T.C.
BİNGÖL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

KAMU KURUMLARINDA ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞI ÜZERİNE BİR ARAŞTIRMA: DİYARBAKIR ÖRNEĞİ

İslam ACAR

YÜKSEK LİSANS TEZİ

Danışman
Dr. Öğr. Üyesi Ömer ÇAMUR

Bingöl – 2024

T.C.

BİNGÖL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE KAMU YÖNETİMİ ANABİLİM DALI

KAMU KURUMLARINDA ÇALIŞANLARIN BİLGİ GÜVENLİĞİ FARKINDALIĞI ÜZERİNE BİR ARAŞTIRMA: DİYARBAKIR ÖRNEĞİ

İslam ACAR

YÜKSEK LİSANS TEZİ

Danışman

Dr. Öğr. Üyesi Ömer ÇAMUR

Bingöl – 2024

İÇİNDEKİLER

BİLİMSEL ETİK BİLDİRİMİ

Yüksek Lisans tezi olarak hazırladığım Kamu Kurumlarında Çalışanların Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Diyarbakır Örneği adlı çalışmanın öneri aşamasından sonuçlanmasına kadar geçen süreçte bilimsel etiğe ve akademik kurallara özenle uyduğumu, tez içindeki tüm bilgileri bilimsel ahlak ve gelenek çerçevesinde elde ettiğimi, tez yazım kurallarına uygun olarak hazırladığım bu çalışmamda doğrudan veya dolaylı olarak yaptığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu beyan ederim.

…/…/2024

İmza

İslam ACAR

BİNGÖL ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İslam ACAR tarafından hazırlanan Kamu Kurumlarında Çalışanların Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Diyarbakır Örneği başlıklı bu çalışma, *17/04/2024* tarihinde yapılan tez savunma sınavı sonucunda *[oybirliği]* başarılı bulunarak jürimiz tarafından Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

TEZ JÜRİSİ ÜYELERİ (Unvanı, Adı ve Soyadı)

Başkan	: Dr. Öğr. Üyesi Yunus Emre AYNA	İmza: …….
Danışman	: Dr. Öğr. Üyesi Ömer ÇAMUR	İmza: …….
Üye	: Dr. Öğr. Üyesi Ali ÇİÇEK	İmza: …….

ONAY

Bu Tez, Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Kurulunun …/…/ 2024 tarih ve ..... Sayılı oturumunda belirlenen jüri tarafından kabul edilmiştir.

Unvanı Adı Soyadı

Enstitü Müdürü

ÖNSÖZ

Kamu Kurumlarında Çalışanların Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Diyarbakır Örneği konusu, kamu kurumlarında çalışanların, bilgi güvenliği farkındalığı seviyesinin belirlenmesi ve geliştirilmesi gereken alanlarda önerilerin sunulmasıdır. Bu doğrultuda, Diyarbakır ilinde bulunan kamu kurumlarında toplam 164 çalışana araştırma anketi elektronik ortamdan ulaştırılarak uygulanmıştır.

Bu çalışmanın hazırlanmasında yardımlarını esirgemeyen danışman hocam Dr. Öğr. Üyesi Ömer ÇAMUR'a, tezin yazım aşamasında ve tashihinde katkılarını esirgemeyen *Dr. Öğr. Üyesi Yunus Emre AYNA*, *Dr. Öğr. Üyesi Ali ÇİÇEK, Yaşar KODATKU, Sevgi EFE, Müslüm ACAR*'a ve eğitim hayatım boyunca yetişmemde katkısı olan tüm hocalarıma teşekkürlerimi sunmayı bir borç bilirim.

Çalışmamı tamamlamam konusunda moral ve motivasyonumu üst düzeyde tutmama yardımcı olan aileme şükranlarımı sunarım.

…/…/2024

İslam ACAR

ÖZET

Tezin Başlığı :	Kamu Kurumlarında Çalışanların Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Diyarbakır Örneği
Tezin Yazarı :	İslam ACAR
Danışman :	Dr. Öğr. Üyesi Ömer ÇAMUR
Anabilim Dalı:	Siyaset Bilimi ve Kamu Yönetimi
Bilim Dalı :	Siyaset Bilimi ve Kamu Yönetimi
Kabul Tarihi :	17.04.2024
Sayfa Sayısı :	12 (ön kısım) + 77 (Tez) + 3 (Ekler)

Bu çalışmanın amacı, kamu kurumlarında çalışan personelin bilgi güvenliğine ait bilinç ve farkındalığı yükseltmek ve geliştirilmesi ihtiyaç duyulan alanlarda öneride bulunmaktır. Diyarbakır ilinde rastgele seçilen kamu kurumlarında çalışan personelin bilgi güvenliği farkındalıkları çeşitli veri ve istatistiklerden yararlanılarak ölçülmüştür. Çeşitli kademelerde çalışan toplam 164 personele "Bilgi Güvenliği Farkındalık Ölçeği" uygulanmıştır. Bu çalışmada araştırmanın çerçevesini oluşturan bilgi ve bilgi güvenliği ile ilgili kavramlar, bilgi güvenliği unsurları, amacı ve önemi, yönelik tehditler, yaşanan ortak sorunlar, yönelik alınması gereken önlemler, bilgi güvenliği farkındalığı üzerinde durulmuştur.

Faktör analizi sonucunda ölçeğin, 31 maddeden oluştuğu ve personelin yaş, cinsiyet, öğrenim durumu, görev türü, görev süresi, kaç yıldır internet kullandığı ve günlük internet kullanım süresi değişkenlerine göre farklılık gösterip göstermediği araştırılmıştır. Bu kapsamda araştırmada elde edilen veriler, Kaiser-Mayer-Olkin (KMO) Testi ve Bartlett Sphericitiy Testi ile incelenmiştir. KMO değeri 1'e yakındır; Bartlett küresellik testi ise anlamlı bulunmuş ve p değeri, 0,05'den küçüktür. Cranbach Alfa güvenirlik değeri ise 0,971'dir. Daha sonra anlamlı farklılık bulunan grupların tespiti için Kruskall Wallis ve Mann-Whitney U testleri kullanılmıştır.

Araştırma sonucunda bilgi güvenliği farkındalığı alt faktörlerinin personelin cinsiyetine göre, kadınların ve erkeklerin bilgi güvenliği farkındalığına göre fark bulunmaktadır ($p<0,05$). Hem bilgi güvenliği farkındalığında hem de faktörlerde, erkeklerin puan ortalaması, kadınlardan daha fazladır. Yaş, görev türü, eğitim durumu ve günlük internet kullanım süresine göre görev süresine göre anlamlı farklılık bulunmamaktadır ($p>0,05$). İnternet kullanma yılı değişkenine göre bilgi güvenliği farkındalıklarında ve birinci faktöründe anlamlı farklılık bulunmaktadır ($p<0,05$). 20 yıl ve üzeri olanların bilgi güvenliği farkındalığı daha yüksektir. Ancak ikinci faktörde katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$).

Anahtar Kelimeler: Bilgi, Bilgi Güvenliği, Farkındalık, Kamu Çalışanı

ABSTRACT

Title of the Thesis: A Research On Information Security Awareness OfEmployees In Public Institutions:Diyarbakır Example	
Author	**:** İslam ACAR
Supervisor	**:** Doctor Assistant Professor Ömer ÇAMUR
Department	**:** Political Science And Public Administration
Sub-field	: Political Science And Public Administration
Date	**:** 17.04.2024

The purpose of this study is to raise the awareness and awareness of information security among personnel working in public institutions and to make suggestions in areas that need improvement. It is to measure the information security awareness of personnel working in randomly selected public institutions in Diyarbakır province by using various data and statistics. "Information Security Awareness Scale" was applied to a total of 164 personnel working at various levels. In this study, concepts related to information and information security, which constitute the framework of the research, information security elements, its purpose and importance, threats, common problems experienced, precautions to be taken, information security awareness are emphasized.

As a result of the factor analysis, it was investigated whether the scale consists of 31 items and whether it differs according to the variables of the personnel's age, gender, education level, type of job, tenure, how many years they have been using the internet and daily internet usage time. In this context, the data obtained in the research were examined with the Kaiser-Mayer-Olkin (KMO) Test and Bartlett Sphericity Test. The KMO value is close to 1; Bartlett's test of sphericity was found to be significant and the p value was less than 0.05. Cranbach Alpha reliability value is 0.971. Then, Kruskall Wallis and Mann-Whitney U tests were used to identify groups with significant differences.

As a result of the research, there is a difference in information security awareness sub-factors according to the gender of the personnel and the information security awareness of men and women ($p < 0.05$). In both information security awareness and factors, the average score of men is higher than that of women. There is no significant difference according to age, type of duty, education level and daily internet usage time and duration of duty ($p > 0.05$). There is a significant difference in information security awareness and its first factor according to the variable of years of internet use ($p < 0.05$). Those with 20 years or more have higher information security awareness. However, in the second factor, there is no significant difference between the participants' information security awareness ($p > 0.05$).

Key Words: Information, Information Security, Awareness, Public Employee

KISALTMALAR

CD	Yoğun Disk (Compact Disc)
DVD	Çok Amaçlı Sayısal Disk (Digital Versatile Disc)
USB	Flash Bellek
KMO	Kaiser- Mayer-Olkin
IAEA	Uluslararası Atom Enerjisi Kurumu
ISO	Uluslararası Standardizasyon Örgütü
p.	Page
S.	Sayfa
TC	Türkiye Cumhuriyeti
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TDK	Türk Dil Kurumu
TSE	Türk Standartları Enstitüsü
vb.	Ve benzeri

TABLO LİSTESİ

Tablo No **Sayfa**

ŞEKİL LİSTESİ

Şekil No **Sayfa**

1. GİRİŞ

Bilgi ve iletişim teknolojilerinde meydana gelen gelişmeler sonucunda devletlerin, kurumların ve şirketlerin temel amaçları, bilginin elde edilmesi, depolanması, saklanması ve bilgi çağına tutunabilmeleri için gerekenleri araştırma ve geliştirme faaliyetlerinin yürütülmesidir. Bilgi, geçmişten günümüze kadar yaşamın her kademesinde yer alması ve hayatı kolaylaştırması nedeniyle kıymetlidir. Bilgi konusundaki bu önem vatandaşlara hizmet sunmakla görevli bulunan kamu kurumları için ayrıca önemlidir. Kamu kurumları için değerli ve vazgeçilmez bir nitelikte bulunan bilginin, saldırılara ve tehditlere karşı korunabilmesi için, gizliliğinin ve bütünlüğünün korunması, bilgiye erişilebilirliğin kontrol altında tutulması gerekmektedir.

Günümüzde gelişen teknolojik gelişmelerle birlikte bilginin bilişim sistemlerine aktarılması sonucu bilgi güvenliğinin sağlanmasının sadece yazılım, donanım ya da teknik önlemler ile mümkün olmadığı, çalışan personelin ya da insan faktörünün de göz önünde bulundurulması gerektiği önemini ortaya çıkarılmaktadır. Bilgi güvenliği açıkları genellikle insan faktöründen kaynaklanır ve yazılım, donanım veya teknik önlemlerden ziyade bu faktörün etkisiyle ortaya çıkmaktadır.

Kamu kurumlarında bilgi güvenliği ile ilgili hataların, saldırıların ve tehditlerin belirtilerinin azaltılması için en etkileyici çözüm, kamu kurumlarında çalışan personelin hatalarının ortadan kaldırılmasıdır. Kamu kurumlarında çalışan personelin bilgi güvenliği farkındalığının oluşturulması, kendini geliştirmeleri, güvenlik politikalarını ve kurallarını önemsemeleri, benimsemeleri ve desteklemeleri gerekmektedir. Bunun sağlanabilmesi için çalışan personelin belirli zaman aralıklarında eğitime tabi tutulması ve bilinçlendirilmesi oldukça önemlidir.

Yazın literatüründe bilgi güvenliğinin sağlanabilmesi hususunda farklı önerilerin geliştirildiği görülmektedir. Bireylerin bilgi güvenliği farkındalığı konusunda ne kadar bilgiye sahip olduğu ve bilgi güvenliği ile farkındalık arasındaki ilişkide aracı konumda bulunan kavramların neler olduğuna yönelik birçok unsur belirlenmiştir. Osterman Research'un (2020), 2019 yılında Amerika'da çeşitli kuruluşlarda tam ve yarı zamanlı çalışan bin on beş kişiye yönelik bilgi güvenliği farkındalık düzeylerini ölçmek için yaptığı MediaPRO adlı araştırmada, personelin çoğu zaman çalıştıkları ortamlarda

çeşitli saldırılara maruz kaldıkları ortaya konmuştur. Kamu kurumlarında çalışan personel bilgi güvenliği hakkında yeterli bilgiye ve eğitim düzeyine sahip olmadığı için kamu kurumları çeşitli saldırılara ve tehditlere maruz kalmaktadır (Nezgitli, 2022, s. 1-16). Özdemir ve Uluyol (2020, s. 649-666) tarafından yapılan araştırmada, kamu kurumlarında çalışan personelin orta seviye bilgi güvenliği farkındalığına sahip olduğu belirtilmiştir. Parsons, McCormac, Pattinson, Butavicius ve Jerram'ın (2014, s. 334-345) çalışmasında, Avustralya'daki kamu kurumlarında çalışan bireylerin bilgi güvenliği hakkındaki bilgiye yeteri düzeyde sahip olduğu fakat bunun bilgi güvenliği farkındalığına yansımadığı ve kişilerin bilgi güvenliği farkındalığının yetersiz olduğu belirtilmiştir. Murat Güngör (2015), ulusal bilgi güvenliği için gerekli olan kurumsal yapılanma ile stratejiler konusunu ele almıştır. Alkan, Atalay, Canbek ve Bilirgen (2012, s. 1-34) çalışmalarında, siber güvenlik kültürünün oluşması ve siber güvenlik tehditlerine karşı kritik altyapıların korunması hususunda kurum, kuruluş ve işletmelerle beraber yönetici, çalışan ve kullanıcıya yönelik bilgi güvenliği farkındalığını arttıran etkinlikler düzenlenmesi gerektiğini önermişlerdir. SANS Enstitüsü'nün (2021) Güvenlik Farkındalığı Raporu'na göre, birçok kurum çalışanlarının güvenlik farkındalığına yeterince önem vermediklerini belirtilmiştir. Shehri ve Clarke (2007, s. 12-22) yaptığı çalışmada, bilgi güvenliği farkındalığı konusunda gerekli eğitimleri almayan çalışanların bilgi güvenliği farkındalığı konusunda eğitim alanlara göre daha düşük çıkmıştır. Lim, Chang, Maynard ve Ahmad'ın (2009) araştırmalarında, örgüt kültürünün çalışanlar üzerindeki etkisinden bahsetmişlerdir. Çalışmada, bilgi güvenliği kültürünün oluşmasında örgüt kültürünün rolünü ortaya koymuşlardır. Johnson ve Goetz'in (2007, s. 16-24), yaptıkları araştırmada, kurumsal bilgi güvenliği sağlaması konusunun işyerindeki herkesin görevi olduğu belirtilmiş ve örgütsel bir hareket ile yürütülmesi gerektiği ifade edilmiştir. Maynard, Ruighaver ve Chia (2002) çalışmalarında, gelişen teknolojinin işyerinin sahip olduğu bilgi varlıklarını riske atarak tehdit edebildiği ifade edilerek bunun sonucunda bilgi güvenliği hassasiyetinin arttırılarak bu konunun örgüt kültürünün bir parçası olan tüm çalışanlarca benimsenmesi gerektiğini ifade edilmiştir. Yapılan araştırmalarda, örgüt kültürü ile kurumsal bilgi güvenliğinin birbirlerine katkı sağladığı ve birbirleriyle bağlantılı olduğu ortaya konmuştur.

Daha önceki yapılan çalışmalar doğrultusunda bilgi güvenliği farkındalığının ölçülmesi ile ilgili farklı parametrelerin kullanıldığı görülmektedir. Bu çalışmada kamu kurumlarında çalışan personelin bilgi güvenliği farkındalığı araştırma yöntemlerinden nicel araştırma yöntemi benimsenmiş olup araştırma yöntemlerinden anket yöntemi tercih edilerek incelenmiştir. Dolayısıyla kamu kurumlarında çalışan personelin bilgi güvenliği farkındalığı ölçeğinden elde edilen veriler ile cinsiyet, yaş, öğrenim düzeyi, görev türü, görev süresi, kaç yıldır internet kullandığı ve günlük ortalama internet kullanım süresi gibi değişkenler arasındaki ilişki incelenmiştir.

Tezin planı şu şekilde geliştirilmiştir. Birinci bölüm bilgi güvenliği ile ilgili giriş amaçlanmakta, daha sonra ikinci bölümde ise bilgi ve bilgi güvenliği ile ilgili kavramlar, bilgi güvenliği unsurları, bilgi güvenliğinin amacı ve önemi, bilgi güvenliğine yönelik tehditler, bilgi güvenliğinde yaşanan ortak sorunlar, bilgi güvenliğine yönelik alınması gereken önlemler, bilgi güvenliği farkındalığı, bilgi güvenliği ile ilgili yapılan araştırmalar üzerinde durulmuştur. Çalışmanın üçüncü bölümünde ise materyal ve yöntem olarak araştırmanın problemi, amacı, yöntemi, evren ve örneklemi, hipotezleri, kısıtlılıkları, araştırmada kullanılan ölçme araçları olarak sunulmuştur.

Çalışmanın dördüncü bölümünde ise araştırmanın bulguları, kamu kurumlarında çalışan personelin bilgi güvenliği farkındalığını belirlemek amacıyla kamu kurum ve kuruluşlarında e-anket yöntemi kullanılarak uygulanmıştır. Anket sonuçları bulgular ve analiz sonuçları yapılmıştır. Araştırmanın beşinci bölümünde ise çalışmanın sonuçları, tartışmalar ve öneriler ele alınmıştır.

2. BİLGİ VE BİLGİ GÜVENLİĞİ

Günümüzde gelişen teknolojik gelişmelerle beraber bilgi güvenliği birden fazla anlam ve ilkeleri kapsamaktadır. Bu başlık altında bilgi ve bilgi güvenliği ile ilgili kavramlar, bilgi güvenliği unsurları, bilgi güvenliğinin amacı ve önemi, bilgi güvenliğine yönelik tehditler, bilgi güvenliğinde yaşanan ortak sorunlar, bilgi güvenliğine yönelik alınması gereken önlemler, bilgi güvenliği farkındalığı, bilgi güvenliği ile ilgili yapılan araştırmaları incelenmiştir.

2.1.Bilgi ve Bilgi Güvenliği ile İlgili Kavramlar

Bu başlıkta mevzunun daha kolay ve basit şekilde anlaşılması için; bilgi güvenliği ile ilgili kavramlar açıklanmıştır.

2.1.1. Bilgi

Bilginin ne olduğu ile ilgili çeşitli tanımlar ve tartışmalar yapılmıştır. Ama genel olarak kabul gören ve benimsenen ise, "bilen özne ile bilinen nesne arasında ortaya çıkan ürün olarak tanımlanmaktadır. Özne ve nesne arasındaki ilişki sonucunda oluşan ürün, bilgidir" (Yıldırım, 2019). Bilginin ne olduğu önemli olmakla beraber nasıl elde edildiği de önemlidir. Günümüzde meydana gelen teknolojik gelişmeler sayesinde birçok alanda değişmeler ve yenilikler meydana gelmektedir. Bu durum bilginin elde edilme yöntemini etkilemiştir.

Bilim ve araştırmalar sonucunda elde edilen bilgi, kök itibariyle bilmek kelimesinden gelmektedir. Kamu kurumlarının değişmelere, gelişmelere, yeniliklere ayak uydurması, toplumlar ile ilgili daha net etkileşimin olması için doğru ve tam bilginin önemi oldukça büyüktür. Sparrow (1998)' a göre "bilgi günlük yaşamda öğreti, sezgi, his ve yargı gibi kavramlarla iç içe geçmişti." Bilgi, kamu kurumları için kıymetli bir varlıktır. Küreselleşen dünyada meydana gelen teknolojik gelişimlerle kamu kurumlarında çalışan personelin elde etmiş olduğu veriler ve bu verilerin üretimi, dağıtımı, çalışanların katkılarıyla oluşturulmuş bilgilerin ve bu bilgilerin muhafaza edilmesi ve amacına uygun şekilde kullanması gerekmektedir.

Bilgi çağı dediğimiz bu dönemde meydana gelen teknolojik gelişmeler zaman içerisinde birçok problemi beraberinde getirmiştir. Kamu kurumlarının gelişmesi, şeffaflaşması, hızlanması, demokratikleşmesi ve çağdaşlaşması için teknolojinin nimetlerinden faydalanması gerekmektedir. Bilgi, toplumların yaşamlarını

kolaylaştıran ve aynı zamanda çeşitli tehditlere ve saldırılara maruz kalan, kimi zaman da toplumların gelişmesi için bir araç olarak kullanılmaktadır. Bu durum bilginin elde edilmesi ve üretilmesini zorlaştıran unsurlardan biridir. Şekil 2.1'de görüldüğü üzere bilgi farklı aşamalar ile ortaya çıkmaktadır ve bu durum bilginin elde edilmesinin kolay bir iş olmadığını göstermektedir.

.

Şekil 2. 1:Bilgi Piramidi (DIKW)

Kaynak: (Hey, 2004).

Bilgi farklı unsurları kendi içerisinde barındıran karmaşık bir süreç ağıdır. Şekil 2.1'de görüldüğü gibi bilgi, veri (data), enformasyon (information), malumat (knowledge) ve hikmet (wisdom) unsurlarını barındırmakta ve bir süreç dahilinde ortaya çıkmaktadır. Bilginin ortaya çıkmasında etkili olan bu unsurların açıklanması kavramın ne olduğunun daha kolay bir şekilde anlaşılması açısından önemlidir.

- **Veri (Data):** Bilginin kaynağıdır. Herhangi bir olay veya iş hakkında işlenmemiş, düzenlenmemiş, ham olan veya üzerinde herhangi bir işlem yapılmayan, bir anlam ifade etmeyen ve ilişkisiz olan sinyallerdir (Davenport & Prusak, 2001)
- **Enformasyon (Information):** İnsanların akıl yürütme veya gözlem yoluyla edindikleri bilgilere güvenir ve onları doğru olarak kabul ettikleri bildirimlerdir. Bilginin alınması ve verilmesi bilinçli yapılır. Verinin anlamlı hale geldiği ve birbirleriyle ilişkilendirildiği form bilgi olarak ifade edilir (Davenport & Prusak, 2001).

- **Malumat (Knowledge):** Arapça kökenli bir kelime olup "bilgi ve haber" anlamına gelir. Kişisel deneyim, inançlar ve yaşantılar yoluyla elde edilir. Bilme aşamasındaki bir üst derecedir ve kişisel bilginin oluşmasını sağlar. Kesin değildir. Zamana ve çevreye göre değişebilir (Brakensiek, 2002).
- **Hikmet (Wisdom):** Bilgiyi kullanarak değer ve fark yaratmak, öngörmek, güvenilir ve doğru sonucu bulmak için neyin, nasıl ve nerede kullanacağını anlamaktır (Canbek ve Sağıroğlu, 2006, s. 165-174).

Günümüzde meydana gelen teknolojik gelişmeler bilgi alanında bazı sorunların ortaya çıkmasına neden olmuştur. Bilgi kamu kurumları için değerli ve önemli bir varlıktır ve hizmetlerin sürekliliği için muhafaza edilmesi gerekir. Bilginin önemli olması sebebiyle elde edilmesi zor veya elde edilen bilginin doğru bir şekilde korunması hem vatandaşın hem de kamu kurumlarının güvenliğinin sağlanması ve bunun ile ilgili düzenlemelerin yapılması gerekmektedir. Bu durum bilginin güvenliğinin sağlanmasını gerektirmektedir (Özdemir ve Uluyol, 2021, s. 649-666).

2.1.2. Güvenlik

Dünyaya adım atan her varlığın ilk amacı varlığını korumak ve sürdürmektir. Güvenlik, insanların hayatında kaygıdan, endişeden, üzüntüden emin olunması ve emniyet içinde hukuk kurallarının ihlal edilmeden uygulanması ve bireylerin korkusuzca ve özgürce yaşayabilmesidir. Güvenlik, 1986 yılında meydana gelen Çernobil Nükleer Santrali kazasından sonra ortaya atılmış bir kavramdır (Cox & Flin, 1998, s. 190). Uluslararası Atom Enerjisi Kurumu (IAEA), 1991 yılında güvenlik kavramını şu şekilde tanımlar: "Kurumun sağlık ve güvenlik programlarının yeterliliğine, tarzına ve uygulamadaki ısrarına karar veren birey ve grupların değer, tutum, yetkinlik ve davranış örüntülerinin bir ürünüdür" (Özkan ve Lajunen, 2003, s. 3).

Güvenlik kavramı günümüzde meydana gelen teknolojik gelişmeler dikkate alınarak birçok yönden ele alınması ve değişen şartlara göre çerçevesinin tekrardan belirlenmesi gereken kavramlardan biridir. Yaşanan gelişmeler bir yandan güvenlik kavramı ile ilgili tanımları artırırken diğer yandan kavramın tanımlanmasını zorlaştırmaktadır. Bu durum her dönemde geçerli olabilecek bir güvenlik tanımının

yapılmasını zorlaştırmaktadır. Literatürde güvenliğin ne olduğu ile ilgili birçok tanıma ulaşmak mümkündür (Akalp ve Yamankaradeniz, 2013, s. 96-109).

Güvenlik, genel olarak tehlikelerden, zararlı etkilerden, istenmeyen olaylardan veya istismardan korunma durumunu ifade eder. Güvenlik, bir sistemin, varlıklarının (verilerin, kaynakların, kullanıcıların vb.) korunmasını sağlamak amacıyla uygulanan önlemler ve süreçlerdir. Güvenlik, bireylerin, kurumların veya organizasyonların hassas bilgilerini ve kaynaklarını tehditlere ve saldırılara karşı korumak için alınan tedbirlerin bir bileşenidir. Kurumsal güvenlik, bir şirketin veya kuruluşun faaliyetlerini koruma çabalarını ifade eder. Kurumsal güvenlik, yetkisiz erişim, veri sızıntıları, hırsızlık veya sabotaj gibi tehditlere karşı korumayı hedefler (Dursun, 2011).

Yapılan tanımlardan anlaşılacağı üzere güvenlik farklı anlamlara gelen ve birçok alanı kapsayan geniş kapsamlı bir kavramdır. Aynı zamanda bilgiyi de kapsamaktadır. Özellikle teknolojinin ve bilginin önemli hale geldiği günümüz modern dünyasında bilginin güvenliğinin sağlanabilmesi gerek bireysel anlamda insanların ve gerekse toplumsal anlamda devletlerin öncelikli konularının başında yer almaktadır.

2.1.3. Bilgi Güvenliği

Küreselleşen dünyanın bilişim sistemlerinde meydana gelen yenilikler sonucunda veriler çeşitli saldırılara maruz kalmaktadır. Bu durum bilginin güvenliğinin sağlanması zorunluluğunu beraberinde getirmektedir. Bilgi güvenliği farklı anlamlara gelen kavramlardan biridir. Bilgi güvenliği, bir organizasyonun veya bireyin sahip olduğu bilgilerin yetkisiz erişim, ifşa, değişiklik veya yok olmaya karşı korunmasıyla ilgili bir disiplindir. Bilgi güvenliği, bilgi varlıklarının korunması, risk yönetimi, yasal uyumluluk ve iş sürekliliği açısından önemli bir alandır. Bilgi güvenliği, bilginin bir varlık olarak risklerden ve saldırılardan korunması, doğru teknolojinin kamu amaçları için ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemek olarak ifade edilmektedir (Canbek ve Sağıroğlu, 2006, s.165).

Bilgi güvenliği konusu, meydana gelen teknolojik yeniliklerin takip edilerek gerekli önlemlerin alınması ve değişimlere açık olunmasını gerektiren bir alandır. Bilgi güvenliği sadece bilişim sistemlerindeki güvenlik demek değildir. Bilgi güvenliği, kişi, teknoloji ve süreç ile birlikte uygulanması ile mümkün olmaktadır. Bilgi

güvenliği, sürekli olarak izlenmesi ve güncellenmesi gereken bir süreçtir, başlangıcı ve sonu olmayan bir çaba gerektirir. Bu kapsamda bilgi güvenliği sürekli gerçekleştirilmesi gereken bir faaliyettir (Güngör, 2015, s.1).

Bilgi güvenliği her alanda gerçekleştirilmesi gereken bir amaç olarak kamu kurumları açısından ayrıca önemli bir yere sahiptir. Vatandaşların ihtiyaç duyduğu hizmetlerin sunulması amacıyla faaliyet gösteren kamu kurumları, bilgi güvenliğin sağlanması ile anlam kazanmaktadır. Vatandaşların ortak çıkarlarının ve haklarının korunması hususunda bilgi güvenliğinin oldukça önemli bir rolü bulunmaktadır.

Kamu kurumları teknolojide meydana gelen gelişmelerle beraber geleneksel hizmet sunumunu terk etmek zorunda kalmışlardır. Çünkü kurumların teknolojik gelişmelerle sunduğu hizmetlerde, fayda, hız, şeffaflık ve harcamalar gibi farklı alanlarda önemli avantajlar elde edilmiştir (Güngör, 2015, s.1). Kamu kurumlarında teknolojinin sunmuş olduğu imkânlardan faydalanılarak birçok bilgi dijital ortama aktarılmıştır ve kamu kurumları geleneksel hizmet sunma yöntemlerini terk etmiştir. Kamu kurumlarının değerli bilgileri elektronik ortamda sunması bilgilerin güvenirliğinin risklere ve saldırılara maruz kalmasına sebep olmuştur. Bundan dolayı kamu kurum ve kuruluşlarında bilgi güvenliği problemi ortaya çıkmıştır (Öğütçü, 2010, s. 7).

Bilgi güvenliği bilişim sistemlerindeki ulusal, kurumsal ve özel kişilerin geniş bir güvenlik sistemini ve yönetim alanını kapsayan bir anlayıştır (Yılmaz, 1998, s.147-158). Kurumsal bilgi güvenliği ise kamu kurumlarının oluşturduğu veri, ürün ya da hizmetin sürekliğini oluşturmak maksadı ile kurumsal bilginin olası risklere ve saldırılara karşı tüm önlemleri kapsayan yaklaşımdır (Bensghir, 2011, s. 1-99). Kamu kurumlarında, bilgi güvenliği geniş bir alanı ve karmaşık bir değişimi gerektiren bir alandır (Wright & Kakalık, 2007, s.187).

Kamu kurumları açısından bilgi güvenliği, verinin saklanması, bilişim sistemlerindeki çeşitli nedenlerle bilginin kullanımı, verinin tahribatı, silinmesi, değiştirilmesi, bozulması amacına uygun olmayan nedenlerle incelemesi, yok edilmesi yetkili olmayan kişilere karşı muhafaza edilmesi konularında her türlü önlemleri barındırmaktadır (Canbek ve Sağıroğlu, 2006, s.165).

Bu kapsamda, kamu kurumlarında bilgi güvenliği ağ, personel, teknoloji ve politika gibi geniş bir alanı kapsayan ve yönetilmesi zor bir süreçtir. Bu sürecin doğru bir

şekilde yönetilmesi için güvenlik ağlarının geliştirilmesi ve politikaların uluslararası standartlara uygun hale getirilmesi gerekmektedir.

2.2. Bilgi Güvenliği Unsurları

Kamu kurumlarında hizmetlerin sürekli yerine getirilmesi ve aksamaması için elektronik ortamda bilgi güvenliğinin temel prensiplerinin birlikte sağlanması gerekir. Kurumsal bilgi güvenliğinde bilgi gizliliğinin oluşması için erişilebilirliğin aksatılmaması ve bilginin bütünlüğünün oluşturulması gerekir. Kurumsal hizmetlerin sürekliliği için bilgi gizliliği gerekli şartları oluşturulduğunda eğer erişim de aksamalar oluyorsa o zaman bilgiye erişim engellendiği için bu bilgi bir anlam ifade etmez. Bunun yanı sıra erişim için gerekli şartları oluşturulduğunda ama bilginin bütünlüğü erişim için elverişli değilse o zaman hatalı bilgi olasılığı olacağından kurumsal bilgi güvenliği açısından bir anlamı olmayacaktır. Kamu kurumlarında hizmetlerin sürekliliği ve şeffaflığı, hız ve maliyetlerin azaltması için bilgi güvenliği ile ilgili temel unsurların birlikte sağlanması gerekir. Aksi takdirde kamu kurumlarında güvenlik eksikliği sorunu ortaya çıkar ve bu durum kurumların saldırılara maruz kalmasına sebep olur (Güngör, 2015, s. 8).

Bilgi güvenliği denilince ilk önce akla gelmesi gereken, bize ait olan bilgilerin başkaları tarafından kullanılmamasıdır. Literatürde bilgi güvenliğinin üç önemli unsuru olduğu ifade edilmektedir. Bu unsurlar gizlilik, bütünlük ve erişilebilirliktir.

Şekil 2. 2: Bilgi Güvenliği Temel Unsurları

Kaynak: (Coinwhales, 2023)

2.2.1. Gizlilik (Confidentiallity)

Gizlilik, bilginin yetkili olmayan şahısların eline geçmesini engellemektir. Gizliliğin en önemli unsuru başkası tarafından bilinmemesidir. Gizlilik, kişisel veya özel bilgilerin başkalarıyla paylaşılmasını istememe veya izin verilmemesi durumudur. Gizlilik, hassas veya özel bilgilerin yetkisiz erişimden, ifşadan veya kötüye kullanımdan korunmasını sağlayan bir kavramdır. Gizlilik, bir kişinin veya kurumun sahip olduğu bilgilerin gizli kalmasını ve sadece yetkili kişilerin erişebilmesini gerektirir. Gizlilik, bir kişinin veya organizasyonun sahip olduğu bilgilerin sadece yetkili kullanıcılar tarafından erişilebilmesini ve ifşa edilmemesini gerektirir (Andress, 2011, s. 5).

Kamu kurumlarındaki bilgiler hem vatandaşı hem de devletin güvenliğini etkilediği için önemlidir. Dolayısıyla kamu kurumları bilgi güvenliği konusunda daha hassas olmalıdır. Bilgi gizliliği konusunda bilgiler elektronik ortama aktarılırken, saklanırken, depolanırken veya internet üzerinde gönderirken yetkili olmayan kişilerden muhafaza edilmelidir.

Kamu kurumlarında bilgi güvenliği siber saldırılara karşı bilişim sistemlerindeki açıklardan, teknik eksikliklerden veya yetkili personelin hatasından dolayı bilişim sistemlerine izinsiz ulaşılabilmeyi beraberinde getirebilir. Siber saldırılar son zamanlarda kötü niyetli kişiler veya gruplar tarafından sıklıkla kullanılmaya başlanmıştır. Bu yüzden bilişim alt sistemlerinin modern ve güvenli olması gerekmektedir. Aynı zamanda personel bu konularda sürekli olarak eğitilmelidir. Bundan dolayı personelin sürekli donanımlı bir şekilde bilgi güvenliğine karşı hazırlıklı olması ve verilerin gizlenmesini bütün olarak güvence altına alması gerekmektedir (Tekerek, 2008, s. 133). Gizliliğin sağlanması ile kamu kurumlarında bilgi güvenliği sağlanabilecektir.

2.2.2. Bütünlük:(Integrity)

Kamu kurumlarında hizmetlerin devamlılığı için veriler veya bilgiler tümüyle muhafaza edilmelidir. Bütünlük, bilişim sistemlerindeki bilginin yetkili olmayan kişilerce bozulmasını, saklanmasını, değiştirilmesini, eklenmesini veya silinmesini önlemeyi amaçlar. Bütünlük, bilginin doğruluk, eksiksizlik ve tutarlılık açısından korunması anlamına gelir. Bu kavram, bir bilgi veya veri setinin yetkisiz değişikliklere

veya bozulmalara uğramadan korunmasını ifade eder (Yılmaz, 2013, s. 15) Bilginin bütünlüğü, verilerin orijinal hallerinin korunduğu ve izinsiz değişikliklerin önlenerek doğruluğunun sağlandığı anlamına gelir. Bilginin bütünlüğü zaman içinde meydana gelen teknolojik gelişmelere bağlı olarak pek çok değişiklikleri beraberinde getirmiştir. Bilgisayar ortamındaki verilerin muhafaza edilmesi için veriler arasındaki bağlantının tam anlamıyla sağlanması gerekir (Gelbstein & Kamal, 2002, s. 15).

Bütünlük, kamu kurumlarında bilgi güvenliğinin sağlanabilmesi için gerekli olan temel unsurlardan biridir. Bütünlük, kamu kurumlarında bilginin olduğu şekliyle kalmasını sağlamaktadır. Bu durum bilginin kamusal hizmetlerin sunumunda kendisinden beklenen amacı gerçekleştirmesini beraberinde getirmektedir. Dağınık, değiştirilmiş veya bir kısmı silinmiş, bütünlüğü sağlanamamış bilginin verimli hizmetler üretmesi mümkün değildir. Dolayısıyla kamu kurumları açısından bilginin bütünlüğünün sağlanması hizmetlerde verimliliğin sağlanması açısından oldukça önemlidir (Yılmaz, 2013, s. 15).

2.2.3. Erişilebilirlik (Availability)

Kamu kurumlarında bilişim sistemlerindeki bilginin amacı yetkili çalışanlar tarafından talep edildiğinde ya da ihtiyaç duyulması halinde ulaşılabilir veya kullanılabilir olmasıdır. Bu durum bilginin kusursuz bir şekilde kullanılmasını sağlayan prensiptir. Erişilebilirlik kurumsal bilgiye gelebilecek siber saldırılara mâni olmayı ve korumayı sağlar (Gelbstein & Kamal, 2002, s. 15). Erişilebilirlik, yetkili kullanıcıların bilgiye gerektiği şekilde erişebilmesini sağlar. Erişilebilirlik, bilginin doğru zamanda ve doğru kişilere ulaşılabilir olmasını hedefler. Bu, kullanıcıların bilgilere yetkili bir şekilde erişim sağlaması, güvenli kimlik doğrulama mekanizmalarının kullanılması ve gerektiğinde bilgilerin uygun formatlarda sunulması anlamına gelir (Karakuzu, 2015, s. 42).

Erişilebilirlik, kamu hizmetlerinin herkes için erişilebilir olması anlamına gelir. Kamu hizmetleri, hükümetlerin vatandaşlarına sağladığı temel hizmetlerdir ve tüm bireylerin bu hizmetlere eşit şekilde erişebilmesi için önemlidir. Erişilebilirlik gereksinimleri, kamu hizmetlerinin tasarımında ve uygulanmasında yenilikçi çözümlere teşvik eder. Bu da kamu hizmetlerinin genel kalitesini artırır ve tüm kullanıcılar için daha iyi deneyimler sunar. Erişilebilirlik, toplumun her kesiminin kamu hizmetlerine erişebilmesini sağlar ve demokratik bir toplumun temel taşlarından biridir. Kamu hizmetlerinin erişilebilir olması, insan haklarının korunması, toplumsal katılımın

teşvik edilmesi ve toplumsal eşitliğin sağlanması için önemlidir (Doğantimur, 2009, s.7).

2.3. Bilgi Güvenliğinin Amacı ve Önemi

Tarihsel dönemde teknolojinin gelişmesiyle beraber kamu kurumlarında bilgi güvenliği son derece önemli bir konuma gelmiştir. Kamu kurumlarında verilerin elektronik ortama aktarılması nedeniyle bilgi güvenliğinin önemi artmıştır. Bundan dolayı bilginin temel prensiplerine yönelik tehditlerin korunmaya çalışılması gerekmektedir.

Kamu kurumlarında bilgi güvenliğini sağlamanın temel amacı elektronik ortamdaki bilgilerin bütünlüğünü, gizliliğini ve erişilebilirliğini koruyarak, oluşabilecek tehditleri ve riskleri minimum düzeye düşürmektir. Bunun yanı sıra kamu kurumlarında oluşabilecek olası sistem sorunlarına anında müdahale ederek gereken çözümü sunmak, çalışanları bilgi güvenliği ile ilgili bilinçlendirmek ve personelin kurumun güvenlik kanunlarına ve politikalarına bağlı kalarak her türlü sistem açığını kapatmaktır (Şahinaslan, Kandemir ve Şahinaslan, 2009, s.1-6). Aslında bilgi güvenliği kamu kurumlarında hizmetleri sürekli, şeffaf, hızlı, kaliteli ve daha az maliyetle yerine getirmeyi amaçlamaktadır. Kamu kurumlarında bilgi güvenliğinin temel amaçları şunlardır:

- Ülkenin menfaatlerini korumak
- Kurumsal imaj, itibar, şeffaflık ve güvenirliğin oluşturulması
- Veri bütünlüğünün sağlanması
- Yetkili olmayanların bilgilere erişiminin engellenmesi
- Kurumsal gizliliğin ve mahremiyetin korunması
- Bilişim sistemlerin devamlığının sağlanması
- Bilgi güvenliği unsurlarının korunması

Yukarıda saydığımız bilgi güvenliğinin temel amaçları hizmet sunumu sırasında bilgilerin güvende kalmasını sağlamaktadır. Bu amaçlar aynı zamanda kurumun şeffaflığını, açıklığını, dürüstlüğünü ve itibarını da desteklemektedir. Dolayısıyla bilgi güvenliği ile ilgili kurumsal amaçların gerçekleştirilmesi önem arz etmektedir.

2.4. Bilgi Güvenliğine Yönelik Tehditler

Bilgi güvenliği, kamu kurumlarında hizmetlerin güvence altına alınabilmesi için çeşitli politikalar geliştirmektedir. Çünkü günümüzde meydana gelen teknolojik gelişmeler siber saldırıların çeşitlenmesine neden olmuş, bu durum ise tehditlerin kapasitesini geliştirmiştir. Küreselleşen dünyada bilgi güvenliğine yönelik saldırılar çeşitli değişimlere ve dönüşümlere de sebep olmuştur.

Kamu kurumlarında hizmetlerin devamlılığı ve bilgiye daha kolay ulaşabilmek için bilgi neredeyse tümüyle bilişim sistemlerine aktarılmıştır. Bilgilerin elektronik ortama aktarılması ve kurumların geleneksel hizmet düşüncesinden vazgeçmesi ile artık evrak, dosya vb. işlemler nedeniyle yaşanan zaman kaybının önlenmesine ve maliyetlerin azaltılmasına olanak sağlanmıştır. Bunun yanı sıra hizmetlerin hızlı ve şeffaf biçimde gerçekleştirilmesi sağlanmış, bürokrasinin azalmasına yönelik imkânlar ortaya çıkmıştır. Bu önemli gelişmelerle birlikte bilginin elektronik ortama aktarılması çeşitli tehditlerin de ortaya çıkmasına sebebiyet vermiştir (Şahinaslan, 2013, s. 9).

Bireyler işlerini herhangi bir zaman ve maliyet kaybı yaşamadan, bürokrasiye takılmadan internet üzerinde halledebilmektedirler. Bundan dolayı kamu kurumlarında bilgilerin daha hassas, gizli ve kişisel verilerin korunması gerekmektedir. Bilgi güvenliğinde bilişim sistemlerinin oluşturduğu teknik eksikler sonucunda meydana gelen olaylar bireylerin önemli verilerinin yetkisiz kişilerin eline ulaşmasına sebep olabilmektedir (Gülmüş, 2010, s. 3).

Bilgi güvenliğinde meydana gelen teknolojik gelişmeler bazen telafisi güç ve imkânsız zararların doğmasına, risklerin oluşmasına ve yeni saldırıların ortaya çıkmasına neden olmaktadır. Kamu kurumlarında bilgi güvenliğine yönelik saldırılar daha çok ağ üzerinden virüsler, zararlı yazılımlar ve insandan kaynaklanan hatalar sonucunda meydana gelmektedir. Bundan dolayı kamu kurumlarında hizmetlerin aksaması, gizlilik ihlali, kurumların itibarlarının zedelenmesi, güven sorunu ve bilgilere yetkisiz kişilerce ulaşılması gibi sorunlar ortaya çıkmaktadır (Tekerek, 2008, s. 132-137). Bu başlık altında insan kaynaklı tehditlere ve zararlı yazılımlardan kaynaklanan tehditlere değinilecektir.

2.4.1. İnsan Kaynaklı Tehditler

Kamu kurumlarında çalışan personelin bilgi güvenliği hakkında yeterli bilgiye sahip olması oldukça önemlidir. Bilişim sistemlerinde teknik yöntemlerle yapılan müdahaleler verilerin güvenirliğini, bütünlüğünü ve ulaşılabilirliğini korumaktadır. Kamu kurumları teknolojik gelişmeler sonucunda çeşitli politikalar geliştirerek yenilikler ve değişimler yaparak, teknik altyapılarını güçlendirerek gerekli tedbirleri almaktadır. Fakat kamuda çalışan personelin yanlışları, dikkatsizliği ve işini ciddiye almaması vb. gibi problemler nedeniyle bilgi güvenliği ihlal edilebilmektedir (Kınay, 2012, s. 12).

İnsan kaynaklı tehditler sosyal mühendislik ve oltalama olmak üzere iki farklı şekilde belirginleşen bir yapıya sahiptir. Bu tehlike türlerinin açıklanması konunun anlaşılması açısından önem arz etmektedir (Şahinaslan, 2013, s. 7).

- ***Sosyal Mühendislik:*** Çalışanların karşılıklı iletişim halinde bulunması veya kamu kurumlarındaki bilişim sistemlerinin takip edilmesi neticesinde gizlice bilgilerin toplanması durumuna sosyal mühendislik denilmektedir. Sosyal mühendislik, kamuda çalışan personelin sistemlerine aldatılma, zorlanma, kandırılma, ikna edilme veya yardım amaçlı olarak ulaşılmasıdır. Saldırganlar bahsedilen yöntemleri kullanarak kamu personelini aldatmaya veya onlar ile kurduğu etkileşim ile onları ikna etmeye çalışarak kurumsal bilgilerin çalınmasına neden olabilmektedirler (Elbahadır, 2016, s. 198-199).

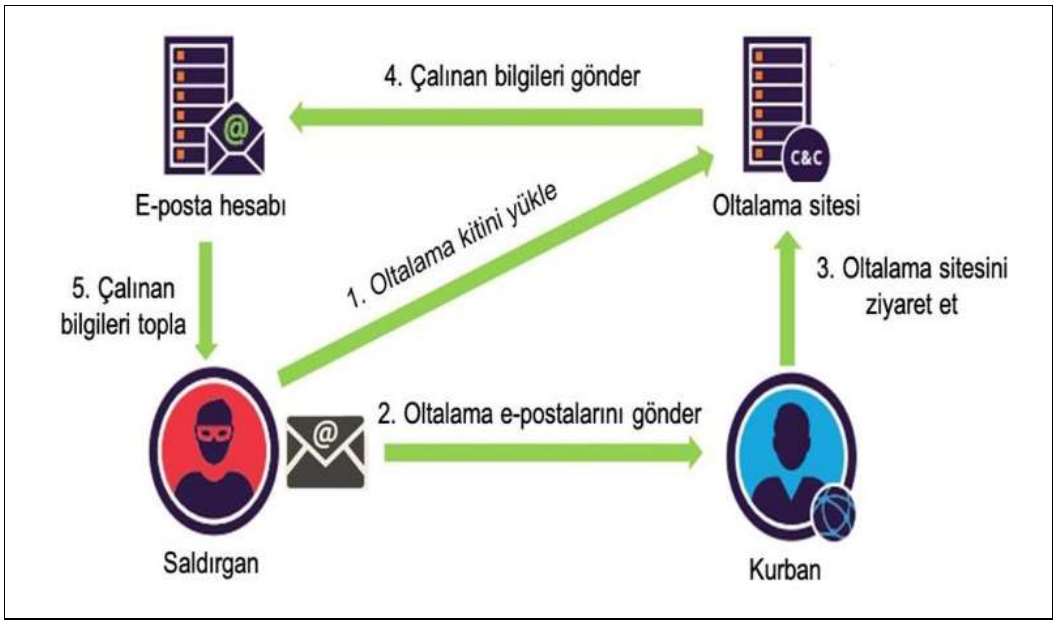
Son dönemde meydana gelen gelişmelerle beraber teknik olmayan ve durdurulması güç olan ataklar artmaktadır. Kamu kurumlarında sosyal mühendislik saldırıları, kişileri temel olarak aldatma sonucunda bilgi güvenliğini zarara uğratabilecek ve teknik prosedürlere göre bilgi sistemlerine daha çok zarar verebilecektir (Munro, 2005, s. 44). Saldırganların temel amaçları, veriler konusunda yetkili olan personelin ikna edilmesi ve aldatılması yöntemiyle teknik yöntemlerin kullanılmasıdır. Bilişim sistemlerindeki teknik tedbirler sosyal mühendislik saldırıları karşısında eksik kalmaktadır. Çünkü günümüzde teknolojinin en zayıf halkası insanlardır ve saldırganlar kamu kurumlarındaki bilgileri ele geçirmek için genellikle çalışanları hedef almaktadır.

Şekil 2. 3: Sosyal Mühendislik Yöntemi

Kaynak:(Yaşar ve Çakır, 2015, s. 496)

Kamu kurumlarında bilgi güvenliğine yönelik hızlı bir şekilde tedbir alınması gerekir. Ama teknolojinin devamlı olarak gelişmesi ve saldırganların sürekli tekniklerini değiştirmesi, oluşturulan tedbirleri etkisiz kılmaktadır. Dolayısıyla kamu kurumlarında çalışan personelin güvende olduğu düşünülmemelidir. Bilişim sistemlerinde meydana gelen gelişmeler sonucunda sistemlerin sürekli güncellenmesi gerekmektedir (Canberk ve Sağıroğlu, 2006, s. 172). Çünkü bilişim sistemleri ne kadar güvenilir de olsa çalışan personelin dikkatsizliği bilgi güvenliği sorunu ortaya çıkarabilecektir.

- ***Oltalama (Yemleme)****:* Elektronik sistem tarihinin en eski ve güçlü yöntemlerinden biridir. İnsan hatalarından veya eksiklerinden verilerin elde edilmesi ya da kullanıcı bilgilerinin çalınması en çok başvurulan tekniklerden biridir. Oltalama ya da yemleme yöntemi, çoğunlukla uyduruk ve düzmece ağlar oluşturarak yapılmaktadır (Hekim ve Başıbüyük, 2013, s. 135-157).



Şekil 2. 4: Oltalama Saldırı Yöntemi

Kaynak: (Bergnet, 2023)

Oldukça yaygın bir şekilde karşılaşılan oltalamaya kamu kurumlarında çalışan personelin ikna edilmesini ve aldatılmasını önlemek için seminer, konferans ve eğitim yoluyla bireylerde farkındalık oluşturularak gerekli tedbirlerin sağlanması gerekmektedir. Bunun yanı sıra oltalama yöntemi konusunda farkındalık oluşturmak amacıyla farklı bazı yöntemler de bulunmaktadır (Vural ve Sağıroğlu, 2008, s.1-16). Bu yöntemler şunlardır:

- Kamu çalışanlarının kişisel bilgilerinin (T.C. kredi kartı, parola, hizmet ile ilgi kurumsal bilgiler vb.) girildiği web sayfaları güvenilir olmalıdır.
- Personelin kişisel işlemlerinde kurum e-postası kullanılmamalıdır.
- Bireyler aldatıcı ve belirsiz e-postaları gerekli yerlere veya sorumlu kişilere haber verilmelidir. Kamu kurumlarının web adresleri "gov" şeklindedir. Kamu çalışanları web adresleri bunun dışında bir adres ise bunu hemen engellemeli ve gerekli yerlere bildirilmelidir (Yıldız, 2014, s. 38).
- Kamu çalışanları şüphe duyulan e-postaları açmamalı hatta okumadan silmelidir.

Meydana gelen teknolojik gelişmelerle beraber kamu kurumlarındaki teknik önlemlerin geri planda kalacağı tahmin edilmektedir. Çünkü bilgi güvenliği

farkındalığına ve eğitimine sahip olmayan kamu çalışanları önemli derecede güvenlik açığının ortaya çıkmasına sebep olabilmektedirler.

2.4.2. Zararlı Yazılımlardan Kaynaklanan Tehditler

Günümüzde bireyler bilgi, araştırma, haberleşme, oyun vb. gereksinimlerini yerine getirmek için teknolojik gelişmeler sonucunda artık yaşantımızın bir parçası haline gelmiş olan bilgisayar, telefonlar, tablet, akıllı televizyonlarla işlemlerini yapmaktadırlar. Gereksinimleri yerine getirme noktasında faydalı olan ve işlerin hızlanmasına sebep olan bu teknolojilerin eseri olan yazılımlar ve donanımların aynı zamanda kötü kullanımı da yaygınlaşmıştır (Çalışkan, 2013, s. 58).

Kötü yazılımlar, kötü kişiler tarafından bilişim sistemlerine girerek hasar oluşturmak, verileri almak, kişilere ve sistemlere zarar vermek, sistemlerin sürekliliğini bozmak amacıyla oluşturulan yazılımlardır (Canbek, 2005, s. 32). Dolayısıyla zararlı yazılımlar amaçlarına, kullanıcıların ve çalışan personelin farkında olmadan ulaşabildikleri gibi onları aldatarak da ulaşabilmektedir. Bu konuda çok farklı yollar ve yöntemler söz konusu olabilmektedir. Bu eylemlerden bazıları şunlardır:

- Kişinin dokunduğu tuşların kaydedilmesi,
- Kurumsal verilerin ve parolanın öğrenilmesi, verilerin başka kişilerle paylaşılması,
- Kurumsal veya kişisel dosyaların okunması, bozulması, yok edilmesi ve parola koyarak okunmaz duruma getirilmesi,
- Kurumsal bilgisayarın yazılım ve donanımlarının kullanılamaz hale getirilmesi,
- Kurumun bilişim sistemlerinde güvenlik açıkları oluşturulması (Uluyol ve Demirci, 2022).

Yukarıda saydığımız zararlı yazılımlar kurumların bilişim sistemlerine zarar vererek bilgileri ele geçirmektedir. Bu hususlar, kamu kurumlarında çalışan personelin eğitim ve farkındalık bilincine sahip olmamasından kaynaklanmaktadır. Bundan dolayı kamu kurumlarının bilgi güvenliğinin sağlanması için tedbirlerini oluşturmaları ve çalışanlarını da eğitim ile bilinçlendirmeleri gerekmektedir. Bilgi güvenliğinde doğru olarak bilinen ama yanlış olan bazı bilgi ve düşünceler bulunmaktadır:

- Kurum bilgisayarımda virüs programı var o zaman güvendeyim
- Kurumumuzda güvenlik duvarı ve teknik önlemler alınmış sıkıntı yok
- Kurum bilgisayarıma hafıza kartını ve flaş belleği yeni biçimlendirdim onun için sıkıntı yok
- Kurum zaten bizim için tüm teknik tedbirleri almış benim bir şey yapmama gerek yok

Yukarda görüldüğü gibi kamu çalışanlarının kendinden emin olması ve kendine aşırı güvenmesi, sistemlerde güvenlik açıkların oluşmasına sebep olmaktadır. Bu nedenle kurumların ve çalışan personelin ciddi maliyetlerin oluşmaması için bu konulara gerekli önemi göstermeleri ve çalışanlara farkındalık oluşturulması amacıyla eğitimlerin düzenlenmesi önem arz etmektedir (Canbek ve Sağıroğlu, 2007, s. 1-12). Kamu kurumların bilgi güvenliğine ait saldırıların başında, zararlı yazılım türleri bulunmaktadır. Bu zararlı yazılım türlerinden konunun daha iyi anlaşılması için kısaca bahsetmek faydalı olacaktır.

- **Bilgisayar Virüsleri:** Kamu çalışanlarının ve bireylerin haberi olmadan ağlara ve bilgisayarlara bulaşan, kendi kendine çoğalan, diğer dosyalara bulaşan, bilişim sistemlerinde hasara yol açan yazılımlardır (Yılmaz ve Salcan, 2008, s. 56-57). Kamu kurumları, özel sektör ve bireyler için virüsler çok ciddi bir problem haline gelmiştir.

Şekil 2. 5: Bilgisayar Virüsleri

Kaynak: (Media, 2023)

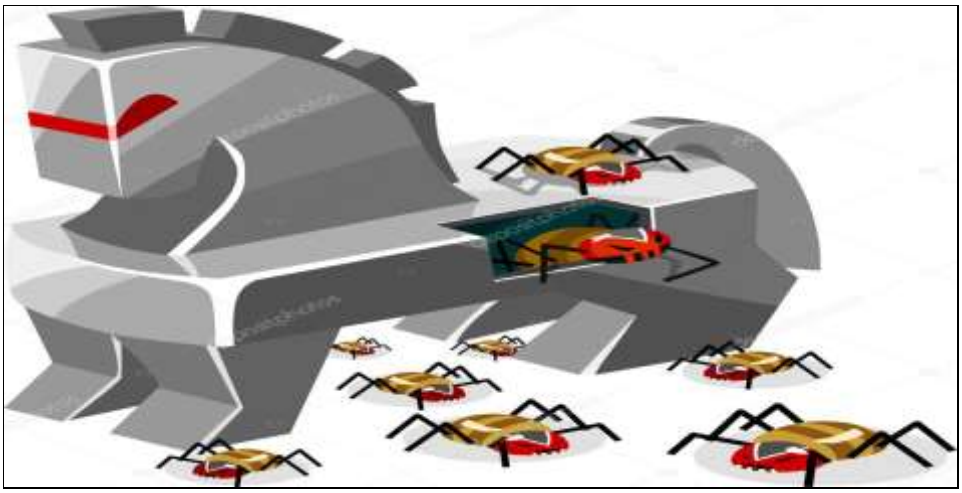
Virüsler daha çok e-posta, hard diskler, flash bellekler ve taşınabilir cihazlar sayesinde bulaşmaktadırlar. Aslında bu zararlı yazılımlar kişinin asıl amacına göre bilişim sistemlerine zarar vermektedir. Kamu kurumlarındaki bilgi güvenliğine yapılan saldırılar daha çok dosyaların çalınması, silinmesi ve kullanılmaz hale getirilmesi şeklinde olmaktadır (Gülmüş, 2010, s. 93).

- **Solucan (Worms):** Aynı virüsler gibi bilgisayar sistemlerinde kendi kendini çoğaltan ve dağıtan zararlı yazılımlardır. Solucanlar kişilerin herhangi bir etkisi olmadan kendi kendine çalışan, bilişim sistemleri arasında gezinen ve internet ağlarına bağlı bilgisayarlara bulaşan zararlı yazılımlardır (Ulaşanoğlu, Yılmaz ve Tekin, 2010). Dolayısıyla virüslere göre daha seri bir şekilde genişleyen solucanlar, virüslerden daha tehlikelidir.

Şekil 2. 6: Solucan

Kaynak: (Elbir, 2020)

- **Truva Atı (Trojan):** Bunlar kendini gizleyen, kendini normal bir program gibi gösteren daha sonra sistemlere girerek zararlı hareketlerde bulunan yazılımlardır. Truva atları kendilerini zararsız veya değişik türde gösteren, yetkili kişilere faydalıymış veya sorunlarını çözüyormuş gibi görünen ama izinsiz erişimi basitleştiren zararlı kodlara sahip zararlı yazılımlardır. Truva atları bilgisayar sistemlerini bozabilmekte, kişilere özgü parolalara ulaşabilmektedir. Kendisi sisteme yapışarak ve güvenlik açıklarını bularak saldırganların amaçlarına hizmet etmektedir (Turhan, 2010, s. 41).



Şekil 2. 7: Truva Atı

Kaynak: (Dikmen, 2023)

Truva atının bilişim sistemlerine yayılması, ağ veya internet sayesinde olmaktadır. Bilgi güvenliğine yönelik bu zararlı yazılımlar daha çok e-posta, eğlence, ücretsiz programlar ve oyunlar yoluyla buluşmaktadır (Taş, 2010, s. 11).

- **Klavye İşlemlerini Kaydeden Yazılımlar (Key Logger):** Klavyedeki tuş fillerini izleyerek verileri saldırganlara iletmek üzere saklayan zararlı yazılımlardır (Taş, 2010, s. 12). Klavye izleme yazılımlarının amacı, yetkili kişilerin klavye kullanmaları sonucunda tüm kişisel verileri kaparak saldırganlara ulaşmasını sağlamaktır. Bu durumun önüne geçmek maksadıyla, kamu kurumlarında çalışanların ve bireylerin bilgi güvenliğini oluşturmak için bazı tedbirleri almaları gerekmektedir.

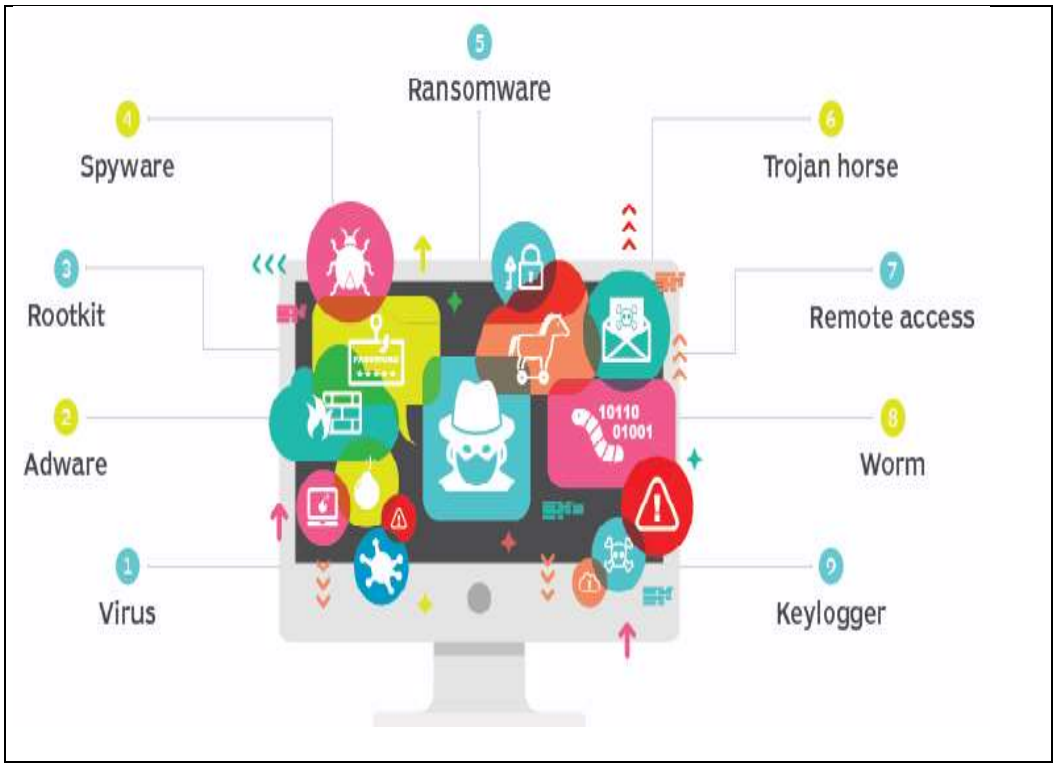
  Kamu kurumlarında çalışan personelin uygulaması gereken tedbirler, sanal klavye kullanılması, dijital imza kullanılması ve belirli aralıklarla şifrelerin değiştirilmesi şeklindedir. Ama meydana gelen teknolojik gelişmeler, zamanla bu tür tedbirleri de etkisiz bırakabilmektedir. Çünkü geliştirilen zararlı yazılımlar, bilgisayarda yapılan her şeyi kaydedilebilmektedir. Bundan dolayı klavye dinleme ve önleme programlarının kullanılması gerekli olmaktadır. (Canbek ve Sağıroğlu, 2007, s. 126).

- **Casus/Köstebek Yazılımlar (Spyware):** Yetkili kişilere ait verileri, gerçekleştirmiş olduğu işlemleri, kullanıcının izni olmadan saldırganlara gönderen yazılımlardır (Canbek, 2005, s. 39). Bu yazılımlar, kişilerin bilgisayarına haberi olmadan yüklenmekte, kişinin dolaşmış internet sayfalarına ait verileri toplayıp saldırganlara göndermektedirler. Casus yazılımlar kullanıcıların haberi olmadan ve izinsiz şekilde sistemlere yüklendiği için bilgi güvenliğine yönelik en ciddi tehditlerden bir tanesidir.

  Bilgisayarda saklanan bu casus yazılımların temel prensipleri, kişilerden daha fazla veri toplamaktır. Bu tür zararlı yazılımlar, daha çok özel şirketler tarafından kullanılmaktadır. Çünkü bu yazılımlar firmalar tarafından kullanıcıların internet üzerinde gezdikleri sayfaları, alışkanlıkları ve tutkuları belirlemekte ve bunun neticesinde kişilere özel reklamlar oluşturulmaktadır (Canbek ve Sağıroğlu, 2007, s. 125-126). Bilgi güvenliğinin sağlanması için bu casus yazılımlara yönelik anti-virüs yazılımların kullanılması eksik kalmakta ve bunların muhafaza edilmesi için

kişilerin eğitim ile bilinçlendirilmeleri ve anti spware yazılımların sistemlere yüklenmesi gerekmektedir (Taş, 2010, s. 14).

- **Hizmet Aksatma (DOS):** Kurumlarda kullanılan programları işlevsiz hale getiren saldırılardır. Bunların amaçları hizmet sağlayıcıların devre dışı bırakılmasıdır. Hizmet aksama saldırıları, saldırganların herhangi bir internet sayfasına veya web sitesine birden fazla saldırı göndermeleri ve sitenin fonksiyonlarının güçsüz ve dirençsiz kalması veya sitenin kullanılmaz duruma gelmesini amaç edinmektedir (Krause ve Tipton, 2007).
- **Mantık Bombaları:** Bilişim sistemlerine bulaşan ancak eyleme başlaması için planlanan tarih ve saati veya kişilerin sistemlerine girmelerini bekleyen türdeki yazılımlardır. Bu yazılımlar, saldırganlar tarafından emir verilene kadar sistem içinde gizlenen ve yeri geldiğinde hareket ederek kalıcı zararlar veren yazılımlardır (Taş, 2010, s. 12).
- **Arka kapı (Back Door):** Güvenlik açıklarından faydalanarak hazırlanan yazılımlardır. Bilişim sistemlerinde yapılan çalışmalar sonucunda kaldırılan parolalar güvenlik açıkları oluşturabilmektedir. Bu durumda bu güvenlik açıklarını gören kişiler ve zararlı yazılımlar sistemlere girerek zararlara yol açmaktadır. Bilgi güvenliğinde arka kapılar kendilerini saklayarak ve muhafaza ederek sisteme ulaşım ve erişim oluşturan yazılımlardır. Arka kapı, bilişim sistemlerine sızmak için yapılan gizli ve saklı bir ulaşım noktasıdır. Kamu kurumlarında uygun geliştirmelerin ve güncellemelerin yapılması ve gizli bağlantı yollarının arındırılması gerekmektedir (Gülmüş, 2010, s. 95).



Şekil 2. 8: Zararlı Yazılımlar

Kaynak: (Trojan Virüs Tehdidi(Tectharget), 2023)

- **Reklam Yazılımı (Adware):** Kamu çalışanları ve bireylerin onayları olmadan bilgisayarlara, ağlara ve cihazlara bulaşan ve sistemin gerisinde çalışan kötü niyetli yazılımlardır. Reklam yazılımının amacı; reklamları göstermek, ağlarda arama bilgilerini bularak ticari şirketlere ve reklam sitelerine göndermektir (Krause ve Tipton, 2007). Kişilere, gezdikleri sitelere göre reklam bilgileri gösterilmekte veya kişiler amaçları dışında başka web sitelerine yönlendirilmektedirler (Timus(Bergnet), 2020).

- **Rootkit:** Bilişim sistemlerine sızarak yazılan ve saldırganlar tarafından devamlı olarak kullanılan yazılımlardır. Kurumsal bilgisayarlar ve kişisel verilere izinsiz olarak ulaşan saldırganlar bilgileri çalabilmekte, silebilmekte sistemlerin doğru çalışmasını engelleyebilmekte, istenmeyen elektronik e-postalar için zemin oluşturabilmektedirler (Timus(Bergnet), 2023).

- **Fidye Yazılımı (Ransomware):** Kullanıcıların hassas bilgilerinin ve dosyalarının rehin alınması ve bunlara parola konularak bu parolanın çözülmesi için fidye istenmesidir. Bu nedenle sistemlerin parolası ancak bir fidye verildiği zaman

saldırganlar tarafından açılabilmektedir. Ödemenin yapıldıktan sonra bile şifre kilidini açılacağının bir garantisi bulunmamaktadır. Bu sebeple bilgilerin ve dosyaların yedeklenmesi bu gibi kötü amaçlı yazılımlardan kurtulma konusunda önem arz etmektedir (Uzman Posta , 18 Mayıs 2023)

- **Remote Access Trojan:** Kurumların ve kişilerin kullandığı aygıtların arka planda, kullanıcının haberi olmadan gizlice çalışmasını ve aygıtların içerisindeki verilerin ve dosyaların farklı şahıslara kanunsuz bir biçimde aktarılmasını ya da aygıtın kanunsuz fonksiyonlarında kullanılmasını sağlayan kötü yazılımlardır. (Dikmen, 2023)

2.5. Bilgi Güvenliğinde Yaşanan Ortak Sorunlar

Günümüzde meydana gelen teknolojik gelişmelerle ile beraber hem dünyada hem de ülkemizde birçok alanda bilgi güvenliği ile ilgili düzenlemeler yapılmıştır. Elektronik ve haberleşme alanında kademeli olarak analizler, metotlar, kanunlar, kararnameler, yönetmelikler, genelgeler, kurul kararları gibi düzenlemeler yapılmıştır (Tipton & Krause, 2007); (T.S.E., 2006); (ISO, 2005).

Bilgi güvenliğinin temel problemleri, bu mevzuya yönelik halkın veya şahısların ilgi, idrak ve olaya bakış açısındaki hatalar ve eksikliklerdir. Bu nedenle ilk etapta, devletlerin, kurumların, şirketlerin ve kullanıcıların algı ve görüşlerinin değişmesi gerekir. Kamu kurumlarındaki amirlere, sosyal medyaya, yasaları oluşturan yetkililere ciddi sorumluluklar düşmektedir. Bilgi güvenliğinin teknik önlemlerden önce insanları eğitim, konferans, seminer gibi yollarla bilinçli duruma getirmesi ve kamu kurumlarındaki üst düzey yöneticilerden başlayarak en alt kademedeki kamu çalışanlarına kadar bilgi güvenliğinin anlatılması, öğretilmesi, bilinçlendirilmesi, desteklenmesi ve yaşamın bir parçası haline getirilmesi amaçlanmaktadır. Çünkü bilgi güvenliğinin devamlı ve gelişen bir teknoloji olduğu hususunun gözden kaçırılmaması gerekmektedir (Eminağaoğlu, 2008).

Teknolojik gelişmeler sonucunda verinin çalınması için teknoloji ajanlarının, istihbarat elemanlarının veya yetenekli siber saldırganların çok masraflı teknolojiler kullanmalarına günümüzde pek fazla ihtiyaç bulunmamaktadır. Çünkü meydana gelen teknolojik gelişmelerle beraber artık basit ve ucuz bir şekilde veri hırsızlığı yapabilen zararlı yazılımlar ve aygıtlar bulunmaktadır. Ayrıca kamu kurumlarının dışarısındaki

tehditlerden ziyade kurumların çalışanları ve kullanıcıları tarafındaki bilişim sistemleri ve çalışanları kullanılarak tehditler oluşturulmaktadır. Dolayısıyla kurumların problem ve tutarsızlıklarından bir tanesi de kurumların gizli bilgilerini içeren USB, DVD, CD, tablet, telefon vb. gibi çeşitli cihazların zayi olması, çalınması teşkil etmektedir. Kurumlarda çalışanlar, bu cihazları bulundurma yetkisine sahip olmalarına rağmen, bilinçsiz kullanımı ve tehlikeler konusunda yeterince bilgilendirilmemeleri, sorunların ortaya çıkmasına neden olabilmektedir (Eminağaoğlu, 2008).

Kamu kurumlarında genellikle amirlerin bilgi güvenliğini desteklemesi gerekmektedir. Yöneticilerin üst kademedeki amirlerine yaranmak için daha çok ivedi, hızlandırılmış programlara, günübirlik sorunları çözmeye ve sadece teknik sorunlara yoğunlaşarak insan unsurunu ihmal ettikleri görülmektedir. Dolayısıyla bilgi güvenliği ile ilgili tehlikeler ve sorunlar karşısında teknik yöntemler çare olmamaktadır. Kamu kurumlarının bilgi güvenliği konusundaki tüm süreçlerinde çalışanların teknik önlemlerle beraber hareket etmesi gerekmektedir (T.S.E., 2006); (ISO, 2005). Kamu kurumlarında yöneticilerin bilgi güvenliği ile ilgili sorunları teknik çalışanlarca halledilmesi gereken teknik ve düşük maliyetli bir iş olarak görmesi ile problemler ve tehlikeler eksilmemekte ve dolayısıyla her geçen gün daha çok artmaktadır (Mitnick, 2005).

Teknoloji ile ilgili sorunların ve tehlikelerin giderilmesi için kurumların kendine ait iş oluşturma biçimlerine ve yapısına uygun bilişim sistemlerini ve teknoloji alternatiflerini oluşturmaları gerekmektedir. Bu teknolojilerin kurum ile tutarlı olacak biçimde devamlı düzenlenmesi, denetlenmesi ve yenilikleri takip ederek uygulanması büyük bir avantaj sağlayacaktır. Kamu kurumlarında yapılan başka bir yanlış ise, bilgi güvenliği ile ilgili güvenlik politikalarının yasalara ve mevzuata dikkat edilmeden, yazılı olmaksızın telefon veya e-posta yoluyla çalışanlara haber verilmesidir. Bundan dolayı politikalar ciddiye alınmamaktadır. Bunun için güvenlik politikalarının doğru bir şekilde uygulanması, önemsenmesi ve desteklenmesi gerekmektedir. Kamu kurumlarınca güvenlik politikalarının desteklenmesi halinde uygulanması basit ve daha çözümleyici teknikler uygulanmalıdır (Gülmüş, 2010, s. 126).

Kurumlar ve bireyler için kıymetli olan bilgi veya verilerin gizliliği, bütünlüğü ve erişilebilirliği tesis edilerek sürekli bir biçimde korunması için bazı fiziksel ve teknik tedbirlerin sağlanması gerekir. Bu durum öngörülen tedbirlerin kişilerin bilgi

güvenliğine yönelik tehlikelere ve saldırılara karşı nasıl davranılacağının kullanıcılar tarafından öğrenilmesi ve bilinmesi ile mümkün olabilecektir (Şahinaslan, Kandemir ve Şahinaslan, 2009, s. 1).

Gelecek yıllarda kamu kurumlarında bilgi güvenliği kültüründen yoksun olan kişilerin dolandırılması, aldatılması ve ikna edilmesi yollarıyla güvenlik açıklarının artacağı söylenmektedir. Bu nedenle güvenlik açıklarının oluşmaması için sistemlerin engellenmesi, çalışanların eğitilmesi, bilinçlendirilmesi ve bunların plan dâhilinde yapılması gerekmektedir (Vural, 2007, s. 6).

2.6. Bilgi Güvenliğine Yönelik Alınması Gereken Önlemler

Günümüzde tehditlere karşı önlem almak, şahsi bilgilerimizin korunması ve kurumun işlerinin sürekli bir biçimde devam etmesi için önemli bir durum olmuştur. Artık evlerimizde, kurumlarımızda, üniversitelerimizde, kafelerde hayatımızın her noktasında yer alan yazılımları ve web siteleri kullanmak zorunda kalınmaktadır (Alemdaroğlu, 2020). Aslında kullandığımız bu programlar faydalı olduğu kadar bazen tehlikeler ve tehditler nedeniyle riskler de barındırmaktadır. Bilgi güvenliği kavramı kurumları ve kişileri, gelebilecek tehlikeler ve saldırılara karşı çözüm aşamaları geliştiren, kurumlarda güvenlik duvarlarını kuran ve açıkları kapatmaya çalışan araç niteliği taşımaktadır (Yavanoğlu, Sağıroğlu ve Çolak, 2012, s.15-27).

Bilgi güvenliği kıymetli ve vazgeçilmez olan verilere izinsiz ve yetkili olmayan kişiler tarafından ulaşılması, yararlanması, işletilmesi, yayılması, yok edilmesi ve zarar verilmesini önlemek biçiminde de tanımlanmaktadır. Bu nedenle saldırıların etkilerini minimum düzeye indirmek için, kişisel bilgilerin ve kurumsal verilerin düzenli bir şekilde korunması ve olası zararların en aza indirgenmesi için tedbirler alınması gerekmektedir. Kurumlar ve bireyler gerekli tedbirleri almadıkları için büyük hasar ve kayıplar yaşayabilmektedirler. Bu nedenler kurumların ve bireylerin olası tehditlere karşı tedbir almak kadar işi önemsemeleri ve bilinçli olmaları önemli ve gereklidir (Karakoç, 2011, s. 419-423).

Önümüzdeki yıllarda teknolojik gelişmelerle beraber hayatımızın her alanında yer alması ve kurumsal işlerin sağlıklı bir biçimde devam etmesi için teknolojinin olumlu yanlarından yararlanmak ancak olumsuz taraflarına karşı gerekli tedbirleri almakla mümkündür. Hem kişisel hem de kurumsal tedbirlerin merkezinde insan

bulunmaktadır. Aslında bu tedbirlerin ortak noktası insan faktörüdür. Teknik tedbirlerin alınması ile bilgi güvenliğin oluşturulması oldukça güçtür. Bu nedenle bilgi güvenliğinde insanın tüm aşamalara dâhil edilmesi ve gerekli eğitimlerin verilmesi ile güvenliğin oluşturulması gerekmektedir. Fakat bilgi güvenliğinde %100 güvenlik mümkün değildir. Alınan tedbirler tehlikeleri minimuma getirmektedir. Yani aslında tehditleri kabul edilebilir aşamaya getirmeye çalışmaktadır (Çetinkaya, Güldüren ve Keser, 2017, s. 33-52).

Bilgi güvenliği sistem ve birey düzeyinde alınacak bazı tedbirler ile sağlanabilir. Dolayısıyla kamu kurumlarında bilgi güvenliğinin sağlanması için hem kişisel hem de kurumsal bazı önlemlerin alınması gerekmektedir.

2.6.1. Kişisel Önlemler

Kişisel veriler, bireylerle ilgili olan ve belirli bir kişinin tanımlanmasına ya da tanımlanabilir hale getirilmesine olanak sağlayan her türlü bilgiyi ifade eder. Kişisel bilgiler yalnız ad ve soyadı, telefon numarası, e-posta adresi, sosyal medya profilleri ve yeri gibi bilgileri değil, aynı zamanda fiziksel, sosyal, iktisadi, psikolojik tüm verileri kapsamaktadır. Teknolojik gelişmeler kişisel verilerin paylaşılmasını kolaylaştırdığı ölçüde kişisel bilgilerin internet ortamında korunması da güç duruma gelmiştir. Kişisel bilgiler kişiler tarafından teknolojinin getirmiş olduğu kolaylıklar sayesinde paylaşılmaktadır. Bireyler sosyal medya platformlarında kendilerini tanıtan, fotoğraf, video ve görsel araçları kullanarak kişisel bilgilerini paylaşmaktadır (Alemdaroğlu, 2020, s.26-27).

Kişisel bilgilerin korunması ile ilgili dünyada ve Türkiye'de çeşitli kanunlar, sözleşmeler olmasına rağmen kişisel güvenlik ve gizlilik bireyde başlamaktadır. Bu tehlikeleri minimum seviyeye indirmek için çeşitli konferans, seminer ve eğitimler verilerek kişilerde farkındalık oluşturmalıdır (Taner, 2019, s. 26). Günümüzde teknoloji artık her ortama girmiştir. Bu nedenle teknolojik gelişmeleri takip ederek haberdar olmak ve gelişmelere ilgisiz kalmamak da farkındalığın oluşmasına katkı sağlamaktadır. Bilgi güvenliğine dair kurallar, bireysel kullanıcılar için önemli ve dikkat edilmesi gereken kurallardır. Kişisel bilgi güvenliği için alınması gereken bazı önlemlere aşağıda yer verilmektedir (Taner, 2019, s. 26).

- **Güçlü Parola Kullanımı:** Hesapların korunması için güçlü parolalar kullanılmalı ve bu parolalar karmaşık olmalıdır. Büyük ve küçük harfler, sınırlar ve semboller içermelidir. Ayrıca, her hesap için farklı parola kullanılması gerekli ve önemlidir.
- **İki Faktörlü Kimlik Doğrulama:** Çevrimiçi hesaplarında iki faktörlü kimlik doğrulaması etkinleştirilmelidir. Parolanın yanı sıra bir doğrulama kodu veya SMS ile sonuca erişim sağlanması önemlidir.
- **Yazılım Güncellemelerini İzlemek:** İşletim sistemi, uygulamalar ve anti-virüs programları gibi yazılımların güncel tutulması gereklidir. Güncellemeler, yeni güvenlik yamalarını ve önlemlerini içermektedir.
- **Zararlı Yazılımlara Karşı Korunma:** Bilgilerin korunması hususunda anti-virüs programının yüklenmesi ve düzenli taramalar yapılması önemlidir. Kullanıcıların kaynağı bilinmeyen bilgilerden gelen e-posta eklerini veya indirme bağlantılarını açmamaya dikkat etmeleri gerekmektedir.
- **Güvenilir WİFİ Ağları Kullanımı:** Kamu WiFi ağlarında veri paylaşılmasından kaçınılması ve özellikle finansal işlemler gibi hassas bilgileri aktarırken güvenilir bir WİFİ ağının kullanması veya mobil veri bağlantının tercih edilmesi gerekmektedir.
- **E-posta ve Mesajlara Dikkat Edilmesi:** Bireylerin kaynağı bilinmeyen veya şüpheli e-postaları veya mesajları açmamaları veya içinde yer alan bağlantıları tıklamamaları gerekmektedir. Ek dosyaları veya bağlantıları tıklamadan önce gönderenin kim olduğunun öğrenilmeye çalışılması gerekmektedir.
- **Bilgiler Paylaşılırken Dikkatli Olunması**: Kişisel veya mali bilgileri paylaşırken dikkatli olunması gerekmektedir. Kişinin yalnızca güvenilir web sitelerini ve interneti kullanması ve hassas bilgi edinmek isteyenlere dikkat ederek gerekli önlemleri alması gereklidir.
- **Bilgi/Veri Yedeklemesi:** Kullanıcıların değerli ve önemli bilgileri ile dosyalarını düzenli olarak yedeklemeleri gereklidir. Böylece kişiler veri kaybı durumunda verilerini ve dosyalarını kurtarılabileceklerdir.

- **Sosyal Medya Ayarlarının Kontrol Edilmesi**: Kişilerin sosyal medya hesaplarının gizliliğini muhafaza etmeleri ve gizlilik ayarlarını düzenli olarak kontrol etmeleri gerekmektedir. Kişilerin yaptıkları bazı özel paylaşımları ailesi, arkadaşları ve tanıdığı kişilerle sınırlandırmaları tehditlerin oranını azaltacaktır.
- **Fiziksel Güvenlik:** Kişiler cihazlarını fiziksel olarak da korumalıdır. Kişinin cihazlarında şifreli ekran kilidi kullanmaları ve cihazlarını güvendiği yerlerde tutmaları gereklidir.

Yukarıda sayılan hususlar, bilgi güvenliğinin sağlanmasına yardımcı olacaktır. Ancak unutulmamalıdır ki, kişilerin güvenlik konusunda her zaman dikkatli olmaları ve teknolojiyle ilgili güncel bilgilere sahip olmaları gerekmektedir (Canbek ve Sağıroğlu, 2006, s. 172).

2.6.2. Kurumsal Önlemler

Kamu kurumlarının bilişim sistemleri konusunda güvenli bir altyapı oluşturmaları ve tüm saldırılara hazırlıklı hale gelmeleri gerekmektedir. Kamu kurumlarının sadece teknik olarak korunması yeterli olmayıp, personelin teknolojik yenilikleri takip etmeleri ve güvenliği önemseyen, destekleyen bir farkındalığın oluşturulması gerekmektedir (Glasshouse, 2020).

Bilgi güvenliği konusunda kurumsal önlemler, bir organizasyonun bilgi varlıklarını koruması ve güvenliğini sağlaması için alması gereken adımları içermektedir. Kamu kurumlarında güvenli bir teknik altyapı oluşturmak isteniyorsa, bilgi güvenliğinin varlıkları olan gizlilik, bütünlük, erişilebilirlik unsurlarına dikkat edilmesi gerekmektedir. Bilgi güvenliğiyle ilgili alınması gereken kurumsal önlemlerden bazılarına aşağıda yer verilmektedir (Özkaya, Sarıca ve Durmaz, 2019, s. 305).

- **Bilgi Güvenliği Politikası**: Kurumun, bilgi güvenliği politikasını belirlemesi ve bu politikanın tüm çalışanlar tarafından anlaşılır ve uygulanabilir olması önemlidir. Bu politika, kurumsal bilgi varlıklarının korunması, yetkisiz erişimin engellenmesi, güvenlik önlemlerinin kullanılması ve bilgi güvenliğiyle ilgili sorumlulukların tanımlanmasını içermelidir.

- **Risk Değerlendirmesi:** Bir risk değerlendirmesi yapılmalı ve organizasyonun bilgi güvenliği tehditlerinin ve risklerinin belirlenmesi sağlanmalıdır. Bu değerlendirme, potansiyel tehditlerin, zayıf noktaların ve güvenlik açıklarının tanımlanmasını sağlar. Riskler belirlendikten sonra, uygun önlemler alınarak risklerin azaltılması veya ortadan kaldırılması sağlanmalıdır.
- **Bilgi Sınıflandırması:** Bilgi önemine göre sınıflandırılmalıdır. Bu sınıflandırma, bilginin hassasiyet düzeyini belirleyerek, uygun güvenlik kontrollerinin uygulanmasını sağlar. Örneğin, kamuoyuyla paylaşılan bilgiler, ticari sırlar veya müşteri verileri farklı sınıflara ayrılabilir.
- **Erişim Kontrolleri:** Bilgiye erişim, sadece yetkilendirilmiş kullanıcılar tarafından sağlanmalıdır. Erişim kontrolleri, kimlik doğrulama mekanizmaları, parola politikaları, çok faktörlü kimlik doğrulama, rol tabanlı erişim kontrolü ve fiziksel güvenlik önlemleri gibi yöntemler ile sağlanmalıdır. Bu şekilde, bilgilere izinsiz erişimin önlenmesi ve sadece yetkilendirilmiş kişilere erişim sağlanması ile önlemler alınabilir.
- **Güvenlik Eğitimi ve Farkındalığı:** Tüm kamu çalışanları, bilgi güvenliği konularında eğitilmeli, bilinçlendirilmeli ve farkındalık düzeyleri artırılmalıdır. Bu eğitimler, güçlü şifre kullanımı, yemleme (oltalama) saldırılarını tanıma, güvenli internet kullanımı, verilerin doğru saklanması ve paylaşılması gibi konuları kapsamalıdır.
- **Güvenlik Yazılımları ve Cihazları**: Güvenlik yazılımları ve cihazları, organizasyonun bilgi varlıklarını korumasında önemli bir rol oynamaktadır. Anti-virüs programları, güvenlik duvarları, zararlı yazılım tarama araçları ve veri şifreleme gibi güvenlik yazılımları ve cihazları kullanılmalıdır.
- **Olay İzleme ve Müdahale:** Kamu kurumlarında, olayları izlemek ve potansiyel güvenlik ihlallerine hızlı bir şekilde müdahale etmek için güvenlik olaylarına yanıt verme süreçleri oluşturulmalıdır. Bu, potansiyel saldırıları veya güvenlik ihlallerini tespit ederek, gerektiğinde müdahale etmeyi ve hasarı en aza indirmeyi sağlamalıdır.
- **Sürekli İyileştirme:** Kamu kurumlarında bilgi güvenliği politikaları, önlemler ve kontroller sürekli olarak gözden geçirilmeli ve iyileştirilmelidir. Dolayısıyla

teknoloji, tehditler ve iş gereksinimleri değiştikçe, güvenlik önlemleri de güncellenmelidir.

Bu önlemler, kamu kurumlarının bilişim sistemlerini ve bilgi güvenliği yönetimini güçlendirmeyi ve bilgi varlıklarının korunmasını amaçlamaktadır. Ancak bu önlemler, yalnızca temel adımlar olup organizasyonun ihtiyaçlarına ve sektöre göre daha spesifik önlemlerin alınması gerekmektedir (Alemdaroğlu, 2020, s.23-25).

2.7. Bilgi Güvenliği Farkındalığı

Farkındalık sözcüğü Türk Dil Kurumu (TDK) sözlüğünde "Farkında olma durumu veya bir şeyin bilincinde olma" olarak ifade edilmektedir. Farkında olmak ise "görülmesi veya bilinmesi gereken şeylerden haberi bulunmak, kavranması gereken bir şeye dikkat etmek" şeklinde tanımlanmaktadır (TDK, 2019). Başka bir tanımda ise, bir varlığın etrafında meydana gelen veya gelişen olayların bilmesi, kavraması ve işitme kabiliyetidir. Bilgi güvenliği farkındalığı, bir kamu kurumunun veya bireyin bilgi güvenliği konularında bilgi sahibi olması ve bu konuda eğitimli, dikkatli, özenli ve bilinçli davranması anlamına gelir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009, s.567-602).

Bilgi güvenliği, bilgi ve verilerin yetkisiz erişime, manipülasyona, silinmesine, değiştirilmesine, ifşasına veya yok olmasına karşı korunmasıdır. Bilgi güvenliği farkındalığı ise bir tehlikenin, risklerin veya güvenlik önlemlerinin bilincinde olma durumudur. Bilgi güvenliği farkındalığı, bir kamu kurumunun veya bireyin bilgi güvenliği politikalarına uyması ve güvenlik risklerini tanıması için önemlidir (Şahinaslan, Kandemir ve Şahinaslan, 2009, s. 189-194). Bilgi güvenliği konularında farkındalık sahibi olan kişiler siber saldırılar, veri sızıntıları veya dolandırıcılık gibi tehditlerle karşılaştıklarında daha iyi bir şekilde tepki verebilir ve riskleri azaltabilirler.

Kamu kurumlarında bilgi güvenliği farkındalığının temel amacı; bilgi ve bilgi varlıklarının muhafaza edilmesi için çalışanların sorumluluklarının bilicinde olmasını sağlamaktır. Çünkü kamu kurumları için bilgi güvenliği hayati öneme sahiptir. Bilişim sistemlerinde bilgi güvenliği teknik yöntemlerle sağlanması bulunmakla beraber en önemli görev insan üzerine düşer (Kjorvik, 2010, s. 5). Ancak kamu kurumlarında bilgi güvenliği farkındalığının oluşturulması için kamu politikalarının amacına uygun

ve hatasız bir şekilde uygulanması gerekir. Kamu kurumlarında bilgi güvenliği bilincinin oluşturulması ve başarılı bir şekilde yerine getirilmesi için kurum amirlerine büyük sorumluluklar düşmektedir. Kurumlarda bilgi güvenliği ile ilgili verilecek seminer, konferans ve uzman kişiler tarafından verilecek eğitimleri destekleme ve finansal destek sağlamak gibi faaliyetlerin kurum yöneticisi tarafından yerine getirilmesi ve denetlenmesi gerekmektedir (Wright & Kakalık, 2007, s.187).

Bilgi güvenliğinin yalnızca yazılım, donanım ve teknik yöntemlerle mümkün olmadığının bilinmesi gerekir. Günümüzde bilişim sistemlerini hiç kullanmayan herhangi bir devlet kurumu olmayacağına göre bütün kamu çalışanları için zorunlu bir unsur haline gelmektedir. Bunun için kamu kurumlarının kendilerine ait tehlikeleri ve maliyetleri önem derecelerine göre planlanması ve gerekli çalışmaların yapılması gerekmektedir (Özdemir ve Uluyol, 2020,s. 649-666). Kamu kurumlarında bilgi güvenliğinde önemli faktör gönüllü, arzulu, farkında olan ve bilgili çalışanlardır. Bilgi güvenliği kamu çalışanları tarafından kurum kültürü haline gelmesi gerekmektedir. Saldırganlar tarafından yapılacak olan saldırılardan daha tehlikeli olan kamu kurumlarında çalışan personelin, dikkatsiz, bilinçsiz ve kurum kültürünü önemsemeyenlerin olduğu unutulmamalıdır. Bilgi güvenliği farkındalığını artırmak için aşağıdaki önlemler alınabilecektir (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009, s. 597-602):

- Kurumlarda bilgi güvenliği konularında seminer, konferans ve eğitimler düzenlemek ve kamu çalışanları ile kullanıcıları bu yolla bilgilendirmek.
- Kamu kurumları bilgi güvenliği ile ilgili politika ve prosedürlerini belirlemesi ve bunları çalışanlara aktarması gerekmektedir.
- Kamu kurumlarında bilişim sistemlerinde güvenlik yazılımları, bilgisayar sistemlerini, ağları ve verileri korumak için kullanılmalıdır. Anti-virüs programları, güvenlik duvarları ve zararlı yazılım tarama araçları gibi yazılımların kullanılması.
- Kamu kurumlarında güçlü şifreler kullanmak, hesapların ve sistemlere erişimin güvende olmasını sağlar. Şifrelerin karmaşık, uzun ve tahmin edilemez olması önemlidir. Ayrıca, düzenli olarak şifreler değiştirilmelidir.

- Kurumlarda önemli verilerin düzenli olarak yedeklenmesi, veri kaybı durumunda geri alınabilmesini sağlar. Veri yedeklemeleri, güvenli bir şekilde saklanmalı ve düzenli olarak geri dönüş testleri yapılmalıdır.

Bilgi güvenliği farkındalığı, sadece kamu kurumlarının değil, her bireyin sorumluluğundadır. Herkes, günlük hayatta bilgi güvenliği konularında bilinçli olmalı, güvenlik politikalarının benimsenmesi, önemsenmesi, kurum olarak geliştirilmesi ve gerekli önlemlerin alınmasıdır.

2.8. Bilgi Güvenliği ile İlgili Yapılan Araştırmalar

Ünver, Canbay ve Mirzaoğlu (2009), yapmış oldukları "Kritik Altyapıların Korunması" isimli çalışmada, bilgi güvenliği yetersizliğinden bahsetmiştir. Hemen hemen bütün işlemlerin elektronik ortamda kimlik bilgileri ile yapılması ve kişisel verilere ulaşılması nedeniyle oluşabilecek risk ve tehlikelerden bahsetmişlerdir. Bu doğrultuda yapılan çalışmada kritik altyapıların korunması hususunda kamusal hizmetlerin güvenliğinin sağlanması gerektiğini ifade etmişlerdir.

Vroom ve von Solms (2004, s.222-240), yapmış oldukları "Bilgi Güvenliği Davranış Uyumuna Doğru" isimli çalışmada, bilgi güvenliği farkındalığının sağlanması üzerinde durmuşlardır. İlgili çalışmada bilgi güvenliğinin sağlanması için kurumsal politikaların oluşturulması, kurum çalışanlarının bilgilendirilmesi ve kurum kültürünün geliştirilmesi gibi faktörlerin etkili olduğu sonucuna varılmıştır.

Tekerek ve Tekerek (2013, s. 61-70), yapmış oldukları "Öğrencilerin Bilgi Güvenliği Farkındalıkları Üzerine Bir Araştırma" isimli çalışmada, Kahramanmaraş ilindeki ilkokul ve ortaokul öğrencilerinin bilgi güvenliği farkındalık düzeylerini belirlemek için ölçek uygulamışlardır. Araştırma sonucuna göre öğrencilerin ahlaki konularda yeterli düzeyde bilinçli ve bilgi sahibi oldukları fakat bilişim konularında farkındalıklarının yetersiz olduğu saptanmıştır. Bunun nedeni olarak, öğrencilerin bilgi ve bilgisayar güvenliği ile ilgili bilgi ve farkındalık eğitim ve politikaların yetersiz olduğu ifade edilmiştir. Bu konuda öğrencilere yönelik eğitim faaliyetlerin artırılması yönünde öneride bulunulmuştur.

Gökmen ve Akgün (2014, s. 61-84), yapmış oldukları "Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli

Değişkenlere Göre İncelenmesi" isimli çalışmada, öğretmenlerin birçoğunun bilişim sistemlerinin güvenliği sorunu ile ilgili müfredatta herhangi bir dersin olmadığı, böyle bir dersi görmedikleri ve bilişim sistemlerinin güvenliği ile sorunlarını anlatacak kapasitede yeterli olmadıklarını ortaya koymuşlardır.

Karaoğlan Yılmaz, Yılmaz ve Sezer (2014, s.179-199), yapmış oldukları "Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış" isimli çalışmada, üniversite öğrencilerinin bilgi güvenliği ile ilgili temel konularda yeteri kadar bilgiye sahip olduğu fakat meydana gelen teknolojik gelişmelere uyum sağlayamadığı için bazı konularda eksik kaldıkları ortaya konmuştur. Bu sorunun giderilmesi için üniversite öğrencilerinin teknolojik gelişmelerden haberdar edilmesi gerektiği ifade edilmiştir.

Keser ve Güldüren (2015, s. 1167-1184.), yapmış oldukları "Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması" isimli çalışmada, ölçek geliştirme sürecinde çalışma grubuna verilen bilgi güvenliği farkındalık eğitimlerinin, etkinliklerinin kanıtlanmış olduğu sonucuna varılmıştır. Ayrıca çalışmada bilgi güvenliği ile ilgili politikaların ve eğitimlerin gerekli olduğu ifade edilmiştir.

Keser, Çetinkaya ve Güldüren (2016, s.692-693), yapmış oldukları "Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması" isimli çalışmada, bilgi güvenliği farkındalığı ile cinsiyet arasında belirgin bir değişiklik tespit edilmiştir. Bilgi güvenliği hususunda erkek öğrencilerin kız öğrencilere kıyasla daha fazla duyarlılık gösterdiği ortaya konmuştur.

Albrechtsen (2007), yapmış olduğu "A Qualitative Study of Users' View on Information Security" isimli çalışmada, personelin bilgi güvenliğine bakışına ilişkin niteliksel bir çalışma ortaya koymuştur. Araştırmada çalışma grubu olarak bilişim teknolojileri alanında faaliyet gösteren firmaları ve Norveç'teki bankaları konu edinmiştir. Yapılan çalışmada bilgi güvenliği koruma amirleri ile çalışanlar arasındaki iletişim kopukluğu üzerinde durulmuş ve güvenlik ile ilgili risklerin ve tehditlerin nedeni olarak kamu çalışanlarının konu ile ilgili bilgi yetersizliği öne sürülmüştür. Sorunun giderilmesi konusunda ise yöneticilerin ve personelin beraber hareket etmeleri, bilgi güvenliği ile ilgili politikaların oluşturulması ve bilgi güvenliği eğitimlerinin düzenlenmesi gerektiği ifade edilmiştir.

Öğütçü (2010), yapmış olduğu "E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi" isimli çalışmada, araştırmaya katılan bireylerin bilgi güvenliği konusunda yeterince donanımlı olmadıkları ortaya konmuştur. Çalışmanın sonucunda ise, bilgi güvenliği farkındalık eğitimlerinin verilmesi gerektiği ifade edilmiştir.

Kaşıkçı, Çağıltay, Karakuş ve Ogan (2014, s.230-243), yapmış oldukları "Türkiye ve Avrupa'daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanımı" isimli çalışmada, ebeveynlerin çocuklarını internet kullanımının beraberinde getirdiği zararlardan koruyacak düzeyde bilgiye sahip olmadıklarını ortaya koymuşlardır. Çalışmada çözüm önerisi olarak, ebeveynlerin güvenli internet kullanımı konusunda bilgilendirilmeleri hususunda konferans ve seminerlerin düzenlenmesi, bilgi güvenliği eğitimlerinin verilmesi gerektiği ifade edilmiştir.

Çavuş ve Erçag (2016, s.76-90), yapmış oldukları "The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies" isimli çalışmada, öncelikle öğretmenlerin güvenli internet kullanım bilincinin yüksek olduğunu ortaya koymuştur. Ayrıca çalışmada, günlük bilgisayar kullanım süresi ve günlük internet kullanım süresi arttıkça, bilgi güvenliği ile aralarında pozitif bir ilişki olduğu, branş, öğrenim kademesi, öğrenim durumu ve mesleki kıdem faktörlerine göre ise negatif bir ilişki olduğu saptanmıştır.

Kuru ve Ocak (2016, s.57-65), yapmış oldukları "Determination of Cyber Security Awareness of Public Employees and Consciousness-rising Suggestions." isimli çalışmada, kamu kurumlarında çalışanların gerek siber güvenlik gerekse siber savaşlara dair yeterli donanıma sahip olduğu ortaya konmuştur. Çalışmada öneri olarak, kamu kurumlarında çalışan personele devamlı bir şekilde eğitim verilmesi ve üniversitelerde siber güvenlik ile ilgili derslerin müfredata eklenmesi gerektiği belirtilmiştir. Ayrıca çalışmada, kamu kurumlarının siber güvenlik ile ilgili politikalarını kendi aralarında paylaşmaları ile siber güvenlik konusunda farkındalık oluşturulabileceği ifade edilmiştir.

Şahinaslan ve arkadaşları (2009), yapmış oldukları "Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri," isimli çalışmada, kamu kurumlarında çalışan personelin bilgi güvenliğini kazanmak için yalnızca bilişim tedbirlerinin yeterli

olmadığı, en değerli faktörün insan olduğu ve bilgi güvenliği ile ilgili sorunların ve saldırıların önlenmesinin yalnızca farkındalık ve eğitim seviyelerinin yükseltilmesiyle mümkün olacağı belirtmiştir.

Yukarıda yapılan çalışmalarda bilgi güvenliği farkındalıklarının yeterince anlaşılmadığı ve eksik kaldığı görülmektedir. Dolayısıyla teknik sorunlar, teknolojinin yetersiz bilgi ve dikkatsiz kullanımı, farkındalığın ve eğitimlerin yetersiz olması ve teknolojik gelişmelerle beraber bilgi güvenliğiyle ilgili saldırıların ve tehlikelerin farklılaşması nedeniyle bilgi güvenliğinin sağlanması zorlaşmaktadır. Bilgi güvenliğinin güvence altına alınması ve bu alanda farkındalık ile eğitimlerin geliştirilmesi, kamu kurumlarında giderek daha büyük bir öncelik haline gelmektedir. Yapılan bu çalışmada, bilgi güvenliği konusunda daha önce yapılmış çalışmalara destek sunulması, çeşitli risk ve tehlikelere maruz kalan kamu personelinin bilgi güvenliği ile ilgili farkındalığının artırılması amaçlanmaktadır. Bu doğrultuda çalışmanın devamında, kamu personelinin bilgi güvenliği farkındalığının cinsiyet, yaş, eğitim, görev düzeyi, görev süresi, ortalama kaç yıldır internet kullandığı gibi değişkenlere göre farklılık gösterip göstermediği incelenecektir.

3. MATERYAL VE YÖNTEM

Bu başlık altında, araştırmanın problemi, araştırmanın amacı, araştırmanın yöntemi, araştırmanın evreni ve örneklemi, araştırmanın hipotezleri, araştırmanın kısıtlılıkları, araştırmada kullanılan ölçme araçları olan kişisel bilgi formu ve bilgi güvenliği farkındalık ölçeği hakkında bilgiler verilerek incelenecektir.

3.1. Araştırmanın Problemi

Bilgi güvenliğinin sağlanmasında insan unsurunun kritik bir rolü vardır. Çünkü teknolojik önlemler kadar insan davranışları da güvenliği etkilemektedir. İnsanlar, bilinçli ve dikkatli olmalı, güvenlik politikalarına uymalı ve güvenlik ihlallerine karşı duyarlı olmalıdır. Bilgi güvenliği farkındalığının yeterince oluşturulmaması paradoksal bir şekilde en büyük tehdit unsuru haline gelebilmektedir. Bu nedenle bilgi güvenliği stratejileri, personelin bilinçlendirilmesi ve eğitilmesiyle birlikte sürekli olarak güncellenmeli ve iyileştirilmelidir. Bu çerçevede değerlendirildiğinde çalışanların bilgi güvenliği farkındalığı, kurumsal bilişim sistemlerinin oluşturulmasında önemli bir rol oynamaktadır. Bu sistemlerin etkin bir şekilde işlevsel hale gelmesinde belirleyici bir faktördür.

Bilgi güvenliği yönetimi, başarılı ve sürdürülebilir bir şekilde işletilebilir ve çalışanların bilgi güvenliği konusundaki farkındalık düzeyleri yüksek olduğunda sağlanabilir. Çalışanların bilgi güvenliği konusundaki yeterli bilgiye ve beceriye sahip olmaları, bilgi varlıklarının korunmasında kritik bir faktördür ve bu nedenle bilgi güvenliği farkındalığı stratejilerin önemli bir parçasını oluşturmaktadır. Kamu kurumlarında bilgi güvenliğinin sağlanmasına yönelik alınan önlemlerin çoğunluğunu teknik önlemler oluşturmaktadır. İnsan unsurunun bu süreçteki rolüne ise genellikle önem verilmemektedir. Yapılan açıklamalar ışığında bu araştırmanın problem cümlesi aşağıdaki şekildedir (Alemdaroğlu, 2020, s. 42).

Problem cümlesi: “Kamu kurumlarında çalışan personelin bilgi güvenliği farkındalık düzeyi nedir?”.

3.2. Araştırmanın Amacı

Dünyada meydana gelen teknolojik gelişmeler hayatımızın her yönüne temas etmektedir. Günlük rutin hayatımızı sürdürmekten çalışma hayatına kadar her alanda var olan teknolojik ürünler hayatımızı oldukça kolaylaştırmaktadır. Bu durum, teknolojinin getirdiği imkanlardan faydalanırken ortaya çıkabilecek sorunlara karşı dikkatli olmamızı gerektirmektedir. Bilgi güvenliği teknoloji konusunda dikkate alınması gereken temel konuların başında gelmektedir. Bilgi teknolojilerinin yoğun bir şekilde kullanıldığı kamu kurumları açısından bilgi güvenliği konusu ayrıca önem taşımaktadır. Çünkü kamu kurumları bir yandan vatandaşlara ihtiyaç duydukları hizmetlerin üretilmesinde etkin bir rol oynarken diğer yandan, vatandaşlar ile ilgili gizli kalması gereken bilgilerin de toplandığı merkezlerdir.

Kamu kurumlarında çalışan bireylerin bilgi güvenliği konusundaki duyarlılıkları bilgi güvenliğinin sağlanması açısından oldukça önemlidir. Çünkü elektronik ortama taşınan ve kaydedilmiş olan personel verilerinin ya da kamu kurumlarında bilgilerin herhangi bir nedenden dolayı bozulmaya, silinmeye, değişikliğe uğraması ya da bu bilgilerin geri dönülemez bir şekilde kaybolması halinde kamu kurumlarının işleyiş sürecini olumsuz bir şekilde etkileyecektir. Gerekli güvenlik önleminin alınmaması sonucu kamu kurumlarında maddi ve manevi kayıpların oluşmasına sebep olmaktadır. Ayrıca eğitim amacıyla kullanılan bilgisayar laboratuvarlarının veya çevrimiçi eğitim sistemlerinin çeşitli nedenlerle (örneğin, virüs bulaşması gibi) işlevsiz hale gelmesi, zaman ve işgücü kaybına neden olabilir ve çeşitli kayıplara yol açabilmektedir. (Vardal, 2009, s. 23). Yaşanabilecek bu olumsuz durumların tümü kamu personelinin bilgi güvenliği konusunda sahip olduğu farkındalık ile yakından ilişkilidir. İnsan unsurunun kamu kurumlarında bilgi güvenliğinin sağlanmasında temel belirleyici olması, onun bilgi güvenliği konusunda belirli bir farkındalık düzeyine sahip olmasını gerektirmektedir.

Bu çalışmanın temel amacı, kamu kurumlarında çalışan personelin bilgi güvenliği farkındalığının ölçülmesi, demografik ve çalışma hayatına dair parametrelerin bilgi güvenliğine etkisinin belirlenmesi ve kamu kurumlarında bilgi güvenliği sağlanması hususunda çözüm önerilerinin geliştirilmesidir. Bu temel amaç dışında çalışma içerisinde farklı alt amaçlar da belirlenmiştir. Alt amaçlar doğrultusunda aşağıda yer alan problem başlıklarına da cevap aranacaktır.

- Kurumunda çalışan personelin bilgi güvenliği farkındalığı cinsiyete göre farklılık göstermekte midir?
- Kurumunda çalışan personelin bilgi güvenliği farkındalığı yaşa göre farklılık göstermekte midir?
- Kurumunda çalışan personelin bilgi güvenliği farkındalığı eğitim düzeyine göre farklılık göstermekte midir?
- Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev düzeyine göre farklılık göstermekte midir?
- Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev süre düzeyine göre farklılık göstermekte midir?
- Kurumunda çalışan personelin bilgi güvenliği farkındalığı ortalama internet kullanım yılına göre farklılık göstermekte midir?
- Kurumunda çalışan personelin bilgi güvenliği farkındalığı günlük internet kullanım süresine göre farklılık göstermekte midir?

3.3. Araştırmanın Yöntemi

Araştırmada öncelikle bilgi ve bilgi güvenliği, bilgi güvenliğini tehdit eden durumlar ve bilgi güvenliğinin ihlal edilme türleri konusunda derinlemesine bir literatür taraması gerçekleştirilmiştir. İlgili literatür taraması sonucunda elde edilen bilgiler doğrultusunda çalışmanın yazın alanı oluşturulmuştur.

Çalışmada bilgi güvenliği farkındalığının belirlenebilmesi için Diyarbakır ilinde kamu kurumlarında çalışan personele yönelik gerçekleştirilen araştırma yöntemlerinden nicel araştırma yöntemi benimsenmiş olup araştırma yöntemlerinde anket yöntemi tercih edilerek veri toplama işlemi gerçekleştirilmiştir. Analizler SPSS paket programında gerçekleştirilmiştir.

3.4. Araştırmanın Evreni ve Örneklemi

Araştırmanın evreni için basit tesadüfi örnekleme yöntemi kullanılmıştır. Bu doğrultuda Diyarbakır ilinde rastgele seçilen kamu kurumlarında çalışan personel örnekleme alınmıştır. Bu çalışmada araştırma yöntemlerinden nicel araştırma yöntemi benimsenmiş olup veri toplama hususunda anket yöntemi tercih edilmiştir.

3.5. Araştırmanın Hipotezleri

Kamu kurumlarında çalışan personelin bilgi güvenliği farkındalıklarını çeşitli kategorilere göre farklılık gösterip göstermediğini incelemek için oluşturulan hipotezler:

H_1 Kurumunda çalışan personelin bilgi güvenliği farkındalığı cinsiyete göre farklılık göstermektedir.

H_2 Kurumunda çalışan personelin bilgi güvenliği farkındalığı yaşa göre farklılık göstermektedir.

H_3 Kurumunda çalışan personelin bilgi güvenliği farkındalığı eğitim düzeyine göre farklılık göstermektedir.

H_4 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev düzeyine göre farklılık göstermektedir.

H_5 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev süresi düzeyine göre farklılık göstermektedir.

H_6 Kurumunda çalışan personelin bilgi güvenliği farkındalığı ortalama kaç yıldır internet kullanım düzeyine göre farklılık göstermektedir.

H_7 Kurumunda çalışan personelin bilgi güvenliği farkındalığı günlük internet kullanım süresine göre farklılık göstermektedir.

3.6. Araştırmanın Kısıtlılıkları

Bu araştırmanın en önemli sınırlılığı sadece Diyarbakır'da bulunan kamu kurum ve kuruluşları bünyesinde çalışan personeli kapsıyor olmasıdır.

3.7. Araştırmada Kullanılan Ölçme Araçları

Keser ve Güldüren tarafından geliştirilen Bilgi Güvenliği Farkındalık Ölçeği, yapılan araştırmada bazı sorular için değişiklik yapılarak kullanılmıştır. Yapılan bu değişiklikler ölçeğin daha spesifik ihtiyaçlara ve araştırma gereksinimlerine uygun hale getirilmesini sağlamaktır. Bu ölçek EK-2'de yer almaktadır (Keser & Güldüren, 2015, s. 1167). Aynı zamanda çalışanların demografik özelliklerini belirlemek amacıyla Kişisel Bilgi Formu oluşturulan ilgili form ise EK-1'de yer almaktadır. Yapılan değişiklik sonucunda öncelikle

ölçeğin güvenirlilik testi yeniden yapılmıştır ve ölçek kamu kurumlarında çalışan personele uygulanmıştır.

3.7.1. Kişisel Bilgi Formu

Araştırmada çalışanlara yöneltilen kişisel bilgi formunda (cinsiyet, yaşınız, eğitim durumu, çalıştığınız kamu kurumdaki göreviniz, kamu kurumdaki görev süreniz, ortalama kaç yıldır internet kullanıyorsunuz, günlük internet kullanım süreniz nedir) yedi adet soru bulunmaktadır. Bu sorular, çalışanların profillerini ve araştırma amacına yönelik bilgilerini derlemek için kullanılmıştır.

3.7.2. Bilgi Güvenliği Farkındalık Ölçeği

Araştırmada kullanılan Bilgi Güvenliği Farkındalık Ölçeği, toplamda 24 maddeden oluşmaktadır. Bu maddeler 5'li likert tipi bir ölçekten değerlendirilmiştir. Ölçekte "Kesinlikle katılmıyorum", "katılmıyorum", "kararsızım", "katılıyorum" ve "Kesinlikle katılıyorum" derecelerine ayrılmış olumlu ve olumsuz ifadeler bulunmaktadır. Ölçek katılımcıların bilgi güvenliği konusundaki farkındalık düzeylerini ölçmek amacıyla kullanılmıştır. Katılımcılar her maddeye verdikleri yanıtlarla kendi farkındalık seviyelerini ifade etmişlerdir. Bu ölçek, araştırmanın sonuçlarını değerlendirmek ve bilgi güvenliği farkındalığı ve eğitim programlarının etkinliğini belirlemek için önemli bir araçtır.

4. ARAŞTIRMANIN BULGULARI

Diyarbakır ilinde rastgele seçilen kamu kurumlarında toplam 164 çalışana araştırma anketi elektronik ortamdan ulaştırılarak uygulanmıştır. Örneklemi ise 25 yönetici, 4 akademik personel, 14 idari personel, 89 memur ve 32 diğerleri olmak üzere kamu kurumlarında çalışan personelden oluşmaktadır. Çalışmanın örneklemini ise uygun örnekleme yöntemi kullanılarak seçilmiş 42 kadın ve 122 erkek personel oluşturmaktadır. Bu örnekleme yöntemi toplamda kamu kurumlarının bünyesinde çalışan 164 personelden oluşmaktadır. Araştırmanın amaçlarına ve kapsamına uygun bir şekilde katılımcıların seçilmesini sağlamıştır. Bu örnekleme yaklaşımı araştırmanın güvenilirliği ve geçerliliği açısından önemli bir rol oynamaktadır.

Bilgi güvenliği farkındalık ölçeğinin faktör analizi sonucunda birinci ve ikinci faktör olmak üzere 2 farklı alt boyut elde edilmiştir. Bilgi güvenliği farkındalığı alt boyutlarının sosyo-demografik özelliklere göre fark yaratıp yaratmadığını tespit etmek için uygulanan Kaiser-Mayer-Olkin (KMO) Testi ve Bartlett Sphericitiy Testi uygulanmıştır. Ayrıca değişkenler ile sosyo-demografik özellikler arasında ilişkiyi analiz etmek için Bilgi Güvenliği Farkındalıkları arasında fark olup olmadığını belirlemek için non-parametrik testlerden Kruskall Wallis ve Mann-Whitney U testleri gerçekleştirilmiştir.

4.1. Demografik Özellikler

4.1.1. Cinsiyet Değişkenine İlişkin Mann-Whitney U Testi Sonuçları

H_1 "Kurumunda çalışan personelin bilgi güvenliği farkındalığı cinsiyete göre farklılık göstermektedir." hipotezini test etmek için Mann-Whitney U Testi gerçekleştirilmiş ve sonuçları Tablo 4.1'de sunulmuştur.

Tablo 4 1: Cinsiyet ve Bilgi Güvenliği Farkındalığı

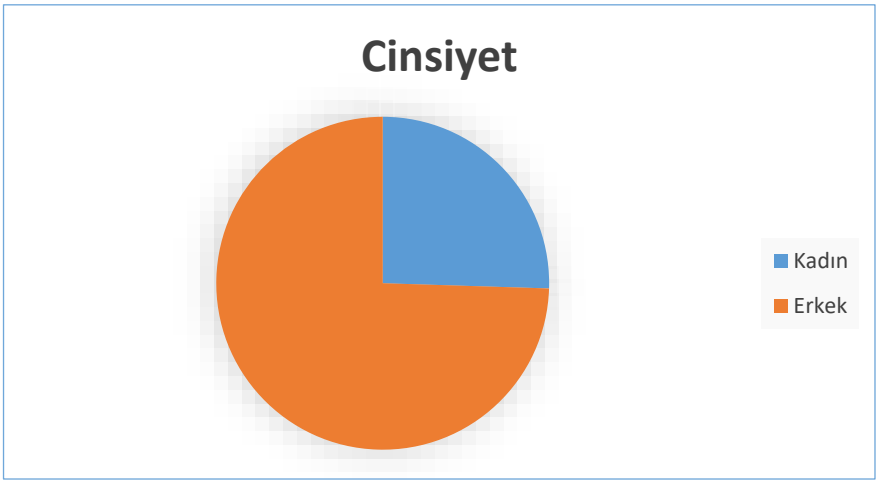
	Grup	N	%	Sıra ortalaması	Standart sapma	Sıra toplamı	Z	P
	Kadın	42	25,6	67,21	25,576	2823	1920	0,015

Bilgi Güvenliği Farkındalığı	Erkek	122	74,4	87,21	18,313	10707		
Birinci Faktör	Kadın	42	25,6	67,76	14,89399	2849,5	1946,5	0,02
	Erkek	122	74,4	87,55	11,38852	10680,5		
İkinci Faktör	Kadın	42	25,6	68,27	11,6038	2867,5	1964,5	0,022
	Erkek	122	74,4	87,4	7,8019	10,662		

Tablo 4.1'de göre, kadın ve erkek katılımcıların bilgi güvenliği farkındalıklarında ve bu anketten ortaya çıkan faktörler arasında anlamlı bir fark vardır ($p<0,05$). Hem bilgi güvenliği farkındalığında hem de faktörlerde, erkeklerin puan ortalaması, kadınlardan daha fazladır. Hipotezi tutarlıdır. Burada H_1 Kurumunda çalışan personelin bilgi güvenliği farkındalığı cinsiyete göre farklılık göstermektedir. Hipotezi erkeklerin kadınlara göre daha fazla duyarlıdır.

4.1.2. Cinsiyet Kriterine Göre Dağılım

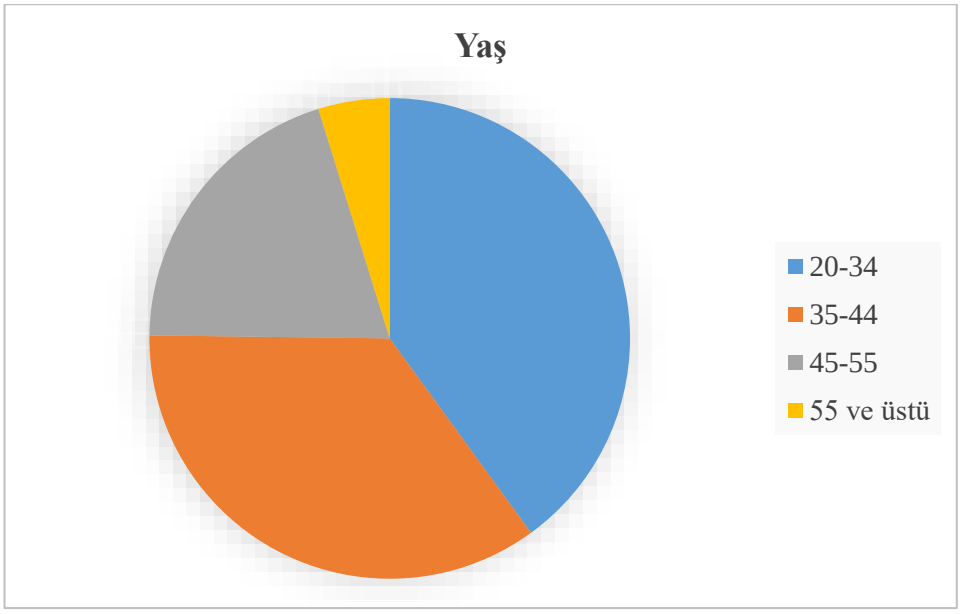
Diyarbakır'da kamu kurumlarında yapılan ankette araştırmaya katılanların %74,4 erkek, %25,6 kadındır. H_1 Kurumunda çalışan personelin bilgi güvenliği farkındalığı cinsiyete göre farklılık göstermektedir. Yapılan araştırmada erkeklerin katılım oranı kadınlara göre daha fazladır.



Şekil 4. 1: Cinsiyet Dağılım Grafiği

4.1.3.Yaş Kriterine Göre Dağılım

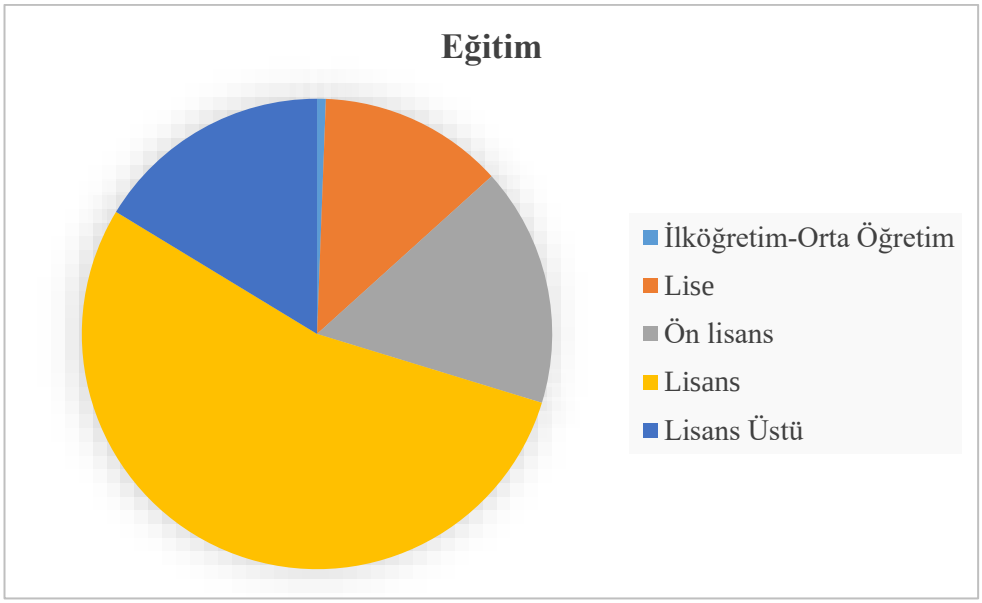
H_2 Kurumunda çalışan personelin bilgi güvenliği farkındalığı yaşa göre farklılık göstermektedir. Araştırmaya katılanların %39,6'ı 20-34 yaş grubunda, %35,4'si 35-44 yaş grubunda, %20,1'si 45-55 yaş grubunda, %4,9'sı 55 yaş ve üstü gruptadır araştırmada genç yaş ve orta yaş grupların katılım oranları daha fazladır.



Şekil 4. 2: Yaş Dağılım Grafiği

4.1.4. Eğitim Durumu Kriterine Göre Dağılım

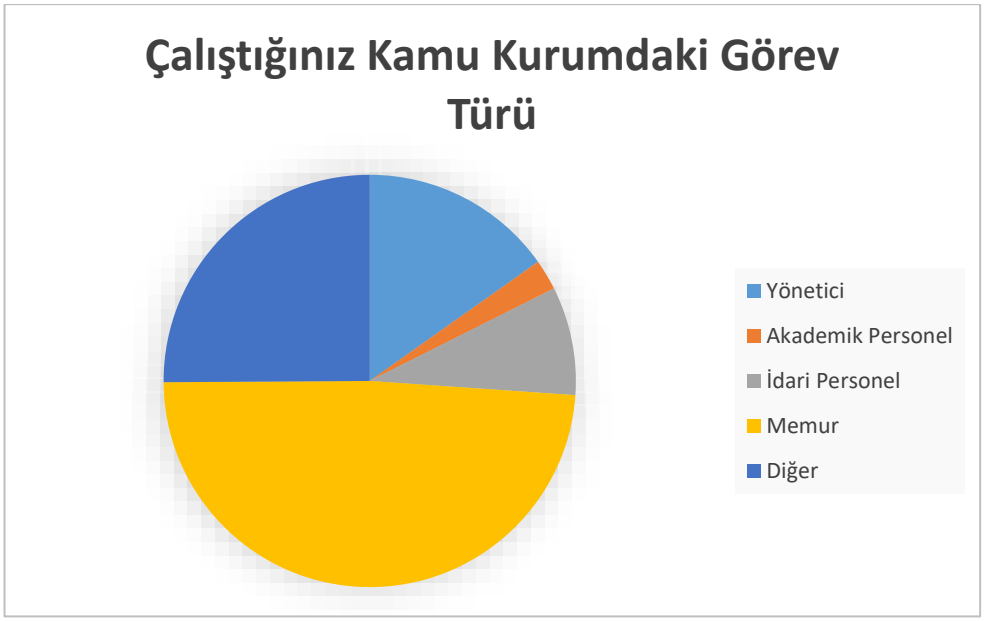
H_3 Kurumunda çalışan personelin bilgi güvenliği farkındalığı eğitim düzeyine göre farklılık göstermektedir. Araştırmaya katılanların %0,6 ilköğretim-orta öğretim, %12,8'si lise, %16,5'i ön lisans, %53,7'si lisans, %16,3'ü Lisans üstü seviyesinde eğitim düzeyine sahiptir.



Şekil 4. 3: Eğitim Durumu Dağılım Grafiği

4.1.5. Çalıştığınız Kamu Kurumdaki Görev Kriterine Göre Dağılım

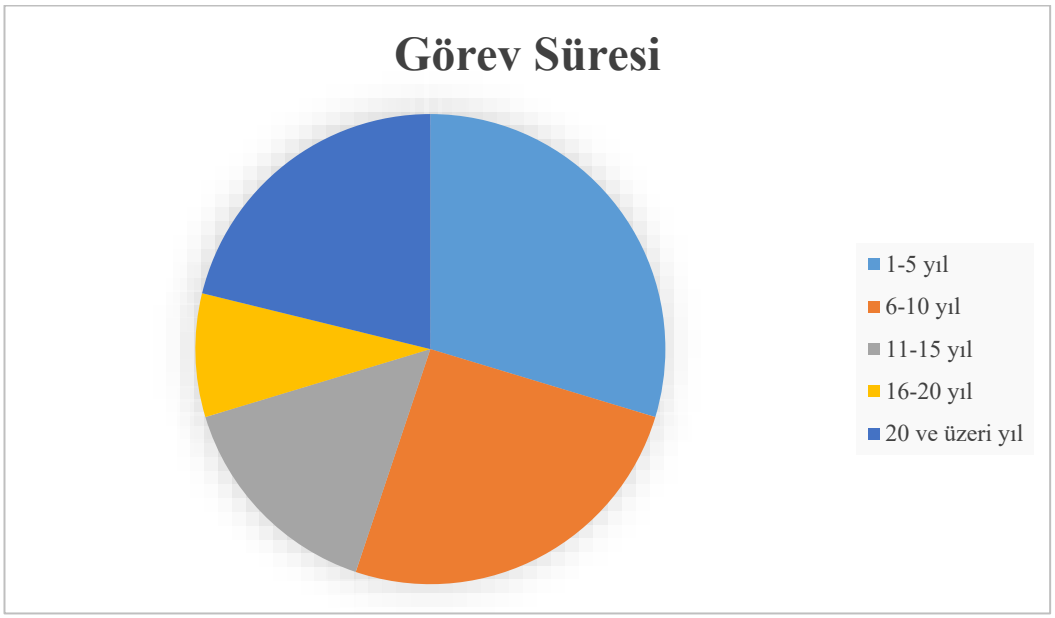
H_4 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev düzeyine göre farklılık göstermektedir. Araştırmaya katılanların %15,2'si yönetici, %2,4'ü akademik personel, %8,5'i idari personel, %48,8 memur, %25,1'ü diğerleridir.



Şekil 4. 4:Çalıştığınız Kamu Kurumdaki Görev Türü dağılım Grafiği

4.1.6. Kamu Kurumdaki Görev Süresi Kriterine Göre Dağılım

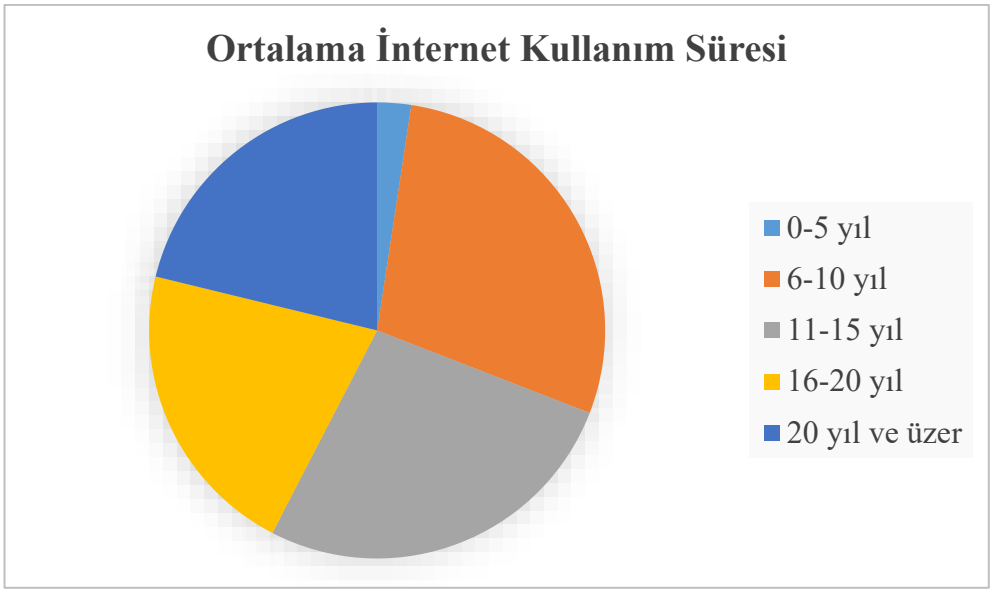
H_5 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev süresi düzeyine göre farklılık göstermektedir. Araştırmaya katılanların %29,3'ü 1-5 yıldır, %25,6'si 6-10 yıldır, %15,2'si 11-15 yıldır, %8,5'i 16-20 yıldır, %21,3'ü 20 yıl ve üzeri çalışmaktadır.



Şekil 4. 5: Görev Süresi Dağılım Grafiği

4.1.7 Ortalama İnternet Kullanım Süresi Kriterine Göre Dağılım

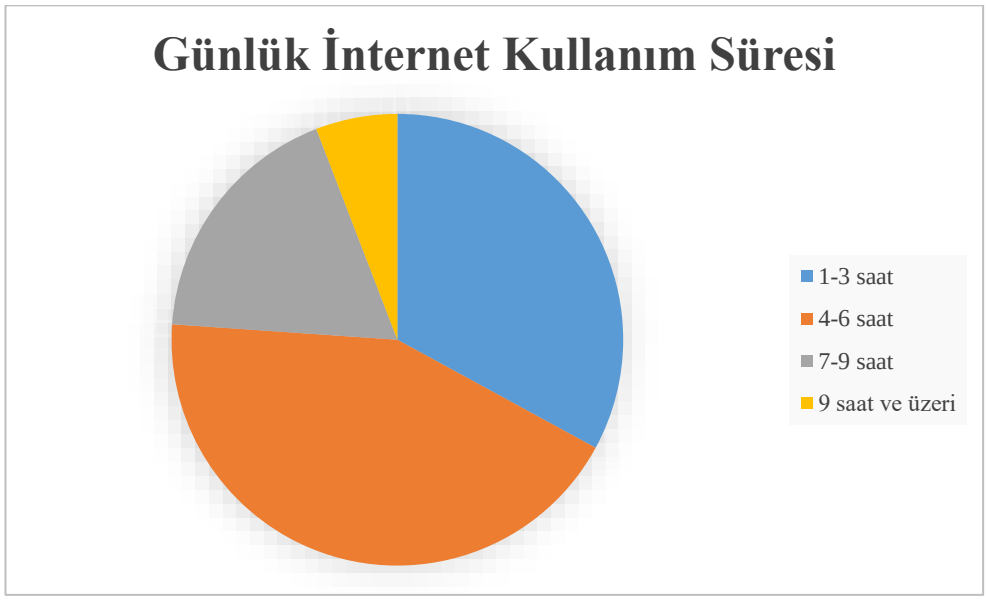
H_6 Kurumunda çalışan personelin bilgi güvenliği farkındalığı ortalama kaç yıldır internet kullanım düzeyine göre farklılık göstermektedir. Araştırmaya katılanların %2,4'ü 0-5 yıldır, %28,7'i 6-10 yıldır, %26,8'si 11-15 yıldır, %20,7'si 16-20 yıldır ve %21,3'si 20 yıl ve üzeri internet kullanmaktadır.



Şekil 4. 6: Ortalama İnternet Kullanım Süresi Dağılım Grafiği

4.1.8. Günlük İnternet Kullanım Süresi Kriterine Göre Dağılım

H_7 Kurumunda çalışan personelin bilgi güvenliği farkındalığı günlük internet kullanım süresine göre farklılık göstermektedir. Araştırmaya katılanların %37'si günde 1-3 saat, %40,6'sı günde 4-6 saat, %17'si günde 7-9 saat ve %5,5'i günde 9 saat ve üzeri internet kullanmaktadır.



Şekil 4. 7: Günlük İnternet Kullanım Süresi Dağılım Grafiği

4.2. İstatistiksel Analiz

Diyarbakır'ın çeşitli kurumlarında yapılan araştırmaya göre, 164 katılımcıdan elde edilen veriler, IBM SPSS paket programı aracılığı ile analiz edilmiştir. Öncelikle katılımcıların özellikleri betimsel analizler aracılığı ile belirlenmiş; tablo aracılığı ile sunulmuştur. Daha sonra 24 maddeden oluşan Bilgi Güvenliği Farkındalığı anketinden elde edilen verilerin faktör analizi yapılmış ve bulgular bölümünde verilmiştir. Ardından normalliği incelenmiş ve güvenirlik değeri hesaplanmıştır. Bu bilgiler Tablo 4.2'de verilmiştir.

4.2.1.Bilgi Güvenliği Farkındalığı anketinin normalliği ve güvenirliği

Tablo 4 2: Bilgi Güvenliği Farkındalığı Anketinin Normalliği ve Güvenirliği

Özellik	Değeri
Ortalama	100,27
Standart sapma	20,77
Çarpıklık	-1,597
Basıklık	2,719
Kolmogorov-Smirnov (p)	0,000
Shapiro-Wilk (p)	0,000
Cronbach Alpha	0,971

Tablo 4.2'ye göre, 164 katılımcının Bilgi Güvenliği Farkındalığı anketinden elde edilen verilerin ortalaması 100,27 ve standart sapması 20,77'dir. Çarpıklık ve basıklık değerlerinin ise +1 ve -1 Aralığında olmadığı görülmüştür. Ayrıca K-S ve S-W değeri 0,05'ten büyük değildir. Bu nedenle verilerin normal dağılıma sahip olmadığı söylenebilir. Bu nedenle verilerin analizinde non-parametrik testler kullanılmıştır. 24

maddelik anketten elde edilen verilerin Cronbach Alpha değeri ise 0,971'dir. Bu değer, anket ile toplanan verilerin yüksek güvenirlikte olduğunu göstermektedir.

4.3.Faktör Analizi Sonuçları

Araştırmanın bu bölümünde Bilgi Güvenliği Farkındalığı anketine ilişkin boyutlara ve bu boyutlar arasındaki ilişkilere ilişkin bulgulara yer verilmiştir. Bunun için öncelikle faktör analizi yapılmıştır; Varimax rotasyonu kullanılarak yorumlanabilir faktörlerin oluşturulması saptanmıştır. Verilerin uygunluğunu belirlemek için faktör analizinden önce Kaiser-Mayer-Olkin (KMO) katsayısı ve Bartlett Sphericitiy test değerleri hesaplanmış; Tablo 4. 3'de verilmiştir.

4.3.1.Kaiser- Mayer-Olkin(KMO) ve Bartlett Sphericitiy Testi sonuçları

Tablo 4 3: KMO ve Bartlett Sphericitiy Testi sonuçları

Kaiser-Meyer-Olkin Örneklem Yeterliliği Ölçütü		0,94
Bartlett' Küresellik Testi	Ki-kare	4371,632
	sd	276
	p	0,000

Tablo 4.3'de göre, KMO değeri 1'e yakındır; Bartlett küresellik testi ise anlamlı bulunmuş ve p değeri, 0,05'den küçüktür. Bu nedenle faktör analizi yapılmasının uygun olduğuna karar verilmiş; anketteki maddelerin faktör yüklerini belirlemek ve yapı geçerliliğini açıklamak için faktör analizi gerçekleştirilmiştir.

4.3.2.Temel Bileşenler Analizi ve Açıklanan Toplam Varyans Değerleri

Bilgi Güvenliği Farkındalığı anketi iki faktörlü bir yapıya sahiptir ve toplam açıklanan varyans %69,636'tür. Birinci faktör varyansın %35,168'ünü ve ikinci faktör varyansın %34,468'ini oluşturmaktadır. Ayrıca, birinci faktörün güvenirliği 0,956 ve ikinci faktörün güvenirliği 0,949'dur.

4.3.3.Bilgi Güvenliği Farkındalığı Faktörlerinin Betimsel İstatistik Değerleri

Tablo 4 4: Faktörlerin Betimsel İstatistik Değerleri

	N	Ortalama	Standart Sapma
Birinci Faktör	164	51,9695	12,57538
İkinci Faktör	164	48,2988	9,06634

4.4. Kruskall Wallis ve Mann-Whitney U testleri Fark Testleri Sonuçları

Katılımcıların demografik özelliklerine göre Bilgi Güvenliği Farkındalıkları arasında fark olup olmadığını belirlemek için nonparametrik testlerden Kruskall Wallis ve Mann-Whitney U testleri gerçekleştirilmiştir. Çünkü parametrik testlerin normallik ve homojenlik varsayımlarını veriler karşılamamaktadır.

4.4.1.Yaş Değişkenine İlişkin Kruskall Wallis Testi Sonuçları

"H_2 Kurumunda çalışan personelin bilgi güvenliği farkındalığı yaşa göre farklılık göstermektedir." hipotezini test etmek için Kruskall Wallis Testi gerçekleştirilmiş ve sonuçları Tablo 4.5'de sunulmuştur.

Tablo 4 5: Yaş ve Bilgi Güvenliği Farkındalığı

	Gruplar	N	%	Sıra Ortalaması	Standart Sapma	sd	X^2	p
Bilgi Güvenliği Farkındalığı	20-34	65	39,6	81,89	18,787	3	1,22	0,748
	35-44	58	35,4	84,6	22,224			
	45-54	33	20,1	76,82	23,753			
	55 ve üzeri	8	4,9	95,63	9,493			

Birinci Faktör	20-34	65	39,6	82,55	11,32471	3	2,115	0,549
	35-44	58	35,4	84,91	13,50499			
	45-54	33	20,1	74,21	14,24349			
	55 ve üzeri	8	4,9	98,75	5,74301			
İkinci Faktör	20-34	65	39,6	82,61	8,4115	3	0,369	0,947
	35-44	58	35,4	84,13	9,65685			
	45-54	33	20,1	78,5	10,20732			
	55 ve üzeri	8	4,9	86,31	4,52769			

Tablo 4.5'de göre, farklı yaş gruplarından olan katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Hipotezi tutarlı değildir. Burada kurumunda çalışan personelin bilgi güvenliği farkındalığı yaşa göre farklılık göstermemektedir. Araştırmanın yapıldığı yaş grupları arasında belirli ölçüm veya değişken açısında istatistiksel olarak önemli bir farklılık tespit edilmemiştir.

4.4.2. Eğitim Düzeyi Değişkenine İlişkin Kruskall Wallis Testi Sonuçları

Kamu kurumlarında "H_3 Kurumunda çalışan personelin bilgi güvenliği farkındalığı eğitim düzeyine göre farklılık göstermektedir" hipotezini test etmek için Kruskall Wallis Testi gerçekleştirilmiş ve sonuçları Tablo 4.6'da sunulmuştur.

Tablo 4 6: Eğitim Düzeyi ve Bilgi Güvenliği Farkındalığı

	Gruplar	N	Sıra Ortalaması	Standart Sapma	sd	X^2	p
Bilgi Güvenliği Farkındalığı	İlköğretim-Lise	22	83,16	20,712	3	5,452	0,142
	Ön lisans	27	99,96	17,587			
	Lisans	88	76,03	23,178			
	Lisansüstü	27	85,57	12,792			
Birinci Faktör	İlköğretim-Lise	22	89,45	11,67572	3	7,072	0,07
	Ön lisans	27	101,74	10,64555			
	Lisans	88	75,21	13,96196			
	Lisansüstü	27	81,35	8,6372			
İkinci Faktör	İlköğretim-Lise	22	73,55	9,47416	3	4,178	0,243
	Ön lisans	27	94,5	7,58798			
	Lisans	88	78,45	10,13023			
	Lisansüstü	27	91	5,26262			

Tablo 4. 6'ya göre, farklı eğitim düzeyleri olan katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Hipotezi tutarlı değildir. Burada kamu kurumunda çalışan personelin bilgi güvenliği farkındalığı

eğitim düzeyine göre farklılık göstermemektedir. Çünkü bilgi güvenliği, çalışanların eğitim seviyesine göre değil kurumun sağladığı eğitim ve politikalara olan erişimine, bilgi güvenliği kültürünün kurum içinde ne kadar güçlü olduğuna ve çalışanların bilinçlenme düzeyine bağlıdır.

4.4.3. Çalıştığınız Kamu Kurumdaki Görev Değişkenine İlişkin Kruskall Wallis Testi Sonuçları

"H_4 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev düzeyine göre farklılık göstermektedir." hipotezini test etmek için Kruskall Wallis Testi gerçekleştirilmiş ve sonuçları Tablo 4. 7'de sunulmuştur.

Tablo 4 7: Çalıştığınız Kamu Kurumdaki Görev ve Bilgi Güvenliği Farkındalığı

	Gruplar	N	%	Sıra Ortalaması	Standart Sapma	sd	X^2	p
Bilgi Güvenliği Farkındalığı	Yönetici	25	15,2	97,42	20,128	4	4,586	0,332
	Akademik personel	5	2,4	91,9	6,107			
	Memur	89	48,8	82,24	23,27			
	İdari personel	13	8,5	67,35	17,866			
	Diğer	32	25,1	76,27	15,757			
Birinci Faktör	Yönetici	25	15,2	95,5	11,4327	4	3,479	0,481
	Akademik personel	5	2,4	96,8	4,30116			
	Memur	89	48,8	81,2	14,1376			

	İdari personel	13	8,5	70,5	11,3753			
	Diğer	32	25,1	78,59	9,72007			
İkinci Faktör	Yönetici	25	15,2	95,04	9,21376	4	3,797	0,434
	Akademik personel	5	2,4	83,4	5,41295			
	Memur	89	48,8	83,06	10,0014			
	İdari personel	13	8,5	66,04	7,51238			
	Diğer	32	25,1	77,7	7,13853			

Tablo 4. 7'ye göre, kurumlarda farklı görevlerde çalışan katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Burada kamu kurumunda çalışan personelin bilgi güvenliği farkındalığı görev düzeyine göre farklılık göstermektedir" hipotezi tutarlı değildir. Çünkü kamu çalışanlarının eğitim düzeyleri ayrım edilmeksizin herkesin bilgi güvenliği farkındalık eğitimine sahip olması gerekir. Dolayısıyla bilgi güvenliği ile ilgili risklerin ve tehditlerin azaltılması için gerekli eğitimleri, eğitim düzeyleri fark edilmeksizin herkesin alması gerekir.

4.4.4. Kamu Kurumdaki Görev Süresi Değişkenine İlişkin Kruskall Wallis Testi Sonuçları

Araştırmada kamu kurumlarında "H_5 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev süresi düzeyine göre farklılık göstermektedir" hipotezini test etmek için Kruskall Wallis Testi gerçekleştirilmiş ve sonuçları Tablo 4. 8'de sunulmuştur.

Tablo 4 8: Kamu Kurumdaki Görev Süresi ve Bilgi Güvenliği Farkındalığı

	Gruplar	N	%	Sıra Ortalaması	Standart Sapma	sd	X^2	p
Bilgi Güvenliği Farkındalığı	0-5 yıl	48	2,4	73,9	17,678	4	6,775	0,148
	6-10 yıl	42	28,7	96,24	22,87			
	11-15 yıl	25	26,8	77,42	24,48			
	16-20 yıl	14	20,7	94,07	18,388			
	20 yıl ve üzeri	35	21,3	76,81	20,59			
Birinci Faktör	0-5 yıl	48	2,4	74,86	11,16217	4	8,12	0,087
	6-10 yıl	42	28,7	97,81	12,82413			
	11-15 yıl	25	26,8	76,42	15,21239			
	16-20 yıl	14	20,7	94,64	9,65333			
	20 yıl ve üzeri	35	21,3	74,09	12,79653			

İkinci Faktör	0-5 yıl	48	2,4	76,48	7,78703	4	3,136	0,535
	6-10 yıl	42	28,7	90,04	10,33226			
	11-15 yıl	25	26,8	76,52	10,07422			
	16-20 yıl	14	20,7	93,64	9,44998			
	20 yıl ve üzeri	35	21,3	81,53	8,66006			

Tablo 4. 8'e göre, kurumlarda farklı sürelerde görev yapan katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Burada "H_5 Kurumunda çalışan personelin bilgi güvenliği farkındalığı görev süresi düzeyine göre farklılık göstermektedir" hipotezi tutarlı değildir. Çünkü kamu çalışanları için önemli olan bilgi güvenliği bütün kamu personeli için aynı seviyeye sahip olmasıdır. Burada makam ve mevki ayrımı olmaksızın bilgi güvenliğinin sağlanmasıdır. Yapılan çalışma ise bu durumu ortaya koymaktadır.

4.4.5. Ortalama İnternet Kullanma Yılı Değişkenine İlişkin Kruskall Wallis Testi Sonuçları

Yapılan araştırmada kamu kurumlarında, "H_6 Kurumunda çalışan personelin bilgi güvenliği farkındalığı ortalama kaç yıldır internet kullanım düzeyine göre farklılık göstermektedir" hipotezini test etmek için Kruskall Wallis Testi gerçekleştirilmiş ve sonuçları Tablo 4. 9'da sunulmuştur.

Tablo 4 9: Ortalama İnternet Kullanma Süresi ve Bilgi Güvenliği Farkındalığı

	Gruplar	N	%	Sıra Ortalaması	Standart Sapma	sd	X^2	p
Bilgi Güvenliği Farkındalığı	0-5 yıl	4	2,4	53,13	30,859	4	10,096	0,039
	6-10 yıl	46	28,7	85,14	18,083			
	11-15 yıl	44	26,8	74,52	23,443			
	16-20 yıl	35	20,7	73,19	16,344			
	20 yıl ve üzeri	35	21,3	101,73	22,493			
Birinci Faktör	0-5 yıl	4	2,4	59,5	20,3306	4	10,753	0,029
	6-10 yıl	46	28,7	89,14	11,68425			
	11-15 yıl	44	26,8	74,02	12,92367			
	16-20 yıl	35	20,7	69,51	11,41074			
	20 yıl ve üzeri	35	21,3	100,04	12,88429			

İkinci faktör	0-5 yıl	4	2,4	48,25	11,08678	4	9,302	0,054
	6-10 yıl	46	28,7	78,12	7,15923			
	11-15 yıl	44	26,8	75,38	11,11355			
	16-20 yıl	35	20,7	82,36	5,95671			
	20 yıl ve üzeri	35	21,3	101,27	10,33538			

Tablo 4. 9'a göre, farklı internet kullanma süreleri olan katılımcıların bilgi güvenliği farkındalıklarında ve bunun birinci faktöründe anlamlı farklılık bulunmaktadır ($p<0,05$). 20 yıl ve üzeri internet kullanım süresi olan katılımcıların, bilgi güvenliği farkındalığı daha yüksektir. Bu bulgu, uzun süreli internet kullanımının bireylerin bilgi güvenliği konusunda daha derinlemesine anlayış geliştirmesine katkı sağladığını göstermektedir. Ancak ikinci faktörde katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Burada "H_6 Kurumunda çalışan personelin bilgi güvenliği farkındalığı ortalama kaç yıldır internet kullanım düzeyine göre farklılık göstermektedir" hipotezi tutarlıdır. Hipotezinde bilgi güvenliği duyarlıkları daha fazladır. Kamu kurumunda çalışan personelin çeşitli saldırılara karşı daha dikkatli olduğunu söyleyebiliriz. 20 yıl ve üzeri olan grubun, diğer gruplara göre bilgi güvenliğinde daha dikkatli ve tedbirli davrandığı görülmektedir.

4.6.6. Günlük İnternet Kullanma Süresi Değişkenine İlişkin Kruskall Wallis Testi Sonuçları

Kamu kurumlarında yapılan araştırmaya göre "H_7 Kurumunda çalışan personelin bilgi güvenliği farkındalığı günlük internet kullanım süresine göre farklılık göstermektedir" hipotezini test etmek için Kruskall Wallis Testi gerçekleştirilmiş ve sonuçları Tablo 4. 10'da sunulmuştur.

Tablo 4 10: Günlük İnternet Kullanma Süresi ve Bilgi Güvenliği Farkındalığı

	Gruplar	**N**	**%**	**Sıra Ortalaması**	**Standart Sapma**	**sd**	**X^2**	**p**
Bilgi Güvenliği Farkındalığı	1-3 saat	60	36,6	72,65	20,367	3	5,352	0,148
	4-6 saat	67	40,9	84,93	21,789			
	7-9 saat	28	17,1	96,68	15,464			
	9 saat ve üzeri	9	5,5	85,94	27,816			
Birinci Faktör	1-3 saat	60	36,6	71,41	12,94211	3	6,351	0,096
	4-6 saat	67	40,9	85,28	12,76165			
	7-9 saat	28	17,1	96,18	9,24161			
	9 saat ve üzeri	9	5,5	93,17	15,67642			
İkinci Faktör	1-3 saat	60	36,6	75,98	8,62725	3	3,811	0,283
	4-6 saat	67	40,9	84,02	9,68257			
	7-9 saat	28	17,1	95,66	7,03619			
	9 saat ve üzeri	9	5,5	73,72	12,27803			

Tablo 4. 10'a göre, günlük farklı internet kullanım süreleri olan katılımcıların, bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Burada **"**H_7 Kurumunda çalışan personelin bilgi güvenliği farkındalığı günlük internet kullanım süresine göre farklılık göstermektedir" hipotezi tutarlı değildir. Çünkü bilgi güvenliğinde günlük farklı internet süreleri olan katılımcıların, farklı saatlerde olmasına rağmen fark bulunmamıştır. Çünkü bilgi güvenliğine sahip çalışanların her zaman veya daima saldırılara karşı hazırlıklı olması gerekir. Bunlar için saat farkı olmaması gerekir. Yapılan çalışmada da bu kanıtlamaktadır.

5. SONUÇ, TARTIŞMA ve ÖNERİLER

Günümüzde meydana gelen teknolojik gelişmelerle beraber kamu kurumlarının bu gelişmelere ayak uydurmak ve kamu hizmetlerinin devamlılığı için gerekli düzenlemeler yapılmıştır. Bu nedenle meydana gelen teknolojik yenilikler ile beraberinde birtakım teknolojik tehlikeleri ve tehditleri meydana getirmiştir. Çünkü bilginin elektronik ortama aktarılmasıyla birlikte bilgi güvenliğinin sağlanması da bir takım sorun haline gelmiştir. Dolayısıyla kamu kurumlarının bilgi güvenliği alanında daha fazla politika oluşturma, altyapı yatırımı yapma ve planlama yapma sürecine girdiklerini göstermektedir. Kamu kurumlarında son dönemlerde meydana gelen saldırılar sonucunda daha fazla bahsedilen bir konu haline gelen bilgi güvenliği özellikle kamu kurumları için kıymetli ve vazgeçilmez öneme sahiptir (Gazdağı ve Çetinyokuş, 2020, s. 475-491). Hem kamu kurumlarının sahip olduğu bilgilerin değeri, hem de bu bilgilerin muhafaza edilmesine dair denetim mekanizmasına sahip kurumların varlığı bu kapsamdaki faaliyetleri daha önemli kılmaktadır ve bilgi güvenliği değeri her geçen gün artmaktadır.

Kamu kurumlarında bilgi güvenliğinin muhafaza edilmesi için alınan tedbirler ile yalnızca teknik yöntemlerin oluşturulması ve uygulanmasının yeterli olmadığı görülmüştür. Dolayısıyla kamu kurumlarında bilgi güvenliğinin sağlanması adına teknik sistemlerin, politikaların ve altyapı yatırımlarının yanı sıra insan faktörünün ihmal edilmemesi gerekmektedir. Yapılan araştırmada, kamu kurumlarının bilgi güveliği farkındalığını artırma, politika oluşturma, uygulama ve tedbirler alma konularında pasif kalındığı gözlemlenmiştir. Bu da bilgi güvenliğinin sağlanmasından eksiklikler olduğunu göstermektedir.

Bu nedenle kamu kurumlarında bilgi güvenliği farkındalığının kurumlar için vazgeçilmez bir öneme sahip olması ve devamlı olarak kendilerini yenilemeleri gerekmektedir. Bilgi güvenliği farkındalığını arttırmak amacıyla Diyarbakır'da bulunan kamu kurumlarında yapılan bu araştırmadan elde edilen sonuçlar şöyle özetlenebilir:

Yapılan araştırmada katılımcıların demografik özelliklerinde cinsiyete göre hem bilgi güvenliği farkındalığında hem de faktörlerde, erkeklerin puan ortalaması, kadınlardan daha fazladır. Aynı şekilde yapılan başka bir araştırmaya göre ortaöğretim

öğrencilerine uygulanan bilgi güvenliği farkındalığı belirleme çalışmasında aynı verilere ulaşmışlardır. Ortaöğretim düzeyindeki erkek öğrencilerin bilgi güvenliği konusundaki farkındalık düzeyinin kız öğrencilere göre daha yüksek olduğu tespit edilmiştir (Güldüren, Çetinkaya ve Keser, 2016, s. 692-693). Yine başka bir araştırmaya göre öğretmenlerin dijital veri güvenliği farkındalığı üzerine yapılan çalışma, benzer sonuçları doğrulamaktadır (Yılmaz, Şahin ve Akbulut, 2016, s. 35). Yapılan çalışma sonuçlarına göre, erkek öğretmenlerin dijital veri güvenliği konusundaki farkındalığı, kadın öğretmenlere kıyasla yüksek olduğu tespit edilmiştir. Fakat yapılan araştırmaya göre, kadın öğretmenlerin bilgisayar güvenliğine dair duyarlılıklarının azaldığı tespit edilmiştir (Bostan ve Akman, 2011, s. 51-56). Sonuç olarak araştırmaya göre kadınların bilgi güvenliği konusundaki farkındalık seviyeleri erkeklere göre daha düşük seviyededir.

Kamu kurumlarında çalışanların farklı yaş gruplarından olan katılımcılarının bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Gökmen ve Akgün (2015, s.61-84) yapılan çalışmada yaşın, öğretmen adaylarının bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmadığına ilişkin benzer neticelere ulaşılmıştır. Yine Okul, Şimşek, Hafçı ve Barış (2018, s.189-201) araştırmaya göre, konaklama işletme yöneticilerinde bilgi güvenliği farkındalığını incelediği çalışmasında farklı sonuçlara ulaşılmıştır.

Kamu kurumlarında çalışanların farklı eğitim düzeylerinde olan katılımcılarının bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır ($p>0,05$). Yine daha önce yapılan araştırma sonucuna göre; katılımcıların eğitim durumu ile ilgili bilgi güvenliği konusundaki farkındalıkları istatistiksel olarak anlamlı bir ilişki bulunmamaktadır (Mart, 2012, s. 57-58). Yılmaz, Şahin ve Akbulut (2016, s.26-45)' tarafından yapılan araştırma sonuçlarına göre, öğretmenlerin dijital veri güvenliğini inceledikleri çalışmalarında öğretmenlerin öğrenim durumuna göre farkındalıkları değişmemektedir. Hakan Çetin (2014, s.86-105) tarafından yapılan araştırmaya göre kişisel veri güvenliği ve kullanıcıların farkındalık düzeylerinin incelenmesi amacıyla yapılan araştırma sonucuna göre kullanıcıların eğitim seviyesi ile kişisel veri güvenliği ve farkındalığı arasında istatistiksel olarak anlamlı bir ilişki bulunmamaktadır.

Kamu kurumlarında farklı görevlerde çalışan katılımcıların bilgi güvenliği farkındalıkları arasında istatistiksel olarak anlamlı bir fark tespit edilmemiştir

(p>0,05). İnci Mart (2012, s. 63) tarafından yapılan araştırma sonucuna göre mühendis olan bireylerin, diğer meslek dallarına göre daha yüksek düzeyde bilgi güvenliği farkındalığına sahip olduğu tespit edilmiştir.

Kamu kurumlarında çalışanların görev süresi farklı internet kullanma süreleri olan katılımcıların bilgi güvenliği farkındalıklarında ve bunun birinci faktöründe anlamlı farklılık bulunmaktadır (p<0,05). Katılımcıların interneti 20 yıl ve üzeri daha uzun bir süre kullananlarının, bilgi güvenliği konusundaki farkındalığının diğer katılımcılara göre daha yüksek olduğu tespit edilmiştir. Ancak ikinci faktörde katılımcıların bilgi güvenliği farkındalıkları arasında anlamlı bir fark bulunmamaktadır (p>0,05). Emre Taner (2019, s. 57) tarafından yapılan çalışmaya göre; saldırı ve tehditler konusunda çalışanların görev süreleri ile ilişkili olarak anlamlı bir farklılık gözlenmediğine, fakat görev süresi 8 ve üstünde olan çalışanların, diğer gruplara kıyasla kişisel verilerin korunması konusunda daha yüksek bir farkındalığa sahip oldukları tespit edilmiştir. Başka bir çalışmada ise, kamu kurumlarında grup çalışanları üzerinde yapılan araştırmaya göre, bilgi güvenliği farkındalığı ile çalışanların internet kullanım süreleri arasında anlamlı bir ilişki tespit edilmediğini ortaya koymuştur. (Çöp, 2017, s. 67). Nazlı Başdinkçi (2017, s. 91) tarafından yapılan çalışmada, bilgi güvenliği risk değerlendirmesi yapma ve kullanıcıların bilgi güvenliği farkındalık düzeyini ölçme amacıyla yapılan araştırma sonucunda yapılan araştırmayı destekleyen sonuçlar elde edilmiştir.

Günlük farklı internet kullanım sürelerine sahip katılımcılar arasında, bilgi güvenliği farkındalıkları açısından anlamlı bir fark bulunmamaktadır (p>0,05). Yılmaz, Şahin ve Akbulut (2015, s. 26-45) tarafında yapılan araştırmaya göre öğretmenlerin dijital veri güvenliği farkındalıkları ile günlük internet kullanım süreleri arasında anlamlı bir ilişkinin olup olmadığı belirlemek amacıyla yapılan araştırmanın sonuçları incelediğinde, günlük olarak daha fazla internet kullanan öğretmenlerin, dijital veri güvenliği konusunda daha yüksek bir farkındalığa sahip olduğu araştırma sonuçları ile ortaya konulmuştur. İnci Mart (2012, s. 64) tarafından yapılan araştırmaya göre; bireylerin günlük internet kullanım süreleri ile bilgi güvenliği farkındalıkları arasındaki ilişkiyi inceleyen araştırma sonuçları, benzer bulguları ortaya koymuştur. Sonuç olarak, günlük internet kullanım süresinin, bireylerin bilgi güvenliği konusundaki farkındalıklarını etkilemediğini göstermektedir.

Kamu kurumlarında çalışan personelin bilgi güvenliği farkındalıklarının incelendiği araştırma sonuçlarına göre, bilgi güvenliğinin sağlanması ve korunması için sunulan öneriler şu şekildedir:

- Kamu kurumlarındaki bilgi güvenliği farkındalığı faaliyetleri, uygulamaları ve politikaları yalnızca çalışanlar değil, bütün paydaşları oluşturacak şeklinde yapılması gerekmektedir.
- Kamu personelin üst ve ast ilişkisine ve görev sürelerine ayrıt etmeksizin herkesin bilgi güvenliği farkındalığının sağlanması ve muhafaza edilmesi bilincinin oluşturulması gerekmektedir.
- Kamu kurumlarında teknoloji ile iç içe olan birimlerin ile biraz daha uzak olan birimlerinin bilgi alışverişinde bulunulması gerekmektedir.
- Kamu kurumlarında haftalık veya aylık olarak dünyada meydana gelen teknolojik gelişmelerin ve yeniliklerin kurum çalışanları ile paylaşılması ve bilgilendirilmesi gerekmektedir.
- Kamu kurumlarında bilgi güvenliği farkındalığının saldırılara karşı hazırlıklı olması için, sosyal mühendislik ile tatbikat ve testler yapılması gerekmektedir. Bunun sonucunda personelin eksiklikleri fark edilerek buna göre adımların atılması gerekir.
- Devletin bilgi güvenliği farkındalığın, okullarda ders olarak verilmesi sonucunda bilincin oluşturulması hem kişisel verilerin korunması hem de ilerde kamu çalışanı veya özel sektörde çalışması halinde, bilgi güvenliği tehlikelerin en aza indirilmesi tahmin edilmektedir.
- Kamu kurumlarında bilgi güvenliği farkındalığı ile ilgili eğitimler herkese tek tip verilmemelidir. Çalışan personelin ihtiyaçları, bilgi seviyeleri ve anlama kapasiteleri düşünülerek eğitimlerin planlanması gerekmektedir.
- Türkiye'de kamu kurumlarında bilgi güvenliği farkındalığı hakkında problemler görülmektedir. Kurumların öncelikle farkındalığa yönelik politikaların, uygulamaların, faaliyetlerine ve yasal düzenlemelerin değiştirilmesi gerekmektedir.

Teknolojik gelişmeler sonucunda kamu kurumlarında bilgi güvenliği bir kereye özel olarak yapılacak bir konferans veya seminer olmadığı devamlı olarak gelişen bir süreçtir. Şahinaslan ve arkadaşlarına (2009) göre günümüzde kurumlara yönelik saldırılar artık yıkıcı olmaktan ziyade, daha çok bilgi sızdırma, bilgi hırsızlığı ve istihbarat amaçlı gerçekleştirilmektedir. Bu saldırganların kurumların hassas bilgilerine erişerek, bu bilgileri kötü niyetli amaçlar için kullanmayı hedeflediğini göstermektedir. Bunun için teknolojik yenilikleri takip edilerek ve çalışanlara devamlı ve belirli aralıklarla eğitimlerin verilmesi ve çalışanların gelişmelerden haberdar edilmesi gerekmektedir. Dolayısıyla çalışanların risklerin ve saldırıların farkında olması ve yükümlülüklerin bilincinde olmasıyla sağlanabilecektir. Yapılan araştırmalarda eğitim ve bilgilendirmenin tamamen farkındalığı oluşturmadığını bilimsel çalışmalarda görülmektedir. Kamu çalışanların yeterli bilgi birikime sahip olduğu halde devamlı bir şekilde ekran köşelerinde görünen açıklama ve hatırlatmalar görmezden gelindiği bilinmektedir. Bunun için kamu kurumlarında bilgi güvenliği farkındalığının saldırılara karşı hazırlıklı olması için, sosyal mühendislik ile ilgili personelden habersiz tatbikat ve testler yapılması gerekmektedir.

Kamu kurumlarında bilgi güvenliği farkındalığı devamlı olarak yapılması, yeniliklere adapte olmak, devamlı olarak değişime ve adaptasyona açık olunmalıdır. Çünkü teknolojik gereksinimler sürekli değişmektedir. Bilgi güvenliği yalnızca teknik önlemler ve ağ korunması değildir. Çünkü bilgi güvenliği teknoloji, insan ve devamlılık üçlüsünün bir ahenk için çalışması gereken bir sistemdir. Kurum çalışanların iş hayatlarında alışması gerenken, önemsenmesi, desteklenmesi ve devamlılık arz eden bir süreçtir. Bunun için çalışanlara korkuyla, yıldırmayla veya ceza ile değil saygı, sevgi, eğitimle ve bilincin oluşturmasıyla kazanılabilir.

Evrak Tarih ve Sayısı: 27.03.2024-E.150305

T.C.
BINGÖL ÜNİVERSİTESİ REKTÖRLÜĞÜ
Sosyal ve Beşeri Bilimler Bilimsel Araştırma ve Yayın Etiği Kurulu

Sayı :33117789/302.01.08/150305 28.03.2024
Konu :Etik Kurul İzni

ENSTİTÜLERE
(SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ)

İlgi :
08.03.2024 tarihli ve E-40711683-302.01.08-149193 sayılı yazınız.

Sosyal Bilimler Enstitüsü Müdürlüğü tarafından Kurulumuza sunulan "Kamu Harcamalarında Çalışanların Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Diyarbakır Örneği" isimli araştırma Kurulumuz tarafından etik yönden değerlendirilmiştir. Değerlendirme sonucunda; söz konusu anket çalışmasının Üniversitemiz Etik Kurul Yönergesi ilkeleri çerçevesinde değerlendirilmiş ve araştırma etiği açısından "UYGUN OLDUĞUNA" oy birliği ile karar verilmiştir.

e-imzalıdır
Prof. Dr. Hamza ALTIN
Kurul Başkanı

e-imzalıdır
Prof. Dr. Abdulnasır SÜT
Üye

e-imzalıdır
Prof. Dr. Ervin ERKAN
Üye

e-imzalıdır
Prof. Dr. Sabip BEROJE
Üye

e-imzalıdır
Prof. Dr. Sait PATIR
Üye

e-imzalıdır
Prof. Dr. Sıtkı ULUERLER
Üye

e-imzalıdır
Prof. Dr. Yaşar BAŞ
Üye

e-imzalıdır
Dr. Öğr. Üyesi Fatma GÖRGÜLÜ
Raportör

18.03.2024 Kur.Bşk : Prof. Dr. H.ALTIN

Sosyal ve Beşeri Bilimler Bilimsel Araştırma ve Yayın Etiği Kurulu Bingöl Üniversitesi Rektörlüğü Selahaddin-i Eyyübi Mah. Üniversite Cad. No:1 BİNGÖL/TÜRKİYE
Tel:0426 216 00 12-13-14-15 Faks:0426 215 10 20
E-Posta :basinyayin@bingol.edu.tr Elektronik Ağ :www.bingol.edu.tr

KAYNAKÇA

Adress, Jason, (2011), *The Basics of İnformation Security,* 1. Basım. United State: Elsevier, s. 5.

Akalp, Gizem ve Yamankaradeniz, Nürettin, (2013), *İşletmelerde Güvenlik Kültürünün Oluşumunda Yönetimin Rolü ve Önemi,* Sosyal Güvenlik Dergisi, 3(2), s. 96-109.

Akbulut, Bilal, (2015), *Güvenlik,* Ankara, Barış Kitap.

Al-Awadi, Maryam, ve Karen, Renaud, (Ekim, 2012), *Success factors in İnfarmation Security mplementation İn Organization*, 1 Mayıs 2023, Karen/papers/Success factors2.pdf : http://www.dcs.gla.ac.uk adresinden alındı.

Albrechtsen, Eirik, (2007), *A qualitative study of users' view on information security.* Computer&Security, *26*(4), s.276-289.

Alemdaroğlu, Aykut, (2020), *Çalışanların Bilgi Güvenliği Farkındalığına İlişkin Algıları: Bankacılık Sektöründe Bir Araştırma*, İstinye Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Alkan, Mustafa, Atalay, Ahamet Hamdi, Canbek, Gürol, ve Bilirgen, Cabir (2012), *Türkiye Ulusal Siber Güvenlik Stratejisi Önerisi. Proje: Ulusal/Uluslararası Siber Güvenlik,* Bilgi Güvenliği Derneği, s.1-34.

Al-Shehri, Yahia, (2012), *Information security awareness and culture*. British Journal of Arts and Social Sciences, *6*(1), s. 61-69.

Atabek, Ümit, (2001), *İletişim ve Teknoloji: Yeni Olanaklar Yeni Sorunlar,* Ankara, Seçkin Yayıncılık.

Başdinkçi, Nazlı, (2017), *Sağlık Kurumlarında Bilgi Güvenliği Risk Değerlendirmesi ve Kullanıcıların Bilgi Güvenliği Farkındalık Düzeyini Ölçme,* Çukurova Üniversitesi, Fen Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Adana.

Bensghir, Türksel, Kaya (2011), *Kurumsal Bilgi Güvenliği Yönetim Süreci*, *Bilgi Yönetimi Semineri*, s. 1-99.

Bergnet(Timus), (Nisan, 2023), *Kötü Amaçlı Yazılımlar.* 4 Mayıs 2023, berqnet: https://berqnet.com/blog/kotu-amacli-yazilimlar adresinden alındı.

Karel, (Ocak, 2023), *Bilgi Güvenliği Nedir? Bilgi Güvenliği Nasıl Sağlanır?*, 1 Şubat 2023, Karel: https://www.karel.com.tr/blog/bilgi-guvenligi-nedir-bilgi-guvenligi-nasil-saglanir adresinden alındı.

Bogart, John Kelley, (Ekim, 2012), *Docs/Whitepepers/IS_Awrenes.pdf* . Information security awareness: How to get users asking for more, 5 Mayıs 2023, http://iasec.eller.arizona.edu/. adresinden alındı.

Bostan, Atila ve Akman, İbrahim, (2011), *Bilişim güvenliği: Kullanıcı Açısından Bir Durum Tespiti,* IV. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, s. 51-56.

Boujettif, Mohammed ve Wang, Yonggee (Ekim, 2012), *Constructivist approach to information security awareness in the Middle East.* Stamp/Stamp.jsp?tp=&arnu ber=633845 : http://ieeexplore.ieee.org adresinden alındı.

Brakensiek, Fay C, (2002), *Knowledge Management For EHS Professionels,* Healt Safety, s. 72-74.

Büyüköztürk, Şener, (2002), *Faktör Analizi: Temel Kavramlar ve Ölçek Geliştirmede Kullanımı,* Kuram ve Uygulamada Eğitim Yönetimi, (32), s. 470-483.

Canbek, Gürol (2005), *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme,* Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Canbek, Gürol ve Sağıroğlu, Şeref, (2006), Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, *9* (3), s.165-174.

Canbek, Gürol ve Sağıroğlu, Şeref (2006), *Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar Yöntemleri,* Ankara, Grafiker Yayıncılık.

Canbek, Gürol ve Sağıroğlu, Şeref, (2007), Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme, Kayseri, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 33(2), s.1-12.

Canbek, Gürol ve Sağıroğlu, Şeref, (2007), Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma, Gazi Üniversitesi Mühendislik Mimarlık Falüktesi Dergisi, 22(1), s.121-136.

Cavus, Nadire, ve Ercag, Eric (2016), The scale for the self-efficacy and perceptions in the safe use of the Internet for teachers: The validity and reliability studies. British Journal of Educational Technology, s.76-90.

Coinwhales, (Eylül, 2023), *Bilgi Güvenliği Nedir ve Bir Kurum İçin Neden Hayati Önem Taşır,* 1 Eylül 2023, Steemit: (https://steemit.com/staj/@coinwhales adresinden alındı.

Cox, Sue & Flin, Rhona, (1998), *Safety culture: Philosopher's stone or man of straw?, Work & Stress,* An International Journal of Work, Health & Organisations, 12(3), s.189-201.

Çalışkan, Emin, (2013), *Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği,* İstanbul Bilgi Üniversitesi Sosoyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

Çek, Eray, (2017), *Kurumsal Bilgi Güvenliği Yönetişim ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans, İstanbul.

Çelik, Çiğdem ve Yarar, Onur, (2019), *Kalite Yönetim Direktörlerinin Bilgi Güvenliği farkındalığı: İstanbul İli Örneği,* Sağlıkta Performans ve Kalite Dergisi,17(2), s. 29-48.

Çetin, Hakan, (2014). *Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin incelenmesi,* Akdeni, Akdeniz Üniversitesi İktisadi Ve İdari Bilimler Fakülte Dergisi, 14(29), s. 86-105.

Çetinkaya, Levent, Güldüren, Can ve Keser, Hafize, (2017), *Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması,* Milli Eğitim Dergisi, 46(216), s. 33-52.

Çöp, Çiğdem Çelik, (2017), *Kalite Yöneti Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği,* Okan Üniversitesi Sağlık Bilimleri Esntitüsü, Yayımlanmamış Yüksek Lisans Tezi İstanbul.

Davenport , Thomas H, & Prusak, Laurence, (2001), *İş Dünyasında Bilgi Yönetimi: Kuruluşlar Ellerindeki Bilgiyi Nasıl Yönetirler*, (G. Günay, Çev.) İstanbul, Rota yayınları.

Dikmen, Tahir, (2023, Ocak 12), *Remote Access Trojan (RAT) Nedir?* BTK Akademi: https://www.btkakademi.gov.tr/portal/blog/remote-access-trojan-rat-nedir-1550 adresinden alındı.

Doğantimur, Fatma (2009). *ISO 27001 standardı çerçevesinde kurumsal bilgi güvenliği,* TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Mesleki Yeterlilik Tezi, *Ankara.*

Dursun, Salih. (2011). *Güvenlik Kültürünün Güvenlik Performansı Üzerine Etkisine Yönelik Bir Uygulama,* Uludağ Üniversitesi Sosyal Bilimler Enstitüsü,Yayınlanmamış Doktora Tezi. Bursa.

Elbahadır, Hamza (2023). *Hackıng Interface,* İstanbul, Kodlab, (02.Ocak.2023) Dergi Park Akademik.

Elbir, Sait, (2020). *Worm (Solucan) Nedir?* Teknorun, 8.Nisan.2023 https://www.teknorun.net adresinden alındı.

Eminağaoğlu, Mete, (2008), Dikkat Casus Var! Bilgi Güvenliği Yazı Dizisi, Tekborsa Dergisi(15),

Eminağaoğlu, Mete ve Gökşen, Yılmaz, (2009), *Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri,* Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü Dergisi, 11(4), s.1-15,

E-Posta Güvenliği. (Nisan, 2023), uzmanposta, 1 Nisan 2023, (https://uzmanposta.com/blog/ransomware/.adresinden alındı.

Gazdağı, Oya ve Çetinyokuş, Tahsin, (2020), *Bankacılık Sektöründe Bilgi Güvenliği ve İş Sürekliğinin Sağlanması Amacıyla ISO/IEC 27001 ve ISO 22301 Standartlarının Uygulanmasına Yönelik Kavramsal İnceleme,* Journal of Humanities and Tourism Research, 10(2), s. 475 - 491.

Gelbstein, Eduardo & Kamal, Ahmad (2002). *Information Insecurity. New York.* United Nations ICT Task Force and the United Nations Institute for Training and Research.

Glass, House, (2023), *Siber Saldırıdan Korunmanın Yolları*, 1 Mayıs 2023, https://www.glasshouse.com.tr adresinden alındı.

Göçoğlu, Volkan, (2014). *Kamu Politikası ve Sosyal Medya İlişkisi,* Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Gökmen, Ömer Faruk ve Akgün, Özcan Erkan (2015). *Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi*, Adana, Çukurova Üniversitesi Eğitim Fakültesi Dergisi, 44(1).s.61-84.

Güldüren, Can, Çetinkaya, Levent ve Keser, Hafize, (2016), *Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması,* İlköğretim Online, 15(2), s.692-693.

Gülmüş, Mustafa, (2010). *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği.* İstanbul Yıldız Teknik Üniversitesi Fen Bilimler Ensitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul .

Güngör, Murat, (2015), *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma.* T.C Kalkınma Bakanlığı Bilgi Toplumu Daire Başkanlığı, Uzmanlık Tezi, Ankara.

Hekim, Hakan ve Başıbüyük, Oğuzhan, (2013). *Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları,* Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), s.135-157.

Henkoğlu, Türkay ve Yılmaz, Bülent, (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları, Türk Kütüphaneciliği, *27*(3), s. 451-471.

Hey, Jonathan, (2004), *The Data, Information, Knowledge, Wisdom Chain*. The Metaphorical, 1 Şubat 2023, http77www.dataschemata.com adresinden erişildi adresinden alındı.

ISO, (2005), *International Organization for Standardization.* ISO/IEC 27001.

Johnson, M. Eric, & Goetz, Eric (2007). *Embedding information security into the organization.* IEEE Security & Privacy, 5(3), s. 16-24.

Karakoç, Mehmet Ali, (2011), *Bilişim Suçlarına Genel Bakış, Bilişim Suçlarını Önleme Çalışmaları ve Güvenli İnternet Kullanımı,* Suç Önleme Sempozyumu Bildiriler Kitabı, Bursa, s. 419-423.

Karakuzu, Özkan. (2015)., *Bilgi Toplumu Dönüşüm Sürecinde E - Devlet Kavramının Siber Ülke Güvenliği Açısından Değerlendirilmesi,* İnönü Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Malatya.

Karaoğlan Yılmaz, Fatma Gizem, Yılmaz, Ramazan, ve Sezer, Barış (2014), Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış, Bartın Üniversitesi Eğitim fakültesi Dergisi. *3*(1), s.179-199.

Kasıkcı, Duygu Nazire, Çağıltay, Kürsat, Karakuş, Türkan, ve Ogan, Christine. (2014), Türkiye ve Avrupa'daki Çocukların İnternet Alışkanlıkları ve Güvenli İnternet Kullanım, Eğitim ve Bilim Dergisi,*39*(171), s. 230-243.

Kaya, Ali ve Mursül, Damla, (2019), *Ulusal Bilgi Güvenliği Politikaları Açısında Kamu Kurumlarının İncelenmesi: Kayseri Örneği,* Assam Uluslararası Hakem Dergisi Özel Sayısı, s. 331-343.

Keser, Hafize ve Güldüren, Can, (2015), *Öğretmenler İçin Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması(BGFÖ),* K.Ü.Kastamonu Eğitim Dergisi, 23(3), s. 1167-1184.

Kınay, Hüseyin, (2012), *Lise Öğrencilerinin Siber Zorbalik Duyarlılığının Riskli Davraniş, Korumacı Davranış, Suça Maruziyet ve Tehlike Algısı İle İlişkisi ve Çeşitli Değişkenler Açısından İncelenmesi.* Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Sakarya.

Kırışık, Fatih ve Sezer, Özcan, (2015), *Bilgi ve İletişim Teknolojilerinin (BİT) Kamu politikası Oluşturma Sürecindeki Rolü,* Ekonomik ve Sosyal Araştırmalar Dergisi,11(2), s.199-216.

Kjorvik, Hallvard, (2010), *Implementing and improving awareness in information security, 1 Şubat 2024,*

https://grimstad.uia.no/ikt590/ikt10/g06/Masteroppgave.pdf adresinden erişildi.

Kuru, Hüseyin ve Ocak, Mehmet Akif (2016), *Determination of Cyber Security Awareness of Public Employees and Consciousness-rising Suggestions,* Journal of Learning and Teaching in Digital Age, 1(2), s.57-65.

LİM, Joon Soon, Chang, Shaton, Maynard, Sean B, & Ahmad, Atif (2009), *Exploring the relationship between organizational culture and information security culture.*

Mart, İnci, (2012), *Bilişim Kültüründe Bilgi Güvenliği Farkındalığı,* Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Kahramanmaraş.

Maynard, Sean B, Ruighaver, Anthonie Bastian, & Chia, P.A (2002), *Exploring organisational security culture*: Developing a comprehensive research model. In Proceedings.

Media, Byc, (Haziran, 2023), *Bilgisayarda Virüs Olduğu Nasıl Anlaşılır ve Temizlenir?* Byc Media, 1 Haziran 2023, https://www.bycmedia.com/blog/bilgisayarda-virus-oldugu-nasil-anlasilir-ve-temizlenir adresinden alındı.

Mitnick, Kevin David, (2005), *Aldatma Sanatı,* Ankara, ODTÜ Geliştirme Vakfı Yayıncılık.

Mitnick, Kevin David & Simon, W. L. (2016). *Aldatma Sanatı* (6 b.). (N. E. Tezcan, Çev.) Ankara, ODTÜ Yayıncılık.

Munro, Kyle, (2005), Social engineering, Infosecurity Today, 2(3), s.44.

Nezgitli, Sena, (2022), *Kamu Kurumu ve Özel Sektöre Yönelik Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme.* Gazi Üniversitesi Bilişim Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara

Okul, Turan, Şimşek , Güntekin, Hafçı , Büşra ve Barış , Zafer (2018). *Bilgi Güvenliği Farkındalığı: Kuşadası'ndaki Konaklama İşletmesi Yöneticileri Üzerine Bir Uygulama*, Uluslararası Türk Dünyası Turizm Araştırmaları Dergisi, 3(2), s.189-201.

Öğütçü, Gizem, (2010), *E-dönüşüm sürecinde kişisel bilişim güvenliği davranışı ve farkındalığın analizi,* Başkent Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Özbilen, Tuba ve Çağlar, Ali, (2020), *Türk Kamu Sektöründe Bilgi ve Bilişim Güvenliği*, Kamu Yönetimi ve Teknoloji Dergisi 2, s.72-94.

Özdemir, Ayşe, (2019), *Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı,* Gazi Üniversitesi Bilişim Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara.

Özdemir, Ayşe ve Uluyol, Çelebi, (2020), *Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı*, Türkiye Sosyal Araştırmalar Dergisi(3), s. 649-666.

Özkan, Türker & Lajunen, Timo, (2003), *Güvenlik Kültürü ve İklimi,* Pivolka, 2(10), s.3-4.

Özkaya, Erdal, Sarıca, Raif ve Durmaz, Şükrü, (2019), *Siber Güvenlik Saldırı & Savunma Stratejileri,* Ankara, Buzdağı Yayınevi.

Öztemiz, Semanur ve Yılmaz, Bülent, (2013), *Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği,* Ankara, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Bilgi Dünyası, 14(1), s.87-100.

Parsons, Kathryn, McCormac, Agata, Pattinson, Malcolm, Butavicius, Marcus, ve Jerram, Cate, (2014), *A study of information security awareness in Australian government organisations.* Information Management ve Computer Security, 22(4), s. 334-345.

Resarch, Osterman (2020), *State of Privacy and Security Awareness Report*, 1 Mart 2024, https://www.bsigroup.com/globalassets/localfiles/en-ie/our_services/mediapro/2020_state_of_privacy_security_awareness_report_mediapro.pdf adresinden alındı.

Richardson, Ransom, (2008), *2008 CSI/FBI Computer Crime & Security Survey, CSI,*

SANS, (2021), Security Awareness Report, 1 Mart 2024, https://www.sans.org/securityawareness-training/resources/reports/sareport adresinden alındı.

Shehri, Yasser Ali, & Clarke, Nathan L, (2007), *Information security awareness and culture. P. Dowland ve S. Furnell (Eds.).* Advances in Networks, Computing and Communications, 6, s.12-22.

Sparrow, John, (1998), *Knowledge in Organizations: Access to thinking at work* (1 b.). London, Sage Publication.

Şahinaslan, Ender, Kandemir, Rembiye ve Şahinaslan, Önder, (2009), *Bilgi Güvenliği Farkındalık Eğitim Örneği.* IV. Akademik Bilişim Konferansı Bildirileri , Şanlıurfa, 11-13 Şubat 2009 Harran Üniversitesi. s. 189-194.

Şahinaslan, Ender, Kantürk, Arzu, Şahinaslan, Önder ve Borandağ, Emin, (2009). *Kurumlarda Bilgi Güvenliği Farkındalığı,Akademik Bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri,11-13 Şubat 2009 Harran Üniversitesi, s.597-602, Şanlıurfa.*

Şahinaslan, Önder, (2013), *Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma,* Trakya Üniversitesi Fen Bilimleri Enstitüsü,Yayınlanmamış Doktora Tezi, Edirne.

Şanagil, Sinem, (2017), *Kamu Politikası Oluşturma Sürecinde Bilgi ve İletişim Teknolojileri: E-Devlet uygulamaları, Mersin*, Mersin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 1(1), s.77-89.

Şeremet, Özgür, (2019), *Bilgi Güvenliği ve Gizliliği Sunumu,* 26 Haziran 2019, https://ozgurseremet.com adresinden alındı.

T.S.E. (2006), *Türk Standardı TS ISO/IEC 27001,* Ankara.

Taner, Emre, (2019), *Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığına Yönelik Bir Betimleme,* Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmamış Yüksek LisansTezi, Afyon.

Taş, Kezban Ataçlıç (2010), *Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi,* Çukurova

Üniversitesi Sağlık Bilimleri Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Adana.

Taş, Sibel, (2023), *Zararlı Yazılım Analiz Teknikleri,* Web Hosting A.Ş., 3 Nisan 2023, https://www.hosting.com.tr adresinden alındı.

Tectharget,(Nisan, 2023), *Trojan Virüs Tehdidi,* Depositphotos Inc., USA, 3 Nisan 2023, https://depositphotos.com.tr adresinden alındı.

Tekerek, Mehmet, (2008), *Bilgi Güvenliği Yönetimi,* Kahramanmaraş Sütçü İmam Üniversitesi Fen ve Mühendislik Dergisi, 11(1), s.132-137.

Tekerek, Mehmet, ve Tekerek, Adem. (2013), Öğrencilerin Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma,Turkish Journal of Education, 2(3), s.61-70.

Timus(Bergnet), (2020). *Kötü Amaçlı Yazılımların Aktiviteleri ve Sistemlerdeki Etkileri Nelerdir?*, Timus(bergnet), 1 Ekim 2023, https://berqnet.com/blog/rootkit adresinden alındı

Tipton, Harold F.& Krause, Micki, (2007), *Information Security Management Handbook,* Auerbach Publicaions.

Turhan, Meltem, (2010), *Siber Güvenliğin Sağlanması, Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri,* Bilgi Teknolojileri ve İletişim Kurumu Uzmanlık Tezi, Ankara.

TÜBİTAK, (Mayıs, 2023), *Siber Güvenlik Enstitüsü Eğitimleri*. TÜBİTAK BİLGEM, 1 Mayıs 2023, https://bilgem.tubitak.gov.tr/sge-egitimleri adresinden alındı

Ulaşanoğlu Emin, Yılmaz, Ramazan ve Tekin, Mehmet Alper, (2010), *Bilgi Güvenliği: Riskler ve Öneriler,* Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Uluyol, Çelebi, ve Demirci, Mehmet, (2022), *Siber Güvenlik Lise,* Ankara, TÜBİTAK Deneyap Kitapları 10, s. 1-121

Uzman Postas (2023). *Ransomware Nedir, Nasıl Çalışır? Ransomware Virüsünün Mail Yoluyla Bulaşmasını Engelleme.* Uzman Posta Sitesi, 18 Mayıs 2023, https://uzmanposta.com/blog/ransomware/ adresinden alındı.

Ünver, Mustafa, Canbay, Cafer, & Mirzaoğlu, Ayşe Gül (2009), *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,* Bilgi Teknolojileri veİletişim Kurumu, Bilgi Teknolojileri ve Koordinasyon Dairesi, Ankara.

Vardal, Necla (2009), *Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulamas,* Gazi Üniversitesi Eğitim Bilimleri Enstitüsü, Yayımlanmamış Doktora Tezi, Ankara.

Vroom, Cherly, & Von Solms, Rossouw, (2004). Towards İnformation Security. Behavioral Complience, Computer&Security, *23*(195), s.222-240.

Vural, Yılmaz, (2007), *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri,* Gazi Üniversitesi Fen Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Vural, Yılmaz ve Sağıroğlu, Şeref, (2008), Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), s.1-16.

Wright , Marie A. & Kakalik, John S., (2010). *Information security: Contemporary cases.* Jones & Bartlett Learning.

Yaşar, Hakan, ve Çakır, Hüseyin, (2015), *Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri,* Düzce Üniversitesi Bilim Ve Teknoloji Dergisi, 3(2), s. 488-507.

Yavanoğlu, Uraz, Sağıroğlu, Şeref, ve Çolak, İlhami (2012). *Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler*. Politeknik Dergisi, 15(1), s.15-27.

Yıldırım, Ömer, (2019), *Blgi Nedir?* Felsefe, 01 Ekim 2023, https://www.felsefe.gen.tr/bilgi-nedir-ne-demektir/ adresinden alındı.

Yıldız, Mithat, (2014), *Siber Suçlar ve Kurum Güvenliği.* Ulaştırma Denizcilik ve Haberleşme Bakanlığı Bilgi İşlem Dairesi Başkanlığı Uzmanlık Tezi, Ankara.

Yilmaz, Bilgen, (2013), *E-Dönüşüm Sistemlerinin Bilgi Güvenliği Açısından İncelenmesi E-Devlet Kullanıcıları Üzerine Bir Araştırma,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi. İstanbul.

Yılmaz, Bülent, (1998), *Bilgi Toplumu: Eleştirel Bir Yaklaşım,* Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi, 15(1), s.147-158.

Yılmaz, Eray, Şahin, Yusuf Levent ve Akbulut, Yavuz, (2016), *Öğretmenlerin Dijital Veri Güvenliği Farkındalığı,* Sakarya University Journal of Education, 6(2), s. 26-45.

Yılmaz, Sait ve Salcan, Olay, (2008), *Siber Uzay'da Güvenlik ve Türkiye*, İstanbul, Milenyum Yayınları.

EKLER

Ek-1: Kişisel Bilgiler

Sayın Katılımcı;

Bu anket, Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Siyaset Bilimi ve Kamu Yönetimi Bölümü'nde hazırlanmakta olan "Kamu Kurumlarında Çalışanların Bilgi Güvenliği Farkındalığı Üzerine Bir Araştırma: Diyarbakır Örneği" başlıklı Yüksek Lisans tez çalışmasında kullanılacaktır. Çalışmanın amacına ulaşması sizlerin değerli katılımlarına bağlıdır. Bu nedenle soruları dikkatli okumanız ve cevaplamanız büyük önem taşımaktadır. Ankette, 7 adet kişisel bilgilere ilişkin soru ile 24 adet bilgi güvenliğine ilişkin soru olmak üzere toplamda 31 soru yer almaktadır.

Katkılarınız için şimdiden teşekkür ederim.

İslam ACAR

Kişisel Bilgiler

Aşağıda bazı kişisel bilgilere ilişkin sorular yer almaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) işareti koyunuz.

1. Cinsiyet? [] Kadın [] Erkek
2. Yaşınız? **[]** 20-34 [] 35-44 [] 45-54 [] 55-
3. Eğitim Durumu? [] İlköğretim-Orta Öğretim [] Lise [] Ön lisans [] Lisans [] Lisans Üstü
4. Çalıştığınız kamu kurumdaki göreviniz? [] Yönetici [] Akademik Personel [] Memur [] İdari Personel [] Diğer
5. Kamu kurumdaki görev süreniz? [] 1-5 yıl [] 6-10 yıl [] 11-15 yıl [] 16-20 yıl [] 20 yıl üzeri
6. Ortalama kaç yıldır internet kullanıyorsunuz? [] 0-5 yıl []6-10 yıl [] 11-15 yıl [] 16-20 yıl [] 20 yıl üzeri
7. Günlük internet kullanım süreniz nedir? []1-3 saat []4-6 saat [] 7-9 saat [] 9 saat ve üzeri

Ek-2: Bilgi Güvenliği Farkındalığı ile İlgili Sorular

Aşağıda kamu kurumlarında çalışanların bilgi güvenliği farkındalığına ilişkin sorular sorulmaktadır. Size yöneltilen her soru için durumunuza en uygun seçeneğin karşısına (X) işareti koyunuz.

	Bilgi Güvenliği Farkındalığı ile İlgili Sorular	**Kesinlikle Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Kesinlikle Katılıyorum**
1	Bilgi güvenliğinin ne olduğunu biliyorum.					
2	Bilgi güvenliği ile ilgili yükümlülüklerimin ne olduğunu biliyorum.					
3	Kamu kurumlarında bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
4	Kamu çalışanlarının kullanıcı adı-parola vb. gizli bilgilerini masa üzerinde yazılı biçimde tutmamaları gerektiğini biliyorum.					
5	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
6	Dijital imzanın ne olduğunu biliyorum.					
7	Kamu çalışanlarının bilgisayarın başından ayrılırken oturumu (**Windows + L**) kilitlemeleri gerektiğini biliyorum.					
8	İstenmeyen elektronik postanın (spam) ne olduğunu biliyorum.					
9	Kurum bilgisayarlarında program kurma özelliğinin açık ve gözetimsiz bırakılmaması gerektiğini biliyorum.					
10	Kurumsal bilgi ve belgeleri telefonda veya sosyal ağlarda kimliğinden emin olmadığım kişilerle paylaşmamam gerektiğini biliyorum.					
11	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
12	Kamu çalışanlarının kritik bilgi ve belgeleri yazıcı, faks ve tarayıcı makinesi üzerinde unutmamaları gerektiğini biliyorum.					
13	Sosyal ağlarda kimlik sahteciliği yapıldığını biliyorum.					
14	Çalışma ortamından ayrılırken gizli bilgi içeren dokümanların kilitlenmesi gerektiğini biliyorum.					
15	Kötü niyetli yazılımlara karşı alınması gereken güvenlik tedbirlerini biliyorum.					
16	Bilgisayarımda casus/köstebek yazılım olup olmadığını anlayabilirim.					
17	Kamu kurumuna ait hizmete özel ve üstü gizlilik sınıfında olan herhangi bir bilginin internette yayılmaması ve sosyal medya ortamlarında paylaşılmaması gerektiğini biliyorum.					
18	Kimlik hırsızlığının ne olduğunu biliyorum.					
19	Suç teşkil edecek nitelikte ve içerikteki dosyaların kurum bilgisayarlarında kullanılmaması gerektiğini biliyorum.					

20	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
21	Türkiye Cumhuriyeti kanunlarında engellenen veya kısıtlanan web sitelerine bağlanılmaması gerektiğini biliyorum.					
22	Bilgi sistemlerini tehlikeye atacak erişimlerin gerçekleştirilmemesi gerektiğini biliyorum.					
23	Sosyal mühendislik saldırısının ne olduğunu biliyorum.					
24	Kamu çalışanlarının kaynağından emin olmadığı kablosuz ağlara bağlanmamaları gerektiğini biliyorum					