PressAcademia Procedia - (PAP), ISSN: 2459-0762

PressAcademia Procedia

*Global Business Research Congress (GBRC), May 26-27, 2016, Istanbul, Turkey.*

# SOCIAL ENGINEERING: AN INFORMATION SECURITY THREAT IN ENTERPRISES

**DOI: 10.17261/Pressacademia.2016118649**

**Ali Acilar[1], Ayse Bastug[2]**

[1]Bilecik Şeyh Edebali Üniversitesi. ali.acilar@bilecik.edu.tr

[2]Bilecik Şeyh Edebali Üniversitesi. ayse.bastug@bilecik.edu.tr

## ABSTRACT

Today, information and communication technologies (ICTs) have become very important tools in business processes. However, especially with the widespread use of the Internet, security threats have also increased, such as customer information and business secrets fraud, changing the digital data easily, data theft, viruses and hackers etc. Furthermore, in many sectors if ICTs do not work a certain amount of time for various reasons, this failure can lead to large losses for the companies. ICTs and information systems in today are faced with many security threats. Whereas some of these security threats are related to technical issues such as software and hardware, human factor is considered as one of the most important security threats. Business employees are accepted as a source of many information security threats. One of these threats is social engineering. This study discusses social engineering as an information security threat in enterprises. Social engineering situations faced by enterprises and measures taken against them are discussed.

**Keywords:** Social engineering, information security, human factor
**JEL Codes:** M10, M15, M19

# İŞLETMELERDE BİR BİLGİ GÜVENLİĞİ TEHDİDİ OLARAK SOSYAL MÜHENDİSLİK

## ÖZET

Günümüzde bilgi ve iletişim teknolojileri işletmelerin iş süreçlerinde çok önemli bir hale gelmiştir. Fakat, özellikle internetin kullanımının yaygınlaşmaya başlamasıyla müşteri bilgilerinin ve işletme sırlarının başkaları tarafından ele geçirilmesi, sayısal verilerin değiştirilmesi, veri hırsızlığı, bilgisayar virüsleri ve korsanlar gibi güvenlik tehditleri de artmıştır. Ayrıca, birçok sektörde bu teknolojilerin çeşitli nedenlerle belli bir süre çalışmaması işletmeler için büyük zararlara sebebiyet verebilmektedir. Günümüz bilgi ve iletişim teknolojileri ve sistemleri birçok güvenlik tehdidi ile karşı karşıyadır. Bu tehditlerden bazısı yazılım ve donanım gibi teknik unsurları içerirken, bilgi güvenliğinde en önemli tehdit unsurlarından birisi olarak insan faktörü kabul edilmektedir. İşletme içinde çalışan insanlar birçok açıdan bilgi güvenliğini tehdit edebilmektedir. Bunlardan birisi de sosyal mühendisliktir. Bu çalışmada işletmelerde bir bilgi güvenliği tehdidi olarak sosyal mühendislik ele alınmaktadır. İşletmelerin sosyal mühendislik tehdidi ile karşılaşabileceği durumlar ve bunlara karşı uygulanabilecek önlemler ele alınmaktadır.

**Anahtar Kelimeler:** Sosyal mühendislik, bilgi güvenliği, insan faktörü
**JEL Kodları:** M10, M15, M19

## 1. GİRİŞ

Bilgi çağı olarak da adlandırılan günümüzde bilgi ve iletişim teknolojilerinin kullanımı dünya genelinde yaygınlaşmıştır. Bu teknolojiler, gerek bireylerin yaşantısında gerekse işletmelerin iş süreçlerini gerçekleştirmesinde önemli değişikliklere ve yeni iş modellerinin ortaya çıkmasına neden olmuşlardır. Internet World Stats Kasım 2015 verilerine göre 2000 yılından 2015 yılına kadar internet kullanıcı sayısı %832,5 artarak yaklaşık olarak 3,37 milyar kişiye (dünya nüfusunun yaklaşık %46,4'ü) ulaşmıştır. Türkiye'de Internet World Stats verilerine göre 46,3 milyon kişi (nüfusun yaklaşık %59,6'sı) internet kullanıcısı olduğu tahmin edilmektedir. Türkiye İstatistik Kurumu (TÜİK) tarafından gerçekleştirilen Hanehalkı Bilişim Teknolojileri Kullanım Araştırması sonuçlarına göre ise 2015 yılı Nisan ayında bilgisayar ve internet kullanım oranları 16-74 yaş grubundaki bireylerde sırasıyla %54,8 ve %55,9 olarak saptanmıştır.

Bilgi ve iletişim teknolojilerinin dünya genelinde yaygınlaşması ile birlikte bu teknolojiler, çok sayıda faydanın kaynağı olduğu gibi, kişisel gizliliği ihlal etmek için yeni fırsatlara da olanak oluşturmakta ve kişisel enformasyonların kayıtsızca kullanılabilmesini mümkün kılabilmektedir (Laudon & Laudon, 2011: 122). Gelişen bilgi ve iletişim teknolojileri ile bilginin saklanması, iletilmesi ve paylaşılmasının kolaylaşması ile birlikte aynı zamanda bilginin kolaylıkla değiştirilmesi, silinmesi, iletilmesi ve yanlış ellere geçmesi gibi önemli güvenlik tehditleri de ortaya çıkmıştır. Veri elektronik olarak saklandığı zaman, manüel olarak bulunmalarına kıyasla çok daha fazla tehdit türüne karşı savunmasızdır ve günümüzde internet başta olmak üzere ağ teknolojilerinin yaygınlaşması, enformasyon sistemlerinin gittikçe daha çok bir birine bağlanması, güvenlik tehdidini de arttırmaktadır (Laudon & Laudon, 2011: 293).

Bireyler ve işletmeler kullandıkları bilgi ve iletişim teknolojileri ile ilgili çok farklı güvenlik tehditleri ile karşı karşıyadır. İşletmeler bilgisayar donanımının bozulmasından kaynaklanan sistem arızaları ve programlama hataları, yanlış kurulum veya yetkisiz değiştirmeler ve yazılım sorunları gibi sorunlarla da karşılaşabilir (Laudon & Laudon, 2011: 294). Ayrıca elektrik kesintisi, seller, yangınlar veya diğer doğal afetler de bilgisayar sistemlerine zarar verebilir (Laudon & Laudon, 2011: 294). Cep telefonu, tablet vb. mobil cihazların bireysel amaçlarla olduğu gibi işletme amaçları için de kullanımının yaygınlaşması da çeşitli güvenlik sorunlarını ortaya çıkarabilmektedir; mobil cihazların, kaybedilmesi, çalınması kolaydır ve internete bağlı diğer cihazların karşılaşabileceği tehditlere de açıktır (Laudon & Laudon, 2011: 294). Günümüze kadar birçok virüs, Truva atı, solucan vb. kötü amaçlı yazılımlar dünya genelinde çok büyük maddi zarara neden olmuştur ve bunlara her geçen gün yenileri eklenmektedir. Diğer bir güvenlik tehdidi de bilgisayar sistemine yetkisiz erişim sağlamaya çalışan bilgisayar korsanlarıdır (Laudon & Laudon, 2011: 298). Dünya genelinde, bilgisayar suçu sorununun büyüklüğü, kaç bilgisayar sisteminin saldırıya uğradığı, kaç kişinin fiili olarak bununla meşgul olduğu veya bilgisayar suçunun neden olduğu toplam ekonomik hasar bilinmemekte olup; çoğu işletme, suçlara çalışanların karışmış olabildiği için veya işletme itibarına, şöhretine zarar vereceğinden endişe ettiği için bilgisayar suçlarını rapor etmeye isteksizdir (Laudon & Laudon, 2011: 300).

Bilgi güvenliği, bilginin; gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak tanımlanabilir (Mellado, Fernández-Medina & Piattini, 2007). Bilginin gizliliği, bilginin ulaşmaya yetkisiz kişilerin eline geçmemesi, bilginin bütünlüğü: bilginin yetkisiz kişilerce değiştirilmemesi, doğruluğu ve tamlığının sağlanması, bilginin erişilebilirliği: bilginin ulaşmaya yetkili kişiler tarafından gerektiği zaman ulaşılabilir ve kullanılabilir olmasıdır (TÜBİTAK, BİLGEM; Mellado, Fernández-Medina & Piattini, 2007). Bilgi güvenliği, her sektör ve büyüklükteki organizasyonun sürekliliğinin sağlanmasında büyük önem taşımakta olup, organizasyonun başta elektronik olmak üzere, farklı ortamlardaki kritik bilgilerinin ve diğer bilgi varlıklarının korunmasına yardımcı olur (Eminağaoğlu & Gökşen, 2009). Sadece büyük şirketler, holdingler değil bunun yanı sıra bireyler, küçük ve orta büyüklükteki işletmeler (KOBİ'ler), devlet kurumları veya kar amacı gütmeyen herhangi bir organizasyon, eğitim kurumları, sağlık kurumları vb. de bilgi güvenliği sorunları ve risklerini farklı düzeylerde de olsa sürekli yaşamaktadır (Eminağaoğlu & Gökşen, 2009). Her büyüklükteki işletme, bilgisayar kullandığı ve internete bağlı olduğu müddetçe güvenlik tehditleri ile karşı karşıya olmakla birlikte büyük işletmeler, bilişim güvenliğini sağlayacak teknik bilgi ve maddi güce sahipken, KOBİ'ler genel olarak bu kaynaklara ve yeteneklere tamamıyla sahip olamamaktadır (Acılar, 2009, b).

İşletmelerde bilgi güvenliğinin sağlanması, sadece bilişim uzmanlarını ilgilendiren teknik bir konu değildir,

işletmede çalışan herkesin bilgi güvenliğinin sağlanması ile ilgili sorumluluğu bulunmaktadır (Johnson & Goetz, 2007). Bir işletmeye yönelik güvenlik tehditlerinin örgüt dışından geldiğini düşünme eğiliminde olsak bile aslında işletme içinde çalışanların ciddi güvenlik sorunlarına yol açtıkları görülmektedir (Laudon & Laudon, 2011: 302). Bilgi güvenliğini tehlikeye sokan en önemli tehditler, sanıldığı gibi kurum dışından gelen saldırılar değil, çalışanların yanlış işlem ve davranışlarıdır (Thomson, Solms & Louw, 2006). İşletmede çalışanlar, ayrıcalıklı enformasyona erişebilir ve yetersiz iç güvenlik kuralları varsa örgütün tüm sisteminde hiç bir iz bırakmadan dolaşmaları mümkündür (Laudon & Laudon, 2011: 302). Pek çok çalışan bilgisayar sistemlerine erişmek için kullanılan şifrelerini unutur veya çalışma arkadaşlarına bu şifreleri kullanmaları için izin verir, bu durum da sistemi tehlikeye düşürür (Laudon & Laudon, 2011: 302). İşletme sistemine erişmek isteyen kötü niyetli saldırganlar bazen işletmenin bir çalışanı gibi davranarak çalışanları kandırarak şifrelerini elde edebilirler, bu yönteme sosyal mühendislik (social engineering) denir (Laudon & Laudon, 2011: 302).

İşletmelerde bilgi güvenliğinin sağlanması için sadece yazılım, donanım ve fiziki güvenlik tedbirlerinin alınması yeterli değildir, bunlarla birlikte işletmede çalışan herkesin bilgi güvenliğinin sağlanmasında önemli görev ve sorumlulukları vardır. İşletmede bilgi güvenliği sağlanırken gerekli teknik önlemlerin alınmasının yanında bilgi güvenliğinde en zayıf halka olarak da kabul edilen insan faktörü de unutulmamalıdır (Acılar, 2009, a). Farklı güvenlik sorunlarına karşı çok miktarda teknolojik yöntem geliştirilmiş olmasına rağmen önemli güvenlik ihlallerine neden olabilen insan faktörleri alınan teknolojik tedbirlere göre ihmal edilmiştir (Luo, Brody, Seazzu & Burd, 2011). Güvenlik ürünlerinin tek başlarına tam bir güvenlik sağlayacağına inanmak, ancak hayal aleminde görülebilecek bir durum olup, güvenlik konusunda kendi kendini kandırmaktır ve er ya da geç, kaçınılmaz olarak bir güvenlik sorunu yaşanmasına neden olur (Mitnick, 2009: 4).

Bu çalışmada, işletmelerde bir bilgi güvenliği tehdidi olarak sosyal mühendislik ele alınmakta olup, işletmelerin sosyal mühendislik tehdidi ile karşılaşabileceği durumlar ve bunlara karşı uygulanabilecek tedbirler sunulmaktadır.

## 2. SOSYAL MÜHENDİSLİK

Sosyal mühendislik, çalışanları ve tüketicileri kandırarak, ağlar veya hesaplarına erişmek için bunları kullanma sanatı olarak tanımlanabilir (Conteh & Schmick, 2016). Sosyal mühendislik, bilişsel önyargılar olarak bilinen insan mantığı açıklarından faydalanarak istenilen bilgilere erişmek için kötü niyetli saldırganlar tarafından kullanılan bir tekniktir (Luo, Brody, Seazzu & Burd, 2011). Sosyal mühendislik, bilgi güvenliği için potansiyel bir tehdittir ve bilgi güvenliğinde teknolojik tehditlerle beraber eşit derecede önemli olduğu kabul edilmelidir (Luo, Brody, Seazzu & Burd, 2011). Teknolojik kontrol dışında ve insan doğasına konu olduğundan sosyal mühendislik, kuşkusuz enformasyon sistemi güvenlik yönetimi alanında en zayıf halkalardan biridir (Luo, Brody, Seazzu & Burd, 2011).

Schneier (2000) başarılı bir sosyal mühendislik atağını 5 adımda açıklamaktadır: 1. adımda hedef seçilir ve hedef ile ilgili birçok kaynaktan çeşitli bilgiler toplanır, 2. adımda toplanan bilgiler analiz edilir, 3. adımda saldırgana iletişim kanalları ile erişilir, 4. adımda ikna ve aldatma yöntemleri ile atak uygulanır, son olarak 5. adımda ise atak tamamlanır ve tüm kanıtlar ortadan kaldırılır (Parsons, McCormac, Butavicius & Ferguson, 2010).

Sosyal mühendislik saldıran profili genel olarak aşağıdaki şekillerde özetlenebilir (TÜBİTAK BİLGEM, 2008):

*1. Otoriter tutum*: Uzman veya üst düzey bir yetkili olduğuna inandırmak.

*2. Yardım teklif etmek*: Kendini yetkili bir kişi gibi göstererek problem oluşturup onu çözümlemek ya da var olan bir problem için yardım önerilerinde bulunmak.

*3. Ortak alanlar bulmak*: Hedef kişi hakkında sanal veya gerçek ortamlardan bilgiler toplayarak, ortak alanlara sahipmiş gibi gösterip hedefle yakınlaşmak.

*4. Karşılık beklemek*: İstenen bir iyilik için bir karşılık önermek.

*5. Bağlılık ve dürüstlüğü kötüye kullanmak*: Çalıştığı kuruma bağlı bir personeli, istenilenlerin yapılmaması halinde kurumun zararları olacağına inandırmak.

*6. Düşük bağlılıktan yararlanmak*: Kuruma bağlılığı zayıf olan personeli aldatmak, ikna etmek.

Sosyal mühendislerin hedefindeki bazı tipik saldırılan profilleri ise şu şekilde özetlenebilir (TÜBİTAK BİLGEM, 2008):

*1. Direkt ulaşılabilir personel*: İşi gereği müşteri ve sağlayıcılarla iletişim içerisinde olan elemanlar.

*2. Önemli personel*: Ayrıcalıklı görev ve erişimleri olan personeller.

*3. Sempati sahibi personel*: Kurum içinde yetkilerinin dışına çıkarak veya kurum içindeki itibarını kullanarak müşterilerine yardımcı olmaya çalışan personel.

*4. Destek ihtiyacı olan son kullanıcılar*: Sistemlere erişimi bulunan fakat destek almaları gerektiğinde meşru destek personeli ile kötü niyetli saldırganı ayırt edemeyebilecek kullanıcılar.

*5. Aldatılmış, ikna edilmiş personel*: Kuruma ya da çalışanlarına olan bağlılığı azalmış personel.

Sosyal mühendisler, genel olarak ikna kabiliyeti yüksek, iyi giyimli, sorulara karşı hazırlıklı, etkili senaryolar üreten, taklit yeteneği olan, iletişimi güçlü, kendini iyi pazarlayabilen insanlardır.

## 3. SOSYAL MÜHENDİSLİK SALDIRILARI

Sosyal mühendislik yöntemleri saldırganların zekâ ve yetenekleri doğrultusunda artırılabilir. Ancak bu çalışmada en çok karşılaşılabilen sosyal mühendislik saldırı yöntemleri ele alınmıştır:

### 3.1. Sahte Senaryolar Uydurmak (Pretexting)

Hedefin kişisel veya iş bilgilerini çalmak için onu hiç şüphelendirmeyecek şekilde saldırgan tarafından inandırıcı sahte senaryoların üretildiği sosyal mühendislik saldırı yöntemidir (Conteh & Schmick, 2016). Telefonla yapılan sosyal mühendislik saldırılarında genelde sahte senaryo üretme yöntemine başvurulur. Saldırgan internet ortamından veya saldırı hedefinin yakın çevresinden edindiği bilgiler ile iletişime geçer. Korku uyandırarak, yetkili kişi gibi davranarak, işe yeni başlamış biri gibi davranarak, aciliyeti vurgulayarak vb. tutumlarla farklı senaryolar üreterek insanları aldatıp saldırı için kullanabileceği bilgileri ele geçirmeye çalışırlar.

### 3.2. Oltalama Saldırıları (Phishing)

Hedef kişiye ait şifre, kart bilgileri gibi hassas bilgileri genellikle e-posta ile aldatarak elde etme yöntemidir (Ferreira & Lenzini, 2015). Oltalama e-postaları, insan psikolojisinden faydalanarak güvenilir bir kaynak gibi görünüp, hedefteki kişiyi bilgi ve parasını vermeye ikna etmeye çalışmaktadır; gönderen kişi tanınmayan biri olabileceği gibi iş, okul, arkadaş görünümü veren hedef odaklı oltalama (spear phishing) e-postaları gönderen sahte kimlikte biri de olabilir (Ferreira & Lenzini, 2015).

Ferreira & Lenzini (2015)'e göre oltalama e-posta metinlerinde bulunan ve ikna etkisini artıran başarılı etkenlerden bazıları şunlardır: kurum iletişim bilgileri, farklı yazı tipi ve büyüklükleri, bilinen bir insanı eke ekleyerek sohbet etme imkanı veren ikonlar, güvenlik şirketine ait bilgi ve logo (güvenilir izlenimi veren ipucu olarak), güncel telif hakkı (copyright) bilgisi, cevap verilmesi için sınırlı bir süre, korkuya neden olan ifadeler, LinkedIn'e bağlanma daveti, e-posta göndericisine iletimi başarısız mailler, yetkili kişi olduğunu belirten ifadeler, linkler, Sayın Müşterimiz şeklinde başlayan girişler, vb.

### 3.3. Tuzak Donanımlar (Baiting)

Mailler yerine usb, dvd, cd gibi donanım aygıtlarına zararlı yazılımlar yüklenerek yapılan saldırı türüdür (Rao & Nayak, 2014, 318). Saldırganın niyeti zararlı yazılımları bilgisayara ve sisteme bulaştırarak, sistem ve ağdaki erişim yetkisinin olmadığı bilgilere erişebilmektir (Rao & Nayak, 2014, 318).

Rao & Nayak (2014, 318)'e göre bu saldırı senaryoları şu şekilde gerçekleşir: Zararlı yazılım yüklenmiş donanım parçaları kurum içerisinde dinlenme alanları, asansörler, resepsiyon gibi ortak sık kullanım alanlarında veya kurum dışında binaya yakın konumlarda ilginç isimler verilerek bırakılır ve bu aygıtları bulan çalışanlar içerisinde ne bulunduğunu keşfetmek isteyip bilgisayarlarına taktıklarında farkında olmadan zararlı içeriği sisteme bulaştırırlar. Böylelikle saldırganlar uzaktan erişim yöntemleriyle kurum içi bilgilere ulaşırlar, ayrıca bu saldırıda sadece bir noktaya bırakmak yoluyla değil çalışanlara ortam dinlemeli, kameralı, zararlı yazılımlı ürünler hediye

edilerek de başarıya ulaşılabilinir (Rao & Nayak, 2014, 318).

## 3.4. Çöp Karıştırmak (Dumpster Diving)

Çöp karıştırma, değerli bilgiyi çöpte araştırma ile ilgilidir (Long, 2007: 2). Çöp karıştırma bir sistemi veya bir kullanıcının potansiyel faydalı bilgilerini elde etmek için bir köşeye atılmış kâğıt, CD gibi öğeleri çöp torbası içerisinden ayrıştıran bir yöntemdir. İsim, adres, numara, şifre gibi kişisel bilgilere, şirket dosyalarının düzenleme aşamalarındaki çıktı örneklerine, hatırlatıcı bilgilere, eski kayıtlara bu şekilde erişilerek hedef hakkında bilgiler toplanır. Buna karşı en basit strateji kâğıt öğütücü makinelere yatırım yapılmasıdır (Parsons, McCormac, Butavicius & Ferguson, 2010). Çöp kutuları içerisinde hassas ve değerli bilgiler bulunabileceği için bu kâğıtları, olası tehditleri elimine etmek için öğütmek gerekmektedir. Çöp karıştırma yöntemiyle elde edilen bilgiler sahte senaryo üretme, oltalama saldırısı gibi yöntemlerde kaynak olarak kullanılabilir.

## 3.5. Omuz Sörfü Ve Kulak Misafirliği

Kullanıcı giriş bilgileri gibi çalışanlara ait bilgileri elde etmek için başkasına omuz üzerinden klavye veya ekranlarına bakmak gibi doğrudan gözlem tekniklerine başvurulduğu sosyal mühendislik saldırı yöntemidir (Krombholz, Hobel, Huber & Weippl, 2014). Bu yöntemde çalışan kişi konuşturularak dikkatini dağıtmak başarı oranını artırır. Ayrıca kulak misafirliği yapılarak çalışanlar gizlice dinlenip bilgiler herhangi bir olası saldırı için kullanılabilir.

## 3.6. Tersine Sosyal Mühendislik

Hedefle doğrudan ilişki kurmak yerine saldırganın, karşı tarafı güvenilir bir kaynak olduğuna ikna ederek hedefle yakın ilişki kurmaya çalışması olan bu dolaylı yaklaşım, tersine sosyal mühendislik olarak bilinir ve 3 temel bölümden oluşur: sabotaj, bildirme, yardımcı olma (Krombholz, Hobel, Huber & Weippl, 2014): İlk adımda kurumun bilgisayar sistemine sabotaj yapılır, böylelikle herhangi bir yerde kurumun bilgisayar ağından, hedef kişilere hileli yazılım uygulamaları bulaştırılır, saldırgan hedef kişiye bu problemi çözebileceğini bildirir. Hedef yardım istediğinde ise sosyal mühendis kendisinin neden olduğu bu problemi çözer. Örneğin, şifresini ister veya bazı yazılımları yüklemesi gerektiğini söyler. İçeriğinde virüsler gibi zararlı öğeler bulunan bu yazılımlar yüklendiğinde hedef bilgisayarına veya ağına erişilerek bilgiler ele geçirilebilir (Krombholz, Hobel, Huber & Weippl, 2014).

## 3.7. Başka Bir Siteye Yönlendirme (Pharming)

Hedef bilgisayarının host dosyası değiştirilerek veya DNS sunucusu sömürülerek sahte bir domain kaydı oluşturulup yasal siteye olan tüm girişlerin doğrudan sahte siteye yönlendirildiği pasif bir sosyal mühendislik saldırı yöntemidir (Spinapolice, 2011). İnsanlar adres çubuğuna doğru web adresini girseler bile sahte web adresine yönlendirilirler. Genelde banka veya satış siteleri gibi yasal sitelerin bir kopyası oluşturulup, hedefi gerçek bir siteye girdiğini düşündürerek web sitenin türüne bağlı olarak girmiş olduğu kredi kartı numarası, kullanıcı adı, şifreler gibi bilgilere ulaşabilmek amaçlanmaktadır (Spinapolice, 2011). Burada aldatma, sadece tasarım olarak yasal web sitesinin kopyasını oluşturulmasını sağlayarak değil ayrıca www.nicebank.com site adresine benzer olarak www.n1cebank.com adresinin kullanılması gibi yasal web site internet adresinin küçük değişikliklerle benzerini oluşturmakla da sağlanabilir (Spinapolice, 2011).

## 3.8. Sesle/Telefonla Oltalama (Vishing)

Saldırganların, IP üzerinden ses (VoIP) uygulamasını kullandığı yeni bir sosyal mühendislik saldırı yöntemidir (Milli Eğitim Bakanlığı Bilişim Teknolojileri Ağ güvenliği, 2013). Sesle oltalamada, güvenilir bir kullanıcıya geçerli bir telefon bankacılığı hizmeti gibi görünen bir numarayı aramasını bildiren sesli mesaj gönderilir ve bunun sonucunda kullanıcının yaptığı aramaya bir saldırgan tarafından müdahale edilir (Milli Eğitim Bakanlığı Bilişim Teknolojileri Ağ güvenliği, 2013). Doğrulama için telefondan girilen banka hesap numaraları veya parolalar çalınarak istenilen bilgilere erişilmiş olunur (Milli Eğitim Bakanlığı Bilişim Teknolojileri Ağ güvenliği, 2013).

## 4. SOSYAL MÜHENDİSLİK TEHDİTLERİ

Başarılı sosyal mühendislik saldırıları, işletmelerde çeşitli tehlikelerin gerçekleşmesine neden olabilmektedir. Bunlar aşağıdaki gibi sıralanabilir (TÜBİTAK BİLGEM, 2008):

*1. Yetkisiz erişim*: Saldırgan, sisteme erişim sağlamak için gerekli bilgileri ele geçirebilir.

*2. Hizmet hırsızlığı*: Ele geçirilmiş şifre ile saldırgan erişimi olmayan belgelere ulaşabilir ya da bant genişliği, işlemci zamanı, disk alanı gibi sınırlı kaynakları kullanabilir.

*3. İtibar ve güven kaybı*: Sosyal mühendislik yoluyla zarara uğramış bir kurum, müşterilerinin ve toplumun gözünde değer kaybedebilir ve yeniden güven kazanmanın bedeli, çoğunlukla baştan önlem almaktan çok daha yüksek olabilir.

*4. Dağıtık hizmet engelleme*: Ele geçirilen sistem ve kaynaklar, kötü amaçlı kişiler tarafından başka sistem ve kaynakların ele geçirilmesi ya da zarar verilmesi için kullanılabilir. Bu durumda dolaylı olarak başka saldırılara sebep olunabilir ve saldırının kaynağı aynı zamanda kurban olabilir.

*5. Hassas bilgiye erişim ve veri kaybı*: Başarılı bir yöntemle kurumun ve müşterilerinin bilgileri ele geçirilebilir. Kurum aleyhinde suiistimal için kullanılabilir ve satılabilir. Saldırgan sadece kurumun zarar görmesini istiyorsa da bilgiye erişimi engelleyebilir, şifreleme ve silme gibi yöntemlerle erişimi imkânsızlaştırabilir.

*6. Yasal yaptırıma uğramak*: Müşteri ve iş ortaklarıyla yapılan gizlilik ve güvenlik anlaşmalarının ve hassas bilgiyi korumak için önlem almamanın yasal sonuçları ve yaptırımları olabilir.

## 5. SOSYAL MÜHENDİSLİK ÖNLEMLERİ

Yüzde yüz bilgi güvenliğini sağlamak imkânsız olup bu kapsamda sosyal mühendislik saldırılarını da tamamen önlemek mümkün değildir. Her çalışanın kişisel özellikleri farklı olduğu için sosyal mühendislik saldırıları için doğru önlemleri bulmak ve onları başarıyla uygulamak da oldukça zordur, ancak bu durum sosyal mühendislik saldırıları için hiçbir tedbir alınmayacak anlamına gelmemektedir (Rao & Nayak, 2014: 320). Bireylerin yanı sıra organizasyonların da, sosyal mühendislik saldırılarından korunmak için bilinçli çalışmalar yapması gerekmektedir (Rao & Nayak, 2014: 320). Organizasyonlar tarafından alınması gereken önemli tedbirlerden bazıları şunlardır (Rao & Nayak, 2014: 320-322, Conteh & Schmick, 2016):

- Kurum çalışanlarından, müşterilerinden, tedarikçilerden beklenen tutumları ve kabul edilemez durumları açıkça içeren, anlaşılabilir ve uygulanabilir güvenlik politikaları belirlenmelidir.
- Tedarikçilerle yapılan anlaşmalar, bilgi güvenliği ile ilgili yapılması ve yapılmaması gereken önemli maddeleri ve bir ihlal söz konusu olduğunda sonuçlarını içermelidir.
- Personel ile yapılan sözleşmelerde, personelin kurum içinde çalışırken ve hatta kurumdan ayrıldıktan sonra da sürecek sorumluluklarını içeren maddeler bulunmalıdır.
- Bilgi güvenliği ile ilgili yapılması ve yapılmaması gereken durumları ayrıntılı ve açık bir şekilde ifade eden bilgi güvenliği farkındalık eğitimleri düzenli olarak yapılmalıdır ve gerektikçe üzerinde değişikliğe gidilmelidir. Ayrıca yenilenme eğitimlerinin düzenli ve periyodik olarak yılda en az bir kez yapılmasına ihtiyaç vardır.
- Bilgi güvenliği olay raporlama mekanizması kurulmalıdır. Bilgi güvenliği ile ilgili durumların nedenleri, buna uygun doğru çözümler analiz edilmelidir. Doğru bir çözümü garantilemek için hedeflenen süre içerisinde işlemler yapılmalıdır.
- Tüm erişim yetkileri periyodik olarak gözden geçirilmeli ve 'gerektiği kadar yapacak' 'gerektiği kadar bilecek' şekilde erişimler revize edilmelidir. Yetkilendirmeler çalışanların işlerini olumsuz etkilemeyecek şekilde en düşük seviyede tutulmalıdır. Yeniden incelemeler sırasında, çalışanın bir uygulamaya veya dokümana geçici erişimi olduğu halde bu erişimin hala devam ettiği fark edildiğinde erişimi durdurulmalıdır. Aynı şekilde daha önceki pozisyonu için gerekli ancak şirketteki şu anki güncel rolü için gerekli olmayan yetkiler sonlandırılmalıdır. Terfi gibi durumlarda gerekli yetki düzenlemeleri yerine getirilmelidir.

- Çok gizli veriler güvence altına alınmalı ve bunlara erişimler sıkı bir şekilde kontrol edilmelidir. Mümkünse bu gizli veriler, diğer verilerden ayrı bir şekilde konumlandırılmalıdır.
- Tüm veriler uygun olarak sınırlandırılmalı ve verilerin hassaslıklarının ve kısıtlamalarının farkına varılabilmesi için bu nitelikleri belirtilmelidir.
- Çalışanlar şifre, kart bilgileri, kimlik bilgileri gibi değerli bilgilerini açığa çıkarmama konusunda duyarlı olmalıdır.
- Sistem, kullanıcıları güçlü parolalar (İçerisinde rakam, özel karakter, büyük harf, küçük harf olmalı ve en az 8 karakterden oluşmalı gibi) kullanması için zorlamalıdır. Sistem tarafından zayıf şifreler kabul edilmemelidir. Belirli sayıdaki başarısız oturum açma girişimlerinden sonra sisteme erişim yasaklanmalıdır. Belirli aralıklarla şifre değişikliği yapmaları zorunlu olmalıdır.
- Hassas bilgilerin bulunduğu alanlarda ek olarak bir güvenlik seviyesi bulunmalıdır.
- Tüm çalışanların her zaman yaka kartları takılı olmalıdır. Bu, dışarıdan gelen bir ziyaretçi ile kurum çalışanının ayırt edilmesini sağlar.
- Ziyaretçi politikası açık olmalıdır. Ziyaretçilere her zaman kurum içinden bir çalışan eşlik etmelidir.
- Atığa çıkmış kâğıtlar çöp kutusuna atılmadan önce kâğıt öğütücülerde parçalanmalıdır.
- Temiz masa, temiz ekran politikası çalışanlar tarafından benimsenmelidir. Yani masada monitör ekranında kurum hakkında bilgi verecek bir şey bulunmamalıdır.
- Çalışanlar gizli konuşma yaparken alçak sesle konuşması konusunda uyarılmalıdır. Ya da bu konuşmaları kapalı odalarda gerçekleştirmesi önerilmelidir.
- Şifrelerin riske atılmaması için hassas sunucular veya ağ donanımlarında çok faktörlü kimlik doğrulama tanımlanmalıdır.
- Ek erişim için tüm izinler iyice gözden geçirilmelidir. Çalışan, müşteri, tedarikçi için gerekli olacak kadar bir erişim dikkate alınmalıdır.
- Zararlı yazılımlara karşı güçlü programlar yüklenmelidir. Organizasyonlar her zaman bu programların güncelliğini sürdürdüğünden emin olmalıdır.
- İşletmeler, çalışanlarının işten ayrılış prosedürlerini takip etmelidir. Çalışanın sunucuya veya uygulamaya erişimi varsa bu hakları iptal edilmeli ve yönetici şifreleri sürekli olarak değiştirilmelidir.
- Çalışanların ve işten ayrılanların kayıtları sıkı bir şekilde takip edilmelidir. Eski bir çalışanın kimlik doğrulama yapabilmesine ve örgüt içerisine girebilmesine izin verilmemelidir.
- Bilgi güvenliği politikalarına olan bağlılık düzenli iç denetimlerle yürütülmelidir. Hemen düzeltilmesi gereken sorunlar tespit edilmelidir.
- Sistemin savunmasızlığını tespit edebilmek ve uygun düzeltici önlemleri alabilmek için yılda en az bir defa sosyal mühendislik etki testleri yapılmalıdır.
- Şirket bilgilerinin korunması için şirket ağında çoklu güvenlik katmanları bulunmalıdır. Saldırı önleme sistemleri, saldırı bulma sistemleri ve güvenlik duvarları her bilgisayara yüklenmelidir. Web filtreleri ve sanal özel ağlar kurumun sistemine kurulmalıdır.

Bunlara ek olarak ayrıca;

- İşten ayrılan personele ait üzerine zimmetli tüm mallar ve evraklar alınmalıdır, ayrılan personelin kaydı telefon rehberi gibi listelerden silinmelidir.
- Sunucular ve diğer önemli donanımlar, güvenli ve kilitli alanlarda muhafaza edilmelidir.
- Şirket içindeki bilgisayar, yazıcı, faks makinesi gibi cihazların kullanım koşulları ile ilgili politikalar belirlenmelidir. Örneğin faks gönderilirken karşı tarafta doğru kişinin bulunduğundan emin olunmalıdır.
- Bilgi güvenliği farkındalığı oluşturulmalıdır. Bilgi güvenliği farkındalığı birçok kanal kullanılarak sağlanabilir. Örneğin; panolara asılmış bilgilendirici posterler, duyurular, ekran koruyucuları, broşürler, e-postalar, eğitimler (yüz yüze veya online) bunlardan bazılarıdır.
- Şirket içi politikalara uyan kişiler ödüllendirilip, uymayan kişiler hakkında cezai süreç başlatılması kişilerin davranışlarının şekillenmesinde önemlidir.

Bireyler tarafından alınması gereken önemli tedbirlerden bazıları ise şunlardır (Rao & Nayak, 2014: 322-323):

- Kişisel hassas bilgileri isteyen taleplere karşı dikkatli olunmalıdır. Şüpheye düşülen durumlar olay bildirim birimlerine aktarılmalıdır.
- Kurum dışından karşı tarafın iddia ettiği kişi olup olmadığı resmi kurumsal siteden kontrolü yapıldıktan sonra işlemler gerçekleştirilmelidir.
- Her zaman güçlü parolalar oluşturulmalıdır. Farklı sistemlerde aynı parolalar kullanılmamalı ve belirli aralıklarla değiştirilmelidir.
- Şifreler bir başkasının görebileceği yerlere yazılmamalıdır.
- Eğer yanında birileri varken bilgilerin girilmesi gerekiyorsa çalışan dikkatli bir şekilde bilgileri gizlemeye çalışarak girilmelidir.
- Bilgisayarlarda oturum açma işlemleri parolalı olmalıdır.
- Bilgisayar ekranları kullanılmadığında kilitli olmalıdır.
- Bilgilerin yazılı olduğu kopyalar yok edilmelidir.
- Kişisel bilgiler herhangi bir ortamda başkalarına paylaşılmamalıdır.
- Telefon ile konuşma yaparken kişisel bilgiler verilmemelidir. Bankalar gibi kimlik doğrulanması yapılması gereken durumlarda az ve yeterli bilgi paylaşılmalıdır.

Yukarıda belirtilen tedbirlere ek olarak;

- Aceleci, dikkatsiz tutumlar sergilenmemeli, emin olunduğunda işlemlere devam edilmelidir.
- Kurum içinden olduğunu iddia eden biri önemli bilgileri istediğinde hemen verilmemeli çalıştığı birimden kontrolü yapılarak paylaşımda bulunulmalıdır.
- Bilgisayardaki güvenlik duvarı, anti virüs programları her zaman güncel tutulmalıdır.
- Bilgi işlem tarafından kontrol edilmeyen yazılım ve uygulamalar bilgisayarlara kurulmamalıdır.
- Bir yerlere bırakılmış ya da birileri tarafından hediye edilmiş donanımlar şirket bilgisayarlarında ve ağında açılmamalı ve bir kayıt cihazı barındırıp barındırmadığı kontrol edilmelidir.
- Güvenilir olmayan kaynaklardan gelen e-postalar açılmamalı ve ek dosyaları indirilmemelidir.
- İnternette ziyaret edilen sitelerin gerçek kurumsal bir site olup olmadığına dikkat edilmelidir.

## 6. SONUÇ VE DEĞERLENDİRME

Günümüzde bilgi ve iletişim teknolojileri, özellikle internet, işletmelerin iş süreçlerinde çok önemli bir hale gelmiş olmakla beraber, aynı zamanda işletmelerde bilgi güvenliği tehditlerinin artmasına da neden olmuştur. Bu güvenlik tehditleri içerisinde insan faktörü belki de en karmaşık ve güvenlik önlemi alınmasında en zorlu kısmını oluşturmaktadır. İşletme çalışanlarının neden olabileceği önemli bilgi güvenliği tehditlerinden biri de sosyal mühendisliktir. Bu çalışmada işletmelerde bir bilgi güvenliği tehdidi olarak sosyal mühendislik ele alınmıştır. İşletmelerin sosyal mühendislik tehdidi ile karşılaşabileceği durumlar ve bunlara karşı uygulanabilecek önlemler sunulmuştur. Sosyal mühendislik ile ilgili farkındalığın artması için bu alanda yapılan ve yapılacak çalışmalar önem arz etmektedir. Ülkemizde farklı sektörlerde faaliyet gösteren işletme çalışanlarının sosyal mühendislik saldırıları ile ilgili bilgi düzeyleri ve bu saldırılara karşı tutumlarına yönelik yapılacak akademik çalışmalar bu konunun aydınlatılmasına ve sosyal mühendislik ile ilgili alınacak önlemlerin daha da geliştirilmesine katkıda bulunacaktır.

## KAYNAKLAR

Acılar, A. (2009, a). İşletmelerde Bilgi Güvenliği ve Örgüt Kültürü, Organizasyon ve Yönetim Bilimleri Dergisi, 1(1), 25-33.

Acılar, A. (2009, b). KOBİ'lerde Bilişim Teknolojileri Güvenliği Sorunu: Tehditler ve Önlemler, Afyon Kocatepe Üniversitesi, İ.İ.B.F. Dergisi, 11(1), 1-16.

Conteh, N. Y. & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks, International Journal of Advanced Computer Research, 6(23), 31-38.

Eminağaoğlu, M. & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(4), 01-15.

Ferreira, A. & Lenzini, G. (2015). An Analysis of Social Engineering Principles in Effective Phishing, 2015 Workshop on Socio-Technical Aspects in Security and Trust, 9-16, 13 July 2015, Verona, Italy.

Internet World Stats, Internet in Europe Stats, http://www.internetworldstats.com/stats4.htm Erişim Tarihi: 21.03.2016.

Johnson, M. E. & Goetz, E. (2007). Embedding Information Security into the Organization, IEEE Security & Privacy, May/June 2007, 16–24.

Krombholz K., Hobel H., Huber M. & Weippl E. (2014). Advanced social engineering attacks, SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria.

Laudon, K. C. & Laudon, J. P. (2011). Yönetim Bilişim Sistemleri Dijital İşletmeyi Yönetme. U. Yozgat (Çev). 12. Basım. Nobel Yayınları, Ankara.

Long, J. (2008). *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*. Syngress.

Luo, X., Brody, R., Seazzu, A. & Burd, S. (2011). Social Engineering: The Neglected Human Factor for Information Security Management, Information Resources Management Journal, 24(3), 1-8.

Mellado, D., Fernández-Medina, E. & Piattini, M. (2007). A common criteria based security requirements engineering process for the development of secure information systems, Computer Standards & Interfaces, 29, 244-253.

Milli Eğitim Bakanlığı Bilişim Teknolojileri- Ağ Güvenliği (2013). http://ayrancicpl.meb.k12.tr/meb_iys_dosyalar/70/02/320095/dosyalar/2014_10/07110159_agvenlii.pdf Erişim Tarihi: 15.04.2016.

Mitnick, K. (2009). Aldatma Sanatı, (çeviren: N. E. Tezcan) ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim A.Ş., Ankara.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment, Report published by Defence Science and Technology Organisation, DSTO-TR-2484, Edinburgh South Australia, 5111, Australia. http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/10094/1/DSTO-TR-2484%20PR.pdf Erişim Tarihi: 22.08.2015

Rao, U. H. & Nayak, U. (2014). The InfoSec Handbook An Introduction to Information Security, Apress Open.

Schneier, B. (2000). Secrets and Lies: Digital Security in a Networked World, Indianapolis, IN: Wiley Publishing, Inc.

Spinapolice M. (2011). Mitigating the Risk of Social Engineering Attacks By Matthew Spinapolice, Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Master of Science in Networking and System Administration Rochester Institute of Technology B. Thomas Golisano College of Computing and Information Sciences 11/1, Advisor JOHNSON Daryl, http://scholarworks.rit.edu/theses/394/ Erişim Tarihi: 26.04.2016

Thomson, K. L., Solms, R. & Louw, L. (2006). Cultivating an organizational information security culture, Computer Fraud & Security, 10, 7-11.

TÜBİTAK BİLGEM (2008), Sosyal Mühendislik Saldırıları, http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html Erişim Tarihi: 10.04.2016.

TÜBİTAK BİLGEM, Bilgi Güvenliği Ne Demektir? http://www.bilgimikoruyorum.org.tr/?b121_bilgi-guvenligi-ne-demektir Erişim Tarihi: 10.05.2016.

TÜİK (2015). Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 Erişim Tarihi: 18.02.2016.

Türkiye Bilişim Derneği Ankara Şubesi Eğitim Etkinliği (2009). Bilgi güvenliği ve yönetimi, http://www.tbd.org.tr/userfiles/4/zeynep/egitim_bgys_sunum.pdf Erişim Tarihi: 05.04.2016.