Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Oltalama Saldırıları Farkındalık Tatbikatı Örneği

Yenal ARSLAN[a,*],

[a]*Sosyal Güvenlik Kurumu, Ankara, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: yarslan@sgk.gov.tr*
DOI:10.29130/dubited.832862

ÖZET

Kullanıcılar bilgi güvenliği zincirinde en zayıf halka olarak görülmektedir. Kurumlarda bilgi güvenliğini sağlamaya yönelik pek çok sistem kurulsa da bunlar tam bir güvenlik sağlayamamakta, bazı saldırıların kullanıcılara ulaşmasını engelleyememektedir. Bu nedenle son kullanıcı seviyesine inmeden kurumsal bir bilgi güvenliğinden bahsedilemez. Kullanıcılara yönelik saldırıların başındaoltalama saldırıları gelmektedir. Bu çalışmanın amacı, kullanıcıların bilgi güvenliği farkındalık düzeylerini tespit etmeye yönelik bir oltalama tatbikatının geliştirilmesi ve doğru sonuçlar elde etmek için oltalama tatbikatlarında dikkat edilmesi gereken hususların belirlenmesidir.

Anahtar Kelimeler: *Bilgi güvenliği, Kullanıcı farkındalığı, Sosyal mühendislik, Oltalama*

Phishing Attacks Awareness Exercise Example

ABSTRACT

Users are seen as the weakest link in the information security chain. While many systems are installed to provide information security in institutions, they cannotprovide full security and cannot prevent some attacks from reaching users. For this reason, enterprise information security can not be mentioned without going down to the end-user level. The most common attack type against end-users is phishing attacks. The purpose of this study is to develop an phishing experiment to determine the users' awareness level of information security and to determine the points that should be considered in case of phishing experiments to obtain accurate results.

Keywords:*İnformation security, User awareness, Social engineering, phishing*

Geliş: 28/11/2020, Düzeltme: 27/01/2021, Kabul: 03/02/2021

I. GİRİŞ

Sosyal mühendislik, bir hedefin belirli bilgilerini açığa çıkarmak için veya gayri meşru sebeplerle bir eylemde bulunmaya yönelik kullanılan tüm teknikleri ifade eder. Oltalama saldırıları sosyal mühendisliğin bir türü olup potansiyel mağdurların kimlik bilgileri, banka ve kredi kartı bilgileri gibi hassas bilgileri açığa çıkarmaya ikna etmek için yapılır [1]. Ayrıca, belirli bir kimliğe bürünerek bir hedeften bilgi elde etmek amacıyla kullanılan ölçeklenebilir aldatma eylemi olarak da tanımlanabilir [2]. Oltalama saldırılarında balıkçılıkta olduğu gibi hedefleri yakalamak için yem kullanılır. Saldırı genellikle bir banka veya sosyal ağlar gibi güvenilir meşru bir kaynak gibi görünen, aslında saldırganların hedeflerine ulaşmak için kullandığı güvenilir olmayan kaynaklardan gelen sahte e-postalar ile başlar ve kişinin zararlı yazılım indireceği ya da istenen bilgileri girebileceği sahte bir web sitesine yönlendirilmesi biçiminde devam eder [2]. "Oltalama" kelimesi ilk olarak 2 Ocak 1996'da bir haber sitesinde, bir grup bilgisayar korsanı tarafından kullanıcıların kimlik bilgilerinin çalınmasını ve o zamandan beri oltalama ölçeğini ve karmaşıklığını açıklamak için kullanılmıştır [3].

L. De Kimpe ve arkadaşları, kullanıcıların oltalama hedefi olmaları konusunda aşağıda belirtilen 4 tane hipotez ortaya atmışlar ve yaptıkları çalışmada hipotezlerini ispatlamaya çalışmışlardır. Birinci hipotez dijital dosyaları sıklıkla kullanan, kopyalayan veya paylaşan kişilerin saldırı hedefi olma olasılığı yüksektir. İkinci hipotez internette ve sosyal medyada, kendine ve yaşantısına dair çokça paylaşım yapanların saldırı hedefi olma olasılığı yüksektir. Üçüncü hipotez sosyal ağ sitelerini daha sık kullanan kişilerin, hedef alınma olasılığı yüksektir. Dördüncü hipotez daha sık internetten alışveriş yapan kullanıcılarının, saldırı hedefi olma olasılığı yüksektir [2].

Molinaro ve Bolton yaptıkları araştırmada Microsoft'un 2014 yılında yayımladığı bir raporu referans göstererek oltalama saldırılarının dünya üzerinde yıllık etkisinin yaklaşık 2,4 milyar dolar olduğunu ifade etmişlerdir [4]. Bir diğer örnek ise 2014 yılında Target şirketine yapılan ve 110 milyon tüketicinin kredi kartlarının ve kişisel bilgilerinin ifşa edilmesine yol açan oltalama saldırısı verilebilir [5]. Oltalama saldırılarını önleme çalışma grubu tarafından 2016'da 1,2 milyondan fazlaoltalama saldırısı tespit ederek 2015'e göre %65 artışla oltalama probleminin büyümeye devam ettiği anlaşılmıştır. Koray ve Arkadaşları yaptıkları çalışmada oltalama saldırılarının özellikle gelişmekte olan ülkeleri hedef aldığını, Çin'deki bilgisayarların %47,09, Çin'in ardından sırasıyla %42,88 ve %38,98 oranında Türkiye ve Tayvandaki bilgisayarların oltalama saldırılarına maruz kaldığını vurgulamışlardır [6]. Ek olarak, Verizon 2017 raporunda, oltalama saldırılarının %95'inin sonunda bir zararlı yazılım kurulumunun olduğu ve e-posta eklerinin bahsedilen bu kötü amaçlı yazılımlar için en çok kullanılan teslimat aracı olduğunu belirtmiştir[4].Tespit edilen oltalama saldırıların %90'ı e-posta kullanılarak gerçekleştirilmiştir [7]. Ancak en sık hedeflenen ortam e-posta olsa da literatürde anlık mesajlaşma uygulamaları, mobil uygulamalar, sosyal ve sesli medya gibi başka hedefler de bulunmaktadır[8].

Oltalama saldırı tehdidine yanıt olarak, oltalama önleme sistemleri geliştirilmiştir. Oltalama önleme sistemleri yeni bir araştırma alanı olmayıp uzun yıllardır üzerinde çalışılan bir konudur. Genel olarak liste tabanlı ve makine öğrenimi tabanlı olarak ikiye ayrılabilirler [9].Ancak saldırganlar mevcut savunma sistemlerini alt etmek için sürekli yeni ve değişik saldırı tipleri geliştirmektedirler. Özellikle sıfırıncı gün atakları konusunda birçok oltalama önleme sistemi çaresiz kalmaktadır[3]. Oltalama saldırıları için saldırganlar bazı teknikler uygular. Mesela, İnternet'teki popüler ve yasal sitelerin tamamen benzer tasarımına sahip sahte web siteleri oluşturarak hedefledikleri kullanıcılar için bu web sitelerini çekici hale getirirler [6]. Neredeyse gerçeğinden ayrılamayacak kadar yakın benzetimlerle ortaya konulan oltalama saldırılarını yalnızca içerik olarak değil aynı zamanda teknik olarak da gerçeğinden ayırmak zordur. Phishlabs'ın son raporlarına göre 2018'in üçüncü çeyreğinde oltalama saldırı web sitelerinin% 49'unun SSL (Secure Sockets Layer- Güvenli Yuva Katmanı) sertifikaları kullandığını göstermektedir [9]. Oltalama saldırılarını tespit etmede güçlük yaşanmasının başlıca nedeni, standart siber güvenlik sistemlerini aşmak yerine bu saldırının özellikle insanların güvenlik farkındalığı eksiklerinden yararlanan bir saldırı tipi olmasıdır [8].

Genellikle sosyal mühendislik, insan unsuruna odaklanan saldırganlar tarafından en yaygın olarak kullanılan tekniktir. Ayrıca sosyal mühendislik saldırganların hedeflerine ulaşmalarına yardımcı olmak, onlardan bilgi almak veya saldırgana bir şekilde fayda sağlayacak bir eylemi gerçekleştirmek için insanları aldatma veya kandırma sanatı olarak tanımlanmaktadır [5].

Bununla birlikte, Makine Öğrenimi ve veri madenciliği tekniklerini kullanan birkaç oltalama önleme sisteminin umut verici doğruluk oranlarına ulaştığı literatürde görülmüştür [3]. Wei ve arkadaşları, makine öğrenmesi kullanarak oltalama URL (Uniform Resource Loader - Tek Düzen Kaynak Bulucu) lerini tespit eden bir sistem geliştirmiştir [9]. Mao ve arkadaşları, 2018 de sahte web sayfalarını gerçeğinden ayırmak için CSS çerçevelerini karşılaştıran bir teknik geliştirmişlerdir [1].

Oltalama saldırılarının çok büyük finansal kayıplara sebep olmasının yanı sıra, bu saldırıya uğrayan firma ya da kurumların itibarları da zedelenebilir. İtibarın zedelenmesi riski bu gibi durumda finansal kayıplardan çok daha önemlidir [5]. Kullanıcılar, internet ve üçüncü uygulama kullanımları aracılığıyla kurumsal ağlarda açık bir arka kapı oluştururlar. Bu güvenlik açığı, kullanıcıların ev ve diğer ticari ağlara katılan mobil sistemleriyle beraber daha da artmaktadır [10].

Sosyal etkinin oltalama saldırılarındaki önemini göz önünde bulundurmak gerekir. Sosyal etki, gerçek veya hayali olan dış baskının neden olduğu tutum veya davranış değişikliğini ifade eder. En yaygın olarak kabul edilen ve kullanılan sosyal etki çerçevesi otorite, tutarlılık, eğilim, karşılıklılık, kıtlık ve sosyal kanıt olmak üzere altı ilkeden oluşur. Bu altı prensip için oltalama e-posta örnekleri Tablo 1'de gösterilmiştir. Bu prensiplere ek olarak, oltalama hedefinin yaşı, cinsiyeti ve bilgisayar kullanım sıklığıda ciddi oranda oltalama duyarlılığını etkilemektedir [11].

Tablo 1. *Sosyal etki çerçevesi*

PRENSİPLER	**E-POSTA KONUSU**	**ÖRNEK YAZI**
Otorite	Yasal Konu	"İhlal Bildirimi aldınız"
Tutarlılık	Hayırseverlik Bağışı	"Daha önceki bağışlarınız için teşekkür ederiz"
Eğilim	Anket İstekleri	"Selam, Katılmak için davet edildiğinizi size bildirmek isteriz."
Karşılıklılık	Bağlılık Çeki	"Tebrikler, 50 TL hediye çeki kazandınız"
Kıtlık	Rekabet	"Kazanma şansın var"
Sosyal Kanıt	İyileştirilmiş Hizmet	"Kullanıcıların %70'i güncelleme yaptı"
-	Şifre Sıfırlama	"[Kullanıcı adı] hesabınızın şifresini sıfırlamak için aşağıdaki bağlantıya tıklayın."

Parsons ve arkadaşları sosyal etki çerçevesi kullanılarak oltalama e-postalarının diğer e-postalardan neden daha etkili olduğunu değerlendirmek için bir çalışma yapmışlardır. Çalışmada, bazı insanların saldırılara daha duyarlı olduğu bireysel farklılıklar analiz edilerek değerlendirilmiştir. Çerçevede belirtilen bazı tekniklerin oltalama e-postalarında daha az yaygın olduğundan, insanların bu e-postalara bağışıklık geliştirecek kadar maruz kalmamış olabileceklerini ifade etmişlerdir [11]. Buradan da saldırganların her zaman yeni ikna yöntemleri geliştirdikleri ve kullanıcı farkındalığını yeni tehditlere göre sürekli güncellemek gerektiği ortaya çıkmaktadır.

Silic ve Back 2016 yılında yapmış oldukları çalışmada efektif eğitim ve deneylerin çalışanların farkındalığını artırdığını ve bu farkındalığın bilgi güvenliğini sağlamada en temel konulardan biri olduğunu Fortune 500 listesindeki 11 farklı şirketin genel müdürleri ile yapmış oldukları görüşmelerden çıkarmışlardır [5].

Dodge ve Ferguson, 2006 yılında yapmış oldukları çalışmada oltalama testlerinin, her ne kadar miktarını ölçmek güç olsa da farkındalığı artırmada önemli bir araç olduğunu belirtmişlerdir[10].

Mohebzada ve arkadaşları 2012 yılında 10.000 üniversite çalışanı ve öğrencisi üzerinde oltalama deneyi yapmışlar ve sonuçlarını yaptıkları çalışmada ortaya koymuşlardır [12].

II. METODOLOJİ

Yapılan çalışmada organizasyonlara güvenlik zincirinin en zayıf halkası olan "insan" faktörü ile oltalama saldırıları kullanılarak gelebilecek olan riskler ve organizasyonların buna ne kadar hazır olduğunun görülmesi hedeflenmiştir.

Saldırganlar güvenlik sistemlerini hedef olarak seçmek yerine en zayıf halka olan insan faktörü üzerine yoğunlaşmakta ve bir sisteme sızmak için sıradan bir kullanıcının bilgilerini ele geçirdikten sonra hak yükselterek ilerlemektedirler. Oltalama saldırıları ile direkt kişilerin kendilerinden bilgilerini almaya çalışmakta ya da web uygulama açıkları üzerinden sistemlere ve kurumsal bilgilere erişim sağlamaya çalışmaktadırlar. Genellikle kullanıcı güvenliği adına kurum ve kuruluşlarca ilk etapta yetki kısıtlamaları uygulanmaya ve anti virüs yazılımları sağlanmaya çalışılmaktadır. Ancak son kullanıcı seviyesine inmeden kurumsal bir bilgi güvenliğinden bahsedilemez. Kurumsal bilgi güvenliği politikasının etkili olabilmesi için politikanın son kullanıcılar tarafından tam olarak anlaşılmış olması önemlidir. Tatbikatlar hem kullanıcı farkındalığını doğru olarak ölçmekte hem de farkındalığı arttırmakta oldukça etkili bir yöntem olarak kabul edilmektedir.

Yapılan çalışmada 33.000 çalışanı ve 400 taşra birimi bulunan büyük bir Kamu Kurumu ile tatbikatlar gerçekleştirilmiştir. Tatbikatlar yapılırken sahte web sayfaları hazırlanmış, farklı senaryolarda sahte e-postalar kurum çalışanlarına gönderilmiştir. Bununla beraber 20 ayrı yere USB (Universal SerialBus – Evrensel Seri Veriyolu) bellekler bırakılarak çalışanların buldukları USB belleklere karşı tutumları değerlendirilmiştir. Tatbikat sonucu istatistikler detaylı olarak karşılaştırılmıştır. 2 ayrı fazda 7 farklı senaryo tablo 2'de gösterilmiş, üç farklı personel statüsüne ayrı ayrı oltalama testi gerçekleştirilmiştir.

Tablo 2. *Senaryo tablosu*

Faz	Senaryo 1	Senaryo 2	Senaryo 3	Senaryo 4
Faz 1	Toplam 548 teknik personele "VPN erişim duyurusu" e-postası gönderilmiştir (Sahte Web Sitesi ve E-posta Senaryosu)	Toplam 5000 personele "Avantaj Paketi Duyurusu" e-postası gönderilmiştir (Sahte Web Sitesi ve E-posta Senaryosu)	Toplam 70 yönetici personele "Gönderi takip + Ekli dosyada Makro çalıştırma" e-postası gönderilmiştir (Sahte Dosya İndirilmesi ve E-posta Senaryosu)	-
Faz 2	Toplam 500 teknik personele "Bilgi güncelleme duyurusu" e-postası gönderilmiştir (Sahte Web Sitesi ve E-posta Senaryosu)	Toplam 5000 personele "Bilgi güncelleme Duyurusu" e-postası gönderilmiştir (Sahte Web Sitesi ve E-posta Senaryosu)	Toplam 70 yönetici personele "Siparişiniz Onaylandı" e-postası gönderilmiştir (Sahte Web Sitesi ve E-posta Senaryosu)	Toplam 20 adet USB bellek rastgele bırakılmıştır (USB Bellek Senaryosu)

A. GERÇEKLEŞTİRİLEN SENARYOLAR

A. 1. Sahte Web Sitesi ve E-Posta Senaryosu

Sahte web sitesinin adresi gerçek hayatta görülen saldırılar gibi kurum adına çok benzer seçilmiştir. Tatbikat için kullanılan alan adı üzerinden e-posta gönderilerek kullanıcıların siteye erişebilmesi sağlanmıştır. Sahte web sitesi, kurum uzaktan erişim servisinin arayüzüne benzer olarak tasarlanmıştır. Sitenin güvenli olmadığı tarayıcıda görülebilmektedir. Açılış sayfasında kullanıcı bilgilerinin girilebileceği kullanıcı adı ve parola alanı bulunmaktadır. Parola giren kişilerin doğru girip girmediği kontrol edilmiş ancak parolalar kayıt altına alınmamıştır. Hatalı parola girilse bile tekrar parola istenmemiş ve içerideki sayfaya yönlendirme yapılmıştır. Yapılan geri dönüşlerden bilinçli yanlış parola denemesi yapan kullanıcılar olduğu görülmüştür. Bu aşamada kullanılan parolaların karmaşıklık seviyesi de analiz edilmeye çalışılmış ancak kurumda uygulanan mevcut güvenlik politikaları nedeniyle parola oluşturmanın belirli standartları olduğundan bu konuda anlamlı bir sonuç elde edilememiştir.

Yapılan bu çalışmada senaryolar hazırlanırken teknik detaylar, görsel sunum, mesajın dili ve içeriği gibi üç oltalama ipucu kategorisi göz önünde bulundurulmuş ve personelden bu ipuçlarını yakalaması beklenmiştir. Teknik kategoride; görünen adlar kolayca taklit edilebilir olması, gönderenin gerçek e-posta adresini gizleyebilir olması, metnin arkasındaki gerçek URL'yi gizleyerek metin ayrıca başka bir bağlantı gibi görünebilir olması, dosya eklerinin ve özellikle de yürütülebilir dosyanın varlığının olması gibi ipuçları kullanılmıştır. Görsel sunum kategorisinde; çok az marka ve ayırmaç kullanılması, genel olarak zayıf biçimlendirme ve tasarım kullanılması gibi ipuçları verilmiştir. Mesajın dili ve içeriği kategorisinde; birden çok yazım veya dil bilgisi hatası içeren e-postalar kullanılarak ipuçları verilmiştir. Kullanıcıların isteğe hızlı bir şekilde uymasını sağlamaya çalışmak için genellikle zaman baskısı veya kurumsal otorite emirleri kullanılmıştır. Gerçek tekliflerde olamayacak kadar iyi teklifler sunulmuş (%60 indirim gibi) ve içerikte kişisel bilgi talep edilerek ipuçları verilmiştir. Kullanıcın bu ipuçlarını yakalaması, oltalama saldırısını tanımlaması ve siber güvenlik birimine iletmesi beklenmiştir.

A. 2. Sahte Dosya İndirilmesi ve E-Posta Senaryosu

A Kurumu için sahte web sitesinin adresi gerçek hayat saldırılarına benzer olarak gerçekçi bir adres seçilmiştir. Sahte alan adı üzerinden tatbikat için e-posta gönderilmiş ve kullanıcıların e-posta içerisindeki bağlantıya tıklayarak ekteki dosyayı indirmeleri teşvik edilmiştir. İletilen e-postanın bağlantısında zararlı makro kodu içeren excel dosyası vardır. Kullanıcılardan bu dosyayı indirerek zararlı makroyu etkinleştirmeleri beklenmiştir.

Zararlı makro kodu powershellyükü (payload) kullanılarak Empire aracı ile oluşturulmuştur [13]. Empire, PowerShell ve Python kullanan oldukça pratik ve gelişmiş özellikleri olan bir araçtır.

A. 3. USB Bellek Senaryosu

A kurumu için hazırlanan bu senaryoda oltalama amaçlı USB bellekler hazırlanmıştır. Hazırlanan USB bellekler kurum içerisinde belirlenen 4 ayrı yerleşkeye bırakılarak kullanıcıların tanımadıkları bir belleğin içindeki dosyaları açıp açmadıkları tespit edilmeye çalışılmıştır. USB belleklerin içine liste. xlsx görünür adlı çalıştırılabilir bir dosya (dosyanın gerçek adı liste. xlsx.exe‘dir) konulmuştur. Dosya çalıştırıldığında arka planda çalışan Windows komutları hedefteki bilgisayarda tanımlı IP adresleri, MAC adresi, kullanıcı dizini, kullanılan DNS adresi ve bilgisayar kullanıcı adı bilgisini merkezi bir veri tabanı sunucusu üzerine kopyalamıştır. Bu sayede kimlerin USB bellekleri alarak dosyayı çalıştırmış olduğu bilgisine erişilmiştir. Zararlı uygulama 20 adet USB cihazına kopyalanmıştır.

B. TATBİKATIN İSTATİSTİKSEL DEĞERLENDİRİLMESİ

Bu makalede belirtilen çalışmaya benzer şekilde Orunsolu ve arkadaşları da yaptıkları çalışmada cinsiyet, akademik yeterlilik ve bilgisayar bilgisi kullanıcıların oltalama saldırılarını fark etmelerinde bir etken olduğunu belirtmişlerdir [14]. Flores ve arkadaşlarının, 2013 yılında 92 katılımcıya yaptıkları genel genel oltalama atağında %8.7 oranında katılımcıların oltalamaya takıldığı görülmüşlerdir[15].

Gerçekleştirilen sosyal mühendislik tatbikatında altı farklı senaryo üzerinden sahte elektronik postalar sahte site adreslerinden gönderilmiştir. Sitelere erişen kullanıcılar daire başkanları, bilişim merkez personeli ve taşra personeline ait bilgilere göre sonuçlar girilen kullanıcı adı ve parolaların doğruluklarına göre değerlendirilmiştir. Ayrıca indirilen makro içeren dosyaların kimler tarafından çalıştırıldığına göre de değerlendirilmiştir.

Kaç kullanıcının e-postayı gördüğü tespiti için e-posta gövdesi içine bir adet gif uzantılı dosya eklenmiş ve bu dosyanın yüklenip yüklenmediği yazılım ile kontrol edilerek kimlerin e-postayı gördüğü ve yine yazılım ile kimlerin e-postadaki bağlantıyı tıkladığı tespit edilebilmektedir. A Kurumu tarafından e-posta hesaplarının düzenli kullanıldığı bilindiğinden sonuçlar kurum özelinde detaylı değerlendirilmiştir.

B. 1. Bilişim Merkez Personeli (Faz 1 - Senaryo 1)

Tablo 3'de gösterilen tatbikat sonucunda, Faz 1 içerisinde gerçekleştirilen 1. senaryo ile A kurumunun Bilişim Merkez personeline 548 e-posta gönderilmiştir. Gönderilen e-posta 87 kişi tarafından açılmış, 81 kişiise e-postadaki bağlantıya tıklamıştır. Toplamda kullanıcı adı ve parola kısmına 106 kez veri girilmiş ve bunların 6 tanesinin doğru olduğu tespit edilmiştir.

Tablo3.*Faz 1- senaryo 1 tatbikat sonucu*

Faz 1 - Senaryo 1	
Oltalama E-postası Gönderilen Personel Sayısı	548
E-postayı Açan Personel Sayısı	87
E-postadaki Bağlantıya Tıklayan Personel Sayısı	81
Toplam Doldurulan Form Sayısı	106
Doğru Girilen Form Sayısı (Oltalama Başarısı %)	6, %1.1

B. 2. Taşra Personeli (Faz 1 - Senaryo 2)

Tatbikatın 1. Faz 2. senaryosu kapsamında A Kurumunun taşra personeline tatbikat için kullanılan alan adı üzerinden sahte e-posta gönderilmiş ve kullanıcıların siteye erişebilmesi sağlanmıştır.

Tablo 4'de bulunan tatbikat sonuçlarına bakıldığında taşra personeline toplamda 5000 adet e-posta gönderilmiştir. Bu e-postaların 1007 tanesi görüntülenmiş ve 953 kişi e-posta içindeki bağlantıya tıklamıştır. Kullanıcı adı ve parola kısmına 1484 adet veri girilmiş ve bunların 310 tanesinin doğru olduğu tespit edilmiştir.

Tablo 4.*Faz 1- senaryo 2 tatbikat sonucu*

Faz 1 - Senaryo 2	
Oltalama E-postası Gönderilen Personel Sayısı	5000
E-postayı Açan Personel Sayısı	1007
E-postadaki Bağlantıya Tıklayan Personel Sayısı	953
Toplam DoldurulanForm Sayısı	1484
Doğru Girilen Form Sayısı (Oltalama Başarısı %)	310, %6.2

B. 3. Özel Yetkili Kullanıcılar ve Yöneticiler (Faz 1 - Senaryo 3)

Tatbikatta 1. Faz 3. senaryo ile A Kurumunda yönetici kademesindeki Daire Başkanlarına ve üst seviye yöneticileree-posta gönderilmiştir.

Tablo 5'de gösterilen tatbikat sonuçlarına bakıldığında yöneticilerin de farkındalık düzeyinin zayıf olduğu görülmüştür. Toplam 70 yöneticiden 53'ü e-postayı görmüş ve48'i ilgili bağlantıdan dosyayı indirmiş ve 21 kişi ise zararlı makroyu aktif etmiştir.

Tablo 5.*Faz 1- senaryo 3 tatbikat sonucu*

Faz 1 - Senaryo 3	
Oltalama E-postası Gönderilen Personel Sayısı	70
E-postayı Açan Personel Sayısı	53
E-postadaki Dosyayı İndiren Personel Sayısı	48
Zararlı Makroyu Aktifleştiren Personel Sayısı (Oltalama Başarısı %)	21, %29.6

B. 4. Bilişim Merkez personeli (Faz 2 - Senaryo 1)

Tablo 6'da gösterilen tatbikat sonucunda 2. Faz 1. senaryo ile gerçekleştirilen oltalama çalışmasına göre A kurumunun Bilişim Merkez personeline 500 e-posta gönderilmiştir. Gönderilen e-postalardan 270 tanesi görüntülenmiş, 145 kişi bağlantıya tıklamıştır. Toplamda kullanıcı adı ve parola kısmına 72 veri girilmiş ve bunların 60 tanesinin doğru olduğu tespit edilmiştir.

Tablo 6.*Faz 2- senaryo 1 tatbikat sonucu*

Faz 2 - Senaryo 1	
Oltalama E-postası Gönderilen Personel Sayısı	500
E-postayı Açan Personel Sayısı	270
E-postadaki Bağlantıya Tıklayan Personel Sayısı	145
Toplam DoldurulanForm Sayısı	72
Doğru Girilen Form Sayısı (Oltalama Başarısı %)	60, %12

B. 5. Taşra Personeli (Faz 2 - Senaryo 2)

2. Faz 2. senaryo kapsamında A Kurumunun taşra personeline tatbikat için kullanılan alan adı üzerinden sahte e-posta gönderilmiş ve kullanıcıların siteye erişebilmesi sağlanmıştır.

Tablo 7'de gösterilen tatbikat sonuçlarına bakıldığında taşra personeline toplamda 5000 adet e-posta gönderilmiştir. Bu e-postaların 3242 tanesi görüntülenmiş ve 1911 kişi e-posta içindeki bağlantıya tıklamıştır. Kullanıcı bilgilerini giren sayısı 1071 olmuş ve bunların 865 tanesinin doğru olduğu tespit edilmiştir.

Tablo 7.*Faz 2- senaryo 2 tatbikat sonucu*

Faz 2 - Senaryo 2	
Oltalama E-postası Gönderilen Personel Sayısı	5000
E-postayı Açan Personel Sayısı	3242
E-postadaki Bağlantıya Tıklayan Personel Sayısı	1911
Toplam DoldurulanForm Sayısı	1071
Doğru Girilen Form Sayısı (Oltalama Başarısı %)	865, %17.3

B. 6. Özel Yetkili Kullanıcılar ve Yöneticiler (Faz 2 - Senaryo 3)

Tatbikatta 2. Faz 3. senaryo ile A Kurumunda yönetici kademesindeki Daire Başkanlarına ve üstseviye yöneticilere e-posta gönderilmiştir.

Tablo 8'de bulunan tatbikat sonuçlarına bakıldığında yöneticilerin de farkındalık düzeyinin birinci faza göre geliştiği görülmüştür. Toplam 70 yöneticiden 42'si e-postayı görmüş, 25 tanesi bağlantıya giriş yapmış ve hiçbirisi kullanıcı ismi/parola bilgilerini girmemiştir.

Tablo 8.*Faz 2- senaryo 3 tatbikat sonucu*

Faz 2 - Senaryo 3	
Oltalama E-postası Gönderilen Personel Sayısı	70
E-postayı Açan Personel Sayısı	42
E-postadaki Bağlantıya Tıklayan Personel Sayısı	25
Toplam Doldurulan Form Sayısı	0
Doğru Girilen Form Sayısı (Oltalama Başarısı %)	0, %0

B. 7. USB Bellek Senaryosu Tatbikat Sonucu (Faz 2 - Senaryo 4)

A Kurumunun 4 ayrı yerleşkesine rastgelen bırakılan 20 adet USB bellekle alakalı "Kaç kişinin USB bellekleri alarak bilgisayarına taktığı" konusunda kesin bir rakama ulaşılamamıştır. Bunun yanı sıra toplamda 3 kişi USB belleğini bilgisayarına takarak liste. xlsx. exe dosyasını toplamda 6 kere çalıştırmışlardır. Bu da yüzdesel olarak yaklaşık %15'lik bir oranda oltalama çalışmasının başarıya ulaştığını göstermektedir. Tatbikat sonucu tablo 9'da gösterilmiştir.

Tablo 9.*Faz 2 – senaryo 4 tatbikat sonucu*

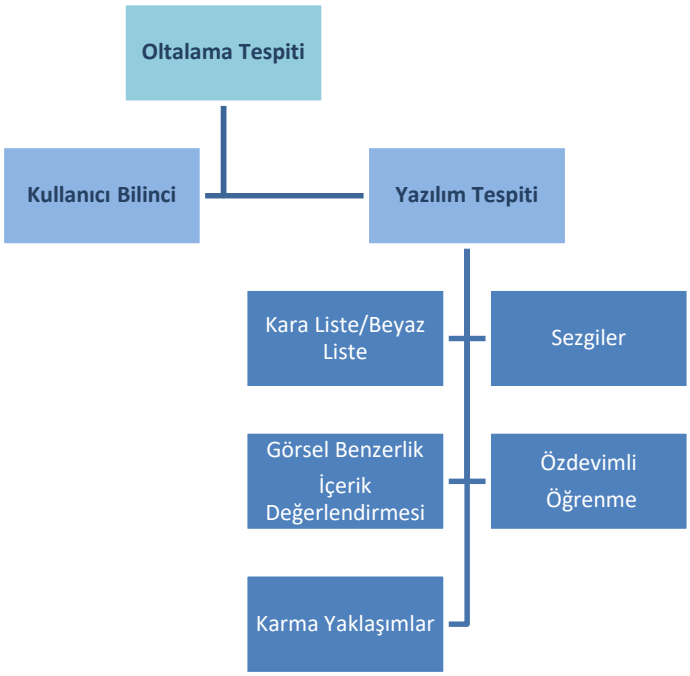
Faz 2 - Senaryo 4	
A Kurumuna Rastgele Bırakılan USB Sayısı	20
USB Belleği Bilgisayara Takan Personel Sayısı	3
USB deki Dosyanın Çalıştırılma Sayısı	6
Oltalama Çalışmasının Başarı Yüzdesi	%15

III. TARTIŞMA VE SONUÇ

Bu makaleye konu olan çalışmada Kurumun birimler ve rol bazında çalışanlarının oltalama saldırılarına karşı farkındalığı ölçülmüş ve literatürde yapılmış olan çalışmalarla kıyaslanmıştır. Bununla beraber oltalama tatbikatı yapılırken dikkat edilmesi gereken konular ortaya konularak bu makaleyi okuyarak oltalama saldırıları ile ilgili sosyal mühendislik deneyi yapmak isteyenlere fikir verilmeye çalışılmıştır. Buna göre; Güvenlik sistemleri e-posta adres aldatmacalarını tespit edebildiğinden gönderilen e-postanın ve yönlendirilen bağlantı adresinin kurumsal bir adres olmaması daha doğru olacaktır. Saldırganın elinde sadece e-posta adreslerinden oluşan bir liste olduğu varsayımı ile hareket edilmelidir.Kişiselleştirilmiş e-posta saldırılarının çok daha etkili olduğu bir gerçek olsa da oltalama saldırıları çoğunlukla genele hitap edecek şekilde olmaktadır.Gönderilecek e-postanın konusunun ilgi çekici ve aynı zamanda gündemde olması, ayrıca tüm hedef kitleyi ilgilendirmesine dikkat edilmelidir.Sonuçların doğru değerlendirilebilmesi için gönderilen tüm e-postalarda bağlantıların kişiye özel olması sağlanmalıdır. Yapılan tatbikatta kullanıcı bilgisi talep edilecek ise kullanıcıların doğru bilgi girip girmediği kontrol edilmelidir. Ancak kullanıcı yanlış bilgi girdiğinde saldırganın bunu bilemeyeceği göz önünde bulundurularak senaryo hazırlanmalıdır. Yapılan tatbikatta

zararlı bir dosya indirilmesi isteniyorsa tüm hedef kitlenin bu dosyayı indirmek ve bilgisayarında çalıştırmak için yetkili olması sağlanmalıdır. Merkez ve taşrada bilgi sistemleri ile ilgili yetkili personele tatbikat ile ilgili bilgi verilmesi ve bu kişiler tarafından genel duyuru yapılmasının önüne geçilmesi gerekir. E-postaya cevap verebilecekler için cevap adresi gerçek bir adres verilebilir. Değerlendirmede kullanılabilecek yaş, cinsiyet, görev, birim gibi kullanıcılara ait bilgiler alınmalıdır. Elektronik postayı, okuyan ve e-postaya tıklayan kişi sayısının belirlenebilmesi faydalı olacaktır.

Oltalama saldırıları, kullanıcıların güvenlik açıklarından yararlanır, bu nedenle sistemlerin ve kullanıcıların korunması için bazı ek destek sistemlerine ihtiyaç vardır. Koruma mekanizmaları iki ana gruba ayrılır. Bunlardan ilki kullanıcıların farkındalığını artırmak ve ikincisi Şekil 1'de gösterildiği gibi bazı ek programlar kullanmaktır. Tüm bunlara ek olarak, oltalama saldırılarında sürekli yeni yöntemler/ türler üretildiği için ağların oltalama tespitini yapan güvenlik yöneticisi tarafından tek bir yaklaşım yerine hibrit modellerin kullanılması gerekliliği çok önemlidir [6].



Şekil 1.*Oltalama tespiti[6]*

Bu zayıflıkların ışığında, oltalama saldırılarıyla mücadele etmek için basit liste tabanlı yöntemlerden makine öğrenimi yaklaşımına kadar birçok uygulama geliştirilmiştir [3].

Tatbikat sonuçlarından görüldüğü üzere kurumlarda kullanıcıların bilgi güvenliği farkındalığı oldukça düşüktür. Sadece kişilerin e-posta adreslerine sahip bir saldırganın kişilerin bilgilerini ele geçirebileceği görülmüştür. Dikkat edilmesi gereken bir diğer nokta da kişilerin bunun bir saldırı olduğunu fark edemediğinden çalınan bilgilerin uzun süre sömürülebileceği gerçeğidir.

Bunun haricinde Kurumda sosyal mühendislik saldırıları ile başarı elde edilmiş olup, taşra personelinin daha az şüphe duyup kullanıcı adı, parola bilgilerini sahte web sayfalarına girme oranının daha fazla olduğu görülmüştür. Fakat yönetici pozisyonunda bulunan kişiler taşra personeline göre biraz daha dikkatli olsa da sonuç yine başarılı olmuş ve yöneticilerin kullanıcı adı, parola bilgisinin elde edilmesi haricinde zararlı dosya etkinleştirdiği gözlemlenmiştir.

Bilgi güvenliği farkındalık çalışmaları en üst yöneticiden başlayarak tüm çalışanları ve kuruma hizmet veren üçüncü tarafları kapsayacak şekilde yapılmalı ve bir çalışanın işe başlamasından ya da bir firma ile sözleşme imzalanmasından itibaren başlayacak şekilde kişiler sürecin içine dâhil edilmelidir. Sahip

oldukları bilgiler ve yetkiler nedeniyle saldırganların hedefindeki kişiler olan yöneticilere yönelik özel farkındalık çalışmaları yapılmalıdır. Doğru tasarlanan, iyi uygulanan ve sürekliliği sağlanan farkındalık faaliyetleri etkili bir güvenlik önlemi olacaktır.

IV. KAYNAKLAR

[1] J. Mao, J. Bian, W. Tian, S. Zhu, T. Wei, A. Live ve Z. Liang, "Detecting phishing web sites via aggregation analysis of pagelayouts," *ProcediaComputerScience*, c. 129, ss. 224–230, 2018.

[2] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels ve K. Ponnet, "You'vegot mail! Explaining individual differences in becoming a phishing target,"*Telematicsand Informatics*, c. *35*, s. 5, ss. 1277–1287, 2018.

[3] A. A. Orunsolu, A. S. Sodiya ve A. T. Akinwale, "A predictive model for phishing detection," *Journal of King Saud University – Computer and Information Sciences*, Basımda.

[4] K. A. Molinaro ve M. L. Bolton, "Evaluating the applicability of the double system lens model to the analysis of phishing email judgments," *Computers and Security*, c. 77, ss. 128–137, 2018.

[5] M. Silic ve A. Back, "The dark side of social networking sites: Understanding phishing risks," *Computers in Human Behavior*, c. 60, ss. 35-43, 2016.

[6] O. Koray, E. Buber, O. Demir ve B. Diri, "Machine learning based phishing detection from URLs, "*Expert Systems With Applications*, c. 117, ss. 345–357, 2019.

[7] A. Ferreira ve S. Teles, "Persuasion: How phishingemails can influence users and bypass security measures," *Int. J. Hum. Comput. Stud.*, c. 125, ss. 19–31, 2019.

[8] A. Aleroud ve L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Comput. Secur.*, c. 68, ss. 160–196, 2017.

[9] W. Wei, Q. Ke, J. Nowak, M. Korytkowski, R. Scherer ve M. Woźniak, "Accurate and fast URL phishing detector: A convolutional neural network approach," *Comput. Networks*, c. 178, 2020.

[10] R. C. Dodge ve A. J. Ferguson, "Using phishing foruser email security awareness," *IFIP Int. Fed. Inf. Process.*, c. 201, ss. 454–459, 2006.

[11] K. Parsons, M. Butavicius, P. Delfabbro ve M. Lillie, "Predicting susceptibility to social influence in phishing emails," *International Journal of Human Computer Studies*, c. 128, ss. 17–26, 2019.

[12] J. G. Mohebzada, A. E. Zarka, A. H. Bhojani ve A. Darwish, "Phishing in a University Community Two large scale phishing experiments," *2012 International Conference on Innovations in Information Technology*, 2012, ss. 249-254.

[13] Ö. H. Durmuş, Kernel Blog. (2019, 1 Temmuz), *Post exploitation: empire kullanımı*. [Online]. Erişim: https://kernelblog.org/2019/07/post-exploitationempire-kullanimi/

[14] A. Oransulu, A. Sodiya, A. Akinwale ve B. Olajuwon, "An anti-phishing kit scheme for secure web transactions," *In the Proceedings of 3rd ICISSP Conference*, Porto Potrugal, Scıtepress, 2017, ss.15-24.

[15] W. RochaFlores, H. Holm, G. Svensson ve G. Ericsson, “Using phishing experiments and scenario-based surveys to understand security behaviours in practice,” *Inf. Manag. Comput. Secur.*, c. 22, s. 4, ss. 393–406, 2014.