Bölüm 4

Sosyal Mühendislik ve Oltalama Saldırılarını Anlamak: Derinlemesine Bir Analiz

Yasin Emül[1]

Ceren Çubukçu Çerasi[2]

Özet

Sosyal mühendislik ve oltalama saldırıları, günümüzün dijital ortamında, güvenlik açıklarından yararlanmak ve hassas bilgilere yetkisiz erişim sağlamak için insan psikolojisinden yararlanan zorlu bir tehdidi temsil etmektedir. Bu çalışma, bu aldatıcı uygulamaların inceliklerini araştırmakta, kullanılan taktiklere, yasal ve etik sonuçlarına ve etkilerini azaltmak için gerekli koruma önlemlerine ışık tutmaktadır. Çalışma, bilgisayar korsanları ile sosyal mühendisler arasında ayrım yaparak başlamaktadır ve sonrasında güvenlik sistemlerini ihlal etme girişimlerinde kullandıkları farklı yaklaşımları açıklamaktadır. Sosyal mühendislik mağdurlarının sergilediği ortak özelliklerin dikkatle incelenmesi, kötü niyetli aktörlerin istismar ettiği ve sonuçta başarılı saldırılara yol açan güvenlik açıklarının ortaya çıkarılmasına yardımcı olmaktadır. Sosyal mühendislik, bahane üretme, yemleme, takip etme ve diğerleri gibi çeşitli saldırıları içerir. Çalışma, sosyal mühendislik saldırı döngüsünü analiz ederek, saldırganların hedefleri belirledikleri, bilgi topladıkları ve hileli planlarını uyguladıkları sistematik süreci açıklamaktadır. Sosyal mühendisliğin etkinliğinin merkezinde kötü niyetli aktörler tarafından kullanılan manipülasyon taktikleri yer almaktadır. Çalışma, hedefleri kandırmak için kullanılan, otorite istismarından duygusal manipülasyona kadar uzanan en yaygın stratejiler hakkında bilgi vermektedir. Sosyal mühendisliğin yaygın bir alt kümesi olan oltalama saldırıları özel bir ilgi gerektirmektedir. Bu çalışma, çeşitli oltalama saldırılarını incelerken, bunların hem bireyler hem de kurumlar üzerindeki olumsuz etkilerini de incelemektedir. Sosyal mühendisliğe karşı acil korunma ihtiyacını ele alarak hem bireysel hem de kurumsal düzeyde uygulanabilecek önlemlerin ana hatlarını çizmektedir. Eğitim ve farkındalık girişimleri, bireylerin manipülasyon girişimlerini fark

1 Öğrenci, Gebze Teknik Üniversitesi, emulyasinn@gmail.com, 0009-0002-1760-5930

2 Dr. Öğr. Üyesi, Gebze Teknik Üniversitesi, cerencubukcu@gtu.edu.tr, 0000-0002-9253-2826

https://doi.org/10.58830/ozgur.pub137.c1385

etmeleri ve bunlara direnmeleri için güçlendirilmesinde önemli faktörler olarak ortaya çıkmaktadır. Sonuç olarak, bu çalışma sürekli gelişen sosyal mühendislik ve oltalama tehditleri karşısında sürekli farkındalık, eğitim ve tetikte olma zorunluluğunun altını çizmektedir. Bireyleri ve kurumları bilgi ve pratik savunma mekanizmalarıyla güçlendirerek, siber savunmalar kolektif olarak güçlendirilebilir ve herkes için daha güvenli bir dijital ortam sağlanabilir.

1. Giriş

Sosyal mühendislik, saldırganlar tarafından insanları istedikleri eylemleri gerçekleştirmeleri veya gizli bilgileri ifşa etmeleri için manipüle etmek için kullanılan bir tekniktir. Sistemlere, verilere veya bilgilere yetkisiz erişim elde etmek için bilgisayar korsanlığı teknikleri kullanmak yerine insan psikolojisinden yararlanma sanatıdır.

Sosyal mühendisler, kurbanlarını manipüle etmek için güven inşa etmek, aciliyet duygusu yaratmak, duygulara hitap etmek veya olmadıkları biri gibi davranmak gibi çeşitli taktikler kullanırlar.

Sosyal mühendislik saldırılarının amacı; insanları, şifreleri veya gizli verileri için ya da çeşitli sistemlere veya verilere erişim elde etmek için kullanılabilecek diğer hassas bilgilerini açığa çıkarmaları için kandırmaktır. Sosyal mühendislik saldırıları, herhangi bir güvenlik sistemindeki en zayıf halka olan insanları kullandıkları için oldukça etkili olabilir (Hadnagy, 2010).

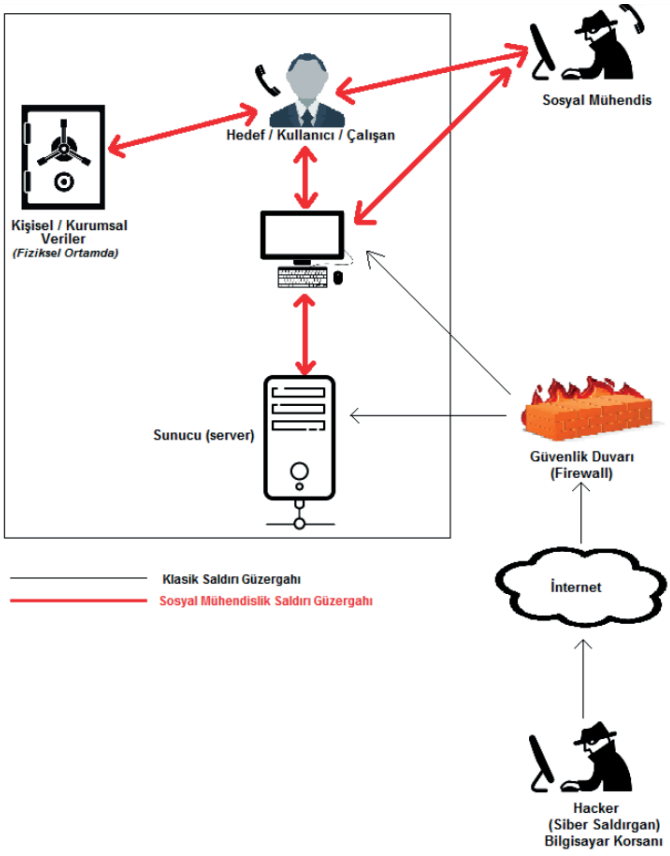
Bu saldırılar genellikle güven, korku veya aciliyet gibi insan duygularını istismar eder ve kimlik avı dolandırıcılığı, yemleme, bahane uydurma ve daha fazlası dahil olmak üzere birçok şekilde olabilir. Bu tür saldırılar genellikle parolalar veya kişisel verilere erişim sağlamak için kullanılır.

Sosyal Mühendisliğin etkisi önemli ve geniş kapsamlı olabilir. Bireyler, parolalar ve kredi kartı numaraları gibi kişisel bilgilerini kaybedebilir, bu durum da mali kayıplara ve kimlik hırsızlığına neden olabilir. Kuruluşlar, hassas bilgilerin çalınması ve müşteri güveninin kaybedilmesiyle sonuçlanan veri ihlallerine maruz kalabilir.

Sosyal Mühendislik saldırılarının tespit edilmesi zor olabilir çünkü insan duygularına ve sosyal normlara dayanırlar. Ayrıca bireylerin güven ve duygularını istismar ettikleri için önlenmeleri kolay değildir.

Sosyal mühendislik saldırılarının arkasındaki motivasyonlar genellikle saldırganların finansal kazanç elde etme, hassas bilgilere erişme, siyasi veya ideolojik motivasyonlara sahip olma, intikam alma veya basitçe kaosa neden olma arzusudur.

Sosyal medya, sosyal mühendislik saldırıları için popüler bir platform haline gelmiştir. Sosyal medya, sosyal mühendislik saldırıları için zengin bir bilgi kaynağıdır. Saldırganlar, sosyal medya etkinliklerini izleyerek hedefleri hakkında bilgi toplar ve bu bilgileri ikna edici kimlik avı e-postaları veya telefon görüşmeleri oluşturmak için kullanır.



Şekil 1. Bilgisayar Korsanları ve Sosyal Mühendisler arasındaki farklar

Şekilde görüldüğü üzere, Bilgisayar korsanları ve sosyal mühendislerin her ikisi de hassas bilgilere veya bilgisayar sistemlerine yetkisiz erişim sağlamak için çeşitli teknikler kullanan kişilerdir, ancak yöntemleri ve hedefleri bakımından farklılık gösterirler.

Bilgisayar korsanları, teknik bilgilerini bilgisayar sistemleri, ağlar veya yazılımlardaki güvenlik açıklarından yararlanmak için kullanan kişilerdir. Sistemlere yetkisiz erişim sağlamak veya hassas verileri çalmak için kötü amaçlı yazılım, kimlik avı ve kaba kuvvet saldırıları gibi çeşitli araçlar ve

teknikler kullanabilirler. Birincil hedefleri hassas bilgileri çalmak, sistemlere zarar vermek veya kesintiye neden olmak gibi kişisel kazançlar için güvenlik zayıflıklarından yararlanmaktır. (Özmen, 2020)

Öte yandan, sosyal mühendisler psikoloji ve insan etkileşimini kullanarak insanları gizli bilgileri ifşa etmeye veya kendi çıkarlarına olmayan eylemleri gerçekleştirmeye yönlendirir. Genellikle kişileri kandırarak parola bilgilerini vermelerini sağlamak için yemleme ve oltalama gibi sosyal mühendislik tekniklerini kullanırlar. Birincil hedefleri, manipülasyon yoluyla hassas bilgilere erişmektir.

Sosyal mühendislik, siber saldırganların insanların duygularını, güvenini ve dikkatini manipüle ederek bilgi veya erişim elde etmeye çalıştığı sofistike bir saldırı yöntemidir. Sosyal mühendislik saldırılarına maruz kalan kişilerin çoğunda ortak özellikler bulunur. Bu özellikler şunlardır:

• **Güvene Dayalı Yapı:** Sosyal mühendislik saldırıları genellikle kurbanın güvenen yapısına dayanır. Mağdurların güvenilir bir otorite figürü ya da tanıdıkları biri gibi görünen birine inanma olasılıkları daha yüksek olabilir (Hadnagy, 2010). Örneğin, bir saldırgan kurbanını parolasını veya giriş bilgilerini paylaşmaya ikna etmek için Bilişim Teknolojileri (BT) teknisyeni gibi meşru bir otorite figürü gibi davranabilir. Alternatif olarak, saldırgan kurbanını para veya diğer kaynakları transfer etmeye ikna etmek için yardıma ihtiyacı olan bir arkadaş veya aile üyesi gibi davranabilir.

• **Farkındalık Eksikliği:** Sosyal mühendislik saldırıları birçok şekilde olabilir. Bu taktiklere aşina olmayan veya bu taktikleri nasıl tespit edecekleri ve bunlara nasıl yanıt verecekleri konusunda eğitim almamış olan mağdurlar, bu dolandırıcılıklara kanma konusunda daha savunmasız olabilirler. Mağdurlar hassas bilgileri paylaşmanın veya belirli eylemleri gerçekleştirmenin potansiyel risklerinin farkında olmayabilirler. (Uebelacker, Quiel, 2014).

• **Dürtüsellik:** Saldırganlar, olası sonuçları düşünmeden aceleci kararlar vermeleri için mağdurlara baskı yapabilir. Örneğin, bir saldırgan kurbanın hesabının ele geçirildiğini ve daha fazla zararı önlemek için derhal şifresini sıfırlaması gerektiğini iddia edebilir. Talebin gerçekliğini doğrulamak için zaman ayırmadan harekete geçen mağdurlar, yanlışlıkla saldırganın hesaplarına erişmesine izin verebilir.

• **Tanınma Arzusu:** Saldırganlar, kurbanın tanınma veya övülme arzusunu istismar ederek onu bilgi paylaşmaya veya eylemde bulunmaya yönlendirebilir (Hadnagy, 2010). Örneğin, bir saldırgan kendisini bir makale veya çalışma için bilgi arayan bir gazeteci veya araştırmacı olarak tanıtabilir ve kurbandan anonimlik kisvesi altında hassas bilgiler isteyebilir. Katkılarının

tanınacağına veya değer göreceğine inanan mağdurların bu bilgileri verme olasılığı daha yüksek olabilir.

• **Hayır Diyememek:** Sosyal mühendislik mağdurları daha yönlendirilebilir ve karşısındakine hayır diyemeyen insanlar olabilirler. (Barber, 2001)

Sosyal Mühendisliğin bazı yasal etkileri mevcuttur. Bu yasal etkiler şunlardır:

• **Sorumluluk:** Sosyal mühendislik saldırıları, özellikle bireylere veya kuruluşlara mali zarar veriyorsa, saldırgan için yasal sorumlulukla sonuçlanabilir. Örneğin, bir saldırgan, birini sahte bir hesaba para aktarması için kandırmak için sosyal mühendislik taktikleri kullanırsa, dolandırıcılık veya hırsızlıktan sorumlu tutulabilir.

• **Veri İhlalleri:** Sosyal mühendislik saldırıları, veri ihlallerine de yol açabilir ve bu da mağdur kuruluş için yasal sorumluluk doğurabilir. Bir şirket, müşterilerinin verilerini yeterince koruyamazsa ve bir sosyal mühendislik saldırısı nedeniyle açığa çıkarsa, ortaya çıkan zararlardan şirket sorumlu tutulabilir. (Johnson, 2018)

• **Sözleşmeden Doğan Yükümlülükler:** Birçok kuruluş, kişisel olarak tanımlanabilir bilgiler (PII) ve kredi kartı verileri gibi hassas bilgileri korumakla yükümlüdür. Bir sosyal mühendislik saldırısı veri ihlaline yol açarsa ve kuruluş sözleşmeden doğan yükümlülüklerini yerine getiremezse yasal sonuçlarla karşılaşabilir.

Sosyal Mühendisliğin bazı yasal etkileri mevcuttur. Bu etik etkiler şunlardır:

• **Manipülasyon:** Sosyal mühendislik saldırıları, insanların hassas bilgilerine erişmek için insanları manipüle edebilir. Bu durum, bireylerin özerkliklerinin ihlali ve güven ihlali olarak görülebilir. (Mouton, Malan, & Venter, 2013)

• **Psikolojik Zarar:** Sosyal mühendislik saldırıları, kurbanlarda stres, endişe ve güven kaybı gibi psikolojik zararlara neden olabilir. Mağdurlar ayrıca bir toplum mühendisliği taktiğine kandıkları için mahcup veya utanmış hissedebilirler.

• **İtibar Üzerindeki Etki:** Sosyal mühendislik saldırıları, özellikle bir veri ihlaliyle sonuçlanırsa, kuruluşların itibarına zarar verebilir (Mouton, Malan, & Venter, 2013). Müşteriler kuruluşa olan güvenlerini kaybedebilir ve gelecekte onlarla iş yapmaktan çekinebilir.

2. Sosyal Mühendislik Türleri

Sosyal Mühendislikte pek çok farklı tür vardır. Bunlar aşağıda detaylı olarak açıklanmıştır.

•**Oltalama (Phishing):** Oltalama, Sosyal Mühendisliğin en yaygın şeklidir. Oltalama saldırıları, saldırganların sahte e-postalar, web siteleri veya diğer iletişim biçimlerini kullanarak bireyleri giriş bilgileri, kredi kartı numaraları gibi hassas bilgileri ifşa etmeleri için kandırdığı bir siber saldırı türüdür.

Oltalama saldırıları genellikle kurbanda aciliyet veya korku hissi yaratarak, talebi dikkatlice değerlendirme fırsatı bulamadan harekete geçmeye ikna etmek gibi sosyal mühendislik taktiklerini içerir. Örneğin, bir saldırgan, bankacı gibi görünen bir e-posta gönderebilir ve alıcıdan bir bağlantıya tıklayıp oturum açma kimlik bilgilerini girmesini isteyebilir.

•**Yemleme (Baiting):** Yemleme, USB sürücü gibi fiziksel bir öğenin şüphelenmeyen bir kişi tarafından alınması muhtemel bir yere bırakılmasıdır. Yem genellikle park yeri veya konferans salonu gibi kurbanın bulma ihtimalinin yüksek olduğu halka açık bir yere bırakılır.

Yem, kurban için daha cazip hale getirmek için "Gizli" veya "Yönetici Maaş Bilgileri" gibi cazip bir etiketle etiketlenebilir. Kurban yemi alıp bilgisayarına veya cihazına yerleştirdiğinde, kötü amaçlı yazılım otomatik olarak yüklenebilir veya kurbandan oturum açma bilgileri veya kişisel bilgiler gibi hassas bilgileri vermesi istenebilir. (Hadnagy, 2010).

Sosyal mühendislik yemleme saldırıları, insan merakını ve güvenini istismar ettikleri için oldukça etkili olabilir. Kurban USB belleğin bir iş arkadaşı ya da satıcı gibi meşru bir kişi tarafından kaybedildiğini varsayabilir ve yemin gerçekliğini sorgulamayabilir.

•**Bahane Üretme (Pretexting):** Pretexting, bir saldırganın kurbanın güvenini kazanmak ve hassas bilgileri elde etmek için uydurma bir senaryo veya bahane yarattığı bir saldırı türüdür. Saldırgan, kurbanı gizli bilgileri ifşa etmeye veya istenilen eylemi gerçekleştirmeye ikna etmek için bir banka çalışanı, devlet ajanı veya BT departmanının bir üyesi gibi güvenilir bir kişi veya otorite figürü gibi davranabilir.

Bahane, ikna edici bir hikaye veya rutin ya da zararsız görünen bir dizi soru içerebilir. Örneğin, kimliğini doğrulama kisvesi altında kurbanın hesap numarasını veya şifresini istemek gibi. Saldırgan ayrıca kurbanın daha rahat veya uyumlu hissetmesini sağlamak için pohpohlama, korkutma veya aciliyet gibi sosyal mühendislik tekniklerini de kullanabilir.

Pretexting saldırılarını tespit etmek zor olabilir çünkü saldırgan genellikle meşru bir kişi gibi görünür ve güvenilirlik sağlamak için bazı gerçek bilgiler sağlayabilir. Mağdurlar çok geç olana ve bilgileri ele geçirilene kadar hedef alındıklarını fark etmeyebilirler.

• **Omuz Sörfü:** Omuz Sörfü, bir saldırganın kurbanın omzunun üzerinden veya uzaktan izleyerek parolalar, PIN'ler veya erişim kodları gibi hassas bilgileri gözlemlediği veya kaydettiği bir saldırı türüdür. Saldırgan, kurbanın ekranını veya klavye etkinliğini yakalamak için dürbün, kamera veya diğer casusluk tekniklerini kullanabilir.

Omuz sörfü saldırıları, ATM'ler, toplu taşıma araçları ve kafeler gibi bireylerin hassas bilgileri girme veya bunlara erişme olasılığının yüksek olduğu çeşitli ortamlarda meydana gelebilir. Saldırgan sıradan bir seyirci gibi görünebilir veya kurbanın dikkatini dağıtarak eylemlerini gözlemlemek veya kaydetmek için bir fırsat yaratabilir.

• **Tersine Sosyal Mühendislik:** Bir saldırgan, potansiyel bir kurbanla doğrudan iletişime geçmek yerine, onları kendisinin güvenilir biri olduğuna inandırmaya çalışabilir. Amaç, kurbanların yardım istemek için kendisine yaklaşmasını sağlamaktır. Bu yaklaşım "tersine sosyal mühendislik" olarak bilinir ve üç ana bölümden oluşur: sabotaj, reklam ve yardım. Bunun ilk adımı sistemi sabote etmektir. Sabotajın ilk adımı şirketin bilgisayar sistemini sabote etmektir. Saldırganlar daha sonra sorunu çözebileceklerinin reklamını yaparlar. Kurban yardım istediğinde, sosyal mühendis daha önce yarattıkları sorunu çözecek, örneğin kurbandan şifresini isteyecek veya belirli bir yazılımı yüklemesini söyleyecektir (Krombholz, Hobel, Huber, Weippl, 2015).

• **Kuyrukçuluk (Tailgating):** Tailgating, piggybacking olarak da bilinir ve bir saldırganın yetkili bir kişinin arkasından yakından takip ederek güvenli bir alana veya sisteme yetkisiz erişim elde ettiği bir saldırı türüdür. Saldırgan kalabalığa karışmak ve şüphe çekmemek için teslimatçı gibi görünmek için bir kutu veya çanta taşımak veya kayıp bir çalışan gibi davranmak gibi çeşitli teknikler kullanabilir.

Takip saldırıları ofis binaları, veri merkezleri ve erişim kontrol önlemlerinin uygulandığı diğer güvenli tesisler gibi çeşitli ortamlarda meydana gelebilir. Saldırgan binaya girmekte olan çalışanları hedef alabilir veya tespit edilmekten kaçınmak için bir grup insanın arkasından gizlice girebilir.

• **Korku (Scareware):** Scareware, kötü amaçlı yazılım indirmeniz veya hassas bilgileri açıklamanız için sizi kandırmak amacıyla korkuyu kullanan bir tür sosyal mühendislik saldırısıdır. Saldırgan, kurbanı sahte antivirüs veya

güvenlik yazılımı indirmeye veya satın almaya ikna etmek için korkutabilir. (Hadnagy, 2010). Saldırgan, kurbanda aciliyet veya korku hissi yaratmak için meşru antivirüs yazılımını taklit eden açılır mesajlar veya sahte uyarı uyarıları kullanabilir. Kurban sahte yazılımı indirdiğinde veya satın aldığında, saldırgan kötü amaçlı yazılım yükleyebilir veya kredi kartı numaraları veya giriş bilgileri gibi kişisel bilgileri çalabilir.

•**Subaşı (Watering Hole):** Watering Hole saldırıları, saldırganların hedeflenen bir grup birey tarafından sıklıkla ziyaret edilen bir web sitesini ele geçirdiği bir tür sosyal mühendislik saldırısıdır. Saldırganlar daha sonra güvenliği ihlal edilmiş web sitesini kötü amaçlı yazılım dağıtmak veya hedeflenen gruba başka saldırılar gerçekleştirmek için kullanır.

•**Taviz (Quid pro quo):** Quid pro quo, başka bir şey karşılığında bir şey teklif etmeyi içeren bir tür sosyal mühendislik tekniğidir. İnsanları hassas bilgileri ifşa etmeleri veya başka türlü yapmayacakları eylemleri gerçekleştirmeleri için manipüle etmek veya kandırmak için kullanılabilir.

•**Sahte Arama (Robocall):** Çok sayıda kişiye belirli bir mesaj iletmek için önceden kaydedilmiş mesajlar kullanan otomatik telefon çağrılarıdır. Robocall'lar genellikle tele-pazarlama veya siyasi kampanyalar için kullanılır, ancak dolandırıcılık veya sahtekarlık gibi başka amaçlarla da kullanılabilirler. (Salahdine, Kaabouch, 2019).

3. Sosyal Mühendislik Saldırı Döngüsü

Sosyal Mühendislik Saldırı Döngüsü 6 aşamadan oluşmaktadır. Bunlar aşağıda detaylı olarak açıklanmıştır.

•**Keşif:** Saldırgan hedef hakkında ilgi alanları, alışkanlıkları ve sosyal bağlantıları gibi bilgileri toplar. Bu bilgiler çevrimiçi araştırma, sosyal medya profilleri veya hatta hedefin güvenini kazanmak için başka birinin kimliğine bürünerek elde edilebilir.

Bu aşamada saldırgan, saldırıyı planlamasına ve gerçekleştirmesine yardımcı olacak hedef hakkında bilgi toplar. Bu, hedefin kişisel ve mesleki ilgi alanlarını araştırmayı, çevrimiçi varlığındaki potansiyel zayıflıkları veya güvenlik açıklarını belirlemeyi veya hatta doğrudan hedeften bilgi toplamak için sosyal mühendislik tekniklerini kullanmayı içerebilir.

•**Hedefleme:** Saldırgan yeterli bilgi topladıktan sonra, genellikle saldırılarına karşı savunmasız olacağına inandığı bir veya daha fazla hedef seçer. Bu bir birey, bir grup birey ya da hatta tüm bir organizasyon olabilir.

•**Geliştirme:** Geliştirme aşamasında, saldırgan saldırının ayrıntılarını planlamaya başlayacaktır. Bu, kullanılacak belirli araçların veya tekniklerin

seçilmesini, sahte kimliklerin veya personaların oluşturulmasını ve hatta saldırının gerçekleşeceği fiziksel konumda keşif yapılmasını içerebilir. (Hadnagy, 2010).

Saldırgan, kullanılacak yöntem ve araçların seçilmesi de dahil olmak üzere saldırı için bir plan geliştirmeye başlar. Bu, sahte e-postalar veya web siteleri oluşturmayı, kimlik avı tekniklerini kullanmayı veya hatta takip etme (birini yetkisi olmadan güvenli bir alana kadar takip etme) gibi fiziksel yöntemleri içerebilir.

• **Konuşlandırma:** Saldırgan planını geliştirdikten sonra bunu uygulamaya koyacaktır. Bu, kimlik avı e-postaları veya mesajları göndermeyi, telefon görüşmeleri yapmayı veya güvenilir bir taraf gibi davranarak kısa mesajlar göndermeyi ve hatta güvenli bir yere fiziksel olarak erişim sağlamayı içerebilir.

Saldırgan saldırı planını uygular. Bu, kimlik avı e-postaları göndermeyi, güvenilir bir taraf gibi davranarak telefon görüşmeleri yapmayı veya kısıtlı bir alana fiziksel olarak erişim sağlamayı içerebilir.

• **İstismar:** Hedefin sistemine veya bilgilerine erişim sağladıktan sonra, saldırgan genellikle bunları kendi amaçları doğrultusunda kullanmaya başlayacaktır. Bu, hassas verilerin çalınmasını, kötü amaçlı yazılım veya virüslerin yerleştirilmesini veya saldırı döngüsünü ilerletmek için erişimin kullanılmasını içerebilir.

Saldırgan hedefin sistemine veya bilgilerine erişim sağladıktan sonra bunları istismar etmeye başlar. Bu, hassas verilerin çalınmasını, kötü amaçlı yazılım veya virüslerin yerleştirilmesini veya saldırı döngüsünü ilerletmek için erişimin kullanılmasını içerebilir.

• **İzleri örtmek:** Son olarak, saldırgan tespit edilmekten kaçınmak için izlerini kapatmaya çalışacaktır. Bu, günlükleri veya dosyaları silmeyi, araştırmacıları yanlış yönlendirmek için sahte ipuçları oluşturmayı veya faaliyetlerini gizlemek için şifreleme tekniklerini kullanmayı içerebilir.

Tespit edilmekten kaçınmak için saldırgan günlükleri veya dosyaları silerek, sahte ipuçları yaratarak veya faaliyetlerini gizlemek için şifreleme teknikleri kullanarak izlerini kapatır.

4. Yaygın Manipülasyon Taktikleri

Bazı yaygın manipülasyon taktikleri aşağıda açıklanmıştır.

• **Aciliyet:** Saldırganlar genellikle bireylerin hızlı ve düşünmeden hareket etmelerini sağlamak için bir aciliyet duygusu yaratır. Bu, bir banka veya

devlet kurumundan geldiğini iddia eden ve acil eylem gerektiren yakın bir sorun hakkında uyarıda bulunan e-postalar yoluyla yapılabilir.

•**Korku:** Saldırganlar, bireylerin hassas bilgileri ifşa etmelerini veya yetkisiz işlemleri tamamlamalarını sağlamak için korkuyu da kullanabilir. Örneğin, bir saldırgan bir bireyin hesabının ele geçirildiğini ve fonlarını korumak için derhal harekete geçmeleri gerektiğini iddia edebilir.

•**Güven:** Saldırganlar genellikle bireylerin kurumlara ve kişilere duyduğu güveni istismar eder. Örneğin, bir saldırgan tanınmış bir şirketin teknik destek temsilcisi gibi davranarak bir kişiyi parolasını açıklamaya veya bilgisayarına kötü amaçlı yazılım yüklemeye ikna edebilir. (Direction, 2015).

•**Merak:** Saldırganlar genellikle kişilerin e-postalardaki bağlantılara tıklamasını veya ekleri açmasını sağlamak için merakı kullanır. Örneğin, bir saldırgan konu satırı ilgi çekici olan ve alıcının e-postayı açıp bilgisayarını kötü amaçlı yazılımlara maruz bırakmasına neden olan bir e-posta gönderebilir.

•**Dikkat Dağıtma:** Sosyal mühendis, kurbanın dikkatini dağıtmak ve saldırısını gerçekleştirmek için soru sormak veya kargaşa yaratmak gibi dikkat dağıtma veya yanlış yönlendirme yöntemlerini kullanabilir.

•**Karşılıklılık:** Sosyal mühendis, mağdurda jeste karşılık verme zorunluluğu hissi yaratmak için hediye veya iyilik gibi değerli bir şey sunabilir.

•**Sosyal Kanıt:** Sosyal mühendis, meşruiyet veya popülerlik algısı yaratmak ve mağduru buna uymaya ikna etmek için referanslar veya onaylar gibi sosyal kanıtlar kullanabilir.

5. Oltalama Saldırıları

Oltalama, güvenilir biri gibi davranarak kurbanları kişisel bilgilerini vermeleri için kandırmayı içeren bir siber saldırı türüdür. Oltalama saldırılarında pek çok farklı tür vardır. Bunlar aşağıda detaylı olarak açıklanmıştır.

•**E-posta Oltalaması:** E-posta oltalamada saldırgan, banka, çevrimiçi perakendeci veya devlet kurumu gibi meşru bir kaynaktan geliyormuş gibi görünen ve tıklandığında alıcıyı kişisel bilgilerini girmeleri istenen sahte bir web sitesine yönlendiren bir bağlantı veya ek içeren bir e-posta gönderir. Sahte web sitesi genellikle meşru web sitesine benzer ve alıcının bunun gerçek olmadığını anlamasını zorlaştırır.

•**Kısa Mesaj Oltalaması (Smishing)**: Smishing, SMS (Kısa Mesaj Hizmeti) veya kısa mesajlar kullanarak bireyleri hassas bilgileri ifşa etmeleri veya belirli eylemleri gerçekleştirmeleri için kandırmayı içeren bir tür oltalama

saldırısıdır. "Smishing" terimi, e-posta yoluyla gerçekleştirilen benzer bir saldırı türünü ifade eden "SMS" ve "phishing" kelimelerinin birleşiminden oluşmaktadır. (Hong, 2012)

Smishing saldırıları genellikle banka, sosyal medya platformu kimliğine bürünerek güvenilir bir kaynaktan geliyormuş gibi görünen bir kısa mesaj gönderilmesidir. Mesajda genellikle alıcıdan bir bağlantıya tıklaması, bir uygulamayı indirmesi veya kişisel bilgilerini vermesi gibi belirli bir eylemde bulunması istenir. Mesajda ayrıca, alıcının hızlı hareket etmesi için baskı altında hissetmesine neden olan acil bir dil veya uyarılar da yer alabilir. (Salahdine, Kaabouch, 2019).

Alıcı oltalama saldırısına kanar ve istenen eylemi gerçekleştirirse, saldırgan oturum açma bilgileri, kredi kartı numaraları veya diğer kişisel veriler gibi hassas bilgilere erişim sağlayabilir. Saldırgan ayrıca alıcının cihazına kötü amaçlı yazılım veya başka bir kötü amaçlı yazılım yükleyebilir, bu da kurbanın bilgilerine daha fazla erişim elde etmesine veya cihazı üzerinde kontrol sahibi olmasına olanak sağlayabilir.

• **Sesli Oltalama (Vishing)**: Sesli oltalama olarak da bilinen Vishing, bir saldırganın kurbanları hassas bilgileri ifşa etmeleri veya hileli bir eylem gerçekleştirmeleri için kandırmak amacıyla genellikle telefon görüşmesi yoluyla sesli iletişim kullandığı bir sosyal mühendislik biçimidir. Saldırgan, banka temsilcisi, devlet memuru veya müşteri hizmetleri temsilcisi gibi güvenilir bir kaynak gibi davranabilir ve kurbanı parolalar, kredi kartı numaraları veya diğer hassas veriler gibi kişisel bilgileri ifşa etmeye ikna etmek için çeşitli taktikler kullanabilir.

Saldırgan, meşru bir arayanın kimliğine bürünmek veya kurbanın güvenini kazanmak için duygularını manipüle etmek için karmaşık teknikler kullanabileceğinden, oltalama saldırılarını tespit etmek zor olabilir. Vishing saldırılarında kullanılan bazı yaygın taktikler arasında aciliyet veya korku temelli mesajlar, ödül veya teşvik vaatleri veya bir sorunu çözmeye yardımcı olacak teklifler yer alır.

• **Hedefli Oltalama (Spear Pishing):** Spear phishing, belirli bir kişi veya kuruluşu hedef alan bir oltalama türüdür. Saldırgan, hedefi kandırarak parolalar veya hesap numaraları gibi hassas bilgileri ifşa etmesini veya bilgisayarına kötü amaçlı yazılım indirmesini sağlamak için bir iş arkadaşı, bir satıcı veya bir finans kurumu gibi güvenilir bir kaynaktan geliyormuş gibi görünen bir e-posta veya başka bir mesaj gönderir.

"Spear phishing" terimi, yüzen herhangi bir şeyi yakalamak için bir ağ yerine belirli bir balığı yakalamak için bir mızrak kullanma balıkçılık

tekniğinden türetilmiştir. Benzer şekilde, mızrakla oltalama geniş bir kitle yerine belirli bir kişi veya grubu hedef alır. (Gupta., Singhal, Kapoor, 2016).

Mızraklı oltalama saldırıları genellikle diğer oltalama türlerinden daha başarılıdır çünkü saldırgan hedef hakkında araştırma yapmıştır ve daha meşru görünen bir mesaj oluşturabilir. Ayrıca, e-posta veya mesaj hedef hakkında isim veya iş unvanı gibi kişisel bilgiler içerebilir, bu da daha güvenilir görünmesini sağlayabilir.

•**Balina Avı (Whaling):** Balina avcılığı, hassas bilgilere veya değerli varlıklara erişimi olan üst düzey yöneticileri veya bireyleri hedef alan bir sosyal mühendislik biçimidir. Kurbanı gizli bilgileri ifşa etmesi veya hileli bir finansal işlemi onaylaması için kandırmak amacıyla kişiselleştirilmiş ve ikna edici mesajlar kullanan bir tür oltalama saldırısıdır.

Whaling saldırıları genellikle e-posta yoluyla gerçekleştirilir, ancak telefon görüşmeleri, kısa mesajlar veya sosyal medya gibi diğer iletişim kanallarını da kullanabilirler. Saldırgan, mesajın meşru görünmesini sağlamak ve başarı şansını artırmak için genellikle sahte veya ele geçirilmiş e-posta hesapları kullanır.

Mesaj genellikle kurbanı sonuçlarını düşünmeden hızlı hareket etmeye teşvik etmek için acil veya zorlayıcı bir dil içerir. Saldırgan ayrıca kurbanın güvenini kazanmak ve gardını düşürmek için kimliğe bürünme gibi sosyal mühendislik taktikleri de kullanabilir.

•**Sosyal Medya Oltalaması:** Sosyal medya oltalamasında, saldırganın güvenilir kaynakların hesaplarını taklit eden sahte sosyal medya hesapları oluşturması ve daha sonra bu sahte hesapları bireylere mesaj göndermek ve onları hassas bilgiler vermeleri için kandırmak için kullanması durumunda ortaya çıkar.

•**Kötü Amaçlı Yazılım Tabanlı Oltalama (Malware-based Phishing)** : Kurbanın bilgisayarından veya cihazından oturum açma bilgileri veya finansal veriler gibi hassas bilgileri çalmak için kötü amaçlı yazılım kullanılmasını içeren bir oltalama saldırısı türüdür. (Chaudhry, Chaudhry, Rittenhouse, 2016).

•**Klon Oltalama (Clone Phishing):** Clone Phishing, bir saldırganın hedeflenen sitenin kullanıcılarından hassas bilgileri çalmak için hedeflenen web sitesiyle aynı görünen sahte bir web sitesi oluşturduğu bir oltalama saldırısı türüdür. Saldırgan, tasarımını, düzenini ve içeriğini kopyalayarak meşru web sitesinin bir klonunu oluşturur ve ardından meşru sitenin kullanıcılarına e-posta veya mesaj göndererek onları sahte web sitesine yönlendirir.

Kullanıcı sahte web sitesine giriş bilgilerini veya diğer hassas bilgilerini girdiğinde, saldırgan bu bilgileri kullanıcının hesaplarına erişmek, kişisel bilgilerini çalmak veya diğer dolandırıcılık türlerini gerçekleştirmek için kullanabilir.

Başarılı bir oltalama saldırısının sonuçları hem bireyler hem de kuruluşlar için önemlidir. Bireyler için, kişisel bilgilerin kaybı kimlik hırsızlığına, mali kayba ve mahremiyet kaybına yol açabilir. Kurumlar içinse bir oltalama saldırısı hassas bilgilerin çalınmasına, iş operasyonlarının aksamasına ve kurumun itibarının zarar görmesine neden olabilir. (Hong, 2012)

6. Sosyal Mühendislikten Korunmak

Sosyal mühendislikten korunma türleri, bireysel korunma ve kurumsal korunma olarak farklılık gösterir.

6.1. Bireysel Olarak Korunmak:

• **Sosyal Medya:** Sosyal medya platformlarında üçüncü taraf yazılımların kullanılması bazı risk ve endişeleri de beraberinde getirmektedir.

Sosyal medyada üçüncü taraf yazılımlarla ilişkili başlıca tehdit gizlilik ve veri güvenliğidir. Üçüncü taraf yazılımlar genellikle sosyal medya hesabınıza erişim gerektirir, bu da onlara belirli izinler vermek anlamına gelir. Bu izinler kişisel bilgilere, gönderilere, fotoğraflara ve arkadaş listelerine erişimi içerebilir. Bu üçüncü taraf uygulamaların verileri kötüye kullanma veya yanlış kullanma riski vardır, bu da gizlilik ihlallerine veya veri sızıntılarına yol açabilir (Thompson, 2018).

Üçüncü taraf yazılımların bir diğer tehdidi Spam ve istenmeyen içeriklerdir. Üçüncü taraf uygulamaları kullanmak spam mesajlara, istenmeyen reklamlara veya uygunsuz içeriğe maruz bırakabilir. Bu uygulamalar, hedefli reklamlar sunmak için kullanıcının ilgi alanları ve tercihleri hakkında veri toplayabilir veya kullanıcı bilgilerini izin olmadan diğer taraflarla paylaşabilir (Thompson, 2018).

Üçüncü taraf yazılımların bir diğer tehdidi de Kimlik hırsızlığıdır. Üçüncü taraf bir uygulamaya aşırı izinler verilirse, bu durum kimlik hırsızlığına yol açabilir. Kişisel bilgiler ve sosyal medya faaliyetlerini ilgili kullanıcıyı taklit etmek, kullanıcının finansal hesaplara erişmek veya diğer dolandırıcılık faaliyetlerinde bulunmak için kullanılabilir (Thompson, 2018).

Bu riskleri azaltmak için, sosyal medya platformlarında üçüncü taraf yazılımları kullanırken dikkatli olmak önemlidir. Kullanılan uygulamalar araştırılmalıdır. Bir uygulamaya erişim izni verilmeden önce itibarı, kullanıcı

yorumları ve gizlilik politikası araştırılmalıdır. Uygulamanın güvenilir ve saygın olduğundan emin olunmalıdır. Uygulamanın İzinleri Gözden Geçirilmelidir. Bir uygulama yüklerken, talep ettiği izinler dikkatlice gözden geçirilmelidir. Kişisel bilgilere gereksiz erişim izni vermekten kaçınılmalı ve artık kullanılmayan uygulamalar için izinler iptal edilmelidir.

Sosyal mühendislik saldırıları için bir araç olarak kullanılabileceğinden sosyal medya kullanılırken dikkatli olunmalıdır. Sosyal medyada paylaşılan kişisel bilgiler sınırlanmalı ve yalnızca tanıdığınız, güvendiğiniz kişilerden gelen arkadaşlık istekleri kabul edilmelidir.

• **Önlemleri Güncel tutmak:** Saldırganlar, şifreli bağlantılar kullanmak, hedef web sitesini gizlemek için kısaltılmış URL'ler kullanmak ve bireyleri hassas bilgiler vermeleri konusunda kandırmak için sosyal mühendislik tekniklerini kullanmak gibi geleneksel kimlik avı önleme tedbirlerinden kaçınmak için sürekli olarak yeni yollar bulmaktadır.

• **İki Faktörlü Kimlik Doğrulama (2FA):** İki faktörlü kimlik doğrulama (2FA), bir kullanıcının bir hesaba erişmek için iki kimlik biçimi sağlamasını gerektiren ek bir güvenlik katmanıdır. İki faktörlü kimlik doğrulamanın uygulanması, kimlik avı saldırılarının kullanıcı hesaplarını tehlikeye atmasını önlemeye yardımcı olabilir. İki faktörlü kimlik doğrulama ile bir kullanıcı hesabına erişmek için yalnızca şifresini değil, aynı zamanda telefonuna gönderilen tek seferlik bir kod gibi ikinci bir kimlik doğrulama biçimini de sağlamalıdır. Bu, saldırganların, kullanıcının şifresini bir kimlik avı saldırısı yoluyla elde etmiş olsalar bile, bir kullanıcının hesabına erişmelerini çok daha zor hale getirir. (Heartfield, Loukas, 2018).

• **URL Kısaltıcılar:** Saldırganlar, kimlik avı e-postası veya mesajındaki bir bağlantının gerçek hedefini gizlemek için URL kısaltıcıları kullanabilir. Bir bağlantıya tıklamadan önce, kişiler URL'nin tamamını görmek ve meşru, güvenilir bir web sitesine yönlendirdiğinden emin olmak için bağlantının üzerine gelmelidir. Bağlantı şüpheli görünüyorsa, en iyisi üzerine tıklamamaktır.

• **Ekler:** Kimlik avı e-postaları, yürütülebilir dosyalar veya gömülü kötü amaçlı yazılım içeren belgeler gibi kötü amaçlı ekler içerebilir. Herhangi bir eki açmadan önce, kişiler ekin güvenilir bir kaynaktan geldiğini ve yürütülebilir bir dosya olmadığını doğrulamalıdır. Ek bilinmeyen veya beklenmeyen bir kaynaktan geliyorsa, en iyisi e-postayı silmektir.

• **Mobil Cihazlar:** Kimlik avı saldırıları masaüstü ve dizüstü bilgisayarlarla sınırlı değildir. Saldırganlar kötü niyetli uygulamalar, kısa mesajlar ve e-postalar yoluyla akıllı telefonlar ve tabletler gibi mobil cihazları da hedef

alabilir. Mobil kimlik avı saldırılarına karşı korunmak için bireyler yalnızca Apple App Store veya Google Play gibi güvenilir kaynaklardan uygulama indirmeli ve hassas bilgiler isteyen kısa mesajlara ve e-postalara karşı dikkatli olmalıdır. (Hadnagy, 2010).

• **En İyi Uygulamalar:** Sosyal mühendislik saldırılarına maruz kalma riskini azaltmak için en iyi uygulamalar takip edilebilir. Yazılım ve güvenlik teknolojilerini düzenli olarak güncellemek ve önemli verileri düzenli olarak yedeklemek bu uygulamalardan bazılarıdır.

• **Alan Adı Sistemi (DNS) Filtreleme:** DNS filtreleme, bilinen kimlik avı siteleriyle ilişkili alan adlarının çözümlenmesini önleyerek kötü amaçlı web sitelerine erişimi engelleyen bir teknolojidir. Kuruluşlar, DNS filtrelemeyi kullanarak çalışanların oltalama sitelerine erişme ve oltalama saldırılarının kurbanı olma riskini azaltabilir.

• **Antivirüs Yazılımı:** Antivirüs yazılımı kötü niyetli ekleri, bağlantıları ve web sitelerini tespit edip engelleyerek oltalama saldırılarını önlemeye yardımcı olabilir. Kuruluşlar antivirüs yazılımlarını düzenli olarak güncelleyerek kimlik avı tehditlerine karşı en son korumalara sahip olduklarından emin olabilirler.

• **Sürekli İzleme:** Sosyal mühendislik sürekli olarak gelişmektedir, bu nedenle bireylerin ve kuruluşların yeni teknikleri sürekli olarak izlemeleri ve savunmalarını buna göre güncellemeleri önemlidir. Bu, yeni güvenlik teknolojilerinin uygulanmasını, çalışan eğitimlerinin güncellenmesini ve güvenlik odaklı bloglar, web siteleri ve haber kaynakları aracılığıyla en son tehditler hakkında bilgi sahibi olmayı içerebilir.

• **Kişisel Bilgilerin İfşası:** Şifre gibi hassas bilgileri paylaşmaktan kaçınılmalıdır. (Kumar, Chaudhary, Kumar, 2015) Saldırganlar tarafından sosyal mühendislik amacıyla kullanılabileceğinden, sosyal medyada ve diğer çevrimiçi platformlarda paylaşılan bilgiler konusunda dikkatli olunmalıdır.

• **Parola Yönetimi:** Her hesap için güçlü, benzersiz parolalar kullanılmalı ve bir parola yöneticisi kullanılmalıdır. Birden fazla hesap için aynı parolayı kullanmak, bu hesaplardan birinin ele geçirilmesi durumunda sizi savunmasız bırakır. Saldırganların hesaplara erişmesini önlemek için güçlü parolalar gereklidir. Şifrelerin ele geçirilme riskini en aza indirmek için şifrelerin düzenli olarak değiştirilmesi gerekmektedir. (Sadıku, Shadare, Musa, 2016).

• **Davranıştan Önce Düşünmek:** Herhangi bir eylemde bulunmadan önce talep düşünülmelidir. Gerçek olamayacak kadar iyi görünen bir teklif alınırsa, muhtemelen gerçek değildir. Hassas bilgileri isteyen her şeye şüpheyle yaklaşılmalıdır.

•**Açılır Pencereler:** Açılır pencereler, kötü amaçlı yazılım indirilmesi veya hassas bilgiler girilmesi için kullanılabilir. Yasal olduğundan emin olunmadığı sürece açılır penceredeki hiçbir şeye tıklanılmamalıdır.

•**Ücretsiz Wi-Fi:** Ücretsiz Wi-Fi noktaları kullanışlıdır, ancak aynı zamanda güvenlik riski de oluşturabilirler. Çevrimiçi bankacılık gibi hassas faaliyetler için kullanmaktan kaçınılmalıdır.

•**Halka Açık Şarj İstasyonları:** Saldırganlar cihaza kötü amaçlı yazılım yüklemek için halka açık şarj istasyonlarını kullanabileceğinden bu durum güvenlik riski oluşturabilir. Mümkün olduğunca bunları kullanmaktan kaçınılmalı veya yalnızca hassas olmayan faaliyetler için kullanılmalıdır.

•**Sanal Özel Ağ (VPN):** Bir VPN internet bağlantınızı şifreleyebilir ve sosyal mühendislik amacıyla kullanılabilecek gözetleme ve dinlemelere karşı korunma için yardımcı olabilir. (Hadnagy, 2010).

•**Teknik Destek Dolandırıcılığı:** Teknik destek dolandırıcılığı, bir saldırganın teknik destek temsilcisi gibi davranarak kötü amaçlı yazılım indirmeniz veya hassas bilgilerinizi ifşa etmeniz için sizi kandırmaya çalıştığı yaygın bir sosyal mühendislik saldırısı türüdür. İstenmeyen teknik destek çağrılarına güvenilmemeli ve her zaman arayan kişinin kimliği doğrulanmalıdır.

•**Web Tarayıcıları:** Sosyal mühendislik saldırılarına karşı korunmaya yardımcı olmak için kimlik avı koruması ve kötü amaçlı yazılım engelleme gibi güvenlik özelliklerine sahip güvenli bir web tarayıcısı kullanılmalıdır.

•**Halka Açık Bilgisayarlar:** İnternet kafeler veya kütüphanelerdeki halka açık bilgisayarlar, kötü amaçlı yazılım bulaşmış olabileceğinden güvenlik riski oluşturabilir. Bu bilgisayarları çevrimiçi bankacılık veya hassas faaliyetler için kullanmaktan kaçınılmalıdır.

•**Anti-spam Hizmeti Kullanımı:** Saygın bir anti-spam hizmeti, kötü niyetli e-postaları filtrelemenize ve sizi kimlik avı ve diğer sosyal mühendislik saldırılarından korumanıza yardımcı olur.

6.2. Kurumsal Olarak Korunmak

Sosyal Mühendislik, riskleri azaltmak için çok katmanlı bir yaklaşım gerektiren karmaşık ve sürekli gelişen bir tehdittir. Kuruluşlar sosyal mühendisliğe yaklaşımlarında uyanık ve proaktif olmalıdır, çünkü bunu yapmamak itibarlarına, mali durumlarına ve operasyonlarına önemli zararlar verebilir.

•**Olay Müdahale Planı:** Olay müdahale planı, siber güvenlik alanındaki güvenlik olaylarını ele almak ve yönetmek için tasarlanmış, belgelendirilmiş

bir dizi prosedür ve kılavuzdur. Kuruluşların güvenlik ihlallerini, siber saldırıları veya diğer güvenlik olaylarını etkili bir şekilde tespit etmeleri, bunlara yanıt vermeleri ve bunlardan kurtulmaları için yapılandırılmış bir yaklaşım sağlar (Thompson, 2018).

Bir olay müdahale planında yer alan aşamalar; Hazırlık, tanımlama, kontrol altına alma, yok etme, kurtarma, çıkarılan dersler, olay sonrası faaliyetler aşamalarıdır.

Hazırlık aşaması, kuruluşun etkili bir şekilde yanıt vermeye hazır olmasını sağlamak için bir olay meydana gelmeden önce yapılan tüm faaliyetleri içerir. Bu aşama şunları içerir:

Olay müdahale planının geliştirilmeli, güvenlik olaylarına müdahale etmek için kuruluşun prosedürlerini, rollerini, sorumluluklarını ve protokollerini özetleyen kapsamlı bir plan oluşturulmalıdır.

Olay müdahale ekibi kurulmalı, olay müdahale planının yürütülmesinden sorumlu olacak BT, güvenlik, hukuk ve iletişim gibi çeşitli departmanlardan kişilerden oluşan özel bir ekibin oluşturulmalıdır.

Rol ve sorumluluklar tanımlanmalı, olay müdahale ekibi üyelerine belirli rol ve sorumlulukların açık bir şekilde atanmalı, her bir kişinin görevlerini ve genel müdahale sürecine nasıl uyduklarını anlamaları sağlanmalıdır (Thompson, 2018).

İletişim protokollerinin belirlenmeli, olay müdahale ekibinin dahili ve harici olarak nasıl iletişim kuracağına dair iletişim listeleri, bildirim prosedürleri ve eskalasyon yolları da dahil olmak üzere kılavuz ilkeleri oluşturulmalıdır.

Gerekli araç ve teknolojiler edinilmeli, olay müdahale çalışmalarını desteklemek için olay yönetimi platformları, adli analiz araçları, izleme sistemleri ve iletişim araçları gibi gerekli araçlar belirlenmeli ve tedarik edilmelidir.

Eğitim ve farkındalık programları yürütülmeli, olay müdahale ekibi üyelerine ve diğer ilgili paydaşlara rolleri hakkında bilgi sahibi olmalarını, olay müdahale planına aşina olmalarını ve olayları etkili bir şekilde ele almaya hazır olmalarını sağlamak için düzenli eğitim ve farkındalık oturumları düzenlenmelidir.

Tanımlama aşaması potansiyel güvenlik olaylarının tanınmasını ve tespit edilmesini içerir. Bu aşama şunları içerir:

Sistemler ve ağlar izlenmeli, saldırı tespit sistemleri (IDS), saldırı önleme sistemleri (IPS), güvenlik bilgi ve olay yönetimi (SIEM) sistemleri ve günlük

analiz araçları gibi anormal faaliyetleri tespit etmek için izleme mekanizmaları uygulanmalıdır (Dorofee vd., 2018).

Güvenlik uyarıları ve raporlarına dikkat edilmeli, izleme sistemleri tarafından tetiklenen güvenlik uyarılarına, şüpheli etkinliklerin kullanıcı raporlarına veya bir güvenlik olayına işaret edebilecek diğer göstergelere yanıt verilmesi.

Olay biletleme yapılmalı, tespit zamanı, ilk değerlendirme ve ilgili bilgiler de dahil olmak üzere her olayın ayrıntılarını izlemek ve belgelemek için olay biletleri veya kayıtları oluşturmalıdır.

Kontrol altına alma aşaması, olayın daha fazla hasara yol açmasını önlemeye ve etkisini sınırlandırmaya odaklanır. Bu aşama şunları içerir:

Etkilenen sistemler izole edilmeli, olayın yayılmasını veya ortamın diğer bölümlerini etkilemesini önlemek için güvenliği ihlal edilmiş sistemler veya ağlar belirlenmeli ve izole edilmelidir.

Güvenliği ihlal edilmiş hesaplar veya hizmetler kapatılmalı, olayda ele geçirilen veya istismar edilen kullanıcı hesaplarının veya hizmetlerin askıya alınmalı veya devre dışı bırakılmalıdır. (Dorofee vd., 2018).

Geçici önlemler uygulanmalı, olay araştırılırken yetkisiz erişimi, daha fazla tehlikeye girmeyi veya veri sızıntısını önlemek için güvenlik duvarı kuralları, erişim kontrolleri veya ağ segmentasyonu gibi geçici önlemlerin alınmalıdır.

Yok etme aşaması, olayın nedeninin ortadan kaldırılmasını ve etkilenen sistemlerdeki kötü niyetli faaliyetlerin ortadan kaldırılmasını sağlar. Bu aşama şunları içerir:

Olayın temel nedeni belirlenmeli, tehlikenin boyutunu anlamak ve daha fazla analiz veya olası yasal işlemler için kanıt toplamak amacıyla ayrıntılı bir araştırma yürütülmelidir.

Kötü amaçlı yazılımlar kaldırılmalı, virüsler, truva atları veya arka kapılar gibi kötü amaçlı yazılımların tespit edilmesi ve etkilenen sistemlerden kaldırılmalıdır.

Güvenlik açıkları yamalanmalı, Yamalar veya güncellemeler uygulayarak olayda istismar edilen tüm sistem veya yazılım güvenlik açıkları belirlenmeli ve ele alınmalıdır.

Tehlike altındaki yapılandırmaları yeniden oluşturarak, yazılımı yeniden yükleyerek veya bilinen iyi yedeklerden kurtararak etkilenen sistemleri veya ağları güvenli bir duruma geri yüklenmelidir. (Thompson, 2018).

Kurtarma aşaması kuruluşun sistemlerinin, hizmetlerinin ve verilerinin normal operasyonlara döndürülmesini içerir. Bu aşama şunları içerir:

Hizmet restorasyonu yapılmalı, Etkilenen hizmetlerin, uygulamaların veya sistemlerin tekrar çevrimiçi hale getirilmeli ve düzgün çalıştıklarından emin olunmalıdır.

Kayıp veya tehlikeye atılmış verilerin yedeklerden veya diğer kaynaklardan kurtarılmalı ve bütünlüğü doğrulanmalıdır.

Geri yüklenen sistemlerin ve hizmetlerin beklendiği gibi çalıştığından ve tüm güvenlik kontrollerinin düzgün bir şekilde uygulandığından emin olmak için kapsamlı testler yapılmalıdır. (Dorofee vd., 2018).

Normal iş operasyonlarına kademeli olarak geri dönülmeli ve kalan sorunların olmadığından emin olmak için sistemler yakından izlenmelidir.

Çıkarılan dersler aşaması, iyileştirme alanlarını belirlemek için olay müdahale sürecinin gözden geçirilmesi ve analiz edilmesine odaklanır. Bu aşama şunları içerir:

Olay sonrası inceleme yapılmalı, alınan önlemler, müdahalenin etkinliği ve karşılaşılan zorluklar veya boşluklar da dahil olmak üzere olayın ayrıntılı bir analizinin yapılması.

İleride referans olması ve bilgi paylaşımı için olay detaylarının, toplanan kanıtların, gerçekleştirilen eylemler ve sonuçları belgelenmelidir.

Güçlü ve zayıf yönler belirlenmeli, olay müdahale sürecinin güçlü ve başarılı yönlerinin yanı sıra iyileştirilmesi veya daha fazla dikkat edilmesi gereken alanlar belirlenmelidir.

Olay müdahale planı güncellenmeli, gelecekteki müdahale kabiliyetlerini geliştirmek ve belirlenen zayıflıkları ele almak için olaydan çıkarılan dersler olay müdahale planına dahil edilmelidir (Dorofee vd., 2018).

Olay sonrası faaliyetler aşaması, olaya müdahale çalışmalarının tamamlanmasını ve kalan görevlerin ele alınmasını içerir. Bu aşama şunları içerir:

Müşteriler, iş ortakları veya düzenleyici makamlar gibi ilgili paydaşların olay, olayın çözümü ve atmaları gereken adımlar hakkında bilgilendirilmelidir.

Kayıt tutma, mevzuata uygunluk veya olası yasal işlemler için olayla ilgili tüm bilgilerin, kanıtların ve analizlerin uygun şekilde belgelenmelidir.

Geri bildirimler değerlendirilmeli, iyileştirme alanlarını belirlemek ve her türlü endişeyi veya sorunu ele almak için olay müdahale ekibi üyeleriyle bilgilendirme oturumları düzenlenmelidir.

Gelecekte benzer olayların meydana gelmesini önlemek için güvenlik kontrolü geliştirmeleri, süreç iyileştirmeleri veya politika güncellemeleri gibi gerekli değişiklikler belirlenmeli ve uygulanmalıdır (Dorofee vd., 2018).

Bu aşamalar genel bir çerçeve sunar ve kuruluşların bunları kendi özel ihtiyaçlarına, olay türlerine ve sektör gereksinimlerine göre uyarlamaları gerekebilir.

Olay müdahale planlamasında, kuruluşlar genellikle olayları kritiklik veya önem düzeylerine göre sınıflandırır. Bu sınıflandırma, her bir olayın etkisini azaltmak ve yanıt vermek için uygun kaynakların önceliklendirilmesine ve tahsis edilmesine yardımcı olur.

Bu sınıflandırma, Kritik Olaylar, Yüksek öncelikli olaylar, Orta öncelikli olaylar, Düşük öncelikli olaylar şeklindedir.

Kritik olaylar, bir organizasyonun operasyonlarına, varlıklarına veya itibarına ciddi etkileri olan olaylardır ve acil ve yoğun müdahale gerektirir. Bu tür olaylar genellikle kuruluşun sistemlerinde, verilerinde, hizmetlerinde veya itibarında önemli kesintilere, hasarlara veya kayıplara yol açar. Bu nedenle, kritik olayların etkilerini azaltmak ve yayılmasını engellemek için hızlı bir şekilde müdahale etmek gereklidir.

Kritik olayların yönetimi genellikle üst düzey yönetim, liderlik ve uzman kaynakların katılımını gerektirir ve ayrıca yasal veya düzenleyici sonuçları da olabilir. Bu nedenle, kritik bir olayın meydana gelmesi durumunda, hemen etkili bir müdahale ekibi oluşturulmalıdır, etkilenen sistemler izole edilmelidir ve olayın öncelikleri belirlenmelidir. Kontrol ve kurtarma planları uygulanarak olayın etkisi azaltılmalı ve olay sonrası detaylı bir analiz yapılmalıdır. Ayrıca, gelecekteki müdahaleleri geliştirmek için alınan dersler olay müdahale planına dahil edilmelidir. (Thompson, 2018)

Yüksek öncelikli olaylar, organizasyon üzerinde önemli bir etkiye sahip olabilir, ancak kritik olaylar kadar ciddi veya zaman açısından acil olmayabilirler. Yine de, bu tür olaylar hızlı ve özel müdahale çabalarını gerektirirler. Bu tür olayların özellikleri şunları içerir: Önemli bir etki yaratabilirler, organizasyonun sistemlerinde, verilerinde, hizmetlerinde veya paydaşlarında kayda değer aksaklıklara, hasarlara veya kayıplara neden olabilirler. Hızlı müdahale gerektirirler; olayın kontrol altına alınması, etkisinin sınırlanması ve etkilenen sistemlerin veya hizmetlerin eski haline getirilmesi için zamanında harekete geçilmesi önemlidir.

Paydaş katılımı da kritiktir, bu nedenle BT ekipleri, bölüm başkanları ve yönetim de dahil olmak üzere ilgili paydaşlar müdahale çalışmalarına dahil edilmelidir. Ayrıca, olayın niteliğine bağlı olarak yasal veya düzenleyici etkileri

de ele alınmalıdır. Bu tür olaylarla başa çıkmak için yapılması gerekenler arasında olay müdahale ekibinin hızla etkinleştirilmesi, olayla ilgili verilerin toplanması ve analiz edilmesi, yayılmanın sınırlanması için önlemlerin uygulanması, adli analiz yapılması ve ilgili taraflarla iletişim kurulması yer almaktadır. Ayrıca, olay sonrası inceleme süreci, müdahale sürecini değerlendirmek ve iyileştirmeler yapmak için önemlidir (Thompson, 2018).

Orta öncelikli olaylar, organizasyonun operasyonları veya varlıkları üzerinde orta düzeyde etkiye sahip olabilir, ancak kritik veya yüksek öncelikli olaylar kadar acil değildirler. Yine de, zamanında müdahale ve çözüm gerektirirler. Bu tür olayların özellikleri şunları içerir: Orta derecede etki yaratabilirler, organizasyonun sistemlerinde, verilerinde, hizmetlerinde veya kullanıcılarında gözle görülür aksaklıklara, rahatsızlıklara veya sınırlı zararlara neden olabilirler. Zamanında müdahale gerektirirler; olayı ele almak ve operasyonlar üzerindeki etkiyi en aza indirmek için makul bir zaman dilimi içinde harekete geçilmesi önemlidir. Departman katılımı da önemlidir, bu nedenle ilgili BT ekipleri, destek personeli veya bu tür olayları yönetmek ve çözmekten sorumlu departman başkanları müdahale sürecine dahil olmalıdır. Orta öncelikli olayların sınırlı yasal veya düzenleyici etkileri olabilir, ancak yine de organizasyonun politika ve prosedürlerine uyulması önemlidir.

Bu tür olaylarla başa çıkmak için yapılması gerekenler arasında olay müdahale sürecinin başlatılması, olayın kapsamının değerlendirilmesi, etkilenen sistemlerin izole edilmesi, kötü amaçlı yazılımların kaldırılması, güvenlik kontrollerinin gözden geçirilmesi ve çalışanlara farkındalık eğitimi verilmesi bulunmaktadır. Bu önlemler, orta öncelikli olayların etkisini en aza indirmeye ve organizasyonun süregelen güvenliğini sağlamaya yardımcı olur (Thompson, 2018).

Düşük öncelikli olaylar, kuruluşun operasyonları, varlıkları veya itibarı üzerinde asgari etkide bulunur. Genellikle rutin süreçler veya düzenli BT destek prosedürleri kullanılarak ele alınabilirler. Bu tür olayların özellikleri, minimum etki yaratmalarıdır; yani kuruluşun sistemlerini, verilerini, hizmetlerini veya kullanıcılarını önemli ölçüde etkilemeyen küçük aksaklıklara, rahatsızlıklara veya izole sorunlara neden olabilirler. Bu nedenle rutin müdahale gerektirirler; standart BT destek prosedürleri, uygulamaları ve iş akışları kullanılarak ele alınabilirler. Personel katılımı genellikle BT destek personeli veya yaygın operasyonel sorunları çözmekten sorumlu departman ekipleri tarafından sağlanır. Düşük öncelikli olayların genellikle yasal veya düzenleyici sonuçları yoktur veya çok azdır; daha çok operasyonel verimlilik ve kullanıcı memnuniyetine odaklanırlar.

Bu tür olaylarla başa çıkmak için yapılması gerekenler arasında sorumluluk atanması ve mevcut politika ve prosedürlerin gözden geçirilmesi bulunmaktadır. Özellikle bu tür olaylar, organizasyonun günlük işleyişini engellemeden hızlı ve etkili bir şekilde ele alınabilirler (Thompson, 2018).

•**Çalışanları Test Etmek:** Kuruluşlar ayrıca çalışanlarını düzenli olarak test ederek Sosyal Mühendislik saldırılarının riskini azaltmak için adımlar atabilirler. Bu, simüle edilmiş kimlik avı saldırıları veya diğer Sosyal Mühendislik senaryoları aracılığıyla yapılabilir. Bu tatbikatlar, çalışanların saldırılara karşı savunmasız olabilecekleri alanların belirlenmesine ve kuruluşların eğitim ve farkındalık çabalarının etkinliğini anlamalarına yardımcı olabilir. (Hadnagy, 2010).

•**Veri Yedekleme ve Kurtarma:** Kurumlar için bir diğer önemli husus da başarılı bir Sosyal Mühendislik saldırısı durumunda veri yedekleme ve kurtarmanın önemidir. Önemli verilerin düzenli olarak yedeklenmesi ve veri kaybından kurtulmak için bir plana sahip olmak, başarılı bir saldırının etkisini en aza indirmeye yardımcı olabilir. Bu, bulut tabanlı depolama, teyp yedeklemeleri veya verilerin korunmasını ve bir güvenlik ihlali durumunda kurtarılabilmesini sağlayan diğer yöntemler gibi yedekleme çözümlerinin kullanılmasını içerebilir.

•**Farkındalık:** Sosyal Mühendislik saldırılarına karşı korunmanın bir diğer önemli bileşeni de en yaygın saldırı türlerinin ve saldırganlar tarafından kullanılan taktiklerin farkında olmaktır. Bu, finansal kazanç, hassas bilgilerin çalınması veya operasyonların sekteye uğratılması gibi saldırıların arkasındaki motivasyonların anlaşılmasını da içerir. Bir Sosyal Mühendislik saldırısının belirtilerinin farkında olmak ve saldırganlar tarafından kullanılan yaygın taktikleri anlamak önemlidir. Örneğin, saldırganlar bireyleri hassas bilgileri ifşa etmeye veya güvenliği tehlikeye atacak eylemlerde bulunmaya ikna etmek için aciliyet, yetki veya yükümlülük duygusunu kullanabilir.

•**Olası Sonuçlar:** Kuruluşlar bir Sosyal Mühendislik saldırısının sonuçlarıyla başa çıkmaya hazırlıklı olmalıdır. Bu, hassas bilgilerin ifşa edilmesinden kaynaklanabilecek itibar zedelenmesini veya yetkisiz işlemlerin mali etkisini içerebilir. Bazı durumlarda, kuruluşlar bir Sosyal Mühendislik saldırısının sonucu olarak yasal işlemlere veya düzenleyici para cezalarına da maruz kalabilir. (Gold, 2010).

Kuruluşlar ayrıca bir Sosyal Mühendislik saldırısının mali kayıplar, itibar zedelenmesi ve yasal sonuçlar gibi olası sonuçlarıyla başa çıkmaya da hazırlıklı olmalıdır. Bazı durumlarda, kuruluşların etkilenen kişi ve kuruluşlara tazminat ödemesi gerekebilir ve ayrıca itibarlarını onarmak ve paydaşlarının güvenini yeniden kazanmak için adımlar atmaları gerekebilir.

•**Marka İtibarı:** Kuruluşlar marka itibarlarını koruma konusunda da dikkatli olmalıdır. Sosyal Mühendislik saldırıları genellikle bireyleri hassas bilgileri ifşa etmeleri veya belirli bir eylemde bulunmaları için kandırmak üzere tasarlanmış sahte veya yanıltıcı e-postaların, web sitelerinin veya telefon görüşmelerinin kullanılmasını içerir. (Hadnagy, 2010). Bu saldırılar, özellikle müşteriler veya iş ortaklarını etkiliyorsa, bir kuruluşun itibarına önemli zararlar verebilir. Kuruluşların bu saldırılara yanıt vermek ve itibarları üzerindeki etkilerini hafifletmek için bir planları olmalıdır.

•**Teknolojinin Kullanımı:** Kuruluşlar Sosyal Mühendislik saldırılarını tespit etmeye ve önlemeye yardımcı olmak için teknolojiden de yararlanabilir. Yapay zeka ve makine öğrenimi algoritmaları, bir saldırıya işaret edebilecek kalıpları ve anormallikleri belirlemek üzere büyük miktarda veriyi analiz etmek için kullanılabilir. Bu algoritmalar ayrıca kimlik avı e-postalarının, spam mesajların ve diğer Sosyal Mühendislik saldırılarının gerçek zamanlı olarak tespit edilmesine ve bunlara yanıt verilmesine yardımcı olabilir.

•**E-posta Güvenlik Önlemleri:** Kimlik avı saldırılarını önlemeye yardımcı olmak için kuruluşlar, Etki Alanı Tabanlı Mesaj Kimlik Doğrulama, Raporlama ve Uygunluk (DMARC), Gönderen İlkesi Çerçevesi (SPF) ve Etki Alanı Anahtarları Tanımlı Posta (DKIM) gibi e-posta kimlik doğrulama protokollerini uygulayabilir. Bu protokoller bir e-postanın gerçekliğini doğrulamaya yardımcı olarak kimlik avı e-postasının alıcının gelen kutusuna gönderilme olasılığını azaltır.

E-postaların iletilebilmesinin sınırlandırılması hassas bilgilerin yetkisiz taraflarla paylaşılmasını önlemeye yardımcı olabilir. Kuruluşlar, hassas bilgiler içeren e-postaların iletilmesini sınırlayan politikalar uygulamalı ve yetkisiz iletmeleri tespit etmek için e-posta faaliyetlerini izlemelidir.

E-posta filtreleme, oltalama e-postalarının çalışanların gelen kutularına ulaşmasını önlemeye yardımcı olabilir. Kuruluşlar, bilinen oltalama e-postalarını engellemek ve şüpheli içerik barındıran e-postaları işaretlemek için e-posta filtrelemesi uygulamalıdır.

E-posta ağ geçidi çözümleri, kurumları kimlik avı saldırıları da dahil olmak üzere e-posta kaynaklı tehditlere karşı korumak için tasarlanmış güvenlik teknolojileridir. E-posta ağ geçidi çözümleri, kimlik avı e-postalarının hedeflenen alıcılara ulaşmasını tespit etmek ve önlemek için filtreler, kural tabanlı politikalar ve tehdit istihbaratının bir kombinasyonunu kullanabilir.

•**Güçlü Parolalar:** Güçlü parolalar güvenliğin önemli bir unsurudur ve hassas bilgilere yetkisiz erişimi önlemeye yardımcı olur. Kuruluşlar,

çalışanların güçlü, benzersiz parolalar kullanmasını ve bunları düzenli olarak değiştirmesini gerektiren parola politikaları uygulamalıdır.

•**Şifreleme:** Hassas bilgilerin şifrelenmesi, kimlik avı saldırısı da dahil olmak üzere yetkisiz erişime karşı korunmasına yardımcı olabilir. Kuruluşlar, başarılı bir kimlik avı saldırısı durumunda veri ihlali riskini azaltmak için hassas verileri hem aktarım sırasında hem de beklemedeyken şifrelemelidir.

•**Yazılımın Güncel Tutulması:** Yazılımları güncel tutmak güvenlik açısından önemlidir ve oltalama saldırılarına karşı korunmaya yardımcı olabilir. Kuruluşlar, bilinen güvenlik açıklarına karşı korunduklarından emin olmak için web tarayıcıları, e-posta istemcileri ve diğer uygulamalar dahil olmak üzere yazılımlarını düzenli olarak güncellemelidir.

•**Sanal Özel Ağlar (VPN'ler):** Sanal Özel Ağlar (VPN'ler) internete şifrelenmiş bir bağlantı sağlar ve hassas bilgileri şifreleyerek ve yetkisiz erişimi önleyerek kimlik avı saldırılarına karşı korunmaya yardımcı olabilir. Kuruluşlar, uzaktan çalışanlar veya hassas bilgilere genel ağlardan erişmesi gereken çalışanlar için VPN'leri uygulamayı düşünmelidir. (Hadnagy, 2010).

•**İzleme ve Günlüğe Kaydetme:** İzleme ve kayıt tutma, kuruluşların kimlik avı saldırılarını tespit etmesine ve zararı en aza indirmek için hızlı bir şekilde yanıt vermesine yardımcı olabilir. Kuruluşlar, kimlik avı girişimleri de dahil olmak üzere şüpheli faaliyetler için sistemlerini ve ağlarını izlemeli ve adli amaçlarla tüm faaliyetlerin ayrıntılı günlüklerini tutmalıdır.

•**Web Uygulaması Güvenlik Duvarları (WAF'lar):** Web uygulaması güvenlik duvarları (WAF'lar), web sitelerini ve web uygulamalarını kimlik avı saldırıları da dahil olmak üzere kötü niyetli saldırılardan korumak için tasarlanmış güvenlik teknolojileridir. WAF'lar, web üzerinden iletilen kimlik avı saldırıları da dahil olmak üzere kötü niyetli trafiği tespit etmek ve engellemek için filtreler, kural tabanlı ilkeler ve tehdit istihbaratının bir kombinasyonunu kullanır. (Hadnagy, 2010).

•**Ağ İzleme:** Ağ faaliyetlerinin düzenli olarak izlenmesi, Sosyal Mühendislik saldırılarının gerçek zamanlı olarak tespit edilmesine ve bunlara yanıt verilmesine yardımcı olabilir. Bu, beklenmedik giden ağ trafiği veya oturum açma davranışındaki değişiklikler gibi şüpheli etkinliklerin izlenmesini içerebilir.

•**Politika ve Prosedürler:** Kuruluşlar ayrıca Sosyal Mühendislik saldırılarını önlemek için sıkı politikaları ve prosedürleri uygulamalıdır. Bu, parola yönetimi, erişim kontrolü ve veri koruma politikalarının yanı sıra e-posta, internet ve diğer teknolojilerin kullanımına ilişkin yönergeleri de içerebilir. Çalışanlar bu politikaların farkında olmalı ve bunları tutarlı

bir şekilde takip etmeleridirler (Hadnagy, 2010). Kuruluşlar ayrıca Sosyal Mühendislik saldırılarına yanıt vermek için, olayların raporlanması ve kolluk kuvvetlerinin bilgilendirilmesi prosedürleri de dahil olmak üzere açık politikalara sahip olmalıdır.

• **Farkındalık Programları:** Düzenli farkındalık programları, çalışanların en son güvenlik tehditleri ve oltalama saldırılarından kaçınmak için en iyi uygulamalar hakkında bilgilendirilmesine yardımcı olabilir. Kuruluşlar, çalışanların bilgi sahibi ve tetikte olmalarına yardımcı olmak için simüle edilmiş kimlik avı tatbikatları da dahil olmak üzere düzenli güvenlik farkındalığı programları geliştirmeli ve uygulamalıdır.

• **Erişim Kontrolü Önlemleri:** Sosyal Mühendislik saldırılarını önlemenin bir diğer önemli yönü de güçlü erişim kontrolü önlemleri uygulamaktır. Bu, kullanıcıların kimliğini doğrulamak için çok faktörlü kimlik doğrulamanın yanı sıra yalnızca yetkili kullanıcıların hassas bilgilere ve sistemlere erişebilmesini sağlamak için rol tabanlı erişim kontrollerinin kullanılmasını içerebilir. Erişim kontrol sistemleri ayrıca yetkisiz erişim girişimlerinin izlenmesine ve tespit edilmesine yardımcı olarak kuruluşların bir saldırı durumunda hızlı bir şekilde yanıt vermelerini sağlayabilir.

• **İletişim Planı:** Bir Sosyal Mühendislik saldırısı durumunda çalışanları, müşterileri ve diğer paydaşları bilgilendirmek için kuruluşların sağlam bir iletişim planına sahip olmaları önemlidir. Bu iletişim planı, etkilenen kişi ve kuruluşlarla iletişim kurma prosedürlerinin yanı sıra güncellemeler sağlama ve soru ve endişelere yanıt verme prosedürlerini de içermelidir.

• **Kullanıcı Eğitimi:** Çalışanların eğitimi ve bilgilendirilmesi, sosyal mühendislik saldırılarını önlemenin önemli bir yönüdür. Bu, çalışanlara oltalama e-postalarını nasıl tanıyacaklarını, oltalama dolandırıcılığına düşmekten nasıl kaçınacaklarını ve şüpheli oltalama girişimlerini nasıl bildireceklerini öğretmeyi içerir. Düzenli eğitim, çalışanların en son oltalama teknikleri hakkında bilgi sahibi olmalarına ve bu tür tehditlere karşı savunmalarını güçlü tutmalarına yardımcı olur.

Buna ek olarak, kuruluşlar hem bilerek hem de bilmeyerek çalışanların oluşturduğu potansiyel risklerin farkında olmalıdır. Çalışanlar Sosyal Mühendislik saldırılarına hedef olabilir veya oltalama dolandırıcılıklarına kanarak ya da hassas bilgileri yetkisiz kişilerle paylaşarak istemeden güvenliği tehlikeye atabilirler. (Hadnagy, 2010). Kurumların çalışanlarını bu riskler konusunda eğitmesi ve bu tür olayların meydana gelmesini önleyecek kontroller uygulaması önemlidir.

•**Güvenlik Politikaları:** Teknik kontrollerin uygulanmasına ek olarak, kuruluşlar işgücü içinde bir güvenlik kültürünü teşvik etme konusunda da proaktif olmalıdır. Bu, güvenlik riskleri ve tehditleri hakkında düzenli iletişimin yanı sıra güvenlik politikaları ve prosedürlerine uymanın önemini de içerir. Düzenli güvenlik eğitimi ve eğitim oturumları da çalışanların Sosyal Mühendislik saldırılarının yarattığı riskleri ve bu saldırıların nasıl tespit edilip karşılık verileceğini anlamalarına yardımcı olabilir. (Mann, 2017).

Sosyal Mühendislik saldırılarında kullanılan yeni trendler ve taktikler hakkında bilgi sahibi olmak önemlidir. Bu, güvenlik bloglarını izleyerek, sektör konferanslarına katılarak veya çevrimiçi topluluklardaki güvenlik uzmanlarıyla etkileşime geçerek yapılabilir. En son Sosyal Mühendislik tehditleri hakkında bilgi sahibi olmak ve güncel kalmak, kuruluşların bu tür saldırılara karşı daha hazırlıklı olmalarına ve daha etkili bir şekilde yanıt vermelerine yardımcı olabilir.

Kurumların Sosyal Mühendislik saldırılarıyla mücadele etmek için güvenlik uzmanlarıyla iş birliği yapması da önemlidir. Bu, tehditler ve saldırılar hakkında bilgi paylaşımının yanı sıra saldırganları tespit etmek ve yakalamak için birlikte çalışmayı da içerebilir. Kuruluşlar, diğer kuruluşlarla bilgi ve en iyi uygulamaları paylaşabilecekleri bilgi paylaşım ağlarının ve topluluklarının bir parçası olmaktan da faydalanabilirler.

Kuruluşların en son Sosyal Mühendislik saldırıları ve tehditleri hakkında bilgi sahibi olmaları ve güvenlik duruşlarını sürekli olarak değerlendirip iyileştirmeleri de önemlidir. Bu, düzenli güvenlik denetimleri ve sızma testleri gerçekleştirmeyi ve bilgi paylaşım ağlarına ve topluluklarına katılmayı içerebilir. (Mann, 2017).

Kuruluşlar, çalışanların şüpheli oltalama girişimlerini bildirmeleri için bir raporlama mekanizmasına sahip olmalıdır. Bu, çalışanların kimlik avı e-postalarını ve diğer şüpheli etkinlikleri bildirmek için kullanabilecekleri bir e-posta adresi, yardım hattı veya özel bir form içerebilir.

Çalışanları şüpheli oltalama girişimlerini bildirmeye teşvik etmek oltalama saldırılarını önlemenin önemli bir parçasıdır. Kuruluşlar, şüpheli oltalama girişimlerini hızlı bir şekilde bildirerek saldırının yayılmasını önlemek ve saldırıdan kaynaklanan zararı en aza indirmek için adımlar atabilir.

Son olarak, kuruluşlar veri ihlalleri ve hassas bilgilerin kaybı riskini en aza indirmek için sağlam veri koruma önlemlerine sahip olduklarından emin olmalıdır. Bu önlemler arasında veri yedekleme ve felaket kurtarma çözümlerinin uygulanması, sistemlerin ve uygulamaların şüpheli faaliyetlere

karşı düzenli olarak izlenmesi ve iyi belgelenmiş bir veri saklama ve imha politikasının yürürlükte olması sayılabilir.

7. Sonuç

Sonuç olarak, bu araştırma sosyal mühendislik ve oltalama saldırıları alanında değerli bilgiler sağlamıştır. Çalışma, kötü niyetli aktörlerin bireyleri manipüle etmek ve hassas bilgilere yetkisiz erişim sağlamak için kullandıkları teknikleri keşfetmeyi amaçlamıştır. Çeşitli vaka çalışmalarının ve mevcut literatürün incelenmesi sonucunda bazı önemli bulgular ortaya çıkmıştır.

İlk olarak, sosyal mühendislik saldırılarının insani zaaflardan ve psikolojik manipülasyondan yararlanması nedeniyle oldukça etkili olduğu ortaya çıkmıştır. Bu saldırılar genellikle kurbanın güvenine, merakına veya aciliyetine dayanır, bu da onları gizli verileri ifşa etmeye veya güvenliği tehlikeye atan eylemler gerçekleştirmeye duyarlı hale getirir.

Dahası, oltalama saldırılarının sosyal mühendisliğin en yaygın biçimlerinden biri olduğu tespit edilmiştir. Saldırganlar genellikle sahte e-postalar, sahte web siteleri veya sahte iletişimler gibi aldatıcı taktikler kullanarak şüphelenmeyen kişileri kişisel bilgilerini, şifrelerini veya finansal detaylarını ifşa etmeleri için kandırmaktadır.

Ayrıca, sosyal mühendislik ve oltalama saldırılarının teknolojik gelişmelere uyum sağlayarak ve yeni platformlar ve iletişim kanallarından yararlanarak evrim geçirmeye devam ettiğini kabul etmek çok önemlidir. Teknoloji daha sofistike hale geldikçe saldırganlar tarafından kullanılan taktikler de gelişmektedir. Bu riskleri azaltmak için bireylerin ve kuruluşların tetikte olmaları ve en son trendler ve karşı önlemler hakkında bilgi sahibi olmaları çok önemlidir.

Sosyal mühendislik ve oltalama saldırılarına karşı koymak için çok yönlü bir yaklaşım gereklidir. Eğitim ve farkındalık programları, bireylerin bu manipülatif teknikleri tanıma ve bunlara direnme bilgisiyle donatılmasında kritik bir rol oynamaktadır. Kuruluşlar, hassas veri ve sistemleri korumak için iki faktörlü kimlik doğrulama, şifreleme ve düzenli güvenlik denetimleri dahil olmak üzere sağlam güvenlik protokolleri uygulamalıdır.

Sosyal Mühendislik saldırılarının önlenmesi ve etkisinin azaltılması, çalışanların farkındalığı ve eğitimi, teknik kontroller, güçlü güvenlik politikaları ve prosedürleri, güvenlik uzmanları ve diğer kuruluşlarla iş birliği ve sürekli izleme ve değerlendirmeyi içeren çok katmanlı bir yaklaşım gerektirir. Kuruluşlar, güvenlik çabalarında proaktif ve dikkatli davranarak

Sosyal Mühendislik saldırılarının kurbanı olma riskini azaltabilir ve bir saldırı durumunda etkili bir şekilde yanıt vermeye hazırlıklı olmalarını sağlayabilir.

Sonuç olarak araştırma, sürekli gelişen tehdit ortamıyla mücadele etmek için sosyal mühendislik ve oltalama saldırılarını anlamanın önemini vurgulamaktadır. Teknolojik savunmaları kullanıcı farkındalığı ve eğitimi ile birleştirerek bireyler ve kuruluşlar bu aldatıcı taktiklere karşı dirençlerini artırabilir ve dijital varlıklarını etkili bir şekilde koruyabilirler. Sektör profesyonelleri, araştırmacılar ve kolluk kuvvetleri arasında devam eden araştırma ve işbirliği, sosyal mühendislik ve oltalama saldırılarının gelişen doğasının bir adım önünde olmak ve herkes için daha güvenli bir dijital ortam sağlamak için hayati önem taşımaktadır.

Kaynakça:

Barber, R. (2001). Social engineering: A People Problem? *Network Security, 2001*(7), 9–11. doi:10.1016/s1353-4858(01)00716-4

Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. *International Journal of Security and Its Applications, 10*(1), 247–256. doi:10.14257/ijsia.2016.10.1.23

Direction, S. (2015). Are you being manipulated? Social marketing, social engineering and democratic government.

Gold, S. (2010). Social engineering today: psychology, strategies and tricks. *Network Security, 2010*(11), 11–14. doi:10.1016/s1353-4858(10)70135-5

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. In *2016 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 537-540). IEEE.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons. (pp. 4-111)

Heartfield, R., & Loukas, G. (2018). Protection Against Semantic Social Engineering Attacks. *Advances in Information Security*, 99–140. doi:10.1007/978-3-319-97643-3_4

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74. doi:10.1145/2063176.2063197

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113–122. doi:10.1016/j.jisa.2014.09.005

Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social Engineering Threats and Awareness: A Survey. *European Journal of Advances in Engineering and Technology, 2*(11), 15-19.

Mann, I. (2017). *Hacking the human: social engineering techniques and security countermeasures*. Routledge.

Özmen, C. (2020). Sosyal mühendislik bağlamında bilgi güvenliğinin endüstri 4.0 tabanlı sistemlere uyarlanması.

Ramzan, Z. (2010). Phishing Attacks and Countermeasures. In *Handbook of Information and Communication Security* (pp. 433–448). doi:10.1007/978-3-642-04117-4_23

Sadıku, M. N., Shadare, A. E., & Musa, S. M. (2016). Social Engineering: An Introduction. *Journal of Scientific and Engineering Research, 3*(3), 64-66.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89. doi:10.3390/fi11040089

Uebelacker, S., & Quiel, S. (2014, July). The social engineering personality framework. In *2014 Workshop on Socio-Technical Aspects in Security and Trust* (pp. 24-30). IEEE.

Johnson, O. C. (2018). Social Engineering: Notes on the Law and Political Economy of Integration. *Cardozo L. Rev., 40*, 1149.

Mouton, F., Malan, M. M., & Venter, H. S. (2013, August). Social engineering from a normative ethics perspective. In *2013 Information Security for South Africa* (pp. 1-8). IEEE.

Shinde, N., & Kulkarni, P. (2021). Cyber incident response and planning: a flexible approach. *Computer Fraud & Security, 2021*(1), 14-19.

Thompson, E. C. (2018). Cybersecurity incident response: How to contain, eradicate, and recover from incidents. Apress.

Dorofee, A., Ruefle, R., Zajicek, M., McIntire, D., Alberts, C., Perl, S., ... & Walters, P. (2018). Incident Management Capability Assessment. *CMU/SEI*. URL: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2018_005_001_538866.pdf (accessed by 27.05.2022).