
GAZİ ÜNİVERSİTESİ
Gazi
1926

KAMU KURUM VE KURULUŞLARINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI

Ayşe ÖZDEMİR

YÜKSEK LİSANS TEZİ

ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

ARALIK 2019

Ayşe ÖZDEMİR tarafından hazırlanan " KAMU KURUM VE KURULUŞLAEINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI " adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Çelebi ULUYOL
Eğitim Fakültesi, Bilgisayar ve Öğretim Teknolojisi Eğitimi, Gazi Üniversitesi

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

Başkan: Dr. Öğr. Üyesi Bülent TUĞRUL
Mühendislik Fakültesi, Ankara Üniversitesi

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

Üye: Dr. Öğr. Üyesi Uraz YAVANOĞLU
Mühendislik Fakültesi, Gazi Üniversitesi

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

Tez Savunma Tarihi: 05/12/2019

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

……

…….……

Doç. Dr. Aslıhan TÜFEKCİ
Bilişim Enstitüsü Müdürü

ETİK BEYAN

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

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

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

Ayşe ÖZDEMİR
...../……/……

KAMU KURUM VE KURULUŞLARINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI

(Yüksek Lisans Tezi)

Ayşe ÖZDEMİR

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Aralık 2019

ÖZET

Bu çalışmanın amacı kamu çalışanlarının bilgi güvenliği farkındalıklarını ortaya koymaktır. Araştırma nicel araştırma yöntemlerinden betimsel yöntem tarama çalışmasıdır. Literatür taramasında daha önce öğretmenler, öğrenciler, öğretim görevlileri gibi çeşitli gruplar için gerçekleştirilmiş ölçekler incelenmiştir. Veri toplama aracı olarak Bilgi Güvenliği Farkındalık Ölçeği kullanılmıştır. Ölçeğin Cronbach alfa güvenilirlik katsayısı ,97' dir. Yapılan bu çalışmada da bir kez daha Cronbach alfa güvenilirlik katsayısı ölçeğin tümü için ,97 olarak hesaplanmıştır. Ölçek otuz dört soru ve iki alt boyuttan oluşmaktadır. Ölçekte ilk alt boyut saldırı ve tehditler, ikinci alt boyut kişisel verilerin korunmasıdır. Veri toplama işlemi 501 kamu çalışanı ile gerçekleştirilmiştir. Çalışanlardan cinsiyet, yaş aralığı, eğitim durumu ve çalıştığı birim olmak üzere çeşitli bilgiler ile ölçek sorularını cevaplamaları istenmiştir. Çalışma sonunda kamu çalışanlarının ölçek genelinden aldıkları ortalama puana göre orta seviyede bilgi güvenliği farkındalığına sahip oldukları görülmüştür. Katılımcılarımızdan erkek ve kadın katılımcılar arasında benzer seviyede bilgi güvenliği farkındalığına sahip oldukları, 40 yaş altı katılımcılar ile teknik eğitim almış olan Bilgi Teknolojileri çalışanlarının bilgi güvenliği farkındalık seviyelerinin yüksek olduğu görülmüştür. Ayrıca çalışmada üniversite düzeyinde eğitim seviyesine sahip olan katılımcılarımızın lise ve altı eğitim seviyesine sahip olan katılımcılardan daha yüksek bilgi güvenliği farkındalığına sahip oldukları görülmüştür. Ülke genelinde kamu çalışanlarının bilgi güvenliği farkındalıklarının artırılmasına yönelik yapılması gereken çalışmalar ve eğitimler konusunda çeşitli önerilerde bulunulmuştur.

Bilim Kodu : 92401

Anahtar Kelimeler : Bilgi güvenliği, farkındalık, kamu çalışanı

Sayfa Adedi : 90

Danışman : Doç. Dr. Çelebi ULUYOL

INFORMATION SECURITY AWARENESS IN PUBLIC INSTITUTIONS AND ORGANIZATIONS

(M. Sc. Thesis)

Ayşe ÖZDEMİR

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

December 2019

ABSTRACT

The aim of this study is to reveal the information security awareness of public employees. The research is a descriptive survey model. In the literature review, the scales previously performed forvarious groups such as teachers, students and lecturers were examined. Information Security Awareness Scale was used as data collection tool. The Cronbach's alpha reliability coefficient of thescalewas 97. In this study, Cronbach alpha reliability coefficient was once again calculated as 97 forthe whole scale. The scale consists of thirty-four questions and two sub-dimensions. The first sub-dimension of the scale is attacks and threats, and the second sub-dimension is the protection of personal data. Data collection was carried out with 501 public employees. The employees were asked to answer the questions of the scale, including gender, age range, education and unit where they worked. At the end of the study, it was seen that public employees had a moderate level of information security awareness based on the average score they received from the over all scale. Among the participants, male and female participants had a similar level of information security awareness and the information security awareness levels of Information Technology employees who were under the age of 40 with technical training were high. In addition, it was seen that the participants who have university level education have higher information security awareness than those who have higher education level or lower. Various recommendations have been made about the studies and trainings to increase the awareness of public employees on information security across the country.

Science Code : 92401
Key Words : Information security, awareness, public employee
Page Number : 90
Supervisor : Doç. Dr. Çelebi ULUYOL

TEŞEKKÜR

Bu tezin belirlenmesi ve hazırlanması sürecinde değerli katkı ve yönlendirmeleriyle her zaman desteğini çok yakından hissettiğim, önerilerinden faydalandığım danışman hocam Sayın Doç Dr. Çelebi ULUYOL' a, kamu çalışanlarına ölçeğin uygulanması sürecinde bana yardımcı olan çalışmama destek veren tüm kamu kurum ve kuruluşları yönetici ve çalışanlarına, Yüksek Lisans eğitimim süresince sabırla maddi manevi her türlü destekleriyle beni hiçbir zaman yalnız bırakmayan çok değerli ailem ile işyerinde abla ve abi bildiğim iş arkadaşlarıma teşekkür ve şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİNLİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar ve açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri
ANOVA	Tek yönlü varyans analizi
APT	Advanced persistent threat
ARPA	Araştırma Projeleri Kurumu
ARPANET	İleri Araştırma Projeleri Ağı
BGFÖ	Bilgi güvenliği farkındalık ölçeği
CERN	Avrupa Nükleer Araştırma Merkezi
CSW	Bilgi Güvenliği Haftası
DDoS	Dağıtık hizmet saldırısı
ENISA	Avrupa Ağ ve Bilgi Güvenliği Ajansı
ITU	Uluslararası Telekomünikasyon Birliği
MEB	Milli Eğitim Bakanlığı
TAIS	İnternet güvenliğinde öğretmen farkındalığı
TDK	Türk Dil Kurumu
TÜİK	Türkiye İstatistik Kurumu
WWW	World Wide Web
BBK	Federal Nüfus ve Afet Yardım Bürosu

1.GİRİŞ

Bilgi ve iletişim teknolojilerindeki gelişmeler günlük hayatımızı kolaylaştırmakta ve sağladığı imkânlarla kendini vazgeçilmez hale getirmektedir. İnternetin de bu müthiş sisteme dâhil olmasıyla birlikte yıllık üretilen bilginin artık zetabytelarla ifade edilmesi şaşırtıcı olmamaktadır. Bilgi insanlığın en başından beri kıymetli kabul ettiği bir varlık olarak hangi ortamda saklanırsa saklansın kullanıcısı ve sahibi tarafından korunmaya muhtaç olmuştur. Bilginin korunma gereği onun güvenliğini sağlama yöntemlerini ve bilgi güvenliği kavramını hayatımıza katmıştır. Bilgi güvenliğinin temel unsurları olan gizlilik, bütünlük ve erişilebilirlik sağlanarak bilginin korunabileceğine dair bilgi güvenliği modelleri oluşturulmuştur. Bilgi güvenliğini sağlamak için güvenlik politikaları belirlenmiş, bireysel veya kurumsal olarak hem de ulusal alanlarda uygulanmaya çalışılmıştır.

Bilgi güvenliği politikaları ne kadar tedbirli ve sıkı oluşturulursa oluşturulsun her sistem en zayıf halkası kadar güçlüdür kuralı gereği insan faktörü göz ardı edildiğinde kurulan bütün sistemin bir kullanıcının bilgi eksikliği yüzünden ciddi sorunlar yaşamasına sebep olmaktadır. Kullanıcılar hangi alanda sistemi kullandığına göre tehlikeye atacağı bilginin değeri ve oluşabilecek risklerin büyüklüğü değişiklik göstermektedir. İnternetin hayatımızda yaygınlaşmasıyla birlikte bu riskler ve tehditler kullanılan bilgi sistemiyle aynı ortamda bulunmadan uzaktan yapılan saldırılar haline gelmiştir. Son yıllarda siber saldırıların boyutu değişmiş, bireysel saldırılar yanında çok ciddi ülkeler arası saldırılar yaşanmaya başlamıştır. Bu saldırılardan en çok etkilenen beş sektör arasında Kamu Kurum ve Kuruluşları da bulunmaktadır. Kamu kurumları aynı zamanda kritik sektörler arasında da yer aldığı için bu kurumda görev yapan tüm çalışanların iş süreçlerinde daha dikkatli çalışması, yapacakları hataların nelere neden olabileceğinin bilincinde ve farkında olarak sorumluluklarını yerine getirmesi hem kurumsal bilgi güvenliği açısından hem de ulusal bilgi güvenliği açısından önem arz etmektedir. İnternetin sunduğu olanaklar sebebiyle pek çok kamu kurum ve kuruluşunun çoğu hizmeti elektronik ortamlar üzerinden kullanıcıya sunması kullanıcı ve çalışan farkındalığının önemini daha da artırmaktadır.

2.BİLGİ NEDİR?

Bilim sayesinde gelişen ve adeta yaratıcısı olduğu teknolojinin baş döndürücü şekilde ilerlemesiyle birlikte pek çok kavram yeni boyutlar kazanmıştır. Bilgi kök itibariyle bilmek kelimesinden geldiğini bildiğimizden bilmek arzusu ile yanan insanoğlunun bilgiye ne kadar önem verdiği ilk insandan beri bilinmektedir. İlk insandan beri tüm din, felsefe ve ilim alanlarında bilgi çok kıymetli bir varlık olmuştur. Günümüzde bilgi kelimesini sıkça kullanılmasına rağmen kesin bir tanım yapmak mümkün değildir.

Sparrow (2008)' a göre bilgi günlük yaşamda öğreti, sezgi, his ve yargı gibi kavramlarla iç içe geçmiştir. İngilizcede kullanılan data, information, knowledge gibi kavramlarının çoğunun karşılığının dilimizde bilgi olarak karşılık bulması da kafa karışıklığını artırmaktadır. Bu terimlerin karşılığını bilgi piramidi ile anlatmak aradaki farkın anlaşılmasına yardımcı olacaktır.

Aşağıdaki şekilde yer alan bilgi piramidine bakıldığında bilgiye ulaşmanın kolay bir iş olmadığı anlaşılır. En alttan yukarıya doğru daha çok çaba ve çalışma gerektirir. Her bir aşama genellikle atlanmadan geçilir ve yukarı doğru çıkıldıkça elde bulunan şeyin miktarı azalırken değeri inanılmaz derecede artar. Bütün bu zorluklardan sonra aşağı basamakta verinin paylaşımı kolay iken yukarı basamaklarda bilginin paylaşımı zorlaşır.

Veri (Data): İngilizce data kelimesi fiilin geçmiş zamanda kullanım haliyle ve verilen şey anlamında kullanılmaktadır. Yine Türkçe' de veri kelimesi verilen şey anlamında kullanılmaktadır. Latince' de ise data kelimesinin karşılığının M.Ö 300 yıllarında Öklit tarafından kullanıldığı söylenmektedir. [7] Birbirleriyle ilişkisi bulunmayan bağımsız ve anlam ifade etmeyen sayısal yada sayısal olmayan setlere verilen isimdir. Başka bir tanıma göre veri bilgi teknolojileri açısından değerlendirildiğinde bir olay veya iş hakkında henüz birbiriyle bağlantısı kurulmamış dolayısıyla henüz anlam ifade etmeyen elde olan kayıtlar veya elektronik ortamlarda bulunan ve iletilen bir sıfırları yani sinyallerdir [9]. Örnekle anlatmak gerekirse "Veri, henüz ilişkilendirilmemiş ham kayıtlardır" ifadesi bir cümle olarak değil de "inüzehrvemkaylıdatarlişlneikidmrilieiş" şeklinde yazılmış olsa hiçbir anlam ifade etmeyecektir. Başka bir örnekle pekiştirmek gerekirse bir kitapta yazan kelimeleri ayrı ayrı yazıp bir kutuya atılsa bu kelimeler tek başına bir anlam ifade etmeyecek, anlaşılamayacaktır.

Enformasyon (Information): Artık verinin anlamlı hale geldiği ve birbirleriyle ilişkilendirildiği şeklidir. Bazı kaynaklarda ise bilginin bir konu hakkındaki bilinmesi gereken şeyleri bilerek belirsizliği yok eden kaynak olduğu söylenmektedir. Bir verinin kullanılabilmesi için bilgiye dönüşmesi gerekmektedir. Bilgi sistemi kullanıcısının kullanmasına uygun olduğu formattır. Örnek vermek gerekirse, bir tabloda bir sütunda yer alan sayısal verilerin tek başına bir anlamı yoktur ancak hemen yanına eklenecek olan diğer bir veri sütunuyla bağlantısı kurulduğunda artık eldeki veri anlamlı hale gelmiş olur. Bu sütunlardan ilki öğrenci notları olsa tek başına bir anlam ifade etmez, ancak yanına eklenen sütunda öğrenci ad-soyadları yer alsa artık anlam kazanmış ve kullanılabilir durumda olur.

Bilgi, Malumat (Knowledge) : Malumat, deneyim kazanma, bilgi ve beceri kazanarak veya içe bakış şeklinde elde edilen hakikatlerin ne olduğunun ayırdında olunması ve anlaşılması olarak tanımlanmaktadır [9]. Malumatın kapsamını bir şeyin ne olduğu, nasıl olduğu, neden olduğu ve kim olduğu gibi soruların cevapları belirler. Örneğin; kendi dilimizde konuşmayı bilinçli bir şekilde öğrenilmediği tecrübe ile öğrenildiği ve sahibine ait bir malumat olduğu gerçeğidir. Malumat açık ve gizli olarak da gruplandırılabilir. Örtülü malumat daha kişisel iken açık malumat başkalarına rahatlıkla semboller, formüller yoluyla aktarılıp paylaşılabilir, anlatılabilir. Kişinin kendine has konuşma tarzının olması veya espri yeteneğinin bulunmasını örtülü malumata örnek olurken, hava sıcaklığı bilgisi açık malumata örnek teşkil eder.

Başka bir deyişle, enformasyon birbiriyle ilişkisi olan anlamlandırılmış veri, bilgi ise değeri olan enformasyondur [26]. Verilerin bir araya getirilip anlamlandırılmasıyla enformasyon oluşturulsa malumat bu bilgilerin toplamından çok daha değerli bir varlıktır.

Hikmet (Wisdom) : Bilgelik diye adlandırılan hikmet ise mevcut ve sahip olunan malumatın nasıl kullanılacağı, nasıl karar verileceği, nasıl değerlendirileceği yönünde bir keşif ve buluş aşamasıdır. Hikmet, ayrıca güvenilir bir sonuca varmak ve doğru karar vermek için bilginin nerede, nasıl, ne şekilde kullanılacağını kavramak olarak tanımlanmaktadır [7].

Şekil 2.1. Bilgi piramidi [55]

Bilgi elde edildiği konuya ve elde ediliş şekline göre dini, teknik, tarihi, akademik, teorik, bilimsel, vb. isimler almaktadır. Zaim (2005) ve Buckland' a göre (1991) bilgi terimi farklı gruplandırılmaktadır.

Süreç Olarak Bilgi, bilgilendirme sürecini ifade etmektedir. Bir diğer ifadeyle yeni bir şeyler öğrenildiğinde yeni öğrenilen bilginin biline önceki bilgiyle kıyaslanması veya değiştirilmesi işlemiyle başkalarına aktarılması sürecidir.

Bilgi Olarak Bilgi, Bilgi süreci içinde diğer taraf aktarılan değer olarak bilgiyi ifade etmektedir.

Nesne Olarak Bilgi, Bilginin bilgi verici nesneler aracılığıyla (kitap, dergi, belge vs.) iletilmesinden dolayı verilen isimdir.

Yukarıda bahsedilen kavramların bilişim teknolojilerinin temel yapı taşı olduğu ve binlerce yıllık insanlık tarihinin bir birikimi ve en kıymetli hazinesi olduğu unutulmamalıdır. Onun kıymetini anlayan her uygarlık korumak için çeşitli yöntemler geliştirmiştir.

Günümüzde bilginin üretilme, depolanma aktarılma, korunma, kullanılma, iletim hızı teknolojiyle birlikte katlanarak artmaktadır. Bu sebeple üretilen konunun büyüklüğü, saklanması ve aktarılması en önemli konulardır.

Her beş yılda bir EMC World tarafından düzenlenen etkinlikte X kuşağı olarak adlandırılan nesile artık bilgi toplumu denildiği ve üretilen bilginin depolama alanlarında devasa boyutlara ulaştığı ve bunun daha da katlanarak devam edeceği açıklanmıştır. 2020 yılında tüm insanlığın ürettiği toplam verinin 44 zettabyte (44 milyon GB) olacağı öngörülmektedir(EMC World,2015).

Bu verilerden anlaşıldığı üzere günümüz insanı bilgi bombardımanına maruz kalmaktadır denilebilir. Ancak bilginin ne derece değer taşıdığını belirlemek yani onun ne kadar değerli yada ne kadar değersiz olduğunu anlamak ve bilmek de bilgi kadar önem arz etmektedir. Elde edilen bilgiyi değerlendirirken bilginin kalitesini gösteren bazı niteliklere dikkat edilir. Bunlar bilginin doğruluğu, konuyla bağlantısı, aktüalitesi, tamlığı, gereksinimlere karşılık vermesi, doğru servis edilmesi ve anlaşılırlığı gibi kriterler, bilginin kalitesini etkileyen faktörlerden bazılarıdır [7].

Bilginin çok kıymetli ve önemli olması bilgiye sahiplik konusunda bazı düzenlemeleri ve şartları da beraberinde getirmektedir. Bilgi sadece kişiler için değil, kurum ve ülkeler için de elde edilmesi ve korunması zor bir metadır. Bu metanın korunması hayati bir önem arz ederken onu elde etmede zorluklar yaşayan özel yada tüzel kişilerin haklarını korumayı hem de bilginin kullanımındaki karmaşa, yozlaşma ve kötüye kullanılmasının da önüne geçecektir. Bunun için telif hakkı, patent gibi önlemler alınmıştır. Ancak bilginin korunması elektronik ortamda çok daha zordur. Bu sebeple bilgi güvenliği, dünya gündeminde ilk sıralarda yer almakta ve bu konuda yapılan çalışmalar artmakta harcanan miktarlar da milyon dolarları aşmaktadır.

3. BİLGİ GÜVENLİĞİ

Bilgi güvenliği, bilgiye erişim yetkisi olan kişilerce güvenilir ve her an erişilebilir ortamda tutulması ve bilgiyi gönderen ve alan taraflar arasında bozulmadan güvenli bir şekilde iletilmesi olarak tanımlanmıştır [35]. Ancak bilişim teknolojilerinin gelişmesiyle birlikte dijital veri güvenliği kavramı ortaya çıkmıştır. Canbek ve Sağıroğlu (2006)' na göre dijital veri güvenliği, sayısal ortamlarda verilerin veya bilgilerin saklanması ve iletilmesi işleminde iletilen şeyin bütünlüğü bozulmadan, yetkisiz erişimlerden korunması güvenilir bir ortam oluşturulmasına dair yapılan işlemlerin tümüdür. Başka bir tanımda ise 'bilgi varlıklarının güvenliğini tehdit eden her türlü tehlikeden korunması için bilgi güvenliğini sağlayacak doğru teknolojinin, doğru zamanda doğru yerde doğru şekilde kullanılması' olarak tanımlanır [7].

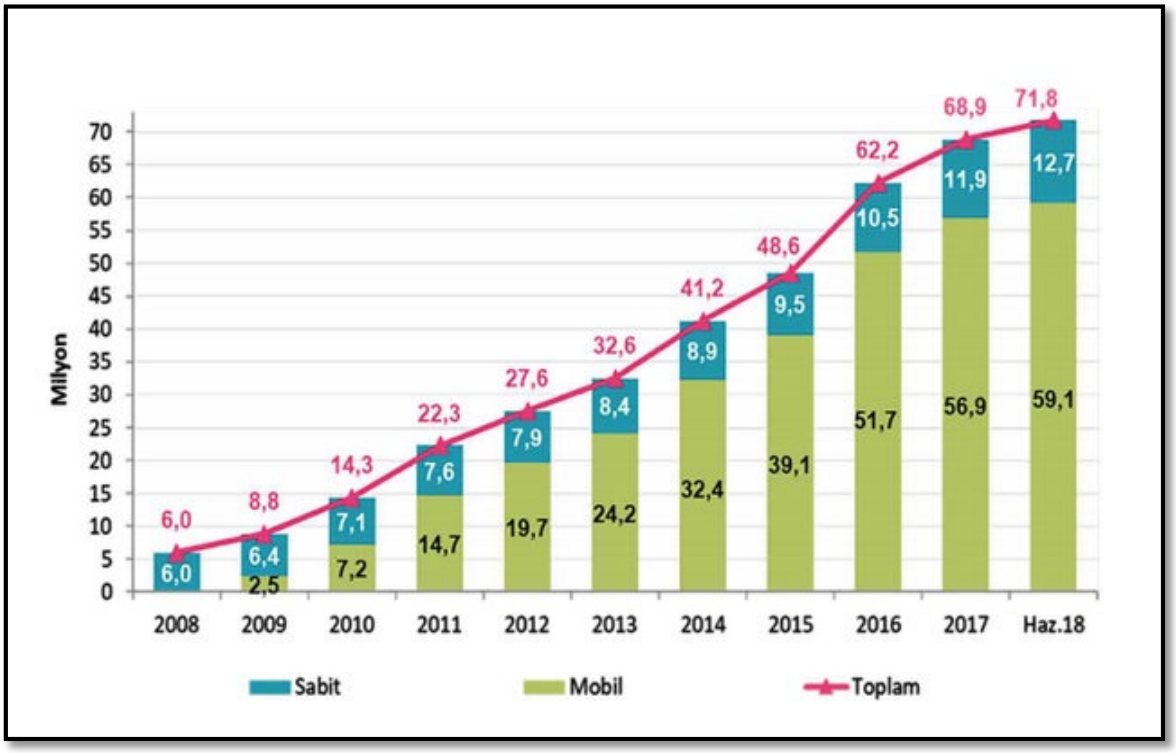
ISO 27002' e göre bilgi güvenliği ise bilginin sadece erişim yetkisi verilmiş kişiler tarafından ulaşılabilir olmasını, bilginin ve bilgiye dair yapılacak işlemlerin bütünlük ve doğruluğunu sağlayarak erişim yetkisi olan kullanıcıların ihtiyaç anında bilgiye ve bağlantılı kaynaklarına erişebilmelerini sağlamak olarak tanımlanmaktadır.

Tüm bu tanımlarda bilgi güvenliği teknolojiyle birlikte düşünülse de aslında kullanıldığı teknolojiden bağımsız bir şekilde de ele alınması gerekmektedir. Bilgi ister kâğıtlarda yazılı şekilde tutulsun ister bilgi sistemlerinde sayısal halde bulunsun kendini kullanan ve depolayarak tutanlar tarafından her türlü saldırıdan korunmaya muhtaç varlıklardır. Bilgi güvenliğinin ilk kullanımı zaten gizlilik gereği diplomatik ve askeri alanlarda olmuştur. Önceleri askeri veya kritik veriyi koruma istihbarata karşı koyma olarak alınması gereken tüm tedbirlerin bütünü olarak algılanmıştır. Ancak iletişim ve bilişim sistemlerinin gelişmesiyle birlikte bilgi artık bu sistemlerde sayısal halde tutulmaya başlanmıştır. Bunun sonucunda bilginin güvenli bir şekilde saklanması ve korunması, gerektiğinde bütünlüğü bozulmamış şekilde her an kullanılabilir olması bilgi sistemlerine ve bilgiye sahip olan her kesimin problemi haline gelmiştir.

Bilgi güvenliği sorunu aslında yazının icat edilmesi ve bilginin yazılı halde saklanabilir olmaya başladığı ilk zamanlardan beri vardır. Bu sorunun temel kaynağı olan bilgi ise o zamanlardan beri çalınabilir, bozulabilir, değiştirilebilir, tahrip edilebilir durumdadır. İnsanlar bu ilk çağlardan beri sahip oldukları bilginin güvenliğini sağlamak için tedbirler

almaya çalışmışlardır.

Ancak güvenlik kaygılarının artan seviyelere ulaşması temel oluşturulma sebebi iletişim olan internetin ortaya çıkmasıyla olmuştur. Önceleri hem sistemden yararlananların hem de sisteme zarar vermek isteyen saldırganların sınırlı sayıda olması ve internetin her eve girecek kadar yaygın olmaması ve kullanıcı sayısının azlığı sebebiyle güvenlik günümüzdeki kadar dikkate alınmıyordu. Ancak bugünkü internet kullanıcı sayısı dünya genelinde yaklaşık 2,3 milyara yaklaştığından kaygıların ciddi boyutlara ulaşması yadsınmamaktadır.



Şekil 3.1. Türkiye genişbant internet abone sayısı [57]

Ülkemiz açısından konuya bakmak gerekirse Şekil 3.1' de ülkemizdeki geniş bant internet abone sayısı görülmektedir. Anlaşılacağı üzere son on yılda internet kullanan abone sayısı yaklaşık 15 kat artmıştır. Bu sayıya mobil internet kullanıcıları ve her bir kullanıcının kullandığı internet tabanlı uygulamaları da eklediğimizde bu rakamlar daha da büyümektedir. Bu durumda bilgi güvenliği sağlanması önemli hale gelmektedir.

Bilgi güvenliği bilginin koruyucusu ve sahibine göre çeşitli şekillerde gruplanabilmektedir. Bu gruplar;

- Kişisel Veri Güvenliği,
- Kurumsal Bilgi Güvenliği,
- Ulusal Siber Güvenlik olarak adlandırılmaktadır.

İsimler üzerinden anlaşılacağı gibi bilginin sahibi ve kıymeti büyüdükçe isimler de değişiklik göstermektedir.

Kişisel veri, Kişisel Verileri Koruma Kanunu' na göre, belirli bir kimliğe sahip veya kimliği tespit edilebilir gerçek kişiye ait her türlü veri olarak tanımlanmıştır. Bu tanım çerçevesinde kişinin kimlik bilgileri, banka bilgileri, bilgisayarının ip adresi, elektronik posta adresi, fotoğrafı, eğitim bilgileri, parmak izi, sağlık bilgileri, kurum sicili, emeklilik bilgileri, sosyal medyada yazdığı yayımladığı her türlü yazı, fotoğraf, ses ve görüntü kayıtları vb. veriler kişisel veri olarak kabul edilebilir.

Kişisel Veri Güvenliği, kişilere ait her türlü özel bilginin hizmet alırken yada hizmet verirken karşı tarafla paylaştığı bilgilerin üçüncü taraflarca elde edilememesi, bozulmaması ve yok edilmemesidir. Bu konuda bireysel olarak bilgi paylaşımında dikkatli ve kişisel verileri koruma kanunundan haberdar olmak gereklidir. Bununla ilgili olarak Kişisel Verileri Koruma Kurumu oluşturulmuştur. Kişisel Verileri Koruma Kurumu' nun görevi öz yaşamın gizliliği, temel hak ve hürriyetlere dair kişisel verilerin korunmasını sağlamaya yönelik bir farkındalık ve bilinç düzeyi geliştirmek üzere etkin ve uluslararası düzeyde söz sahibi olmak olarak tanımlanmıştır.

Kurumların kendilerine özgü değerleri bulunması sebebiyle kendi içinde bilgi üreterek kullanmaları gerekmektedir. Kurumsal bilgi, kurumların faaliyetleri ve gereksinimleri doğrultusunda yapılan sistematik araştırma ve geliştirme çalışmalarının sonucu oluşmaktadır. Kurumsal bilgi, kişisel bilgiye; kişisel bilgi kurumsal bilgiye dönüşüp değişerek bilgi, varlığını korumaktadır.

Kurumsal Bilgi Güvenliği, kurumların bilgi varlıklarının güvenlik zafiyetleri belirlenerek bu varlıkların kendisine yönelik her türlü arzu edilmeyen tehdit ve saldırılardan korunması için gerekli olan güvenlik altyapılarının oluşturularak tedbirlerin alınması şeklinde tanımlanabilir. Kurumsal bilgi güvenliği, sistem, teknoloji, insan, eğitim gibi pek çok faktörü tek çatı altında toplayarak yönetilmesi zor bir süreçtir. Bu sürecin yönetilmesinde

güvenlik sistem ve politikalarının uluslararası standartlarda yönetilmesi ve yapılandırılmasına yönelik tüm dünyada kurumsal bilgi güvenliğinin standartlaştırılması yönünde çalışmalar yapılmaktadır.

Ulusal bilgi güvenliği bir organizasyon yada kurumun kurumsal bilgi güvenliği çalışmalarından çok daha kapsamlı olup kurumsal bilgi güvenliğinin sağlanmasındaki gerekliliklerle birlikte uluslararası işbirliği, siber suçlarla mücadele, kamu- özel işbirliği, ulusal güvenlik gibi kavramları da bünyesinde toplamaktadır [9].

3.1. Bilgi Güvenliğinin Kapsamı

Bilgi güvenliği kişisel bilgisayar ve mobil cihazlardan başlayarak kurumsal ve ulusal çaptaki tüm iletişim cihazlarını ve kritik bilgi altyapılarını da kapsayan geniş bir çerçevede bilgi sistemlerinin dahil olduğu güvenlik yönetimi anlayışı olarak tanımlanmaktadır [9].Bu güvenlik yönetimi anlayışı sayısal ortamda saklanan verinin göndericiden alıcıya bütünlüğü ve doğruluğu bozulmadan taşınması, saklanan veriye her an güvenli bir şekilde erişilmesi ve bilginin izinsiz ve yetkisiz erişimlerden korunması için gerekli tüm çalışmalardır. Bu anlayış çerçevesinde bilgi güvenliği yönetim politikaları oluşturulmalı ve uygulanmalıdır. Bu politikalar bilginin gerekli ve yeteri kadar erişimine izin vermeli, bilginin silinmesi işlemlerini sınırlandırılmalı ve yapılan bütün işlemler için sağlıklı log kayıtlarına olanak sağlamalıdır.

Bilgi güvenliği daha detaylı olarak güvenlik konularını içine aldığından ‘Güvenlik Mühendisliği alanının altında bir alan olarak kabul edilmektedir [7]. Diğer yandan kriptoloji, risk yönetimi, güvenlik kültürü gibi alanlarla bağlantılı olarak hepsini kapsayan geniş bir olgudur. Dahası İngilizce’ de ‘Information Security’ olarak geçen ve dilimize bilgi güvenliği olarak çevrilen bir kavramdır. ‘Information Assurance’ kavramının dilimizdeki karşılığı bilgi güvencesidir. Bu iki kavram birbiriyle içi içedir. Bilgi güvencesi gerekli olan güvenliği sağlamak için daha stratejik bir bakış açısıyla konuyu ele alırken bilgi güvenliği daha taktiksel olarak yaklaşmaktadır.

Şekil 3.2. Bilgi güvenliği ve bilgi güvencesi kavramları [56]

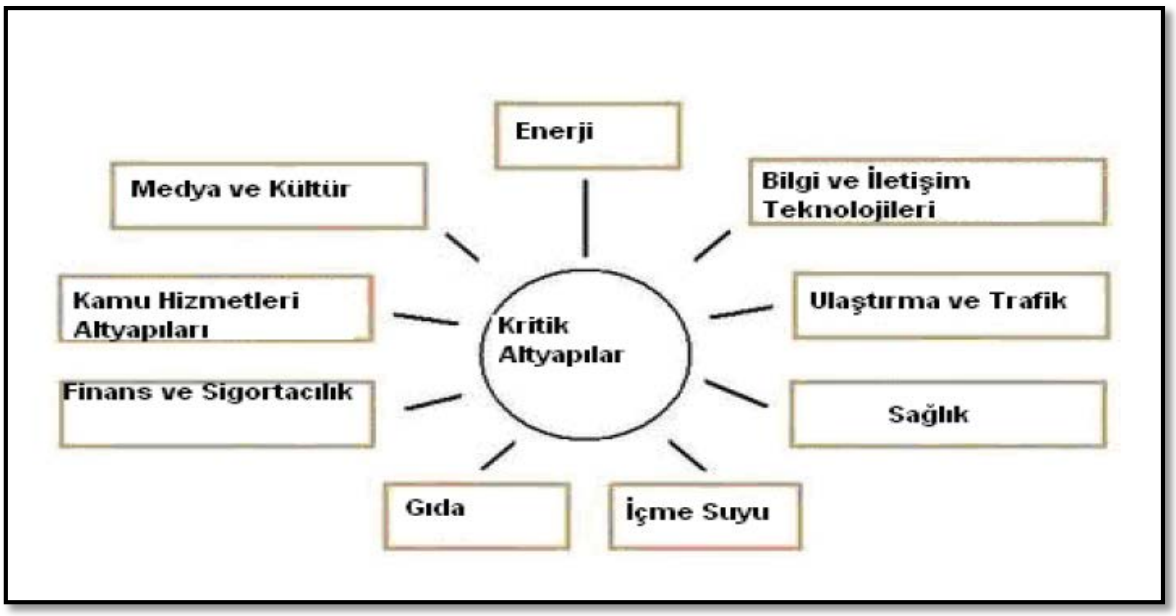
Bilgi güvenliği bağlamında sıkça söz edilen bilgi sistemleri, kritik bilgi altyapıları ve bilgi varlıkları kavramlarını açıklamak gerekmektedir.

Bilgi Sistemleri: Bir bilgi sistemi, bilgi teknolojilerinin ve kullanıcısının etkileşim içinde olduğu taktiksel ve yönetimsel olarak kullanılan karar destek sistemleri şeklinde tanımlanabilir. Bu nedenle bilgi sistemleri yalnızca bilgi iletişim teknolojileri çözümlerini değil insanların da iş süreçlerini destekleyen ve bu teknolojilerle etkileşim halinde olan sistemlerdir. Bilgi sistemleri çağımız nedeniyle teknik açıdan bilgisayar tabanlı çalışmaktadır. Ancak sadece bilgisayarlar değil yazılımlar, donanımlar, iletişim sistemleri ve en önemlisi de internet de bilgi sistemlerinin çalışması için gereklidir.

Bilgi Varlıkları: Bir bilgi sisteminde yer alan bunun saklanmasından işlenmesine ve korunmasına kadar etkili ve dâhil olan tüm yazılım, donanım ve insanların oluşturduğu işleyişi sağlayan varlıkların tümüdür.

Kritik Altyapılar: Adından anlaşılacağı üzere kritik altyapılar bilgi güvenliği açısından büyük öneme sahiptir. Genel geçer bir kritik altyapı tanımı olmamakla birlikte nerede

kullanıldığına göre ülkeler ya da kurumlar bazında çeşitli tanımlamalar yapılmaktadır. Kullanıldığı yer ve duruma göre tanımlar farklılık gösterse de ortak özellikleri ele alındığında işlevlerini kısmen veya tamamen, yerine getirmediğinde, kurum düzeninin ya da toplumsal düzenin sürdürülebilirliğinin kesintiye uğrayabileceği ve/veya kamu hizmetlerinin verilmesinde olumsuzluklar yaşanacağı tüm ağ, varlık, yapı ve sistemlerin tamamı olarak kısaca tanımlamak mümkündür.



Şekil 3.3. Kritik altyapı sektörleri [9]

Kritik altyapılar toplumsal düzenin sağlanmasında ve sürdürülmesinde yaşamsal ve ismiyle müsemma şekilde kritik bir öneme sahiptir. Dünya genelinde yaşanan pek çok olayda bu yapıların ne derece önemli ve hayati seviyede korunması gerektiği anlaşılmıştır. Japonya' da olan deprem sonrası oluşan tsunami sebebiyle nükleer santrallerde meydana gelen sızıntı neticesinde içme suyunun kullanılamaz hale gelmesi ve gıdadan sağlığa kadar pek çok sektörün birbirini etkilediği görülmüştür. Yine Amerika ve İngiltere' de meydana gelen elektrik kesintileri sebebiyle ulaşım ve trafik durmuş ve toplumsal yaşamı ciddi boyutta etkilemiştir. Kritik altyapıların günümüz iletişim ve teknolojileri gereği daha iyi bir hal alırken birbirleriyle daha çok iç içe ve etkileşim halinde olmaları sebebiyle herhangi birinde meydana gelen hizmet aksaması diğerlerinin de sırasıyla hizmet sunumuna sirayet etmekte ve toplumsal yaşamı etkilemektedir.

3.2. Bilgi Güvenliğinin Amacı

Bilgi güvenliği, bilgi sistemlerinin işleyişinin kesintisiz, kaliteli ve güvenilir bir şekilde devam ettirilmesini sağlamaktır. Böylece kurum ve ülke imajının zedelenmemesi güvenliğin sağlanması ile bilgi varlıklarının korunması ve yetkisiz kişilerin erişiminin engellenmesidir.

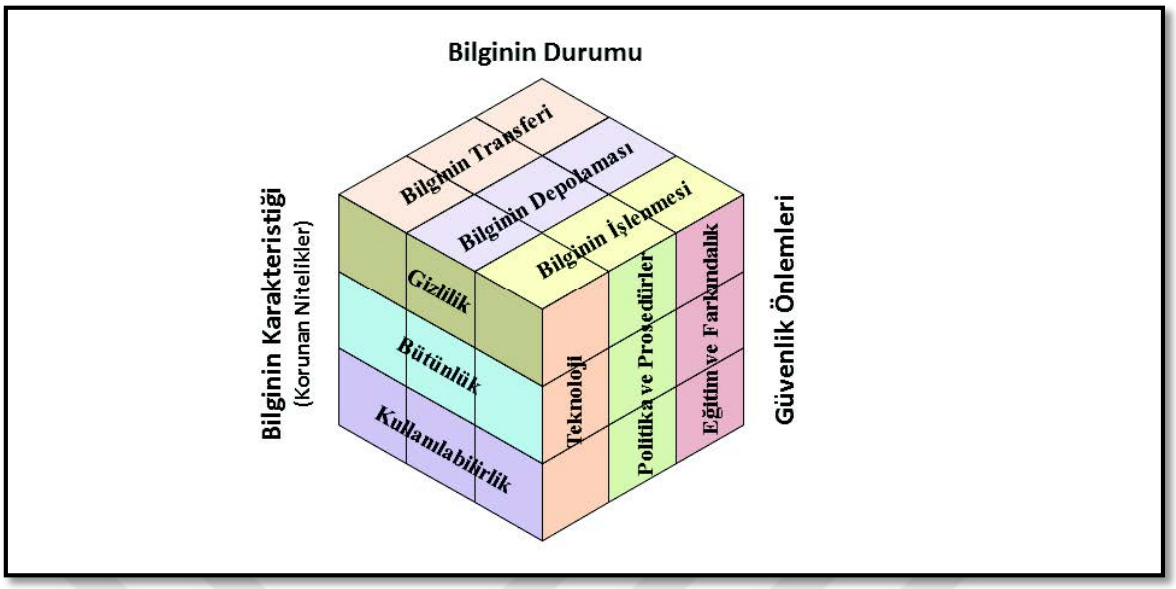
3.3. Bilgi Güvenliğinin Konusu

Bilgi güvenliğinin temeli bilginin gizlilik, bütünlük ve kullanılabilirliğine yönelik her türlü saldırı ve tehditlere karşı korumak ve bu tehditlerin yararlanabileceği güvenlik açıklarının belirleyerek önlem almaktır. İlk bakışta basit ve anlaşılır görünse de tehdit ve saldırıların çeşitlenmesi, çoğalması ve karmaşıklaşması sebebiyle bilgi güvenliğini sağlamak giderek zorlaşmaktadır.

3.4. Bilgi Güvenliği Unsurları

Bilgi güvenliğinin sürekli korunması gereken nitelikleri bir diğer ifadeyle korunması gereken ilkeleri bulunmaktadır. Bilgi güvenliği Solomon'un bilgi güvenliği üçgeninde anlattığı gibi gizlilik, bütünlük ve erişilebilirlik olmak üzere bu üç unsurun bileşimi kabul edilmekte ve bu üç unsur üzerine kurulmaktadır.

Şekil 3.4' te gösterilen McCumber Bilgi Güvenliği modeli bilgi güvenliği alanında hem ulusal hem de uluslararası boyutta bilgi güvenliği politikası geliştirebilmek ve bilgi güvenliğini gerçekten tüm yönleriyle ele alabilmek için temel alınabilecek en uygun ve anlamlı modellerden biridir. Bilgi güvenliğini tüm unsurlarıyla birlikte farklı boyutlarda gruplandırarak gösteren McCumber modeli 1991' den beri geçerliliğini korumuş ve diğer geliştirilen modellerde temel kabul edilerek yol gösterici olmuştur. McCumber bu modeline göre bilgi güvenliği politikaları oluşturulurken ve uygulamaya dönüştürülürken tüm yönleri ile birlikte ele alınmadığı sürece bilgi güvenliğinin sağlanması ve bilgi güvenliği politikalarının başarıya ulaşması mümkün değildir.



Şekil 3.4. McCumber bilgi güvenliği modeli (McCumber,1991)

Bilginin gizliliği, bütünlüğü, erişilebilirliği kadar bilgi güvenliği sürecinde etkili olan bilgi güvenliği politika ve prosedürlerinin ve insan faktörünün büyük önemi bulunmaktadır. Bilgi güvenliği politikalarını olabilecek en iyi ve katı ve kapsamlı kurallarla uygulayan kuruluşlar da McCumber bilgi modeline temel bilgi güvenliği kavramları içerisinde yer ayırmaktadır [23].

Bilgi güvenliği politikalarına farklı açılardan ve detaylı bir perspektiften bakmayı sağlayan McCumber modeli, kurumlar için bilgi güvenliği politika ve prosedürlerini oluştururken dikkate alınması gereken önemli bir modeldir. Modelde bilgi güvenliğinin farklı boyutlarını gösteren gruplar yer almaktadır. Bir yüzünde bilgi güvenliğinin temel unsurları olarak kabul edilen gizlilik, bütünlük ve kullanılabilirlik ilkeleri bilginin karakteristiği adı altında toplanmıştır. Diğer yüzde ise bilginin transferi, bilginin depolanması ve bilginin işlenmesi işlemleri bilginin durumu ismiyle gruplandırılmıştır. Küpün üçüncü ve son yüzünde ise teknoloji, politika ve prosedürler ile eğitim ve farkındalık alanları güvenlik önlemleri başlığı altında toplanmıştır.

3.4.1. Bilginin karakteristiği

Gizlilik (confidentiality), kısaca bilgiye yetkisiz kişiler tarafından erişilememesidir. Büyük verinin bulunduğu bilgi sistemlerinde bazı bilgiler herkesin erişimine açık olduğu halde bazıları yapılan güvenlik yetkilendirmeleri gereği sadece belirli grupta yer alan yetkilerin

erişimine açıktır. Bilgi gizliliğinin sağlanması için yetkilendirme, şifre ile erişim ve verileri şifreleme gibi belli başlı yöntemler uygulanmaktadır. Bilginin gizliliğinin sağlanmasında öncelikli unsur, sayısal olarak bulunan bilgiye, bilgi güvenliği politikası dahilinde belirlenen ve bilmesi gereken ilkesi olarak adlandırılan ilke gereği kurum personelinin sadece görev sorumluluklarıyla ilgili bilgiye erişiminin sağlanması, diğer verilere erişimin engellenmesidir [23]. McCumber modelinde bilginin gizliliğinin sağlanması için bilginin taşınması ve depolanması işlemlerinde kriptolanması tavsiye edilmektedir. Ancak saldırganlar çeşitli yöntemlerle yetkilerinin olmadığı bilgilere erişerek gizlilik unsuruna zarar vermektedir. Şifrelerin çeşitli yöntemlerle kırılması veya çalınması, alıcı ve gönderici taraflar arasındaki veri iletişiminin açığa çıkarılması, gizlilik ilkesine uygun olmayan davranışlar olarak değerlendirilmektedir [7].

Bütünlük (integrity), kısaca bilginin doğruluğunun ve tam olma durumunun bozulmamasıdır, yani gönderici ile alıcı arasında iletilen bilgilerin değiştirilmeden yada bozulmadan ilgili tarafa iletilmesine yönelik uygulamaları içerir. Bütünlük ile kastedilen şey bilginin doğru ve kesin oluşudur. Bilgi değiştirilemez olmalıdır, sadece izin verilen kişilerce izin verilen yollarla değiştirilebilmelidir. Bilgi kendi içinde anlamlı, tutarlı olmalı çelişkiler olmamalıdır. Bilgi bütünlüğü bilgi sistemlerindeki bazı eksiklikler ve hatalar nedeniyle istemsiz olarak veya kötü niyetli kullanıcı faaliyetleriyle isteyerek bozulabilmektedir. McCumber' a göre bilginin bütünlüğünün içinde inkar edememe, kimlik doğrulama, erişim kontrolü, kripto çözümleri ve karşılaştırmalı analiz gibi süreçleri de içine almaktadır [Mccumber,2005]. Bilgi bütünlüğüne bozmaya yönelik saldırılar genellikle zarar verme veya engelleme, değişiklik yapma ve üretim gibi yöntemleri içermektedir. Kimlik doğrulama ile yetkisiz erişimi tespit ederek engelleme yada kimlik doğrulama ve yetkilendirme yöntemleri kullanılarak kullanıcının ihtiyaç duyduğu kadar en düşük yetki ile erişimine izin verilir.

Erişilebilirlik (availability), erişim yetkisi olan kişilerin bilgiye her an ulaşarak kullanabilmesidir. Diğer adıyla süreklilik ilkesi kurum içi veya dışı yetkililerce kurum bilgisinin zarar verilmeden kullanılmasını ve sürekliliğinin sağlanmasını kapsamaktadır. Erişilebilirlikte bilgi, kullanıcıları tarafından her an ulaşılabilir halde ve ulaşım sırasında kaynakların paylaşımı da izin verildiği şekilde olmalıdır. Bu durum en fazla yer sağlayıcılar ve teknik uzmanlar açısından sistemin her an etkin ve erişilebilir olması gerektiğinden bir takım sorumluluklar getirmektedir. Altyapı olarak hizmet veren

cihazların düzenli olarak yedeklerinin alınması ve sorun halinde en hızlı şekilde yeniden hizmet verir hale getirilmesi gerekmektedir. Erişilebilirliği bozmaya yönelik saldırılar genelde engelleme veya değişiklik yapma ve üretim olabilir. Erişilebilirlik ilkesini uygulamak için uygulanan güvenlik tedbirleri sebebiyle en fazla yaşanan sorun bu tedbirlerin bilgiye erişimi olması gerektiğinden zor bir hale getirmesidir.

Bu üç sacayağı birbirinden ayrı düşünülemez. Şöyle ki, bu üç unsur birbirini ihlal etmemeli, bilginin gizliliği erişilebilirliğini, erişilebilirliği bütünlüğünü ve doğruluğunu bozmamalıdır. Eğer bir bilginin gizliliği sağlanırken erişimi engelleniyor ise ya da bilginin erişilebilirliği sağlanırken bilginin bütünlüğü bozuluyor ise kurumlar ve kişiler için doğru bilgi bozulmuş olacağından olumsuz sonuçlar doğuracaktır.

Bilginin karakteristiği unsurlarına daha sonra bilgi güvenliği analizcileri ve araştırmacılar inkâr edememe unsurunu eklemek istemiş ancak McCumber modeli yeniden değerlendirirken yeni unsurların eklenmesine gerek olmadığına karar vermiştir. Yeni unsurlar olarak eklenen inkâr edememe ve kimlik doğrulamanın bilginin bütünlüğü unsurunun içinde olduğunu ifade etmiştir.

Bu unsurlar dışında sorumluluk (accountability), inkar edememe (non-repudiation), kimlik denetimi (authentication), erişim denetimi (accesscontrol), güvenilirlik (reliability) ve emniyet (safety) gibi kavramlarda bilgi güvenliğini sağlamada destekleyici unsurlardan bazılarıdır.

3.4.2. Bilginin durumu

McCumber bilgi güvenliği modelinde bilginin durumu başlığı altında bilginin transferi, bilginin depolanması ve bilginin işlenmesi olarak üç alt başlık yer almaktadır. Herhangi bir sistem üzerindeki bilgi herhangi bir zaman diliminde bu durumlardan birinde veya ikisinde yer almaktadır. Bilginin değerini de bilginin o an bulunduğu durum belirlemektedir. Örneğin; bilginin transferi durumunda bilgi hem iletim halinde hem de orjinali hard diskte bulunduğu için depolama halinde bulunmaktadır. Bilgi güvenliği modelinde risk yönetimi bilgiye değer vererek oluşturulmaktadır. Bilginin durumuna bakarak onu korumak için çeşitli önlemlerin alınması gerekmektedir. Eğer transfer halinde olan bir bilginin korunması gerekiyorsa bilgi güvenliğinin sağlanması için gereken yöntem kriptolamadır.

McCumber modelinden esinlenerek yapılan bazı yeni modellerde bilginin durumunun değiştiği zamanı ifade etmek amacıyla ‘zaman’ olgusu da eklendiği görülmektedir.

3.4.3. Güvenlik önlemleri

McCumber bilgi güvenliği modelinde güvenlik önlemleri boyutunda teknoloji, politika ve prosedürler ve insan olmak üzere üç öğe bulunmaktadır. Güvenlik tedbirleri modelde diğer iki yüzde yer alan unsurların birleşimi noktasında tamamlayıcı olarak yer almaktadır. Örneğin, bilginin iletilmesinde güvenliğin sağlanabilmesi için önerilen yöntem bilginin kriptolanmasıdır. Böylece bilgi güvenliği tamamlanmaktadır. Güvenlik önlemleri boyutu bilgi güvenliğinin diğer iki boyutu olan bilgi durumu ve bilgi karakteristiği boyutlarının birleşimi ile elde edilen sonuca tamamlayıcı olarak eklenir ve bilgi güvenliği eksiksiz şekilde sağlanmış olur. Modelde bulunan boyutlardan birinin eksik olduğu durumda güvenlik açıkları ortaya çıkmaya başlar.

Güvenlik önlemlerini uygulamada öncelik teknoloji boyutuna verilmektedir. Bilgi güvenliğinin sağlanması için sürekli yeni teknik önlemler (güvenlik duvarı, anti-virüs yazılımı vb.) ortaya çıkmaktadır. Teknik güvenlik önlemleri için bilginin karakteristik özelliklerini korumak için bilginin durumuna bağlı olarak uygulanabilecek yazılım ve donanım dâhil tüm önlemler denilebilir.

Modeldeki güvenlik politikası bileşeni ise bilginin kullanıldığı yere, sistemin durumuna ve bilginin değerine göre değişiklik göstermektedir. Hukuksal düzenlemeler, ulusal bilgi güvenliği politikaları ve kullanıcıların şifre belirleme politikalarına kadar bütün planlamalar güvenlik politikası dahilinde değerlendirilir [23]. Bilgi güvenliğinin sağlanmasında doğru politikaların oluşturulması ciddi bir yere sahiptir.

Eğitim ve Farkındalık unsuru ise dikkate alınmaması halinde diğer alınan tüm önlem ve uygulamaları yetersiz kılacak ve bir anda tüm sistemi tehlikeye atabilecek olan insan faktörünü barındırmaktadır.

Bilgi sistemlerinin ve bu sistemlerin sunduğu gelişme süreçlerinin çok hızlı olması, yenilenmenin sürekli olması güvenlik tedbirlerinin de bu hıza ayak uydurmasını gerektirmiştir. Ancak güvenlik tedbirlerinin bu hıza ayak uyduramaması bilgi güvenliğinin

temelini oluşturan gizlilik, bütünlük ve erişilebilirlik ilkeleriyle paralel olmayan gelişmeler sonucu bilgi güvenliğinin güvenlik boyutuna gereken önem verilmemiştir.

3.5. Bilgi Güvenliğinin Gelişim Süreci

Bilgi güvenliği her ne kadar bilgisayar ve iletişim teknolojilerinin gelişmesiyle birlikte hayatımıza girdiği düşünülse de aslında yazının icadı ile, insanoğlu bilgilerini ve tecrübelerini saklama, gerektiğinde tekrar kullanma yada başkalarına aktarma için bilgi güvenliğine ihtiyaç duymuştur. Ancak bu değerli bilginin başkalarının eline geçmesini istemediği durumlarda bilgiyi gizlediği bilinmektedir. Yapılan kazı çalışmalarında tarihin ilk uygarlıklarının alfabelerinin günümüz dillerinin alfabelerinden daha karışık ve zor bir alfabe sistemi kullanılarak yapıldığı ortaya çıkmıştır. Bunun nedeninin okuma yazmayı bilerek zorlaştırarak halktan belirli zümrelerin sosyal hayatta ayrıcalık kazanmasını sağlamak ve sürdürmektir. Ünlü iktisat tarihçisi H. Innis 'bilgi tekelleri' oluşturarak bilginin gücünden sadece belirli bir grup insanın yararlanmasının sağlandığını iddia etmektedir. Eski medeniyetlerde kullanılan yazıların karmaşık bir yapıya sahip olması ilk uygarlıkların alfabelerinin çoğunun alfabelerinin zor olması elbette bir tesadüf değildir. Belirli bir ruhban ya da bürokrasi sınıfının bilgi üzerindeki tekelinin devam ettirilmesi amaçlanmıştır.

İlk çağlarda politikacılar ve yöneticiler aralarındaki yazışma ve haberleşmelerin gizliliğini mühürler, özel kilitli kutular veya özel yapıştırıcılar kullanarak sağlamaktaydı. Tarihte adını sıkça duyduğumuz Jül Sezar tarafından geliştirildiği için ismi verilen Sezar Şifreleme Tekniğinin döneminde oldukça etkili olduğu ve uzun süre kırılamadığı bilinmektedir. Ünlü Hazerfan Al-Kindi tarafından bulunan ve günümüzde kullanılmaya devam eden kriptoanaliz tekniği olan Frekans Analizi yöntemi ile Sezar Şifreleme Tekniği deşifre edilebilmiştir.

Sanayi devrimi ve elektriğin keşfi ile birlikte teknoloji gelişmeye ve yaygınlaşmaya başlamıştır. Artık elektrik akımı ile sinyaller taşınmaya başlamış telgraf sonrası ses taşınmasıyla telefon ve görüntü taşınmasıyla televizyon gibi çok önemli iletişim araçları icat edilmiş ve bilgi güvenliği kavramı çok farklı boyutlara ulaşmıştır. Bu süreçte ilk bilgi güvenliği ihlali, 1903 yılında İngiltere' de birbiriyle rekabet eden iki mucid tarafından geliştirilen ve güvenli olduğu söylenilen radyo alıcısının halkın önünde tanıtımı sırasında

kaynağı belirsiz bazı argo mesajların gönderilmesiyle yaşanmıştır. Bu olaya tarihin ilk bilgisayar korsanlığı denilmektedir.

Devam edegelen süreçte dönemin Nazi Almanya'sı tarafından haberleşmede şifreleme ve deşifre edilmesi amacıyla kullanılan Enigma isimli şifrelemesi zor sayılabilecek bir şifre makinası kullanılmaktaydı. İkinci Dünya Savaşı öncesi şifresinin Polonyalı uzmanlar tarafından kırılması sonucu Almaların savaşı kaybetmeleri savaşın kaderini değiştirmiştir [23].Özellikle İkinci Dünya Savaşı sonrasında hafızada tutma ve internet aracılığıyla haberleşme yapılmasa da İkinci Dünya Savaşında büyük önem taşıyan şifrelerin kırılması için kullanılan bilgisayarların atası sayılan ilk bilgisayarların hayatımıza girmesiyle bilgi ve bilgi güvenliği yepyeni bir boyut kazanmıştır. O dönemlerde bilgi güvenliği askeri ve sivil alanlara izinsiz girişleri önlemek amacıyla görsel ve işitsel şifreleme teknikleriyle sınırlıydı ve bilgi güvenliği, ülke güvenliği, casusluk, sabotaj gibi tehlikelere karşı alınan önlemler olarak ifade edilmekteydi. Nükleer saldırı da dahil olmak üzere en ağır saldırı durumunda dahi askeri iletişime olanak sağlamayı amaçlayan ve Amerika Birleşik Devletleri (ABD) tarafından askeri bir proje olarak geliştirilen Araştırma Projeleri Kurumunun (ARPA) İleri Araştırma Projeleri Ağı (ARPANET) projesiyle birlikte en basit anlamda haberleşmenin alt yapısını oluşturan internet tasarlanmış oldu [23].İlk başlarda son derece güvenli olduğu konusunda neredeyse tüm bilim adamlarının hem fikir olduğu bu sanal ortamın çok geçmeden güvenlik açısından bazı teknolojik ve mantıksal riskleri barındırdığı anlaşılmıştır. Bu bilgi güvenliği risklerinin ne olduğuna dair ilk kapsamlı rapor çıkartılmıştır.

1990' da T.Berners-Lee öncülüğünde bir grup bilim adamıyla Avrupa Nükleer Araştırma Merkezi (CERN)'nde geliştirilen World Wide Web (www) projesi hayata geçtiğinde dünyanın farklı bölgelerinde olan kişisel bilgisayarlar ve bilgi sistemleri birbirleriyle haberleşmeye başlamış ve internet ortaya çıkmıştır [23].

İnternetin ticaret amaçlı kullanılması ve toplumun kullanmaya başlamasıyla küresel bilgi akışından devasa bir artış gözlenmiştir. Bu bilgi akışıyla birlikte iktisadi ve sosyal alanda fayda sağlayan gelişmeler beraberinde bilgisayar sistemleri ve bilgi altyapılarına yönelik güvenlik riskleri ve tehditleri getirmiştir.

3.6. Bilgi Güvenliğine Yönelik Güvenlik Riskleri

Bilgi güvenliğine yönelik güvenlik risk ve açıklıkları bilgi sistemlerini yöneten kimselerden kaynaklanabileceği gibi sistemdeki yazılım, donanım, vb. unsurlardan da kaynaklanabilmektedir. Bilgi sistemiyle ilgisi görünmeyen sebeplerden dolayı bile bilgi sisteminin işleyişini etkiyebilir. Eğer sistemin işleyişinde aksama ya da durma meydana geliyorsa bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik olan üç temel ilkesinden en az biri yada bir kaçı işlemez hale gelecektir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) bilgi sistemlerine yönelik yaptığı güvenlik riskleri sınıflandırmasında bilgi sistemlerinin karşılaştığı risklerin oluş sebeplerini her yönden ele almıştır.

Personel Sebebiyle Oluşan Riskler	Bilgi Sistemi Sebebiyle Oluşan Riskler	İç Süreçteki Aksaklıklar	Dış Etkenler
1.1 Kazara Eylemler 1.1.1 Hata 1.1.2 Yanlış 1.1.3 İhmal **1.2 Kasıtlı Eylemler** 1.2.1 Hile 1.2.2 Sabotaj 1.2.3 Hırsızlık 1.2.4 Vandalizm **1.3 Pasif Eylemler** 1.3.1 Yetenek 1.3.2 Bilgi 1.3.3 Rehberlik	**2.1 Donanım** 2.1.1 Kapasite 2.1.2 Performans 2.1.3 Bakım ve İdame 2.1.4 Eskime **2.2 Yazılım** 2.2.1 Uyumluluk (Compatibility) 2.2.2 Yapılandırma Yönetimi (Configuration Management) 2.2.3 Değişim Kontrolü 2.2.4 Güvenlik Ayarları 2.2.5 Kodlama 2.2.6 Test **2.3 Sistem** 2.3.1 Dizayn 2.3.2 Spesifikasyonlar 2.3.3 Entegrasyon 2.3.4 Karmaşıklık	**3.1 Süreç tasarım veya uygulama** 3.1.1 Süreç akışı 3.1.2 Süreç dokumantasyonu 3.1.3 Roller ve sorumluluklar 3.1.4 Bildirimler ve uyarılar 3.1.5 Bilgi akışı 3.1.6 Sorunların birbiriyle çakışması 3.1.7 Hizmet seviyesi Anlaşmaları 3.1.8 Görev değişimleri **3.2 Süreç kontrolü** 3.2.1 Durum izleme 3.2.2 Metrikler 3.2.3 Peryodik izlemeler 3.2.4 Süreç sahipliği **3.3 Destek süreçleri** 3.3.1 Personel 3.3.2 Finansman 3.3.3 Meslek içi eğitim **3.3.4 Tedarik**	**4.1 Doğal afetler** 4.1.1 Hava olayları 4.1.2 Yangın 4.1.3 Su baskını 4.1.4 Deprem 4.1.5 Ayaklanma kargaşa, iç karışıklıklar 4.1.6 Salgın hastalıklar **4.2 Yasal meseleler** 4.2.1 Sektörel düzenlemelere uyumluluk 4.2.2 Yasama 4.2.3Yargı **4.3 İş alemi ile ilgili meseleler** 4.3.1 Tedarik sorunları 4.3.2 Pazar durumları 4.3.3 İktisadi durumlar **4.4 Hizmet bağımlılıkları** 4.4.1 Elektrik, su, doğal gaz, atık yönetimi 4.4.2 Acil durum hizmetleri 4.4.3 Akaryakıt **4.4.4 Ulaştırma**

Şekil 3.5. Bilgi güvenliğine yönelik güvenlik riskleri sınıflandırması (ENISA,2012)

3.6.1. Personel sebebiyle oluşan riskler

Bilgi sisteminin işleyişi kontrol eden ve onu yöneten personeller gerçekleştirdikleri eylemleriyle bilgi sisteminde riskin gerçekleşmesine neden olabildikleri gibi yapmadıkları eylemleriyle de bilgi sisteminde riskin gerçekleşmesine neden olabilirler. Eğer eylemleri sebebiyle güvenlik riskleri gerçekleşiyorsa kasıtlı veya kazara yaptıkları eylemlerden dolayı meydana gelmektedir.

Kazara Eylemler: Bu tür eylemlerde personelin kötü niyeti ve herhangi bir zarar oluşturma kastı yoktur. Ancak oluşan riskler, yine kişiden kaynaklanmaktadır. Bunlar hata, yanlış ve ihmaldir.

- Hata: Personel gayretine rağmen doğru prosedürü, doğru eylemi gerçekleştiremediği durumdur.
- Yanlış: Personelin yapılması gereken doğru işlemi bilmediği için uygulayamadığı durumdur.
- İhmal: Personelin doğru prosedürü bilmesine rağmen uygulamadığı durumdur.

Kasıtlı Eylemler: Bu tür eylemlerde personel iyi niyetli değildir ve eylemini bilinçli ve zarar verme amacıyla gerçekleştirmektedir. Personelin gerçekleştirdiği eyleme göre bunlar hile, sabotaj, hırsızlık ve Vandalizm olarak ayrılmaktadır.

- Hile: Personelin kendisinin veya başkasının menfaati için kurumu zarara uğrattığı durumlarda oluşan risk ve tehditlerdir.
- Sabotaj: Organizasyonun bilgi varlıklarında veya bilgi sistemlerinde kasıtlı olarak meydana gelen zararlardır. Bu eylem çoğunlukla zarar verilen bilgi varlığına ya da sisteme erişim yetkisi olan kimselerce doğrudan gerçekleştirilir veya erişim izni olan kimselerin bilgilerinin sızdırılarak ele geçirilmesiyle dolaylı olarak gerçekleştirilir.
- Hırsızlık: Bu eylem organizasyonun bilgi varlıklarının yetkisi olmayan kimseler tarafından çalınmasıyla oluşmaktadır.
- Vandalizm: Bütün kasıtlı eylemler içinde en tahrip edici olanıdır. Bu eylemde organizasyonun bilgi varlıklarının yok edilmesi amaçlanmaktadır.

Pasif Eylemler: Bilgi sistemlerinin güvenliğini sağlamak veya yönetmekle görevli olan personelin yetenek veya bilgi eksikliği ya da onları yönlendirecek birinin olmaması gibi durumlarda ortaya çıkan risklerdir.

- Yetenek Eksikliği: Bilgi sisteminin güvenliğini sağlayacak olan personelin yetenek eksikliği olarak tanımlanmaktadır.
- Bilgi Eksikliği: Personelin bilgi sisteminin güvenliğini sağlayacak yeterli bilgiye sahip olmaması olarak tanımlanmaktadır.
- Rehber Eksikliği: Organizasyonun bilgi sistemlerinin güvenliğini sağlayacak olan personeli yönetecek veya doğru şekilde yönlendirecek kimsenin organizasyon bünyesinde bulunmaması durumlarında ortaya çıkmaktadır.

3.6.2. Bilgi sistemi sebebiyle oluşan riskler

Donanım, yazılım veya tümleşik sistemlerde teknoloji ve sistem kaynaklı olarak ortaya çıkan beklenmedik aksaklıklar veya güvenlik açıkları olarak tanımlanmaktadır. Donanımsal Riskler: Bilgi sisteminin işlevini yerine getirebilmesi için gerekli olan donanımın yetersiz olması veya eksik olması durumlarında oluşmaktadır.

- Kapasite: Bilgi sisteminin kapasitesinin yeterli gelmediği iş ve süreçlerde ortaya çıkan risklerdir.
- Performans: Bilgi sisteminin performansını etkileyen parametrelerin sürecin ve işin yapılmasına engel olması durumudur.
- Bakım ve İdame: Donanım araçlarının gerekli olan bakım sürecini gerçekleştirmesinde ortaya çıkan başarısızlıklardır.
- Eskime: Donanım araçlarının kullanılamaz durumda olmasıdır.

Yazılımsal Riskler: Bilgi sisteminin işlevini yerine getirebilmesi için kullanılan programlara yazılım denilmektedir. Ancak bu yazılımlar beraberinde bazı riskleri ve güvenlik açıklarını da getirmektedir.

- Uyumluluk: Bilgi sistemindeki yazılımların çalışırken birbiriyle uyum sağlayamaması sonucu ortaya çıkmaktadır.
- Yapılandırma Yönetimi: Bilgi Sisteminde doğru bir şekilde işleyişini yerine getirmesi için gerekli olan konfigürasyon ayarlarının sağlanamaması sonucu ortaya çıkmaktadır.
- Değişim Kontrolü: Bir programın veya sistemin konfigürasyonunda meydana gelen yetkilendirme sorunlarıdır.
- Güvenlik Ayarları: Bilgi sistemindeki uygulamalardaki erişim ve yetkilendirmede ortaya çıkan sorunlardır.
- Kodlama: Mantık hatası veya dikkatsizlik sonucu program kodlamada yapılan hataların meydana getirdiği güvenlik açıklarıdır.
- Test: Yazılımın kullanıma alınmadan önce yapılan testlerinin yetersiz olmasından kaynaklanan risklerdir.

Sistem Kaynaklı Riskler: Bilgi sisteminin tasarımında ya da başka bir sistemle entegrasyonunda veya uygulama modülleri arasında oluşan bağlantı hataları nedeniyle ortaya çıkan risklerdir.

3.6.3. İç süreçlerde meydana gelen riskler

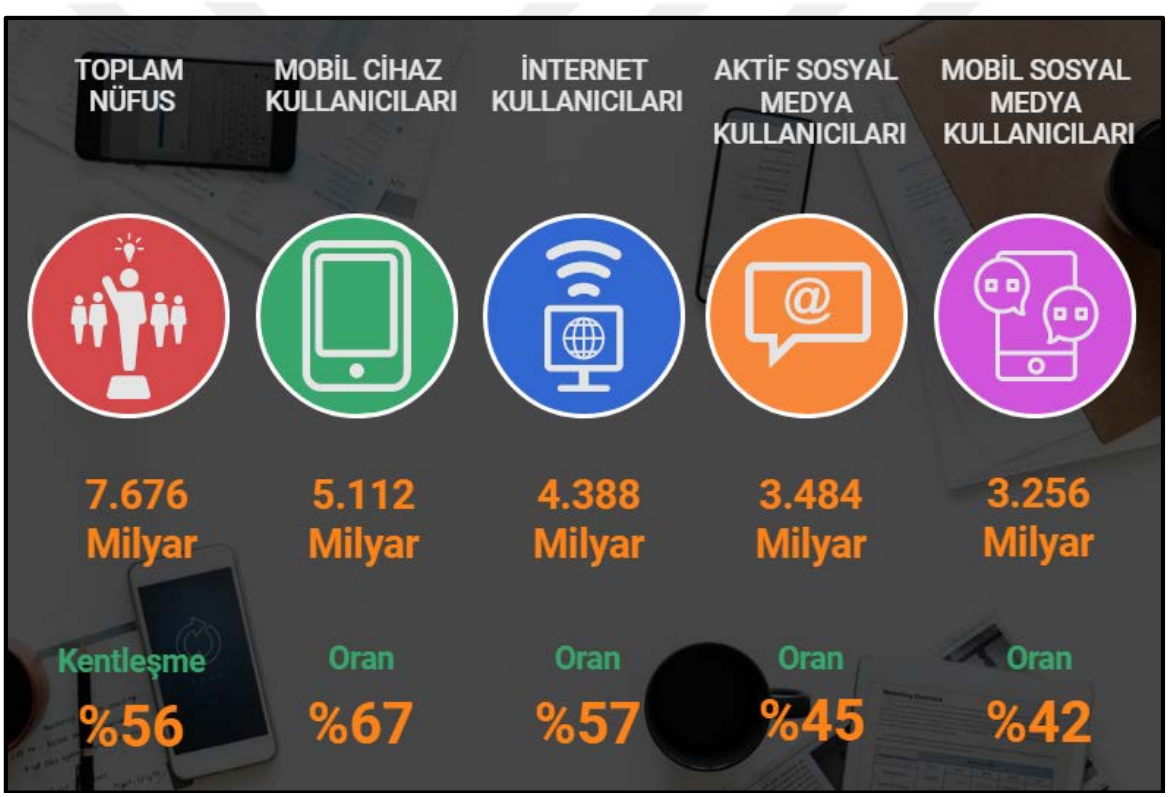
Çoğunlukla yazılım, donanım veya bütünleşik sistemlerde ortaya çıkan bilgi sisteminin düzgün işlemesinin önüne geçen süreç tasarımından veya uygulanması sırasında oluşan sistemsel süreçlerin aksamasına veya durmasına yol açabilecek aksaklıklar olarak tanımlanabilmektedir. Destek süreçlerine ilişkin riskler operasyonel riskler içinde de değerlendirilebilmektedir. Bu alanda ortaya çıkan bilgi güvenliği riskleri daha çok eğitim, muhasebe, tedarik süreçlerinde ortaya çıkmaktadır.

3.6.4. Dış etkenlere ilişkin riskler

Dış etkenler personel veya bilgi sistemleri tarafından kontrol edilemeyen veya gerçekleşmesi tahmin edilemeyen risklerdir. Bunlar daha çok doğal afetler ile ekonomi dünyasına bağlı olarak ortaya çıkabilirler.

4. BİLGİ GÜVENLİĞİNİ TEHDİT EDEN UNSURLAR

İnternetin hayatımıza girmesiyle birlikte internet kullanıcı sayısı müthiş bir şekilde artmaktadır. Şekil 4.1'de dünya genelinde internet, mobil cihaz ve sosyal medya kullanıcılarının sayıları ve penetrasyon rakamları yer almaktadır. Dünya nüfusunun yarısından fazlası internet ve mobil cihaz kullanmakta iken yarısına yakını sosyal medya kullanmaktadır. Türkiye' de ise durum farklı değildir. Türkiye İstatistik Kurumunun 2018 yılında yayınladığı TÜİK Bilgi Toplumu İstatistikleri Raporuna göre ülkemizde bir önceki yıla göre internet kullanıcı oranı artarak %80,7 olarak açıklamıştır. Yine aynı rapora göre web sitesi sahipliği oranı ise %72,9 olarak raporlanmıştır.



Şekil 4.1. Dünya geneli internet, mobil ve sosyal medya kullanıcı istatistikleri 2018 (Wearesocial.com)

Türkiye ve Dünyada internet kullanım rakamlarına bakıldığında internetin hayatımızda ne kadar yer aldığı anlaşılmaktadır. İnternetin sağladığı pek çok kolaylık, rahatlık ve avantajın yanında çeşitli güvenlik sorununu da beraberinde getirmektedir. Bu durum kullanıcılar için birçok risk ortaya çıkarmıştır.

İnternetin kullanılmasıyla ortaya çıkan riskler kullanıcıyı hem ruhsal hem de fiziksel

yönden etkilediği gibi, maddi ve sosyal açıdan zarar da verebilmektedir. Bu riskler saldırı, atak veya tehdit olarak adlandırılmaktadır. Kısaca bilgi veya bilgisayar güvenliğinde kötü niyetli kişiler tarafından yapılan saldırılardır. Bilgi sistemini geçmek veya aldatmak, zayıflıklarını kullanmak, kişilere veya sistemlere direkt olarak veya dolaylı olarak zarar vermek, sistemlerin sürdürülebilirliğini bozmak, durdurmak, işlemez hale getirmek gibi kötü amaçlarla yapılan eylemler saldırı veya atak olarak isimlendirilmektedir [7]. Bu kötü niyetli kişiler amaçlarına ulaşabilmek için çok çeşitli yöntemlerle saldırılar gerçekleştirmektedirler. Kötü niyetli kişiler olarak tanımlanan aslında bilgisayar korsanları olarak da adlandırılmaktadır. Yüksek düzeyde bilgi iletişim teknolojileri bilgisi olan bilgi sisteminin gizlilik, bütünlük ve erişilebilirlik unsurlarını hedef alan saldırganlara bilgisayar korsanları (hacker) denilmektedir. Bu kimseler bilgi veya bilgisayar sistemlerinin güvenlik açıklarını bularak kendi menfaatleri doğrultusunda kullanmaktadırlar.

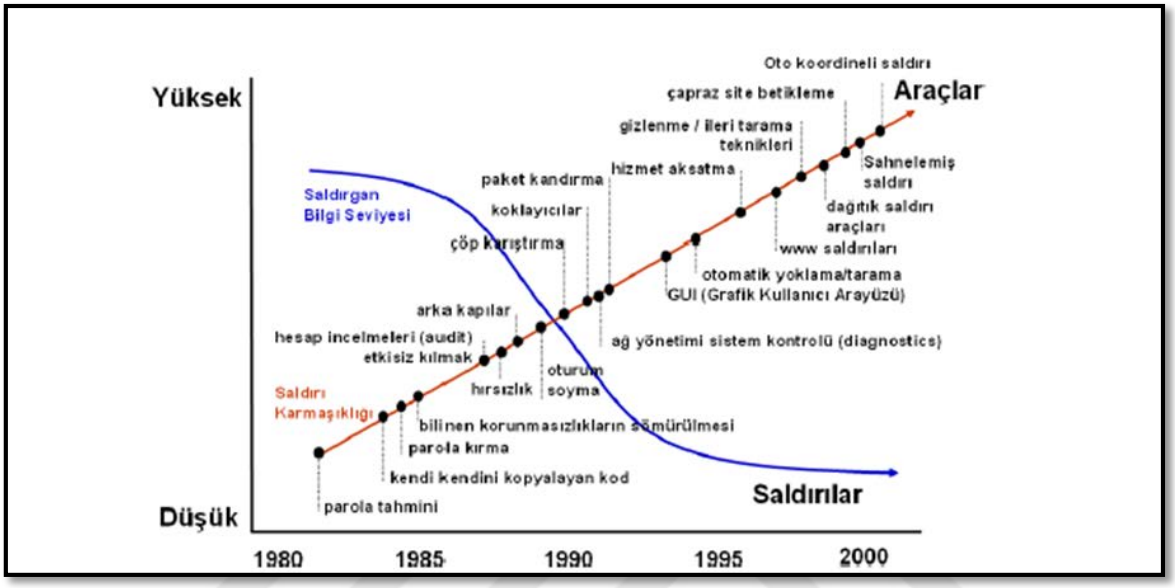
4.1. Bilgisayar Korsanlığı ve Kötücül Yazılımların Ortaya Çıkışı ve Gelişimi

Bilgisayar korsanlığı, ilk zamanlar 1960'larda Yuppilik adı verilen bir karşı kültür akımı olarak başlayan bilgisayar korsanlığı 1981 yılında ünlü olan Phreaking adı verilen yöntemle telefon şebekeleri açıkları üzerinden bedava görüşme yapmak amacıyla telefon sistemlerinin kırılmasıyla ilk basit örneklerini göstermiştir. Daha sonra 1980li yıllarda Almanya, Amerika gibi bilgisayar ağlarının yaygınlaşmaya başladığı ülkelerde bilgisayar korsanlığı oluşumları baş göstermeye başlamıştır. 1981 yılında kurulan Chaos Computer Club isimli bilgisayar korsanlığı grubu, Alman iletişim şirketi Bildschirmtext' in bilgi sistemlerine sızarak şirketi ciddi zararlara uğratmıştır. Amerika' da ise Warelords isimli grup Beyaz Sarayın ana bilgisayar sistemine sızmayı başarmıştır [9]. 1988 yılında ise bir üniversite öğrencisi ARPANET sistemine virüs bulaştırmış ve 60000 bilgisayarı etkileyerek sistemi kullanılamaz hale getirerek tarihin ilk kötücül yazılım ve ilk ciddi saldırısı olarak tarihe geçmiştir.

4.2. Bilgi Güvenliğine Yönelik Tehdit Çeşitleri

Basit düzeyde başlayan kötü niyetli ve kötücül saldırılar zaman içerisinde daha çok çeşitlenip artarak devam etmiştir. Şekil 4.2' de görüldüğü gibi teknoloji geliştikçe saldırılar da farklılıklar göstermektedir. İlk zamanlar kurumlarda notların yazıldığı kağıt çöplerini karıştırma ve parola tahmin etme gibi basit saldırıların yerini günümüzde çapraz site

betikleme (cross site scripting), dağıtık hizmet engelleme saldırıları (distributed denial of service), oto koordineli saldırı (auto coordinated attack), hizmet aksatma (denial of service) ve sahnelenmiş saldırılar (staged attacks) gibi çok daha karmaşık ve kapsamlı, çok daha detaylı, çok daha anlaşılması zor ve önlem alınması uğraştırıcı ve maliyetli saldırılar almıştır.



Şekil 4.2. Saldırı karmaşıklığı ve saldırgan teknik bilgisi [7]

Vural (2007), tehditlerin bilgi sistemlerinde etkili olabilmek için sistem açıklarını kullandıklarını ve bilgi varlıklarına etkilerinin tehlikenin gerçekleşme olasılığı sistemdeki açık miktarı ve bilginin değerine göre değiştiği bilgisi üzerinde durmuştur. Böylece tıpkı vücudumuza girmeyi bekleyen virüs ve bakteriler gibi bağışıklığın çöktüğü an ya da açık verdiği an etkili olmakta tıpkı bunun gibi bilgi sistemlerindeki güvenlik açığı fark edildiği an bilgi sistemlerine zarar vermektedir. Tehditlerin bilgisayar sistemlerine zarar verecek düzeye gelmesinde en önemli etken teknik ve bireysel zafiyetlerdir.

Uluslararası Telekomünikasyon Birliği (ITU, 2011), bilgi güvenliği ile ilgili tehditleri karakterine göre kazayla istemsiz olarak oluşan tehditler veya kasti olan tehditler, etkilerine göre aktif veya pasif tehditler, kaynağına ve gerçekleştirenlere göre farklı gruplara ayırmaktadır.

Bir sistemin ya da varlığın güvenliğine yönelik bilinçli eylemler kasıtlı tehditler grubuna girerken fiziksel arızalar, sistem veya yazılım hataları gibi eylemler kasıtlı tehditler grubunda yer almaktadır.

Pasif tehditler, sisteme zarar vermeden ve fark ettirmeden sistemden bilgi toplanmasını amaçlayan tehditlerdir. Aktif tehditler ise sisteme fizikse olarak zarar verilmesi, bilgilerin yok edilmesi veya tahrip edilmesi gibi sistemin durumuna ya da işleyişine yönelik olan tehditlerdir. Tehdit aktörü diye nitelendirilen tehdit kaynaklarından herhangi birini kullanarak saldırıyı gerçekleştiren birey ya da gruplardır. Güvenlik açığı olarak güvenlik sistemlerindeki zayıflıklar ve zafiyetler düşünülebilir. Bu zafiyetleri gören tehdit kaynakları ve tehdit aktörleri bilgi sistemine zarar vermektedir. Yazılım güncellemelerinin veya yeterli güvenlik konfigürasyonlarının yapılmaması, personelin yeterli teknik bilgisinin bulunmaması ve personelin güvenlik ihlallerine karşı bilgisinin ve farkındalığının düşük olması bilgi güvenliği ihlallerine neden olmaktadır.

Güldüren (2015)' e göre tehditler tehdit kaynağı açısından;

- Doğal afetler veya teknik arızalardan kaynaklanan tehditler,
- Prosedürel eksikliklerden kaynaklanan tehditler,
- İnsan faktöründen kaynaklanan tehditler,
- Kötücül yazılımlardan kaynaklanan tehditler

olmak üzere dört başlık altında toplanmıştır.

Güngör (2015)' e göre ise tehditler beş ana başlık altında toplanmıştır. Bunlar;

- Kaynağına göre tehditler,
- Saldırı hedefine göre tehditler,
- Kazanım amacına göre tehditler,
- Elde edilen sonuca göre tehditler,
- Bilgi sistemindeki hasara göre tehditler

Kaynağına Göre Tehditler

Doğası gereği bu tehditlerin en başında ve içinde insan yer almaktadır. Ancak bu tehditler sosyal, ideolojik, iktisadi veya kültürel olarak çeşitli nedenlerle gerçekleştiren kişi ya da grupların özellikleri benzerdir. Bu benzerliklerden dolayı bu tür tehditlerin kaynağı bireyler, hacktivist oluşumlar, siber suç örgütleri, işletmeler, bilgisayar korsanlığı platformları veya devletler olabilirler [9].

Bireyler: İlk saldırı türleri arasında yer almaktadır. Daha çok internetin halk arasında ilk

yaygınlaşmaya başladığı 90lı yıllarda özellikle kendini ispat etme, kendini kabul ettirme, başarılı olma veya milliyetçilik duygularıyla bir grup veya bir topluluk tarafından gerçekleştirilen saldırılardır. Daha donanımlı bilgiye sahip bireyler bilgi sistemlerinin açıklarını bularak bundan maddi kazanç elde etme amacıyla saldırılar da yapmaktadır. Ancak onar daha çok siber suç veya eylemci bilgisayar korsanlığı olarak tehdit kabul edilmektedir.

Hacktivist Oluşumlar: Bu oluşumların daha çok ideolojik amaçlar doğrultusunda saldırılarını gerçekleştirmektedirler. Bir düşünce, dünya görüşü, bir akım gibi daha idealist yaklaşmaktadırlar. Diğer oluşumlara nazaran oluşturduğu etki ve yoğun katılım olması sebebiyle diğer saldırılardan ayrılmaktadır.

Bilgisayar Korsanlığı Platformları: Kendilerini tanıtmak, yapılmayanı ya da yapılamayanı başarmak, milliyetçi duygular veya kendilerinden söz ettirmek gayesi taşıyan yer altı siber saldırı organizasyonlarıdır. Bu organizasyonlar hacktivist oluşumlar gibi ideolojik amaç taşıyan gruplarla anlaşarak çalışabildikleri gibi tek başlarına da çalışabilmektedirler. İstihbarat kuruluşları tarafından en rahat kullanılabilen oluşumlardır. Bu organizasyonların kendilerine ait saldırı teknikleri, isimleri, armaları ve sloganları bulunmaktadır.

Siber Suç Örgütleri: Reklam dolandırıcılığı, siber zorbalık, uluslararası dolandırıcılık, istismar, porno, şantaj gibi çeşitli alanlarda faaliyet gösteren siber suç örgütleridir. Bu grubun temel amacı maddi menfaatler elde etmektir.

İşletmeler: Özellikle bilgisayar korsanlığı gruplarının temel kazanç kapılarından birini oluşturmaktadırlar. Ticaret alanında yapılan ciddi rekabetler sonucu rakip firmaların itibarını zedeleme ya da rakip firmaların ticari sırlarını çalma veya işlerini yavaşlatarak veya durdurarak ticari zarar verme gibi amaçlarla bireysel ya da örgütsel saldırganlarla işbirliği yaparak saldırılara karışmaktadır.

Ülkeler: Ülkeler arasında rekabet, politikalar arası uyumsuzluk ile ortaya çıkan siyasi gerilimler veya askeri ya da ileri endüstri alanında yapılan casusluk faaliyetleri gibi sebeplerle ülkelere yönelik kaynağını yine ülkelerin oluşturduğu çok ciddi siber saldırı tehditleridir.

Saldırı Hedefine Göre Tehditler

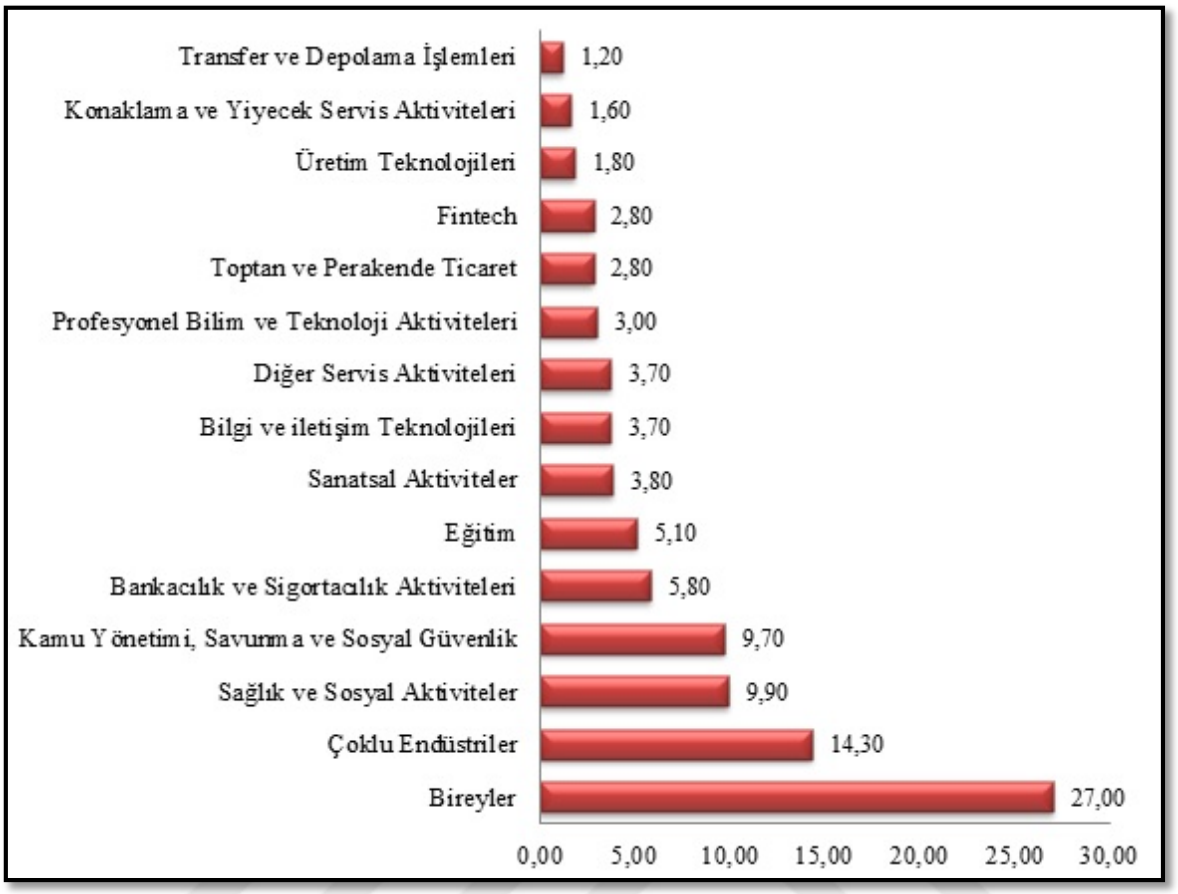
Saldırıların hedefinde bireyler, siyasi oluşumlar, işletmeler ya da kamu kuruluşları veya devletler olabilmektedir.

Kişisel Kullanıcılar: Bireylerin hedefte olması çok sık rastlanan durumlardır. Çoğunlukla çevrimiçi kimlik hırsızlığı saldırılarının hedefi olmaktadırlar. Kötü niyetli yazılımlar veya programlar (malware), Truva atı (trojan), solucan (worm) aldatıcı nitelikli e-posta veya aldatıcı internet siteleri (hoax), oltalama (phishing) saldırıları gibi kişisel bilgisayarlar ele geçirilerek kişinin her türlü kişisel bilgisi, bankacılık bilgilerini öğrenerek maddi zararlar verebilecekleri gibi kişinin bilgisayarına casus yazılım yerleştirerek bilgisayarları birer zombiye yani köle bilgisayara dönüştürülmesi mümkündür. Böylece köleleşen bilgisayarlar istedikleri amaçlar doğrultusunda kullanılabilmekte büyük botnet saldırıları yapılmaktadır.

İşletmeler: İşletmeler yukarıda anlatıldığı gibi saldırının kaynağı olabildikleri gibi saldırıların hedefinde de olabilirler. Birden fazla ülkede faaliyet gösteren çok uluslu şirketler (Google, Facebook, Youtube, Ebay, vb.) de hem şahısların hem bilgisayar korsanlarının hatta devletlerin hedefi haline gelebilmektedir. Çünkü bu çok uluslu şirketlerin bilgi sistemlerinin çok iyi ve güvenlikli korunuyor olması ve bu koruma kalkanının aşılması bilgisayar korsanları arasında başlı başına bir saygınlık sebebi kabul edilmektedir. Ancak kritik altyapıları işleten özel sektör firmaları da bu saldırılardan payını almaktadır.

Siyasi Teşkilatlar: Özellikle siyasi partiler kendi düşüncelerini benimsemeyen bireylerin veya hacktivist oluşumların saldırısına maruz kalabilmektedir.

Kamu Kurumları (Devletler): E-devlet hizmetleri gibi toplumsal düzenin sağlanmasında kullanılan yapıları ve kritik bilgi alt yapılarını elinde bulunduran devlet kurumlarıdır. Bu yönüyle kamu kurumlarında bir şekilde internete bağlı olarak topluma hizmet veren bilgi sistemleri de bireyler, hactivist oluşumlar ve başka devletler tarafından en çok saldırıya uğrayan sistemler arasında yer almaktadır.



Şekil 4.3. 2019' da siber saldırılardan etkilenen sektörlerin yüzdelik dağılımı (Hackmageddon.com)

Kazanım Amacına Göre Tehditler

Saldırılar maddi kazanç sağlamak amacıyla yapılabileceği gibi askeri, ideolojik, politik ve askeri sebepler gibi maddi kazanç sağlamayı amaçlamayan saldırılar da olabilmektedir. Amaçları ne olursa olsun saldırganlar her zaman sistemin açık vermesini beklerler ve fırsat buldukları an saldırı gerçekleştirerek sistemi işlemez hale getirmektedirler.

Elde Edilen Sonuca Göre Tehditler

Bu sefer amaç, bilgi sisteminin açıklarını bularak sistemi işlemez hale getirmek değil casusluk, gizli bilgileri çalma veya yok etme, siber terör ortamı oluşturma gibi eylemlerle çok kapsamlı zararlar vermektir.

Siber Suç (Siber Korsanlık): Suç denildiğinde klasik ceza kanunlarında yer alan suçlar anlaşılmamalıdır. Siber Suç kavramı ile genelde anlatılmak istenen şey bilişim sistemine yönelik veya bilişim sistemlerinin kullanıldığı suçlardır. Geniş açıdan ele alınırsa siber

suçların farklı şekillerde ve içeriklerde olabileceği ve klasik işlenen suçlarla da bağlantısının olabileceğidir. Siber suçlar bilişim suçlarının daha geniş alana yayılan gelişmiş ve karmaşık türleri olup siber uzayda faaliyet gösteren şeklidir. Bu faaliyeti gerçekleştiren kişilere hacker yada cracker adı verilmektedir.

Eylemci Saldırılar: Hacktivist grupların kendi ideolojilerini anlatmak veya belirli bir duruma tepkilerini belli etmek amacıyla belirli hedeflere karşı yapılan eylemsel saldırılardır.

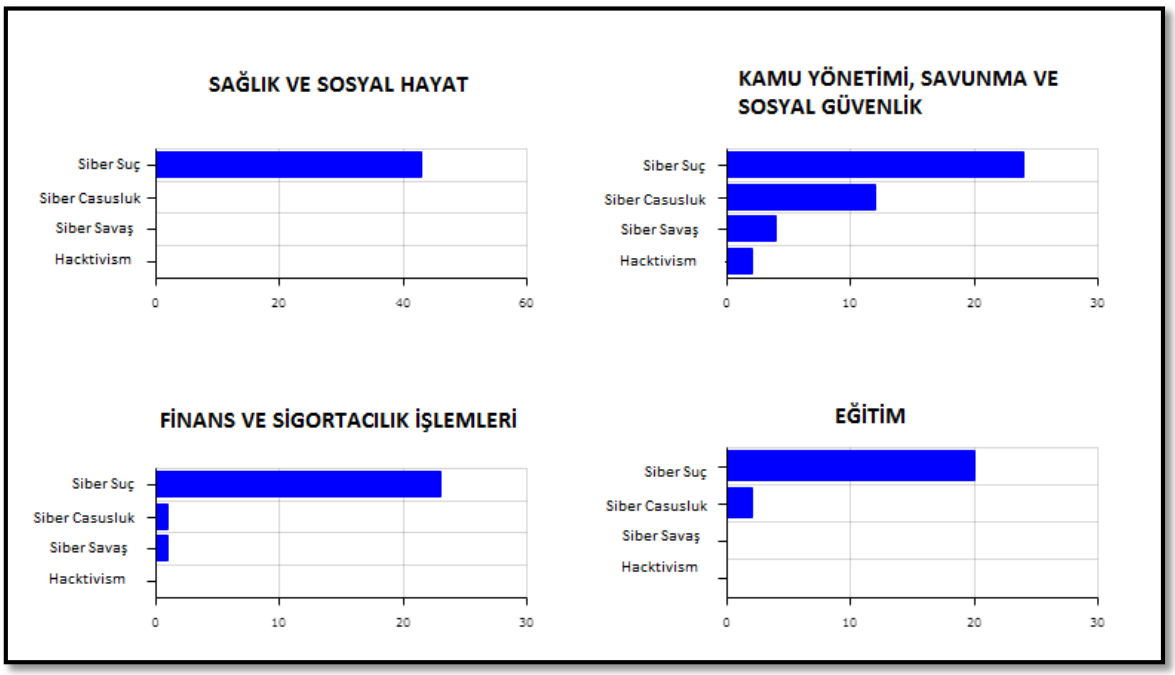
Siber Casusluk (Siber İspiyonaj): Bir şirket ya da kuruluşa alınmak istenen gizli bilgilerin çalınması amacıyla yapılabileceği gibi kişisel, gizli veya hassas bilgiler ile teknolojik sırlar veya askeri bilgilerin ele geçirilmesi amacıyla da yapılabilmektedir. Bu saldırılarda genel olarak amaç tabiri caizse karda yürüyüp izini belli etmemektir yani en az izi bırakarak ya da iz bırakmadan elde edilmesi istenen bilgiye ulaşmaktır. Bu saldırı türleri genellikle yalnızca o iş için yazılmış olan trojan veya solucan yazılımlarla yapılmış olup daha önce hiç benzeri olmadığından antivirüs programları tarafından da tespit edilememektedir. Diğer yandan sosyal ağlar kullanılarak bu yazılımlar hedef olan kurum, kuruluş veya organizasyondaki kimselerin kişisel bilgisayarlarına bulaştırılabilmektedir.

Siber Terör: Geleneksel terör örgütlerinin faaliyetlerini son yıllarda siber ortama taşımaları neticesinde ortaya çıkan bir siber saldırı türüdür. Bu saldırılarda amaç ülkenin sağlık, finans, eğitim, enerji, ulaşım gibi toplumsal düzenin hayati sektörleri hedef alınarak ülkede huzursuzluk oluşturmaktır.

Siber Sabotaj: Genellikle bir ülke için önemli olan askeri, teknolojik veya nükleer faaliyet ya da projelerin durdurulması veya ilerlemesinin yavaşlatılması amacıyla yapılan saldırılardır. Bu saldırılara en iyi örnek 2010 yılında Amerika ve İsrail tarafından geliştirilen Stuxnet isimli bir solucanın İran' ın nükleer programını yaklaşık iki ay kadar geciktirdiği tahmin edilmektedir. Solucan nükleer programın uranyum zenginleştirme aşamasında önemli rol oynayan ve Siemens şirketi tarafından yapılan SCADA isimli sisteme Windows işletim sistemi yoluyla bulaştırılarak kullanılan yazılımlar bozulmuştur. Bu olay milyarlarca dolarla kurulan sistemlerin basit bir solucanla nasıl sabote edileceğini gösteren en iyi örneklerden biridir.

Siber Savaş: Siber saldırıların en iyi organize edilmiş ve en gelişmiş düzeyde geniş bir

alanda yapılan şeklidir. Siber savaş içinde siber sabotaj, siber casusluk ve siber terör gibi kavramları da içine alabilmektedir. Siber savaşın bu durumlarda farkı ise hedef alınan düşman ülkenin tüm kritik altyapıları ve bilgi sistemleri hedef alınarak yoğun ve kesintisiz bir saldırı ile çökertmek ve ciddi zararlar vermeyi amaçlamasıdır. Buna en iyi örnek ise Rusya ve Estonya arasında 2007 yılında bir heykel tartışması ile başlayan ve büyüyen krize Rusya'nın Estonya' ya açtığı siber savaş neticesinde Estonya'nın bankaları, bakanlıkları, parlamentosu da dâhil olmak üzere pek çok sisteminin zarar görmesi ile bankacılık faaliyetlerinin durma noktasına gelmesiyle son bulmuştur.



Şekil 4.4. 2019' da en çok siber saldırıya uğrayan sektörlerin etkilendiği saldırı türleri (Hackmageddon.com)

Bilgi Sistemindeki Hasara Göre Tehditler

Bu tehditler bilgi güvenliğinin temel öğeleri olan gizlilik, bütünlük veya erişilebilirlikten birine ya da birkaçına yönelik olabilmektir.

Gizliliğe unsuruna yönelik tehditler

Kötü niyetli yazılımlar veya program parçaları (malware) olarak bilinen ve Truva atı (trojan), virüs, solucan (worms), bukalemun, çerezler gibi türleri bulunan yazılımsal tehditlerdir. En sık kullanılan türleri şunlardır;

Virüs: Bilgisayar ve internet geliştiğinden beri kullanılagelen bir terimdir. Genellikle

zararlı yazılımları ifade etmek için kullanılsa da her zararlı yazılı virüs değildir. Virüsler, bir bilgisayar programlarına yama programla birleşip kendini kopyalayarak başka sistemlere de yayılabilen, bilgi sistemlerinde gizlenebilen yazılımlardır. Virüsler günümüzde ciddi bir küresel sorun haline gelmiştir.

Truva Atları (Trojanlar) Yasalara uygun görünen faydalı fonksiyonları varmış gibi görünüp aynı zamanda gizli ve güvenlik sistemlerini geçecek zararlı fonksiyonlar içeren bilgisayarları uzaktan yönetmek için arka kapılar açan programlardır. Bu programlarla bilgisayar korsanları, sistem ayarlarını değiştirebilir, bir sistem biriminin meşru olarak yetkilendirmesini aşarak kullanıcının hassas verilerini ve kişisel bilgilerini ulaşabilirler.

En tipik ve tehlikeli olanları botnetlerdir. Botnetler, bilgisayarlar ve sistemler yetkisiz kişilerin kontrolüne girebilirler. Böylelikle bilgisayar kullanıcısının haberi olmadan bilgisayarını çok ciddi suçların işlenmesinde kullanabilirler. Botnet ordusunun parçası haline gelen köle bilgisayarlar bir sisteme aynı anda yönlendirilerek bu sistemin hizmet veremez hale gelmesine neden olurlar. Botnetleri bu kadar tehlikeli kılan bir diğer sebep ise botnet bilgisayarın, suç unsuru olan dosya ve görüntülerin yayınlanmasında, spam faaliyetlerinde ve kullanıcının kimlik bilgileri kullanılarak ciddi suçların işlenmesine olanak sağlamasıdır. Spamlar yani diğer adıyla istem dışı elektronik postaların büyük kısmı reklam amaçlı olmakla birlikte bilgisayarlara zararlı yazılım bulaştırmak veya bir konuda kendi düşüncelerinin yaymak maksadıyla da gönderilmektedir.

Truva atları genellikle ücretsiz kullanılan yazılımlarla birlikte sisteme girmektedirler. Bunlardan korunmanın en kolay yolu bilinmeyen programlardan uzak durmaktır. Ancak bu tarz yazılımlar bazen bir elektronik posta ekinde gönderilen dosyalarda veya mesajda bulunan bağlantılar tıklandığında açılan web sayfaları yoluyla bulaşabilmektedir.

Günümüzde bu tür tehditler şirketler tarafından rakip şirketten bilgi çalmak veya ülkeler tarafından istihbarat maksatlı üretilmektedir. Bu tür zararlı yazılımlara APT (Advanced Persistent Threat) olarak isimlendirilmektedir. APT' ler genellikle hedefe gizlice girerek gerekli bilgiyi almak üzerine programlanabilmektedir. Bu saldırıların en önemli özelliği enerji, ulaşım gibi belirli sistemleri veya belirli programlama dillerinde çalışan sistemleri hedef almakta ve birkaç virüs yazarı tarafından yazılamayacak kadar komplike yapılara sahip olmalarıdır.

*Solucan (Worms):*Solucanlar tıpkı virüsler gibi kendini birebir kopyalayabilme yeteneğine sahiptir. Ancak bunu kendi kendilerine yapabilmektedirler. Öncelikle bilgisayarda veri iletimi yapan fonksiyonları ele geçirmekte ve bu şekilde veri transfer yollarını kullanarak tüm sisteme yayılmaktadır. Solucanların en büyük tehlikesi büyük miktarlarda çoğalabilmeleri ve kullanıcının veri ve dosya iletim yöntemlerini kullanarak bağlantılı tüm bilgisayarlara bulaşabilmekte ve kendilerini tüm elektronik posta adreslerine e-posta yoluyla gönderebilmektedirler. Bu durumda ağ trafiğinin yavaşlamasına neden olmaktadır. Solucanlar virüsler gibi değildir, onlar virüsler dosya açılmadan ortaya çıkmazken bunlar kullanıcı müdahalesi olmada çoğalabilmektedir. Ayrıca virüsler gibi taşıyıcı bir dosya yada programa ihtiyaç duymadıkları için sistemde tüneller açarak başka bilgisayarların denetimini de uzaktan ele geçirebilmektedir.

Bukalemun: Çok kullanıcılı sistemlerde etkili olan bu yöntem kullanıcı adları ve parolaları taklit yeteneği ile kendini dosyalara saklayarak normal bir program gibi çalışır. Daha sonra sistemin bakım için kapatılacağı uyası verir. Bu sırada arka planda sisteme programı yerleştiren kimse sistemdeki gizli dosyalara erişerek bilgileri ele geçirmektedir.

Çerezler (Cookies): Bunlar bilgisayarın sabit diskine kullanıcı izinleri çerçevesinde kullanıcıdan ön izin alınarak yüklenmektedir. Aslında ortaya çıkış itibariyle arama motoru aranan kelime analizi, e-ticaret sitelerinin kullanıcı ve ziyaretçi istatistikleri veya iyi niyetli olarak tüketici davranışlarını anlamak ve pazarlamak yapmak gibi ticari bir takım amaçlar için kullanılmaktadır. Ancak şantaj, kişisel verileri açığa çıkarmak ve mahremiyet ihlalleri gibi amaçlarla da kullanılmaktadır.

Bütünlük unsuruna yönelik tehditler

Bütünlük öğesine karşı yapılan saldırılar daha çok bilgi sisteminde bulunan bilgilerin değiştirilmesi, tahrip edilmesi ya da yok edilmesi gibi amaçlar taşımaktadır. Bu tehditler daha çok bilginin önemli olduğu kritik altyapılar veya sayısal veri merkezleri gibi veritabanı kullanan bilgi sistemlerini hedef belirlemektedir. Bu sistemlere erişim için saldırganların sisteme yönetici olarak giriş yapması gerekmekte ve uygun şifre ve kullanıcı adlarını temin etmek için kriptografik yöntemler ya da virüs, solucan, truva atı gibi kötücül yazılımlar kullanmaktadırlar.

Erişilebilirlik unsuruna yönelik tehditler

Erişilebilirliğe yönelik saldırılarda hedef internet üzerinden hizmet veren web siteleri ya da e-ticaret, e-devlet hizmetleridir. Hizmet aksatma saldırılarında pek çok yöntem bulunmaktadır. Ancak en çok kullanılan yöntemler ise botnet veya DDoS (Distrubuted Denial of Service) saldırılarıdır. Bu yöntemlerin tamamının amacı aynıdır. Sunucu bilgisayarla çok fazla sayıda sahte bağlantı kurarak sunucuyu gerçek taleplere cevap veremez duruma getirerek gerçek bağlantıların önlenmesidir. Günümüzde DDoS saldırıları binlerce bilgisayarın kullanılmasıyla gerçekleştirilmektedir. Böylece bu tür saldırıların gerçek saldırganlarını bulmak mümkün olmamaktadır. Bu saldırılarda kullanılan bilgisayarlar botnet adı verilen zararlı yazılımlarla köle bilgisayar haline getirilmektedir. Kullanıcıları farkında olmadan bilgisayarlarına yüklenmekte ve sahibinin talimatı gelene kadar faaliyet göstermemektedir. Bu sebeple anlaşılması mümkün olmamaktadır.

Tüm bu saldırılar dışında mantık bombası (logicbomb), reklam destekli yazılımlar (Adware), Casus yazılımlar (spyware), arka kapı (backdoor), Sazan avlama-oltalama (phishing), zincir e-posta ve internet aldatmacası (hoax), klavye işlemlerini kaydeden programlar (keyloggers), aldatma (ipspoofing), şebeke trafiğinin dinlenmesi (sniffing), formjacking saldırısı, Living of the Land (Lotl), ransomware (fidye yazılımları) ve sosyal mühendislik saldırıları gibi saldırı türleri de bulunmaktadır.

Mantık bombası (Logic Bomb): Giriş yaptığı sistemin sistem tarihini kontrol ederek daha önceden planlanan ve programlandığı zamanda harekete geçerek programcısından gelen talimatları yerine getiren zararlı yazılımlardır.

Salam Tekniği (Salami Techniques): Genellikle bankacılık ve finans sektörlerinde kullanılmaktadır. Amaç hesaplarda bulunan paraların virgülden sonraki kısımlarının başka bir hesaba aktarılarak orada biriktirilmesidir [47]. Maddi kazanç amaçlı yapılan saldırı tekniğidir.

Arka kapı (Back Door): Zafiyetleri kullanan bir yazılım türüdür. Bilgisayar üzerinde normal yapılan taramalarla bulunamayacak şekilde, kimlik doğrulama aşamalarını atlatarak kurulan ve bu açıkları bilen kişiye o bilgisayara uzaktan erişmeyi sağlayarak bilgisayarı ele geçirmeyi veya kişisel bilgileri çalmayı sağlayan yöntemlerdir [36].

Reklam Amaçlı Yazılımlar (Adware): Reklam veren firmalar tarafından reklamların programın içine gömülmesiyle kullanıcının bu reklamlara tıklaması amaçlanmaktadır.

Veri Aldatmacası (Data Diddling): Bilgisayara veri girişi sırasında yanlış veriler girilmesi veya veri saklama ortamında saklanan verilerin çeşitli yöntemlerle değiştirilmesi ya da silinmesi işlemlerinde bu yöntemle yapılabilmektedir [46].

Casus Yazılımlar (Spyware): Casus yazılımlar genellikle ücretsiz deneme sürümlerine eklenerek kullanıcılar tarafından bilgisayara kurulması sağlanmaktadır. Bu tür yazılımlara örnek olarak anne-babalar için çocuk izleme yazılımı, eş takip etme yazılımı gibi isimlerle ortaya çıkmaktadır [24]. Bu yazılımlar kurulumu sırasında gerekli uyarıları yapmaktadır. Ancak o kadar uzun ve hukuki terimler içeren sözleşmelerde gözden kaçabildiği gibi sözleşmenin okunması ve kurulum sırasında yer alan hızlı ve gelişmiş seçeneklerinden ayarlama yapmak çok zahmetli geldiği için hızlı seçeneğinin seçilmesiyle kullanıcılar kendi rızalarıyla özel bilgilerini vermiş olurlar. Aslında kullanıcılar tarafından gösterilen dikkat ve özen bu sebepten ortaya çıkan problemlerin engellenmesini sağlayacaktır.

Çöpe Dalma (Scavenging): Önceleri bilgisayar sistemleri üzerinde yapılan işlemler sonucu yazıcılarda üretilen ve daha sonra kullanılmamak üzere atılan malzemeler üzerinde kalan bilgilerin toplanması şeklinde olan yöntem günümüzde bilgi sistem hafızasında bulunan ve artık kullanılmayacak silinmiş bilgilerin gelişmiş çeşitli yöntemlerle geri getirilmesi şeklinde gerçekleştirilmektedir [46].

Yerine Geçme (Masquerading): Erişme yetkisi olan kullanıcıların şifreleri ve bilgileri kullanılarak erişim yetkisi sınırlı olan ya da yetkisi hiç olmayan kullanıcıların sisteme erişim sağlamasıdır [46].

Şebeke Trafiğinin Dinlenmesi (Sniffing): Kelime anlamı itibariyle koklamak anlamına geldiğinden anlamının gereği olarak ağda bulunan bilgisayarlar arasındaki veri trafiğini koklar yani dinler. Şebeke trafiğinin dinlenmesiyle iki taraf arasında gelip giden tüm veri paketleri yakalanarak saklanmaktadır. Daha sonra içinden elde edilmek istenen bilgi alınmaktadır. Bu yöntem bilgisayar korsanlarının en çok kullandığı yöntemlerden bir tanesidir. Bu tehditten korunmak için bilgisayarlar arası gidip gelen verinin şifreli olması gerekmektedir. Böylece veri paketi ele geçirilse bile şifreli olduğundan istenilen bilgiye

ulaşılamayacaktır.

Sazan Avlama - Oltalama (Phishing): Yemleme, oltaya düşürme gibi isimleri de bulunmaktadır. Bu yöntemde bir web sitesinin sahtesinin yapılarak kullanıcılardan bilgilerini girmeleri istenmekte ve bu yolla kişisel bilgileri, banka bilgileri, şifreleri çalınmaktadır. Bu şekilde kullanıcılara ciddi maddi kayıplar yaşatmaktadırlar. Bu dolandırıcılık yönteminde sahte siteye genellikle e-posta yoluyla kullanıcılar yönlendirilmektedir. Bu e-postalarda bilgilerini güncellemesi gerektiği, bir ödül kazandığı ya da hesabında bir hareketlilik olduğu ve kontrol etmesi gerektiği gibi bahaneler ile kullanıcıların kimlik, adres bilgilerini güncellemeleri veya banka bilgilerini hesabını kontrol etmeleri gibi bahaneler kullanılmaktadır. Kullanıcı bilgilerini güncellediğini ya da kontrol ettiğini sanırken aslında dolandırıcılara istediği bilgileri vermiş olur. Bu yöntemden korunmak için dikkatli ve bilgili olmak, nereden gelirse gelsin güvenli olmayan bu tarz mesajlar veya maillere itibar etmemek ve açılan web site bağlantılarının güvenli olup olmadığını kontrol etmek hatta internet sitelerinin lisanslarının geçerliliklerini kontrol etmek gerekmektedir [23].

Klavye İşlemlerini Kaydeden Programlar (Keyloggers): Bu programlar adından da anlaşılacağı üzere klavye işlemlerini kaydeden programcıklardır. Bunlar fark edilmeden klavyede basılan her tuşu kaydederek sahiplerine yani bilgisayar korsanlarına göndermektedir [23]. Bu programlar web sitelerinde gezinirken kendiliğinden indirme işlemi başlatan ve sisteme dahil olan programlardır. Bu program sisteme yerleştikten sonra kullanıcının her tuş kullanımını kaydeder. Kaydedilen veriler sisteme programı kuran saldırgana e-posta vb. çeşitli yöntemlerle gönderilmektedir. Bankaların veya çeşitli ticaret sitelerinin sanal klavye kullanarak şifre girdirme isteğinin temel sebebi budur.

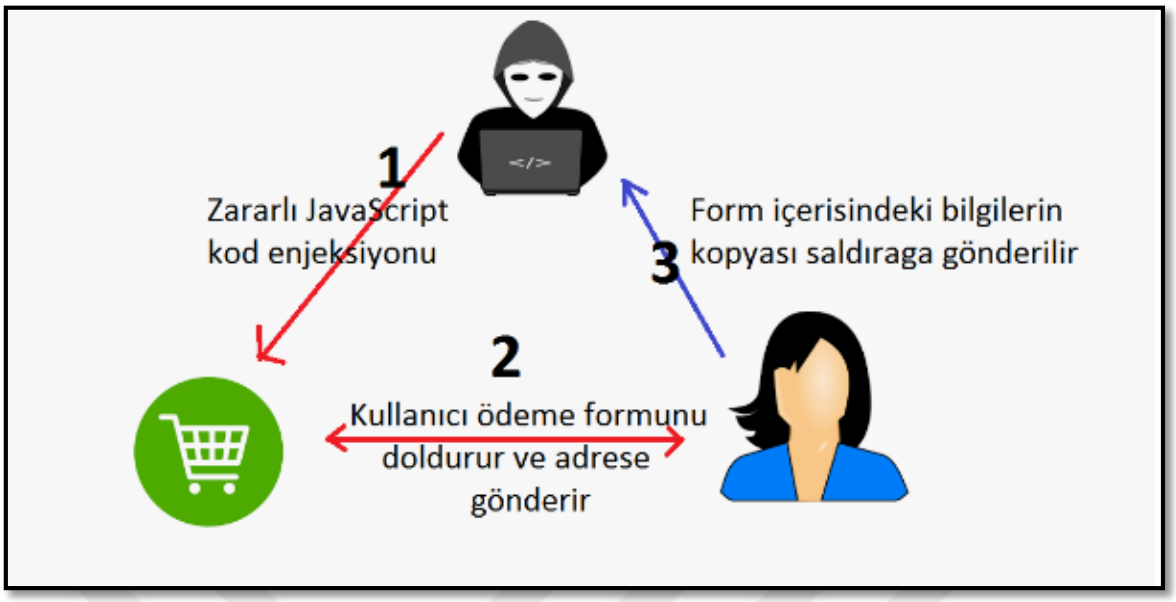
*Süper Darbe (Super Zapping):*Bilgisayar sistemlerinin çeşitli sebeplerle kilitlenmesi veya arızalanması durumunda kısa sürede güvenlik kontrollerinin aşılarak sistemin düzeltilmesi için geliştirilmiş programlardır [46]. Bu tarz programlar sistemlerde geniş çaplı tahribat yapmak isteyen saldırganlara, tüm güvenlik önlemlerini aşabilmelerinden dolayı çok büyük kolaylıklar sağlamaktadır.

Zincir E-Posta ve İnternet Aldatmacası (Hoax): Çok fazla kişinin birbirine gönderdiği ve insanların ilgisini çekebilecek şekilde dini, duygusal, maddi içerikli sömürü mesajlarının

ya da e-postaların alıcının rehberindeki veya e-posta adresindeki kişilerle paylaşmasını isteyen mesaj veya elektronik postalardır. İnternet Aldatmacası ise, büyük bir kuruluş veya ünlü bir şahıs hakkında yalan haber ve hikayeler üreterek kişiyi maddi ve manevi olarak yıpratma ve kayba uğratma ya da ulusal güvenliği tehdit edecek durum olduğu havası oluşturularak kaos yaratmaktır. İletiler güvenilir bir kaynaktan geliyormuş gibi gönderilmekte ve kullanıcının bu mesaj ya da e-postayı tüm listesiyle paylaşması sağlanmaktadır. Böylece elde edilen e-posta adresleri para karşılığı üçüncü kişilere satılmakta ya da spam göndermede kullanılmaktadır [36].

Aldatma (Spoofing): Bilgisayarlar arasında haberleşme çeşitli ağ protokolleri kullanılarak yapılmaktadır. Bu protokollerde bağlantı kurmanın ilk aşamasında bilgisayarlar birbirlerine kendilerini ip adresleriyle yaparlar. Bu aşamada bilgisayarlardan birinin kendi gerçek kimliğini yani ip adresini gizleyerek göstermemesine ip spoofing adı verilmektedir. Sahte ip paketi alan bilgisayar bunu anlayamaz. Genellikle başkasının ip adresinden e-posta gönderilmesi ya da adı kullanılarak forumlara yorum yazılması şeklinde karşımıza çıkmaktadır [23]. Teorikte bu durum mümkün olmamakla birlikte karşı tarafın tamamen ele geçirilmesi gerekmektedir. Aldatma genellikle bir web sitesini işlemez hale getirmede saldırı esnasında ip adresini saklamak için kullanılmaktadır.

Formjacking: Bilgisayar korsanlarının hedef internet sitesinin ödeme formuna zararlı javascript kodlarını enjekte ederek, bu formda doldurulan her bilginin kendilerine gelmesini sağlarlar. Böylece müşterilerin kart bilgilerini çalarak maddi menfaat elde ederler [48].



Şekil 4.5. Formjacking saldırısı çalışma tekniği [48]

Symantec 2019 İnternet Güvenliği Tehdit Raporuna göre bu saldırı türünün saldırganların favorisi haline geldiğini ve aylık ortalama 4800 web sitesinin bu yollarla milyonlarca dolar zarara uğradığı raporlanmıştır. Saldırganlar bu yöntemi kullanarak geçtiğimiz yıl İngiliz Havayolları müşterilerinin ödeme bilgilerini çalmışlardır.

Fidye Yazılımları (Ransomware): Bu yazılımlar şifreleme ve kilitleme gibi iki farklı şekilde hedefe saldırırlar. Birinci yöntemde hedef bilgisayarda bulunan bütün veriler dosyalar şifrelenerek kullanıcının erişimini engellemektedir. Şifrelenen dosyaların şifrelerinin açılması ve mağdur kullanıcıya erişimin verilmesi için saldırgana ödeme yapılmasını isterler. İkinci türde ise hedef bilgisayar tamamen kilitlenerek kullanıcıya tamamen kapatılır ve kilitin çözülmesi için saldırgana para ödenmesi istenilir. Bu saldırı türü her zaman parayla ilgilidir ve diğer saldırı türlerinden farklı olarak mağdur kullanıcıya bilgi verilir, saldırıdan kurtulması için takip etmesi gereken yol anlatılır. Genellikle saldırganın kimliğinin açığa çıkmaması için ödemeler kripto paralar cinsinden istenilir. Bu saldırı türünde talep edilen ortalama para miktarı 300$ civarındadır. Ancak para ödenmesine rağmen saldırıdan kurtulmak her zaman mümkün olmamaktadır. Karspersky firmasının verdiği rakamlara göre fidye yazılımlarına parasını ödemesine rağmen dosyalarını kurtaramayanların oranı yaklaşık %20'dir.

Living of the Land (Lotl): Bu saldırı türünde saldırganlar hedeflenen bilgisayarda zaten yüklü olan araçları (tools) kullanarak doğrudan bellekte basit komut dosyaları ve kabuk

kod (Shell code)lar çalıştırarak hedef bilgisayarın kontrolünü ele geçirirler. Sabit diskte çok küçük boyutta dosyalarla çalıştıkları için ya da dosyasız çalıştıklarından geleneksel güvenlik araçları tarafından tespit edilmesi pek mümkün olmamaktadır. Bu sebeple saldırının engellenmesi pek mümkün olmamaktadır.

Bu yöntemde bilgisayardaki sistemde yasal olarak kullanılan araçlar kullanıldığından mağdurların ve güvenlik yazılımlarının kötü amaçlarla ne zaman sömürüldüklerini bilmeleri zordur. Yalnızca LotL araçlarını kullanarak, saldırganlar herhangi bir kötücül yazılım kullanmaya gerek kalmadan istenilen cihaza uzaktan erişim sağlayabilir, verileri çalabilir veya işlemlerini durdurabilirler. Symantec 2019 İnternet Güvenliği Tehdit Raporuna göre işletmelere ve tedarik zincirlerine yönelik saldırılarda gözde haline gelen LotL saldırıları %78 oranında artmıştır.

Sosyal Mühendislik Saldırıları: İnsanların zaaflarından yararlanmak üzere çeşitli aldatmacalar kullanarak hedef kişi veya sistem hakkında bilgi edinmek, veri ele geçirmek üzere sisteme girmeyi amaçlamaktadır. Oltalama, spam, hoax gibi saldırılar da aslından birer sosyal mühendislik saldırısı olarak kabul edilebilirler. Çünkü bu saldırılar kullanıcıyı kandırarak çeşitli eylemler yaptırmayı hedeflemektedirler.

5. TEHDİTLERE KARŞI ALINMASI GEREKEN ÖNLEMLER

Genel olarak bilgi güvenliğini sağlamak için öncelikle en küçük birimin yani bireyin alması gereken kişisel veri güvenliği önlemlerini daha önceki yapılmış çalışmalardan aşağıdaki şekilde özetleyebiliriz [18, 64].

- Web sayfalarında istemsiz olarak açılan pencerelerin kapatılması,
- Web sayfalarında güvenlik sertifikalarının kontrol edilmesi,
- Bilgisayarda güncel güvenlik yazılımının bulundurulması,
- Lisanslı işletim sistemleri ve lisanslı yazılımların kullanılması,
- Bilgisayarda kullanılan yazılımların (özellikle antivirüs ve işletim sistemi) güncel olması,
- Farklı amaçlar için kullanılan şifrelerin (yani internet alışveriş siteleri, banka şifreleri, bilgisayar açılış şifresi, vb.) birbirinden bağımsız olması, farklı simge, rakam, karakter içermesi ve en az 8 karakterden oluşması,
- Şifre hatırlatma için kullanılan gizli soruların ve yanıtlarının zor olması,
- Bilgisayarda yer alan önemli olduğu düşünülen dosyaların güvenli bir ortama yedeklerinin alınması,
- Güvenli olmayan ve kaynağı bilinmeyen e-postaların açılmadan silinmesi,
- E-postalarda gelen bilinmeyen web sayfalarına giriş işlemi yapılmaması,
- Şifreli işlemlerde sayfadan ‘Oturumu Kapat’ komutuyla çıkılması,
- Kablosuz ağ modemlerinin şifresiz kullanılmaması (fakat kolay şifreler de belirlenmemeli Örn:12345),
- Kablosuz internet modemlerinin parolalarının belirli aralıklarla değiştirilmesi,
- Sosyal paylaşım sitelerinde kişisel bilgilerin paylaşılmaması,
- Sosyal paylaşım sitelerinde mümkün olduğunca özel olan fotoğraf, video gibi medyaların paylaşılmaması,
- Sosyal ağlarda mümkün olduğunca ve gerekmedikçe yer bildirimi yapılmaması,
- Sosyal paylaşım sitelerinde yabancı kişilerden gönderilen arkadaşlık isteklerinde dikkatli davranılması,
- Sosyal paylaşım ağlarından veya e-posta yoluyla gelen para, kontör, vb. isteklerin dikkate alınmaması,
- Sosyal paylaşım veya sohbet sitelerinde yabancı kişiler ile görüntülü, sesli ve hatta gerçek hayatta yüz yüze iletişime geçilmemesi,

- Bankacılık ve çevrimiçi alışveriş işlemlerinin ortak alan bilgisayarlarından yapılmaması,
- Çevrimiçi alışveriş işlemlerinde düşük limiti sanal kartlar kullanılması,
- İnternet üzerinden tehdit, şantaj veya cinsel istismara maruz kalma durumlarında hukuksal yönlerinin öğrenilerek bu yollara başvurulması

olarak sıralamak mümkündür.

Kişilerin bilgi güvenliği kadar kişilerin bilgi güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğini de sağlamak da önemlidir. Kurumsal bilgi güvenliğini sağlamak için çok çeşitli teknolojiler kullanılmaktadır. Bu sistemlerden başlıcaları güvenlik duvarları, dıştan içe saldırı tespit sistemleri ve içten dışa saldırı sistemleridir. Ağlar arasında taşınan verinin bütünlüğü ve gizliliğini sağlamak için kimlik doğrulama ve gönderilen verilerinin şifrelenmesi tercih edilmektedir. Ayrıca yukarıda sayılan kişisel bilgi güvenliği önlemlerine ek olarak kurum personeli tarafından uygulandığında kurum bilgi güvenliğine katkı sağlayacak bazı önlemler bulunmaktadır. Bunlar;

- Kötücül yazılımlardan koruma programlarının ve işletim sistemlerinin güncellemelerinin düzenli olarak yapılması,
- Bilgisayara kurulan yazılımların paylaşıma açık olup olmadığına dikkat edilmesi,
- Bilgisayar ekranlarının şifreli ekran koruyucularla korunması,
- Bilgisayarda işlem yapılmayan sürelerde ekranı kilitlemeden ayrılmaması,
- Bilgisayar başından uzun süre ayrı kalındığında kurum bilgi sistemlerinden çıkış yapılması,
- Disk ve dosya paylaşımlarında dikkatli olunması,
- Önemli dokümanların parola koyularak korunması veya şifrelenerek saklanması,
- Gizli ve önemli bilgilerin güvenli olan yollardan gönderilmesi,
- Önemli bilgi içeren belge ve dosyaların düzenli olarak yedeklenmesi

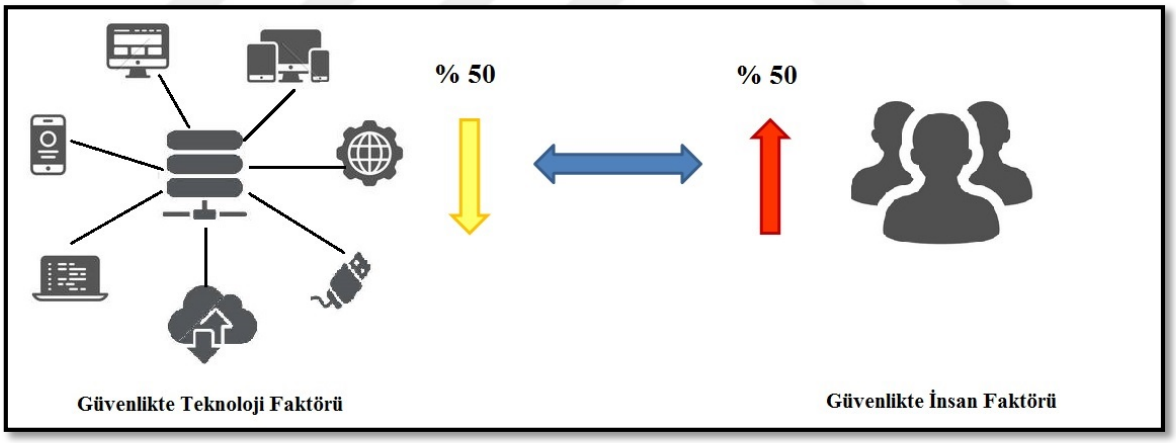
olarak sayılabilir.

Yukarıda sayılan güvenlik tedbirleri hem bireysel hem de kurumsal olarak uygulandığında önemli derecede başarılar elde edilmesine rağmen bu yöntemlerin etkinliği insan faktörünün devreye girmesiyle zafiyete uğramaktadır.

Bu önlem ve tedbirlerin pek çoğu bilgisayar virüsleri, aldatmacalar, yetkisiz erişim, siber

dolandırıcılık, bilgi hırsızlığı gibi teknoloji kaynaklı riskler ve tehditler için uygulandığında önemli ölçüde etkili olacak tedbirlerdir. Ancak ne var ki ne kadar tedbir alınırsa alınsın sistem ne kadar mükemmelleştirilse de bilgi güvenliğini tehdit eden belki de en önemli faktörün insan olduğu unutulmamalıdır. Çünkü insan, bilinçsizce ve yeterli bilgiye sahip olmadan teknolojiyi kullandığında veya zaten sisteme zarar verme amacı güttüğünde en tehlikeli tehdit haline gelmektedir. Araştırmacılar bilgisayar güvenliğindeki insan faktörü gözden kaçırıldığında, kurumların güvenlik duvarı, saldırı yakalama sistemleri, şifreleme ve güvenli erişim cihazları gibi teknolojilere milyarlarca dolarlık harcamalarının insan kaynaklı tehditler ve güvenlik açıkları sebebiyle boşa gittiğini belirmektedir.

Riskleri gidermenin veya minimum seviyeye çekmenin yolu farkındalık oluşturmaktan geçmektedir. Çünkü güvenlik teknolojileri ve alınan tedbirler geliştikçe saldırganlar tarafından teknik açıkları bulmak ve kullanmak zorlaşacağı için sistemin en zayıf ve zafiyetleri bulunan parçası olan insanı kullanma eğilimine girmektedirler. Bu sebeple güvenlik her şeyden önce insana yatırım yapılmasıyla sağlanabilir.



Şekil 5.1. Güvenlikte insan faktörü [32]

Bilgi güvenliği üzerine yapılan çalışmalarda insan ve teknoloji faktörünün aynı oranda etkili olduğu görülmektedir. Bu durum bilgi güvenliği bilinci ve farkındalık düzeyinin yüksekliğinin kişisel veri güvenliği yanında kurumsal bilgi güvenliğini de sağladığını göstermektedir. Kurumsal bilgi güvenliğinin sağlanması da ulusal siber güvenliği getirecektir.

5.1. Bilgi Güvenliği Kültürü

Bilgi güvenliği konusunda kurumsal olarak çalışmaların yapılması, bilgi güvenliği politikalarının oluşturulması ve bu politikalara uygun olarak personele uygulanması gereken işlemlerin öğretilmesi ve benimsenmesi gereken bilgi güvenliği davranışlarını içermektedir. Kurumlarda bilgi güvenliği konusunda kurumsal kültürün oluşturulması ve personelin eski davranışlarından kurtulması kolay ve çabuk olacak bir iş değildir.

5.2. Farkındalık

Farkındalık kelimesi günümüzde günlük yaşamda çokça duyduğumuz bir kavramdır. Türk Dil Kurumu (TDK) sözlüğünde farkındalık kelimesinin karşılığı 'farkında olma durumu' olarak geçmektedir. Farkında olma durumu yani farkında olmak ise 'görülmesi veya bilinmesi gereken şeylerden haberi bulunmak, kavranması gereken bir şeye dikkat etmek' olarak tanımlanmaktadır (TDK, 2019). Farkındalık aynı zamanda şimdiki zamana ait bir kavramdır, geçmişte farkında olmak ya da gelecekte farkında olmanın ana müdahale edebildiğimiz bugün için bir yararı yoktur.

Yani farkındalık şu an görülmesi ve bilinmesi gereken şeyleri bilmek olarak anlaşılabilir. O halde bilgi güvenliği farkındalığını bilgi güvenliği konusunda bilinmesi gereken konu ve kavramları bilmek olarak düşünmek yanlış olmaz.

5.2.1. Kurumsal bilgi güvenliği farkındalığı

Kurumsal bilgi güvenliği farkındalığı sağlamak için üst düzey yöneticiden çalışana kadar bilgilendirilmesi, farkındalık bilincinin oluşturulması, güvenlik politikalarının benimsenmesi, önemsenmesi, desteklenmesi ve birlikte geliştirilmesi gerekmektedir.

İnsan faktörüne bağlı olarak ortaya çıkan güvenlik risklerinin tamamen yok edilmesi mümkün değildir ancak iyi planlanmış bir bilgi güvenliği politikası ve bu politikayı uygulamak için kararlı, bilgili ve farkındalık düzeyi yüksek çalışanlar ile bu risklerin kabul edilebilir seviyelere düşmesi sağlanabilir.

Kurumsal bilgi güvenliğinden sadece kurumun bilgi güvenliği personeli ya da teknik çalışanlar değil kurumun tüm çalışanları, bilgi paylaşımında bulunduğu tüm paydaşları

yani kurum bilgi güvenliği politikasında bulunan taraflar sorumludur. Bu sorumluluk bilincinin bilgi güvenliği farkındalık eğitimleri ile tüm çalışanlara verilmesi, hangi tür risklerle karşılaşabilecekleri ve bu sorunlar karşısında nasıl tedbirler almaları ve davranmaları gerektiği anlatılmalıdır.

Kurumlarda bilgi güvenliği politikalarını uygulamanın yolu, çalışanların yerine getirilmesi gereken bu kuralları tıpkı iş tanımlarıymış gibi uygulamalarından ve benimsemelerinden geçmektedir. Kurumsal bilgi güvenliği farkındalığı sağlamanın en temelinde ise çalışanların bilgi alışverişi yaptığı üçüncü taraflara bu ister bir birey olsun isterse kurum, kurumunun bilgi varlıklarını koruması için üzerlerine düşen sorumlulukların farkında ve bilgisinde olması bulunmaktadır.

Bilgi güvenliği farkındalık çalışmalarına ülkece ihtiyacımız olduğunu Ünver, Canbay ve Mirzaoğlu (2011) çalışmalarında bilgi güvenliğinin sağlanması hususunu; ülkemizde gerek kamu sektöründe gerekse özel sektörlerde uygulanan genel yaklaşımın, mevcut riski azaltacak risk yönetiminin yapılarak bilgi ve iletişim kaynaklarının korunması şeklinde olduğu ve bilgi güvenliği denildiğinde teknik önlemler olarak düşünülmesi ve teknolojik çözümlere ağırlık verilmesi sonucu konunun yasal, idari, ekonomik ve sosyal boyutta ele alınarak kapsamlı bir çözüm geliştirilmesinin önüne geçtiğini, işin yasal boyutunda ise yasaların bilgi güvenliğini her yönüyle ele alacak kadar kapsamlı olmadığını ve güvenlik güçleri ile adli personelin yeterli bilgi ve uzmanlık seviyesine sahip olmadığını, idari boyutunda ise kamu yönetiminin ve çalışanların gerekli bilgi güvenliği farkındalığına ve yeterli siber güvenlik kapasitesine sahip olmadığını, ekonomik yönden ise bilgi güvenliğinin sağlanması için farkındalık çalışmalarına yeterli kaynak ayrılmadığı şeklinde değerlendirilmektedir.

Ayrıca vurguladıkları noktalardan bir tanesi de bilgi güvenliği konusunda alınması gereken teknik tedbirlere ve farkındalık çalışmalarına yeterli önemin verilmediğidir. Bu fikri destekleyen açıklamalar Cyber Security Weekend (CSW) 2019 toplantısında yapılmıştır. Toplantıda siber farkındalık çalışmalarına giderek daha çok ihtiyacımız olduğu, çünkü kurumsal verilere artık mobil cihaz ve bulut bilişimleriyle her yerden erişilebildiği ve teknik güvenlik sistemlerinin karmaşıklaşması saldırganların şirketlerden çok kullanıcıları hedef seçmesine yol açtığı bu nedenle işletmelerin çalışanlarını eğitmeye özen göstermeleri gerektiği vurgulanmıştır.

5.3. Bilgi Güvenliği Farkındalığı Oluşturma Önerileri

Günümüz koşullarında kurumun esas değerini oluşturan insan varlığıdır. Kurum politikası olarak insan varlığına yatırım yapıldığında aslında kuruma yatırım yapıldığıdır. Kurum çalışanlarında bilgi güvenliği farkındalığı oluşturmak için öncelikle yöneticilerin farkındalık çalışmalarını sahiplenmesi ve gerekliliğini inanması gerekmektedir. Sonrasında bu konuda personele eğitim vermek bilgi güvenliği personeline bırakılmalıdır. Eğer bu konuda bilgi güvenliği çalışanları yeterli bilgi donanımına sahip değilse danışmanlık hizmeti alınmalıdır.

- Bilgi güvenliği farkındalık eğitimlerinin üst yöneticiden çalışana kadar görev ve pozisyonlarına dikkat edilerek ihtiyaç ve beklentilerine göre değişen farkındalık eğitimi programları hazırlanmalıdır.
- Farkındalık eğitimleri yeni başlayan personeller için oryantasyon eğitimlerinin parçası haline getirilmeli ve kurum personeline düzenli aralıklarla gelişmelere göre programda güncellemeler yaparak yenilenmelidir.
- Farkındalık eğitimlerinde sınıf içi uygulamalar yerine başka yöntemler seçilerek anlık olarak ya da belirli aralıklarla kısa eğitimler verilebilir. Bu yöntemlerden bazıları şunlardır;
- Belirli dönem aralıklarıyla kurumdaki birimlerin bilgi güvenliği hususunda eksiklikleri belirlenerek önlem alınması gereken güvenlik unsurları açıklanarak farkındalık oluşturulabilir.
- İnteraktif sanal eğitimler ya da bilgi güvenliği konulu videolar ile eğitimler desteklenebilir.
- Çalışanlar için bilgi güvenliği el kitapçıkları, broşürler veya posterler hazırlanabilir.
- Led ekranlarda bilgi güvenliği konulu animasyonlar hazırlanabilir.
- Kurum çalışanlarının kurum e-posta adreslerine bilgi güvenliği e-posta bültenleri gönderilebilir.
- Çalışanların bilgisayar ekranlarında ekran koruyucu olarak bilgi güvenliği farkındalığı oluşturmaya yönelik mesajlar çıkabilir.
- Çalışanların bilgisayar arka planlarında bilgi güvenliğine yönelik eğitici mesajlar tasarlanabilir.
- Çalışanlar bilgisayarlarını açarken güvenliği hatırlatan giriş mesajları ya da sloganlar hazırlanabilir..

6. BİLGİ GÜVENLİĞİ FARKINDALIĞI ÜZERİNE YAPILAN YURT İÇİ ve YURT DIŞI ÇALIŞMALAR

Bilgi güvenliği farkındalığı bireylerin bilgi iletişim teknolojileri kullanımında, kişisel verileri bilgi güvenliğine karşı oluşabilecek risk ve tehlikelerden korumak için gerekli güvenlik tedbirlerini uygulamak ve bu tehditlerin farkında olması durumudur [14]. Bu sebeple bu konuda bilgi güvenliği eğitimiyle alakalı yapılan ulusal ve uluslararası çalışmaları incelemek gerekmektedir. Bilgi güvenliği ile ilgili araştırmaların yapılması, hem internet ve bilgisayar olmak üzere siber alan kullanıcılarının hem de bu konuda eğitim verecek olanlara yol göstermesi açısından önemlidir. Bilgi güvenliği farkındalık boyutunu inceleyen araştırma çalışmalarında genellikle veri toplama aracı olarak yüz yüze görüşme, anket veya ölçek kullanılmıştır.

Alan yazında bilgi güvenliğinin sağlanmasına yönelik oldukça çalışma bulunmaktadır. Ancak McCumber Bilgi Güvenliği Modelinde kabul edildiği gibi küpün tamamlayıcı niteliklere sahip yüzünde yer alan Eğitim ve Farkındalık yani insanın dâhil olduğu alanın öneminin son yıllarda keşfedildiği görülmektedir.

Mastrangelo, Stanton, Jolton ve Stam (2005) kullanıcıların parola belirleme davranışlarını incelemiş ve belirli bir örüntü taşıdığını çalışmalarında belirtmişlerdir.

Kastania, Mylonas ve Gritzalis (2013) araştırmalarında mobil cihazlarından uygulama indiren kullanıcıların indirme ortamı ve indirmek istedikleri programla ilgili olarak güvenlik endişesi yaşamadıklarını ortaya koymuştur.

Herath ve Rao (2009), çalışma alanlarını biraz daha değiştirerek bilgi güvenliği politikalarına uyma niyetleri gibi insan davranışlarını incelemişlerdir. Ancak bu çalışma ne kadar bilgi güvenliğine etkisi olan güvenlik politikaların davranışların etkisini incelese de bilgi güvenliği farkındalığını belirlemeye yönelik bir çalışma değildir.

Ünver, Canbay ve Mirzaoğlu (2009),araştırmalarında daha çok bilgi güvenliği zafiyetlerine üzerinde durmuştur. İnternet üzerinden yapılan işlemlerin çoğunda kimlik numarasının kullanılması ve kimlik numarasından bütün kişisel bilgilere ulaşılmasından dolayı oluşan tehlikelerden bahsetmişlerdir.

Lao ve arkadaşları (2009) tarafından yapılan çalışmada özellikle sosyal ağlarda yayılan ve kullanıcılar tarafından fark edilmeyen tehditler üzerinde durulmuştur. Bu tehditlerin kullanıcıları ve sosyal paylaşım sitelerini nasıl etkilediği ayrı ayrı anlatılmış ve bu tehditlere karşı alınabilecek olan önlemler ile sosyal ağlar için özel bir güvenlik arabirimi önerilmiştir. Aynı zamanda kullanıcıların farkındalığının yükseltilmesi önerisinde de bulunulmuştur.

Vroom ve vonSolms (2004) tarafından yapılan araştırmada bilgi güvenliği farkındalığının oluşmasında bilgi güvenliği politikalarının, kurumsal olarak yapılan bilgilendirme çalışmalarının, kişisel özellikler de dahil olmak üzere kurum kültürünü gibi etmenlerin dahi bilgi güvenliği farkındalığı oluşturulmasında etkili olduğu ifade edilmiştir.

Rezgui ve Marks (2008) yaptıkları çalışmada katılımcıların bilgi güvenliği farkındalıklarını etkileyen faktörler araştırılmıştır. Hedef grup olarak Birleşik Arap Emirlikleri'nde bilgi sistemleri yöneticileri de dahil olmak üzere üniversite personeli seçilmiştir. 'Sorumluluk' , 'kültürel varsayımlar ve inançlar' ile 'toplumsal koşullar' gibi faktörlerin bilgi güvenliği farkındalıklarını kısmen etkilediğini ortaya koymuştur.

Drevin, Kruger ve Steyn (2010) tarafından üniversite öğrencilerinin bilgi güvenliği farkındalıklarını ölçmeye yönelik bir ölçme aracı geliştirme çalışmasında farkındalık eğitimlerinde yer alabilecek konular ve alanların belirlenmesinde yardımcı olabilecek 'bilgi güvenliği sözcük testi' ni geliştirmişlerdir. Çalışmada testin kullanılabilirliğini göstermek için iki bölümden oluşan bir anketle çalışılmıştır. Birinci bölümde sözcük testi yer alırken diğer bölümde katılımcıların davranışları değerlendirilmiştir. Araştırma sonuçları bilgi güvenliği farkındalığını bulmak için testin kullanılmasının yararlı olabileceği yönünde görüş bildirmiştir.

Milli Eğitim Bakanlığı (MEB), Bilgi İşlem Dairesi Başkanlığı (2012) tarafından personelin farkındalık düzeyini ölçmeye yönelik bir anket gerçekleştirilmiştir. Katılımcılara kurum bilgi ve sistem güvenliği politikası, parola oluşturma, sosyal ağlar ve e-posta kullanımı konularında sorular yöneltilmiştir. Personelin bu konuların bazılarında farkındalığının yüksek olduğu bazılarında ise yeterli seviyede olmadığı sonucuna ulaşılmıştır. Yine bilgi güvenliği farkındalığı başlığı altında yapılan bir başka çalışmada geliştirilen anket 157 öğretmen ve başka meslek gruplarından 501 çalışana uygulanmıştır. Öğretmenler ile diğer

meslek gruplarının farkındalık düzeyleri arasında anlamlı bir fark bulunamamıştır.

Tekerek ve Tekerek (2013) tarafından yapılan çalışmada Kahramanmaraş ilindeki ilk ve orta öğretim öğrencilerine bilgi güvenliği farkındalık seviyelerini belirlemek amacıyla geliştirdikleri ölçeği uygulamışlardır. Araştırma sonucu öğrencilerin etik konularda yeterli düzeyde farkındalıklarının olduğu ancak teknik konularda farkındalıklarının düşük olduğu yönündedir. Bunun sebebi olarak bilgi ve bilgisayar güvenliği farkındalık eğitim ve etkinliklerinin yetersiz olması gösterilmiş, bu konudaki eğitimlerin artırılması yönünde öneride bulunulmuştur.

Kınay, Sözcü, Taşkın ve İpek (2014) tarafından geliştirilen Bilgi Güvenliği Farkındalığı Ölçeği, İstanbul ilinde özel bir üniversitenin öğrencilerine uygulanmıştır. Ölçekte eğitim, bilgi ve davranış düzeylerinde 32 soru bulunmaktadır. Ölçekten elde edilen puanlar 100-80 arası 'yüksek', 79-60 arası 'orta', 60 ve aşağısı ise düşük seviye olarak belirlenmiştir. Her farkındalık seviyesi için alınması gereken kararlar tartışılmıştır.

Gökmen ve Akgün (2016) öğretmen adaylarının bilişim suçlarıyla ilgili deneyimlerini ve bilişim güvenliği dersinin müfredatı hakkında düşüncelerini tespit etmek için gerçekleştirdiği çalışmasında öğretmen adaylarının çoğunun bilişim güvenliği ile ilgili bir ders almadığı ve kendilerini bilişim güvenliğini anlatacak kadar yeterli görmediklerini ortaya koymuştur.

Karaoğlan Yılmaz, Yılmaz ve Sezer (2014) tarafından gerçekleştirilen çalışmada öğrencilerin güvenli bilgi iletişim teknolojisi kullanım davranışları belirlenmeye çalışılmıştır. Bu davranış düzeyinin sürekli yenilenen teknoloji karşısında kendini yenileme ve güncellemede yetersiz kaldığı ifade edilmiştir. Yapılan analiz sonuçlarına bakıldığında öğrencilerin zararlı yazılımlar ve bunlardan korunma yollarına, dosya erişim ve paylaşım güvenliği ile ağ ve internet güvenliği gibi konularda temel seviyede olduğu en çok bilinen güvenlik önlemlerinden bazılarını uyguladığı ancak diğer güvenlik önlemlerini ise almadığını görülmektedir. Üniversite öğrencileri aynı zamanda potansiyel kamu çalışanı olduğundan öğrenciler üzerinde yapılan çalışan bir nevi kamu çalışanları bilgi güvenliği farkındalığına ışık tutacaktır.

Keser ve Güldüren (2015) çalışmalarında yükseköğretim kurumlarında çalışan öğretim

elemanlarının bilgi güvenliği farkındalıklarını belirlemeye yönelik bir ölçek geliştirmek istenmiştir. Ölçek geliştirme aşamalarında çalışma grubuna uygulanan bilgi güvenliği farkındalık eğitimlerinin etkili olduğu görülmüştür.

Keser, Çetinkaya ve Güldüren (2016) çalışmasında lisede öğrenim gören öğrencilerin bilgi güvenliği farkındalık seviyeleri ölçülerek bir ölçek geliştirilmek istenmiştir. Araştırma sonucunda veriler değerlendirildiğinde bilgi güvenliği farkındalığı ile cinsiyet arasında anlamlı bir farklılık bulunmuş, erkek öğrencilerin ilgi güvenliği farkındalık seviyelerinin kız öğrencilerden daha yüksek olduğu ifade edilmiştir.

Lang ve arkadaşları (2009) yaptıkları çalışmada sosyal paylaşım sitelerinde bilgi güvenliği farkındalığını belirlemeye çalışmışlardır. Bunun için İrlanda Üniversitesinde öğrenim gören 120 öğrenci gönüllü olmuştur. Elden edilen sonuçlara göre öğrencilerin özellikle taşınabilir bellekler ile bulaşan tehditlere karşı farkındalıktan yoksun olduğunu, bilgi güvenliği standartlarında şifre kullanımı ve veri yedekleme konusunda yeterli bilgiye sahip olmadıkları görülmüştür.

Kruger ve Kearney (2006) yaptıkları çalışmada Uluslararası Bilgi Güvenliği Farkındalığı Ölçeği geliştirmiş ve taslak halini bir madencilik şirketinin Avustralya bölge ofisi çalışanlarına uygulamıştır. 35 sorudan oluşan ölçekte açık uçlu ve çoktan seçmeli sorularda bulunmaktadır. Ölçeğin son hali şirket çalışanlarına uygulanmıştır. Yönetimin farkındalık performansına yönelik görüşleri de alınarak performans aralıkları belirlenmiştir. 100-80 puan arası ‘iyi’, 79-60 puan arası ‘orta’, 59 puandan altta kalan kısım ‘düşük’ olarak belirlenmiş, şirket çalışanlarının bilgi güvenliği farkındalığı %65 olarak ölçülmüştür.

Albrechtsen (2007) çalışmasında personelin güvenlik önlemlerine karşı tutum açısını ortaya koymak istemiş ve çalışma grubu olarak bilişim teknolojileri şirketlerini ve Norveç’ teki bankaları incelemiştir. Güvenliği sağlayan yöneticiler ile personel arasındaki iletişim boşluğuna dikkat çekmiş, güvenlik sorunlarının sebebini personelin bilgi ve farkındalık eksikliğinden kaynaklandığı sonucuna varmıştır.

İnternetin getirdiği güzelliklerden biri de sosyal ağlardır. Ancak ne var ki bu güzellikler yanında bazı riskleri de getirmiştir. Sosyal ağların kullanılmasında güvenliğinin sağlanması için kullanıcıların bilgi güvenliği farkındalıklarının bulunması gerekmektedir. Ülkemizde

pek çok kullanıcı tarafından kullanılan Facebook' un gizlilik ayarları üzerine yaptığı çalışmasında Sel (2013), 60 ortaokul öğrencisiyle birebir görüşmeler yapmıştır. Bu öğrencilerin %70' inin bu ayarlardan haberdar olmadığı sonucu çıkmıştır. Öğrencilere gizlilik ayarlarına dikkat etmediklerinde karşılaşabilecekleri tehdit ve riskler anlatılarak bilinçlendirme çalışması yapılmış ve sonuçlarının olumlu olduğu görülmüştür.

Öğütçü (2010) ise yaptığı çalışmasında katılımcıların bilgi güvenliği farkındalık düzeylerinin istenilen düzeyde olmadığı sonucuna ulaşmıştır.

Kaşıkçı, Çağıltay, Karakuş ve Ogan (2014) Avrupa ve Türkiye' yi kapsayan çalışmasında çocukların güvenli internet kullanımını incelemek istemiştir. İnternetin pek çok olumsuzluklarına maruz kalan çocukların ebeveynlerinin çocukları internet ortamındaki tehlikelerden uzak tutmayı sağlayacak yeterli bilgi düzeyine sahip olmadıklarını göstermiştir.

Çavuş ve Erçağ (2016) tarafından yapılan çalışmada öğretmenlerin güvenli internet kullanımına yönelik yeterliliklerini belirlemeyi hedeflemiştir. Araştırma sonucu, öğretmenlerin dijital veri güvenliği farkındalıklarının yüksek olduğunu göstermiştir. Farkındalık değerlerinin cinsiyet, günlük bilgisayar kullanım süresi, günlük internet kullanım suresi gibi durumlara göre değiştiği ancak branş, öğrenim kademesi, öğrenim durumu ve mesleki kıdem faktörlerine göre değişmediği görülmüştür.

Yılmaz, Yılmaz ve Sezer (2014) çalışmasında üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışlarını incelemiş, bilgi güvenliği eğitimlerinin verilmesi gerektiği sonucuna ulaşmıştır.

Araştırmalar arasında en dikkat çekici olanı 2000-2009 yılları arasında Tayvan' da devlet desteğiyle uygulanan İnternet Güvenliğinde Öğretmen Farkındalığı (TAIS) projesidir. Tayvan Milli Eğitim Bakanlığı internetin risklerinin farkına vararak ada çapında ilk ve ortaokul öğretmenlerine yönelik hazırladığı projede araştırmacılar internet güvenliğini öğretmenlerin fikir sahibi oldukları dört alan üzerinden gerçekleştirmiştir. Bu alanlar iletişim güvenliği, bilgi anlayışı ve uygunluk, çevrimiçi kişiler arası güvenlik, bilgisayar ve internet kullanımı güvenliğidir. Üç aşamalı olan projenin ilk aşamasında yalnızca bilgisayar öğretmenleri dahil olurken ikinci aşamasında tüm ilk ve ortaokul öğretmenleri

dahil edilmiştir. Ancak projenin son aşaması olan veliler, lise öğrencileri, lise öğretmenleri ve öğretmen adayları projeye dâhil edilememiştir. Proje kapsamında eğitim seminerleri, atölye çalışmaları, konferanslar gibi çeşitli etkinlikler yer almıştır.

Kocamustafaoğulları (2013) tarafından yapılan çalışmada organizasyonların bilgi güvenliği farkındalık ve uygulama seviyelerine yönelik kendi değerlendirmelerini yapabilecekleri ISO/IEC 27001 ve ISO/IEC 27002 bilgi güvenliği standartlarını temel alan web tabanlı açık ve anlaşılır, kolay kullanılabilen Türkçe bir araç ortaya konulmuştur [37].

Kuru ve Ocak (2016) ülkemizde kamu çalışanlarında siber güvenlik farkındalığı ve farkındalığın artırılması için alınması gereken önlemlere yönelik olan çalışmasında çalışanların siber güvenlik ve siber savaşlar hakkında yeterli bilgiye sahip olduğu belirtilmiş, kamu çalışanlarına çalışma hayatları boyunca eğitim verilmesi, üniversitelerde bu konuya yönelik derslerin müfredata eklenmesine yönelik önerilerde bulunulmuştur. Ayrıca siber savunma politikasının diğer devlet kurumlarıyla bilgi alışverişi yaparak planlaması gerektiği açıkça belirtilmiştir.

Bilgi güvenliğinin sağlanmasında donanım ve yazılım destekli tedbirler alınmaya ve bilgi güvenliği politikaları oluşturulmaya çalışılsa da en zayıf halkanın insan faktörü olduğu unutulmamalıdır. Eminağaoğlu ve Gökşen (2009), çalışmasında bilgi güvenliğinde başarı sağlanmasındaki en kritik faktörün bilinçli ve bilgili insanlar olduğunu vurgulamaktadır. Geliştirilen donanım ve yazılımları bilgi güvenliği hakkında bilgisi olan kullanıcılar bilinçli olarak kullandığında veri kayıplarının ve zararın çoğu önlenebilir. Şahinaslan ve arkadaşları (2009) yaptığı çalışmasında kurumlarda bilgi güvenliğini sağlamak amacıyla sadece teknik önlemlerin alınmasının yeterli olmayacağını en önemli faktörün insan olduğunu ve bilgi güvenliği risklerinin önlenmesinin ancak farkındalık düzeyinin artırılmasıyla mümkün olacağını belirtmiştir.

Şirketlerde bilgi güvenliğine yönelik yapılan çalışmalar incelendiğinde, yaşanılan güvenlik sorunlarının personelin bilgi eksikliğinden kaynaklandığı ve bu konuda farkındalık çalışmalarının yapılmasına ihtiyaç olduğu söylenebilir.

Buraya kadar anlatılan çalışmalarda çalışma gruplarının öğretmenler, öğrenciler, şirket çalışanları vb. seçildiği çeşitli bilgi güvenliği farkındalığı çalışmaları anlatılmıştır.

Araştırma sonuçları genel olarak ele alındığında bilgi güvenliği farkındalıklarının yeterli olmadığı görülmektedir Çalışmalarda veri toplama aracı olarak anket ya da görüşme yönteminin kullanılmıştır.

Bu çalışmada; yapılmış çalışmalara katkı sağlamak amacıyla siber saldırılar ve tehditler karşısında en çok saldırıya uğrayan kritik altyapılar arasında yer alan kamu kurum ve kuruluşlarında çalışanların bilgi güvenliğine yönelik farkındalıklarını ortaya koymak, farkındalık düzeylerini cinsiyet, yaş, çalışılan birim ve öğrenim durumu gibi değişkenlere göre değişip değişmediği incelenecektir.

7. METODOLOJİ

Alanyazın incelendiğinde bilgi güvenliği veya bilgi güvenliği farkındalığı üzerine yapılan çalışmalarda katılımcıların bilgi güvenliği, güvenli internet ya da internet davranışları, güvenli mobil cihaz kullanımı gibi konularda görüşlerini belirlemek için anket yönteminin kullanıldığı görülmüştür. Bu anketler yoluyla elde edilen veriler yüzde ve frekans değerleri standart sapmasına göre hesaplanarak mevcut durum belirlenmeye çalışılmıştır.

Çalışmamızda nicel araştırma modellerinden betimsel tarama yöntemi kullanılmıştır. Karasar (2016)‘ a göre araştırma modelleri araştırma amacına uygun olan ve istenilen verilerin toplanması ve analizinin yapılması için gerekli koşulların oluşturulması şeklinde tanımlanmaktadır. Yapılan bu çalışmada daha önce Keser ve Güldüren tarafından geliştirilen ve ölçeğin tamamı için Cronbach alfa güvenilirlik katsayısı .97 olan ‘Kişisel Verilerin Korunması’ ve ‘Saldırı ve Tehditler’ olmak üzere iki alt faktör ve 34 likert tipi sorudan oluşan Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) kullanılmıştır.

7.1. Çalışma Grubu

Araştırmanın çalışma grubu destek veren kamu kurum ve kuruluşlarında görev yapmakta olan 501 personelden oluşmaktadır. Katılımcılara ilişkin demografik bilgiler Çizelge 7.1’de sunulmuştur.

Çizelge 7.1. Katılımcılara ilişkin demografik bilgiler

Cinsiyet	N	%
Erkek	199	60,3
Kadın	302	39,7
Yaş Aralıkları	N	%
20-30 Yaş	59	11,8
31-40 Yaş	211	42,1
41-50 Yaş	159	31,7
51-70 Yaş	72	14,4
Eğitim Durumu	N	%
Lise	53	10,6
Üniversite	445	89,4

Çizelge 7.1. (devam) Katılımcılara ilişkin demografik bilgiler

Görev Yapılan Birim	N	%
Bilgi Teknolojileri Daire Başkanlığı	72	14,4
Diğer Birimler	429	85,6

Çizelge 7.1. incelendiğinde katılımcıların 302'sinin (%60,3) erkek, 199'unun (%39,7) kadın olduğu görülmektedir. Katılımcıların 59'u (%11,8) 20-30 yaş aralığında, 211'i (%42,1) 31-40 yaş aralığında, 159'u (%31,7) 41-50 yaş aralığında ve 72'si (%14,4) 51-70 yaş aralığındadır. Katılımcıların büyük çoğunluğu üniversite mezunu olup (%89,4), 72'si (%85,6) Bilgi Teknolojileri Daire Başkanlığında, 429'u (%85,6) ise destek veren kurum ve kuruluşların diğer birimlerinde görev yapmaktadır.

7.2. Veri Toplama Araçları

Yapılan bu çalışmada Cronbach alfa güvenirlik katsayıları "Saldırı ve Tehditler" alt boyutu için ,96; "Kişisel Verilerin Korunması" alt boyutu için ,96; ölçeğin tümü içinse ,97 olarak hesaplanmıştır.

7.3. Verilerin Analizi

Araştırma problemlerine yanıt bulmak için yapılan analizlerde dağılım özelliklerinin belirlenmesi ve betimsel istatistiklerin hesaplanmasında yüzde, frekans analizi ve ortalama puanların analizi vb. yöntemler uygulanmıştır.

7.3.1. Kayıp veri analizi

Araştırma kapsamında destek veren kamu kurum ve kuruluşlarında görev yapmakta olan toplam 504 personele ölçme araçları uygulanmıştır. 3 katılımcı, maddelerin %20'sinden fazlasına yanıt vermediği için veri setinden çıkartılmıştır. Kalan 501 katılımcıdan bazılarının, bazı maddeleri boş bıraktığı görülmüştür. Boş maddelere atama yapmak amacıyla, öncelikle madde bazlı analizler yürütülmüş ve her bir madde için boş bırakan katılımcı sayısının %2'den düşük olduğu bulunmuştur. Boş bırakılan maddelerin rastsal (random) bir şekilde dağılıp dağılmadığının belirlenmesi amacıyla yapılan Little MCAR testi sonucunun anlamsız olduğu (Chi-Square = 499,326; Sd = 495; p= ,437), bir başka deyişle maddelerin tamamen rastlantısal olarak boş bırakıldığı görülmüştür. Bunun sonucunda, maksimum olabilirlik yöntemi kullanılarak boş maddelere atamalar yapılmıştır [52].

7.3.2. Dağılıma ilişkin normallik analizi

Dağılımın normalliğinin belirlenmesi amacıyla basıklık ve çarpıklık katsayıları hesaplanmıştır. Yapılan analiz sonucunda hem ölçeğin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından hem de ölçeğin toplamından elde edilen puanların basıklık ve çarpıklık katsayılarının -1 +1 aralığında olduğu görülmüş (bkz. Çizelge 2.), dolayısıyla verilerin normal dağılım özellikler gösterdiği varsayılmıştır [53]. Bunun sonucu olarak, yapılan analizlerde parametrik tekniklerden yararlanılmıştır.

7.3.3. Kullanılan analizler ve yazılım

Araştırma problemlerine yanıt bulmak amacıyla yapılan analizlerde; dağılım özelliklerinin belirlenmesi ve betimsel istatistiklerin hesaplanmasında yüzde ve frekans analizi, cinsiyet, çalışılan birim ve eğitim düzeyine göre yapılan karşılaştırmalarda bağımsız gruplar için t-testi, yaşa göre yapılan karşılaştırmalarda ise tek yönlü varyans analizi tekniğinden yararlanılmıştır.

Yapılan analizlerde ise SPSS 25.0 paket programı kullanılmıştır.

7.4. Bulgular

Bu bölümde araştırma kapsamında ulaşılan bulgulara yer verilmiştir. İlk olarak betimsel istatistikler bölümünde; madde istatistikleri ve toplam puanlara ilişkin dağılımlar sunulmuştur. Fark istatistikleri bölümünde ise; katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların cinsiyetlerine, yaşlarına, eğitim düzeylerine ve çalıştıkları birime göre karşılaştırma sonuçları sunulmuştur.

7.4.1. Betimsel istatistikler

Madde Dağılımlarının İncelenmesi

Katılımcıların Bilgi Güvenliği Ölçeğinin maddelerine verdikleri yanıtların ortalama puanları Çizelge 7.2' de sunulmuştur.

Çizelge 7.2. Bilgi güvenliği farkındalığı ölçeğinin maddelerine ilişkin ortalama puanlar

Madde No	Bilgi Güvenliği Farkındalığı Maddeleri	Ort.	Ss.
32	Kişisel mahremiyet nedir biliyorum.	3,96	1,03
24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.	3,91	1,13

Çizelge 7.2. (devam) Bilgi güvenliği farkındalık ölçeği maddelerine ilişkin ortalama puanlar

23	Dijital imza nedir biliyorum.	3,84	1,07
17	Bilgi güvenliğinin ne anlama geldiğini biliyorum.	3,75	1,04
26	İstenmeyen elektronik posta (spam) nedir biliyorum.	3,75	1,2
18	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.	3,62	1,05
33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.	3,6	1,13
29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.	3,56	1,15
19	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.	3,41	1,13
30	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.	3,4	1,16
28	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum.	3,37	1,19
31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.	3,37	1,18
22	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.	3,36	1,22
21	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (real time protection) özelliğini kullanmaktayım.	3,15	1,23
7	Kimlik hırsızlığı (identity theft) nedir biliyorum.	3,09	1,28
4	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.	3,05	1,31
2	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.	3,03	1,25
1	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.	2,93	1,22
14	Siber zorbalık (cyber bullying) nedir biliyorum.	2,92	1,3
8	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.	2,85	1,23
3	Aldatmaca (hoax) nedir biliyorum.	2,82	1,31
11	Kimlik avı (phishing) saldırısı nedir biliyorum.	2,82	1,34
16	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.	2,77	1,22
9	Sahte virüs koruma yazılımının ne olduğunu biliyorum.	2,77	1,26

Çizelge 7.2. (devam) Bilgi güvenliği farkındalık ölçeği maddelerine ilişkin ortalama puanlar

15	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.	2,72	1,25
10	Hizmet aksatma (Denial of Service – DoS) saldırısı nedir biliyorum.	2,65	1,3
12	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.	2,64	1,32
13	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.	2,61	1,27
6	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.	2,57	1,22
5	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.	2,55	1,21

Çizelge 7.2 incelendiğinde 32, 24, 23, 17 ve 26 numaralı ölçek maddelerinin en yüksek ortalamaya sahip olduğu görülmektedir. Buna göre, bilgi güvenliği konusunda katılımcıların en iyi bildikleri özellikler kişisel mahremiyet, şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riskler, dijital imza, bilgi güvenliği ve istenmeyen elektronik postanın anlamı şeklinde sıralanmaktadır. Bununla birlikte, katılımcıların en düşük puan aldıkları maddeler göz önünde bulundurulduğunda ilk sırada 5. numaralı ölçek maddesi yer almaktadır. Buna göre katılımcılar en çok bilgisayarlarında casus bir yazılım olup olmadığını anlama konusunda zorlanmaktadır. Bu maddeyi sırasıyla 6, 13, 12 ve 10 numaralı maddeler izlemektedir. Katılımcılar casus yazılımları engelleme, sosyal mühendislik saldırısına uğramamak için yapılacaklar, sosyal mühendisliğin ve hizmet aksatmanın anlamı konularında diğer maddelere oranla daha düşük düzeyde bilgi güvenliği farkındalığına sahiptirler.

Toplam Puanlara İlişkin Dağılımlar

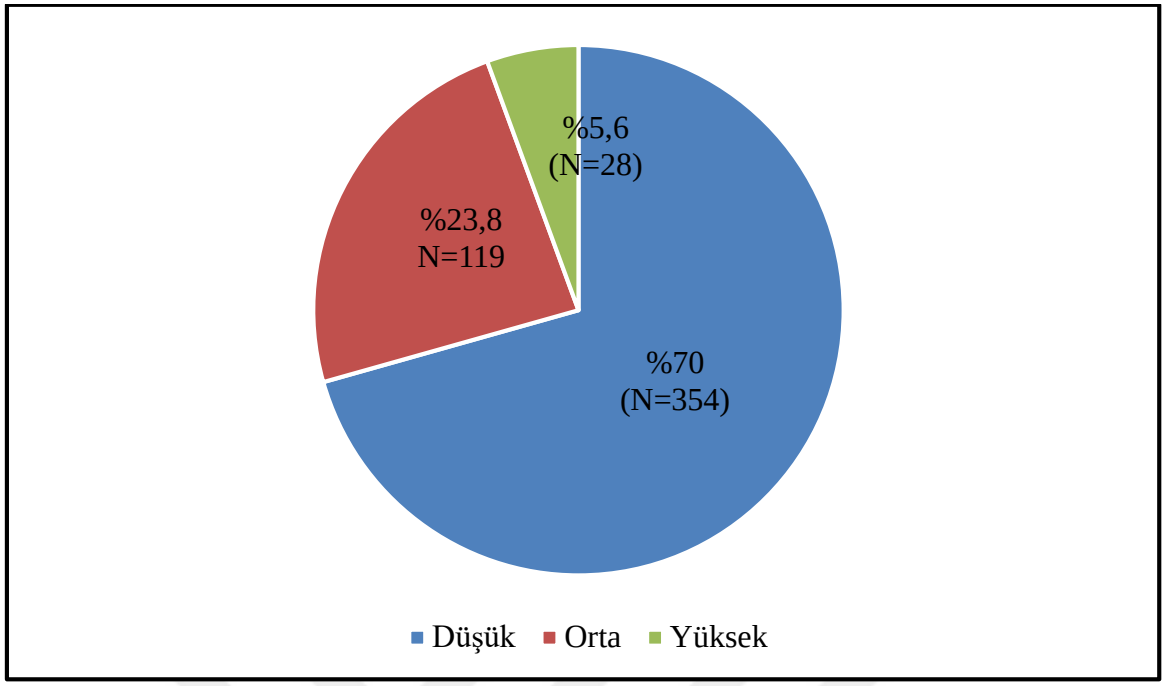
Madde bazlı incelemelerin ardından, katılımcıların bilgi güvenliği farkındalığının saldırı ve tehditler alt boyutu ile kişisel verilerin korunması alt boyutundan ve ölçeğin toplamından elde ettikleri puanlara yönelik betimsel istatistikler yapılmıştır. Bulgular Çizelge 3'te sunulmuştur.

Çizelge 7.3. Katılımcıların bilgi güvenliği farkındalık ölçeğinden elde ettikleri puanlara ilişkin betimsel istatistikler

	Saldırı ve Tehditler	Kişisel Verilerin Korunması	Bilgi Güvenliği Farkındalığı
Ortalama	44,81	63,05	107,87
Standart Sapma	16,08	16,28	30,14
Minimum	16,00	18,00	34,00
Maximum	80,00	90,00	170,00
Çarpıklık	,092	-,670	-,200
Basıklık	-,577	,360	-,218

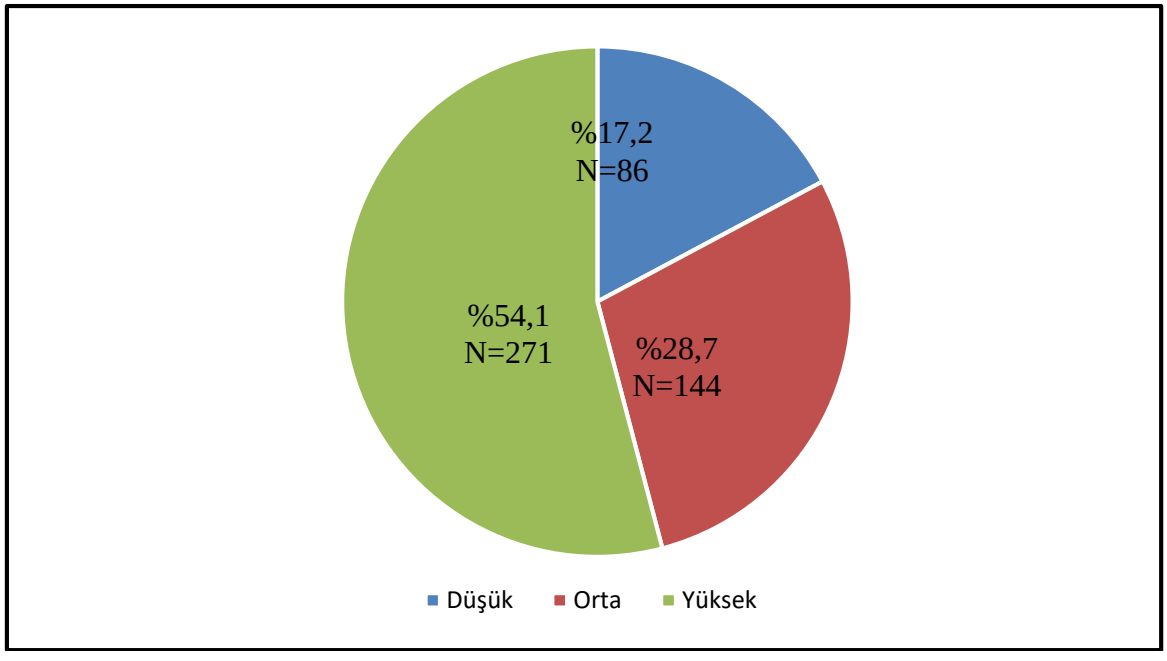
Çizelge 7.3 incelendiğinde, katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puanların 16,00 ile 80,00 arasında değiştiği ve ortalama puanlarının 44,81 (ss=16,08) olduğu; kişisel verilerin korunması alt boyutundan elde ettikleri puanların 18 ile 90 arasında değiştiği ve ortalama puanlarının 63,05 (ss=16,28) olduğu; Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puanların ise 34,00 ile 170,00 arasında değiştiği ve ortalama puanlarının 107,81 (ss=30,14) olduğu görülmektedir.

Bilgi Farkındalığı Ölçeğinden 34-102 puan aralığı "düşük", 103-136 puan aralığı "orta", 137-170 puan aralığı ise "yüksek" düzeyde bilgi farkındalığına sahip olunduğunu göstermektedir. Alt boyutlarda ise saldırı ve tehditler alt boyutu için 18-54 puan aralığı "düşük", 55-72 puan aralığı "orta", 73-90 puan aralığı ise "yüksek"; kişisel verilerin korunması alt boyutu için 16-48 puan aralığı "düşük", 49-64 puan aralığı "orta", 65-80 puan aralığı ise "yüksek" düzeye işaret etmektedir. Bu puan aralıkları dikkate alınarak düşük, orta ve yüksek düzeyde puan alan katılımcılar belirlenmiş ve buna ilişkin dağılımlar aşağıdaki grafiklerde sunulmuştur.



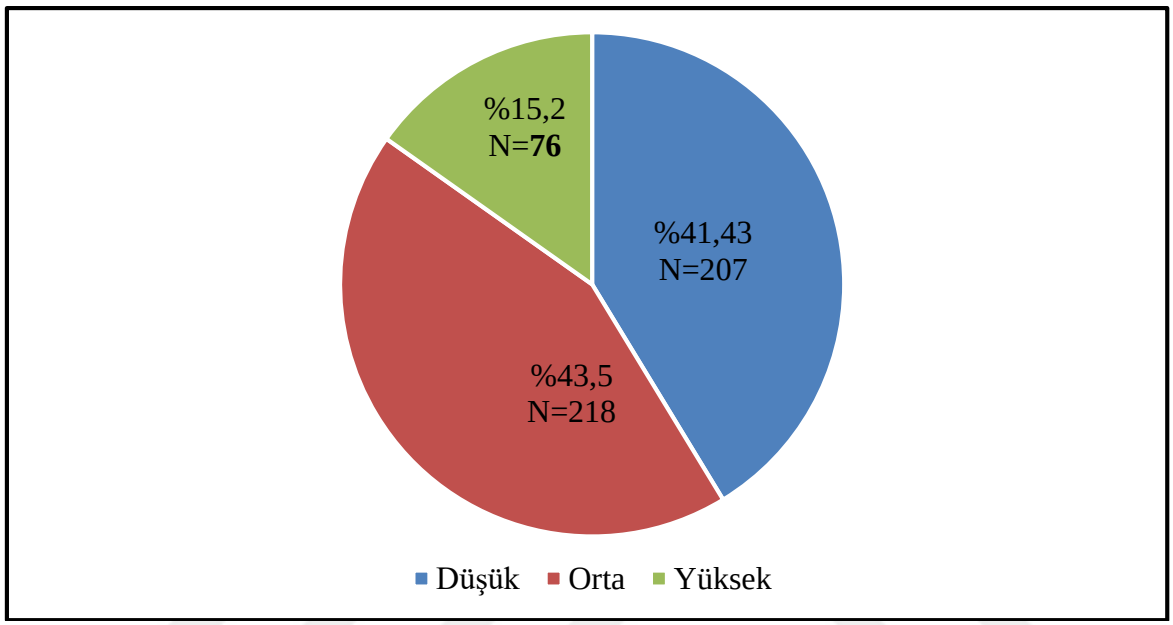
Şekil 7.1. Saldırı ve tehditler alt boyutu için dağılımlar

Şekil 7.1 incelendiğinde katılımcıların büyük çoğunluğunun (%70,7) saldırı ve tehditler alt boyutunda düşük düzeyde puan aldığı görülmektedir. %23,8'i orta düzeyde puan alırken, %5,6'sı ise yüksek düzeyde puan almıştır. Bulgular genel olarak değerlendirildiğinde, katılımcıların saldırı ve tehditlere ilişkin bilgi güvenliği farkındalıklarının düşük olduğu söylenebilir.



Şekil 7.2. Kişisel verilerin korunması alt boyutu için dağılımlar

Şekil 7.2 incelendiğinde katılımcıların yarısından fazlasının (%54,1) kişisel verilerin korunması alt boyutundan yüksek düzeyde puan aldığı görülmektedir. %28,7'si orta düzeyde puan alırken, %17,2'si ise yüksek düzeyde puan almıştır. Bulgular genel olarak değerlendirildiğinde, katılımcıların kişisel verilerin korunmasına ilişkin bilgi güvenliği farkındalıklarının yüksek olduğu söylenebilir.



Şekil 7.3. Bilgi güvenliği farkındalığı ölçeğinin tümü için dağılımlar

Şekil 7.3 incelendiğinde katılımcıların %41,43'ünün Bilgi Güvenliği Farkındalığı Ölçeğinden düşük düzeyde puan aldığı görülmektedir. %43,5'i orta düzeyde puan alırken, %15,2'si ise yüksek düzeyde puan almıştır. Bulgular genel olarak değerlendirildiğinde, katılımcıların bilgi güvenliği farkındalığı düzeylerinin düşük olduğu söylenebilir.

7.4.2. Fark istatistikleri

Çalışma grubundan alınan yanıtların katılımcılardan toplanan demografik verilere göre karşılaştırmalar yapılarak ölçeğin alt boyutlarında ve ölçeğin tamamında puanlar hesaplanmıştır.

Cinsiyet ve Bilgi Güvenliği Farkındalığı

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların cinsiyetlerine göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar

için t-testi yapılmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, kadın ve erkek katılımcıların ortalama puanları belirlenmiş, ortalama puanlar arasında farkın anlamlılığının testi içinse t değeri hesaplanmıştır. Bulgular önce alt boyutlara göre sonrasında ise ölçeğin tümü için olmak üzere sıralı bir şekilde aşağıda sunulmuştur.

Çizelge 7.4. Katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puanların cinsiyetlerine göre karşılaştırılması

Cinsiyet	N	Ort	Ss	Sd	*t*	p
Kadın	302	46,48	16,54	499	2,888	0,004
Erkek	199	42,27	15,03			

Çizelge 7.4 incelendiğinde, kadın katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin saldırı ve tehditler alt boyutundan elde ettikleri puan ortalamalarının 46,48 (ss=16,54) olduğu, erkek katılımcıların elde ettikleri puan ortalamalarının 42,27 (ss=15,03) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, kadın katılımcıların ortalama puanlarının anlamlı olarak daha yüksek olduğu bulunmuştur (t(499)= 2,888; p< ,05). Bir başka deyişle, kadın katılımcılar saldırı ve tehditler konusunda erkek katılımcılara oranla daha yüksek bilgi güvenli farkındalığına sahiptirler.

Çizelge 7.5. Katılımcıların kişisel verilerin korunması alt boyutundan elde ettikleri puanların cinsiyetlerine göre karşılaştırılması

Cinsiyet	N	Ort	Ss	Sd	*t*	p
Kadın	302	63,51	16,36	499	,772	,441
Erkek	199	62,36	16,18			

Çizelge 7.5 incelendiğinde, kadın katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin kişisel verilerin korunması alt boyutundan elde ettikleri puan ortalamalarının 63,51 (ss=16,36) olduğu, erkek katılımcıların elde ettikleri puan ortalamalarının 62,36 (ss=16,18) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, kadın ve erkek katılımcıların ortalama puanlarının birbirinden anlamlı olarak farklılaşmadığı bulunmuştur (t(499)= ,772; p> ,05). Bir başka deyişle, kişisel verilerin korunması konusunda kadın ve erkek katılımcılar benzer düzeyde bilgi güvenliği farkındalığına sahiptirler.

Çizelge 7.6. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puanların cinsiyetlerine göre karşılaştırılması

Cinsiyet	N	Ort	Ss	Sd	*t*	p
Kadın	302	110,00	31,08	499	1,952	,052
Erkek	199	104,64	28,43			

Çizelge 7.6 incelendiğinde, kadın katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puan ortalamalarının 110,00 (ss=31,08) olduğu, erkek katılımcıların elde ettikleri puan ortalamalarının 104,64 (ss=28,43) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, kadın ve erkek katılımcılarının ortalama puanlarının birbirinden anlamlı olarak farklılaşmadığı bulunmuştur (t(499)= 1,952; p> ,05). Bir başka deyişle, genel olarak kadın ve erkek katılımcılar benzer düzeyde bilgi güvenliği farkındalığına sahiptirler.

Yaş ve Bilgi Güvenliği Farkındalığı

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların yaş aralıklarına göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla tek yönlü varyans analizi (ANOVA) yapılmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, yaş aralıklarına göre katılımcıların ortalama puanları belirlenmiş, ortalama puanlar arasındaki farkın anlamlılığının ortaya konulması amacıyla Tukey testi yapılmıştır. Bulgular önce alt boyutlara göre sonrasında ise ölçeğin tümü için olmak üzere sıralı bir şekilde aşağıda sunulmuştur.

Çizelge 7.7. Katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puan ortalamalarının yaş aralıklarına göre dağılımı

Yaş Aralığı	N	Ort.	Ss
20-30 Yaş	59	45,69	13,30
31-40 Yaş	211	47,93	16,43
41-50 Yaş	159	42,22	15,73
51-70 Yaş	72	40,66	16,27

Çizelge 7.7 incelendiğinde Bilgi Güvenliği Farkındalığı Ölçeğinin saldırı ve tehditler alt boyutu için 20-30 yaş aralığındaki katılımcıların puan ortalamalarının 45,69 (ss=13,30);

31-40 yaş aralığındaki katılımcıların puan ortalamalarının 47,93 (ss=16,43); 41-50 yaş aralığındaki katılımcıların puan ortalamalarının 42,22 (ss=15,73); 51-70 yaş aralığındaki katılımcıların puan ortalamalarının ise 40,66 (ss=16,27) olduğu görülmektedir. 31-40 yaş aralığındaki katılımcılar en yüksek puan ortalamasına sahip iken 51-70 yaş aralığındaki katılımcılar en düşük puan ortalamasına sahiptir. Puan ortalamaları arasındaki farkın anlamlı olup olmadığının belirlenmesi amacıyla yapılan tek yönlü varyans analizi sonuçları Çizelge 7.8' de sunulmuştur.

Çizelge 7.8. Katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puanların yaş aralıklarına göre karşılaştırılması

	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
Gruplar Arası	4413,733	3	1471,244	5,854	,001
Grup İçi	124910,003	497	251,328		
Toplam	129323,737	500			

Çizelge 7.8 incelendiğinde katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puan ortalamalarının yaş aralıklarına göre anlamlı olarak farklılaştığı görülmektedir ($F(497)=5,854$; $p< ,05$). Çizelge 8 gruplar arasında farkın olduğunu söylemekle birlikte, hangi gruplar arasında bu farkın olduğunu bildirmemektedir. Hangi yaş grupları arasında anlamlı farklılığın olduğunu belirlemek amacıyla ise Tukey testi yapılmıştır. Tukey testi sonuçlarına göre, 31-40 yaş aralığındaki katılımcıların hem 41-50 yaş aralığındaki hem de 51-70 yaş aralığındaki katılımcılardan anlamlı olarak daha yüksek puan aldıkları bulunmuştur.

Çizelge 7.9. Katılımcıların kişisel verilerin korunması alt boyutundan elde ettikleri puan ortalamalarının yaş aralıklarına göre dağılımı

Yaş Aralığı	N	Ort.	Ss
20-30 Yaş	59	65,05	16,26
31-40 Yaş	211	66,24	15,40
41-50 Yaş	159	61,12	15,61
51-70 Yaş	72	56,34	17,91

Çizelge 7.9 incelendiğinde Bilgi Güvenliği Farkındalığı Ölçeğinin kişisel verilerin korunması alt boyutu için 20-30 yaş aralığındaki katılımcıların puan ortalamalarının 65,05

(ss=16,26); 31-40 yaş aralığındaki katılımcıların puan ortalamalarının 66,24 (ss=15,40); 41-50 yaş aralığındaki katılımcıların puan ortalamalarının 61,12 (ss=15,61); 51-70 yaş aralığındaki katılımcıların puan ortalamalarının ise 56,34 (ss=17,91) olduğu görülmektedir. 31-40 yaş aralığındaki katılımcılar en yüksek puan ortalamasına sahip iken 51-70 yaş aralığındaki katılımcılar en düşük puan ortalamasına sahiptir. Puan ortalamaları arasındaki farkın anlamlı olup olmadığının belirlenmesi amacıyla yapılan tek yönlü varyans analizi sonuçları Çizelge 7.10'da sunulmuştur.

Çizelge 7.10. Katılımcıların kişisel verilerin korunması alt boyutundan elde ettikleri puanların yaş aralıklarına göre karşılaştırılması

	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
Gruplar Arası	6215,485	3	2071,828	8,145	,000
Grup İçi	126419,836	497	254,366		
Toplam	132635,321	500			

Çizelge 7.10 incelendiğinde katılımcıların kişisel verilerin korunması alt boyutundan elde ettikleri puan ortalamalarının yaş aralıklarına göre anlamlı olarak farklılaştığı görülmektedir ($F(497)=8,145$; $p< ,05$). Çizelge 10 gruplar arasında farkın olduğunu söylemekle birlikte, hangi gruplar arasında bu farkın olduğunu bildirmemektedir. Hangi yaş grupları arasında anlamlı farklılığın olduğunu belirlemek amacıyla ise Tukey testi yapılmıştır. Tukey testi sonuçlarına göre, 51-70 yaş aralığındaki katılımcıların hem 20-30 yaş aralığındaki hem de 31-40 yaş aralığındaki katılımcılardan anlamlı olarak daha düşük puan aldıkları bulunmuştur.

Çizelge 7.11. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puan ortalamalarının yaş aralıklarına göre dağılımı

Yaş Aralığı	N	Ort.	Ss
20-30 Yaş	59	110,74	27,47
31-40 Yaş	211	114,18	29,54
41-50 Yaş	159	103,34	29,10
51-70 Yaş	72	97,01	32,00

Çizelge 7.11 incelendiğinde Bilgi Güvenliği Farkındalığı Ölçeğinin toplamı için 20-30 yaş aralığındaki katılımcıların puan ortalamalarının 110,74 (ss=27,47); 31-40 yaş aralığındaki

katılımcıların puan ortalamalarının 114,18 (ss=29,54); 41-50 yaş aralığındaki katılımcıların puan ortalamalarının 103,34 (ss=29,10); 51-70 yaş aralığındaki katılımcıların puan ortalamalarının ise 97,01 (ss=32,00) olduğu görülmektedir. 31-40 yaş aralığındaki katılımcılar en yüksek puan ortalamasına sahip iken 51-70 yaş aralığındaki katılımcılar en düşük puan ortalamasına sahiptir. Puan ortalamaları arasındaki farkın anlamlı olup olmadığının belirlenmesi amacıyla yapılan tek yönlü varyans analizi sonuçları Çizelge 7.12'de sunulmuştur.

Çizelge 7.12. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puanların yaş aralıklarına göre karşılaştırılması

	Kareler Toplamı	Sd	Kareler Ortalaması	F	p
Gruplar Arası	20641,885	3	6880,628	7,887	,000
Grup İçi	433605,939	497	872,447		
Toplam	454247,824	500			

Çizelge 7.12 incelendiğinde katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinden elde ettikleri toplam puanların ortalamalarının yaş aralıklarına göre anlamlı olarak farklılaştığı görülmektedir ($F(497)=7,887$; $p< ,05$). Çizelge 12 gruplar arasında farkın olduğunu söylemekle birlikte, hangi gruplar arasında bu farkın olduğunu bildirmemektedir. Hangi yaş grupları arasında anlamlı farklılığın olduğunu belirlemek amacıyla ise Tukey testi yapılmıştır. Tukey testi sonuçlarına göre, 31-40 yaş aralığındaki katılımcıların hem 41-50 yaş aralığındaki hem de 51-70 yaş aralığındaki katılımcılardan anlamlı olarak daha yüksek puan aldıkları bulunmuştur. Ek olarak, 21-30 yaş aralığındaki katılımcılar 51-70 yaş aralığındaki katılımcılar anlamlı olarak daha yüksek puan almışlardır.

Bilgi Güvenliği Farkındalığı ve Eğitim Düzeyi

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların eğitim düzeylerine göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar için t-testi yapılmıştır. Lise ve altı eğitim düzeyine sahip katılımcılar bir grup, üniversite mezuniyetine sahip katılımcılar ise diğer bir grup olarak ele alınmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, katılımcıların eğitim düzeylerine göre ortalama puanları belirlenmiş, ortalama puanlar arasında farkın anlamlılığının testi içinse t değeri hesaplanmıştır. Bulgular önce alt boyutlara göre

sonrasında ise ölçeğin tümü için olmak üzere sıralı bir şekilde aşağıda sunulmuştur.

Çizelge 7.13. Katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puanların eğitim düzeylerine göre karşılaştırılması

Eğitim Düzeyi	N	Ort	Ss	Sd	*t*	p
Lise ve Altı	53	38,77	15,19	496	-2,973	,003
Üniversite	445	45,65	16,01			

Çizelge 7.13 incelendiğinde, lise ve altı eğitim düzeyine sahip katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin saldırı ve tehditler alt boyutundan elde ettikleri puan ortalamalarının 38,77 (ss=15,19) olduğu, üniversite mezunu katılımcıların elde ettikleri puan ortalamalarının 45,65 (ss=16,01) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, üniversite mezunu katılımcıların ortalama puanlarının anlamlı olarak daha yüksek olduğu bulunmuştur (t(496)= -2,973; p< ,05). Bir başka deyişle, üniversite mezunu katılımcılar saldırı ve tehditler konusunda lise ve altı eğitim düzeyine sahip katılımcılara oranla daha yüksek bilgi güvenliği farkındalığına sahiptirler.

Çizelge 7.14. Katılımcıların kişisel verilerin korunması alt boyutundan elde ettikleri puanların eğitim düzeylerine göre karşılaştırılması

Eğitim Düzeyi	N	Ort	Ss	Sd	*t*	p
Lise ve Altı	53	52,09	18,75	496	-5,414	,000
Üniversite	445	64,49	15,36			

Çizelge 7.14 incelendiğinde, lise ve altı eğitim düzeyine sahip katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin kişisel verilerin korunması alt boyutundan elde ettikleri puan ortalamalarının 52,09 (ss=18,75) olduğu, üniversite mezunu katılımcıların elde ettikleri puan ortalamalarının 64,49 (ss=15,36) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, üniversite mezunu katılımcıların ortalama puanlarının anlamlı olarak daha yüksek olduğu bulunmuştur (t(496)= -5,414; p< ,05). Bir başka deyişle, üniversite mezunu katılımcılar kişisel verilerin korunması konusunda lise ve altı eğitim düzeyine sahip katılımcılara oranla daha yüksek bilgi güvenliği farkındalığına sahiptirler.

Çizelge 7.15. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri toplam puanların eğitim düzeylerine göre karşılaştırılması

Eğitim Düzeyi	N	Ort	Ss	Sd	*t*	p
Lise ve Altı	53	90,87	31,90	496	-4,505	,000
Üniversite	445	110,14	29,15			

Çizelge 7.15 incelendiğinde, lise ve altı eğitim düzeyine sahip katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puan ortalamalarının 90,87 (ss=31,90) olduğu, üniversite mezunu katılımcıların elde ettikleri puan ortalamalarının 110,14 (ss=29,15) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, üniversite mezunu katılımcıların ortalama puanlarının anlamlı olarak daha yüksek olduğu bulunmuştur ($t(496)= -4,505$; $p< ,05$). Bir başka deyişle, üniversite mezunu katılımcılar bilgi güvenliği konusunda lise ve altı eğitim düzeyine sahip katılımcılara oranla daha yüksek farkındalığına sahiptirler.

Bilgi Güvenliği Farkındalığı ve Görev Yapılan Birim

Katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin "Saldırı ve Tehditler" ile "Kişisel Verilerin Korunması" alt boyutlarından ve ölçeğin toplamından elde ettikleri puanların görev yaptıkları birime göre farklılaşıp farklılaşmadığının belirlenmesi amacıyla bağımsız gruplar için t-testi yapılmıştır. Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcılar bir grup olarak ele alınırken, diğer tüm birimlerde görev yapan katılımcılar ise "diğer" olarak ele alınmıştır. Yapılan karşılaştırmalarda, hem alt boyutlar hem de ölçeğin tümü için, katılımcıların çalıştıkları birime göre ortalama puanları belirlenmiş, ortalama puanlar arasında farkın anlamlılığının testi içinse t değeri hesaplanmıştır. Bulgular önce alt boyutlara göre sonrasında ise ölçeğin tümü için olmak üzere sıralı bir şekilde aşağıda sunulmuştur.

Çizelge 7.16. Katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puanların görev yaptıkları birime göre karşılaştırılması

Görev Yapılan Birim	N	Ort	Ss	Sd	*t*	p
Bilgi Teknolojileri Daire Başkanlığı	72	58,77	13,78	499	8,511	,000
Diğer Birimler	429	42,47	15,24			

Çizelge 7.16 incelendiğinde, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin saldırı ve tehditler alt boyutundan elde ettikleri puan ortalamalarının 58,57 (ss=13,78) olduğu, diğer birimlerde görev yapan katılımcıların elde ettikleri puan ortalamalarının 42,47 (ss=15,24) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların saldırı ve tehditler alt boyutundan elde ettikleri puanların diğer birimlerde görev yapan katılımcılardan anlamlı olarak daha yüksek olduğu bulunmuştur (t(499)= 8,511; p< ,05). Bir başka deyişle, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcılar diğer birimlerde görev yapan katılımcılara oranla saldırı ve tehditler konusunda daha yüksek bilgi güvenliği farkındalığına sahiptirler.

Çizelge 7.17: Katılımcıların kişisel verilerin korunması alt boyutundan elde ettikleri puanların görev yaptıkları birime göre karşılaştırılması

Çalışılan Birim	N	Ort	Ss	Sd	*t*	p
Bilgi Teknolojileri Daire Başkanlığı	72	76,36	10,29	499	7,941	,000
Diğer Birimler	429	60,82	16,04			

Çizelge 7.17 incelendiğinde, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin Kişisel Verilerin Korunması alt boyutundan elde ettikleri puan ortalamalarının 76,36 (ss=10,29) olduğu, diğer birimlerde görev yapan katılımcıların elde ettikleri puan ortalamalarının 60,82 (ss=16,04) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların Kişisel Verilerin Korunması alt boyutundan elde ettikleri puanların diğer birimlerde görev yapan katılımcılardan anlamlı olarak daha yüksek olduğu bulunmuştur (t(499)= 7,941; p< ,05). Bir başka deyişle, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcılar diğer birimlerde görev yapan katılımcılara oranla kişisel verilerin korunması konusunda daha yüksek bilgi güvenliği farkındalığına sahiptirler.

Çizelge 7.18. Katılımcıların bilgi güvenliği farkındalığı ölçeğinden elde ettikleri puanların görev yaptıkları birime göre karşılaştırılması

Çalışılan Birim	N	Ort	Ss	Sd	*t*	p
Bilgi Teknolojileri Daire Başkanlığı	72	135,13	22,63	499	8,924	0
Diğer Birimler	429	103,29	28,81			

Çizelge 7.18 incelendiğinde, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların Bilgi Güvenliği Farkındalığı Ölçeğinin toplamından elde ettikleri puan ortalamalarının 135,13 (ss=22,63) olduğu, diğer birimlerde görev yapan katılımcıların elde ettikleri puan ortalamalarının 103,29 (ss=28,81) olduğu görülmektedir. Puan ortalamalarının karşılaştırılması sonucunda ise, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların ölçeğin toplamından elde ettikleri puanların diğer birimlerde görev yapan katılımcılardan anlamlı olarak daha yüksek olduğu bulunmuştur ($t(499)= 8,924$; $p< ,05$). Bir başka deyişle, Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcılar diğer birimlerde görev yapan katılımcılara oranla daha yüksek bilgi güvenliği farkındalığına sahiptirler.

8. SONUÇ, TARTIŞMA VE ÖNERİLER

Bilgi ve iletişim teknolojilerinin kullanımı yaşamımızı kolaylaştırmanın yanında pek çok riski ve tehlikeyi de beraberinde getirmiştir. Bu teknolojilerin kötü niyetli ve uygunsuz kullanımının sonucu ortaya çıkabilecek tehditlerin farkında olunmaması ve tehditlerden habersiz olunması nedeniyle bilgi güvenliği riskleri de artmaktadır. Riskleri gidermenin ve kabul edilebilir seviyelere düşürmenin yolu insana yatırım yapmaktan geçmektedir. Yapılan çalışmalar incelendiğinde bilgi güvenliği konusunda bilgi sistemlerinin güvenliğini sağlamaya yönelik olduğu ve kullanıcıların bilinçlendirilmesine yönelik çeşitli tavsiyeler ve alınması gereken tedbirler yer almaktadır.

Ölçek uygulanan kadın katılımcıların bilgi güvenliği farkındalığı ile erkek katılımcıların bilgi güvenliği farkındalığı benzer seviyede olduğu gözlemlenmiştir. Aynı şekilde Okul, Şişek, Hafçı ve Barış (2018) konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalığını inceledikleri çalışmasında aynı sonuca ulaşmışlardır. Bu durum Keser, Çetinkaya ve Güldüren (2016)'in ortaöğretim öğrencilerine uyguladığı bilgi güvenliği farkındalığı belirleme çalışmasından farklıdır. Ortaöğretim öğrencileri arasında erkek öğrencilerin bilgi güvenliği farkındalığının kız öğrencilerden daha yüksek olduğu bulunmuştu. Yılmaz, Şahin ve Akbulut (2016)' un öğretmenlerin dijital veri güvenliği farkındalığı üzerine yaptığı çalışmasındaki sonuçları desteklemektedir. Çalışmada erkek öğretmenlerin kadın öğretmenlere göre dijital veri güvenliği farkındalığının daha yüksek olduğu bulunmuştur. Yine Arıtürk (2015)' ün mühendislik öğrencileri arasında yapmış olduğu çalışmada kadınların erkeklere göre bilgi güvenliği ve bilgi farkındalığı konusundaki davranışlarının daha yüksek olduğu görülmüştür. Bu çalışma Tekerek ve Tekerek (2013)' in ilk ve ortaöğretim öğrencilerinin farkındalıklarını belirlemek üzere yaptığı çalışmasını ile aynı bulgulara sahiptir. Ortaöğretimde kız öğrencilerin erkek öğrencilere nazaran daha yüksek farkındalık düzeyine sahip olduğu görülmüştür.

Kamu çalışanlarının bilgi güvenliği farkındalıkları yaş aralıklarına göre incelendiğinde 40 yaş altı gruplarda bilgi güvenliği farkındalık seviyesinin 40 yaş üstü katılımcıların bilgi güvenliği farkındalık ölçeğinden aldıkları toplam puandan yüksek olduğu görülmektedir. Gökmen ve Akgün (2015) çalışmalarında yaşın öğretmen adaylarının bilgi güvenliği bilgilerinde bir farklılığa neden olmadığı sonucuna ulaşmıştır. Aynı şekilde Okul, Şimşek, Hafçı ve Barış (2018) konaklama işletme yöneticilerinde bilgi güvenliği farkındalığı

incelediği çalışmasında benzer sonuçlara ulaşmıştır. Ancak Bostan ve Akman (2011) çalışmalarında kadın ve ileri yaştakilerin bilgisayar güvenliği hakkındaki hassasiyetlerinin azaldığını tespit etmişlerdir.

Kamu çalışanlarının çalıştıkları birime göre bilgi güvenliği farkındalıkları karşılaştırıldığında Bilgi Teknolojileri Dairesi Başkanlığı gibi teknik eğitim almış çalışanların olduğu birimin ölçeğin toplam puanından çok yüksek olduğu dolayısıyla birimde çalışanların farkındalıklarının diğer birimlerde çalışanlardan yüksek olduğu görülmüştür. Bu durum Karacı, Akyüz ve Bilgici (2017)' nin yapmış olduğu çalışmada internet ve bilgisayar güvenlik eğitimi alan öğrencilerin bilgi güvenliği tutumlarının daha olumlu olduğu görülmüştür. Bu durum beklenen sonucu desteklemektedir.

Bilgi güvenliği farkındalığı eğitim düzeyine göre incelendiğinde lise ve altı eğitim seviyesine sahip katılımcıların farkındalık seviyelerinin düşük, üniversite ve üstü eğitime sahip katılımcıların ise yüksek olduğu görülmüştür. Bu sonuç eğitim seviyesi arttıkça bilgi güvenliği farkındalığının arttığını göstermektedir. Oktay ve Çakır (2012) ise öğretmenlerin bilgi güvenliği farkındalığını inceledikleri çalışmalarında durumu destekleyen sonuçlara ulaşmışlardır. Öğretmenlerin lisans ve yüksek lisans düzeyi ile ön lisans düzeyi arasında anlamlı bir farklılığın olduğu görülmüş olup eğitim seviyesi arttıkça farkındalığın arttığı yönünde sonuca ulaşılmıştır. Tekerek ve Tekerek (2013)' in ilk ve ortaöğretim öğrencilerinin farkındalıklarını belirlemek üzere yaptıkları çalışmada eğitim düzeyi arttıkça farkındalığın arttığı yönünde sonuçlara ulaşılmıştır. Bu durumun aksine Mart (2012) ise yaptığı çalışmasında eğitim seviyesinin bilgi güvenliği farkındalığı üzerinde anlamlı bir farklılığın olmadığını söylemektedir. Mart (2012)' ın çalışmasını destekleyen sonuçlara Yılmaz, Şahin ve Akbulut (2016)' ta öğretmenlerin dijital veri güvenliğini inceledikleri çalışmalarında öğretmenlerin öğrenim durumuna göre farkındalıkları değişmemektedir.

Yapılan anket çalışmasının genel sonucu değerlendirildiğinde kamu çalışanlarının siber tehditler alt faktöründe düşük seviyede, kişisel verilerin korunması alt faktöründe orta seviyede hesaplanmıştır. Ölçek genelinde ise toplam alınan puan ortalamalarının orta seviyede olduğu görülmüştür. Bu sonuç Öğütçü (2010)' nün kişisel bilişim güvenliği davranışı ve farkındalığı analizi çalışmasındaki sonuçlarla benzerlik göstermektedir.

Siber güvenlik ve bilgi güvenliği konusunda yaşanan tehditler ve yaşanan kayıplar ileride

yaşanabilecek tehdit ve kayıplar konusunda bilgi vermektedir. Bu konuda alınması gereken tedbirlerin çeşitliliği, çokluğu ve ihtiyaç duyulan koordinasyon ve işbirliğini ortaya çıkarmaktadır.

Anlatılan tüm tedbirlerin tek başına bilinçli bir kullanıcının yerini alamayacağı değerlendirilmekte, ayrıca yapılan bu tür farkındalık belirleme çalışmalarının Sıfır Atık Projesinde olduğu gibi üst kurumlar tarafından yapılmasının daha geniş kitlelere ulaşması ve kurumlar ile vatandaşlar tarafından daha ciddiye alınmasını sağlayacağı düşünülmektedir.

İnternet teknolojisinin baş döndürücü hızla gelişmesine paralel olarak getirdiği tehditler artmakta ve bunlara karşı alınabilecek güvenlik önlemleri ve teknolojileri de gelişerek artmaktadır. Ne var ki, yasal ve idari düzenlemeler bu hızı gerisinde kalmaktadır. Bu nedenle konunun hukuki boyutu gelişmeler dikkate alınarak yeniden düzenlenmelidir.

Mart (2012) çalışmasında bilgi güvenliği okullarda zorunlu bir ders olarak küçük yaşlardan itibaren verilmesi, bilgi iletişim teknolojileri ve internetin kullanımında bilgi güvenliği farkındalığını oluşturulmasına yönelik önerilerde bulunmuştur. Bu önerisi ileriye ışık tutacak şekildedir. Zira okul çağında eğitim gören çocuklar gelecekte bir kurum çalışanı olacaklardır. Gelecekte bireyler hangi konumda ve işle alakadar olursa olsun devletle ve özel sektörle yapacakları işler bilgisayar ortamında internet üzerinden yapılacağı düşünüldüğünde bilgi güvenliği ile ilgili bilincin okul çağında verilmesi hem kişisel verilerin korunmasında hem de kurumsal açıdan personelden kaynaklanan bilgi güvenliği risklerini en aza indirilmesinde etkili olacağı öngörülmektedir. Tekerek ve Tekerek (2013) çalışmalarında öğrencilere ve ebeveynlerine ve öğretmenlere bilgi güvenliği farkındalığını oluşturacak eğitimlerin verilmesi gerektiğini söylemiştir. Bu düşünceyi Karaoğlan Yılmaz ve Çavuş Ezin (2017) ebeveynlerin bilgi güvenliği farkındalıklarını inceledikleri çalışmalarında ebeveynlerin bilgi güvenliği ile ilgili bilgi ve farkındalığı geliştirmeye yönelik düzeylerinin düşük olduğu sonucuna ulaşmış ve ebeveynlerin eğitimlerle bilinçlendirilmesi şeklinde öneride bulunmuştur. Kamu çalışanlarının aynı zamanda bir ebeveyn olma durumu da dikkate alındığında bilgi güvenliğinin her şekilde hayatımızda önemli bir yeri olduğu ortaya çıkmaktadır.

Bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte artık geleneksel bilgi güvenliği

yaklaşımları yerini kurumsal hatta ulusal ve küresel bilgi güvenliği yaklaşımları ve bilgi güvenliği politikalarına bırakmıştır. Ülkemizde ise bilgi güvenliği alanında ve farkındalık konusunda sıkıntılar görülmektedir. Bunun için öncelikle bilgi güvenliğine bakış açılarının değiştirilmesi gerekmektedir. Bilgi güvenliğini sadece bilginin korunması işi olarak düşünmek yerine ülke kalkınmasında gerekli olan kritik altyapılar, e-devlet hizmetleri vb. vatandaşı hizmette yararlanmak için kullandığı her bilgisayar ve cihazın güvenliği olarak düşünmek gerekir.

Şahinaslan ve arkadaşlarına (2009) göre son yıllarda kurumlara yapılan saldırılar artık yıkıcı olmaktan ziyade bilgi sızdırma, bilgi hırsızlığı ve istihbarat amacıyla yapılmaktadır.

Kurumlarda bilginin paylaşıldığı o bilgiye erişmek için yetkisi olan kişilerin yapacakları çok küçük hatalar ve dikkatsizlikler, bilerek ya da bilmeyerek yapılan her türlü ihmal veya suistimal teknik olarak tüm önlemleri boşa çıkaracaktır. Bu nedenle kurumlar, özellikle kamu kurumları kurum faaliyetlerine uygun olan güvenlik politikalarını da kapsayan kurum çalışanlarının niteliklerine göre farkındalık eğitimleri vererek kamu bilgi güvenliği kültürü oluşturma noktasında çalışmalıdır.

2008 yılında CSI' nın hazırlamış olduğu rapora göre 1999 yılından 2008 yılına kadar bazı bilgi güvenliği tehditleri için yapılan bilgi güvenliği farkındalık çalışmaları ile bir düşüş yaşandığı söylenmektedir. Bu durum farkındalığın kendiliğinden oluşmayan bir durum olduğunu göstermektedir. Ancak farkındalık eğitimlerinin de etkili olabilmesi için dikkat edilmesi gereken hususlar bulunmaktadır. Bunların başında tabi ki bilgi güvenliği konusunda verilen eğitim ve bilgilendirmelerin çalışanlar tarafından benimsenmesi ve bir görev olarak kabul edilmesi gelmektedir. Çalışmamızda katılımcıların bilgi güvenliği düzeyi orta seviyede çıkmış olmasına rağmen yüz yüze görüşmeler sırasında bilgi güvenliğinin önemli olduğunu bilmelerine rağmen bunun teknik birimin sorumluluğunda olduğunu düşündükleri kendilerinin bu durumdan haberdar olmalarına gerek olmadığı düşüncesinde oldukları yönünde görüş alınmıştır. Bu durum kurumsal bilgi güvenliği kültürü oluşturulmasında bilgi güvenliği farkındalığının önemini bir kez daha göstermektedir.

Diğer bir husus ise bilgi güvenliği farkındalık eğitimlerinin tek tip kullanıcıya göre yapılmamasıdır. Sistemin her aşamasında yer alan kullanıcıların ihtiyaçları, bilgi

birikimleri, anlayış düzeyleri, eğitimleri ve kurumsal anlayışları dikkate alınarak farkındalık geliştirici eğitimlerin düzenlenmesi gerektiğidir.

Bilgi güvenliği farkındalığı bir defaya mahsus oluşturulup bırakılacak bir iş değil sürekli yenilenmek zorunda olan bir süreçtir. Bu sebeple yenilikler takip edilerek sürekli ve belirli periyodlarla çalışanlara verilen eğitimlerin yenilenmesi gerekmektedir. Bu şekilde çalışanların konuya verilen önemin farkına varması, görevlerini yerine getirirken yeterli sorumluluğu hissetmesi ve doğabilecek risklerden sorumlu olduğunu bilmesi ile bu farkındalığı sürdürmesi sağlanabilecektir. Ancak eğitim ile bilgilendirmenin tek başına yeterli farkındalığı oluşturmadığı bilimsel çalışmalarda yer almaktadır. Pek çok çalışan yeterli bilgi seviyesine sahip olduğu halde sürekli ekran köşelerinden çıkan bilgilendirme ve uyarılar sebebiyle duyarsızlaştığını aktarmaktadır. Bu sebeple çalışanların dikkatlerini çekecek ve akılda kalacak şekilde bilgilendirmeler yapılırken kendi bilgilerini de sınama imkanı bulabilecekleri güvenlik testleri veya habersiz tatbikat ve sınamalar yapılarak ödüllendirme yöntemiyle teşvik sağlanmalıdır.

Ayrıca çalışanlar aynı zamanda vatandaş konumunda oldukları için Güvenli İnternet Günü gibi belirli tarihlerde kutlanan ve bilgi güvenliği farkındalığını amaçlayan ulusal çalışmaların kapsamının artırılarak etkili olması için gerekli desteğin ilgili kurumlarca verilmesi ve daha geniş bir kesimde ilgi uyandırması sağlanmalıdır.

KAYNAKLAR

1. Tan, H., Aktaş, A.Z.,(2011). Bir Kuruluşun Bilgi Sistemi Güvenliği İçin Bir Yaklaşım, 4. Ağ ve Bilgi Güvenliği Sempozyumu.

2. Güldüren, C., Çetinkaya, L.,Keser, H.(2016) Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması, Ankara Üniversitesi, Eğitim Bilimleri Fakültesi.

3. Bostan, A., Akman, İ.(2011). Kullanıcı Açısından Bir Durum Tespiti, IV. Ağ Ve Bilgi Güvenliği Sempozyumu Bildiriler Kitabı, s.51-55.

4. Tekerek, M.,Tekerek, A. (2013) A Research on Students' Information Security Awareness, Turkish Journal of Education, Cilt: 2 Sayı: 3, Kahramanmaraş.

5. Keser, H., Güldüren, C.(2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması, Kastamonu Üniversitesi Kastamonu Eğitim Dergisi, Cilt: 23 Sayı:3, 1167-1184, Kastamonu.

6. Baykara, M.,Daş, R., Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensics and Security, 212-215, Elazığ.

7. Canbek, G., Sağıroğlu, Ş. (2006). Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi Cilt:9 Sayı:3 s.165-174, Ankara.

8. T.C Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi Başkanlığı (2011). Bilgi Toplumu İstatistikleri 2011.

9. Güngör, M. (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, T.C Kalkınma Bakanlığı Uzmanlık Tezi, Ankara.

10. Gökmen, Ö.F., Akgün, Ö.E. (2015). Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Bilgilerinin Çeşitli Değişkenlere Göre İncelenmesi, Çukurova Üniversitesi Eğitim Fakültesi Dergisi Cilt: 44 Sayı:1, Adana.

11. Yılmaz, E., Şahin, Y.L., Akbulut, Y. (2015). Dijital Veri Güvenliği Farkındalığı Ölçeğinin Geliştirilmesi, AJIT-e: Online Academic Journal of Information Technology Cilt: 6 Sayı: 21 , İstanbul.

12. Çetinkaya, M.,Gökçöl, O. (2010). Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi, 3.Ağ ve Bilgi Güvenliği Sempozyumu, Ankara.

13. Eminağaoğlu, M., Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi Cilt: 11, Sayı:4 s.1-15, İzmir.

14. Vural, Y.,Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi Dergisi. Cilt 23, No 2, 507-522, Ankara.

15. Alagöz, A.,Allahverdi, M. (2011) Kurumsal Bilgi Güvenliği Ve Muhasebe Bilgi Sistemi, Muhasebe ve Vergi Uygulamaları Dergisi, Ankara.

16. Çetinkaya, M. (2008). Bilgi Güvenliği Yönetim Sistemleri Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi, Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

17. Hekim, H.,Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, Cilt: 4 Sayı: 2, Ankara

18. Yavanoğlu, U.,Sağıroğlu, Ş., Çolak, İ. (2012). Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler, Politeknik Dergisi Cilt:15 Sayı: 1 s. 15-27, Ankara.

19. Vural, Y.,Sağıroğlu, Ş. (2011). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler, Gazi Üniversitesi, Mühendislik Mimarlık Fakültesi Dergisi. Cilt 26, No 1, s. 89-103, Ankara.

20. Haklı, T. (2012). Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi, Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta.

21. Sparrow, J.,(1998). Knowledge in organizations: Access to thinking at work. London: Sage Publication.

22. Henkoğlu, T., Yılmaz, B. (2013). Avrupa Birliği Bilgi Güvenliği Politikaları, Türk Kütüphaneciliği Cilt: 27 Sayı :3, Ankara.

23. Öğün,M.N., Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler, Güvenlik Stratejileri Dergisi, İstanbul.

24. Karaoğlan Yılmaz, G.,Yılmaz, R., Sezer, B. (2014) Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış, Bartın Üniversitesi Eğitim Fakültesi Dergisi, Bartın.

25. Çetin, H. (2014) Kişisel Veri Güvenliği ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi, Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, Antalya.

26. Erol, O.,Şahin, Y.L, Yılmaz, E., Haseski, H.İ. (2015) Kişisel Siber Güvenliği Sağlama Ölçeği Geliştirme Çalışması, International Journal of Human Sciences, Sakarya.

27. Şimşek, G.,Okul, T., Hafçı, B., Barış, Z. (2018) Konaklama İşletmesi Yöneticilerinde Bilgi Güvenliği Farkındalığı: Kuşadasındaki Beş Yıldızlı Oteller Örneği, Uluslararası

Türk Dünyası Turizm Araştırmaları Dergisi, Kastamonu.

28. Talan, T.,Aktürka, C., Korkmaz, A., Gülseçen, S. (2015) Üniversite Öğrencilerinin Akıllı Telefon Kullanımında Güvenlik Farkındalığı, International Journal of Organisational Design and Engineering.

29. Özdemirci, F.,Aydın, C. (2007). Kurumsal Bilgi Kaynakları ve Bilgi Yönetimi, Türk Kütüphaneciliği Cilt: 21 Sayı: 2, Ankara.

30. Yalçıntaş, L. (2013). İnternet Değişim Noktası ve Veri Merkezlerinin Bilgi Güvenliği Perspektifinden İncelenmesi; Dünyadaki Durum ve Ülkemiz İçin Öneriler, Teknik Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

31. Şahinaslan, E.,Kantürk, A., Şahinaslan, Ö., Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, 11.Akademik Bilişim Konferansı Bildirileri, s.605-610, Şanlıurfa.

32. Seferoğlu, S.,Yıldız Durak, H., Karaoğlan Yılmaz, F.G., Yılmaz, R. (2018) Bilgi Güvenliği Farkındalığı ve Bilgi Güvenliği Politikalarıyla İlgili Bir İnceleme, Eğitim Teknolojileri Okumaları, s.29-43, Adapazarı.

33. Öztemiz, S.,Yılmaz, B. (2013) Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara' daki Üniversite Kütüphaneleri Örneği, Bilgi Dünyası, Ankara.

34. Yılmaz, E.,Şahin, Y.L., Akbulut, Y. (2016) Öğretmenlerin Dijital Veri Güvenliği Farkındalığı, Sakarya University Journal of Education, Sakarya.

35. Ünver, M.,Canbay, C., Mirzaoğlu, A.G. (2011) Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler, Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

36. Yılmaz, E., (2015) Öğretmenlerin Dijital Veri Güvenliği Farkındalığı, Doktora Tezi, Eskişehir Anadolu Üniversitesi Eğitim Bilimleri Enstitüsü, Eskişehir.

37. Karaoğlan Yılmaz, F.G.,Çavuş Ezin, Ç. (2017) Ebeveynlerin Bilgi Güvenliği Farkındalıklarının İncelenmesi, Eğitim Teknolojisi Kuram ve Uygulama,Cilt:7 Sayı:2, Ankara.

38. Karacı, A.,Akyüz, H.İ., Bilgici, G. (2017) Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi, Kastamonu Eğitim Dergisi, Cilt:25 Sayı:6, Kastamonu.

39. Kuru, H., Ocak, M.A., (2016).Determination of Cyber Security Awareness of Public Employees and Consciousness-rising Suggestions, Journal of Learning and Teaching in Digital Age, Cilt: 1 Sayı:2, s.57-65, Ankara.

40. Korkmaz, E.V. (2018). Üniversite Öğrencilerinin İnternet ve Veri Güvenliği Farkındalıkları, Journal of Social an Humanities Sciences Research, Kahramanmaraş.

41. Çakır, H.,Hava, K., Gülen, Ş.B., Özüdoğru, G. (2015) Öğretmen Adaylarının Sosyal Ağ Sitelerinde Güvenlik Farkındalıklarının İncelenmesi, International Journal of Human Sciences, Sakarya.

42. Ünver, M., Canbay, C. (2010) Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik, Elektrik Mühendisliği Dergisi, Sayı: 438 s.94-103, Ankara.

43. İnternet: STM Mühendislik Teknoloji Danışmanlık. 2018 Ocak-Mart Dönemi Siber Tehdit Durum Raporu. URL: https://www.stm.com.tr/documents/file/Pdf/siber-tehdit- durum-raporu-ocak-mart-2018.pdf, Son Erişim Tarihi: 20.09.2019.

44. Kruger, H.,Drevin, L., Steyn, T. (2010) A vocabulary test to assess information security awareness. Information Management & Computer Security, Cilt:18 Sayı:5, s.316-327.

45. Rezgui, Y., Marks, A. (2008) Information security awareness in higher education: An exploratory study. Computers & Security, Cilt: 27 Sayı:7-8, 241-253.

46. Aslay, F. (2017) Siber Saldırı Yöntemleri ve Türkiye' nin Siber Güvenlik Mevcut Durum Analizi, International Journal of Multi disciplinary Studies and Innovative Technologies, Cilt:1 Sayı: 1, Sayfa 24-28.

47. Altınok, E., Vural, A.F. (2007). Bilişim Suçları, Kamu Denetçileri Derneği, Denetişim, Cilt,Sayı: 8,s.74-84, Ankara.

48. İnternet: Gunal, O. Formjacking Yöntemi ile Kredi Kartı Hırsızlığı URL: https://ogunal.com/formjacking-yontemi-ile-kredi-karti-hirsizligi/ Son Erişim Tarihi:10.10.2019.

49. İnternet: Symantec, 2019 İnternet Güvenliği Tehdit Raporu, URL:https://www.symantec.com/content/dam/symantec/docs/reports/istr-24- executive- summary-en-apj.pdf, Son Erişim Tarihi: 15.10.2019.

50. Çakır, H. (2013) İnternet, Etik ve Bilişim Suçları, Eğitimciler İçin Bilgisayar Eğitimi, Bölüm 4, s.1-29, Ankara Üniversitesi.

51. S. Aslan, (2019). Bilişim Teknolojileri Alanındaki Meslek Lisesi Öğrencilerinin Siber Güvenliğe Yönelik Bilgi Düzeylerinin Belirlenmesi, Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Eğitim Bilimleri Enstitüsü, Konya.

52. Büyüköztürk, Ş. (2013). Sosyal Bilimler İçin Veri ve Analizi El Kitabı: İstatistik, Araştırma Deseni, SPSS Uygulamaları ve Yorum. Ankara: Pegem Yayıncılık.

53. Sağıroğlu, Ş., Ersoy, Alkan, (2007). Bilgi Güvenliğinin Kurumsal Bazda Uygulanması, Uluslararası Katılımlı Bilgi Güvenliği e Kriptoloji Konferansı, Ankara.

54. Türkiye Cumhuriyeti 5237 sayılı Türk Ceza Kanunu, Kişisel Verileri Koruma

Kanunu, 2016.

55. İnternet: Bilgi, DIKW Hiyerarşisi ve Dijital Devrim (2011). URL: http://www.ulugsungur.com/2011/11/bilgi-bilgi-hiyerarsisi-ve-dijital.html, Son Erişim Tarihi: 18.12.2018.

56. İnternet: Information Assurance Versus Information Security (2011). URL: https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/,Son Erişim Tarihi: 03.09.2019.

57. İnternet: Bilgi Teknolojileri ve İletişim Kurumu, Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu. URL: btk.gov.tr/uploads/pages/pazar-verileri/4-ceyrek-2018kdisi.pdf, Son Erişim Tarihi: 13.09.2019.

58. Oktay, S., Çakır, R. (2012). İlköğretim Öğretmenlerinin Teknoloji Kullanımları ve Teknolojiye Yönelik Tutumları Arasındaki İlişkinin İncelenmesi. X. Ulusal Fen Bilimleri ve Matematik Eğitimi Kongresi, Niğde.

59. Öğütçü, G. (2010). E-dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığın Analizi. Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

60. Mart, İ, (2012). Bilişim Kültüründe Bilgi Güvenliği Farkındalığı, Yayımlanmamış Yüksek Lisans Tezi, Kahramanmaraş Sütçü İmam Üniversitesi, Fen Bilimleri Enstitüsü, Kahramanmaraş.

61. Arıtürk, M. (2015). Bilgi Farkındalığı ve Bilgi Güvenliğinin Karşılaştırılması. XVII. Akademik Bilişim Konferansı Bildirileri, s.178-185, Eskişehir.

62. Bostan, A., Şengül, G. Sağıroğlu, Ş., Alkan, M.(Editörler) (2018). Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Ankara: Grafiker Yayınları. 145-160s.

63. Erol.,S.E., (2016). Siber Güvenlik Farkındalığı İçin Yetenek Tabanlı Dinamik Model, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

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

EKLER

EK-1. Bilgi güvenliği farkındalık ölçeği

	Maddeler	**Hiç Katılmıyorum**	**Katılmıyorum**	**Kararsızım**	**Katılıyorum**	**Tamamen Katılıyorum**
1	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
2	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
3	Aldatmaca (hoax) nedir biliyorum.					
4	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					
5	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
6	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
7	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
8	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					
9	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
10	Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.					
11	Kimlik avı (phishing) saldırısı nedir biliyorum.					
12	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
13	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
14	Siber zorbalık (cyber bullying) nedir biliyorum.					
15	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					
16	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.					
17	Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
18	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
19	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
20	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum.					
21	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtimeprotection) özelliğini kullanmaktayım.					

EK-1. (devam) Bilgi güvenliği farkındalık ölçeği

22	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
23	Dijital imza (digitalsignature) nedir biliyorum.					
24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
25	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
26	İstenmeyen elektronik posta (spam) nedir biliyorum.					
27	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
28	Sosyal ağ sitelerini (socialnetworkingsites) güvenli olarak nasıl kullanacağımı biliyorum.					
29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
30	Taşınabilir cihazlara (portabledevices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
32	Kişisel mahremiyet nedir biliyorum.					
33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
34	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					

Evrak Tarih ve Sayısı: 23.08.2019-E.103306

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

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

BİLİŞİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 17.06.2019 tarih ve E.74003 sayılı yazınız

İlgi yazınız ile göndermiş olduğunuz, Enstitünüz Adli Bilişim Anabilim Dalı **Yüksek Lisans Öğrencisi Ayşe ÖZDEMİR'in, Doç.Dr.Çelebi ULUYOL'un** danışmanlığında yürüttüğü ***"Kamu Kurum ve Kuruluşlarında Bilgi Güvenliği Farkındalığı"*** adlı tez çalışması ile ilgili konu Kurulumuzun **26.07.2019** tarih ve **08** sayılı toplantısında görüşülmüş olup,

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

Bilgilerinizi ve gereğini rica ederim.

e-imzalıdır
Prof. Dr. Mehtap ÇAKAN
Kurul Başkanı

Araştırma Kod No: 2019-243

Ek: 1 Liste

Ankara
Tel:0 (312) 202 20 57 - 0 (312) 2... Faks:0 (312) 202 38 76
İnternet Adresi: http://etikkomisyon.gazi.edu.tr/

Bilgi için :Nursel Ciliner
Birim Evrak Sorumlusu
Telefon No:202 20 57

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : Ayşe ÖZDEMİR
Uyruğu : T.C
Doğum tarihi ve yeri : 07/11/1985 ÇANKIRI
Medeni hali : Bekar
Telefon :
Faks :
e-posta : ayse.ozdemir1@gazi.edu.tr

Eğitim Derecesi	Okul/Program	Mezuniyet yılı
Yüksek lisans	Gazi Üniversitesi /Bilişim Enstitüsü / Adli Bilişim Ana Bilim Dalı	Devam Ediyor
Lisans	Gazi Üniversitesi/ Bilgisayar Mühendisliği Bölümü	2011
Lise	Tevfik İleri İmam Hatip Lisesi (YDA)	2003

İş Deneyimi, Yıl	Çalıştığı Yer	Görev
2013- devam ediyor	Tapu Kadastro Genel Müdürlüğü	Mühendis

Yabancı Dili

İngilizce , Korece

GAZİLİ OLMAK AYRICALIKTIR…