RECEP ALMALI

İŞLETME YÖNETİMİ ANABİLİM DALI

ŞUBAT 2025

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

ÇALIŞANLARIN SİBER GÜVENLİK FARKINDALIKLARININ ÖLÇÜLMESİ VAN İLİ ÖRNEĞİ

RECEP ALMALI

İŞLETME YÖNETİMİ
ANABİLİM DALI

ŞUBAT 2025

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME YÖNETİMİ ANA BİLİM DALI

ÇALIŞANLARIN SİBER GÜVENLİK FARKINDALIKLARININ ÖLÇÜLMESİ: VAN İLİ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

HAZIRLAYAN
RECEP ALMALI

DANIŞMAN
DOÇ.DR. CELAL KIZILDERE

VAN – 2025

KABUL VE ONAY

.RECEP ALMALI tarafından hazırlanan "Çalışanların Siber Güvenlik Farkındalıklarının Ölçülmesi: Van İli Örneği" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Van Yüzüncü Yıl Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri	**İmza**
Danışman: Unvanı Adı SOYADI: Doç.Dr Celal KIZILDERE Üniversite Adı, Anabilim Dalı Yüzüncü yıl Üniversitesi, İktisadi Gelişme Ve Uluslararası İktisat Anabilim Dalı Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.	...……
Başkan: Unvanı Adı SOYADI: Prof. Dr. Faruk KALAY Üniversite Adı, Anabilim Dalı Yüzüncü yıl Üniversitesi, Yönetim Ve Organizasyon Anabilim Dalı Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.	……...
Üye: Unvanı Adı SOYADI: Doç. Dr. Abdullah OĞRAK Üniversite Adı, Anabilim Dalı Bursa Teknik Üniversitesi, Yönetim Ve Organizasyon Anabilim Dalı Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.	……...
Üye: Unvanı Adı SOYADI Üniversite Adı, Anabilim Dalı Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.	……...
Yedek Üye: Unvanı Adı SOYADI Üniversite Adı, Anabilim Dalı Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.	……...
Yedek Üye: Unvanı Adı SOYADI Üniversite Adı, Anabilim Dalı Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.	……...
Tez Savunma Tarihi:	30/01/2025
Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini ve imzaların sahiplerine ait olduğunu onaylıyorum. …….……. Doç. Dr. Ercan ÇALIŞ Sosyal Bilimler Enstitüsü Müdürü	

ETİK BEYAN

Van Yüzüncü Yıl Üniversitesi, Sosyal Bilimler Enstitüsü **Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;**

- 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 çalışmasında 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. (Tarih)

İmza
RECEP ALMALI

Yüksek Lisans Tezi

RECEP ALMALI

VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

02, 2025

ÇALIŞANLARIN SİBER GÜVENLİK FARKINDALIKLARININ ÖLÇÜLMESİ: VAN İLİ ÖRNEĞİ

ÖZET

Günümüzde, Bilgi Teknolojileri hayatımızın her alanında olduğu gibi iş hayatının da vazgeçilmez bir unsuru haline gelmiştir ve hemen hemen her alanda etkin bir şekilde kullanılmaktadır. Bilgi teknolojilerinin çalışma hayatında giderek artan etkisini ve çalışanların siber güvenlik farkındalıklarının iş sürekliliği açısından da kritik bir öneme sahip olduğunu göstermektedir. Araştırma kapsamında, bilgi güvenliği ve siber güvenlik kavramları ele alınmış, Van ilinde ikamet eden ve aktif olarak çalışma hayatında bulunan çalışanların siber güvenlik bilgi düzeylerini ölçmek amacıyla bir anket araştırması gerçekleştirilmiştir.

Katılımcılardan çevrimiçi ve yüz yüze görüşmeler ile veriler elde edilmiş olup, SPSS istatistik programı kullanılarak analizler yapılmıştır. Elde edilen sonuçlar, çalışanların genel olarak orta seviyede siber güvenlik farkındalığına sahip olduklarını göstermektedir. Bu bulgular, iş sürekliliğini sağlamak ve bilgi güvenliğini korumak adına siber güvenlik farkındalık bilincinin artırılmasının önemli bir gereklilik olduğunu ortaya koymaktadır. Özellikle iş yerlerinde, çalışanların bu konuda daha fazla bilinçlenmesi için eğitim ve farkındalık programlarının uygulanması kritik bir öneme sahiptir.

Anahtar Kelimeler: Bilgi teknolojileri, Bilgi Güvenliği, Siber Güvenlik, Çalışanlar.

Sayfa Sayısı: ix+92

Tez Danışmanı: Doç. Dr. Celal KIZILDERE

M.Sc. Thesis

RECEP ALMALI

VAN YÜZÜNCÜ YIL UNIVERSITY

INSTITUTE OF SOCIAL SCIENCES

02, 2025

MEASURING EMPLOYEES' CYBER SECURITY AWARENESS: AN EXAMPLE OF VAN PROVINCE

ABSTRACT

In today's world, Information Technology has become an indispensable element in every aspect of our lives, including the business world, and it is actively utilized in almost every field. This highlights the increasing impact of information technologies in the workplace and the critical importance of employees' cybersecurity awareness for business continuity. The research focuses on information security and cybersecurity concepts, aiming to measure the cybersecurity knowledge levels of employees residing in Van who are actively engaged in their professional lives.

Data were collected through online and face-to-face interviews with participants, and analyses were conducted using the SPSS statistical software. The results indicate that employees generally have a moderate level of cybersecurity awareness. These findings reveal the essential need to enhance cybersecurity awareness in order to ensure business continuity and protect information security. Particularly in workplaces, implementing training and awareness programs to increase employees' consciousness in this area holds critical importance.

Key Words: Information Technology, Information Security, Cybersecurity, Employees.

Quantity of Page: ix+92

Supervisor: Doç. Dr. Celal KIZILDERE

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
İÇİNDEKİLER iii
TABLOLAR LİSTESİ vi
ŞEKİLLER LİSTESİ vii
SİMGELER VE KISALTMALAR DİZİN viii
ÖNSÖZ VE TEŞEKKÜR ix
GİRİŞ 10
1. BİLGİ GÜVENLİĞİ 14
1.1. Bilgi Güvenliği Genel Tanımı 14
1.2. Bilgi Güvenliğinin Önemi 16
1.3. Bilgi güvenliğinin Unsurları 17
1.3.1. Gizlilik (Confidentiality) 18
1.3.2. Bütünlük (Integrity) 19
1.3.3. Erişilebilirlik (Availability) 20
1.4. Bilgi güvenliğinin temel kavramları 21
1.4.1. Veri 21
1.4.2. Bilgi 21
1.4.3. Enformasyon 22
1.5. Bilgi Güvenliğinin Amaçları 22
1.6. Bireysel Bilgi Güvenliği 23
1.6.1. Bireysel Bilgi Güvenliğinin Önemi 24
1.6.2. Kişisel Verilerin Korunması 24
1.6.3. Bireysel Bilgi Güvenliği İçin Alınacak Temel Önlemler 25
1.7. Bilgi Güvenliği ve Politika Geliştirme İhtiyacı 26
1.7.1. Bilgisayar ve Ağ Güvenliği 26
1.7.2. Bilgi Güvenliği Yönetim Sistemi: 27
1.7.3. Bilgi Güvenliği Yönetişimi: 27
1.7.4. Kriptoloji: 27
1.7.5. Siber Güvenlik: 27
1.7.6. Bilişim Suçları: 27

1.7.7. Veri Mahremiyeti ve Korunması: 27
1.7.8. Ulusal Güvenlik: 27
1.7.9. Uluslararası İşbirliği: 27
1.8. Türkiye'de Bilgi Güvenliği Çalışmaları 28
1.9. Bilgi Güvenliğinin Tarihsel Gelişimi 29
2. SİBER GÜVENLİK 34
2.1. Siber Güvenliğin Tanımı 34
2.2. Siber Güvenliğin Önemi 36
2.3. Siber Güvenliğin Amaçları 37
2.3.1. Dijital Varlıkları Koruma 37
2.3.2. Ağ ve Sistem Güvenliğini Sağlama 37
2.3.3. Veri Gizliliğini ve Bütünlüğünü Koruma 37
2.3.4. Saldırılara Karşı Proaktif Önlemler Alma 37
2.4. Siber Tehdit Türleri 37
2.4.1. Zararlı Yazılımlar(Malware) 37
2.4.2. Sosyal Mühendislik Saldırıları 38
2.4.3. Dağıtık Hizmet Reddi(DDoS) Saldırıları 38
2.4.4. İleri Seviye Kalıcı Tehditler(APT) 39
2.4.5. Ransomware (Fidye Yazılımı) 39
2.5. Siber Tehdit Yöntemleri 40
2.5.1. Phishing (Kimlik Avı, Oltalama) 40
2.5.2. SQL Injection 41
2.5.3. Man-in-the-Middle (MitM) Saldırıları 42
2.5.4. Zero-Day Saldırıları(Sıfırıncı Gün Saldırıları) 42
2.5.5. Cross-Site Scripting (XSS) 42
2.6. Siber Saldırılardan Korunma Yöntemleri 43
2.6.1. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı(2020-2023) **45**
2.6.2. Olay Müdahale Planları ve Prosedürleri 45
2.6.3. Veri Yedekleme ve Kurtarma 46
2.6.4. Şifreleme Teknikleri 47
2.6.5. Bilgi Güvenliği Yönetim Sistemleri (BGYS) 48
2.6.6. Güvenlik Politikalarının Oluşturulması 50

2.6.7. Risk Yönetimi ve Değerlendirmesi 52
2.6.8. Kişisel Verilerin Korunması Kanunu (KVKK) 53
2.6.9. Genel Veri Koruma Yönetmeliği (GDPR) 53
2.7. Türkiye'de Siber Güvenlik 54
3. LİTERATÜR ARAŞTIRMASI 56
3.1. Siber Güvenlik Alanında Yapılan Önceki Çalışmalar 56
4. YÖNTEM 59
4.1. Araştırmanın Modeli 59
4.2. Evren ve Örneklem 59
4.3. Veri toplama araçları 62
4.4. Araştırmanın Hipotezleri 62
4.5. Siber Güvenlik Ölçeği 63
4.6. Verilerin Analizi 63
5. BULGULAR 71
5.1. Siber Güvenliğin Cinsiyete Göre Farkındalık Seviyesinin Ölçülmesi 71
5.2. Siber Güvenliğin Yaşa Göre Farkındalık Seviyesinin Ölçülmesi 72
5.3. Siber Güvenliğin Eğitim durumuna Göre Farkındalık Seviyesinin Ölçülmesi 74
5.4. Siber Güvenliğin Çalışılan Sektöre Göre Farkındalık Seviyesinin Ölçülmesi 76
6. SONUÇ VE ÖNERİLER 78
KAYNAKÇA 80
ÖZGEÇMİŞ
TEZ ORJİNALLİK RAPORU

TABLOLAR LİSTESİ

Tablo 1 Tablo 1 Güvenirlik Analizi Sonucu 63

Tablo 2 Ortalama, Çarpıklık ve Basıklık Değerleri (N=451) 64

Tablo 3 Doğrulayıcı Faktör Analizi 66

Tablo 4 Korelasyon Analizi 68

Tablo 5 Cinsiyete Göre Genel Siber Güvenlik Farkındalığı T-Testi Sonuçları 71

Tablo 6 Cinsiyete Göre Alt Boyutlar T-Testi Sonuçları 71

Tablo 7 Yaş gruplarına Göre Genel ANOVA sonuçları 72

Tablo 8 Yaş grupları Alt Boyutlara göre ANOVA sonuçları 73

Tablo 9 Eğitim Durumuna göre genel ANOVA sonuçları 74

Tablo 10 Eğitim durumu Alt Boyutlara göre ANOVA sonuçları 75

Tablo 11 Çalışılan Sektöre Göre genel ANOVA sonuçları 76

Tablo 12 Çalışılan Sektöre göre Alt boyutlar ANOVA sonuçları 76

ŞEKİLLER LİSTESİ

Şekil 1 McCumber Bilgi Güvenliği Modeli (McCumber, 1991) 18

Şekil 2 Ddos Saldırısı 38

Şekil 3 SQL injection Saldırısı 41

Şekil 4 MITM Saldırısı 42

Şekil 5 ISO 27001 Bilgi Güvenliği Yönetim Sistemi 49

Şekil 6 Araştırmanın katılımcılarına ait cinsiyet dağılımı 60

Şekil 7 Araştırmanın katılımcılarına ait yaş dağılımı 60

Şekil 8 Araştırmanın katılımcılarına ait eğitim düzeyi dağılımı 61

Şekil 9 Araştırmanın katılımcılarına ait çalışılan sektör dağılımı 62

SİMGELER VE KISALTMALAR DİZİN

APT	Advanced Persistent Threat
BGYS	Bilgi Güvenliği Yönetim Sistemi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
DDOS	Ditrubited Denial of Service
DPO	Data Protection Officer
GDPR	General Data Protection Regülation
KVKK	Kişisel Verilerin Korunması Kanunu
SIEM	Security Information and Event Management
SPSS	Statistical Package for the Social Science
SQL	Structed Query Language
TUBİTAK	Türkiye Bilimsel Araştırmalar Kurumu

ÖNSÖZ VE TEŞEKKÜR

Teknolojinin hızla geliştiği dünyada Bilişim teknolojileri her alanda hayatımızın içinde daha çok yer almaya başlamıştır. Bununla birlikte siber dünyada suç oranı ’da artış göstermiştir. Bununla paralel olarak Çalışma hayatında da hemen hemen her alanda iş ve işlemler bilgisayarlar ve internete bağlı birçok cihaz ile gerçekleştirilmektedir. Bu tehlikelerden korunmak için bireylerin farkındalıklarının arttırılması ve Siber suçlara karşı bilinçlendirilmesi kaçınılmaz bir hale gelmiştir.

Yüksek Lisans Tez çalışmam Süresince verdiği destekleri için Danışman Hocam Doç. Dr. Celal Kızıldere ’ye, Akademik anlamda kendimi geliştirmem için sürekli bilgisine danıştığım Dr. Öğretim Üyesi Vedat Almalı ’ya, verilerin analiz sürecinde desteklerini esirgemeyen Adem IŞIK, Tolga Demirel ve Yücel Ayçiçek’e bana her türlü desteğini esirgemeyen Elif Kurtboğa’ya teşekkürlerimi sunarım.

Son olarak, yüksek lisans eğitimim ve tez sürecimde yanımda olan, sabırla destek veren eşim Hande Akgün Almalı ve kızım Nehir Almalı ‘ya en içten teşekkürlerimi sunarım.

Recep ALMALI

GİRİŞ

Siber güvenlik, dijitalleşen dünyada bireyler ve kurumlar için hayati bir konu haline gelmiştir. Gelişen teknoloji, iş dünyasının her alanında bilgi güvenliğinin önemini artırmış ve siber tehditlere karşı bireylerin farkındalık seviyesini önemli bir unsur haline getirmiştir. Bu çalışma, Van ilinde çeşitli sektörlerde çalışan bireylerin siber güvenlik farkındalık düzeylerini belirlemeyi ve bu düzeyin demografik faktörlerle ilişkisini incelemeyi amaçlamaktadır. Siber güvenlik farkındalığının iş sürekliliği, veri güvenliği ve kurumsal itibar açısından kritik öneme sahip olduğu düşünüldüğünde, çalışanların bu alandaki bilgi düzeylerinin ölçülmesi büyük önem taşımaktadır. Araştırma sonuçları, Van ilindeki kurumların siber güvenlik stratejilerini geliştirmelerine ve çalışanların eğitim ihtiyaçlarını belirlemelerine yardımcı olmayı hedeflemektedir.

Bu araştırma, bireylerin siber tehditlere karşı ne kadar hazırlıklı olduklarını, bu tehditleri ne kadar iyi tanıdıklarını ve hangi önlemleri bildiklerini ölçmeyi amaçlar. Ayrıca, bireylerin bu alandaki farkındalıklarını artırmak için hangi tür eğitimlerin veya bilgilendirme faaliyetlerinin daha etkili olacağını belirlemeye çalışır.

A. Çalışmanın Metodolojisi

Bu çalışmada Nicel araştırma yöntemi kullanılmıştır. Araştırmanın temel veri toplama aracı olarak Arpaci ve Sevinç (2022) tarafından geliştirilen Siber Güvenlik Ölçeği kullanılmıştır. Anketler, Van ilinde çeşitli sektörlerde çalışan toplam 389 katılımcı ile gerçekleştirilmiştir. Veriler, çevrimiçi anket formu ve yüz yüze görüşme yöntemleri ile toplanmıştır. Nicel veriler, SPSS (Statistical Package for the Social Sciences) programı kullanılarak analiz edilmiştir. Demografik veriler ve siber güvenlik farkındalık düzeyleri arasındaki ilişkiler t-testi ANOVA, Welch Testi ve Brown-Forsythe Testi gibi istatistiksel yöntemlerle incelenmiştir. Aynı zamanda katılımcıların eğitim durumu, yaş, cinsiyet ve çalıştıkları sektör gibi demografik değişkenlerin siber güvenlik farkındalıkları üzerindeki etkileri de değerlendirilmiştir.

B. Çalışmanın Problem Cümlesi

Bu araştırmanın problem cümlesi, "Van ilinde çalışan bireylerin siber güvenlik farkındalıklarını etkileyen başlıca faktörler nelerdir?" şeklinde ifade edilmiştir. Bu çalışma, siber güvenlik farkındalığının çalışanlar arasında ne düzeyde olduğunu ve bu farkındalığı etkileyen unsurların neler olduğunu belirlemeyi hedeflemektedir. Aynı zamanda bu farkındalık seviyesinin artırılması için ne tür önlemlerin alınabileceği de araştırmanın merkezinde yer almaktadır.

C. Çalışmanın Soruları

Araştırmanın problemine dayalı olarak şu sorulara yanıt aranmıştır:

1. Van ilindeki çalışanların siber güvenlik konusundaki genel bilgi düzeyleri nedir?
2. Çalışanların siber güvenlik farkındalıkları hangi seviyededir ve bu farkındalık hangi demografik faktörlerle ilişkilidir?
3. Van ilindeki mevcut siber güvenlik eğitim programlarının kapsamı ve etkinliği ne düzeydedir?
4. Çalışanların siber güvenlik politikalarına uyumları ne kadar güçlüdür ve bu uyumun nedenleri nelerdir?
5. Siber güvenlik farkındalığını artırmak için hangi strateji ve yöntemler daha etkili olabilir?
6. Çalışanların siber tehditlere karşı hazırlık seviyeleri nedir ve bu hazırlık düzeyini artırmak için hangi önlemler alınmalıdır?

D. Çalışmanın Amacı ve Hedefleri

Bu araştırmanın temel amacı, Van ilinde çalışan bireylerin siber güvenlik farkındalık seviyelerini ölçmek ve bu farkındalık seviyelerinin demografik faktörlerle nasıl ilişkilendiğini incelemektir. Aynı zamanda, çalışanların siber tehditlere karşı ne kadar hazırlıklı olduklarını ve siber güvenlik konusunda hangi eğitimlere ihtiyaç duyduklarını belirlemek amaçlanmaktadır. Araştırmanın hedefleri arasında,

farkındalık düzeylerini artıracak eğitim ve bilgilendirme faaliyetlerinin belirlenmesi ve bu faaliyetlerin etkisinin değerlendirilmesi de yer almaktadır. Bölgesel düzeyde yapılan bu araştırmanın sonuçları, Van ilindeki kurumların siber güvenlik stratejilerini güçlendirmelerine yardımcı olacak ve çalışanların siber tehditlere karşı daha hazırlıklı olmalarını sağlayacak öneriler sunacaktır.

E. Çalışmanın Önemi

Siber güvenlik, günümüzde iş sürekliliğinin sağlanması ve veri güvenliğinin korunması, bu bağlamda büyük bir öneme sahiptir. Çalışanların siber güvenlik farkındalıklarının ölçülmesi, kurumların karşı karşıya kalabilecekleri potansiyel tehditlere karşı ne kadar hazırlıklı olduklarını anlamak açısından büyük bir değer taşır. Van ilindeki çalışanların farkındalık düzeylerini incelemek, yerel düzeyde siber güvenlik açıklarını tespit etmek ve bu açıkları kapatmak adına alınması gereken önlemleri belirlemek için önemlidir. Ayrıca, bu çalışma bölgesel düzeyde siber güvenlik farkındalığı konusunda bir ilk niteliği taşıması bakımından da önemlidir. Siber güvenlik bilincinin artırılması, hem bireylerin hem de kurumların bu tür tehditlere karşı daha dayanıklı hale gelmesine katkı sağlayacaktır.

F. Özgün Değer ve Yaygın Etki - Katma Değer

Bu çalışmanın özgün değeri, Van ilindeki çalışanların siber güvenlik farkındalık seviyelerini detaylı bir şekilde inceleyen ilk araştırmalardan biri olmasından kaynaklanmaktadır. Van ilinin sosyo-ekonomik yapısı göz önüne alındığında, bu çalışmanın sonuçları, bölgesel ve ulusal düzeyde siber güvenlik stratejilerinin geliştirilmesine önemli katkılar sağlayabilir. Ayrıca, siber güvenlik farkındalık düzeyini ölçmeye yönelik araştırmalar genellikle büyük şehirlerde yapılmakta olup, bu çalışma kırsal bölgelerdeki çalışanların farkındalık düzeyini de incelemesi bakımından yenilikçi bir yaklaşıma sahiptir. Araştırmanın bulguları, sadece yerel düzeyde değil, ulusal düzeyde de politika yapıcılar ve eğitim kurumları için önemli bilgiler sunarak, Türkiye'nin siber güvenlik kapasitesinin artırılmasına katkı sağlayacaktır.

G. Çalışmanın Organizasyonu

Bu çalışma toplam altı bölümden oluşmaktadır. İlk bölümde araştırmanın amacı, kapsamı ve problem durumu açıklanmıştır. İkinci bölümde kavramsal çerçeve oluşturulmuş ve bilgi güvenliği ile siber güvenlik kavramları detaylandırılmıştır. Üçüncü bölümde literatür taraması sunulurken, dördüncü bölümde araştırmanın yöntemi ele alınmış; evren, örneklem, veri toplama araçları ve analiz yöntemleri açıklanmıştır. Beşinci bölümde araştırma verileri SPSS programı ile analiz edilmiş ve bulgular sunulmuştur. Altıncı bölümde ise bulgular ışığında sonuçlar ve öneriler değerlendirilmiştir.

1. BİLGİ GÜVENLİĞİ

Bilim ve teknolojinin hızla gelişmesiyle birçok kavram farklı anlamlar kazanmıştır. "Bilgi" kelimesi, aslında "bilmek" fiilinden türemiştir ve bu nedenle bilme arzusuyla yanıp tutuşan insanoğlunun bilgiye verdiği değer, tarih boyunca oldukça belirgindir. İlk insanlardan günümüze kadar din, felsefe ve bilim alanlarında bilgi her zaman değerli bir unsur olarak kabul edilmiştir. Ancak günümüzde bilgi kavramı sıkça kullanılsa da, net bir tanım yapmak zordur. Sparrow (2008), bu durumu bilginin günlük hayatta öğreti, sezgi, duygu ve yargı gibi kavramlarla iç içe geçtiği şeklinde açıklamaktadır. İngilizcedeki "data", "information" ve "knowledge" gibi kavramların dilimizde genellikle "bilgi" olarak ifade edilmesi, bu karmaşayı daha da derinleştirmektedir (Canbek ve Sağıroğlu, 2006).

1.1. Bilgi Güvenliği Genel Tanımı

İçinde bulunduğumuz dönemi "bilgi toplumu" ya da başka bir ifadeyle "bilgi çağı" olarak tanımlamak olanaklıdır. Bilgi toplumunun ana unsurlarından olan bilginin, teknoloji ve kitle iletişim araçlarıyla hızlı yayılması, bilgi güvenliği meselesini gündeme getirmiştir. Bilgi, fiziksel ortamlara kaydedilebilen, düzenlenebilen, depolanabilen ve çeşitli iletişim araçlarıyla başkalarına iletilebilen bir özelliğe sahiptir (Dura ve Atik, 2002: 114). Bu sebeple, bilginin yaygınlaşmasının yanı sıra güvenliğinin sağlanması da büyük önem taşır.

Bilgi güvenliği, bilginin depolanması sürecinde silinme gibi zarar verici durumlara ve muhtemel risklere karşı korunmasını amaçlayan çeşitli uygulamaları içermektedir (Önel ve Dinçkan, 2007: 6). Bilgi güvenliği, işlenmiş verinin yetkili kişiler tarafından kaynaktan alıcıya gizlilik içinde, herhangi bir değişikliğe uğramadan ve bütünlüğü bozulmadan aktarılmasını ifade eder (Pfleeger, 1997: 15). Ayrıca, bilgi güvenliği, izinsiz erişimlerin engellenmesiyle bilginin ifşa edilmesini, değiştirilmesini, bozulmasını ya da yok edilmesini önlemek amacıyla yapılan koruma önlemlerini de içerir (Şen ve Yerlikaya, 2013: 677). Başka bir deyişle, bilgi güvenliği, bilgiyi dijital dünyada karşı karşıya kaldığı her türlü tehditten koruma mücadelesini temsil eder. Bu süreç, hem veri bütünlüğünü sağlamak hem de bilginin gizliliğini korumak için sürekli bir çaba gerektirir.

Bilgi güvenliği, elektronik ortamda verilerin veya bilgilerin saklanması, iletilmesi, işlenmesi aşamasında bu bilgilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması amacıyla yapılan çalışmaların bütününü kapsar. Temel hedef, bu bilgilerin yetkisiz kişilerce erişilmesini, değiştirilmesini ya da yok edilmesini engellemek, aynı zamanda verilerin doğruluğunu ve kullanılabilirliğini garanti altına almaktır (Baykara, Daş ve Karadoğan, 238). Burada vurgulanması gereken önemli bir husus, bilgi güvenliğinin kullanılan teknolojiden bağımsız olarak ele alınması gerektiğidir. Bilgi, ister kâğıt ortamında isterse dijital sistemlerde bulunsun, korunmaya muhtaçtır ve tehditlere karşı önlemler alınması zorunludur.

Tarihsel olarak, bilgi güvenliği ilk olarak diplomatik ve askeri alanlarda, gizlilik ve sırların korunmasının önemli olduğu durumlarda ortaya çıkmıştır. İlk zamanlarda, bilgi güvenliği yalnızca istihbarata karşı koyma ve büyük öneme sahip bilgiyi koruma açısından ele alınmıştır. Ancak, bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte, bilginin dijitalleşmesi ve bilgi sistemlerinde saklanabilir hale gelmesi, güvenlik gereksinimini geniş bir kitleye yaymıştır. Bilgi toplumuna geçiş süreciyle birlikte, kişisel bilgisayarlardan karmaşık bilgi altyapılarına kadar birçok sistem bilgi depolamaya başlamış, bu da bilgi güvenliği olgusunun önemini artırmıştır. Bilgi güvenliği, aslında yeni bir kavram değildir. Yazılı bilginin saklanabildiği ilk çağlardan itibaren, bilgi çalınabilir ve yok edilebilir bir değer olarak görülmüş, bu nedenle de korunması için çeşitli tedbirler alınmıştır (Güngör, 2015: 6).

Bilgi güvenliği, giderek artan dijitalleşme ve siber tehditlerin gelişmesiyle birlikte daha fazla önem kazanan bir alandır. Bu güvenliğin sağlanabilmesi için uygun ve etkili güvenlik politikalarının belirlenmesi ve titizlikle uygulanması gerekmektedir. Güvenlik politikaları, bilgi sistemlerine erişimlerin izlenmesi, kullanıcı yetkilerinin yönetilmesi, veri değişikliklerinin kaydedilmesi (loglama) ve verilerin silinme süreçlerinin sınırlandırılması gibi yöntemleri kapsar. Örneğin, bir sistemde yapılan her değişikliğin izlenebilir olması, sorumlulukların dağıtılması ve yanlış bir müdahale durumunda kimin ne zaman müdahale ettiğinin bilinebilmesi, bilgi güvenliğinin sürdürülebilirliği açısından kritik önem taşır.

Bilgi güvenliği aynı zamanda, yazılım güvenliği, ağ güvenliği, veri şifreleme, kimlik doğrulama ve güvenli erişim kontrolü gibi teknik önlemleri de içerir. Bu teknik

önlemler, potansiyel tehditlere karşı proaktif olarak savunma yapmayı amaçlar ve siber saldırılara karşı sistemin dayanıklılığını artırır.

Daha genel anlamda bilgi güvenliği, güvenlik mühendisliğinin bir alt alanı olarak kabul edilir ve bu disiplin, güvenlik tehditlerinin analiz edilmesi, risk yönetimi süreçlerinin tasarlanması, güvenlik zafiyetlerinin giderilmesi gibi geniş kapsamlı çalışmaları içerir (Canbek ve Sağıroğlu, 2006: 168). Güvenlik mühendisliği, sistematik bir yaklaşımla güvenlik politikalarının oluşturulması ve uygulanmasını sağlayarak, hem bilgi hem de fiziksel varlıkların korunmasına yönelik çözümler sunar. Dolayısıyla bilgi güvenliği sadece teknik bir mesele değil, aynı zamanda kurumsal bir disiplin ve sürekli gelişim gösteren bir alandır.

1.2. Bilgi Güvenliğinin Önemi

Günümüzde elektronik ortamda depolanan bilgi, önemli bir varlık olarak değerlendirilmektedir. Özellikle kütüphaneler, arşivler ve bilgi merkezlerinde, bilginin gizliliği ve bütünlüğünün korunması, bilgi profesyonelleri için bir zorunluluk haline gelmiştir. Bu merkezlerin artan dijitalleşme ve veri depolama oranları, siber saldırılara daha açık hale gelmelerine neden olmaktadır. Bilgi sistemlerine bağımlılık arttıkça, bu tehditlere karşı alınacak güvenlik önlemleri de bilgi profesyonellerinin sorumlulukları arasına girmektedir. Elektronik bilgiye yönelik klasik güvenlik önlemleri ise, büyük ölçüde fiziksel güvenlik dışında önemini kaybetmiştir (Henkoğlu ve Uçak, 2012:379).

Bilgi güvenliği, özellikle internet üzerinden yayılan virüsler, solucanlar, truva atları, kötü amaçlı yazılımlar, iç saldırganlar (internal hacker), güvenlik açıklarından kaynaklanan istismarlar ve yapılandırma hataları gibi unsurlarla tehdit edilmektedir. Bu tür ihlaller, veri kaybı, finansal zararlar, itibar kayıpları, hizmetlerin aksaması veya kesintiye uğraması, gizli bilgilerin sızdırılması gibi istenmeyen sonuçlara yol açabilmektedir (Tekerek, 2008: 132)

Bilgi güvenliğinin sağlanmasında, güvenlik politikaları ve standartların belirleyici bir rolü bulunmaktadır. Bu politikalar, üst yönetim tarafından desteklenmeli, kullanıcılar tarafından kolayca anlaşılabilir ve uygulanabilir olmalıdır. Kurum kültürü ile uyumlu, kurum genelinde kabul görmüş güvenlik politikaları olmadan, bilgi güvenliğinin etkin bir şekilde sağlanması ve yönetilmesi son derece

güçtür. Bilgi güvenliğinin tam anlamıyla tesis edilebilmesi için teknik önlemler tek başına yeterli değildir. Bu önlemlerin yanı sıra, idari tedbirler (kurallar, cezalar, yaptırımlar vb.), güvenlik standartları (ISO 27001, Ortak Kriterler vb.) ve insan faktörü de dikkate alınmalıdır (Fussell, 2005).

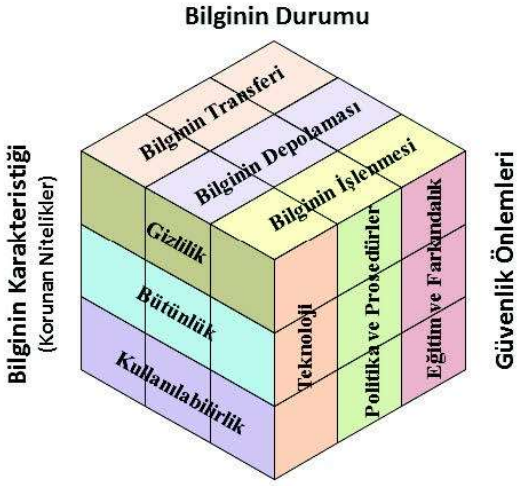
Bilgi güvenliğini sağlamanın kurumlara sağlayacağı yararları şu şekilde sıralayabiliriz:

- Bilgileri korumak, yetkisiz ve izinsiz erişimleri engellemek,
- Siber ihlalleri önleyerek veri bütünlüğünü güvence altına almak,
- Siber saldırı risklerine karşı koruma sağlamak,
- Rekabet üstünlüğü elde etmek,
- İş sürekliliğini güvence altına almak,
- Bilgisayar kaynaklarının verimli kullanımını desteklemek,
- Üçüncü taraflara güven vererek iş ilişkilerini güçlendirmek,
- Yasal sorunların yaşanmasını önlemek (Çubukçu, 2018: 4).

1.3. Bilgi güvenliğinin Unsurları

Bilgi teknolojilerindeki hızlı gelişmeler, bilginin depolanması ve taşınmasını daha erişilebilir ve etkin hale getirmiştir. Çok fonksiyonlu ve kompakt teknolojik cihazların yaygınlaşmasıyla birlikte, gün geçtikçe daha fazla veri dijital ortamlara aktarılıyor, depolanıyor ve işleniyor. Bu süreç, hem kişisel hem de kurumsal bilgilerin hızla dijitalleşmesine ve elektronik sistemlerde saklanmasına olanak tanıyor. Dijitalleşmenin artışıyla, bilgilere daha hızlı erişim, verilerin daha kolay analiz edilmesi ve daha büyük miktarda veriyle çalışabilme imkânları doğarken, aynı zamanda bilgi güvenliği konusunda da daha fazla dikkat ve özen gerektiriyor. Verilerin dijital ortamlarda işlenmesi, siber tehditlere karşı korunması ve gizliliğinin sağlanması için etkili güvenlik politikalarının uygulanmasını zorunlu hale getiriyor. Dolayısıyla bilginin elektronik ortamda yaygın olarak kullanılması ve hareketliliği, bireyler, şirketler ve kurumlar için çeşitli güvenlik risklerini ve sorunlarını da beraberinde getirmektedir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009: 597).

Bilgi güvenliği, sürekli korunması gereken belirli ilkelerle şekillenir. Solomon'un (Solomon ve Chapple, 2005) bilgi güvenliği üçgenine göre, bu ilkeler gizlilik, bütünlük ve erişilebilirlik olarak tanımlanır. Bu üç temel unsur, bilgi güvenliğinin yapı taşlarını oluşturur ve bilgi güvenliği uygulamaları bu prensipler etrafında gelişir.



Şekil 1 McCumber Bilgi Güvenliği Modeli (McCumber, 1991)

1.3.1. Gizlilik (Confidentiality)

TSE-17799 "Bilgi Güvenliği Yönetim Standardı" belgesinde gizlilik, bilginin yalnızca yetkilendirilmiş kişilerin erişimine açık olmasını sağlama olarak tanımlanmaktadır (32). Ülker, Canbay ve Sağıroğlu (2017: 34) gizliliği, kullanıcı ile teknolojik ekosistem (ağ, sunucu ve uygulama) arasında korunması gereken bir bilgi güvenliği unsuru olarak tanımlamaktadır.

Yerlikaya'ya (2019) göre, gizlilik kavramı, yetkisiz kişilerin kötü niyetli bir şekilde verilere erişse bile, bu verilerin anlaşılmasını ve çözümlenmesini engellemeyi hedefler. Bu amaçla, bilginin anlaşılmasını zorlaştıracak çeşitli yöntemler devreye sokulur. Özellikle şifreleme prosedürleri ve steganografi teknikleri kullanılarak, gizlilik ilkesinin devamlılığı sağlanır.

Fussell'e (2005) göre gizlilik, hassas bilgilere yetkisi ve izni olmayan kişilerin erişimini engellemek anlamına gelir. Gizlilik, statik ortamlarda ve ağ üzerinde dinamik verilerin bir göndericiden bir alıcıya iletilmesi sırasında sağlanmalıdır. Saldırganlar,

gizli bilgilere çeşitli yollarla erişim sağlayabilirler; bu yollar arasında şifrelerin yer aldığı veri tabanlarının ele geçirilmesi ve sosyal mühendislik saldırıları, siber güvenlik tehditleri arasında önemli bir yer tutar. Şifre veri tabanlarının kötü niyetli kişilerce çalınması, kullanıcı hesaplarının tehlikeye girmesine yol açarken, sosyal mühendislik ise insan psikolojisini hedef alarak bilgilerin kandırma yoluyla elde edilmesi anlamına gelir. Bu tür saldırılar, güvenlik zafiyetlerinden faydalanarak kritik verilere erişim sağlamayı amaçlar. Bilgisayar başında çalışan bir kullanıcının gözetlenmesi ya da kullanıcıdan fark ettirmeden özel bilgilerin (şifre vb.) ele geçirilmesi gibi durumlar da mümkündür.

Gizliliğin sağlanmasında kullanılan başlıca yöntemler şunlardır:

- **Şifreleme:** Bilgilerin yetkisiz kişiler tarafından okunmasını engellemek için kullanılır.
- **Erişim Kontrolleri:** Kimlerin hangi bilgilere erişebileceğini belirler ve sınırlar.
- **Kimlik Doğrulama:** Kullanıcıların kimliklerini doğrulamak için şifreler, biyometrik veriler veya iki faktörlü kimlik doğrulama gibi yöntemler kullanılır.

1.3.2. Bütünlük (Integrity)

Bilginin bütünlüğü, verilerin doğru, eksiksiz ve yetkisiz değişikliklere karşı korunmasını sağlayan bir özelliktir. Bu ilke, verilerin tüm yaşam döngüsü boyunca tutarlı, doğru ve güvenilir kalmasını hedefler. Veriler transfer edilirken, herhangi bir değişiklikten korunmalı ve yetkisiz kişiler tarafından müdahale edilmemelidir. Bu amaçla, dosya izinleri ve kullanıcı erişim kontrolleri gibi teknik önlemler uygulanmalıdır. Ayrıca, verilerin bütünlüğünü doğrulamak için sağlama toplamları ve şifreleme sağlama toplamları kullanılabilir. Verilerin etkilenmesi durumunda doğru hale getirilebilmesi için yedekleme sistemleri ve veri yedekleri bulunmalıdır (Gündüz ve Daş, 2020: 975).

Fussell (2005), bilginin göndericiden alıcıya değişmeden, ekleme veya çıkarma yapılmadan, sırası değiştirilmeden ve tam olarak ulaştırılmasıyla bütünlüğün sağlandığını belirtir. Verinin bütünlüğünü korumak amacıyla çeşitli özetleme algoritmaları kullanılmaktadır.

- **Hash Fonksiyonları**: Verilerin değiştirilip değiştirilmediğini tespit etmek için kullanılır.
- **Dijital İmzalar**: Verilerin kaynağını ve bütünlüğünü doğrulamak için kullanılır.
- **Yedekleme ve Kurtarma**: Verilerin kaybolması veya bozulması durumunda geri yüklenebilmesi için düzenli yedeklemeler yapılır.

1.3.3. Erişilebilirlik (Availability)

Erişilebilirlik, bir bilginin ihtiyaç duyulduğunda yetkili kullanıcılar tarafından erişilebilir ve kullanılabilir olması anlamına gelir. Bu özelliği sağlamak için bilgi sistemlerindeki donanım ve yazılımlar dikkatle korunmalı, gerektiğinde hızlıca onarımlar yapılmalı ve yazılım hatalarından arındırılmış bir işletim sistemi sağlanmalıdır. Ayrıca, sistem güncellemelerinin düzenli olarak yapılması önemlidir (Gündüz ve Daş, 2020: 975).

İletişim bant genişliği sağlanmalı ve sistemde oluşabilecek darboğazlardan kaçınılmalıdır. Yedekleme, yük dengeleme ve RAID sistemleri gibi yüksek kullanılabilirlik çözümleri, donanım arızalarının ciddi sonuçlara yol açmasını önlemeye yardımcı olabilir. Felaket senaryolarına karşı hızlı ve esnek bir felaket kurtarma planı (DRP) oluşturulmalıdır. Bu plan, veri kaybını veya bağlantı kesintilerini önlemek için doğal afetler ve yangın gibi beklenmedik olaylara karşı önlemler içermelidir. Kritik verilerin farklı bir lokasyonda, yangına ve suya dayanıklı bir ortamda yedeklenmesi uygun olabilir. Bunun yanı sıra, güvenlik duvarları ve ara sunucular gibi ek güvenlik önlemleri, sistemin durmasına ve erişim problemlerine neden olabilecek hizmet aksatma (DoS) saldırıları ve ağdaki yetkisiz girişimlere karşı koruma sağlayabilir (Campbell, 2003).

- **Yedekli Sistemler**: Sistemlerin sürekli olarak çalışmasını garantilemek amacıyla yedekli donanım ve yazılım kullanılır. Bu, kesintisiz hizmet sunulmasına yardımcı olur.
- **DDoS Koruması**: Dağıtık Hizmet Engelleme (DDoS) saldırılarına karşı sistemlerin korunması sağlanır, bu sayede hizmetin aksaması önlenir.

- **Acil Durum Planları**: Sistemlerin arızalanması durumunda hızla toparlanabilmek için acil durum planları geliştirilir ve uygulanır.

Bu unsurlar, bilgi güvenliğinin etkin bir şekilde sağlanmasında hayati öneme sahiptir.

Yerlikaya'ya (2019) göre, erişilebilirlik hizmetinin temel amacı, hem kurum içinden hem de dışından kaynaklanabilecek erişilebilirliği azaltıcı tehditlere karşı bilişim sistemlerini korumaktır. Bu hizmet sayesinde, kullanıcılar verilere zamanında, hızlı ve güvenilir bir şekilde ulaşabilir. Sistemlerin erişilebilirliğini olumsuz yönde etkileyen bazı faktörler arasında doğal felaketler, yazılımlardaki yetersiz şifreleme uygulamaları ve bilinçsiz çalışanlar bulunmaktadır. Erişilebilirliğin sağlanması için fiziksel güvenlik önlemleri alınmalı, ayrıca casus yazılımlara karşı koruyucu yazılımlar ve virüs engelleyici programlar sürekli olarak güncel tutulmalıdır.

1.4. Bilgi güvenliğinin temel kavramları

1.4.1. Veri

Veri terimi, İngilizce "data" kelimesinden türetilmiştir ve bu kelime, Latince "datum" (çoğul şekli "data") kelimesine dayanır. Latince "datum" kelimesi, "vermek" fiilinin geçmiş zamanı anlamına gelir ve "verilen şey" olarak tanımlanır. M.Ö. 300 yıllarında Öklid'in çalışmalarında bu kavramın kullanıldığı belirtilmiştir. Türkçede de "veri" terimi, "verilen şey" anlamında kullanılır. Bilişim teknolojileri bağlamında veri, bir duruma ilişkin henüz birbirleriyle ilişkisi kurulmamış bilgilerdir. Bu bilgiler, dijital platformlarda yer alan ve iletilen sinyaller ya da bit dizileri şeklinde ifade edilebilir (Canbek ve Sağıroğlu, 2006).

1.4.2. Bilgi

Veri, belirli bir anlam ifade edecek şekilde düzenlendiğinde bilgiye dönüşür. Bu süreçte, veriler ve ilgili konular bir araya getirilerek bilgi üretilir. Bilgi, işlenmiş veriler olarak nitelendirilebilir ve Shannon tarafından "bir durum hakkında var olan belirsizliği azaltan bir kaynak" olarak tanımlanmıştır. Özetle, veriler üstünde gerçekleştirilen uygun işlemler mantıksal dönüşümler, ilişkiler kurma, formüller uygulama, varsayımlar yapma ve basitleştirmeler gibi bilgi üretir (Canbek ve Sağıroğlu, 2006).

1.4.3. Enformasyon

Enformasyon Toplumu veya Bilgi Çağı (Castells, 2005) olarak bilinen bu dönemde, bilginin tanımı, doğruluğu, yanlışlığı, tasarımı, edinim yöntemleri, kapsamı, araçları, teknolojisi, etik boyutları, kuralları, ölçüm yöntemleri, ekonomik etkileri, yasaları ve suçları gibi birçok alt alanın doğru bir şekilde kavranması son derece önemlidir.

Enformasyon bilimi sürekli olarak gelişmekte ve değişmektedir, bu da enformasyon bilimcilerinin tanım yapmasını zorlaştırır. Bu durum, bilimcilerin düzenli olarak bu değişimi takip ederek tanımlarını güncellemelerine neden olur (Zins, 2007: 479).

İtalyan filozof Luciano Floridi, bu zorluğu vurgulayarak, enformasyonun tanımlandığı birçok anketin tek bir ortak tanıma ulaşamadığını ifade eder Floridi, Stanford Encyclopedia of Philosophy'deki yazısında, bilginin çok biçimli ve çok anlamlı bir kavram olduğunu vurgular (Floridi, 2016).

1.5. Bilgi Güvenliğinin Amaçları

Bilgi güvenliği; iş sürekliliğinin sağlanması, kaçınılmaz felaket durumlarında kayıpların en aza indirilmesi ve firmaların temel yapı taşları olan kaynakların her koşulda gizlilik, erişilebilirlik ve bütünlüğünün korunmasını hedefler(Yılmaz, 2016: 46)

Bilgi güvenliğinin amaçları, internet ve kişisel bilgisayarların kullanımının 1990'lardan itibaren yaygınlaşmasıyla daha da önem kazanmıştır. Önceden bilgi kâğıt üzerinde olup dolaplarda saklanabilirken, bu dönemde bilgi bilgisayar ortamına geçiş yapmış ve daha kolay paylaşılır hale gelmiştir. Özellikle internetin hayatın her alanına yayılmasıyla, bilgi, küreselleşen iş dünyasında önemli bir rekabet aracı olmuştur. Firmalar, kuruluşlarından itibaren sektörlerine özgü uzmanlaşmış bilgileri depolamakta ve bu bilgi zamanla kurumsal yapı taşlarına dönüşmektedir. Dolayısıyla, bu depolanan bilgilerin erişilebilir ve kullanılabilir olması giderek daha kritik hale gelmiştir.

Günümüzde kurumlar, yalnızca çalışanlarıyla değil, aynı zamanda müşterileri, iş ortakları ve hissedarlarıyla tanımlandığından, bilginin korunması ve mahremiyeti

konusunda güven ortamının sağlanması stratejik bir öneme sahiptir. Güvenlik tehditleri, sadece iş sürekliliğini tehdit etmekle kalmayıp, aynı zamanda kuruluşların pazar payı kaybetmesine ve müşteriler, iş ortakları ile hissedarlar nezdinde itibar yitirmesine yol açabilir. Bu tür kayıpların telafisi, genellikle önleyici tedbirler almaktan daha pahalı bir süreç haline gelmektedir. Bilgi güvenliği, iş sürekliliğini sağlamak, kaçınılmaz kriz anlarında zararları en aza indirmek ve firmaların temel yapı taşları olan kaynakların gizliliğini, erişilebilirliğini ve bütünlüğünü her koşulda korumak gibi önemli hedefleri kapsamaktadır (Çetinkaya, 2008: 512).

1.6. Bireysel Bilgi Güvenliği

Chen ve Shi'nin (2009) çalışmasında sosyal ağlardaki kişisel bilgilerin güvenliği, çeşitli açılardan ele alınmış ve yeni saldırı teknikleri detaylandırılmıştır. Çalışmada, kişisel bilgilerin tamamen güvence altında olmadığı ve güvenliğin piyasa koşulları, bireysel önlemler ve hükümet düzenlemeleriyle sağlanmaya çalışıldığı ifade edilmiştir. Saldırılar iki ana kategoriye ayrılmıştır: doğrudan saldırılar ve kötücül yazılım saldırıları. En sık karşılaşılan saldırı yöntemleri arasında Dağıtık Hizmet Reddi (DDoS) ve oltalama (phishing) yer almaktadır. Sosyal medya platformlarında bireysel bilgilerin korunabilmesi amacıyla koruyucu temelli sosyal ağ modellerinin geliştirilmesi gerektiği önemle belirtilmiştir.

Cutillo ve arkadaşlarının (2009) araştırmasında, sosyal ağların kullanıcı güvenliği sorunları oluşturduğu ve internet ortamındaki tehditlerin sosyal ağlar için daha büyük problemler yarattığı belirtilmiştir. Sosyal ağların merkeziyetçi yapıları nedeniyle, tehditlerin tüm ağı etkilememesi için merkeziyetçi yaklaşımlar yerine noktadan noktaya çözümler önerilmiştir.

Yang ve Ng (2007) tarafından gerçekleştirilen araştırmada, web günlüklerinin terörizm ve suç amaçlı kullanım biçimleri ele alınmıştır. Web günlükleri, büyük grupların ideolojilerini açıklaması ve kitlelere ulaşması için önemli platformlar olarak değerlendirilmiştir. Çalışmada, web günlükleri için yazılım arabirimleri kullanılarak sosyal paylaşım ağlarındaki içerik analizi ve semantik bağlantılar aracılığıyla bağlantı analizi yapılması önerilmiş ve bu yöntemlerle günlük yazarları arasındaki ilişkilerin ve haberleşme güvenliğinin sağlanması hedeflenmiştir.

Buchegger ve Datta'nın (2009) çalışmasında, Facebook ve Myspace gibi merkezi sosyal medya platformlarının web tabanlı yapıları ve bu platformların sahiplerinin kişisel verilere erişim hakkının yarattığı güvenlik sorunları ele alınmıştır. Bu sorunların çözülmesi için, mevcut kullanıcı çiftleri yerine noktadan noktaya kontrol yeteneğine sahip sosyal paylaşım ağlarının oluşturulması gerektiği ifade edilmiştir.

1.6.1. Bireysel Bilgi Güvenliğinin Önemi

Kişisel bilgi güvenliği söz konusu olduğunda, genellikle bilgisayar güvenliği ön plana çıkmaktadır. Bu alandaki tehditler ise çoğunlukla kötü niyetli kişiler tarafından oluşturulmaktadır. Yani korsanlar veya saldırganlar önemli bir rol oynamaktadır. Bu tür tehditler karşısında korsanlar, bilgisayar güvenlik sistemlerini geçebilmek amacıyla çeşitli teknikler geliştirmiştir. Dolayısıyla, saldırı türlerinin doğru bir şekilde incelenmesi, bilgi güvenliği açısından büyük önem taşımaktadır (Canberk ve Sağıroğlu, 2006:168-169).

Fakat bilgisayar güvenliğini tehdit eden korsanlar ve saldırganlardan önce, bilgisayar kullanıcılarının kişisel güvenlik önlemleri alması da oldukça önemlidir. Kişisel bilgisayar güvenliği kapsamında, kullanıcıların şu önlemleri alması önerilmektedir: bilgisayar işletim sisteminin düzenli olarak güncellenmesi, anti-virüs yazılımının yüklenmesi, güvenilir olmayan internet sitelerine giriş yapılmaması, tanımadıklarından gelen e-posta eklerinin açılmaması ve bilgisayarların kullanılmadığı durumlarda kapalı tutulması (TÜBİTAK, 2009). Bu tür önlemler, kişisel bilgisayar güvenliğini artırmada etkili olabilir.

1.6.2. Kişisel Verilerin Korunması

Kişisel veri (personal data) ifadesi, bir kişiye ait verileri ifade etmektedir. Ancak, "veri" kavramının açıklığa kavuşturulması gerekir. Latince'de "datum, dati" olarak bilinen bu terim, İngilizce 'ye "debit" ve "that which is a given" şeklinde çevrilmiştir. Zamanla, İngilizce 'de "datum" ve "data" terimleri kullanılmaya başlanmıştır. Kelime anlamı açısından "datum", "bilginin bir unsuru" olarak tanımlanırken, "data" ise "referans almak veya analiz yapmak amacıyla toplanmış olgular ve istatistikler" olarak tasvir edilebilir. Bu çerçevede, veri kavramı, bilgi sistemleri ve analiz süreçlerinde önemli bir rol oynamaktadır (Avcı, 2019: 4).

Kişisel veri, bireylerin kimliklerini tespit etmeye yönelik her türlü bilgiyi kapsamaktadır. Bu tanım, kişinin kimlik bilgileri, iletişim detayları, sağlık durumu, mali bilgileri, özel hayatı, dini inançları ve siyasi görüşleri gibi unsurları içermektedir. Anayasa Mahkemesi, kişisel veriyi; "Kişisel veri kavramı, belirli veya kimliği belirlenebilir olma koşuluyla, bir kişiye ait tüm bilgileri ifade etmektedir." şeklinde tanımlamaktadır (Çelik, 2017: 395). Bu tanım, kişisel verilerin korunması ve yönetimi açısından yasal çerçeveyi belirlerken, bireylerin mahremiyetinin önemini de vurgulamaktadır.

1.6.3. Bireysel Bilgi Güvenliği İçin Alınacak Temel Önlemler

Dijital veri güvenliği, maddi zarara ve yaşamsal tehlikeye yol açabilecek bir alan olarak hem bireysel hem de teknik önlemler gerektirir. Ayrıca, bu konuda yasal düzenlemeler de önemli bir rol oynamaktadır. Ancak, bu tedbirlerin başında insan unsuru gelmektedir (Yılmaz, Şahin ve Akbulut, 2016). Bireyler ve kuruluşlar genellikle ciddi sorunlarla karşılaştıklarında bilgi güvenliği tedbirlerini ele almaya başlarlar. Ancak bilgi güvenliği, süreçlerin her aşamasında kritik öneme sahiptir. Dolayısıyla, bilgi güvenliği farkındalığının artırılması (Kruger ve Kearney, 2006) ve bilgi güvenliği kültürünün (Da Veiga ve Eloff, 2010; Nasir, Arshah, Ab Hamid ve Fahmy, 2019) bilgi okuryazarlığı desteği ile geliştirilmesi son derece kritik bir konudur. Dijital çağda bu iki kavram arasındaki ilişkiyi incelemek önem arz etmektedir (Ramalho Correia ve Carlos Teixeira, 2003). Bu çerçevede, nitelikli ve etkili hizmet içi eğitim programlarına odaklanılmalıdır. Bilgi güvenliği ile ilgili hizmet içi eğitimlerin, bireylerin ihtiyaçlarına uygun ve etkileşimli bir biçimde tasarlanması gerekmektedir (Şahinaslan vd., 2009). Bu yaklaşım, bireylerin bilgi okuryazarlık seviyelerini ve dijital veri güvenliği konusundaki farkındalıklarını artırmayı hedeflemektedir. Ayrıca, verilen eğitimlerin etkinliğini değerlendirmek ve bireylerin bilgi okuryazarlıkları ile dijital veri güvenliği farkındalıkları arasındaki ilişkiyi analiz etmek sürecin çok yönlü bir şekilde değerlendirilmesine yardımcı olacaktır.

Bilgi güvenliği önlemlerinin alınmaması, temel düzeyde veri kaybına yol açar. Yanlışlıkla veya kötü niyetle ele geçirilen veriler okunamaz hale gelir ve bu durum hem kişisel hem de kurumsal anlamda erişim kaybına neden olur (Henkoğlu, 2017: 47). Bilginin üçüncü şahıslar tarafından ele geçirilmesi, veriler üzerinde birçok

değişikliğin yapılabilmesine imkân tanır. Bu noktada, ifşa, izinsiz paylaşım ve verinin yok edilmesi gibi sorunlar ortaya çıkar. Gözden kaçan hatalar nedeniyle bilgiler sızdırılabilir ve bu durum maddi ve manevi zararlara yol açabilir (Taner ve Kılıç, 2019: 254-255).

Bilgi ve veri güvenliğini sağlamak için çeşitli önlemler alınmalıdır. Bireysel tedbirler ve kişisel verilerin üçüncü taraflara ulaşmasını engelleme bu sürecin önemli parçalarıdır. Sosyal ağlarda kişisel yaşam bilgilerinizi yalnızca güvendiğiniz kullanıcılarla paylaşmalısınız. Sosyal ağlarda paylaşımlarınızı dikkatli bir şekilde yaparak, verilerinizi koruma altına alınabilir. Güçlü ve karmaşık parolalar kullanmak, mobil bankacılık ve sosyal medya gibi kişisel bilgilerinizin bulunduğu hesapları korumanın temel adımlarından biridir. Bağlantılara tıklamadan önce kaynağını ve güvenilirliğini kontrol etmek, dolandırıcılık ve kimlik avı saldırılarından korunmanıza yardımcı olur (Gündüz ve Daş, 2022: 433-434).

Wi-Fi güvenliği de önemlidir; halka açık mekânlarda Wi-Fi kullanırken bağlantının güvenliğinden emin olmak gerekmektedir. Güvenli olmayan ağlar üzerinden yapılan işlemler, veriler yetkisiz erişime yol açabilir Gizlilik ve güvenlik ayarlarını düzenli olarak kontrol etmek, kişisel verilerini korunmasına yardımcı olur Şahinaslan vd., 203). Ayrıca, işletim sistemlerini sürekli olarak güncel tutmak, güvenlik açıklarını kapatır ve sistemi korur (Gündüz ve Daş, 2022: 433-434).

Bilgi güvenliği, bireyin mahremiyetini, önemli verilerini ve kaynaklarını güvence altına almak için titizlikle ele alınması gereken bir konudur. Bu tedbirlerin alınması, dijital dünyada güvenliğinizi sağlamada büyük rol oynar.

1.7. Bilgi Güvenliği ve Politika Geliştirme İhtiyacı

Bilgi güvenliği, hem özel hem de kamu sektöründe çeşitli alanlarda güçlü politikaların geliştirilmesini zorunlu kılar. Bu alanlar şunlardır:

1.7.1. Bilgisayar ve Ağ Güvenliği

Ağların güvenliği, kötü niyetli saldırılara karşı korunmayı gerektirir. Güçlü güvenlik önlemleri, bu alandaki riskleri minimize eder.

1.7.2. Bilgi Güvenliği Yönetim Sistemi:

Kuruluşların bilgi varlıklarını korumak için sistematik bir yaklaşım geliştirmesi gerekmektedir. Bu sistem, standartlara ve en iyi uygulamalara dayalı olarak yapılandırılmalıdır.

1.7.3. Bilgi Güvenliği Yönetişimi:

Bilgi güvenliğini yöneten stratejilerin oluşturulması, tüm paydaşların rollerini ve sorumluluklarını belirleyerek etkin bir yönetişim sağlamalıdır.

1.7.4. Kriptoloji:

Verilerin güvenli bir şekilde saklanması ve iletilmesi için güçlü şifreleme yöntemlerinin uygulanması önemlidir. Kriptoloji, güvenli iletişimin temel taşlarındandır.

1.7.5. Siber Güvenlik:

Dijital tehditlere karşı koruma sağlamak için kapsamlı stratejiler geliştirilmelidir. Bu, sürekli izleme ve güncellemeyi içerir.

1.7.6. Bilişim Suçları:

Bilişim suçlarına karşı etkili yasalar ve cezai yaptırımlar oluşturulmalı, toplum bu konuda bilinçlendirilmelidir.

1.7.7. Veri Mahremiyeti ve Korunması:

Kişisel verilerin korunması, veri koruma yasaları çerçevesinde sağlanmalı ve kullanıcılar bilgilendirilmelidir.

1.7.8. Ulusal Güvenlik:

Bilgi güvenliği, ulusal güvenlik stratejileriyle entegre edilmeli ve kriz yönetimi senaryoları geliştirilmelidir.

1.7.9. Uluslararası İşbirliği:

Ülkeler arasında bilgi güvenliği alanında işbirliği, bilgi paylaşımı ve standartların oluşturulmasını teşvik etmelidir (Güngör, 2015: 13-24).

İnsan faktörü, bilgi teknolojilerinin uygulanmasında kritik bir rol oynamaktadır. Bilgi güvenliği kaygıları, çoğunlukla insan kaynaklı ihmal ve

hatalardan kaynaklandığı için, bilgi güvenliğini etkileyen temel sorunların başında insan gelir. Bireyler, bilinçli veya bilinçsiz bir şekilde, kötüye kullanım, veri çalma, izinsiz erişim ve sistemleri etkisiz hale getirme gibi riskler oluşturabilirler. Dolayısıyla, hem bilgiyi üreten hem de güvenliğini tehdit eden yine insanlardır (Güngör, 2015: 2).

İnsan faktörünün etkisi, bilgi güvenliği politikalarının oluşturulmasında hem teknik hem de sosyal ve kültürel boyutları içerir. İlk aşamada, çoğu uygulama alanı teknik ve fiziksel özelliklere odaklansa da, toplumsal ve kültürel dinamiklerin göz ardı edilmesi bilgi güvenliği stratejilerinin etkinliğini azaltabilir

1.8. Türkiye'de Bilgi Güvenliği Çalışmaları

Türkiye'de bilgi güvenliği kapsamında yürütülen yasal çalışmalar, Anayasa ve kanunlar kapsamında kişisel hak ve özgürlüklerin dışında bilişim güvenliği ve suçlarıyla ilgili hükümler çerçevesinde incelenebilir. Bu hukuki düzenlemeler arasında 1982 Anayasası başı çeker. Anayasa'nın 19. maddesi kişi hürriyetini ve güvenliğini, 20. maddesi özel hayatın gizliliğini, 22. maddesi ise haberleşme hürriyetini tanımlayarak, bilişim güvenliği ve suçları açısından kritik bir rol oynar. Anayasa'ya göre, kişisel veriler ancak kanunda belirtilen hallerde ve kişinin açık rızasıyla işlenebilir. Herkesin kişisel verilerinin korunmasını isteme hakkı vardır ve bu verilerin korunmasına yönelik esas ve usuller kanunla düzenlenir. Bu nedenle işletmeler ve kurumlar, sakladıkları kişisel verilerden sorumlu tutulurlar. Bilgi güvenliği konusunda bir diğer önemli düzenleme, 5237 Sayılı Türk Ceza Kanunu'dur. Bu kanun, geniş bir çerçevede bilişim suçlarını ele alır. Bilişim sistemine izinsiz giriş, sistemi bozma, haberleşmenin engellenmesi, kişisel verilerin izinsiz kaydedilmesi ve silinmemesi gibi suçlar bu kapsamda yer alır. Ayrıca 5809 Sayılı Elektronik Haberleşme Kanunu ile bilgi güvenliği temel ilkelerden biri olarak kabul edilmiştir. Bu kanun, haberleşme gizliliğinin korunmasını ve kurumların bu konuda sorumluluklarını belirler. 5070 Sayılı Elektronik İmza Kanunu da bilgi güvenliği ile ilgili önemli bir düzenlemedir. Elektronik imza verilerinin izinsiz kullanımı ve elektronik sertifikalarda sahtekârlık gibi bilişim suçlarını kapsar. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, internet hizmet sağlayıcıları ve içerik sağlayıcıların sorumluluklarını belirler.

Aynı zamanda 5846 Sayılı Fikri ve Sanat Eserleri Kanunu, bir eserin çoğaltılması, yayılması veya temsil hakkının eser sahibine ait olduğunu düzenler. 6698 Sayılı Kişisel Verilerin Korunması Kanunu ise kişisel veri kavramını tanımlayarak, bu verilerin işlenmesinde özel hayatın gizliliğini koruma amacı güder. Bu kanun, kişisel verilerin işlenmesine dair esasları düzenleyerek, veri işleyen gerçek ve tüzel kişilerin uyması gereken kuralları belirler. Ayrıca 6279 Sayılı Çoğaltılmış Fikir ve Sanat Eserlerini Derleme Kanunu ve İnternet Alan Adları Yönetmeliği gibi düzenlemeler de bilgi güvenliğinin farklı yönleriyle korunmasını sağlar (BilgiGüvende, 2021).

Türkiye'de bilgi güvenliğinin korunması kapsamında faaliyet gösteren çeşitli kurumlar bulunmaktadır. Bu kurumlar arasında Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) öne çıkar. Bankacılık sektöründeki düzenlemeler ve denetimler **BDDK** tarafından yürütülmektedir ve bilgi sistemleri denetimi, 5411 Sayılı Bankacılık Kanunu temelinde yürütülmektedir. Bankalarda kullanılan verilerin korunması ve bilgi güvenliğinin sağlanması adına önemli çalışmalar gerçekleştirilmiştir. Bir diğer kritik kurum ise Sermaye Piyasası Kurulu (SPK) olup, Türkiye'de sermaye piyasalarının düzenlenmesi ve denetlenmesi görevi SPK'ya aittir. Kurul, Sermaye Piyasası Kanunu'na uygun olarak kuruluşların bilgi sistemlerinin güvenliği ve denetimi konusunda gözetim ve denetim faaliyetleri yürütür. Ayrıca, bu sistemlerin bağımsız ve güvenilir bir şekilde işlemesini sağlamaya yönelik çalışmalar yapmaktadır. T.C. Maliye Bakanlığı'na bağlı İç Denetim Koordinasyon Kurulu (İDKK) da bilgi güvenliği alanında faaliyet gösteren bir diğer önemli kuruluştur. Bununla birlikte Sayıştay, Hazine Müsteşarlığı ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) gibi kurumlar da Türkiye'de bilgi güvenliğinin sağlanmasında rol oynamaktadır (Meral, 2016: 29-50).

Bu kurumların yanı sıra, Türkiye'de bilgi güvenliği alanında çeşitli mevzuatlar ve birçok çalışma da bulunmaktadır. Bu çalışmalar, ülkenin bilgi güvenliği altyapısının güçlendirilmesine katkıda bulunmaktadır.

1.9. Bilgi Güvenliğinin Tarihsel Gelişimi

Bilgi güvenliği, bilgisayarların insan hayatına girmesiyle birlikte önem kazanmış bir kavramdır; ancak bilginin toplumsal ve ekonomik bir değer olarak tarih boyunca var olduğu ve başkalarının erişiminden korunmak istendiği de bilinmektedir

Yazının keşfi, insanlara bilgiyi ve deneyimleri saklama, başkalarına iletme ve gerektiğinde yeniden kullanma imkânı sağlamıştır. Ancak bu avantaj, yalnızca yazıyı okuyabilen ve yazabilen bireyler için geçerlidir (Rosenberg, 2003). Antropolojik araştırmalar, yazının ilk kullanıldığı uygarlıkların alfabelerinin günümüzdeki sistemlerden daha karmaşık olduğunu göstermektedir. Bu durumun, eski toplumlarda okuma ve yazma öğreniminin zorlaştırılarak belirli sosyal grupların (örneğin ruhban ve yöneticiler) avantajlarını koruması amacı taşıdığı düşünülmektedir. Kanadalı iktisat tarihçisi Harold Innis'in ifadesiyle, "bilgi tekelleri" oluşturarak bilginin gücünün yalnızca belli bir sosyal grup veya zümrede tutulması sağlanmıştır (Innis, 2007).

Örneğin, Eski Mısır'da kullanılan hiyeroglif yazısı oldukça karmaşık bir sistemdir ve bu alfabenin çözülmesi 1820'lere kadar mümkün olmamıştır (Champollion, 1822). İlk uygarlıkların alfabelerinin öğrenimi zorluğu, bu karmaşık sistemlerin seçilmesinin ardındaki amacın dönemin ruhban ve bürokrasi sınıfının bilgi üzerindeki hâkimiyetini sürdürme isteğiyle bağlantılı olduğu görülmektedir. İlk çağlarda, krallar, yöneticiler, askeri liderler ve politikacılar arasındaki yazışmaların gizliliği mühürler ve özel yapıştırıcılar kullanılarak korunuyordu. Romalı lider ve general Jül Sezar'ın geliştirdiği "*Sezar Şifrelemesi Tekniği,"* bilhassa o dönemde oldukça etkili bir yöntem olmuş ve politik rakipler tarafından deşifre edilememiştir. (Kahn, 1996). Bununla birlikte, ünlü Arap bilim insanı Al-Kindi tarafından icat edilen frekans analizi tekniği sayesinde Sezar Şifrelemesi'nin çözülmesi mümkün hale gelmiştir (Singh, 1999). Ortaçağ boyunca, krallar ve elçiler arasındaki iletişimde şifreleme ve özel kilitli kutular gibi çeşitli yöntemler, bilginin güvenliğini sağlamak amacıyla geliştirilmiştir (Kahn ve P. L., 2013).

Sanayi devrimiyle beraber elektriğin keşfi, iletişim teknolojilerinin hızla gelişmesine ve yaygınlaşmasına büyük katkı sağlamıştır. Elektrik akımıyla iletilebilen sinyal, ses ve görüntü, iletişim alanında bilgi güvenliği anlayışının farklı seviyelere ulaşmasına imkân tanımıştır. (Castells, 2000). Elektrik kullanılarak icat edilen telgraf ve telsiz gibi iletişim cihazlarının ilk ortaya çıkış döneminde, bu cihazların son derece güvenli olduğu yönünde yaygın bir inanç oluşturulmaya çalışılmıştır (Hafner ve Lyon, 1996).

1903 yılında İngiltere'de, dönemin ünlü mucitlerinden Sir John Ambrose Fleming ve Nevil Maskelyne arasındaki mesleki rekabet oldukça gerilmiştir. Dönemin önde gelen mucitlerinden Guglielmo Marconi tarafından geliştirilen ve güvenli olarak nitelendirilen radyo alıcısı ve vericisinin halka açık bir gösterisi sırasında, Fleming'in gizlice sistemin güvenliğini ihlal ederek kaynağı belirsiz kaba mesajlar göndermesi, teknoloji tarihindeki ilk bilgisayar korsanlığı (hackerlik) girişimini başarılı bir şekilde gerçekleştirmiştir (Brenner, 2010).

II. Dünya Savaşı öncesinde, Almanların savaşta başarısız olmasında kritik bir rol oynayan Enigma Şifreleme Sistemi, Polonyalı kriptologlar ve matematikçiler Marian Rejewski, Henryk Zygalski ve Jerzy Różycki tarafından çözülmüştür. Enigma, Nazi Almanyası'nın iletişim güvenliği için kullandığı bir şifreleme makinesiydi ve dönemin şartlarına göre oldukça karmaşık bir algoritmaya sahipti (Kahn, 1996). Bu çözümleme, kriptoloji alanında devrim niteliğinde bir adım olarak değerlendirilmekte ve savaşın seyrini değiştirmede önemli bir rol oynadığı kabul edilmektedir (Singh, 1999).

II. Dünya Savaşı sonrasında, anaçatı bilgisayarların hayatımıza girmesi, bilgi çağının başlangıcını simgelemekte ve bilgi güvenliği kavramının tanınmasına yol açmıştır. Bu bilgisayarlar, günümüzün veri depolama ve internet üzerinden iletişim sağlama işlevlerinin ötesinde, savaş sırasında kritik öneme sahip olan şifre kırma teknolojisinin bir uzantısı olarak ortaya çıkmıştır (Ceruzzi, 2003). Bu dönemde bilgi güvenliği kavramı, özellikle ülke güvenliğiyle ilgili hassas bilgilerin bulunduğu askeri ve sivil alanlara izinsiz girişleri engellemeye yönelik şifreleme teknolojileri gibi görsel ve işitsel tekniklerden yararlanmakla sınırlıydı (Denning, 1982).

Yani, bu dönem için bilgi güvenliği, casusluk, bilgi hırsızlığı ve sabotaj gibi tehditlere karşı alınan önlemlerle tanımlanabilir. Ayrıca, askeri alanda bilgisayarların yaygınlaşması ve belgelerin depolanmasına yönelik olanakların gelişimi, bu belgelerin izinsiz erişimlerinin önlenmesi gibi modern bilgi güvenliği kavramına doğru bir yakınsama sürecini başlatmıştır (Pfleeger ve Pfleeger, 2007).

ABD tarafından geliştirilen İleri Araştırma Projeleri Kurumu (ARPA), nükleer saldırılar karşısında askeri iletişimin sürekliliğini sağlamak amacıyla bir projeyi hayata

geçirmiştir. Bu proje çerçevesinde oluşturulan İleri Araştırma Projeleri Ağı (ARPANET), 1968 yılının ortalarında, günümüz internetinin temel taşlarını atmıştır (Leiner et al., 1997). Başlangıçta ARPANET'in son derece güvenli olduğu yönünde bir konsensüs bulunmaktaydı; ancak bu siber ortamın güvenlik açılarından bazı mantıksal ve süreçsel riskler taşıdığı kısa süre içinde fark edilmiştir (Kahn, 1996).

Bu güvenlik riskleri ve alınması gereken önlemler hakkında kapsamlı bir rapor hazırlanmıştır. "RAND Report R-609-1" adlı bu rapor, bilişim sistemlerinin birbirinden izole durumda görünürken güvenli olduğunu, fakat sistemlerin terminaller aracılığıyla entegre hale geldiğinde öngörülemeyen bilgi güvenliği risklerinin ortaya çıkabileceğini ilk kez net bir şekilde ifade etmiştir (Hafner ve Lyon, 1996). İnternetin ilk hali olarak bilinen ARPANET projesinin, sistemlerin entegrasyonunun bilgi güvenliği açısından bazı riskleri beraberinde getireceği düşüncesinin yaklaşık 45 yıl önce dile getirilmesi, günümüzdeki bilgi güvenliği kavramının kapsamını anlamada büyük bir öneme sahiptir.

1990 yılında Tim Berners-Lee'nin liderliğinde, CERN (Avrupa Nükleer Araştırma Merkezi'ndeki) bir grup bilim insanı tarafından hayata geçirilen Dünya Çapında Ağ (World Wide Web - WWW) projesi, ünlü İngiliz bilimkurgu yazarı Sir Arthur C. Clarke'ın 1970'lerde tasvir ettiği küresel iletişim ağının gerçek olması anlamına gelmiştir (Clarke, 1974). Bu küresel ağ sayesinde, dünyanın dört bir yanındaki kişisel bilgisayarlar ve bilgi sistemleri arasındaki iletişim mümkün hale gelmiş ve böylece internet adı verilen yapı ortaya çıkmıştır (Berners-Lee, 1999). Bu gelişim, bilgi paylaşımının ve iletişimin sınırlarını ortadan kaldırarak, insanlık tarihinde önemli bir dönüm noktası oluşturmuştur.

İnternetin ticarileşmesi ve sivil kullanıma açılmasıyla beraber, küresel bilgi akışı hızla artmıştır. Bu durum, bilginin ekonomik ve sosyal fayda sağlama maksadıyla kullanılmasını kolaylaştırmış olsa bile, aynı zamanda bilgi sistemleri ve altyapılarına dair güvenlik risklerinin ve tehditlerin hem nitelik hem de nicelik açısından artmasına yol açmıştır (OECD, 1992). İlk dönemlerde ülkeler, bu tür tehditler karşısında genellikle saldırı sonrası cezai yaptırımlar uygulamaya odaklanmış; önleyici veya zarar azaltıcı stratejilere yeterince önem vermemiştir. Özellikle ceza kanunlarına eklenen bilgisayar suçlarıyla saldırganları yakalamaya ve cezalandırmaya

çalışmışlardır (United Nations, 1998). Ancak bu yaklaşım, bilgi güvenliğine dair daha kapsamlı çözümler geliştirilmesini zorunlu kılmıştır.

Bu bağlamda, uluslararası kuruluşlar olan İktisadi Kalkınma ve İşbirliği Örgütü (OECD), Birleşmiş Milletler (BM) ve Kuzey Atlantik Antlaşması Örgütü (NATO) gibi yapılar, siber güvenlik alanındaki tehditlere karşı dikkat çekmiş ve bu alanda çeşitli çalışmalar başlatmışlardır (NATO, 2008). Özellikle OECD tarafından hazırlanan Bilgi Sistemleri Güvenliği Rehber Dokümanı, ülkelerin bilişim suçları ile mücadele edebilmesi için hukuki altyapılarını güçlendirmeleri ve evrensel standartlar oluşturmaları gerektiğini vurgulamaktadır (OECD, 1992).

2000 yılından itibaren internet, bilgi sistemleri ve bilgisayar ağlarının birbirleriyle ve kullanıcılarıyla sürekli bir etkileşim içinde olmasına olanak tanımıştır. Bu gelişme, ağlar arası bağlantıları ve veri alışverişini daha hızlı ve verimli hale getirmiştir. Dolayısıyla süreç sonucunda internet, büyük bir siber alan haline geldi (Anderson, 2001). İnternet teknolojileri, insan yaşamını her yönüyle kolaylaştıran birçok fırsat sunarken, aynı zamanda saldırganlar için de hedeflerine ulaşmalarında uygun bir ortam oluşturmuştur (Schneier, 2000). Bu durum, internet üzerinden gerçekleştirilen siber saldırılarda büyük bir artışa neden olmuştur. Bilgi güvenliği kavramının, ulusal güvenlik ve kamu düzeni ile olan ilişkisi daha belirgin hale gelmiştir. Ulusal bilgi güvenliği, yalnızca bağımsız çalışan bilgi sistemlerinin güvenliğinden, etkileşim halindeki ve birbirine bağımlı sistemlerin güvenliğine kadar genişlemiştir (Sweeney, 2000). Bu kavramsal değişim, ulusal bilgi güvenliği stratejilerine de derin etkiler yapmıştır.

2. SİBER GÜVENLİK

2.1. Siber Güvenliğin Tanımı

Siber güvenlik, bilgi güvenliğinin bir alt bileşeni olan ağ ve bilgisayar güvenliğinin, internetin yaygınlaşması ve gelişmesiyle birlikte dönüşerek yeni bir kavramsal çerçeveye oturmuş halidir. Her ne kadar siber güvenlik, bilgi güvenliğinin bir alt dalı olarak kabul edilse de, son dönemdeki ulusal strateji belgelerinde, siber güvenlik kavramının bilgi güvenliğinin yerine de kullanılmaya başlandığı görülmektedir. Siber güvenlik, ağlar ve bilişim sistemlerine yönelik siber saldırıların önlenmesi ve siber suçlarla mücadelenin odak noktasını oluşturur. Bilgi güvenliği ise daha geniş bir perspektife sahiptir ve bir ülkenin bilgi varlıklarını, önemli altyapılarını, bilgi ve iletişim teknolojileri altyapısını, işletmelerin ve vatandaşların güvenliğini kapsar. Bu bağlamda, bilgi güvenliği hem teknik hem de sosyo-kültürel bir kavram olarak ele alınır. Ulusal bilgi güvenliği, dijitalleştirilmiş her türlü bilginin korunmasını ve güvenliğinin sağlanmasını hedefler (Güngör, 2015: 19).

Siber güvenlik, siber alanı meydana getiren bilgi teknolojilerinin saldırılardan korunması, bu ortamda işlenen verinin gizliliğinin, bütünlüğünün ve erişilebilirliğinin koruyarak güvenliğinin sağlanması, saldırıların ve siber güvenlik hadiselerinin saptanması, bu tür olaylara karşı reaksiyon gösteren sistemin faaliyete geçirme ve sonrasında önceki haline geri döndürme durumunu yansıtmaktadır (BTK, 2016a).

Gelişen teknolojiyle birlikte, bilgisayar kullanımının yaygınlaşması, internetin günlük hayatımızın bir parçası haline gelmesi ve dijital hizmetlerin öneminin artması gibi faktörler, yönetim ve hizmet anlayışının dijital ortama adapte olmasını sağlamıştır. Bu durum, günlük yaşamın elektronik platformlara taşınması gibi etkileri de beraberinde getirmiştir. Tüm bu olgular, siber uzayı oluşturan ve fiziksel uzaylardan ayrılan sanal bir ortamda gerçekleşmektedir. Bu dijital ortam, kara, deniz, hava ve uzay gibi fiziksel uzaylardan ayrılan bir olgu olan siber uzayı temsil eder. İlerleyen teknoloji ve dijitalleşme ile birlikte, siber uzay, insanların etkileşim kurduğu, bilgi alışverişi yaptığı, ticaretin gerçekleştiği bir platform haline gelmiştir. Bu ortamda, iletişim, ticaret, eğlence, bilgi alışverişi gibi birçok faaliyet dijital olarak gerçekleşmektedir.

Dolayısıyla, siber uzay, geleneksel fiziksel alanlardan farklı bir şekilde organize edilen ve yönetilen sanal bir ortamı ifade eder (Aldemir ve Kaya, 2020: 12).

Siber güvenlik" terimi, bilgisayar sistemlerini, ağları ve diğer dijital varlıkları korumak için alınan tedbirleri ifade eden bir terim olarak 1990'lı yılların başlarında yaygın olarak kullanılmaya başlanmıştır. Bu terim, bilgisayar korsanlığı, kötü amaçlı yazılımlar ve diğer dijital tehditlere karşı korunma amacıyla ortaya çıkmıştır. Özellikle 1990'lı yıllarda internet kullanımının yaygınlaşmasıyla birlikte, bilgisayar sistemleri ve ağlar arasında veri iletimi artmış ve bu da siber tehditleri beraberinde getirmiştir. Bu dönemde, siber saldırıların önlenmesi ve bilgisayar güvenliğinin sağlanması için alınan önlemleri ifade etmek amacıyla "siber güvenlik" terimi sıkça kullanılmaya başlanmıştır. Bu süreçte, siber güvenlik alanındaki bilgi ve teknolojilerin gelişmesiyle birlikte, terim zaman içinde daha geniş bir kapsama sahip hale gelmiş ve sadece bireysel bilgisayar sistemleri değil, aynı zamanda büyük ölçekli kurumsal ağlar, endüstriyel kontrol sistemleri ve ulusal güvenliği kapsayan bir alan haline gelmiştir (Aslay, 2017: 25).

Siber tehditler, yalnızca bilgisayar sistemlerine zarar verme potansiyeli olarak değerlendirilmemektedir. Günümüzde bu tehditler, ülkelerin kritik iletişim ağlarına, enerji ve ulaşım sistemlerine, hatta askeri komuta sistemlerine bile zarar verebilecek boyutlarda asimetrik savaş şekilleri olarak ortaya çıkmaktadır. Tüm dünya, siber tehditleri önemli bir tehlike olarak kabul etmektedir. Bu nedenle, etkili savunma sistemlerinin oluşturulması ve acil durumlar için hazırlıkların yapılması büyük bir önem taşımaktadır (Aytekin, 2015).

Bilişim sistemlerinin siber ortamda, saldırı ve tehditlere karşı korumak, bilgi gizliliğini sağlamak, bu ortamda oluşacak tehdit ve saldırıların mahiyetini ve nerden geldiklerini saptamak gereklidir. Bu kapsamda yapılacak olan önlemler ve hamleler geliştirmek maksadıyla oluşturulan Ulusal Hukuk, Uluslararası Hukuk Ve İnsan Haklarına Uygun Tüm Müdahale Ve Önlem Ve Sistemler, Siber Güvenlik Olarak Nitelendirilmektedir (Atakan, 2021: 30-31).

2.2. Siber Güvenliğin Önemi

21. yüzyılda toplumların bilgisayarları ve bilgi çağını hızla benimsediği gözlemlenmiştir. Günümüzde, arabalardan trafik ışıklarına, su ve enerji altyapısına kadar pek çok alanda bilgisayarlar aktif bir şekilde kullanılmaktadır. Toplum, bu bilgisayar sistemlerinin sağladığı verimlilik artışından memnuniyet duymaktadır; ancak bu memnuniyet, sistemlerin güvenliği ve kesintisiz çalışması ile doğrudan ilişkilidir. Bilgisayar sistemlerinin nasıl işlemesi gerektiği ile gerçek işleyişi arasındaki farklılıkların bilgisayar korsanları tarafından tespit edilmesi, milyarlarca dolarlık siber suçların meydana gelmesine yol açmıştır (Tarter, 2017: 213). Bu durum, sistem zafiyetlerini istismar eden kötü niyetli faaliyetlerin artmasına ve siber güvenlik tehditlerinin çeşitlenmesine neden olmaktadır.

Dijital teknolojilerin yaygınlaşmasıyla birlikte, alışverişten sosyal etkileşimlere, iş dünyasından çeşitli sektörlere kadar toplumsal yaşamın birçok boyutu çevrimiçi bir hale gelmiştir. (Lallie vd., 2021: 1). Siber tehditler, sadece bilgisayar sistemlerine zarar vermekle kalmayıp, aynı zamanda bir ülkenin ulusal çıkarları açısından kritik olan haberleşme sistemleri, enerji ve ulaşım ağları ile askeri sistemler gibi önemli altyapılara da zarar verebilecek asimetrik savaş yöntemleri olarak değerlendirilmektedir. Bu nedenle, siber tehditler dünya çapında büyük bir tehdit unsuru olarak kabul edilmeye başlanmıştır (Aytekin, 2015: 19).

Geçmiş yıllara oranla dünya, teknolojiye daha fazla bağımlı hale gelmiş ve bu durum dijital verilerin üretiminde büyük bir artışa yol açmıştır. Oluşturulan bu veriler, şirketler, devlet kuruluşları, bireyler gibi çeşitli aktörler tarafından bilgisayarlar aracılığıyla depolanmakta ve günlük olarak bir ağ üzerinden diğer bilgisayarlara aktarılmaktadır. Ancak, bilgisayarlar ve bağlantılı sistemlerde güvenlik açıkları bulunabilmekte, bu da saldırganlar tarafından istismar edilerek oluşturulan yapının çökmesine neden olabilmektedir. Bu nedenle, siber güvenlik kritik bir öneme sahiptir.

2010 yılı haziranında ortaya çıkan bir bilgisayar solucanı, yayılma şekli ve siyasi kullanım tarzıyla dikkat çekmiştir. Bu solucan, Microsoft'un Windows tabanlı işletim sistemi vasıtasıyla yayılarak Siemens'in S7 300 modüllerini hedef almıştır. Supervisory Control and Data Acquisition Systems (SCADA) yazılımı, Simatic WinCC SCADA kodu ile çalışmaktadır (Başeskioğlu, 2021).

2.3. Siber Güvenliğin Amaçları

2.3.1. Dijital Varlıkları Koruma

Dijital varlıklar, kişisel bilgilerden ticari sırlar ve fikri mülkiyete kadar geniş bir yelpazeyi kapsar. Bu varlıkların korunması, yetkisiz erişim ve veri hırsızlığına karşı önlemler almayı içerir (Berqnet, n.d.).

2.3.2. Ağ ve Sistem Güvenliğini Sağlama

Ağ ve sistem güvenliği, bilgisayar ağlarının ve sistemlerinin güvenliğini sağlamayı amaçlar. Bu, güvenlik duvarları, antivirüs yazılımları ve izinsiz giriş tespit sistemleri gibi araçlarla sağlanır (AWS, n.d.).

2.3.3. Veri Gizliliğini ve Bütünlüğünü Koruma

Veri gizliliği, bilgilerin yetkisiz kişiler tarafından erişilmesini önlemeyi amaçlar. Veri bütünlüğü ise bilgilerin doğruluğunu ve tutarlılığını korumayı hedefler. Bu, verilerin yetkisiz değişikliklere karşı korunmasını sağlar (IHS Teknoloji, n.d.).

2.3.4. Saldırılara Karşı Proaktif Önlemler Alma

Siber saldırılara karşı proaktif önlemler almak, potansiyel tehditleri önceden tespit etmek ve bunlara karşı savunma mekanizmaları geliştirmek anlamına gelir. Bu, düzenli güvenlik taramaları, güncellemeler ve eğitim programları ile sağlanır (Berqnet, n.d.; AWS, n.d.; IHS Teknoloji, n.d.)

2.4. Siber Tehdit Türleri

2.4.1. Zararlı Yazılımlar(Malware)

Bilgisayar ve internet kullanımının artışı, bu sistemlere yönelik siber saldırıların sayısında önemli bir artışa yol açmıştır. Geçmişte daha basit hedeflere yönelik gerçekleştirilen saldırılar, günümüzde geniş çaplı ve küresel ölçekli hedef odaklı saldırılara dönüşmüştür. Bu tür saldırıların büyük bir kısmı, zararlı yazılımlar (ZY) aracılığıyla yapılmaktadır. Kötü amaçlı yazılım olarak bilinen bu yazılımlar, sistem ve uygulama yazılımlarındaki güvenlik açıklarını ve zafiyetleri (örneğin, arabellek taşması, yetersiz veri girişi kontrolü, hassas verilerin şifrelenmemesi gibi) kullanarak saldırılar gerçekleştirmektedir. Bu durum, siber güvenlik önlemlerinin

güçlendirilmesi ve sistemlerin daha dayanıklı hale getirilmesi ihtiyacını gündeme getirmektedir (Aslan vd. 2020).

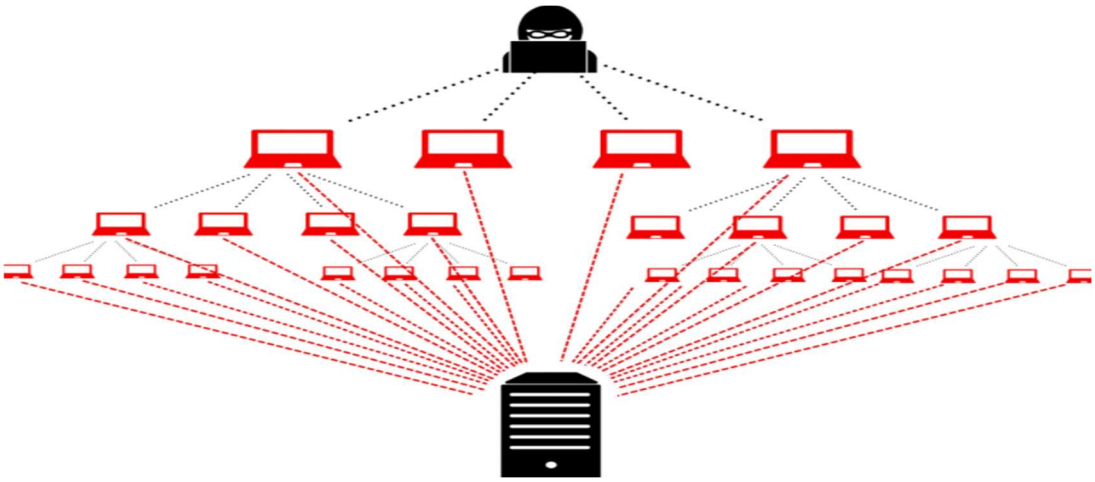
2.4.2. Sosyal Mühendislik Saldırıları

Sosyal mühendislik saldırıları, saldırganların insanların doğal eğilimlerini, güvenini kazanma yeteneklerini ve duygusal tepkilerini manipüle ederek bilgi elde etme veya kötü niyetli eylemlerde bulunma amacı taşıyan siber saldırı türleridir. Bu saldırılar genellikle teknik güvenlik önlemlerini aşmak için insan faktörünü hedef alır (Çakır ve Uzun, 2021: 361).

2.4.3. Dağıtık Hizmet Reddi(DDoS) Saldırıları

İnternete bağlı bir cihazın kaynaklarını tüketerek geçici veya süresiz olarak devre dışı bırakma saldırı türüdür (Çakır ve Uzun, 2021: 361).

DDoS saldırısı, çok sayıda bilgisayarın eşgüdüm içinde kullanıldığı bir saldırı biçimidir. Bu tür bir saldırıda, saldırgan birçok bilgisayarın kaynaklarını gizlice devreye sokarak hedefe aşırı bir yük bindirir. Eğer istemci/sunucu teknolojisi kullanılıyorsa, saldırının etkisi daha da güçlenebilir. DDoS saldırıları, saldırıyı başlatan gerçek saldırgan, zombi bilgisayarları kontrol eden güvenliği ihlal edilmiş ana bilgisayarlar, zombi bilgisayarlar ve saldırının hedefi olan bilgisayar olmak üzere dört ana bileşenden oluşur (Kara, Zengin ve Hızal, 20223: 191).



Şekil 2 Ddos Saldırısı

Kaynak: https://www.siberiletisim.com.tr/ddos-saldirisi-nedir/

2.4.4. İleri Seviye Kalıcı Tehditler(APT)

Gelişmiş kalıcı tehditler, genellikle sistemlere çeşitli yollarla (örneğin, oltalama saldırıları ve USB bağlantıları aracılığıyla) sızarak, sistem içinde kendilerini gizleyerek kalmayı hedeflerler. Bu tehditler, ya belirli bir zamanda sistemi devre dışı bırakmak ya da bilgi sızdırmak (casusluk faaliyetleri) amacıyla sistemde uzun süre kalırlar. Bu tür saldırılar, normal işleyen yazılımlar üzerinden kendilerini kamufle ederek varlıklarını sürdürmeye çalışır. Bu durumun önüne geçmek için, Güvenlik Bilgisi ve Olay Yönetimi (SIEM) sistemleri, İndikatörler ve APT (Gelişmiş Sürekli Tehdit) taramaları gibi yöntemlerin uygulanması önem arz etmektedir (Gençoğlu, 2021: 475). Bu önlemler, tehditlerin tespit edilmesi ve sistemin güvenliğinin sağlanması açısından kritik rol oynamaktadır.

APT'ler çeşitli motivasyonlarla gerçekleştirilen siber saldırılardır. Bu motivasyonlar genellikle dört ana kategoriye ayrılır: aktivizm, siber suç, şirket casusluğu ve siyasi/askeri casusluk. APT'ler, genellikle ileri düzey teknolojiler ve geniş finansal kaynaklar kullanarak uzun vadeli hedeflere odaklanır ve bazen bu süreç yıllar sürebilir. Saldırganlar, tek bir yöntem yerine birden fazla teknik ve strateji kullanarak hedef sistemlere sızmayı amaçlar. Bu saldırılar genellikle hızlı veri çalmak yerine, hedef sistemde uzun süre fark edilmeden kalarak değerli bilgileri toplama amacını güder. Saldırganlar, standart saldırı araçlarının yanı sıra insan hatalarından da faydalanarak sistemlere erişim sağlar. APT'ler, genellikle devletler veya devlet destekli gruplar tarafından finanse edilir ve yürütülür, çünkü bu tür saldırılar ciddi bir zaman ve mali kaynak gerektirir. (Andress ve Winterfeld, 2014: 175).

2.4.5. Ransomware (Fidye Yazılımı)

Fidye terimi, günümüz dünyasında yeni bir kavram değildir. Tarih boyunca, eski Roma döneminden korsanlık faaliyetlerine ve günümüzdeki rehine alma olaylarına kadar saldırganlar tarafından yaygın bir şekilde kullanılmıştır. Günümüzde ise bu taktik, siber ortamda uygulanmaya başlanmıştır. Saldırganlar, sistemleri korumak için keşfedilen şifreleme teknolojilerinden faydalanarak, kendileri için kazanç elde etmek amacıyla fidye yazılım saldırılarını etkili ve kolay bir şekilde gerçekleştirebilmektedir. Bu tehditkar yazılımlar, reklamlar, bilgilendirme e-postaları ve sosyal mühendislik saldırıları gibi çeşitli yollarla kullanıcıların bilgisayarlarına

kolayca sızabilmektedir. Ransomware bulaştıkları sistemlerdeki dosyaları çözülmesi güç şifreleme algoritmalarıyla şifreleyerek özel anahtarlar oluşturmakta ve bu anahtarlar ayrı bir sunucuda güvenli bir şekilde saklanmaktadır (Luo, X. , Liao, Q., 2007: 197).

Kullanıcının tüm dosya ve sistemini şifreleyerek şifre çözme anahtarı için para talep edilen saldırı türüdür. Ransomware, bilgisayar sistemlerini veya dosyaları şifreleyen ve ardından mağdurdan fidye isteyen kötü amaçlı yazılımlardır. Bu tür yazılımlar, bir sistem veya dosya üzerinde kontrol sağlar, ardından mağdurdan belirli bir miktar para veya kripto para birimi talep ederler. Eğer fidye ödenmezse, şifrelenen verilere erişim engellenmiş olur (O'Kane-Sezer ve Carlin: 2018).

2010 yılından itibaren fidye yazılımlar, siber ortamda saldırganlar için önemli bir kazanç kapısı haline gelmiş ve zararlı fidye yazılım türlerinin sayısı her geçen gün artmıştır. Birçok anti-virüs firmasının raporlarına göre, fidye yazılımlarının 2017 yılı sonunda önceki yıllara göre üç kat daha fazla arttığı belirtilmektedir. Son dönemlerdeki saldırıların "vektörleri ve motivasyonları" göz önünde tutulduğunda, fidye yazılım saldırılarında kullanılan teknolojiler ve araçlar oldukça ileri bir seviyeye ulaşmış, saldırıların yoğunluğu ve büyüklüğü artmıştır. Saldırıların hedefleri arasında stratejik öneme sahip kamu kurumları, çeşitli altyapı sistemleri, hastaneler, üniversiteler ve büyük ölçekli işletmeler yer almaktadır. (Crowe, 2017: 2).

2.5. Siber Tehdit Yöntemleri

Siber tehditler ve saldırı türleri, gün geçtikçe evrim geçirir. Hackerler, dijital verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini manipüle etmek için çeşitli işlemler gerçekleştirirler. Bazı yaygın siber tehditler ve saldırı türleri;

2.5.1. Phishing (Kimlik Avı, Oltalama)

E-posta yoluyla kullanıcıyı sahte bilgilerle ikna edip hassas bilgilerini, finansal bilgileri almayı hedefleyen saldırı türüdür. Bu yolla ülkeden ülkeye zararlı yazılımlar yayılabilmektedir (Öğün ve Kaya, 2013: 152).

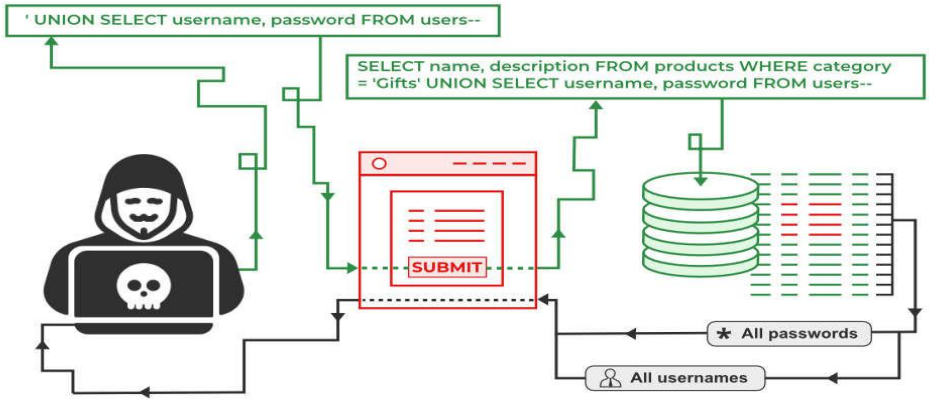
Chen ve Walsh, (2009) Phishing'i, genellikle sosyal mühendislik saldırıları kategorisine girer. Sosyal mühendislik, hedef sistemlere erişim sağlamak amacıyla

insanın zayıflıklarından (güven duygusu, acelecilik, merak, korku gibi) yararlanarak yapılan bir saldırı türü olarak tanımlamaktadır.

Oltalama saldırılarında, Saldırganlar e-posta yoluyla kandırmak için çeşitli inandırıcı senaryolar kullanılır. Bu e-postalar, kullanıcıların gerçek mesajlarından ayıramayacakları kadar hazırlanmıştır. Kullanıcılar bu e-postalara yanıt vererek, kişisel bilgileri toplayarak veya diğer hassas şekilde şifreleyerek saldırganlara iletebilirler. İçerikler genellikle basit ve düşük takviyeli olarak hazırlanır, bu da onları geniş bir kitleye hızlı bir şekilde ulaştırmayı mümkün kılar. Saldırganlar sürekli olarak yeni senaryolar ve teknikler geliştirerek bu tür saldırıları daha etkili hale getirir. Bu durum, oltalama saldırılarının tespit edilmesi ve korunmasını son derece zorlaştırır(Özker, 2021: 7).

2.5.2. SQL Injection

Bir veri tabanındaki zafiyetleri zararlı SQL kod enjekte ederek istismar eder ve bir web uygulamasına gönderilen kullanıcı tarafından sağlanan verilerin, kötü niyetli SQL sorgularının enjekte edilmesi yoluyla manipüle edilmesine dayanan bir siber güvenlik saldırı türüdür. Bu tür saldırılar, web uygulamalarının güvensiz bir şekilde kullanıcı girdilerini işlemesi veya doğrulamaması durumunda gerçekleşebilir. SQL Injection saldırıları, saldırganlara veritabanına yetkisiz erişim sağlama, veri çalma veya değiştirme, hatta sistem üzerinde kontrol elde etme imkânı tanır (Polat ve Bülbül, 2023: 18).



Şekil 3 SQL injection Saldırısı

Kaynak: https://www.caniasforum.com/2024/02/09/2024-te-en-cok-gorulecek-siber-saldirilar/

2.5.3. Man-in-the-Middle (MitM) Saldırıları

İletişimde olan iki kaynağın iletişim bilgileri olmadan kesip ve manipüle edilmesi sonucu yetkisiz erişim veya veri hırsızlığına yol açan saldırı türüdür. Bu tür bir saldırının temel amacı, hedef sistem üzerindeki kaynakları kullanılamaz hale getirerek, kullanıcılara normal hizmet sağlanmasını engellemektir (Masum, 2017: 5).



Şekil 4 MITM Saldırısı

Kaynak: https://mehmetozgul.com/assets/img/blog/

2.5.4. Zero-Day Saldırıları(Sıfırıncı Gün Saldırıları)

Sistemlerdeki tasarım hataları, yanlış yapılandırmalar veya kodlama hataları, üretici tarafından değil de saldırganlar tarafından fark edilip kötüye kullanıldığında, gizlilik, bütünlük ve erişilebilirlik gibi kritik güvenlik alanlarına zarar verme riski doğar. Sıfırıncı gün saldırıları, yazılımda bulunan bir güvenlik açığının ilk kez keşfedildiği andan itibaren başlar. Yazılım geliştiricileri, bu tür açıklar tespit edildiğinde, güvenlik yamaları hazırlayarak kullanıcıların sistemlerini güncellemelerini önerirler. Ancak, saldırganlar bu güvenlik açıklarını belirlemeye ve bunları kullanarak hedef sistemlere sızmaya çalışır (Kara, 2019: 64).

2.5.5. Cross-Site Scripting (XSS)

Web sitesine kötü amaçlı kod ekleyerek siteye giren kullanıcıların bilgilerini çalmayı hedefleyen saldırıdır (Mustafa ve Kılıçaslan, 221: 3147).

OWASP'a (Açık Web Uygulama Güvenliği Projesi) göre, Cross-Site Scripting (XSS) en sık rastlanan saldırı türlerinden biridir (Wibowo ve Sulaksono, 2021)

Son dönemlerde, zayıf şekilde geliştirilen yazılım programları, güvenlik tehditleri olarak kabul edilmektedir. Bir sistemin karşı karşıya kalabileceği virüslerin sayısı, ağ altyapısının ve sunucu yapısının karmaşıklığıyla doğrudan bağlantılıdır. Birçok gelişmiş uygulama, ciddi güvenlik açıklarına ve bilinen birkaç zayıf noktaya sahiptir. Ayrıca, ağ sunucuları genellikle karmaşık yapıda olup çok yönlü uygulamalar olarak görülür. Web siteleri de bu anlamda oldukça karmaşık sistemlerdir ve çoğu zaman kullanıcılarından ek bilgi talep ederler. Siteler arası betik çalıştırma (XSS), günümüzde en tehlikeli ve en çok suiistimal edilen saldırı türlerinden biridir. Web sitelerinin yaklaşık %65'inde XSS güvenlik açıklarından bir veya birkaçının bulunduğu tespit edilmiştir (Alsaffar vd., 2022).

2.6. Siber Saldırılardan Korunma Yöntemleri

Siber saldırılardan korunma, bireylerin, kurumların ve devletlerin siber güvenlik önlemleri alarak, bilgi sistemlerini, ağlarını ve dijital varlıklarını güvende tutma çabalarını içerir. Siber güvenlik önlemleri doğrultusunda, ihtiyaç duyulan verilere ulaşmak bütün organizasyonlar gerekli ve elzemdir. Bu veriler, talep edilen ve gerekli olan siber güvenlik yatırımlarını gerçekleştirebilecek finansal kaynaklar olabileceği gibi, siber güvenlik projelerine tahsis edilebilecek ek kaynak kapasitesine sahip olmayı ve siber güvenlik uzmanlığına da sahip olmayı içerebilir (Türkmen, 2022: 108).

1. Güçlü Şifreler Kullanma: Güçlü, karmaşık ve benzersiz şifreler kullanmak, şifreleri düzenli aralıklarla değiştirmek ve çift faktörlü kimlik doğrulama kullanmak, siber güvenlik önlemleri arasında önemlidir (Yılmaz, 2021: 75).
2. Güvenlik Yazılımları Kullanma: Antivirüs, antispyware ve güvenlik duvarı gibi güvenlik yazılımlarını güncel tutmak ve yazılımları düzenli olarak güncelleyerek otomatik güncelleme seçeneklerini etkinleştirmek, sistem güvenliğini sağlamak için gereklidir (Öztürk ve Koca, 2020: 115).

3. Eğitim ve Bilinçlendirme: Personeli ve kullanıcıları siber güvenlik konularında eğitmek ve bilinçlendirmek, fidye yazılımları ve phishing gibi siber tehditlere karşı farkındalık oluşturmak açısından kritik öneme sahiptir (Kaya, 2021: 47)
4. Güvenlik Politikaları Oluşturmak: Kurum içinde güvenlik politikaları ve prosedürleri belirlemek ve çalışanlara bu politikalar doğrultusunda eğitim vermek, güvenlik standartlarını korumak için gereklidir (Yılmaz, 2021: 75).
5. Güvenlik Duvarları ve Ağ Güvenliği: Güvenlik duvarları ve ağ güvenliği önlemleri ile ağı korumak, güvenilir VPN (Sanal Özel Ağ) kullanarak güvenli iletişim sağlamak, siber saldırılara karşı savunmayı güçlendirir (Çelik, 2022: 125).
6. Veri Yedekleme: Önemli verileri düzenli olarak yedeklemek ve yedekleri güvenli bir yerde saklamak, fidye yazılımları gibi saldırılara karşı etkili bir savunma stratejisidir (Çelik, 2022: 123).
7. Güncel Yazılımları Kullanma: İşletim sistemleri, uygulama yazılımları ve diğer yazılımları düzenli olarak güncellemek ve güvenlik yamalarını zamanında uygulamak, siber güvenlik açıklarını kapatmak için kritik öneme sahiptir (Öztürk ve Koca, 2020: 117).
8. Personel İzin ve Erişim Kontrolleri: Çalışanların erişim haklarını belirlemek ve sınırlamak, personelin ihtiyaç duyduğu minimum erişim seviyelerini belirlemek, bilgi güvenliğini artırır (Yılmaz, 2021: 78).
9. Fidye Ödemezden Kaçınma: Fidye yazılımlarıyla mağdur olmamak için fidye ödememe politikası benimsemek ve alternatif çözümler ile yedekleme stratejileri geliştirmek önemlidir (Aydın, 2023: 87).
10. Incident Response Planı Oluşturma: Bir siber saldırı durumunda hızlı ve etkili bir tepki verebilmek için bir incident response planı oluşturmak ve planı düzenli olarak test edip güncellemek, olay yönetimi için gereklidir (Aydın, 2023: 89).

Bu önlemler, siber saldırılara karşı korunmada yardımcı olabilir. Ancak siber güvenlik, sürekli bir çaba gerektirir ve teknolojik gelişmeler ile yeni tehditlerle başa çıkabilmek için güvenlik önlemlerinin sürekli olarak güncellenmesi önemlidir.

2.6.1. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı(2020-2023)

2018 yılında Cumhurbaşkanlığı Hükümet Sistemi'ne geçiş öncesinde, "*yürütmenin başı olan Bakanlar Kurulu'nun 11/06/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararı, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazete 'de yayımlanarak yürürlüğe girmiştir*". Bahse konu karar ile "Siber Güvenlik Kurulu" tesis edilmiştir.. Türkiye'nin siber güvenlik alanındaki vizyonunu ve misyonunu doğrultusunda ulusal siber güvenliği bir adım daha ileriye taşımak amacıyla hazırlanmıştır (Öcal ve Turan, 2021: 90). "2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" 12 bölümden oluşmaktadır. Bu strateji ve eylem planı, teknolojik gelişmelerin etkilerini, siber tehditlerdeki eğilimleri, ulusal ihtiyaçları ve uluslararası uygulamaları dikkatle inceleyerek hedefleri belirlemiştir. Bu kapsamlı planın temel hedefleri şunlardır (Çakır ve Uzun, 2021: 369-374).

1. **Siber Tehditlerin Etkilerinin Azaltılması**: Ülkeyi etkileyen siber tehditlerin etkilerini en aza indirmek için önlemler alınmalıdır.
2. **Ulusal Kapasitenin Geliştirilmesi**: Yerli ve milli siber güvenlik yeteneklerini artırmak ve güçlendirmek önemlidir.
3. **Daha Güvenli Bir Ulusal Siber Ortamın Oluşturulması**: Hem bireyler hem de kurumlar için güvenli bir siber ortam sağlanmalıdır.
4. **Ülkemizin Siber Güvenlik Alanında Uluslararası Seviyede En Üst Sıralarda Yer Alması**: Uluslararası arenada siber güvenlikte lider bir konumda olmak hedeflenmektedir (TC. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi).

2.6.2. Olay Müdahale Planları ve Prosedürleri

Siber güvenlik olay müdahale planları, bir organizasyonun siber saldırılara veya güvenlik ihlallerine karşı etkili bir şekilde yanıt vermesini sağlamak amacıyla oluşturulan stratejik belgelerdir. Bu planlar, olayın tespitinden, yanıt verilmesine,

raporlanmasına ve sonrasında yapılacak iyileştirme adımlarına kadar olan süreçleri kapsar. Olay müdahale planları ve prosedürleri, genellikle aşağıdaki aşamalardan oluşur:

1. ***Hazırlık***: Olası siber güvenlik olaylarına karşı hazırlıklı olmayı sağlar. Bu aşamada, gerekli araçlar ve kaynaklar sağlanır, ekip üyeleri eğitilir ve olay müdahale stratejileri geliştirilir (Harris, 2009: 345-370).
2. ***Tespit ve Analiz****:* Güvenlik olaylarının tanımlanması ve analiz edilmesi sürecidir. Bu aşama, olayın gerçek mi yoksa yanlış alarm mı olduğunu belirlemeyi içerir (Scarfone ve Mell, 2007: 23-65).
3. ***Yanıt ve Kurtarma****:* Olayın etkilerini en aza indirmek ve sistemleri geri yüklemek için yapılan işlemler. Bu aşamada, olayın kapsamı belirlenir ve gerekli müdahaleler yapılır (Miller ve McDonald, 2015: 58-80).
4. ***Gözden Geçirme ve İyileştirme****:* Olay sonrası süreçlerin değerlendirilmesi ve gelecekte benzer olayların önlenmesi için iyileştirme yapılmasıdır. Bu aşama, olayın nedenlerini anlamak ve süreçlerdeki eksiklikleri gidermek için önemlidir (Kossakowski, 2017: 112-145).

2.6.3. Veri Yedekleme ve Kurtarma

Veri yedekleme ve veri kurtarma, modern bilgi teknolojilerinde kritik öneme sahip süreçlerdir. Veri yedekleme, verilerin düzenli aralıklarla kopyalanmasını ve bu kopyaların güvenli bir ortamda saklanmasını ifade eder. Bu işlem, veri kaybı durumunda verilerin geri yüklenmesini sağlar ve çeşitli nedenlerle meydana gelen veri kayıplarına karşı koruma sağlar (Harris, 2009: 225-250; Yılmaz ve Demir, 2018: 130-145). Yedekleme yöntemleri arasında tam yedekleme, artımlı yedekleme, farklı yedekleme ve sürekli yedekleme bulunur. Tam yedekleme, tüm verilerin yedeklenmesini sağlar ve büyük veri setlerinde yüksek depolama gereksinimleri doğurabilir (Miller ve McDonald, 2015, 89-110; Türk, 2020, 102-115). Artımlı yedekleme, yalnızca son yedeklemeden bu yana değişen verileri kopyalar, bu da yedekleme sürecini hızlandırır ve depolama alanını verimli kullanır (Kossakowski, 2017, 78-100). Farklı yedekleme ise son tam yedeklemeden sonra değişen verileri kopyalar ve daha kapsamlı bir veri kümesi oluşturur (Scarfone ve Mell, 2007, 15-45).

Sürekli yedekleme, verileri gerçek zamanlı olarak veya belirli aralıklarla yedekler, bu da veri kaybı riskini minimize eder (CERT Division of the Software Engineering Institute, n.d. 23-55).

Veri kurtarma, veri kaybı yaşandığında verilerin geri getirilmesi sürecidir. Bu süreç, yedekleme medyasından verilerin geri yüklenmesini içerir (Scarfone ve Mell, 2007, 15-45; Yılmaz ve Demir, 2018, 130-145). Bir kurtarma planı, etkili bir veri kurtarma sürecinin temelini oluşturur ve verilerin nasıl geri yükleneceğini, kimlerin bu işlemi gerçekleştireceğini ve hangi araçların kullanılacağını belirler (Harris, 2009: 225-250; Türk, 2020, 102-115). Kurtarma süreci, yedekleme türüne ve veri kaybının boyutuna göre değişiklik gösterebilir; örneğin, tam bir yedekleme gerektiriyorsa, tüm veri seti geri yüklenir. Artımlı veya farklı yedekleme durumunda, gerekli tüm yedeklemeler sırasıyla geri yüklenir (Miller ve McDonald, 2015, 89-110). Kurtarma işlemi tamamlandıktan sonra, verilerin doğruluğunu ve bütünlüğünü kontrol etmek önemlidir. Bu aşama, verilerin beklenildiği gibi geri yüklenip yüklenmediğini doğrulamak için testler yapmayı içerir (Scarfone ve Mell, 2007, 15-45).

2.6.4. Şifreleme Teknikleri

Şifreleme teknikleri, verilerin yetkisiz erişimlerden korunmasını sağlamak için kullanılan önemli güvenlik yöntemleridir. Bu teknikler, veriyi anlaşılmaz bir biçime dönüştürerek sadece yetkili kişilerin veriyi tekrar anlaşılır hale getirebilmesini sağlar. Şifreleme teknikleri genellikle iki ana kategoriye ayrılır:

Asimetrik şifreleme ve simetrik şifreleme, şifreleme ve şifre çözme işlemleri için aynı anahtarın kullanıldığı bir yöntemdir. Bu tür şifreleme yöntemleri hızlıdır ve büyük veri setleri için uygundur. Ancak, anahtarın paylaşımı sırasında güvenlik riskleri taşır çünkü anahtarın gizliliği korunmalıdır. AES (Advanced Encryption Standard) ve DES (Data Encryption Standard), simetrik şifreleme yöntemlerinin en yaygın örneklerindendir. AES, 128-bit, 192-bit ve 256-bit anahtar uzunlukları ile çeşitli güvenlik seviyeleri sunar ve günümüzde birçok uygulamada tercih edilmektedir (Stallings, 2017, 45-55; Yılmaz, 2019: 88-95). DES ise daha eski bir standarttır ve günümüz güvenlik gereksinimlerine göre daha zayıf kabul edilmektedir (Paar ve Pelzl, 2010: 12-20).

Asimetrik şifreleme, bir veri parçasını şifrelemek ve şifresini çözmek için iki farklı anahtar kullanır: bir genel anahtar ve bir özel anahtar. Genel anahtar veriyi şifrelerken, özel anahtar ise bu veriyi çözer. Asimetrik şifreleme, anahtarların paylaşımında daha güvenlidir çünkü yalnızca özel anahtarın korunması gerekir. Bu tür şifrelemenin yaygın bir örneği RSA (Rivest-Shamir-Adleman) algoritmasıdır. RSA, büyük veri kümelerini güvenli bir şekilde şifreleyebilir ve genellikle dijital imzalar ve güvenli anahtar değişimi için kullanılır (Menezes, van Oorschot, ve Vanstone, 2015, 101-110; Yılmaz, 2019: 100-105).

Hibrid şifreleme, simetrik ve asimetrik şifreleme tekniklerinin bir araya getirilmesini içerir. Bu yöntemde, asimetrik şifreleme genellikle güvenli bir anahtar değişimi için kullanılırken, simetrik şifreleme büyük veri setlerinin şifrelenmesi için kullanılır. Bu, her iki tür şifrelemenin avantajlarını birleştirir ve performansı artırır (Stallings, 2017: 55-60). Veri şifrelemenin etkinliği, kullanılan algoritmanın ve anahtar yönetim stratejilerinin gücüne bağlıdır. Ayrıca, şifreleme anahtarlarının güvenli bir şekilde saklanması ve yönetilmesi, şifrelemenin güvenliğini sağlamada kritik bir rol oynar (Kaufman, Perlman ve Speciner, 2002: 112-130).

2.6.5. Bilgi Güvenliği Yönetim Sistemleri (BGYS)

İletişim teknolojilerinin hızla yaygınlaşması ve kullanımının artması, bilgi güvenliğine olan ihtiyacı da aynı hızla artırmıştır. Kurumsal bilgi güvenliğinin sadece teknik tedbirlerle (örneğin, güvenlik duvarları, saldırı algılama sistemleri, antivirüs yazılımları ve şifreleme gibi) tam anlamıyla korunamayacağı anlaşılmıştır. Bu yüzden, teknik çözümlerden daha fazlasına ihtiyaç duyulmuş ve insan unsuru, süreçler ve bilgi sistemlerini içeren, üst yönetimin desteğiyle oluşturulmuş bir yönetim sistemi gereksinimi ortaya çıkmıştır (Yılmaz, 2016: 51).

Bilgi Güvenliği Yönetim Sistemleri (BGYS), organizasyonların bilgi güvenliğini etkin bir şekilde yönetmelerine ve korumalarına yardımcı olan yapılandırılmış yaklaşımlardır. BGYS'ler, organizasyonların bilgi varlıklarını tehditlere ve risklere karşı korumak için oluşturulan kapsamlı bir politika, prosedür ve kontrol setidir. BGYS'nin amacı, bilgi güvenliği risklerini tanımlamak, analiz etmek, yönetmek ve minimize etmek suretiyle bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak olarak özetlenebilir.



Şekil 5 ISO 27001 Bilgi Güvenliği Yönetim Sistemi

Kaynak: KPGM BT Denetim Standartları ve Uygulamaları Araştırma Raporu.

Bilgi güvenliği kapsamında yönetim, denetim ve tetkik sistemlerinin uygulanması, bilgi güvenliği yönetim sistemlerinin ve standartlarının gelişimini hızlandırmıştır. 1990'lı yıllardan itibaren elektronik yönetim sistemlerinin yaygınlaşmasıyla ISO/IEC 17799 standartları oluşturulmuş, daha sonra bu standartlar ISO/IEC 27000 serisi olarak geliştirilmiştir. Bu serinin en bilinen standartları olan ISO/IEC 27001 ve 27002, bilgi güvenliği yönetimi için temel ilkeleri belirler. Bu standartlar, organizasyonların iş sürekliliğini güvenlik risklerine karşı korumak için rehberlik sunar ve adeta bir yapılacaklar listesi işlevi görür. Avantaj olarak, bu standartlar kuruluşlara yapılandırılmış ve güvenilir bir yaklaşım sunarak bilgi güvenliğini sistematik şekilde yönetmelerine olanak tanır. Ayrıca, bu standartların uygulanması, iş sürekliliğini sağlamak ve siber tehditlere karşı koruma sağlamak için kritik öneme sahiptir(Güngör, 2015: 15).

Öte yandan, bu standartların uygulanması zaman ve maliyet gerektirir, özellikle küçük veya orta ölçekli işletmeler için bu süreç karmaşık olabilir. Ayrıca, her organizasyonun kendi ihtiyaçlarına göre özelleştirme yapması gerektiğinden, standartların genel yapısı her zaman tüm işletmelere birebir uymayabilir

Bir BGYS genellikle aşağıdaki bileşenlerden oluşur:

1. **Politikalar ve Prosedürler**: Bilgi güvenliği politikaları, organizasyonun bilgi güvenliği hedeflerini belirler ve bu amaçlara ulaşmak için gereken prosedürleri ve kuralları içerir. Bu politikalar, güvenlik kontrol önlemlerini, risk değerlendirmelerini ve uyum gereksinimlerini kapsar (ISO/IEC 27001, 2013: 9-14; Aydın, 2020: 45-50).

2. ***Risk Yönetimi***: BGYS, bilgi güvenliği risklerini tanımlama, değerlendirme ve yönetme süreçlerini içerir. Risk yönetimi, potansiyel güvenlik tehditlerini ve zayıflıkları belirleyerek, bunlara karşı uygun güvenlik önlemlerini geliştirmeyi amaçlar (Smith, 2018: 22-28; Turgut, 2019: 63-70).
3. ***Kontroller ve Uygulama***: Bilgi güvenliğini sağlamak için çeşitli teknik ve idari kontroller uygulanır. Bu kontroller, ağ güvenliği, erişim kontrolü, veri şifreleme ve fiziksel güvenlik gibi alanları kapsar. Kontrollerin etkinliği düzenli olarak gözden geçirilir ve güncellenir (ISO/IEC 27002, 2013, 35-45; Karakaya ve Kaya, 2021: 78-85).
4. ***İzleme ve Denetleme****:* BGYS'ler, bilgi güvenliği uygulamalarının etkinliğini izlemek ve değerlendirmek için düzenli denetimler ve izleme faaliyetleri gerçekleştirir. Bu süreçler, sistemlerin ve kontrol önlemlerinin sürekli olarak gözden geçirilmesini ve iyileştirilmesini sağlar (Johnson ve Wilson, 2016: 40-50; Demir, 2021: 90-95).
5. ***Sürekli İyileştirme***: BGYS, bilgi güvenliğini sürekli olarak iyileştirmek için bir dizi süreç ve araç sağlar. Bu süreç, bilgi güvenliği olaylarından öğrenme, uygulama güncellemeleri yapma ve politika revizyonlarını içerir (ISO/IEC 27001, 2013, 51-55; Akman, 2022: 102-110).

Bilgi Güvenliği Yönetim Sistemleri, organizasyonların güvenlik standartlarına uyum sağlamalarına ve uluslararası güvenlik standartlarına göre hareket etmelerine yardımcı olur. ISO/IEC 27001, BGYS'leri kurmak ve sürdürmek için en yaygın kabul gören standartlardan biridir ve organizasyonların bilgi güvenliği yönetimini uluslararası standartlara göre yapılandırmalarına yardımcı olur (ISO/IEC 27001, 2013).

2.6.6. Güvenlik Politikalarının Oluşturulması

Güvenlik politikalarının oluşturulması, bir organizasyonun bilgi ve veri güvenliğini sağlamak için temel bir adımdır. Güvenlik politikaları, bir organizasyonun bilgi güvenliği hedeflerini belirleyen, güvenlik önlemlerini açıklayan ve bu önlemlerin nasıl uygulanacağını tanımlayan resmi belgelerdir. Bu politikalar, organizasyonun

bilgi varlıklarını koruma amaçlarını ve uygulama yöntemlerini net bir şekilde ortaya koyar.

Güvenlik politikalarının oluşturulmasında dikkate alınması gereken temel adımlar şunlardır:

1. **İhtiyaçların Belirlenmesi ve Risk Değerlendirmesi**: Güvenlik politikalarının oluşturulması süreci, organizasyonun bilgi güvenliği ihtiyaçlarını ve risklerini belirlemekle başlar. Risk değerlendirmesi, potansiyel tehditleri ve zayıflıkları tanımlamak için gerçekleştirilir. Bu aşama, güvenlik politikalarının hangi alanlara odaklanması gerektiğini ve hangi önlemlerin alınması gerektiğini belirler (ISO/IEC 27005, 2011, 10-15; Yılmaz, 2019: 40-45).
2. **Politikaların Geliştirilmesi**: Risk değerlendirmesinden elde edilen bilgiler doğrultusunda, güvenlik politikaları geliştirilir. Bu politikalar, bilgi güvenliği hedeflerini, veri koruma yöntemlerini, erişim kontrolünü ve diğer güvenlik önlemlerini kapsar. Politikalarda, organizasyonun bilgi güvenliğine yönelik yaklaşımı ve uyulması gereken kurallar net bir şekilde tanımlanmalıdır (ISO/IEC 27001, 2013, 15-20; Öztürk, 2020: 55-60).
3. **Politikaların Onaylanması ve İletilmesi**: Geliştirilen güvenlik politikalarının organizasyon içindeki ilgili paydaşlar tarafından onaylanması gereklidir. Onay süreci, genellikle üst yönetim tarafından gerçekleştirilir. Politikalardan tüm çalışanların haberdar olması ve politikaların uygulanabilirliği için gerekli eğitimlerin verilmesi sağlanır (Cohen ve Goel, 2018, 25-30; Arslan, 2021: 65-70).
4. **Uygulama ve İzleme**: Güvenlik politikaları onaylandıktan sonra, uygulanabilirliğini sağlamak için belirli prosedürler ve kontrol mekanizmaları oluşturulur. Politikalara uyumu izlemek için düzenli denetimler yapılır ve gerektiğinde güncellemeler gerçekleştirilir. İzleme ve değerlendirme, politikaların etkinliğini ve organizasyonun güvenlik hedeflerine ulaşma düzeyini değerlendirir (ISO/IEC 27002, 2013, 25-30; Demirtaş, 2022: 75-80).
5. **Sürekli İyileştirme**: Güvenlik politikalarının oluşturulması ve uygulanması bir defalık bir süreç değil, sürekli bir iyileştirme döngüsüdür. Politikalarda

ortaya çıkan eksiklikler veya değişen tehdit ortamları doğrultusunda düzenli olarak gözden geçirilir ve güncellenir. Bu süreç, bilgi güvenliğinin sürekli olarak iyileştirilmesini sağlar (Johnson ve Wilson, 2016, 40-45; Çelik, 2021, 90-95).

2.6.7. Risk Yönetimi ve Değerlendirmesi

Risk yönetimi ve değerlendirmesi, bir organizasyonun bilgi güvenliği ve Operasyonel sürekliliğini sağlamak için hayati öneme sahip bir süreçtir. Bu süreç, potansiyel risklerin belirlenmesi, analiz edilmesi ve yönetilmesi aşamalarını içerir. İlk olarak, organizasyonun karşılaşabileceği potansiyel riskler tanımlanır. Bu aşamada, iç ve dış çevredeki tehditler ve zayıflıklar detaylı bir şekilde incelenir (ISO/IEC 27005, 2011, 10-15; Demirtaş, 2022: 85-90). Riskler belirlendikten sonra, her riskin olasılığı ve potansiyel etkisi analiz edilir. Risk analizi, risklerin önem derecelerini ve organizasyon üzerindeki potansiyel etkilerini değerlendirir; bu süreçte riskler sınıflandırılarak bir risk haritası oluşturulur (Yılmaz, 2019, 50-55; Öztürk, 2020: 70-75).

Analiz aşamasından sonra, risklerin öncelikle dirilmesi yapılır. Bu aşamada, hangi risklerin daha acil ve önemli olduğu belirlenir ve bu risklere yönelik stratejiler geliştirilir. Risklerin kabul edilebilir düzeyde olup olmadığını belirlemek için risk eşiği belirlenir (Johnson ve Wilson, 2016, 50-55; Arslan, 2021: 85-90). Risk yönetim stratejileri, risklerin azaltılması, transfer edilmesi, kabul edilmesi veya tamamen ortadan kaldırılması amacıyla oluşturulur. Risk yönetim stratejileri genellikle risk azaltma, risk transferi, risk kabulü veya risk paylaşımı yöntemlerini içerir (ISO/IEC 27001, 2013, 25-30; Çelik, 2021: 95-100).

Son olarak, risklerin izlenmesi ve gözden geçirilmesi süreci gelir. Risk yönetimi, sürekli bir izleme ve gözden geçirme aşamasını içerir. Bu süreçte, risklerin yönetimi ve kontrolü belirli aralıklarla gözden geçirilir ve gerekli güncellemeler yapılır. İzleme, risk yönetim stratejilerinin etkinliğini değerlendirir ve organizasyonun risk profilindeki değişikliklere göre yeni stratejiler geliştirir (Cohen ve Goel, 2018, 45-50; Demirtaş, 2022: 95-100).

2.6.8. Kişisel Verilerin Korunması Kanunu (KVKK)

Kişisel Verilerin Korunması Kanunu (KVKK), Türkiye'de kişisel verilerin korunmasına yönelik kapsamlı düzenlemeleri belirleyen bir yasadır. Bu kanun, kişisel verilerin yasalara uygun ve etik kurallara dayanarak işlenmesini öngörürken, verilerin doğruluğunu ve güncelliğini sağlamak amacıyla belirli ilkeler belirlemektedir. (Kişisel Verilerin Korunması Kanunu, 2016, md. 4: 1-2). KVKK, kişisel verilerin sadece belirli ve meşru amaçlarla toplanmasını ve kullanılmasını öngörür, ayrıca verilerin gizliliği ve güvenliğini koruma yükümlülüğü getirir (Güven, 2020: 45). Kanun, veri sorumlusunun kişisel verilerin işlenmesinden sorumlu olan kişi olduğunu, veri işleyenin ise veri sorumlusunun talimatları doğrultusunda verileri işleyen kişi olduğunu belirtir (Yılmaz, 2018: 112). Kişisel verilerin işlenmesi için açık rıza, sözleşme, yasal yükümlülük veya haklı menfaat gibi şartlar öngörülür (Çetin, 2021: 89). Bireyler, KVKK kapsamında verilerine erişim, düzeltme, silme ve itiraz etme haklarına sahiptir (Akman, 2019: 78). Ayrıca, veri sorumluları, kişisel verilerin güvenliğini sağlamak için gerekli önlemleri almak zorundadır ve veri ihlali durumunda hem ilgili kişilere hem de Kişisel Verileri Koruma Kurumu'na (KVKK) bildirimde bulunmalıdır (Kişisel Verileri Koruma Kurumu, 2022: 25). KVKK, kişisel verilerin korunmasını denetleyen ve ihlallerde cezai yaptırımları uygulayan bir kurum olarak önemli bir rol oynar (Kara, 2023: 33). Uyum sağlamak, veri güvenliği açısından kritik bir öneme sahiptir.

2.6.9. Genel Veri Koruma Yönetmeliği (GDPR)

Genel Veri Koruma Yönetmeliği (GDPR), Avrupa Birliği'nin kişisel verilerin korunmasına yönelik getirdiği kapsamlı bir düzenlemedir ve 25 Mayıs 2018'de yürürlüğe girmiştir. GDPR, kişisel verilerin işlenmesinde hukuka uygunluk, şeffaflık, veri minimizasyonu, doğruluk, saklama süresi ve güvenlik gibi temel ilkeleri belirler (Avrupa Birliği, 2016: 1). Bireylere erişim hakkı, düzeltilme hakkı, silinme hakkı (unutulma hakkı), işleme sınırlaması hakkı, veri taşınabilirliği hakkı ve itiraz hakkı gibi çeşitli haklar tanır (Aydın, 2020: 45). GDPR, veri sorumlusunu kişisel verilerin işlenme amaçlarını belirleyen kişi olarak tanırken, veri işleyeni ise veri sorumlusunun talimatları doğrultusunda verileri işleyen kişi olarak tanımlar (Korkmaz, 2019: 78). Ayrıca, veri koruma görevlisi (DPO) atanmasını öngörür ve veri koruma etki

değerlendirmesi (DPIA) yapılmasını teşvik eder (Özkara, 2021: 89). Veri ihlali durumunda, veri sorumlusunun 72 saat içinde hem ilgili denetim otoritesine hem de etkilenen bireylere bildirimde bulunması gerekmektedir (Çelik, 2022: 33). GDPR, uyumsuzluk durumunda yüksek para cezaları öngörür ve bu cezalar, yıllık global cirosunun %4'üne kadar çıkabilir (Avrupa Birliği, 2016: 83). GDPR'nın amacı, kişisel verilerin korunmasını sağlamak ve bireylerin veriler üzerindeki kontrolünü güçlendirmektir.

2.7. Türkiye'de Siber Güvenlik

Siber güvenlik alanında dolaylı olarak pek çok yasa düzenlemesi yapılmıştır. Gelişen teknoloji ve artan bilgi güvenliği ihtiyacı, Türkiye'de bu konunun önemini artırmış ve 2003 yılında başlayan "*Dünya Bilgi Toplumu Zirvesi*" çalışmalarının titizlikle incelenmesine yol açmıştır (Şener ve Erdikmen, 2019: 130-131).

Türkiye'de siber güvenliğin geliştirilmesi amacıyla yapılan düzenlemeler, bu alandaki ilk adımlardan biri olmuştur. 5237 Sayılı Türk Ceza Kanunu'na eklenen hükümlerle elektronik ağlar üzerinden işlenen suçlar ağırlaştırıcı sebep sayılmış ve kanunun onuncu bölümünde "Kanundaki Suçlar" başlığı altında ele alınmıştır. 2004 yılında çıkarılan 5070 Sayılı Elektronik İmza Kanunu, siber güvenlik alanında önemli bir dönüm noktası olmuş ve elektronik imzanın hukuki ve teknik yönlerini düzenlemiştir (Tamyapar, 2019: 10).

1990'ların sonlarında, Milli Savunma Bakanlığı'nın koordinatörlüğünde devletin bilgi güvenliğine yönelik çalışmalar yapılmış, ancak uygulanabilir bir mutabakata varılamamıştır. 3713 Sayılı Terörle Mücadele Kanunu'nda yapılan değişiklikler ile bilişim suçları, terör amacıyla işlenen suçlar kapsamına alınarak, siber güvenliğin terörizmin faaliyet sahası olabileceği kabul edilmiştir. 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Kanunu (2007), 5809 Sayılı Elektronik Haberleşme Kanunu (2008) ve E-Devlet ve Bilgi Toplumu Kanunu Tasarısı (2009) da bu süreçteki diğer önemli yasal düzenlemeler arasındadır (Karasoy ve Babaoğlu, 2021: 5-137).

Türkiye Siber Güvenlik Kurulu ilk toplantısını 21 Aralık 2012'de gerçekleştirmiş ve "2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı"

onaylanmıştır. 2013'te faaliyete geçen Ulusal Siber Olay Müdahale Merkezi'nin kurulmasının ardından, aynı yıl Türk Silahlı Kuvvetleri bünyesinde Siber Savunma Komutanlığı da oluşturulmuştur (Erdoğan, 2023: 15).

Türkiye'de siber güvenlik alanında yapılan çalışmalara bakıldığında, Bilgisayar Olaylarına Müdahale Ekibi (TR BOME), Bilgi Toplumu Stratejisi ve Bilgisayar Acil Müdahale Merkezi gibi oluşumlar hayata geçirilmiştir (Hekim ve Başıbüyük, 2013: 140). Siber güvenlik konusundaki bir diğer önemli adım, ulusal düzeyde siber güvenlik politikalarının, stratejilerinin ve eylem planlarının oluşturulmasıdır. Bu süreçte, 28447 Sayılı Bakanlar Kurulu kararıyla, Amerika Birleşik Devletleri modeline benzer şekilde Ulaştırma ve Altyapı Bakanlığı'na (UAB) Siber Güvenlik Kurulu (SGK) sekreterlik hizmetlerinin sağlanması görevi verilmiştir. Ayrıca, siber güvenlik stratejileri geliştirmek, kamu kurumlarının altyapılarını oluşturmak ve test etmek, farkındalık artırıcı eğitimler düzenlemek gibi görevler belirlenmiştir (Erdoğan, 2023).

2013-2014 yıllarına ait "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı", UAB'nin koordinasyonunda hazırlanmış ve SGK tarafından onaylanmıştır. Ardından, 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planı ile süreç devam etmiştir. Türkiye'nin bilişim teknolojileri alanındaki kalkınmasını hedefleyen bu planlar, 2016-2019 ve 2020-2023 yılları için de hazırlanmıştır. Türkiye'de siber güvenliğe ilişkin ilk stratejik belge olan 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, bir öncü niteliği taşımaktadır.

2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, UAB tarafından hazırlanmış ve Cumhurbaşkanlığı genelgesi ile yayımlanmıştır. Bu belgede, siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu vurgulanmıştır. Planın kamuoyuna açıklanan stratejik amaçları arasında, siber tehditlere karşı hazırlıklı olmak, kamu kurumları ve altyapıları korumak ve siber farkındalık oluşturmak yer almaktadır (UAB, 2021).

3. LİTERATÜR ARAŞTIRMASI

Siber güvenlik farkındalığı, bireylerin ve kurumların dijital ortamda karşılaştıkları tehditlere karşı nasıl savunma yapabileceklerini anlamalarını sağlayan önemli bir bileşendir. Bu alandaki literatür, siber güvenliğe dair farkındalık düzeylerini ve bu farkındalığı etkileyen faktörleri inceleyen çeşitli çalışmalara dayanmaktadır. Birçok araştırma, siber güvenlik farkındalığının organizasyonların bilgi güvenliğini sağlamak adına kritik bir öneme sahip olduğunu vurgulamaktadır.

3.1. Siber Güvenlik Alanında Yapılan Önceki Çalışmalar

Kınay, Sözcü, Taşkın ve İpek (2014) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği, İstanbul'daki özel bir üniversitede öğrencilerin bilgi güvenliği farkındalık düzeylerini değerlendirmiştir. Bu ölçek, farkındalık seviyelerini "yüksek", "orta" ve "düşük" olarak sınıflandırmış ve her seviyeye uygun öneriler sunmuştur. Tayvan'da 2000-2009 yılları arasında yürütülen ve Tayvan Milli Eğitim Bakanlığı tarafından desteklenen İnternet Güvenliğinde Öğretmen Farkındalığı (TAIS) projesi ise, öğretmenlerin iletişim güvenliği, çevrimiçi kişisel güvenlik ve internet güvenliği gibi alanlardaki farkındalıklarını artırmayı amaçlamıştır. Üç aşamada planlanan proje, başlangıçta bilgisayar öğretmenleriyle başlamış, daha sonra tüm ilk ve ortaokul öğretmenlerine genişletilmiştir; ancak son aşamada veliler, lise öğrencileri, lise öğretmenleri ve öğretmen adaylarına ulaşılamamıştır. Projede seminerler, atölye çalışmaları ve konferanslar gibi etkinlikler düzenlenmiştir.

Fulya Aslay'ın (2017) çalışmasında, STM ve Fortinet tarafından yayımlanan 2016 raporlarına göre, Türkiye'nin zararlı yazılım (malware) ve istismar kiti (exploit kit) tespit edilen ülkeler sıralamasında dünya çapında ilk 5'te yer aldığı belirtilmiştir. Trend Micro'nun 2016 raporu ise Türkiye'nin Avrupa'da fidye yazılımı (ransomware) saldırılarının en yoğun yaşandığı ülke olduğunu ortaya koymaktadır. Ayrıca, online bankacılık saldırılarının Türkiye'yi ciddi ölçüde etkilediği ve Türkiye'nin bu alanda Avrupa'da en çok saldırıya uğrayan ülke olduğu ifade edilmektedir. Cybersecurity Ventures'in tahminlerine göre siber suçların küresel maliyeti 2015'te 3 trilyon dolarken, 2021'de 6 trilyon dolara ulaşması beklenmektedir. Bu bağlamda, siber tehditlerin artmasıyla beraber ülkeler siber güvenlik yatırımlarını artırmakta ve şirketler bilgi güvenliği danışmanlık hizmetlerine yönelmektedir. Türkiye'nin de bu

doğrultuda daha etkili siber güvenlik stratejileri geliştirerek yatırımlarını artırması gerekmektedir.

Cengiz Gündüz Alp'in (2021) çalışmasında, Türkiye'deki üniversitelerin bilgi işlem daire başkanlıklarında çalışanların dijital veri güvenliği ve siber güvenlik farkındalıkları incelenmiştir. Çalışma, bilgi işlem alanında kadın çalışanların dijital veri güvenliği farkındalığının erkeklere göre daha yüksek olduğunu ortaya koymuştur. Ancak, bizim çalışmamızda daha geniş bir sektör yelpazesinden çalışanlar incelenmiş ve erkeklerin yanıtlarının birbirine benzer olduğu, ayrıca erkeklerin siber güvenlik eğitimlerine katılım, cihaz güncellemeleri ve kişisel verilerin sosyal medyada paylaşılmaması gibi konularda kadınlardan daha fazla hassasiyet gösterdiği belirlenmiştir.

Cengiz Gündüz Alp'in (2021) araştırmasında dijital veri güvenliği farkındalıklarının yaş gruplarına göre değişiklik gösterdiği ve özellikle 51-60 yaş arasındaki çalışanların diğer gruplara kıyasla daha yüksek farkındalığa sahip olduğu belirtilmiştir. Bu farkındalık düzeyinin, deneyim ve bilinç düzeyiyle ilişkili olduğu ifade edilmiştir. Ancak, bizim çalışmamızda daha geniş bir sektörel örneklem kullanılarak 34-40 yaş grubundaki çalışanların antivirüs kullanımı, güvenlik eğitimlerine katılım, yazılım güncellemeleri yapma ve e-postaları spam olarak işaretleme gibi dijital güvenlik davranışlarında diğer yaş gruplarına göre daha duyarlı oldukları gözlemlenmiştir.

Cengiz Gündüz Alp'in (2021) araştırması, dijital veri güvenliği farkındalıklarının eğitim düzeyine göre farklılık gösterdiğini, özellikle doktora mezunu bireylerin daha yüksek farkındalığa sahip olduğunu ortaya koymuştur. Bu durum, doktora mezunlarının konuya dair bilgi ve deneyimlerinin daha fazla olmasına bağlanmıştır. Bizim çalışmamızda da benzer şekilde, eğitim seviyesi arttıkça siber güvenlik farkındalığının arttığı ve daha yüksek eğitim düzeyine sahip bireylerin bu konuda daha duyarlı davrandığı görülmüştür. Her iki araştırma, dijital veri güvenliği ve siber güvenlik farkındalıklarının demografik faktörlere göre değişiklik gösterdiğini, ancak sektörel farklılıkların ve örneklem büyüklüğünün de önemli etkiler yarattığını vurgulamaktadır. Bu tür bulgular, güvenlik farkındalığını artırma stratejilerinin geliştirilmesine rehberlik edebilir.

Jeong ve arkadaşları (2022), siber güvenlik alanında ulusal kültürün anlaşılmasının önemine işaret ederek, kültürel faktörlerin özel ve kamu kuruluşlarının siber güvenlik yatırımlarını etkilediğini belirtmişlerdir. Kott ve Linkov (2021) ise siber sistemlerin direnç seviyelerinin ölçülmesinin zor olduğunu, bu nedenle siber güvenliğin daha sıkı ve nicel bir şekilde değerlendirilmesi gerektiğini vurgulamıştır. Kumar ve arkadaşları (2023), siber tehdit avcılığı için güvenlik mekanizmaları tasarlanırken açıklanabilir yapay zekanın önemine dikkat çekmiş, AI tabanlı siber güvenlik sistemlerinde şeffaflık ve yorumlana bilirliğin gerekliliğini vurgulamıştır.

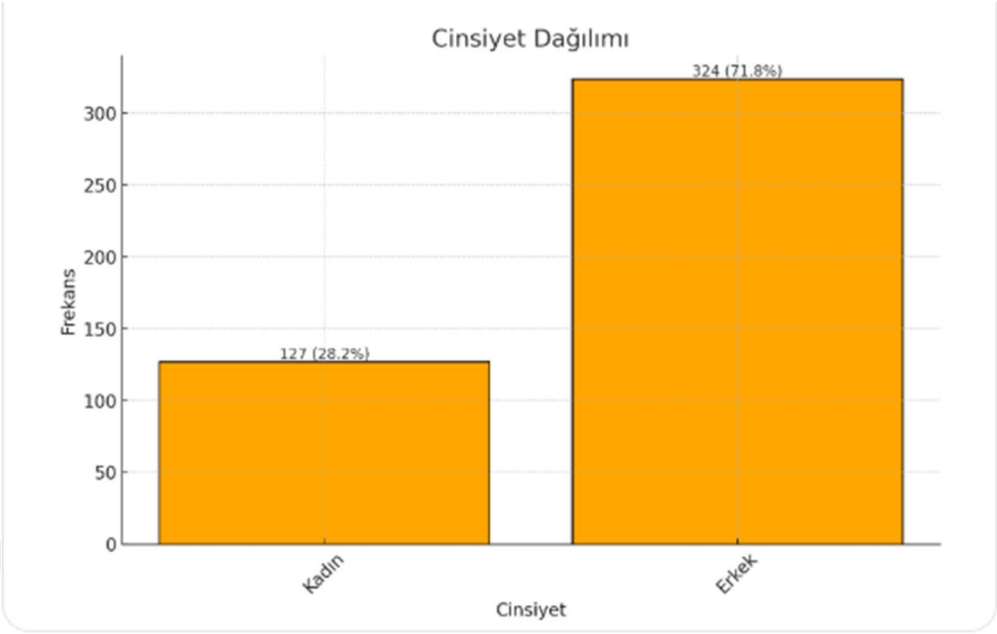
4. YÖNTEM

4.1. Araştırmanın Modeli

Bu araştırma tarama modellerinden tekil tarama modeli kullanılarak hazırlanmıştır. Bu tarama modeli var olan durumu olduğu gibi açıklamayı benimseyen bir yaklaşımdır. Bu yaklaşım olayların sebeplerine odaklanmak yerine mevcut durumlarını, özelliklerini ve aralarındaki bağlantıları incelemeye öncelik verir. Araştırmanın odağındaki olay, kişi ya da nesne, kendi koşulları çerçevesinde, olduğu haliyle açıklanmaya çalışılır; bu süreçte herhangi bir değiştirme ya da müdahale hedeflenmez. Tekil tarama modeli, değişkenlerin türlerini veya miktarlarını ayrı ayrı inceleyip belirlemeyi amaçlayan bir araştırma modelidir (Karasar, 2008). Bu araştırmada tarama modellerinden biri olan tekil tarama modeliyle Van ilinde ki çalışanların siber güvenlik farkındalıklarının ölçülmesi amaçlanmaktadır.

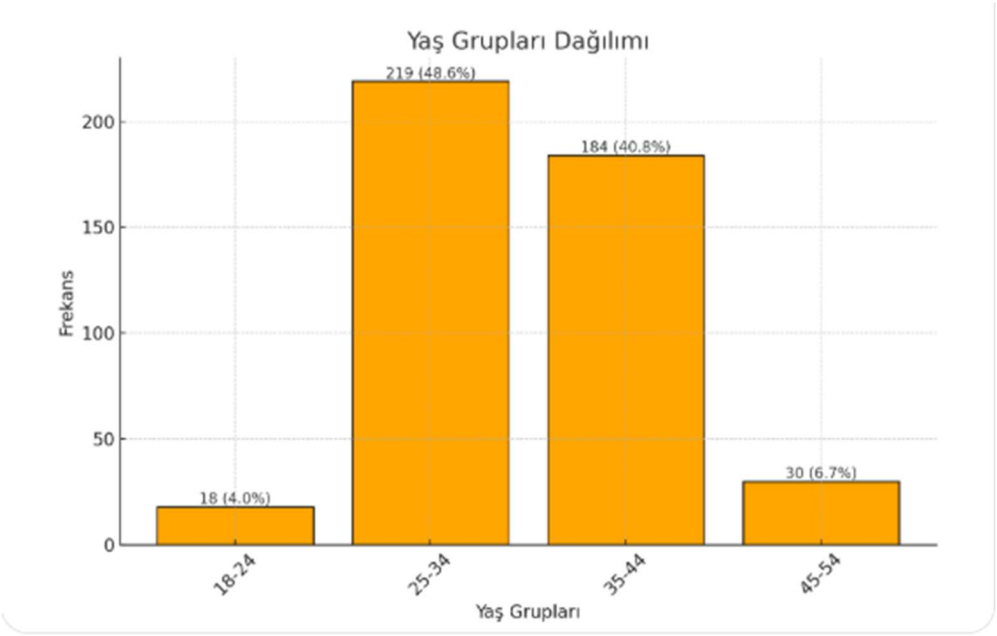
4.2. Evren ve Örneklem

Araştırma Evreni, Van ilinde ikamet edip aktif iş hayatı içinde olanları kapsamaktadır. Örneklem rastgele seçilen 451 katılımcıdan oluşmaktadır. Araştırmaya katılıp Van ilinde mi yaşıyorsunuz? Sorusuna hayır cevabı verenler ile Van ilinde yaşamasına rağmen çalışıyor musunuz? Sorusuna Hayır cevabı verenler kapsam dışında tutulmuştur. Ankete katılım sağlayanların dağılımları Aşağıdaki Tablolar ’da gösterilmiştir.



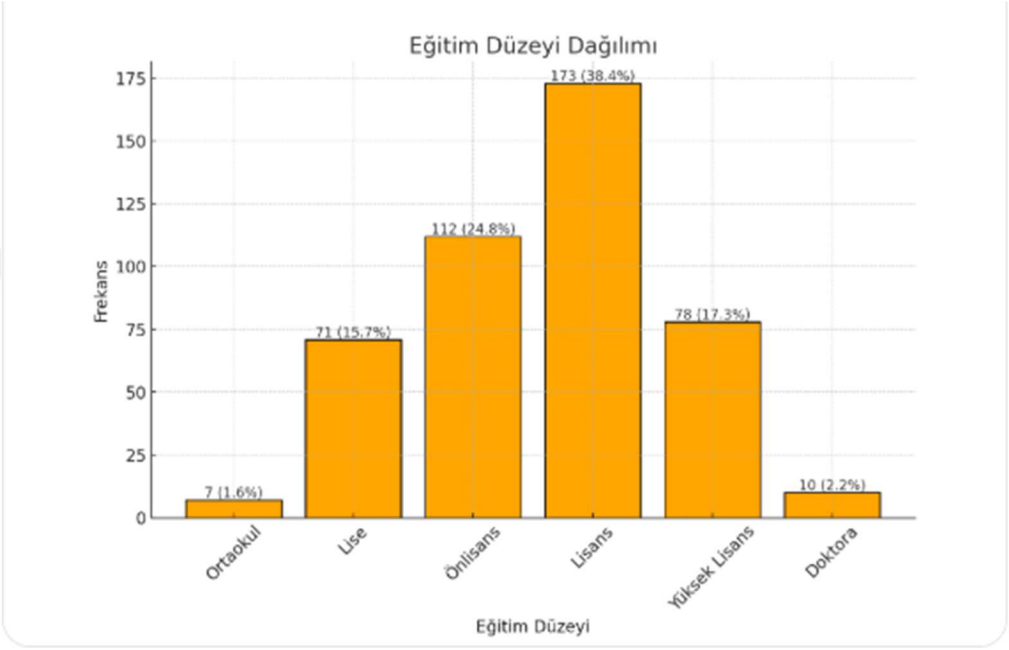
Şekil 6 Araştırmanın katılımcılarına ait cinsiyet dağılımı

Şekil 6 da gösterildiği gibi anket çalışmasına katılan ve Van ilinde ikamet edip aktif olarak çalışma hayatının içinde bulunan 451 katılımcıdan %71,8'i (324) erkek iken %28,2'si (127) kadındır.



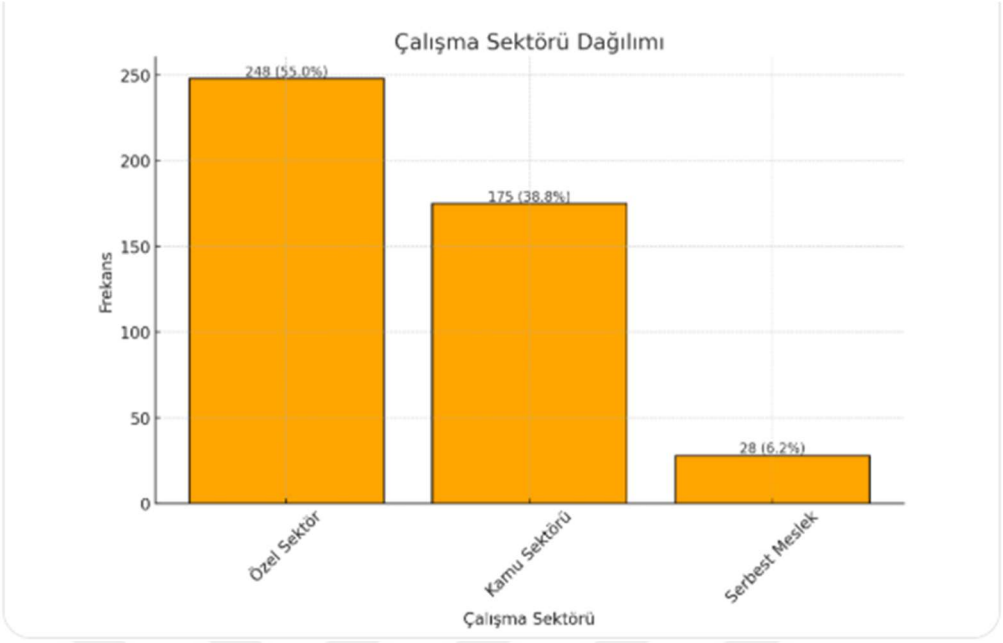
Şekil 7 Araştırmanın katılımcılarına ait yaş dağılımı

Anket çalışmasına katılan ve Van ilinde ikamet eden, aktif çalışma hayatında bulunan katılımcıların yaş dağılımına bakıldığında, en yüksek katılımın %48,6 ile 25-34 yaş aralığında olduğu tespit edilmiştir. Bunu %40,8 ile 35-44 yaş aralığındaki katılımcılar takip etmektedir. Katılımcıların %6,7'si 45-54 yaş Aralığında, %4,0'ı ise 18-24 yaş aralığında yer almaktadır.



Şekil 8 Araştırmanın katılımcılarına ait eğitim düzeyi dağılımı

Şekil 8'de gösterildiği gibi, anket çalışmasına katılan ve Van ilinde ikamet edip aktif olarak çalışma hayatında bulunan katılımcıların eğitim düzeyi incelendiğinde, katılımcıların %1,6'sının Ortaokul %15,7'sinin lise, %24,8'inin ön lisans, %38,4'ünün lisans, %17,3'nün yüksek lisans ve %2,2'sinin doktora mezunu olduğu belirlenmiştir.



Şekil 9 Araştırmanın katılımcılarına ait çalışılan sektör dağılımı

Şekil 9'da gösterildiği gibi Anket çalışmasına katılan ve Van ilinde ikamet edip aktif olarak çalışma hayatının içinde bulunan katılımcıların çalıştıkları sektör incelendiğinde, katılımcıların %55,0'ının Özel Sektör, %38,8'inin Kamu Sektörü, %6,2'sinin Serbest Meslek çalışanı olduğu belirlenmiştir.

4.3. Veri toplama araçları

Bu araştırmada, nicel araştırma yöntemlerinden biri olan anket tekniği kullanılarak veriler toplanmıştır. Arpacı ve Sevinç (2022) tarafından geliştirilen Siber Güvenlik Ölçeğinden yararlanılarak, Google Forms aracılığıyla çevrimiçi olarak uygulanmış ve katılımcılara elektronik ortamda ulaştırılmıştır. Ayrıca, bazı katılımcılarla yüz yüze görüşmeler gerçekleştirilmiştir. Araştırmanın birinci bölümünde katılımcıların demografik özelliklerini belirlemeye yönelik 4 soru yer alırken, ikinci bölümde çalışanların siber güvenlik farkındalık düzeylerini ölçmeyi amaçlayan 24 ifade yer almıştır.

4.4. Araştırmanın Hipotezleri

H1: Cinsiyet, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir.

H2: Yaş, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir.

H3: Eğitim düzeyi, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir.

H4: Çalışılan sektör, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir.

4.5. Siber Güvenlik Ölçeği

Arpaci & Sevinç (2022) tarafından geliştirilen Siber Güvenlik Ölçeğinden (SGÖ) oluşmaktadır. 24 maddeden oluşan bu 5'li Likert tipi ölçek, Gizlilik, Kontrol/Sahiplik, Bütünlük, Gerçeklik, Erişilebilirlik ve Fayda olmak üzere 6 faktörü kapsamaktadır. Ölçekteki ifadeler "Kesinlikle Katılıyorum" (5) ile "Kesinlikle Katılmıyorum" (1) arasında derecelendirilmiştir. Puanlama sırasında, 17 normal madde doğrudan 5'ten 1'e, 7 ters madde ise tersine, yani 1'den 5'e doğru puanlanmıştır. SGÖ'nin Cronbach Alfa iç güvenirlik katsayısı genel olarak 0.88'dir. Faktörler için bu değerler şu şekildedir: Gizlilik için 0.784, Kontrol/Sahiplik için 0.810, Bütünlük için 0.795, Gerçeklik için 0.784, Erişilebilirlik için 0.734 ve Fayda için 0.735. Bu çalışmada, ölçeğin genel Cronbach Alfa iç güvenirlik katsayısı 0.818 olarak hesaplanmıştır. Faktörler için ise sırasıyla 0.819, 0.912, 0.607, 0.826, 0.721 ve 0.714 olarak bulunmuştur. Bu sonuçlar, orijinal ölçek değerleriyle büyük ölçüde uyumlu olup, ölçeğin genel olarak ve faktörler bazında yeterli güvenirliğe sahip olduğunu göstermektedir.

4.6. Verilerin Analizi

Bu çalışmada elde edilen veriler, SPSS 30.0 ve AMOS 24.0 analiz programları kullanılarak incelenmiştir. Analiz sürecinde, araştırmada kullanılan ölçeğin güvenilirliğini değerlendirmek için **Cronbach Alpha güvenilirlik testi**, ölçeklerin yapı geçerliliğini belirlemek amacıyla **Doğrulayıcı faktör analizi,** Değişkenler arasındaki ilişkileri incelemek için **korelasyon analizi** ve katılımcıların demografik özelliklerine ve farklı gruplar arasındaki farklara yönelik değerlendirmeler için **t-testi** ve **ANOVA analizi** kullanılmıştır. Ayrıca, betimleyici istatistikler ile katılımcıların genel eğilimleri ve veri dağılımları analiz edilmiştir.

Tablo 1 Tablo 1 Güvenirlik Analizi Sonucu

Cronbach Alfa Kat sayısı	Standartlaştırılmış Maddeler Cronbach Alfa Kat sayısı	İfade sayısı
0,790	0,802	24

Tablo 1'de görüldüğü üzere, Cronbach Alpha değeri 0.7'nin üzerindedir. Bu durum, ölçeğin genel boyut bazında yüksek bir güvenilirliğe sahip olduğunu

göstermektedir. Cronbach Alpha, bir ölçeğin iç tutarlılığını ölçen ve maddelerin birbiriyle olan ilişkisini değerlendiren bir güvenilirlik katsayısıdır. Değerin 0,7'nin üzerinde olması, ölçeğin maddelerinin aynı yapıyı ölçtüğünü ve tutarlı sonuçlar verdiğini göstermektedir.

Tablo 2 Ortalama, Çarpıklık ve Basıklık Değerleri (N=451)

	Min.	Max.	Ort.	S.S.	Çar.	Bas.
1-Siber ortamda paylaştığım kişisel bilgiler konusunda temkinliyimdir.	1	5	4,06	0,942	-1,167	1,397
2-Gerçek hayatta üçüncü şahıslarla paylaşmak istemediğim bilgi ve belgeleri siber ortamda da paylaşmam.	1	5	4,16	0,897	-1,318	2,034
3-Siber ortamda paylaştığım verilerin sadece gerekli kişilerce görüntülenmesini sağlarım.	1	5	3,98	1,018	-1,257	1,324
4-Hesaplarıma ait şifrelerin güvenliği konusunda dikkatliyim.	1	5	4,24	0,880	-1,532	2,997
5-Şifremi oluştururken sembol, rakam ya da büyük küçük harflerden oluşan tahmini zor bir şifre seçerim.	1	5	4,30	0,870	-1,580	2,813
6-E-posta şifremin güvenliği için telefon doğrulaması hizmetini kullanırım.	1	5	4,19	0,973	-1,382	1,488
7-Cevabını hatırlayacağım bir güvenlik sorusu seçmeye özen gösteririm.	1	5	4,21	0,912	-1,571	2,787
8-Kredi kartı bilgilerimin kaydedilmemiş olmasına dikkat ederim.	1	5	4,23	0,989	-1,445	1,699
9-Siber ortamda veri saklamak güvenli değildir.	1	5	3,91	0,968	-0,845	0,574
10-Siber ortamda sakladığım bilgi ve belgeler kaybolabilir ya da silinebilir.	1	5	3,82	0,997	-0,900	0,617
11-Siber ortamda veri paylaşımı yapmak herhangi bir risk içermez.	1	5	3,92	1,071	-0,959	0,435
12-Siber ortamda saklanan bilgi ve belgelere üçüncü şahısların erişme olasılığı vardır.	1	5	3,96	1,031	-1,269	1,422
13-Tanımadığım kişilerden gelen e-postalardaki linkleri ve eklentileri açarım.	1	5	4,00	1,151	-1,169	0,536
14-Girdiğim web sitesinin güvenlik sertifikası olmadığı yönünde bildirim gelse de kullanmaya devam ederim.	1	5	3,64	1,154	-0,543	-0,624
15-E-postama gelen istenmeyen (spam) postaları açtığım olmuştur.	1	5	3,47	1,258	-0,225	-1,287
16-E-postama gelen müşteri edinme/oltalama amaçlı postaları açtığım olmuştur.	1	5	3,65	1,146	-0,552	-0,609

17-Belirsiz kaynaklardan gelen bağlantıları (linkleri) ve dosyaları açtığım olmuştur.	1	5	3,64	1,161	-0,535	-0,783
18-Cihazımda güncel bir anti virüs programı var.	1	5	3,31	1,244	-0,401	-0,976
19-Cihazımı düzenli olarak anti virüs programı ile taratırım.	1	5	3,27	1,274	-0,315	-1,056
20-Cihazıma Kurulu gelen güvenlik duvarı açık.	1	5	3,29	1,179	-0,379	-0,803
21-İnternetten indirdiğim dosyaları cihazımda yüklü anti virüs programı olmasa da açarım.	1	5	3,33	1,189	-0,183	-1,029
22-Siber ortamda sosyal medya uygulamalarını bilgi paylaşımı için kullanırım.	1	5	3,10	1,153	-0,292	-0,928
23-Günlük hayatta karşılaştığım problemleri çözmek için siber ortamı yaygın olarak kullanırım.	1	5	3,22	1,170	-0,301	-0,876
24-Siber ortamda sunulan hizmetlerden bilgi yönetimi (bilgiyi elde etmek, saklamak, paylaşmak ve kullanmak) için faydalanırım.	1	5	3,58	1,069	-0,738	-0,012

Tablo 2'de araştırmanın normal dağılıp dağılmadığını incelemek adına çarpıklık basıklık değerlerine bakılmıştır. Literatüre göre, normallik için basıklık ve çarpıklık değerlerinin belirli sınırlar içerisinde olması gerekmektedir. Bu bağlamda, Tabachnick ve Fidell (2015) basıklık ve çarpıklık değerlerinin −1.5 ile +1.5 Aralığında, George ve Mallery (2002) −2 ile +2 Aralığında, Kalaycı (2015) ise −3 ile +3 Aralığında olmasını kabul etmektedir. Araştırmada elde edilen değerlerin bu sınırlar içinde yer alması nedeniyle, verilerin normallik varsayımını karşıladığı söylenebilir. Ayrıca, Merkezi Limit Teoremi 'ne göre, sosyal bilimlerde yeterli bir örneklem büyüklüğüne ulaşıldığında (N>400), normallik varsayımının sağlandığı kabul edilmektedir. Bu doğrultuda, araştırmanın örneklem büyüklüğü ve analiz edilen verilere dayanarak normallik varsayımının geçerli olduğu varsayılmaktadır (Karasar, 2012: 102-103). Bu nedenle, araştırmanın sonraki aşamalarında yapılan analizler, normallik varsayımının sağlandığı kabulüyle gerçekleştirilmiştir.

Tablo 3 Doğrulayıcı Faktör Analizi

Madde	Yol	Faktörler	β0	β1	S.E.	C.R.	P
Giz1	<---	Gizlilik	0,573	1			
Giz2	<---	Gizlilik	0,785	1,303	0,13	10,06	***
Giz3	<---	Gizlilik	0,59	1,112	0,123	9,018	***
Kont5	<---	Kontrol/sahiplik	0,537	1			
Kont4	<---	Kontrol/sahiplik	0,688	1,181	0,114	10,339	***
Kont3	<---	Kontrol/sahiplik	0,64	1,172	0,118	9,907	***
Kont2	<---	Kontrol/sahiplik	0,839	1,375	0,121	11,386	***
But4	<---	Bütünlük	0,453	1			
But3	<---	Bütünlük	0,165	0,377	0,139	2,706	0,007
But2	<---	Bütünlük	0,698	1,49	0,231	6,456	***
But1	<---	Bütünlük	0,568	1,178	0,182	6,463	***
Kont1	<---	Kontrol/sahiplik	0,792	1,312	0,118	11,121	***
Ger5	<---	Gerçeklik	0,757	1			
Ger4	<---	Gerçeklik	0,794	1,034	0,065	15,798	***
Ger3	<---	Gerçeklik	0,753	1,078	0,071	15,075	***
Ger2	<---	Gerçeklik	0,588	0,775	0,066	11,748	***
Ger1	<---	Gerçeklik	0,578	0,76	0,066	11,545	***
Er1	<---	Erişilebilirlik	0,798	1			
Er2	<---	Erişilebilirlik	0,944	1,21	0,099	12,216	***
Er3	<---	Erişilebilirlik	0,381	0,452	0,057	7,898	***
Er4	<---	Erişilebilirlik	0,169	0,202	0,059	3,432	***
Fay1	<---	Fayda	0,6	1			

Fay2	<---	Fayda	0,717	1,215	0,141	8,606	***
Fay3	<---	Fayda	0,621	0,96	0,112	8,577	***

β0(Standardize değerler)
β1(Standardize olmayan değerler)

Tablo 3'te doğrulayıcı Faktör Analizi (DFA) sonuçları, modelin genel olarak kabul edilebilir bir uyum düzeyine sahip olduğunu göstermektedir. Analiz sonuçlarında Ki-kare / Serbestlik Derecesi Oranı 2,136 olarak hesaplanmıştır. Bu değer, modelin gözlemlenen veri ile kuramsal model arasındaki uyumunun iyi olduğunu ifade etmektedir.

Modelin genel uyumunu değerlendiren Yaklaşımın Ortalama Kök Hata Kareleri (RMSEA) değeri 0,050 bulunmuştur. Bu değer, modelin popülasyon düzeyinde mükemmel uyum kriterini karşıladığını göstermektedir. Ayrıca, Uyum İyiliği İndeksi (GFI) 0,915 ve Karşılaştırmalı Uyum İndeksi (CFI) 0,918 olarak hesaplanmıştır. Bu değerler, modelin genel uyumunun kabul edilebilir düzeyde olduğunu ve kuramsal model ile gözlemlenen veri arasında yeterli bir uyum sağladığını ortaya koymaktadır.

Modelde yer alan faktörlerin, ilgili maddelerle olan ilişkileri incelendiğinde, maddelerin büyük çoğunluğunun faktör yüklerinin 0,5'in üzerinde olduğu gözlemlenmiştir. Faktör yükleri, maddelerin ilgili faktörleri ne kadar iyi temsil ettiğini göstermektedir ve genellikle 0,5 ve üzerindeki değerler yeterli kabul edilmektedir. Bununla birlikte, Bütünlük faktörüne ait But3 maddesi (0,165) ve Erişilebilirlik faktörüne ait Er4 maddesi (0,169) düşük faktör yüklerine sahiptir. Bu durum, bu maddelerin ilgili faktörleri temsil etme gücünün sınırlı olduğunu göstermektedir. Ancak, bu maddelerin modelin genel uyum istatistiklerini olumsuz etkilemediği ve teorik bağlamda anlamlı olduğu göz önüne alınarak analizde tutulmasına karar verilmiştir.

Analiz sürecinde, modifikasyon indeksleri incelenmiş, ancak teorik çerçevenin korunması amacıyla herhangi bir modifikasyon yapılmamıştır. Modelin mevcut haliyle genel uyum istatistiklerinin yeterli düzeyde olması, modifikasyona gerek olmadığını desteklemektedir.

Genel olarak, DFA sonuçları modelin geçerli ve güvenilir bir yapı sunduğunu göstermektedir. Modelin genel uyum istatistikleri ve faktör yükleri değerlendirildiğinde, elde edilen sonuçlar araştırma modelinin kuramsal çerçeveye

uygun bir şekilde çalıştığını ortaya koymaktadır. Sonuçlar, modelin araştırma bağlamında uygun bir temel sunduğunu ve analizler için yeterli kabul edildiğini göstermektedir.

Tablo 4 Korelasyon Analizi

	Gizlilik	Kontrol/Sahiplik	Bütünlük	Gerçeklik	Erişilebilirlik	Fayda
Gizlilik	1					
Kontrol/Sahiplik	0,516**	1				
Bütünlük	0,295**	0,312**	1			
Gerçeklik	0,295**	0,289**	0,098*	1		
Erişilebilirlik	0,165**	0,305**	0,081	0,278**	1	
Fayda	0,059	0,040	0,120*	-0,191**	0,010	1

Tablo 4'te gösterildiği gibi korelasyon analizi sonuçlarına göre, değişkenler arasında anlamlı ilişkiler tespit edilmiştir ve bu ilişkiler araştırma bağlamında anlamlı çıkarımlar yapmayı mümkün kılmaktadır.

Gizlilik ile diğer değişkenler arasında pozitif ve anlamlı ilişkiler bulunmaktadır. Özellikle gizlilik ile kontrol sahipliği arasındaki ilişki ($r = 0.516$, $p < 0.001$) pozitif ve güçlüdür, bu da gizliliğin artmasının bireylerin kontrol hissini artırabileceğini göstermektedir. Aynı şekilde, gizlilik ile bütünlük ($r = 0.295$, $p < 0.001$) ve gerçeklik ($r = 0.295$, $p < 0.001$) arasında pozitif ve orta düzeyde ilişkiler görülmektedir. Bu bulgular, gizlilik düzeyinin bireylerin bütünlük ve gerçeklik algıları üzerinde anlamlı bir etkisi olabileceğini ortaya koymaktadır. Ancak, gizlilik ile erişilebilirlik arasındaki ilişki ($r = 0.165$, $p < 0.001$) pozitif olmakla birlikte daha zayıftır, bu da gizlilik ile erişilebilirlik arasında sınırlı bir ilişki olduğunu göstermektedir. Gizlilik ile fayda arasındaki ilişki ($r = 0.059$, $p = 0.213$) ise anlamlı bulunmamıştır, bu nedenle gizlilik değişkeninin fayda algısı üzerinde kayda değer bir etkisi olmadığı sonucuna varılabilir.

Kontrol/sahiplik ile diğer değişkenler arasındaki ilişkiler de dikkat çekicidir. Kontrol sahipliği, erişilebilirlik ile pozitif ve orta düzeyde ($r = 0.305$, $p < 0.001$), bütünlük ile ise pozitif ve anlamlı bir ilişki göstermektedir ($r = 0.312$, $p < 0.001$). Ayrıca, kontrol sahipliği ile gerçeklik arasındaki ilişki ($r = 0.289$, $p < 0.001$) pozitif ve orta düzeydedir. Bu sonuçlar, bireylerin kontrol sahibi olma hissinin diğer algılarla güçlü bir şekilde ilişkili olduğunu ve bu hissin artırılmasının bütünlük, erişilebilirlik ve gerçeklik algılarını olumlu yönde etkileyebileceğini göstermektedir. Ancak, kontrol sahipliği ile fayda arasındaki ilişki ($r = 0.040$, $p = 0.393$) anlamlı bulunmamış, dolayısıyla kontrol sahipliği değişkeninin fayda algısı üzerinde anlamlı bir etkisi olmadığı sonucuna ulaşılmıştır.

Bütünlük ile diğer değişkenler arasındaki ilişkiler incelendiğinde, gerçeklik ile ($r = 0.098$, $p = 0.038$) ve fayda ile ($r = 0.120$, $p = 0.011$) pozitif ve anlamlı ancak zayıf düzeyde ilişkiler gözlenmiştir. Bu bulgular, bütünlük algısının gerçeklik ve fayda algıları üzerinde sınırlı bir etkisi olabileceğini göstermektedir. Erişilebilirlik ile bütünlük arasındaki ilişki ($r = 0.081$, $p = 0.085$) anlamlı bulunmamıştır.

Gerçeklik değişkenine bakıldığında, erişilebilirlik ile pozitif ve orta düzeyde bir ilişki gözlenmiştir ($r=0.278$, $p<0.001$). Bu, gerçeklik algısının artmasının erişilebilirlik algısını artırabileceğini göstermektedir. Ancak, gerçeklik ile fayda arasındaki ilişki ($r=-0.191$, $p<0.001$) negatif ve anlamlı bulunmuştur. Bu, gerçeklik algısının artmasının fayda algısında bir azalmaya neden olabileceğini düşündürmektedir. Bu sonuç, fayda ve gerçeklik algılarının çelişkili bir yapıya sahip olabileceğini işaret edebilir ve bu durumun araştırma bağlamında detaylı bir şekilde incelenmesi gerekebilir.

Son olarak, fayda değişkeni ile diğer değişkenler arasındaki ilişkiler incelendiğinde, anlamlı korelasyonların genellikle zayıf olduğu görülmüştür. Örneğin, fayda ile bütünlük arasındaki ilişki ($r=0.120$,$p=0.011$) zayıf ve anlamlıdır. Ancak, fayda ile diğer değişkenler (örneğin gizlilik, kontrol sahiplik ve erişilebilirlik) arasındaki ilişkiler istatistiksel olarak anlamlı bulunmamıştır.

Genel olarak bu bulgular, gizlilik, kontrol sahipliği, bütünlük ve gerçeklik gibi değişkenlerin birbirleriyle ilişkili olduğunu ve bireylerin bu algılarının yapısal bir düzen içinde değerlendirilebileceğini göstermektedir. Ancak fayda değişkeninin diğer değişkenlerle olan ilişkilerinin genelde zayıf veya anlamsız olması, fayda algısının araştırma bağlamında farklı faktörler tarafından etkilenebileceğine işaret etmektedir.

5. BULGULAR

5.1. Siber Güvenliğin Cinsiyete Göre Farkındalık Seviyesinin Ölçülmesi

Çalışanların siber güvenlik farkındalık düzeylerinin cinsiyete göre farklılaşıp farklılaşmadığını incelemek amacıyla bağımsız örneklem t-testi yapılmış ve sonuçlar aşağıdaki tabloda gösterilmiştir:

Tablo 5 Cinsiyete Göre Genel Siber Güvenlik Farkındalığı T-Testi Sonuçları

Cinsiyet	N	Ort.	S.S.	t	P
Kadın	127	3.7920	0.34100	0.775	0.439
Erkek	324	3.7607	0.48186		

Tablo 5'te gösterildiği gibi yapılan bağımsız gruplar t-testi analizi sonuçlarına göre, cinsiyetin genel siber güvenlik farkındalığı üzerinde istatistiksel olarak anlamlı bir etkisi bulunmamıştır (**t = 0.775, p = 0.439**). Kadın katılımcıların genel ortalama puanları (**Ort. = 3.79, S.S = 0.34**) erkek katılımcıların genel ortalama puanlarından (**Ort. = 3.76, S.S = 0.48**) biraz daha yüksek olsa da, bu fark istatistiksel olarak anlamlı değildir.

Bu sonuç, cinsiyetin genel siber güvenlik farkındalığı üzerinde belirgin bir etkisi olmadığını ve kadınlar ile erkekler arasında genel farkındalık düzeyleri açısından önemli bir farklılık olmadığını göstermektedir. Cinsiyet, genel siber güvenlik farkındalığını anlamlı şekilde etkileyen bir değişken olarak değerlendirilmemektedir.

Tablo 6 Cinsiyete Göre Alt Boyutlar T-Testi Sonuçları

	Cinsiyet	N	Ort.	S.S.	t	P
Gizlilik	Kadın	127	4.1339	0.65769	-1.268	0.205
	Erkek	324	4.0350	0.77598		
Kontrol/Sahiplik	Kadın	127	4.2094	0.59674	-0.481	0.631
	Erkek	324	4.2451	0.74606		
Bütünlük	Kadın	127	3.8858	0.58989	-0.320	0.749
	Erkek	324	3.9074	0.66386		
Gerçeklik	Kadın	127	3.8173	0.69466	2.347	0.020
	Erkek	324	3.6253	0.96834		
Erişilebilirlik	Kadın	127	3.2913	0.73582	-0.157	0.875
	Erkek	324	3.304	0.85556		
Fayda	Kadın	127	3.2546	0.78843	-0.685	0.494
	Erkek	324	3.3179	0.91772		

Tablo 6'da gösterildiği gibi yapılan bağımsız gruplar t-testi analizi sonuçlarına göre, cinsiyetin siber güvenlik farkındalığının tüm boyutları üzerinde anlamlı bir etkisi bulunmamış, ancak **Gerçeklik** boyutunda istatistiksel olarak anlamlı bir fark tespit edilmiştir **(t = 2.347, p = 0.020).** Kadın katılımcıların Gerçeklik farkındalığına ilişkin ortalama puanlarının **(Ort. = 3.82, S.S = 0.69)**, erkek katılımcıların ortalama puanlarından **(Ort. = 3.63, S.S = 0.97)** anlamlı derecede daha yüksek olduğu belirlenmiştir. Bu bulgu, kadınların çevrimiçi ortamda gerçeklik farkındalığına ilişkin algılarının erkeklere kıyasla daha yüksek olduğunu göstermektedir.

Ancak, siber güvenlik farkındalığının diğer boyutları olan Gizlilik, Kontrol/Sahiplik, Bütünlük, Erişilebilirlik ve Fayda değişkenlerinde cinsiyetler arasında anlamlı bir fark bulunmamıştır **(p>0.05)**. Bu durum, cinsiyetin siber güvenlik farkındalığı üzerindeki etkisinin sınırlı olduğunu ve belirli bir boyutta yoğunlaştığını göstermektedir.

Cinsiyetin, siber güvenlik farkındalığının tüm boyutları üzerinde değil, yalnızca **Gerçeklik** boyutunda anlamlı bir etkisi bulunmaktadır. Bu doğrultuda, **H_1**: Cinsiyet, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir. Hipotezini desteklememektedir.

5.2. Siber Güvenliğin Yaşa Göre Farkındalık Seviyesinin Ölçülmesi

Araştırmaya katılan çalışanların yaş değişkeninin ANOVA testi sonuçları analiz edilmiştir.

Tablo 7 Yaş gruplarına Göre Genel ANOVA sonuçları

	Kareler Top.	S.d	Kareler Ort.	F	P
Gruplar arası	1,086	3	0,362	1,826	0,142
Gruplar içi	88,650	447	0,198		
Toplam	89,737	450			

Tablo 7'de gösterildiği gibi yapılan tek yönlü ANOVA analizi sonuçlarına göre, yaş grupları arasında genel siber güvenlik farkındalığı skorları açısından istatistiksel olarak anlamlı bir fark bulunamamıştır (**F = 1.826, p = 0.142**). Yaş grupları arasındaki varyasyon toplamı (Kareler Toplamı) 1.086 olarak hesaplanmış ve bu varyasyonun ortalama karesi 0.362'dir. Gruplar içindeki varyasyon toplamı ise 88.650 olarak bulunmuş ve ortalama kare değeri 0.198'dir. Elde edilen p değeri (**p = 0.142**)

0.05'ten büyük olduğu için, yaş grupları arasında genel siber güvenlik farkındalığı açısından anlamlı bir fark olmadığı sonucuna ulaşılmıştır. Bu bulgu, yaş değişkeninin genel siber güvenlik farkındalığı üzerinde belirgin bir etkisi olmadığını göstermekte ve farklı yaş gruplarının genel farkındalık düzeylerinin benzer olduğunu ortaya koymaktadır.

Tablo 8 Yaş grupları Alt Boyutlara göre ANOVA sonuçları

		Kareler Top.	S.d	Kareler Ort.	F	P
Gizlilik	Gruplar arası	5,153	3	1,718	3,137	0,025
	Gruplar içi	244,733	447	0,548		
	Toplam	249,887	450			
Kontrol/Sahiplik	Gruplar arası	3,073	3	1,024	2,066	0,104
	Gruplar içi	221,693	447	0,496		
	Toplam	224,766	450			
Bütünlük	Gruplar arası	2,005	3	0,668	1,621	0,184
	Gruplar içi	184,230	447	0,412		
	Toplam	186,234	450			
Gerçeklik	Gruplar arası	2,479	3	0,826	1,013	0,387
	Gruplar içi	364,559	447	0,816		
	Toplam	367,038	450			
Erişilebilirlik	Gruplar arası	2,545	3	0,848	1,255	0,289
	Gruplar içi	302,120	447	0,676		
	Toplam	304,665	450			
Fayda	Gruplar arası	1,013	3	0,338	0,432	0,731
	Gruplar içi	349,711	447	0,782		
	Toplam	350,723	450			

Tablo 8'de gösterildiği gibi yapılan tek yönlü ANOVA analizi sonuçlarına göre, yaş gruplarının siber güvenlik farkındalığının alt boyutları üzerindeki etkisi incelenmiştir. Analiz sonuçları, yalnızca **Gizlilik** boyutunda yaş grupları arasında istatistiksel olarak anlamlı bir fark olduğunu göstermiştir (**$F = 3.137$, $p = 0.025$**). Bu bulgu, yaşın gizlilik farkındalığı üzerinde etkili bir değişken olabileceğini ortaya koymaktadır.

Diğer alt boyutlar olan **Kontrol/Sahiplik, Bütünlük, Gerçeklik, Erişilebilirlik ve Fayda** açısından ise yaş grupları arasında anlamlı bir fark bulunmamıştır (**$p > 0.05$**).

Bu durum, yaş değişkeninin siber güvenlik farkındalığının genelinde sınırlı bir etkisi olduğunu, ancak belirli bir boyutta (Gizlilik) farklılık yaratabileceğini göstermektedir. Sonuç olarak, yaşın özellikle gizlilik farkındalığı üzerindeki etkisi dikkate değer bulunurken, diğer boyutlar açısından gruplar arasında fark olmadığı görülmektedir. Gizlilik boyutundaki farkın hangi yaş grupları arasında olduğunu belirlemek için post-hoc testi yapılmıştır.

Post-hoc testi sonuçlarına göre, Gizlilik boyutunda yaş grupları arasında anlamlı bir fark bulunmamaktadır (**p > 0.05**). ANOVA analizinde anlamlılık tespit edilmesine rağmen, post-hoc test sonuçları yaş grupları arasındaki farklılıkların belirgin olmadığını göstermektedir. Bu durum, farkların gruplar arasında homojen dağılabileceğini veya farkların küçük olduğunu gösterebilir.

Elde edilen bu sonuçlara göre, "**H_2** Yaş, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir." Hipotezini desteklememektedir.

5.3. Siber Güvenliğin Eğitim durumuna Göre Farkındalık Seviyesinin Ölçülmesi

Tablo 9 Eğitim Durumuna göre genel ANOVA sonuçları

	Kareler Top.	S.d	Kareler Top.	F	P
Gruplar arası	2,294	5	0,459	2,335	0,041
Gruplar içi	87,442	445	0,196		
Toplam	89,737	450			

Tablo 9'da gösterildiği gibi yapılan ANOVA analizi sonuçlarına göre, eğitim düzeyi grupları arasında Genel Ortalama açısından istatistiksel olarak anlamlı bir fark olduğu belirlenmiştir (**F = 2.335, p = 0.041**). **Gruplar arası varyans = 2.294** ve **gruplar içi varyans = 87.442** arasındaki oran, eğitim düzeyinin Genel Ortalama üzerinde anlamlı bir etkisi olduğunu göstermektedir. Bu sonuçlar, eğitim düzeyinin siber güvenlik farkındalığı üzerinde etkili bir değişken olduğunu ortaya koymaktadır.

Ancak, hangi eğitim düzeyleri arasında anlamlı farklar olduğunu belirlemek için yapılan post-hoc testi sonuçlarına göre, anlamlı farkın yalnızca **Ortaokul** ve **Ön lisans** grupları arasında olduğu bulunmuştur (**p = 0.038**). Diğer eğitim düzeyleri arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (**p > 0.05**). Bu bulgular, eğitim

düzeyinin siber güvenlik farkındalığını etkileyen sınırlı bir değişken olduğunu göstermektedir.

Tablo 10 Eğitim durumu Alt Boyutlara göre ANOVA sonuçları

		Kareler Top.	S.d	Kareler Ort.	F	P
Gizlilik	Gruplar arası	11,302	5	2,260	4,216	0,001
	Gruplar içi	238,585	445	0,536		
	Toplam	249,887	450			
Kontrol/Sahiplik	Gruplar arası	6,018	5	1,204	2,448	0,033
	Gruplar içi	218,749	445	0,492		
	Toplam	224,766	450			
Bütünlük	Gruplar arası	2,746	5	0,549	1,332	0,249
	Gruplar içi	183,488	445	0,412		
	Toplam	186,234	450			
Gerçeklik	Gruplar arası	4,202	5	0,840	1,031	0,399
	Gruplar içi	362,836	445	0,815		
	Toplam	367,038	450			
Erişilebilirlik	Gruplar arası	4,419	5	0,884	1,310	0,259
	Gruplar içi	300,246	445	0,675		
	Toplam	304,665	450			
Fayda	Gruplar arası	14,046	5	2,809	3,713	0,003
	Gruplar içi	336,677	445	0,757		
	Toplam	350,723	450			

Tablo 10'da gösterildiği gibi yapılan analizler sonucunda, eğitim düzeyinin siber güvenlik farkındalığı üzerinde kısmi olarak anlamlı bir etkisinin olduğu belirlenmiştir. ANOVA analizi sonuçlarına göre, eğitim düzeyi grupları arasında **Gizlilik**, **Kontrol/Sahiplik** ve **Fayda** boyutlarında anlamlı farklar bulunmuştur (**$p < 0.05$**). Ancak, diğer boyutlar olan **Bütünlük**, **Gerçeklik** ve **Erişilebilirlik** açısından eğitim düzeyi grupları arasında anlamlı bir fark tespit edilmemiştir (**$p > 0.05$**).

Post-hoc testi sonuçları, bu farkların detaylarını ortaya koymuştur. **Gizlilik** boyutunda, Ortaokul düzeyindeki katılımcıların farkındalık puanlarının Lise, Önlisans, Lisans ve Yüksek Lisans düzeylerine kıyasla anlamlı derecede daha düşük olduğu görülmüştür. **Fayda** boyutunda ise, Lise düzeyindeki katılımcıların farkındalık puanlarının Lisans, Yüksek Lisans ve Doktora düzeylerine kıyasla anlamlı derecede daha düşük olduğu tespit edilmiştir. **Kontrol/Sahiplik** boyutunda ANOVA sonucunda anlamlılık

bulunmasına rağmen, post-hoc test sonuçlarında gruplar arasında belirgin bir fark tespit edilmemiştir.

Sonuç olarak, eğitim düzeyinin siber güvenlik farkındalığı üzerinde özellikle **Gizlilik** ve **Fayda** boyutlarında etkili olduğu görülmüştür. Diğer boyutlarda ise eğitim düzeyine bağlı anlamlı bir fark bulunmamaktadır. Bu durum, eğitim düzeyinin siber güvenlik farkındalığının bazı boyutlarında etkili bir değişken olduğunu, ancak genel olarak sınırlı bir etkisi bulunduğunu göstermektedir. Elde edilen bu sonuçlara göre, "**H_3** Eğitim Düzeyi, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir." Hipotezini desteklememektedir.

5.4. Siber Güvenliğin Çalışılan Sektöre Göre Farkındalık Seviyesinin Ölçülmesi

Tablo 11 Çalışılan Sektöre Göre genel ANOVA sonuçları

	Kareler Top.	S.d	Kareler Ort.	F	P
Gruplar arası	0,283	2	0,142	0,709	0,492
Gruplar içi	89,453	448	0,200		
Toplam	89,737	450			

Tablo 11'de gösterildiği gibi yapılan ANOVA analizi sonuçlarına göre, gruplar arasında **Genel Ortalama** açısından istatistiksel olarak anlamlı bir fark bulunmamıştır (**F = 0.709, p = 0.492**). **p-değeri (0.492)**, 0.05 anlamlılık düzeyinden büyük olduğu için, gruplar arasında anlamlı bir farklılık olmadığı sonucuna ulaşılmıştır. Bu durum, incelenen değişkenin Genel Ortalama üzerinde etkili olmadığını ve gruplar arasında farklılık yaratmadığını göstermektedir.

Tablo 12 Çalışılan Sektöre göre Alt boyutlar ANOVA sonuçları

		Kareler Top.	S.d	Kareler Ort.	F	P
Gizlilik	Gruplar arası	0,292	2	0,146	0,262	0,770
	Gruplar içi	249,595	448	0,557		
	Toplam	249,887	450			
Kontrol/Sahiplik	Gruplar arası	2,145	2	1,072	2,158	0,117
	Gruplar içi	222,622	448	0,497		
	Toplam	224,766	450			
Bütünlük	Gruplar arası	1,702	2	0,851	2,066	0,128
	Gruplar içi	184,533	448	0,412		
	Toplam	186,234	450			

Gerçeklik	Gruplar arası	2,994	2	1,497	1,842	0,160
	Gruplar içi	364,044	448	0,813		
	Toplam	367,038	450			
Erişilebilirlik	Gruplar arası	2,442	2	1,221	1,810	0,165
	Gruplar içi	302,223	448	0,675		
	Toplam	304,665	450			
Fayda	Gruplar arası	1,020	2	0,510	0,653	0,521
	Gruplar içi	349,704	448	0,781		
	Toplam	350,723	450			

Tablo 12'de gösterildiği gibi yapılan analiz sonuçlarına göre, çalışılan sektörün siber güvenlik farkındalığı üzerinde anlamlı bir etkisi bulunmamıştır (**p > 0.05**). Çalışılan sektör, siber güvenlik farkındalığının Gizlilik, Kontrol/Sahiplik, Bütünlük, Gerçeklik, Erişilebilirlik ve Fayda boyutlarında anlamlı bir farklılık yaratmamaktadır. Bu sonuçlar, sektörün siber güvenlik farkındalığını etkileyen bir değişken olmadığını göstermektedir. **H_4** Çalışılan sektör, siber güvenlik farkındalığı üzerinde anlamlı bir etkiye sahiptir." Hipotezini desteklememektedir.

6. SONUÇ VE ÖNERİLER

Dijital çağda bireylerin ve kurumların bilgi güvenliğini sağlama konusundaki temel ihtiyaçlarından biri, siber güvenlik farkındalığıdır. Bu çalışmada, siber güvenlik farkındalığının cinsiyet, yaş, eğitim seviyesi ve çalışılan sektör gibi demografik faktörlerden nasıl etkilendiği incelenmiş ve farkındalığı artırmaya yönelik öneriler geliştirilmiştir. Araştırma sonuçları, bu demografik faktörlerin genelde farkındalık düzeyi üzerinde belirleyici olmadığını, ancak alt boyutlarda bazı farklılıklar yarattığını göstermiştir.

Cinsiyet değişkeni bağlamında, kadın ve erkek katılımcılar arasında genel farkındalık düzeyi açısından anlamlı bir fark bulunmamıştır. Bununla birlikte, "Gerçeklik" alt boyutunda kadınların farkındalık düzeyinin erkeklere göre daha yüksek olduğu belirlenmiştir. Bu bulgu, kadınların belirli siber güvenlik konularında daha duyarlı olduğunu ve bu duyarlılığın eğitim süreçlerinde dikkate alınması gerektiğini göstermektedir.

Yaş faktörü ele alındığında, farklı yaş gruplarının genel farkındalık düzeyleri arasında anlamlı bir fark bulunmamıştır. Yaşın, farkındalığın gelişimi üzerinde etkili bir faktör olmadığı, ancak farklı yaş gruplarının öğrenme stilleri ve teknolojik yetkinlikleri dikkate alınarak eğitim materyallerinin düzenlenmesinin fayda sağlayabileceği gözlemlenmiştir.

Eğitim seviyesine ilişkin analizler, mezun olunan eğitim seviyesinin farkındalık üzerinde anlamlı bir etkisinin olmadığını göstermiştir. Bu sonuç, farkındalığın yalnızca formal eğitim düzeyiyle ilişkilendirilemeyeceğini ve sürekli eğitim ile bireysel farkındalık artırma çabalarının önemini ortaya koymaktadır.

Çalışılan sektör açısından ise kamu, özel sektör ve serbest meslek grupları arasında farkındalık düzeylerinde anlamlı bir fark gözlemlenmemiştir. Ancak sektörlere özgü tehditlerin farklılık gösterebileceği dikkate alınarak, sektörlere yönelik özelleştirilmiş eğitim programlarının bazı durumlarda etkili olabileceği düşünülmektedir.

Bu bulgular doğrultusunda aşağıdaki öneriler geliştirilmiştir:

Cinsiyete Yönelik Özelleştirilmiş Eğitim Programları: Kadınların "Gerçeklik" alt boyutundaki farkındalık düzeyi erkeklere kıyasla daha yüksek olduğundan, erkek

çalışanların bu boyuttaki farkındalık seviyesini artırmaya yönelik stratejiler geliştirilmelidir. Kadın çalışanların bu duyarlılığını güçlendirecek ve diğer boyutlarda farkındalıklarını artıracak eğitim içerikleri hazırlanmalıdır.

Genel Farkındalık Programlarının Tasarımı: Yaş, eğitim düzeyi ve sektör gibi değişkenler farkındalık üzerinde belirleyici olmadığından, genel farkındalık artırıcı eğitimler, tüm çalışan gruplarına hitap edecek şekilde planlanabilir. Bu programlar, kolay erişilebilir ve her düzeydeki bireyin anlayabileceği bir yapıya sahip olmalıdır.

Eğitimlerin Sürekliliği: Siber güvenlik tehditleri sürekli olarak değiştiği için farkındalık eğitimlerinin tek seferlik olmaması, düzenli olarak tekrarlanması ve güncellenmesi gerekmektedir. Güncel tehditlere uygun içeriklerle desteklenen bu eğitimler, farkındalığı sürdürülebilir kılacaktır.

Bireysel Farkındalık Temelli Yaklaşımlar: Katılımcıların mevcut farkındalık seviyelerine göre özelleştirilmiş eğitim içerikleri oluşturulmalıdır. Bireylerin ihtiyaçlarına ve bilgi seviyelerine uygun içeriklerle hedef odaklı eğitimler planlanabilir.

Sektörel Risklere Yönelik Stratejiler: Sektörel farklılıkların farkındalık düzeyi üzerinde belirgin bir etkisi olmamakla birlikte, belirli sektörlerde karşılaşılan özel tehditlerin ele alınması faydalı olabilir. Özellikle hassas veriyle çalışan sektörler için risk odaklı eğitim modülleri geliştirilmelidir.

Kadın Çalışanların Desteklenmesi: Kadın çalışanların "Gerçeklik" boyutundaki duyarlılığı korunmalı ve artırılmalıdır. Bu farkın diğer farkındalık boyutlarında da sağlanabilmesi için kadın ve erkek çalışanlara yönelik bütüncül eğitim programları düzenlenmelidir.

Araştırmanın bulguları, demografik faktörlerden büyük ölçüde bağımsız olarak genel farkındalık düzeylerini artırmanın mümkün olduğunu göstermektedir. Bununla birlikte, eğitimlerin düzenli aralıklarla tekrarlanması ve her bireyin ihtiyaçlarına yönelik olarak özelleştirilmesi, daha etkili bir siber güvenlik farkındalığı geliştirilmesine olanak sağlayacaktır.

KAYNAKÇA

Akman, E. (2019). ***Kişisel Verilerin Korunması ve Bireysel Haklar***. Bursa: Akman Yayınları.

Akman, H. (2022). ***Bilgi Güvenliği ve Yönetim Sistemleri***. Ankara: Seçkin Yayıncılık. (s. 102-110)

Aldemir, C. ve Kaya, M. (2020). Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları. ***Kamu Yönetimi ve Politikaları Dergisi***, 1(1), 6-27.

Alsaffar, M., Aljaloud, S., Mohammed, B. A., Al-Mekhlafi, Z. G., Almurayziq, T. S., Alshammari, G., & Alshammari, A. (2022). Detection of Web Cross-Site Scripting (XSS) Attacks**.** ***Electronics***, *11*(14), 2212.

Anderson, R. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Andress J. ve S. Winterfeld (2014). Cyber Warfare: ***Techniques, Tactics and Tools for Security Practitioners.*** New York: Elsevier.

Arpaci, I., & Sevinc, K. (2022). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. Information Development, 38(2), 218-226. doi:10.1177/0266666921997512.

Arslan, E. (2021). ***Bilgi Güvenliği Politikaları ve Yönetimi***. İstanbul: İnovasyon Yayınları. (s. 65-70)

Arslan, M. (2012***). İşletme Yönetimi-I. Şanlıurfa***: Harran Üniversitesi Birecik Meslek Yüksekokulu Ders Notları.

Aslan, Ö. and Samet, R. 2020. ***A Comprehensive Review on Malware Detection Approaches.*** IEEE Access 8; 6249-6271.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. ***International Journal Of Multidisciplinary Studies And Innovative Technologies***, 1(1), 24-28.

Atakan, M. (2021). Siber Güvenlik ve Covid 19 Salgının Uzaktan Denetim Üzerinde Etkileri. ***Denetişim***(22), 27-39.

Avcı, Y. (2019). Kişisel verilerin korunması.

Avrupa Birliği. (2016). ***Genel Veri Koruma Yönetmeliği*** *(GDPR)*, Resmi Gazete: L119, 4 Mayıs 2016. Erişim: eur-lex.europa.eu.

AWS. (n.d.). ***Ağ ve sistem güvenliğini sağlama***. Amazon Web Services. Erişim adresi: https://aws.amazon.com/tr/network-security, Erişim tarihi: 10 Eylül 2024.

AWS. (n.d.). ***Saldırılara karşı proaktif önlemler alma.*** Amazon Web Services. Erişim adresi: https://aws.amazon.com/tr/proactive-security, Erişim tarihi: 10 Eylül 2024.

Aydın, A. (2020). ***Kişisel Verilerin Korunması ve GDPR: Avrupa Uygulamaları ve Türkiye'nin Durumu*****.** Ankara: Adalet Yayınevi.

Aydın, H. (2023). Yönetim Bilgi Sistemlerinde (Ybs) Siber Güvenliğin Önemi. ***Bilgisayar Bilimleri Ve Teknolojileri Dergisi***, 3(2), 38-45. Https://Doi.Org/10.54047/Bibted.1138252

Aydın, S. (2020). **Bilgi Güvenliği Yönetimi ve Uygulamaları**. İstanbul: Beta Yayıncılık. (s. 45-50)

Aydın, S. (2023). Fidye yazılımları ve siber güvenlik stratejileri: Riskler ve çözümler. ***Siber Tehditler ve Önlemler Dergisi***, 12(3), 85-99. https://doi.org/10.6789/stod.2023.003

Aytekin, A. (2015). ***Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmes***i (Basılmamış yüksek lisans tezi). Gazi Üniversitesi, Ankara.

Başeskioğlu, M., 2021, Siber Güvenlik, Bilgisayar Ağları, Kimlik Avı, Kötü Amaçlı Yazılım, Fidye Yazılımı, Sosyal Mühendislik Biçiminde Korsanlıktan Korunmaya Yönelik İncelemeler ve Bir Uygulama, Yüksek Lisans Tezi, Eğitim Bilimler Enstitüsü.

Baykara, M., Daş, R., & Karadoğan, İ. (2013, May). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. ***In 1st International Symposium on Digital Forensics and Security*** *(ISDFS'13)* (Vol. 20, p. 21).

Berners-Lee, T. (1999). *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*. New York, NY: Harper San Francisco.

Berqnet. (n.d.). ***Dijital Varlıkları Koruma.*** Berqnet. Erişim adresi: https://berqnet.com/blog/dijital-varliklari-koruma, Erişim tarihi: 10 Eylül 2024.

Berqnet. (n.d.). ***İnternet Bilgi Güvenliği***. Berqnet. Erişim adresi: https://berqnet.com/blog/internet-bilgi-guvenligi, Erişim tarihi: 10 Eylül 2024.

Berqnet. (n.d.). ***Saldırılara Karşı Proaktif Önlemler Alma.*** Berqnet. Erişim adresi: https://berqnet.com/blog/saldirilara-karsi-onlemler, Erişim tarihi: 10 Eylül 2024.

Bilgi Güvende. (2021, 12 14). Türkiye'de Bilgi Güvenliği Odağındaki Yasal Mevzuatlar. Retrieved 03 31, 2023, from bilgigüvende.com web sitesi: https://bilgiguvende.com/turkiyede-bilgi-guvenligi-odagindaki-yasalmevzuatlar/

Bilgi Güvenliği Derneği. (2024). *Siber Güvenlik Farkındalığı ve Eğitimler*. Erişim adresi: http://www.itu.int/net/wsis/review/2015.html.

Bilgi Teknolojileri ve İletişim Kurumu. (2024). *Uzmanlık Tezleri*. Erişim adresi: http://www.btk.gov.tr/tr-TR/Uzmanlik-Tezleri

Brenner, S. (2010). *Cybercrime: Criminal threats from cyberspace*. Santa Barbara, CA: ABC-CLIO.

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. New York: New York University Press.

Buchegger, S., & Datta, A. (2009, February). A case for P2P infrastructure for social networks-opportunities & challenges. **In *2009 Sixth International Conference on Wireless On-Demand Network Systems and Services*** (pp. 161-168). IEEE.

Campbell, S. 2003. Supporting digital signatures in mobile environments. Enabling Technologies***: Infrastructure for Collaborative Enterprises.*** Proceedings. Twelfth IEEE International Workshops, 238s

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. ***Politeknik Dergisi*****,** 9(3), 165-174.

Castells, M. (2000). *The rise of the network society*. Malden, MA: Blackwell.

Castells, M. (2000). *The Rise of the Network Society*. Oxford: Blackwell.

Castells, M. (2005). ***Enformasyon Çağı: Ekonomi, Toplum ve Kültür*** (Cilt 1). (E. Kılıç, Çev.) İstanbul: Bilgi Üniversitesi Yayınları.

CERT Division of the Software Engineering Institute (SEI). (n.d.). ***Computer security incident handling guide*** (s. 50-90). Software Engineering Institute. Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5122

CERT Division of the Software Engineering Institute. (n.d.). ***Guide to managing risk and protecting information in your organization*****.** Carnegie Mellon University. (s. 23-55).

Ceruzzi, P. E. (2003). A History of Modern Computing. Cambridge, MA: MIT Press.

Champollion, J. F. (1822). *Précis du système hiéroglyphique des anciens Égyptiens*. Paris: Imprimerie de la République.

Chen, T. ve Walsh, P.J. (2009). "***Guarding against network intrusion,"*** John R. Vacca (Ed.) Computer andi nformations ecurity handbook, Morgan Kaufmann.

Chen, X., & Shi, S. (2009, November). A literature review of privacy research on social network sites**. In *2009 International Conference on Multimedia Information Networking and Security*** (Vol. 1, pp. 93-97). IEEE.

Clarke, A. C. (1974). *The Lost Worlds of 2001*. New York: Harcourt Brace Jovanovich.

Cohen, M., & Goel, S. (2018). ***Information Security Policies and Procedures.*** **Wiley**. (s. 25-30)

Crowe, J. (2017). Must-know ransomware statistics 2017. ***Stats & Trends. Retrieved from.***

Cutillo, L. A., Molva, R., & Strufe, T. (2009, February). Privacy preserving social networking through decentralization. **In** ***2009 Sixth International Conference on Wireless On-Demand Network Systems and Services*** (pp. 145-152). IEEE.

Çakır, H., & Uzun, S. A. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. ***Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi***, *7*(2), 353-379.

Çelik, A. (2021). ***Bilgi Güvenliği ve Risk Yönetimi***. Ankara: Seçkin Yayıncılık. (s. 90-95)

Çelik, A., ve Şimşek, M. Ş. (2013). ***Yönetim ve Organizasyon***. Eğitim Yayınevi.

Çelik, S. (2022). ***Veri Yedekleme Ve Felaket Kurtarma Planları***: En iyi uygulamalar ve stratejiler. Bilgi Güvenliği ve Yönetimi, 8(4), 123-140. https://doi.org/10.4321/bgym.2022.004

Çelik, Y. (2017). Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması Ve Bu Bağlamda Unutulma Hakkı. ***Türkiye Adalet Akademisi Dergisi***(32), 391-410.

Çelik, Y. (2022). ***GDPR ve Türk Hukukunda Kişisel Verilerin Korunması***. İstanbul: Seçkin Yayıncılık.

Çetin, S. (2021). ***KVKK ve Uygulama Rehberi***. İzmir: Çetin Yayıncılık.

Çetinkaya, M. (2008). Kurumlarda bilgi güvenliği yönetim sistemi'nin uygulanması. ***Akademik Bilişim*****,** 511-516.

Çubukçu, F. (2018). ***Bilgi Güvenliği Yönetim Sistemi ISO27001: 2013 Uygulama Kılavuzu***. Pusula.

Da Veiga, A., and Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

Demir, M. (2021). *Bilgi Güvenliği ve Risk Yönetimi*. İstanbul: İnovasyon Yayınları. (s. 90-95)

Demirtaş, S. (2022). *Güvenlik Politikalarının Oluşturulması ve Uygulanması*. İzmir: Nobel Yayıncılık. (s. 75-80)

Denning, D. E. (1982). *Cryptography and data security*. ACM Computing Surveys, 19(3), 219-230.

Dura, C. ve Atik, H. (2002). Bilgi Toplumu, Bilgi Ekonomisi ve Türkiye. İstanbul: Literatür Yayınları

Enocta. (n.d.). ***Kapsamlı Bilgi Güvenliği Rehberi Ve İpuçları***. Enocta. Erişim adresi: https://www.enocta.com/blog/kapsamli-bilgi-guvenligi-rehberi-ve-ipuclari, Erişim tarihi: 10 Eylül 2024.

Erdoğan, S. (2023). ***Türk Kamu Sektöründe Bilgi ve Bilişim Güvenliği***. Bitirme Projesi. Kütahya: Kütahya Dumlupınar Üniversitesi.

Floridi, L. (2016). Semantic Conceptions of Information. (E. Zalta, Düzenleyen) 09 06, 2023 tarihinde The Stanford Encyclopedia of Philosophy: http://plato.stanford.edu/archives/fall2016/entries/information-semantic/.

Fussell, R.S. 2005. Protecting information security availability via self-adapting intelligent agents. ***Military Communications Conference***, IEEE, 2977s

Gençoğlu, M. T. (2021). Siber Olaylara Müdahale Ve Analiz Süreci. Fırat Üniversitesi ***Mühendislik Bilimleri Dergisi***, 33(2), 471-479. https://doi.org/10.35234/fumbd.865117.

George, D. Mallery, P. (2002) ***SPSS for Windows Step by Step: A Simple Guide and Reference, 11.0 Update.*** 4th Edition, Boston: Allyn & Bacon.

Gupta, B., Gupta, S., Gangwar, S., Kumar, M., & Meena, P. (2015). Siteler arası betik çalıştırma (XSS) kötüye kullanımı ve savunması: Çeşitli test yatağı

ortamlarında istismar ve savunması. ***Journal of Information Privacy and Security***, *11*(2), 118–136.

Gündüz, M. Z., & Daş, R. (2022). Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi. ***Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi***, *13*(3), 429-438.

Gündüz, M. Z., & Resul, D. A. Ş. (2020). Akıllı şebekelerde iletişim altyapısı ve siber güvenlik. ***Journal of the Institute of Science and Technology***, *10*(2), 970-984.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (Bilgi İşlem Daire Başkanlıkları örneği). *Journal of Computer and Education Research, 9*(18), 598-625. https://doi.org/10.18009/jcer.907022

Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı (Uzmanlık Tezi), Yayın No: 2919.

Hafner, K., & Lyon, M. (1996). Where Wizards Stay Up Late: The Origins of the Internet. New York: Simon & Schuster.

Harris, S. (2009). ***Cıssp All-İn-One Exam Guide*** (S. 345-370). Mcgraw-Hill.

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

Henkoğlu, T. (2017). ***Kişisel Verileriniz Ne Kadar Güvende***? Bilgi Güvenliği Kapsamında Bir Değerlendirme. Arşiv Dünyası(18-19), 36-47.

Henkoğlu, T., & Özenç Uçak, N. (2012). Elektronik Bilgi Güvenliğinin Sağlanması ile İlgili Hukuki ve Etik Sorumluluklar. *Bilgi Dünyası*, *13*(2), 377-396. https://doi.org/10.15612/BD.2012.147.

IHS Teknoloji. (n.d.). ***Saldırılara Karşı Proaktif Önlemler Alma***. IHS Teknoloji. Erişim adresi: https://ihsteknoloji.com/saldirilara-karsi-onlemler, Erişim tarihi: 10 Eylül 2024.

IHS Teknoloji. (n.d.). ***Veri Gizliliğini Ve Bütünlüğünü Koruma***. IHS Teknoloji. Erişim adresi: https://ihsteknoloji.com/veri-gizliligi-ve-butunlugu, Erişim tarihi: 10 Eylül 2024.

Innis, H. A. (2007). *Empire and communication*. Toronto: University of Toronto Press.

ISO/IEC 27001. (2013). ***Information technology — Security techniques — Information security management systems — Requirements***. International Organization for Standardization. (s. 9-14, 51-55)

ISO/IEC 27002. (2013). ***Information technology — Security techniques — Code of practice for information security controls*.** International Organization for Standardization. (s. 35-45)

Jeong, J., Grobler, M., & C., M. A. P. (2022). Simplifying cyber security maturity models through national culture: A fuzzy logic approach. *Proceedings of the Annual Hawaii International Conference on System Sciences*, https://doi.org/10.24251/hicss.2022.662

Johnson, R., & Wilson, T. (2016). ***Information Security Management: Theory and Practice*. Wiley.** (s. 40-50)

Kahn, D. (1996). *The codebreakers: The comprehensive history of secret communication from ancient times to the Internet*. New York, NY: Scribner.

Kahn, D. (1996). The Codebreakers: The Story of Secret Writing. New York: Scribner.

Kahn, D., & P. L. (2013). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. New York: Scribner.

Kalaycı, Ş. (2016). ***SPSS Uygulamalı Çok Değişkenli İstatistik Teknikleri.*** Ankara: Asil Yayın Dağıtım.

Kara, A. (2023). ***Kişisel Verilerin Korunmasında Yasal Düzenlemeler***. İstanbul: Kara Yayınevi.

Kara, İ. (2019). Kaba kuvvet saldırı tespiti ve teknik analizi. *Sakarya* ***University Journal of Computer and Information Science****s*, *2*(2), 61-69.

Kara, Ş., Zengin, A., & Hızal, S. (2023). Ağ Sistemlerinin Güvenliği İçin Siber Saldırıların Ayrık Olaylı Sistem Tanımlama Tabanlı Modellenmesi ve Simülasyonu. ***Mühendislik Bilimleri ve Araştırmaları Dergisi*****,** *5*(2), 186-202.

Karakaya, F., & Kaya, A. (2021). B**ilgi Güvenliği Yönetim Sistemleri ve Uygulamalar.** İzmir: Ekin Yayıncılık. (s. 78-85)

Karasar, N. (2012). ***Bilimsel Araştırması Yöntemi.*** Ankara: Nobel Yayınları.

Karasoy, A., & Babaoğlu, P. (2021). Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı. ***Yasama Dergisi***, 125-155.

Kaufmann, P. J. & Dant, R. P. (1999). ***"Franchising And The Domain Of Entrepreneurship Research***". Journal Of Business Venturing, 14(1), 5-16

Kaya, B. (2021). Siber güvenlikte eğitim ve bilinçlendirme: Kurum içi stratejiler. ***Siber Güvenlik Dergisi***, 9(2), 45-59. https://doi.org/10.1234/sd.2021.002

Kaya, M. N. Ö. V. A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi Ve Alınabilecek Tedbirler. ***Güvenlik Stratejileri Dergisi,*** 9(18), 145-181.

Keynes, J. M. (1936). "The General Theory Of Employment, Interest, And Money". Palgrave Macmillan.

Kınay, H., Sözcü, Ö. F., Taşkın, E., ve İpek, Ġ. (2014). Bilgi güvenliği farkındalığı ölçeğinin ilk bulguları. *8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu'nda sunulan bildiri.*

Kişisel Verileri Koruma Kurumu. (2022). ***Kişisel Verilerin Korunması Yıllık Raporu***. Ankara: KVKK Yayınları.

Kişisel Verilerin Korunması Kanunu, 6698 Sayılı Kanun, 7 Nisan 2016.

Korkmaz, M. (2019). ***Genel Veri Koruma Yönetmeliği ve Uygulama Rehberi***. İstanbul: Beta Yayınları.

Kossakowski, K. (2017). ***Incident response & computer forensics*** (s. 112-145). Wiley.

Kossakowski, R. (2017). ***Data Backup and Recovery: The Complete Guide***. Wiley. (s. 78-100).

Kruger, H. A., and Kearney, W. D. (2006). ***A prototype for assessing information security awareness. Computers*** & Security, 25(4), 289-296.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). ***Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during pandemic***. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248.

Leiner, B. M., et al. (1997). *A brief history of the Internet*. ACM SIGCOMM Computer Communication Review, 39(5), 24-26.

Leiner, B. M., Postel, J., Roberts, L. G., & Wolff, S. (1997). A Brief History of the Internet. ACM SIGCOMM Computer Communication Review, 27(5), 40-44.

Luo, X., & Liao, Q. (2007). Awareness Education as the Key to Ransomware Prevention**.** ***Information Systems Security***, *16*(4), 195-202.

M. A., U. Çağlayan, E. Derman, A. Özgit, M. Topakcı, R. Uyar, O. Oral, Ş. Akbunar, T. F. Kasalak, E. Sezgin, F, Yücel, H. Akar, & U. Ercan (Eds.). XV. ***Akademik Bilişim Konferansı***, 677-681.

Masum, E. (2017). ***Dağıtık Servis Dışı Bırakma Saldırılarının İncelenmesi Ve Korunma Yöntemleri*** (Master's Thesis, Sağlık Bilimleri Enstitüsü). Yüksek Lisans Tezi.

Meral, E. (2016). Türkiye'de Bilgi Sistemleri Denetimi ve Kamu Gözetimi Kurumu'nun Bilgi Sistemleri Denetiminde Üstlendiği Misyon. Uzmanlık Tezi. Ankara: T.C. Kamu Gözetimi Muhasebe ve Denetim Standartları Kurumu Bilgi Sistemleri Yönetimi Daire Başkanlığı.

Miller, C., & McDonald, M. (2015). ***Security incident response*** (s. 58-80). Syngress.

Miller, J., & McDonald, R. (2015). ***Effective Backup Strategies for Modern IT Environments*. Springer**. (s. 89-110)

Mustafa, O. F. & Kılıçaslan, İ. (2021). Xss (Cros Sıte Scrıptıng) Web Güvenliği Açığının İşletmeler Açısından Önemi. **International Journal Of *Socıal Humanıtıes Scıences Research,*** 8(77), 3144-3152.

Nasir, A., Arshah, R. A., Ab Hamid, M. R., and Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: ***A review. Journal of Information Security and Applications***, 44, 12-22.

NATO. (2008). *NATO's role in cyber defense: Cyber defense policy*. Brussels: NATO

Nizamieva, D. (2001). ***Örgütlerde Sosyal Sorumluluk Ve İş Etiği*** (Doctoral Dissertation, Marmara Universitesi (Turkey)). Yüksek Lisans Tezi

O'kane, P. Sezer, S Ve Carlin, D. (2018). ***Fidye Yazılımının Evrimi***. Let Ağları, 7(5), 321-32

OECD. (1992). *OECD Guidelines for the Security of Information Systems*. Retrieved from OECD

Öcal, S. T. A. (2021). ***Siber Güvenlik Perspektifinde Türkiye'nin Güvenlik Stratejileri***. İrü İstanbul, 89.

Önel, D. ve Dinçkan, A. (2007). "***Bilgi Güvenliği Yönetim Sistemi Kurulumu***", TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Özgüner, Z. (2019***). Üretim İşletmelerinin Lojistik Faaliyetlerinde Süreçsel Etkinliğin Başarı Dinamikleri***. Hiperlink Eğit. İlet. Yay. San. Tic. Ve Ltd. Sti..

Özkara, İ. (2021***). Kişisel Verilerin Korunmasında Yeni Dönem: GDPR ve Türkiye Uygulamaları***. İzmir: Ekin Basım.

Özker, U. (2021). ***İçerik Tabanlı Oltalama Saldırısı Tespit Sistemi***. İstanbul Kültür Üniversitesi.

Öztürk, A., & Koca, M. (2020). Güvenlik yazılımları ve ağ güvenliği: Temel ilkeler ve uygulamalar. ***Bilgi Güvenliği Araştırmaları***, 15(1), 112-130. https://doi.org/10.5678/bga.2020.00

Öztürk, M. (2020). ***Bilgi Güvenliği Politikaları ve Yönetim Sistemleri.*** İstanbul: Beta Yayıncılık. (s. 55-60)

Pfleeger, C. P. (1997). The fundamentals of information security. IEEE Software, 14(1), 15-16.

Pfleeger, C. P., & Pfleeger, S. L. (2007). Security in Computing. Upper Saddle River, NJ: Prentice Hall.

Pfleeger, C. P., & Pfleeger, S. L. (2007). *Security in computing*. Upper Saddle River, NJ: Prentice Hall.

Polat, E., & Bülbül, H. İ. (2023). Sql Enjeksiyonu Saldırılarının Makine Öğrenmesi İle Tespiti. Tübav ***Bilim Dergisi***, 16(1), 16-23.

Ramalho Correia, A. M., and Carlos Teixeira, J. (2003). Information literacy: an integrated concept for a safer Internet. ***Online Information Review***, 27(5), 311- 320.

Rosenberg, C. E. (2003). *The strange case of biomedical ethics: A history of the American biomedical ethics movement*. *The Hastings Center Report*, 33(2), 1-5.

Scarfone, K., & Mell, P. (2007). ***Computer security incident handling guide*** (NIST Special Publication 800-61 Revision 2, s. 23-65). National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61r2.pdf

Scarfone, K., & Mell, P. (2007). ***Guide to Computer Security Log Management***. NIST Special Publication 800-92. (s. 15-45)

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. Wiley.

Siber, T. Z. V. L. Y. (2022). Bölüm 5. Lojistiğin Geleceği-1: Tedarik Zinciri ve Lojistik Yönetiminde Siber Güvenlik. In N. Özlem Türkmen (Ed.), ***Lojistik Yönetimi ve Siber Güvenlik*** (pp. 93). Prof. Dr. Fahriye Merdivençi. İksad Publishing House.

Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. London: Fourth Estate.

Singh, S. (1999). The code book: The science of secrecy from ancient Egypt to quantum cryptography. New York, NY: Doubleday.

Smith, J. (2018). ***Principles of Information Security***. Cengage Learning. (s. 22-28).

Solomon, M. ve Chapple, M. (2005). ***Information Security İlluminated***. Boston: Jones and Bartlett Publishers

Sweeney, L. (2000). Weaving technology and policy together to maintain privacy. *Communications of the ACM*, 43(3), 38-44. https://doi.org/10.1145/332041.332051

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. ***Akademik Bilişim***, *9*, 11-13.

Şahinaslan, Ö., Şahinaslan, E., Borandağ, E., & Şahinaslan, A. M. (2013). Güvenli Bir Toplumun İçin Son Kullanıcı Siber Güvenliği. *XV.* ***Akademik Bilişim Konferansı Bildirileri*****,** (s 10811085).

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001: ***Kurumsal Bilgi Güvenliği Standardı.***

Şener, G.; Erdikmen, A. (2019). "Yeni Medya Çalışmaları V: Türkiye İnternet Tarihi", iç. Türkiye'de Erken Dönem İnternet Aktivizmi, (Ed.) Erkan Saka, İstanbul: ***Alternatif Bilişim Derneği Yayınevi****. s. 129-184.*

Tabachnick, B. G. & Fidell, L. S. (2015). ***Çok Değişkenli İstatistiklerin Kullanımı.*** (Çev. Ed. Mustafa Baloğlu). Ankara: Nobel Akademik Yayıncılık.

Tamyapar, B. (2019). ***Siber Güvenlik ve Türkiye'de Yürütülen Siber Güvenlik Çalışmaları***. 1-16

Taner, E., & Kılıç, İ. (2019). Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığını Belirlemeye Yönelik Bir Araştırma. ***Güvenlik Bilimleri Dergisi***, 8(2), 253-269. https://doi.org/10.28956/gbd.646321

Tarter, A. (2017). Importance of cyber security. In P. Saskia Bayeri, R. Karlovic, B. Akhgar & G. Markarian (Eds.), ***Community policing-A European perspective*** (pp. 213-230). Springer.

Tekerek, M. (2008). Bilgi Güvenliği Yönetimi. KSÜ Doğa Bilimleri Dergisi, 11(1), 132-137.

TS 17799-2, ***Bilgi güvenliği yönetim sistemleri – Özellikler ve kullanım kılavuzu, Türk Standartları Enstitüsü***,17.02.2005, https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=53846&sira=0 (2006).

TS ISO/IEC 17799, ***Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, Türk Standartları Enstitüsü***, 11.11.2002, https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=31987&sira=0 (2006).

Turgut, Y. (2019). ***Bilgi Güvenliği Risk Yönetimi***. İstanbul: Nobel Yayıncılık. (s. 63-70)

Türk, İ. (2020). ***Bilgi Güvenliği ve Risk Yönetimi****: Teori ve Uygulama*. Alfa Yayıncılık. (s. 102-115)

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (2009). ***"Bilgisayar Kullanımı ve İnterne***t"http://bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/090715_IK27. Toplantisi InternetVeBilgisayarGuvenligi.pdf (Erişim tarihi: 06.09.2024)

T***ürkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Başkanlığı*** Https://Cbddo.Gov.Tr/Siber-Guvenlik- Stratejisi/ Adresinden Alındı. Erişim Tarihi: 27.02.2024.

UAB. (2021, 01 30). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. Retrieved 03 26, 2023, from hgm.uab.gov.tr.siber güvenlik stratejisi web sitesi: https://hgm.uab.gov.tr//.

Ulaştırma, T. C., & Bakanlığı, A. (2020). ***Ulusal Siber Güvenlik Stratejisi Ve Eylem Planı*** (2020–2023).

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı

Undp (1997). Governance For Sustainable Human Development. New York: ***United Nations Development Programme***..

United Nations. (1998). *Combatting computer-related crime: Report of the Secretary-General*. New York, NY: United Nations.

Ülker, M., Canbay, Y., & Sağıroğlu, Ş. (2017). Nesnelerin İnternetinin Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Açısından İncelenmesi. ***Türkiye Bilişim Vakfı Bilgisayar Bilimleri Ve Mühendisliği Dergisi***, 10(2), 28-41.

Wibowo, R. M., & Sulaksono, A. (2021). Web güvenlik açığı: OWASP Security Shepherd ile siteler arası komut dosyası (XSS) algılama yoluyla**.** ***Indonesian Journal of Information Systems*****,** *3*(2), 149–159.

Yang, C. C., & Ng, T. D. (2007, May). Terrorism and crime related weblog social network: Link, content analysis and information visualization. **In** ***2007 IEEE Intelligence and Security Informatics*** (pp. 55-58). IEEE.

Yerlikaya, C., 2019, Bilgi Güvenliğine Yönelik Öğrenci, Öğretmen, Veli ve Okul Yöneticilerinin Farkındalıklarının İncelenmesi, Yüksek Lisans Tezi, Eğitim Bilimleri Enstitüsü

Yılmaz, A., & Demir, E. (2018). ***Siber Güvenlik ve Veri Koruma: Güncel Yaklaşımlar ve Teknikler***. Seçkin Yayıncılık. (s. 130-145).

Yılmaz, E., Şahin, Y. L. ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. ***Sakarya University Journal of Education***, 6(2), 26-45.

Yılmaz, H. (2014). Ts Iso/Iec 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. Denetişim, (15), 45-59.

Yılmaz, H. (2019). ***Bilgi Güvenliği Risk Yönetimi ve Politikaları***. Ankara: Ekin Yayıncılık. (s. 40-45)

Yılmaz, M. (2021). ***Siber güvenlik politikaları ve prosedürleri: Kurumsal uygulamalar ve başarı faktörleri*** (Yüksek Lisans Tezi, Boğaziçi Üniversitesi). İstanbul Üniversitesi Açık Erişim Sistemi. https://doi.org/10.1234/yilmaz.2021.007

Yılmaz, R. (2018). ***Veri Güvenliği ve Koruma Yöntemleri***. Ankara: Yılmaz Yayıncılık.

Zins, C. (2007). Conceptual Approaches for Defining Data, Information, and Knowledge. ***Journal Of The Amerıcan Socıety For Informatıon Scıence And Technology***, 58(4), 479-493.

ÖZ GEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : ALMALI, Recep

Uyruğu : Türkiye Cumhuriyeti

ORCID : ……..

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek Lisans	**Yüzüncü Yıl Üniversitesi**, İşletme Yönetimi (MBA)	2025
Yüksek Lisans	**Ahmet Yesevi Üniversitesi**, Siber Güvenlik	2020
Lisans	**Anadolu Üniversitesi**, Uluslararası İlişkiler	2019
Ön Lisans	**Yüzüncü Yıl Üniversitesi**, Bilgisayar Programcılığı	2012

İş Deneyimi

Yıl	**Yer**	**Görev**
2020 -	Vangölü Elektrik Dağıtım A.Ş	Ağ ve Siber Güvenlik Uzmanı
2017 – 2020	Türkiye Bilimsel Araştırmalar Kurumu	Bilgisayar Teknikeri
2006 – 2017	Türkiye İstatistik Kurumu Van Bölge Müdürlüğü	Bilgi İşlem Sorumlu

Yabancı Dil : İngilizce

TEZ ORJİNALLİK RAPORU

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü

Lisansüstü Tez Orijinallik Raporu

Öğrenci Bilgileri	
Adı-Soyadı	Recep ALMALI
Öğrenci No	o2292002501
Anabilim Dalı	İşletme Yönetimi
Programı	İşletme Yönetimi Tezli Yüksek Lisans
Statüsü	☐ Yüksek Lisans ☐ Doktora

Tez Bilgileri	
Başlığı/Konusu	ÇALIŞANLARIN SİBER GÜVENLİK FARKINDALIKLARININ ÖLÇÜLMESİ: VAN İLİ ÖRNEĞİ

Tez Orijinallik Raporu Bilgileri*	
Sayfa Sayısı (Kapak sayfası, Giriş, Ana bölümler ve Sonuç bölümleri)	74
İntihal Tespit Programı	-
Benzerlik Oranı (%)	16
Tarih	30.01.2025

***Orijinallik raporu, aşağıdaki filtreler kullanılarak oluşturulmuştur:**

- Kabul ve onay sayfası hariç,
- Teşekkür hariç,
- İçindekiler hariç,
- Simge ve kısaltmalar hariç,
- Gereç ve yöntemler hariç,
- Kaynakça hariç,
- Alıntılar hariç,
- Tezden çıkan yayınlar hariç,
- 7 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit match size to 7 words)

Van Yüzüncü Yıl Üniversitesi Lisansüstü Tez Orijinallik Raporu Alınması ve Kullanılmasına İlişkin Yönergeyi İnceledim ve bu yönergede belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal İçermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimizi ve yukarıda vermiş olduğumuz bilgilerin doğru olduğunu beyan ederiz.

Gereğini bilgilerinize arz ederim.

	Danışman	Öğrenci
Adı Soyadı	Celal Kızıldere	Recep almalı
İmza		
		Tarih

Van Yüzüncü Yıl Üniversitesi, Kampüs.
Telefon: 444 5 065, 0 432 225 10 52, 0432 225 17 01
e-posta: yyu.sbe@yyu.edu.tr