kontrol ve güvenlik politika ve prosedürlerinin belirlenmesi kritik önem taşımaktadır.

Bilgi teknolojilerinin varlığı ve sistemin etkinliği, işletmenin iç kontrol sisteminin etkinliğini arttırmaktadır. Teknoloji kullanımı bazı faydalar sağlarken, yeni risklere de ortam hazırlamaktadır.

Sosyal mühendislik saldırılarını önlemek, açıkları tam olarak kapatabilecek garanti edilmiş bir yöntem bulunmamakla beraber, riskleri azaltabilecek ve zararları minimize etmeye yönelik önlemler mevcuttur.

Bilgi teknolojileri denetimi, iç veya dış denetim olarak gerçekleştirilebilmektedir. Bilgi teknolojileri sistemleri denetimi iç denetimin içinde bağımsız bir grup tarafından gerçekleşebildiği gibi finansal ve uygunluk denetimleri ile bütünleşik bir şekilde de yürütülebilmektedir. Bunun yanı sıra, dışarıdan bir kuruluş tarafından da uygulanabilmektedir. (Yıldırım, 2017)

İç denetim birimi, bilgi sistemleri temelli hile riskini tespit etmeli, bilgi sistemlerine yönelik belirlenen politika ve prosedürlere uyum açısından güvence, aynı zamanda da

sistemin geliştirilmesi konusunda danışmanlık hizmeti vermelidir. Buna paralel olarak yönetimin eylemleri etkili biçimde uygulamasını sağlamak ve izlemek için denetim sonrası izleme süreci oluşturmalıdır. Aksi takdirde üst yönetim harekete geçmemenin riskini kabul etmelidir. Denetim sonrası izleme faaliyetleri sorumluluğu, iç denetim birimi yönetmeliğinde tanımlanabilmektedir. Dış bilgi sistemleri denetçileri, kendilerinin üzerinde anlaştıkları önerileri izlemek için bir iç bilgi sistemleri denetim birimine güvenebilmektedir. Uygulanmamış önerileri de kapsayan, denetim sonrası izleme faaliyetlerinin durumuyla ilgili bir rapor da var ise denetim komitesine veya işletme yönetimine sunulabilmektedir.

Sosyal mühendislik saldırılarına karşı alınabilecek önlemler hem bireysel hem kurumsal olarak bilgisayar ve ağ altyapısının dışında, düzenli eğitim ve çevresel güvenlik boyutlarını da içermelidir. İster teknoloji odaklı, ister insan odaklı yöntemler kullanılsın sosyal mühendislik saldırılarını önlemek amacıyla alınabilecek en etkin önlem human-firewall (insan güvenlik duvarı), yani insanın kendi yaşamında davranışlarına dikkat edeceği, uygulayacağı ve sorgulayıcı güvenlik duvarı olduğu unutulmamalıdır. (Yıldırım, 2017)

5. SONUÇ VE DEĞERLENDİRME

Sosyal mühendislik saldırıları kişileri ve kurumları hedef almaktadır. Saldırıların bireyler ve kurumlar üzerinde farklı etkileri bulunmaktadır. Kurumsal bilgi sistemlerinin güvenliği sadece teknik önlemlerin alınmasıyla sağlanmamaktadır. Sosyal mühendislik yöntemlerine karşı bireysel ya da kurumsal düzeyde en etkili savunma temel güvenlik politikalarının bilinmesi, uygulanması ve dış etmenlere karşı farkındalık sağlanmasıdır. Hayatın her anında bireyler ve kurumlar, çevresindeki insanlar ve teknolojik sistemler tarafından tehditlerle karşı karşıyadır.

Günümüzde insanlar, dış dünya ile şeffaf bir şekilde daha fazla etkileşim halindedirler. Dış çevreye, yeni tanışılan insanlara, teknolojik sistemlere karşı tedbirli davranmak, muhtemel senaryolar karşısında her zaman sorgulayıcı bir tutum içerisinde bulunmak güvenliği arttırmaktadır.

Güvenliğin korunması için sistemler kurulup, kurumlar geliştirdiği programlar ve yenilikler ile bir yandan güvenliği sağlarken, bir yandan da yeni oluşan dünya düzeni, bu sistemlerde daha fazla kişisel verilerin paylaşılmasına sebep olmaktadır. Basit bir örnek

ile akıllı cihazların insanların hayatını kolaylaştırmak için sunduğu bazı özellikler ve uygulamalar sosyal mühendisler için eşsiz bir kaynak olabilmektedir. Cihazlara kişisel bilgilerin kaydedilmesi, kredi kartı ve uygulama şifre bilgilerinin girişlerinin kayıtlı kalması, konum bilgilerinin paylaşılması, parmak izi okuyucuları, yüz tanıma sistemleri ve birçok sunulan özellik kişilere ait bilgilere kolayca erişim imkanı sunmaktadır. Güvenlik amacıyla yönlendirmelerle girilen bu bilgilerin tek bir yerde toplandığını ve en güvenli devletlerin bile sistemlerine sızılabildiğini ve şirketlerin daha sonra bu bilgileri ne amaçla kullanacağının bilinmediği düşünüldüğünde bu basit örnek ile sosyal mühendislik adına kafamızda büyük bir soru işareti belirmektedir. Bu bağlamda hem çevreyle hem de dış etkenlerle etkileşim kurulurken kişilere, kurumlara, internet ortamlarında dikkatli ve tedbirli olunmalıdır. Teknoloji ve internet bazında internet ortamının silgisiz olduğu unutulmamalıdır.

Toplum, sosyal mühendislik saldırılarına karşı eğitilmeli, bilinçlendirilmelidir. Dünya'da güvenlik açıklarına ve sosyal mühendislik saldırılarını yüzde yüz engelleyebilecek bir sistem, teknoloji ya da insan tutumu yoktur. Sürekli eğitim ve bilinçlendirme sosyal mühendislik saldırılarını engellemek adına en büyük silahtır.

Sosyal mühendislik olaylarına karşı temel kural olarak sorgulayıcı ve şüpheci yaklaşımdan asla vazgeçilmemelidir. Şifrelerin sosyal mühendislerin eline geçebilmeli ihtimaline karşı kâğıda yazarak cüzdanda ya da başkalarının ulaşabileceği yerlerde bulundurmamalı, telefona kaydedilmemelidir. Güvenilmeyen kurum ve kuruluşlara kimlik, ehliyet ya da fotokopi örnekleri bırakılmamalıdır.

Dolandırıcılık amacı ile farklı şekillerde telefonda kendisini savcı, asker, polis, bir kurum çalışanı vb. şekillerde tanıtan sosyal mühendisler belirledikleri hesaba para yatırılması gerektiğini ya da söyledikleri yerlere altın, para bırakılmasının istendiği bir telefon aramaskarşılaşıldığında ivedilikle 155[3] polis hattı aranmalıdır.

Her internet sitesi güvenli değildir. İnternet ortamında kredi kartı bilgileri, hesap numaraları paylaşılmamalıdır. Kredi kartlarınızla veya başka bir ödeme şekliyle yapacağınız alış-

3 Ülke genelinde, Bakanlık tarafından koordine edilen ve valilikler bünyesinde hizmet vermekte olan 112 acil çağrı merkezleriyle, 110 İtfaiye, 112 Sıhhi İmdat, 155 Polis İmdat ve 156 Jandarma gibi acil çağrı hizmetlerinin tüm illerde tek bir merkez altında birleştirilmesi ve acil çağrıların bu merkezlerden karşılanarak sevk ve koordine edilmesi hedeflenmektedir. 2010 yılında başlanılan proje kapsamında 2019 yılı itibariyle 45 ilde uygulanmaya geçilmiş, diğer illerde uyum çalışmaları ise devam etmektedir.

verişlerde sitenin güvenilir olup olmadığına dikkat edilmelidir. İnternet alışverişlerinde 3D güvenlik özelliği olan sitelerden ve sanal kart oluşturarak işlem yapmanız güvenliğinizi arttıracaktır. Ürün alışverişlerinizde site hakkında önce bir araştırma yapılmalıdır. Vergi levhaları olmayan şirketlerin sitelerinden alışveriş yapmamaya dikkat edilmelidir. Kredi kartı ve hesaplar 3. kişilere kullandırılmamalıdır. İyilik yapıldığı düşünülürken hesaptan ya da karttan yapılacak işlem sonucunda mağdur durumda kalınabilmektedir. Hesaba gelen ya da hesaptan giden bir paranın ne amaçla kullanıldığını hedef kişilerce bilinmemektedir. Yaşanılan dolandırıcılık örneklerinde hesabını kullandıran mağdurlar ile görüşmelerde 3. kişilerin hesap numarası olmadığı için iyilik amacıyla kendi hesap numarasını verdiği, gelen parayı da o kişiye verdiklerini bildirmektedir.

Sadece güvenliğinden emin olunan bilgisayarlardan işlem yapılmalıdır. Bilgisayarın nasıl korunduğu hususunda bir bilgi yoksa internet bankacılığı gibi riskli işlemler yapılmamalıdır. İnternet kafe gibi ortak kullanıma açık alanlardaki bilgisayarlarda ve iş yeri bilgisayarı gibi başkalarına ait ya da başkalarının erişimine açık bilgisayarlarda internet bankacılığı işlemi yapılması güvenli değildir.

Gün içerisinde insanlar birçok kez farklı insanlar ile etkileşim halindedir. Sosyal mühendislerin en büyük özelliklerinden biri elde etmek istediği bilgiye ulaşmak için hedef kişilerin ağzından laf almak ya da bir şekilde üçüncü kişilerden farklı yöntemlerle bu bilgiyi elde etmektedir. Kurum ya da bireysel olarak, hedef kişi için önemsiz olan bir bilgi, sosyal mühendis için çok şey ifade edebilmektedir. Tanımadığınız, yeni tanıştığınız kişiler ile iletişimde daha dikkatli olunmalıdır. Özellikle satış pazarlama alanında karşılaşılan kişilerin ikna etme kapasiteleri yüksek kişilerdir. Sorgulayıcı olunmalıdır.

Sosyal medya hesaplarınızda kişisel bilgilerin herkese açık görünür şekilde yer almasına izin verilmemesi gerekir. Sosyal mühendislerin en çok bilgi aldığı alanların biri de sosyal medya hesaplarıdır.

İnternet bankacılığı işlemleri yapılan bilgisayarın kişisel bilgisayar olması ve zararlı yazılımlara karşı her zaman güncel anti virüs programları kullanılması, hesap bilgilerinin hackerlerin eline geçmesini engelleyecektir. Bilgisayarlarda muhakkak düzenli olarak virüs taraması yapılmalıdır.

İnternet sitelerine arama motoru kullanarak giriş yapmak, kişilerin bilgilerini ele geçirme-

ye yönelik benzer isimler ile açılmış oltalama (phishing) diye tabir edilen siteye yönlendirebilmektedir. Sitenin yüzü ve içeriği aynı olmak ile beraber güvenli bir sitede gezinildiği düşünülmektedir. Kullanıcı bilgilerinin bu sitelere girilmesi, farklı kişisel bilgilerin girişi sonucunda sosyal mühendisler bu bilgileri ele geçirmektedir. İnternet sitelerine girişte arama motoru kullanmadan direk sitenin ismiyle giriş yapılması güvenliği artıracaktır. Bilinmeyen yerlerden gelen e-postalara itibar edilmemeli, açılmamalı, cihazdan ivedilikle silinmelidir. Bilinmeyen linkler tıklanılmamalıdır.

ATM işlemlerinde kart giriş yuvası, para çıkış haznesi ve cihazın herhangi bir yerinde kamera düzeneği olup olmadığı kontrol edilmeli, şifre girişi esnasında bastığınız tuşlar diğer elinizle gizlenmelidir. İlgili önlem POS üzerinden fiziki olarak yapılan alışverişlerde de kullanılmalıdır.

İhtiyaç duyulan dosyalar ve uygulamalar güvenli kaynaklardan ve mümkünse yasal olarak teyitli yapımcılardan indirilmelidir. Akıllı cihazlardan indirilen uygulamalar incelendiği zaman, indirilen bir uygulama kişi listesine, konuma, fotoğraflara ve birçok kayıtlı bilgiye ulaşabilmektedir.

Kurumlar ise bilgi sistemine yönelik hile karşıtı politikalarını ve prosedürlerini periyodik olarak değerlendirerek ve geliştirerek, sosyal mühendislerin kurumlarında yaratacakları zararları azaltıcı önlemeler almaya yönelik stratejiler belirlemelidirler.

Kaynakça

Bağcı, H. (2009, 02 18). Sosyal Mühendislik ve Denetim. 12 03, 2019 tarihinde http://kidder.org.tr/wp-content/uploads/denetisim/1.%20SAYI.pdf adresinden alındı

Basaran, A. (2016, 02 07). *Sosyal Mühendislik Saldırıları*. 12 05, 2019 tarihinde www.slideshare.net: https://www.slideshare.net/AlperBasaran/sosyal-muhendislik-saldrlar adresinden alındı

Gündüz, M. Z., & Daş, R. (2016). 12 01, 2019 tarihinde http://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-Yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf adresinden alındı

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.

Karabulut, Y. (2010, 5 4). 11 22, 2019 tarihinde http://www.karabulut.co/sosyal-muhendislik-evet-evet-teknigi/ adresinden alındı

Karabulut, Y. (2010, 3 28). 11 22, 2019 tarihinde https://www.karabulut.co/sosyal-muhendislik-moonlight-yontemi/ adresinden alındı

Karabulut, Y. E. (2010, 6 17). *"Önce Ver Sonra Geri Al" Tekniği / SM*. 11 22, 2019 tarihinde www.karabulut.co: http://www.karabulut.co/once-ver-sonra-geri-al-teknigi-sm/ adresinden alındı

Kardeş Selimoğlu, S., Özbirecikli, M., & Uzay , Ş. (2017). *Bağımsız Denetim.* Ankara: Nobel Akademik Yayınevi.

Katharina Krombholz, H. H. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*.

Mengi vd., B. T. (2013, 12 04). Yatırım Hileleri. Öneri Dergisi, 31-39. turkcebilgi.com: https://www.turkcebilgi.com/saadet_zinciri adresinden alındı

Mengi, T. (2012). HİIe DEnetiminde Yetkinliklerin Değerlendirilmesi-Hile Karosu. *Mali Çözüm*, 113-128.

TBB. (2015). *TBB.* 11 28, 2019 tarihinde www.tbb.org.tr: https://www.tbb.org.tr/Content/Upload/Dokuman/7328/TBB-Dolandiricilik-Eylemleri-ve-Korunma-Yontemleri.html adresinden alındı

teknochain.com. (2017, 05 28). 12 03, 2019 tarihinde teknochain.com: https://teknochain.com/ponzi-saadet-zinciri-nedir-dikkat-etmeniz-gerekenler/ adresinden alındı

terramedusa. (2019). 11 25, 2019 tarihinde terramedusa.com: https://terramedusa.com/man-in-the-browser-tehditi/ adresinden alındı

trendmicro.com.tr. (2019, 12 04). http://blog.trendmicro.com.tr/siber-saldirganlar-kalbimizi-calmaya-hazirlaniyor/ adresinden alındı

Vural, Y., & Sağıroğlu, Ş. (2011). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler . *Gazi Ünv. Mim. Müh.Fak. Dergisi*, 89-103.

www.trendmicro.com.tr. (2019). 12 01, 2019 tarihinde www.trendmicro.com.tr: https://www.trendmicro.com.tr/media/resource_lib/social/5-reasons-why-social-engineering-tricks-work-tr.pdf adresinden alındı

Yavanoğlu, U., Sağıroğlu, Ş., & Çolak, İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler. *Politeknik Dergisi*, 15-27. https://www.guvenliweb.org.tr/dosya/QvnJ1.pdf adresinden alındı

Yıldırım, S. (2017). Bilgi Sistemleri Denetim Süreçleri. *SERMAYE PİYASASI KURULU*.

Yılmaz, A. (2015). *Türkiye'deki Dolandırıcılık Tipolojileri: Dolandırıcılık Olaylarının Kategorik Tasnifi ve Yapılış Şekilleri.* Dr.Yılmaz,Abdurrahman ,"Türkiye'deki Dolandırıcılık Tipolojileri: Dolandırıcılık Olaylarının Kategorik Tasnifi ve Yapılış Şekilleri", İstanbul,2015.