



**SİBER GÜVENLİKTE SOSYAL MÜHENDİSLİĞE KARŞI BİR MODEL
GELİŞTİRİLEREK TEST EDİLMESİ**

Berna TOZLU

**YÜKSEK LİSANS TEZİ
BİLİŞİM SİSTEMLERİ ANA BİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

MART 2021

Berna TOZLU tarafından hazırlanan “SİBER GÜVENLİKTE SOSYAL MÜHENDİSLİĞE KARŞI BİR MODEL GELİŞTİRİLEREK TEST EDİLMESİ” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Çelebi ULUYOL

Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

.....

Başkan: Prof. Dr. Refik SAMET

Bilgisayar Mühendisliği Bölümü, Ankara Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

.....

Üye: Dr. Öğr. Üyesi Uraz YAVANOĞLU

Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

.....

Tez Savunma Tarihi: 20/03/2021

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....

Prof. Dr. Aslıhan TÜFEKÇİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Berna TOZLU

20 /03/2021

SİBER GÜVENLİKTE SOSYAL MÜHENDİSLİĞE KARŞI BİR MODEL GELİŞTİRİLEREK TEST EDİLMESİ

(Yüksek Lisans Tezi)

Berna TOZLU

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

Mart 2021

ÖZET

Günümüzün gelişen teknolojisi, yapılan bilimsel çalışmalar, geliştirilen sistemler ve bu sistemlere artan erişim imkânları insanların hayatlarını kolaylaştırdığı gibi beraberinde pek çok tehlikeyi de getirmiştir. Siber güvenlik kavramı soyut bir ifade olduğu için siber güvenlik alanında en zayıf halka olan kişiler, bu kavramı anlamakta ve uygulamakta güçlük çekmektedir. Şirketler, kurum ve kuruluşlar bu durumu göz önüne alarak hem çağın gerisinde kalmamak hem de yönetim alanlarında yüksek güvenlik önlemleri almak için büyük bütçeler ayırmaktadır. Ülkemiz genelinde kurum ve kuruluşlar siber güvenlik konusunda gerekli tedbirleri alıp çalışanlarını bu yönde bilgilendirmektedir. Son zamanlarda Sosyal Mühendislik uygulamaları ile kullanıcılarının bilgileri toplanmakta ve zafiyetleri test edilmektedir. Bu araştırmada çalışanlara yönelik sosyal mühendislik saldırıları gerçekleştirilmiştir. Araştırma bulgularından yola çıkılarak kullanıcıya pratik yoldan yol gösterecek, aldığı siber güvenlik eğitimlerini pekiştirecek ve olası bir siber saldırı anında doğru karar vermesini sağlayacak yeni bir filtre model geliştirilmiştir. Ortaya konan model genelden özele filtreleme yapmaktadır. Genelden kasıt burada kamu kurumunun alması gereken önlemler iken özel ise kamuda çalışan kullanıcıların alması gereken önlemleri ifade etmektedir. Çalışmanın sonunda model sosyal mühendislik saldırı senaryoları ile test edilmektedir. Sonuç olarak geliştirilen modelin siber güvenlik farkındalığını artıracak ve büyük bütçeler harcanarak alınan fakat istenen başarıyı sağlayamayan eğitimlerin yanında destekleyici unsur olarak olumlu katkılar sağlayacağı değerlendirilmektedir. Çıkan sonuçlar incelendiğinde kullanıcıların siber güvenlik hakkında daha fazla farkındalığa ve bilince ihtiyaç duyduğu açıkça görülmektedir.

Bilim Kodu : 92403
Anahtar Kelimeler : Siber güvenlik, sosyal mühendislik, insan zafiyeti, siber saldırı, farkındalık, eğitim, model
Sayfa Adedi : 149
Danışman : Doç. Dr. Çelebi ULUYOL

DEVELOPING AND TESTING A MODEL AGAINST SOCIAL ENGINEERING IN CYBER SECURITY

(M. Sc. Thesis)

Berna TOZLU

GAZİ UNIVERSITY
INSTITUTE OF INFORMATICS

March 2021

ABSTRACT

While developing technology of today, scientific studies, developed systems and increasing access opportunities to these systems have made lives of people easier; they also have brought many dangers with them. Since the concept of cyber security is an abstract expression, people who are the weakest link in the field of cyber security have difficulty understanding and applying this concept. Considering this situation, companies, institutions and organizations have allocated large budgets both in order to take high security measures in management areas and not to stay behind the time. Institutions and organizations throughout our country have taken the necessary precautions regarding cyber security and informed their employees in this direction. Recently, many organizations have collected information of their users and tested their vulnerabilities with Social Engineering applications. In this research, social engineering attacks were carried out against employees. Based on the findings of the research, a new filter model has been developed that will guide the user in a practical way, reinforce the cyber security training it received, and make the right decision at the time of a possible cyber attack. The model developed filters from general to specific. What the general means is the measures that the public institution should take, while the specific refers to the precautions that the users working in the public sector should take. At the end of the study, the model is tested with social engineering attack scenarios. As a result, it is considered that the developed model will increase cyber security awareness and will provide positive contributions as a supportive factor in addition to the trainings that are received by spending large budgets but cannot achieve the desired success. When the results are examined, it is clear that the users need more awareness and consciousness about cyber security.

Science Code : 92403
Key Words : Cyber security, social engineering, human vulnerability, cyber-attack, awareness, education, model
Page Number : 149
Supervisor : Doç. Dr. Çelebi ULUYOL

TEŞEKKÜR

Bu tezin belirlenmesi ve yazılması sürecinde katkı ve yönlendirmeleri ile destek veren danışmanım Doç. Dr. Çelebi ULUYOL'a; konu hakkındaki teknik bilgileri, yorumları ve değerlendirmeleri ile tezime katkıda bulunan kıymetli hocalarıma ve arkadaşlarıma; içerik, dilbilgisi ve eleştirel yaklaşımları ile yardımlarını esirgemeyen Üst Kurul Uzman Yardımcısı Uğur Can KOLANCI 'ya ve Yüksek Lisans eğitimim süresince destekleriyle beni yalnız bırakmayan değerli aileme teşekkür ve şükranlarımı sunarım.



İÇİNDEKİLER

	Sayfa
ÖZET	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER	vii
ÇİZELGELERİN LİSTESİ.....	ix
ŞEKİLLERİN LİSTESİ	xv
SİMGELER VE KISALTMALAR.....	xvii
1. GİRİŞ.....	1
2. TEMEL BİLGİLER	9
2.1. Siber Güvenlik Kavramı	10
2.1.1. Siber güvenlik zafiyeti	13
2.2. Siber Saldırıları	20
2.2.1. Siber saldırı yöntemleri.....	21
2.2.2. 2019 yılının öne çıkan siber saldırı örnekleri	29
2.3. Siber Saldırıların Tespiti ve Sınıflandırılması	35
2.3.1. Amaçlarına göre sınıflandırma	37
2.3.2. Yasal sınıflandırma.....	37
2.3.3. Dâhil olma şiddetine göre sınıflandırma.....	38
2.3.4. Kapsamına göre sınıflandırma	39
2.3.5. Ağ türüne göre sınıflandırma.....	39
2.4. Sosyal Mühendislik.....	41
2.4.1. Sosyal mühendislik saldırı döngüsü	44
2.4.2. Yaygın sosyal mühendislik saldırı türleri	46
2.4.3. Bazı popüler sosyal mühendislik teknikleri.....	54

	Sayfa
2.4.4. Sosyal mühendislik saldırıları nasıl gerçekleşir?	56
2.4.5. Sosyal mühendislik saldırılarının hedefleri kimlerdir?	59
2.4.6. İnsan faktörü	61
2.4.7. Sosyal mühendislerin kullandığı insani duygular	63
2.4.8. Sosyal mühendislik saldırılarından korunma	67
3. LİTERATÜR ÖZETİ	73
3.1. Sosyal Mühendislikte İnsan Faktörünün Yeri	76
3.2. Siber Güvenlik Farkındalık Eğitimi	79
3.3. Farkındalık Modelleri Literatür İncelemesi	83
4. MATERYAL VE YÖNTEM	87
4.1. Çalışma Grubu	88
4.2. Önerilen Model	89
4.2.1. Modelin adımları	92
4.3. Araştırmada Kullanılan Materyaller	108
4.4. Uygulama Süreci	114
5. ARAŞTIRMA BULGULARI	117
5.1. Sosyal Mühendislik Uygulamaları Sonuçlarının İncelenmesi ve Analizi	117
5.1.1. Uygulama senaryosu-1 sonuçlarının incelenmesi	117
5.1.2. Uygulama senaryosu-2 sonuçlarının incelenmesi	119
5.1.3. Uygulama senaryosu-3 sonuçlarının incelenmesi	122
6. SONUÇ, TARTIŞMA VE ÖNERİLER	127
KAYNAKLAR	137
EKLER	147
EK-1. Etik kurul kararı	148
ÖZGEÇMİŞ	149

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 2.1. Ağ türüne göre saldırıların farklı türleri	41
Çizelge 4.1. Çalışma grubunun cinsiyete göre dağılımı	88
Çizelge 4.2. Çalışma grubunun yaş dağılımları	89
Çizelge 4.3. Çalışma grubunun öğrenim durumuna göre dağılımı	89
Çizelge 5.1. Uygulama senaryosu-1 sonuçlarının cinsiyete bağlı dağılımı	119
Çizelge 5.2. Uygulama senaryosu-1 sonuçlarının yaş gruplarına göre dağılımı	119
Çizelge 5.3. Uygulama senaryosu-2 sonuçlarının cinsiyete bağlı dağılımı	122
Çizelge 5.4. Uygulama senaryosu-2 sonuçlarının yaşa göre dağılımı	122
Çizelge 5.5. Uygulama senaryosu-3 sonuçlarının cinsiyete bağlı dağılımı	125
Çizelge 5.6. Uygulama senaryosu-3 sonuçlarının yaşa göre dağılımı	125

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 1.1. Dünya’da siber güvenlik yatırımları (Dolar)	4
Şekil 1.2. Türkiye’de siber güvenlik yatırımları (Dolar)	4
Şekil 2.1. Bilgi güvenliği üçlüsü (CIA Triad).....	11
Şekil 2.2. Siber güvenlik zaafıları ve sonuçları	15
Şekil 2.3. Siber güvenlik zafiyetleri.....	16
Şekil 2.4. En yüksek saldırı türü oranları.....	22
Şekil 2.5. 2019 yılında türe göre ihlal olayları.....	34
Şekil 2.6. 2019 yılında ihlal edilen kayıtlar	35
Şekil 2.7. Saldırıların sınıflandırılma diyagramı.....	36
Şekil 2.8. Sosyal mühendislik saldırı yolu.....	43
Şekil 2.9. Sosyal mühendislik saldırısının yaşam döngüsü	44
Şekil 2.10. Sosyal mühendislik saldırısının ontolojik modeli	47
Şekil 2.11. Tersine sosyal mühendislik adımları	48
Şekil 2.12. En yaygın insan zafiyetleri	64
Şekil 3.1. 2020 Türkiye internet kullanım istatistikleri	73
Şekil 3.2. Türkiye’de siber güvenliğin gelişimi.....	74
Şekil 3.3. Kurum çalışanları risk algısı araştırması	75
Şekil 3.4. Zararlı yazılım yükleme vektörü	78
Şekil 4.1. Model geliştirilirken uygulanan adımlar	87
Şekil 4.2. Çalışma kapsamında önerilen filtre model	91
Şekil 4.3. Ana başlıklar halinde kurumların alması gereken önlemler	97
Şekil 4.4. Ana başlıklar halinde kullanıcıların alması gereken önlemler	102
Şekil 4.5. Uygulama senaryo-1 giriş ekranı.....	104
Şekil 4.6. Uygulama senaryo-2 giriş ekran.....	106
Şekil 4.7. Uygulama senaryo-3 uyarı ekranı.....	107

Şekil	Sayfa
Şekil 4.8. E-Kampüs giriş ekranı	109
Şekil 4.9. Siber güvenlik eğitim videoları örnek sayfa	110
Şekil 4.10. Eğitim içeriği örnek sayfa.....	110
Şekil 4.11. Eğitim adımları örnek sayfa.....	112
Şekil 4.12. Eğitim sınav sonuç ekranı.....	113
Şekil 5.1. Uygulama senaryosu-1 sonuçları.....	118
Şekil 5.2. Uygulama senaryosu-2 sonuçları.....	121
Şekil 5.3. Uygulama senaryosu-3 sonuçları.....	124

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ATM	Bankamatik (Automated Teller Machine)
B2B	Business to Business
BT	Bilgi Teknolojileri
CD	Yoğun Disk (Compact Disc)
CEO	Genel Müdür (Chief Executive Officer)
CFO	Finans Departmanı Başkanı (Chief Financial Officer)
DDOS	Dağıtık Hizmet Engelleme (Distributed Denial of Service)
DNS	Bölge Ad Sunucusu (Domain Name Server)
FTP	Dosya Transfer Protokolü (File Transfer Protocol)
HTTP	Hipermetin Aktarma İletişim Protokolü (Hypertext Transfer Protocol)
IANA	İnternet Atanmış Numaralar Yetkilisi (Internet Assigned Numbers Authority)
IIS	İnternet Bilgi Sunucusu (Internet Information Service)
KVKK	Kişisel Verileri Koruma Kanunu
LDAP	Dizin Erişim Protokolü (Lightweight Directory Access Protocol)
MAC	Ortam Erişim Yönetimi (Media Access Control)
NIST	Ulusal Teknoloji ve Standartlar Enstitüsü (ABD)
NLP	Duyu Dilsel Programlama (Neuro Linguistic Programming)
OWASP	Açık Kaynak Web Uygulama Güvenliği Projesi (The Open Web Application Security Project)
RAM	Rastgele Erişimli Bellek (Random Access Memory)
SOME	Siber Olaylara Müdahale Ekibi

Kısaltmalar**Açıklamalar****SQL**

Yapılandırılmış Sorgu Dili

T.C.

Türkiye Cumhuriyeti

TCP/IP

Transmission Control Protocol/Internet Protocol

TÜBİTAK

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

URL

Standart Kaynak Bulucu (Uniform Resource Locator)

USB

Evrensel Seri Veri Yolu (Universal Serial Bus)

VPN

Sanal Özel Ağ (Virtual Private Network)

WEB

World Wide Web

XSS

Çapraz Site Kod Çalıştırma (Cross Site Script)

1. GİRİŞ

Problemin durumu

Gelişen teknoloji ve artan erişim imkânları ile birlikte bilgisayar sistemlerine yapılan saldırıların türü değişmiş ve bu saldırılar, daha da karmaşıklâşarak günbegün artış göstermeye başlamıştır. Başlangıçta meydana gelen siber saldırılar kolayca tespit edilip önlenebilirken zamanla bu, çözümü zor bir durum haline gelmiştir. Hem fiziksel hem de sanal ortamlarda oluşan güvenlik çerçevesinde bu olumsuz duruma neden olan en önemli etken şüphesiz en zayıf halka olan insan faktörüdür. Beşeri, ekonomik ve demografik etmenlerin biri veya birden fazlası insanların bilerek veya bilmeyerek hata yapmasına, zafiyet göstermesine, kendilerini ve çevrelerini riske atmasına sebep olmaktadır.

Son yıllarda ortaya çıkan güvenlik ihlallerine bakıldığında, yanlışlıkla veya kasıtlı olarak zararlı yazılım girişi yapıp yapılmadığına bakılmaksızın; insan faktörünün güvenlik açığı açısından en büyük kaynak olduğu düşünülmektedir [1]. Donanım ve işletim sistemleri en son sürümler ile güncellenirken, açıklar yamalarla kapatılmakta ve güvenlik riskleri ortadan kaldırılmaya çalışılmaktadır. Nitekim çalışanların da bilgileri sürekli güncellenmeli ve olası yeni siber saldırılardan nasıl kaçınacağı konusunda ilgili personel bilinçlendirilmelidir [2].

Organizasyonlar, siber güvenlik sürecini mevcut durumdan daha başarılı bir şekilde yönetebilmek, olası tehlikeleri ortadan kaldıracırmak ve veri güvenliğinin sağlandığı bir ortam oluşturabilmek için sosyal mühendislik saldırıları yapıp; organizasyon yapılarını test etmektedir. Bu çalışmalar; zafiyetlerin ortaya çıkması, olası risklerin tespit edilmesi, eksikliklerin belirlenmesi ve gerekli önlemlerin alınması konusunda oldukça önemlidir.

Sosyal mühendisliğin organizasyonlarda ne gibi sıkıntıları ortaya çıkardığına dair en başarılı sosyal mühendislik deneylerinden biri ABD (Amerika Birleşik Devletleri)'de yapılmıştır. Lares isimli güvenlik danışmanlık şirketinin kurucusu olan Chris Nickerson, 4 dolara satın aldığı bir Cisco tişörtü ile hedefindeki binaya kolayca giriş yapmıştır. Resepsiyondaki görevliler onu Cisco'nun teknik elemanlarından biri olarak düşünmüşler ve şüphe duymamışlardır. Nickerson, içeriye girdikten sonra USB (Universal Serial Bus) bellek içinde getirdiği birçok zararlı yazılımı network cihazlarına kurmayı başarmıştır. Chris Nickerson'a

göre insanların ilk eğilimi sizi sorgulamak değil, güvenmektir. Burada dikkat edilmesi gereken husus, çalışanlar bir şirketin, kurumun ve kuruluşun en önemli varlığı olmanın yanı sıra aynı zamanda en büyük güvenlik riskini de oluşturabilmektedirler [3].

Şirket, kurum ve kuruluşlar sanal ortamda yaşanabilecek güvenlik ihlallerine karşı çoğu zaman birkaç yazılım ile güvenlik önlemi almaya çalışmaktadır. Bu gibi çözümler kısa vadede yarar sağlasa da güvenlik ile ilgili olası riskleri tamamen ortadan kaldıramamaktadır. Çünkü burada dikkat edilmesi gereken güvenlik ağının en zayıf halkasının insan faktörü olduğudur.

Şirket, kurum ve kuruluşlara yapılan siber saldırıların sebep olduğu maddi zararlar, saygınlık kayıpları ve hassas bilgilerin çalınması gün geçtikçe artmakta olan olumsuz durumların başındadır.

“Veri Güvenliğinde İnsan Faktörü” üzerine yaptığı çalışmada Ponemon Enstitüsü, kullanıcıların karşılaştığı 10 riskli uygulamayı şu şekilde belirlemiştir [4];

- Kişisel bilgisayarları güvensiz ağlara bağlamak,
- İhtiyaç kalmayan bilgilerin bilgisayarlardan silinmemesi,
- Parolaların başkalarıyla paylaşılması,
- Farklı sitelerde aynı kullanıcı adı ve parolaların kullanılması,
- Veri şifreleme gibi özellikleri olmayan standart USB’lerin kullanılması,
- Çalışma alanı dışındayken bilgisayarları kontrolsüz bırakmak,
- Gizli veri içeren USB’lerin kaybedilmesi ve derhal kuruma haber verilmemesi,
- Gizli ekranlar kullanmadan yolculuk esnasında dizüstü bilgisayar kullanmak,
- İhtiyaç olmayan hassas bilgilerin yolculuk esnasında bilgisayarda bulundurmak ve
- Kişisel mobil cihazların kurum ağında kullanılmasıdır.

Araştırmanın amacı

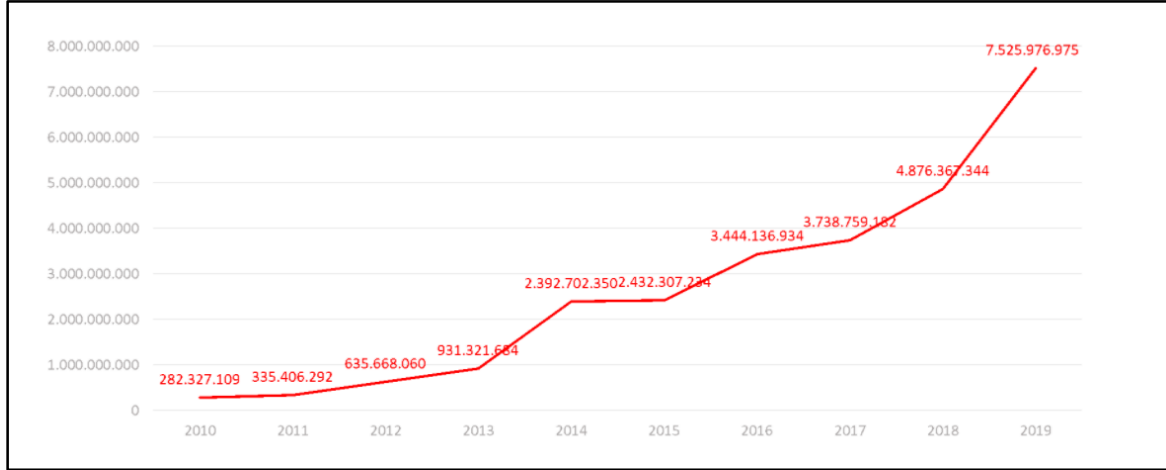
Bilgi toplumuna dönüşüm sürecinde, bilgi ve iletişim teknolojilerinin daha büyük kitleler tarafından etkin, kaliteli ve uygun maliyetle kullanılmasının yanı sıra, söz konusu teknolojilere yönelik bilişim sistemlerinin kullanımında siber güvenliğin sağlanması da son derece önemlidir [5]. Kamu kurumlarının da siber güvenliği sağlamak ve hassas verileri daha

iyi korumak için çeşitli güvenlik önlemlerini aldığı kabul edilmektedir. Ancak zayıf halkanın insan faktörü olduğu yerlerde bu önlemlerin yeterli olmadığı sık sık gündeme gelmektedir. Böyle değerlendirildiğinde; şirket, kurum ve kuruluşların güvenlik açıklıkları iki şekilde ortaya çıkar. Birincisi savunma sistemlerinin güvenlik zafiyetine neden olabilecek şekilde eksik ya da yanlış yapılandırılmasıdır. Bu durum beraberinde organizasyonların farklı teknik ve yöntemlerle sömürülmesini getirir.

İkincisi ise doğrudan zayıf halka olan kişileri hedef alan ve kişilerin bilinçsiz olması, yeterli farkındalık düzeyine sahip olmaması ya da zayıf noktalarının hedef alınmasından kaynaklı sosyal mühendislik saldırıları ile organizasyonları sömürmektir. Birinci neden çeşitli güvenlik önlemi elemanları ile engellenebilirken, ikinci neden bireyin iradesine bağlı olduğu için çoğu zaman engellenememektedir. Bu noktada organizasyonlar farkındalık eğitimlerine yönelerek duruma çözüm aramaktadır. Eğitimin bu kapsamda önemi çeşitli güvenlik strateji planlarında vurgulanmıştır [5,6]. Siber tehditleri önlemek, sosyal mühendislik saldırılarına karşı daha bilinçli ve duyarlı olmak, hassas veriyi erişmemesi gereken kişi veya yapılardan korumak, olası bir saldırıyı tamamen engellemenin veya en azından etkisini azaltabilmenin en etkili yollarından birinin eğitim olduğuna önceki başlıklarda da değinilmektedir. Gerek kişisel olarak kendimizi gerekse kurumsal olarak çalışan profilini siber güvenlik konusunda eğitmek ve güncel bilgilerle donatmak artık kaçınılmaz hale gelmiştir. Bu duruma istinaden kurumlardaki ve kişisel kullanımdaki bilgisayarlar en son teknoloji ve güvenlik yazılımları ile donatılmalıdır [7].

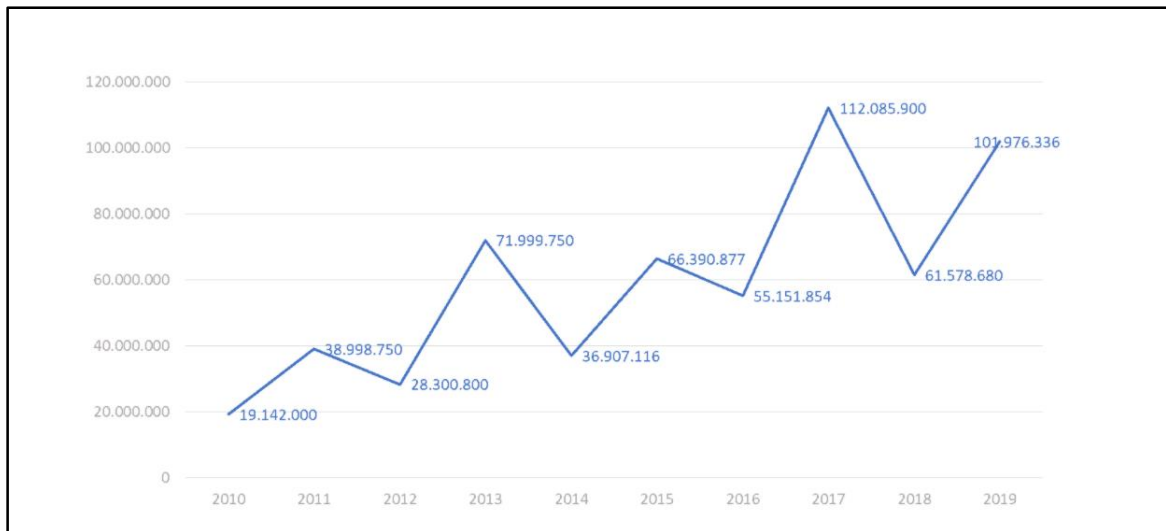
Pek çok kurum yılın belirli zamanları bütçelerinden pay ayırarak personelini siber güvenlik, siber saldırılar, sosyal mühendislik vb. konularda eğitimlere göndermekte ya da online (çevrimiçi) eğitimlere katılmaya sevk etmektedir. Bu süre zarfında personelinden iş verimliliği konusunda da taviz vermeyi de çoğu kurum göze almaktadır. Ancak zaman içerisinde eğitimlerinde tek başına yeterli olmadığı personelin büyük çoğunluğunun sosyal mühendislik saldırı ağına düştüğü gözlemlenmiştir. Gerek yıllık siber güvenlik raporları, gerek kurum yöneticileri, gerekse alanında uzmanlaşmış siber güvenlik firmaları zayıf halka olan insan faktörünün zafiyetinin önemli ölçüde devam ettiğini belirtmektedir. Her geçen gün artan ve çeşitlenen siber saldırılar karşısında ülkemizdeki kişi ve kurumların siber saldırılardan olumsuz etkilendiği güvenlik raporlarında ortaya çıkmaktadır. Bu raporlardan konu ile ilgili çıkarım yapıldığında ise; ülkemizdeki siber savunmanın yetersiz olduğu ve kişilerinde siber saldırılar karşısında yeteri kadar bilinçli olmadığı açıkça söylenebilir [8].

Beklenen sonucun elde edilmemesi kurumları elbette yeni arayışlara sokmuştur. Kamu kurumlarının kısıtlı bütçesi ve imkânları göz önüne alınarak hareket edildiğinde mevcuttaki farkındalık eğitimlerinin iyileştirilmesi fikri daha uygun gözükmektedir.



Şekil 1.1. Dünya’da siber güvenlik yatırımları (Dolar)

Bahse konu durum Şekil 1.1 ile daha net ifade edilecek olursa; Crunchbase verisine göre, dünyada siber güvenlik alanında girişimcilere yapılan yatırım miktarı, dünya genelinde 10 yılda üssel olarak artış göstermiş, 2017 yılından itibaren ise bu yatırım artışları ciddi sıçrama gerçekleştirmiştir [9, 10].



Şekil 1.2. Türkiye’de siber güvenlik yatırımları (Dolar)

Türkiye özelinde ise siber güvenlik alanında girişimcilere yapılan yatırım miktarı, 10 yılda kendi içinde artış ve azalışlar yaşamış olmakla birlikte, hacim olarak dünya ölçeği ile

kıyaslandığında az gelişmiş olduğu Şekil 1.2’de görülmektedir [9,10]. Örneğin İngiltere’de siber güvenlik verilerine bakıldığında, 2018 sonu itibarıyla siber güvenlik endüstrisinin net değerinin 5 milyar dolar, Birleşik Krallık genelinde devletin siber güvenliğe yaptığı yatırımın ise 2,5 milyar dolar olduğu belirtilmekteyken, TÜBİSAD verilerine göre, Türkiye’nin 2018 siber güvenlik pazar büyüklüğü 1,5 milyar dolar civarındadır [11]. Bu kıyas göstermektedir ki Türkiye yatırımlar konusunda geri kalmıştır.

Kişilerin, organizasyonların ve devlet desteğinin mevcut şartları göz önüne alındığında, var olan farkındalık eğitimlerinin bünyesine destekleyici yapılar eklenmesi gerekliliği ortaya çıkmıştır. Bu tezde de kullanıcılara siber güvenlik konusunda gerekli eğitimler ile beraber, farkındalığı ve bilinci artıracak bir filtre model önerisi verildiğinde siber saldırıların kamusal alanda en etkili ve yoğun türü olan sosyal mühendislik saldırılarına karşı verdikleri tepkiler gözlemlenecek ve sonuçlar incelenecektir. Uygulama senaryoları bundan hareketle hazırlanacak ve kurumsal alanda çalışanlar üzerinde uygulanacaktır. İlk uygulama sadece eğitime tabi tutulan personele uygulanmıştır. Her ne kadar personele eğitim verilse de sosyal mühendislik saldırı tuzağına düştüğü gözlemlenmiştir. Bu veriler problemin doğruluğunu destekleyecek niteliktedir. İlk çalışmada amaç gerekli eğitimler verilse dahi kullanıcıların siber güvenlik konusunda bilinçli hale gelip olası bir sosyal mühendislik saldırısını tespit edebilme düzeyine ulaşamadıklarını tespit etmektedir.

Nitekim kullanıcılara gerekli eğitim imkânları sunulsa dahi istenilen bilinç ve farkındalık seviyesine ulaşamadıkları Uygulama-1 sonucunda görülmektedir. Temel problem, zayıf halka olan insan hala siber güvenlik konusunda yetersiz ve sosyal mühendislik saldırılarına karşı savunmasızdır. Varılan nokta ise eğitimin tek başına sosyal mühendisliğin önüne geçmede, insan zafiyetini önlemede beklenen başarıyı sağlayamadığıdır.

Tüm bu çıkarımlar kamu kurumlarında çalışanları siber güvenlik ve sosyal mühendislik saldırılarına karşı istenen bilinç ve farkındalık düzeyine getirmeye yardımcı olacak bir yapının tasarlanmasını ortaya koymaktadır. Geliştirilecek modelin de bu ihtiyaca karşılık vermesi değerlendirilmektedir.

Araştırmanın önemi

Son zamanlarda siber saldırıların önüne geçebilmek için farklı metotlar denenmeye başlanmış olmakla beraber bunların içinde doğrudan insan unsurunu özne alanların başında farkındalık eğitimleri gelmektedir. Bu eğitimler çoğunlukla çevrimiçi (online) olarak karşı tarafa verildiği gibi yüz yüze seminerler, konferanslar, dersler vb. şekilde de verilebilmektedir. Eğitimler başta kullanıcılarda farkındalık oluştursa da bunların üzerinden zaman geçtikçe hatırlanabilirliğini ve uygulanabilirliğini kaybettiği görülmüştür. Buna en iyi kanıtlardan biri de sosyal mühendislik saldırısı üzerine yapılan Uygulama-1'in sonuçlarıdır. Kullanıcılar çevrimiçi (online) olarak erişebilecekleri, detaylı olarak siber güvenlik konularının verildiği farkındalık eğitimlerine aylarca tabi tutulmuştur. Eğitim videolarına paralel olarak hazırlanan sosyal mühendislik saldırısına uğrayan kullanıcıların istenen başarı oranını gösteremedikleri, insan faktörünün zafiyet oluşturmaya devam ettiği gözlemlenmiştir. Tezin çıkış noktası olan bu konu, elde edilen bulgularla pekişmiş ve eğitimlerin yanında destekleyici unsur olabilecek bir model tasarlanması gerekliliğini ortaya koymuştur. Filtre model olarak adlandırılan bu modelde, kullanıcılara kolay kavrayıp uygulayabilecekleri bir yapı oluşturulup uzun metinler yerine maddeler halinde önemli noktalar vurgulanacak ve siber suçlara karşı mücadele ederken sadece kendilerinin değil çalıştıkları kurumların da onlarla beraber hareket etmeleri gerektiği, bu mücadelenin bir ekip işi olduğu anlatılmaya çalışılacaktır. Nitekim bir bütün olarak hareket etmeyen yapılar tek bir kişinin hatasıyla bile gerek maddi gerekse itibari olarak büyük zararlara uğrayabilmektedir.

Varsayımlar / Sınırlılıklar

Şirket, kurum ve kuruluşlar öncelikle kendileri almaları gereken önlemleri eksiksiz alıp uygulamalı, ardından çalışanlarından bunu beklemelidir. Kurumsal ve kullanıcı bazlı tedbirler yerinde ve zamanında alındığında olası bir siber saldırının ya da sosyal mühendislik atağının önüne geçmek zor olmayacaktır. Filtre model de yapısı ve uygulanışı ile bunu başarmayı hedeflemiştir.

Modelin akılda kolay kalır yapısı ve uygulanışı sayesinde kurumlar, çalışanlarına yönelik gerçekleştirdiği farkındalık eğitimleri sırasında veya akabinde filtre modeli kullanıcılarına sunarak bilgilerini pekiştirebilir. Bunun yanında modelin dayandığı ilkeler, kurumlarda;

kullanıcıların erişim sağladıkları cihazlarında açılır kapanır (pop-up) pencereler halinde, broşür, afiş veya reklam panosu gibi çeşitli şekillerde destekleyici unsur olarak kullanılabilir. Modelin içeriğini oluşturan maddeler ve konular kısa bilgi notları şeklinde, açık ve anlaşılır biçimde verildiği için kullanıcılar tarafından özümsemesinin kolay olacağı düşünülmektedir. Maliyeti az, temin edilmesi kolay, kullanıcılara kısa maddeler halinde ve görsellik sağlayacak şekilde aktarılacak ve anlaşılması kolay bir modeldir. Aynı zamanda geliştirilmeye uygundur.

Çalışma sürecinde belirlenen araştırma soruları aşağıda verilmiştir. Söz konusu soruların yanıtları göz önünde bulundurularak modelin test aşaması değerlendirilecektir.

- 1) Ödül ve teşvik amacıyla eğitim sonunda kullanıcılara katılım sertifikası veriliyor mu [12]?
- 2) Siber saldırı sorununun sadece teknoloji sorunu olmadığı bilinci var mı [12]?
- 3) Kurumun tüm çalışanları bilgi güvenliğinin bir parçası mı [12]?
- 4) Periyodik olarak düzenlenen eğitimler var mı [12]?
- 5) Bilgi güvenliği ve siber güvenlik prosedürleri düzgün uygulanıyor mu [12]?
- 6) Kullanıcı bilinçlendirme ve farkındalık eğitimlerinde verilen bilgi, kullanıcılar tarafından yeterli derecede öğrenilmiş mi [12]?
- 7) Kurum yönetimi, siber saldırıya reaksiyon göstermeye hazırlandı mı [13]?



2. TEMEL BİLGİLER

Bu çalışmada geçen kavramlar,

Atak: Hedef seçilen şahıs, şirket, kurum gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırı amaçlı hareketlerdir.

Bilgi Güvenliği: Bilginin güvenliğini, bütünlüğünü sağlayan, izinsiz veya yetkisiz bir biçimde erişilebilir ve ulaşılabilir olmasının önüne geçen, hassas bilginin değiştirilme, ifşa edilme, ortadan kaldırılma, el değiştirme ve hasar verilmesini önlemek olarak tanımlanır.

Bilişim Sistemleri: Verileri toplamak, sınıflandırmak, özetlemek ve kullanıcıların hizmetine sunmak için kurulan ve bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir.

Hackleme: Bilgisayar, ağ ve sistemlere yetkisiz erişim veya kullanımı olarak tanımlanmaktadır.

Kamu Kurumu: Kamu hizmetlerinin görülmesi amacıyla kurulmuş, tüzel kişiliği olan kurumlar, amme müesseseleri olarak tanımlanmaktadır.

Kurban: Siber saldırıya uğrayan kişi olarak kısaca ifade edilebilir.

Saldırgan (Hacker): Kısaca bilgisayar korsanı olarak tanımlanmasının yanında şahsi bilgisayarlara veya çeşitli kurum ve kuruluşlara ait bilgisayarlara ve ağlara izinsiz olarak giriş yapan kişi olarak da ifade edilir.

Siber Uzak: Bilgisayar ağları ve bu ağlarla erişilebilen bütün veri kaynaklarını içeren ortam veya birbirine bağlı olan cihazlar teknolojisidir.

Siber Zorbalık: Bir birey ya da grup tarafından iletişim teknolojilerini kullanarak başka bir birey ya da gruba zarar vermek için tasarlanan kasıtlı ve düşmanca davranış içeren zorbalık türüdür.

Siber Tehdit: Bilgi güvenliği ve kritik altyapıların korunmasına yönelik güvenlik riski oluşturabilecek durum veya olaylardır.

Siber Zafiyet: Bir sistem veya uygulamayı siber saldırılara açık hale getiren hatalar olarak tanımlanır.

Son Kullanıcı: Bir yazılımın veya donanımın en son halini kullanan veya kullanmayı amaçlayan kişidir.

Toplum Mühendisliği: İnsanlara bazı eylemleri yaptırmak veya güvenli bilgileri ele geçirmek için kullanılan tekniklerin bütünüdür.

2.1. Siber Güvenlik Kavramı

Siber saldırıların bireyleri, kurumları ve ülkeleri hedef aldığı son yıllarda siber güvenlik kavramı, ciddi gelişmelerin yaşandığı ve üzerinde kapsamlı çalışmalar yapıldığı bir konu haline gelmiştir.

Siyasi ve finansal kazanç arayan dış aktörler ile ele geçirme (hackleme) yetenekleri olan kişiler vasıtasıyla kişi, kurum ve kuruluşlar siber güvenlik tehditleri ile karşı karşıya kalmaktadır. Tehditler, ayrıca çalışanlar gibi iç kaynaklardan ya da sisteme yasadışı erişim ile giriş yapanlarca da oluşabilmektedir [14, 15]. Siber saldırganlar artık kuruluşlarda var olan güvenlik duvarına atakta bulunmak yerine, kuruluşun network ağı katmanlarındaki güvenlik açıklıklarını bulup buradan saldırıyı tercih etmektedir.

Siber saldırıların meydana getirdiği etki ve tahribattan dolayı, bu saldırıların tespiti önemli bir konu olmuş ve bu yönde akademik çalışmalara da büyük ölçekte ağırlık verilmiştir. Siber ortamlarda gerçekleştirilen saldırılardaki amaç, genellikle karşı tarafa farklı mahiyetlerde zarar vermektir. Siber ortamlara yapılan zararlı müdahaleler, ekonomik zarar verebileceği gibi istihbarı bilgilerin istenmeyen taraflarca ele geçirilmesi ile siyasi, sosyal ve kişisel zararlara da neden olmaktadır. Gerçekleşen saldırılarda bilişim teknolojileri, “aracı” olarak kullanılabilir. Artan ve çeşitlenen bilişim sistemlerinin istenmeyen bu saldırılardan korunması, saldırıların ve siber güvenlik olaylarının tespit edilmesi ve tespitlere karşı tepki mekanizmalarının kurulması gerekmektedir. Siber güvenlik konusunda gerçekleşen

saldırılar gerekli önlemler alındığında en aza indirilebilmekte veya tamamen önlenebilmektedir.

Siber Güvenlik, ”siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür” [16] şeklinde tanımlanabilir.

Siber güvenlik kavramının bir diğer tanımı ise temel malzemesi olan bilgi üzerinden yapılmaktadır. Buradan hareketle, siber dünyanın güvenli olabilmesi için ana kaynak bilginin; gizliliği (confidentiality), bütünlüğü (intergrity) ve erişebilirliği (availability) sağlaması gerekmektedir [17] .



Şekil 2.1. Bilgi güvenliği üçlüsü (CIA Triad) [18]

Şekil 2.1’de bilgi güvenliği için gereken bu hedefler somutlaştırılmıştır.

Gizlilik, sistem verilerine sadece yetkili kişi veya sistemlerce erişilmesini; yetkisiz kişi veya sistemlerce verilerin ifşa edilmemesi olarak kabul edilmektedir. Burada erişimden kast edilen; yazılı bir bilginin okunması, sistem bilgisinin görüntülenmesi, çıktı olarak bilginin alınması hatta hassas bilgilerin varlığından sadece yetkili kişilerin haberdar olmasıdır.

Bütünlük, sistemde depolanan verilerin bozulmadan, değiştirilmeden, kısmen veya tamamen silinmeden saklanmasıdır. Veriyi gerektiği gibi korumak ve tutmak nihai amaçtır.

Erişilebilirlik, yetkili kişilerin bilgiye her an ulaşabilir ve kullanabilir olmasının gerekliliğini anlatmaktadır.

Bu üç kavramı ele alırken aralarındaki ters ilişki göz önünde bulundurulmalıdır. Nitekim verinin bütünlüğünü veya gizliliğini artırmaya yönelik atılacak bir adım, erişilebilirliği negatif yönde etkilemekte; tam tersi erişilebilirliği artırmaya yönelik bir adım da bütünlük veya gizliliği tehlikeye atabilmektedir. Öyle ki bilgi güvenliği üçlüsü, siber ortamlardaki bilgi güvenliğini sağlayacak aktörler olsa da optimal bir denge kurulması, aralarındaki ters ilişkiden dolayı zordur. Nihayetinde “bilgi” en temel yapıtaşdır. Siber güvenliğin amacı da bilgi ve bilgi sistemlerinin korunmasıdır.

Siber güvenlik kontrollerinin içeriği kısaca aşağıda verilmiştir [19].

- Çalışanların güvenliği,
- Fiziksel ve çevresel güvenlik,
- Hesapların ve şifrelerin yönetimi,
- Hassas verilerin gizliliği,
- İşletme sürekliliği yönetimi kullanılması,
- Güvenlik konusunda bilinçlilik ve eğitim,
- Vaka yönetimi,
- Erişim kontrolleri,
- Varlık yönetimi,
- Değişim yönetimi,
- Uygunluk,
- Gizlilik ilkeleri,
- Sistemler ve verilerin korunması,
- Sigorta işlemleridir.

Şirket, kurum ve kuruluşlar her yıl siber güvenlik denetimlerini planlamalı, kendi güvenlik politikalarını belirleyip alanında uzman kişilerle bu süreci yönetmelidirler.

2.1.1. Siber güvenlik zafiyeti

Siber güvenlik zafiyeti ya da açığı; siber saldırganlar tarafından güvenliğin aşılmamasına neden olan ve böylece bir sistem, ağ veya uygulamayı siber saldırılara karşı açık ve savunmasız hale getiren hatalar veya kusurlar olarak ifade edilmektedir. The National Institute of Standards and Technology (NIST) siber güvenlik açığını; kötü niyetli kişi veya grupların politikaları bozmak ve zarar vermek amacıyla istismar edebileceği yazılım zayıflığı olarak tanımlar [20]. Pek çok farklı alanda yaptığı araştırmalar ile bu alanların liderlerine bilgi, tavsiye ve araçlar sağlayan küresel araştırma firması Gartner, siber güvenlik açığını teknoloji, süreç veya yönetimde Bilgi Teknolojileri (BT) güvenliğini tehlikeye atmak için kullanılabilecek zayıflık olarak tanımlar [21].

Bugünün artan veri miktarı, sistemlerin çeşitliliği ve yazılımların karmaşıklığı göz önüne alındığında siber güvenlik zafiyetleri sürekli olarak artmaktadır ve fark edilmesi zor zafiyetlere sebep olmaktadır. Bunlardan faydalanan bir siber saldırgan hedefindeki sisteme erişerek buradaki önceliklerde değişiklikler yapabilir, yetkili bir kullanıcının bilgisayar ağına erişimini engelleyebilir, gizli verilerin yayılmasına sebep olabilir, kötü amaçlı yazılımı yükleyebilir, sistemin kontrolünü tamamen ele geçirebilir veya hassas verileri tamamen yok edebilir. Siber güvenlik zafiyetleri sadece sistem üzerinde değil aynı zamanda sistemin güvenlik bileşenleri, kontrolleri ve işleyişinde de bulunabilmektedir. Şirket, kurum ve kuruluşlar için tüm bu zafiyetler elbette zaman, para ve güven kaybı anlamına gelmektedir. Devlet kurumları ve finans sektörü ise zafiyet çokluğu konusunda başı çekmektedir. Zafiyetler sonucu zarar gören yapılar ülkeden ülkeye farklılık gösterebilir, çoğunlukla savunma, finans, enerji, ulaşım, elektronik haberleşme, sağlık, eğitim, nükleer tesisler ve temel kamu hizmetlerine ait altyapılardır ve tüm bu unsurlar kritik altyapı olarak ifade edilmektedir [22]. Türkiye’de yer alan kritik altyapı sektörleri;

1. Ulaştırma
2. Elektronik ve Haberleşme
3. Bankacılık ve Finans
4. Enerji
5. Su yönetimi
6. Kritik Kamu Hizmetleri
7. Kritik Üretim Ticari Servisleri

8. Sağlık
9. Tarım ve Gıda
10. K lt r ve Turizm

2016-2019 Ulusal Siber G venlik Stratejisi ve 2013-2014 Eylem Planı'na g re hazırlanmış kritik altyapılar yukarıda g r ld ğ   zere sırasıyla verilmiştir [23,6].

Zafiyet y netimi; Őirket, kurum ve kuruluŐların sahip oldukları varlıkları etkileyecek a ıklıkların d zenli olarak takibi ve kontrol  iŐlemidir. Zafiyet y netiminde en  nemli aŐama tarama aŐamasıdır. G venlik a ıėı taramasında hassas verilere ve sistemlere eriŐmek i in aėdaki saldırganların yararlanabileceėi yanlış yapılandırılmış veya hatalı aygıtları ve sistemleri tanımlamak esastır. Haftalık, aylık veya yıllık olarak yapılacak taramalar sızma testi deėildir. Daha  ok mevcut ve  ıkması muhtemel zafiyetlerin tespit edilmesine olanak saėlayan bir adımdır. Sistemlerin yapısal ya da iŐletimsel a ıklıkları bulunabilir. G ncellemelerin zamanında yapılıp yapılmaması, cihazların yapılandırılma ayarlarında ki hatalar, Őifre kırma ara ları ile sistemdeki zayıf Őifrelerin ele ge irilmesi taramalarda ortaya  ıkabilecek zafiyet ya da a ıklıklara  rnek olarak verilebilir. Tespit edilen zafiyetler, saldırganın sisteme giriŐ yapması durumunda kullanabileceėi tehditleri belirleyerek bu tehditlerin sistem  zerindeki etkisi ve ger ekleŐme ihtimallerinin  nceden deėerlendirilmesini saėlayacaktır. Bilgi g venliėinin saėlanması en  nemli fakt r insan ve bilin  d zeyi olduėundan bu zafiyetlerin incelenmesi olduk a faydalı olacaktır.   nk   eŐitli sosyal m hendislik giriŐimleriyle insani zafiyetlerden faydalanıp kullanıcı adı ve Őifreler ile gizli kurumsal bilgiler elde edilmeye  alıŐılmaktadır. Bu zafiyet taraması sayesinde kurumsal bilgi g venliėi hakkında  alıŐanlar  zerinde ortalama bilin  d zeyi ortaya  ıkarılabilecektir. Temele bakıldıėında y netilmesi gereken en  nemli zafiyet bileŐeninin insan olduėu g r lmektedir.   nk  insanları kandırılması ile yapılan sosyal m hendislik saldırılarının  oėu, baŐarıyla sonu lanmaktadır [25].  zetlemek gerekirse;

G venlik zaafıları sonucunda Őirket, kurum ve kuruluŐlar zararlara uėrayarak, beklenmedik kayıplar yaŐayabilmektedirler. Mukhopadhyay ve arkadaşlarının yaptıkları bir  alıŐmada g venlik a ıklarının nasıl ve ne Őekilde olduėu ve Őirket, kurum ve kuruluŐlara zararlarının hangi aŐamalar sonucu ortaya  ıktıėı, Őekil 2.2'de genel haliyle g sterilmiştir [26].

kullanıcılarının etkisiyle gerçekleşmektedir. Saldırganlar bu tür zafiyetleri ya da açıklıkları fark ettiğinde bunlardan yararlanmak isteyecektir.



Şekil 2.3. Siber güvenlik zafiyetleri [28]

Şekil 2.3'te belirtilen siber güvenlik zafiyetleri ya da açıklıkları, detaylandırılarak alt başlıklar halinde verilmiştir.

Yazılım güvenlik zafiyetleri

Yazılım şirketleri veya üreticiler, yazılım geliştirilmesi safhasında güvenlik açığına neden olabilecekleri için olası güvenlik zafiyetlerinin de temel sorumlusu olarak kabul edilmektedir. Çoğu yazılım geliştirici, projeyi bir an önce bitirmek için alması gereken önlemleri ihlal etmektedir. Ancak yazılım pazarında etkin bir konuma gelmeye başladıklarında yazılım güvenliğini önemseyip bu konuya öncelik vermeye başlamaktadırlar. Yazılımların güvenlik politikalarını sağlamasında insan faktörünün, bilinçli olmasıyla temeli oluşturduğu görülmektedir. Yazılım geliştirici olarak karşımıza çıkan insan unsuru, destek sağlamakla sorumlu olduğu ürünlerde bulunan güvenlik açıklarını herkesten önce tespit etmeli ve yamalar üretmelidir. Zira yazılım şirketleri üzerindeki kamuoyu baskısı, daha hızlı yama yapmaları konusunda onları zorlamaktadır [29].

Yazılımdan kaynaklı birçok zafiyet ya da açıklık vardır, bunların bir kısmı [30,31]

- Eksik veri şifreleme,
- Yetersiz yazılım testi,
- Denetim izi eksikliği,
- Sistem yöneticisi ya da kullanıcı kayıtlarının tutulmaması,
- Yazılım tasarım hataları,
- Bellek güvenlik ihlalleri,
- Arabellek taşması,
- SQL (Structured Query Language), e-posta ve HTTP (Hyper-Text Transfer Protocol) başlık enjeksiyonu hataları,
- Yaygın kullanıcı ağına sahip yazılımlar,
- Eksik yetkilendirme,
- Güvenli olmayan sitelere URL (Uniform Resource Loader) yönlendirmesi,
- Hata kodları,
- Zamanlama saldırıları,
- Uygulama yazılımlarına zaman damgasının doğru uygulanmaması,
- Karmaşık kullanıcı ara yüzü,
- FTP (File Transfer Protocol) sıçrama saldırısı,
- Önceden virüs bulaşmış yazılımlar,
- Zayıf şifreler,
- Bütünlük kontrolü olmayan kodların indirilmesi,
- Doğru sonuç vermeyen algoritmaların kullanımı,
- Doğru silme yöntemi yapılmadan depolama ortamının elden çıkarılması ya da yeniden kullanıma alınması,
- Tehlikeli dosya türlerinin sınırsız yüklenmesi,
- Kritik işlevler için eksik kimlik doğrulama,
- Oturumun kapalı (log out) olmaması ya da süresinin uzun olması,
- Güvenlik kararında güvenli olmayan girdilere güvenme şeklinde verilebilir.

Donanım güvenlik zafiyetleri

Donanım güvenlik zayıflıkları genellikle donanım tasarım kusurları şeklinde adlandırılır. Donanım güvenlik zafiyetleri ya da açıklıkları, cihaz modellerine özeldir ve rastgele saldırılarla ele geçirilip sömürülemezler. Kapsamlı bir saldırı ile donanımsal zafiyetler sömürülse de kullanıcıdan kaynaklı basit bir hata da saldırıya istediği fırsatı verebilmektedir. Birçok etmen, donanım zafiyetine ya da açıklığına neden olabilmektedir. Bunlar [31];

- Bilgisayar donanımlarının nem, toz, kir ve doğal afetlere karşı duyarlılığı,
- Elektromanyetik radyasyona karşı duyarlılığı,
- Sıcaklık farklılıklarına karşı duyarlılığı,
- Yetersiz bakım ve hatalı yapılandırma (konfigürasyon) yapılması,
- Korumasız arşivleme ve depolama ortamlarına sahip olması,
- Etkin yapılandırma değişikliği denetiminin olmaması,
- Yazılımsal olarak zayıf olan ürünlerin kullanılması,
- Kullanılmayan araçların imha sürecinin dikkatsiz ve yetersiz olması,
- Kontrolsüz fotokopi cihazlarının varlığı şeklinde verilip daha da artırılabilir.

Ağ güvenlik zafiyetleri

Ağ güvenlik zafiyetleri ya da açıklıkları;

- Kimlik doğrulama mekanizmalarının olmaması,
- Korumasız iletişim hatları,
- Korumasız parola tabloları,
- Yetersiz parola yönetimi,
- Ağdaki hareketlerin izlenmemesi,
- Gereksiz kullanıcıların erişim yetkilerinin etkinliği,
- Ağ yönetim raporlarının oluşturulmaması,
- Değişiklik yönetimi olmaması,
- Kontrolsüz yazılım indirme,
- Giriş kontrollerinin güvenliğinin etkin yapılmaması,

- Parola aktarımında yetersiz önlem alınması ya da hiç alınmaması,
- Güvenilmeyen ağ mimarisi,
- Güvenli olmayan Wi-Fi erişim noktalarının varlığı gibi sebepleri içermektedir [31].

İnsan güvenlik zafiyetleri

Siber güvenlik mimarisinin birçoğunda en zayıf halka, insan unsurudur. Kullanıcı hataları; hassas verilerin kolayca açığa çıkmasına, siber saldırganlar için sömürülebilir erişim noktalarının oluşmasına veya sistemlerin tamamen ele geçirilerek bozulmasına yol açabilir. İnsanlardan dolayı sistemlerde meydana gelen güvenlik zafiyet ya da açıklıkları;

- Personel yetersizliği,
- İşe alma süresinde yetersiz işlemler,
- Yetersiz güvenlik eğitimleri,
- Yanlış yazılım ya da donanım kullanımı,
- İzleme mekanizmalarının eksikliği,
- Kontrolsüz dış kaynak (temizlik, destek elemanı) kullanımı,
- Varlıkların kabul edilebilir kullanımı kurallarının yazılı olmaması gibi örneklendirilebilir [32, 33].

Bu tezde de sıklıkla üzerinde durulacak kavramlardan biri olan insan faktörü, ne kadar önlem alınsa da bilerek veya bilmeyerek en büyük siber güvenlik zafiyet unsuru olmaktadır.

Organizasyon güvenlik zafiyetleri

Güvenlik zafiyeti ya da açıklığının bir kısmı da belirli işlem denetimleri veya bunların eksikliğine bağlı olarak organizasyondan kaynaklı ortaya çıkabilmektedir.

- Hata kayıtlarının eksikliği,
- Yetersiz bakım hizmeti alımı,
- Bilgi güvenliği yönetim sistemi kontrolü için prosedür eksikliği,
- E-posta yönetimi denetimi eksikliği,
- Yazılımı gerçek ortama aktarmadan önceki güvenlik önlemlerinin eksikliği,

- Mobil cihaz politikasına uyulmaması,
- Güvenlik veya olay müdahale planı eksikliği gibi konular organizasyon güvenlik zafiyetleri ya da açıklıklarına örnek teşkil etmektedir [32, 33].

2.2. Siber Saldırıları

Güvenlik zafiyetlerinin şirket, kurum ve kuruluşlar üzerinde olumsuz etkiye sahip olabileceği göz önüne alındığında siber güvenlik kavramı günümüzün en büyük risklerinden biri haline gelmiştir. Siber suçluların bu süreçte karmaşık bir yapıya bürünmesinden ve siber saldırıların her geçen gün yaygınlaşmasından dolayı meydana gelen saldırının ekonomik, yönetsel ve itibarsal zararı; üzerinde durulması gereken çok önemli bir risktir. İşletmeler herhangi bir kayba uğramamak için, olabilecek tüm siber saldırı ve siber tehdit çeşitlerini detaylı olarak analiz etmeli ve gerekli güvenlik önlemlerini almalıdır.

Siber saldırı, " hedef seçilen şahıs, şirket, kurum, örgüt gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır" [16].

Gerçekleşen saldırılar ile sistemlerin güvenliğine büyük oranda zararlar verilebilir. Saldırıları önceden tespit edebilmek, ortaya çıkan zararları en aza indirebilmek veya tamamen önleyebilmek için önemlidir. Siber saldırıları normal saldırılardan ayıran en önemli farklardan biri sıfırinci gün açıklığıdır. Yazılımı üretenler tarafından fark edilmeyen ve üreticiler var olan açıklığın farkına varıp açıklığı kapatana kadar bilgisayar korsanları tarafından sömürülen açıklıklar sıfırinci gün (zero day) açıklığı olarak tanımlanır [34]. Saldırı tespit sistemleri öngörülemeyen zararlı network hareketlerini tespit edemeyebilir. Yapılan araştırmalara göre klasik güvenlik teknikleri daha çok güvenlik duvarları, anti-virüsler, anti-casus yazılımları ve saldırı tespit sistemlerini içeren savunmaya dayalı çalışmalardır. Var olan teknolojilerin gelişmiş hedefli bir siber saldırıyı durduramayacağı ve daha kapsamlı bir çözümün bulunup kullanılması gerektiği de araştırmalarda değinilen önemli noktalardan [24]. Bu kısmı biraz açmak gerekirse güvenlik duvarı (Secure Shell-SSH) servisine yönelik engelleme kuralı girildiğinde güvenlik duvarından SSH servisine yönelik hiçbir olası trafiğin geçmeyeceği iddia edilmektedir ancak gelişmiş siber saldırıları engellemede böyle bir kesinlik söz konusu değildir. Bu duruma istinaden aktif siber savunma, siber saldırı öncesinde ve saldırı sırasında saldırganı engellemeye yönelik proaktif eylemlerdir. Gelişmiş bir saldırıyı engellemek için keşif aşamasında saldırganın keşif

yapmasını yavaşlatmak ve sisteme girişini zorlaştırmak için etkili bir model olan siber ölüm zinciri kullanılabilir. Aktif savunma da siber saldırı sırasında saldırgana karşılık vermekte saldırganı yavaşlatabilir.

Siber saldırıların meydana gelir gelmez tespit edilmesi, saldırılara karşı yeterli önlem ve müdahale imkânlarının bulunması kadar önemli bir etmendir. Nitekim siber saldırıyı engelleme noktasında gerekli yöntem, araç ve kabiliyetler elde mevcut olsa bile iş işten geçtikten sonra yapılan bir müdahale pek bir anlam taşımayacaktır [35]. Aktif siber savunma teknikleri ile önceden tespiti mümkün olmayan veya saldırı sırasında dahi tespiti zor olan gelişmiş siber saldırılara karşı görüldüğü üzere çözüm üretilmeye çalışılır.

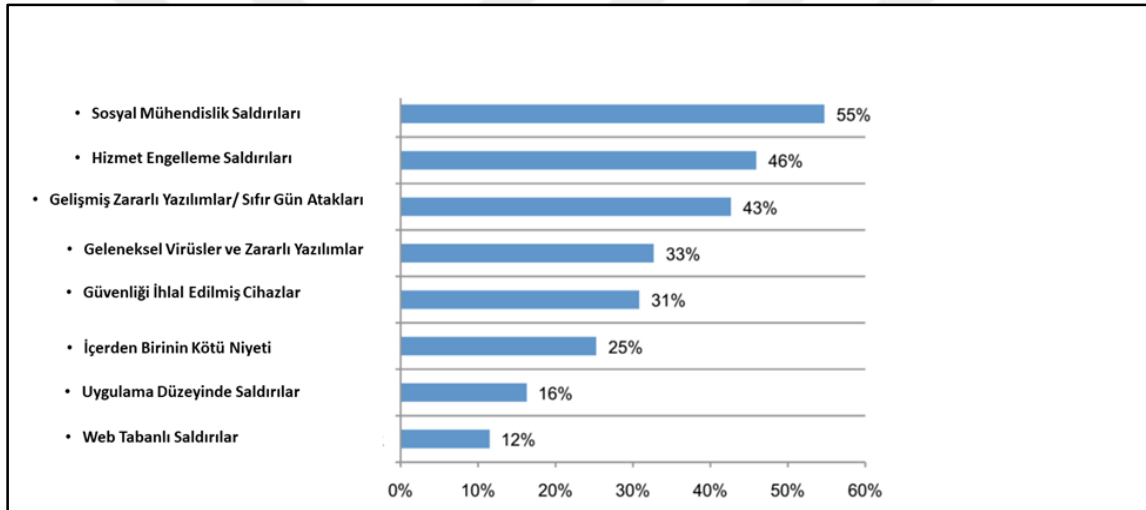
2.2.1. Siber saldırı yöntemleri

Hızla gelişmekte olan teknolojiler ve bu gelişime ayak uydurarak sürekli değişen operasyonel uygulamalar ve ihtiyaçlar, hem özel hem de kamu kuruluşlarını, birbiriyle son derece bağlı ve teknolojik yönden yakın bilgi ağlarına yönlendirmektedir. Veri yönetim sistemleri, işletim sistemleri, bilgisayar ağları ve ara yazılımlar gibi bilgi sistemleri siber tehditlere açık hale gelmiştir. Sistemlere yönelik gerçekleştirilen siber saldırılarda kullanılan bazı yöntemler şu şekildedir [36].

- Bilgi ve veri aldatmacası (Data Diddling),
- Salam tekniği (Salami Techniques),
- Süper darbe (Super Zapping),
- Eşzamansız saldırılar (Asynchronous Attacks),
- Truva atı (Cusus Yazılımlar),
- Zararlı yazılımlar (Kötücül Yazılımlar),
- Mantık bombaları (Logic Bombs),
- Oltalama (Phishing),
- Tarama (Scanning),
- Bukalemun (Chamelon),
- İstem dışı alınan elektronik postalar (Spam),
- Çöpe dalma (Scavenging),
- Gizli kapılar (Trap Doors),

- Sırtlama (Piggybacking),
- Yerine geçme (Macquerading),
- Sistem güvenliğinin kırılıp içeri sızılması (Hacking),
- Hukuka aykırı içerik sunulması,
- Web sayfası hırsızlığı ve yönlendirme,
- Sosyal mühendisliktir.

Bu saldırı yöntemlerini gelişen, değişen ve çeşitlenen teknoloji ve imkânlarla artırmak elbette ki mümkündür. Aşağıdaki Şekil 2.4'te bu saldırı yöntemlerini kullanan en yüksek oranlı saldırı türleri genel hatları ile verilmiştir.



Şekil 2.4. En yüksek saldırı türü oranları [37]

Şekil 2.4'te verilen saldırı türlerini artırmak mümkün olmakla beraber, bahsedilen saldırı yöntemlerinin birini veya birkaçını kullanarak hassas verileri ele geçiren bilindik saldırılardır. Bu saldırı türlerinden birkaçı detaylandırılarak bir sonraki kısımda anlatılmaktadır.

Zararlı yazılımlarla saldırılar

Zararlı yazılımlar; bilgisayarımızı ve kişisel güvenliğimizi tehdit eden siber güvenliğin en temel silahlarından biridir. Bilgisayar ve türevleri gibi cihazların çalışma performansını etkileyebileceği gibi geri dönüşü olmayan zararlarda verebilirler. En sık rastlanan zararlı

yazılımlar; Solucan (Worm), Casus Yazılımlar (Spyware), Truva Atı (Trojan), Virüsler ve Botnetler olarak sıralayabiliriz.

Botnet benzeri yazılımlar genellikle sistemlere Truva atı olarak adlandırılan, normalde kullanıcı tarafından bilinen ve istenen işlevinin yanında bilinmeyen ve kullanıcının istemeyeceği işlevleri de olan yazılımlar vasıtasıyla yüklenmektedir. Bu yazılımlar bir kere sisteme yüklendikten ve erişim sağladıktan sonra sisteme her defasında daha kolay giriş sağlamak üzere arka kapı açabilmekte veya kayıtlı bilgileri istedikleri her yere aktarabilmektedir. Botnet gibi zararlı yazılımlar örneğin e-posta ekinde gönderilen bir PDF uzantılı dosyada yer alan zararlı bir kod veya e-posta mesajı içeriğinde yer alan bağlantılara tıklayarak açılan internet sayfaları vasıtasıyla da sistemlere bulaşabilmektedir. Bu türden yazılımlar genellikle hedef sistemlere sızarak veri aktarımı yapmak ve istihbarat amaçlı bilgi toplamak üzere programlanmıştır. Yakın zamanda İran'ın nükleer sistemlerini kontrol eden cihazlara Stuxnet zararlı yazılımının sızması alanının en dikkat çeken örneklerinden biri olmuştur [38].

Hizmet engelleme saldırıları

Bilişim sistemlerinin erişilebilirliğine yönelik düzenlenen en meşhur saldırı türlerinden biri DDoS (Distributed Denial of Service Attack) saldırısı olarak bilinen hizmeti engelleme saldırılarıdır. Özellikle son zamanlarda Türkiye'nin gündeminde olan siber saldırılar içerisinde en yoğun kullanılan DoS, bant genişliğini istila ederek sistemlerin ve sunucuların hizmet vermesini engeller. Hizmet engellemesini pek çok farklı yönden yapabileceği gibi ana hedef sunucu bilgisayarla çok sayıda gerçek olmayan bağlantı kurarak sunucuya beklenenden fazla iş yükü yüklemek ve gerçekten bağlantı kurmayı bekleyen kullanıcılara da cevap vermemektir. Kısaca ağ üzerinde yoğun bir trafik yaratarak sistemleri erişilmez hale getirir.

DoS saldırısı birden fazla bilgisayar üzerinden hedef sistem veya sistemlere yapıldığında ortaya Dağıtık Hizmeti Engelleme Saldırıları anlamına gelen Distributed DoS veya DDoS saldırıları çıkmaktadır. Böylece yapılacak saldırının etkisi de arttırılmaktadır. Soruşturulması zor olan bu tür saldırılarda saldırganlar birden çok sistemi ele geçirebilmek için zararlı yazılımları kullanmaktadır. Zararlı yazılımlar başlığımızda ele aldığımız Botnetler burada da karşımıza çıkmaktadır. Botnet isimli yazılımların çalışmasından

bahsetmek gerekirse; Botnetler kullanıcılardan habersiz bilgisayarlarına yüklenmekte ve siber saldırganlardan talimat geldiğinde yazılımın bulaştığı bilgisayarlar saldırının hedefinde bulunan internet adresleriyle bağlantı kurarak sunucuyu meşgul etmektedirler. Diğer taraftan Botnetler günümüzde zararlı program üreticileri tarafından iyi bir kazanç kapısı olarak da görülmektedir. Botnet yöneticileri sahip oldukları Botnet ordusunu saatlik 200-300 dolar gibi bir ücretle isteyenlere kiralayabilmektedirler [39]. Belirtildiği üzere artık siber saldırıda bulunmak için üst düzey bir teknik bilgiye sahip olmaya gerek yoktur, sistemin güvenlik açıklarını bilmek ve bunlardan faydalanmak yeterlidir.

Web uygulamalarına yönelik saldırılar

Kullanılan web uygulamaları kişisel ve kurumsal verileri, finansal bilgileri ve pek çok hassas veriyi işlemekte ve depolamaktadır. Web uygulama açıklıklarının istismar edilmesi kişi ve kurumları maddi ve manevi zarara sokabilmektedir. Olabilecek her türlü zararın önüne geçmek için web uygulamalarının güvenliği sağlanmalıdır. Bu sayede üzerinde bulundurduğu verilerin gizlilik, bütünlük ve erişilebilirliği de büyük ölçüde sağlanmış olacaktır. Web uygulamaları yapıları gereği internet veya iç ağda genele açık olarak hizmet vermekte ve bu durumda onları saldırması kolay hedefler haline dönüştürmektedir. Siber saldırganların bu uygulamaları tercih etmelerinde ki başlıca sebep, web uygulamaları pek çok farklı yazılım dilinden oluşturulabilir ve bu yazılım dillerinde yer alan bazı unsurlar sömürülmeye açıktır.

İnternet kullanımının artması ve yaygınlaşmasıyla birlikte web servisleri ve uygulamaları bilgi paylaşımını şekillendirmiş, web uygulamalarının kullanımını çeşitlendirerek arttırmıştır [40]. Web uygulamaları ise herhangi bir web sunucusu üzerinde çalışan yazılımların tümü olarak basitçe tanımlanabilir. Günümüzde web uygulamaları e-devlet, bankalar ve kurumsal ortamlar tarafından sıklıkla kullanılmaktadır. Diğer taraftan yazılımların organizasyon içinde yaygın kullanılması, işletim sistemleri ve ağ servisleri kadar sıkı korunmamaları, ihtiyaç duyulan bakım ve desteğin az yapılması, uygulamanın çalıştığı tarayıcılarda güvenlik açıklıklarının olması ve web uygulamalarına karşı gerçekleştirilen siber saldırı yöntemlerinin diğer bilişim sistemlerine karşı yapılanlardan daha basit olması da gelmektedir.

Web uygulamalarında amaç herkese en kısa sürede hizmet verebilmektir. Bu amaç doğrultusunda yazılımı geliştirenler daha kolay hata yapabilmektedir. Bu etkenleri ise, geliştirilen uygulamanın güvenliğinden ziyade fonksiyonelliğinin göz önünde bulundurulması, güvenlik bilgisinden yoksun kişilerin web uygulaması geliştirilmesiyle oluşan açıklıklar tetiklenmektedir [41]. Yapılan küçük bir hata bile tüm bilgisayar ağını tehlikeye atacak seviyede olabilir. Öyle ki saldırganın saldırmak için sizi takip etmesine gerek olmayabilir, Google üzerinden aramalarla da sayfalarınız hacklenebilir. Saldırganların bu yöntemleri tercih ederek web uygulamalarına saldırmasında merak, zarar verici niyet, para kazanma umudu gibi pek çok sebep vardır. OWASP (Open Web Application Security Project) kuruluşu web uygulama güvenliğinde farkındalığı artırmak için her yıl yıl içerisinde meydana gelen en bilindik web uygulama açıklıklarını yayınlamaktadır.

OWASP tarafından yayınlanan listeye göre 2019'un en bilindik 10 web uygulama açıklıkları aşağıda başlıklar halinde ele alınmıştır [42].

1) *Injection (Enjeksiyon)*: Güvenilir olmayan veriler bir sorgunun parçası olarak (örneğin SQL sorguları, PHP (Hypertext Preprocessor) sorguları, LDAP (Lightweight Directory Access Protocol) sorguları ve işletim sistemi komutları gibi) yorumlayıcıya gönderildiğinde enjeksiyon (akıtma) meydana gelebilir.

2) *Broken Authentication (Kırık Kimlik)*: Uygulamanın kullanıcının kimliğini tehlikeye sokacak şekilde oturum bilgilerini yanlış yönetmesi durumunda hatalı kimlik doğrulama oluşur. Saldırgan burada birinin oturumuna girmeye ya da kullanıcı tarafından sonlandırılan bir oturumu kullanmaya devam etmek ya da oturumla ilgili bilgileri çalmak istemektedir.

3) *Sensitive Data Exposure (Hassas Veri Ortaya Çıkarma)*: Uygulama tarafında veriler güvenli bir şekilde kullanılmazsa saldırganlar hassas verileri kopyalayabilir veya değiştirebilir. Zayıf şifreleme algoritmalarının kullanılması bu web uygulamalarını saldırılara açık hale getirmektedir.

4) *XML External Entities (XXE) (XML Dış Varlık)*: Bir web uygulaması kötü amaçlı bir XML (Extensible Markup Language) yüklemesini sağladıysa kullanıcıların güvenlik açısından faydalanan XXE (XML External Entity) saldırılarına karşı savunmasız hale

gelebilir. Kötü amaçlı kod ile saldırgan dâhili dosya paylaşımını engelleyebilir, hizmetleri engelleyebilir, bağlantı noktalarını tarayabilir ve gizli dosyaları ifşa edebilir.

5) *Broken Access Control (Bozuk Erişim Kontrolü)*: Kullanıcıların iş tanımları düzgün yapılmadığında dosyalara, veri tabanlarına, dizinlere vb. yetkisiz kaynaklara rahatça erişebilecek hale gelme durumuna bozuk erişim kontrolü denilmektedir. Böyle bir durumda her kullanıcı yönetici gibi hareket eder ve ardında güvenlik açığı bırakabilir. Saldırganların en çok atakta bulunduğu yetkisiz erişimin ortaya çıkması bu senaryoda kaçınılmazdır.

6) *Security Misconfigurations (Yanlış Güvenlik Yapılandırılması)*: En sık görülen güvenlik sorunlarından biridir. Genel olarak yapılandırmaların eksik veya geçici, güvenli olmayan kanallar aracılığıyla yapılmasından kaynaklanmaktadır. İşletim sistemlerinin, kullanılan kütüphanelerin güvenli olarak güncellenmesinin yanında zamanında da güncellenmesi, bakımlarının yapılması gerekmektedir.

7) *Cross Site Scripting (XSS-Siteler Arası Komut Dosyası Yazma)*: Saldırgan web sayfasına güvenilmeyen veri veya komut dosyaları ekleyebildiği zaman bu sorun meydana gelir. HTML (Hyper Text Markup Language) veya JavaScript ile oluşturulan bir tarayıcıya yerleştirilen saldırganların eklediği veriler veya komut dosyaları, kullanıcıların verilerini çalabilir, web sitelerini istediği şekilde güncelleyebilir, kullanıcının oturum bilgilerini ele geçirebilir ya da komut satırları ile bilgisayar her açıldığında kullanıcının kötü amaçlı sitelere yönlendirilmesine neden olabilir.

8) *Insecure Deserialization (Güvenli Olmayan Tersine Serileştirme)*: Önceden düzene oturtulmuş, belirli kurallara göre serileştirilmiş verilerin güvensiz yollarla değiştirilmesi işlemidir. Saldırganlar kodu uzaktan yönetebilme yeteneğine de sahip olurlar. Genellikle kullanıcı sıfatına sahip kişiler yönetici olarak rol değiştirirler ve ayrıcalık yükseltme saldırıları olarak da anılırlar.

9) *Using Components with Known Vulnerabilities (Bilinen Güvenlik Açıklarına Sahip Bileşenleri Kullanma)*: Kütüphaneler, çerçeveler ve diğer yazılım modülleri uygulama ile aynı ayrıcalıklara sahip olarak çalışırlar. Bilinen güvenlik açıklarına sahip bileşenleri kullanan uygulamalar saldırılara açık hale gelebilirler hatta sunucuları ele geçirilebilir.

10) *Insufficient Logging and Monitoring (Yetersiz loglama ve izleme)*: Günlük log kaydı yetersiz tutulduğunda ve eksik gözlemlendiğinde sisteme yapılan herhangi bir saldırı ya hiç fark edilmeyebilir ya da geç fark edilebilir. Zamanında tespit edilmeyen saldırı kalıcılığını sürdürmeye devam edebilir. Sonucunda daha fazla sunucuya erişim sağlayan siber saldırgan verileri kurcalamaya, ayıklamaya veya yok etmeye kadar işi götürebilir. Yapılan çalışmalar bu gibi ihlallerin log trafiğini 200 günden fazla takip etmeyen işletmelerde daha fazla görüldüğünü ortaya koymaktadır.

Sosyal mühendislik saldırıları

Günümüz teknolojisinin hızlı gelişmesi buna paralel olarak güvenlik açıklarının artmasına, veri hırsızlığının çeşitlenmesini de beraberinde getirmiştir. Her ne kadar kullanıcılar bilgi güvenliği konusunda eğitimlerle bilinçli hale getirilmeye çalışılsa da saldırganlar yeni bir saldırı metodu ile varlıklarını devam ettirmektedirler. Bu noktada son yılların en popüler saldırı yöntemlerinden biri olan sosyal mühendislik karşımıza çıkmaktadır. Şekil 2.4'te de görüldüğü üzere sosyal mühendislik saldırılarının oranı oldukça yüksektir [37]. Sosyal mühendislik, bilişim dünyasında insanların davranışları ve iletişimlerindeki zaaflarından yararlanarak ikna, telkin ve kandırma gibi çeşitli yöntemlerle istenilen bilgileri elde etmeye çalışmaktır. Bu tür saldırılar insan kaynaklı olabileceği gibi bilgisayar kaynaklıda olabilir. Saldırıların temel amacı; kimlik hırsızlığı, izinsiz ağa girmek, yetkisiz bağlantı kurmak, veri hırsızlığı veya dolandırma, sistem ya da ağın bozulmasına yol açmaktır.

Sosyal mühendislik saldırıları kişisel becerilere dayanan, basit ve etkili saldırılar olması yönünden teknik yöntemlere göre tespit edilmesi daha sıkıntılıdır. İlk sıralarda yer alan bu saldırı türünün önüne geçebilmek için kurumsal olarak güvenlik politikalarında düzenlemeler yapılmalı, son kullanıcıdan en üst yönetime kadar herkes eğitime tabi tutulmalı, eğitimlerde kullanıcılara olası senaryolar anlatılmalı ve olay gerçekleştiğinde nasıl müdahale edilebilir sorusunun cevabı önceden hazırlanmalıdır [37]. Tür ve yöntem olarak öne çıkan sosyal mühendislik saldırıları, hassas veriler ve yer aldıkları sistemler için tehlike arz etmeye devam etmektedir.

Bilginin ve hassas verilerin korunmaya çalışıldığı ilk zamanlardan itibaren ortaya konan güvenlik zincirinin en zayıf halkası her zaman insanlar olmuştur. Bilgi güvenliğini en üst

düzeyde tehdit eden, hassas veriye kolay yoldan erişim imkânı veren ve güvenlik kontrollerinin aşılmasını sağlayan önemli risk faktörlerinin başında “insan faktörü” gelmektedir [43]. Şirketler, kurum ve kuruluşlar üst düzey tekniklerle güvenlik kontrolleri uygulasa dahi siber saldırganlar en zayıf halka olan insanı çeşitli yöntemlerle kullanmayı bir şekilde başarmış, güvenlik duvarlarını aşmıştır. Geriye dönüp bakıldığında ise güvenlik ihlallerine sebep olan insan zafiyetinin son kullanıcıdan en üst yönetime kadar farklı kademelerde görev yapan insanların bilgi güvenliği konusunda eksikliklerinden, bilinçsizliklerinden ve eğitimsizliklerinden kaynaklandığı görülür.

En sık kullanılan sosyal mühendislik yöntemleri şunlardır [44,45]:

- Şirket, kurum veya kuruluşun çalışanı gibi davranmak.
- Karşı tarafı güvenilir bir kaynak olduğuna ikna etmek.
- Özellikle telefonda karşı tarafı aldatmak için başkasını taklit etmek.
- Ortak tanıdıkları öne sürerek yakınlık kurmaya çalışmak.
- Karşı tarafı zor durumda bırakarak yardım ediyormuş izlenimi vermek.
- E-posta ekinde virüs veya Truva atı göndermek.
- Karşı tarafın yeniden bağlanmasını ya da parola girmesini isteyen sahte bir giriş ekranını kullanmak.
- Hedef sistemin kullanmadığı, çöpe çıkardığı donanımları veya programları karıştırarak bilgi toplamaya çalışmak.
- Kullanıcılara bilgisayarlarına yüklemeleri için bedava yazılım veya yama göndermek.
- Güven kazanmak için şirket ya da kurumun ortak kullandığı kelimeleri kullanmak.
- Bir sisteme yeni bir ürün ya da güncelleme sunmak için arayan bir satıcı ya da firma gibi davranmak.

Daha da artırabileceğimiz bu yöntemlerin önüne geçebilmek adına insan unsurunun hata payını en aza indirecek tedbirlerin alınması, alınan tedbirlerin insanlar ne biliyor, ne düşünüyor ve ne yapıyor gibi kavramları değiştirebilmesi ve geliştirebilmesi büyük önem taşımaktadır.

Tezimizin temel çalışma alanı olan sosyal mühendislik konusu ilerleyen kısımlarda daha detaylı incelenip insan faktörüyle birlikte ele alınacaktır.

2.2.2. 2019 yılının öne çıkan siber saldırı örnekleri

Siber saldırıların, yasadışı sistemleri ele geçirme olaylarının ve veri ihlallerinin ortaya çıkardığı yıkım hiçbir zaman ortadan kalkmayacaktır. Son birkaç yılda tıbbi bilgilerin çalınması, hesap veya kimlik bilgilerinin çalınması, e-posta adreslerinin çalınması ve kurumsal verilerin dışarıya sızması gibi veri ihlali konulu haberleri daha sık duymaktayız. Çünkü Risk Based Security raporuna göre, 2019'da yaşanan siber güvenlik saldırıları yüzde 33 artış göstermiştir ve saldırıya uğrayan hedeflerin başında medikal hizmetler, perakende ve kamu kurumları gelmiştir [46]. Hassas verilerin olduğu sunucular dahi korunmasız yapılar içerisine girmiştir. Dünyanın sayılı bulut depolama şirketlerinden olan Amazon Web Services ve Elasticsearch gibi şirketler kendi isimlerini siber güvenlik haberlerinde görmeye alışır hale gelmişlerdir. Yine dünyanın sayılı şirketlerinden biri olan IBM yıllık veri ihlali maliyetinin en son 3.92 milyon dolara ulaştığını ve bu maliyetin son beş yılda % 12 arttığını duyurmuştur.

Aşağıda, 2019 boyunca gerçekleşen en büyük veri ihlallerine neden olan siber saldırılar verilmiştir [47,48,49].

Ocak

Apple FaceTime: Bir Fortnite oyuncu, kullanıcıları arayarak iPhone'a cevap vermeden o iPhone ortamını gizlice dinlemeyi ve canlı video yayınlarını görüntülemeyi başararak Apple iOS hatasını bulmuştur.

Marriott Hotel: Siber suçlular, pasaport numaraları ve kredi kartı bilgileri dâhil 383 milyon müşterinin verilerine erişim sağlamıştır.

Ministry of Health Singapore: Singapur'da Sağlık Bakanlığı, bir veri ihlali sonucu HIV teşhisi konmuş 14.000'den fazla kişinin gizli ve son derece hassas kayıtlarının çevrimiçi (online) olarak yayımlandığını duyurmuştur.

Şubat

620 Million Accounts: Siber suçlular aralarında Dubmash, Armor Games, 500px, Whitepages gibi şirketlerin yer aldığı 16 web sayfasından 617 milyon kişiye ait kişisel verileri çalıp ve Dark Web üzerinde satışa sunmuşlardır.

Web sayfalarından alınan verilerin tümü, 20.000 dolar değerindeki BTC (bitcoin) karşılığında karaborsada satılmıştır.

Medical Advice Calls: İsveç ulusal sağlık hizmeti hattına ait çağrı hattı verileri açık bir sunucuda depolanmaktaydı. Saldırganlar 2,7 milyon İsveç vatandaşının sağlık raporlarını ve telefon numaralarını ele geçirerek internete sızdırmışlardır.

Mart

Facebook, Facebook Lite and Instagram: Yüz milyonlarca Facebook ve Instagram kullanıcısının verileri internete sızdırılmıştır.

Sızıntının kaynağı ise hesap kimlik bilgilerinin düz metin olarak saklanması ve kalitesiz şifre depolama yönetiminin kullanılması olarak belirlenmiştir.

Legal Documents: ABD’de 2002-2010 yılları arasında görülmüş sayısız davaya ait çoğu gizli ve üzerlerinde “yayınlamak yasaktır” yazılı 250.0000 yasal belgenin bulunduğu sunucu siber suçlular tarafından ele geçirilmiştir. Saldırganlar ele geçirdiği dokümanları en az 2 hafta çevrimiçi (online) olarak internette yayınlamışlardır.

Nisan

Toyota: Japon otomobil üreticisi Toyota, satış iştiraklerinde ve bayilerde veri ihlalinin olduğunu, sistemlere yetkisiz erişimlerin gerçekleştiğini sonuç olarak verilerinin açık edildiğini duyurmuşlardır.

Pregnant Women: Hindistan’da devlete bağı bir sağık kuruluşuna ait sunucuya yapılan siber saldırı sonucunda 12,5 milyondan fazla hamile kadına ait bilgiler saldırganlar tarafından ele geçirilmiştir.

Mayıs

First American Financial: Gayrimenkul devi First American Financial şirketine ait 2003 yılından itibaren ki yüz milyonlarca sigorta belgesi, banka hesap numaraları, hesap özetleri, ipotek ve vergi kayıtları siber saldırganlar tarafından internete sızdırılmıştır.

Burger King: Firma, çocuklara yönelik özel olarak tasarlanmış Kool King Shop internet hizmetine ait 40.000 müşteri kaydının tutulduğu veri tabanının siber saldırganlar tarafından ele geçirildiğini duyurmuştur.

Git Repositories: Bir siber saldırgan GitHub kaynak verilerini sistemden kaldırdı ve verileri önce halka açıklamak sonrada tamamen veri depolarından silmekle yetkileri tehdit edip fidye istemiştir.

Haziran

American Medical Collection Agency (AMCA): Amerikan Medikal Veri Toplama Derneğı’nin (AMCA) sunucularına yönelik gerçekleşen siber saldırı sonucunda veri tabanlarında bulunan en az 20 milyon hastanın ödeme bilgilerinden sosyal güvenlik numaralarına, medikal verilerinden doğum tarihlerine ve hatta telefon numaraları ve adreslerine kadar sayısız kritik bilgi siber suçluların eline geçmiştir.

Sayısız dava ile karşılaşan AMCA karşılaştığı finansal darboğazı kaldıramayarak iflasını açıklamıştır.

Tech Data Corporation: Fortune 500 şirketi müşteri sunucuları, faturaları, SAP entegrasyonları ve parolalarının olduğu 264 GB veri içeren açık veri tabanının siber saldırganlar tarafından ele geçirildiğini duyurmuştur.

Temmuz

Capital One Bank: Kanada'daki 100 milyon ABD vatandařını etkileyen güvenlik ihlalinde siber saldırganlar 140 bin sosyal güvelik numarası, 80 bin banka hesap numarası ve pek çok kişisel veriyi ele geçirmişlerdir. FBI tarafından soruşturulan olayda saldırganın, bankanın bilgi teknolojileri departmanında çalışan bir biliřim uzmanı olduđu ortaya çıkmıştır.

Equifax: 2017 yılında uğradıđı siber saldırının yaralarını saramamış olan Equifax hükümet düzenleyicileri ile bu dönemde 700 milyon dolara anlaşmış ve verileri çalınan müşterilerine 150 milyon dolara yakın tazminat ödemiřtir.

Ağustos

Cybercrime in Space: Bir NASA astronotunun, eski eşinin banka hesabını izinsiz olarak uzay boşluğundan izlediđi tespit edilmiştir.

3Fun: 1,5 milyon aktif kullanıcıya sahip mobil uygulama olan 3Fun “gizli kötü durum” olarak adlandırdıđı yer bildirim aracı ile kullanıcıların konumlarını tespit etmiş ve bu bilgileri ilerleyen zamanlarda kötüye kullanmıştır.

Eylül

Ecuador: 17,5 milyon nüfuslu Ekvador'da hükümete ait veri tabanlarının yanlış yapılandırılması sonucu vatandařlara ait kişisel bilgiler çalınmış ve internete sızmıştır.

DK-LOK: Güney Koreli sanayi üreticisi DK-LOK uğradıđı siber saldırı sonucunda güvenli olmayan veri tabanı sunucusu ele geçirilmiş ve řirket ile müşteriler arasındaki gizli e-postalar deřifre olmuřtur. Yapılan arařtırmalar sızıntının etkinliklerin iletiřim bilgilerinin e-postalarının çöp kutusu kısmına gönderilmesi sonucunda kaynaklandıđını tespit etmiştir.

Ekim

Yahoo: Yahoo, 2012 ve 2016 yılları arasında Yahoo hesabı olanlar için tazminat fonu başlatmıştır. Çünkü siber saldırganlar bu tarihler arasında var olan her Yahoo hesabına

erişmiş, kullanıcıların kişisel verilerinin yanı sıra şifrelerini ve güvenlik sorularını da ele geçirmişlerdir.

Adobe: Adobe, 7,5 milyon Creative Cloud müşterisinin bilgilerinin veri tabanlarına erişirken kimlik doğrulama istemedikleri için ele geçirildiğini duyurmuştur.

20 Million Russians: Rus vatandaşlarına ait 2009-2016 yılları arasındaki vergi bilgileri açık sistem bir veri tabanında tutulduğu için korunmasız halde bırakılmış ve bu vergi kayıtları siber saldırganlar tarafından internette yayınlanmıştır.

Kasım

Trend Micro: Siber güvenlik firması olan Trend Micro da “içten saldırı” vakası ortaya çıkmıştır. Firmanın çalışanı müşterilere ait 70.000 veriyi ele geçirmiş hem müşterileri kendi dolandırmış hem de bilgileri başka dolandırıcılara satmıştır. Olayın anlaşılması üzerine çalışan tutuklanmıştır.

UK Labour Party: İngiltere İşçi Partisi maruz kaldığı DDoS saldırısı ile partinin web sitesinin yanı sıra kampanya araçlarına ait verilerini de siber saldırganlara kaptırmıştır.

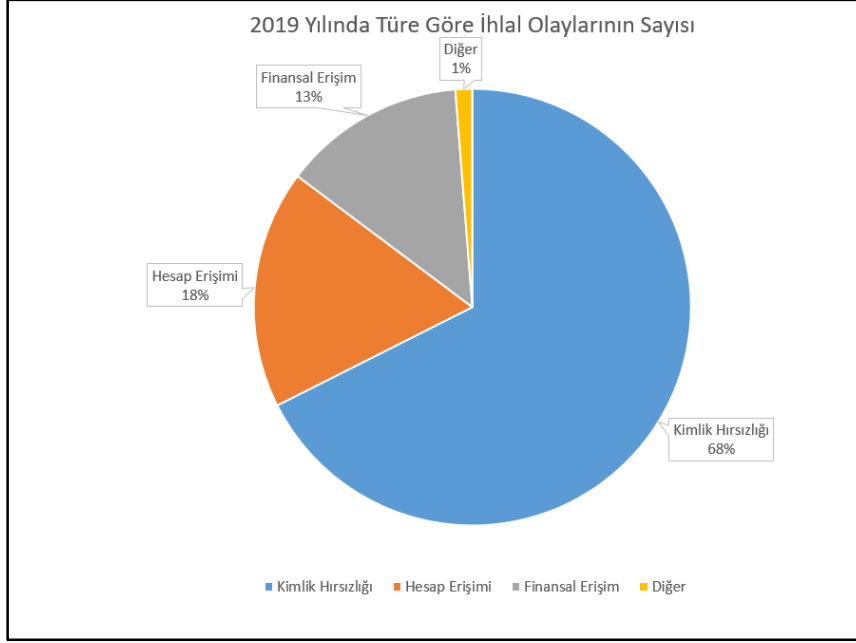
Aralık

Politician by Day, Hacker by Night: Yılın son günlerine damga vuran bu olaya göre Hollandalı bir politikacının yıllardır internet üzerinden kadınlara şantaj yapan bir hacker olduğu ortaya çıkmıştır. Üyesi olduğu grupla birlikte 100 kadının iCloud hesaplarına sızmış ve özel fotoğraflarını ele geçirmişlerdir. Aralarında Hollywood ünlüleri dâhil sosyal medyada tanınan kişiler ve dünyaca ünlü sporcularında olduğu 100 kadına şantaj yapan politikacı hapis cezası ile yargılanmaktadır.

New Zealand's Gun Buyback: Yeni Zelenda'nın Christchurch şehrindeki kitlesel saldırı atışlarından sonra başlatılan silah geri alım programı SAP (Systems Analysis and Program)'deki insan hatasından kaynaklı veri ihlali ile karşılaşmış, gizli tutulması gereken bilgiler açığa çıkmıştır. Silah sahiplerine ait bilgilerin yayılması yetkilileri harekete

geçirmiştir. SAP daha sonra yetkililerden özür dilemiş ve onlar için özel bir lisans uygulaması geliştirmiştir.

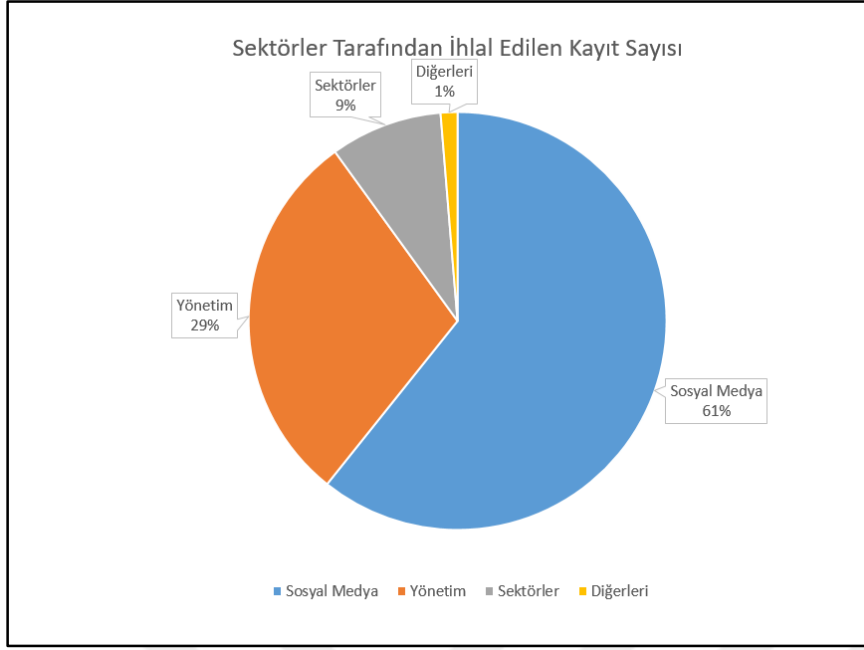
Şekil 2.5'te 2019 yılı içerisinde gerçekleşen sosyal mühendislik saldırıları sonucunda ele geçirilen verilerin istatistiksel dağılımı verilmiştir.



Şekil 2.5. 2019 yılında türe göre ihlal olayları [50]

Şekil 2.5'te görüldüğü üzere gerçekleşen saldırılar büyük oranla kimlik hırsızlığına sebebiyet vermiştir. Bunu hedefin hesap ve finansal erişim bilgileri takip etmektedir.

Şekil 2.6'da ise 2019 yılında gerçekleşen sosyal mühendislik saldırıları sonucunda hangi sektörün içerisinde barındırdığı kayıtların ne kadarını ihlal ettiği istatistiksel olarak verilmiştir.



Şekil 2.6. 2019 yılında ihlal edilen kayıtlar [50]

Şekil 2.6’da belirtilene göre 2019 yılında gerçekleşen sosyal mühendislik saldırıları Dünya genelinde; sosyal medya 2,5 milyar, yönetim 1,2 milyar, çeşitli sektörler 380 milyar ve diğer sebeplerden kaynaklı 357 milyar değerinde kaydın ihlal edilmesine neden olmuştur [50].

2.3. Siber Saldırıların Tespiti ve Sınıflandırılması

Şirket, kurum ve kuruluşlarda çalışanların, sistemi yöneten kullanıcıların bilgi güvenliği farkındalığının artırılabilmesi için öncelikle karşılarındaki tehlikeyi detaylı olarak tanımları gerekmektedir. Saldırıların hangi kaynaklardan geldiğini, adımlarının neler olduğunu, varsa türlerinin ve sınıflandırılmalarının genel bilgi birikimi oluşturulmalıdır. Sistemi kullanan bütün kullanıcıların saldırı olması durumunda teknik personel gibi hareket etmesi, konuya hâkim olması beklenmese de ne ile karşılaştıklarını, içerik olarak neler olduğunu kavrayabilecekleri bilgiye sahip olmalıdır.

Günümüz dijital dünyasında sistemlerin sahip olduğu verilerin önemi ve miktarı artmış buda saldırganların ağ ve web hizmetlerine farklı yöntemlerle daha sık saldırmasına yol açmıştır. Şirket, kurum ve kuruluşlar ağ yapılarını güçlendirmek için Güvenlik Duvarı, VPN (Virtual Private Network) ve şifreleme gibi metotların yanı sıra saldırı tespiti metodunu da benimsemişlerdir.

Saldırı tespiti; olası atak, tehdit ve ihlallerin tespiti için ağda gerçekleşen olayları gözlemleyen ve ağda gerçekleşen bir saldırının varlığını belirlemek için kontrol eden bir işlemdir.

Siber saldırıyı yazılım veya donanım aracı ile tespit etmek mümkündür. Tespit yöntemleri bilgisayar ağında hizmet engeli, bilgi sızması veya yetkisiz girişler varsa bunları açığa çıkarmaya yarar. Çok iyi teknik bilmeyen kişilerin dahi rahatlıkla hedef sistemlere saldırabildiği göz önüne alındığında saldırı tespit sisteminin her türlü kötü niyetli ağ trafiğini tespit edebiliyor olması gerekmektedir. Sıklıkla port taraması, sosyal mühendislik, ağa yerleşerek trafiğin izlenmesi, ağ topolojisinin çıkarılması gibi saldırılar yapılırken Google, kırma (hacking) ve shodan gibi arama motorlarından hedef sistem hakkında bilgi toplama ve keşif yapmakta siber saldırganların en çok tercih ettiği yollardır. Siber saldırıların yapabilecekleri ve ortaya çıkarabilecekleri zararın boyutu düşünüldüğünde saldırı tespit sistemleri gerçek zamanlı izleme yapabildiği gibi gerçek zamanlı olmayan izleme kontrollerini de yapabiliyor kabiliyette olmalıdır.

Siber saldırı yaşam döngüsü bilgi toplama, keşif, zafiyet taraması, açıklıkları istismar etme, sistemin ele geçirilmesi, izlerin temizlenmesi, kazanç ve hedef belirleme adımlarından oluşan dinamik bir yapıya sahiptir. Bu adımların içeriğini oluşturan siber saldırıların, 5 ana başlıkta sınıflandırıldığı Şekil 2.7’de görülmektedir [51].



Şekil 2.7. Saldırıların sınıflandırılma diyagramı

Siber saldırılar sınıflandırılırken ana başlıklarda kendi aralarında detaylandırılmıştır.

Şekil 2.7’de bu ana başlıklar ve alt başlıkları birlikte verilirken detayları ayrı ayrı bir sonraki kısımda ele alınmıştır.

2.3.1. Amaçlarına göre sınıflandırma

Keşif saldırısı, erişim saldırısı ve servisin engellenmesi saldırısı olarak kendi içinde ayrılır [51]. Keşif saldırısında amaç, saldırmak değil saldırı için ön çalışma yapmaktır. Nereden, hangi yolla, nasıl saldırı gerçekleştirileceğini önceden belirlemektir. Saldırgan gizlice ağ trafiğini dinler, bağlantı noktalarını tarar, DNS (Domain Name System) sorgularını ve IP (Internet Protokol) aralığını öğrenmeye çalışır [51]. Sistem üzerinde yetkisiz keşifler, sistemi haritalama veya adlandırma işlemleri bu kısma girer, saldırgan ıssız bir eve girmeye çalışan hırsız gibi düşünülebilir.

Erişim saldırısında, saldırgan erişim hakkı olmamasına rağmen sistemin güvenlik açığından yararlanarak içeri sızar [51]. Hackleme işleminde şifre kombinasyonları çokça kullanılır ve kullandıkları şifre atakları şifre tahmini ve şifre sıfırlama olarak ikiye ayrılır. Kimlik doğrulama hizmetleri, FTP (Dosya Aktarım Protokolü) hizmetleri ve web hizmetleri yetkisiz erişimden en çok etkilenip veri kaybı yaşayan hizmetlerdir. Ortadaki adam saldırısı, sosyal mühendislik ve oltalama saldırıları bu türe örnek olarak verilebilir. Erişim saldırısında saldırganın amacı her yöntemde aynıdır, içerden biri gibi davranarak sisteme sızmak ve hassas verileri ele geçirmektir [51].

Servisin engellenmesi saldırısı ise sistemin zayıflatılması veya sisteme zarar verilmesi olarak tanımlanır [51]. Saldırgan direkt bilgisayar ağına yoğunlaşarak ağı devre dışı bırakmaya veya ağa gelen kullanıcı hizmetlerine yönelik servisleri reddetmeye çalışır. Bu atakla verileri tamamen silmek ya da tamamen değiştirmek mümkündür.

2.3.2. Yasal sınıflandırma

Siber suç, siber casusluk, siber terörizm, siber zorbalık ve veri savaşı bu grubun içerisinde yer almaktadır [51].

Siber suç sistemi bir araç olarak, bilgisayarı da suçun tesadüfî bir parçası olarak görmektedir. Çünkü bilgisayar suçlarında suçu işleyen genelde bilinmez, işletim sistemlerinin zayıflıkları vardır ve kullanıcılar farkındalık konusundan yoksundurlar [52].

Siber casuslukta daha çok kötü amaçlı yazılımlar ile kişilerin, şirketlerin, kurum ve hükümetlerin yasadışı tekniklerle gizli bilgilerini elde etme, kendi yararları için kullanma söz konusudur. Saldırganlar evde oturarak ülkeler arası veri casusluğu yapmayı son zamanlarda sıklıkla yapmaktadırlar [51]. Bu tür operasyonları genelde özel eğitilmiş casuslar, kötü amaçlı hackerler ve programcılar tercih etmektedir.

Siber terörizm, 21. Yüzyılda ortaya çıkarak değişikliğe uğramış terörün bir diğer boyutudur. Bilgisayar virüsleri gibi araçlarını kullanarak internet ağlarına büyük hasarlar vermeye yönelik terörist faaliyetleri içerir. Terörün bu formuna karşı savaşmak, karşı koymak oldukça zordur [53].

Siber zorbalıkta durum biraz daha değişir. Kişisel veya grup olarak tasarlanmış, belirli aralıklarla tekrarlanan bir zarar verme söz konusudur. Siber zorbalar karşı gruba kötü içerikli e-posta gönderme, aşağılayıcı web sitesi yayınlama, kullandıkları anlık mesajlaşma veya diğer uygulamalara zararlı içerik gönderme şeklinde bilgi ve iletişim tekniklerini kullanarak saldırılarını gerçekleştirirler [54].

Bahsedilen tüm bu yan başlıklar aslında temelde kıymetli veriyi, değerli bilgiyi ele geçirmeye, onu kontrol edebilmeye yönelik savaştır. Bilgiye dayalı süreçleri, bilgi sistemlerini, bilgiye dayalı ağ sistemlerini etkilemek, onları korumak ve yönetmek içinde bulunduğumuz yüzyılın en büyük güç hareketi olarak kabul görmektedir.

2.3.3. Dâhil olma şiddetine göre sınıflandırma

Siber saldırılar dâhil olma şiddetine ve ilişkisine göre de sınıflandırılmışlardır. Aktif saldırılar ve pasif saldırılar olarak incelenirler [51].

Aktif saldırılarda, gerçekleşen bir saldırı tüm taraflara veri iletimine ya izin verir ya da tek veya çok yönlü veri iletimini engeller. Saldırganın bulunduğu ağda telekomünikasyon tarafları arasında bir veri iletimi varsa saldırı bunları kolayca sonlandırabilir [51].

Ardından da kimlik doğrulama sürecinde alıcı tarafın yerine geçmesi uzun sürmeyecektir. Çünkü hedef tarafın doğrulama sunucusu ele geçirilmiş haldedir ve alıcının kimliğini gerçek manada doğrulaması beklenemez. Siber saldırgan bir bilgisayarı iki alt ağ arasında bir bağlantı olarak kullanmış, onlar gibi davranarak fazladan çaba sarf etmeden atağını gerçekleştirmiştir.

Pasif saldırıda, yetkisiz saldırgan iki taraf arasında ki iletişim ağını gizlice dinler. Sistemde depolanan verileri hattı dinleme yoluyla ele geçirmeye çalışır. Aktif saldırıdan farkı veri tabanına hiç karışmaz, dinlediği hatta ne veri varsa ona sahip olur [51].

2.3.4. Kapsamına göre sınıflandırma

Kötü niyetli büyük ölçekli ve iyi niyetli küçük ölçekli olarak iki kategoride toplanmıştır [51].

Kötü niyetli büyük ölçekli de, kötü niyet “*zarar vermek maksadıyla kasıtlı olarak yapılan*” anlamında kullanılmaktadır [51]. Bir kişi veya grup tarafından kişisel kazanç, zarar ve kaosa sebep olma amacıyla ortaya çıkmaktadır. Amacına ulaşan saldırılar dünya çapında binlerce sistemin zarar görmesine, çökmesine ve büyük oranda veri kaybının yaşanmasına neden olmaktadır.

İyi niyetli küçük ölçekli olan genellikle kazara meydana gelen saldırılardır. Sistemlerin yanlış kullanımı, operasyonel hatalar, düşük maliyetli güvenlik önlemleri vb. bu saldırıların temel nedenleri arasındadır. Veri kaybı ve sistem çökmesi diğerlerine kıyasla daha azdır [51]. Bu gibi durumlarda ağdaki sadece birkaç sistem tehlikeye girer ve veriler çoğunlukla kurtarılabilir.

2.3.5. Ağ türüne göre sınıflandırma

Saldırıları bu başlıkta mobil adhoc ağları ve kablosuz sensör ağları olarak iki grupta kategorize edilmiştir. Çizelge 2.1’de ağ türüne göre sınıflandırmalar verilmiştir.

Çizelge 2.1’de belirtilen mobil adhoc ağları saldırıları detaylandırılırsa, bağlantılar arasındaki bilgi akışını yavaşlatmayı veya durdurmayı amaçlar. Kendi içerisinde Bizans

saldırısı, kara delik saldırısı, sel baskın saldırısı ve Bizans solucan deliği saldırısı olarak dörde ayrılır. Bunlar [51];

- Bizans saldırısı, yalnızca mobil adhoc ağlarda görülen ve cihazda kimlik doğrulama işlemi yapıldığı anda meydana gelen güvenlik sızıntılarından yararlanan bir saldırdır.
- Kara delik saldırısında saldırgan, tüm ağ trafiğini belli bir bağlantı noktasına yönlendirir. Gerçekte var olmayan bağlantıya bütün verilerin aktarılmasıyla kara delik adı verilen bu bağlantı noktasında veriler yok olmaktadır.
- Sel baskın saldırısı, adından anlaşıldığı üzere yoğun bir veri akışında meydana gelen saldırı türüdür. Kurallara uygun ve uygun olmayan veri akışı arasında ki yarıştan faydalanır. Veri yayılması olduğu anda harekete geçer ve kimlik doğrulama sistemlerini çökertir.
- Bizans solucan deliği saldırısı, iş birliği halinde çalışan saldırganlar farklı bağlantı noktalarından birden fazla bağlantıyı aynı anda keserek sisteme giriş yaparlar. Çok güçlü bir saldırı tekniği olmasına rağmen aynı anda en az iki bağlantı noktasını ele geçiremezler saldırganlar için başarısız bir durum ortaya çıkar.

Kablosuz sensör ağları ise, ağ üzerinde ki bilginin iletimini ve tespitini sağlayan sensörleri engelleyen bir saldırı türüdür. Buda Çizelge 2.1’de verildiği üzere; uygulama katmanı saldırıları, taşıma katmanı saldırıları, ağ katmanı saldırıları ve çok katmanlı saldırılar olmak üzere dörde ayrılır. Bunlar [51];

- Uygulama katmanında saldırılar, verileri reddetme ve bozma şeklinde gerçekleşir.
- Taşıma katmanında, oturumu ele geçirerek ve iletişim hattına baskın yaparak saldırılır.
- Yukarıda bahsedilen Bizans saldırısı, kara delik saldırısı, sel baskın saldırısı, Bizans solucan deliği saldırısı ve konumun açığa çıkma saldırıları ağ katmanında ortaya çıkan saldırılardır.
- Çok katmanlı saldırılar içerisinde de hizmet engelleme saldırılar (DoS), kimliğe bürünme saldırıları ve ortada ki adam saldırıları yer almaktadır.

Çizelge 2.1. Ağ türüne göre saldırıların farklı türleri [51]

Saldırıların İsmi	Tanımı	Örnekler
Mobil Adhoc Ağları	Bu saldırılar bağlantılar arasındaki bilgi akışını yavaşlatmayı ya da durdurmayı amaçlar.	• Bizans saldırısı • Kara delik saldırısı • Sel baskın saldırısı • Bizans solucan deliği saldırısı
Kablosuz Sensör Ağları	Ağ üzerinde ki bilginin iletimini ve tespitini sağlayan sensörleri engelleyen bir saldırı türüdür.	• Uygulama katmanı saldırıları • Taşıma katmanı saldırıları • Ağ katmanı saldırıları • Çok katmanlı saldırılar

2.4. Sosyal Mühendislik

Teknolojik gelişmeler büyük bir hızla artarken beraberinde getirdiği yenilikler kuşkusuz hem bizleri hem de sosyal hayatımızı etkilemektedir. Öyle ki bu yenilikler, insanların yaşam kalitesini artırmış, her sektörde yeni hizmetlerin ortaya çıkmasına olanak sağlamış, uzağı yakınlaştırmış, sunduğu kolaylıklarla evden dışarı çıkmadan da pek çok işi rahatlıkla yapma imkânını sağlayarak insan hayatının vazgeçilmezleri arasına girmiştir.

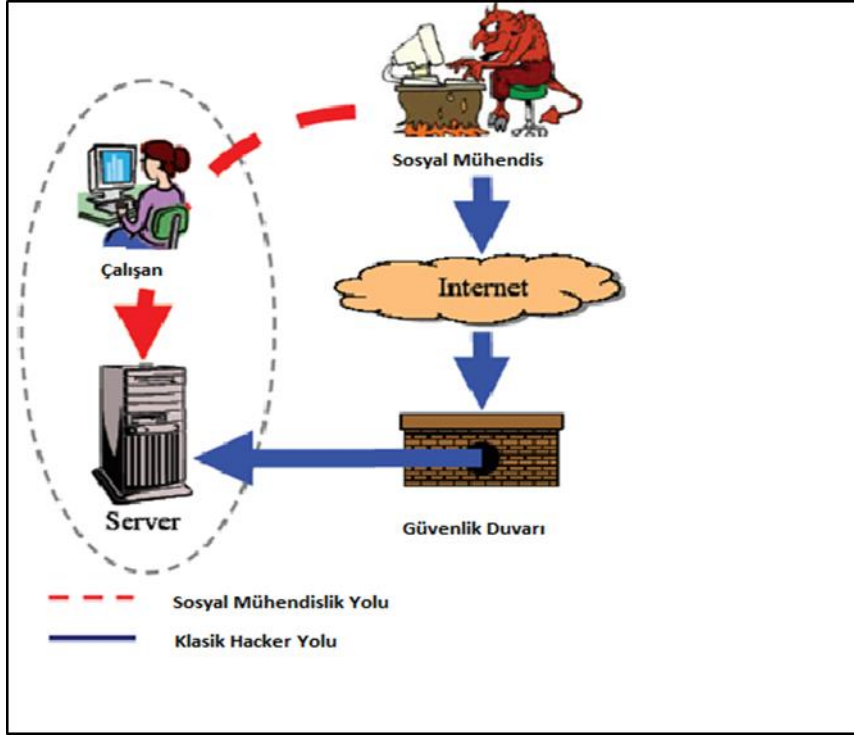
Günlük hayatın olağan akışı içerisinde, artık garipsemediğimiz hatta daha fazlasını da beklediğimiz teknolojik yenilikler, siber güvenlik ve siber saldırı kavramlarını da beraberinde getirmiştir. Siber saldırı denildiğinde sıklıkla akıllara bilgisayar üzerinden yapılan saldırılar gelmektedir; oysaki bilgisayar sistemleri insandan bağımsız düşünülemez ve doğrudan insanlar da siber saldırıların içerisinde kendilerini bulabilirler. Gerçek şu ki; insanoğlunun müdahalesinin olduğu herhangi bir sistemdeki güvenlik mefhumu önemli ve ele alınması gereken bir detay olarak karşımıza çıkmaktadır. Nitekim ünlü sosyal mühendislerden biri olan Kevin Mitnick “*Art Of Deception*” adlı kitabında, “*Güvenlik zincirindeki en zayıf halka insandır.*” sözüyle durumun insan aleyhine olan hassasiyetini ifade etmiştir [55]. Çoğu zaman duyguları ile hareket eden bir varlık olan insanı kandırmak teknolojik bir ürünü kandırmaktan daha kolaydır. Duruma benzer bir bakış açısıyla bakan ünlü bilim insanı Albert Einstein “*Yalnızca iki şey sonsuzdur, evren ve insanoğlunun aptallığı; aslında evrenin sonsuzluğundan o kadar da emin değilim*” sözüyle insanoğlunun kandırılmaya ve istismar edilmeye çok müsait bir varlık olduğunu belirtmiştir [55].

İnsanların güvenini kazanarak onlara istemedikleri şeyleri yaptırmak, onları istismar etmek siber güvenlik konu başlığı altında sosyal mühendislik ile ilişkilidir. Tanımlayacak olursak, sosyal mühendislik; insan davranışlarındaki yanlışları veya zaafırları kötüye kullanarak bir

sistemin ele geçirilmesi işlemidir. Sosyal mühendislik başka bir ifadeyle toplum mühendisliği, yalan söyleme ve ikna etme üzerine kurulan, inandırma ve bilgi toplama sanatıdır [55].

Sosyal mühendislik saldırıları, genellikle sosyal mühendis olarak adlandırılan kişilerce dışardan yapılır. Ancak dışardan yapılan saldırıların yanında herhangi bir organizasyon içerisinde de saldırılar yapılabilmektedir. Sosyal mühendis ise, insan psikolojisini anlayan ve bunu manipüle ederek, siber saldırılar vasıtasıyla yetkisiz erişim sağlamaya ya da gizli ve hassas içerikli verileri ele geçirmeye çalışan, hedefteki kurbanı kullanan kişidir. Sosyal mühendisler, ihtiyaç duydukları bilgileri, çoğunlukla sistem kullanıcılarından psikolojik hileler kullanarak elde etmektedir. Teknik olarak bakıldığında bu mühendislerin, yapmış oldukları saldırılar sonucunda risk almadan ve fazla zaman kaybı yaşamadan başarılı bir şekilde amaçlarına ulaştıkları gözlenmektedir. Bu saldırılarda hedef seçilen kişinin bilgisizliğinden, dikkatsizliğinden ve kişisel zaaflarından yararlanmak sosyal mühendisler adına daha iyi sonuç vermektedir.

Sosyal mühendisler, karşılarındaki kurbanı ve kendilerine, ellerindeki saldırı senaryosuna göre rol biçerler. Genelde saldırganlar arkadaş canlısı davranıp iyi ilişkiler kurmayı, kendilerini karşı cins gibi gösterip etkilemeyi, telefon yoluyla taklit ve ikna yöntemini kullanmayı tercih etmektedir. Bu tarz yolların tercih edilmesinin sebebi sistem ağına doğrudan atakta bulunup zaman kaybetmek yerine daha hızlı sonuç verecek aksiyonlar gerçekleştirmektir. Sosyal mühendislik saldırılarının başarılı olabilmesi için atak yapacak olan sosyal mühendislerin; ikna ve taklit yeteneği yüksek, hazır cevap, konuşkan, her türlü soruya cevap verebilecek, kişiler üzerinde olumlu etkiler bırakan, karşı tarafı iyi çözümleyen, değişen durumlara ayak uydurup yeni senaryo yazan, iletişim kabiliyetine sahip kişiler olması gerekir.



Şekil 2.8. Sosyal mühendislik saldırı yolu [56]

Şekil 2.8’de klasik bir sosyal mühendislik saldırısının işleyişi gösterilmektedir. Görüldüğü üzere sosyal mühendis hedef sistemin bağlantısını kesmek, güvenlik duvarını aşmak veya diğer güvenlik önlemlerini aşmak yerine, daha kısa ve daha az riskli yoldan direkt sistem kullanıcılarını hacklemeye çalışmaktadır. Sosyal mühendisliğin mucidi olarak görülen Kevin Mitnick, sosyal mühendislik alanında yazdığı kitabında bu yolu kullandığını ve girdiği sistemlerin %80’ine sosyal mühendislik yöntemleriyle eriştiğini ifade etmiştir [55]. Mitnick, dünyanın en güvenli bazı bilgisayar sistemlerine dahi teknik bir yol izlemek yerine sosyal mühendislik yöntemleriyle sızmış, binlerce Telekom verisine erişim sağlamıştır.

İnsanların büyük çoğunluğu, güvenlik ihlallerinin sadece teknik yollardan kaynaklandığını düşünmektedir, oysaki sistemdeki açıklıklar çoğu zaman davetsiz misafirler tarafından istismar edilebilir veya kötüye kullanılabilir. Teknik önlemler tam anlamıyla hiçbir zaman yeterli olmamaktadır. Örneğin sistemde yapılan her güncelleme farklı kusurlar veya güvenlik açıkları doğurabilmektedir. Buna ek olarak sosyal mühendislik saldırıları da yazılım ve donanım güvenliği önlemleri arasında kolayca gezinmeye imkân sağlamaktadır. Saldırganın bazen yapması gereken tek şey hedef sisteme ait, kontrolü ele geçirebileceği bir kimlik bilgisini elde etmektir. Saldırıdan önce, sosyal mühendisler hedefteki sistem kullanıcısının zayıflıklarını ve eksik yönlerini tespit eder, ardından doğru zamanı bekler ve

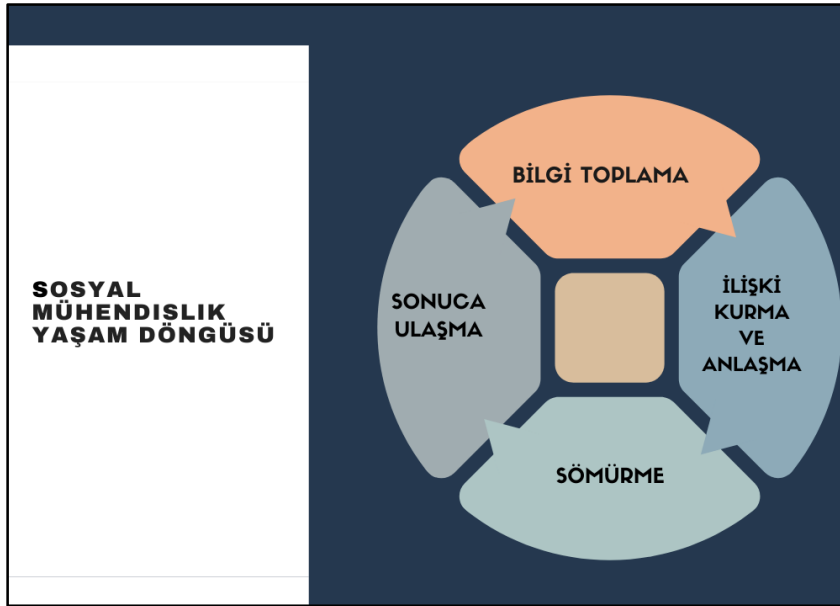
saldırı tekniğini uygular. Sistem kullanıcılarının güvenlik politikalarını eksik ya da hiç bilmemesi, güvenlik bilincine sahip olmaması, olumsuz sonuçların göz ardı edilmesi ve zamanında kapatılmayan güvenlik açıklıkları sosyal mühendislerin işini oldukça kolaylaştırmaktadır.

2.4.1. Sosyal mühendislik saldırı döngüsü

Sosyal mühendislikte saldırının türü değişse de işleyiş olarak genelde aynı yolu izlerler. Bilgi toplama, ilişki kurma ve anlaşma, ilişkiyi sömürme ve sonuca ulaşma olarak bu döngü dörde ayrılmaktadır ve her atakta döngünün işleyişi aynı olmayabilir.

Çeşitli faktörler, döngünün hedefe ulaşmak için aşamalarının birini veya birkaçını tekrarlamasını gerektirebilir. Hedef sistemin niteliğine bağlı olarak saldırgan vazgeçene kadar veya istediği sonuca ulaşana kadar döngü adımlarında tekrara düşebilir. Örneğin sosyal mühendis saldırı esnasında daha önce kullanılmış başka bir yöntemi hatırlayıp onun bilgilerini de kullanmak isteyebilir.

Şekil 2.9’da bir sosyal mühendislik saldırısının gerçekleşmesi sırasındaki yaşam döngüsü verilmiştir.



Şekil 2.9. Sosyal mühendislik saldırısının yaşam döngüsü [57, 58]

Döngü adımlarını tek tek inceleyecek olursak Şekil 2.9'da;

- Bilgi Toplama (Information Gathering), saldırının ilk adımıdır ve diğer adımların varlığı için çok önemlidir. Çünkü başarı olasılığını artıran kısım burasıdır. Sosyal mühendisler hedef sistem hakkında bilgi toplayabilmek için zaman ve dikkatin çoğunu burada harcarlar. Belirledikleri çerçeve içerisinde saldıracakları sistem kullanıcısının alışkanlıklarını, becerilerini, kişisel özelliklerini vb. keşfetmeye başlarlar. Hedefi hassaslaştırmak için olası şifreler denenebilir ya da başka kullanıcılara verdiği cevapları aleyhine kullanıp hedef mağdur edilebilir. Sosyal mühendis bilgi toplamak için birçok araç, program, sosyal medya hesabı ve web sitesini kullanabilmektedir [58,59].
- İlişki Kurma ve Anlaşma (Establish Relationship and Rapport), bu adımda daha çok hedefle ilişki kurulmaya, bir şekilde iletişime geçilmeye çalışılır. Sosyal mühendisin kuracağı ilişkinin kalitesi hedefle iş birliği içerisine girip saldırıyı kısa yoldan gerçekleştirme imkânı sağlar. Saldırıya uğrayan kurbanı, duruma ve çevreye göre ilişki kurma tekniği de değişiklik göstermektedir. Bazen bir göz teması, gülümseme, yakın davranma, telefonda görüşme veya sosyal medya üzerinden sahte kullanıcı hesabı ile kurulabilecek bir arkadaşlık istenen ilişkinin kurulup anlaşma ortamını yaratabilmektedir [58, 59].
- İlişkiyi Sömürme(Exploitation), hedefteki son kullanıcı ile temasa geçtikten sonraki aşama sömürüdür. Saldırgan aslında burada hem topladığı bilgileri hem kurduğu ilişki bağını kullanmaktadır. Bu bağın şüphe uyandırmadan devam etmesi akabinde önemsiz gibi görülen bilgilerden faydalanılmayı getirir. Sosyal mühendisin yapması gereken zamanı iyi kovalamak ve edindiği bilgileri doğru taktik ile kullanmaktır. Şifre ve kullanıcı adını telefon üzerinden ifşa etme, virüslü bir e-posta ekini açma, şirket bilgisayarına kötü amaçlı dosya taşıyan bir USB flash sürücü takma gibi örnekler başarılı ilişki sömürme örneklerindendir [58, 59].
- Sonuca Ulaşma (Execution), döngüdeki son adım yürütme ya da uygulama adımı olarak adlandırılmaktadır. Sosyal mühendis tüm taktiklerini ve tekniklerini eyleme dönüştürmeye başlamıştır. Saldırı ya amacına ulaşır ya da şüphe uyandırmadan çeşitli nedenlerle sona erer. Saldırıyı sonlandırmak iyi bir tercih kabul edilmediği için bunun yerine hedef sistemde gizli kalmayı saldırganlar tercih etmektedir. Son adımda işi biten saldırgan ya da sosyal mühendis dijital ayak izlerini siler ve bir saldırının gerçekleştiğine

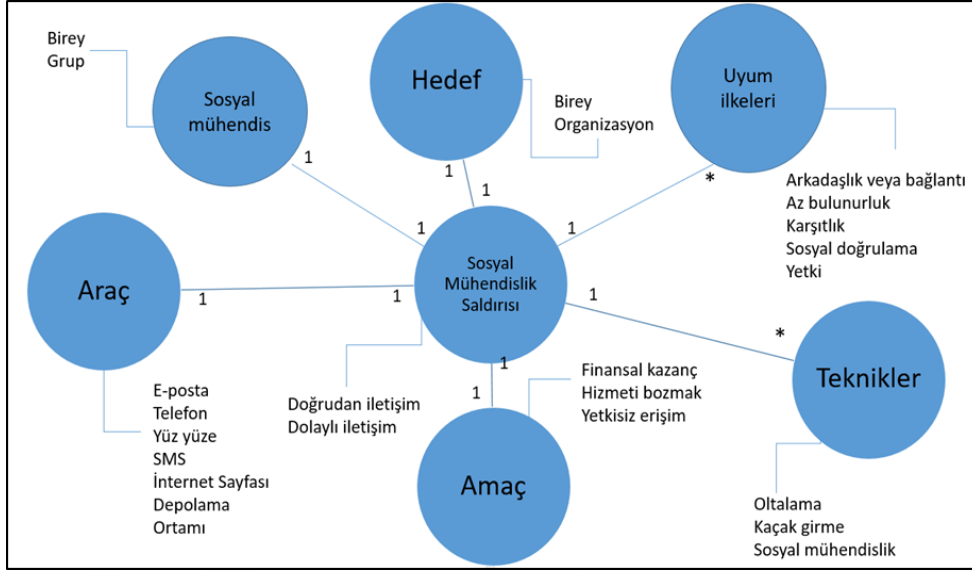
dair veya saldırıda bulunanın kimliğini açığa çıkaracak hiçbir delil bırakmadan iyi planlanmış bir çıkış stratejisi ile son hamlesini bu kısımda gerçekleştirir [58, 59].

2.4.2. Yaygın sosyal mühendislik saldırı türleri

Sosyal mühendisliğin en basit tanımı; saldırganın bir şirket, kurum ve kuruluşun ağına sızmak istemesidir. Sisteme girmenin en kolay yolu ise sorumlu sistem kullanıcısından izin istemektir. Elbette ki hedefe ulaşmak her zaman bu kadar basit değildir. Sosyal mühendislik atakları fiziksel, sosyal ve teknik içerikleri ile çok yönlü yapıya sahiptir. Gerçek bir saldırıda, farklı stratejiler ile sosyal mühendisler bunları kullanabilirler. Yazılım ve şifreleme güvenliği konusunda ne kadar önlem alınır alınsın, bir bilgisayar ağı teknik veya teknik olmayan saldırılara karşı asla tam olarak güvende olmayacaktır. Tam olarak güvenli olduğu düşünülen sistemi ise sistemin en zayıf halkası olan insan tehlikeye atacaktır. Sistem kullanıcısı, tanımadığı ya da amacını tam olarak bilmediği birine sisteme erişim izni verdiği sürece güvenlik duvarının, antivirüsün, kötü amaçlı yazılımdan koruma yazılımının veya şifreleme cihazının önemi kalmayacaktır. Sosyal mühendis doğru zamanda en zayıf halka insana, doğru yaklaşımla doğru saldırı tekniğini uygularsa hedefine ulaşması kaçınılmazdır.

Sosyal mühendislik, iyi bir yalancı olmakla alakalı değildir. Daha ziyade var olan birçok saldırı model ve bakış açısını, insan psikolojisini anlayarak kullanmaktır. Kevin Mitnick sosyal mühendislik kitabında bunu aldatma sanatı olarak adlandırır [55]. Konuya değinen yazarların genel ilkesine göre ise sosyal mühendislik saldırısı, *“çalışanlarla doğrudan ya da dolaylı iletişim kurmaktır ve sosyal mühendis bunu sağlamak için bir hedefe, bir ortama, bir amaca, bir ya da daha fazla ilkeye ve pek çok tekniğe sahiptir ”* [59].

Sosyal mühendislik saldırılarının ontolojik modeli Şekil 2.10’da verilmiştir.



Şekil 2.10. Sosyal mühendislik saldırısının ontolojik modeli [59]

Şekil 2.10'da görüldüğü üzere sosyal mühendislik saldırısı birden fazla aşamaya ayrılabilir ve her aşama yeni bir saldırı modeli gibi ele alınabilmektedir.

Tersine sosyal mühendislik (Reverse social engineering)

Tersine sosyal mühendislikte, saldırgan ya da sosyal mühendis hedefteki kurban ile doğrudan temasa geçmek yerine güven bağı kurmaya, karşı tarafa o güveni vermeye çalışır. Amaç mağdur tarafın yaklaşmasını, yardım istemesini sağlamaktır.

Tersine sosyal mühendislik kendi içerisinde üç önemli kısma ayrılır; sabote etme, hazırda bekleme ve sömürmedir [60]. Başlangıçta saldırgan şirketin, kurumun veya kuruluşun bilgisayar sistemini yavaşlatmaya veya durdurmaya yönelik girişimlerde bulunur. Örneğin virüs bulaştırmak, sistem ağını sabote etmek için bir yoldur. Ağ bağlantısı kesilen sistem kullanıcısının, yazılım uygulamalarına dahi bu yolla karmaşık müdahalelerde bulunmak mümkündür. Saldırımı gerçekleştirdikten sonra karşı tarafı gözlemlemeye başlayan sosyal mühendis yardım arayışında olan kurbanı yardım edebileceğini, bozulan sistemi düzeltebileceğini, güvenlik danışmanlığı yaptığını dair söylemlerde bulunur. Bir şekilde kurbanı ikna edip güvenini kazanan, kendi reklamını iyi yapan saldırgan ikinci adımı da başarıyla tamamlamış olur. Son kısımda saldırgan sorunu çözebilmek için bazı şifrelere, yetkilere ihtiyacı olduğunu söyleyerek istediği bilgileri edinir. Sistemin kontrolünü ele

geçirip istediği değişikliği yapması artık kaçınılmazdır [61]. Şekil 2.11’de tersine sosyal mühendisliğin hedef sisteme uygulanış adımları verilmiştir.



Şekil 2.11. Tersine sosyal mühendislik adımları

Şekil 2.11’i açıklamak gerekirse; tersine sosyal mühendislikte, sosyal mühendis sorun yaratır, sorunu çözecek kişi gibi hareket eder, sorunu kısa sürede çözerek kahraman konumuna gelir ve hedef sistemin yeni sahibi olur.

Kaçak girme (Piggyback rides)

Kaçak girme tekniği, hedef sistemde yetkili birinin bilmeden yetkisiz birinin güvenli kısma geçmesine izin vermesi durumudur. Sosyal mühendis yetkili bir çalışanı takip ederek içeri girmiş olur sonrasında güvenli binada çalışan gibi davranmaya başlar. Bu durumun en klasik örneği yağmurlu bir günde, sabah erken saatlerde sosyal mühendis elinde ağır koli taşıyan biri olarak kapıya gelir. Elleri dolu olduğu için giriş kartını gösteremeyeceğini ve kapıyı açamayacağını karşısındakine söyler. Böyle bir durum karşısında insanlar genellikle karşısındakine yardımcı olmak isteyecektir. Yetkili çalışan sorgulamadan güvenli kapıyı açar ve saldırganla kolaylıkla içeri girme şansı vermiş olur [61]. Başka bir kaçak girme yöntemi ise, saldırgan yardıma ihtiyacı olduğunu belirtir ve yetkili çalışandan dizüstü bilgisayarını kısa süre için ödünç ister. Ödünç alan saldırgan hızlı bir şekilde kötü amaçlı yazılımı sistem kullanıcısının bilgisayarına yükleyerek istediğini yapabilecektir.

Teknik konuşma (Technical talk)

Penetrasyon testi yapanlar veya kötü niyetli hackerlerin pek çoğu teknik bir geçmişe ve alt yapıya sahip kişilerdir. Doğal olarak teknik bir sosyal mühendislik saldırısında karşımıza bu teknikerlerin çıkması olağandır. Teknik bilgisini kullanan saldırganın karşı tarafı ikna etmesi çokta zor olmamaktadır [61]. Örneğin sosyal mühendis hedefindeki şirket, kurum ve kuruluşu arayarak kendisini yardım masası çalışanı veya bilgi teknolojileri personeli olarak tanıtır. Ardından güvenlik sızıntısı olduğunu, bazı kullanıcıların parolalarının deşifre olduğunu bu yüzdende kullanıcı şifrelerinin değiştirilmesini gerektiğini söyler. Daha güvenli bir şifre oluşturmak içinde kendisinin yardımcı olacağını da ekler. Buradaki saldırgan, çoğu kullanıcının bilmediği, duymadığı veya hakkında fikir yürütemediği teknik kavramları kullanarak karşı tarafı etkisi altına alır.

Hedefteki mağdurun parolasını değiştirmesini sağlayan saldırgan bu kez de yeterince güçlü bir parola olup olmadığını kendisinin kontrol etmesi gerektiğini söyler. Çalışan kendini güvene aldığını düşünürken aslında saldırgana kendi sistemini teslim ettiğinden habersizdir [62]. Önemli pozisyonlarda çalışan personeller bu tarz çağrılara karşı dikkatli olmalıdır. Arayan kişinin bahsettiği gibi kurumun bilgi işlem departmanında çalıştığına emin olmalıdır. Emin olduğu zaman bilgisayarına uzak bağlantı yapmasına izin vermelidir. Bağlantı esnasında kontrolü karşı tarafa verse dahi bilgisayar başından ayrılmamalıdır [63].

Oltalama (Phishing)

Oltalama veya kimlik avı saldırısı, hassas verileri ele geçirmek için genellikle gerçek sistem kimliğine bürünerek sahte e-posta, sohbet, web reklamı veya web sitesi biçiminde tasarlanan içeriğin hedefteki sistem kullanıcısının e-posta adresine link olarak gönderilmesidir. Bu iletiler karşı tarafın aciliyet veya korku duygusu içerisin de hareket etmesini sağlayacak şekilde hazırlanırlar. Oltalama da gönderilen içerik bir bankadan, hükümetten veya büyük şirketten çalışanın bilgilerinin teyit edilmesi amacıyla gelebilir. Bu sahte siteler ve senaryolar orijinalinden farksız tasarlanıp tüm yasal haklara sahipmiş izlenimi verir. Bazen son kullanıcıdan bir hesabın giriş bilgilerini “doğrulamasını” ister ve kusursuzca hazırlanmış bir giriş sayfasına yönlendirirler [63]. Bazen de son kullanıcının büyük bir ödülün kazananı olduğu söylerler ve ödülün verilmesi için bir banka hesabına erişim talebinde bulunurlar. Bu saldırı çok basit görülebilir, ancak birçok kullanıcı iyi tasarlanmış

bir banka hesap bilgisi ekranını karşısında gördüğünde banka bilgilerini vermektedir. Genellikle saldırganlar kurbandan kart bilgileri, kart şifreleri, parolalar, kişisel bilgiler gibi daha sonradan kişiyi zarara uğratabilecek hassas bilgiler istenmektedir [64].

Oltalama saldırısının bir diğer çeşitleri de whaling (balina avı) ve vishing (telefon oltalaması) saldırılarıdır. Balina avı saldırısı da, sosyal mühendis CEO, CFO, daire başkanı gibi üst düzey yöneticiyi veya profili yüksek kişiyi hedef almaktadır [63]. Saldırgan öncesinde bu kişiler hakkında internetten bilgi toplar. Genellikle şirketler, kurum ve kuruluşlar üst düzey yöneticilerinin özgeçmişlerini web sayfalarında yayınlar. Sosyal mühendis buralardan edindiği bilgiler doğrultusunda uygun saldırı senaryoları hazırlamaya başlar [63]. Örneğin yöneticinin mezun olduğu okul bilgisini kullanarak sahte bir mezunlar yemeği organizasyon maili yöneticiye gönderebilir. Mailde davete katılacak kişinin kimlik bilgilerini ya da kredi kart bilgilerini istemesi sonrasında muhtemeldir. Hedefteki yöneticinin böyle bir davetten şüphe duyma ihtimali çok düşüktür. Nitekim yöneticiler veya yüksek profilili hedefler, haklarında çok fazla bilgi olması nedeniyle sosyal mühendislerin ikna edici hedef olarak seçme ihtimallerini kolaylaştırmış ve balina avı saldırısının da giderek popüler hale gelmesine yol açmıştır. Fakat saldırganın odaklanması gereken tek bir hedef olduğu için oltalama saldırısına göre çok daha zordur.

Oltalama veya balina avı (sazan avı) saldırısında başarılı olamayan ya da istediğini elde edemeyen sosyal mühendisin başvurduğu diğer yöntem ise telefonla oltalama saldırısıdır. Bu saldırıda da hedef hem normal çalışanlar hem de üst düzey yönetici veya profili yüksek kişilerdir. Hedefi ile iletişim kurabilmek için sosyal mühendis araç olarak bu kez telefonu kullanır [63]. Örneğin sosyal mühendisler, kurbanın şirketi veya şirket bankası gibi davranarak önceden kaydedilmiş mesaj veya çağrı kaydı ile iletişim kurar. Ardından hazırladığı senaryoya göre karşı tarafın cep telefonu numarasını, kredi kartı bilgilerini, iş yeri telefon numarasını veya sosyal güvenlik numarasını gibi hassas verilerini öğrenmeye çalışır. Son kısımda bazı işlemleri sistemlerine not ettiklerini, istedikleri zaman iptal edebileceklerini ve eğer isterseler kendilerine yeni kart gönderebileceklerini söyleyerek aramayı sonlandırır. Bu anlatılanların hepsi sahtedir, gerçekte hedefteki kurbanın banka hesabına erişim gerçekleşmiştir. Günümüzde kendilerini polis, jandarma, savcı olarak tanıtır kişilerle iletişim kurmaya çalışan ya da telefon, araba, takım forması kazandınız şeklinde sesli mesajlarla da sesle oltalama saldırısı yapılmaktadır.

Sosyal medya

Sosyal medya ya da sosyal ağ saldırıları günümüzde sıkça karşılaşılan sosyal mühendislik saldırı türlerindendir [63]. Facebook, MySpace, Twitter, Instagram, LinkedIn gibi daha birçok sosyal ağ siteleri artan kullanım oranları ile sosyal mühendislerin gözdesi haline gelmiştir. En basit hali ile bu siteler sosyal mühendis için bilgi havuzudur. Çünkü yalnızca bazı sayfalara tıklayıp birkaç arama yaparak bu tür sitelerden hedefteki kurban hakkında fazlasıyla bilgi edinebilirler [61]. İnsanların nerede çalıştıkları, ne yapmayı sevdikleri, hangi gruplara üye oldukları, ne tür müzikler dinledikleri, hobileri, fobileri ve daha fazlasını edinmek sadece birkaç dakikalarını alabilmektedir [63]. Edindikleri kişiye özel bilgileri sosyal mühendisler, sahte kullanıcı hesapları ile internette yayımlayabilecekleri gibi insanların anlık yer bildirimi yaptığı uygulamalarla da hedefin yakınlarında olup ona göre saldırı senaryosu da hazırlayabilir.

Örneğin sosyal mühendis, LinkedIn gibi profesyonel bir sosyal medya sitesinde bir şirket için işe alım görevlisi gibi davranır ve hedefine özel bir işe alım mesajı gönderir. Saygın bir şirkette, inanılmaz görünen bir pozisyon hakkında hedefine bilgilendirmeler yapar. Hedefi hakkında daha önce topladığı verilerden yola çıkarak aradıkları çalışma arkadaşı olduğunu söyleyip başvuru sayfasına yönlendirir. Başvuru sayfası aslında kimlik hırsızlığı yapan sözde iş sitesidir. Kurbanın bilgileri ile artık istedikleri her şeyi yapabilirler.

Sosyal medya ya da sosyal ağ saldırısından korunmak için önemli husus vardır. Bunlar [63];

- Kişisel verileri sosyal medyada paylaşmak konusunda dikkatli olunmalı,
- Online arkadaşlık sitelerinde arkadaş olunan kişilerin kimliklerinden emin olunmalı,
- Kaliteli markalarla bile iletişim kurulduğunda dolandırıcılık tehlikesini göz önünde bulundurulmalı,
- Güncel antivirüs kullanılmalı,
- Parola ve şifre güvenliğinde hassas olunmalı, güçlü ve tahmini zor şifreler üretilmeli gibi dikkat edilmesi gereken noktalar vardır.

Duyu dilsel programlama (Neuro linguistic programming)

İyi bir sosyal mühendis, insan aklının nasıl manipüle edileceğine dair güçlü bir kavrayışa ve düşünme yapısına sahiptir. NLP (Neuro Linguistic Programming) saldırısı, doğru yapıldığında oldukça başarılı sonuçlar veren, insanları psikolojik araçlarla kullanan sosyal mühendislik saldırı türüdür. NLP teknikleri ile verdiğimiz tepkileri, davranışları değiştirebilmek mümkündür [61]. Duyu dilsel programlama da hedefteki kişinin nörolojik süreçleri, dili ve öğrenilmiş davranışları üzerinde durulur. Duyu dilsel programlama başlangıçta iyileştirici özelliğinden yola çıkarak tedavi amaçlı kullanılmak üzere tasarlanmış olsa da zamanla sosyal mühendisler insanları manipüle etmek, istedikleri çoğu şeyi yaptırmak için kullanmaya başlamışlardır [65].

Bir satış görevlisi mağazadaki ürünleri müşterilere beğendirmek için üstün performans sergiler, sosyal mühendiste karşı tarafı etkilemek için aynı yolu izler. Örneğin, sosyal mühendis NLP tekniği ile saldıracaksa hedefteki kişiye bilinçaltı mesajları vermek için beden dilini kullanır, dikkatli kelimeler seçer aynı zamanda karşı tarafın sesini, nefes hızını, hareketlerini ve kelime bilgisini de kontrol ederek hareket eder [61]. Bunları gözlemleyen saldırgan konuşma esnasında karşı tarafın ruh halini etkilemeyi başarır. Sohbet esnasında kişiye hafifçe dokunarak, gülümseyerek veya koluna girerek yakın davranıp olumlu imaj çizerler. Tüm bu dokunsal, görsel ve sözlü eylemler duyu dilsel programlamada kullanılan karşı tarafı çerçeveleme hareketidir. Kontrol altına alan ve istediği gibi bir konuşma çerçevesi hazırlayan sosyal mühendis bu konuşmayı yavaş yavaş istediği yöne çekerek istediği bilgileri edinmeye başlar.

Özetle bu teknikte, saldırgan kişilik stilleri ve davranış profili ile uyumlu giderse ve kendisini kurbanı göre düzenlerse başarılı olmaktadır. Bol taktik ve pratik gerektiren bu sosyal mühendislik türünün başarılı olma ihtimali çok yüksektir [61].

Çöp karıştırma

Çoğu insanın önemsiz olarak gördüğü bilgiler sosyal mühendisler için öyle değerlendirilmemektedir. Saldırı esnasında işe yarar bilgiler bulabilmek için şirket, kurum ve kuruluşların, aynı zamanda burada çalışanların çöpleri saldırganlar tarafından karıştırılmaktadır. Çoğu zaman çöpler halka açık yerlere bırakılırlar, bunları kurcalamakta

yasadışı bir durum söz konusu değildir. Dışarıya bırakılan çöplerin sorumluluğundan kişiler ve kurumlar mesuldür.

Kulağa pek hoş gelmeyen bu sosyal mühendislik saldırı türü saldırganların vazgeçemediği tekniklerdendir ayrıca veri getirisi küçümsenmeyecek kadar çoktur [90]. Önemsiz görülen belgeler, dokümanlar, yazım yanlışı yapıldığı için atılan raporlar, küçük kâğıtlara yazılan notlar, telefon numaraları, CD, disket gibi hassas veri içerebilecek materyaller, büyük şirketlerin organizasyon şemalarını içeren el kitapçıkları, toplantı takvimleri, kullanıcı isim ve parolalarının dökümleri gibi pek çok veri kurbanın çöpünde bulunabilir. Ünlü sosyal mühendis Kevin Mitnick çöp karıştırma tekniği hakkında, *“Yeni rehberlerin çıktığı akşamlarda çöp ziyaretleri yapardım, çünkü çöp bidonlarında düşünmeden atılmış yığınla eski rehber olurdu. Başka tuhaf zamanlarda da ilginç bilgi cevherleri içerebilecek not kâğıtları, mektuplar, raporlar bulmak içinde giderdim ”* demiştir [55].

Çöp karıştırma tekniğinden korunmak için [63];

- Kritik veriler sınıflandırılmalı ve ona göre imha edilmelidir.
- Kâğıt öğütücü makinaların kullanılması tercih edilmelidir.
- Şirket, kurum ve kuruluş dışındaki büyük çöp bidonları kilitlenmelidir.
- Mümkünse çöp bidonları organizasyon içerisinde olmalıdır.

Omuz sörfü

Sosyal mühendislik saldırı türlerinden en sık karşılaşılanlardan biride omuz sörfüdür. Saldırganın, hedefindeki kurban parola yazarken, çok özel bilgilerini tanımlanırken veya erişim kısıtlı sistemlere erişim sağlarken onu izlemesi olarak tanımlanmaktadır. Günlük hayatın her alanında böyle bir saldırıya maruz kalmak mümkündür. Örneğin işyerinde meraklı ya da kötü niyetli olarak omuz sörfü gerçekleştirmeye çalışan insanlar var olabilir. Bu kişiler; iş arkadaşlarımız, amir ve müdürlerimiz, işyerine dışarıdan gelen kişiler vb. olabilir [66].

Dışarıda otururken, restaurantta yemek yerken, herhangi bir yerde arkadaşımızı beklerken, otobüste yolculuk ederken yanımızda oturan ya da arkamızdaki kişiler tarafından da omuz

sörfü yapılabilir. Çoğunluk anlık mesajlaşmalarımızı okumaya çalışırlar, facebookta incelediğimiz gönderilere, twitterdan okuduğunuz tweetlere göz atarlar. Sosyal medya hesaplarında ki kullanıcı adını bu şekilde öğrenip bağlantı kurmaya çalışan pek çok insan vardır. Ya da ATM (Automatic Teller Machine)’lere işlem yapmaya gidildiğinde de kredi kartı veya bankamatik kartının şifresini öğrenip hırsızlık yapabilmek için arka tarafta bekleyenler tarafından omuz sörfüne maruz kalınabilir [66]. Böyle durumlarda şifrenizi girmeyebilir, çok acil durumda ise tuşlara hızlıca basabilirsiniz. Yanınıza biri geldiğinde ve görmemesi gereken şeylerle meşgulseniz ekranınızı değiştirme ya da monitörü tamamen kapama yöntemine gidebilirsiniz. Masanızda bulunan önemli evrakları mümkün olduğunca dağınık ve açıkta bırakmamak, ters yüzünü çevirerek koruma altına almakta korunma yollarından olabilir [66].

Omuz sörfü görüldüğü üzere sadece sosyal mühendisler tarafından gerçekleştirilmeyebilir. Çevredeki sıradan birçok insan da uygulayabilmektedir. Bunun içinde normal zamanlarda dahi çok dikkatli olunmalı, gizli verilerle işlem yapılırken izlenip izlenilmediğine kişiler emin olmalıdır.

2.4.3. Bazı popüler sosyal mühendislik teknikleri

Bir sosyal mühendis hedefindeki kurbanı etkilemek ve yönetmek zorundadır. İsteddiği bilgileri elde etmek için her türlü yolu deneyecek olan sosyal mühendisler, ahlaki sınırlara etik değerlere dikkat etmezler. Amaçları biran önce hedefleri hakkında bilgi toplamak ve istedikleri saldırıyı gerçekleştirmektir.

Kendini sevdirmeye ve karşılık bekleme tekniği

Sosyal mühendis veya saldırgan kendini sevdirmeye ve karşılık bekleme tekniğinde (reciprocation) hedef seçilen kurban ile yakın temasa geçerler, kişisel bağlantılar kurarlar, kurbanla ortak ilgi alanları, inançları ve yaşantıları varmış gibi gösterirler [67]. İnsanlar kendileri ile ortak özellikleri olan kişilere karşı çoğu zaman yakınlık duygusu hisseder. Bunu bilen sosyal mühendisler bu durumu kendilerinden tarafa kullanmayı ihmal etmeyecektir. Öncelikle kurbanın bireysel ilgi alanlarına yönelik (sevdiği filmler, müzikler, yemekler, tuttuğu takım, hobileri, fobileri vb.) ortak noktalar belirlemeye çalışarak, karşı tarafa güven duygusu verilip ikna yoluyla saldırı gerçekleştirmek sosyal mühendisin bu teknikte

amacıdır. Bunu da örneğin kurbana değerli bir hediye vererek ya da verebileceğini söyleyerek veya ciddi bir işini çözerek, yardımcı olarak karşı tarafta yapılan iyiliğe karşılık vermeliyim algısı oluşturarak gerçekleştirir. Kendini karşı tarafa borçlu hissedenden kurban aralarında ki yakınlık bağına da güvenerek saldırganın isteklerini yerine getirir [63].

Evet-Evet tekniği

Sosyal mühendis hedefiyle bağlantı kurarken kurbanın zihninde olumlu bir izlenim bırakmak isteyebilir. Bu sayede istediği bilgileri karşı taraftan edinmesi olasılığı artacak, başarıya ulaşması kolaylaşacaktır. Evet- evet tekniğinde (yes-yes technique) hedef kişi veya kitleye “evet” cevabı verme ihtimali yüksek sorular sorulmaya başlanır. Örneğin “*hayatta başarılı olmak istiyorsun değil mi?*”, “*geleceğini teminat altına almak ister misin?*”, “*daha iyi bir işte çalışmak ister misin?*” gibi sorular karşı tarafın çoğunlukla evet yanıtı vereceği sorulardır [61]. Böylece uygun evet yanıtı altyapısı oluşturulmuş olur. Sırada hedefteki kurbanı ele geçirecek asıl soruyu sormak vardır.

Saldırı senaryosuna göre sosyal mühendis, “*o halde bizim firmamızla çalışmak istersiniz değil mi?*”, “*bize güvenerek sistemlerinizi emanet edersiniz değil mi?*”, “*yarın sizlerle sistemsel bir çalışma yapmamızda sakınca yoktur diye düşünüyorum değil mi?*” şeklinde sorular yöneltebilir [61]. Hedefin zihninde oluşturulan evet yanıtı verme dürtüsü burada da devreye girer ve cevabı “*evet*” olur.

Art arda, soluksuz bir şekilde yöneltile sorular, hedefteki kurbanın karşı taraftan gelen bilgileri ayrıntılı bir şekilde bilişsel işleme sokmasına olanak tanımamakta ve kestirme yoldan yapılan bilişsel işlem olmaktadır [68].

Önce ver sonra geri al tekniği

Önce ver sonra geri al tekniğinde (throw a ball technique) hedefte ki kurbana son derece cazip gelecek koşullar vaat edilir (ürün için oldukça düşük bir fiyat, uygun ödeme koşulları sunulması gibi) [69]. Hedefteki kişiye önerilen vaatler eğer istediği yönde, aklını karıştırmaya yetecek vaatlerse hedef önerilen yeni tutuma sorun yaşamadan bağlılık geliştirir. Saldırgan vaatlerinden sonra bir müddet hedefteki kurban ile kurbanın hayalleri

arasında bir bağ kurulmasını bekler. Kurban iyice bağıllık gösterdiği anda saldırgan çeşitli sebepler öne sürerek vaatlerinde değişikliğe gider ya da onları gerçekleştiremeyeceğini söyler. Önerilen tutuma bağıllık gösteren ve vazgeçmek istemeyen kurban geri dönmek istemeyeceği için saldırganın ona sunduğu yeni teklifi sorgulamadan kabul eder [63]. Örnekle açıklamak gerekirse; alışveriş için bir mağazaya gidildiğinde görevli öncelikle müşteriye bir kıyafet beğendirir, ardından çok yakıştığını, alması gerektiği söyler. Müşteri aynada kıyafete tekrar tekrar bakar ve ona bağlanmaya başlar. Ödeme esnasında etiketin yanlış basıldığı gerçek fiyatı olmadığı ifade edilir. O süre zarfında formlar doldurulmuş, taksit koşulları konuşulmuş olur. Bu gibi durumlarda duygusal bağıllığın artmasına elbette neden olmaktadır. Müşteri kıyafeti almaktan vazgeçmez, sunulan yeni koşullar ve fiyat üzerinden kıyafeti alıp mağazadan çıkar. Güncel hayatta sıkça karşılaştığımız bu teknik sosyal mühendislikte kurbanı ikna etmek için saldırı tekniği olarak sıkça kullanılmaktadır.

Etkili konuşma

Sosyal mühendislik saldırılarında başarılı olmak kadar başarıya azimli kişilerle saldırı senaryosunu harekete geçirmek de büyük önem taşımaktadır. Sosyal mühendislik, genellikle en zayıf halka olan insana yönelik olduğu için insanı etkilemek çok önemlidir. İyi konuşabilen, etkili cümleler kurabilen ve hitabeti yüksek sosyal mühendislerin hedeflerine ulaşması daha kolay olabilmektedir. Etkisi altına aldıkları insanlara istediklerini yaptırma ihtimalleri de hitabet güçleriyle doğru orantılıdır. Araştırmalara göre konuşma sanatında ilerlemiş biri yeni girdiği bir ortamda daha özgüvenli hareket edebiliyor, daha kolay kararlar alabiliyor, ekip çalışmasına daha yatkın olabiliyor, sosyal temaslarda daha başarılı adımlar atabiliyor ve kendi kararlarını başkalarına daha kolay uygulatabiliyor. Sosyal mühendislikte de saldırgan hedefi etkileyebilmek için etkili konuşmanın püf noktalarını doğru şekillerde kullanır. Duygu ve düşüncelerini hedefteki kurbana başarılı şekilde pazarlar. Ses tonu, kullanılan sözcükler ve dildeki üslup iletmek istenilen mesajın, istenilen hissi uyandırarak hedefe ulaşmasını sağlar [63].

2.4.4. Sosyal mühendislik saldırıları nasıl gerçekleşir?

Sosyal mühendislik saldırı tekniklerinden popüler olan birkaç tanesine önceki başlıklarda değinilmiştir. Bu saldırı teknikleri, listelerle sınırlı olmaktan çok, sosyal mühendisin veya saldırganın kararlılığıyla ve yaratıcılığıyla sınırlı olabilmektedir. Gerçek dünyada yaşanan

ve her geçen gün artan tipik dolandırıcılık yöntemlerinin de uygulanmasıyla, siber saldırılarda olası saldırı tekniklerinin sayısı ve tipleri de artacaktır. Var olan ve artmakta olan sosyal mühendislik saldırı tekniklerinin dijital dünyaya aktarılması da elbette git gide önemli hale gelecektir. Bu kısımda da saldırı tekniklerinin nasıl uygulamaya geçtiğine, bazı yöntemler üzerinden değinilmektedir [64].

Sahte senaryolar uydurmak

Sosyal mühendislik saldırıları gerçekleştirilirken öne çıkan başlıklardan birisi, nitekim sahte senaryolar uydurmak (pretexting) olmaktadır. Gizli verilere ulaşmak için kişinin kendini başka biri olarak tanıtmaları şeklinde tanımlanır [70]. Telefonla gerçekleştirilebildiği gibi birebir iletişim ile gerçekleştirilmesi mümkündür. Karşı tarafa yalan söylemekten öte yeni bir kimlik yaratarak o kimliğe bürünme ve hedefteki kurbanı manipüle etmektir. Sosyal mühendisler olmadıkları kişileri ve rolleri taklit ederek hedefteki kurbanla iletişime geçer. Amaçları, sahte bir senaryo kurgulayarak edinmek istedikleri bilgileri içine serpiştirmek ve hedefteki kişiden bu bilgileri almaktır. Kurmaca senaryoları tek boyutlu değildir yani değişime açıktır ve usta bir sosyal mühendis hedefle kurduğu iletişimin gidişatına göre senaryoda değişikliğe gidebilir. Eğer sosyal mühendis saldırı öncesinde hedef sistem ve kullanıcı hakkında yeterli araştırmayı yapmışsa elindeki bilgilere göre senaryoda değişiklikler yapmasında sorun olmayacaktır.

Sahte senaryo kurgulayarak karşı taraftan istenilen bilgileri edinme yöntemini sadece sosyal mühendisler değil avukatlar, doktorlar, terapistler ve NLP uzmanları da karşı tarafı huzursuz etmeden haklarında bilgi edinmek için sıkça kullanmaktadır. Konuyu bir örnekle açıklayacak olursak; bir sosyal mühendis müşteri gibi geldiği bankada önceden hakkında araştırma yaptığı çalışanın yabancı film izlemeyi çok sevdiğini öğrenir. Sahte işlemleri sırasında görevliyle sohbet etmeye, güven vermek için de kendinden bahsetmeye başlar. Bir müddet sonra sevdiği şeylerden bahsederken yabancı film izlemeyi çok sevdiğini söyler. Banka çalışanı kendiyle benzer özelliği olan müşteriye daha yakın davranmaya ve izledikleri filmler hakkında konuşmaya başlar. Müşteri kılığındaki sosyal mühendis beklediği fırsat eline geçince elinde çok etkileyici, kesinlikle beğeneceği bir yabancı film olduğunu ve isterse filmi banka çalışanına gönderebileceğini söyler. Teklifi kabul eden çalışana birkaç gün sonra kargo ile film gelir. Saldırgan bu kez de telefonla arayarak filmin sorunsuz gelip gelmediğini hemen kontrol etmesini ister. Ofisteki bilgisayarında filmi çalıştıran banka

çalışanı arka planda film ile birlikte zararlı yazılımın da çalıştığından habersizdir. Bankanın sistemi artık ele geçirilmiştir [70]. Görüldüğü gibi kurgu bir senaryo ile saldırgan teknik herhangi bir araç kullanmadan hedefine kolaylıkla ulaşabilmektedir.

Güvenli kaynak olduğuna ikna etmek

Sosyal mühendis, hedefine ulaşmak için kurban seçtiği kişi veya kişilere yönelik saldırısını güvenilir ya da doğruluğu sorgulanamaz bir kaynaktan gerçekleştirir. Genellikle e-posta, telefon ve hatta yüz yüze olmak üzere çeşitli şekillerde uygulanırken, sosyal mühendis temelde kendini güvenilir bir kaynak olarak gösterme çabasındadır [64]. Bu sayede kurban bir saldırıya maruz kaldığını anlamayacak belki de siber saldırıya uğrandığı açığa çıktığında kendinden kaynaklandığını dahi tahmin etmeyecektir.

Örneğin sosyal mühendis ya da saldırgan gönderdiği iletinin şirket, kurum veya kuruluşun bilgi işlem dairesinden geldiğine ikna etmek isterse, aynı birimin önceden gönderdiği bir ileti şablonunu taklit edebilir ve zararlı bir yazılımın olduğu sayfaya yönlendirebilir. Çalıştığı yerin bilgi işlem dairesinden aynı isim ve logo (ayırmaç) ile gelen bu iletiden hedefteki kişi veya kişiler şüphe duymayacak ve bağlantı adresine tıklayacaktır. Amaç zaten hassas veriyi ele geçirmek, zarar vermek ya da kullanıcıyı sahte web sayfasına yönlendirmek, zararlı yazılımı ofis bilgisayarına kurdurmak gibi hatalı bir işlem yapmaya sevk etmektir.

Güven kazanma yöntemiyle bilgi edinmek

Sosyal mühendis veya saldırgan saldırıya geçmeden önce hedefinde ki kurbanla güveninin sağlayacak şekilde iletişime geçmeye çalışır. Bağlantıyı iş sırasında ya da iş dışından kurarak kurbanın güvenini kazanan sosyal mühendis bu yöntemle kurbanı ikna ederek bilgi edinir veya yaptırmak istediklerini karşı tarafa yaptırır [64]. Burada önemli noktalardan biri saldırgan, çoğunlukla herhangi bir personelle değil sistemlere erişim yetkisi olan personellerle güvene dayalı arkadaşlık kurma, ortak zevkleri ve beğenileri varmış gibi hareket etme yoluna gitmektedir.

Truva atları (Trojanlar) kullanmak

Truva atı efsanesi ve Truva atı zararlı yazılım kodunun her ikisinin de eski zamanlara dayandığı düşünülmektedir. Elbette ki Yunanlıların yıllarca süren kuşatmasını zafere ulaştıran Truva atı efsanesi siber saldırganlarında dikkatini çekmiştir. 1974 yılında ilk kez bilgisayar tehdidi olarak ortaya çıkan teknik adını tüm zararlı yazılım sınıfına verecek kadar önemsenmiştir. Zararlı yazılımlara tarihi bir olayın benzetmesinin yapılmasının nedeni, güvenli olmayan kaynaklardan gelip zararsız bir işlevi varmış gibi görünmesi ve indirilen programlarla, dosyalarla veya şüpheli kaynaklarla gönderilen yazılımları beraberinde hedefteki sistemlere yerleştirmesidir [64].

Son zamanlarda ise yayılımını sıkça sosyal medya ağları üzerinden gerçekleştirmektedir. Bilgisayarını ya da cep telefonunu çoğunlukla sosyal ağlar için kullanan kullanıcılarda basit bir linke tıkladığı veya ücretsiz bir uygulama indirmek istediği zaman daha çok Truva atı saldırısına uğradığı görülmektedir.

Truva atı ile gerçekleştirilen sosyal mühendislik saldırılarında hedef sistem kullanıcıları yeterli seviyede güvenlik önlemlerine sahip olduklarına inandırılır bir anlamda uyutulurlar. Gerçekte büyük yatırımlar yapılarak oluşturulan güvenlik önlemleri, insan psikolojisi üzerine oynanan sosyal mühendislik oyunları ile beklenmedik bir anda devre dışı bırakılabilmektedir.

2.4.5. Sosyal mühendislik saldırılarının hedefleri kimlerdir?

Şirket, kurum ve kuruluşlara yönelik yapılan sosyal mühendislik saldırılarında, saldırganın kendine seçtiği, suiistimal edebileceği bir hedef personel kitlesi vardır.

Sosyal mühendislerin saldırılarında hedef seçtiği kişilere bu kısımda değinilmektedir.

Doğrudan ulaşılabilir personeller

Şirket, kurum ve kuruluşun dışı bakan yüzü olarak tanımlanan, işi gereği müşterilerle ya da sağlayıcılarla iletişime geçen personellerdir. Bunlar müracaat görevlileri, teknik servis elemanları, güvenlik görevlileri veya çağrı merkezi çalışanları olabilmektedir [71]. Bu gibi

pozisyonlarda çalışan personele bilgi güvenliği ve siber güvenlik konularında sıkı eğitimler verilmesi gerekmektedir.

Üst düzey yöneticiler ve önemli personeller

Şirket, kurum ve kuruluşlarda görevleri gereği ayrıcalıklı yetkilere sahip ya da hassas verilere çeşitli sebeplerden dolayı erişim hakkı olan personeller sosyal mühendislerin en çok hedef aldığı kişilerdir [64]. Görevleri gereği bu personeller bir takım gizli bilgilere, sistem üzerinde sınırsız erişim yetkisi sağlayan şifrelere sahiptir. Kendilerine verilen şifreleri hatırlamakta zorluk çektikleri ya da işlerinin yoğunluğu sebebiyle unuttukları için çok basit şifreler kullanmaları, hatırlamak için bir yerlere not halinde yazmaları veya yanlarında çalışan sekreter, hizmetli gibi kişilere emanet etmeleri bu personellerin sosyal mühendislik saldırılarının hedefi haline gelmesinde en önemli etkenlerdendir [71].

Yardımsever personeller

Bu personeller gerek çalıştıkları yerde gerekse diğer insanlara yardım etmeyi seven, destek vermekten zevk alan kişilerdir. Çoğu zaman görev ve yetkilerini aşarak bu yardımlarda bulunan personeller sevecen bir kimliğe bürünerek yetki ve itibar elde etmeye çalışabilirler. Amaçları iyi bir şeyler yapmak olan yardımsever personeller saldırganlarında da dikkatinden kaçmamaktadır [71]. Bundan dolayı bazen yardım isteyen müşteri görünümlü bir saldırganla da denk gelebilirler. Saldırgan sisteme giriş yapamadığını söyleyerek giriş hakkı isteyebilir veya hesabının kilitlendiğini acil işlem yapması gerektiğini iddia edebilir. Devamında yardım isteyen saldırgan, ayrıca personele işin uzmanı olduğu, sadece onun bu işi çözebileceği havası vererek birçok bireyin zayıf noktası olan reddedememe düzeyini etkilerler. Hassas bilgileri daha iyi koruyabilmek için personellerin yetki sınırları iyi belirlenmeli, bu sınırlar içerisinde hareket etmeleri istenmelidir.

İşe yeni başlayan personeller

Bunlar daha çok desteğe muhtaç personeller veya kullanıcılarıdır. Çalıştıkları yere yeni başlayan personellere hizmetlerden yararlanırken bazı sistemlere erişim hakkı da verilmektedir. Ancak sistemlerin tam olarak nasıl kullanıldığı konusunda yeterli bilgiye sahip olmadıkları için saldırganların hedefi olmaktadır [71]. Bu personeller yardıma

ihtiyaları olduėunda kendilerine destek verecek personel ile saldırı iin hazırda bekleyen sosyal mhendisi ayırt edemeyebilirler. Kendi kullanıcı bilgilerini ve Őifrelerini ok kolay karşı tarafla paylařarak sistemlerini tehlikeye atabilirler. Tm olumsuz senaryoların nne geebilmek iin iře yeni bařlayan personele yetkiler verilemeden nce gerekli eėitimler verilmeli, veri gvenliėi konusunda gerekli řartları saėladıktan sonra yetkilendirmeler yapılmalıdır.

Baėlılık seviyesi dřk personel

řirket, kurum ve kuruluřun hedef ve politikalarını kavraması zor olan, aktif olarak alıřmasına raėmen alıřtıėı yere baėlılıėı zayıflamıř belki de iřten ayrılmayı dřnen personellerdir. Genellikle sıradan memurlar, gvenlik grevlileri, resepsiyon grevlileri ve hizmetliler sosyal mhendislerin en kolay saldırı hedefidir [71]. Saldırganın aėına dřen, gvenlik politikalarını ihlal eden alıřanlardır. Bazen de insani hırslarına yenik dřp saldırganın ne srdė byk vaatlere inanan personeller alıřtıkları yere ait hassas verileri dıřarıya sızdırıp zarar verici eylemlerde bulunabilir. Yaptıkları grevin bilincinde ve sorumluluėunda olmayan bu personeller bilinli veya bilinsiz saldırganın onlara sorduėu sorularda neyi elde etmek istediėini anlamayarak cevap vermektedir [71]. İnsan kaynakları departmanı personel denetimini iyi yapmalı ve olumsuz davranıřlar sergileyen personelleri yneticilerine bildirmelidirler.

2.4.6. İnsan faktr

İnsan faktrn bilgisayar ve bilgi gvenliėi kapsamında iliřkilendirme ve analiz metotları geliřtirme, halen zerinde alıřılan tamamlanmamıř bir konudur. nceki alıřmaların oėu gvenlik metodu geliřtirmek iin akıllı kartlara, Őifrelere veya biyometrik cihazlara odaklanmıřlar esas organizasyonlar iin insan faktrnn nemini gz ardı etmiřlerdir. Arařtırmacılar ve geliřtiriciler uzun sre bilgisayar ve bilgi gvenliėinin etkin bir řekilde saėlanmasında en byk engelin insan olduėunu ya fark edememiř ya da ok az fark etmiřtir. řimdilerde ise insan, teknoloji ve organizasyon kavramaları birbirlerinden ayrı deėerlendirilmemektedir. nk organizasyonların finansal kayıplarının %80'i gvenlik ihlallerinden kaynaklanmakta ve bu ihlallerin byk oėunluėu kullanıcı, geliřtirici, paydař, tedariki gibi eřitli rollerle srece dhil olan insanlardan kaynaklanmaktadır [4].

Bilgi güvenliği için ortaya konan altyapı artan veri miktarı ile artık eskisi kadar yeterli değildir. Organizasyonların, bilgi ve iş gücünü ilerletmek için siber güvenliğin insan faktörü boyutunu da ciddi şekilde ele alması gerekmektedir. Siber güvenliğin insan faktörü, insan hatasından kaynaklı siber saldırı veya veri ihlali olması ile sonuçlanan eylemleri veya olayları ifade eder. Parolaların paylaşımı, zayıf yama yönetimi, uzaktan çalışmalardaki artış, güvenli olmayan URL'lerin çift tıklanması ve kişisel bir cihaz aracılığıyla kurumsal erişim sağlanması güvenlik tehdidine yol açan birkaç insan hatasıdır.

Yapılan araştırmalar insan faktörünün siber güvenlik risklerini artırma konusunda ki etkisinin göz ardı edilmeyecek şekilde olduğunu ve organizasyonların endişe duymaları gerektiğini sıklıkla vurgulamaktadır [63]. Çalışanların çoğu dikkatsizlik, kullanım özenini göstermeme ya da yaptıkları işi koruma konusunda gerekli eğitime sahip olmadıkları için organizasyonun verilerini veya sistemlerini riske atmaktadır. Kaspersky Lab and B2B International tarafından dünya çapında 5000'den fazla işletme üzerinde yapılan çalışmanın sonuçları da bunu destekler niteliktedir. Çalışmanın sonuçlarına göre işletmelerin %52'si çalışanları tarafından risk altındadır [72].

İşletmelerin %57'si, her geçen gün değişen türleri ile karmaşık hale gelen siber saldırılara karşı oluşturdukları zırhlarındaki zayıflığın kendi çalışanlarından kaynaklandığını bilmektedirler. İnsan faktörü ve çalışan davranışı, içeriden risk altına girme ve güvenlik korkusuyla doğru orantılıdır. Aynı çalışmada belirtildiğine göre, çalışanların %47'si çalıştıkları yerin hassas verilerini mobil cihazları üzerinden paylaşmışlar, %46'sı içerisinde veri barındıran fiziksel cihazların kaybına sebep olmuşlar ve %44'ü BT (Bilgi Teknolojileri) kaynaklarını uygunsuz şekilde kullanmışlardır [72]. Elbette çalışanların pek çoğu çalıştıkları yeri tehlikeye attığının farkında veya bilincinde değildir. Özellikle küçük ölçekli işletmelerde bilgi güvenliği, BT kaynakları kullanımı, siber güvenlik politikaları vb. konularda çalışanlar esnek ve denetimsiz bırakılmış, gerekli eğitimler sağlanmadığı içinde yukarda bahsedilen yüzdeler yüksek çıkmıştır.

Siber güvenlikte insan faktörünün neden olduğu saldırı risklerini en aza indirmek için önerilen birkaç yol aşağıda verilmiştir.

- Birinci yol, çalışanları sosyal mühendislik konusunda eğitmektir. Sosyal mühendislikte insanların çeşitli yollarla manipüle edilerek gizli bilgileri açığa çıkarmaları

amaçlanmaktadır. Sosyal mühendislik ile sistemlere yetkisiz giriş için pek çok yol olduğundan önceki başlıklarda bahsedilmektedir. Bu kısımda detaylarına girmeden değinilecektir. Kimlik avı, tersine sosyal mühendislik veya dost görünümlü saldırılara karşı çalışanların bilgi eksikliklerinin giderilmesi, yaşanmış olaylar üzerinden konunun öneminin vurgulanması gerekmektedir. Güvenliğe yönelik en yaygın yaklaşım, çalışanları saldırganların veya sosyal mühendislerin siber saldırıları nasıl işlediğine dair farkındalık yaratmaya odaklamak olmuştur. Herkesin bir siber tehdidi tespit edebilecek düzeyde eğitilmesi ve tehdidin başarısız olmasının pozitif sonuçlarının farkında olmasını sağlamak, kullanıcıları daha dikkatli hale getirecektir.

- İkinci yol, dış tedarikçilerden güçlü BT güvenliği politikası izlemelerini istemektir. Çoğu organizasyon çalışmalarını dış tedarikçiler ile yürütmekte ya da desteklerine başvurmaktadır. Bu tedarikçilerin güvenli kaynaklar olduğunu, sistemi riske atacak eylemlerde bulunmamaları gerektiğini bilmek önemlidir. Meydana gelen siber saldırılarda dış tedarikçilerin çalışmalar esnasında sistemde açık bıraktığı, bunda saldırganlar için sistemlere giriş noktası oluşturabildiğini gösteren örnekler vardır. Bu nedenle çalışmalardan önce dış tedarikçilere olabilecek kötü senaryolara karşı endişeleri belirtmek ve güvenlik politikalarını ne şekilde yürüttüklerini sormak önemlidir.
- Üçüncü yol, değişiklik algılama yazılımı kullanmaktır. CimTrak gibi kapsamlı güvenliği, bütünlüğü ve uyumu sağlayabilecek değişiklik algılama yazılımları büyük ölçekli ağlara dahi uygulanıp ağdaki hareketlilikleri tespit edebilmektedir. Bu tür yazılımlar esnek yanıt seçenekleri ve denetim yetenekleri ile güçlü siber saldırılarda dahi işe yarayabilmektedir. Sistemde gerçekleşen değişikliği kimin yaptığını, hangi değişikliklerin yapıldığı ve değişikliklerin nerede meydana geldiğini bu yazılımlar ile öğrenmek mümkündür.

Sistem tasarımlarının ve uygulamalarının yetersiz oluşu yukarda bahsedilen hataların kötü amaçlı saldırganlara fırsat yaratmasına ve güvenlik zafiyetlerini sömürmelerine imkân vermektedir. Kullanıcı dostu güvenlik metotlarının tasarlanmasına ve yapılmasına, bu metotlarında insan ve organizasyon faktörlerine dayanmasına ihtiyaç vardır.

2.4.7. Sosyal mühendislerin kullandığı insani duygular

Ünlü hacker Kevin Mitnick, sosyal mühendislik hedeflerini gerçekleştirmek ve hedeflerini manipüle etmek için insanların duygularını kullanmış ve bu alandaki ilk örneklerin ortaya çıkmasında öncülük etmiştir. Sosyal mühendislik alanında yazdığı kitabında da bu konuya

değinen Mitnick, insanlarda kullanmayı en sevdiği duygunun korku olduğunu dile getirmiştir [55]. Hedeflediği şirketleri arayarak kendisini destek personeli olarak tanıtır sonrasında sistemlerinde hata tespit ettiğini ve ciddi bir veri kaybı yaşanabileceğini söyleyen Mitnick, veri kaybetme korkusuyla çoğu insanın işbirliği yapmayı kabul ettiğinden kitabında bahsetmektedir. Yeterince korkmuş bir çalışanı ikna etmenin zor olmayacağını ve bu tekniği sıklıkla kullandığını da satırlarına eklemiştir [55]. Günümüzde de hackerler tarafından insani duygular hedefleri sömürmek için çoğunlukla kullanılmaktadır. Bugünlerde ise coronavirüse karşı yardımcı olmak veya korunmak için coronavirus izleme ve tespit etmeye yönelik ücretsiz yazılımlar ya da bağlantı adresleri insanlara çeşitli yollarla gönderilmektedir. İnsanların içinde bulundukları korku halinden yararlanmak isteyen saldırganların, aslında gönderdikleri sistemlere zarar veren veya ele geçirilmesine sebep olan kötü amaçlı yazılımlardır. Görüldüğü üzere sosyal mühendisler veya saldırganlar, insan doğasında yer olan psikolojik etmenlerden birini veya birden fazlasını bizlere karşı kullanabilmektedir. SANS Enstitüsüne göre sosyal mühendislerin en fazla sömürdükleri insan zafiyetleri Şekil 2.12’de verilmiştir [73].



Şekil 2.12. En yaygın insan zafiyetleri [73]

Şekil 2.12’ye göre sosyal mühendisler saldırılarında insanların; korku, dikkatsizlik, rahat bölge ve yardım etme isteğini sömürmektedir. Numaralandırmalar çoğunluğa göre değil rastgele verilmiştir.

Dikkatsizlik (Carelessness)

Yapılan araştırmalara göre yaşanan bir siber güvenlik saldırısının kötü amaçlı yazılımlardan sonra ikinci sebebi dikkatsiz ve bilgisiz çalışanlardır [72]. Alınan önlemler teknik anlamda her geçen gün artırılsa da, her zaman var olan insan faktörünün neden olduğu tehlikelerin önüne geçilememektedir. Sosyal mühendis ya da saldırgan hedefine sistem kullanıcılarını aldığı anda şirket, kurum veya kuruluşların siber güvenlik kalkanındaki en zayıf nokta olan çalışan dikkatsizliğine yoğunlaşmaktadırlar. Bazen yapımı uzun çaba gerektiren kötü amaçlı yazılım veya ileri teknoloji içeren saldırı teknikleri yerine faydalanması en kolay insan tabiatı kolaylıkla saldırganlara istediğini vermektedir. Geçen yıl meydana gelen her üç hedefli saldırıdan birinin sistemlere giriş noktası ortalama saldırısıyla yapılan sosyal mühendislik olmuştur. Kötü amaçlı yazılımlar söz konusu olduğunda da durum çok değişmemektedir. Bilinçsiz ve dikkatsiz çalışanların etkisi burada da hayli yüksektir. Karşılaşılan siber saldırıların %59'unda kötü amaçlı yazılımların şirket, kurum ve kuruluşun ağına bulaşmasının sebebi çalışanlardır [72].

Örneğin dikkatsiz bir büro personeli, iş ortaklarından herhangi birinden gelen resmi belge görünümlü zararlı yazılımı şüphe duymadan açabilir. Böyle bir olayda organizasyonun altyapısı çalışmaz hale gelir ve personel istemeden saldırganı yardım etmiş olur. Yine çalışanların pek çoğu anımsamakta zorluk çektiği için kullanıcı şifrelerini kâğıda yazarak masanın bir kenarına koymakta veya bilgisayarın kenarına yapıştırmaktır. Bu dikkatsiz davranış da sosyal mühendisin şifre hırsızlığını kolaylaştırır.

Çalışanlar, ortalama e-postaları, zayıf şifreler veya kötü amaçlı bir yazılımından dolayı saldırganların sistem ağına girişine istemeden de olsa müdahil olmuşlar durumu yetkililere bildirmeleri gerekmektedir. Saklanan her bir güvenlik zafiyeti daha kötü sonuçlar ortaya çıkarabilmektedir. Çoğu zaman cezalandırılmaktan korkan çalışanlar sorunu bildirmektense sessiz kalmayı tercih edebiliyor. Oysaki siber güvenlik konusunda alınması gereken tedbirler sadece teknolojik bir mesele değildir. Aynı zamanda şirket, kurum ve kuruluşun kültürüyle ve eğitimle alakalı bir konudur. Bu noktada üst yönetimler ve varsa insan kaynakları departmanı, çalışanlara gerekli eğitimleri sağlamalı, destek ekipleri oluşturmaları ve olumsuz bir olay olduğunda çalışanların üzerinde fazla baskı ve korku oluşturmamalıdır.

Rahat bölge (Comfort zone)

İnsanlar kendilerine ait yaşam alanlarında, iş yerlerinde olsun evlerinde olsun kendilerini daha rahat daha güvende hissetmektedir. Bunu bilen sosyal mühendislerde hedeflerindeki kurbanın bu özelliğini sömürmektedir. Günlük eylemlerini kendine ait güvenli bölgesinde devam ettiren kişinin olası bir saldırıyı, tehdidi veya dolandırıcılığı algılama ihtimali oldukça azdır [63]. Tam da böyle zamanlarda saldırganlar iş başına geçer ve insani bir duygu olan güvende hissetmeyi kullanmaya başlar. Örneğin sosyal mühendis veya saldırgan şirket, kurum ve kuruluşta görev alan birinin kimliğine bürünerek içeriden birini taklit edebilmektedir. Genelde de taklit edilen BT (Bilgi Teknolojileri) çalışanları olmaktadır. Kendisini BT personeli gibi tanıtır teknik konularda bilgi veren kişiden hedefteki kurban şüphe duymayacaktır. Çalıştığı yerin teknik destek ekibinden olduğunu düşünüp kullanıcı şifresini paylaşmakta veya yazılım güncellemesi diyerek yolladığı zararlı yazılımı kendi bilgisayarında çalıştırmakta sakınca görmeyecektir [63].

Omuz sörfü de bir diğer örnek olarak verilebilir. İnsanlar çoğu zaman çalışırken arkalarında birinin olduğuna dikkat etmezler. Nitekim kendine ait bir alanda, görevine yoğunlaştığında kullanıcı adı ve şifresinin arkadan biri tarafından izlendiğini düşünmeyecektir.

Çalışanlar işyerindeki rahat bölgelerinde kendilerini güvende hissettikleri için güvenlik önlemlerine dikkat etmemekte, bir şey olmaz güdüsü ile hareket etmektedirler. Unutulmamalıdır ki sosyal mühendisler veya saldırganlar her fırsatı değerlendirip siber saldırıya geçecek, hassas verileri ele geçirecek ya da bu verilere zarar vereceklerdir.

Korku (Fear)

Korku, sosyal mühendisler tarafından en çok sömürülen insani özelliktir [74]. Genellikle de kurban üzerinde aciliyet duygusu oluşturulmak istenir. Hedefteki kurban kısa bir zaman aralığında karar vermek için sıkışıp kalır, korkup telaşa kapıldığı anda da yardımcı olabileceğini söyleyen tarafa güvenmeyi tercih eder. Salırganlar insani duyguları yine insanlara karşı kullanırken aslında kurbanı düşünmeyi bırakıp kötü şeyler olmadan önce harekete geçirmeyi amaçlar. Korku duygusunu hisseden çalışan kendini kapana kısılmış

gibi hissedecektir ve hemen harekete geçmezse işini kaybedeceği belki hâkim karşısına çıkarılacağını düşünecektir [63].

Sosyal mühendis veya saldırgan teknik destek personeli görünümünde kurbanı arayarak kullanıcı adı, şifresi ve e-posta adresinin siber saldırı sonucu ele geçirdiğini iddia ederek acil değiştirilmesi gerektiğine dair bir senaryo kurgulayabilir. Kendisinin bu konuda hemen yardımcı olabileceğini zaman kaybetmesi halinde kurumun verileri dışarı çıkacağı için başının derde girebileceğini de senaryosuna ekler. Kendisinin ve ailesinin zarar göreceğini düşünüp korkan kurban teklifi hemen kabul eder. Gerçekte ele geçirilmemiş kullanıcı bilgilerini kendi eliyle saldırgana teslim eder. Üst düzey bir teknik gerektirmeden saldırı amacına kolaylıkla ulaşmış olur.

Yardım etme isteği (Desire to help)

Çoğu insan yardım etmeye isteklidir. Özellikle zor durumda olan birini gördüklerinde yardımcı olma arzuları daha da artar. Bazen bu başkalarına karşı nazik olma isteğiyle de gerçekleşir. Örneğin kargo firması çalışanı gibi giyinmiş birine elleri dolu olduğu için sorgusuzca kurum kapısını açıp içeri almak yardımsever bir hareketken, saldırganı içeri almakta olabilir [73]. Gerçekte sosyal mühendisler veya saldırganlar yardıma ihtiyaçları varmış gibi göstererek durumu kullanmaktadırlar. Mart 2019 da Yeni Zelanda da meydana gelen cami patlamasında 50'den fazla insan yaşamını yitirmiştir. Kendilerini Yeni Zelanda'nın en büyük bankalarından biri gibi gösteren saldırganlar, sahte e-posta adresi ile binlerce insana ulaşmış ve yardım için banka hesap numarası göndermişlerdir. Aslında gönderilen hesap gerçek bağış hesabı değildi ve yaşanan trajediden faydalanarak yüksek meblağda para kazanmışlardır [74].

2.4.8. Sosyal mühendislik saldırılarından korunma

Sürekli gelişen ve değişen teknoloji beraberinde yeni alanlarda getirmiştir. Elbette ki bunlar sosyal mühendislerin dikkatinden kaçmamış, çeşitliliğin ve yeni olmanın getirdiği dezavantajlardan yararlanmışlardır. Yeni yöntemler geliştirerek siber saldırılarda daha da başarılı olmaktadır. Bu saldırılar sosyal, ekonomik ve itibari olarak kurbanlara da ciddi hasarlar vermeye devam etmektedir [75]. Sosyal mühendislik saldırılarını önleyebilecek bir yöntem tam olarak bulunmasa da riskleri ve ortaya çıkacak zararları hafifletecek yöntemlerin

varlığı mümkündür. Siber saldırılara karşı alınan tüm tedbirler sosyal mühendislik saldırıları içinde kabul görmektedir. Fakat sistem ve ağ altyapısına yönelik tedbirlerin yanında sosyal mühendislik saldırılarında, çalışan kişilerin bilincine ve eğitime yönelik tedbirlerde büyük önem kazanmaktadır. Çünkü saldırılar üst düzey yöneticileri hedef alabileceği gibi, temizlik görevlisini, güvenlik görevlisini veya işe yeni başlayan bir çalışanı dahi hedef alabilmektedir. Sosyal mühendisler için güvenlik zincirinin en zayıf halkası olan insanı hedef almak en iyi güvenlik önlemleri ile korunan organizasyonlara dahi kolaylıkla erişmek için her zaman cazip gelmiştir. İnsan unsurunun yer aldığı bir sistemin kesin güvence altında olmayacağını göz ardı etmeyerek, sosyal mühendislik saldırılarına karşı alınabilecek tedbirleri organizasyonlar bünyelerine uygulamalıdır. Bu tedbirlerden bazıları [71,76];

- Farkındalık eğitimi ve güvenlik bilinci,
- Etkili güvenlik politikası oluşturma,
- Fiziksel güvenlik,
- Dijital güvenlik,
- Şifre güvenliği politikası şeklinde aşağıda detaylandırılmaktadır.

Farkındalık eğitimi ve güvenlik bilinci

Makinalara kıyasla insanlara erişmek ve onları sömürmek daha kolay olmuştur [75]. Bundan dolayı organizasyonlarda insan unsuru, sosyal mühendisler için daha savunmasız kalmaktadır. Çalışanlar sistemlere erişim sağladıkları kartların ve şifrelerin güvenliğini sağlamanın önemini yeterince bilmiyorsa güçlü parola sağlama, iki faktörlü kimlik doğrulama, güvenlik duvarı gibi organizasyon politikaları pek önem arz etmemektedir [75]. Şirket, kurum ve kuruluşun güvenliği, en zayıf halkası olan çalışanı kadar güçlüdür de denebilir. Modern teknolojinin başlangıcından bu yana sosyal mühendisler ve hackerler, herhangi bir teknolojik denklemin insan ile bağlantısı varsa onun en sömürücü unsur olduğunu anlamıştır [75]. Herhangi bir ağa, sisteme veya verilere erişme için kolayca manipüle edilecek giriş anahtarı olarak insanı görmektedirler. Yalnızca teknolojiyi kullanarak hedeflerine sızma eğilimleri bu nedenle değişmiştir. Sahte iddialar, aldatma, manipülasyon ve baskı altına alma ile bilgi edinme artık sosyal mühendisler için olağan bir tutum haline gelmiştir. Çalışanların siber saldırılara karşı farkındalık eğitimi alması, bilgi güvenliği konusunda bilinçlendirilmeleri temel noktadır. Organizasyonlar sosyal

mühendislik ile baş etmeye çalışırken en etkili stratejileri eğitim olmalıdır. Periyodik ve sistematik olarak verilen eğitimler çalışanları siber saldırılara karşı daha şüpheci ve bilinçli hale getirecektir. Belki de bu sayede şirket, kurum ve kuruluşlar için en zayıf halka en güçlü halkaya dönüşecektir. Çalışanların hassas verileri korumanın önemini anlamaları ve sosyal mühendisleri isterseler nasıl zora sokabileceklerini bilmelerini sağlamak organizasyonlar için hayati önem taşımaktadır. Eğitimle daha ileri bir farkındalık sağlandığında ise, çeşitli saldırı vektörlerine karşı nereden, ne şekilde, hangi kanal aracılığıyla saldırının gerçekleştiğine dair ayırım yapabilme becerileri oluşacaktır. Karşısında bilinçli bir çalışan bulan sosyal mühendisin işi zorlaşacak, bilgi edinebilmek için daha fazla çalışana ulaşmaya çalışacak, edindiği ufak bilgileri birleştirerek bir bütün oluşturmaya çalışacak, daha fazla zaman harcayacak hatta çoğu kez başarısız olacaktır. Bir organizasyonu sosyal mühendislik saldırısından koruyabilecek en önemli nokta sürekli farkındalık programıdır. Farkındalık eğitiminin sürekli olması gerekir çünkü insanlar bilimsel olarak edindikleri bilginin bir saatte %50'sini, bir günde %70'ini ve bir haftada %90'ını unutma eğilimindedir [76]. Şirket, kurum ve kuruluşlar yoğun ve maliyetli olsa da sosyal mühendislik saldırılarına karşı bu eğitimlerden kaçınmamalıdır. Guido Robling, *“Sosyal mühendisliğe karşı sadece iki şey yardımcı olabilir: farkındalık ve dikkatli olmak. Çalışanların sosyal mühendisliğin nasıl gerçekleştiğini bilmesi ve tuhaf bir telefon ya da e-posta geldiğinde tetikte olması gerekir [77]”* sözüyle güvenlik bilincinin önemini vurgulamıştır. Bahsedildiği üzere kesin bir güvenlik kavramı garanti edilemez. Ancak bilinçli hareket etmek ve çalışanları bilgi güvenliği konusunda eğitmek her bir çalışanın birer güvenlik duvarı olmasını sağlar. Eğitim ve öğretimin sosyal mühendislik saldırılarında en etkili savunma yöntemi olduğu unutulmamalıdır [75].

Etkili güvenlik politikası oluşturma

Günümüz bilgi teknolojileri dünyasında sürekli değişen dinamiklerden dolayı, yöneticilerin ve çalışanların güncel güvenlik politikalarından ve prosedürlerinden haberdar olmaları gerekmektedir [75]. Güvenlik politikası şirket, kurum ve kuruluşun hassas verilerini ve varlıklarını koruma yöntemlerini belirler. Etkin bir güvenlik politikası için kurallar dizisi açık, anlaşılır, makul, uygulanabilir, erişilebilir ve tüm kullanıcılar tarafından kullanılabilir olmalıdır. Politikalar ayrıca sosyal mühendislerin organizasyonun iç işleyişi hakkında bilgi edinip erişim sağlamalarından da koruyacak nitelikte olmalıdır. Net ve açık olmayan

güvenlik politikaları çalışanlar arasında uyumsuzluğa neden olabilir [75]. Bu gibi durumlarda saldırılar amacına ulaşır.

Kevin Mitnick, “Anlamsal saldırıların etkisini azaltmak için tasarlanan, iyi korunan politika ve organizasyon prosedürleri, kullanıcıların teknik yeteneklere dayanmadan olası bir istismar riskini önemli ölçüde azaltmasına ve ortadan kaldırmasına yardımcı olur [55]” diyerek organize ve tutarlı güvenlik politikasının önemini vurgulamıştır. Güvenlik politikası sadece organizasyonu değil aynı zamanda çalışanları da olası zararlardan koruyacaktır. Bu nedenle yöneticilere bu bağlamda büyük iş düşmekte ve güvenlik politikasında meydana gelecek herhangi bir değişikliğin erkenden farkında olmaları gerekir. Bunun yanında bilinmeyen ve öngörülmeyen saldırılara ve onların sürekli değişen yöntemlerine karşı esnek ve güncel politikalar üretmelidirler.

Güçlü ve etkili bilgisayar erişim ve yetkilendirme politikaları, güvenlik duvarı ve kurumsal anti virüslerle olası bir sosyal mühendislik saldırısı bazen durdurulabilir.

Fiziksel güvenlik

Güvenlik bilincine sahip hemen hemen her organizasyonda güçlü bir fiziksel güvenlik uygulanmaktadır. Güvenlik önlemleri gevşekse saldırganlar dijital saldırıya daha kolay başlayacaktır. Açık ve etkili güvenlik politikaları oluşturmak yeterli olmaz, çalışanlar arasında güvenlik bilincinin yerleşip yerleşmediğine dair testler de yapılmalıdır. Çünkü saldırgan dışardan olabileceği için organizasyon içinden biride olabilir [75]. İçeriden biri olması durumunda ise fiziksel güvenlikten bahsetmek zordur. Sistemlere erişim yetkisi olan çalışanların güvenilirliği de gözden geçirilmelidir, aksi takdirde fiziksel tehditlerin olma olasılığı artacaktır. Koruyucu fiziksel bariyerler, güvenlik aydınlatmaları, alarmlar, hareket algılama kurulumu, kilitli dolaplar, kamera sistemleri ve çalışanları tanımlamak için biyometrik kullanımı organizasyonu potansiyel saldırılardan koruyacak fiziksel önlemler arasındadır [75]. Fiziksel güvenlik konusunda normal zamanlarda da çalışanlar bilgilendirilmelidir. Örneğin herhangi bir USB sürücüsünü veya buldukları diğer dijital cihazları emin olmadan kullanmamaları gerektiğine dair organizasyon içerisinde hatırlatıcı işaretler olmalıdır. Yeterli fiziksel kontroller sağlandığında ciddi bir sosyal mühendislik

saldırısını geri püskürtmek mümkün olabilir. Ancak sert fiziksel güvenlik politikaları uygulanmazsa şirket, kurum ve kuruluşun kapıları saldırılara hep açık olacaktır [64].

Dijital güvenlik

Sosyal mühendislik saldırılarına karşı alınması gereken bir diğer önlem, bir dizi dijital koruyucu hizmet ve yazılım aracının organizasyonda hayata geçirilmesidir. Dijital güvenlik hizmetlerinin kullanımı bazı sosyal mühendislik saldırı türlerine karşı etkili olsa da diğer saldırı türlerinde tamamen işe yaradığı söylenemez. Saldırı riskini ortadan kaldırmak için çoğunlukla uygulanmaktadırlar [75]. Örneğin antivirüs veya kötü amaçlı yazılım koruması ve beraberinde iyi bir güvenlik duvarı (firewall) kullanan şirket, kurum ve kuruluşun kimlik avı saldırısına uğrama ihtimali azdır.

Güncellemeleri zamanında yapmak, koruyucu yazılımlar kullanmak vb. çalışmalar organizasyon için tamamen bir koruma sağlamayacaktır. Tabi bu yazılımların kullanılması gereksizdir anlamına da gelmez. Çünkü dijital veri ve varlıkların korunmasında ne kadar çok önlem alınırsa o kadar iyidir. Bu önlemler kısmi olarak koruma sağlayacaktır. Bunların dışında korumalı alan oluşturma sanal makinaların kötü amaçlı yazılımlardan korunması için yalıtılmış bir alan oluşturur. Koruma alanı kullanımı bazı sanal saldırılara karşı oldukça etkilidir. Popüler tarayıcılarından Chromium ve Firefox, internet tarayıcıları aracılığıyla sömürüyü engellemek için dâhili sanal alan teknolojilerini kullanmışlardır [75]. Şöyle ki bu yapı güvenliği ihlal edilmiş web sitesine bağlantı kurulduğu zaman web kullanıcısının izni olmadan kötü amaçlı bir yazılımın indirilmesini engeller. Gerçekleşen tüm indirmelerin önce korumalı bir alana yönlendirilmesini sağlar buradan olur gelirse kullanıcı bilgisayarına öğe güvenle iner.

Proaktif izleme, saldırgan kullanıcı kimlik doğrulaması, makine öğrenmesi ve algoritma analizi gibi özel önlemlerde sosyal mühendislik saldırılarına karşı etkili azaltma stratejisi oluşturabilir [75]. Bu yapılar ile normal sistem davranışları gözlemlenerek yasal ve yasal olmayan kullanıcı eylemleri ile paket veya veri iletim tutarsızlıkları arasında saptamalar yapılır. Ortaya çıkan saptama sonuçları makine öğrenmesinde kullanılarak makine tabanlı öğrenme sistemi oluşturulur. Makine tabanlı öğrenme sistemi kullanıcının yazı stili, noktalama işaretleri kullanımı, karakter tanıma, kelime sıklığı, e-posta kutusu içeriği, e-posta akışı ve diğer parametreleri inceleyerek bir kullanıcı profili geliştirir. Geliştirilen profil her

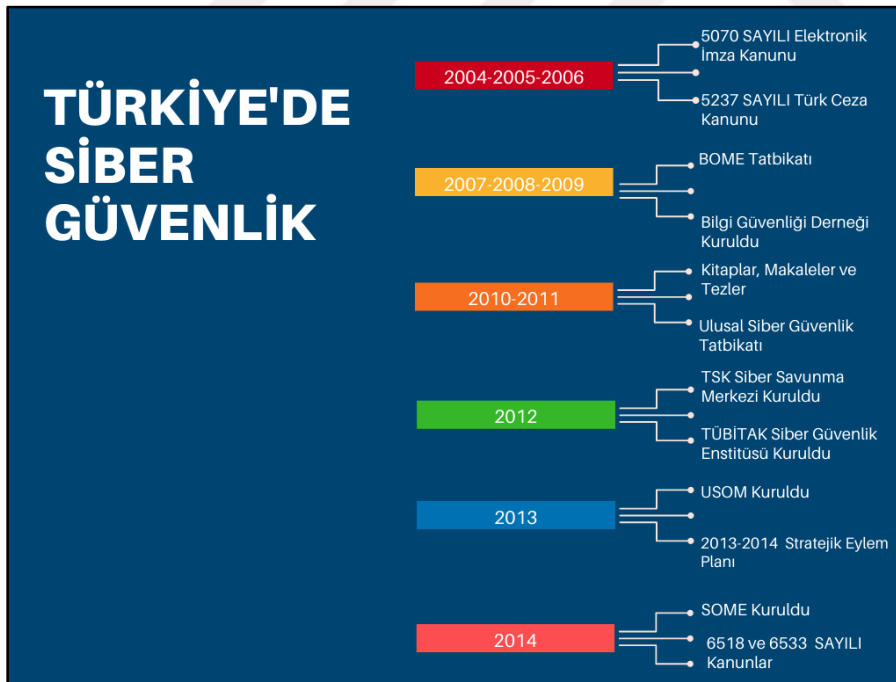
e-posta alışverişinde güncellenir. Sonuç olarak ortaya çıkan algoritma pek çok sosyal mühendislik saldırısını tespit edip engelleyebilmektedir [75]. Dijital koruyucu önlemler saldırıları ilk aşamada tespit etmede isteneni sağlamaktadır. Önemli olan saldırı girişimlerini sürekli analiz etmek ve organizasyon altyapısını ona göre yükseltmektir.

Şifre güvenliği politikası

Şirket, kurum ve kuruluş genelinde bir şifre güvenlik politikası belirlenerek yönetim de dâhil herkesin bu politikaya uyması beklenir. Sistemlerde yer alan her türlü hassas verinin şifrelerle korunduğu düşünüldüğünde saldırganlar verilere erişmek için hedef kullanıcının şifrelerini ele geçirmek isteyecektir [75]. Şifrelerin yetkisiz kişilerce ele geçirilmesi, yanlış ve kötü amaçlı kullanımları organizasyonlar için ciddi güvenlik sorunlarına yol açabilecektir. Çalışanlar şifre güvenliği konusunda bilinçlendirilmeli, kolay tahmin edilen şifreleri seçmeleri engellenmeli, şifre güvenlik politikasına uygun olmayan şifreler tespit edilip gereken uyarılar yapılmalıdır [71]. Çalışanların çoğunun şifreleri doğum tarihi gibi kolay tahmin edilecek şifrelerdir. Bazıları ise karmaşık ve zor şifre verdiğini, unutabileceğini düşünerek kullanıcı şifrelerini bir kâğıda yazıp masa üstüne bırakabilmektedir. Bu gibi durumların sosyal mühendisler tarafından sömürüleceği unutulmamalıdır. Her hesap veya erişim sağlanan sistem için çalışanlar ayrı kullanıcı şifrelerini tercih etmelidir. Şifreler belirli aralıklarla değiştirilmeli, artarda belirli sayıda yanlış şifre girildiğinde kullanıcı hesabını devre dışı bırakacak güvenlik mekanizmaları kullanılmalıdır. Şifrelerinin yetkisiz kişilerce ele geçirildiğini veya kullanıcı hesaplarına izinsiz giriş yapıldığını düşünen çalışanların gerekli birimleri haberdar etmeleri ve güvenlik önlemlerini alınması sağlanmalıdır [71].

bir artış olduğunu ortaya koyarken; dünya genelinde hükümetler bu konuyu şirket, kurum ve kuruluş inisiyatifine bırakmadan, kanun koyucular ve prosedürlerle geliştirmeye ve siber güvenlik sağlanması hususunda gerekli atılımları yapmak için teknolojik yatırımlarda bulunmaya başlamışlardır.

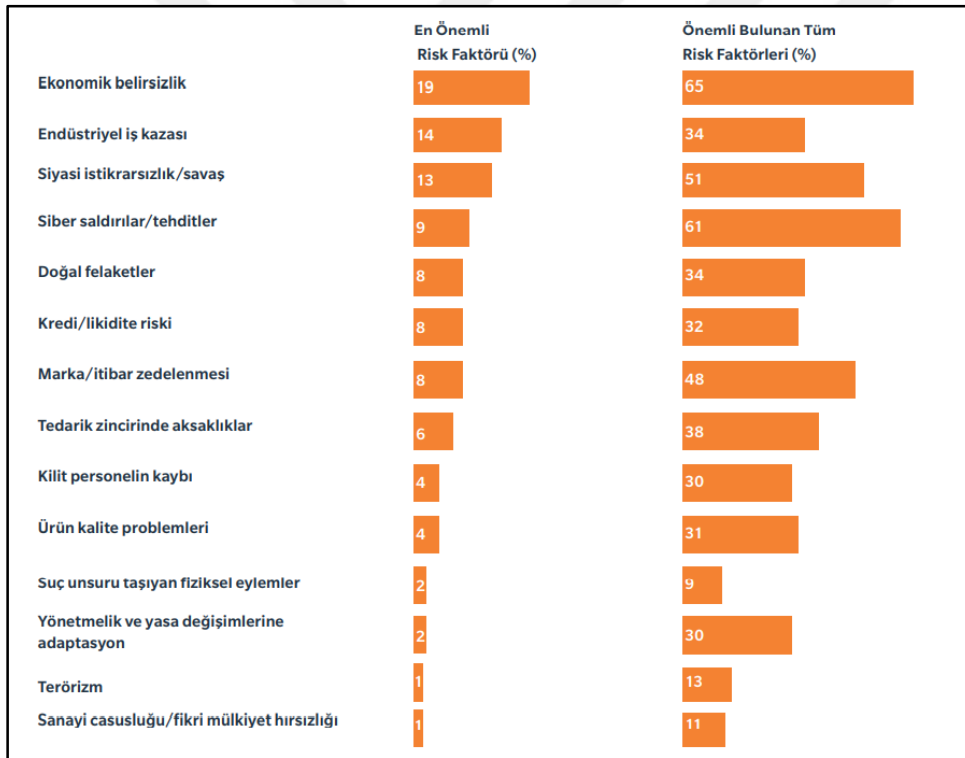
Türkiye nezdinde Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nce kurulan Siber Güvenlik Dairesi Başkanlığı, siber güvenlik alanında ihtiyaç duyulan atılımların gerçekleşmesi ve gerekli adımların eksiksiz atılması için çalışmalar yapmaktadır. Belirlenen politikalar dâhilinde ulusal siber güvenlik ve bilgi güvenliğini destekleyici projeler geliştirmekte, siber güvenlik ile ilgili strateji ve eylem planlarının uygulanmasına yönelik gelişmelerin takibini sağlamakta ve kritik altyapıların belirlenmesine yönelik çalışmaları sürdürmektedir [80]. Ayrıca ülkemizde, Savunma Sanayi Başkanlığı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Türkiye Siber Güvenlik Kümelenmesi gibi kurumlar aracılığıyla kamu, özel sektör ve üniversiteler arasındaki işbirliğinin artırılması suretiyle ulusal siber güvenlik ekosisteminin oluşturulmasına yönelik çalışmalar devam etmektedir [81].



Şekil 3.2. Türkiye’de siber güvenliğin gelişimi [15]

Türkiye’de siber güvenliğin gelişimi üzerine yapılan çalışmalar artırılabilir gibi Şekil 3.2’de en geniş anlamda yıl bazlı bu çalışmalar özetlenmiştir.

Öte yandan Ahram ve Nicholson, siber alanın sosyal, ekonomik ve davranış yönlerinin genel siber güvenlik tartışmalarından büyük ölçüde eksik olduğunu savunmaktadır [78]. Gartner’ın araştırmasına göre dünya genelinde siber güvenlik harcamalarının 2022’de 133,7 milyar dolara ulaşacağı tahmin edilmektedir. Yine aynı araştırmaya göre 2021 yılı itibarıyla siber suçlardan korunmak için dünya genelinde 6 Trilyon Dolar harcanması beklenmektedir [82]. Türkiye’de ise risk yönetimi ve/veya bilgi teknolojilerinden sorumlu çalışanların %9’u kurumunun karşı karşıya olduğu en büyük riski siber tehdit olarak görmektedir [83]. (Bkz. Şekil 3.3)



Şekil 3.3. Kurum çalışanları risk algısı araştırması

Şekil 3.3’e bakıldığında 10 kurumdan 6’sı için siber güvenlik riski, en önemli ilk 5 risk faktörü arasında yer almaktadır. Marsh ve Microsoft’un 2019 yılında birlikte yaptığı Global Siber Risk Algı araştırmasının sonuçlarına göre; araştırmaya katılan benzer profildeki katılımcıların %22’si siber saldırıları ve tehditleri en önemli risk faktörü olarak değerlendirmiştir. Bu oranın Türkiye’de %9 düzeyinde olması ülkemizin siber risk

farkındalığı açısından henüz küresel şirketlerin oranını yakalayamadığını ve bu konuya öncelik vermediğini açıkça göstermektedir [84].

Siber güvenlik riskinin yönetiminde ise en önemli konu yeterli ve yetkin insan kaynağı olarak görülmektedir [83]. Şirket, kurum ve kuruluşlarda siber risk konusundaki sorumluluk genellikle BT (Bilgi Teknolojileri) çalışanlarında gibi gözükse de insan faktörünün yer aldığı her birim ve kademe, bu sürecin başarıyla yönetilmesinde vazgeçilmez bir parçadır.

Ahram ve Nicholson'a göre insan unsuru, siber güvenlik alanını karmaşık ve uyarlanabilir bir sistem yapan şeydir. Siber alanın insan unsurunun ve teknik yönlerinin birleştirildiğinde ise güvenli bir ağ elde edilebileceğine inanmaktadırlar [78].

3.1. Sosyal Mühendislikte İnsan Faktörünün Yeri

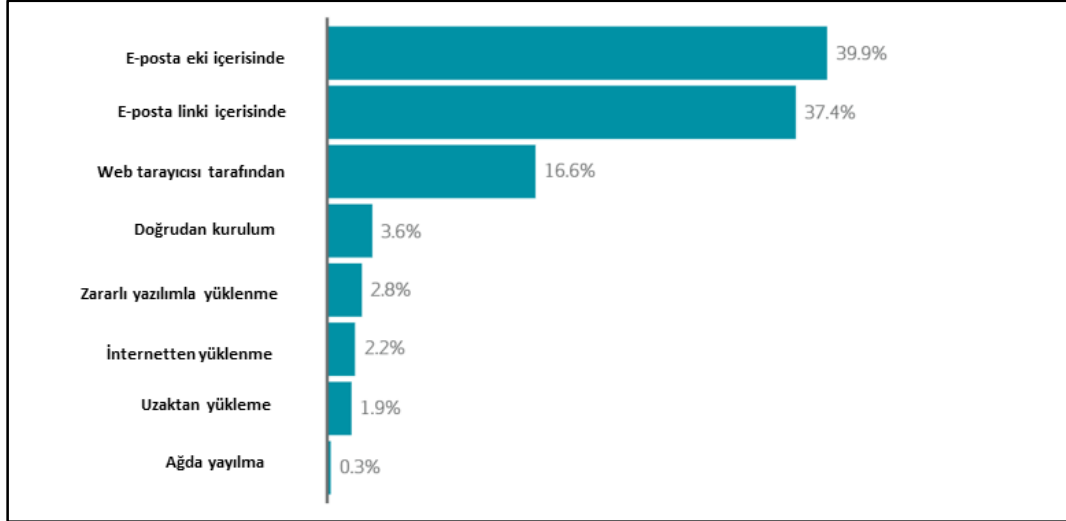
Sosyal mühendislikten bahsedilirken hakkında; belirli kriterlere göre sınıflandırılmış bilgilerin, psikolojik manipülasyonlarla ortaya çıkarılması sanatı denilmektedir. Bir diğer genel ifade şekli ise, bilgi güvenliği sistemlerinin en zayıf halkası olan ve bu sistemleri kullanan insanlardan yararlanma sanatıdır [65]. Yapılan stratejik ataklar ve karmaşık sahtekârlık sistemi ile kişisel bilgilerin elde edilmesine dayanan insan etkileşimidir.

Sosyal mühendisler, teknolojik ataklardan çok insanların güvenini sömürmeyi tercih ederler çünkü insanların doğal eğilimlerini sömürmek her zaman daha kolay olmuştur. Şirket, kurum ve kuruluşlarda çalışanların çoğu sosyal mühendislik saldırılarına karşı bilinçsizdir. Bu durum sosyal mühendislik saldırılarının göz ardı edilmesine ve büyük bir tehdit olarak algılanmamasına neden olmaktadır. Her geçen gün sayısı artan, hedefi en zayıf halka insan olan sosyal mühendislik saldırıları hem bireyin hem de organizasyonun ciddi kayıplar vermesine neden olmaktadır. Sosyal mühendislik, verdiği kayıplar neticesinde hakkında araştırmalar yapılan en popüler siber suçlardan biridir [61]. Ortada teknik bir problem olmadığı için de bilgisayar güvenlik alanının dışında görülür. Oysaki bilgi sistemlerinin güvenlik yönetimi hem teknolojik önlemlere hem de yönetsel çabalara bağlıdır. Çeşitli güvenlik sorunlarına hep teknolojik yöntemler geliştirilmiş ancak ciddi güvenlik ihlallerine sebep olan insan faktörü nispeten ihmal edilmiştir [86]. İhmal edilen insan unsuru, bilinmelidir ki güvenlik sistemi içindeki hatalı ya da savunmasız en temel elemandır. Genel olarak özü gereği ahlaki erdemlerine sahip çıkmak ve iyi bir birey olarak toplumda yer

edinmek olan insanoğlu, bu fitratından dolayı sosyal mühendisler tarafından manipüle edilmektedir. Bireyler çoğu zaman bir saldırının kurbanı olacaklarını düşünmezler buda onları sosyal mühendislik saldırılarına karşı daha savunmasız hale getirir ve birçoğu böyle bir saldırının kurbanı olduğunu asla bilmez. Sosyal mühendislik saldırı tekniklerinden habersiz olan bireyler bu tekniklerin bilgi edinme derecesini, ne ölçüde kullanılabileceğini ve ciddi kişisel, ekonomik ve sosyal kayıplara sebebiyet verebileceğini kavrayamamaktadır. İnsanlar genellikle sahip oldukları bilgilerin başkaları için bir şey ifade etmeyeceğini veya herhangi bir kötü niyet için kullanamayacaklarını düşünür ve gizli bilgileri açıklama konusunda sakınca görmezler. Benzer durum çalışanlar arasında ise diğer çalışanlar arasında kimsenin bilmediği bilgileri bildiğini gösterme, diğerleri ile arasında fark yaratmaya çalışma ve daha prestijli gözükme isteminden mütevellit ortaya çıkmaktadır. Fakat unutulmuş gerçek sosyal mühendislerin bilgi toplamak için her türlü kaynağa ve yöntemine başvuracağıdır. Sosyal mühendislerin veri veya bilgi toplama yaklaşımları psikolojik ve bilgisayar bilimi odaklı olarak değerlendirilebilir. Psikolojik bakış açısında, kurbanlarının duygusal durumlarına ve bilişsel yeteneklerine odaklanırken, bilgisayar bilimi bakış açısında bilgi güvenliğinin temel yapıtaşlarından biri olan hassas bilgiye odaklanmaktadır [87]. Psikolojik olarak insanlar, karşı tarafın tavır ve düşüncelerinden etkilenmeye müsaittir. Sosyal mühendisler ele geçirdiği duygusal ipuçları ile kurbanı ikna etmeye ve etkilemeye çalışır. Basit gibi gözükse de gerçek dışı senaryolar üretilmeden kurbanlardan istenilen bilgiler bu şekilde alınabilmektedir. Doğrudan kurbandan bilgi almak sosyal mühendisler için sağlıklı bir yol gibi gözükmediğinde ise kurbanın yanıt verme yeteneğine müdahale ederek heyecan ve korku gibi güçlü duyguları tetiklemeye çalışırlar. Üzerinde hissettiği heyecan veya korku durumunda da kurban, sosyal mühendise karşı savunmasız hale gelebilmektedir.

Organizasyonlar için gereksiz ve değersizmiş gibi görünen her türlü veriden sosyal mühendis, bir şekilde yarar sağlamaktadır. Sosyal mühendisliğin en büyük kozu, kurbanlarının güvenlerini kazandıkları takdirde; yarar sağlayan verileri, aldatılmaya karşı oldukça hassas olan bireyleri manipüle etmek için kullanmaktır. Anlaşılabileceği üzere bir organizasyonun güvenliğini en çok tehlikeye atan, ne bilgisayar virüsü ne de kötü kurulmuş bir güvenlik duvarıdır. Gerçekte en ciddi tehdit birey, çalışan veya kurban adı ne olursa olsun insandır. İnsan tabanlı bir sosyal mühendislik saldırısında sosyal mühendis hedefindeki kurban ile iletişime geçerek bilgi edinmeye çalışır. Teknoloji tabanlı saldırısında ise önemli bilgilere erişmek için kurbanın bilgisayarında olan programlardan yararlanır. E-posta ekinde

gönderilen zararlı bir yazılımın sisteme girişi buna en iyi örnektir. 2015 yılında Verizon tarafından yapılan Veri İhlali Araştırma Raporu'nun sonuçları Şekil 3.4'te verilmiştir. Raporda zararlı bir yazılımın hedef sisteme hangi yollarla yüklendiğinin istatistiksel değerleri verilmiştir [88].



Şekil 3.4. Zararlı yazılım yükleme vektörü

Şekil 3.4'te de görüldüğü üzere zararlı bir yazılımın hedef sisteme yüklenmesinde vasıta vektör, toplamda yaklaşık %78 oranında e-posta ekinde ve e-posta linkinde zararlı yazılımın karşı tarafa gönderilmesidir. Elbette burada da e-posta ekini açması ve akabinde olanlara mahal vermesi sebebiyle insan faktörü yine dolaylı olarak yer almaktadır. E-postalardaki aldatıcı unsurları gözden kaçırarak bireyler yüksek mağduriyet oranlarını ortaya çıkarmaktadır. Ortalama denilen bu sosyal mühendislik saldırı türünde bireylerin ya da çalışanların aldatıcı unsurları fark edip bilişsel olarak değerlendirmelerini sağlayacak eğitimlerin verilmesi gerekmektedir.

Kevin Mitnick sosyal mühendislik üzerine yazdığı kitabında, *“Hem insanları hem teknolojiyi aynı zamanda sömürdüğünüzde bu, ölümcül bir kombinasyondur”*[55] diyerek yukarıda bahsedilen iki ayrı durumu teke düşürmüştür.

Sistemlere erişim sağlayan bir kurban, sosyal mühendislerin işini kolaylaştırır ki böylece sisteme sızmak için fazladan teknikler aranmaz. Bu sebepten ötürü, sisteme erişim yetkisi

olan çalışanların, diğer çalışanlara göre daha bilinçli ve dikkatli olması ve teknoloji ve insan birleşimi avantajını sosyal mühendislere vermemesi gerekmektedir.

Çevre, kişilik, risk algısı, idrak etme süresi, önyargılar ve çeşitli demografik etkiler bireylerin sosyal mühendislik sürecinde karar alma duyarlılıklarını etkiler [89]. Bu faktörlerin kombinasyonları, bireylerin savunmasızlığını artırdığı gibi sosyal mühendislik saldırı ağına düşme olasılıklarını da artırır. Önyargıları sonucu yanılgıya düşen kişi gerçekte mantıksız olduğunu bildiği bir kararı doğru kabul edip uygulayabilmektedir. Bu yanılgılar bireyin kişiliğinin ve o anki duygusal durumunun ürünüdür. Risk ve güven algısı da bireyin sosyal mühendislik saldırısı sırasında karar vermesinde önemli rol oynar. Riskli karar verme; çalışma hafızası, bilişsel süreçler, önyargılar, kişilik, zaman baskısı ya da stres ile bağlantılıdır [90]. İnsan doğası gereği karmaşık bir canlıdır ve duyarlılıkları, zafiyetleri yukarıda bahsedilen tek bir faktör ile açıklanamayabilir. Birden fazla faktörün etkisinde ise savunmasızlığı daha da artacaktır. Diğer taraftan bu çoklu faktörler, sosyal mühendislik saldırısını tespit edebilmede de kişiye bir bütün halinde yardımcı olur. “İnsanın çevresi, davranışları, algısı ve demografik özelliklerinin sosyal mühendislikle ilişkisi var mıdır? “ sorusuna da cevap verilmiş olunur.

Sosyal mühendislik saldırıları sürekli gelişmekte ve artmakta, böylece şirket, kurum ve kuruluşların siber güvenlik zincirleri zayıflamaktadır. Teknoloji ve iletişimin hızlı büyümesi, coğrafi bölünmeler arasında köprü oluşturan daha fazla sosyal iletişim yaratmıştır. Bu ilerlemenin ve büyümenin dezavantajı sosyal mühendislik saldırıları için artan fırsatlar olmuştur. Daha fazla erişim ve iletişim noktasının varlığı, insanların sosyal mühendisliğin olumsuz etkisine diğer sebeplerden daha duyarlı olduğunu anlamak için önemlidir. Sosyal mühendisler kurbanları ile iletişim sağlamak ve onları çekmek için sıklıkla güncel olayları da kullanır. Bunlar, hedeflenen ve etkisi olan hafifletme stratejilerinin, tekniklerin ve prosedürlerin geliştirilmesine ve uygulanmasına izin verecektir [91].

3.2. Siber Güvenlik Farkındalık Eğitimi

Siber güvenlik bilinci veya farkındalığı eğitimi, siber güvenlik konusunda ortaya çıkan yeni bir düşünce okuludur [92]. Kuruluşlar siber güvenlik bütçelerinin çoğunu çevre savunmaları için harcamaya devam etseler de, gittikçe daha fazla şirket, kullanıcıların zayıf bir bağlantı olduğunu ve savunmaları artırmak için genel siber güvenlik programlarına güvenlik bilinci

eđitimini de dâhil etmeye başlaması gerektiđini anlamaya başlamışlardır. Güvenlik bilinci eğitimi, sınıf stili eğitim oturumları, güvenlik bilinci web siteleri, e-posta yoluyla yardımcı ipuçları veya posterler gibi çeşitli biçimlerde olabilir [93]. Simüle edilmiş sosyal mühendislik ortalama saldırısı e-postaları, kullanıcıları güvenlik bilinci konusunda eğitmek için yöntem olarak da kullanılır [94].

Kurumsal bilgi güvenliđi farkındalıđı denildiđinde akla daha çok kurumun standart ve politikalarının kurum çalışanlarına öğretilmesi ve ortaya çıkabilecek riskli durumlar, olumsuz sonuçlar ve karşılaşılan tehditlere yönelik olarak yapılması gerekenlerin üzerinde durularak gerçekleştirilmesi gelmektedir [44]. Ancak, internet ve bilgisayar kullanan her bir birey için kişisel bilgi güvenliđi farkındalık eğitimlerinin verilmesi artık gereklilik deđil zorunluluktur. Özellikle sosyal paylaşım sitelerini (facebook, twitter, blogger, linkedin vb.) kullanan insanlar, kendi istekleriyle veya farkında olmadan iş bilgileri, kişisel bilgiler gibi özel bilgilerini internet ortamında herkesin erişebileceđi şekilde paylaşmaktadır. Bu durum bilgisayar korsanlarına istedikleri fırsatı sağlamakta ve sosyal mühendislik yöntemlerini de kullanarak dolandırıcılık gibi suç faaliyetlerini gerçekleştirmelerine imkân sağlamaktadır [44].

Sosyal mühendisliđin insanları nasıl aldattıđını ve etkilediđini anlamak, yapılacak müdahaleler için önemlidir. Kişi sosyal mühendislik saldırısına uğradıđında çalıştıđı şirket, kurum ve kuruluş bilgi ve veri kaybedebilir, ihlal yaşayabilir, para tuzađına düşebilir ve diđer birçok ihtimal meydana gelebilir. Sistem kullanıcılarının organizasyonun önemli bileşenleri ile bağlantılı olması buradaki kilit noktadır. Organizasyonlar çalışanlarına yönelik farkındalık eğitimlerinde tüm bunlara değinmelidir. NIST 800-16'ya [96] göre farkındalık bir eğitim deđildir ve farkındalık sunumlarının amacı dikkatin güvenlik konusu üzerine yoğunlaştırılmasıdır. Farkındalık sunumları kişilerin BT güvenlik tehditlerini tanınması ve uygun şekilde davranmasını hedefler. Özetle kişilerin sadece tehditleri fark etmesini sağlamaya yönelik deđil olası tehditlere karşı da uygun davranışları sergilemesi gerektiđini belirtmektedir. Kişinin tehditler dođrultusunda uygun davranışları seçmesi ise bilgi güvenliđi algısı ile mümkün olmaktadır [97].

Önceki başlıklarda yapılan araştırmaların sosyal mühendislik saldırısına maruz kalsa dahi bireyde farkındalıđın oluşmadıđı, duyarlılıđın az olduđu konusuna değinilmiştir. Bireysel siber farkındalık araştırmasının sonuçlarına göre kullanıcılar halen nelerin siber saldırı

olduđuna dair net bir bilgiye sahip deđildir. Arařtırmaya katılan kullanıcıların %82'si siber saldırıyı, sadece parolalarının alınması veya bilgisayarına virüs bulařması olmadıđı gibi kiřisel verilerinin alınmasını da tek saldırı türü örneđi olmadıđını ifade ederken, %18'i ise belirtilen seenekler dıřındakilerin siber saldırı olup olmadıđının farkında deđildirler [98]. Bu eksiklik sadece bireyden deđil sosyal mühendislik saldırısı sonucunda gerekli raporlamaları yapıp alıřanları bilgilendirmeyen organizasyonlardan da kaynaklanmaktadır.

řirket, kurum ve kuruluşlar aksine daha fazla alıřmalar yapmalı, nerede eksiklik ve yanlışlık olduđunu, zayıflıkların kimlerden ya da nelerden kaynaklandıđını tespit etmek için daha fazla uğrař vermelidir. Sađırođlu, Erol ve Ceyhan'a göre, günümüzde farkındalık eđitimleri dönemsel olarak kullanıcıların bilgilerini tazelemektedir. Ancak saldırıların yařadıđı dönüşüm ve gelişim çođu zaman iki eđitim arasındaki zamandan çok daha hızlıdır. Dolayısıyla kullanıcı bir önceki gün aldıđı eđitime rađmen ertesi gün hi duyulmamıř bir saldırının kurbanı olabilmektedir [44].

Benzer bir yaklařım, *“Siber Güvenlik Farkındalıđı İçin Yetenek Tabanlı Dinamik Model”* bařlıklı tezde de řu řekilde ifade edilmiřtir;

Teknolojik önlemlerin günümüzde bilgi güvenliđinin sađlanması ve hassas verilerin korunması noktasında tek bařına yeterli olması imkânsız hale gelmiřtir. Farkındalık eđitimleri ise etkili olmakla beraber günümüzde siber saldırıların iki eđitim arasında geen süreden çok daha kısa sürelerde gelişmesi ve farklılařması sebebiyle yetersiz kalmaktadır [99].

Kullanıcılar arasında istenilen farkındalıđın tam olarak yerleřebilmesi için yapıyı bir döngüye oturtmanın gerekliliđi açıka görölmektedir. Yapı bir döngüye oturtulduđunda ise, hem süreklilik sađlanmış hem de edinilen güvenlik bilgileri taze tutulmuř olacaktır. Farkındalık kavramı kullanıcılara planlanan eđitimlerden ziyade günlük hayatta yaptıkları işlemlerin ierisine entegre olarak sunulmalıdır [44].

Bahse konu arařtırmalar ve incelemeler dođrultusunda siber güvenlik farkındalıđının kullanıcı ve kurum bađlamında süreklilik arz edecek bir yapı ile ifade edilmesi gerekliliđinin önemli bir hale geldiđi görölmektedir.

Kurumlarda çalışanların teknolojik kavramlara hâkimiyetleri, bilgileri, risk algılama durumları ve kurumsal verilerin güvenliğinde sorumluluk taşıdıklarını bilme düzeyleri aynı değildir. BT çalışanının sosyal mühendislik saldırısını fark etme ihtimali yüksek iken başka bir birimde görev yapan bir çalışanın saldırıyı fark etme ihtimali daha düşüktür. Son kullanıcı, kurum çalışanı, yaş, cinsiyet, statü gibi etmenleri gözlemeksizin kurumların kapsayıcı bir şekilde siber güvenliğe karşı hareket etmesi ve olası durumları ve sonuçlarını gözlemlemesi gerekmektedir. Farkındalık eğitimleri herkese aynı şekilde verilse dahi sosyal mühendisliğe karşı bir model geliştirilerek çalışanların olası bir saldırı halinde verdikleri tepkinin test edilmesi bundandır. Farkındalık seviyesi ile insan davranışının ayrı yönlerde hareket edebildiği göz önünde bulundurulduğunda, farkındalık üzerine yapılan eğitim ve çalışmalar davranış değişikliğini hedeflemelidir. Davranış değişikliği ise ancak tekrarlayan ve dinamik bir döngü ile hareket edildiğinde güvenlik kültürü olarak kullanıcılar tarafından içselleştirilebilir [44].

İnsanların doğası güvene dayanır bu da sosyal mühendislik tehditlerine karşı farkındalık eğitimlerini büyük bir zorluğa sokabilir. Bireylerin ve kuruluşların fiziksel ve veri güvenliklerinin organizasyonda çalışan kişiler tarafından daha ciddiye alınması gerekir [100]. Kişiler, çalıştıkları yerin BT altyapısı ve çalışanlarına olan fazla güven duygusundan dolayı güvenliği bir tehdit olarak görmezler. Organizasyonlar, eğitim materyallerine ayrıca bireylerin bu güven boşluğunu kapsayacak yöntemlerde eklemelidir [101]. Kişilerin güven boşluğunu doldurmak için ise şirket, kurum ve kuruluşların bünyelerine yeni hizmetler eklemesi ya da var olan hizmetlerini geliştirmesi gerekmektedir. Bunun yanı sıra sosyal mühendisler tarafından kullanılan en son teknikler hakkında kuruluşlar güvenlik bilinci düzeyini yeterli ölçüde korumazsa saldırı tehdidi riski de artacaktır. Sosyal mühendislik saldırıları hem değişen teknolojilerle hem de güvenlik önlemleriyle birlikte gelişecek şekilde tasarlandığından, olası tehditlere karşı daha kategorik bir eğitim anlayışına ihtiyaç vardır. Teze konu olan filtre model, beraberinde daha az maliyetle daha etkin bir farkındalık eğitimi imkânı organizasyona ve çalışanlarına sunmayı hedeflemektedir. Aldawood ve Skinner şirket, kurum ve kuruluşların siber saldırılara karşı ayırabilecekleri bütçenin azlığından dolayı destekleyici yapıların kullanılmasını öne sürmüştür. Organizasyonların eğitim bütçelerinin eksikliği de düşünüldüğünde eğitim ve bilinçlendirme programlarının çeşitli yöntem veya modellerle geliştirilmesi daha iyi sonuçlar elde edilmesine yardımcı olacaktır [102].

Sıklıkla üzerinde durulan ve zafiyeti oluşturan insan faktörünün eğitimi konusuna destekleyici unsurların eklenmesi de yeterli değildir. Bu yapının sürekliliği sağlamak da büyük önem arz etmektedir.

Gündüz ve Daş da konuya benzer bir bakış açısı getirmişlerdir. İnsanlar sosyal mühendislik saldırılarını fark edecek şekilde eğitilmediği ve yetiştirilmediği sürece mağdur insanların sayısında bir azalma olacağını söylemek mümkün değildir. Kişilere yönelik bu yetiştirilme süreci ise oluşturulmak istenen bilincin veya farkındalığın sürekliliğini bir yapı ile sağlamakla mümkün olabilir. Dünyada sosyal mühendislik saldırılarını engelleyebilecek bir teknoloji henüz yoktur ancak sürekli bir bilinçlilik durumu bunu engelleyebilecek en etkili silah olacaktır [45].

Bu çalışmada siber güvenlik farkındalık eğitiminin tek başına yeterli olmamasına yoğunlaşmış ve farkındalığın, ortaya konulacak model ile daha başarılı rol oynayacağı düşünülmektedir. Siber güvenlik konusunda sosyal mühendisliğe karşı bir farkındalık modelinin geliştirilerek test edilmesi ve işlemi bir döngü halinde sürekli ve canlı tutmasına yönelik olarak ülkemizde yapılan ilk çalışma olması sebebiyle literatüre büyük katkı sağlayacağı değerlendirilmektedir. Teze konu olan saldırı önleyici model, sosyal mühendislik yaşam döngüsü, siber güvenliğe karşı ortaya konulan öneriler, kurumların ve kişilerin aldıkları önlemler ve alanında önde gelen siber güvenlik firmalarının çözüm raporları temel alınarak hazırlanmıştır. Oluşturulan modelin, kamu kurumlarının siber güvenlik teşkilatlanmaları dâhil siber güvenliğe ilişkin tüm alanlarda kurumlara katkı sağlayacağı, her seviye kullanıcı için filtreleme mantığı geliştireceği, kuruluşların çalışanlarını yetiştirme süreçlerinde hem işe yeni başlayanlar hem de eski çalışanlar için siber güvenlik farkındalıklarını destekleyeceği ve artıracığı düşünülmektedir. En önemlisi, kullanıcıların olası bir sosyal mühendislik saldırısında saldırıyı tespit edip engelleme yoluna gitmelerine vesile olması beklenmektedir.

3.3. Farkındalık Modelleri Literatür İncelemesi

Siber güvenlik alanında farkındalığı artırmak için farklı yollar, tasarımlar, yöntemler denenerek çeşitli modeller öne sürülmüştür. Konuyu ele alma biçimlerine göre yapılan çalışmaların hepsi literatüre çeşitlilik kazandırmıştır. En sık duyulan modellerden biri olan siber güvenlik olgunluk modelinde, bir güvenlik programının olgunluğunun ölçülmesi ve bir

sonraki seviyeye nasıl geçildiğine dair bir çerçeve sunulmaktadır. Forbes’da yayınlanan bir makaleye göre; siber güvenlik olgunluk seviyesi yetkinlik modeli (C2M2) ve Ulusal Standartlar ve Teknoloji Enstitüsü Siber Güvenlik Çerçevesi (NIST CSF), kapsamlı bir yaklaşım sunan modellerdir [103]. Olgunluk modelinde, kurum ve kuruluşların zayıf ve güçlü yönlerini belirlemeye yönelik ölçüm sağlayan alanlar vardır. Bu modelin başarıya ulaşması için ise her kurum ve kuruluşun kendi ölçme ve iyileştirme olgunluk seviye modelini benimsemeleri gerekmektedir. Dolayısıyla bir olgunluk modeli, bir kurumun uygulamalarının, süreçlerinin ve yöntemlerinin mevcut yetenek seviyesine dair değerlendirmelerde ve iyileştirmelerde bulunarak kıyaslama sağlamaktadır [103].

Gizli Markov modeli, sistemin durumunu temsil eden gizli süreçleri ele alarak çalışır. Çok fazla saldırı olasılığını tahmin etmek ve izinsiz girişleri belirlemek üzere hazırlanmış bir modeldir [104]. Ağ üzerine kurulan sensörler yardımıyla cihaz ya da program aracılığıyla bilgi toplanıyorsa bunu tespit edip, verileri filtreleyen bir yapısı vardır.

Kritzinger ve Von Solms [105] büyük çoğunluğu ev kullanıcılarının oluşturduğu bir kitleye yönelik öne sürdükleri modelde, güvenliğin önemi hakkında bilinçlendirme yoluna gitmişlerdir.

Model, kullanıcı tarafından benimsenmesi kolay bir modeldir. Bu sayede bazı davranışsal değişiklikler yapma etkisi daha yüksektir. Ağ yapısı ile ev kullanıcısı arasında doğrudan ya da dolaylı olarak güven ilişkisi kurması da tercih edilme şansını artırmaktadır.

Diğer yaygın model türlerinden biri de matematiksel analizlere dayalı olan kavramsal modeldir. Bilimsel olarak kabul edilmiş tutarlı bilgiyi kabul eder. Yani zihinsel ya da içsel güdülere dayanan, kişisel deneyimlerden ortaya çıkan bilgidense matematiksel formülasyonlarla açıklanan bilgiyi yapısında kullanır. Kavramsal model ayrıca gerçek nesneler, olaylar ve durumları basitçe temsil eder. Kavramsal modelin oluşturulması ve kişiler tarafından anlaşılabilmesi için bilgi birikimi gerekmektedir [106].

Siber güvenlik kümeleme modelinde ise; araştırma ve geliştirme faaliyetleri kümelenme oluşumunun en temel gayeleri sayılmaktadır. Küme, kamu ve özel sektörün yanı sıra üniversitelerin siber güvenlik alanındaki uzmanlık ihtiyaçlarına cevap verecek şekilde düzenlenmelidir ilkesini de benimsemiştir. Bu model; siber güvenlik alanında milli kritik

ihtiyaların karřılanması iin kamuda yrtlen projeler kapsamında kmeyle entegre olmalı ve oluřturulacak platforma fon akıřı saėlamalıdır [107].

Ortaya konan modellerin ortak paydası; organizasyonların yapısını glendirmek, olası saldırıları nceden tespit etmek ve nlem almak, kurum/ kuruluř ile kullanıcılar arasındaki birlikteliėi saėlamak ve kullanıcıları siber gvenlik konusunda daha fazla bilinli hale getirmektir.

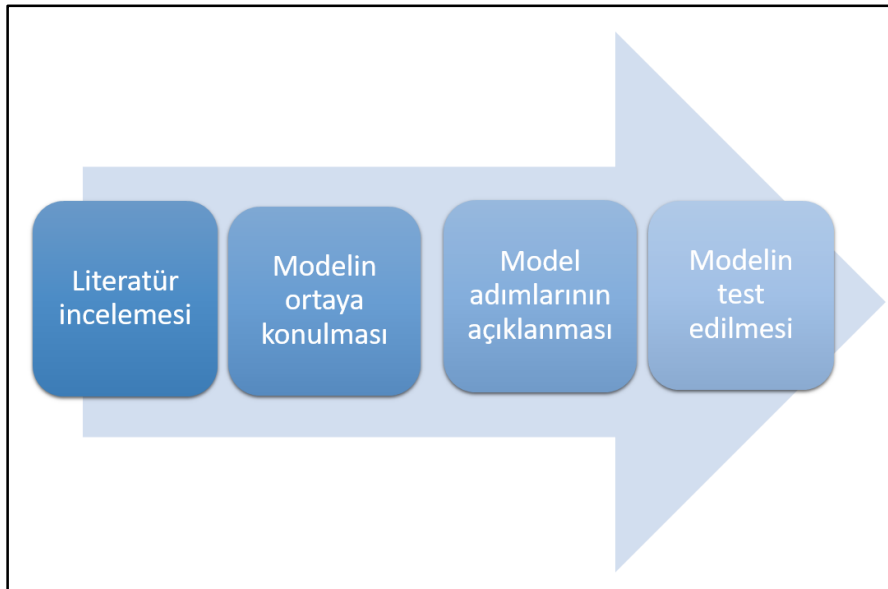




4. MATERYAL VE YÖNTEM

Bu araştırma 2020 yılı içinde kamu kurumları ve çalışanları temel alınarak gerçekleştirilmiştir. Araştırma süreçleri, araştırmaya katılanlar, tasarlanacak olan modelin girdileri kamu kurumlarından elde edilmiştir. Bu bağlamda ortaya çıkan çözüm modelinin, kamu kurumlarının kullanımı için olduğu söylenebilir.

Siber güvenliğin en zayıf halkası olan insan faktörü üzerinde durulan bu çalışmada, insanlardan kaynaklanan zafiyetleri en aza indirmek ya da tamamen ortadan kaldırmak amacıyla yola çıkılmıştır. İncelenen siber güvenlik raporları, bu alandaki çalışmalar, tezler, makaleler ve birçok doküman insan unsurunun eğitim olsa dahi istenen bilinç ve farkındalık düzeyine erişmediğini açıkça ortaya koymaktadır. Bu tezin çıkış noktası da burası olmuş ve geliştirilecek modelin eğitimle beraber kullanıcılarda istenen bilinç ve farkındalık seviyesini oluşturması planlanmıştır. Siber güvenlik, sosyal mühendislik, bilgi güvenliği gibi konularda çeşitli modeller önceki çalışmalarda da yapılmıştır. Fakat bu tezin ortaya koyduğu model sadece kamu kurumlarına özel olmakla beraber yapısındaki filtre mantığıyla bir filtreleme yaparak aşama aşama ilerlemesi ve en son kısımda kullanıcıyı doğru karar vermeye yönlendirmesi açısından tektir.



Şekil 4.1. Model geliştirilirken uygulanan adımlar

Şekil 4.1’de sosyal mühendisliğe karşı bir model geliştirilirken uygulanan adımlar gösterilmektedir. Bu adımlara ilerleyen başlıklarda tek tek değinilecektir.

4.1. Çalışma Grubu

Çalışmaya katılan kullanıcılar kamu kurumunda görev yapan, yaşları 21 ile 65 arasında değişen kadın ve erkeklerden oluşmaktadır. Katılımcıların eğitim durumlarını Ortaöğretim ve Yükseköğrenim (Ön Lisans, Lisans, Yüksek Lisans ve Doktora) mezunları oluşturmaktadır. Katılımcıların görev ve unvanları çalıştıkları birimlere göre değişkenlik göstermektedir. Tekniker veya mühendis kökenli olup teknik bilgisi olan kullanıcıların yanı sıra bilgisayar kullanım becerisi, teknolojik gelişmeleri takip etme ve ayak uydurma konusunda yeterli düzeyde olmayan kullanıcılarda çalışmada yer almıştır. Yaş, cinsiyet ve teknolojik cihazları kullanım becerileri farklılıklar gösteren kullanıcılar, hemen hemen her kamu kurumunda karşımıza çıkacağı için çalışmanın ortaya koyacağı sonuçları değerlendirmede bu önemlidir.

Çizelge 4.1’de çalışmaya katılan kullanıcıların cinsiyete göre dağılımları verilmiştir. Bu tablodan anlaşılabacağı üzere, katılımcılar büyük oranda erkeklerden oluşmaktadır. Nitekim bu oranlar; birinci uygulamada yaklaşık %63, ikinci uygulamada %54 ve üçüncü uygulamada %74’tür. Kadınlar ise yaklaşık olarak birinci uygulamada %37, ikinci uygulamada %46 ve üçüncü uygulamada %26’lık oranlara tekabül emektedir.

Çizelge 4.1. Çalışma grubunun cinsiyete göre dağılımı

CİNSİYET	Birinci Uygulamaya Katılan	İkinci Uygulamaya Katılan	Üçüncü Uygulamaya Katılan
KADIN	258	56	7
ERKEK	442	67	20

Çizelge 4.2’de çalışmaya katılan kullanıcıların yaş gruplarına göre dağılımları verilmiştir. Bu tabloyu ele aldığımızda gerçekleştirilen üç uygulama için yaşa bağlı genel bir oran belirlemek zordur. Keza birinci uygulamada uygulamaya katılanların büyük çoğunluğu 51 yaş ve üzeri iken üçüncü uygulamaya katılanların çoğunluğu 21-30 yaş arası kişilerden oluşmaktadır.

Çizelge 4.2. Çalışma grubunun yaş dağılımları

YAŞ DAĞILIMLARI	Birinci Uygulamaya Katılan	İkinci Uygulamaya Katılan	Üçüncü Uygulamaya Katılan
21-30	135	38	10
31-40	196	30	7
41-50	165	31	4
51 ve Üzeri Yaş	204	24	6

Çizelge 4.3'te birinci uygulamaya katılan kullanıcıların öğrenim durumları ve cinsiyetlerine göre dağılımları verilmiştir. İlk uygulama daha fazla kişi üzerinde uygulandığı ve öğrenim durumlarının hemen hemen hepsine ait kullanıcı profili barındırdığı için tabloya alınmıştır. Tablo incelendiğinde; katılımcıların yaklaşık %34'ü ortaokul, lise ve ön lisans mezunu iken yaklaşık %53'ü lisans ve yaklaşık %12'si yüksek lisans ve doktora mezunudur.

Çizelge 4.3. Çalışma grubunun öğrenim durumuna göre dağılımı

CİNSİYET	Ortaokul, Lise ve Ön Lisans	Lisans	Y. Lisans ve Doktora
KADIN	79	148	31
ERKEK	160	228	54

4.2. Önerilen Model

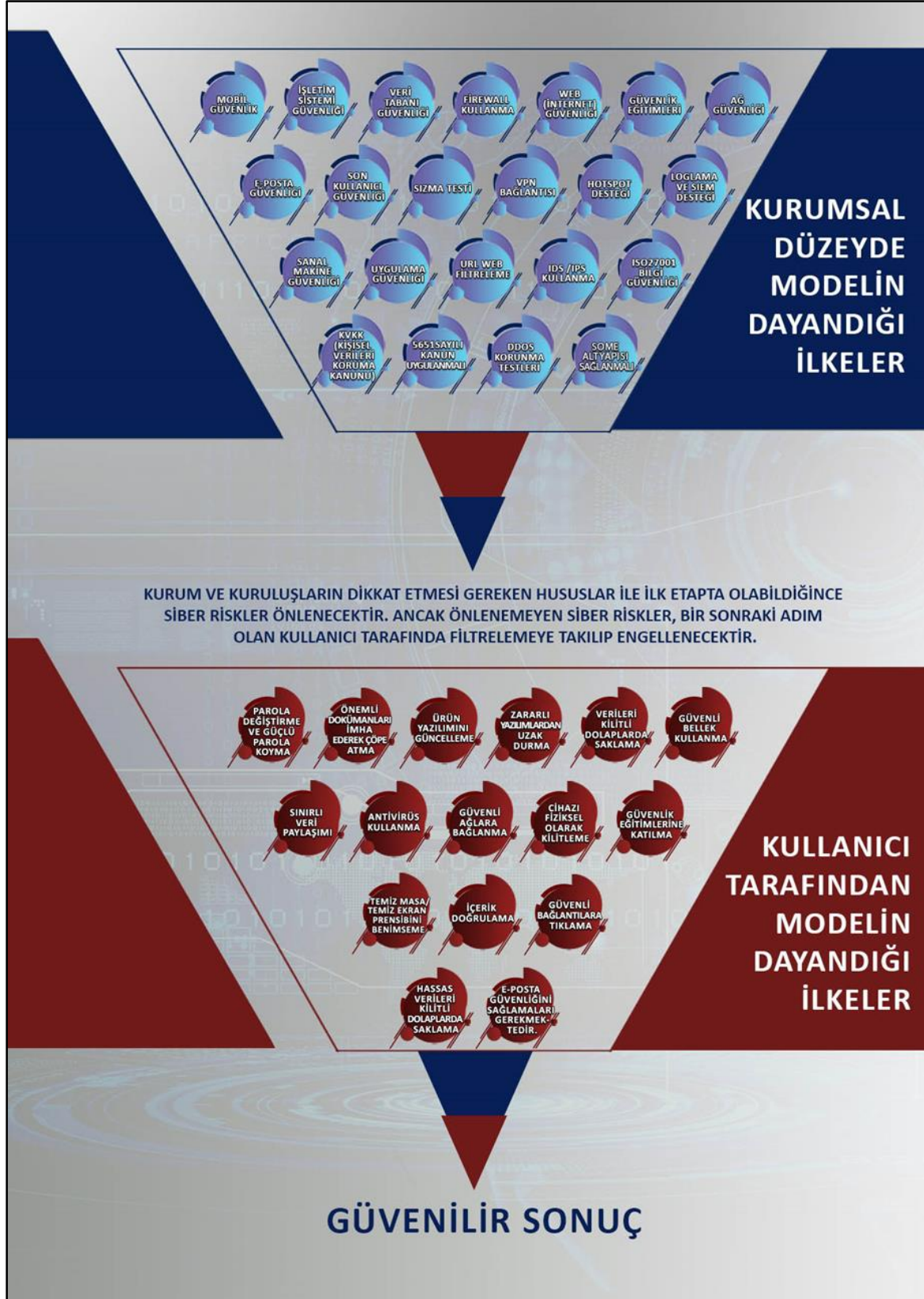
Günümüzde kamu kurum ve kuruluşları, siber tehdit ve risklere karşı kendi sistem altyapılarında farklı katmanlarda siber güvenlik çözümleri kullanmakta, ayrıca zaman zaman sistemlerinde olabilecek güvenlik açıkları ve zafiyetleri tespit ederek önlem almak maksadıyla sızma testleri yaptırmaktadırlar. Fakat güvenlik cihazlarına ve klasik sızma testlerine dayalı bir siber güvenlik algısı, birçok kamu kurum ve kuruluşunu siber saldırılara karşı korumada yetersiz kalmaktadır. Dahası bazen tersine sahte bir güvenlik duygusu yarattığı için o kamu kurum ve kuruluşunu siber saldırılara karşı daha hassas hale getirmektedir. Oysa siber güvenlik, insan ve cihazın içinde yer aldığı her işlem ve adımını kapsayan geniş ve uzun bir süreç yönetimidir.

Siber güvenlikte sosyal mühendisliğe karşı bir model geliştirilmesine yönelik yapılan bu çalışmada süreci doğru ve kapsamlı olarak yönetmek çıkış noktası olmuştur. Öncelikle literatürde bulunan farkındalık modellerine dayalı çalışmalar detaylı olarak incelenmiş ve bu çalışmaların zayıf ve güçleri yönleri tespit edilmiştir. Ayrıca gerçek hayatta kurumlarda

alıřan personel ve ynetimler gzlemlenmiř eksik ynleri belirlenmiřtir. Bu doėrultuda alıřma řekillenmiř, zayıf ve eksik ynlerin giderilmesini saėlayacaėı dřnlen bir model geliřtirilmiřtir. Literatrde bulunan alıřmalar ve Trkiye’de bulunan, alanında en iyi hizmet veren siber gvenlik firmalarının yıllık raporları ve zm nerileri doėrultusunda model adımları ve ierikleri řekillenmiřtir. Model genel anlamda  adımdan oluřturulup her adım kendi arasında detaylandırılmıřtır. Birinci adım kurumun siber gvenlik tehditlerine karřı alması gereken nlemleri ifade ederken, ikinci adım alıřanların bireysel olarak siber gvenlik tehditlerine karřı almaları gereken nlemleri ifade etmektedir. nc ve son adım ise monitoring olarak isimlendirilen aslında modelin gerek ortamda gerek kullanıcılarla hazırlanan sosyal mhendislik saldırı senaryoları ile test edildiėi adımdır. Bu adım geliřtirilen siber gvenlikte sosyal mhendisliėe karřı bir modelin doėrulanması ve deėerlendirilmesi aısından nemlidir.

Modelin oluřturulurken temel aldıėı ilkeler;

- Modelin tasarımının amacı problemi zmektir.
- Problemi doėru tanımlamak, kamu kurumlarına ve alıřanlarına sunulabilecek ilk ve belki de en deėerli hizmettir.
- Zaman, yeri doldurulamayan bir kaynaktır. Verimlilik ise hizmet edilen sre boyunca kutsaldır. Ortaya konan model bunların kullanımını gz ardı etmemelidir.
- Model geliřen teknoloji ve aėın gereksinimlerine ayak uydurabilecek řekilde dinamik bir yapıya sahiptir. Kapsamı oluřturan tanımlamalar deėiřirse, yeniden tanımlanabilir. Modele ekleme, ıkarma ya da herhangi bir deėiřiklik kolaylıkla yapılabilir.



Şekil 4.2. Çalışma kapsamında önerilen filtre model

Filtre model Şekil 4.2’de görüldüğü gibi aşama aşama ilerler ve sonuca ulaşır. İlk filtrede kurum ve kuruluşların dikkat etmesi gereken ilkelerden bir kısmı genel hatları ile verilmiştir. Bu ilkelerin tamamı eksiksiz organizasyon bünyesine uygulandığında olası bir siber riskin önlenebileceği değerlendirilmektedir. Önlenemeyen siber riskler ise ikinci adım olan kullanıcı tarafında filtrelemeye takılarak engellenecektir. İkinci filtrede de modelin kullanıcı tarafında dayandığı ilkelerin bir kısmı genel hatları ile verilmiştir. Bu ilkelerin tamamının da eksiksiz olarak kullanıcılar tarafından uygulanıyor olması büyük önem arz etmektedir. Nihayetinde kamu kurum ve kuruluşu ile kullanıcı filtrelerinde yer alan saldırı önleyici adımlar, son kullanıcıyı güvenli hareket etmeye sevk edecektir.

4.2.1. Modelin adımları

Siber saldırılarda sosyal mühendislik yöntemi ile kullanıcıları sömürmek en yaygın yöntemlerden biridir. Sosyal mühendislerin kullanıcı zafiyetlerinden sıklıkla yararlanması ve kurumsal yapıya maddi ve manevi zararlar vermesi geçmişten beri süregelen bir durumdur. Kurumsal yapıyı kullanıcıdan, kullanıcıyı da kurumsal yapıdan ayrı düşünerek hareket etmek bu bağlamda yanlış olacaktır. İkisi arasındaki ilişkiyi kullanmak ve bir döngüye oturtarak hareket etmek bu modelde önem arz etmektedir. En genelden en özele doğru düşünülecek olursa kurumsal yapı geneli, kullanıcı ise özeli temsil eder. Model ise genelden özele doğru filtreleme yaparak ilerleyeceği için alınabilecek önlemler öncelikle kurumsal yapının filtresinden daha sonra kullanıcının filtresinden geçer. Son olarak filtrenin süzgecinde kalan ise kullanıcının güvenli dediği, sosyal mühendislik saldırı riskini ortadan kaldırdığı güvenli adımdır. Daha detaylı bu adımları başlıklar halinde aşağıda incelenmektedir.

Kurumsal düzeyde modelin dayandığı ilkeler

Kurumlar, günümüzde güvenli ve riskten uzak bir çalışma ortamına daha çok ihtiyaç duymaktadır. Sahip oldukları verilerin gizliliğini sağlayarak, erişim haklarını kontrol altında tutabildikçe, iş sürekliliklerini ve varlıklarını da uzun yıllar boyunca sürdürebileceklerdir. Bunların sağlanabilmesi içinde kurumların bünyelerinde olması gereken güvenlik tedbirleri derlenerek modelin ilk aşaması oluşturulmuştur. Bu maddeler, Türkiye’de hizmet veren büyük güvenlik şirketlerinin çalışmaları, siber güvenlik raporları ve akademik çalışmalar derlenerek, ortak payda da en çok vurgulanan kamu kurumlarının dikkat etmesi gereken

hususlar ışığında hazırlanmıştır. Eğer bir kamu kurumunda belirtilen ilkeler mevcutsa olası bir sosyal mühendislik saldırısını büyük oranda elimine edeceklerdir.

Modelin ilk adım girdileri maddeler halinde aşağıda belirtilmektedir.

- Kurumsal bilgi güvenliği süreci ISO 27001 standardı gereksinimlerine uygun olarak yürütülmelidir [39].
- Kurum sistem odasının emniyeti sağlanmalıdır [39]. Kimlik doğrulama kartı ya da PIN koruması gibi yöntemlerle yetkili kişilerin içeri girişi sağlanmalıdır.
- Kurumlar bilgi güvenliği olaylarına müdahale prosedürleri hazırlamalı, olay anında prosedüre uygun olarak müdahale edilmelidir [39].
- Kurumlar en az iki yılda bir kez bilgi sistemlerine açıklık analizi ve sızma (penetrasyon) testi yaptırmalı, elde edilen sonuçlara göre gerekli düzeltmeleri gerçekleştirmelidir [39].
- Kurumlar mevzuattan kaynaklanan insan kaynakları güvenliğinin sağlanması, denetim kayıtları tutulması, lisanslı yazılım kullanılması vb. bilgi güvenliği önlemlerini almalıdır [39].
- Kurum, işten ayrılan çalışanlar için uyulması gereken güvenlik prosedürleri hazırlamalıdır. İşten ayrılan çalışanın kimlik kartı alınmalı ve yazıyla idareye iade edilmelidir [45].
- Kurum, işten ayrılan personellerin kullandıkları sistem parolalarını hemen pasif hale getirmelidir [45].
- Kurum, kendi içinde belirlediği hassas bölgelere 24 saat aktif güvenlik kameraları yerleştirilmelidir [45].
- Kurum personeline belirli aralıklarla bilgi güvenliği bilinçlendirme eğitimleri verilmelidir. Kullanıcılar riskler hakkında bilgilendirilmelidir [45].
- Kurum yakın zamanda meydana gelen sosyal mühendislik ile ilgili vakaları takip etmeli ve yeni çıkan sosyal mühendislik yöntemlerini bilmelidir [45].
- Kurum periyodik olarak, sosyal mühendislik saldırı testini de içerisinde barındıran bilgi güvenliğine dayalı testler gerçekleştirmelidir [45].
- Kurum sosyal mühendislik konusunda farkındalığı artırmak için Catch me if you can (Sıkıysa Yakala), Who am I (Ben Kimim), Plastic gibi içeriği sosyal mühendislik olan filmleri personeline izletebilir [45].
- Kurumların antivirüs politikası olmalıdır [85].
- Kurumların operasyon güvenliği politikası olmalıdır [85].

- Bilgi varlıkları yönetim politikası olmalıdır [85].
- E-posta ve mesajlaşma güvenliği politikası olmalıdır [85].
- Kurum içerisinde parola belirleme politikası olmalıdır [85].
- Kurumlarda Sanal Özel Ağ (VPN-Virtual Private Network) bağlantısı olmalıdır. Kullanıcılara verilen şifreler e-posta yoluyla değil SMS yoluyla gönderilmelidir [99].
- Kurumsal Siber Olaylara Müdahale Ekibi (SOME) altyapısı sağlanmış ve SOME ekipleri kurulmuş olmalıdır [99].
- Kurumda sistem ele geçirilse dahi verilerin sızdırılmasını engellemek için Veri Kaybı Önleme (DLP-Data Loss Prevention) desteği olmalıdır [108].
- Kurumlarda Dağıtık Hizmet Engelleme Saldırılarına (DDoS-Distributed Denial of Service) karşı korunma testleri yapılmalıdır [108].
- Kurumda URL Web Filtreleme (URL Web Filtering) yöntemi olmalıdır. Bu filtreleme yöntemi güvenli web trafiği sağlayarak zararlı sitelerden ve yazılımlardan koruma sağlayacaktır [108].
- Kurum, özellikle misafir kullanıcılar için tek kullanımlık şifre gönderen HotSpot desteği sağlamalıdır. İnternet erişimini sınırlayarak güvenlik açıklıklarının azaltılmasına yarayacaktır [108].
- Kurumlarda olası saldırıları tespit etmek için Saldırı Tespit Sistemleri (IDS-Intrusion Detection Systems) olmalıdır. Ağın izlenmesinde ve trafiğin analiz edilmesinde önemli bir güvenlik bileşeni olarak hizmet verecektir [108].
- Saldırıların saptanıp engellenmesi işlemlerini kapsayan ağ güvenlik sistemi, Saldırı Önleme Sistemleri (IPS-Intrusion Prevention Systems) olmalıdır [108].
- Kurumlarda logları daha iyi analiz edecek ve muhtemel siber saldırıları tespit etmeye yardımcı olacak Güvenlik Bilgileri ve Olay Yönetimi (SIEM -Security Information and Event Management) korelasyon tekniği olmalıdır [108].
- Kurumlar veri tabanındaki verilerini önem derecesine göre sınıflandırmalıdır. Veri tabanı güvenlik analizlerini düzenli yapmalı ve raporlamalıdır [108].
- SQL komutları izlenmeli, loglanmalı ve zararlı bir komut gelmesi engellenmelidir [108].
- Kurumlarda 5651 kanun maddesi internet erişiminin kontrolü için uygulanmalıdır [108].
- Kurumlarda, kullanıcıların izni olmadan kişisel verilerinin işlenmesini önleyecek düzenlemeler getiren Kişisel Verilerin Korunması Kanunu (KVKK) benimsenmelidir [108].

- Kurumlar dışardan gelecek ataklara karşı kullanıcılarını korumak, içerideki veri dolaşımını ve dışarıya veri çıkışını düzenleyebilmek için Son Kullanıcı Güvenliği (End-User Security) denetimini uygulamalıdır [109].
- İnternet bağlantıları için Güvenlik Duvarı (Firewall) kullanılmalıdır [110].
- Kurumlar kullandıkları işletim sistemlerinin ve uygulamalarının güncellemelerini zamanında yapmalıdır [110].
- Kurumun önemli verileri ve bilgileri düzenli olarak yedeklenmeli, yedekleri kurum sunucuları dışında bir yerde muhafaza edilmelidir [110].
- Kurumda bulunan Wi-Fi ağlarının güvenliğinden gizliliğinden emin olunmalıdır [110].
- Kurumdaki her çalışana, özel ve ayrı birer kullanıcı girişi ve şifresi tanımlanmalıdır [110].
- Kurumlar kullanıcı kimlik doğrulaması ve grup yönetimi için Active Directory, LDAP entegrasyonu kullanılmalıdır [111].
- Kurumlar URL adresleri ve sayfa içerikleri için filtreleme özelliği olan yapılar kullanılmalıdır [111].
- Kurumlar gizlilik ihtiva eden yazılar için çalışanlarına kilitli dolaplar tahsis etmelidir [112].
- Kurumlar faks makinelerinde giden gelen yazıları sürekli kontrol etmeli ve makinelerde yazı kalmamasına dikkat etmelidir [112].
- Kurum varlıklarının yetkisiz olarak kurum dışına çıkarılıp çıkarılmadığına dair denetimler yapılmalıdır. Bu denetimlerden kurum çalışanlarının haberdar olması sağlanmalıdır [112].
- Kurumlar mevcut envanterleri dışındaki donanımların kurum bilgisayarlarında kullanımını engellemelidir [112].
- Kurumlar, kullandıkları işletim sistemlerinde kurulumda gelen yönetici hesaplarının (Administrator, root) kaba kuvvet saldırılarına karşı, Microsoft ürünlerinde pasif hale getirmesi, Linux tabanlı ürünlerde root hesabına SSH erişimi yapılmasını engellemesi gerekmektedir [112].
- Kurumlar kullanıcıların aktivitelerini, güvenlik zafiyetlerine ve bilgi sızdırmalarına karşı loglayarak kayıt altına almalıdır [112].
- Kurumlar kullanıcıların farkında olmadan yapabilecekleri ve sonunda zafiyet yaratabilecek değişiklikleri merkezi grup politikalarıyla engellemelidir [112].
- Kuruma hizmet veren tüm uygulama, veri tabanı sunucuları ve disk üniteleri kurumun veri merkezlerinde veya idarece uygun görülen güvenli fiziksel alanlarda konumlandırılmalıdır [112].

- Kurum sunucularında, üçüncü parti firmalar ile yapılacak çalışmalarda, ilgili sunucuyla yetkilendirilmiş personel çalışmaya eşlik etmelidir [112].
- Kurum kullanılmayan sunucu, servis ve uygulamaları kapatmalıdır [112].
- Kurumun sistem yöneticileri 'Administrator' ve 'root' gibi genel sistem hesaplarını kullanmamalıdır. Sunuculardan sorumlu personelin istemciler ve sunuculara bağlanacakları kullanıcı adları ve parolaları farklı olmalıdır [112].
- Kurum sunucularına ait bağlantılar normal kullanıcı hatlarına takılmamalıdır. Sunucu VLAN'larının tanımlı olduğu portlardan bağlantı sağlanmalıdır [112].
- Kurumlar kablosuz ağ güvenliği için güçlü bir şifreleme ve erişim kontrol sistemi kullanmalıdır. Bunun için Wi-Fi Protected Access2 (WPA2-kurumsal) şifreleme kullanılabilir. IEEE 802.1x erişim kontrol protokolü ve TACACS+ ve RADIUS gibi güçlü kullanıcı kimlik doğrulama protokolleri de kullanılabilir [112].
- Kurumlarda erişim cihazları üzerinden gelen kullanıcıların internete çıkış bant genişliğine sınırlama getirilmeli ve kullanıcılar tarafından kurumun tüm internet bant genişliğinin tüketilmesi engellenmelidir [112].
- Kurumda kablosuz ağa dâhil olan kurum çalışanları için bile erişimler gerektiğinde sınırlandırılmalıdır. Sadece internete çıkacak olan kullanıcıların kablosuz ağ üzerinden diğer uygulamaların (ses, güvenlik, mobilite vb.) çalıştığı networklere erişimi engellenmelidir. Bu duruma ilaveten gerekirse erişim sağlanan networkler farklı IP aralıkları üzerinde ayarlanmalı, cihaz üzerinde yetki kuralları (Access Control Listler) oluşturulmalıdır [112]. Ağ Erişim Kontrolü (NAC-Network Admission Control) devreye alınmalıdır.
- Kurumda geliştirilen yazılımların gizlilik, bütünlük ve erişebilirlik şartlarına uygun olması sağlanmalıdır [112].
- Kurum ile dış dünya arasında ki yazışmalar bir e-posta güvenlik cihazı ile kontrol edilmelidir. SPAM, virüs, kurum politikalarına uygun olmayan içerikler engellenmelidir [112].
- Kurum sunuculara erişim politikasında kullanıcı erişimi için SSH, RDP gibi protokollerle sunucu yönetimi için belirli portlara erişim izni vermelidir [112].
- Kurum dış dünyadan sunucular üzerindeki servislere erişmek için 80, 443, 7001, 8080, 8443 gibi servis portlarına özel durumlarda izin vermelidir. Kurum adına Güvenlik Birimi tarafından bu işlem sağlanmalıdır [112].
- Kurum içerisinde oluşturulan ortak dosyalara erişecek kullanıcılar ve hakları “bilmesi gereken” prensibine göre belirlenmelidir. Erişecek kullanıcıların hakları yazma, okuma,

değiştirme ve çalıştırma yetkileri göz önüne alınarak oluşturulmalıdır. Verilen haklar belirli zamanlarda kontrol edilmeli, üzerlerinde değişiklik gerekiyorsa yapılmalıdır [112].

Bahsedilen tüm maddeler artırılabilceği gibi bu maddeler kendi içlerinde alt başlıklar halinde de kısımlara ayrılabilir. Şekil 4.3 kurumların alması gereken önlemleri ifade etmektedir.



Şekil 4.3. Ana başlıklar halinde kurumların alması gereken önlemler

Modelin ilk adımı olan kurumların alması gereken önlemler Şekil 4.3'te tüm kurumsal ilkelerin filtre modele girişlerini temsil etmesi açısından genel başlıklar halinde verilmiştir. Maddeler, bu genel başlıkların daha özele indirgenmiş halleridir ve detaylı olarak bu başlık altında açıklamaları ile verilmiştir.

Kullanıcı tarafından modelin dayandığı ilkeler

Modelin ikinci adımı kullanıcıların alması gereken önlemleri içermektedir. Kullanıcı önlemlerinin ikinci adım olması dikkat çekebilir. Elbette ki tezin amacı, kullanıcı zafiyetlerini en aza indirecek veya tamamen ortadan kaldıracak bir model ortaya koymaktır. Fakat bir kamu kurumunda siber saldırıya uğrama boyutunu en genelden en özele doğru indirgeyerek ilerlemek daha sağlıklı bir sonuç ortaya koyacaktır. Modelin her adımı tüm

olası durumları düşünerek onlara göre de en genel çözüm önerilerini içermektedir. Modelin ilk adımı kurumun alabileceği önlemleri içerir ve saldırgan bir şekilde bu adımdan geçebilmişse ikinci adımda filtreye takılacaktır. Yine burada belirtilen maddeler de Türkiye’de hizmet veren büyük güvenlik şirketlerinin çalışmaları, siber güvenlik raporları ve akademik çalışmalar derlenerek, ortak payda da en çok vurgulanan kullanıcıların dikkat etmesi gereken hususlar ışığında hazırlanmıştır. İkinci adımın kullanıcı tarafından alınabilecek önlem girdileri aşağıda belirtilmektedir.

- Kullanıcılar çöpe atacakları belge veya dokümanları, kırpıcılardan geçirmeli veya okunamayacak şekilde imha etmelidir [45].
- Kullanıcılar şifre korumalı ekran koruyucular kullanmalıdır [45].
- Şifrelerini kâğıtlar üzerine yazarak görülebilecek yerlere asmamalı ve bu konuda dikkatli olmalıdırlar [45].
- Tanımadıkları kişilerden gelen isteklere karşı her zaman şüphecî ve temkinli davranmalıdırlar [45].
- Kullanıcılar kişisel şifrelerini bir başkasıyla kesinlikle paylaşmamalıdır [45]. Sistemlere etki alanı dâhilinde kurumun verdiği kullanıcı adı ve şifreleri ile giriş yapmalıdırlar.
- Telefonda kendisini polis, savcı, asker vb. şekillerde tanıtırak bankaya para yatırımları gerektiğini veya belirttikleri yere para, altın bırakmalarını isteyen bir telefon araması ile karşılaştıklarında 155’i veya yetkili kişileri arayarak durumu bildirilmelidirler [45].
- Sosyal mühendisler, kişisel bilgilerini ele geçirdikleri kullanıcılar adına habersizce telefon hatları çıkarabilirler. Kullanıcılar operatörlere ait sitelerden veya e-devlet üzerinden adlarına kayıtlı bulunan telefon numaralarını takip etmelidir [45].
- Kullanıcılar çevrelerindeki en yakın kişilerin bile sosyal mühendislik teknikleri ile birbirlerini aldatabileceğini unutmamalıdır [45].
- Kullanıcılar bilgi güvenliği için birden fazla e-posta kullanmanın bazı durumlarda daha etkili olabileceğini bilmelidir. Özellikle internet alışverişlerinde ve kurum dışı işlemlerinde kurum e-posta adreslerini kullanmamalıdır [45].
- Kullanıcılar çoğunlukla temiz masa/temiz ekran politikası uygulamalıdır [45].
- Sosyal mühendislerin kurbanlarına daha çok yardım talebi tekniğiyle yaklaştıklarını bilmelidirler [45].
- Özellikle telefonda, her hangi bir istekte bulunan kişinin sesi tanıdık gelmiyorsa ve istekte bulunmak için herhangi bir nedeni yoksa hiç kimseye kişisel bilgilerini ve kredi kartı bilgilerini vermemelidirler [45].

- Kullanıcılar T.C. kimlik numarası, telefon numarası, doğum yeri ve tarihi gibi hassas kişisel bilgilerini facebook, twitter vb. sosyal medya platformlarında paylaşmamalıdır [45].

Profillerini kısıtlı kullanmalı ve tanımadıkları kişilerden gelen arkadaşlık isteklerini kabul etmemelidirler.

- Kullanıcılar sosyal mühendislik saldırılarına karşı en etkin yolun insan güvenlik duvarı, yani kendi yaşamlarında davranışlarıyla uygulayacakları güvenlik duvarının olduğunu bilmelidir [45].
- Kullanıcılar herhangi bir yetki talebinde bulunuyorsa bağlı olunan kurumdan resmi yazı almalıdır [68].
- Kullanıcılar kurulumda gelen modem şifresini değiştirmeli ve başkaları ile paylaşmamalıdır [99].
- Kamera, akıllı TV vb. cihazların internet bağlantılı olarak kullanıldığını ve bunlara erişilebileceğini bilmelidirler [99].
- Kullanıcılar güvenlik olaylarını kurumsal ya da kişisel olarak nereye bildirmeleri gerektiğini bilmelidir [99].
- Kullanıcılar kişisel verilerin korunmasına yönelik temel kanunları bilmelidir [99].
- Kullanıcılar “sertifika süresi doldu”, “... hatası onaylayın” gibi sıra dışı uyarılardan şüphelenmelidir [99].
- Kullanıcılar kontrolleri dışında kurulan eklentileri cihazlarından kaldırmalıdır [99].
- Kullanıcılar mobil cihazlarının güvenli kullanımına yönelik önlemleri almalıdırlar. Güvenilir olmayan yerlerde cihazlarını şarj etmemelidir [99].
- Mobil güvenlik konusunda kullanıcılar ihtiyaç duyduğu uygulamalar dışında uygulamaları cihazlarına kurmamalıdır [99].
- Kullanıcılar çerez (cookies) kayıtlarını düzenli olarak silmelidir [99].
- Kullanıcılar SMS olarak gelen iletilerdeki bağlantı linklerine tıklamamalıdırlar [99].
- Kullanıcılar mobil güvenlikleri için ayrıca otomatik ekran kilidini kullanmalıdırlar [99].
- Kullanıcılar internet üzerinde şifreli bazı sayfalara girmişse, işleri bittiğinde çıkış (sign-out, logout) yapmayı unutmamalıdır [108]. Sadece browserı kapatmak yeterli olmayabilir.
- Kullanıcılar kimliklerini belgeleyen kurum kartlarını görünür şekilde üzerlerinde bulundurmamalıdır [112].

- Kullanıcılar kurumsal yönetim sistemi üzerinden işlem yaptığında (izin kâğıdı, yıllık izin gibi) ekranda bulunan kişisel bilgilerinin diğer kişi veya kişilerce görülmemesine dikkat etmelidir [112].
- Kullanıcılar saklanan veya iletilen hassas veya kritik bilgide gizlilik, bütünlük ve güvenlik esasına göre kriptolama yöntemi yani şifreleme, sayısal imza veya mesaj doğrulama kodlarını kullanmalıdır [112].
- Kullanıcılar sunuculara kriptolu bağlantı ile bağlanmalı, kripto (şifreli yazı) kullanmayan yöntemleri tercih etmemelidir. Düz metin kullanarak veri alışverişi yapan yöntemlerin kullandığı portları gerekirse kapatılmalıdırlar [112].
- E-postaya eklenecek dosya uzantıları “.exe”, “.vbs” veya yasaklanan diğer uzantılar olamaz. Zorunlu olarak bu tür dosyaların iletilmesi gerektiği durumlarda, kullanıcılar dosyaları sıkıştırarak (zip veya rar formatında) mesaja eklemelidir [112].
- Kullanıcılar sunucu üzerinde zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırmamalıdır [112].
- Kullanıcılar bilinmeyen veya şüpheli kaynaklardan dosya indirmemelidir [112].
- Kullanıcılar “kazaa, emule” gibi dosya paylaşım yazılımlarını kullanmamalıdır [112].
- Kullanıcılar kuruma ait hiçbir gizli bilgiyi, yazıyı sosyal medyada paylaşmamalıdır [112]. Kurum içi bilgi mahremiyetini sağlamalıdırlar.
- Kullanıcılar güvenli olmayan kablosuz ağlar üzerinden internete çıkmaya çalışmamalıdır [113].
- Kullanıcılar bilgisayarlarında yer alan gereksiz bilgileri, gereklilerden ayırt ederek düzenli olarak silmelidir [113].
- Kullanıcılar aynı kullanıcı adı ve şifre ile farklı web sitelerine veya online (çevrimiçi) hesaplara giriş yapmamalıdır [113].
- Kullanıcılar gizli bilgilerini depolamak için düzgün şekilde şifrlenmemiş USB sürücülerini kullanmamalıdır [113].
- Kullanıcılar ofis dışına çıktıklarında ya da başka bir sebeple yerlerinden ayrıldığında bilgisayarlarını açık, güvensiz şekilde bırakmamalıdır [113]. Örneğin Windows + L tuşu ile ekran kilitlenebilir.
- Kullanıcılar kuruma ait önemli verilerin olduğu bir USB sürücüyü kaybettiği zaman vakit kaybetmeden bunu yetkililere bildirmelidir [113].
- Uzaktan çalışmakta olan kullanıcı kurumun önemli belgeleri üzerinde çalışıyorsa gizli ekranları kullanmalıdır [113].

- Kullanıcılar yolculuğa çıktığında kurumun hassas verilerini laptoplarında taşımamalıdır [113].
- Kullanıcılar kurum ağına erişmek için kişisel mobil cihazlarını kullanmamalıdır [113].
- Kullanıcılar pop-up'lardan, bilinmeyen e-postalardan ve linklerden kaçınmalıdır. Böyle bir durumda yetkililere haber vermelidirler [114].
- Kullanıcılar parolalarını ve kimlik doğrulamalarını güçlü seçmelidir [114].
- Kullanıcılar güvenli Wi-Fi ağına bağlanmayı her zaman tercih etmelidir [114].
- Kullanıcılar hem kurumda hem de evde güvenlik duvarı korumasını etkinleştirmelidir [114].
- Kullanıcılar düzenli olarak güvenlik yazılımı güncellemelerini yüklemeli ve dosyalarını yedeklemelidir [114]. Ayrıca güvenilir antivirüs programları ve anti-spy yazılımlar kullanılmalıdır.
- Kurumun sağladığı farkındalık eğitimlerine düzenli katılmalı ve benimsemelidirler [114].
- Kullanıcılar internet üzerinden alışveriş yaptığında güvenilir, bilinen siteleri tercih etmelidir [115].
- Kullanıcılar ödeme sayfalarında 3D güvenlik seçeneğini tercih etmeli, ödeme sürecinin tamamlanması için ödeme yapılan banka üzerinde kayıtlı cep telefonu numarasına SMS şifresi ile bankaya ait siteden son bir teyit işleminin gerçekleştirilmesi sağlanmalıdır. Sanal kart kullanımını tercih etmelidirler [115].
- Kullanıcılar alışveriş yaptıkları sitenin güvenlik sertifikası olup olmadığına dikkat etmelidir. Alışveriş yapılan sitedeyken adres çubuğunda “ http:// “ ifadesi yerine “https:// “ ifadesi olup olmadığına dikkat etmelidirler [115].
- Kullanıcılar taraflarına iletilen e-postalarda gönderen kişiyi tanıyıp tanımadıklarını kontrol etmeli, gönderen kişinin görünen adına hemen inanmamalı, gönderici adresini kontrol etmeli ve tanıımıyorsa gelen e-postayı dikkate almadan silmelidir [116].
- Kullanıcılar gelen e-postanın yazım dilini kontrol etmeli; imla hataları veya anlam düşüklüğü varsa bunun büyük olasılıkla sahte bir e-posta olduğunu düşünmelidir [116].
- E-posta genele hitaben mi gönderilmiş yoksa kişisel olarak kullanıcıya mı gönderilmiş kontrol edilmelidir; saldırı e-postalarının genellikle kişiye hitaben değil genele hitaben oluşturulduğu unutulmamalıdır [116].
- Kullanıcılar e-posta içinde yer alan adres linkleri gerçekten belirtilen adrese mi gidiyor diye üzerine tıklamadan kontrol etmeli, mümkünse bağlantıyı tıklamak yerine browser üzerinden kendileri adresi yazarak erişim sağlamalıdır [116].

- Kullanıcılar e-posta ekinde gelen dosyayı açmak istediklerinde çalıştırmak için izin isteyen uygulamaları asla bilgisayarına kurmamalıdır [116].
- Kullanıcılar, kurumların ve bankaların kişisel bilgileri asla e-posta yoluyla istemediklerini unutmamalıdır. Böyle bir durumda gönderen kişinin imza, kurum ve iletişim bilgilerini kontrol etmelidirler [116].
- E-postada her şey yolunda gibi görünüyor olsa bile görünüşe kullanıcılar aldanmamalıdır; en ufak şüphede bile söz konusu e-postayı dikkate almamalı, açmamalı, tıklamamalı ve silmelidirler [116].
- Kullanıcılar “EarthLink Toolbar” gibi zararlı siteleri tespit eden yazılımlar kullanabilir [117].

Bu kısımda da tüm maddeler artırılabilceği gibi alt başlıklar halinde de kendi içlerinde kısımlara ayrılabilir. Şekil 4.4 kullanıcıların alması gereken önlemleri ifade etmektedir.



Şekil 4.4. Ana başlıklar halinde kullanıcıların alması gereken önlemler

Modelin ikinci adımı olan kullanıcıların alması gereken önlemleri Şekil 4.4'te tüm kullanıcı ilkelerinin filtre modele girişlerini temsil etmesi açısından genel başlıklar halinde verilmiştir. Maddeler, bu genel başlıkların daha özele indirgenmiş halleridir ve detaylı olarak bu başlık altında açıklamaları ile verilmiştir.

İzleme (Monitoring) süreci

Modeli test etmek üzere kullanıcılar üzerinde gerçekleştirilen sosyal mühendislik saldırı senaryoları detaylı olarak aşağıda anlatılmaktadır. Test aşamasında amaç ortaya konan modelin kullanılabilirliğini ve başarısını test etmektir.

Ortaya konan model ilkeleri hem kamusal tarafta hem de kullanıcı tarafında başarıyla takip edildiğinde izleme sürecinde kullanıcıların doğru karar vererek hareket edeceği ve doğru sonuca ulaşacakları görülecektir.

Uygulama senaryosu-1

Kullanıcılara sunulan ilk eğitim videoları ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), Veri Güvenliği, E-Posta Güvenliği, USB Cihaz Güvenliği ve Sosyal Mühendislik Eğitimi şeklindedir. Bu eğitimler kullanıcılara e-posta adresleri üzerinden duyurulmuş ve en kısa sürede tamamlamaları istenmiştir. Çoğu kullanıcının beklenen sürede eğitim videolarını izledikleri ve istenen farkındalık seviyesine eriştikleri düşünülerek ilk sosyal mühendislik saldırı senaryosu eğitimleri takiben birkaç ay sonra uygulanmıştır. Uygulama senaryo-1, farklı yaş gruplarından ve çeşitli öğrenim durumlarına sahip kadın ve erkeklerden oluşan katılımcılar ile gerçekleştirilen bir ortalama saldırısıdır. Her kullanıcının isim ve soy ismine özel e-posta gönderilmiştir. E-postalar gerçek kullanıcıların yanı sıra birimlerin iş akışını sağlamak üzere oluşturulmuş e-posta adreslerine, görevlendirme ile başka kurumlara giden kullanıcılara ve dışardan erişim sağlama yetkisi olan destek personellerine de gönderilmiştir. E-postalar kullanıcılara “okundu” bilgisi vermek suretiyle iletilmiştir. Bu sayede maili okuyanların bilgisi de daha sağlıklı tutulmaya çalışılmıştır. E-posta içeriğinde personele iş yerinde kullanmak üzere USB Hard disk (Flash Bellek) dağıtılacağı bunun için bağlantı adresine giderek talepte bulunmaları gerektiği yazmaktadır. Kullanıcılara sunulan eğitim videolarının ilk aşamasında sıklıkla kaynağı belli olmayan kaynaklardan gelen e-postalara karşı dikkatli olmaları, kurum bilgisayarlarında güvenliğinden emin olmadıkları USB bellekleri kullanmamaları gerektiği bu yolla siber saldırıya uğrayabilecekleri vurgulanmıştır. Burada amaç kullanıcıların güvenilir olmayan bir kaynaktan gelen adres linkine tıklayarak istenen bilgileri girmesini ve böyle bir kaynaktan gelen USB belleği işyeri için temin edip kullanma durumlarını tespit etmektir. Sosyal mühendislik saldırı senaryosu-1 aşağıdadır;

Sayın \${isim} \${soy isim},

Kurumsal işlerde kullanılmak üzere, kurum personeline güvenli USB Hard disk (Flash Bellek) dağıtılacaktır. Bu çerçevede aşağıdaki sayfa üzerinden talepler alınarak, talepleri onaylanan personellere en kısa sürede dağıtımlar yapılacaktır. Taleplerinizi bu hafta içerisinde mesai bitimine kadar linkte bulunan sayfa üzerinden iletmeniz gerekmektedir.

E-posta kullanıcınız ve şifreniz ile sayfaya erişebilirsiniz.

Sayfaya erişmek için **TIKLAYINIZ**

İyi çalışmalar.

Yukarıdaki senaryo kullanıcılara bilgiislem@kamusal.com.tr adresi üzerinden gönderilmiş ve geri dönüşler gözlemlenmiştir. Kullanıcıların bağlantı adresine tıkladıklarında karşlarına çıkacak sayfa Şekil 4.5'tir.

Şekil 4.5. Uygulama senaryo-1 giriş ekranı

Şekil 4.5'te kullanıcıların, kullanıcı adı ve parolaları ile giriş yapacağı login sayfası gösterilmiştir. USB bellek dağıtımı üzerine gerçekleştirilen bu sosyal mühendislik saldırı senaryosu çerçevesinde kullanıcı linke tıkladığında sahte e-posta sayfası karşlarına çıkarılmış ve e-posta adresleri ve şifrelerini girmeleri istenmiştir. Şifrelerini girdiklerinde sistem şifrelerini giren personeli kaydetmiş fakat girilen şifreyi saklamamıştır. Şifre girildikten sonra kurumun gerçek e-posta sayfası girişi kullanıcının karşısına çıkarılmış ve şüphe duymaları beklenmiştir. Sistem üzerine kurulan sanal bir sunucuda bağlantıya giden

her kullanıcının bilgileri saldırı sürecinde kaydedilmiş ve tutulmuştur. Araştırma bulguları kısmında bu saldırı senaryosunun sonuçları detaylı olarak anlatılmaktadır.

Uygulama senaryosu-2

Kullanıcılara sunulan eğitim videolarının ikinci adımında Parola Güvenliği, Fiziksel Güvenlik, Çalışanlar İçin Güvenlik, Seyahat Güvenliği ve Kişisel Verilerin Korunması hakkında eğitimler verilmiştir.

Bu eğitim videoları da aynı şekilde e-posta adresleri üzerinden kullanıcılara duyurulmuş ve en kısa sürede tamamlamaları istenmiştir. Eğitimlerin izlenip önemli noktaların karşı tarafa aktarıldığı ve kullanıcıların bu konular hakkında da gerekli farkındalık seviyesine geldikleri düşünüldüğü zamanda ikinci sosyal mühendislik saldırı senaryosu uygulanmıştır. Bu uygulama ilk uygulamadan farklı olarak genele yönelik değil, ilk uygulamada sosyal mühendislik saldırı tuzağına düşen kullanıcıların bir kısmına uygulanmıştır. Bu kullanıcılara aynı zamanda tezde ortaya konan filtre model adımları ve adımların dayandığı ilkelerde aktarılmıştır. İkinci uygulamanın amacı, kullanıcılar üzerinde ilk kez denenilen bu filtre model ne kadar etkili olacak ve bir önceki saldırı senaryosuna kıyasla sosyal mühendislik saldırı tuzağına düşen kullanıcılarda azalma olacak mı? Tespit etmektir. Sosyal mühendislik saldırı senaryosu-2 aşağıdadır;

Sayın \${isim} \${soy isim},

Görev yapan personelin kullanımı için dizüstü bilgisayar temin edilmesi planlanmaktadır. Mevcutta dizüstü bilgisayar kullanımını ve ihtiyaç durumunu görebilmek adına aşağıdaki linkte yer alan formun herkes tarafından doldurulması gerekmektedir.

Dizüstü bilgisayarı bulunan ve/veya talebi olmayan personel “Donanım Talebi” kısmına HAYIR, talebi olanların ise EVET yazarak alttaki açıklama kısmına gereksinimlerini belirtmeleri gerekmektedir.

https://www.kamusal.com.tr/donanim_talebi.html

İyi çalışmalar.

Yukarıdaki senaryo belli sayıda kullanıcıya gönderilmiş ve geri dönüşler gözlemlenmiştir. Kullanıcıların bağlantı adresine tıkladıklarında karşlarına çıkacak sayfa Şekil 4.6'dır.

Şekil 4.6. Uygulama senaryo-2 giriş ekran

Dizüstü bilgisayar temini konulu gerçekleştirilen bu sosyal mühendislik saldırısında kullanıcılardan isim, soy isim, e-posta, talep isteği olup/olmadığı ve talep varsa bunun detay içeriği üzerine bilgi girişleri Şekil 4.6'da istenmiştir. Donanım talep formunu dolduran kullanıcılar maili gönder diyerek geri dönüş yapmıştır. Kullanıcıların geri dönüş yaptığı e-posta adresi iç tarafta verilerin tutulduğu bir sayfaya yönlendirilmektedir. Burada kullanıcıların işlem girişleri görülmekte ve sayısal değerlerle tutulmaktadır. Araştırma bulguları kısmında bu sayısal verilerden bahsedilmektedir.

Uygulama senaryosu-3

Kullanıcılara sunulan eğitim videolarının üçüncü ve son adımında Web Güvenliği, Yöneticiler için Güvenlik Eğitimi, Zararlı Yazılımlar Eğitimi, Sosyal Ağlar Güvenliği Eğitimi ve Mobil Güvenlik Eğitimi konuları yer almaktadır. Bu eğitim videoları da diğerleri gibi kullanıcılara e-posta adresleri üzerinden iletilerek takip etmeleri istenmiş ve en kısa sürede tamamlamaları beklenmiştir. Eğitimlerin kullanıcılar tarafından izlenip, sertifika sınavlarını başarı ile geçtikleri ve konular üzerinde gerekli farkındalık seviyesine geldikleri düşünüldükçe üçüncü sosyal mühendislik saldırı senaryosu uygulanmıştır. Modelin

kullanılabilirliği ve etkinliği üzerinde daha iyi yorum yapabilmek için bu uygulamaya ikinci uygulamada sosyal mühendislik saldırı tuzağına düşen kullanıcılar arasından bazı kişiler katılmıştır. Uygulama öncesinde ortaya konan model kullanıcılara adımları ve adımların dayandığı ilkeler doğrultusunda basit, net ve anlaşılabilir en pratik yollardan anlatılmıştır. Üçüncü uygulamanın amacı kullanıcılar üzerinde ikinci kez test edilecek olan filtre modelin ne kadar etkili olduğunu ve önceki saldırı senaryoları sonuçlarına kıyasla ne kadar başarı gösterdiğini tespit etmektir. Sosyal mühendislik saldırı senaryosu-3 aşağıdadır;

Sayın $\{isim\}$ $\{soy isim\}$,

Personel bilgisayarları ile ilgili yenileme çalışması düzenlenmektedir.

Donanım yetersizliği yaşayan personelin aşağıdaki dosya indirme adresinden başvuru formunu doldurarak tarafımıza iletmesi gerekmektedir.

Dosya indir

İyi çalışmalar.

Yukarıdaki senaryo belli sayıda kullanıcıya gönderilmiş ve dosya indir kısmında yer alan zararlı dosyayı bağlantıya tıklayarak indirip / indirmeme durumları gözlemlenmiştir.

Personel bilgisayarlarının yenilenmesi konulu gerçekleştirilen bu sosyal mühendislik saldırısında kullanıcılar “Dosya İndir” dedikten sonra ekte yer alan zararlı yazılım kullanıcının erişim sağladığı cihaza inmektedir. Bağlantıya tıklayan kullanıcılar Şekil 4.7’de yer alan uyarıyı almaktadır.



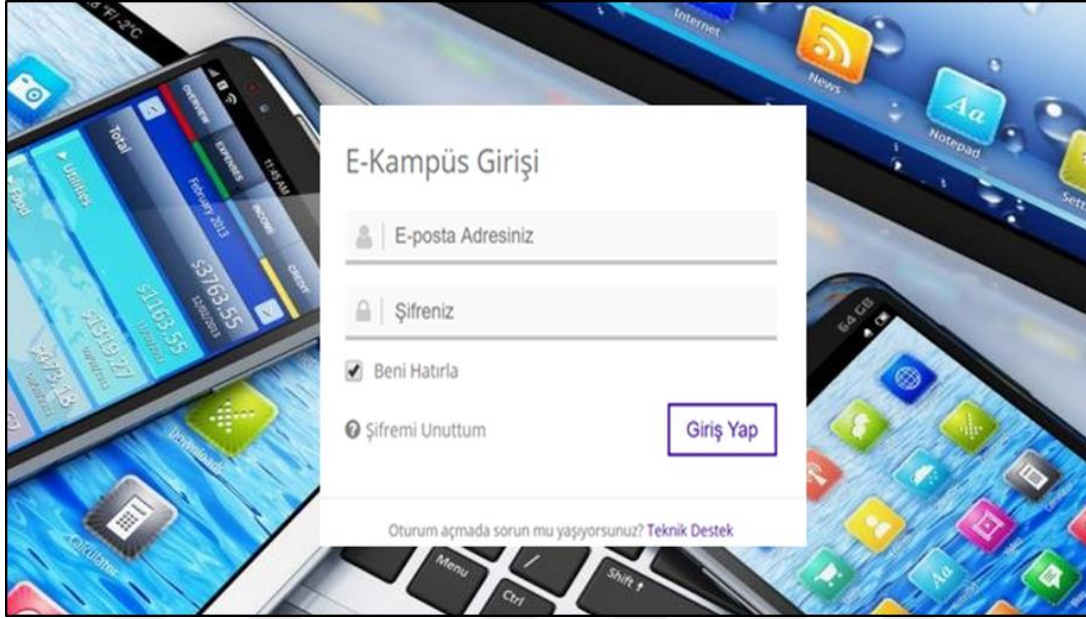
Şekil 4.7. Uygulama senaryo-3 uyarı ekranı

Şekil 4.7’de yer alan uyarı ekranı tüm girişlerde her defasında gelmekte ve gerçekte kullanıcıya hiçbir zaman e-posta da bahsedilen başvuru formu ekranı gelmemektedir. Kullanıcılar doğrudan kendi e-posta adresleri üzerinden dosya indir bağlantısına tıkladıkları için e-posta adresleri iç tarafta sanal bir sunucuya otomatik kaydedilmektedir. Son sosyal mühendislik saldırı senaryosu diğer senaryolar gibi kullanıcılardan veri girişi istememiş, doğrudan dosya içerisinde yer alan zararlı yazılım ile hedef sistemi ele geçirmeyi amaçlamıştır. Kullanıcıların verdiği tepki sonuçları araştırma bulguları kısmında detaylı olarak anlatılmaktadır.

4.3. Araştırmada Kullanılan Materyaller

Tezi yazarken en çok üzerinde durulan kavramlar şüphesiz siber güvenlik, sosyal mühendislik, sosyal mühendislik saldırıları, insan zafiyetleri ve farkındalık eğitimleri olmuştur. İnsan faktörünün eğitimle sosyal mühendislik saldırılarına karşı daha bilinçli olacağı ve farkındalık yaratılacağı düşünülmüş ve sıklıkla bunun vurgusu yapılmıştır. Kullanıcılara yönelik sosyal mühendislik senaryoları ile saldırıda bulunmadan önce hedefteki kurbanlara online (çevrimiçi) erişim sağlayacakları eğitim videoları sunulmuştur. Her bir sosyal mühendislik saldırısında farklı bir güvenlik elemanına yönelik senaryo hazırlandığı için eğitim videoları içeriği de ona göre çeşitlenmiştir. Eğitim birimi tarafından bilgi güvenliği üzerine çalışmalar yürüten özel bir işletmeye videolar hazırlanmıştır. Kullanıcılar internet tarayıcılarından “ .com “ uzantılı adrese giriş yapıp açılan giriş sayfasından kurumsal e-posta adreslerini ve parolalarını girdikleri takdirde sisteme giriş yapmışlardır. Sisteme giriş yaptıktan sonra kendilerine özel hazırlanmış e-eğitimleri izleyebilirler.

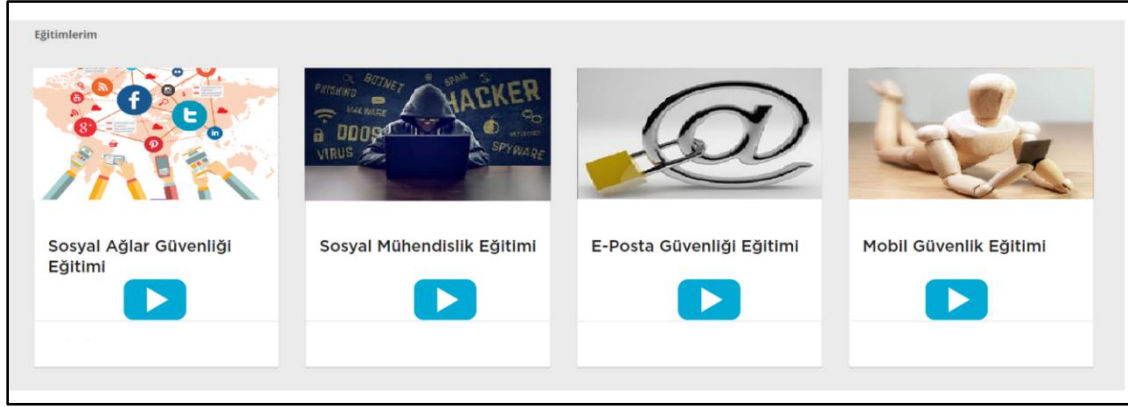
Şekil 4.8’de sisteme giriş ekranı belirtilmiştir.



Şekil 4.8. E-Kampus giriş ekranı

Eğitim videolarını izlemek isteyen kullanıcı Şekil 4.8’de görüldüğü üzere kurumsal e-posta adresi ve şifresi ile sisteme giriş yapabilmektedir.

Eğitimler online (çevrimiçi) ortamda 1 yıl sürecek şekilde kısım kısım kullanıcılara verilmiştir. Online eğitimler 7/24 erişime açıktır. Kullanıcılar diledikleri yerden bağlanabilir ve tekrar tekrar izleyebilir. Eğitim içerikleri son kullanıcının siber güvenlik konusunda bilmesi ve dikkat etmesi gereken konuları kapsamaktadır. ISO 27001 Bilgi Güvenliği, Fiziksel Güvenlik, Parola Güvenliği, Seyahat Güvenliği, Web Güvenliği, Çalışanlar İçin Güvenlik, Sosyal Ağlar Güvenliği, E-Posta Güvenliği, Mobil Güvenlik, USB Cihaz Güvenliği, Veri Güvenliği, Kişisel Verilerin Korunması, Sosyal Mühendislik ve Zararlı Yazılımlar Eğitimi kullanıcılara online (çevrimiçi) ortamda verilen eğitim başlıklarıdır. Bu sayede güvenlik elemanları üzerinde tek tek durulmuş, önemleri daha iyi vurgulanmış ve konular arasında bağlantılar daha sağlıklı kurulmuştur. Ayrıca kullanıcıların hangi konuda eksiklikleri olduğunu anlaması ve o konuya eğilerek eksikliklerini gidermesi içinde ayrı değerlendirilmeleri yararlarına olacaktır. Şekil 4.9 farklı kategorize edilmiş eğitim videoları sayfasına bir örnektir.



Şekil 4.9. Siber güvenlik eğitim videoları örnek sayfa

Siber güvenlik ile ilgili kavramlar ayrı eğitim videoları halinde Şekil 4.9’da görüldüğü gibi kullanıcılara sunulmuştur. Video içeriklerinde ilk adımda konu hakkında bilgi verilir, varsa alt başlıkları detaylandırılır ve önemli noktalar üzerinde durularak ön bilgi verilir. Şekil 4.10 eğitim videolarının içeriğine yönelik örnek bir görseldir.

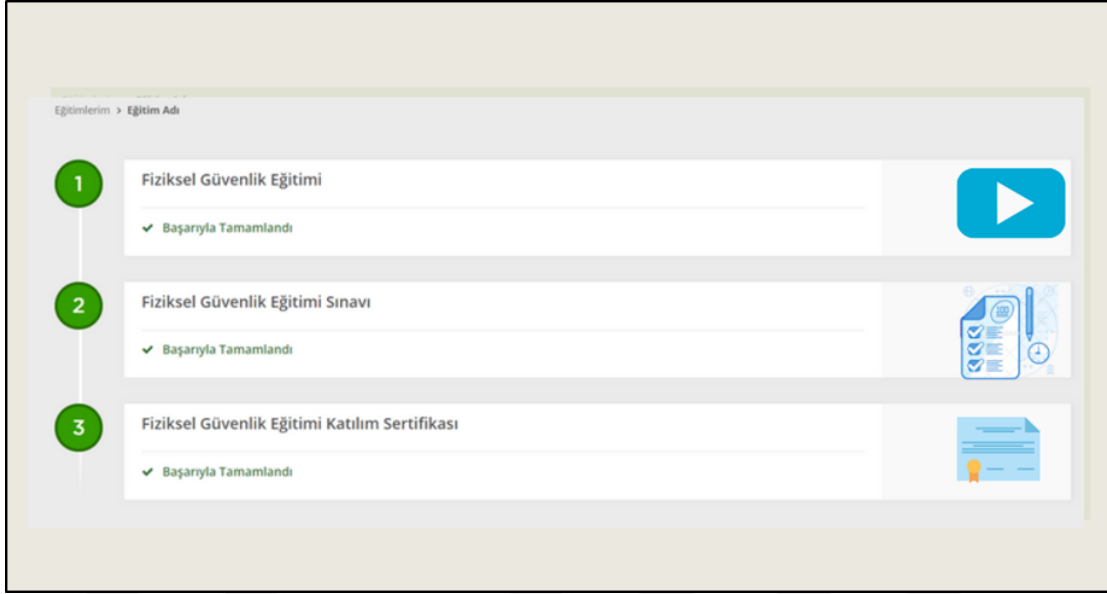


Şekil 4.10. Eğitim içeriği örnek sayfa

Şekil 4.10’da ifade edildiği gibi eğitim videosunun konusu kendi içerisinde birden fazla başlığa ayrılarak detaylıca kullanıcıya sunulmaktadır.

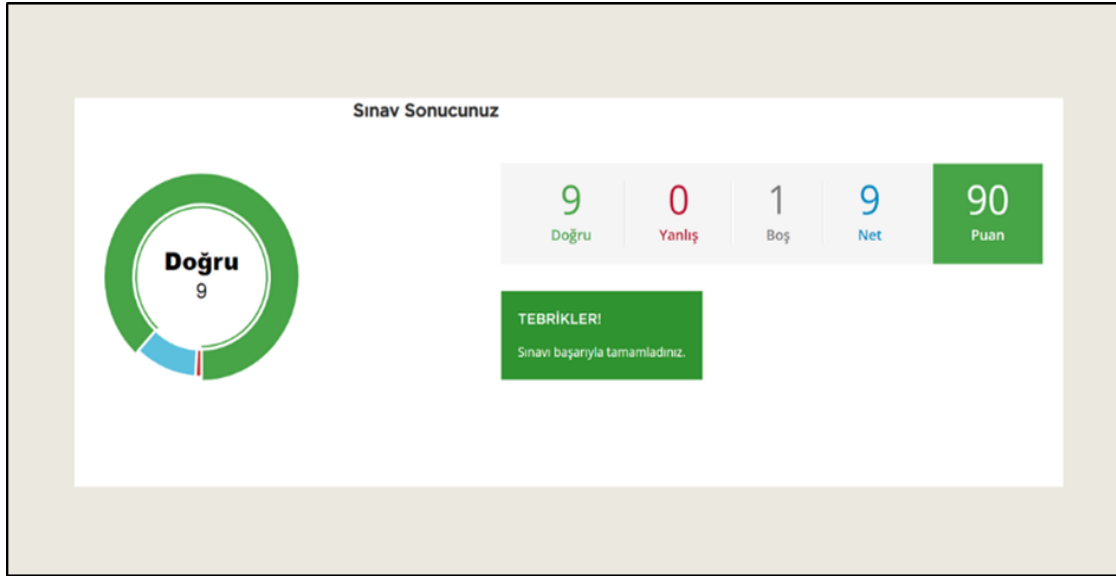
Her eğitim konu başlığı sonunda kullanıcılar sınava tabi tutulurlar, bu sınavlardan %60 oranında başarı gösterenler bir sonraki adıma geçmeye hak kazanabilir. Sınavda istenen başarıyı gösteremeyen kullanıcı isterse eğitime geri dönerek eksik kaldığı ya da yanlış yaptığı yerleri tekrar öğrenme imkânı bulur, isterse de tekrar sınava girer. Kullanıcılar istedikleri kadar aynı eğitim videosunu izleyebileceği gibi başarılı olana kadar da sınava girebilir. Eğitimin konusundan başarılı olan kullanıcı adına online ortamda sertifika düzenlenir. Belirli sayıda test ve sorudan oluşan sınavda başarılı olan kullanıcılar sertifika almaya hak kazanırlar. Kullanıcının eğitimden başarılı olması demek ayrıca o eğitim konusunu tam olarak anladığını ve istenen farkındalık seviyesine eriştiğini de ifade eder. Örneğin USB güvenliği hakkında eğitim videolarını eksiksiz izleyen, sonundaki sorulara %60 oranında başarılı cevap veren bir kullanıcının yanlış USB kullanımından kaynaklı zafiyet ortaya çıkarması beklenmemektedir. Diğer konu başlıkları içinde bu durum geçerlidir. Eğer kullanıcılar zafiyet göstermeye devam ediyorsa verilen farkındalık eğitimlerinin kullanıcılar için yetersiz olduğu kanaatine varılmaktadır.

Bahsedilen bütün kısımları sonuna kadar eksiksiz tamamlayan kullanıcı bahsi geçen güvenlik elemanı konusunda başarılı olarak değerlendirilir. Şekil 4.11 eğitim videolarının işleyiş adımlarına ve başarıyla tamamlanmış bir güvenlik eğitimine ait örnek görseldir.



Şekil 4.11. Eğitim adımları örnek sayfa

Kullanıcının öncelikle eğitim videolarını eksiksiz izlemiş bir sonraki adımda sınava girmiş ve geçmiş en son kısımda ise katılım sertifikasını almış olduğu Şekil 4.11’de görülmektedir. Örneğin sadece eğitimin bilgi veren kısmını izleyip online sertifika sınavına katılmayan ya da katılsa dahi başarılı olamayan kullanıcı o güvenlik elemanından başarılı olmuş sayılmaz. Bu kısım önem arz eder çünkü güvenlik elemanları üzerine hazırlanmış eğitim videoları sistemi yılsonunda erişime kapatılır. Kullanıcılara ve yöneticilerine güvenlik eğitimlerini tamamlayıp/tamamlamadıklarına yönelik bilgi maili gider. Herhangi bir olası siber güvenlik saldırısında ise zafiyet güvenlik eğitimlerini tamamlamayan kullanıcıdan kaynaklanıyorsa, o çalışanın kurum için zafiyet oluşturduğu ortaya çıkar. Şekil 4.12 eğitim sınavına giren kullanıcıya ait örnek bir sonuç ekranıdır.



Şekil 4.12. Eğitim sınav sonuç ekranı

Şekil 4.12 tüm adımları geçip sınavını başarı ile tamamlayan ve sertifika almaya hak kazanan başarılı bir kullanıcıya aittir.

Sosyal mühendislik saldırı senaryolarından ilki kullanıcıdan bilgi girişi isteyen ortalama saldırısıdır. Bu bağlamda ilk eğitim videoları hem bilgi güvenliğine yönelik kapsayıcı videolar hem de sosyal mühendislik saldırı senaryosuna uygun videolar olacaktır. ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), Veri Güvenliği, E-Posta Güvenliği, USB Cihaz Güvenliği Eğitimi ve Sosyal Mühendislik Eğitimi kullanıcılara ilk aşamada verilen eğitim videolarıdır. Bu eğitimler kullanıcılara e-posta üzerinden duyurularak en kısa sürede tamamlamaları istenir. Çoğu kullanıcının beklenen sürede eğitim videolarını izledikleri ve istenen farkındalık seviyesine eriştikleri düşünülerek ilk sosyal mühendislik saldırı senaryosu uygulanmıştır.

İkinci sosyal mühendislik saldırı senaryosu e-posta adresleri ve kullanıcı şifrelerini isteyen ortalama saldırısıdır. Bu bağlamda eğitim videoları farkındalık yaratmaya yönelik olacaktır. Ayrıca uygulama senaryo-1 de tespit edilen güvenlik zafiyetleri de bu aşamada dikkate alınmış eğitim videolarına bunlara yönelik konularda eklenmiştir. Kişisel Verilerin Korunması, Seyahat Güvenliği, Parola Güvenliği ve Çalışanlar İçin Güvenlik kullanıcılara ikinci aşamada verilen eğitimlerdir.

Üçüncü ve son sosyal mühendislik saldırı senaryosu öncesi kullanıcılara verilen online eğitim videoları Web Güvenliği, Yöneticiler için Güvenlik Eğitimi, Zararlı Yazılımlar Eğitimi, Sosyal Ağlar Güvenliği Eğitimi ve Mobil Güvenlik Eğitimi konuları yer almaktadır. Aynı zamanda ortaya konan model de saldırı öncesi kullanıcılara sunulmuştur.

Yapılacak olan son saldırı senaryosu da diğer iki uygulama gibi verilen eğitimlere paralel olarak gerçekleştirilmiştir. Üçüncü uygulama, zafiyet göstermeye devam eden kullanıcılara yönelik gerçekleştirilmiştir. Bu kullanıcıların bir diğer ortak yönü ise eğitim videolarının tamamına erişim sağladıktan sonra üçüncü uygulama ile test edilmişlerdir.

4.4. Uygulama Süreci

Eğitim videolarının tüm kullanıcılara iletilerek izlenmeleri için verilen süre 1 yıldır. 1 yıl içerisinde aşama aşama kullanıcılara e-posta adresleri üzerinden bilgilendirme yapılarak “.com” uzantılı sisteme eğitim videoları yüklenmiştir. Aynı şekilde 1 yıl boyunca online erişime de açık tutulmuştur. Sosyal mühendislik saldırı senaryoları da bu eğitimlere paralel olarak gerçekleştirilmiştir. İlk yapılan sosyal mühendislik saldırısı eğitim videolarının ilk konuları kullanıcılara iletdikten yaklaşık 3 ay sonra gerçekleştirilmiştir. Gönderilen USB Hard disk talep mailine geri dönüşlerin 1 hafta boyunca mesai bitimine kadar linkteki sayfaya iletilmesi istenmiştir. Bir hafta süren veri toplama işleminin ardından toplanan veriler bir sonraki iş günü değerlendirilmeye alınmıştır.

İkinci yapılan sosyal mühendislik saldırı senaryosu zaman olarak ilk sosyal mühendislik saldırı senaryosundan yaklaşık 4 ay sonra gerçekleştirilmiştir. Bu 4 aylık sürede yine kullanıcılara sıradaki eğitim videoları online olarak sunulmuştur. Gönderilen dizüstü bilgisayar temini konulu talep mailine geri dönüşler 3 gün ile sınırlandırılmıştır. 3 günün sonunda tutulan veriler bir sonraki iş günü değerlendirmeye alınmıştır.

Üçüncü sosyal mühendislik saldırı senaryosu da benzer şekilde ikinci uygulama yapıldıktan 3 ay sonra gerçekleşmiştir. Eğitim videoları bu sürede kullanıcılara eksiksiz olarak düzenli bir şekilde kurumsal e-posta adresleri ve şifreleriyle giriş yapacakları şekilde verilmiştir. Bu aşamada verilen eğitimler son olup, içerik olarak siber güvenlikle dikkat edilmesi gereken en önemli konular tek tek ele alınmıştır. Üçüncü uygulama da verilen eğitimlere bağlı kalınarak hazırlanmış ve farkındalık eğitimlerinin tamamını hedefteki kullanıcıların

tamamladığı düşünöldüğü zamanda yapılmıştır. Kullanıcılara hafta başında personel bilgisayarları ile ilgili yenileme çalışmasına düzenleneceğine dair e-posta atılmış ve 3 gün içerisinde e-postaya geri dönüş yapmaları istenmiştir. Üçüncü günün sonunda sistem erişime tamamen kapatılmış ve geri dönüşler bir sonraki gün değerlendirilmeye alınmıştır.





5. ARAŞTIRMA BULGULARI

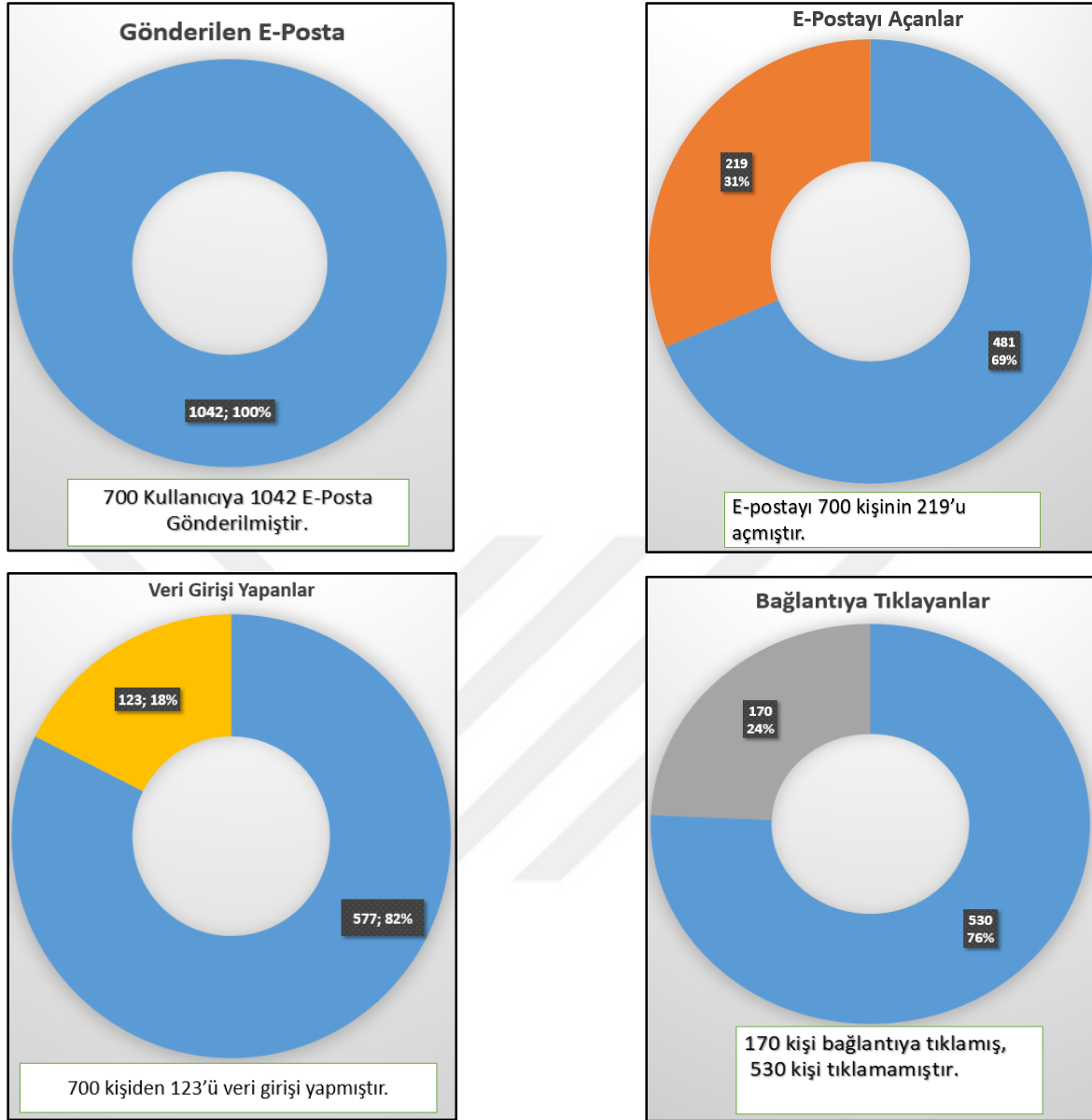
Tezde anlatılan modelin kullanılabilirliğini ve etkinliğini test etmek için birbirinden ayrı üç sosyal mühendislik saldırı senaryosu kamuda çalışan personel üzerinde gerçekleştirilmiştir. Elde edilen bulgular tek tek bu kısımda açıklanmaktadır.

5.1. Sosyal Mühendislik Uygulamaları Sonuçlarının İncelenmesi ve Analizi

Belirli aralık ve kriterlere göre gerçekleştirilen sosyal mühendislik saldırılarının sonuçları aşağıda ayrı ayrı incelenmiştir. Çıkarılan sonuçlar oluşturulacak modelin dayandığı ilkeleri desteklemesi, onları oluşturması ve dikkat edilmesi gereken noktaları daha somut ifade edebilmek için büyük önem taşımaktadır.

5.1.1. Uygulama senaryosu-1 sonuçlarının incelenmesi

Uygulama senaryosu-1, sosyal mühendislik saldırıları üzerine yapılan çalışmanın ilk uygulamasıdır. Bu çalışma e-posta yoluyla yapılan Sosyal Mühendislik testidir. Bu çerçevede eğitim videolarına paralel bir senaryo belirlenmiş ve başarıyla uygulanmıştır. Gönderilen e-postanın içeriği önceki kısımlarda anlatılmaktadır. Hedefimiz bu uygulamada zayıf halka olarak nitelendirilen insan faktörünün gerekli eğitimi aldıktan sonraki farkındalığını tespit etmektir. Sosyal mühendislik saldırı senaryosu sistemde aktif olan 1042 e-posta adresine %100 başarı oranı ile e-posta üzerinden gönderilmiştir. Bu 1042 değeri çalışanların yanı sıra birimlerin iş akışını sağlamak üzere birimlere özel oluşturulmuş e-posta adresleri, görevlendirme ile başka kurumlara giden kullanıcılar ve dışardan erişim sağlama yetkisi olan destek personellerini de içermektedir. 700 kamu çalışanından 219'u e-postayı açmıştır. Bu 219 kişi de oransal olarak %31 temsil etmektedir. E-postayı açan 219 kişiden 170'i linke tıklamış ve 123 kişinin şifresini sisteme girdiği gözlemlenmiştir. E-postayı açan, bağlantı adresine tıklayan %24'lük bir kesimken ve şifre bilgilerini şüphe duymadan karşı tarafla paylaşan %18'lik bir oranı temsil etmektedir. Şekil 5.1 bu değerlerin grafiksel gösterimidir.



Şekil 5.1. Uygulama senaryosu-1 sonuçları

Kullanıcıların taraflarına gönderilen saldırı senaryosuna karşı verdikleri tepki Şekil 5.1’de sayısal değerlerle ifade edilmiştir. Her grafiğin altında temsil ettiği değere ait açıklama yer almaktadır. Bu değerler diğer senaryoların sonuçları ile karşılaştırma yapabilmek açısından oldukça önemlidir. Değerlerin cinsiyet ve yaş gruplarına göre demografik değerlendirmeleri de aşağıda Çizelge 5.1. ve Çizelge 5.2’de sunulmuştur. Uygulama-1’in sonuçlarında erkeklerin kadınlardan sayıca daha fazla veri girişi yaptığı Çizelge 5.1’de ifade edilmiştir.

Çizelge 5.1. Uygulama senaryosu-1 sonuçlarının cinsiyete bağlı dağılımı

CİNSİYET	VERİ GİRİŞİ YAPAN KİŞİ SAYISI
KADIN	56
ERKEK	67

Uygulama senaryosu-1'in sonuçlarında 35 yaş üzeri kullanıcıların 25-35 yaş arası kullanıcılara göre daha fazla sosyal mühendislik tuzağına düştüğü Çizelge 5.2'de görülmektedir.

Çizelge 5.2. Uygulama senaryosu-1 sonuçlarının yaş gruplarına göre dağılımı

YAŞ GRUPLARI	VERİ GİRİŞİ YAPAN KİŞİ SAYISI
21-35 Yaş Arası	50
36 Yaş ve Üzeri	73

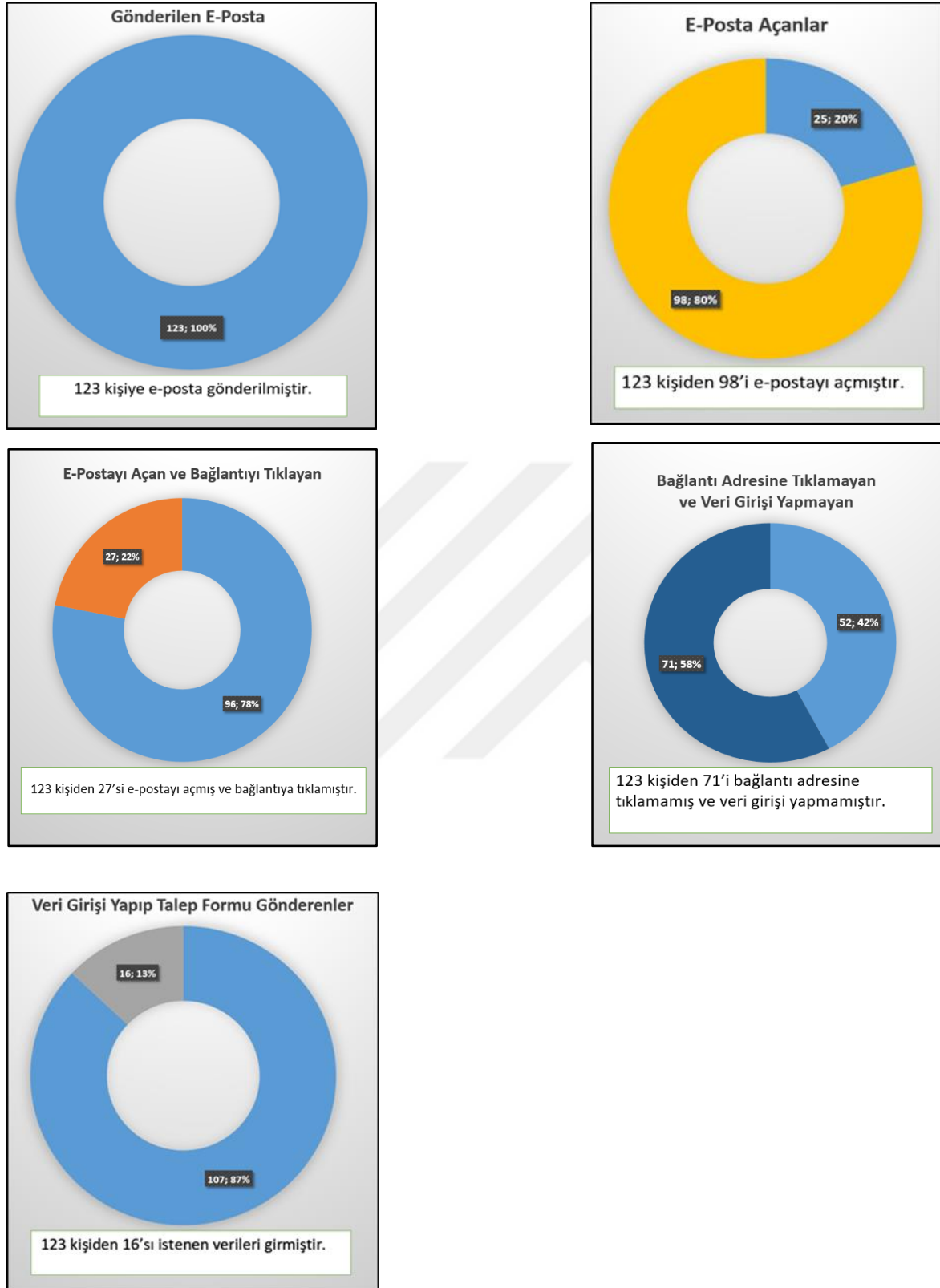
5.1.2. Uygulama senaryosu-2 sonuçlarının incelenmesi

Uygulama senaryosu-2, sosyal mühendislik saldırıları üzerine yapılan çalışmanın ikinci uygulamasıdır. Bu uygulama aslında modeli test edecek olan uygulamadır. Başarı ile gerçekleşen ikinci olumsuz saldırısının sonuçları, çalışmanın amacını büyük oranda sağlamaktadır. Eğitim videolarının ikinci aşamasında yine bazı temel güvenlik konuları ele alınmış ve kullanıcılar üzerinde bir farkındalık yaratılmaya çalışılmıştır. Sistemlerin en zayıf halkası insanın bilinçlenmesi ve gerekli hassasiyetleri iş hayatında göstermesi büyük önem taşımaktadır. Verilen eğitimlerle birlikte kullanıcılara tezde ortaya konan filtre model adımları ve adımlarının dayandığı ilkelerde verilmiştir. İkinci uygulamanın amacı daha önce de bahsedildiği üzere kullanıcılar üzerinde ilk kez denenilen bu filtre model ne kadar etkili olacak ve bir önceki saldırı senaryosuna kıyasla sosyal mühendislik saldırı tuzağına düşen kullanıcılarda ne kadar azalma olacağı durumunu tespit etmektir.

Sosyal mühendislik saldırı senaryosunun 2.'si farkındalık eğitimi almasına rağmen zafiyet gösteren 123 kişiye uygulanmıştır. Senaryo kullanıcılara %100 başarı oranı ile e-posta üzerinden gönderilmiştir. 25 kişi gelen maili hiçbir şekilde yanıtlamamıştır. Bu %20'lik bir orana tekabül etmektedir. Yani bu kesim iletilen e-postayı okumadan direkt silmiştir. Geri kalan 98 kişi gelen e-postayı açmış ve içeriğini okumuştur. Bu 98 kişiden 27'si e-postayı açmakla beraber bağlantı adresine de tıklamıştır. Bu kullanıcılar da %22'lik bir oranı temsil

etmektedir. E-postayı açan ve bağlantı adresine tıklayan 27 kullanıcıdan 16'sı ise istenen bilgileri girmiş ve karşı tarafa talep formunu mail olarak göndermiştir. E-postayı açmış, bağlantı adresine tıklamış ve istenen bilgileri girmiş bu 16 kişi ise %13'lük bir oranı oluşturmaktadır. E-postayı açıp okuyan fakat herhangi bir işlem yapmayan kişi sayısı ise 71'dir. Bağlantı adresine tıklamayan ve karşı tarafın istediği bilgileri girmeyen bu kişiler %58'lik oranı temsil etmektedir. Şekil 5.2 bu değerlerin grafiksel gösterimidir.





Şekil 5.2. Uygulama senaryosu-2 sonuçları

Kullanıcıların taraflarına gönderilen uygulama-2 saldırı senaryosuna karşı verdikleri tepki Şekil 5.2'de sayısal değerlerle ifade edilmiştir. Her grafiğin altında temsil ettiği değere ait

açıklama yer almaktadır. Bu değerler yapılan ilk uygulama ve yapılacak olan üçüncü uygulamanın sonuçları ile karşılaştırma yapabilmede kullanılacaktır. Değerlerin cinsiyet ve yaş gruplarına göre demografik değerlendirmeleri de aşağıda Çizelge 5.3. ve Çizelge 5.4'te sunulmuştur. Erkeklerin kadınlara göre sosyal mühendislik saldırısına sayıca daha çok düştüğü Çizelge 5.3'te görülmektedir.

Çizelge 5.3. Uygulama senaryosu-2 sonuçlarının cinsiyete bağlı dağılımı

CİNSİYET	VERİ GİRİŞİ YAPAN KİŞİ SAYISI
KADIN	5
ERKEK	11

Çizelge 5.4'te 25-35 yaş arası kullanıcıların 35 yaş üzeri kullanıcılara göre sosyal mühendislik saldırısına daha çok düştüğü görülmektedir.

Çizelge 5.4. Uygulama senaryosu-2 sonuçlarının yaşa göre dağılımı

YAŞ GRUPLARI	VERİ GİRİŞİ YAPAN KİŞİ SAYISI
21-35 Yaş Arası	9
36 Yaş ve Üzeri	7

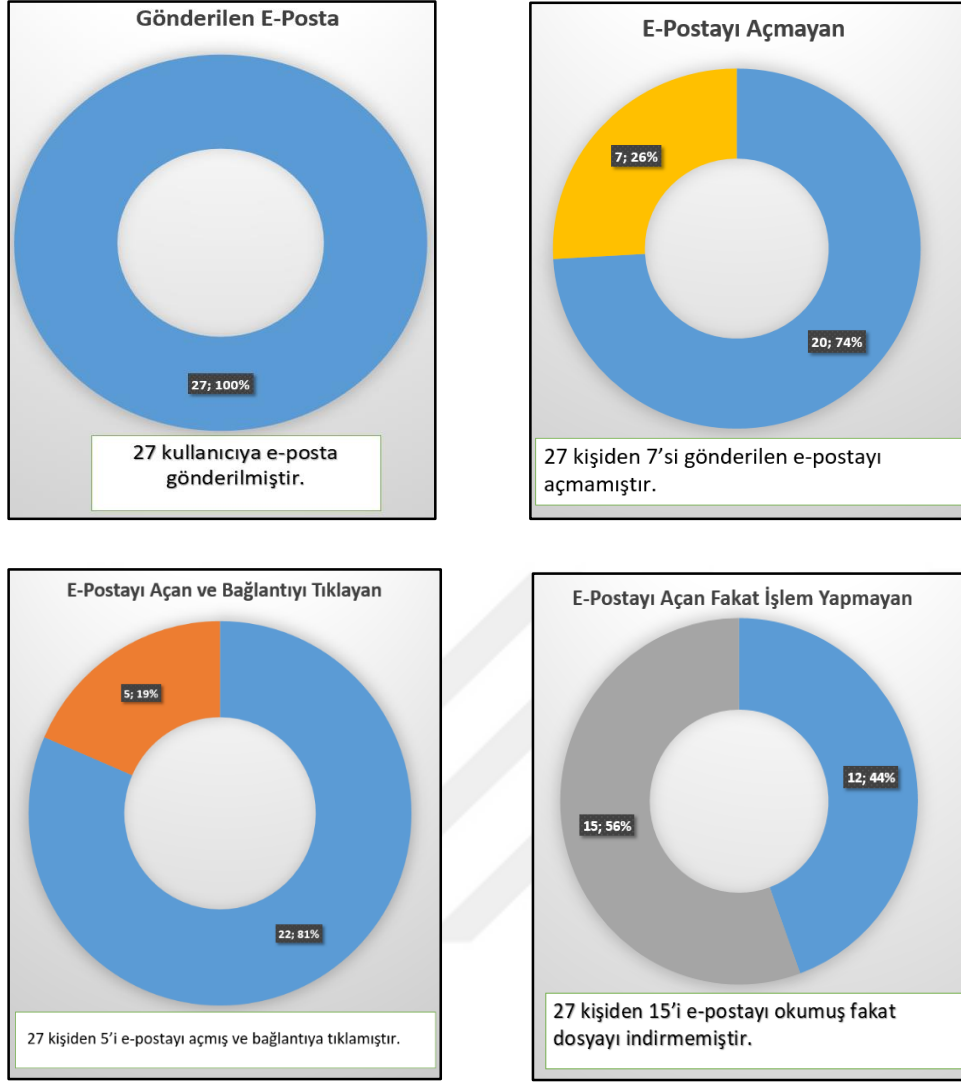
5.1.3. Uygulama senaryosu-3 sonuçlarının incelenmesi

Uygulama senaryosu-3, sosyal mühendislik saldırıları üzerine yapılan çalışmanın üçüncü ve son uygulamasıdır. Bu uygulama aynı zamanda modeli test edecek olan ikinci uygulamadır. Başarı ile gerçekleşen bu sosyal mühendislik saldırısının sonuçları tez çalışmasında ortaya konan modelin başarısını da görmeyi sağlayacaktır. Eğitim videolarının üçüncü aşamasında yine en kritik siber güvenlik konuları ele alınmış ve kullanıcılar üzerinde bir farkındalık yaratılmaya çalışılmıştır. Sistemlerin ve hassas verilerin güvenliği için zafiyet gösteren tek bir kullanıcının bile istenen farkındalık ve bilinç düzeyine erişmesi büyük önem taşımaktadır. Verilen farkındalık eğitimleri başından beri insan zafiyetini en aza indirmeye veya tamamen ortadan kaldırmaya yönelik olmuştur. Bu tezde tasarlanan modelde kullanıcılara aynı amaçla sunulmuş, modelin adımları ve adımlarının dayandığı ilkelerde eksiksiz verilmiştir. Eğitimlere ve modele paralel gerçekleştirilen son sosyal mühendislik saldırısı zafiyet göstermeye devam eden kullanıcılar üzerinde uygulanmıştır. Üçüncü uygulamanın amacı da ikinci uygulamada bahsedildiği gibi kullanıcılar üzerinde ikinci kez

test edilen filtre modelin ne kadar etkili olduğunu ve bir önceki saldırı senaryosuna kıyasla sosyal mühendislik saldırı tuzağına düşen kullanıcılarda azalma olup olmadığını tespit etmektedir.

İkinci uygulamada veri girişi yapıp talep formu gönderen, sosyal mühendislik saldırı tuzağına düşen 16 kişi olmuştur. Fakat sosyal mühendislik saldırı senaryosunun 3.'sü ikinci uygulamada e-postayı açan ve bağlantıya tıklayan 27 kişiye uygulanmıştır. Çünkü yapılacak olan saldırı, herhangi bir veri girişi istemeyen direkt bağlantı linkine tıklayarak zararlı yazılımın erişim sağlanan cihaza indirilmesine neden olan bir saldırdır. İkinci uygulamada veri girişi yapmasalar dahi onlara gönderilen bağlantı linkine güvenerek tıklamayı tercih eden bu kullanıcılarda zafiyet göstermeye devam etmektedir.

Üçüncü senaryo da kullanıcılara %100 başarı oranı ile e-posta üzerinden gönderilmiştir. 7 kişi gelen maili hiçbir şekilde yanıtlamamıştır. Bu %26'lık bir orana tekabül etmektedir. Yani bu kesim iletilen e-postayı okumadan direkt silmiştir. Geri kalan 20 kişi gelen e-postayı açmış ve içeriğini okumuştur. Bu 20 kişiden 5'i e-postayı açmakla beraber bağlantı adresine de tıklamıştır. E-postayı açan, bağlantı adresine tıklayan ve "Dosya İndir" kısmında yer alan zararlı yazılımı erişim sağladıkları cihazlarına indirmiş olan bu 5 kullanıcı %19'luk bir oranı oluşturmaktadır. E-postayı açıp okuyan fakat herhangi bir işlem yapmayan kişi sayısı ise 15'tür ve %56'lık dilimi oluşturmaktadırlar. Şekil 5.3 bu değerlerin grafiksel gösterimidir.



Şekil 5.3. Uygulama senaryosu-3 sonuçları

Kullanıcıların taraflarına gönderilen uygulama-3 saldırı senaryosuna karşı verdikleri tepki Şekil 5.3'te sayısal değerlerle ifade edilmiştir. Her grafiğin altında temsil ettiği değere ait açıklamalar yer almaktadır. Bu değerler yapılan ilk iki uygulama ile bu üçüncü uygulamanın sonuçlarının karşılaştırılmasının yapılabilmesinde kullanılacaktır. Değerlerin cinsiyet ve yaş gruplarına göre demografik değerlendirmeleri de aşağıda Çizelge 5.5. ve Çizelge 5.6'da verilmiştir. Erkeklerin kadınlara göre sosyal mühendislik saldırısına sayıca daha çok düştüğü Çizelge 5.5'te görülmektedir.

Çizelge 5.5. Uygulama senaryosu-3 sonuçlarının cinsiyete bağlı dağılımı

CİNSİYET	DOSYAYI İNDİREN KİŞİ SAYISI
KADIN	2
ERKEK	3

Çizelge 5.6'da 25-35 yaş arası kullanıcıların 35 yaş üzeri kullanıcılara göre sosyal mühendislik saldırısının son uygulamasında tuzağa daha az düştüğü görülmektedir.

Çizelge 5.6. Uygulama senaryosu-3 sonuçlarının yaşa göre dağılımı

YAŞ GRUPLARI	DOSYAYI İNDİREN KİŞİ SAYISI
21-35 Yaş Arası	1
36 Yaş ve Üzeri	4



6. SONUÇ, TARTIŞMA VE ÖNERİLER

Bu tez çalışmasında elimizde bulunan hassas verilerin güvenliği tehditleri mümkün olduğunca geniş kapsamlı ele alınmaya çalışılmış, güvenliğe karşı gerçekleştirilen siber tehditler ve güncel siber saldırı yöntemleri, nasıl gerçekleştirildikleri ve sonuçları üzerinde durulmuştur. Bunun yanı sıra, siber saldırıların önüne geçmede özellikle kamu kurumlarında sıklıkla tercih edilen bir uygulama olan farkındalık eğitimleri üzerinde durulmuştur. Eğitim faktörünün insan zafiyetinin önüne geçmede tek başına yeterli olamadığı, beraberinde destekleyici yapıların da kullanılması gerekliliği üzerinde durulmuş ve bundan hareketle de filtre model ortaya konmuştur. Amacımız insan faktörünün kişisel, kurumsal ve ulusal düzeyde siber güvenlik konusunda farkındalığını artırmak ve olası siber saldırı risklerini mümkün olan en aza indirmektir. Kurumlarda çalışanların yaklaşık %65'i siber güvenlik konusunda yeterli bilgiye ve farkındalık düzeyine sahip değildirler. Bu durum göz önüne alındığında kurumlarda siber güvenlik konusunda farkındalık çalışmalarının yapılması ve çalışanların siber riskler konusunda bilinç düzeylerinin artırılması gerekliliği ortaya çıkmaktadır [118].

Siber saldırılar için dinamik bir çözüm modeli konulu tezde de nitekim gelecekte yapılacak çalışmalarda sunucu tarafında alınan önlemlerden ziyade şimdiye kadar üzerinde fazla durulmamış kullanıcı tarafından hissedilen yedeklilik seviyesi ve hizmet sürekliliği kavramlarına yoğunlaşılabilirliğinden bahsetmektedir [119]. Bunun için en çok hata yapılan konular, dikkat edilmesi gereken noktalar, hem ülkemizde hem dünya genelinde siber zafiyete sebep olan etmenler ve doğrulukları çeşitli akademik çalışmalarda ve raporlarda kabul görmüş çözüm önerileri kurumsal ve kişisel bazda ayrı ayrı maddeler halinde ele alınmış ve yeni bir model destekleyici yapı olarak sunulmuştur. Sunulan modelin görselliği, tasarımı ve siber güvenlik konusunda dikkat edilmesi gereken noktaları akıcı, kolay ve anlaşılır maddeler halinde anlatması nedenleriyle başarılı sonuçlar vereceği düşünülmektedir. Sağiroğlu ve Vural yayınladıkları makalelerinde de kullanıcılara bilgi vermenin yanı sıra bilginin veriliş şeklinin de önemi üzerinde durmuştur. Kullanıcılara göre kurum güvenlik önlemleri olmaksızın bugüne kadar gayet iyi çalışmıştır ve hiçbir sorunla karşılaşmamıştır. Yeni güvenlik önlemleri kullanıcı tarafında hayatı zorlaştıran gereksiz değişiklikler olarak görülür. Bunun önüne geçebilmek için farkındalık eğitimleri güvenlikle

ilgili bilgi vermenin yanı sıra kullanıcının var olan yanlış alışkanlıklarından nasıl kurtarılacağı göz önüne alınarak hazırlanmalı, akıcı ve eğlenceli bir içerikle kullanıcılara sunulmalıdır [120].

Başka bir çalışmada da yine insan beyninin bilgiyi özümsemesi ve uygulaması noktasında bilgiyi olduğu gibi düz aktarmaktan ziyade kişide etki yaratacak, dikkat çekmesine yol açacak ve hafızasında görsel bir yapı oluşturacak aktarımların daha iyi sonuçlar vereceğinden bahsetmektedir. Social Engineering Awareness Program (SEAP) modeline göre insan beyninin bilgiyi daha efektif işlemesi için resim, şekil gibi etkin malzemelerle desteklenmesi gerekmektedir. Kullanılan görüntüler okuyucu üzerinde istenen etkiyi önemsemeleri gerektiğini düzeyde anlamalarına yardımcı olacaktır [121].

Siber güvenlikte sosyal mühendisliğe karşı bir model geliştirilerek test edilmesi konulu tez çalışmasında; öncelikle temel bilgiler verilmiş, literatür taranmış, model adımları tek tek anlatılmış ve son aşama olan test aşaması gerçekleştirilmiştir. Test aşaması birbirinden farklı üç sosyal mühendislik saldırı senaryosu ile gerçekleştirilmiş, bulgular tek tek açıklanmıştır. Tasarlanan modellerin kullanıcılar üzerinde ki etkinliğini tespit etme noktasında bu tarz testlerden yararlanılmaktadır. Yetenek olgunluk modeli sosyal mühendislik saldırılarının tehditlerini azaltmak ve sosyal mühendislik farkındalık eğitimlerinin teorik araştırmalarını onaylamanın yanı sıra bunları nicel analizlerle de değerlendirmeyi amaçlamıştır. Teorileri test, gözlem, ölçüm gibi araçlarla katılımcılar üzerinde deneyerek ve sonuçları öncesi/sonrası şeklinde ortaya koyarak sosyal mühendislik farkındalık programlarının etkinliğini değerlendirmektedir [122]. Bu üç saldırı senaryosunun sonuçları ortaya konan modelin varlığı ve ilerleyen dönemlerde gelişimi için önem arz etmektedir.

Sosyal mühendislik uygulamalarından ilkinden elde edilen bulgulara göre değerlendirmeler modelden önce ki farkındalık eğitimi almış olan genel kullanıcı davranışını temsil etmektedir.

Uygulama senaryo-1’de ilk aşamada gönderilen senaryoya cevapsız kalan 300 e-posta adresi vardır. Bunlar gelen e-postanın içeriğine bakılmaksızın silinmiş e-postalar olabilir. Ya da eğitim videolarını dikkatli bir şekilde izlemiş, sonundaki sorulara başarılı yanıtlar vermiş ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), Veri Güvenliği, E-Posta Güvenliği, USB Cihaz Güvenliği ve Sosyal Mühendislik Eğitimi konularına dair güvenlik bilincine ve

farkındalığına ulaşmış kişilerin e-postaları olabilirler. Bir diğer hususta iş akışları için oluşturulmuş, aktif olarak kullanılmayan e-posta adresleri olabilme durumlarıdır.

Böyle değerlendirildiğinde farklı yaş aralıklarında, farklı cinsiyetlerde, farklı birimlerde ve farklı görevlerde çalışan kullanıcıların %29'luk bir kesiminin sosyal mühendislik saldırılarına karşı bilinçli olduğu kanaatine varılabilir. Diğer taraftan bu kullanıcıların uygulama-1 senaryosu sonucunda taraflarına iletilen e-postayı bilinçsizce sildiği aslında bunun bir sosyal mühendislik saldırısı olduğunu fark etmemiş olmaları da ihtimaller arasındadır.

Bir diğer sayısal verimiz ise e-postayı açan, bağlantı adresine tıklayan ve şifre bilgilerini paylaşan 123 kişidir. Bunlar herhangi bir sosyal mühendislik saldırısında kurum için zafiyet oluşturabilecek, farkındalık eğitimlerinden istenen verimi sağlayamayan kişilerdir. Sayısal olarak 67 erkek, 56 kadın kullanıcı bu aşamada veri girişi yapan sayıdır. Değerler birbirine yakın olmakla beraber kadınların eğitim videolarını daha dikkatli dinlemiş ve olası sosyal mühendislik saldırılarına karşı daha tedbirli oldukları söylenebilir. Diğer taraftan 25- 35 yaş arasında 50 kişi, 35 yaş üzeri ise 73 kişi ilk uygulamada zafiyet göstermiştir. Belli bir yaş aralığında olan kişilerin sosyal mühendislik saldırılarına karşı daha bilinçli olduğu da buradan hareketle söylenebilir. İkinci uygulamaya katılacak kullanıcılar ilk uygulamada zafiyet gösteren 123 kişi üzerinde gerçekleştirilmiştir.

İkinci uygulamanın sonuçları ele alındığında verilen eğitimlerin yanında modelin kullanımı ile birlikte kullanıcılarda pozitif veya negatif yönde gelişme var mı burada ortaya çıkacaktır.

İlk aşamada gelen maili hiç okumadan direkt silen 25 kullanıcı için; onlara önerilen model ile birlikte eğitim videolarını dikkatli bir şekilde izlemiş, sonundaki sorulara başarılı yanıtlar vermiş olarak değerlendirilebilir. Bu kişiler ayrıca; Seyahat Güvenliği, Fiziksel Güvenlik, Parola Güvenliği, Çalışanlar İçin Güvenlik ve Kişisel Verilerin Korunması konularına dair güvenlik bilincine ve farkındalığına ulaşmış kişiler olarak da nitelendirilebilir. Böyle değerlendirildiğinde kullanıcıların %20'lik bir kesiminin sosyal mühendislik saldırılarına karşı hazırlıklı olduğu ve üzerinde çalışılan filtre modelin başarılı olduğu kanaatine varılabilir. Diğer taraftan, bu kullanıcıların taraflarına iletilen e-postayı bilinçsizce sildiği aslında bunun bir sosyal mühendislik saldırısı olduğunu fark etmemiş olmaları da ihtimaller arasındadır. Bir diğer sayısal verimiz ise e-postayı açan ve bağlantı adresine tıklayan 27

kişidir. Bu kişilerden 11'i adrese gitmesine rağmen talep formunu doldurmamıştır. Doldurmama sebepleri, bu olayın bir ortalama saldırısı olduğunu anlamaları veya onlara önerilen modelin maddelerini bu aşamada fark etmiş olabilme durumu olabileceği gibi dizüstü bilgisayar ihtiyaçları olmadığı için talebe cevap vermeye gerek duymamış da olabilirler. Eğer ilk sebepteki gibi bunun bir ortalama saldırısı olduğunu bağlantıya tıkladıktan sonra fark etmişlerse bu 11 kişi içinde verilen güvenlik eğitimlerinin ve anlatılan filtre modelin birlikte başarılı olduğu söylenebilir. İnsan zafiyetini aza indirmeyi hatta ortadan kaldırmayı hedefleyen, güvenlik eğitimlerini destekleyecek filtre modelin burada bilinç ve farkındalık yarattığı düşünülebilir.

En son sayısal verimiz ise e-postayı açmış, bağlantı adresine tıklamış ve istenen bilgileri girmiş 16 kişidir. Normal şartlarda ele alındığında fazla risk taşımayan bir değer olsa da belirli aralıklarla gerekli güvenlik eğitimlerini almaya devam eden ve üstüne farkındalıklarını artıracak görsel ve pratik maddelerden oluşan filtre model anlatılmış kullanıcılar için istenmeyen bir değerdir. Çünkü tüm personelin siber güvenlik, sosyal mühendislik saldırısı, veri güvenliği, sistem güvenliği, hassas verilerin korunması gibi konularda hâlihazırda bilinçli, farkında, dikkatli ve hazırda olması beklenmektedir. Unutulmamalıdır ki sadece bir kişi bile şirket, kurum ve kuruluşun hassas verilerinin ele geçirilmesine, istenmeyen durumların maddi/manevi yaşanmasına sebebiyet verebilir. Bu 16 kişinin 11'i erkek, 5'i ise kadındır. İlk uygulamada da kadınların sayıca daha az olduğu gözlemlenmişti ve ikinci uygulamada aradaki fark da yarıdan fazladır. Bundan hareketle kadınların aynı şekilde eğitim videolarını daha dikkatli takip ettiği ve sunulan modeli daha iyi özümseyerek olası bir sosyal mühendislik saldırısına karşı hazır oldukları söylenebilir. Sonuçlara yaş aralığı olarak bakıldığında ise 25-35 yaş arasında 9 kişinin, 35 yaş üzeri ise 7 kişinin zafiyet gösterdiği görülmektedir.

Üçüncü ve son uygulama ise ilk iki uygulamada da zafiyet gösteren kullanıcılar üzerinde gerçekleştirilmiştir. Bu saldırı öncesinde de kullanıcılara Web Güvenliği, Yöneticiler için Güvenlik Eğitimi, Zararlı Yazılımlar Eğitimi, Sosyal Ağlar Güvenliği Eğitimi ve Mobil Güvenlik Eğitimi konularında farkındalık eğitimleri ve ortaya konan filtre model verilmiştir.

İlk aşamada gelen maili hiç okumadan direkt silen 7 kullanıcı vardır. %26'lık bir oranı oluşturan bu kullanıcılar için; onlara önerilen model ile birlikte eğitim videolarını dikkatli bir şekilde izlemiş, sonundaki sorulara başarılı yanıtlar vermiş, önerilen modeli benimsemiş

denilebilir. Ayrıca Web Güvenliği, Yöneticiler için Güvenlik Eğitimi, Zararlı Yazılımlar Eğitimi, Sosyal Ağlar Güvenliği Eğitimi ve Mobil Güvenlik Eğitimi konularına dair güvenlik bilincine ve farkındalığına ulaşmış kişiler olarak da nitelendirilebilirler. Aynı zamanda bu kullanıcıların sosyal mühendislik saldırılarına karşı hazırlıklı olduğu ve üzerinde çalışılan filtre modelin de başarılı olduğu kanaatine varılabilir. Diğer taraftan bu kullanıcıların taraflarına iletilen e-postayı bilinçsizce sildiği aslında bunun bir sosyal mühendislik saldırısı olduğunu fark etmemiş olmaları veya kullanıcı izinde olduğu için iletilen e-postayı görmemişte olabileceği ihtimaller arasındadır. Bir diğer sayısal verimiz ise e-postayı açan ve içeriği okuyan 20 kişidir.

E-postayı açıp okuyan fakat herhangi bir işlem yapmayan kişi sayısı 15'tir ve %56'lık dilimi oluşturmaktadırlar. Bağlantıya tıklamama sebepleri, bu olayın bir ortalama saldırısı olduğunu anlamaları veya onlara önerilen modelin maddelerini bu aşamada fark etmiş olabilme durumu olabileceği gibi donanım yetersizliği yaşamadıkları için talebe cevap vermeye gerek duymamış olabilmeleri de olabilir. Eğer bunun bir ortalama saldırısı olduğunu e-postayı okuduktan sonra fark etmişler, bu 15 kişi içinde verilen güvenlik eğitimlerinin ve filtre modelin birlikte başarılı olduğunu söyleyebiliriz. Geri kalan 5 kişi ise bağlantıya giderek zararlı dosyayı indirmiştir. 5 kişi nicel olarak az bir değer olsa da yukarıda da bahsedildiği gibi tek bir kişinin dahi zafiyet göstermesi tüm sistemin saldırganlar tarafından ele geçirilmesine ve hassas verilerin zarar görmesine neden olabilmektedir. Uygulama-3 de zafiyet gösteren 5 kullanıcının 2'si kadın 3'ü ise erkektir. İlk iki uygulamada da kadınların zafiyet gösterme durumu erkeklere göre sayı olarak daha az olduğu tespit edilmiştir. Buda kadınların verilen farkındalık eğitimlerini ve modeli daha iyi takip ettiklerini ortaya koymaktadır. Yine bir diğer kıstas olan yaş durumunda ise 25-35 yaş arasında 1 kişinin, 35 yaş üzerinde ise 4 kişinin zafiyet gösterdiği görülmektedir. Belli yaş aralığında ki insanların teknolojiye eğilimleri farklı olduğu için teknik bir sıkıntı yaşamamak adına onlara sunulan bağlantıya gitme ihtimalleri yüksektir. Aksi takdirde daha fazla teknik sorunla karşılaşacaklarını düşünmektedirler.

İlk uygulamada 700 kişi de 123 kişi veri girişi yaparken oranı %18, ikinci uygulamada 123 kişi de 16 kişi veri girişi yaparak oranı %13, üçüncü uygulamada ise 27 kişi de 5 kişi veri girişi yaparak %18 oranına sahip olmuşlardır. Oranlara bakıldığında önce bir azalış sonrasında artış ile eski seviyesine gelen bir durum gözlenmiştir. Değerler birbirine yakın çıksa da gerek zaman gerekse imkân kısıtları daha fazla uygulama ile modelin test

edilmesine ve daha net bir çıkarımlar yapılmasına engel olmuştur. Şu aşamada modelin kullanılabilirliği için kesin bir değerlendirme yapmak zordur. Daha fazla uygulama ile elde edilen artış/azalış oranları ise istenen değerlendirmeyi yapacaktır. Burada bir diğer önemli hususta bu çalışmada yürütülen uygulamaların katılımcıları, zafiyet gösteren kullanıcılar ile sınırlandırılarak değil de ilk uygulamaya katılan 700 kişi ile sürekli yapılsaydı elde edilen veriler ve oranlar daha farklı değerlendirmeleri ve sonuçları beraberinde getirebilirdi. Sayısal olarak büyük farklar olmasa da ortaya çıkan azalış, modelin ilk kez kullanılması ve modelden sonra yapılan ilk iki sosyal mühendislik uygulamaları olması sebepleriyle büyük önem taşımaktadır. Filtre modelin kullanımı yaygınlaştıkça ve uygulama senaryoları çeşitlendikçe başarı oranının daha da artacağı değerlendirilmektedir. Uygulama senaryo-2 ve uygulama senaryo-3'ün tuzağa düşen personellere uygulanan sosyal mühendislik çalışmaları olmasının temel amacı da buradan çıkmaktadır. Düzenli aralıklarla devam eden eğitimlere ek pratik, öğrenmesi ve kavranması basit, kısa bilgiler içeren bir model sunulmasına rağmen aynı kullanıcılar zafiyet göstermeye devam ediyorsa genele yapılan bir sosyal mühendislik saldırısında sonuç ne olur? Kullanıcılar meydana gelebilecek bir saldırıya ne kadar hazır? Bir sonraki adımımız ne olmalıdır? Bütün personeli sosyal mühendislik saldırılarına karşı nasıl eğitebiliriz? Ortaya koyduğumuz filtre modelin eksikleri neler? Hangi eklemeler ile modeli daha kullanışlı hale getirebiliriz? Aynı kullanıcıların zafiyet göstermeye devam etme sebebi nedir? Bunlar ilerleyen çalışmalarda cevaplanması gereken sorulardır.

Yapılan uygulama senaryolarının sonuçları genel olarak değerlendirildiğinde ise kurumsal yönetimlerin siber saldırılara karşı etkin reaksiyon göstermede gerekli hazırlıklarını tam olarak sağlayamadıkları bununda çalışanların güvenliğini ilk etapta tehlikeye attığı söylenebilir. Bu süreçte hem uygulamalar boyunca hem de normal iş akışı boyunca gözlemlenen kamu kurumlarının, siber saldırıları teknolojik bir sorun olarak görmeye devam ettiği ve bu yollarla engel olmaya çalıştıkları tespit edilmiştir. Nitekim model ortaya konarken kurumsal bazda yapılması gereken 60 farklı maddenin çoğu uygulamaların gerçekleştiği ortamlarda da henüz tam olarak sağlanabilmiş değildir. Filtre modelin ilk adımı olan kurumsal bazda alınacak önlemler kısmı tam olarak kurumların bünyesine uygulandığında daha etkin sonuçlar alınacağı söylenebilir. Güvenlik testleri farklı yöntemlerle daha sık yapıldığında gözden kaçan ya da daha önce önemsenmeyen noktalar bu sayede fark edilip kurumlarda işleme alınacaktır. Ülkemizde sızma testi olarak adlandırılan güvenlik testlerinin henüz istenen ölçüde yaygınlaşmadığı ve kurumlar

tarafından siber güvenlik ve kurumsal bilgi güvenliğinin sağlanması noktasında önemli bir bileşen olduğunun bilinmediği tespit edilmiştir. Bu durum güvenlik testlerinin kurumlara olumlu geri dönüşler yapacağını, sağlayacağı farkındalığın ve güvenlik seviyesinin artırılmasına katkısının ülkemiz geneli kurumlar tarafından pek bilinmediğinin ve yeterince önem verilmediğinin göstergesidir [82]. Model adımlarının eksiksiz izlenmesi bu bağlamda değer kazanmaktadır. Öncelikle kurumlar kendi sorumluluklarını eksiksiz yapıp sonrasında kullanıcı tarafından hassasiyet beklemelidirler.

Çalışmaya kaynaklık eden bir diğer husus insan faktörüdür. İnsan faktörünün siber güvenlikte ki rolü tam olarak benimsenmediği gibi kurumun bütün çalışanlarının bu sürecin bir parçası olduğu ve ayırım gözetmeksizin her çalışanın sürece dâhil edilmesi gerektiği fikrinin yerleştirilmesi gerekmektedir. Periyodik olarak düzenlenen ve takibi yapılan eğitimler olsa da kullanıcıların bu eğitimlere ne kadar dikkat ve özveri ile devam ettiği daha fazla önem arz etmektedir. Modelin ikinci aşaması olan kullanıcı tarafında dikkate alınması gereken 60 farklı madde sunulmasına rağmen bu maddelerin çoğunun da kullanıcılar tarafından sağlanmadığı uygulamalar süresince gözlemlenmiştir. İnsan faktörünün bilinçlendirme ve farkındalık düzeylerini artırma eğitimleri siber güvenlikle mücadele de kurumların ellerindeki en büyük koz gibi gözüксе de kullanıcıların verilen eğitimleri özümsemesi ve hem iş hem özel yaşantılarında uygulayabiliyor hale getirmeleri daha önemlidir. Çalışmanın amaç kısmında da eğitimlerin tek başına yeterli olmadığı vurgulanmış bu çalışma kapsamında yapılan uygulama senaryoları ile de bu durum desteklenmiştir. Eğitimlerin sonunda kullanıcılara verilen sertifikalara ek, sürekliliği ve uygulanabilirliği artıracak teşvik amaçlı çeşitli ödüller verilebilir.

Kurumsal ve kişisel düzeyde siber güvenlik bilincinin, eğitimin ve sunulan hizmetlerin toplumumuza tam olarak yerleşmediği dikkate alındığında bu çalışmada sunulan hususlara ve yapılan önerilere dikkat edilmesi halinde daha iyi geri dönüşler alınacağı düşünülmektedir.

Karşılaşılan güçlükler

- Kurumsal ve kullanıcı tarafında modelin dayandığı ilkeler belirlenirken veri bulmada ve bulunan verilerin derlenmesinde eksikliklerin olması,

- Büyük ve küçük ölçekli siber güvenlik firmalarının öne sürdüğü çözüm önerilerinin tamamını paylaşmaması ve paylaştıkları önerilerinde doğruluğunu tam olarak sağlayamamaları,
- Farkındalık modeli tasarlanırken bu konu ile ilgili akademik anlamda çalışmaların yetersizliği ve özellikle Türkçe çalışmaların az sayıda olması,
- Modeli test etmek için sosyal mühendislik alanında yeterince uygulama yapmaya imkân olmaması şeklinde sıralanabilirler.

Gelecek çalışmalara öneriler

Gelecek çalışmalara önerilerde bulunulacak olunursa; elbette bu çalışmada karşılaşılan güçlüklerin giderilmesi için pek çok yeni fikir ortaya çıkabilir. Değişen ve gelişen teknolojiye her zaman cevap verebilecek şekilde yeni modellerin oluşturulması, her yeniliğin de bu modellere kolay entegre olabiliyor şekilde takip edilmesinin dinamik ve sistemli bir siber güvenlik bilinci yaratacağı değerlendirilmektedir. Burada bir diğer önemli hususta yeni modellerin daha fazla kişi ve daha fazla uygulama senaryosu ile test ediliyor olmasının sonuç odaklı ilerlemede her zaman daha verimli olacağıdır. Yapılan her yeni çalışma eksiklerin ortaya çıkmasına büyük katkı sağlayacaktır.

Bu çalışmada uygulamalar zafiyet gösteren kullanıcılara yönelik gerçekleştirilirken ilerleyen çalışmalarda başlangıçta kaç kişi varsa her uygulamanın da aynı kişilere uygulanarak gerçekleştirilmesinin daha farklı değerlendirmelere ve sonuçlara imkân sağlayacağı düşünülmektedir.

Bu tez çalışmasında bilgisayar kullanım becerilerine göre kişiler düşük, orta ve yüksek şeklinde kategorize edilerek sosyal mühendislik uygulamalarına tabi tutulmamıştır. Buda sonuçların ayrı ayrı değil de genel bir değerlendirmeye aktarılmasını sağlamıştır. Konu ile alakalı çalışma yapacak kişilerin bu hususlara dikkat ederek kişileri bilgisayar kullanım becerilerine göre kategorize ederek çalışmalarını gerçekleştirmeleri daha yararlı olacaktır.

Önerilebilecek bir diğer çalışmada siber güvenlikte cinsiyet ve yaş faktörünün etkisi üzerinde durmak olacaktır. Çünkü yukarıda uygulanan saldırı senaryolarının sonuçlarına bakıldığında sayıca kadınların daha az tuzığa düştüğü görülmektedir. Fakat yaş aralığı konusunda net bir çıkarım yapılamamıştır. İlk uygulamada 25-35 yaş aralığı daha iyi sonuç

verirken ikinci uygulamada 35 yař zerinin sonucu ve nc uygulamada da yine 25-35 yař aralıėının sonucu daha iyi olmuřtur. Bu demografik durumların doėruluėu ve sebepleri zerine de alıřma yapılması, insan faktrn sadece bilgisayar bilimi aısından deėil; aynı zamanda sosyolojik, psikolojik ve hukuki aıdan da siber gvenlik srecine dhil etmek literatre farklı bir bakıř aısı katacaktır.





KAYNAKLAR

1. Soydan, F. (2020). Siber Güvenlik. *Target Dergisi*, 5(5), 38.
2. İnternet: Çalışanlarınızın siber güvenliğe önem vermelerini sağlayacak ipuçları. *H4CKTIMES*. URL: <https://h4cktimes.com/nasil-yapilir/calisanlarinizin-siber-guvenlige-onem-vermelerini-saglayacak-ipuclari.html>, Son Erişim Tarihi: 04.08.2020.
3. İnternet: Siber Saldırıların Yeni Kıskaçı. *DÜNYA*. URL: <https://www.dunya.com/tekno-trend/siber-saldirilarin-yeni-kiskaci-sosyal-muhendislik-haberi-377630>, Son Erişim Tarihi: 04.08.2020.
4. İnternet: The Human Factor in Data Protection. (2012). *Ponemon Institute*. URL: https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf&date=2020-08-27, Son Erişim Tarihi: 27.08. 2020.
5. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. (20 Haziran 2013). *Resmi Gazete*, Ankara.
6. İnternet: 2016-2019 Ulusal Siber Güvenlik Stratejisi. (2016). *T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı*, URL: <http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf&date=2020-11-20>, Son Erişim Tarihi: 20.11.2020.
7. Öğün, M. N., & Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri*, 9(18), 145-181.
8. İnternet: Altundal, Ö. F. (2014). *Siber Güvenlik Raporu 2014*. URL: <http://www.siberguvenlik.org.tr/2015/01/2014-Siber-Guvenlik-RaporuYayinlandi.html>, Son Erişim Tarihi: 01.09.2020.
9. İnternet: Global Report. *CRUNCHBASE*. URL: <https://news.crunchbase.com/news/q4-2017-global-report-vc-sets-annual-records-back-strong-late-stage-results/>, Son Erişim Tarihi:29.11.2020.
10. İnternet: Dünyada ve Türkiye’de Siber Güvenlik Gerçekleri-1: İstatistikler, Analizler, Öngörüler. *CUBE INCUBATION*. URL: <https://www.cubeincubation.com/blog/dunyada-ve-turkiyede-siber-guvenlik-gercekleri-1-istatistikler-analizler-ongoruler>, Son Erişim Tarihi:29.11.2020.
11. İnternet: Bilgi ve İletişim Teknolojileri Sektörü 2018 Pazar Verileri. (2019). *TÜBİSAD*. URL: <http://www.tubisad.org.tr/tr/images/pdf/tubisad290419.pdf&date=2020-11-29>, Son Erişim Tarihi:29.11.2020.
12. TÜBİTAK Bilgem. (2013). *Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri*. Ankara: Siber Güvenlik Enstitüsü.
13. Hasanefendioğlu, B. (2018). *101 Soruda Siber Güvenlik Riski Yönetim ve Kontrol Çerçevesi*. Türkiye: Google Books. 103-105.

14. İnternet: Bıçakçı, S., Ergun, D. ve Çelikpala, M. (2015). Türkiye’de Siber Güvenlik, URL: https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf&date=2020-11-25, Son Erişim Tarihi: 25.11.2020.
15. Ünver, M. (2016). *Türkiye’de Siber Güvenlik*. Ankara: Bilgi Güvenliği Derneği.
16. Alkan, M. (2012, Mayıs). *Siber Güvenlik ve Siber Savaşlar*. Ankara: Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu.
17. İnternet: Goodrich, M. ve Tamassio, R. (2010). Introduction to computer security. Addison-Wesley. Host Exploit (2020). *World hosts report*. URL: <http://hostexploit.com/?p=whr-201403>, Son Erişim Tarihi: 11.03.2020.
18. Singh, A., Vaish, A., and Keserwani P. K. (2014). *Information Security: Components and Techniques*. Allahabad, India: Indian Institute of Information Department Technology.
19. İnternet: Internal audit summary report. (2016). *City of Vancouver*. URL: <http://vancouver.ca/files/cov/internal-audit-cyber-security.pdf&date=2020-03-14>, Son Erişim Tarihi: 14.03.2020.
20. İnternet: NIST. General Information. URL: <https://www.nist.gov/>, Son Erişim Tarihi: 23.04.2020.
21. İnternet: Cybersecurity. GARTNER. URL: <https://www.gartner.com/en/informationtechnology/glossary/cybersecurity>, Son Erişim Tarihi: 23.04.2020.
22. Cavelt, M. D. (2008). *Cyber-Security and Threat Politics: US Efforts To Ensure The Information Age*, New York: Routledge.
23. İnternet: T.C. Başbakanlık AFAD. (2014). *2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi*. URL: <https://www.afad.gov.tr/Dokuman/TR/123-20141010111330-kritikaltyapi%20-son.pdf&date=2020-11-20>, Son Erişim Tarihi: 20.11.2020.
24. Pingree, L., MacDonald, N., and Firstbrook, P. (2015). *Best Practices for Mitigating Advanced Persistent Threats*. Gartner.
25. İnternet: Güvenliği Artırmak için Tehdit İstihbaratı ve Zafiyet Yönetiminin Birleşimi. BGA Bilgi Güvenliği. URL: <https://www.slideshare.net/bgasecurity/gvenlii-artırmak-iin-tehdit-stihbarat-ve-zafiyet-ynetiminin-birleimi>, Son Erişim Tarihi: 23.11.2020.
26. Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A., and Sadhukhan S. K. (2013). Cyber-risk decision models: to insure IT or not? *Decision Support Systems*, 56, 11-26.
27. İnternet: Sızma Testi Hizmeti Veren Personel ve Firmalar İçin Yetkilendirme Programı .(2015). TSE. URL: <https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2224/07102015112307-3.pdf&date=2020-11-25>, Son Erişim Tarihi: 25.11.2020.

28. İnternet: UPGUARD. URL: <https://www.upguard.com/blog/vulnerability>, Son Erişim Tarihi:24.04.2020.
29. Frei, S. (2009). *Security Econometrics, The Dynamics (In)security*, Doctoral Thesis, Zurich University ETH Zurich, Zurich.
30. İnternet: Top Computer Security Vulnerabilities. *SOLARWINDS*. URL: <https://www.solarwindmsp.com/content/computer-security-vulnerabilities>, Son Erişim Tarihi: 24.11.2020.
31. İnternet: Vulnerabilities. *NIST NVD*. URL: <https://nvd.nist.gov/vuln/categories>, Son Erişim Tarihi: 24.11.2020.
32. İnternet: Öztürk, A. (2013). ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Farkındalık Eğitimi. URL: http://www.tekirdag.bel.tr/content/WebSource/file/dokuman/1464098219_bilgi-guvenligi-yonetim-sistemi_sunumu.pdf&date=2020-11-25, Son Erişim Tarihi: 25.11.2020.
33. İnternet: Bilişim Sistemleri Denetim Rehberi. (2013). *SAYIŞTAY*. URL: https://www.sayistay.gov.tr/tr/Upload/95906369/files/mevzuat/Rehberler/Bilisim_sistemleri_denetim_rehberi.pdf&date=2020-11-25, Son Erişim Tarihi: 25.11.2020.
34. İnternet: What is a Zero-Day Vulnerability? (2020). *Symantec*. URL: <http://www.pctools.com/security-news/zero-day-vulnerability/>, Son Erişim Tarihi:11.03.2020.
35. Öğün, M. N., ve Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi*, 9(18), 145-181.
36. Benzer, R. (2014). Siber Suçlar ve Teorik Yaklaşımlar. H. Çakır, M.S. Kılıç (Editörler). *Güncel Tehdit: Siber Suçlar içinde* (Birinci Baskı). Ankara: Seçkin Yayıncılık, 21-41.
37. İnternet: The Risk of An Uncertain Security Strategy. *SECURITYWIZE*. URL: <http://securitywize.com/the-risk-of-an-uncertain-security-strategy/1430>, Son Erişim Tarihi: 23.03.2020.
38. İnternet: Stuxnet Virüsü İran'a Nasıl Etki Etti? *TUIC AKADEMİ*. URL: <http://www.tuicakademi.org/stuxnet-virusu-iran-a-nasil-etki-etti/>, Son Erişim Tarihi: 10.11.2020.
39. Wilson, C. (2008). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. *CRS Report for Congress*.
40. Manikanta, Y. V. N., and Sardana, A. (2012). Protecting web applications from SQL injection attacks by using framework and database firewall. *In Proceedings of the International Conference on Advances in Computing, Communications and Informatics* (609-613). New York: Association for Computing Machinery.
41. H. J., Richard Lin, C. H., Lin, Y. C., and Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16-24.

42. İnternet: OWASP. URL: <https://owasp.org/www-project-top-ten/>, Son Erişim Tarihi: 28.03.2020.
43. Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma Testleri*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
44. Sağıroğlu, Ş., Erol, S. E., ve Ceyhan, E. B. (2015). *Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme*. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara.
45. Gündüz, M. Z., ve Daş, R. (2016). Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri. ISCTURKEY 2016 - 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTÜ, 9(1), 11-18.
46. İnternet: 2019 Year End Report Data Breach Quick View. (2019). *Risk Based Security*. URL: <https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf&date=2020-03-22>, Son Erişim Tarihi: 22.03.2020.
47. İnternet: Bilgi Güvende. URL: <https://bilgiguvende.com/2019-siber-saldirilar/>, Son Erişim Tarihi: 22.03.2020.
48. İnternet: VXCHNGE. URL: <https://www.vxchnge.com/blog/biggest-cyberattacks-2019>, Son Erişim Tarihi: 22.03.2020.
49. İnternet: ZDNET. URL: <https://www.zdnet.com/article/these-are-the-worst-hacks-cyberattacks-and%20data-breaches-of-2019/>, Son Erişim Tarihi: 22.03.2020.
50. İnternet: 2020 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. *PURPLESEC*. URL: <https://purplesec.us/resources/cyber-security-statistics/>, Son Erişim Tarihi: 23.03.2020.
51. Uma, M., and Padmavathi, G. (2013). A Survey on Various Cyber Attacks and Their Classification, *International Journal of Network Security*, 15(5), 390-396.
52. Seth, K. (2008). *Cyber crimes and legal enforcement in India*, National Conference of CIRC On Corporate laws-Ghaziabad.
53. Gedik, D. (2018). *Siber Güvenlik ve Terörizmin Evrilişi: Türkiye Üzerine Etkileri*, Yüksek Lisans Tezi, Düzce Üniversitesi Sosyal Bilimler Enstitüsü, Düzce.
54. İnternet: Siber zorbalık nedir, siber zorbalıkla mücadele için hangi önlemler alınabilir? *BBC NEWS*. URL: <https://www.bbc.com/turkce/haberler-turkiye-51614553>, Son Erişim Tarihi: 22.11.2020.
55. Mitnick, K. D. and Simon, W. L. (2006). *Aldatma Sanatı*. (Çev. Nejat Eralp Tezcan). Ankara: ODTÜ Yayıncılık, 303.
56. Hermansson, M. and Ravne, R. (2005). *Fighting Social Engineering*, University of Stockholm / Royal Institute of Technology.
57. İnternet: SECURITY. URL: www.social-engineer.org, Son Erişim Tarihi: 02.04.2020.

58. İnternet: SECURITY.URL: <https://www.social-engineer.org/framework/attack-vectors/attack-cycle/>, Son Erişim Tarihi: 02.04.2020.
59. Mouton, F., Malan, M. M., Leenen, L. and Venter, H. (2014, August). Social engineering attack framework, In *2004 Information Security for South Africa, Johannesburg*, (p. 1–9). South Africa.
60. Nelson, E. R. (2001). *Methods of Hacking: Social Engineering*, Institute for Systems Research, University of Maryland.
61. Tosun, A. (2015). *A Survey About The Integration of Social Engineering Attacks With Cyber Security Exploiting Turkish Vulnerabilities in Turkey*, Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi Bilişim Enstitüsü, Ankara.
62. İnternet: INFORMIT. URL: <https://www.informit.com/articles/article.aspx?p=1350956>, Son Erişim Tarihi: 11.04.2020.
63. Yalçın, N., ve Avşar, A. (2018). *Sosyal Mühendislik Atakları ve Alınması Gereken Önlemler*, 20. Akademik Bilişim 2018 Konferansı Bildirileri, Karabük Üniversitesi, 77-85.
64. İnternet: Karabulut, Y.E. (2010). URL: <https://www.karabulut.co/sosyal-muhendislik-saldirilari-tubitak-uekae/>, Son Erişim Tarihi: 25.04.2020.
65. Hadnagy, C. (2010). *Social Engineering: The Art of Human Hacking*. Indianapolis, Indiana: Wiley Publishing, Inc.
66. İnternet: Siber Güvenlik. *BLOGGER*. URL: <http://siberhat.blogspot.com/2015/08/omuz-sorfu.html>, Son Erişim Tarihi: 24.03.2020.
67. İnternet: The Social Engineering Framework. *SECURITY*. URL: <https://www.social-engineer.org/framework/influencing-others/influence-tactics/reciprocity/>, Son Erişim Tarihi: 24.11.2020.
68. Petty, R. E. and Cacioppo, J. T. (1996). *Attitudes and persuasion: Classic and contemporary approaches* (First edition). Boulder, CO: Westview Press.
69. Cialdini, R. (2009). *İkna Etmenin Bilimsel Olarak Kanıtlanmış 50 Yolu*. (Çev. Fulya Özgener). İstanbul: Pegasus Yayınları.
70. İnternet: Karabulut, Y.E. (2012). URL: <https://www.karabulut.co/sahte-senaryolar-uydurmak-pretexting/>, Son Erişim Tarihi: 15.11.2020.
71. İnternet: Bağcı, H. (2016). Sosyal Mühendislik ve Denetim. *Denetişim*, (1), 42-51. URL: <https://dergipark.org.tr/tr/pub/denetisim/issue/22499/240554>, Son Erişim Tarihi: 13.11.2020.
72. İnternet: Kaspersky. URL: <https://www.kaspersky.com/blog/the-human-factor-in-it-security/>, Son Erişim Tarihi: 18.04.2020.

73. Charles, E., and Lively, Jr. (December, 2004). Psychological Based Social Engineering, *SANS Institute*, Global Information Assurance Certification Paper, GIAC Certification.
74. İnternet: 5 Emotions Used in Social Engineering Attacks. *SECUREWORLD*. URL: <https://www.secureworldexpo.com/industry-news/5-emotions-hackers-use-social-engineering-attacks>, Son Erişim Tarihi: 24.04.2020.
75. Saleem, J., and Hammoudeh, M. (2020). Defense methods against social engineering attacks, *In Computer and Network Security Essentials*, 603-618.
76. İnternet: Kohn, A. (2014). Brain Science: The Forgetting Curve—the Dirty Secret of Corporate Training. URL: <https://learningsolutionsmag.com/articles/1379/brain-science-the-forgetting-curve-the-dirty-secret-of-corporate-training>, Erişim Tarihi: 13.11.2020.
77. Robling, G., and Muller, M. (2009). Social engineering: a serious underestimated problem. URL: https://www.researchgate.net/publication/220807213_Social_engineering_a_serious_underestimated_problem, Son Erişim Tarihi: 26.04.2020.
78. Ahram, T. (2018). *Advances in human factors in cybersecurity: proceedings of the ahfe 2018 international conference on human factors in cybersecurity*. Orlando, Florida, USA: AHFE 2018 Conference on Human Factors in Cybersecurity, 11.
79. İnternet: Digital in 2020. *Wearesocial*. URL: <https://wearesocial.com/digital-2020>, Son Erişim Tarihi: 27.11.2020.
80. İnternet: Siber Güvenlik. *Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi*. URL: <https://cbddo.gov.tr/siber-gvenlik/>, Son Erişim Tarihi: 27.11.2020.
81. İnternet: Siber Güvenlik Kümelenmesi Hakkında. *Türkiye Siber Güvenlik Kümelenmesi*. URL: <https://www.siberkume.org.tr/Index>, Son Erişim Tarihi: 27.11.2020.
82. İnternet: Gartner Top 10 Trends in Data and Analytics for 2020. *GARTNER*. URL: <https://www.gartner.com/smarterwithgartner/gartner-top-10-trends-in-data-and-analytics-for-2020/>, Son Erişim Tarihi: 27.11.2020.
83. TUSIAD & MARSH. (2020). *2020 Türkiye Siber Risk Algı Araştırması*, 3-7.
84. Microsoft & MARSH. (2019). *2019 Global Cyber Risk Perception Survey*, 4-6.
85. Çek, E. (2017). *Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi*, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
86. Luo, R., Brody, R., Seazzu, A. and Burd, S. (2011, July). Social Engineering: The Neglected Human Factor for Information Security Management, *Information Resources Management Journal*, 24(3), 1-8.
87. Bezuidenhout, M., Mouton, F., and Venter, H. S. (2010). Social Engineering Attack Detection Model: SEADM, *Conference: Information Security for South Africa (ISSA)*.

88. İnternet: 2015 Data Breach Investigations Report. (2015). *Verizon Risk Team*. URL: <https://enterprise.verizon.com/resources/reports/dbir/>,p. 52-54.Son Erişim Tarihi: 28.11.2020.
89. Anıl-Keskin, D. ve Gözenman, S. (2019). Hile Riski Açısından Sosyal Mühendislik. *TİDE AcademIA Research*, 1(2), 281-306.
90. Jones, H., Towse, J. and Race, N. (2015). Susceptibility to email fraud: A review of psychological perspectives, data-collection methods, and ethical considerations. *International Journal of Cyber Behavior, Psychology and Learning*, 5(3), 13-29.
91. Williams, E., Beardmore, A. and Joinson, A. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412-421.
92. Anthony, B. (2019). Social Engineering: The Human Element of Cybersecurity, A *Capstone Project Submitted to the Faculty of Utica College, ProQuest Dissertations Publishing*.
93. Brodie, C. (2009). The importance of security awareness training. *SANS Institute Information Security Reading Room*, 1-24.
94. İnternet: Utility company reduces phishing susceptibility by more than 67%. (2020). *Proofpoint*. URL: <https://www.proofpoint.com/sites/default/files/2020-06/pfpt-es-state-of-the-phish-2020-reports-a4.pdf>
95. Mishra, B. K. and Saini, H. (2009). Cyber attack classification using game theoretic weighted metrics. *Approach World Applied Sciences Journal (Special issue of computer and IT)*, 206-215.
96. İnternet: Information Technology Security Training Requirements: A Role- and Performance-Based Model, Special Publication 800-16. *NIST*. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fnlpubs.nist.gov%2Fnistpubs%2Flegacy%2FSP%2Fnistspecialpublication800-16.pdf&date=2020-06-07>, Son Erişim Tarihi: 07.06.2020.
97. Huang, D. L., Rau, P. P. and Salvendy, G. (2010). Perception of information security. *Behaviour & Information Technology*, 29(3), 221-232.
98. İnternet: Bireysel Siber Güvenlik Farkındalık Araştırması. (2018). *KPMG*. URL: <https://assets.kpmg/content/dam/kpmg/tr/pdf/2018/05/bireysel-siber-farkindalik-arastirmasi.pdf&date=2020-11-28>, Son Erişim Tarihi: 28.11.2020.
99. Erol, S. E. (2016). *Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
100. Pazey, B. L and Cole, H. A. (2013). The role of special education training in the development of socially just leaders: Building an equity consciousness in educational leadership programs. *Educational Administration Quarterly*. 49, 243–271.
101. Jansson, K. (2011). *A Model for Cultivating Resistance to Social Engineering Attack*, Ph. D. Thesis, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa.

102. Aldawood H. and Skinner G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues. *Future Internet*, 11(3), 73.
103. İnternet: Siber Güvenlik Olgunluk Seviyesi. SPARTA. URL: <https://sparta.com.tr/blog/siber-guvenlik-olgunluk-seviyesi/>, Son Erişim Tarihi: 25.06.2020.
104. Zhang, Q., Man, D. and Yang, W. (2009). *Using HMM for Intent Recognition in Cyber Security Situation Awareness*. Proceedings of the Second International Symposium on Knowledge Acquisition and Modeling, Wuhan, China. 231-236.
105. Kritzing, E. and von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, 29(8), 840-847.
106. Greca, I. M. and Moreira, M. A. (2000). Mental models, conceptual models, and modelling. *International Journal of Science Education*. 22(1), 1-11.
107. Özbenli H. H. ve Özlü M. (2017, 20-21 Ekim). *Siber Güvenlik Ekosisteminin Geliştirilmesi Modeli: Siber Güvenlik Kümelenmesi*. Proceedings of X. International Conference on Information Security and Cryptology.
108. İnternet: Güvenlik Çözümleri. BEYAZ NET. URL: https://www.beyaz.net/tr/guvenlik/cozumler/loglama_ve_siem_cozumlerimiz.html, Son Erişim Tarihi: 23.06.2020.
109. İnternet: Güvenlik Çözümleri. SIBERTIS. URL: <https://sibertis.com.tr/bilgi-guvenligi/>, Son Erişim Tarihi: 23.06.2020.
110. İnternet: Siber Saldırılarına Karşı Alınacak Önlemler. İŞNET. URL: <https://www.isnet.net.tr/BlogIcerik/siber-saldirilara-karsi-alinacak-onlemler-min>, Son Erişim Tarihi: 10.06.2020
111. İnternet: Güvenlik Önlemleri. DOLPWAY. URL: <https://dolpway.com/>, Son Erişim Tarihi: 11.06.2020.
112. İnternet: Sağlık Bilgi Sistemleri Genel Müdürlüğü. Sağlık Bakanlığı. URL: <https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%B1Politikalar%C4%B1K%C4%B1lavuzu.pdf&date=2020-06-21>, Son Erişim Tarihi: 21.06.2020.
113. İnternet: Trend Micro. URL: https://www.trendmicro.com/tr_tr/business.html, Son Erişim Tarihi: 26.08.2020.
114. İnternet: Norton. URL: <https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html>, Son Erişim Tarihi: 13.06.2020.
115. İnternet: Medium. URL: <https://medium.com/@halilozel1903/sosyal-m%C3%BChendislik-nedir-754984e5b0aa>, Son Erişim Tarihi: 16.06.2020.
116. İnternet: BT Günlüğü. URL: <https://www.btgunlugu.com/sosyal-muhendislik-saldirilari-nasil-korunuruz/>, Son Erişim Tarihi: 16.06.2020.

117. İnternet: Earthlink. URL: <https://www.earthlink.net/security-and-tools/>, Son Erişim Tarihi: 17.06.2020.
118. Yeniman Yıldırım, E. (2018). Bilişim Sistemlerine Yönelik Siber Saldırıları ve Siber Güvenliğin Sağlanması. *Mesleki Bilimler Dergisi (MBD)*, 7(2), 24-33.
119. Kör, A. (2015). *Siber Saldırıları İçin Dinamik Bir Çözüm Modeli*, Yüksek Lisans Tezi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara.
120. Vural, Y. ve Sağiroğlu, Ş. (2008, 25-27 Aralık). Ülke Bilgi Güvenliği. 3. *Uluslararası Katılımlı Bilgi güvenliği ve Kriptoloji Konferansı*, Ankara.
121. Mohammed, S. and Apeh E. (2016, January). A Model for Social Engineering Awareness Program for Schools. *10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*. Chengdu, China.
122. Curtis, B., Hefley, W. E. and Miller, S. A. (2002). *The people capability maturity model: Guidelines for improving the workforce*, Addison-Wesley: Software Engineering Institute.





EKLER

EK-1. Etik Kurul Kararı

Evrak Tarih ve Sayısı: 21.10.2020-E.113152



T.C.
GAZİ ÜNİVERSİTESİ
Ölçme Değerlendirme Etik Alt Çalışma Grubu



Sayı : 91610558-302.08.01-
Konu : Bilişsel ve Eğitim Amaçlı

BİLİŞİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 24.07.2020 tarih ve E.79158 sayılı yazı

İlgi yazınız ile göndermiş olduğunuz, Enstitünüz Bilişim Sistemleri Anabilim Dalı **Yüksek Lisans Öğrencisi Berna TOZLU'nun, Doç.Dr.Çelebi ULUYOL'un** danışmanlığında yürüttüğü **"Siber Güvenlikte Sosyal Mühendisliğe Karşı Bir Model Geliştirilerek Test Edilmesi"** adlı tez çalışması ile ilgili konu Kurulumuzun 08.09.2020 tarih ve 08 sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi ve gereğini rica ederim.

e-imzalıdır
Prof. Dr. İsmail KARAKAYA
Kurul Başkanı

Araştırma Kod No: 2020 -539

Ek: 1 Liste



ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : Tozlu, Berna
 Uyuğu : T.C.
 Doğum tarihi ve yeri :
 Medeni hali :
 Telefon :
 e-posta :

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilişim Sistemleri	Devam ediyor
Lisans	Selçuk Üniversitesi/ Bilgisayar Mühendisliği	2016
Lise	Namık Kemal Anadolu Lisesi	2011

İş Deneyimi

Yıl	Yer	Görev
2019-Halen	Radio ve Televizyon Üst Kurulu	Üst Kurul Uzman Yardımcısı
2018-2019	Sosyal Güvenlik Kurumu	Programcı

Yabancı Dil

İngilizce

Yayınlar

1. Tozlu, B. (2020). Kamu Kurum ve Kuruluşlarında Sosyal Mühendislik ve Siber Güvenlik Algısı. *UBAK 9. Uluslararası Bilimsel Araştırmalar Kongresi, Fen ve Mühendislik Bilimleri, Bildiri Tam Metin Kitabı*, 301-316, Ankara.



GAZİLİ OLMAK AYRICALIKTIR..