



T.C.

Ardahan Üniversitesi

Lisansüstü Eğitim Enstitüsü

İleri Teknolojiler Ana Bilim Dalı

İleri Teknolojiler Bilim Dalı

KAMU PERSONELİNİN SİBER GÜVENLİK FARKINDALIĞININ TESPİTİ

Barış DAŞDEMİR

Dr. Öğr. Üyesi Salih Serkan KALELİ

Yüksek Lisans Tezi

Ardahan, 2024

KAMU PERSONELİNİN SİBER GÜVENLİK FARKINDALIĞININ TESPİTİ

Barış DAŞDEMİR

Dr. Öğr. Üyesi Salih Serkan KALELİ

Ardahan Üniversitesi Lisansüstü Eğitim Enstitüsü

İleri Teknolojiler Ana Bilim Dalı

İleri Teknolojiler Bilim Dalı

Yüksek Lisans Tezi

Ardahan, 2024

KABUL VE ONAY

Barış DAŞDEMİR tarafından hazırlanan “Kamu Personelinin Siber Güvenlik Farkındalığının Tespiti” başlıklı bu çalışma, 26.06.2024 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Doç. Dr. Mehmet BAYĞIN (Başkan)

Dr. Öğr. Üyesi Salih Serkan KALELİ (Danışman)

Dr. Öğr. Üyesi Nihat Emre BÖREKÇİ

Bu tez, Enstitü Yönetim Kurulunca belirlenen ve yukarıda adları yazılı jüri üyeleri tarafından kabul edilmiştir.

Prof. Dr. Mustafa ŞENEL
Enstitü Müdürü

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Ardahan Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan **“Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge”** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / Ardahan Üniversitesi Açık Erişim Sisteminde erişime açılır.

Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. ⁽¹⁾

Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ay ertelenmiştir. ⁽²⁾

Tezimle ilgili gizlilik kararı verilmiştir. ⁽³⁾

26.06.2024

Barış DAŞDEMİR

“Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge”

*Madde 6. 1. Lisansüstü teze ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

*Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez **danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulunun** gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

*Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı, **tezin yapıldığı kurum** tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise, **ilgili kurum ve kuruluşun önerisi** ile **enstitü** veya **fakültenin** uygun görüşü üzerine **üniversite yönetim kurulu** tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*

Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

** **Tez danışmanının** önerisi ve **enstitü anabilim dalının** uygun görüşü üzerine **enstitü** veya **fakülte yönetim kurulu** tarafından karar verilir.*

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, Tez Danışmanının Dr. Öğr. Üyesi Salih Serkan KALELİ danışmanlığında tarafımdan üretildiğini ve Ardahan Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

Barış DAŞDEMİR

ÖN SÖZ

Bu çalışmanın gerçekleştirilmesinde, değerli bilgilerini benimle paylaşan, kendisine ne zaman danışsam bana kıymetli zamanını ayırıp sabırla ve büyük bir ilgiyle bana faydalı olabilmek için elinden gelenden fazlasını sunan, güler yüzünü ve samimiyetini benden esirgemeyen ve gelecekteki mesleki hayatımda da bana verdiği değerli bilgilerden faydalanacağımı düşündüğüm kıymetli ve danışman hoca statüsünü hakkıyla yerine getiren Dr. Öğr. Üyesi Salih Serkan KALELİ 'ye teşekkürü bir borç biliyor ve şükranlarımı sunuyorum.

Yine Yüksek lisans ders sürecimde ve tez aşamasında bana verdiği destekleri bilgileri güler yüzü için kıymetli hocam Doç. Dr. Mehmet BAYĞIN'a sonsuz teşekkürlerimi sunarım.

Araştırmamda gerekli olan veri toplama ve anket çalışmaları için gerekli izinleri veren eğitimin kurum mevki yer zaman fark etmeksizin ne kadar önemli ve değerli olduğunu her defasında bize hissettiren kıymetli İl Emniyet Müdürümüz Sayın Gökalp ŞENER'e, Şube Müdürüm Semih DUMANOĞLU'na ve desteklerini ve yardımlarını esirgemeyen tüm mesai arkadaşlarıma sonsuz teşekkürü bir borç biliyor ve saygılarımı sunuyorum.

Çalışmam boyunca benden bir an olsun yardımlarını esirgemeyen çalışma süresince tüm zorlukları benimle göğüsleyen ve hayatımın her evresinde bana destek olan değerli eşim Aslı Türk DAŞDEMİR'e sonsuz teşekkürlerimi sunarım.

Barış DAŞDEMİR

Ardahan-2024

ÖZET

DAŞDEMİR, Barış. *Kamu Personelinin Siber Güvenlik Farkındalığının Tespiti*, Yüksek Lisans, Ardahan, 2024.

Bu tez çalışmasının temel amacı, kamu personelinin siber güvenlik farkındalık düzeylerinin belirlenmesi ve bu alandaki pratik uygulamalarının değerlendirilmesidir. Araştırma, toplam 302 kamu personeli katılımcı ile yürütülmüş olup, Siber Güvenlik Ölçeği (SGÖ) kullanılarak altı farklı boyut (gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda) üzerinden bir analiz gerçekleştirilmiştir. Çalışmada elde edilen verilerin analizi için IBM SPSS 28 ve AMOS 24 istatistik paket programından faydalanılmış ve veri seti üzerinde çeşitli istatistiksel testler uygulanmıştır. Araştırmanın güvenilirlik ve geçerlilik düzeyini artırmak amacıyla tanımlayıcı istatistikler yardımıyla frekans ve çapraz tablolar analizi yapılmış, kategorik parametreler için sayı ve yüzdelik değerler, sayısal değişkenler için ise ortalama, standart sapma, minimum ve maksimum değerler dikkate alınmıştır. Sayısal değişkenlerin dağılım özelliklerini değerlendirmek üzere normallik varsayımları çarpıklık ve basıklık değerleri ile incelenmiştir. Elde edilen bulgular, verilerin normal bir dağılım gösterdiğini ortaya koymuştur.

Araştırma bulguları, kamu personelinin genel olarak siber güvenlik farkındalık düzeylerinin yeterli olduğunu, ancak fayda boyutunda daha fazla bilinçlendirme çalışmasına ihtiyaç duyulduğunu göstermektedir. Katılımcıların büyük çoğunluğunun erkek ve 26-35 yaş aralığında olduğu tespit edilmiştir. Eğitim düzeyi olarak çoğunluğun lisans mezunu olduğu ve mesleki sürelerinin genellikle 6-10 yıl arasında değiştiği belirlenmiştir. Katılımcıların günlük internet kullanım süreleri incelendiğinde, yarısından fazlasının günde 3-4 saat internet kullandığı ve mobil bankacılık, e-devlet hizmetleri ve e-ticaret amaçlarıyla interneti yoğun olarak kullandığı görülmüştür. Cinsiyetin siber güvenlik davranışları üzerindeki etkisi incelendiğinde, erkek katılımcıların daha aktif bir şekilde siber güvenlik önlemleri aldığı ve bu konudaki eğitimlere daha sık katıldığı belirlenmiştir. Faktör analizi sonuçları, ölçeğin altı boyutlu yapısının veri seti ile uyumlu olduğunu ve öngörülen kuramsal altyapıyı doğru bir şekilde yansıttığını ortaya koymaktadır. Güvenirlilik analizlerinde Cronbach Alpha katsayısının arzu edilen düzeyde (0,7 ve üzeri) olduğu tespit edilmiştir. Sonuç olarak, kamu personelinin siber güvenlik farkındalık düzeylerinin genel olarak yeterli olduğu ancak belirli boyutlarda (özellikle

fayda boyutu) daha fazla bilinçlendirme çalışmalarının yapılması gerektiği anlaşılmaktadır. Araştırma sonucunda, siber güvenlik eğitim programlarının ve politikalarının geliştirilmesine katkı sağlayarak, kamu personelinin siber güvenlik farkındalığını artırmaya yönelik stratejilerin oluşturulmasına yardımcı olacağı değerlendirilmektedir.

Anahtar Kelimeler:

Siber, Güvenlik, Siber güvenlik farkındalığı, Kamu Personeli.



ABSTRACT

DAŞDEMİR, Barış. *Determination of Cyber Security Awareness of Public Personnel*, Post Graduate, Ardahan, 2024

The main purpose of this thesis is to determine the cyber security awareness levels of public personnel and to evaluate their practical applications in this field. The research was conducted with a total of 302 public personnel participants and an analysis was conducted on six different dimensions (confidentiality, control/ownership, integrity, authenticity, accessibility and utility) using the Cyber Security Scale (CSS). IBM SPSS 28 statistical package program was used to analyze the data obtained in the study and various statistical tests were applied on the data set. In order to increase the reliability and validity of the research, frequency and cross-tabular analysis were performed with the help of descriptive statistics, number and percentage values for categorical parameters, and mean, standard deviation, minimum and maximum values for numerical variables. In order to evaluate the distribution characteristics of the numerical variables, normality assumptions were examined with skewness and kurtosis values. The findings revealed that the data showed a normal distribution.

The findings of the research show that the cyber security awareness levels of public personnel are generally sufficient, but more awareness-raising activities are needed in the benefit dimension. It was determined that the majority of the participants were male and between the ages of 26-35. In terms of education level, it was determined that the majority of the participants were bachelor's degree graduates and their professional periods generally ranged between 6-10 years. When the daily internet usage time of the participants was analyzed, it was seen that more than half of them use the internet 3-4 hours a day and use the internet intensively for mobile banking, e-government services and e-commerce purposes. When the effect of gender on cybersecurity behaviors was examined, it was found that male participants took cybersecurity measures more actively and participated in trainings on this subject more frequently. Factor analysis results reveal that the six-dimensional structure of the scale is compatible with the data set and accurately reflects the theoretical background. In the reliability analysis, it was determined that the Cronbach Alpha coefficient was at the desired level (0.7 and above).

As a result, it is understood that the cyber security awareness levels of public personnel are generally sufficient, but more awareness-raising activities should be carried out in certain dimensions (especially the benefit dimension). As a result of the research, it is evaluated that it will contribute to the development of cyber security training programs and policies and will help to create strategies to increase the cyber security awareness of public personnel.

Keywords:

Cyber, Security, Cyber security awareness, Public Personnel.



İÇİNDEKİLER

KABUL VE ONAY	iv
YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI.....	v
ETİK BEYAN	vii
ÖN SÖZ.....	viii
ÖZET.....	ix
ABSTRACT	xi
TABLolar DİZİNİ	xvi
SEKİLLER DİZİNİ	xvii
GİRİŞ	1
1. BÖLÜM.....	3
KAVRAMSAL ÇERÇEVE.....	3
1.1. BİLGİ ÇAĞI.....	3
1.2. BİLGİ İLETİŞİM TEKNOLOJİLERİ VE İNTERNET.....	4
1.3. BİLGİ VE BİLGİ GÜVENLİĞİ KAVRAMI.....	5
1.3.1. Bilgi Güvenliğinin Kapsamı	7
1.3.2. Bilgi Güvenliğinin Tarihsel Gelişimi	7
1.3.3. Bilgi Güvenliğinin Temel Unsurları.....	8
1.3.3.1. Gizlilik.....	8
1.3.3.2. Bütünlük.....	9
1.3.3.3. Erişilebilirlik	9
1.4. BİLGİ GÜVENLİĞİNİ TEHDİT EDEN UNSURLAR VE ALINMASI GEREKEN ÖNLEMLER.....	10
1.5. KAMU KURUMLARININ SINIFLANDIRILMASI	10
1.6. ULUSLARARASI STANDARTLAR VE BİLGİ GÜVENLİĞİ KRİTERLERİ	11
1.6.1. Standartlar	11

1.6.2. Öncelikli Güvenlik Önlemleri	12
1.6.3. Bilgi Güvenliği Kriterleri	13
1.6.3.1. Kamu Kurumlarının Sağlaması Gereken Kriterler	13
1.6.3.2. Bilgi Güvenliği Süreci.....	14
2. BÖLÜM.....	15
SİBER GÜVENLİK.....	15
2.1. SİBER TEHDİTLER	15
2.2. TÜRKİYE’DE SİBER GÜVENLİK.....	17
2.2.1. Yasal Düzenlemeler	18
2.2.2. Kurumlar ve Kuruluşlar	20
2.2.2.1. Bilgi Teknolojileri ve İletişim Kurumu (BTK)	20
2.2.2.2. Telekomünikasyon İletişim Başkanlığı (TİB)	20
2.2.2.3. Siber Suçlarla Mücadele Daire Başkanlığı	20
2.2.2.4. Siber Güvenlik Kurulu	21
2.2.2.6. Kurumsal SOME’lerin Görev ve Sorumlulukları	23
3. BÖLÜM.....	25
SİBER GÜVENLİK FARKINDALIĞI VE EĞİTİMİ	25
3.1. SİBER GÜVENLİK KAVRAMI.....	25
3.2. SİBER GÜVENLİK BİLGİSİ.....	25
3.3. SİBER GÜVENLİK FARKINDALIĞI.....	26
3.4. SİBER GÜVENLİK DAVRANIŞI	27
3.5. SİBER GÜVENLİK EĞİTİMİ	28
3.6. LİTERATÜR ÖZETİ.....	30
4. BÖLÜM.....	34
YÖNTEM.....	34
4.1. ARAŞTIRMA SORULARI.....	34
4.2. VERİ TOPLAMA ARAÇLARI.....	34
4.2.1. Genel Bilgiler	34
4.2.2. Siber Güvenlik Ölçeği	34

4.2.3. Siber Güvenlik Ölçeğinin Güvenirliliği ve Dağılım Özelliği.....	35
4.3. VERİ DEĞERLENDİRME SÜRECİ.....	35
5. BÖLÜM.....	37
BULGULAR.....	37
5.1. KATILIMCILARA YÖNELİK TANIMLAYICI BULGULAR.....	37
5.2. SİBER GÜVENLİK ÖLÇEĞİNE YÖNELİK GEÇERLİK VE GÜVENİRLİLİK ANALİZLERİ	38
5.2.1. Açıklayıcı Faktör Analizi (AFA) Sonuçları.....	38
5.2.2. Doğrulayıcı Faktör Analizi (DFA) Sonuçları	39
5.2.3. Güvenirlilik Analizi Sonuçları ve Dağılım Özellikleri	41
5.3. SİBER GÜVENLİK ÖLÇEĞİNE İLİŞKİN BULGULAR	41
5.4. SİBER GÜVENLİĞİN SOSYODEMOGRAFİK ÖZELLİKLERE GÖRE İNCELENMESİ.....	43
5.4.1. Gizlilik boyutunun sosyodemografik özelliklere göre incelenmesi.....	44
5.4.2. Kontrol-sahiplik boyutunun sosyodemografik özelliklere göre incelenmesi	46
5.4.2. Bütünlük boyutunun sosyodemografik özelliklere göre incelenmesi	47
5.4.3. Gerçeklik boyutunun sosyodemografik özelliklere göre incelenmesi	49
5.4.4. Erişebilirlik boyutunun sosyodemografik özelliklere göre incelenmesi ...	50
5.4.5. Fayda boyutunun sosyodemografik özelliklere göre incelenmesi	52
SONUÇ.....	54
KAYNAKÇA.....	64
EKLER.....	77
EK 1. ORJİNALLİK RAPORU FORMU	77
EK 2. ETİK KURUL İZİN FORMU	78
EK 3. VERİ TOPLAMA İZNİ	79
EK 4. ANKET FORMU	80
ÖZ GEÇMİŞ	83

TABLOLAR DİZİNİ

Tablo 1. Güvenirlilik ve Dağılım Özellikleri	33
Tablo 2. Sosyo-Demografik Özelliklere Yönelik Bulgular.....	35
Tablo 3. AFA Analizi Sonuçları.....	37
Tablo 4. Güvenirlilik ve Dağılım Özellikleri	39
Tablo 5. Katılımcıların Siber Güvenlik Durumları	39
Tablo 6. Siber Güvenlik ve Genel Özellikler Karşılaştırması.....	41
Tablo 7. Gizlilik Boyutu ve Genel Özellikler Karşılaştırması	43
Tablo 8. Kontrol-Sahiplik Boyutu ve Genel Özellikler Karşılaştırması	44
Tablo 9. Bütünlük Boyutu ve Genel Özellikler Karşılaştırması	46
Tablo 10. Gerçeklik Boyutu ve Genel Özellikler Karşılaştırması.....	47
Tablo 11. Erişilebilirlik Boyutu ve Genel Özellikler Karşılaştırması	49
Tablo 12. Fayda Boyutu ve Genel Özellikler Karşılaştırması.....	50

SEKILLER DİZİNİ

Şekil 1. DFA Analizi Sonuçları	38
--------------------------------------	----



GİRİŞ

Günümüzde bilgi ve iletişim teknolojileri, yaşamımızın neredeyse her alanında vazgeçilmez bir rol oynamakta ve bu durum, siber güvenliği sadece bireysel ya da kurumsal bir mesele olmaktan çıkararak, ulusal bir güvenlik sorununa dönüştürmektedir. Kamu sektörü, bu teknolojilerin etkisi altında giderek dijitalleşen bir yapıya bürünürken, kamu personelinin siber güvenlik konusunda yeterli bilgiye sahip olması ve bu alanda etkin bir farkındalığa ulaşması büyük önem arz etmektedir. Siber güvenlik, bilgisayarlar, ağlar, yazılım uygulamaları ve kritik sistemler başta olmak üzere dijital verilerin korunmasını amaçlayan önemli bir disiplindir. Kamu personelinin siber güvenlik farkındalığını tespit etmek ve bu alandaki bilgi düzeyini artırmak hem kişisel verilerin korunmasını hem de kamu hizmetlerinin kesintisiz yürütülmesini sağlamak için kritik bir adımdır. Hassas verilerin yetkisiz erişimden korunması ve iş operasyonlarında istenmeyen ağ etkinliği nedeniyle oluşabilecek kesintilerin önlenmesi, siber güvenlik önlemleri ve araçlarının etkin kullanımını zorunlu kılar. Ayrıca, dijital ortamda meydana gelebilecek siber saldırılar, doğal afetler veya terör olayları gibi faktörler nedeniyle de ülkelerin bilişim sistemleri zarar görebilmekte, bu durum ulusal güvenliği doğrudan etkilemektedir.

Bu araştırma, siber güvenlik kültürünün kamu çalışanları arasında ne derece benimsendiğini ve siber tehditlere karşı ne kadar hazırlıklı olduklarını ortaya koymayı hedeflemektedir. Araştırmanın temel amacı, kamu personelinin siber güvenlik konusunda farkındalık düzeyini belirlemek ve bu alanda gerekli eğitim ve önlemlerin artırılmasına yönelik önerilerde bulunmaktır. Çalışma, Türkiye özelinde kamu kurumlarında çalışan personelin siber güvenlik farkındalığını ve bu alandaki eğitim ihtiyaçlarını derinlemesine inceleyerek, bilgi güvenliği politikalarının ve uygulamalarının nasıl iyileştirilebileceğine dair kapsamlı bir bakış açısı sunmayı amaçlamaktadır. Siber güvenlik eğitimi ve farkındalık programlarının geliştirilmesi, bu tehditlerin azaltılmasında ve kamu sektöründe daha güvenli bir bilgi işlem ortamının sağlanmasında önemli bir rol oynayacaktır.

Bu kapsamda çalışmanın birinci bölümünde, siber güvenlik alanında kavramsal bir çerçeve sunulmuştur. Bu bölümde, bilgi ve iletişim teknolojileri, bilgi güvenliğinin kapsamı, temel unsurları, bilgi güvenliğini tehdit eden faktörler ve bu tehditlere karşı alınması gereken önlemler, kamu kurumlarının sınıflandırılması, bilgi güvenliği kriterleri

ile kamu kurumlarının saęlaması gereken kriterler detaylı bir řekilde incelenmiřtir. Çalışmanın ikinci bölümünde ise siber güvenlik konusu, bu alandaki mevcut tehditler, Türkiye'de yürürlükte olan siber güvenlik yasal düzenlemeleri ve bu düzenlemeler çerçevesinde faaliyet gösteren kurum ve kuruluşlar detaylı olarak ele alınmıştır. Dördüncü bölümde, siber güvenlik farkındalığı ve eğitimi konularına odaklanılmıştır. Bu bölümde, siber güvenlik kavramının yanı sıra, siber güvenlik farkındalığı, siber güvenlik eğitimi ve siber güvenlikle ilgili yapılmış arařtırmalar ayrıntılı bir řekilde irdelenmiştir. Çalışmanın yöntem ve bulgular bölümünde ise arařtırmanın metodolojisi ve elde edilen bulgular geniş bir perspektifte sunulmuřtur.



1. BÖLÜM

KAVRAMSAL ÇERÇEVE

Bu bölümde bilgi çağı, endüstri 4.0, bilgi iletişim teknolojileri ve internet ve bilgi ve bilgi güvenliği kavramı gibi bilgiler kavramsal çerçeve başlığı altında ayrıntılı olarak ele alınacaktır.

1.1. BİLGİ ÇAĞI

İnsanlık tarihinde, tarım toplumundan endüstri toplumuna ve nihayetinde bilgi toplumuna doğru üç aşamalı bir geçiş yaşanmıştır. Endüstri Devrimi, üretim biçimleri ve sosyo-ekonomik yapılanma bakımından kendi kültürünü oluşturarak, bu süreci tamamlamış ve yeni bir dönemin başlangıcını işaret etmiştir (Özdemirci ve Torunlar, 2018). 1970'lerden itibaren dünya çapında bilgi ve iletişim teknolojilerinde meydana gelen göze çarpan gelişmeler, bu yeni dönemi "Bilgi Çağı" olarak adlandırılmasını sağlamıştır (Aldemir ve Merve, 2020). Bu dönem, "kapitalist-ötesi toplum", "bilişim toplumu", "bilgi ekonomisi" gibi çeşitli tabirlerle de tanımlanmaktadır. Bu tanımlamalar arasında en yaygın olarak kabul gören ve tüm toplumlarda anlam birliği sağlayan ifade, "bilgi çağı" ve eş anlamlısı "bilgi toplumu" terimleridir (Bekar ve Sağlam, 2023). Bilgi çağı, yeni bir değişim sürecinin yönünü ve karakterini tanımlayan "bilgi toplumu" kavramını beraberinde getirmiştir (Öğün ve ark. 2020). 21.yüzyılın, bilginin merkezde olduğu bir çağ olarak tanımlanması, bilim dünyasında ve genel toplumda geniş kabul gören bir yaklaşımdır (Aldemir ve Merve, 2020). 20. yüzyılın ikinci yarısından itibaren bilgi ve iletişim teknolojilerindeki hızlı ilerleme, endüstri çağından bilgi çağına geçişi hızlandırmıştır. Bu yeni dönemde, bilgi ve teknolojinin artan değeri, "bilgi çağı" ve "bilgi toplumu" gibi kavramların yaygınlaşmasına yol açmıştır (Aldemir ve Merve, 2020).

Mevcut dönem, üretimde mekanik teknolojilerin programlanabilir dijital teknolojilere yerini bırakmasıyla karakterize edilen ve dünyada bilgi iletişim teknolojilerinin büyük bir hızla geliştiği bir dönem olarak tanımlanmaktadır. Bu süreç, "informatik devir" olarak da adlandırılmaktadır (Yıldırım, 2020). Bilgi çağının bu evresi, bilgisayar, fiber-optik, çipler ve atom enerjisi kullanım teknolojisi gibi mikro elektronik teknolojiler üzerine inşa edilmiştir. Gelişen bilgi iletişim teknolojileri ve bilişim sistemleri, makinelerin birbirleriyle etkileşim kurabilmesi, yorumlar yapabilmesi,

karmaşık problemlere çözümler üretebilmesi ve birbirine olayları öğretebilmesi gibi yetenekleri somutlaştırmış, bu gelişmeler dördüncü endüstriyel devrim olarak tanımlanmıştır (Seçmen, 2022). Bu dönemde, makinelerin birbirleriyle iletişime geçerek çeşitli sorunlarla başa çıkabilmesi mümkün hale gelmiştir.

Endüstri 4.0 kavramı, ilk olarak Almanya'daki Hannover Fuarı'nda gündeme gelmiş ve Alman Hükümeti'nin talebi üzerine uzmanlar tarafından hazırlanan bir çalışma ile büyük ilgi görmüştür. MacDougall (2014), 2011 Hannover Fuarı'nda resmi belgelerle ortaya çıkan Endüstri 4.0'ın, dördüncü sanayi devriminin habercisi olduğunu ifade etmektedir. Endüstri 4.0, bilgisayar, internet ve bilgi iletişim teknolojilerindeki gelişmelerle birlikte, insan gücüne ihtiyaç duymadan yönetilebilen ileri teknolojilerin sanayide üretimi olarak tanımlanabilir (Munirathinam, 2020). Önceki endüstriyel devrimlerden çok daha hızlı ilerleyen bu süreç, dünya genelinde yönetim ve üretim sistemlerinde önemli dönüşümlere yol açmaktadır (Yang ve Gu, 2021).

Günümüzdeki teknolojik gelişmeler, Endüstri 4.0 olarak adlandırılan yeni bir endüstriyel devrimi tetiklemektedir. Bu devrim, siber-fiziksel sistemlere dayalı üretim süreçlerine odaklanmakta ve bulut bilişim gibi verimliliği artıran yenilikçi bilgi iletişim teknolojilerini kullananlara rekabet avantajı sağlamaktadır (Bai ve ark., 2020). Makinelerin "akıllı" hale gelmesiyle bazı üretim sistemlerinde insan gücünün yerini makinelerin alması, Endüstri 4.0 kavramının ortaya çıkmasında önemli bir faktördür. Endüstri 4.0'ın hedeflerine ulaşabilmesi için nesnelerin interneti ve siber-fiziksel sistemler gibi araçlara ihtiyaç duyulmaktadır. Bu yeni yapılanmada, siber-fiziksel sistemler ve nesnelerin interneti kritik bir rol oynamaktadır (You ve Feng, 2020).

1.2. BİLGİ İLETİŞİM TEKNOLOJİLERİ VE İNTERNET

Teknoloji, bilimsel bilginin pratiğe dönüştürülmesi süreci olarak akademik literatürde tanımlanır ve bu tanım, insan-makine sistemlerinin tasarımı, organizasyonunu ve yönetimini içermektedir (Yorgancıoğlu ve Demircan, 2023). Bilgi ve iletişim teknolojileri ise, insanların kendi aralarında ve elektronik sistemler aracılığıyla etkileşim kurmalarını kolaylaştıran, her türlü bilginin elde edilmesine olanak tanıyan teknolojiler olarak ifade edilmektedir (Batur, 2022). Bu teknolojilerle son yıllarda bilgi iletişim alanındaki değişim ve gelişim, baş döndürücü bir biçimde birçok alanı etkilediği gibi kullanılan araç ve gereçler bakımından çeşitli yeniliklere yol açmıştır (Özdemir,

2013). Bu teknolojiler, iletişim kurma, bilgi oluşturma, yayma, depolama ve yönetme süreçlerinde kullanılan çeşitli teknolojik araçları ve kaynakları kapsar; ayrıca bilgilerin toplanması, depolanması, geri alınması ve aktarılması işlemlerinde de etkin bir role sahiptirler. Bu bağlamda, bilgi ve iletişim teknolojileri, farklı kaynaklardaki bilgi ile iletişim ve teknoloji arasında bir köprü veya aracı olarak tanımlanmakta ve depolama, yayma, saklama, iletme, geri alma gibi işlevlerle ilişkilendirilmektedir

Son yıllarda bilgi ve iletişim teknolojilerinin hızla yaygınlaşması, dünya çapında hem bilgisayar hem de internet kullanıcılarının sayısında önemli bir artışa neden olmuştur. İnternet, dünya genelindeki tüm bilgisayarları birbirine bağlayan ve kullanıcıların içerik paylaşımına ve paylaşılan içeriğe erişimine olanak tanıyan en geniş ağ olarak tanımlanmaktadır (Sezen, 2023). Bu ağ, günümüzde bilgi ve iletişim teknolojilerinin merkezinde yer almakta ve insanların günlük yaşamlarında önemli bir rol oynamaktadır.

2021 yılında yayımlanan bir rapora göre, dünya genelinde internet kullanıcılarının sayısı 4,66 milyara ulaşmış ve bu, dünya nüfusunun yaklaşık %56,5'ine denk gelmektedir. Önceki yıla göre internet kullanıcı sayısında 317 milyon kişilik bir artış, yani %7,3'lük bir yükseliş gözlemlenmiştir (Kumar ve ark. 2022). Türkiye İstatistik Kurumu'nun verilerine göre, Türkiye'de de internet ve bilgisayar kullanımı bu dönemde önemli ölçüde artmıştır. 2019 yılında evden internet erişimi %88,3 iken, 2020 yılında bu oran %90,7'ye yükselmiştir; aynı dönemde internet kullanım oranı %75,3'ten %79,0'a çıkmıştır. Bilgisayar kullanımı ise 2017 yılında %56,6 iken, 2018 yılında %59,6'ya ulaşmıştır (TÜİK, 2020).

1.3. BİLGİ VE BİLGİ GÜVENLİĞİ KAVRAMI

Bilgi kelimesi, Latince'de herhangi bir şeyi şekillendirmek anlamına gelse de sözlüklerde bu kavram çok daha geniş ve derin anlamlar içermektedir. Çeşitli tanımlar incelendiğinde bilgi; geçerliliği kanıtlanmış inançlar, ilim ve bulgu yoluyla elde edilen realite, veri ve kavrayışlar, sosyal hayatta karşılaşılan durumları anlamamıza yardımcı olan işaretler, kodlar ve insanın varlık bilgisi ile ilk sezgilerinde aklın benimsediği temel fikirler yöntemlerden faydalanan bireyin bulgulara yüklediği anlam olarak tanımlanmaktadır. Bilgi, günümüz dünyasının etkilenmesinde en önemli varlık olarak kabul edilmekte. Bilgiyi anlamak, özümsemek ve ilgili konular üzerine araştırmalar

yapmak, insanlık var olduđu günden beri geçen zamanda geleceğe yönelik ilerlememizi şekillendiren en önemli araç haline gelmiştir (Nezgitli ve Gökçearsan, 2022).

Günümüzde bilgi, sadece mevcut zamanı anlamak ve geleceğe yön vermek için değil, aynı zamanda geçmişini kavramak için de anahtar bir rol oynamaktadır. Bilginin değeri, eğitimden sağlığa, sanattan yaşama kadar çeşitli alanlarda insanlık tarihinin ilk çağlarından itibaren anlaşılmakta ve gelecek kuşaklara farklı yollarla aktarılmaktadır. İlk zamanlarda masallar, hikayeler ve destanlar aracılığıyla nesilden nesile geçen bilgi, sonraki dönemlerde medreseler, kiliseler, üniversiteler ve yazılı kaynaklar yoluyla yayılmıştır. Ancak, son dönemlerde teknolojinin gelişimiyle birlikte insanlar arasındaki iletişim hızlanmış ve iş birliği artmıştır (Ecek ve Çakmak, 2022). Bu durum, "bilgi çağı" olarak adlandırılan yeni bir dönemin başlangıcını işaret etmiştir. Günümüzde, bilgi sadece insanların günlük yaşamını yönlendirmekle kalmayıp, gelecekte de insan hayatının yönünü belirleyen temel bir unsurdur (Korucu, 2021). Bu bağlamda, bilgi çağının gelişimi, toplumların yapısını, işleyişini ve geleceğini şekillendirmekte, aynı zamanda küresel ölçekte sosyal, ekonomik ve kültürel dönüşümlere öncülük etmektedir. Dolayısıyla, bilgiye erişim, kullanım ve paylaşımının, çağımızın en temel dinamiklerinden biri olduğu açıkça görülmektedir. Bu gelişmeler ışığında, bilgi ve iletişim teknolojilerinin önemi daha da artmakta ve bilginin rolü, toplumların geleceğini belirleyen en kritik faktörlerden biri haline gelmektedir (Ecek ve Çakmak, 2022).

Bilgi güvenliği kavramı ise, çeşitli boyutları ve düşünce tarzlarını kapsayan, veri koruma kavramlarının geliştirilmesi, şifreleme yöntemleri ve güvenlik politikalarının uygulanması gibi unsurları içermektedir (Wylde ve ark. 2022). Kriptografi, saldırı tespiti ve bilgi akışı güvenliği gibi alt alanları da barındıran bilgi güvenliği, modern bilgi güvenliği politikalarının gerekliliklerini karşılamak üzere şekillenmiştir (Nair ve Tyagi, 2021). Akademisyenler, bilgi güvenliğinin temel hedefleri olarak gizlilik, bütünlük ve erişilebilirlik (CIA) kavramlarının önemini vurgulamışlardır (Usmonov, 2021). Ayrıca, bilgi güvenliği çok boyutlu bir kavram olup, genellikle ayrı olarak ele alınan özel bilgi ve siber güvenlik yönlerini de içermektedir (Usmonov, 2021). Geleneksel olarak, bilgi güvenliği, verilerin korunmasına ve sistemlerin tasarlandığı gibi çalışmasının sağlanmasına odaklanmaktadır (Ecek ve Çakmak, 2022).

1.3.1. Bilgi Güvenliğinin Kapsamı

Bilgi teknolojilerinin ilerlemesiyle birlikte, bu teknolojiler insan hayatının ayrılmaz bir parçası haline gelmiş ve bu durum, bilgi güvenliğinin önemini önemli ölçüde artırmıştır. Veri, işlenmemiş ve yorumlanmamış gözlemler, sayılar, karakterler ve semboller gibi unsurlardan oluşan, yazılı, işitsel veya görsel formların dönüştürülmemiş halidir. Örneğin, bir hastanın hastaneye kayıt olması işlemi, kaydın zamanı, yapılan poliklinik ve ödenen ücret gibi verilerle ifade edilebilir. Ancak bu veriler, tek başına, hasta hakkında bilgi vermezler; örneğin, hasta neden bu hastaneyi tercih etti veya tekrar gelir mi gibi soruları bu veriler tek başına cevaplayamaz, bu nedenle tek başına anlamlı olamazlar (Meral ve Bülbül, 2022).

Enformasyon, bahsedilen verilerin ihtiyaçlar doğrultusunda belirli bir amaca yönelik düzenlenip anlamlı bir mesaj oluşturulması sürecidir. Yani verinin düzenlenmiş ve anlamlı hale getirilmiş formudur. Enformasyon, veriden daha zengin içeriğe sahip olup yazılı, sözlü veya görsel bir mesaj olarak karşımıza çıkar. Bilgi ise, insan ile nesne arasındaki ilişkiden çıkan, ihtiyaçlara göre insan aklı tarafından işlenip anlamlandırılan bir sonuçtur. Veri, enformasyon sürecinin girdisi olarak kabul edilirken, enformasyon ise bu sürecin çıktısı olarak değerlendirilir (Yıldız ve ark. 2023). Bilgi, insanların çevreleriyle etkileşim sürecinde edindikleri tecrübelerin ve enformasyonun bir araya getirilerek değerlendirilmesi ile zihinde oluşturulan kavramsal yapıdır. İşlenmemiş verilerin kullanılacak yere göre düzenlenmesi, gruplandırılması ve hatasız olarak belli mesajlar verebilecek şekilde enformasyon haline getirilmesinden sonra, bu enformasyonun organizasyon eylemlerinin niteliğine veya gereksinimine göre ilgili bireyler tarafından analiz edilmesi ve yeniden değerlendirilmesi sürecinden geçerek bilgiye dönüşür. Bilgi, enformasyonun yorumlanmış, analiz edilmiş ve bağlamla zenginleştirilmiş hali olarak tanımlanabilir. Literatürde bazen bilgi ve enformasyon kavramları birbirinin yerine kullanılmakta, ancak bu iki kavram birbirinden farklı anlamlara sahiptir (Yıldız ve ark. 2023).

1.3.2. Bilgi Güvenliğinin Tarihsel Gelişimi

Bilgi güvenliğinin tarihsel gelişimi, özellikle dijital çağın ortaya çıkışından bu yana, teknoloji ile etkileşimimizin kritik ve gelişen bir yönü olmuştur. Bu evrim, bilgisayar teknolojisinin ilk günlerine, özellikle de silah planlaması ve askeri istihbaratta araştırma

ve geliřtirmeyi desteklemek iin gl bilgisayarların geliřtirildiėi Soėuk Savař dnemine kadar izlenebilir. zellikle RAND Corporation, bu gl bilgisayar sistemlerinin geliřimine paralel olarak, silah planlamasına ynelik teknokratik yaklařımların ykseliřinde nemli bir rol oynamıřtır (Stewart, 2021).

Bilgi gvenliėi ihtiyaı, modern internetin ncs olan ARPANET'in oluřturulması ile daha da belirgin hale gelmiř ve 2 Kasım 1988'deki internet solucanı nedeniyle ilk yaygın internet kesintisine yol amıřtır. Bu olay, geliřmekte olan dijital altyapının doėasında var olan gvenlik aıklarının altını izmiřtir (Packard, 2023). İnternet geliřtike, zellikle de 1990'ların sonundaki dot-com patlaması sırasında, internet gvenlik aıklarında ve bu aıkları gidermek iin tasarlanan gvenlik rnlerinde buna karřılık gelen bir artıř oldu. Bu dnemde, bilgisayar korsanlarının gvenlik aıklarını ortaya ıkardıėı ve daha sonra bunların dzeltilmesine yardımcı olmak iin para aldıėı "kazanlı bir geri bildirim dngs" grld (Stewart, 2021). 2000'li yılların bařında Microsoft'un Gvenilir Bilgi İřlem giriřiminin kurulmasıyla birlikte bilgi gvenliėi alanında nemli bir deėiřim yařanmıřtır. Bu giriřim, daha sonra diėer řirketler tarafından da taklit edilen yazılım gvenliėini iyileřtirmeye ynelik bir hamleyi temsil ediyordu. Bilgi gvenliėine ynelik ekonomik ve psikolojik yaklařımların bymesi de bu dnemde ortaya ıkmıř ve gnlk bilgisayar kullanıcılarına ařırı yk getirmeyecek "kullanılabilir gvenlik" yaratma ihtiyaını vurgulamıřtır (Packard, 2023).

1.3.3. Bilgi Gvenliėinin Temel Unsurları

Bilgi gvenliėinin temel unsurları, bilgiyi yetkisiz eriřim, kullanım, ifřa, kesinti, deėiřiklik veya imhadan korumak iin tasarlanmıř bir dizi ilke ve uygulama olarak anlařılabilir. Bu unsurlar, bilgi gvenliėinin  temel ilkesi olan bilginin gizliliėinin, btnlėnn ve eriřilebilirliėinin korunmasında hayati neme sahiptir.

1.3.3.1. Gizlilik

"Gizlilik", bilgi gvenliėinin temel unsurlarından biridir ve hassas bilgilerin yalnızca yetkili kiřilere eriřilebilir olduėu anlamına gelir. Gizlilik, kiřisel mahremiyeti ve ticari sırları korumak iin nemlidir. Bu, verilerin dinlenmesini, okunmasını veya bařkaları tarafından izlenmesini engelleyen tekniklerle saėlanır (Forsyth, 2022). Gizliliėi saėlamak iin kullanılan bařlıca yntemler arasında řifreleme, eriřim kontrol listeleri ve

veri maskelenmesi yer alır. Örneğin, şifreleme, verileri yetkisiz erişime karşı korumak için kritik bir tekniktir ve verilerin dinlenmesini veya izinsiz okunmasını önlemek için kullanılır. Erişim kontrol listeleri, belirli kullanıcıların veya grupların belirli verilere erişimini sınırlar ve bu sayede hassas bilgilerin yalnızca yetkili kişiler tarafından görüntülenebilmesini sağlar (Whitman ve Mattord, 2021).

1.3.3.2. Bütünlük

Bilgi güvenliğinin temel unsurlarından biri olan "Bütünlük", verilerin yetkisiz veya yanlışlıkla değiştirilmesini önleyerek veri doğruluğu ve güvenilirliğini korumayı ifade eder. Bütünlük, verilerin tutarlılığını, doğruluğunu ve güvenilirliğini tüm yaşam döngüsü boyunca sürdürmeyi amaçlar. Bu durum, verilerin kasıtlı veya kazara değiştirilmeden korunmasını sağlamak için çeşitli yöntemler ve kontrollerin uygulanmasını gerektirir (Forsyth, 2022). Bütünlüğü korumak için kullanılan yöntemler arasında veri karma (hashing) ve dijital imzalar yer alır. Veri karma, bir veri parçasının benzersiz bir değere dönüştürülmesi işlemidir ve bu işlem sonucunda oluşan karma değeri, verinin değişip değişmediğini tespit etmek için kullanılır. Eğer veri değiştirilirse, karma değeri de değişir, bu da yetkisiz değişiklikleri tespit etmeye yardımcı olur. Dijital imzalar, verinin bütünlüğünü ve veriyi gönderenin kimliğini doğrulamak için kullanılır. Bu teknikler, özellikle dijital işlemler ve iletişimlerde, eylemlerin ve iletişimin doğruluğunu sağlamak için kritik öneme sahiptir (Whitman ve Mattord, 2021).

1.3.3.3. Erişilebilirlik

Erişilebilirlik, bilgi güvenliğinin temel prensiplerinden biri olarak, yetkili kişilerin gerektiğinde bilgilere ulaşabilmesini ifade etmektedir. Bilgi güvenliğinin diğer temel prensipleri olan gizlilik ve bütünlük ile birlikte, erişilebilirlik, bilgi sistemlerinin etkin ve verimli bir şekilde kullanılmasını sağlamaktadır (Whitman ve Mattord, 2021). Erişilebilirlik, özellikle acil durumlar veya kritik iş süreçleri sırasında, bilginin kesintisiz ve hızlı bir şekilde elde edilmesini gerektirmektedir. Bu prensip, kullanıcıların belirli verilere zamanında ve güvenli bir şekilde erişebilmelerini sağlamak için alınan önlemleri kapsamaktadır.

1.4. BİLGİ GÜVENLİĞİNİ TEHDİT EDEN UNSURLAR VE ALINMASI GEREKEN ÖNLEMLER

İnternetin yaygınlaşmasıyla birlikte, dünya genelinde ve Türkiye'de internet ve mobil cihaz kullanım oranları önemli ölçüde artmıştır. Bu artış, özellikle sosyal medya platformlarının aktif kullanımında da gözlemlenmektedir. Ancak, internetin sağladığı kolaylıkların yanı sıra, kullanıcıları çeşitli güvenlik risklerine maruz bıraktığı da bir gerçektir. Bu riskler, kullanıcıları psikolojik, fiziksel, maddi ve sosyal açıdan etkileyebilmekte ve genellikle saldırı, atak veya tehdit olarak adlandırılmaktadır. Bilgi veya bilgisayar güvenliğini hedef alan bu tehditler, kullanıcıların güvenliğini ve mahremiyetini tehlikeye atabilmektedir (Gündüz ve Resul, 2021).

Kötü niyetli kişiler tarafından gerçekleştirilen siber saldırılar, bilgi sistemlerine sızma, zafiyetleri istismar etme, bireylere veya sistemlere doğrudan veya dolaylı zarar verme ve sistemlerin iş sürekliliğini bozma gibi amaçlar taşımaktadır (Aydın, Barışkan ve Çetinkaya, 2021). Bilgi sistemlerindeki güvenlik açıkları, tıpkı vücuttaki virüs ve bakteriler gibi, sistemin bağışıklık sisteminin zayıfladığı veya açık verdiği anlarda etkili olmaktadır. Teknik ve bireysel zafiyetler, tehditlerin bilgisayar sistemlerine zarar verebilecek düzeye ulaşmasında önemli rol oynamaktadır. Bu nedenle, bilgi güvenliğine yönelik tehditlerin etkin bir şekilde yönetilmesi ve önlenmesi, günümüzün teknolojik gelişmelerinin getirdiği kaçınılmaz bir gerekliliktir.

1.5. KAMU KURUMLARININ SINIFLANDIRILMASI

Kamu kurumlarının bilgi güvenliği standartlarını belirlemeden önce, bu kurumların özelliklerine göre kategorilere ayrılması ve her kategoriye uygun asgari güvenlik kriterlerinin saptanması zorunludur. Türkiye'deki kamu kurumları, temel özelliklerine göre iki ana kategoriye ayrılmaktadır (Siber Güvenlik Enstitüsü, 2019). Bu sınıflandırma, kamu kurumlarının işlevleri ve sahip oldukları bilgi sistemlerinin kritikliğine göre yapılmaktadır (Siber Güvenlik Enstitüsü, 2019). Kamu kurumları, aşağıdaki tanımlamaları göz önünde bulundurarak, hangi kategoride yer alacaklarını belirlemelidir:

Kritik Bilgi Sistemi: Bu kategori, kamu hizmetlerinin devamlılığını doğrudan etkileyen bilgi sistemlerini içermektedir. Eğer bir bilgi sisteminin bozulması veya yetkisiz

erişime maruz kalması sonucunda aşağıdaki durumlar meydana gelirse, bu sistem kritik olarak değerlendirilmelidir (Resmî Gazete, 2013):

- a. Enerji, su, acil yardım hizmetleri, gıda tedariki gibi hayati hizmetlerin durması, bu durumun can kaybına veya bazı bölgelerin boşaltılmasına neden olması,
- b. Para piyasalarının durması, ulaştırma sistemlerinden birinin işlevsiz hale gelmesi gibi sebeplerle ulusal ekonominin ciddi düzeyde zarara uğraması,
- c. Ulusal güvenliğin ciddi şekilde sekteye uğraması.

Kritik Kamu Kurumları: Bu kategorideki kurumlar, bünyelerinde “kritik bilgi sistemi” barındıran kamu kurum ve kuruluşlarıdır. Bu kurumlar, kamu hizmetlerinin aksamadan yürütülmesi ve ulusal güvenliğin korunması açısından hayati öneme sahiptir (Resmî Gazete, 2013).

1.6. ULUSLARARASI STANDARTLAR VE BİLGİ GÜVENLİĞİ KRİTERLERİ

1.6.1. Standartlar

Kamu kurumları için asgari bilgi güvenliği kriterlerinin belirlenmesinde, uluslararası alanda kabul görmüş standartlardan yararlanılmaktadır. Bu bağlamda, ISO/IEC 27001 ve ISO/IEC 27002 standartları, bilgi güvenliği yönetimi alanında dünyada en yaygın olarak kabul gören rehberler arasında yer almaktadır. ISO/IEC 27001 standardı, bilgi güvenliği yönetim sürecini tanımlamakta ve bu süreci destekleyen kontrolleri ve güvenlik önlemlerini içermektedir (Kılıç, Yalçın ve Kılıç, 2021). Standartta yer alan Ek-A bölümünde, çeşitli güvenlik önlemleri ve bu önlemlerin açıklamaları özet halinde sunulmaktadır. ISO/IEC 27002 standardı ise, ISO/IEC 27001 standardının Ek-A’sında yer alan güvenlik önlemlerinin detaylı açıklamalarını ve iyi uygulama örneklerini içermektedir. Bu standartlar, kurumların bilgi güvenliği yönetim sistemlerini kurarken ve geliştirirken rehberlik etmektedir (Onur, 2021).

Bunlara ek olarak, farklı sektörler için hazırlanmış olmakla birlikte tüm kurum ve kuruluşlara genel bilgi güvenliği anlayışı kazandırabilecek diğer standartlar da bulunmaktadır. Örneğin, Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından hazırlanan bilgi güvenliği dokümanları, süreç kontrolüyle uğraşan veya iletişim sektöründe yer alan kurumlar için özel olarak geliştirilmiş olup, bu dokümanlar geniş bir yelpazede uygulanabilir bilgiler sunmaktadır (Fonseca-Herrera ve

ark. 2021). Ayrıca ISO/IEC 27032 Siber Güvenlik Standardı, siber güvenlik alanında giderek artan önemiyle dikkat çekmekte ve bu alanda rehberlik etmektedir. Bu standardın yanı sıra, ISO/IEC 27002 standardının iletişim ve enerji sektörlerine özgü türevleri de, özellikle bu sektörlerde faaliyet gösteren kurumlar için faydalı bilgiler içermekte ve bilgi güvenliği konusunda geniş bir perspektif sunmaktadır (Fonseca-Herrera ve ark. 2021).

1.6.2. Öncelikli Güvenlik Önlemleri

ISO/IEC 27002 standardı, bilgi güvenliği yönetiminde kapsamlı bir rehber sunmakta olup, toplamda 11 başlık altında 133 güvenlik önemi içermektedir. Ancak bu önlemler içerisinde özellikle vurgulanması gereken ve öncelik taşıyan 10 tanesi bulunmaktadır. Bu önlemler, kurumların bilgi güvenliği yönetim sistemlerini etkin bir şekilde planlamaları ve uygulamaları için temel taşları oluşturmaktadır (Coşar ve Tüfekçi, 2021). Öncelikli güvenlik önlemleri ve ISO 27002 referansları şu şekildedir (International Organization for Standardization, 2022a):

1. Bilgi Güvenliği Politikası (5.1.1): Kurumların bilgi güvenliği konusunda temel ilkelerini ve yaklaşımlarını belirleyen resmî belgedir.
2. Bilgi Güvenliği Sorumluluklarının Atanması (6.1.3): Kurum içinde bilgi güvenliği yönetiminin sorumluluğunun belirli kişi veya ekiplere atanması gerekmektedir.
3. Bilgi Güvenliği Eğitimleri (8.2.2): Tüm çalışanlara ve ilgili taraflara yönelik düzenli bilgi güvenliği farkındalığı ve eğitim programlarının uygulanması.
4. Yazılım Uygulamalarında Güvenlik (12.2): Yazılım ve uygulamaların güvenlik açısından tasarlanması, geliştirilmesi ve bakımının yapılması.
5. Teknik Açıklık Yönetimi (12.6): Sistemlerdeki güvenlik açıklıklarının tespiti, değerlendirilmesi ve yönetilmesi.
6. İş Sürekliliğinin Yönetilmesi (14): İş süreçlerinin kesintisizliğini sağlamak amacıyla kriz durumlarına ve afetlere karşı hazırlık ve önlemlerin alınması.
7. Bilgi Güvenliği Olaylarının Yönetilmesi (13.2): Güvenlik ihlalleri ve olaylarının etkin bir şekilde yönetilmesi ve raporlanması.
8. Veri Koruma ve Kişisel Bilgilerin Mahremiyeti (15.1.4): Kişisel verilerin korunması ve mahremiyetin sağlanması için gerekli tedbirlerin alınması.

9. Kurumsal Kayıtların Korunması (15.1.3): Kurumun resmi kayıtlarının korunması, erişilebilirliği ve bütünlüğünün sağlanması.

Fikri Mülkiyet Hakları (15.1.2): Kurumun ve ilgili tarafların fikri mülkiyet haklarının korunması ve yönetilmesi (International Organization for Standardization, 2022a).

Bu önlemler, bir kurumun bilgi güvenliği yönetim sistemini oluştururken ve güçlendirirken dikkate alması gereken temel öğelerdir. Özellikle, bilgi güvenliği politikasının oluşturulması, bilgi güvenliği sorumluluklarının net bir şekilde atanması ve bilgi güvenliği eğitimlerinin tüm çalışanlara verilmesi, kurumun bilgi güvenliği kültürünü güçlendiren ve riskleri azaltan temel adımlardır. Teknik açıklık yönetimi ve iş sürekliliğinin yönetilmesi gibi önlemler ise, kurumların siber tehditlere ve beklenmedik durumlara karşı direncini artırmaktadır. Bu standartlar, uluslararası alanda kabul görmüş en iyi uygulamaları temsil etmekte ve kurumlara bilgi güvenliğini sağlamada yol göstermektedir.

1.6.3. Bilgi Güvenliği Kriterleri

1.6.3.1. Kamu Kurumlarının Sağlaması Gereken Kriterler

Kamu kurumlarının sağlaması gereken bilgi güvenliği kriterleri, iki ana başlık altında toplanmış olup, bu başlıklar "Önlemler" ve "Bilgi Güvenliği Süreci" olarak tanımlanmıştır. Önlemler başlığı altında, kurumların bilgi sistemlerini siber tehditlere karşı korumak, veri kaybını önlemek ve bilgi güvenliğinin sürekliliğini sağlamak için gerekli olan güvenlik duvarı, sistem odasının emniyeti, veri yedekleme gibi çeşitli politika ve prosedürler yer almaktadır. Bu tedbirler, dış tehditlere karşı ilk savunma hattı olarak güvenlik duvarlarını, iç tehditler ve doğal afetlere karşı ise sistem odasının emniyeti ve veri yedeklemeyi kapsamaktadır (Meral ve Bülbül, 2022).

Bilgi Güvenliği Süreci ise, kurumların bilgi güvenliği yönetim süreçlerinin ele alındığı bölümdür. Bu süreç, risklerin tespiti, alınan önlemlerin düzenli izlenmesi, iç tetkikler yoluyla önlemlerin gözden geçirilmesi ve yönetim tarafından uygulanan düzenleyici ve önleyici faaliyetleri içermektedir (Özdemir ve Uluç, 2021). Bu, kurumların bilgi güvenliği uygulamalarını sürekli olarak iyileştirmelerini ve güncel tehditlere karşı proaktif bir yaklaşım sergilemelerini sağlamaktadır. Kamu kurumları

tarafından sağlanması gereken bu kriterlerin belirlenmesinde ISO/IEC 27001 standardı başta olmak üzere, diğer uluslararası standartlar, TÜBİTAK SGE'nin kurumsal deneyimi ve Ulusal Siber Güvenlik Tatbikatlarından elde edilen sonuçlar dikkate alınmıştır. Bu çok yönlü yaklaşım, kamu kurumlarının bilgi güvenliği yönetim sistemlerinin uluslararası en iyi uygulamalar ve yerel deneyimlerle uyumlu olmasını hedeflemektedir (Özbilen ve Çağlar, 2020).

1.6.3.2. Bilgi Güvenliği Süreci

Bilgi güvenliği yönetimi alanında kurumların odaklanmaları gereken temel nokta, sadece çeşitli güvenlik önlemlerinin uygulanması değil, aynı zamanda bu önlemlerin sürekli olarak izlenmesi, değerlendirilmesi ve geliştirilmesidir. Bilgi güvenliğinin etkin bir şekilde sağlanabilmesi için kurum üst yönetiminin bu alana gerekli yatırımları yapması, uygun insan ve maddi kaynakların tahsis edilmesi gerekmektedir. Bu sürecin temel bileşenleri arasında, ISO/IEC 27001 standardı kapsamında belirtilen "Risk Analizi ve Tedavisi", "İç Tetkik ve Gözden Geçirme" ve "Düzeltilici/Önleyici Faaliyetler" gibi adımlar bulunmaktadır (International Organization for Standardization, 2022b).

Risk Analizi ve Tedavisi aşamasında, kurumların işleyişinde kritik öneme sahip olan bilgi sistemleri ve varlıkları tanımlanır ve bu varlıklarda mevcut güvenlik açıklıkları ile potansiyel tehditler titizlikle değerlendirilir. Elde edilen risk analizi sonuçlarına göre, bu riskleri azaltmak veya tamamen ortadan kaldırmak için gerekli önlemler belirlenir. Bu süreç, kurumların güvenlik durumlarını sürekli güncel tutmaları amacıyla yılda en az bir kez tekrarlanmalıdır (International Organization for Standardization, 2022b).

İç Tetkik ve Gözden Geçirme sürecinde, kurumun bilgi güvenliği süreçleri ve uygulamalarının etkinliği, kurum tarafından bu alanda deneyimli, ancak günlük güvenlik operasyonlarına katılmayan tetkikçiler tarafından yıllık olarak denetlenir. Bu denetimler sonucunda elde edilen bulgular detaylı bir şekilde raporlaştırılarak kurum yönetimine sunulur.

2. BÖLÜM

SİBER GÜVENLİK

Bu bölüm başlığı altında siber güvenlik kavramı, farkındalığı, davranışı, eğitimi ve siber güvenlik ile ilgili yapılmış olan çalışmalar ele alınmıştır.

2.1. SİBER TEHDİTLER

•Siber saldırılar, günümüzde kişisel, kurumsal ve devlet düzeyinde önemli sorunlara yol açmaktadır (Gönç, 2022). Saldırganlar, bilgi sistemlerine sızmak ve saldırılarını gerçekleştirmek için çeşitli siber tehdit yöntemlerini kullanmaktadırlar. Siber tehditler, sadece bilgi ve iletişim teknolojilerinin kötüye kullanılmasıyla ortaya çıkan yeni suç türlerini değil, aynı zamanda geleneksel suçların siber ortama taşınmış versiyonlarını da içermektedir (Gönç, 2022). Siber saldırıların neden olduğu ekonomik kayıplar ve itibar zedelenmesi, kurumların ve hükümetlerin siber güvenliğe öncelik vermelerinin temel nedenleri arasında yer almaktadır. Siber tehditlerin geniş kapsamı, suçların çeşitliliği ve teknolojideki hızlı gelişimin beklenmedik etkileri nedeniyle, siber suçlar çok farklı biçim ve içeriklerde ortaya çıkabilmektedir (Özkan, 2019).

•Siber tehditlerin sınıflandırılması, farklı araştırmacılar tarafından çeşitli açılardan yapılmıştır. Öztürk (2014) tarafından yapılan sınıflandırmada, siber tehditler şu şekilde tanımlanmıştır:

•Kötü Amaçlı Kod/Kötü Amaçlı Yazılım (Malicious Code/Malware): Virüsler, solucanlar, truva atları, botlar ve botnet'ler gibi zararlı yazılımlar, ağdaki bir bilgisayara bulaşarak diğer bilgisayarlara yayılır ve bu sistemlere zarar vermek veya çalışamaz hale getirmek için tasarlanmıştır.

•İstenmeyen Program (Unwanted Program): Reklam yazılımları, casus yazılımlar ve tarayıcı korsanları gibi istenmeyen yazılımlar, kullanıcıların açık rızası olmaksızın bilgisayar sistemlerine yüklenebilir ve reklam gösterimi, internet etkinliklerinin izlenmesi, kişisel veri toplanması gibi istenmeyen eylemlerde bulunabilirler. Bu tür zararlı yazılımlar, kullanıcı deneyimini olumsuz etkilemenin yanı sıra, gizlilik ihlalleri ve güvenlik açıkları gibi ciddi sorunlara yol açar.

- İstenmeyen Elektronik Posta (Spam): Kullanıcıların istemediği elektronik postalar, genellikle reklam içerikli olup, bazen zararlı bağlantılar veya yazılımlar içerebilir.
- Oltalama/Yemleme (Phishing): Kullanıcıların güvenliğini ihlal ederek kişisel ve hassas bilgilerini çalmayı hedefleyen dolandırıcılık faaliyetleri.
- Koklama (Sniffing): Ağ trafiğinin izlenmesi ve bu trafik üzerinden bilgi çalınması.
- Yanıltma (Spoofing): Bir kişi veya kurumun kimliğinin taklit edilerek güveni kötüye kullanma.
- Hizmet Engelleme (DoS and DDoS): Hedeflenen sistem veya ağın hizmet dışı bırakılması.
- İçeriden Saldırıları (Insider Attacks): Kurum içinden bir kişinin kötü niyetle gerçekleştirdiği saldırılar (Öztürk, 2014).

Bu tehditler, siber güvenlik alanında sürekli güncellenmeyi ve yenilikçi savunma stratejilerinin geliştirilmesini gerektirmektedir. Siber güvenlik, yalnızca teknolojik önlemlerle sınırlı kalmayıp, eğitim ve farkındalık çalışmaları ile bütünsel bir yaklaşım gerektiren bir alan haline gelmiştir. Bu nedenle hem bireylerin hem de kurumların, siber güvenlik konusunda sürekli bilgi ve becerilerini güncellemeleri, teknolojik gelişmelere ayak uydurarak savunma mekanizmalarını kuvvetlendirmeleri büyük önem taşımaktadır.

İstenmeyen elektronik postalar, yaygın olarak spam mesajları olarak adlandırılmaktadır ve bu mesajlar sadece e-posta yoluyla değil, SMS, MMS, anlık mesajlaşma, arama motorları, bloglar ve VoIP gibi çeşitli elektronik iletişim kanalları aracılığıyla da gönderilebilmektedir. Bu tür iletileri daha geniş bir çerçevede, internetle ilişkili elektronik mesajlar, önemsiz postalar, haber gönderileri ve özellikle ticari amaçlı toplu gönderimler şeklinde tanımlamaktadır (Arunkrishna ve Mukunthan, 2020). Phishing, bilinen diğer adıyla oltalama veya yemleme, kullanıcıların finansal bilgilerine, örneğin banka ve kredi kartı hesaplarına erişmek amacıyla gerçekleştirilen dolandırıcılık girişimleridir ve bu süreçte kullanıcıların sosyal güvenlik numaraları, oturum açma bilgileri ve şifreleri gibi hassas bilgiler hedef alınmaktadır (Öztürk, 2014). Koklama (sniffing) ise, bilgisayar ağlarındaki veri akışını gizlice izleyerek bilgi toplama girişimidir (Oppliger, 2020).

Yanıltma ise sahte kimlikler kullanarak kullanıcı bilgilerine erişme girişimlerini ifade etmektedir (Öztürk, 2014). Hizmet engelleme saldırıları, DoS (Hizmeti Engelleme)

ve DDoS (Dağıtılmış Hizmeti Engelleme) olmak üzere ikiye ayrılır. DoS saldırıları, bir ağ veya sunucu tarafından sağlanan hizmetin bozulmasını amaçlarken, DDoS saldırıları birden fazla kaynaktan gelerek savunmanın zorlaşmasına yol açar. İçeriden yapılan saldırılar, kurum çalışanlarının daha az çaba ile sisteme zarar verebileceği, verileri bozabileceği veya çalabileceği durumları kapsamaktadır (Salim ve ark. 2020).

Siber tehditler, hizmet engelleme (DoS ve DDoS) saldırıları, kötü amaçlı yazılımlar, kimlik avı (phishing), istenmeyen e-posta (spam) ve ağ trafiği dinleme (sniffing, monitoring) gibi beş ana kategoriye ayrılmaktadır. DoS ve DDoS saldırıları, hedef sistemin kaynaklarını tüketerek hizmet verme yeteneğini engellemeyi amaçlayan, genellikle güvenlik açıklarından yararlanarak uzaktan gerçekleştirilen saldırılardır (Salim ve ark., 2020). Kötü amaçlı yazılımlar ise bilgisayar virüsleri, solucanlar, Truva atları, mantık bombaları, klavye kaydediciler, zombi veya bot ağları, istenmeyen reklam yazılımları ve casus yazılımları içerir ve siber güvenlik tehditlerinin önemli bir bölümünü oluşturur (Bijalwan, 2021). Özellikle virüsler, kullanıcı bilgisi dışında bir sisteme sızarak, kendi kendini kopyalayan veya mutasyon geçirebilen kötü amaçlı kodlardır ve bulaştıkları sistemlere zarar vermektedirler. Bu virüslerin tanımlanabilmesi için, imzalarını, davranışlarını, yayılma biçimlerini ve neden oldukları hasar türlerini bilmek gerekmektedir. Klavye izleme araçları, hem yazılım hem de donanım tabanlı olabilir ve kullanıcının tuş vuruşlarını kaydederek gizli bilgilere erişim sağlayabilir (Bijalwan, 2021). Botlar, gizli bir ordu oluşturmak ve sisteme uzaktan müdahale etmek için kullanılan programlardır. İstem dışı reklam yazılımları, kullanıcıların çevrimiçi davranışlarına göre özelleştirilmiş ticari içerik sunar. Casus yazılımlar ise, kullanıcıların bilgilerini gizlice toplar ve bir bilgisayara kurulduğunda kullanıcıdan habersiz faaliyet gösterir; ortalama bir kullanıcının bilgisayarında 28, kurum bilgisayarlarında ise en az bir casus yazılım programının bulunduğu belirtilmiştir (Salim ve ark. 2020).

2.2. TÜRKİYE'DE SİBER GÜVENLİK

Türkiye, siber güvenlik alanında hem saldırıların kaynağı hem de hedefi olarak küresel bir aktör konumundadır. Özellikle DDoS saldırıları konusunda dünya sıralamasında üst sıralarda yer alması, bu alandaki etkinliğini göstermektedir. Bu durum, bilgi ve iletişim teknolojilerinden etkin bir şekilde yararlanabilmenin, ulusal siber güvenlik çalışmalarının sürekliliği ve etkinliğine bağlı olduğunu göstermektedir.

Türkiye'nin ekonomik büyümesi için siber güvenliğin sağlanması, bireysel, kurumsal ve ulusal düzeyde kritik öneme sahiptir. COVID-19 pandemisi, teknolojik dönüşümü hızlandırarak siber güvenlik ihtiyaçlarını (altyapı, yeni teknolojiler, insan kaynakları, farkındalık) daha da artırmıştır (Çakır ve Uzun, 2021).

Yabancı ülkelerden alınan siber güvenlik ürün ve çözümlerinin kendileri birer siber güvenlik riski ve tehdidi (arka kapılar vb. güvenlik açıkları) oluşturduğu için, Türkiye'de yerli ve milli ürün ve çözümlerin geliştirilip kullanılmasına büyük önem verilmektedir (Aydemir, 2022). Siber uzayın ortaya çıkışı, bireyler ve hükümetler için çeşitli güvenlik tehditleri oluşturmuş, saldırganlar hükümetlerin güvenlik altyapılarına zarar vererek ciddi boyutta hasarlara neden olabilmektedirler (Gündoğdu, 2023). Siber saldırılar, kişisel ve kurumsal düzeyin ötesine geçerek ulusal güvenliği de tehdit etmekte, siber casusluğun ötesine geçerek siber savaş boyutlarına ulaşmaktadır. Bu bağlamda, siber güvenlik alanı dünya genelinde kritik bir öneme sahip olmakta ve sadece Türkiye'de değil, dünya genelinde büyük bir insan kaynağı ihtiyacı doğurmaktadır. 2019 yılı itibarıyla siber güvenlik alanında dünya genelinde 1,5 milyon iş gücüne ihtiyaç duyulduğu tahmin edilirken, Türkiye'de yaklaşık 15-20.000 siber güvenlik uzmanına ihtiyaç duyulduğu öngörülmektedir (Altınar, 2021). Siber tehditlerin sayısı ve çeşitliliği artarken, bu tehditlerin yol açtığı zararlar da giderek büyümektedir. Bu nedenle, siber tehditlerle mücadelede kaynakların doğru şekilde planlanması, detaylı risk analizleri yapılması ve teknolojik trendlere uygun kısa ve uzun vadeli planlamalar yapılması, güvenli bir siber uzayın temelini oluşturacaktır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020).

2.2.1. Yasal Düzenlemeler

Siber güvenlik, Türkiye'de başlangıçta asayiş ve hukuk alanında ele alınmış, ancak zamanla ulusal güvenlik boyutuna ulaşan bir konu haline gelmiştir. Bu süreçte, orduların beşinci bir savaş alanı olarak gördüğü siber alan, devletlerin yasal düzenlemelere odaklanmasına neden olmuştur. Türkiye'de siber suçlarla mücadele kapsamında ilk yasal düzenleme, 6 Haziran 1991'de 3756 Sayılı Türk Ceza Kanunu ile gerçekleştirilmiştir. Bu düzenleme, "Bilişim Alanında Suçlar" başlığı altında çeşitli suç unsurlarını tanımlamıştır (Kiziltan, 2007). 26 Eylül 2004 tarihinde kabul edilen 5237 sayılı Türk Ceza Kanunu ile bu alanda daha kapsamlı düzenlemeler yapılmış ve Madde 243, 244, 245 gibi maddelerle detaylandırılmıştır (Kiziltan, 2007). 18 Temmuz 2006'da ise 3713 sayılı Terörle

Mücadele Kanunu'nda yapılan değişikliklerle bazı bilişim suçları terör suçu kapsamına alınmıştır (Öcal, 2021). 23 Mayıs 2007'de yürürlüğe giren 5651 sayılı Kanun, internet ortamındaki yayınlar ve bu yayınlar yoluyla işlenen suçlarla ilgili düzenlemeleri içermiştir. Türkiye'nin siber suçlarla mücadelesinde önemli bir adım ise, Avrupa Siber Suçlar Sözleşmesine taraf olması olmuştur. Bu sözleşme, siber suçlarla mücadelede uluslararası iş birliğini vurgulayan ve 1 Temmuz 2004'te yürürlüğe giren ilk uluslararası anlaşma olarak önem taşımaktadır (Ozbek, 2015).

Bilgi Güvenliği Derneği'nin Haziran 2012'deki Siber Güvenlik Strateji Çalıştay'ında tavsiye edilen Ulusal Siber Güvenlik Stratejisi Belgesi, siber güvenliğin artırılması için çeşitli adımlar önermiştir. Bu adımlar arasında, farkındalığın artırılması, verilerin korunması, uluslararası iş birliğinin güçlendirilmesi ve siber güvenlik Ar-Ge politikalarının geliştirilmesi yer almaktadır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2012). 20 Haziran 2013'te yayımlanan "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", siber güvenlik mevzuatının geliştirilmesi ve kritik altyapıların korunması gibi konuları kapsamıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2013). "2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ise siber güvenlik risklerini azaltmaya ve siber savunmayı güçlendirmeye odaklanmıştır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2016).

Son yıllarda Türkiye'de siber güvenlik çalışmaları önemli bir ivme kazanmış, 5809 sayılı Elektronik Haberleşme Kanunu ile çeşitli politika ve stratejiler belirlenmiş, siber güvenlik prosedürleri ve standartları oluşturulmuştur. Ulaştırma ve Altyapı Bakanlığı'na verilen bu görev ve sorumluluklar kapsamında, eğitim ve farkındalık çalışmaları da büyük önem taşımaktadır (Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 2020). 10 Temmuz 2018 tarihinde kurulan Dijital Dönüşüm Ofisi, siber güvenlik konusunda proje geliştirme görevini üstlenmiş ve 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Bilgi ve İletişim Güvenliği Tedbirleri belirlenmiştir. Ayrıca, Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) siber saldırıların engellenmesi ve yaptırım uygulama yetkisi verilmiştir (Altınar, 2021).

2.2.2. Kurumlar ve Kuruluşlar

2.2.2.1. Bilgi Teknolojileri ve İletişim Kurumu (BTK)

Bilgi Teknolojileri ve İletişim Kurumu (BTK), 27 Ocak 2000 tarihinde Telsiz Kanunu'nda yapılan değişikliklerle Telekomünikasyon Kurumu olarak kurulmuş olup, 10 Kasım 2008'de Elektronik Haberleşme Kanunu ile mevcut adını almıştır (Gürkan, 2013). Türkiye'nin telekomünikasyon sektörünü düzenleyen ve denetleyen ilk resmi kurum olan BTK, yetkilendirme, denetim, ihtilaf çözümü, tüketici haklarının korunması ve sektör rekabetinin düzenlenmesi gibi temel sorumlulukları üstlenmektedir. Ayrıca, teknik yönergeler yayınlama ve spektrum yönetimi ile izleme gibi görevleri de yerine getirmektedir (Yorgancıoğlu ve Demircan, 2023).

2.2.2.2. Telekomünikasyon İletişim Başkanlığı (TİB)

Telekomünikasyon İletişim Başkanlığı (TİB), 2005 yılında telekomünikasyon ve internet hizmetlerindeki iletişim ve sinyal bilgilerinin denetimi ve kaydı amacıyla kurulmuştur (Altınır, 2021). Millî İstihbarat Teşkilâtı, Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı'ndan temsilciler içeren yapısıyla, faaliyetlerini doğrudan Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı'na raporlar (Altınır, 2021). TİB'in görevleri, internet hizmetlerinin güvenliği, içerik, yer, erişim ve toplu kullanım sağlayıcılarının denetimi gibi geniş bir alanı kapsar (Gödekli, 2013). Bu bağlamda, internet erişim engelleri, kullanıcı gizliliği ve ağ takibi gibi konularda yetkili merci olarak, internet üzerindeki işlemlerin izlenmesi, takibi, perdelenmesi ve filtrelenmesi için gerekli yazılım ve donanım kriterlerini belirleme sorumluluğunu taşır (Gödekli, 2013).

2.2.2.3. Siber Suçlarla Mücadele Daire Başkanlığı

Bilişim teknolojilerinin yaygınlaşmasıyla birlikte siber suçlarda görülen artış, Emniyet Genel Müdürlüğü bünyesinde 2011 yılında Bilişim Suçlarıyla Mücadele Daire Başkanlığı'nın kurulmasına yol açmıştır. Bu kuruluşun temel amacı, farklı birimlerde dağınık halde yürütülen siber suçlarla mücadele çalışmalarını tek bir çatı altında toplayarak daha etkili ve koordineli bir mücadele ortamı sağlamaktır. (Hekim ve Başbüyük, 2013). Şubat 2013'te ise bu birimin adı Siber Suçlarla Mücadele Daire

Başkanlığı olarak güncellenmiştir. Siber Suçlarla Mücadele Daire Başkanlığı, kendine aşağıdaki vizyonları belirlemiştir:

Siber suçlarla mücadele stratejileri geliştirmek ve uygulamak.

- Toplumda siber suçlar konusunda farkındalık ve bilinç düzeyini artırıcı çalışmalar yürütmek,
- Uluslararası alanda siber suçlarla mücadele iş birliğini geliştirmek ve güçlendirmek,
- Ülkeye yönelik siber suç tehditlerini analiz etmek, değerlendirmek ve bu tehditlere karşı önleyici ve proaktif tedbirler almak,
- Siber suçlar alanında uzmanlaşmış soruşturma ve adli bilişim personeli yetiştirmek ve bu alandaki insan kaynağını geliştirmek,
- Teknolojik gelişmeleri yakından takip ederek, siber suçlarla mücadele kapasitesini artırmak ve yeni teknolojileri bu mücadelede etkin bir şekilde kullanmak (Siber Suçlarla Mücadele Daire Başkanlığı, 2023).

Siber Suçlarla Mücadele Daire Başkanlığı, bu vizyon doğrultusunda, siber suçların tespiti, soruşturulması ve önlenmesi konusunda kritik bir rol oynamaktadır (Siber Suçlarla Mücadele Daire Başkanlığı, 2023). Kurumun faaliyetleri, bilişim suçları konusundaki uzmanlık ve deneyimi artırmak, bu alanda gerekli yasal ve teknik altyapının geliştirilmesi ve güncellenmesi, siber suçlarla mücadelede ulusal ve uluslararası iş birliklerinin güçlendirilmesi, toplumsal farkındalığın artırılması, siber suç tehditlerine karşı etkili stratejilerin geliştirilmesi ve uygulanması gibi geniş bir yelpazeyi kapsamaktadır (Erdem ve Özocak, 2017). Ayrıca, kurum siber güvenlik alanında yetkin ve deneyimli personel yetiştirme görevini de üstlenerek, siber suçlarla mücadelede etkin bir güç oluşturma hedefini gütmektedir. Bu doğrultuda, Siber Suçlarla Mücadele Daire Başkanlığı'nın Türkiye'nin siber güvenlik ekosisteminde önemli bir rol oynadığı ve siber suçlarla mücadeledeki kapasitesini sürekli olarak artırdığı görülmektedir (Siber Suçlarla Mücadele Daire Başkanlığı, 2023).

2.2.2.4. Siber Güvenlik Kurulu

Haziran 2012'de düzenlenen Siber Güvenlik Strateji Çalıştayını sonrasında, Türkiye'de siber güvenlik politikalarının yönetimi ve koordinasyonu amacıyla Ulusal Siber Güvenlik Kurulu'nun oluşturulması, 20 Ekim 2012 tarihinde Bakanlar Kurulu'nun

2012/3842 sayılı kararıyla resmiyet kazanmıştır. Bu kurul, siber güvenlikle ilgili politikaları şekillendirmek, hazırlanan plan, program, rapor ve standartları onaylamak ve bunların uygulanmasını etkin bir şekilde koordine etmek amacıyla kurulmuştur (Çakır ve Uzun, S2021). Kurulun yapısı, Ulaştırma, Denizcilik ve Haberleşme Bakanı başkanlığında ve çeşitli bakanlıkların müsteşarları, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı ve diğer ilgili kurumların üst düzey yöneticilerinden oluşmaktadır, bu da kurulun multidisipliner bir yapıya sahip olduğunu göstermektedir (Hekim ve Başbüyük, 2013). Bu kurulun kurulması, Türkiye'nin siber güvenlik alanında attığı stratejik adımlardan biri olarak değerlendirilmekte ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın bu alandaki koordinatör kurum olarak belirlenmesi, bu alandaki politikaların daha etkin bir şekilde yürütülmesini sağlamaktadır (Altınar, 2021).

Türkiye'nin siber güvenlikle ilgili yasal düzenlemeleri, 20 Ekim 2012 tarihinde 28447 sayılı Resmi Gazete'de yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile önemli bir dönüşüm geçirmiştir (Resmi Gazete, 2012). Bu karar öncesinde siber güvenlikten sorumlu ana kurum TÜBİTAK iken, bu kararla görev ve sorumluluklar Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na devredilmiştir (Kurnaz ve Önen, 2019). Bu değişiklik, kurulun görev ve yetkilerini daha net bir şekilde tanımlamış ve siber güvenlik alanında Türkiye'nin politika ve stratejilerinin belirlenmesinde kritik bir rol oynamıştır. Ayrıca, Türkiye'nin siber güvenlik alanında attığı adımlar, Siber Olaylara Müdahale Ekiplerinin Kuruluşu, Görevleri ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ gibi diğer yasal düzenlemelerle desteklenmiştir. 2008 yılında yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu da, siber güvenlikle ilgili yasal çerçevenin oluşturulmasında önemli bir rol oynamıştır. Bu düzenlemeler topluca, Türkiye'nin siber güvenlik alanında hem ulusal hem de uluslararası düzeyde etkin bir rol oynamasını sağlamakta, siber tehditlere karşı koymak için gerekli hukuki altyapıyı oluşturmakta ve ulusal siber güvenlik stratejisinin temelini oluşturmakta birer temel taş olarak önem taşımaktadır (Altınar, 2021).

2.2.2.5. Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Bilgi ve iletişim teknolojilerinin dünya genelinde hızla yaygınlaşması, siber ortamda tehditlerin artmasına neden olmuştur. Bu durum, ülkeleri kapsamlı idari, teknik ve

hukuki alt yapılar geliştirmeye itmiştir. Türkiye de bu gelişmeleri takip ederek, 20 Ekim 2012 tarihli Resmi Gazete'de yayımlanan Bakanlar Kurulu Kararı ile "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar"ı almış ve Siber Güvenlik Kurulu'nu oluşturmuştur (Resmi Gazete, 2012). Kurul, siber güvenlikle ilgili alınacak önlemleri, programları, raporları, usul ve esasları belirleyip onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamakla görevlendirilmiştir (Gençoğlu, 2021). Ayrıca, kurulun ilk toplantısında, ulusal ve uluslararası düzeyde siber güvenlik olaylarına müdahalede koordinasyon sağlamak amacıyla "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurulmasına karar verilmiştir. USOM, internet aktörleri, kolluk kuvvetleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasında iletişim ve koordinasyonu sağlamak, siber güvenlik olaylarına yönelik alarm, uyarı ve duyuru faaliyetleri yapmak ve kritik sektörlere yönelik siber saldırıların önlenmesinde koordinasyon sağlamakla görevlendirilmiştir (Sağıroğlu ve ark. 2019). SOME ise sektör ve kurum bazında oluşturulacak Siber Olaylara Müdahale Ekipleri'nin kısaltması olup, sektörel ve kurumsal bazda faaliyet göstermektedirler. USOM ve SOME'ler, siber olayların bertaraf edilmesi, olası zararların önlenmesi veya azaltılması ve siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde kritik bir öneme sahiptirler (Sağıroğlu ve ark. 2019).

2.2.2.6. Kurumsal SOME'lerin Görev ve Sorumlulukları

Bilgi ve iletişim teknolojilerinin hızlı yaygınlaşması, siber tehditlerin ulusal güvenlik üzerindeki etkisini artırarak ülkeleri yeni zorluklarla karşı karşıya bırakmıştır. Bu durum, gelişmiş idari, teknik ve hukuki altyapıların oluşturulmasını zorunlu kılmıştır. Türkiye, bu gelişmelere yanıt olarak 20 Ekim 2012 tarihli Bakanlar Kurulu Kararı ile "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna İlişkin Karar"ı kabul etmiş ve Siber Güvenlik Kurulu'nu kurmuştur (Resmi Gazete, 2012). Kurulun temel görevi, siber güvenlikle ilgili önlemleri belirlemek, ilgili program, rapor, usul, esas ve standartları onaylamak, uygulama ve koordinasyonu sağlamaktır. Bu kapsamda, Türkiye'de "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurulmuş ve faaliyetlerine başlamıştır. USOM'un görevleri arasında, internet aktörleri, kolluk kuvvetleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasında iletişim ve koordinasyonu sağlamak, siber güvenlik olaylarına yönelik alarm, uyarı ve duyuru

faaliyetleri yürütmek ve kritik sektörlere yönelik siber saldırıların önlenmesinde koordinasyonu sağlamak yer almaktadır (Yıldırım ve Kaplan, 2021).

Kurumsal Siber Olaylara Müdahale Ekipleri (SOME), farklı bakanlıklar ve bağlı kuruluşlar bünyesinde, kurumların özel ihtiyaçlarına göre oluşturulan birimlerdir. SOME'lerin temel sorumlulukları arasında, kurumlarına yönelik siber saldırılara karşı önleyici tedbirler almak, siber olaylara müdahale mekanizmaları geliştirmek ve kurumun bilgi güvenliğini sağlamak yer almaktadır (Bıçakcı ve ark., 2015). Ayrıca, siber olayların önlenmesi veya etkilerinin azaltılmasına yönelik teknik ve idari önerilerde bulunma görevini de üstlenirler. Bir siber olayla karşılaşmaları durumunda, SOME'ler Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve ilgili sektörel SOME'lerle bilgi paylaşımı ve koordinasyon sağlamakla yükümlüdürler. Olayın suç teşkil ettiği düşünülürse, durumu yetkili mercilere ve USOM'a bildirmeleri gerekmektedir (Yıldırım ve Kaplan, 2021).

25 Mart 2013 tarihli ve 4890 sayılı Bakanlar Kurulu Kararı, kritik altyapıların önemini vurgulamış ve bu altyapıları; can kaybına, büyük ekonomik zarara, ulusal güvenlik açıklarına veya toplumsal düzenin bozulmasına yol açabilecek bilişim sistemlerini içeren yapılar olarak tanımlamıştır. 2013-2014 Eylem Planı çerçevesinde, Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve USOM koordinasyonunda faaliyet gösterecek sektörel Siber Olaylara Müdahale Ekipleri (SOME) oluşturulmuştur (Bıçakcı ve ark., 2015). Bu yapılanmalar, siber olaylara müdahalede etkin bir rol oynayarak ulusal siber güvenlik kapasitesinin geliştirilmesine ve siber tehditlere karşı koyma kabiliyetinin artırılmasına katkı sağlamaktadır. Kurumsal SOME'ler, USOM ve Sektörel SOME'lerle iş birliği içerisinde siber güvenlik yönetimini sağlamak, siber olaylar öncesinde ve sonrasında gerekli tedbirleri almak ve koordinasyonu sağlamakla yükümlüdürler.

3. BÖLÜM

SİBER GÜVENLİK FARKINDALIĞI VE EĞİTİMİ

Bu bölüm başlığı altında siber güvenlik kavramı, siber güvenlik bilgisi, siber güvenlik farkındalığı, siber güvenlik davranışı ve siber güvenlik eğitimi ile ilgili yapılmış olan çalışmalar ele alınmıştır.

3.1. SİBER GÜVENLİK KAVRAMI

İnternet kullanıcı sayısının dünya genelinde her geçen gün artış göstermesi, siber güvenlik kavramının önemini daha da artırmıştır. Uluslararası Telekomünikasyon Birliği (ITU) 2021 verilerine göre, 2021 yılı sonu itibarıyla dünya genelinde yaklaşık 4.9 milyar kişi (%63) internet kullanıcısıdır ve bu sayı, 2019 yılına göre %17'lik bir artış göstermiştir (International Telecommunication Union, 2022). Artan internet kullanımı ile birlikte siber tehdit ve saldırılara maruz kalan kullanıcı sayısı da artmakta, teknolojik gelişmelerle birlikte siber suçlar da çeşitlenmekte ve artmaktadır (Salem, Moreb ve Rabayah, 2021). Bilgi teknolojilerinin hızla gelişmesiyle siber saldırı yöntemleri de yenilenmekte, bu durum siber güvenlik konusunu gündemde tutmaktadır (Tanrıverdi, 2020).

Siber güvenlik terimi, 1990'lı yılların başında ağa bağlı bilgisayarların güvenlik sorunlarını tanımlamak amacıyla bilgisayar bilimcileri tarafından kullanılmaya başlanmıştır. Zamanla siber güvenlik ve bilgi güvenliği kavramları sıklıkla birbirinin yerine kullanılsa da, bu iki kavram arasında önemli farklılıklar bulunmaktadır. Bilgi güvenliği, bilginin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasına odaklanırken, siber güvenlik bu unsurların yanı sıra siber uzay üzerinden erişilebilen tüm varlıkların ve bireylerin güvenliğini de kapsamaktadır (Solms ve Niekerk, 2013). Siber güvenlik, inkâr edememe ve kimlik doğrulama gibi ek güvenlik unsurlarını da içerir.

3.2. SİBER GÜVENLİK BİLGİSİ

Siber güvenliğin sağlanması, günümüzde sadece güvenlik yazılımlarının kullanılmasından öte, interneti kullanan bireylerin siber güvenlik konusunda bilinçlenmelerini ve bilgi sahibi olmalarını gerektirmektedir (Aksoğan, Bayer, Gülada ve Çelik, 2018). Siber güvenlik olaylarının temel nedenleri arasında insan hataları ve bilgi

eksiklikleri bulunmaktadır. Dolayısıyla, kullanıcıların siber saldırılardan korunması için bilgilendirilmesi ve siber güvenlik davranışlarının teşvik edilmesi büyük önem taşımaktadır. Siber güvenlik davranışlarının sergilenmesi için gerekli olan siber güvenlik bilgisi, bireylerin konuya olan ilgileri ve geçmiş tecrübeleri doğrultusunda şekillenmektedir. Bu bilgi, kullanıcıların siber tehditleri algılamalarına ve risklerin değerlendirilmesine yardımcı olmaktadır (Erol ve Sağıroğlu, 2018).

Siber tehditler arasında yığın e-posta, kayıt ediciler, sosyal mühendislik saldırıları, virüs, solucan, Truva atı, fidye yazılımı, casus yazılım ve reklam yazılımı gibi çeşitli formlar bulunmaktadır. Bu tehditlerin tanımları ve özellikleri, kullanıcıların siber güvenlik bilgilerini artırarak bu tehditlere karşı daha bilinçli ve etkin bir şekilde korunmalarını sağlamaktadır (Sağıroğlu, 2018). Kullanıcıların siber güvenlik bilgisinin eksik olması ve güvenli davranış sergilememeleri, siber ortamda güvende hissetmemelerine yol açmaktadır. Bu nedenle, güvenlik sorunlarının azaltılması veya engellenmesi için insanları güvenlik konusunda bilinçlendirmek ve eğitmek gerekmektedir (Kovačević, Putnik ve Tošković, 2020).

Eğitim programları, kullanıcıların siber güvenlik bilgilerini geliştirmede önemli bir rol oynamaktadır. Siber güvenlik bilgisi, farkındalık kazanmanın temel bir unsuru olarak kabul edilmektedir; ancak, bu bilginin yeterli düzeyde olmaması durumunda farkındalık kazanmak zorlaşabilir (Bostan ve Şengül, 2018). Kullanıcıların, siber güvenlik bilgisinin yeterli düzeyde olması ve farkındalık yaratılması, siber tehditlere karşı daha etkin koruma sağlamakta büyük önem taşımaktadır (Alotaibi ve Alfehaid, 2018). Bu bilgi ve farkındalık, siber güvenlik politikalarının ve stratejilerinin etkin şekilde uygulanmasını, birey ve kurumların siber tehditlere karşı daha hazırlıklı olmalarını ve siber güvenlikle ilgili olaylara hızlı ve doğru bir şekilde müdahale edebilmelerini sağlamaktadır. Bu nedenle, siber güvenlik eğitim ve bilgilendirme çalışmalarının sürekli olarak güncellenmesi, çeşitlenmesi ve toplumun her kesimine ulaştırılması siber güvenlik alanında ulusal ve uluslararası düzeyde etkin bir mücadele yürütülmesi için kritik bir öneme sahiptir.

3.3. SİBER GÜVENLİK FARKINDALIĞI

Siber güvenlik, günümüz dijital çağında hayati bir önem taşımaktadır. Bu kavram, Schatz, Behrend ve Meyer (2017) tarafından, bilgisayar ağları, aygıtlar ve değerli

verilerin yetkisiz erişimden korunması, bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin sağlanması süreci olarak tanımlanmıştır. İnsanların büyük bir kısmının zamanlarını dijital ortamlarda geçirmesi, dijital dünyadan kaynaklanan tehditlerin artmasına neden olmakta, bu durum da siber güvenlik kavramının önemini daha da artırmaktadır. Siber saldırıların giderek artan sıklığı, güvenlik yazılımlarının tek başına yeterli olmadığını ve internet kullanıcılarının siber güvenlik bilgisiyle donatılmasının gerekliliğini ortaya koymaktadır (Aksoğan, Akçayol ve Akgül, 2018).

Siber güvenlik farkındalığı, bireylerin, kurumların veya toplumların, siber güvenlik eksikliğinin potansiyel sonuçlarının bilincinde olma durumu olarak tanımlanabilir (Erol ve Sağiroğlu, 2018). Bu farkındalığın yüksek olması, siber güvenliğe yönelik önlemlerin alınmasını ve risklere karşı daha iyi korunmayı sağlayabilir. Tüketicilerin satın alma niyetlerinin siber güvenlik farkındalık düzeylerinden etkilenmesi, Algılanan Risk Teorisi ile açıklanmaktadır (Aggarwal ve ark., 2020). Çevrimiçi alışverişlerde, tüketicilerin algıladığı riskin azaltılması ve siber güvenliğin sağlanması, alışveriş deneyimini pozitif yönde etkiler. Araştırmalar, kullanıcıların siber saldırılara karşı bilgi güvenliği düzeylerinin yükselmesinin e-ticareti olumlu etkilediğini göstermektedir (Acar ve Çiçek, 2021). Ancak, artan siber güvenlik risklerinin çevrimiçi alışverişini olumsuz etkilediği de gözlemlenmiştir (Akdeniz ve Dursun, 2021). Tüketicilerin satın alma davranışları, yaş ve kuşak farklılıklarına göre değişkenlik gösterir. X, Y ve Z kuşakları arasında ürün satın alma davranışlarında farklılıklar olduğu tespit edilmiştir (Saritaş ve Barutçu, 2016). Bu bulgular, siber güvenlik farkındalığının tüketicilerin çevrimiçi alışveriş kararlarını ve davranışlarını doğrudan etkileyebileceğini ve bu etkinin kuşaklar arasında farklılaşabileceğini göstermektedir. Bu nedenle, siber güvenlik farkındalığı ve eğitiminin farklı kuşakların ihtiyaçlarına ve beklentilerine uygun şekilde özelleştirilmesi büyük önem taşımaktadır.

3.4. SİBER GÜVENLİK DAVRANIŞI

Siber güvenlik, günümüz teknolojik çağında vazgeçilmez bir öneme sahip olmuştur. Bu bağlamda, kullanıcıların siber güvenlik konusundaki davranışları ve bilgi düzeyleri, güvenlik olaylarının devam etmesindeki temel etmenler arasında yer almaktadır. Araştırmalar, bilgi seviyesi yüksek olan bireylerin, daha düşük bilgiye sahip kullanıcılara kıyasla daha etkili siber güvenlik davranışları sergilediklerini göstermektedir (Donald ve

Osei-Bryson, 2020). Özellikle, siber uzayda gerekli güvenlik önlemlerinin alınması ve güvenli davranışların benimsenmesi, artık bir zorunluluk haline gelmiştir.

Siber güvenlik davranışı, bireylerin siber tehditlere ve saldırılara karşı korunmak için aldıkları önlemleri ifade eder. Bu önlemler arasında anti-virüs yazılımı kullanımı, güvenli olmayan web sitelerinden kaçınma, tehditlere karşı dikkatli olma ve veri yedekleme gibi stratejiler bulunmaktadır (Hong ve Furnell, 2021). Coventry ve arkadaşlarının (2014) gerçekleştirdiği çalışmada, siber güvenlik davranışlarının temel unsurları şu şekilde belirlenmiştir:

1. Güçlü parolalar kullanımı: Birçok kullanıcı zayıf parolalar oluşturmakta ve aynı parolayı birden fazla hesap için kullanmaktadır.
2. Anti-virüs yazılımları ve güvenlik duvarı kullanımı: Kullanıcıların çoğu bu yazılımları etkin olarak kullanmayı ihmal etmektedir.
3. Güncel yazılım kullanımı: Teknolojik cihazlardaki yazılımların düzenli olarak güncellenmemesi yaygın bir sorundur.
4. Oturum sonlandırma ve bilgisayarı kapatma: Çoğu kullanıcı, hesaplarından çıkış yapmadan siteyi terk etmek gibi riskli davranışlarda bulunmaktadır.
5. Güvenilir internet bağlantıları, web siteleri ve cihazları kullanımı: Güvenilir olmayan kaynaklardan kaçınmanın önemi her ne kadar bilinse de bazı kullanıcılar bu önlemleri ihmal etmektedir.
6. Kişisel bilgilerin korunması ve paylaşımının sınırlanması: Çoğu kullanıcı, kişisel bilgilerini çevrimiçi olarak paylaşırken yeterli dikkat göstermemektedir.
7. Fiziksel çevrenin farkında olmak: Kullanılan cihazlar çevredeki kişiler tarafından gözlemlenebilir ve bu durum siber güvenliğe zarar verebilir.

3.5. SİBER GÜVENLİK EĞİTİMİ

Siber güvenlik eğitimi, bilgi teknolojileri çağında ve internetin yaygın kullanımıyla birlikte, her kullanıcı için elzem bir öneme sahip olmuştur. Bu alandaki eğitimlerin, sadece bilgi teknolojisi personelinin değil, internet kullanıcılarının tamamını kapsayacak şekilde genişletilmesi gerekmektedir. Son kullanıcıların siber güvenlik bilincinin geliştirilmesinin, güvenlik ihlallerinin önlenmesinde hayati bir rol oynadığı vurgulanmaktadır (Shaw et al., 2019). Etkili bir siber güvenlik eğitiminin, siber güvenliği sağlamanın en önemli adımlarından biri olduğu da belirtilmiştir (Alqahtani, 2022). Siber

güvenlik eğitimlerinin, bireylerin siber güvenlikle ilgili konuları anlamalarını, farkındalık kazanmalarını ve günlük çevrim içi güvenlik davranışlarını iyileştirmelerini hedeflemesi gerekmektedir (Cain, Edwards ve Still, 2018).

Siber güvenlik kültürünün oluşturulması için eğitim kurumlarının da bu konuda aktif rol oynaması gerekmektedir. Üniversite öğrencilerinin internet teknolojilerini kullanırken karşılaşılabilecekleri tehditler ve bu tehditlerden korunma yöntemleri konusunda bilinçlendirilmeleri gerektiği vurgulanmaktadır (Aljohani et al., 2021). Yoğun internet kullanıcısı olan bu yaş grubuna yönelik eğitim programlarının, siber tehditlerden korunma konusunda bilgi ve becerilerini artırmada önemli bir yere sahip olduğu belirtilmiştir. Siber güvenlik eğitimlerinin, saldırıları tamamen ortadan kaldırmasa da kullanıcıların farkındalıklarını artırarak önlemler almalarına katkıda bulunabileceği ifade edilmiştir (Muniandy et al., 2017). Bu eğitimlerin amacı, bireylerin bilgi ve iletişim teknolojilerini kullanırken karşılaşılabilecekleri tehditleri tanımalarını ve buna uygun davranışlar sergileyebilmelerini sağlamaktır (Salem et al., 2021). Tuğal, Almaz ve Sevi (2021) tarafından yapılan bir çalışmada, kullanıcılara verilmesi gereken eğitimlerin içeriği şu şekilde belirlenmiştir:

- Şifre Güvenliği Eğitimi,
- Güvenli İnternet Kullanma Eğitimi,
- E-Posta Güvenliği Eğitimi,
- Sosyal Mühendislik Eğitimi,
- Mobil Cihaz Güvenliği Eğitimi,
- Siber Tehdit Türleri Eğitimi,
- Kişisel Veri Gizliliği Eğitimi,
- Üniversite Uygulamaları Tanıtımı Eğitimi,
- Sorumluluklar ve Hukuki Süreçler Eğitimi (Tuğal, Almaz ve Sevi, 2021).

Bu eğitim konularının, kullanıcılara siber güvenlik alanında kapsamlı bir bilgi ve beceri seti kazandırılmasında büyük bir rol oynayacağı açıktır. Bu nedenle, siber güvenlik eğitiminin hem bireysel hem de toplumsal güvenliğin sağlanmasında anahtar bir faktör olduğu anlaşılmaktadır.

3.6. LİTERATÜR ÖZETİ

Siber güvenlik, modern teknolojik sistemlerin kritik bir yönünü oluşturmakta ve siber tehditlere karşı istihbarat toplamak, siber uzaydaki sistemlerin, ağların ve verilerin korunmasını sağlamak açısından hayati önem taşımaktadır (Humayun ve ark., 2020). Twitter gibi sosyal medya platformlarının kullanımı, siber tehdit istihbaratını toplamak için bir araç olarak incelenmiş ve siber tehdit tespitinde derin sinir ağları gibi tekniklerin kullanılması üzerine araştırmalar yapılmıştır (Dionísio ve ark., 2019). Ayrıca, yapay zekâ (AI) entegrasyonunun, potansiyel siber tehditlere ve saldırılara karşı savunma konusunda önemli bir ilerleme olarak vurgulandığı görülmektedir (Srivastava, 2019).

Jeong ve arkadaşları (2022) tarafından yapılan bir çalışmada, siber güvenlikle ilgili iş ve politika alanlarında ulusal kültürün anlaşılmasının önemi vurgulanmış ve kültürel faktörlerin özel ve kamu kuruluşlarının siber güvenlik yatırımlarına olan kapasitesini etkilediği belirtilmiştir. Kott ve Linkov (2021) tarafından siber sistemlerin siber direnç seviyesinin ölçülmesinin bir zorluk olduğu ve siber güvenliğin sıkı ve niceliksel ölçümünün geliştirilmesi gerektiği ifade edilmiştir. Kumar ve arkadaşları (2023) ise, siber tehdit avcılığı için güvenlik mekanizmaları tasarlanırken açıklanabilir yapay zekanın gerekliliğine dikkat çekerek, AI tabanlı siber güvenlik sistemlerinde şeffaflık ve yorumlana bilirliliğin önemini vurgulamıştır.

Ünver, Canbay ve Mirzaoglu'nun (2009) araştırması, bilgi güvenliği zafiyetlerine odaklanarak, internet üzerinden gerçekleştirilen işlemlerde kullanılan kimlik numaralarının kişisel bilgilere erişimde nasıl bir tehlike arz ettiğini incelemiştir. Lao ve diğerleri (2009) ise, sosyal ağlarda fark edilmeyen tehditleri ve bu tehditlerin kullanıcılar ve sosyal paylaşım siteleri üzerindeki etkilerini ayrıntılı bir şekilde ele almışlardır. Araştırmada, bu tehditlere karşı alınabilecek önlemler ve sosyal ağlar için özel bir güvenlik arabirimi geliştirilmesinin yanı sıra, kullanıcı farkındalığının artırılması önerisinde bulunulmuştur.

Bilgi güvenliği farkındalığının oluşumunda, Vroom ve von Solms (2004) tarafından yapılan araştırmada, bilgi güvenliği politikaları ve kurumsal bilgilendirme çalışmalarının yanı sıra, kurum kültürü ve kişisel özelliklerin de etkili olduğu ifade edilmiştir. Tekerek ve Tekerek (2013) ise, Kahramanmaraş ilindeki ilk ve orta öğretim öğrencilerine uyguladıkları özgün bir ölçekle, bu öğrencilerin bilgi güvenliği konusunda etik ve teknik konularda ne düzeyde farkındalığa sahip olduklarını belirlemiştir. Araştırma sonucunda,

öğrencilerin etik konularda yeterli farkındalığa sahip olduğu, ancak teknik konularda eksiklikler gösterdiği tespit edilmiştir. Bu durumun sebebi olarak, yetersiz bilgi ve bilgisayar güvenliği eğitim ve etkinlikleri gösterilmiş ve bu alandaki eğitimlerin artırılmasına yönelik önerilerde bulunulmuştur.

Kınay, Sözcü, Taşkın ve İpek (2014) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği, İstanbul'da özel bir üniversitenin öğrencilerine uygulanarak eğitim, bilgi ve davranış düzeylerindeki farkındalıkları ölçmüştür. Ölçek, farkındalık seviyelerini 'yüksek', 'orta' ve 'düşük' olarak sınıflandırmış ve her farkındalık seviyesine uygun kararlar tartışılmıştır. 2000-2009 yılları arasında Tayvan'da uygulanan ve devlet desteği alan İnternet Güvenliğinde Öğretmen Farkındalığı (TAIS) projesi, Tayvan Milli Eğitim Bakanlığı tarafından başlatılarak, ilk ve ortaokul öğretmenlerine yönelik gerçekleştirilmiştir. Proje, iletişim güvenliği, bilgi anlayışı ve uygunluk, çevrimiçi kişisel güvenlik, bilgisayar ve internet kullanım güvenliği gibi alanlarda öğretmenlerin bilgi ve farkındalığını artırmayı hedeflemiştir. Üç aşamalı proje kapsamında, bilgisayar öğretmenleri ile başlayıp, tüm ilk ve ortaokul öğretmenlerini kapsayacak şekilde genişletilmiş, ancak son aşamada veliler, lise öğrencileri, lise öğretmenleri ve öğretmen adaylarına ulaşılamamıştır. Projede eğitim seminerleri, atölye çalışmaları ve konferanslar gibi etkinlikler yer almıştır.

Eminağaoğlu ve Gökşen (2009), bilgi güvenliğinde başarının anahtarının bilinçli ve bilgili kullanıcılar olduğunu vurgulamışlardır. Gelişmiş donanım ve yazılımların, bilgi güvenliği konusunda bilgili ve bilinçli kullanıcılar tarafından kullanılması durumunda veri kayıplarının ve zararların önemli ölçüde önlenebileceğini belirtmişlerdir. Benzer şekilde, Şahinaslan ve arkadaşları (2009), kurumlarda bilgi güvenliğini sağlamak için teknik önlemlerin tek başına yeterli olmadığını, insan faktörünün kritik öneme sahip olduğunu ve bilgi güvenliği risklerinin ancak farkındalık düzeyinin artırılmasıyla önlenebileceğini ifade etmişlerdir. Bu çalışmalar, bilgi güvenliğinin sağlanmasında insan faktörünün kritik önemini ve bu alanda eğitim ve farkındalık çalışmalarının gerekliliğini vurgulamaktadır.

Siber güvenliği destekleyen olgunluk modellerinin rolü, Cains ve arkadaşları (2021) tarafından yapılan araştırmada detaylı bir şekilde incelenmiştir. Bu çalışmada, siber güvenlik ve siber güvenlik risklerinin bağlamsal çerçeveler ve insan faktörlerini içerecek şekilde kapsamlı tanımlarının önemi vurgulanmıştır. Ayrıca, Ali ve arkadaşları

(2021) ile Kang ve arkadaşları (2022) tarafından yapılan çalışmalarda, bilgi güvenliği bağlamında bireysel davranış, yetkinlik ve tutumlar arasındaki karmaşık etkileşimin, bilgi güvenliğinin sağlanmasında kritik rol oynadığı gösterilmiştir. Siber güvenlik profesyonellerinin karşılaştığı zorluklar, Elradi ve arkadaşları (2021) tarafından ele alınmış, siber güvenlik tehditleri, saldırıları, olaylara müdahale ve savunma mekanizmalarının çeşitli yönleriyle ilgili entegre bir platform çözümü önerilmiştir. Onwubiko ve Ouazzane (2019) ise, etkili bir Siber Güvenlik Operasyon Merkezi'nin (SOC) inşasının önemine dikkat çekmiş, SOCların olay yönetimi, saldırı tespiti ve sürekli güvenlik izleme sorumluluklarını vurgulamışlardır.

Yıldırım ve Varol (2013) tarafından yürütülen bir diğer araştırma, sosyal ağ kullanıcıları olan öğretim elemanları, üniversite öğrencileri ve diğer kullanıcıların sosyal ağlarda alınabilecek güvenlik önlemleri hakkındaki farkındalıklarını betimsel tarama modeli kullanarak değerlendirmiştir. Araştırmaya iki devlet üniversitesinden 211 öğrenci, 72 öğretim elemanı ve 23 diğer kurum çalışanı katılmıştır. Bulgular, öğrencilerin ve diğer kullanıcıların sosyal ağlardaki güvenlik önlemleri konusunda yeterli farkındalığa sahip olmadıklarını ve kişisel bilgilerinin kötüye kullanılmasına maruz kaldıklarını göstermiştir.

Özdemir ve Uluyol (2021) tarafından yapılan araştırma, kamu çalışanlarının bilgi güvenliği farkındalıklarını ortaya koymayı amaçlamıştır. Bu nicel araştırma, betimsel tarama modeli kullanılarak 501 katılımcı ile yürütülmüş ve Bilgi Güvenliği Farkındalık Ölçeği kullanılarak veri toplanmıştır. Araştırma sonucunda kamu çalışanlarının bilgi güvenliği farkındalığının orta seviyede olduğu ve özellikle teknik eğitim almış bilgi teknolojileri çalışanlarının ve 40 yaş altı katılımcıların yüksek farkındalık seviyelerine sahip olduğu belirlenmiştir. Karakaya ve Yetgin (2020) ise Karabük Üniversitesi çalışanlarına yönelik kişisel siber güvenlik üzerine bir araştırma yapmıştır. Bu çalışmada, sosyal ağlardan gelen arkadaşlık isteklerinin kabul edilmemesi, şahsi bilgisayar dışındaki cihazlarda bilgilerin tutulmaması ve antivirüs yazılımı kullanımı gibi konularda hipotezler test edilmiştir. Çalışma, katılımcıların dış tehditlere karşı farkındalıklarının olduğunu, ancak anti-virüs kullanımı konusunda eksiklikler gösterdiğini ortaya koymuştur.

Özbilen ve Çağlar (2020) tarafından Türk kamu sektöründe bilgi ve bilişim güvenliğinin mevcut durumunun tespiti amacıyla bir çalışma yapılmıştır. Bu çalışma,

siber güvenlik kavramı ve ilgili kurumların sorumluluklarına odaklanmış, veriler ikincil kaynaklardan toplanmış ve analiz edilmiştir. Çalışma, ülkemizde bilgi ve bilişim güvenliği konusunda önemli adımlar atıldığını, ancak daha ileri düzeyde hazırlıklı olunması gerektiğini vurgulamıştır.

Taner ve Kılıç (2019), güvenlik güçlerinin bilgi güvenliği farkındalığını ölçmeyi amaçlayan bir araştırma gerçekleştirmişlerdir. Siirt'te görev yapan jandarma ve polislerin bilgi güvenliği farkındalık düzeylerini inceleyen bu çalışma, genel olarak düşük bir farkındalık seviyesi tespit etmiştir. Bu sonuç, emniyet personelinin bilgi güvenliği farkındalığının artırılması için ek önlemler alınması gerektiğini göstermektedir. Yılmaz ve arkadaşları (2016) ile Karadağ ve Abuhanoğlu (2015) tarafından yapılan çalışmalar ise öğretmenlerin ve Gülhane Askeri Tıp Akademisi çalışanlarının bilgi güvenliği farkındalık seviyelerini incelemiş ve yaş ile unvan gibi faktörlerin bu farkındalık üzerinde etkili olduğunu ortaya koymuştur. Ayrıca, Akgün ve Topal (2005) tarafından eğitim fakültesi öğrencileri üzerinde yapılan bir çalışma, bilgi güvenliği eğitiminin önemini vurgulamıştır.

4. BÖLÜM

YÖNTEM

Bu bölüm başlığı altında çalışmanın hangi yöntem ile ele alındığı ayrıntılı olarak anlatılmıştır. Çalışmanın soruları, veri toplama araçları ve veri değerlendirme süreci bu bölüm içerisinde anlatılmıştır.

4.1. ARAŞTIRMA SORULARI

1. Siber güvenlik düzeyleri, genel özelliklere göre farklılık göstermekte midir?
2. Gizlilik boyutu, genel özelliklere göre farklılık göstermekte midir?
3. Kontrol-sahiplik boyutu, genel özelliklere göre farklılık göstermekte midir?
4. Bütünlük boyutu, genel özelliklere göre farklılık göstermekte midir?
5. Gerçeklik boyutu, genel özelliklere göre farklılık göstermekte midir?
6. Erişilebilirlik boyutu, genel özelliklere göre farklılık göstermekte midir?
7. Fayda boyutu, genel özelliklere göre farklılık göstermekte midir?

4.2. VERİ TOPLAMA ARAÇLARI

Veri toplama aracı, katılımcılarına yönelik genel bilgiler ve siber güvenlik ölçeğini içeren 2 bölümden oluşmaktadır.

4.2.1. Genel Bilgiler

Genel bilgiler bölümünde cinsiyet, yaş, eğitim durumu, meslekteki süre, günlük internet kullanım süresi ve internet kullanım amacı gibi sorulara yer verilmiştir.

4.2.2. Siber Güvenlik Ölçeği

Sevinç (2021) tarafından geliştirilen, 24 soruluk siber güvenlik ölçeği kullanılmıştır. Ölçek gizlilik (1-3 soru), kontrol-sahiplik (4-8), bütünlük (9-12), gerçeklik (13-17), erişilebilirlik (18-21) ve fayda (22-24) boyutlarından oluşmaktadır. Ölçekte “kesinlikle katılmıyorum” ile “kesinlikle katılıyorum” cevaplarını içeren, 5li likert ölçeği

kullanılmıştır. Ölçekten alınabilecek puan aralığı 24 ile 120 arasında değişmektedir. Ölçeğin 11, 13, 14, 15, 16, 17, ve 21'nci soruları ters kodlanmaktadır.

4.2.3. Siber Güvenlik Ölçeğinin Güvenirliliği ve Dağılım Özelliği

Katılımcıların araştırmada kullanılan siber güvenlik ölçeğine yönelik yapılmış olan güvenirlilik ve dağılım özellikleri Tablo 1'de gösterilmiştir.

Tablo 1. Güvenirlilik ve Dağılım Özellikleri

	Cronbach Alpha	Madde Sayısı	Çarpıklık	Basıklık
Siber Güvenlik Ölçeği	0,880	24	0,286	-0,280
Gizlilik	0,810	3	-0,152	-0,068
Kontrol-Sahiplik	0,822	5	-0,416	-0,381
Bütünlük	0,752	4	-0,078	-0,351
Gerçeklik	0,771	5	-0,939	1,007
Erişilebilirlik	0,807	4	0,074	-0,524
Fayda	0,704	3	-0,539	0,435

Güvenirlilik analizi için, genellikle Cronbach Alpha katsayısı kullanılmaktadır. Cronbach Alpha katsayısının en az 0,7 olması arzu edilmektedir (Karagöz; 2021). Karagöz (2021)'e göre, siber güvenlik ölçeği ve boyutlarının ait Cronbach Alpha katsayısı güvenilir düzeydedir.

Verilerin normal dağılım gösterip göstermediğini anlamanın yollarından biri, çarpıklık ve basıklık değerlerine bakmaktır. Çarpıklık ve basıklık değerleri -1,5 ile +1,5 arasında yer alması, verilerin normal bir dağılıma sahip olduğunu göstermektedir (Tabachnick ve Fidell; 2013). Tabachnick ve Fidell (2013)'e göre, siber güvenlik ölçeği ve boyutlarına ait çarpıklık ve basıklık değerlerinin normal dağılım sınırları içerisinde yer aldığı görülmektedir.

4.3. VERİ DEĞERLENDİRME SÜRECİ

Araştırmada toplanan verilerin analiz edilebilmesi için, IBM SPSS 28 paket programı kullanılmıştır. Araştırma parametreleri hakkında tanımlayıcı istatistikler frekans analizi yapılarak verilmiştir. Kategorik parametreler için sayı ve yüzde, sayısal değişkenler için ise ortalama, standart sapma, minimum ve maksimum değerlerden faydalanılmıştır. Sayısal değişkenler normallik varsayımları, çarpıklık basıklık değerleri ile değerlendirilmiştir. Verilerin normal dağılım gösterdiği tespit edilmiş olması

sebebiyle, bağımsız örneklem T-testi ve Anova (tek yönlü varyans) analizi kullanılmıştır. Anova analizinin anlamlı çıkması durumunda, hangi gruplar arasındaki farkın anlamlı olduğunu belirlemek amacıyla Post-Hoc testlerinden Bonferroni testi kullanılmıştır.

Araştırma raporu oluşturulurken, anlamlılık düzeyi için %95 güven aralığı ($p < ,05$) kullanılmıştır.



5. BÖLÜM

BULGULAR

5.1. KATILIMCILARA YÖNELİK TANIMLAYICI BULGULAR

Çalışmaya katılım gösteren 302 emniyet personeline yönelik tanımlayıcı bilgiler Tablo 2’de gösterilmiştir.

Tablo 2. Sosyo-Demografik Özelliklere Yönelik Bulgular

Genel Bilgiler		n	%
Cinsiyet	Erkek	273	90,4
	Kadın	29	9,6
Yaş	18-25 Yaş	6	2,0
	26-35 Yaş	229	75,8
	36-45 Yaş	44	14,6
	46 Yaş ve Üzeri	23	7,6
Eğitim	Lise	7	2,3
	Önlisans	32	10,6
	Lisans	232	76,8
	Yüksek Lisans	31	10,3
Meslekteki Süre	2-5 Yıl	36	11,9
	6-10 Yıl	186	61,7
	11-15 Yıl	40	13,2
	16 Yıl ve Üzeri	40	13,2
Günlük İnternet Kullanım Süresi	1-2 Saat	42	13,9
	3-4 Saat	154	51,0
	5-7 Saat	74	24,5
	8 Saat ve Üzeri	32	10,6
İnternet Kullanım Amacı*	Mobil Bankacılık	260	86,1
	e-devlet Hizmetleri	193	63,9
	e-ticaret Alışverişi	189	62,6
	Diğer	51	16,9

*Çoklu Cevap

Katılımcıların 273’ü (90,4) erkek, 229’u (%75,8) 26-35 yaşa aralığındadır. Çalışmaya katılan emniyet personelinin 232’si (%76,8) lisans mezunu ve 186’sı (%61,7) 6-10 yıllık mesleki süreye sahiptir. Katılımcıların 154’ü (%51) günlük 3-4 saat interneti kullandığı belirtmiştir. Emniyet personelinin 260 ‘ı(%88,1) personel mobil bankacılık, 193’ü (%63,9) e-devlet hizmetleri ve 189’u (%62,6) e-ticaret alışverişi yapmanın internet kullanım amacı olduğunu belirtmiştir. Katılımcıların 51’i ise, haber, eğlence, sosyal medya gibi diğer nedenlerle internet kullandığını belirtmiştir.

5.2. SİBER GÜVENLİK ÖLÇEĞİNE YÖNELİK GEÇERLİK VE GÜVENİRLİLİK ANALİZLERİ

Siber güvenlik ölçeğine yönelik yapılmış olan açıklayıcı faktör analizi, doğrulayıcı faktör analizi ve güvenirlilik analizi sonuçları bu başlık altında sunulmuştur.

5.2.1. Açıklayıcı Faktör Analizi (AFA) Sonuçları

Açıklayıcı faktör analizi, çok sayıdaki değişkeni belirli sayıda gruplara ayırarak, değişkenler arasındaki ilişkiyi maksimum ve gruplar arasındaki ilişkiyi ise minimum yaparak, grupları yeni değişkenlere dönüştüren bir analiz türüdür (Karagöz; 2021:639). Faktör analizinde varimax döndürme yöntemi kullanılmıştır. Analiz sonucunda, Kaiser Maier Olkin (KMO) ve Barlett küresellik testi sonuçları değerlendirilmiştir. KMO değerinin 0,6 üzerinde olması, örneklemin faktör analizi için yeterli olacaktır. Barlett küresellik testinin anlamlı olması ($p<0,05$), faktör analizi yapılabileceği anlamına gelmektedir. Sonrasında, faktör yüklerinin en az 0,4'ün üzerinde olmasına dikkat edilmiştir (Gürbüz ve Şahin; 2016, 311).

Siber güvenlik ölçeğinin yapısını belirlemek amacıyla yapılmış olan açıklayıcı faktör analizi sonuçları Tablo 3'de gösterilmiştir.

Siber güvenlik ölçeğinin orijinali altı boyuttan oluşmaktadır. Tablo 3.'de görüldüğü gibi siber güvenlik ölçeği, bu çalışmada da altı boyuttan oluşmaktadır. KMO değerinin 0,812 olması, örneklemin faktör analizi için oldukça yeterli olduğunu göstermektedir. Barlett küresellik testi sonucu ($p<0,05$) ise, anlamlıdır. Binişik ve çapraz yüklenme eğiliminde olan maddeler bulunmamaktadır. Siber güvenlik ölçeğine ait maddeler, toplam varyansın %63,05'ini açıklamaktadır. Alt boyutlardan gizlilik %23,47; kontrol %11,86; bütünlük %9,80, erişebilirlik %6,76 ve fayda %3,96, toplam varyansın açıklanmasına katkı sağlamaktadır. Madde faktör yüklerinin 0,493 ile 0,907 aralığında değiştiği görülmektedir. Bu sonuçlar siber güvenlik ölçeğinin geçerliliğinin sağlandığını göstermektedir.

Tablo 3. AFA Analizi Sonuçları

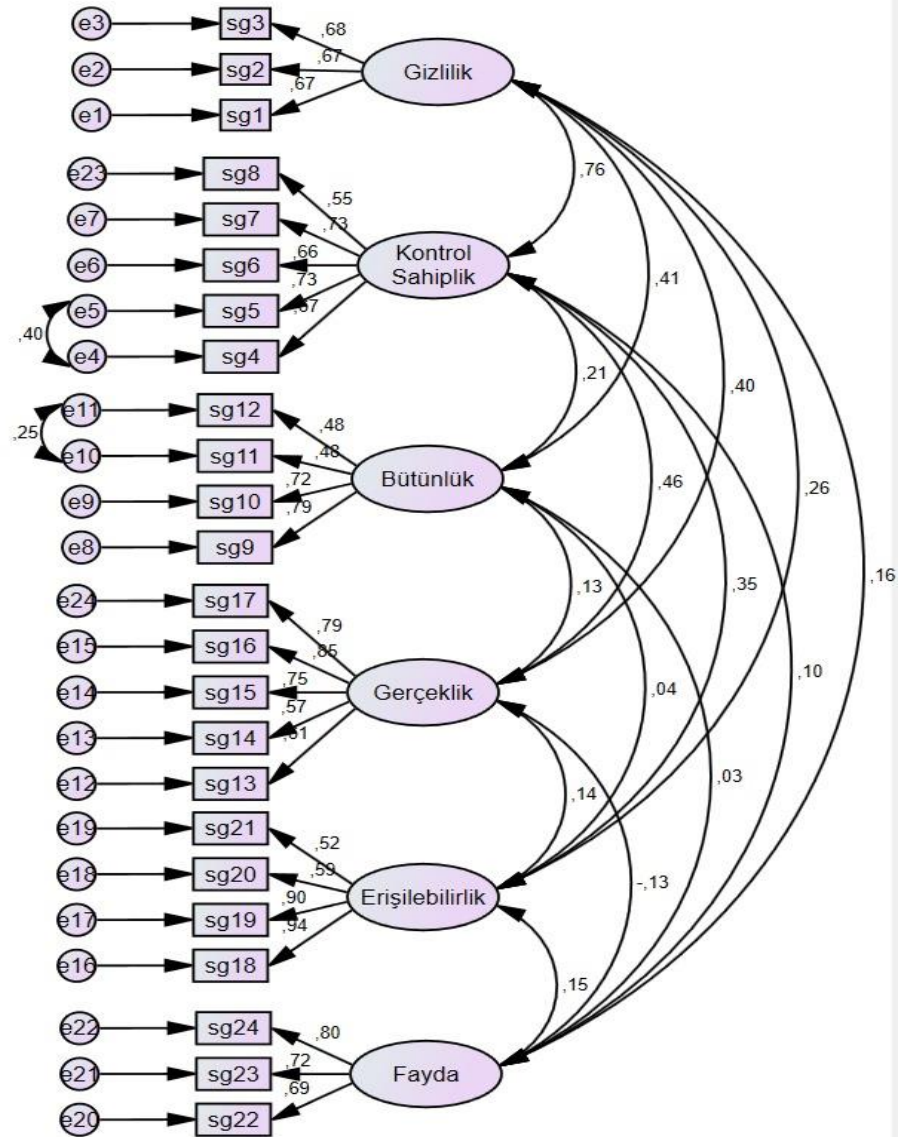
Ölçek Maddeleri	Gizlilik	Kontrol	Bütünlük	Gerçeklik	Erişebilirlik	Fayda
1	,493					
2	,857					
3	,661					
4		,828				
5		,892				
6		,636				
7		,608				
8		,561				
9			,857			
10			,782			
11			,600			
12			,626			
13				,701		
14				,688		
15				,802		
16				,852		
17				,822		
18					,907	
19					,895	
20					,754	
21					,594	
22						,785
23						,838
24						,876
Varyans:	23,473	11,865	9,803	7,384	6,760	3,968
Toplam Varyans: 63,053						
KMO: 0,812; Bartlett küresellik testi: 2886,403; p<0,05						

5.2.2. Doğrulayıcı Faktör Analizi (DFA) Sonuçları

Doğrulayıcı faktör analizi (DFA), önceden geliştirilmiş, önceki çalışmalarda kullanılmış, kuramsal dayanağı olan veya modelin doğruluğunu teyit etmek için kullanılan bir analiz türüdür. Araştırma verilerin normal dağılım göstermesi nedeniyle maximum likelihood hesaplama yöntemi kullanılmıştır. Faktör analizinde uyum iyiliği indeksine ait değerlerin, kabul edilebilir seviyede olması gerekmektedir (Gürbüz ve Şahin; 2021).

Siber güvenlik ölçeğine yönelik yapılmış olan birinci düzey doğrulayıcı faktör analizi sonuçları Şekil 1’de gösterilmiştir.

Altı alt boyutlu ve toplam 24 maddeden oluşan siber güvenlik ölçeğinin birinci düzey faktöriyel yapısı, AMOS 24 paket programı kullanılarak test edilmiştir. Verilerin normal dağılım göstermesi nedeniyle maximum likelihood hesaplama yöntemi kullanılmıştır (Gürbüz ve Şahin; 2019). Analiz sonucunda, tüm maddelerin faktör yükünün 0,54 ile 0,94 arasında olduğu belirlenmiştir. Birinci düzey DFA sonucunda elde edilen uyum değerleri (χ^2 [65, N=302]=385,004; $p<0,01$; $\chi^2/df=1,638$, RMSEA=0,046; GFI=0,905; AGFI=0,878; CFI=0,944; IFI=0,945; TLI=0,935), Gürbüz ve Şahin (2021) ile Karagöz (2021)'e göre kabul edilebilir düzeydedir. Bu sonuçlar, araştırmadan elde edilen verilerin siber güvenlik ölçeğinin öngörülen kurumsal altyapısı (24 maddeli ve 6 faktörlü) ile uyumlu olduğunu göstermektedir.



Şekil 1. DFA Analizi Sonuçları

5.2.3. Güvenirlilik Analizi Sonuçları ve Dağılım Özellikleri

Katılımcıların araştırmada kullanılan siber güvenlik ölçeğine yönelik yapılmış olan güvenirlilik ve dağılım özellikleri Tablo 4’te gösterilmiştir.

Tablo 4. Güvenirlilik ve Dağılım Özellikleri

	Cronbach Alpha	Madde Sayısı	Çarpıklık	Basıklık
Siber Güvenlik Ölçeği	0,822	24	0,332	-0,186
Gizlilik	0,713	3	-0,204	0,004
Kontrol-Sahiplik	0,805	5	-0,416	-0,381
Bütünlük	0,726	4	-0,362	0,401
Gerçeklik	0,838	5	-0,939	1,007
Erişilebilirlik	0,822	4	-0,226	-0,451
Fayda	0,777	3	-0,661	0,574

Güvenirlilik analizi için, genellikle Cronbach Alpha katsayısı kullanılmaktadır. Cronbach Alpha katsayısının en az 0,7 olması arzu edilmektedir (Karagöz; 2021). Karagöz (2021)’e göre, siber güvenlik ölçeği ve boyutlarının ait Cronbach Alpha katsayısı güvenilir düzeydedir.

Verilerin normal dağılım gösterip göstermediğini değerlendirmek için çarpıklık ve basıklık katsayıları incelenir. Tabachnick ve Fidell (2013), bu değerlerin -1.5 ile +1.5 aralığında olması durumunda verilerin normal dağılıma uygun olduğunu belirtmektedir. Siber güvenlik ölçeği ve alt boyutlarının çarpıklık ve basıklık değerlerinin bu aralıkta olduğu görülmüştür (Tabachnick ve Fidell, 2013).

5.3. SİBER GÜVENLİK ÖLÇEĞİNE İLİŞKİN BULGULAR

Katılımcıların siber güvenlik ölçeğinden almış oldukları puan ortalamaları ve almış oldukları minimum maksimum puan ortalamaları Tablo 5’te gösterilmiştir.

Tablo 5. Katılımcıların Siber Güvenlik Durumları

Ölçek ve Alt Boyutları	$\bar{X}$	Ss	Alınan	
			Min.	Maks.
Siber Güvenlik Ölçeği	94,41	9,71	73	120
Gizlilik	12,72	1,56	7	15
Kontrol-Sahiplik	21,73	2,71	12	25
Bütünlük	16,27	2,35	8	20
Gerçeklik	20,04	4,06	5	25
Erişilebilirlik	13,31	3,69	4	20
Fayda	10,34	2,48	3	15

Katılımcıların siber güvenlik ölçeğinden 94,41 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Ölçekten alınabilecek toplam puan 24 ile 120 arasında değişmektedir.

Katılımcıların gizlilik boyutundan ölçeğinden 12,72 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Gizlilik boyutundan alınabilecek toplam puan 3 ile 15 arasında değişmektedir.

Katılımcıların kontrol-sahiplik boyutundan ölçeğinden 21,73 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Kontrol-sahiplik boyutundan alınabilecek toplam puan 5 ile 25 arasında değişmektedir.

Katılımcıların bütünlük boyutundan ölçeğinden 16,27 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Bütünlük boyutundan alınabilecek toplam puan 4 ile 20 arasında değişmektedir.

Katılımcıların gerçeklik boyutundan ölçeğinden 20,04 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Gerçeklik boyutundan alınabilecek toplam puan 5 ile 25 arasında değişmektedir.

Katılımcıların erişebilirlik boyutundan ölçeğinden 13,31 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Erişebilirlik boyutundan alınabilecek toplam puan 4 ile 20 arasında değişmektedir.

Katılımcıların fayda boyutundan ölçeğinden 10,34 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Fayda boyutundan alınabilecek toplam puan 3 ile 15 arasında değişmektedir.

Katılımcıların gerçeklik boyutundan ölçeğinden 20,04 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Gerçeklik boyutundan alınabilecek toplam puan 5 ile 25 arasında değişmektedir.

Katılımcıların erişebilirlik boyutundan ölçeğinden 13,19 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Erişebilirlik boyutundan alınabilecek toplam puan 4 ile 20 arasında değişmektedir.

Katılımcıların fayda boyutundan ölçeğinden 10,08 toplam puan ortalamasına sahip olduğu tespit edilmiştir. Fayda boyutundan alınabilecek toplam puan 3 ile 15 arasında değişmektedir.

5.4. SİBER GÜVENLİĞİN SOSYODEMOGRAFİK ÖZELLİKLERE GÖRE İNCELENMESİ

Katılımcıların siber güvenlik ölçeğinden almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 6’te gösterilmiştir.

Tablo 6. Siber Güvenlik ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	94,50	9,80	t=0,914	0,435
	Kadın	93,44	8,93		
Yaş	18-25 Yaş	94,50	9,69	F=1,434	0,233
	26-35 Yaş	94,13	9,54		
	36-45 Yaş	96,52	10,71		
	46 Yaş ve Üzeri	93,00	9,43		
Eğitim	Lise	87,85	6,91	F=3,006	0,031*
	Önlisans	94,93	9,74		
	Lisans	90,78	8,11		
	Yüksek Lisans	95,64	10,47		
Meslekteki Süre	2-5 Yıl	95,25	8,73	F=2,044	0,108
	6-10 Yıl	94,54	9,73		
	11-15 Yıl	91,20	8,13		
	16 Yıl ve Üzeri	96,22	11,38		
Günlük İnternet Kullanım Süresi	1-2 Saat	96,00	9,30	F=4,104	0,007*
	3-4 Saat	93,53	9,28		
	5-7 Saat	93,16	10,19		
	8 Saat ve Üzeri	99,37	9,77		

*p<0,05

Erkeklerin ($\bar{X}$ =94,50), kadınlara ($\bar{X}$ =93,44) göre daha yüksek siber güvenlik toplam puan ortalamasına sahip oldukları görülmüştür. Ancak cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (t=0,914; p>0,05).

18-25 yaş aralığındaki katılımcıların ($\bar{X}$ =94,50), 26-35 yaş aralığındaki katılımcıların ($\bar{X}$ =94,13), 36-45 yaş aralığındaki katılımcıların ($\bar{X}$ =96,52) ve 46 yaş üzerindeki katılımcıların ($\bar{X}$ =93,00) siber güvenlik toplam puan ortalamasına sahip oldukları görülmüştür. Ancak yaşa göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (F=1,434; p>0,05).

Lise mezunu katılımcıların ($\bar{X}$ =87,85), önlisans mezunu katılımcıların ($\bar{X}$ =94,93), lisans mezunu katılımcıların ($\bar{X}$ =90,78) ve yüksek lisans mezunu katılımcıların ($\bar{X}$ =95,64) siber güvenlik toplam puan ortalamasına sahip oldukları görülmüştür (F=3,006; p<0,05).

Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; önlisans mezunu katılımcıların siber güvenlik toplam puan ortalamalarının, lisans mezunu katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}=95,25$), 6-10 yıl aralığında olan katılımcıların ($\bar{X}=94,54$), 11-15 yıl aralığında olan katılımcıların ($\bar{X}=91,20$) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}=96,22$) siber güvenlik toplam puan ortalamasına sahip oldukları görülmüştür. Ancak mesleki süreye göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=2,044$; $p>0,05$).

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=96,00$), 3-4 saat olan katılımcıların ($\bar{X}=93,53$), 5-7 saat olan katılımcıların ($\bar{X}=93,16$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=99,37$) siber güvenlik toplam puan ortalamasına sahip oldukları görülmüştür ($F=4,104$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; 8 saat üzerinde internet kullanımı olan katılımcıların siber güvenlik toplam puan ortalamalarının, 3-4 saat ve 5-7 saat internet kullanımı olan katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

5.4.1. Gizlilik boyutunun sosyodemografik özelliklere göre incelenmesi

Katılımcıların gizlilik boyutundan almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 7’te gösterilmiştir.

Tablo 7. Gizlilik Boyutu ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	12,71	1,56	t=-0,158	0,875
	Kadın	12,75	1,50		
Yaş	18-25 Yaş	12,83	1,32	F=0,677	0,567
	26-35 Yaş	12,64	1,53		
	36-45 Yaş	12,88	1,74		
	46 Yaş ve Üzeri	13,04	1,49		
Eğitim	Lise	11,85	1,06	F=2,775	0,042*
	Önlisans	12,71	1,58		
	Lisans	12,34	1,51		
	Yüksek Lisans	13,29	1,32		
Meslekteki Süre	2-5 Yıl	12,88	1,48	F=0,641	0,589
	6-10 Yıl	12,62	1,55		
	11-15 Yıl	12,72	1,60		
	16 Yıl ve Üzeri	12,95	1,61		
Günlük İnternet Kullanım Süresi	1-2 Saat	13,00	1,62	F=2,650	0,049*
	3-4 Saat	12,63	1,48		
	5-7 Saat	12,47	1,61		
	8 Saat ve Üzeri	13,28	1,54		

*p<0,05

Erkeklerin ($\bar{X}$ =12,71), kadınlara ($\bar{X}$ =12,75) göre daha düşük gizlilik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (t=-0,158; p>0,05).

18-25 yaş aralığındaki katılımcıların ($\bar{X}$ =12,83), 26-35 yaş aralığındaki katılımcıların ($\bar{X}$ =12,64), 36-45 yaş aralığındaki katılımcıların ($\bar{X}$ =12,88) ve 46 yaş üzerindeki katılımcıların ($\bar{X}$ =13,04) gizlilik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak yaşa göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (F=0,677; p>0,05).

Lise mezunu katılımcıların ($\bar{X}$ =11,85), ön lisans mezunu katılımcıların ($\bar{X}$ =12,71), lisans mezunu katılımcıların ($\bar{X}$ =12,34) ve yüksek lisans mezunu katılımcıların ($\bar{X}$ =13,29) gizlilik boyutu toplam puan ortalamasına sahip oldukları görülmüştür (F=2,775; p<0,05). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; yüksek lisans mezunu katılımcıların gizlilik boyutu toplam puan ortalamalarının, lisans mezunu katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}$ =12,88), 6-10 yıl aralığında olan katılımcıların ($\bar{X}$ =12,62), 11-15 yıl aralığında olan katılımcıların ($\bar{X}$ =12,72) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}$ =12,95) gizlilik boyutu toplam puan ortalamasına sahip

oldukları görülmüştür. Ancak mesleki süreye göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=0,641$; $p>0,05$).

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=13,00$), 3-4 saat olan katılımcıların ($\bar{X}=12,63$), 5-7 saat olan katılımcıların ($\bar{X}=12,47$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=13,28$) gizlilik boyutu toplam puan ortalamasına sahip oldukları görülmüştür ($F=2,650$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; 8 saat üzerinde internet kullanımı olan katılımcıların gizlilik boyutu toplam puan ortalamalarının, 5-7 saat internet kullanımı olan katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

5.4.2. Kontrol-sahiplik boyutunun sosyodemografik özelliklere göre incelenmesi

Katılımcıların kontrol-sahiplik boyutundan almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 8’te gösterilmiştir.

Tablo 8. Kontrol-Sahiplik Boyutu ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	21,77	2,71	$t=0,944$	0,346
	Kadın	21,27	2,75		
Yaş	18-25 Yaş	22,16	2,78	$F=1,728$	0,161
	26-35 Yaş	21,70	2,63		
	36-45 Yaş	22,29	2,96		
	46 Yaş ve Üzeri	20,73	2,86		
Eğitim	Lise	20,57	2,29	$F=0,798$	0,496
	Önlisans	21,81	2,73		
	Lisans	21,28	2,57		
	Yüksek Lisans	21,80	2,89		
Meslekteki Süre	2-5 Yıl	22,05	2,58	$F=0,634$	0,594
	6-10 Yıl	21,80	2,73		
	11-15 Yıl	21,32	2,58		
	16 Yıl ve Üzeri	21,47	2,89		
Günlük İnternet Kullanım Süresi	1-2 Saat	22,00	2,69	$F=2,717$	0,045*
	3-4 Saat	21,46	2,83		
	5-7 Saat	21,60	2,40		
	8 Saat ve Üzeri	22,90	2,56		

* $p<0,05$

Erkeklerin ($\bar{X}=21,77$), kadınlara ($\bar{X}=21,27$) göre daha yüksek kontrol-sahiplik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($t=0,944$; $p>0,05$).

18-25 yaş aralığındaki katılımcıların ($\bar{X}=22,16$), 26-35 yaş aralığındaki katılımcıların ($\bar{X}=21,70$), 36-45 yaş aralığındaki katılımcıların ($\bar{X}=22,29$) ve 46 yaş üzerindeki katılımcıların ($\bar{X}=20,73$) kontrol-sahiplik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak yaşa göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=1,728$; $p>0,05$).

Lise mezunu katılımcıların ($\bar{X}=20,57$), önlisans mezunu katılımcıların ($\bar{X}=21,81$), lisans mezunu katılımcıların ($\bar{X}=21,28$) ve yüksek lisans mezunu katılımcıların ($\bar{X}=21,80$) kontrol-sahiplik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak eğitim durumuna göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=0,798$; $p>0,05$).

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}=22,05$), 6-10 yıl aralığında olan katılımcıların ($\bar{X}=21,80$), 11-15 yıl aralığında olan katılımcıların ($\bar{X}=21,32$) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}=21,47$) kontrol-sahiplik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak mesleki süreye göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=0,634$; $p>0,05$).

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=22,00$), 3-4 saat olan katılımcıların ($\bar{X}=21,46$), 5-7 saat olan katılımcıların ($\bar{X}=21,60$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=22,90$) kontrol-sahiplik boyutu toplam puan ortalamasına sahip oldukları görülmüştür ($F=2,717$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; 8 saat üzerinde internet kullanımı olan katılımcıların kontrol-sahiplik boyutu toplam puan ortalamalarının, 3-4 saat internet kullanımı olan katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

5.4.2. Bütünlük boyutunun sosyodemografik özelliklere göre incelenmesi

Katılımcıların bütünlük boyutundan almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 9'da gösterilmiştir.

Tablo 9. Bütünlük Boyutu ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	16,26	2,32	t=-0,18	0,985
	Kadın	16,27	2,63		
Yaş	18-25 Yaş	16,50	2,58	F=2,235	0,084
	26-35 Yaş	16,07	2,42		
	36-45 Yaş	16,88	2,01		
	46 Yaş ve Üzeri	16,95	1,94		
Eğitim	Lise	15,00	1,00	F=1,335	0,263
	Önlisans	16,25	2,40		
	Lisans	16,12	1,89		
	Yüksek Lisans	16,83	2,47		
Meslekteki Süre	2-5 Yıl	16,25	2,22	F=0,690	0,559
	6-10 Yıl	16,23	2,43		
	11-15 Yıl	16,00	2,48		
	16 Yıl ve Üzeri	16,72	1,92		
Günlük İnternet Kullanım Süresi	1-2 Saat	16,69	2,31	F=3,311	0,020*
	3-4 Saat	15,90	2,23		
	5-7 Saat	16,39	2,52		
	8 Saat ve Üzeri	17,15	2,30		

*p<0,05

Erkeklerin ($\bar{X}$ =16,26), kadınlara ($\bar{X}$ =16,27) göre daha düşük bütünlük boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (t=-0,18; p>0,05).

18-25 yaş aralığındaki katılımcıların ($\bar{X}$ =16,50), 26-35 yaş aralığındaki katılımcıların ($\bar{X}$ =16,07), 36-45 yaş aralığındaki katılımcıların ($\bar{X}$ =16,88) ve 46 yaş üzerindeki katılımcıların ($\bar{X}$ =16,95) bütünlük boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak yaşa göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (F=2,235; p>0,05).

Lise mezunu katılımcıların ($\bar{X}$ =15,00), ön lisans mezunu katılımcıların ($\bar{X}$ =16,25), lisans mezunu katılımcıların ($\bar{X}$ =16,12) ve yüksek lisans mezunu katılımcıların ($\bar{X}$ =16,83) bütünlük boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak eğitim durumuna göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (F=1,335; p>0,05).

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}$ =16,25), 6-10 yıl aralığında olan katılımcıların ($\bar{X}$ =16,23), 11-15 yıl aralığında olan katılımcıların ($\bar{X}$ =16,00) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}$ =16,72) bütünlük boyutu toplam puan ortalamasına

sahip oldukları görülmüştür. Ancak mesleki süreye göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=0,690$; $p>0,05$).

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=16,69$), 3-4 saat olan katılımcıların ($\bar{X}=15,90$), 5-7 saat olan katılımcıların ($\bar{X}=16,39$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=17,15$) bütünlük boyutu toplam puan ortalamasına sahip oldukları görülmüştür ($F=3,311$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; 8 saat üzerinde internet kullanımı olan katılımcıların bütünlük boyutu toplam puan ortalamalarının, 3-4 saat internet kullanımı olan katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

5.4.3. Gerçeklik boyutunun sosyodemografik özelliklere göre incelenmesi

Katılımcıların gerçeklik boyutundan almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 10'de gösterilmiştir.

Tablo 10. Gerçeklik Boyutu ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	20,00	4,13	$t=-0,426$	0,671
	Kadın	20,34	3,21		
Yaş	18-25 Yaş	21,33	3,61	$F=2,121$	0,098
	26-35 Yaş	19,84	4,00		
	36-45 Yaş	21,29	3,57		
	46 Yaş ve Üzeri	19,21	5,08		
Eğitim	Lise	18,42	1,81	$F=2,019$	0,111
	Ön lisans	20,23	3,90		
	Lisans	18,59	4,93		
	Yüksek Lisans	20,41	4,29		
Meslekteki Süre	2-5 Yıl	20,41	3,89	$F=0,918$	0,432
	6-10 Yıl	20,05	4,05		
	11-15 Yıl	19,15	3,75		
	16 Yıl ve Üzeri	20,50	4,48		
Günlük İnternet Kullanım Süresi	1-2 Saat	20,54	3,92	$F=1,484$	0,219
	3-4 Saat	20,06	4,17		
	5-7 Saat	19,32	4,16		
	8 Saat ve Üzeri	20,90	3,14		

* $p<0,05$

Erkeklerin ($\bar{X}=20,00$), kadınlara ($\bar{X}=20,34$) göre daha düşük gerçeklik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($t=-0,426$; $p>0,05$).

18-25 yaş aralığındaki katılımcıların ($\bar{X}=21,33$), 26-35 yaş aralığındaki katılımcıların ($\bar{X}=19,84$), 36-45 yaş aralığındaki katılımcıların ($\bar{X}=21,29$) ve 46 yaş üzerindeki katılımcıların ($\bar{X}=19,21$) gerçeklik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak yaşa göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=2,121$; $p>0,05$).

Lise mezunu katılımcıların ($\bar{X}=18,42$), ön lisans mezunu katılımcıların ($\bar{X}=20,23$), lisans mezunu katılımcıların ($\bar{X}=18,59$) ve yüksek lisans mezunu katılımcıların ($\bar{X}=20,41$) gerçeklik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak eğitim durumuna göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=2,019$; $p>0,05$).

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}=20,41$), 6-10 yıl aralığında olan katılımcıların ($\bar{X}=20,05$), 11-15 yıl aralığında olan katılımcıların ($\bar{X}=19,15$) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}=20,50$) gerçeklik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak mesleki süreye göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=0,918$; $p>0,05$).

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=20,54$), 3-4 saat olan katılımcıların ($\bar{X}=20,06$), 5-7 saat olan katılımcıların ($\bar{X}=19,32$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=20,90$) gerçeklik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak günlük internet kullanım süresine göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=1,484$; $p>0,05$).

5.4.4. Erişilebilirlik boyutunun sosyodemografik özelliklere göre incelenmesi

Katılımcıların erişilebilirlik boyutundan almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 11’de gösterilmiştir.

Tablo 11. Erişilebilirlik Boyutu ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	13,41	3,73	t=1,491	0,137
	Kadın	12,34	3,21		
Yaş	18-25 Yaş	10,00	4,83	F=1,993	0,115
	26-35 Yaş	13,28	3,49		
	36-45 Yaş	13,54	4,49		
	46 Yaş ve Üzeri	14,04	3,52		
Eğitim	Lise	13,71	3,86	F=0,480	0,696
	Önlisans	13,43	3,56		
	Lisans	12,87	3,77		
	Yüksek Lisans	12,77	4,51		
Meslekteki Süre	2-5 Yıl	13,02	3,68	F=3,723	0,012*
	6-10 Yıl	13,26	3,69		
	11-15 Yıl	12,22	3,20		
	16 Yıl ve Üzeri	14,87	3,78		
Günlük İnternet Kullanım Süresi	1-2 Saat	13,64	3,60	F=1,323	0,267
	3-4 Saat	13,24	3,53		
	5-7 Saat	12,83	3,75		
	8 Saat ve Üzeri	14,31	4,28		

*p<0,05

Erkeklerin ($\bar{X}$ =13,41), kadınlara ($\bar{X}$ =12,34) göre daha yüksek erişilebilirlik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlıdır (t=1,491; p<0,05).

18-25 yaş aralığındaki katılımcıların ($\bar{X}$ =10,00), 26-35 yaş aralığındaki katılımcıların ($\bar{X}$ =13,28), 36-45 yaş aralığındaki katılımcıların ($\bar{X}$ =13,54) ve 46 yaş üzerindeki katılımcıların ($\bar{X}$ =14,04) erişilebilirlik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak yaşa göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (F=1,993; p>0,05).

Lise mezunu katılımcıların ($\bar{X}$ =13,71), ön lisans mezunu katılımcıların ($\bar{X}$ =13,43), lisans mezunu katılımcıların ($\bar{X}$ =12,87) ve yüksek lisans mezunu katılımcıların ($\bar{X}$ =12,77) erişilebilirlik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak eğitim durumuna göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir (F=0,480; p>0,05).

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}$ =13,02), 6-10 yıl aralığında olan katılımcıların ($\bar{X}$ =13,26), 11-15 yıl aralığında olan katılımcıların ($\bar{X}$ =12,22) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}$ =14,87) erişilebilirlik boyutu toplam puan ortalamasına sahip oldukları görülmüştür (F=3,723; p<0,05). Farkın hangi gruplar arasında olduğunu

tespit edebilmek için yapılan Bonferroni testine göre; 16 yıl üzerinde mesleki süreye sahip olan katılımcıların erişilebilirlik boyutu toplam puan ortalamalarının, 6-10 yıl ve 11-15 yıl arasında mesleki süreye sahip olan katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=13,64$), 3-4 saat olan katılımcıların ($\bar{X}=13,24$), 5-7 saat olan katılımcıların ($\bar{X}=12,83$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=14,31$) erişilebilirlik boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak günlük internet kullanım süresine göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=1,323$; $p>0,05$).

5.4.5. Fayda boyutunun sosyodemografik özelliklere göre incelenmesi

Katılımcıların fayda boyutundan almış oldukları toplam puanların, genel özelliklerine göre farklılık gösterip göstermediğini belirlemek amacıyla yapılmış olan analiz sonuçları Tablo 12’de gösterilmiştir.

Tablo 12. Fayda Boyutu ve Genel Özellikler Karşılaştırması

Genel Bilgiler		$\bar{X}$	Ss	Test	p
Cinsiyet	Erkek	10,32	2,52	$t=-0,244$	0,807
	Kadın	10,44	1,99		
Yaş	18-25 Yaş	11,66	1,86	$F=4,976$	0,002*
	26-35 Yaş	10,58	2,32		
	36-45 Yaş	9,61	2,72		
	46 Yaş ve Üzeri	9,00	2,98		
Eğitim	Lise	8,28	1,63	$F=3,033$	0,030*
	Ön lisans	10,48	2,29		
	Lisans	9,56	3,09		
	Yüksek Lisans	10,51	2,98		
Meslekteki Süre	2-5 Yıl	10,61	2,67	$F=2,186$	0,090*
	6-10 Yıl	10,54	2,31		
	11-15 Yıl	9,77	2,49		
	16 Yıl ve Üzeri	9,70	2,90		
Günlük İnternet Kullanım Süresi	1-2 Saat	10,11	2,62	$F=0,768$	0,512
	3-4 Saat	10,21	2,47		
	5-7 Saat	10,52	2,25		
	8 Saat ve Üzeri	10,81	2,83		

* $p<0,05$

Erkeklerin ($\bar{X}=10,32$), kadınlara ($\bar{X}=10,44$) göre daha düşük fayda boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak cinsiyete göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($t=-0,244$; $p>0,05$).

18-25 yaş aralığındaki katılımcıların ($\bar{X}=11,66$), 26-35 yaş aralığındaki katılımcıların ($\bar{X}=10,58$), 36-45 yaş aralığındaki katılımcıların ($\bar{X}=9,61$) ve 46 yaş üzerindeki katılımcıların ($\bar{X}=9,00$) fayda boyutu toplam puan ortalamasına sahip oldukları görülmüştür ($F=4,976$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; 46 yaş üzerindeki katılımcıların fayda boyutu toplam puan ortalamalarının, 26-35 yaş aralığındaki katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha düşük olduğu belirlenmiştir.

Lise mezunu katılımcıların ($\bar{X}=8,28$), ön lisans mezunu katılımcıların ($\bar{X}=10,48$), lisans mezunu katılımcıların ($\bar{X}=9,56$) ve yüksek lisans mezunu katılımcıların ($\bar{X}=10,51$) fayda boyutu toplam puan ortalamasına sahip oldukları görülmüştür ($F=3,033$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; önlisans mezunu katılımcıların fayda boyutu toplam puan ortalamalarının, lise mezunu katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha yüksek olduğu belirlenmiştir.

Mesleki süresi 2-5 yıl aralığında olan katılımcıların ($\bar{X}=10,61$), 6-10 yıl aralığında olan katılımcıların ($\bar{X}=10,54$), 11-15 yıl aralığında olan katılımcıların ($\bar{X}=9,77$) ve 16 yıl üzerinde olan katılımcıların ($\bar{X}=9,70$) fayda boyutu toplam puan ortalamasına sahip oldukları görülmüştür ($F=2,186$; $p<0,05$). Farkın hangi gruplar arasında olduğunu tespit edebilmek için yapılan Bonferroni testine göre; 16 yıl üzerinde mesleki süreye sahip olan katılımcıların fayda boyutu toplam puan ortalamalarının, 6-10 yıl arasında mesleki süreye sahip olan katılımcılara göre istatistiksel olarak anlamlı bir şekilde daha düşük olduğu belirlenmiştir.

Günlük internet kullanım süresi 1-2 saat olan katılımcıların ($\bar{X}=10,11$), 3-4 saat olan katılımcıların ($\bar{X}=10,21$), 5-7 saat olan katılımcıların ($\bar{X}=10,52$) ve 8 saat üzerinde olan katılımcıların ($\bar{X}=10,81$) fayda boyutu toplam puan ortalamasına sahip oldukları görülmüştür. Ancak günlük internet kullanım süresine göre belirlenen puan farkı, istatistiksel olarak anlamlı değildir ($F=0,768$; $p>0,05$).

SONUÇ

Bu tez çalışmasının temel amacı, kamu personelinin siber güvenlik farkındalık düzeylerinin belirlenmesi ve bu alandaki pratik uygulamalarının değerlendirilmesidir. Araştırmada, toplam 302 kamu personeli katılımcı ile yürütülmüş olup, Siber Güvenlik Ölçeği (SGÖ) kullanılarak, altı farklı boyut (gizlilik, kontrol/sahiplik, bütünlük, gerçeklik, erişilebilirlik ve fayda) üzerinden bir analiz gerçekleştirilmiştir.

Araştırmada, katılımcıların büyük bir çoğunluğunu (%90,4) erkekler ve %75,8'ini 26-35 yaş aralığındaki bireyler oluşturmaktadır. Bu demografik yapı, çalışmanın sonuçlarının özellikle bu yaş grubu ve cinsiyet üzerinden genellemeler yapılmasına olanak sağlamaktadır. Eğitim düzeyi olarak, katılımcıların çoğunluğu (%76,8) lisans mezunu olup, mesleki süreleri genellikle 6-10 yıl arasında (%61,7) değişmektedir. Bu bulgular, emniyet personelinin genel olarak yüksek eğitim düzeyine ve orta düzeyde mesleki tecrübeye sahip olduğunu göstermektedir. Günlük internet kullanım süreleri incelendiğinde, katılımcıların yarısından fazlası (%51) günlük olarak 3-4 saatini internete ayırdığını belirtmiştir. İnternet kullanım amaçları arasında mobil bankacılık (%88,1), e-devlet hizmetleri (%63,9) ve e-ticaret (%62,6) en sık zikredilen sebepler olmuştur. Bu durum, kamu personelinin interneti işlevsel ve günlük yaşamı kolaylaştırıcı hizmetler için kullandığını göstermektedir. Literatürde yer alan Masum (2022)'un çalışmasında, internet kullanımının sosyal medya için daha yüksek oranda kadınlar tarafından yapıldığı belirtilmiştir. Bu çalışmada ise internet kullanım amacı olarak sosyal medya düşük oranlarda (%17,3) yer almaktadır, bu da demografik yapıdan kaynaklanan farklılıkları işaret edebilir. Bu bulgular, cinsiyetin siber güvenlik davranışları üzerindeki etkisini vurgulamaktadır ve çalışmamızda da benzer bir eğilim görülmektedir. Erkek katılımcıların daha aktif bir şekilde siber güvenlik önlemleri aldığı ve bu konudaki eğitimlere daha sık katıldığı belirlenmiştir.

Literatürdeki benzer çalışmalar, ölçeklerin geçerlilik ve güvenirlilik değerlendirmelerinde benzer metodolojilerin kullanıldığını göstermektedir. Örneğin, Yılmaz (2023) tarafından yapılan araştırma, ortaokul öğrencileri için geliştirilen bir ölçeğin kapsam geçerliği ve yapı geçerliğini değerlendirerek ölçeğin geçerli olduğunu ortaya koymuştur. Faktör analizi sonuçları, ölçeğin birden çok boyutlu yapıya sahip olduğunu ve uyum değerlerinin kabul edilebilir sınırların üzerinde olduğunu belirlemiştir. Bu, çalışmamızda elde edilen sonuçlarla paralellik göstermektedir. Ayrıca, Erol ve

diğerleri (2015) ile Çetinkaya ve Öktelik (2022) tarafından geliştirilen ölçekler, yapısal özellikler açısından benzer sonuçlara ulaşmıştır. Bu çalışmalar, ölçeklerin belirli yaş gruplarına uygun olarak geliştirilmesinin, siber güvenlik eğitimi planlamasında önemli katkılar sağlayabileceğini vurgulamaktadır. Özellikle ortaokul öğrencilerine yönelik geliştirilen ölçekler, bu yaş grubuna uygun içerik ve sorular içerdiğinden, daha doğru ve etkili ölçüm yapma imkânı sunmaktadır.

Literatürdeki benzer çalışmalarda, güvenirlik ve geçerlilik değerlerinin yüksek olması genel olarak araştırmanın kalitesini ve sonuçların güvenilirliğini artırmaktadır. Erol ve diğerleri (2015) ile Makhabbat ve Gülseçen (2020) tarafından geliştirilen ölçeklerde elde edilen geçerlilik katsayıları, bu çalışmadaki sonuçlarla uyumlu olarak yüksek değerler göstermiştir. Çetinkaya ve Öktelik (2022) tarafından geliştirilen ölçeğin yüksek geçerlilik katsayısına sahip olması ve büyük örneklem büyüklükleri, ölçeğin genel popülasyona uygulanabilirliğini artırırken, iç tutarlık katsayılarının yüksek olması da ölçeğin güvenilirliğini pekiştirmektedir.

Çalışmada, katılımcıların siber güvenlik durumları, çeşitli boyutlar altında değerlendirilmiştir. Siber güvenlik ölçeği üzerinden yapılan analizler sonucunda, katılımcıların genel toplam puan ortalaması 94,41 olarak tespit edilmiştir. Bu ölçeğin toplam puan aralığı 24 ile 120 arasında değişmektedir, dolayısıyla elde edilen ortalama puan, ölçeğin üst orta segmentinde yer almaktadır ve katılımcıların genel olarak siber güvenlik konusunda yeterli farkındalığa sahip oldukları yorumlanabilir. Katılımcıların siber güvenlik ölçeğinin alt boyutlarından aldıkları puanlar ayrı ayrı incelenmiştir. Gizlilik boyutundan elde edilen ortalama puan 12,72'dir ve bu boyut için mümkün olan puan aralığı 3 ile 15 arasında değişmektedir. Bu sonuç, katılımcıların gizlilik konusunda yüksek düzeyde farkındalık gösterdikleri anlamına gelmektedir.

Kontrol-sahiplik boyutu için katılımcıların ortalama puanı 21,73 olarak hesaplanmıştır. Bu boyuttan alınabilecek maksimum puan 25 olup, katılımcıların kontrol ve sahiplik konularında oldukça yetkin oldukları görülmektedir. Bütünlük boyutunda katılımcılar ortalama 16,27 puan almışlardır ve bu boyut için puan aralığı 4 ile 20 arasında değişmektedir. Bu, katılımcıların bütünlük boyutunda ortalamanın üzerinde bir performans sergilediklerini göstermektedir. Gerçeklik boyutu için elde edilen ortalama puan 20,04 olup, bu boyutun toplam puan aralığı 5 ile 25 arasındadır. Bu sonuç, katılımcıların gerçeklik boyutunda oldukça yüksek bir performans gösterdiklerini işaret

etmektedir. Erişebilirlik boyutunda ise katılımcıların ortalama puanı 13,31'dir. Bu boyut için puan aralığı 4 ile 20 arasında olduğundan, katılımcıların erişebilirlik konusunda da yeterli düzeyde farkındalığa sahip oldukları söylenebilir. Son olarak, fayda boyutu için katılımcıların ortalama puanı 10,34'tür ve bu boyuttan alınabilecek maksimum puan 15'tir. Bu, katılımcıların siber güvenlik tedbirlerinin faydalarını anlama konusunda ortalama bir farkındalık düzeyine sahip olduklarını göstermektedir. Genel olarak, çalışmanın sonuçları katılımcıların siber güvenlik konusunda farklı boyutlarda yeterli düzeyde bilgiye ve farkındalığa sahip olduğunu ortaya koymaktadır. Ancak, özellikle fayda boyutunda daha fazla bilinçlendirme çalışmasına ihtiyaç duyulduğu anlaşılmaktadır.

Araştırmada Siber güvenlik düzeyleri, genel özelliklere göre farklılık göstermekte midir? sorusunun cevabi aranmış ve katılımcıların cinsiyet, yaş, eğitim düzeyi, mesleki süre ve günlük internet kullanım süresi gibi genel özelliklerin siber güvenlik toplam puanları üzerindeki etkileri araştırılmıştır. Cinsiyet üzerine elde edilen bulgulara bakıldığında, erkeklerin siber güvenlik puanları kadınlara göre daha yüksek çıkmıştır; ancak bu fark istatistiksel olarak anlamlı değildir. Bu sonuç, literatürdeki diğer çalışmalarla kısmen uyumlu görünmektedir. Örneğin, Keser, Çetinkaya ve Güldüren (2016) ve Yılmaz, Şahin ve Akbulut (2016) çalışmalarında erkek öğrenci ve öğretmenlerin siber güvenlik farkındalığının kadınlardan daha yüksek olduğu belirtilmiştir. Bununla birlikte, Arıtürk (2015) ve Nezgıtlı ve Gökçearslan (2022) gibi çalışmalar cinsiyet açısından anlamlı bir fark bulunmadığını rapor etmiştir. Bu durum, cinsiyetin siber güvenlik farkındalığı üzerinde belirleyici bir faktör olmadığını göstermektedir.

Yaş kategorilerine göre incelediğimizde, farklı yaş grupları arasında da siber güvenlik puanlarında anlamlı bir fark olmadığı görülmüştür. Benzer şekilde, Gökmen ve Akgün (2015) ve diğer bazı çalışmalarda da yaşın siber güvenlik bilgisinde belirleyici bir faktör olmadığı gözlenmiştir. Ancak, Yılmaz ve diğerleri (2016) gibi çalışmalar yaş ve kullanım sıklığının farkındalık düzeyinde önemli rol oynadığını bildirmiştir. Bu sonuçlar, farklı yaş grupları arasında siber güvenlik farkındalığı açısından genel bir eğilimin olmadığını, ancak belirli koşullar altında yaşın etkili olabileceğini düşündürmektedir.

Eğitim seviyesi bazında yapılan analizde, ön lisans mezunlarının lisans mezunlarına göre siber güvenlik puanlarının istatistiksel olarak anlamlı derecede yüksek olduğu tespit

edilmiştir. Diğer eğitim seviyeleri arasında ise anlamlı bir fark bulunmamıştır. Literatürde eğitim düzeyi ile siber güvenlik farkındalığı arasındaki ilişki genellikle pozitif yönde belirtilmiştir. Örneğin, Oktay ve Çakır (2012) ve Tekerek ve Tekerek (2013) çalışmaları eğitim seviyesi arttıkça siber güvenlik farkındalığının arttığını göstermiştir. Bu durum, daha yüksek eğitim düzeylerindeki bireylerin siber tehditlere karşı daha hazırlıklı olabileceğini düşündürmektedir.

Mesleki süre ile siber güvenlik puanları arasında anlamlı bir ilişki bulunamamışken, günlük internet kullanım süresi arttıkça siber güvenlik farkındalığının arttığı gözlemlenmiştir. Bu bulgu, özellikle yoğun internet kullanıcılarının siber tehditlere karşı daha duyarlı hale geldiğini göstermektedir. Bu durum, internet kullanımı arttıkça karşılaşılan siber tehdit türlerinin çeşitlenmesi ve bu tehditlere karşı farkındalık kazanılması ile açıklanabilir. Son olarak, günlük internet kullanım süresine göre yapılan analizde, 8 saatten fazla internet kullanan katılımcıların siber güvenlik puanlarının, diğer kullanım sürelerine göre istatistiksel olarak anlamlı derecede yüksek olduğu belirlenmiştir.

Çalışmada, “Gizlilik boyutu, genel özelliklere göre farklılık göstermekte midir?” sorusu ele alınmış ve katılımcıların demografik özellikleri ve günlük davranışları temelinde gizlilik boyutları detaylı bir şekilde incelenmiştir. Cinsiyet temelli yapılan analizlerde, erkeklerin gizlilik puan ortalamaları kadınlara kıyasla biraz daha düşük bulunmuştur; ancak bu farklılık istatistiksel olarak anlamlı değildir ($t=-0,158$; $p>0,05$). Yaş gruplarına yönelik analizler, farklı yaş kategorileri arasında gizlilik puanları açısından anlamlı bir farklılık olmadığını ortaya koymuştur ($F=0,677$; $p>0,05$). Eğitim düzeyi ile ilgili olarak yapılan değerlendirmelerde, yüksek lisans mezunlarının gizlilik puanları lisans mezunlarına göre istatistiksel olarak anlamlı derecede yüksek bulunmuştur ($F=2,775$; $p<0,05$), ve bu farklılık Bonferroni testi ile yapılan detaylı grup karşılaştırmalarında teyit edilmiştir. Mesleki deneyim süresi dikkate alındığında ise, çalışma süreleri farklı olan gruplar arasında gizlilik puanları bakımından anlamlı bir farklılık gözlemlenmemiştir ($F=0,641$; $p>0,05$). Günlük internet kullanım süresi üzerine yapılan analizlerde, günde sekiz saat ve üzeri internet kullanan bireylerin gizlilik puanları, beş ile yedi saat arası internet kullananlara göre istatistiksel olarak anlamlı derecede yüksek çıkmıştır ($F=2,650$; $p<0,05$), ve bu sonuçlar Bonferroni testi ile yapılan detaylı karşılaştırmalarda da doğrulanmıştır.

Bu bulgular, daha geniş kapsamlı araştırmalarla uyumlu olup, internet kullanıcıları arasında gizlilik endişelerinin yaygın olduğunu göstermektedir (Malhotra ve diğ., 2004). Bilgi mahremiyeti, kişisel iletişim mahremiyeti ve veri mahremiyeti gibi çeşitli boyutları içermekte olup, bu yönleriyle geniş bir yapıyı kapsamaktadır (Crossler, 2011). Eğitim seviyesi gibi faktörler, gizlilik endişelerindeki farklılıklarla ilişkilendirilmiş olup, yüksek eğitim seviyeleri genellikle gizlilikle ilgili artan farkındalık ve endişelerle ilişkilendirilmiştir (Wang ve diğ., 2022). Ayrıca, internet kullanım süresinin bireylerin mahremiyet algılarını nasıl etkileyebileceği üzerine yapılan çalışmalar, daha uzun süreli kullanımın daha yüksek endişelerle ilişkili olduğunu ortaya koymuştur (Denis ve diğ., 2023).

Araştırmada, "Kontrol-sahiplik boyutu, genel özelliklere göre farklılık göstermekte midir?" sorusu incelenmiş ve, katılımcıların demografik ve davranışsal özelliklerine dayalı olarak kontrol-sahiplik düzeylerini analiz edilmiştir. Araştırmanın sonuçları, erkeklerin kontrol-sahiplik puan ortalamalarının kadınlardan hafifçe daha yüksek olduğunu göstermekle birlikte, bu fark istatistiksel olarak anlamlı bulunmamıştır. Yaş gruplarına yönelik yapılan analizlerde, 18-25, 26-35, 36-45 ve 46 yaş üstü katılımcılar arasında kontrol-sahiplik puanlarında farklılıklar saptanmış, ancak bu farklar da istatistiksel olarak anlamlı değildir.

Eğitim seviyesi açısından yapılan değerlendirmeler, lise, ön lisans, lisans ve yüksek lisans mezunları arasında kontrol-sahiplik puanlarında belirgin farklar ortaya çıkarmıştır; fakat bu farklar istatistiksel açıdan önemsiz kalmıştır. Mesleki deneyim süresine göre yapılan analizlerde de, 2-5 yıl, 6-10 yıl, 11-15 yıl ve 16 yıl ve üzeri çalışma süresine sahip bireyler arasında kontrol-sahiplik puanları açısından anlamlı bir fark tespit edilmemiştir. Ancak, günlük internet kullanım süresi ile kontrol-sahiplik puanları arasında istatistiksel olarak anlamlı bir ilişki bulunmuştur. Özellikle, günde sekiz saat ve üzeri internet kullanan bireyler, üç-dört saat internet kullananlara kıyasla istatistiksel olarak anlamlı derecede daha yüksek kontrol-sahiplik puanlarına sahip olmuşlardır. Bu sonuç, Bonferroni testi ile yapılan detaylı grup karşılaştırmalarında da doğrulanmıştır. Çalışmada genel popülasyon içinde kontrol-sahiplik düzeylerinin cinsiyet, yaş, eğitim ve mesleki süre gibi faktörlere göre genel bir eğilim göstermediğini; ancak yoğun internet kullanımının kontrol-sahiplik algısını artırabileceğini ortaya koymaktadır. Literatürde,

kontrol-sahiplik boyutunun genel özelliklere göre incelendiği başka bir çalışmaya rastlanmamıştır.

“Bütünlük boyutu, genel özelliklere göre farklılık göstermekte midir?” araştırma sorusu kapsamında elde edilen bulgular, cinsiyet, yaş, eğitim düzeyi ve mesleki süre gibi değişkenlerin bütünlük boyutunda istatistiksel olarak anlamlı bir farklılık yaratmadığını göstermektedir. Cinsiyet açısından yapılan analizlerde, erkeklerin ve kadınların bütünlük puan ortalamaları arasında hemen hemen hiçbir fark olmadığı ve bu durumun istatistiksel olarak anlamlı olmadığı belirlenmiştir. Yaş gruplarına yönelik yapılan karşılaştırmalarda ise, farklı yaş gruplarındaki katılımcıların bütünlük puanlarında anlamlı bir farklılık saptanamamıştır.

Eğitim düzeyi ile ilgili olarak yapılan analizler, lise mezunlarından yüksek lisans mezunlarına kadar farklı eğitim kademelerindeki katılımcıların bütünlük puanlarında bazı varyasyonlar olduğunu ortaya koymuştur. Ancak bu farklılıklar istatistiksel olarak yine anlamlı değildir. Aynı şekilde, mesleki deneyim süresine göre yapılan değerlendirmelerde, farklı çalışma sürelerine sahip gruplar arasında bütünlük puanları açısından anlamlı bir fark bulunamamıştır. Öte yandan, günlük internet kullanım süresine yönelik yapılan analizler, bütünlük boyutunda belirgin bir fark ortaya koymuştur. Özellikle, günde sekiz saat ve üzeri internet kullanan katılımcıların bütünlük puanları, üç-dört saat internet kullananlara göre istatistiksel olarak anlamlı derecede daha yüksek bulunmuştur. Bonferroni testi ile yapılan detaylı grup karşılaştırmaları, bu farkın özellikle yoğun internet kullanıcıları lehine olduğunu doğrulamıştır. Bu bulgular, yoğun internet kullanımının bireylerin bütünlük algısını artırabileceğine işaret etmektedir. Araştırmanın genel popülasyon içinde bütünlük düzeylerinin cinsiyet, yaş, eğitim ve mesleki süre gibi faktörlere göre genel bir eğilim göstermediğini; ancak yoğun internet kullanımının bütünlük algısını artırabileceğini ortaya koymuştur. Literatürde, bütünlük boyutunun genel özelliklere göre incelendiği başka bir çalışmaya rastlanmamıştır.

Araştırmada, " Gerçeklik boyutu, genel özelliklere göre farklılık göstermekte midir?" sorusu kamu personelinin siber güvenlik farkındalığına yönelik gerçeklik boyutu, katılımcıların cinsiyet, yaş, eğitim durumu, mesleki süre ve günlük internet kullanım süresi gibi çeşitli demografik özelliklere göre incelenmiştir. Elde edilen bulgular, bu demografik özelliklerin gerçeklik boyutundaki puanlar üzerinde belirgin bir etkiye sahip olmadığını göstermiştir.

Analiz sonuçları, erkeklerin gerçeklik boyutunda kadınlara kıyasla daha düşük puanlar aldığını göstermiş, ancak cinsiyete göre belirlenen puan farkının istatistiksel olarak anlamlı olmadığı tespit edilmiştir. Bu sonuç, her iki cinsiyetin siber güvenlik konularındaki gerçeklik algısının benzer olduğunu işaret eder. Bu bulgu, eğitim ve farkındalık programlarının cinsiyet ayrımı gözetmeksizin etkili bir şekilde tasarlanabileceğine işaret etmektedir. Yaş gruplarına göre yapılan analiz, 18-25 ve 36-45 yaş aralıklarında katılımcıların, diğer yaş gruplarına göre daha yüksek puanlar aldığını göstermiştir. Ancak, yaşa göre belirlenen puan farklarının istatistiksel olarak anlamlı olmaması, yaşın gerçeklik boyutu üzerinde belirleyici bir faktör olmadığını ortaya koymaktadır.

Eğitim durumu ile ilgili bulgular, ön lisans ve yüksek lisans mezunlarının lise ve lisans mezunlarına göre daha yüksek puanlar aldığını göstermiş olsa da, eğitim durumuna göre puan farkının istatistiksel olarak anlamlı olmadığını belirtmiştir. Benzer şekilde, mesleki süre ile ilgili bulgular da, farklı mesleki süre grupları arasında gerçeklik boyutu puanlarında belirgin bir fark olmadığını göstermiştir. Bu, siber güvenlik gerçeklik algısının mesleki tecrübe ile doğrudan ilişkili olmadığını düşündürmektedir. Günlük internet kullanım süresine göre yapılan analiz, kullanım süresinin artması ile gerçeklik boyutu puanlarında bir artış gözlemlenmiş olmakla birlikte, bu farkların istatistiksel olarak anlamlı olmadığı saptanmıştır. Bu sonuç, günlük internet kullanım süresinin siber güvenlik gerçeklik algısını önemli ölçüde etkilemediğini göstermektedir. Elde edilen bulgular, kamu personelinin siber güvenlik gerçeklik boyutunda, incelenen demografik özelliklerin belirgin bir etkisi olmadığını ortaya koymaktadır. Bu sonuçlar, siber güvenlik eğitim programlarının ve politikalarının, geniş bir demografik yelpazeye hitap edecek şekilde tasarlanmasının önemini vurgulamaktadır.

Araştırmada, "Erişilebilirlik boyutu, genel özelliklere göre farklılık göstermekte midir?" sorusu incelenmiş ve katılımcıların genel özelliklerine göre erişilebilirlik boyutu açısından incelenmiştir. Analiz sonuçları, erişilebilirlik boyutunda cinsiyet, yaş, eğitim durumu, mesleki süre ve günlük internet kullanım süresi gibi faktörlerin siber güvenlik erişim algıları üzerindeki etkilerini ortaya koymaktadır. Araştırmada erkeklerin, kadınlara göre erişilebilirlik boyutunda anlamlı derecede daha yüksek puanlar aldığı tespit edilmiştir. Bu bulgu, erkeklerin teknolojiye daha fazla erişimi olduğu veya teknolojiyi kullanma konusunda daha fazla güvene sahip oldukları yönünde yorumlanabilir. Bu

sonuç, cinsiyetin siber güvenlik araçlarına erişimde önemli bir faktör olduğunu göstermektedir ve bu bağlamda eğitim programlarının her iki cinsiyete eşit erişim sağlamasının önemi vurgulanmalıdır.

Yaş grupları arasında yapılan analizde, 46 yaş ve üzeri grupların, genç yaş gruplarına kıyasla daha yüksek erişilebilirlik puanlarına sahip olduğu görülmüştür, ancak bu farklar istatistiksel olarak anlamlı değildir. Bu, yaşın teknoloji kullanımı ve erişiminde belirleyici bir faktör olmadığını göstermektedir. Eğitim durumu açısından incelendiğinde, farklı eğitim seviyeleri arasında erişilebilirlik puanlarında istatistiksel olarak anlamlı bir fark bulunamamıştır. Bu sonuç, siber güvenlik erişiminde eğitim düzeyinin belirleyici olmadığını işaret etmektedir. Öte yandan, mesleki süre ile yapılan değerlendirme sonucunda, uzun mesleki süreye sahip olanların, daha kısa süreli meslektaşlarına göre erişilebilirlik konusunda daha yüksek puanlar aldığı belirlenmiştir. Bu, deneyimin, siber güvenlik araçlarına erişim konusunda olumlu bir etkisi olduğunu göstermektedir.

Erişilebilirlik boyutunun incelenmesi, siber güvenlik politikaları ve eğitim programlarının tasarımında cinsiyet, yaş, mesleki deneyim gibi faktörlerin dikkate alınması gerektiğini ortaya koymaktadır. Her ne kadar bazı demografik değişkenler arasında anlamlı farklar tespit edilmişse de bu sonuçlar eğitim ve politika geliştirme süreçlerinde bu faktörlerin nasıl ele alınabileceğine dair önemli içgörüler sunmaktadır. Literatür incelendiğinde ise, erişilebilirlik boyutunun genel özelliklere göre incelendiği başka bir çalışmaya rastlanmamıştır.

Araştırmada, "Fayda boyutu, genel özelliklere göre farklılık göstermekte midir?" sorusu incelenmiş ve katılımcıların yaş gruplarına göre yapılan analizinde, genç katılımcıların (18-25 yaş aralığı) fayda algısının daha yüksek olduğu, yaş arttıkça bu algının düştüğü tespit edilmiştir. Özellikle 46 yaş ve üzeri grupların, 26-35 yaş aralığındaki bireylere kıyasla anlamlı derecede düşük fayda algısına sahip olduğu belirlenmiştir. Bu durum, yaşın artmasıyla birlikte teknolojik adaptasyon ve yeniliklere açıklığın azalabileceği veya bu yaş gruplarının eğitimlerden aldıkları faydanın daha az olabileceği şeklinde yorumlanabilir.

Eğitim seviyesine göre yapılan değerlendirmede ise, ön lisans mezunu katılımcıların lise mezunu olanlara göre siber güvenlik eğitimlerinden daha fazla fayda sağladıkları görülmüştür. Bu sonuç, ön lisans düzeyindeki bireylerin siber güvenlik konularına daha duyarlı olabileceğini veya bu seviyede verilen eğitimlerin içeriğinin,

katılımcıların ihtiyaçlarına daha uygun düşebileceğini düşündürmektedir. Cinsiyete göre elde edilen bulgular, erkek ve kadın katılımcılar arasında fayda algısında istatistiksel olarak anlamlı bir fark olmadığını göstermiştir. Bu sonuç, her iki cinsiyetin siber güvenlik eğitimlerinden benzer düzeyde fayda sağladığını işaret etmektedir. Mesleki süre açısından değerlendirildiğinde, 16 yıl ve üzeri mesleki deneyime sahip olanların, 6-10 yıl arasındaki süreye sahip olanlara göre daha düşük fayda algısına sahip oldukları tespit edilmiştir. Bu bulgu, mesleki deneyim arttıkça siber güvenlik eğitimlerinden alınan faydanın azalabileceğini göstermekte olup, bu durum tecrübeli profesyonellerin eğitim içeriklerini yeterince zorlayıcı veya ilgi çekici bulmamalarından kaynaklanıyor olabilir.

Günlük internet kullanım süresinin analizi, sürenin artmasıyla fayda algısının arttığını göstermiş olmakla birlikte, bu ilişkinin istatistiksel olarak anlamlı olmadığı tespit edilmiştir. Bu, günlük internet kullanım süresinin siber güvenlik eğitimlerinden alınan faydayı önemli ölçüde etkilemediğini göstermektedir. Nezgiti ve Gökçearsan'ın (2022) çalışması, iş yerinde alınan bilgi güvenliği eğitiminin farkındalık düzeyini anlamlı şekilde artırdığını belirtmektedir. Bu, eğitimlerin etkinliğinin iş yerinde de gözlemlenebileceğini gösterirken, Gökçearsan ve diğerlerinin (2021) çalışması ortaokul öğrencilerinde bilişim teknolojileri derslerinin farkındalığı artırdığını ortaya koymuştur. Yayla'nın (2018) çalışması ise öğretmenlerin alınan eğitimi yeterli bulduklarını ve bu durumun istatistiksel olarak anlamlı farklar yarattığını göstermektedir. Bu bulgular, siber güvenlik fayda boyutunun çeşitli eğitim seviyelerinde ve mesleki gruplarda farklı etkiler yaratabileceğine işaret etmektedir.

Çalışmadan elde edilen sonuçlar kapsamında kamu personelinin siber güvenlik konularında genel bir bilgiye sahip olduğu; ancak, özellikle gelişmiş tehditlere karşı yeterli bilgi ve pratiğe sahip olmadıkları tespit edilmiştir. Kamu personelinin siber güvenlik farkındalığının artırılması için gerekli eğitimlerin yetersiz kaldığı ve bu eğitimlerin daha etkili, uygulamalı ve sürekli hale getirilmesi gerektiği sonucuna ulaşılmıştır. Eğitim programlarının içeriği, güncel siber tehditleri kapsayacak şekilde genişletilmeli ve personelin bu tehditlere karşı daha bilinçli ve donanımlı hale gelmesi için pratik uygulamalar içermelidir. Analiz sonuçlarına göre, kamu kurumlarında siber güvenlik politikaları mevcut olmasına rağmen, bu politikaların uygulanabilirliği ve etkinliği konusunda ciddi eksiklikler bulunmaktadır. Bu politikaların gözden geçirilerek, gerçekçi ve uygulanabilir hale getirilmesi, kurum içi denetim mekanizmalarının

güçlendirilmesi önerilmektedir. Ayrıca, siber suçların ve güvenlik ihlallerinin doğurabileceği zararların ciddiyeti göz önüne alındığında, kamu personelinin bu tehditlere karşı daha iyi korunabilmesi için, bilgi güvenliği kültürünün her kademedeki çalışan arasında yaygınlaştırılması büyük önem taşımaktadır. Bu kültürün yerleştirilmesi, bireylerin hem kendi verilerini koruma bilincini artıracak hem de kamu kurumlarının bütün olarak siber tehditlere karşı daha dirençli hale gelmesine katkıda bulunacaktır.



KAYNAKÇA

- Acar, S. ve Çiçek, H. K. (2021). E-ticaret sitelerine yönelik siber saldırılar ve güvenlik tedbirleri. VII. Uluslararası TURKCESS Eğitim ve Sosyal Bilimler Kongresi'nde sunulan bildiri, Girne, Kıbrıs (Kktc).
- Aggarwal, N., Albert, L. J., Hill, T. R., ve Rodan, S. A. (2020). Risk knowledge and concern as influences of purchase intention for internet of things devices. *Technology in Society*, 62, 101311.
- Akdeniz, P. C., ve Dursun, Y. (2021). Çevrimiçi kimlik hırsızlığı korkusunun çevrimiçi gizlilik endişesi ve satın alma davranışına etkisi. *Erciyes Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, (60), 609-632.
- Akgün, Ö., ve Topal, M. (2015). Eğitim fakültesi son sınıf öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi Eğitim Fakültesi örneği. *Sakarya University Journal of Education*, 5(2), 98-121.
- Akkaş, A. H. (2015). Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi koruma tedbirinin şartlarında 6526 sayılı kanun ile yapılan değişikliklerin değerlendirilmesi. *Türkiye Adalet Akademisi Dergisi*, 6(21).
- Aksoğan, M., Bayer, H., Gülada, M., ve Çelik, E. (2018). İletişim fakültesi öğrencilerinin siber güvenlik farkındalığı: İnönü Üniversitesi örneği. *Kesit Akademi Dergisi*, 4(13), 271-288.
- Aktaş, M. (2020). Toplumsal dönüşüm ve bilgi toplumu. *Social Mentality and Researcher Thinkers Journal*, 35, 1606.
- Al-Kahla, W., Shatnawi, A. S., ve Taqieddin, E. (2021, Mayıs). A taxonomy of web security vulnerabilities. 2021 12th International Conference on Information and Communication Systems (ICICS)'de sunulan bildiri (ss. 424-429). IEEE.
- Aldemir, C., ve Merve, K. (2020). Bilgi toplumu, siber güvenlik ve Türkiye uygulamaları. *Kamu Yönetimi ve Politikaları Dergisi*, 1(1), 6-27.
- Ali, R. F., Dominic, P., Ali, S., Rehman, M., ve Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383. <https://doi.org/10.3390/app11083383>

- Alotaibi, M., ve Alfehaid, W. (2018). Information security awareness: A review of methods, challenges and solutions. ICITST-WorldCIS-WCST-WCICSS2018 Konferansı'nda sunulan bildiri, Cambridge, UK.
- Altınır, İ. (2021). *Öğretmenlerin kişisel siber güvenlik farkındalık düzeylerinin farklı değişkenlere göre değerlendirilmesi* [Yüksek Lisans Tezi, Ankara Üniversitesi].
- Arıtürk, M. (2015). Bilgi farkındalığı ve bilgi güvenliğinin karşılaştırılması. XVII. Akademik Bilişim Konferansı Bildirileri (ss. 178-185). Eskişehir.
- Arslan, Y., ve Özbilger, H. İ. (2022). Ulusal mevzuat perspektifinde bilgi işlem birimlerinin iç denetiminde bir kontrol listesi önerisi. *Denetim*, (26-Ek Sayı), 1-12.
- Arunkrishna, M., ve Mukunthan, B. (2020). Evolutionary traits in digital spam: History, types, techniques and anti spam solutions.
- 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.
- Aybike, C. (2022). Ulusal güvenlik açısından kritik altyapı ve siber alan: Sivil hazırlıklılık ve dirençlilik perspektifinden kavramsal bir inceleme. *Diplomasi ve Strateji Dergisi*, 3(2), 279-311.
- Aydemir, M. (2022). The use of communication technologies in web attacks and hacker tagging: Analysis of the zone-h model: İletişim teknolojilerinin web saldırılarında kullanımı ve hacker etiketlemesi: Zone-H modelinin analizi. *Ases Ulusal Sosyal Bilimler Dergisi*, 2(1), 158-179.
- Aydın, H., Barışkan, M., ve Çetinkaya, A. (2021). Siber güvenlik kapsamında enerji sistemleri güvenliğinin değerlendirilmesi. *Güvenlik Bilimleri Dergisi*, 10(1), 151-174.
- Bai, C., Dallasaga, P., Orzes, G., ve Sarkis, J. (2020). Industry 4.0 technologies assessment: A sustainability perspective. *International Journal of Production Economics*, 229, 107776.
- Bar Ilan, J. (2008). The history of information security: A comprehensive handbook. *Library Hi Tech*, 26(4), 682-683.
- Batur, M. (2022). Yeni iletişim teknolojileri çerçevesinde uzaktan eğitimde iletişim ve etkileşim. *Sosyal Bilimler Araştırmaları Dergisi*, 12(2).

- Bekar, S., ve Sağlam, M. (2023). Siber âlem: Yeni medya ve dijital yurttaşlık. *Niğde Ömer Halisdemir Üniversitesi İletişim Fakültesi Akademik Dergisi*, 2(2), 133-144.
- Bıçakçı, S., Ergun, F., ve Çelikkpala, M. (2015). Türkiye’de siber güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi*, 1, 1-35.
- Bijalwan, A. (2021). *Network forensics: Privacy and security*. CRC Press.
- Bostan, A., ve Şengül, G. (2018). Siber güvenlik farkındalığı oluşturma. Ş. Sağıroğlu ve M. Alkan (Ed.), *Siber güvenlik ve savunma farkındalık ve caydırıcılık içinde* (ss. 145-164). Ankara: Grafiker Yayınları.
- Burgin, M. (2011). Information: Concept clarification and theoretical representation. *Triplec Communication Capitalism ve Critique Open Access Journal for a Global Sustainable Information Society*, 9(2), 347-357. <https://doi.org/10.31269/triplec.v9i2.284>
- Capurro, R., ve Hjørland, B. (2003). The concept of information. *Annual Review of Information Science and Technology*, 37(1), 343-411.
- Coventry, L., Briggs, P., Blythe, J., ve Tran, M. (2014). Using behavioural insights to improve the public’s use of cyber security best practices. Government UK report.
- Coşar, İ. Y., ve Tüfekci, A. (2021). CMMC v1. 02 ile ISO IEC 27001 standardının karşılaştırılması ve CMMC’ye geçiş için yapılması gerekli temel faaliyetler. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7(2), 60-73.
- Crossler, R. (2011). Privacy in the digital age: A review of information privacy research in information systems. *Mis Quarterly*, 35(4), 1017. <https://doi.org/10.2307/41409971>
- Çakır, H., ve Uzun, S. A. (2021). Türkiye’nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi*, 7(2), 353-379.
- Çetinkaya, L., ve Öktelik, B. (2022). Ortaokul düzeyi öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği geliştirme çalışması. *Cumhuriyet Uluslararası Eğitim Dergisi*, 11(4), 696-708.
- Denis, N., Laurent, M., ve Chabridon, S. (2023). Integrating usage control into distributed ledger technology for internet of things privacy. *IEEE Internet of Things Journal*, 10(22), 20120-20133. <https://doi.org/10.1109/jiot.2023.3283300>

- Ding, J., Qammar, A., Zhang, Z., Karim, A., ve Ning, H. (2022). Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, 15(18), 6799.
- Dionísio, N., Alves, F., Ferreira, P., ve Bessani, A. (2019). Cyberthreat detection from twitter using deep neural networks. <https://doi.org/10.1109/ijcnn.2019.8852475>
- Donalds, C., ve Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51(1), 1-16.
- Durdu, A., ve Ali, E. (2021). ISO 27001 bilgi güvenliği yönetim sistemi yazılım tasarımı. *Bilişim Teknolojileri Dergisi*, 14(3), 255-266.
- Ecek, N., ve Çakmak, A. F. (2022). Çalışanların bilgi güvenliği önlemlerine dair tutumları: Ampirik bir değerlendirme. *International Journal of Applied Economic and Finance Studies*, 7(2), 26-44.
- Elradi, M., Abdelmaged, K., ve Mohammad, M. (2021). Cyber security professionals' challenges: a proposed integrated platform solution. *Electrical Science ve Engineering*, 3(2). <https://doi.org/10.30564/ese.v3i2.3376>
- Eminağaoğlu, M., ve Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 11(4), 1-15.
- Erdem, M., ve Özocak, G. (2017). Sınırşan bir suç olarak siber suçlarla mücadelede uluslararası iş birliği. Erişim Tarihi, 15.04.2024
- Erol, E. S., ve Sağıroğlu, Ş. (2018). Siber güvenlik farkındalığı, farkındalık ölçüm yöntem ve modelleri. *Siber güvenlik ve savunma farkındalık ve caydırıcılık*, Ankara: *Grafiker Yayınları*, 105-141
- Erol, O., Şahin, Y. L., Yılmaz, E., ve Haseski, H. İ. (2015). Personal cyber security provision scale development study kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. *Journal of Human Sciences*, 12(2), 75-91.
- Fonseca-Herrera, O. A., Rojas, A. E., ve Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci*, 48(2), 213-222.
- Forsyth, C. (2022). Understanding the fundamentals of information security. Erişim adresi: www.eccu.edu

- Garnham, N. (2020). Information society theory as ideology. In *The information society reader* (pp. 165-183). Routledge.
- Gençoğlu, M. T. (2021). Siber olaylara müdahale ve analiz süreci. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 33(2), 471-479.
- Gödekli, M. (2013). Telekomünikasyon iletişim başkanlığı. Telecommunications presidency. *Journal of Istanbul University Law Faculty*, 71(1), 511-546.
- Gökçearsan, Ş., Yıldız Durak, H., Berikan, B., ve Saritepeci, M. (2021). Smartphone addiction, loneliness, narcissistic personality, and family belonging among university students: A path analysis. *Social Science Quarterly*, 102(4), 1743-1760.
- Gökmen, Ö. F., ve Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algılarının incelenmesi. *İlköğretim Online*, 14(4), 1208-1221.
- Gönç, D. (2022). Siber tehdit taksonomilere siber aktivizm çerçevesinde bir değerlendirme.
- Gunduz, M. Z., ve Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169, 107094.
- Gupta, A., ve Sharma, L. S. (2020). Detecting attacks in high-speed networks: Issues and solutions. *Information Security Journal: A Global Perspective*, 29(2), 51-61.
- Güldüren, C., Çetinkaya, L., ve Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *İlköğretim Online*, 15(2).
- Gündoğdu, S. (2023). Uluslararası politikada bir etki aracı olarak siber güvenlik ve Türkiye'nin siber güvenlik politikası uygulaması: Ulusal siber olaylara müdahale merkezi (USOM). *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33(3), 1325-1337.
- Gündüz, M. Z., ve Resul, D. (2021). Akıllı şebekeler: Siber güvenlik unsurları ile veri iletimi. *Bingöl Üniversitesi Teknik Bilimler Dergisi*, 2(2), 47-61.
- Gürbüz, S., ve Şahin, F. (2016). *Sosyal bilimlerde araştırma yöntemleri* (3. baskı). Seçkin Yayıncılık.
- Gürbüz, S., ve Şahin, F. (2021). *AMOS ile yapısal eşitlik modellemesi temel ilkeler ve uygulamalı analizler*. Seçkin Yayıncılık.
- Gürkan, M. F. (2013). Düzenleyici ve denetleyici kurum olarak bilgi teknolojileri ve iletişim kurumu BTK. *İnönü Üniversitesi Hukuk Fakültesi Dergisi*, 4(2), 333-356.

- Hekim, H., ve Başbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158.
- Hong, Y., ve Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, 57(1), 1-9.
- Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., ve Mahmood, S. (2020). Cyber security threats and vulnerabilities: A systematic mapping study. *Arabian Journal for Science and Engineering*, 45, 3171-3189.
- Hündür, S. (2023). *E-ticaretin ekonomik büyüme ve vergi gelirlerine etkisi: Türkiye için ekonometrik bir analiz* [Yüksek Lisans tezi, Karamanoğlu Mehmetbey Üniversitesi].
- International Organization for Standardization. (2022a). ISO/IEC 27002: Information security, cybersecurity and privacy protection. ISO.
- International Organization for Standardization. (2022b). ISO/IEC 27001: Information security management systems - Requirements. ISO.
- International Telecommunication Union. (2018). Global cybersecurity index 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- International Telecommunication Union. (2022). 2.9 billion people still offline. <https://www.itu.int/en/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx>
- Jeong, J., Grobler, M., ve C., M.A.P. (2022). Simplifying cyber security maturity models through national culture: A fuzzy logic approach. <https://doi.org/10.24251/hicss.2022.662>
- Kang, P., Kang, J., ve Monsen, K. (2022). Nurse information security policy compliance, information competence, and information security attitudes predict information security behavior. *CIN Computers Informatics Nursing*, 41(8), 595-602. <https://doi.org/10.1097/cin.0000000000000981>
- Karagöz Yalçın, Y. (2021). *Bilimsel araştırma yöntemleri* (3. baskı). Atlas Akademik Basım Yayın.
- Karakaya, A., ve Yetgin, M. A. (2020). Karabük Üniversitesi çalışanlarına yönelik kişisel siber güvenlik üzerine araştırma. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10(2), 157-172.

- Karakoç, M. A. (2011). Bilişim suçlarına genel bakış, bilişim suçlarını önleme çalışmaları ve güvenli internet kullanımı. Suç Önleme Sempozyumu Bildiriler Kitabı (ss. 419-423). Bursa.
- Karakulle, S. Ç. İ. (2022). Bilgi toplumu ve eğitim Türkiye’de eğitime genel bir bakış. *Social Sciences Studies Journal (SSSJJournal)*, 4(14), 695-705.
- Kazar, G., Kazar, A., ve Akpınar, T. (2023). Siber güvenlikte bilişim ve iletişim teknolojisi becerilerinin önemi. *The Journal of Social Sciences*, 65(65), 67-82.
- KHK. (2016). 671 sayılı olağanüstü hal kapsamında bazı kurum ve kuruluşlara ilişkin düzenleme yapılması hakkında kanun hükmünde kararname.
- Kılıç, B., Yalçın, N., ve Kılıç, E. (2021). Hukuk bürolarında bilgi güvenliğinin artırılmasında model önerileri. *Türkiye Barolar Birliği Dergisi*, 2021(152), 335-366.
- Kınay, H., Sözcü, Ö. F., Taşkın, E., ve İpek, Ğ. (2014). Bilgi güvenliği farkındalığı ölçeğinin ilk bulguları. 8. Uluslararası Bilgisayar ve Öğretim Teknolojileri Sempozyumu'nda sunulan bildiri.
- Kızıltan, M. B. (2007). 5237 sayılı Türk ceza kanununda bilişim sistemine girme, sistemi engelleme ve bozma suçları [Yüksek Lisans tezi, Sosyal Bilimler Enstitüsü].
- Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44-60.
- Kott, A., ve Linkov, I. (2021). To improve cyber resilience, measure it. *Computer*, 54(2), 80-85. <https://doi.org/10.1109/mc.2020.3038411>
- Kovačević, A., Putnik, N., ve Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, 8(1), 125140-125148.
- Kumar, P., Wazid, M., Singh, D., Singh, J., Das, A., ve Rodrigues, J. (2023). Explainable artificial intelligence envisioned security mechanism for cyber threat hunting. *Security and Privacy*, 6(6). <https://doi.org/10.1002/spy2.312>
- Kumar, Y., Hamdan, A., ve Sinha, A. (2022). *Consequential development of internet and its conclusive impact on people and economy: An India perspective* (No. 7331). EasyChair.
- Kurnaz, S., ve Önen, S. M. (2019). Avrupa Birliğine uyum sürecinde Türkiye’nin siber güvenlik stratejileri. *International Journal of Politics and Security*, 1(2), 82-103.

- Kuzminykh, I., Ghita, B., Sokolov, V., ve Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia*, 1(3), 602-617.
- Mace, J., Parkin, S., ve Moorsel, A. (2010). A collaborative ontology development tool for information security managers. <https://doi.org/10.1145/1873561.1873566>
- Makhabbat, A., ve Gülseçen, S. (2020). Ortaokul öğrencilerinin siber güvenlik farkındalık durumu. *Edebiyat, Dil ve Eğitim*, 213, 1-12.
- Malhotra, N., Kim, S., ve Agarwal, J. (2004). Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355. <https://doi.org/10.1287/isre.1040.0032>
- Mamade, B. K., ve Dabala, D. M. (2021). Exploring the correlation between cyber security awareness, protection measures and the state of victimhood: The case study of Ambo University's academic staffs. *Journal of Cyber Security and Mobility*, 699-724.
- Meral, S., ve Bülbül, H. İ. (2022). Kamu kurumlarının bilgi güvenliği politikalarının kurumsal bilgi güvenliğinin sağlanması açısından etkinliğinin analiz edilmesi. *Gazi University Journal of Science Part C: Design and Technology*, 10(2), 314-329.
- Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). In *Advances in computers* (Vol. 117, No. 1, pp. 129-164). Elsevier.
- Nair, M. M., ve Tyagi, A. K. (2021). Privacy: History, statistics, policy, laws, preservation and threat analysis. *Journal of Information Assurance ve Security*, 16(1).
- Narayan, A. S., ve Tripathi, G. (2021). Cybercrimes: A Socio-Legal Study of Its Impact in the Society. *Indian JL ve Legal Rsch.*, 3, 1.
- Nezgitli, S., ve Gökçearslan, Ş. (2022). Kamu kurumu ve özel sektöre yönelik bilgi güvenliği farkındalığı üzerine bir inceleme. *Instructional Technology and Lifelong Learning*, 3(1), 19-44.
- Oktay, S., ve Çakır, R. (2012). İlköğretim öğretmenlerinin teknoloji kullanımları ve teknolojiye yönelik tutumları arasındaki ilişkinin incelenmesi. X. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi'nde sunulan bildiri.
- Onwubiko, C., ve Ouazzane, K. (2019). Challenges towards building an effective cyber security operations centre. *International Journal on Cyber Situational Awareness*, 4(1), 11-39. <https://doi.org/10.22619/ijcsa.2019.100124>

- Onur, A. (2021). *ISO 27001 bilgi güvenliği yönetim sistemi ve ISO 27002 uygulama kılavuzu*. Cinius Yayınları.
- Oppliger, R. (2020). *End-to-end encrypted messaging*. Artech House.
- Öcal, S. T. A. (2021). Siber güvenlik perspektifinde Türkiye'nin güvenlik stratejileri. *İstanbul Üniversitesi İktisat Fakültesi Mecmuası*, 89.
- Öğün, M. N., Öznacar, B., Tatar, A., ve Debeş, G. (2020). Information technologies and reaching to information society. *REICE: Revista Electrónica de Investigación En Ciencias Económicas*, 8(16), 412-449.
- Ozbek, M. (2015). The impacts of European cybercrime convention on Turkish criminal law. *GSI Articletter*, 13, 73.
- Özbilen, T., ve Çağlar, A. (2020). Türk kamu sektöründe bilgi ve bilişim güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi*, 2(1), 72-94.
- Özdemir, A., ve Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. *Türkiye Sosyal Araştırmalar Dergisi*, 25(3), 649-666.
- Özdemir, Ö. C. (2013). Ardahan Üniversitesi sosyal bilimler meslek yüksekokulu büro yönetimi ve yönetici asistanlığı programı öğrencilerinin; teknoloji ve bilgisayar konularında, tutum ve kullanım düzeylerinin tespit edilmesine ilişkin alan çalışması. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 17-29.
- Özdemirci, F., ve Torunlar, M. (2018). Bilgi-değişim-siber güvenlik-bağımsızlık. *Bilgi Yönetimi*, 1(1), 78-83.
- Özkan, İ. (2019). *Siber saldırıların ekonomik boyutu* [Yüksek Lisans tezi, Bilecik Şeyh Edebali Üniversitesi, Sosyal Bilimler Enstitüsü].
- Özkul, O. (2023). *Bilgi sosyolojisi ve problemleri* (Cilt 15). Gündoğan Yayınları.
- Öztürk, O. (2014). *Digital dark side: Cyber warfare* [Yayınlanmamış yüksek lisans tezi]. Boston University Metropolitan College.
- Packard, N. (2023). Internet prehistory: ARPANET chronology. *Cogent Social Sciences*, 9(2), 2245237.
- Petekci, A. R. (2021). Endüstri 4.0: Fırsat mı tehlike mi?. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, 2(1), 7-15.
- Pikhart, M., ve Klimova, B. (2020). Information and communication technology-enhanced business and managerial communication in SMEs in the czech republic. *Information*, 11(6), 336.

- Resmî Gazete. (2012). Ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar, 1.
- Resmî Gazete. (2013). Ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı.
- Sağiroğlu, Ş., Şenol, M., Bayındır, R., Bilge, Y., Bensghır, T. K., Akleylek, S., ... ve San, G. O. M. R. (2019). *Siber güvenlik ve savunma: Problemler ve çözümler*.
- Sajid, A. (2020). *A taxonomy of cyber-attacks on computer networks* [Doktora tezi, University of Bradford].
- Salem, Y., Moreb, M., ve Rabayah, K. S. (2021, Temmuz). Evaluation of information security awareness among Palestinian learners. International Conference on Information Technology'de sunulan bildiri (ss. 21-26).
- Salim, M. M., Rathore, S., ve Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: A survey. *The Journal of Supercomputing*, 76, 5320-5363.
- Sandılaç, N. (2022). Siber suç, siber terör ve siber savaş üçgeninde siber dünya. *Bilişim Hukuku Dergisi*, 4(1), 81-140.
- Sarıtaş, E., ve Barutçu, S. (2016). Tüketici davranışlarının analizinde kuşaklar: Sosyal medya kullanımı üzerinde bir araştırma. *Pamukkale Journal of Eurasian Socioeconomic Studies*, 3(2), 1-15. DOI: 10.5505/pjess.2016.27146
- Schatz, D., Bashroush, R., ve Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, 12(2), 53-74.
- Seçmen, S. (2022). Kamu personelinin endüstri 4.0 bilgi düzeyleri ile rol belirsizliği algıları arasındaki ilişkinin yaratıcı örgüt kültürünün ılımlaştırıcı etkisi açısından incelenmesi: TÜBİTAK Bilgem örneği.
- Sevinç, K. (2021). *Siber güvenlik ölçeği geliştirme: Geçerlik ve güvenirlik çalışması* [Yüksek Lisans tezi, Tokat Gaziosmanpaşa Üniversitesi].
- Sezen, E. N. (2023). *Dünyada ve Türkiye'de video akış servislerinde rekabet-porter'in beş güç modeli üzerinden bir inceleme* [Doktora tezi, Marmara Üniversitesi].
- Siber Güvenlik Enstitüsü. (2019). Kamu kurumlarının uyması gereken asgari bilgi güvenliği kriterleri. T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı.
- Siber Suçlarla Mücadele Daire Başkanlığı. (2023). Hakkımızda. <https://www.egm.gov.tr/siber/hakkimizda2>

- Slayton, R. (2023). A Vulnerable System: The History of Information Security in the Computer Age by Andrew Stewart (review). Project MUSE.
- Solms, R. V., ve Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
- Srivastava, K. (2019). A new approach of artificial intelligence (ai) to cyber security. *International Journal of Research in Advent Technology*, 7(1), 410-412. <https://doi.org/10.32622/ijrat.71201980>
- Stewart, A. J. (2021). *A vulnerable system: The history of information security in the computer age*. Cornell University Press.
- Tabachnick, B. G., ve Fidell, L. S. (2013). *Using multivariate statistics* (6. baskı). Pearson.
- Taner, E., ve Kılıç, İ. (2019). Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma. *Güvenlik Bilimleri Dergisi*, 8(2), 253-269.
- Tanrıverdi, M. (2020). A systematic review of privacy preserving healthcare data sharing on blockchain. *Journal of Cybersecurity and Information Management*, 5, 31-37.
- Tek, S. (2022). *Türkiye ve dünyada gerçekleştirilen siber saldırı yöntemlerinin ve bu saldırılara karşı alınan önlemlerin incelenmesi* [Yüksek Lisans tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü].
- Tekerek, M., ve Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, 2(3).
- Tripathi, N., ve Hubballi, N. (2021). Application layer denial-of-service attacks and defense mechanisms: a survey. *ACM Computing Surveys (CSUR)*, 54(4), 1-33.
- TÜİK. (2020). *Türkiye'de de son dönemde internet ve bilgisayar kullanımı hızı*. <https://data.tuik.gov.tr/Kategori/GetKategori?p=bilgiteknolojileri-ve-bilgi-toplumu-102&dil=1>
- Ulusal Siber Güvenlik Stratejisi. (2012). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı ve Bilgi Güvenliği Derneği.
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. (2013). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.
- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. (2016). Ulusal siber güvenlik stratejisi ve eylem planı (2016-2019). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

- Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. (2020). Ulusal siber güvenlik stratejisi ve eylem planı (2020-2023). T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.
- Ünver, M., Canbay, C., ve Mirzaoglu, A. G. (2009). *Bilgi teknolojileri ve iletişim kurumu. Siber güvenliğin sağlanması Türkiye'deki mevcut durum ve alınması gereken tedbirler.*
- Usmonov, M. (2021). Basic concepts of information security. *Scienceweb Academic Papers Collection.*
- Vroom, C., ve Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, 23, 191-198.
- Wang, Q., Zhang, W., ve Wang, H. (2022). Privacy concerns toward short-form video platforms: Scale development and validation. *Frontiers in Psychology*, 13. <https://doi.org/10.3389/fpsyg.2022.954964>
- Whitman, M. E., ve Mattord, H. J. (2021). *Principles of information security.* Cengage Learning.
- Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., ... ve Platts, J. (2022). Cybersecurity, data privacy and blockchain: A review. *SN Computer Science*, 3(2), 127.
- Yang, F., ve Gu, S. (2021). Industry 4.0, a revolution that requires technology and national strategies. *Complex ve Intelligent Systems*, 7, 1311-1325.
- Yavanoğlu, U., Sağiroğlu, Ş., ve Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, 15(1), 15-27.
- Yavuz, A., ve Tuna, G. (2020). *Yazılım tanımlı ağların ve geleneksel bilgisayar ağlarının güvenlik karşılaştırması* [Yüksek Lisans tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü].
- Yayla, H. G. (2018). *Fatih projesi uygulanan ve uygulanmayan okullardaki öğretmenlerin bilgi güvenliği farkındalığının incelenmesi* [Yüksek lisans tezi, Ankara Üniversitesi]. YÖK Tez Merkezi.
- Yıldırım, H., ve Kaplan, V. (2021). 2010 anayasa değişikliğinin bilişim suçlarıyla mücadele politikası bakımından etkilerinin analizi ve bu amaçla kurulan kuruluşların incelenmesi. *Kamu Yönetimi ve Politikaları Dergisi*, 2(3), 299-324.

- Yıldırım, N., ve Varol, A. (2013). Sosyal ağlarda güvenlik: Bitlis Eren ve Fırat Üniversitelerinde gerçekleştirilen bir alan çalışması. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 6(1).
- Yıldırım, Y. (2020). Farklı disiplinlerde endüstri 4.0. *OPUS International Journal of Society Researches*, 15(21), 756-789.
- Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Digital data security awareness of teachers. *Sakarya University Journal of Education*, 6(2), 26-45.
- Yılmaz, O., ve İbret, B. Ü. (2023). Ortaokul öğrencilerinin dijital vatandaşlık düzeylerini belirlemeye yönelik bir ölçek geliştirme çalışması. *Muş Alparslan Üniversitesi Eğitim Fakültesi Dergisi*, 3(1), 59-77.
- Yorgancıoğlu, E., ve Demircan, Y. T. (2023). Bilgi teknolojileri ve iletişim kurumu tarafından toplanan internet trafik verilerinin kişisel verilerin korunması hakkı bağlamında değerlendirilmesi. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 22(48), 1189-1215.
- You, Z., ve Feng, L. (2020). Integration of industry 4.0 related technologies in construction industry: A framework of cyber-physical system. *IEEE Access*, 8, 122908-122922.

EKLER

EK 1. ORİJİNALLİK RAPORU FORMU



ARDAHAN ÜNİVERSİTESİ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

ARDAHAN ÜNİVERSİTESİ LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ İLERİ TEKNOLOJİLER ANA BİLİM DALI BAŞKANLIĞINA

Tarih: 26/06/2024

Tez Başlığı: Kamu Personelinin Siber Güvenlik Farkındalığının Tespiti

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 64 sayfalık kısmına ilişkin, 07.06.2024 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %19 'dur.

Uygulanan filtrelemeler:

- 1- ☒ Kabul/Onay ve Bildirim sayfaları hariç
- 2- ☒ Kaynakça hariç
- 3- ☒ Alıntılar hariç
- 4- ☒ 5 kelimedenden daha az örtüşme içeren metin kısımları hariç

Ardahan Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği'nde belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

26.06.2024

Adı Soyadı: Bariş DAŞDEMİR
Öğrenci No: 21408700013
Ana Bilim Dalı: İleri Teknolojiler
Programı: İleri Teknolojiler Programı
Statüsü: ☒ Yüksek Lisans ☐ Doktora

DANIŞMAN GÖRÜŞÜ VE ONAYI

Dr. Öğr. Üyesi, Salih Serkan KALELİ

EK 2. ETİK KURUL İZİN FORMU



T.C.
ARDAHAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Rektörlük



Sayı : E-67796128-000-2300037382
Konu : Bilimsel Yayın ve Etik Kurul Kararı
(Dr.Öğr.Üyesi Salih Serkan KALELİ)

Sayın Dr. Öğr. Üyesi Salih Serkan KALELİ

Danışmanı olduğumuz Yüksek Lisans Öğrencisi Barış DAŞDEMİR'in "Kamu Personelinin Siber Güvenlik Farkındalığının Tespiti" başlıklı tez çalışması ve bu tez çalışması kapsamında yapılacak araştırmalarda uygulayacağımız ölçekler Üniversitemiz Etik Kurulu tarafından değerlendirilmiş olup, yapılan değerlendirme sonucu söz konusu çalışmanızın Bilimsel Araştırma ve Yayın Etik Kriterlerine uygun olduğuna karar verilmiştir.

Bilgilerinize rica ederim.

Prof. Dr. Mustafa YILDIZ
Bilimsel Araştırma ve Yayın Etik Kurulu Başkanı

Adres: Ardaahan Üniversitesi Yenisey Kampüsü Rektörlük Hizmet Binası , Çamlıçatak Mevkii, Ardaahan
75002
Telefon No: (0 478) 2117575
e-Posta: hayek@ardahan.edu.tr
Kep Adresi: ardahanuniv@tr01.kep.tr

Faks No: (0 478) 2117509
İnternet Adresi: www.ardahan.edu.tr

Bilgi için :
Telefon No:
Direkt Hat:

Derya Kuruçam
Etik Kurul Görevlisi
(0 478) 2117575



EK 3. VERİ TOPLAMA İZİNİ

T.C.
ARDAHAN VALİLİĞİ
İl Emniyet Müdürlüğü



Sayı : E-30714686 -91244-2023121311345054048
Konu : Anket Hk.

13.12.2023

DAĞITIM YERLERİNE

İlgi : 13.12.2023 tarihli ve - sayılı yazı.

İlgi sayılı yazı ile Müdürlüğümüz personeli olan Barış DAŞDEMİR'in dilekçesinde belirtmiş olduğu "Kamu Personelinin Siber Güvenlik Farkındalığının Tespiti" adlı tez çalışması için veri toplama talebinde bulunmuştur. Bu kapsamda Müdürlüğümüz personelinin aşağıdaki internet adresi üzerinden erişim sağlayarak 20.12.2023 tarihine kadar ankete katılım sağlaması hususunda;
Gereğini rica ederim.

Adem NAZLI
İl Emniyet Müdürü a.
İl Emniyet Müdür Yardımcısı
2. Sınıf Emniyet Müdürü
E-İMZA

İlgili Link:

https://docs.google.com/forms/d/e/1FAIpQLSf6DkV5m0_R1NvLuls7us-g5Y-o0huBdbVicDaVuTGHwV-Kw/viewform?usp=sf_link

Dağıtım :
Merkez ve İlçe Teşkilatına

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu: c362c3b5-1996-4e13-abbf-8a4b37c537ac Belge Doğrulama Adresi: <https://simza.egm.gov.tr>

Adres : İnönü Mahallesi Kongre Caddesi No:171-B Merkez/ARDAHAN
Telefon/Fax: 0(478) 211 57 20/0(478) 211 57 19
Kop : emniyetgenelmudivlugu@hs01.kop.tr

Ayrıntılı Bilgi : Strateji Geliştirme Ş.M.
Unvanı :
Elektronik Ağ : www.ardahan.pol.tr

1/1



EK 4. ANKET FORMU

Bu çalışma, kamu personellerinin siber güvenlik farkındalığını siber güvenlik ölçeği (sgö) kullanarak incelemektedir. Çalışma kapsamında Ardahan Emniyet Müdürlüğü'ndeki personellerinden anket uygulaması yoluyla elde edilecek veriler istatistiksel analiz yöntemleri ile yorumlanacaktır. Araştırmanın amacına ulaşabilmesi için en az 200 personele anket uygulanması gerekmektedir. Katılımcıların anketi cevaplama süresi yaklaşık 20 dakikadır. Katılımcıların araştırmada yer almaları tamamen gönüllülük esasına dayanmaktadır. Katılımcı istediği zaman araştırmadan çekilebilmektedir. Bu durumda, katılımcıyla ilgili veriler kullanılmayacaktır. Katılımcıların ankete katılması durumunda hiçbir özel bilgi istenmeyecek, herhangi bir ücret talep edilmeyecektir. Araştırma sonuçları ile ilgili bilgi alınmak istenmesi halinde araştırmacılar ile iletişime geçilebilir.

ANKET SORULARI

Katılımcı Bilgi Formu					
Cinsiyet	() Erkek	() Kadın			
Yaş	() 18-25	() 25-35	() 35-45	() 45 +	
Eğitim Durumunuz	() Lise	() Lisans	() Ön Lisans	() Yüksek Lisans	() Doktora
Kaç yıldır bu meslektesiniz ?	() 2 – 5 yıl	() 5- 10 yıl	() 10- 15 yıl	() 15 yıl +	
İnternet kullanımı Süreniz ?	() 1-2 saat	() 3-4 saat	() 5-7 saat	() 8 saat ve üzeri	
Mobil Cihazınızda internet var mı?	() Evet	() Hayır			
İnternet Kullanma Amacınız ?	() İnternet/mobil bankacılık hizmetini kullanırım () E-devlet hizmetlerini kullanırım () E-ticaret siteleri üzerinden internet alışverişi yaparım () Kullanmıyorum ve kullanmayı düşünmüyorum () Diğer (Belirtiniz)				

Siber Güvenlik Ölçeği (SGÖ)						
SORU NO	SORULAR	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
Gizlilik Ölçeği						
1	Siber ortamda paylaştığım kişisel bilgiler konusunda temkinliyimdir.					
2	Gerçek hayatta üçüncü şahıslarla paylaşmak istemediğim bilgi ve belgeleri siber ortamda da paylaşmam.					
3	Siber ortamda paylaştığım verilerin sadece gerekli kişilerce görüntülenmesini sağlarım.					
Kontrol / Sahiplik Ölçeği						
4	Hesaplarıma ait şifrelerin güvenliği konusunda dikkatliyim.					
5	Şifremleri oluştururken sembol, rakam ya da büyük küçük harflerden oluşan tahmini zor bir şifre seçerim.					
6	E-posta şifremin güvenliği için telefon doğrulaması hizmetini kullanırım.					
7	Cevabını hatırlayacağım bir güvenlik sorusu seçmeye özen gösteririm.					
8	Kredi kartı bilgilerimin kaydedilmemiş olmasına dikkat ederim.					

Bütünlük Ölçeği						
9	Siber ortamda veri saklamak güvenli değildir.					
10	Siber ortamda sakladığım bilgi ve belgeler kaybolabilir ya da silinebilir.					
11	Siber ortamda veri paylaşımı yapmak herhangi bir risk içermez (T: Ters Madde).					
12	Siber ortamda saklanan bilgi ve belgelere üçüncü şahısların erişme olasılığı vardır.					

Gerçeklik Ölçeği					
13	Tanımadığım kişilerden gelen e-postalardaki linkleri ve eklentileri açarım (T).				
14	Girdiğim web sitesinin güvenlik sertifikası olmadığı yönünde bildirim gelse de kullanmaya devam ederim (T).				
15	E-postama gelen istenmeyen (spam) postaları açtığım olmuştur (T).				
16	E-postama gelen müşteri edinme/ortalama amaçlı postaları açtığım olmuştur (T).				
17	Belirsiz kaynaklardan gelen bağlantıları (linkleri) ve dosyaları açtığım olmuştur (T)				
Erişilebilirlik Ölçeği					
18	Cihazımda güncel bir anti virüs programı var.				
19	Cihazımı düzenli olarak anti virüs programı ile taratırım.				
20	Cihazıma kurulu gelen güvenlik duvarı açık.				
21	İnternette indirdiğim dosyaları cihazımda yüklü anti virüs programı olmasa da açarım (T).				
Fayda Ölçeği					
22	Siber ortamda sosyal medya uygulamalarını bilgi paylaşımı için kullanırım.				
23	Günlük hayatta karşılaştığım problemleri çözmek için siber ortamı yaygın olarak kullanırım.				
24	Siber ortamda sunulan hizmetlerden bilgi yönetimi (bilgiyi elde etmek, saklamak, paylaşmak ve kullanmak) için faydalanırım.				

ÖZ GEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Barış DAŞDEMİR

Doğum Yeri ve Tarihi :

Eğitim Durumu

Lisans Öğrenimi : Samsun 19 Mayıs Üniversitesi Bilgisayar ve Öğretim Teknolojileri Öğretmenliği

Yüksek Lisans Öğrenimi : Ardahan Üniversitesi İleri Teknolojiler Anabilim dalı İleri Teknolojiler Programı

Bildiği Yabancı Diller : İngilizce (İyi)

Bilimsel Faaliyetleri :

İş Deneyimi

Stajlar :

Projeler :

Çalıştığı Kurumlar : Emniyet Genel Müdürlüğü

İletişim

E-Posta Adresi :

Tarih

Jüri Tarihi : 26.06.2024