T.C

ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ YÖNETİM SÜRECİNDE SİBER GÜVENLİK

YÜKSEK LİSANS TEZİ

RÜMEYSA MOĞOL DEMİR

BİLGİ VE BELGE YÖNETİMİ ANA BİLİM DALI

ANKARA, 2024

T.C

ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

BİLGİ YÖNETİM SÜRECİNDE SİBER GÜVENLİK

YÜKSEK LİSANS TEZİ

Rümeysa MOĞOL DEMİR

BİLGİ VE BELGE YÖNETİMİ ANA BİLİM DALI

Tez Danışmanı

Doç. Dr. Mustafa BAYTER

ANKARA, 2024

ONAY SAYFASI

Rümeysa Moğol Demir tarafından hazırlanan "Bilgi Yönetimi Sürecinde Siber Güvenlik" adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

<table>
<tr><td colspan="2">JÜRİ ÜYESİ</td><td>Kurumu</td><td>İmza</td></tr>
<tr><td colspan="2">Mustafa Bayter</td><td rowspan="2">Ankara Yıldırım Beyazıt Üniversitesi İnsan ve Toplum Bilimleri Fakültesi</td><td rowspan="2"></td></tr>
<tr><td>Kabul ☑</td><td>Red ☐</td></tr>
<tr><td colspan="2">Erdinç Alaca</td><td rowspan="2">Ankara Yıldırım Beyazıt Üniversitesi İnsan ve Toplum Bilimleri Fakültesi</td><td rowspan="2"></td></tr>
<tr><td>Kabul ☑</td><td>Red ☐</td></tr>
<tr><td colspan="2">Sacit Arslantekin</td><td rowspan="2">Ankara Üniversitesi Dil ve Tarih Coğrafya Fakültesi</td><td rowspan="2"></td></tr>
<tr><td>Kabul ☑</td><td>Red ☐</td></tr>
</table>

Tez Savunma tarihi:

Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü Bilgi ve Belge Yönetimi Anabilim Dalı'nda Yüksek Lisans tezi olması için şartları yerine getirdiğimi onaylıyorum.

Sosyal Bilimler Enstitüsü Müdürü Unvan, Ad Soyad

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda patent ve telif haklarını ihlal edici etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tezde kullanılmış olan tüm bilgi ve yorumlara kaynak gösterdiğimi beyan ederim. Tarih (…/…/…)

Rümeysa MOĞOL DEMİR

TEŞEKKÜR

Bu teze başlarken beni her anlamda özgür bırakan, bilimsel düşünceyi yaşam biçimi olarak algılamamı sağlayan lisanstan yüksek lisansa olan yolculuğumda beni destekleyen, bir meslektaş edasıyla yaklaşan bana hep güvenen sayın hocam Prof. Dr. Mustafa Bayter' e teşekkürü borç bilirim. Ayrıca jürimde yer alan kıymetli hocalarım, Prof. Dr. Sacit Arslantekin ve Dr. Öğr. Üyesi Erdinç Alaca'ya çalışmama katkılarından dolayı teşekkür ederim.

Sevgili eşim, Seydi Demir'e de bu süreçteki bana olan inancı, sabrı, sevecenliği ile en önemlisi beni bu süreçte manevi olarak hiç yalnız bırakmadığı için sonsuz teşekkürler.

Hayatımın her aşamasında benim yanımda olan, sadece başarılarımla değil her halimde bana destek olan sevgili aileme teşekkürlerimi sunuyorum. Bu başarılar sizlerin desteği sayesinde.

ÖZET

Bilgi Yönetim Sürecinde Siber Güvenlik

Bilim ve teknolojideki hızlı ilerlemeler, yapılan yenilikler ve gelişimler bilginin yönetim sürecini etkilediği gibi bilgiyi yöneten toplumu da etkilemiştir. Bilgi toplumu bilgi üretim ve yönetim sürecini ele alan bir toplumdur. Gelişen ve değişen bu dünyada her gelişim bilgi ile mümkündür. Bilgilerin yönetimi, değişimi ile birlikte korunması ve bu bilgilerin yönetim sürecindeki koruma protokolleri de bilgi güvenliği gerekliliğini ortaya koymuştur. Nitelikli bir bilgi yönetim süreci için siber güvenlik gerekli bir bağlamdır. Hayatımızın her aşamasında kullanılan bilginin, dijital ortamlarda yaygınlaşmasıyla birlikte siber tehditlere karşı daha savunmasız hale gelinmiştir. Siber tehditler, bilgi yönetim sürecinde büyük riskler oluşturur. Bu tehditler arasında veri ihlalleri, fidye yazılımları, kimlik avı saldırıları ve iç tehditler yer alırken daha birçok tehditlerin varlığı da bilgi yönetiminde siber güvenliğin uygulanması gerekliliğini ortaya koymaktadır.

Bilgi yönetiminde siber güvenliğin gerekliliği, sadece verilerin korunması değil, aynı zamanda iş sürekliliğinin sağlanması, yasal uyumlulukların yerine getirilmesi ve itibarın korunması açısından da kritik öneme sahiptir. Bu durumda da bilgi dünyasında ve her şeyin bilgi ile erişilebilir hale gelmesi kontrollü ve korunaklı bir şekilde olmasını gerektirmektedir. Bu yüzden bu çalışmada amaçlanan bilgi uzmanı gözünden siber güvenlik kavramına bilgi yönetim süreci perspektifinden bakmaktır. Aynı zamanda bilginin korunması ve güvenlik sınırları siber güvenlik sınırlarıyla da daha güvenilir hale gelmesi için siber güvenlik önlemlerinin ve bilgi yönetiminin nasıl yapılması gerektiği üzerinde çalışılarak farkındalık oluşturmak amaçlanmıştır.

Bu çalışmada bilginin yönetim sürecinden sibere yolculuk, siber güvenliğin günümüzde bilgi dünyasındaki yeri ve önemine, stratejilerine ve siber güvenlik uygulamalarına değinilmiştir. Bunun yanında siber güvenlik kavramı ve bilgi yönetimi üzerindeki etkileri incelenmiştir. Siber tehditlerin ve saldırıların artan karmaşıklığına dikkat çekerek, bu tehditlerin bilgi yönetim süreçlerine etkisinden bahsedilmiştir. Bir diğer bölümde bilgi yönetim sürecinde siber güvenliğin sağlanmasına yönelik stratejiler ve en iyi

uygulama örneklerine değinilmiştir.

Çalışmada betimleyici araştırma yöntemi kullanılmıştır. Yazılı, görsel ve işitsel materyallerin incelenmesi, web sitelerinin incelenmesi, belge araştırması, internet ve dijital veri toplama yöntemleriyle çalışma ilerletilmiştir.

Araştırma siber güvenlik tehditlerine karşı koymak için önerilen yeni politika ve prosedürleri içerir ve bilgi güvenliği politikalarını güçlendirmelerine ve güncellemelerine yardımcı olabilir. Bu tez bilgi yönetimi ve siber güvenlik arasındaki ilişkiyi daha iyi anlamak için gelecekte yapılacak araştırmalara yönelik çeşitli araştırmalar sunmaktadır.

Yapılan çalışmalar sonucunda siber güvenlik, veri ihlallerini engelleyerek bilgilerin doğruluğunu korumaktadır ve sistemlerin kesintisiz çalışmasını sağlayarak iş süreçlerinin aksamasını önleyebilmektedir. Bunun sonunda siber güvenlik uygulamaları, bilgi yönetiminde hem güvenilirliği artırarak kurumsal itibarın korunmasına katkıda bulunmaktadır.

Çalışmanın sonucunda elektronik ortamların artmasıyla birlikte bilgi güvenliği zafiyetleri oluşmaktadır. Bu zafiyetler siber tehditleri beraberinde getirmektedir. Bu tehditler için belirlenmiş olan siber güvenlik tedbirleri kullanılarak siber dayanıklılık artırılmaktadır. Teknolojik yetkinliğe sahip kurum ve kuruluşlardaki personel, siber güvenlik eğitimleri alarak kurumlardaki stratejilerin gelişmesine katkı sağlamaktadır. Siber güvenlik çalışmalarını daha nitelikli ve geliştirilebilir hale getiren BTK, TÜBİTAK, SGE, USOM, TÜBİTAK BİLGEM gibi kurumlar siber güvenlik konusunda kurumsal planlamalarını yapmaktadır. Yerli ve milli yazılımlar, uygulama üretimleriyle birlikte siber güvenlik çalışmalarının gerekliliği de ortaya konulmaktadır.

Anahtar Kelimeler: Bilgi, Bilgi Yönetimi, Bilgi Güvenliği, Siber, Siber Güvenlik.

ABSTRACT

Cyber Security in the Information Management Process

Rapid advances in science and technology, innovations and developments have affected the information management process as well as the society that manages information. The information society is a society that addresses the information production and management process. In this developing and changing world, every development is possible with information. The management, change and protection of information and the protection protocols in the management process of this information have also revealed the need for information security. Cyber security is a necessary context for a qualified information management process. As the information used at every stage of our lives becomes widespread in digital environments, it has become more vulnerable to cyber threats. Cyber threats pose major risks in the information management process. While these threats include data breaches, ransomware, phishing attacks and internal threats, the existence of many more threats also reveals the necessity of implementing cyber security in information management.

The necessity of cyber security in information management is critical not only in terms of protecting data, but also in terms of ensuring business continuity, fulfilling legal compliance and preserving reputation. In this case, in the information world and making everything accessible with information requires it to be in a controlled and protected manner. Therefore, the aim of this study is to look at the concept of cyber security from the perspective of the information management process through the eyes of an information expert. At the same time, it is aimed to raise awareness by studying how cyber security measures and information management should be carried out in order to protect information and make it more reliable with security boundaries and cyber security boundaries.

In this study, the journey from the information management process to cyber, the place and importance of cyber security in the information world today, strategies and cyber security applications are discussed. In addition, the concept of cyber security and its effects on information management are examined. Drawing attention to the increasing complexity of cyber threats and attacks, the effects of these threats on information management

processes are mentioned. In another section, strategies and best practice examples for ensuring cyber security in the information management process are discussed.

The descriptive research method was used in the study. The study was advanced with the examination of written, visual and audio materials, examination of websites, document research, internet and digital data collection methods.

The research includes new policies and procedures recommended to counter cyber security threats and can help them strengthen and update information security policies. This thesis presents various studies for future research to better understand the relationship between information management and cyber security.

As a result of the studies, cyber security protects the accuracy of information by preventing data breaches and prevents the disruption of business processes by ensuring the uninterrupted operation of systems. As a result, cyber security applications contribute to the protection of corporate reputation by increasing reliability in information management.

As a result of the study, information security vulnerabilities occur with the increase in electronic environments. These vulnerabilities bring cyber threats. Cyber resilience is increased by using cyber security measures determined for these threats. Personnel in institutions and organizations with technological competence contribute to the development of strategies in institutions by receiving cyber security training. Institutions such as BTK, TÜBİTAK, SGE, USOM, TÜBİTAK BİLGEM, which make cyber security studies more qualified and improvable, make their corporate plans on cyber security. The necessity of cyber security studies is also revealed with domestic and national software and application productions.

Keywords: Information, Information Management, Information Security, Cyber, Cyber Security.

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

APA: American Psychological Association (Amerikan Psikologlar Birliği)

BBY: Bilgi ve Belge Yönetimi

BGY: Bilgi Güvenliği Yönetimi

BGYS: Bilgi Güvenliği Yönetim Sistemi

BSI: British Standards Institute (İngiliz Standartları Enstitüsü)

BTK: Bilgi Teknolojileri ve İletişim Kurumu

COBIT: Information Systems Audit and Control Association (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)

DDoS: Distributed Denial of Service Attack (Dağıtık Hizmet Reddi Saldırıları)

EBYS: Elektronik Belge Yönetim Sistemi

ENISA: European Union Agency for Cybersecurity (Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı)

IEEE: Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)

IDS: Intrusion Detection System (Saldırı Tespit Sistemi)

ILSIS: İl Milli Eğitim Müdürlüğü Bilgi Sistemleri

ITIL: Information Technology Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)

IoT: Internet of Things (Nesnelerin İnterneti)

ISO: International Organization for Standardization (Uluslararası Standardizasyon Örgütü)

KTÜ: Karadeniz Teknik Üniversitesi

KVKK: Kişisel Verileri Koruma Kanunu

MERNİS: Merkezi Nüfus İdare Sistemi

NATO: North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması Örgütü)

NCIRC: NATO Computer Incident Response Capability (NATO Bilgisayar Olaylarına Müdahale Ekibi)

ORION: Veri Güvenlik Platformu

SGE: Siber Güvenlik Enstitüsü

SİBERLAB: Sanal Siber Güvenlik Laboratuvarı

SOME: Siber Olaylara Müdahale Ekibi

SSCB: Sovyet Sosyalist Cumhuriyetler Birliği

TDK: Türk Dil Kurumu

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

TÜİK: Türkiye İstatistik Kurumu

ULAKBİM: Ulusal Akademik Ağ ve Bilgi Merkezi

UEKAE: TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

USOM: Ulusal Siber Olaylara Müdahale Merkezi

UYAP: Ulusal Yargı Ağı Projesi

VPN: Virtual Private Network (Sanal Özel Ağ)

YÖK: Yüksek Öğretim Kurulu

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

GİRİŞ

Konunun Önemi

Gelişen ve değişen bilgi dünyasında, yaşama damgasını vuran ve tarım toplumundan bilgi toplumuna geçiş sürecinde en önemli olgu bilgi olmuştur. Bilginin günümüzde artış hızının kontrol edilebilmesi ve yönetilmesi şarttır. Endüstri 4.0 ile birlikte internet ve bilgisayarın olduğu her ortamda veri akışından ve veri yönetiminden söz etmemek mümkün değildir. Bilgisayar teknolojilerindeki gelişim ile birlikte bilgi yönetim şekillerinde farklılıklar olmuştur. Bu farklılıklara karşılık bilgi yönetim süreçleri belirlenmiş olup bilgi yönetimindeki riskler için de bilgi güvenliği yöntemleri belirlenmiştir. Bilgi yönetimindeki değişkenler ve yenilikler sistemlerde, yönetimlerde, cihazlarda ve insan faktörü olan her yerde farklılığa uğramıştır. Bilginin güç olduğu, bilgiye sahip toplumun bilgi toplumu olarak adlandırılabildiği bir bilgi dünyasında tüm bu değişiklikleri risklerden ve oluşabilecek her türlü tehditten korunması için de güvenlik önlemleri gerekmektedir. Bilgi güvenliğinin sağlanması sadece yönetimsel değil bilgi organizasyonlarının bilgi varlıklarını koruyarak, operasyonel verimliliği artırmak odaklı, yasalara uygun olabilecek şekilde, teknik ve stratejik önlemlerle sürdürülebilir bir siber güvenlik sürecini ele almak gerekmektedir.

Siber güvenlik stratejilerine bütüncül bir bakış açısıyla bakarak bilgi yönetimi sürecindeki gereklilikler ele alınmalı ve siber saldırıların, siber tehditlerin arttığı bir düzende işletmelerin, organizasyonların ve hatta devletlerin bilgi güvenliğine karşı ciddi risklere karşı tedbirlerinin de üst düzey olması beklenmektedir. Bu nedenlerle, siber güvenlik, bireyler, organizasyonlar ve devletler için hayati bir öncelik taşımaktadır. Etkili siber güvenlik önlemleri, bilgi varlıklarının korunmasını, iş sürekliliğinin sağlanmasını ve dijital dünyada güvenliğin sürdürülebilir olmasını sağlamaktadır. Bilgi dünyasındaki siber güvenlik stratejilerinin detaylandırılması ve uygulanmasıyla birlikte de organizasyonlarda siber güvenliğe olan ilgi ve bilinçlenme her geçen gün artmaktadır. Tüm bu süreçlere göre siber bilinçlenmenin artması, bilgi güvenliklerinin daha nitelikli hale getirilmesi, çeşitli tehditlere karşılık tedbirlerin geliştirilmesi için bu konu işlenmekte ve detaylandırılmaktadır.

Bu çalışmada bilginin güç olduğu bilgi dünyasında bilgi yönetiminin nitelikli ve güvenilir olmasını, farklılıklara karşılık bilgi yönetim süreçlerinin belirlenmesini, bilgi yönetimindeki değişkenlerin farklılıklara uğramasını, bilginin her türlü tehditten korunması gerektiğini, güvenlik önlemlerinin alınması gerekliliği üzerinde durulmaktadır. Bu çalışmayla siber güvenlik kavramına bilgi yönetim sürecinden bakılarak literatürde siber güvenlik ve bilgi güvenliği çalışmalarının yanına eklenecektir. Literatürdeki siber güvenlik çalışmaları incelendiğinde siber güvenlik kavramı genel ele alınmıştır. Bu çalışmayla da siber güvenlik bilgi ve bilgi yönetimi çerçevesinde, bilgi güvenliği odağında şekillenmiştir.

Araştırmanın Amacı, Problem ve Hipotezi

Bu araştırmada temel amaç, bir bilgi uzmanı gözünden siber güvenlik kavramına bilgi yönetim süreci açısından incelemektir. Ayrıca çalışmanın iki alt amacı bulunmaktadır. Bunlardan ilki, bilgi güvenliği ve bilgi yönetiminin gereklilikleri ve başarı odakları incelenerek, bilgi güvenliğinde başarılı olunması için hangi şartların oluşması gerektiği üzerine odaklanmaktır. Diğer alt amaç ise siber güvenlik seviyesinde bilgi yönetiminin nasıl yapılması gerektiğine değinerek farkındalık oluşturmak ve bu alana ilgi duyan kitlede bilinç oluşturmaktır.

Araştırmanın problemi; " Bilgi yönetim sürecinde bilgi güvenliği şarttır ve siber güvenliğin bu süreçteki rolü ve etkisi nedir?" olarak düşünülmüştür. Buna bağlı olarak da aşağıdaki sorulara cevap aranmıştır:

1) Bilgi yönetiminde siber güvenliğin yeri ve önemi nedir ve ne olmalıdır?
2) Bilgi güvenliğini sağlamak için yapılan siber güvenlik sistemleri nelerdir?
3) Bilgi güvenliği yönetim süreci nasıl ilerler?
4) Bilgi güvenliğinde siber gereklilikler nelerdir?
5) Bilgi yönetim sürecinde siber güvenliğin gerçekleştirilmesi için nasıl bir strateji izlenmelidir?

Bu bağlamda araştırmanın hipotezi; " Bilgi yönetim ilkelerine dayanılarak bilginin yönetiminin sağlanması için günümüz dünyasında siber güvenlik ilkelerine de bağlı kalarak, güvenlik önlemleri alınmalıdır. Nitelikli bir bilgi yönetim süreci için siber güvenlik gerekli

bir bağlamdır.” şeklinde belirlenmiş ve araştırmalar bu doğrultuda devam etmiştir.

Araştırmanın Yöntemi ve Veri Toplama Teknikleri

Araştırma yöntem ve teknik olarak betimleyici araştırma yöntemi kullanılmıştır. Betimleme yöntemi, “araştırma çerçevesinde belirlenen amaç için varlıkların, kurumların, grupların ne olduğunu betimlemeyi ve mevcut durumları olduğu gibi açıklamayı benimsemektedir” (Alaca, 2021, ss.329). Nitel araştırma yöntemlerinden de belge analizi seçilmiştir. Nitel araştırma, “gözlem, görüşme ve doküman analizi gibi nitel veri toplama tekniklerinin kullanıldığı, algıların ve olayların doğal ortamda gerçekçi ve bütüncül bir biçimde ortaya konmasına yönelik nitel bir sürecin izlendiği bir araştırma yöntemidir” (Demirel, 2023).

Veri toplama tekniği olarak; yazılı, görsel veya işitsel materyallerin incelenmesi, belge araştırması, internet ve dijital veri toplama kullanılmıştır. Her bir veri toplama tekniği, araştırmanın geçerliliği, güvenirliği ve genel kalitesi açısından farklı avantajlar ve zorluklar sunar.

Araştırmanın Kapsamı

Araştırmanın kapsamı; bilgi yönetimini sürekli güncellenmekte olan siber güvenlik kavramı çerçevesinde incelemek ve bilgi yönetim sürecine entegre etme yöntem ve tekniklerini ortaya koymaktır. Araştırmada, bilginin temelinden, bilgi yönetimi, bilgi yönetim süreci, bilgi güvenliği, bilgi güvenliğinin gerekliliği, siber ve siber güvenlik gerekliliği, bilgi güvenliğiyle siber güvenliğin ilişkisi incelenmiş, bilgi yönetiminde siber stratejiler ortaya konulmaya çalışılmıştır. Siber güvenlik için yapılan çalışmalar ele alınmış ve Türkiye’deki etkilerine ve uygulamalarına değinilmiştir. Bilgi ve Belge Yönetimi Bilim dalında siber güvenlik ve bilgi güvenliği arasındaki ilişki ele alınarak sentez yapılmıştır.

Kaynaklar ve Literatür Taraması

Literatür araştırmasında; Fehmi Volkan Akyön’ün 2001’de “Bilgi Kavramı ve

Yönetimi" adlı makalesinde bilgiye kavramsal bakış açısı ve bilgi yönetiminin nasıl olması gerekliliği üzerinde durulan bir çalışmadır. Bilgi yönetimindeki değişikliklerin bilgi teknolojileri ile bağlantılı olduğundan bahsedilmektedir.

Hüseyin Balcılar'ın 2008'de "Türkiye'nin Bilgi Toplumu Olma Yolunda Bilgi Teknolojilerinden İnternetin Kullanımı" adlı çalışmasında bilgi, bilgi toplumu, bilgi toplumu ile Türkiye ilişkisi, Türkiye'de bilgi toplumu olunması için yapılması gereken çalışmalara değinilmiştir. Bilgi teknolojilerindeki gelişim ve bu gelişimin bilgi toplumundaki etkilerine değinilmesiyle birlikte bilgi yönetim sürecine değinen bir çalışma olmuştur. Bu çalışmadan yola çıkılarak TÜİK verilerine de bakılmış ve internet kullanımının etkilerinin bilgi yönetim sürecindeki etkileriyle paralel olduğu gözlemlenmiştir.

Osman Yazıcıoğlu, Kemal Varol, Oğuz Borat'ın 2011'de beraber yazdığı " Bilgi Yönetimi" adlı makale bilgi yönetimi ve bilgi kavramlarını anlamak için çeşitli bakış açısıyla incelemelerde bulunulmuştur. Bilgi türelerine, bilgi yönetimin tarihçesine ve bu kavramların analiz tekniği ile incelenmesine yer verilmiştir.

Hasan Yılmaz'ın 2014'de hazırlamış olduğu "TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi" adlı raporunda bilgi ve bilgi güvenliği konusunu detaylı incelemiş olup bilginin temel üç unsuru olan gizlilik, bütünlük, erişilebilirlik kavramlarını detaylandırmıştır. Kişisel ve kurumsal alınması gereken önlemlerden bahsederek örnekler vermiştir.

Zeynep Akdoğan'ın 2022'de hazırlamış olduğu "Kamu Kurumlarında Bilgi Güvenliği Yönetim Sistemleri için Politika Geliştirme Metodolojisi" adlı doktora tezinde bilgi güvenliği çerçevesine geniş bakış açısı ile bakarak ulusal düzeyde yapılan çalışmalardan bahsedilmiştir. Bilgi güvenliğine ilişkin standartların neler olduğuna değinilen ve bunun yanında kavramsal çerçeve de oluşturan bir çalışmadır.

Ali Akın Bozkurt'un 2024'de hazırlamış olduğu "Siber Suçların İncelenmesi ve Siber Güvenlik Kavramları" adlı tezinde siber kavramalarına çerçeve çizilmiş ve siber suçlara yönelik neler yapılması gerekliliği üzerinde durulmuştur. Siber güvenlik kavramlarında hackerlar ve hacker çeşitlerine detaylıca değinerek siber suçların işleniş yöntemlerini de etraflıca çalışılmıştır.

Salim Kurnaz ve Mustafa Özen'in 2019'da "Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri" adlı makalesinde siber güvenlik yönetimi, siber güvenlik stratejilerinin oluşması ve gelişmesine katkı sağlayan çalışmaları ele almıştır. Türkiye'deki siber güvenlik stratejilerinin oluşturulmasında etkili bir çalışma olmuştur. Ulusal siber stratejiler için neler yapıldığı ve iyileştirmek için düzenlemelerin nasıl olması gerektiği üzerinde durulmuştur.

Ceray Aldemir ve Merve Kaya'nın 2020'de yazdığı "Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları" adlı çalışmasında bilgi toplumunun gereklilikleri ve sonucu olarak da bilgi güvenliği ele alınmıştır. Bilginin korunmasında kötüye kullanım sonucunda güvenlik stratejilerinin geliştirilmesine ve önlem alınmasına önem verilmiş bu konuda da neler yapılması gerektiği üzerinde durulmuştur. Siber güvenlik için farkındalık çalışmalarının artırılması ve siber güvenlik yasal çalışmaların iyileştirilmesi gerekliliği vurgulanmıştır.

Vahit Güntay'ın 2016'da "Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi" adlı tezinde ulusal ve uluslararası siber güvenlik çalışmalarına değinerek geniş bir perspektif oluşturmuştur. Siber uzay, siber caydırıcılık, siber terörizm gibi siber ilişkili kavramlara yer verilmiştir.

Bu çalışmada bazı yabancı kaynaklardan da yararlanılmıştır. Dhillon'un "The Role of Information Security in the Organization" adlı eserinde bilgi organizasyonlarında bilgi

güvenliğinin nasıl sağlnaması gerektiği üzerinde inceleme yapmıştır.

Bu tezde, literatürde yer alan kaynaklara erişimde Ankara Yıldırım Beyazıt Üniversitesi, Bayburt Üniversitesi Çevrimiçi Kataloğu ve veri tabanlarından yararlanılmıştır. Ayrıca Google Akademik, YÖK Ulusal Tez Kataloğu ve ULAKBİM veri tabanlarından sağlanarak yazılmıştır. Bunun yanında literatür taramasında kullanılan diğer kaynaklar:

- Bilgi Dünyası
- DergiPark
- ScienceDirect Scopus
- JSTOR
- Proquest
- HiperKitap
- Ebscohost
- Sobiad
- Web of Science
- Türk Kütüphaneciliği
- Sayısal Kitap: Türkçe Dijital Kütüphane
- Resmi Gazete
- Mevzuat Bilgi Sistemi
- Library Archive and Museum Research Journal (LAMRE)
- IEEE
- TÜBİTAK
- TÜİK
- BTK Akademi

Araştırma yapılırken literatür tarama yapılırken aşağıdaki anahtar kelimeler, konu başlıkları ve konularla alakalı olabilecek anahtar kelimler seçilmiştir;

- Bilgi
- Bilgi Yönetimi
- Information
- Information Management
- Information Society
- Information Security
- Information Security Management System

- Bilgi Toplumu
- Bilgi Güvenliği
- Bilgi Güvenliği Yönetim Sistemi
- Bilgi Teknolojileri
- Bilgisayar güvenliği ve ağları
- Dijitalleşme
- Siber
- Siber Güvenlik
- Siber Tehditler
- Siber Stratejiler

- Information Technologies
- Computer security and networks
- Digitalization
- Cyber
- Cyber Security
- Cyber Threats
- Cyber Strategies

Çalışma, Ankara Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü'nün (2023) "Tez Yazım Kılavuzu" esas alınarak yazılmıştır.

Atıflar ve kaynakça, APA7 sistemine göre oluşturulmuştur.

1.BİLGİ KAVRAMI

Bilgi kavramı, Latince ‘informatio’ kökünden gelmiştir ve şekillendirme, biçim verme, bilgi veya haber verme eylemi olarak tanımlanmaktadır (Koçak & Memiş, 2018). Bilgi, Türk Dil Kurumu’nun tanımına göre “İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünüdür” (TDK, 1932). Başka bir kaynakta bilgi kavramı; haber verme, enformasyon, şekillendirme şeklinde tanımlanmaktadır (Selvi, 2012). Edinilen deneyimlerin sonucunda karşılıklı iletilebilen, işlenmemiş verilerin bir arada olması ve anlamlı bir şekilde kaydedilmiş hâline de bilgi denilmektedir. Bilgi (information) kelimesinin temeli, Latince karşılığı herhangi bir şeye şekil vermek anlamına gelen “informare” kelimesinden gelmektedir (Demirtaş, 2013). Bayter’in Kütüphanecilik açısından da en genel bilgi tanımı : “Çeşitli kaynaklardan farklı kanallarla belirli bir amaç için elde edilen, özümsenen ve daha önce var olan bilgide değişiklik yaratarak, bir etkinlik için kullanılabilen ve başkalarına iletilebilmek üzere farklı ortamlara kaydedilebilen bir olgudur” (Bayter, 2015).

Bilgi kavramı incelendiğinde Sebetci’nin Bilgi Teknolojileri ve Yönetim Bilişim Sistemleri adlı kitabında bahsettiği bilgi türleri:

1. Kullanılma Biçimlerine göre: (İdealist, Sistematik, Otomatik)

2. Kaynağına göre: (Açık bilgi, Örtük bilgi)

3. Rekabet üstünlüğüne göre: (İşaretsel, Deneyimsel, Girişimci, Kurumsal)

4. Niteliklerine göre: (Kişisel, Yapısal, Müşteri)

Yukarıda bahsi geçen bilgi türleri sınıflaması farklılıklar göstermektedir. Kavramsal farklılıklar farklı bakış açılarını ortaya koymaktadır.

Bilgi türlerinden konu ile daha alakalı ikinci madde olan kaynağına göre bilgi türleri incelenmektedir. Kaynağına göre bilgi türleri; açık ve örtük bilgi olmak üzere iki tanedir. Açık bilgi; kodlanabilen, kaydedilebilen ve dijital ağlar üzerinden aktarılabilen gerek enformatik gerekse bilimsel bilgiye denir (Selvi, 2012). Buna karşı olarak kodlanıp kaydedilemeyen ve kaydedilmediğinden aktarılamayan bilgiye de örtük yani kapalı bilgi denir. Usta-çırak ilişkilerinde, dededen toruna aktarılan geleneksel deneyimler ve bilgileri,

halk dilinde de nene-dede bilgileri olarak anılan bilgiler de uygulanmasına rağmen kaydedilmeyen ve aktarılamayan bilgi olmasından örtük bilgi özelliğini taşımaktadır. Bilgi ve enformasyon farkı da burada ortay çıkmaktadır. Bilgi, insan davranışından ve anlık oluşan, toplumlarca üretilen, insan düşüncelerinden ortaya çıkan bir olgudur. Bilgi, enformasyon birimlerinin anlamlı ve faydalanılabilir bir biçimde bir araya getirilmesidir (Balcılar, 2008). İşlem görmüş verilerin toplanması ve yönetilmesini kapsayan süreç, bilgidir. Sınıflanmış, organize edilmiş, yönetimi sağlanmış ve yorumlanmış olan verilerin bir sistem içerisinde aktarılması işlemidir. Bilginin oluşum süreci veri, enformasyon, bilgi, bilgelik gibi kavramları ortaya çıkarmıştır. Enformasyon, bilginin kodlanarak kaydedilmiş ve sonrasında saklanmış halidir. Barutçugil'in (2002) de tanımı ile enformasyon; düzenlenmiş verilerdir. Verilerin düzenlemesini başkaları yapmaktadır ve yalnızca ilgili kişi için veriler bir anlam taşımaktadır. Veriler anlamlıdır ve bir amaç için değişime uğramıştır.

Verilerin işlenerek enformasyona dönüşmesi sağlanarak enformasyon detaylandırılır, geliştirilerek işlenmesi sonucu da bilgi oluşmaktadır. Bilginin işlenmesi, erişilmesi, yönetilmesi, saklanması, depolanması gibi süreçler ile birlikte anlam kazanan bilgi karar alma aracı olabilmektedir. Amaca, hedefe ulaşabilmek için elde edilen çözümler ve uygulamalar kararı oluşturmaktadır. Bu durumda bilgi kullanılmadığında bir anlam ifade etmezken karar ve eylemlere geçerken bilginin önemi büyüktür. Ünal'ın (2018) verinin evrimleşme sürecine bakış açısı gelişerek karar aşamasına kadar gelmektedir.

Şekil 1

Verinin dönüşümü

Şekil 1'de verinin bilgeliğe ve sonrasında karar aşamasına gelme süreci gösterilmiştir. Verinin evrimleşmesinde yönetimi, saklanması işlenmesi ve aktarılmasından

sonra elde edilen değerler vardır. Bunlar; veriyi işleyerek değer elde etmek, işlenen veriyi değere dönüştürmek, veriyi bilgiye dönüştürmek ve verinin ekonomisini oluşturmaktır. Günümüzde de ekonomide bilgi üretimi çok önemli hale gelmiştir. Rekabet ortamında bilgi üretme ve yayma ve hatta bu bilgi sürecini yönetme tamamen kuruluşların felsefesi haline gelmiştir. Fabrikalardaki üretim sürecindeki hammadde gibi bilgi de ekonomide değerli hale gelmiştir. Bilginin gücü ve erişimi bazı şirketlerde ana madde haline gelmiştir. Yazıcıoğlu(2011) çalışmasında: "Bilgi kullanılmakla tükenmez fakat hammadde kullanıldıkça tükenir." diyerek bilgiye farklı bir bakış açısı getirmiştir. Bilgi kullanıldıkça çoğalan çoğaldıkça da sermaye haline gelebilen bir değerdir. Bilgi sermayesi çok olan zengindir. Bilgi ekonomisi, bilgi ve bilgiye dayalı faaliyetlerin ekonomik büyüme ve rekabet gücü üzerinde belirleyici bir rol oynadığı bir ekonomik sistemdir. Bilgi ekonomisinin temel özellikleri denilince akla bilgiye dayalı üretim ve inovasyon, rekabet yapısı, bilginin değerinin artması, insan kaynağının önemli hale gelmesi, dijitalleşme ve teknolojik ilerleme gelmektedir. Teknolojik ilerlemeye kadar bilgiye giden yolda oluşan verilerin işlenmesiyle de bilgi oluşumu ve yayılımı söz konusudur. Artan bilgi üretimi ile birlikte de bilginin organizasyonu gerekli hale gelmiştir. "20. yüzyılın sonlarına doğru bu bilgi değişim ve gelişim evresi daha yaygın hale gelmiştir. Bu bilgi değişim ve gelişim evresi bilginin yönetimini daha aktif hale getirebilmek için teknoloji kullanımını yaygın hale getirmiştir. İnsan yaşamı boyunca bilgi 21.yüzyıla kadar değerli ve önemli olmamıştır. 21.yüzyılda bilgi stratejik bir duruma gelmiştir" (Barutçugil , 2002). Bilgi tüm dünya için önemli olup bilgi yarışları başlamış ve bilgiye sahip olan toplumlar da bilginin güç olduğu bilincine varmıştır. Rekabet ortamları oluşturan bilginin yönetimde ve ekonomide de yeri çok önemlidir. Bilgi : "Ekonomik, siyasi, sosyal ve kültürel alanlarda bazı ortak değerlerin yerel ve ulusal sınırları aşarak dünya çapında yayılmasını ifade etmektedir" (Bedük, 2008). Yayılım gösteren bilginin etkileşim ve değişim sonucu bir toplum bilinci oluşmaktadır. Bu toplum bilgi çerçevesinde gelişime ve gelişen dünya düzeninde bilgi çağı diye adlandırılmaktadır. Bir sonraki bölümde bu kavram bilgi odağında ele alınmaktadır.

1.1. Bilgi Çağı-Bilgi Toplumu

Bilgiye ve bilgi teknolojilerine sahip olmak oldukça önemlidir. "Bilgi toplumu, 1950 ve 1960'lı yıllarda Amerika, Japonya, Batı Avrupa ülkeleri gibi gelişmiş ülkelerde bilgi

teknolojilerinin giderek artan bir şekilde kullanımıyla meydana gelmiş bir aşamadır (Koçak & Memiş, 2018; Selvi, 2012). Bilgi toplumu, bilginin oluşturulması, dağıtılması, yayılması, kullanılmasının uygun olduğu ekonomik, politik ve kültürel etkinliğin içinde bulunduğu bir toplumdur (Sebetci, 2018). Bilgi toplumu, toplumların gelişmişlik seviyelerinin teknoloji kullanımı ile paralellik göstermesi ile alakalıdır. Bilgi toplumu, toplumun dinamik değerlerinden biri olarak bilgi ve bilgiye dayalı faaliyetlerin ön planda olduğu bir yapıyı ifade eder. 19.yüzyılda sanayi toplumu olarak bilinen ve sonrasında gelişerek 20. Yüzyılda yerini bilgi toplumuna bırakmıştır. Bilgisayarlarla insanların hayatına giren teknoloji mekanik anlayıştan insan beynindeki ağa geçilmesini sağlayan bir düzen sunmuştur. Her dönemden sonra bilgi toplumunda değişim şart olmuş ve bilgi toplumunun gelişimi üzerinde çalışmalar yapılmıştır. Bu süreçlerde de bazı kavramlar ortaya çıkmıştır. Örneğin; bilgi çağı, enformasyon çağı, küresel çağ, sanayi ötesi gibi… Bu teknolojik ve bilgi gelişimlerine sahip olan Endüstri 4.0, nesnelerin iletişimini, akıllı sistemleri, verilerin etkileşimini ele almaktadır. Bu durumların sonucu olarak en genel tanım ve kavram olarak da bilgi çağı kullanılmaktadır. Bilginin etkisi ile bilginin yaşadığı ve bilgiyi hayatlarında temel faktör gören toplum bilgi toplumudur.

Bilgi toplumunun özellikleri:

- Bilgi odaklıdır.
- Bilgiye erişim ve eşitliğe önem verir.
- Sosyal ve kültürel değişime oldukça açıktır.
- Sürdürülebilirliğe önem verir.
- Eğitim ve öğrenme kültüründe yenilikçiliği benimser.
- Teknolojik gelişimleri önemser ve değişime ayak uydurur.

Bilgi toplumunda, teknoloji ve bilgi merkezli bir yaşam benimsenmektedir. Modern toplum algısına daha yakın ve yatkındır. Bilgi toplumu insanının genel özellikleri ise; öğrenmeye açık, teknolojiyi kullanmaya daha yatkın, yenilikçi ve inovatif, iletişim becerileri diğer kuşaklara göre daha kuvvetli, sosyal sorumluluk sahibi, esnek ve uyumludur. Her bireyin bu gibi özellikleri taşımasının yanında farklı derecelerde olduğu gerçeği de unutulmamalıdır. Ayrıca bilgi toplumu insanının internet kullanımı çok yaygındır. 2023 TÜİK(2024) verilerine göre internete erişim imkânı olan hane oranı %95,5 iken, internet

kullanan bireylerin oranı da %87,1'dir İnternete bağlı olarak da dijital araçları kullanmaları, temel bilgisayar becerileri oldukça gelişmiştir. Veri analiz güçleri ve programlama becerileri daha belirgin olarak ortaya çıkmaktadır. Mobil teknoloji kullanımları, doğdukları yıldan itibaren internet ve teknoloji kuşağı olmalarından daha etkindir. Bu beceriler de bilgiye erişimlerini kolaylaştırırken gelişimlerini de artırmaktadır. Bilginin yüzyıllar içerisindeki bu köklü değişimi teknolojideki ilerleme ile paraleldir. Sebetci'nin (2018) bahsettiği bilgi teknolojileri alt yapısının kronolojik sırası şöyledir:

1) Elektronik Hesaplama Makineleri Devri

2) Genel Amaçlı Merkezi Sistemler ve Mini Bilgisayar Devri

3) Kişisel Bilgisayar Devri

4) İstemci-Sunucu Devri

5) Bulut Bilişim ve Mobil Bilgi İşlem Dönemi

Bilgi teknolojilerinde donanımlar işlemciler, sunucular ele alınırken bunların yanında yazılımlar ve yazılım altyapıları sürekli gelişme olmazsa olmazlardandır. "Günümüzdeki işletmelerin üretim faaliyetlerinde kullandıkları otomasyon sistemlerinde meydana gelen artışlar, denetim 4.0 olarak adlandırılmıştır. Bu sistem nesnelerin interneti, akıllı sistemler sayesinde sürekli gelişme olmaktadır" (Yel & Atasoy, 2021). Yazılım alt tabanlı donanımlar ve kullanımları kontrollü olmak durumundadır. Bilgi çağında en yaygın kullanılan iletişim aracı bilgisayardır ve buna bağlı olarak da bilgisayar teknolojileri alanındaki gelişim ve değişimler de artmaktadır. Sanayi toplumundan ayıran en belirgin özelliklerden olan maddesellikten bilişimciliğe yöneltmektir. Sanayi toplumunda meta kavramı daha çok somut ürünleri işaret ederken bilgi çağında ise meta kavramını bilgi, enformasyon, veri kavramları karşılamaktadır. Sanayi toplumu ile karşılaştırmalarda:

- Kol gücünün yerini beyin gücü aldı.
- Maddiyatın yerini bilgi toplumunda bilgi ve insan aldı.
- Fiziksel sermayenin yerini düşünsel zekâda nitelikli insanlar aldı.
- Fabrikaların yerini daha çok bilgi ağları ve veri bankaları aldı.
- Sanayi toplumundaki buharlı makinaların yerini bilgisayarlar aldı.
- Sanayi toplumundaki tekdüze ve genel eğitimin yerini daha inovatif eğitim

sistemiyle sürekliliği sağlayan bir eğitim düzeni aldı (Selvi, 2012).

Yukarıdaki kıyaslamalara bakılarak sanayi toplumundan bilgi toplumuna geçişlerde hep ilerleyiş ve yenilikler gözlemlenmektedir. Bilgi çağının ve bilgi insanının gelişimi o devri de gelişime sürüklemektedir. Bilgi toplumunun artan teknoloji ve bilgi ile evrilmesi de bilgi ötesi toplumu ortaya çıkarmaktadır. Bilgi çağından sonraki evre de bilgi ötesidir. Yapay zekâların, yazılımların, robotların, simülasyonların ve dijitalleşmelerin daha yaygınlaştığı bir dönemdir. Değişimin olduğu her evrede bir düzen bir kural gerekliliği söz konusudur. Bilginin değişmesi sonucu bilgi yönetimlerindeki değişimlerin de revize edilmesi gerekmektedir.

1.2. Bilgi Yönetimi

"Bilgi yönetimi ifadesi 1980'lerin sonunda popüler olarak kullanılmaya başlandı" (Yazıcıoğlu vd.,2011). Bilgi yönetiminin alt yapısını oluşturan bazı unsurlar vardır. Bu unsurlar; teknoloji, kurum kültürü, organizasyon yapısı ve sermayedir. Bu unsurlar göz önünde tutularak bilgi ve yönetim kavramları ele alındığında ortak noktada buluşması zor iki kavram gibi görünmektedir. Fakat bilgi keşfedilen, bilinen, bulunan ve kullanılan, kodlanan bir yapıdadır. Bu değişkenliğe uğrarken de bir kurala bir sisteme göre olması daha sistematik hale getirir. Yönetim ise ortak amaçlar için toplanmış bir süreci ifade eder. Bu sebeple bilgi yönetimi; artan bilgi kapasitesini güncelleyip kontrol altına alan, oluşan bilgileri erişime sunan, istenen bilgiye erişim için gereken aşamaları yapan ve gereken bilginin toplumun tüm çalışanlarıyla paylaşılmasını sağlayan bir disiplindir (Güçlü & Sotirofski, 2006). Bilgi yönetimi, üretken bilginin elde edilmesi, paylaşılması, geliştirilmesi ve kullanılması ile ilgilidir.

Bilginin nasıl tanımlanması gerekliliği ve tanımlandığı yönü, bilgi yönetiminde önemli rol almaktadır. Bilginin sosyal ya da teknik yapısıyla değişimi sonucunda bilgi yönetim tekniklerinde farklılıklar oluşur. Böylelikle bilgi yönetiminde teknoloji kullanımı daha etkin hale gelmektedir. Günümüz teknolojisinde de veri kullanımı ve işleyişi buna bağlı olarak da bilgi akışı çoktur. Bilgiden bilgeliğe giden bu süreç büyük veri ve yapay zekâ kavramlarını da ortaya çıkarır. Büyük verilerin işlenmesi kontrol altında tutulması ve

yönetilmesi gerekliliktir. Bilgi yönetimi ile örtük bilgiler açık bilgilere dönüştürülür. Bilginin üretiminden kullanılmasına kadar olan süreçleri yani; bilginin oluşumu, elde edilmesi, bilginin saklanması, organize edilmesi, yaygınlaştırılması, bilginin kullanılması, uygulanması gibi süreçleri kapsayan yönetim bilgi yönetimidir. "Bilgi yönetimi, bilgiyi kontrol edilebilir bir değer olarak ele alan bir yönetim aracıdır" (Akyön, 2001).

Bilginin üretilmesi, çoğaltılması, yaygın hale getirilmesi, sınıflanması ve organize edilmesi süreci bilgi yönetimidir. Bilginin güç olduğu çağda bilgi yönetimi sistemlerini de en etkili kullananlar için güç olmaya devam etmektedir. "Bilgi yönetimi süreci, örgütsel amaçlar doğrultusunda kuruluşun genelini koordine eden sistematik ve entegre bir süreçtir" (Ustaoğlu & Akyol, 2021). Yukarıda bahsedilen unsurlardan olan kurum kültüründe; kurum ve kuruluşların bilgilerini belli bir düzende tutması ve yönetmesi sürecini ele almak gerekir. Bu süreç incelenirken kurumda çalışan tüm personelin tutumu ve bilgiye olan bakış açıları önemlidir. Organizasyonel bilgiyi yönetebilmek için kurumun sahip olduğu bilgi birikimini harekete geçirmek o kurum adına olumlu bir imaj oluşturur. Bilgi yönetimi: Bilgi odaklı, bilgi dostu ve kurum kültürünün oluşmasını sağlamaktadır.

Artan bilgi düzeninde bilgiye kolay erişim ve sistematik kullanım için kurallar gereklidir. Kurumlarda bilgi yönetimini nitelikli olarak kullananlar daha kârlı daha başarılı ve daha etkin olmuşlardır. Rekabetçi olan bugünkü düzende başarı ve başarısızlık arasındaki fark, kurumlar arasındaki bilgi yönetim becerileriyle ilişkilidir. Bilgi yönetimini en aktif ve verimli kullanan işletmelerde başarı da paralel olarak ilerlemektedir (Demirtaş, 2013). Buna bağlı olarak bilgi yönetiminin gerekliliğine sebep olan etmenler; küreselleşme, internet, inovasyon bilinci, teknolojik gelişmeler, e-ortamlar ve bilgi toplumudur.

Küreselleşme, bilgi yönetiminde önemli bir yere sahiptir. Kültürlerarası etkileşimde bilgi ve tecrübelerin paylaşılması sonucunda farklı bakış açıları ile birlikte çözümler üretilir. Çözümlerde de bu değişim bilgi yönetim süreçlerindeki inovasyona sebep olur. Avantajının yanında küreselleşmenin dezavantajları da vardır. Bilgi yönetim sürecinde dil ve kültür farkından dolayı sorun olabilir. Fakat küreselleşmenin etki sürecinde fırsata çevirmek

önemlidir.

İnternetin yaygınlaşması ve kullanımı ile kişilerarası iletişimde ve kurumlar arası iletişimde basılı kaynakların yanında ekstra kullanılan elektronik ortamlardan da bilgi akışı söz konusudur. Bu artan bilgi akışının yönetiminde de internetin yeri yadsınamaz. Bilgi erişimi ve toplama işlerinde internet etkin kullanılır ve süreci hızlandırır. Bilgi paylaşımını ve işbirlikleri internet kolaylaştır. Kültürel etkileşimi ve kültürel çeşitliliği buna bağlı olarak da bilgi hizmetlerinin farklılaşmasını sağlar. Olumlu birçok özelliği vardır fakat internetin bilgiye erişimde ve bilginin korunmasında bazı sorunlar ortaya çıkabilir. Kaliteli ve verimli bir bilgiye erişmek için bilginin uygun elektronik platformlarda taranması gerekir. Doğru bilgiyi doğru kanalda aramak bilgi yönetiminin gerekliliklerindendir. Buna ek olarak da bilgi yönetiminde sahip olunan bilgilerin korunmasında da dikkat edilecek birçok unsur vardır. Hassas bilgilerde ve yetersiz erişimli bilgilerde önlemler alınmalıdır. Kaliteli bilgi olup olmadığı tespit edilmeli, uygun paylaşımın yapılacağı platform seçilmeli ve teknolojik altyapısı sağlanmalıdır. Bu teknolojik altyapı sürecinde erişilebilirlik, ağ güvenliği, kimlik doğrulama gibi yöntemler olmalıdır. Bu teknik yöntemlerin uygulanma sürecinde ise kullanıcı potansiyeli sürekli gelişen ve değişen bir toplum haline gelmektedir. Dolayısıyla da inovasyon bilinci gelişmektedir. Değişime ayak uyduran ve yenilikleri yapmaya çalışan bireyler ise bilgi toplumu olmaya devam etmektedirler. Bilgi toplumunun en büyük gerekliliği ise doğru bilgi ve bu bilgiyi kullanan bilinçli bireylerdir.

Bilgi yönetimi kavramının temel unsurları vardır. Bunlar; "bilgi toplama, bilgi işleme, bilgi depolama, bilgi erişimi, bilgi koruma, bilgi kullanımıdır" (Güçlü & Sotirofski, 2006). Bilgi toplama; bir organizasyonun işleyişinden, araştırma süreçlerinden, kullanıcı geribildirimlerinden, çalışan anketlerinden, iş süreçlerini yönetirken oluşan veri düzeninden elde edilen bilgilerin derlenmesi anlamına gelmektedir. Bilgi depolama; organizasyonlarda toplanan verilerin veri tabanlarında, bulut sistemlerinde tutulması ve sonrasında tutulan bilginin güvenliği ve erişimini kolaylaştırmak için yapılan süreçlerdir. Bilgi işleme; toplanan verilerin organizasyonun amaçları doğrultusunda işlenmesi, anlamlı hale getirilmesi işlemidir. Bu süreçte yeniçağın konularından veri madenciliği çok önemli olmakla birlikte verilerin analizi yapılır ve analitik düşünce ile birleştirilir. Bilgi paylaşımı; bilginin

kullanıcıları arasındaki iletişimi ve süreçte akışı sağlayan bilgi yoludur. Bilgi paylaşımını yaparken doğru kanalı kullanmak önemlidir. Bilgi koruma; organizasyonlardaki kullanılan, üretilen her türlü bilginin hassasiyetlerine uygun şekilde saklanması ve bunun belirlenmiş protokol gereğince yapılmasıdır. Erişimlerin kontrolleri, şifrelerin belirlenmesi, güncellenmesi ve önlemeleri bilgi korumanın işlemleri arasındadır. Bilgi güvenliğinde gizlilik, bütünlük, gerçekçilik, erişilebilirlik esas alınmalıdır. Bilgi kullanımı; stratejik karar alma süreçlerinde, organizasyonel çalışmaların her anında bilgi kullanımı gerçekleşmektedir. Bilgi kullanımı ve bilgi yönetiminde organizasyonların bilgilerin yönetim ve stratejilerini en iyi şekilde kullanımını teşvik ederken bazı durumlarda da rekabet kavramını ortaya koymaktadır. Bu rekabet ortamı özel sektörde daha ekonomik altyapı çerçevesinde yaygın iken devlet kurumlarında daha çok nitelik ve nicelik özelinde değişim yapılmıştır. Bilgi yönetimindeki amaç bir süreçte gerekenleri yerine getirmek, gerekeni yakalamak ve bilgi için çalışan bilgi uzmanlarının bilgi paylaşımlarına destek olmaktır. Tüm bu süreçlerin gerçekleşmesi için de bilgi yönetiminde bazı ilkeler vardır. Güçlü ve Sotirofski (2006) çalışmasında bilgi ilkelerinden aşağıdaki şekilde bahsetmişlerdir.

- Bilgi yönetimi maliyetlidir.
- Bilgi yönetimi süreklilik ister.
- Bilgi yönetiminde insan, bilgi ve teknoloji harmanlanmıştır.
- Bilgi yönetimi, sürecin kolaylaştırılması anlamına gelir.
- Bilgi yönetimi, bir örgütün amaçları doğrultusunda bilgi vizyonu oluşturmaktır.

Bilgi toplumunun gerekliliklerinden yola çıkarak da bilgi yönetiminde farklılıklar olmuştur. Eğitim programlarında, örgütlerin yönetim şekillerinde, bireylerin hayata devam edebilmesi için ihtiyaçları olan bilginin bir yönetim şeklinin olması gerekliliği ortaya çıkmıştır. Bilgi yönetim sürecini bilgi teknolojileri de geliştirir ve daha erişilebilir hale getirir. Sürekli ve erişilebilir olması ilkeleri arasında da vardır. Sürekli öğrenme gibi kavramlar da bu vesile ile hayatımıza girmiştir. Bunun bilimsel adı ise yaşam boyu öğrenmedir. Yaşam boyu öğrenme denilince, sürekli eğitim, kapsamlı gelişim ve düzenleme-planlama akla gelir. Bilgi yönetiminde de bilgiyi toplama, saklama, paylaşma, kullanma gibi kavramlar gelirken ikisi arasında sıkı bir bağ vardır. Sürekli öğrenme için bilgilerin güncelliği önemlidir. Bir bilgi organizasyonunun bilgi yönetim sistemi en güncel

olmalıdır. Yaşam boyu öğrenme bireylerin gelişimini önemserken, bilgi yönetim süreci de bu gelişime katkı sağlayan altyapı çalışmalarının verimliliğini önemsemektedir. Bilgi organizasyonlarında kurumsal eğitim programları düzenlenerek, çevrimiçi öğrenme artırılarak, bilgi paylaşımı için alternatif ağlar üreterek de yaşam boyu öğrenme sürecinde bilgi yönetimi daha aktif kullanılır hale gelmiştir. Bunların etkin kullanımı da bireyleri yenilikçi olmaya ve sürekli gelişime iteklemektedir.

1.2.1. Bilgi Yönetim Süreci

Bilgi yönetim sürecinde etkin olunabilmesi için bazı temel adımlar vardır. Bunlar; stratejik bir planlama yapılması, politika ve prensiplerin belirlenmesi, teknolojik araçların kullanılması, verilerin yönetimi, erişim ve paylaşılması, geribildirimler ve geliştirmeler, iyileştirmelerdir (Arslan, 2023). Bu adımlarla birlikte bilgi yönetim süreci daha sistematik bir şekilde ilerlemektedir. Değişen ve gelişen bilgi durumunda bilgi yönetim şekillerinde de değişiklikler gözlemlenmiştir. Eğitim ve araştırma alanlarında, bilgi teknoloji alanlarında kamu kurum ve kuruluşlarında bazı çalışmalar yapılmıştır. Darıcılı'nın (2019) çalışmasında incelediği maddeler ile birlikte kütüphanelerde, bilgi merkezlerinde bilgi yönetiminin ve siber güvenliğin gerekliliğinin üzerinde durulmuştur. Elektronik ortama yansıması ve diğer bilgi yönetim süreçlerinden bazıları ise aşağıda sıralanmıştır.

1) Kütüphanelere yaygın erişim, bilgi kaynaklarının kullanıcı kitlesine kolayca ulaşılabilmesidir. Yaygın erişimi sağlayan unsurları vardır. Dijital kütüphaneler, E-Kaynaklar, kütüphane ağları, uzun çalışma saatleri(7-24), hareketli kütüphaneler (gezici araç kütüphaneleri), teknolojik altyapılar, engellilere yönelik hizmetler, toplum merkezleri, işbirlikleri gibi hizmetlerle yaygın erişimi destekleyerek kütüphaneleri daha erişilebilir hale getirmek bilgi yönetim sürecini de kolaylaştırmaktadır.

2) Elektronik Ticaret, bilgi yönetiminde işletmelerin etkili ve nitelikli olarak çalışmasında kritik rol oynamaktadır. Elektronik ticaretin yönetiminde veri toplama, depolama, işleme, analiz etme ve kullanma aşamaları önemlidir. Pazarlama verileri toplanarak veri yönetimi gerçekleştirmek için raporlamalar

kullanılmaktadır.

3) Uluslararası E-Üniversiteler, çevrimiçi eğitim sunan üniversitelerdir. Dünya genelinde sunulan bu hizmetten faydalanmak isteyen kitle için çeşitli programlar, eğitimler, fırsatlar sunularak bilgi paylaşım ve yönetim süreci daha aktif kullanılmaktadır. E-Üniversitelere örnek olarak; University of Phoenix (ABD), Open University (Birleşik Krallık), University of Maryland Global Campus (UMGC) (ABD) verilebilir.

4) Elektronik Arşivler, bilgi ve belgelerin dijital hale getirilmesi ve yönetilmesini sağlayan sistemlerdir. Fiziksel arşivlerin yerini yenidünya düzeninde dijital arşivler almıştır. Elektronik arşiv yönetimi süreci; belge tarama, dijitalleştirme, depolama, yedekleme, erişim, güvenlik, arşivleme, indeksleme, imhadır. Elektronik arşiv sitemleri ve teknolojileri DMS, Open Text ve bulut tabanlı çözücülerdir.

5) E-Devlet uygulaması, devletin hizmetlerinin dijital formatta sunulması ve yönetilmesidir. Bu uygulama ile birlikte vatandaşlar devlette olan işleri için daha hızlı daha kolay yapmaktadır. E-devletin amaçları, kolay erişim, verimli ve hızlı olmak, maliyet tasarrufu sağlamak, daha şeffaf daha eşitlikçi bir hizmet sunmaktır.

6) 5070 Sayılı Elektronik İmza Kanunu, Türkiye'deki elektronik imza alt yapısını düzenleyen kanundur. Elektronik imzalar elle atılan imzalar gibi hukuki geçerliliğe sahiptir.

7) Elektronik Belge Yönetim Sistemi (EBYS), kuruluşların belgelerini dijital ortamda oluşturması, yönetmesi, paylaşması, saklanmasını sağlayan bir yazılım sistemidir. Belgelerin oluşum sürecinin yönetilmesidir. EBYS'nin avantajları; zamandan tasarruf sağlar, maliyet tasarrufu sağlar, güvenli bir koruma gerçekleşir.

8) 5809 Elektronik Haberleşme Kanunu, elektronik haberleşme sektörünün tüm kuralları ve yasal düzeni oluşturan kanundur. Elektronik haberleşme sürecinin nasıl olması gerekliliği ile alakalı düzenlemeleri içermektedir.

Bu ve benzeri çalışmaların yapılması kurumları veri sahibi yapar ve kurum kültüründe bilgi odaklı çalışmaları ön planda tutar. Kurum ve kuruluşlarda istenilen bilgiye erişimleri ve paylaşımları daha kontrollü ve güvenli hale gelmesi için yapılan bu uygulamalar özellikle kamuda veri toplama, saklama, ayıklama, imha süreçlerini daha kolay hale getirmektedir. 2010 yılından bu güne kurumlarda elektronik bilgi yönetim sistemlerine geçişi önemseyen ve geliştiren birtakım çalışmalar yapılmaktadır. Bilgi teknolojilerinin gelişimin de etkisiyle 21.yüzyılda elektronik ortamlar daha yaygın kullanılmaktadır. Her kurumun bir bilgi akışı olması sebebiyle kurum bilgi arşivi de oluşmaktadır. Tüm bunların bir havuzda güvenli bir şekilde tutulması da bulut bilişimleri ve elektronik arşiv kavramlarını ortaya çıkarmıştır.

Bulut bilişim, internet kaynaklı olan her türlü bilgiye erişim sağlama hizmetidir. Öncesine nazaran bulut bilişim hizmetleri esnektir ve maliyet olarak daha etkin kullanım sunmaktadır. “Bulut bilişimin özelliklerine değinilirse; kolay erişim ve kullanımlıdır. İnternetin bağlı olduğu çeşitli cihazlardan erişilebilirdir. Çoklu kullanıma uygundur. Hızlı bir şekilde aktarım yapılabilir ve isteğe bağlı olarak artırıp azaltılabilir” (Çelik, 2021). Ayrıca bulut bilişimler zaman ve mekân kısıtlaması olmaksızın erişime uygun haldedir. “Bulut bilişim, kuruluşlara veri depolama ve işleme kapasitesini ihtiyaçlarına göre artırma veya azaltma esnekliği sunar. Bu, özellikle mevsimsel taleplerin yoğun olduğu veya ani artışların yaşandığı dönemlerde faydalıdır. Veri hacmindeki artışa kolayca uyum sağlayabilir ve işletmelerin hızla değişen ihtiyaçlarına yanıt verir” (Atan, 2020). Kurumların ayırmış olduğu maliyetlerde fiziksel sunucular ve veri merkezlerine yapılan büyük yatırımları ortadan kaldırarak başlangıç maliyetlerini düşürmektedir. Ayrıca aynı konu üzerinden çalışan personel bulut tabanlı uygulamalar ve platformlar aracılığıyla aynı belgeler üzerinde gerçek zamanlı olarak çalışmaktadır. Bu durumda da süreçlerin otomasyonunu ve entegrasyonunu kolaylaştırarak verimliliği artırmaktadır. İnternet bağlantısı olan her yerden bilgiye erişim imkânı sunmaktadır. Bu, uzaktan çalışma ve işbirliğini kolaylaştırarak mobil

erişim ve yönetim imkânı da sunmaktadır. Bulut bilişim güvenli ve gelişmiş protokoller kullanarak verilerin korunmasını sağlamaktadır. Verilerin yaygın kullanımından dolayı avantajlarının yanında güvenlik, gizlilik, internet kalitesi, yasal düzenlemelerin yetersizliği gibi dezavantajları da mevcuttur.

Bulut hizmet sağlayıcılarının sistemlerinde yaşanabilecek güvenlik açıkları nedeniyle, kullanıcı verileri çalınabilir veya yetkisiz kişilerin eline geçebilir durumdadır. Bu durumda da veri ihlalleri oluşmaktadır. Zaman zaman hizmet kesintileri de olmaktadır; bu da elektronik bilgi yönetim süreçlerini aksatmaktadır. Bazı zamanlarda da büyük miktarda veri buluta yüklenirken veya buluttan indirilirken zaman ve maliyet sorunları yaşanmaktadır. Bu zararlar, uygun güvenlik önlemleri, düzenlemelere uyum ve dikkatli planlama ile minimize edilebilir haldedir. Bulut bilişimin sağladığı esneklik ve maliyet avantajları, bu risklerle dengelendiğinde, birçok işletme için cazip bir seçenek olmaya devam etmektedir. Birçok kurum çalışma düzenini EBYS'ye çevirirken arşiv düzenleri de E-Arşiv sistemine geçirilerek daha kolay ve erişilebilir hale getirilmiştir.

Elektronik arşiv düzenine Türkiye'de önemli bir adım olan e-devlet uygulamasıyla birlikte adım atılmıştır. "E-devlet; devletin vatandaşlarına karşı yerine getirmekle yükümlü olduğu görev ve hizmetler ile vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesidir" (Yılmaz vd.,2015). E-devlet uygulamasındaki amaç devlet hizmetlerinin vatandaşa en hızlı en uygun şekilde kesintisiz erişim sunulmasıdır. Bilgi yönetim sürecinin daha sistematik hale getirilmesinin uygulama halidir. Klasik devlet anlayışından sıyrılıp daha gelişmiş bir devlet anlayışı ile e-devlet süreci; bütünleşmiş bir ağ çözümü sunar. İşleri daha hızlı ve kolay hale getirir. Açık, şeffaf ve sorgulanabilir bir devlet anlayışıyla elektronik hizmet alınan bir uygulamadır. Web düzeninden sonra mobil uygulamada da yer alması tamamen yenilikçi hizmet anlayışıyla yapılan uygulamalardandır. E-devlet uygulamalarının en önemli kriterlerinden biri kişisel verilerin doğruluğu, yapılan işlemlerin güvenli ve devlet kontrolünde gerçekleşiyor olmasıdır. Bilgi paylaşımlarında koruma, yeterlilik ve güvenlik ilkeleri öncelikli haldedir. Bu prensipler doğrultusunda bilgi yönetim süreci başlar ve hizmetler sunulur.

E-devlet hizmeti sonrasında 2004 E-İmza Kanunu kabul edilmiştir. Kamu kurumlarında kullanılması zorunlu hale getirilen Elektronik Belge Yönetim Sistemi (EBYS) 2011 yılında hayata geçirilmiştir. Bu sistemle birlikte kamu kurumlarında elektronik ortamlar oluşmuş ve bilgilerin üretimi, paylaşımı, saklanması, arşivlenmesi sağlanmıştır. Belgelerin dijital ortamda üretilip paylaşılması ile birlikte artık elektronik ortamlarda bilgi akışı daha da arttı. Bu düzen kamu kurumlarında EBYS yardımıyla olurken özel sektörde ise e-fatura, e-defter, e-arşiv uygulamaları ile yaygınlaşmıştır. Bu bakış açısıyla Türkiye'de elektronik arşiv uygulamasına geçiş 2000 yıllarında başlamış ve günümüze kadar gelmiştir. Günümüzde e-Arşiv uygulamasına ek olarak da e-İmza uygulaması hayata geçirilmiştir.

Tablo 1

E-Arşiv kolaylık ve zorlukları

E-Arşivlerin Sağladığı Kolaylıklar	E-Arşiv ile Karşılaşılabilecek sorunlar
Zaman ve işgücünden tasarruf sağlanır.	İmha edilmesi daha kolaydır.
Çoklu erişim imkânı sunar.	Dijitalleştirme yapılırken hatalar yapılabilir.
E-arşivlenmiş belgelin kaybolma riski azalır.	Siber saldırılara, risklere daha açıktır.
Belge kullanımı artar.	Veri kaybı yaşanabilir.
Verimlilik artar, maliyet azalır.	Kalıcı silmelerde kurtarılamayan belgeler olabilir.
Belgelerin yıpranmasının önüne geçilir.	Dosya paylaşımlarında sorunlar olabilir.
Fiziksel kullanımı azaltmasıyla fotokopi, kâğıt maliyeti düşer.	Dosyalar işlenirken kaydetme, silme, değişiklik sorunları olabilir.
Zaman ve işgücünden tasarruf sağlanır.	İmha edilmesi daha kolaydır.

Değişimlerle birlikte verilecek hizmetlerin de süreçleri değişikliklere uğramıştır. Tablo 1'de e-arşivin sağladığı kolaylıklara değinilmiştir. Avantajları ve dezavantajları ele alınırsa e-ortamdaki yapılabilecek işler iş gücü tasarrufu sağladığı görülmektedir. Elektronik ortamlardaki bilgilerin yönetiminde zaman ve mekân kavramı ortadan kalkmıştır. Belge yönetiminde de zaman ve fiziki kolaylık sağladığı aşikârdır. Elektronik ortamlardaki bilgilerin basılısına göre yıpranma riski yoktur. Kaydetme ve silme gibi sorunlarla birlikte bellek sorunları yaşanabilmektedir. Buna ek olarak da geri dönüşü olmayan silme işlemlerinden sonra geri alma işleminin olmaması da sorun teşkil edebilir.

1.2.2. Bilgi Yönetim Sürecinde Dikkat Edilmesi Gerekenler

Bilgi yönetim sürecinde dikkat edilmesi gerekenler bilginin toplanmasından erişilmesine kadar olan sürecin etkin kullanımıdır. Bilgi yönetim süreci, bilgiyi toplamak, düzenlemek, depolamak, paylaşmak ve kullanım için prosedürler ve stratejiler geliştirmektir. Bu sürecin başarılı olması için kurumların prosedürlerini düzenlemeleri ve politika haline getirmeleri gerekmektedir. Kurum ya da kuruluşların bilgi akışının sürekliliğine karşın alacağı önlemlerden olan bilgi yönetimi dikkatle uzmanlar tarafından yönetilmelidir. Bilgi yönetim sürecinde dikkat edilmesi gereken unsurlar arasında da: bilgi ihtiyacının belirlenmesi, bilgi toplama/derleme ve değerlendirme, bilginin sınıflandırılması ve düzenlenmesi, bilginin depolanması, bilginin kullanımı ve paylaşılması, bilgi yönetimi için farkındalık ve eğitim vardır (Yazıcıoğlu vd., 2011). Bir kurumun bilgi ihtiyacının belirlenmesi doğru kitle belirlemek ve kitleye uygun verilerin derlenmesini sağlamakla olur. Bu ihtiyaçların tanımlanmasıyla birlikte bireylerin doğru bilgiye erişimleri sağlanmış olur. Gerekli bilgilerin daha sistemli toplanması için gerekli bazı veri tabanları kullanılmaktadır. Gelen anketler, analizler de buna örnek verilebilir. Toplanan bilgilerin doğruluğu ve güvenilirliği kontrol edildikten sonra sınıflama ve düzenleme işlemleri yapılmaktadır. Bu aşamada bilgi yönetim sistemleri devreye girmektedir. Bilgi yönetim sistemlerine örnek verilirse; Evernote Business, M-Files, Box, Open Text, Microsoft SharePoint, IBM FileNet, Alfresco gibi sistemler kullanılmaktadır (BTK Akademi, 2024). Bulut tabanlı olan, açık kaynak kodlu olan bu ve benzeri platformlar yenilenen bilgi akışlarını güncel tutmakta fayda sağlamaktadır. Kurumlara göre seçilebilen ve kurum kültürüne ve kitlesine uygun olabilecek bilgi yönetim istemleri seçilmektedir. Bilginin kayıt altına alınması, depolanması ve sonradan kullanıma açık hale gelmesi değişen teknolojilerle birlikte de yeniliğe uğramaktadır. Bu yeniliği yakalamak için kurum çalışanlarının da bilgilerini ve uygulama becerilerini güncel tutmaları şart olmuştur. Bilgi yönetim becerilerinin gelişmesi için; eğitim ve farkındalık çalışmaları yapılmalıdır. Bilgi yönetim sistemlerinin zaman zaman tanıtımları gerçekleşmelidir. Kılavuz ve dokümanlar hazırlanıp çalışanlarla paylaşılmalıdır. Motivasyonlarının artması ve bilgi yönetimine dair becerilerini geliştirmek için teşvik ve ödüllendirme programları düzenlenmelidir. Bilgilendirme amaçlı kurum sosyal medyaları aktif kullanılmalı ve geribildirimler için anketler yapılıp değerlendirmeye alınmalıdır. Bu ve benzeri çalışmalar bilgi yönetimi farkındalığını artırarak kurumlardaki verimliliğe de katkı sağlamaktadır. Tüm bunların yanında bilginin erişiminde sınır olmalıdır. Bilginin güvenliği

sağlanmalı; veri şifreleme, güvenlik kontrolleri ve protokolleri olmalıdır. Her kurumun işleyişine göre güvenlik önlemlerinde de değişiklikler gözlemlenmektedir. Güvenlik önlemlerini sıralayacak olursak; fiziki güvenlik, ağ güvenliği, bilgi güvenliği, siber güvenlik olarak değerlendirilebilir. Fiziki güvenlikte erişim ve donanım güvenliği ele alınır. Güvenlik kameraları da buna örnektir. Ağ güvenliklerinde; güvenlik duvarları, VPN kullanımları ve IDS'ler (saldırı tespit ve önleme sistemleri) vardır. Bunlara ek olarak da bilginin güvenliğinde veri şifreleme, yedekleme ve kurtarma çalışmaları ve hassas bilgiler için veri maskeleme yapılmaktadır. Böylelikle güven ve kalite odaklı standartlaşma sağlanmaktadır.

1.2.3. Bilgi Yönetimi ile Bilgi Güvenliği Yönetim Sistemi Arasındaki İlişki

Bilgi yönetimi ve bilgi güvenliği birbirini destekleyen ve tamamlayan iki süreçtir. Bilgi yönetiminin eksiksiz ve nitelikli bir süreç olabilmesi için bilgi güvenliğinin sağlanması gerekliliktir. Bilgi güvenliğinin sağlanması için de etkin bir bilgi yönetimi sürecinin olması gereklidir. Bu iki döngü birbirinden ayrılmaz süreçlerdir. Bilgi yönetimi bilginin değerini ortaya koyar ve kullanılabilir hale getirirken bilgi güvenliği bu değeri korumak için çalışmalar gerçekleştirir. Bilgi yönetimi bilgiyi doğru zamanda doğru kitleye erişimi sağlamak için politikalar üretirken bilgi güvenliği, bu erişim politikalarının uygulanmasını ve kontrolünü sağlamaktadır. Bilgi yönetimi bir bilginin ne kadar tutulması ve ne kadar önemli olduğunu belirlerken bilgi güvenliği bilgi sınıflandırmalarına uygun güvenlik önlemleri alır (Davenport & Prusak, 1998). Örneğin; hasta kayıtlarının düzenli olarak yapıldığı sistemlere hastane personelinin ihtiyaç halinde istediği ortamda erişebilmesi bilgi yönetimi iken hasta bilgilerinin yetkili olmayan bireyler tarafından erişiminin olmaması ve önlem alınarak erişilmesine şifre koymak, kontrollerin yapılması gibi yollarla izin verilmemesi de bilgi güvenliğidir. Bilgi merkezlerindeki örnekleri de kullanıcıların kayıtlarının yapıldığı bilgilerinin alındığı durumlarda korunması gerekliliği, paylaşılmasında KVKK gereği davranmak gereklidir.

Bilgi yönetimi ile bilgi güvenliği yönetim sistemi arasındaki ilişki, iki sistemin nasıl birbirini tamamladığı ve desteklediği ile ilgilidir. BGYS, bilgi yönetim süreçlerinin güvenliğini sağlamak için risk yönetimi ve güvenlik önlemleri sağlar. Örneğin, bilgi paylaşım platformlarının güvenliğini sağlamak, veri şifreleme ve erişim kontrolü gibi

önlemler BGYS'nin sorumluluğundadır. Bu güvenlik önlemleri, bilgilerin yetkisiz erişim, veri kaybı veya bilgi sızıntısı gibi risklerden korunmasına yardımcı olur. Dolayısıyla, BGYS'nin sağladığı güvenlik politikaları ve uygulamaları, bilgi yönetim süreçlerinin etkinliğini artırmakla birlikte, bilgi güvenliğini de garanti altına alır (Balcılar, 2008).

Bilgi Yönetimi ve Bilgi Güvenliği Yönetim Sistemi arasındaki ilişki, organizasyonların bilgi yönetim süreçlerini güvenli bir şekilde yürütmeleri için birbirini tamamlayıcı bir yapı oluşturur. Bilgi Yönetimi, bilgi akışını ve paylaşımını optimize ederken, Bilgi Güvenliği Yönetim Sistemi, bu bilgilerin güvenliğini sağlar. Her iki sistemin birlikte çalışması bilgi yönetim süreçlerinin hem verimli hem de güvenli bir şekilde yürütülmesini mümkün kılar, bu da organizasyonel başarı için kritik bir bileşendir (Güçlü & Sotirofski, 2006).

Bilgi güvenliği yönetim sisteminin; etkin ve sürekliliğinin sağlanması için planlama, risk değerlendirme, bilgi politikası geliştirme ve belirleme, biçimlendirme ve eğitim düzenlenmelidir. Bilgi güvenliği yönetim sistemi sadece teknik manada önlemler almaz. Bunun yanında güvenliği sağlanan kurumun güvenlik kültürünü ve güvenlik bilincini de kapsar (Dhillon & Backhouse, 2002). Bilgi güvenliği yönetim sisteminde kurumların rekabet gücünü ve her geçen gün artan bilgi güvenliği risklerine karşılık alınabilecek tedbirleri ele almak mühimdir. Bu gelişim kurumların performansını doğrudan etkilemektedir (Akdoğan, 2022). Kurumlar bazında Bilgi Yönetimi ve Bilgi Güvenliği Yönetim Sistemi arasındaki ilişki, organizasyonel bilgi varlıklarının hem etkin hem de güvenli bir şekilde yönetilmesini mümkün kılar. Bilgi yönetimi, bilgilerin verimli bir şekilde kullanılmasını sağlar, BGYS ise bu bilgilerin güvenliğini temin eder. Her iki sistemin uyumlu bir şekilde çalışması, kurumların bilgi süreçlerinin etkinliğini artırırken, aynı zamanda bilgi güvenliği risklerini minimize eder ve düzenleyici gerekliliklere uyumu destekler.

2. BİLGİ GÜVENLİĞİ

Bilgi güvenliğinin basit tanımı; bilginin yetkisi olmayan kişiler tarafından erişilmesini önlemek ve yalnızca yetkili kişilerin erişimine açmaktır. Başka bir tanımda; bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla alınan önlemlerin tamamına denir (Yılmaz, 2014).

> "Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanmaktadır.(Demirtaş, 2013,ss.12-33)

Yenilenen teknoloji ile güvenlik kavramında da farklılıklar oluşmuştur. Buna etki eden ise günümüz bilgi teknolojilerinin oluşturduğu sanal ortamlarla küresel topluma dönüşümü için güvende olma hissidir.

Güvenlik kavramı Maslow pramidinde fizyolojik olarak incelense de günümüz gelişimlerinde sanal güvenlik ortamlarında oluşmaktadır (Güngör & Güney, 2017). İlk insandan bugüne can ve mal güvenliği ön planda olsa bile bilim ve teknoloji alanındaki hızlı değişim ile birlikte bilgilerin art niyetle kullanılabilir korkusu ortaya çıkmıştır. Bilgi toplumunda bilgi teknolojileri alanındaki gelişmelerin sonucunda muhafaza edilmesi gereken bir süreç vardır. Bu süreç bilgi güvenliği kavramıyla detaylandırılmıştır. "Bilgi güvenliği, geçmişten günümüze kadar var olmayı başarmış olan risk, tehlike ve tehditlerin yarattığı korkunun günümüz bağlamında tekrardan ortaya çıktığı alanlardan biridir" (Koçak & Memiş, 2018). Çünkü bilgi güvenliğinin amacı, iş sürekliliğiyle birlikte güvenliği sağlamak, güvenlik olaylarını sınırlandırmak, iş zararını da en aza indirmektir. Bilgi güvenliği bir ürün ya da teknoloji değil bir süreçtir. Bilgisayarların, ağların gelişmesiyle birlikte bilgisayarları ve ağları güvence altına almak teknik olarak değerlendirilse de bir süreç olarak bakmak daha doğrudur. Bilgi güvenliği denilince akla sadece bilginin muhafaza

edilmesi gelmemelidir. Günümüz düzeninde bilgi güvenliği bilginin kullanım sürecinden başlamaktadır. Bu durumlarda kişisel ve kurumsal bilgi güvenlikleri, sosyal medya güvenlikleri, e-posta güvenlikleri akla gelmektedir. Bilginin kullanım aşamasında da güven duyabilmek için süreç yönetiminde bilgi güvenliği ilkelerine bağlı kalmak gerekmektedir.

Şekil 2

Bilgi güvenliği adımları

Bilgisayar teknolojilerinde kişi veya kurumların teknolojileri kullanırken karşılarına çıkabilecek güvenlik açıklarının dikkate alınması ve buna önlemler alınmasıdır. "Bilgilere, yetki kapsamı dışında ulaşılıp kullanılması, ortaya çıkarılması, silinmesi, değiştirilmesi veya zarar verilmesi kısaca kişisel veya kurumsal mahremiyeti, bütünlüğü ve ulaşılabilirliği ihlal eden olguların öne geçilmesine bilgi güvenliği denilmektedir" (Baykara vd. 2013, ss.231-232). Hayatımızın her aşamasında da bilgi ve teknolojik tabanlı gelişmelerin etkisiyle internet kullanımının artmasıyla birlikte bilginin korunması ön plana çıkmıştır. Kamu hizmetlerinden tutun bankacılık hizmetlerine, bilgi merkezlerinden tutun özel sektör faktörlerine kadar bilginin hedef olduğu bir düzen vardır. Bu durum bilginin oluşumunda erişimine olan tüm süreçte de tehditlerin varlığına karşı tedbirlerin olması gerekliliği üzerinde durulmasını gerektirmiştir (Aldemir & Kaya, 2020).

1986'da Ulrich Beck'in "Risk Toplumu Kuramı" bilgi güvenliği sorununun açıklanmasında öncü bir çalışma olmuştur. Beck sanayi toplumunda alınan kararları risk toplumunu hazırlayıcı nitelikte olduğunu söylemiştir. Kuramı gerçekleştirirken de risk kavramı üzerinde durmuştur. Bilgi güvenliğinin sağlanması öncelikle risk kavramının anlaşılmasıyla olacaktır (Çuhacı, 2007). Risk toplumunda da bazı kronikleşen özellikler oluşmuştur. Bunlar; belirsizlik, güven kaybı, bireyselleşme, bilgi ve iletişimin artması gibi özelliklerdir. Modern teknolojiler, internetin yaygınlaşması, yeni tür riskleri ortaya çıkarmıştır. Siber riskler, bilgi gizliliği, güvenlik açıkları ve toplumsal etkenler değişen düzen ile birlikte dikkat edilmesi gereken etmenlerdir. Beck'in bu kuramı bilgi güvenliği alanında da farklı bakış açıları sunarak ortaya çıkabilecek risklere karşı nasıl olunması gerekliliğini ele alır.

Şekil 3

Bilgi güvenliği unsurları

Yukarıda verilen şekilde de görüldüğü üzere bilgi güvenliğinin unsurları ele alınmıştır. Bilginin yönetimindeki güvenlik, sürekliliği, gizlilik, yetkilendirme gibi unsurlar bilgi güvenliğinin kullanılmasında olmazsa olmazlardandır. Bilgi

güvenliğinin sağlanması günümüzde devletlerin temel hedefidir. Bu amaçla askeri, bürokra tik ve sivil temelli birçok girişim ve atılım yapılmaktadır. Güvenlik, tarihi çağların en başın dan itibaren devletlerin dikkat ettiği önemli bir konu olmuştur (Şeşen & Kuzucuoğlu, 2021). Özellikle II. Dünya Savaşı'ndan sonra bilginin değişimi sonrasında devletlerin bilgiye ve bilgi güvenliğine olan bakış açıları çok gelişmiştir. Uluslar tehdit ve tedbirlerin neler olduğunu değişen teknolojiyle birlikte tekrar gözden geçirmişlerdir. Küreselleşmenin getirdiği sonuçlar itibariyle güvenlik bilgi temeli üzerinden ele alınmıştır. Bilgi toplumunun gerekliliklerinden olan bilginin evrim süreci ne kadar nitelikli olursa güç o kadar büyüktür (Güngör & Güney, 2017). Bilginin güç ve sermaye olarak bakıldığı küresel bir dünyada da bilgi güvenliği çok önemlidir.

Bilgi güvenliği, bilginin doğru yerde doğru teknoloji ile doğru zaman ve mekân ile erişilmesinde alınan önlemler olarak da bilinir. Alınacak önlemlerin prosedürler çerçevesinde seçilmesi ve uygulanması sonucu bilgi güvenliği temelleri atılmış ve uygulanmış olur. Bilgi güvenliği yönetim sisteminin gerçekleştirilmesi güvenli bir yapı için gereklidir. Bu şekilde riskler minimize edilir, iş sürekliliği sağlanır, yasal kriterler sağlanmış olur. Kurumsal güven ve saygınlık sağlanmış olur (Tuğal vd., 2021). Bilgi güvenliğinin temel prensiplerini oluşturan kavramlar vardır. Bunlar: Gizlilik, Bütünlük, Erişilebilirlik, Kimlik doğrulama yani kullanılabilirliktir.

Şekil 4

Bilgi güvenliğinin temel prensipleri

Bilginin sadece yetkili kişiler tarafından erişilmesini sağlayan kontrollü ve güvenilir düzen gizlilik ilkesidir. Şifreleme, kontrollü erişim sağlama, güvenlik protokolleri gizlilik ilkesini destekleyen niteliklerdendir. Kuruluşların sahip oldukları bilgi protokollerine uyarak bilginin korunmasını sağlayan önlemler alınması da gizlilik ilkesiyle alakalıdır. Bilgiye erişimi sınırlayan teknolojik gelişimler, yazılımlar, programlar ve sistemler geliştirilmiştir.

Bütünlük, bilginin doğru ve eksiksiz olmasını önemseyerek değiştirilmesine karşı önlemleri benimser. "Bilginin özgün halini koruması anlamına gelir" (Akdoğan, 2022). Yetkisi olmayan bireyler tarafından değiştirilmesini ve bilginin asıl formatından uzaklaşmaması için gösterilen çabadır. Zaman zaman bu dijital süreçler iken bazen de kullanılan teknolojilerin daha nitelikli hale getirilmesiyle alakalıdır. Veri bütünlüğünü sağlamak bilgi güvenilirliğini artırır. Buna uygun teknolojiler de kullanılmaktadır. Elektronik imzalar bu bütünlüğü sağlamak için kullanılan teknolojilere örnektir.

Erişilebilirlik, bilgiye ihtiyaç duyanlar için yetkili kişiler tarafından kullanılabilir ve paylaşılabilir hale getirilmesidir. Kesintisiz erişim ve alınabilecek önlemler için kullanılan bir yöntemdir. Doğal afetlerde yaşanan yedekleme sorunları, risk altındaki bilgiler, ağ güvenlik bilgileri gibi durumlarda erişilebilirliği sağlamak için yapılan çalışmaları kapsamaktadır.

Kimlik doğrulama, bir kişinin veya bir sistemin kimliğini doğrulama sürecidir. Bu, genellikle güvenliğin ve erişim kontrolünün sağlanması amacıyla kullanılmaktadır. Kimlik doğrulama, güvenli bir sistemin oluşmasını ve yetkisiz erişimi önlemek için kullanılmaktadır.

Bilgi güvenliğinin prensiplerinden olan kavramlar yukarıdaki alanda açıklanmıştır. Bu unsurlardan birinin ihmal edilmesi sonucu veri açığı, bilgi hırsızlığı ya da birçok riskleri de beraberinde getirir. Verimli bir bilgi güvenliği için bu adımların eksiksiz ilerlemesi gerekir. Bazen prosedürlerle bazen kurallarla bazen de alınan tedbirlerle bilgi güvenliği sağlanmaktadır.

2.1.Bilgi Güvenliği Yönetim Sistemi

BGY; bilginin yönetimi karşılaştığı riskler, uygulanabilir prosedürler ve standartları, bilginin saklanması, düzenlenmesi süreçlerinin tamamını oluşturur (Akdoğan, 2022). Bilgi Güvenliği Yönetim Sistemi deyimi ilk kez 1998 yılında BSI (British Standards Institute) tarafından yayınlanan BS 7799-2 standardında kullanılmıştır (Demirtaş, 2013). Bilgi Güvenliği Yönetim Sistemi (BGYS), bir organizasyonun bilgi varlıklarını güvence altına almak için tasarladığı, uyguladığı ve yönettiği politikalar, süreçler, prosedürler ve kontroller bütünüdür. BGYS'nin amacı, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak ve organizasyonun bilgi güvenliği risklerini yönetmektir (ISO27001: Bilgi Güvenliği İhlal Prosedürü , 2016). Bilgi güvenliği yönetim sistemlerinde en yaygın kullanılanlardan biri de ISO/IEC 27001'dir. ISO/IEC 27001, bilgi güvenliği yönetim sistemleri BGYS'ler için uluslararası bir standarttır.

> Bilgi; para ve diğer ticari varlıklar gibi, işletme için değeri olan ve bu nedenle korunması gereken bir varlıktır. Bilgi, kuruluşun faaliyetleri ve devamı için büyük bir önem taşır. Günümüzde "bilgi kaybı" firmalara büyük zararlar vermektedir. Kuruluşlara ait bilgilerin "yetkisiz, kötü niyetli" kişilerin eline geçmesi olumsuz etkilere yol açmaktadır ve bu durum sıklıkla yaşanmaktadır. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), bu problemlere yönelik alınan tedbirler paketini içeren dünya çapında bir standarttır. (ADL Uluslararası Belgelendirme ve Eğitim, 2024, ss.1-9)

Bilgi güvenliği yönetim sistemi; bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası olmaktır (Yılmaz, 2007).

ISO/IEC 27001, hangi sektörden olursa olsun büyük küçük tüm kuruluşlara uygulanmaktadır. Bu standart BGYS ihtiyaçlarını belirler ve güvenli yönetimler için bir çerçeve oluşturur. ISO9001 gibi şirketlerin ya da kurumların benimsediği bir standarttır. 9001 bir hizmet kalitesi prosedürleri iken ISO27001 kurumların bilgi güvenliği alanındaki

düzenlemeleri ele alır. ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. "ISO Standartları dışında da kurumların kullandığı Control Objectives for Information and Related Technology(COBİT), The Information Technology Infrastructure Library(ITIL)" gibi standartlar bulunmaktadır (Akdoğan, 2022). ITIL, bilgi teknolojileri alanında önemli bir yer tutar. Büyük ve küçük ölçekli kurumlarda kullanılıyor olması tercih edilen ve bilgi teknolojileri alanında altyapısal çalışmaları olduğu anlamına gelmektedir. Bilgi varlıklarının korunması, iş sürekliliği sağlanması, yasal ve düzenleyici uyumun sağlanması, kurumların itibarının korunması ve ekonomik faydaların sağlanması için BGYS'ler gereklidir. Demirtaş çalışmasında BGYS'nin faydaları üzerinde durmuştur. Bu faydalar incelendiğinde çıkarımlar aşağıdaki şekilde olmuştur:

- ✓ Kurum-Kuruluşlar bilgi varlıklarının farkına varırlar.
- ✓ Kurum özelinde koruma metotları belirlenir ve daha sistematik ilerlenir.
- ✓ İş sürekliliği sağlanır.
- ✓ Sürdürülebilirlik artar.
- ✓ Bilgi sistemlerini ve ağlarını gelebilecek her türlü tehdit ve tehlikelerden korur.
- ✓ Bilginin gizliliğini, güvenilirliğini ve kullanılabilirliğini artırır.
- ✓ Kullanıcıların ve çalışanların güveni kazanılır.
- ✓ Güvenlik risklerinin azaltılması sağlanır.
- ✓ Yasal uyumluluk sağlanır ve yasal tepkiler önlemiş olur.
- ✓ Operasyonel verimlilik artar.
- ✓ Rekabet ortamıyla kazanç elde edilir.

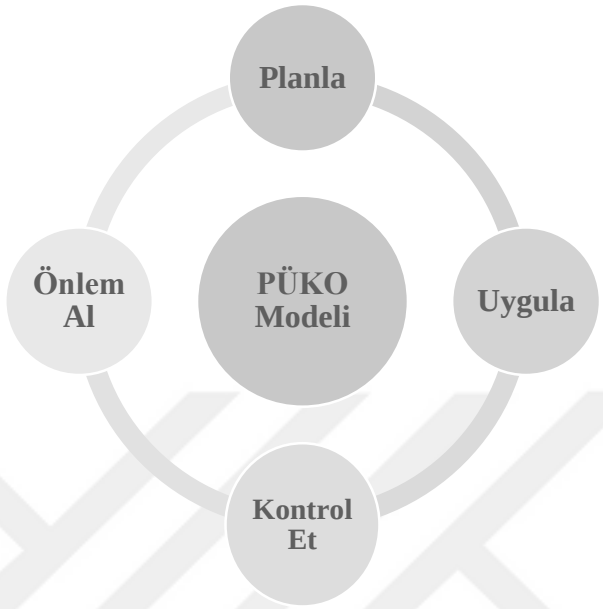
BGYS düzeninde gerekli olan bazı adımlar vardır. "BGYS'nin verimli olması ve bilgi yönetiminde güvenliğin sağlanması için bu adımların işlemesi gerekir. Bunlar; planlama, uygulama, kontrol etme, önlem almadır" (Yılmaz vd., 2014, s.51). Planlama yaparken hangi bilgi bütününü kapsayacağı belirlenmelidir. Fiziksel ve mantıksal sınırlar belirlenir ve BGYS uygulama alanları netleşir. BGYS kurulumu için üst yönetim kabulü alınır ve bilgi yönetim politikası oluşturulur. Bilgi varlıklarının tehditleri araştırılır ve tehditlere göre korunma stratejileri geliştirilir. Politikalar oluşturulduktan sonra kurum kültürü haline gelmesi açısından politikalar duyurulur. Risk analizleri yapılır ve değerlendirmeler sonucunda riskleri azaltmak için uygun tedbirler oluşturulur. Yönetilecek

bilgiler için bilgi güvenliği hedefleri belirlenir ve ISO/IEC 27001'deki kontrollerden geçerek uygulama yapılır. Uygulamada dikkat edilmesi gereken bazı detaylar vardır. Politika ve prosedürler BGYS kurallarına göre düzenlenmişse uygulamaya geçilmelidir. Çalışanlara BGYS'yi uygulayacak çalışanlara eğitim verilir ve farkındalık oluşturulmalıdır. Uygulama sonrası denetimlerle performans izleme yapılır ve yönetim gözden geçirir. Analizler sonrası düzeltici faaliyetler talep edilebilir ya da devamlılığı için güncellemeler yapılabilir. Böylelikle adım adım izlenen BGYS süreci uygun hale gelir. Ülkemizde bu gerekliliklerin yanında kamu ve özel sektörde BGYS 28/07/2006 tarihli ve 26242 sayılı Resmi Gazete 'de yayımlanan Bilgi Toplumu Stratejisi Belgesinde bilgi güvenliğinin elektronik ve ağ bağlantılarında düzenleme yapılacağından bahsedilerek önemsendiği de ortaya konulmuştur (T.C. Cumhurbaşkanlığı Resmi Gazete, 2016).

Kurum ve kuruluşların BGYS'den beklentileri tüm faaliyetlerin sürecine hâkim olmaktır. Bu da PUKÖ modeline bağlı olarak yapılmaktadır. Yılmaz (2014), BGYS'nin yönetim süreci olduğunu ve bunun etkisinin sürekli iyileştirme ile mümkün olduğunu dile getirmiştir. Ayrıca çalışmasında PUKÖ modelinden bahsedilmiştir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nde incelenen PUKÖ modeli belli bir standardı yakalayabilmek için kullanılmaktadır. PUKÖ modeli; planla, uygula, kontrol et, önlem al anlamına gelmektedir. Kurumlarda süreç iyileştirmek amacıyla kullanılan bir yöntemdir.

Şekil 5

PUKÖ modeli



Planlama; sorun olan ve iyileştirilmesi gereken süreç tanımlanır ve sonrasında durum analizleri yapılır. Hedefe göre planlama yapılır.

Uygulama; planlamada alınan kararlar doğrultusunda hayata geçirilir. Test etme ve analizleri doğrulama için geribildirimler önemlidir.

Kontrol etme; Uygulanan değişikliklerin sonuçları değerlendirilir ve analizler değerlendirmelere alınır. Hedeflerle uygulama paralel ilerleyip ilerlememe durumu kontrollerden geçirilir.

Önlem alma; yapılan analizler, anketler ve uygulamalardan sonra standartlara uymayan bir durum söz konusu ise yeniden düzenleme yapılır ve uygun olabilecek gelişmelerle süreç yeniden başlatılır. Bu süreç süreklilik ve nitelikli bir yönetim düzeni oluşturmak için vardır. BGYS'de oluşabilecek herhangi bir aksaklıkta da bu döngü kullanılarak daha verimli bir yönetim sistemi benimsenmektedir. BGYS içinde yer alan belgelendirmelerde, elektronik yazışmalarda, bilgi paylaşımı olabilecek her türlü ortamda standardı yakalamak için kontroller yapılmaktadır. Uygunsuz olan bir durumda düzeltici

faaliyet önerilir. Geliştirmeye yönelik sürekli iyileştirmeler verilir. Prosedürlere uygunsuz değil ama uygunsuzluğa yol açabilecek durumlar için de önleyici faaliyetler önerilir. BGYS için bu faaliyetlerin dikkate alınması etkili bir yönetim sistemi ortaya koymaktadır. Kaliteli işletmeler elde edebilmek için katkıları çoktur.

Kuruluşlarda BGYS'nin başarısını yükselten faktörler:

- Üst yönetim desteği
- Çalışanların katılımı
- Çalışanların farkındalığı
- Uygun Belgelendirme Sistemleri
- Son teknolojinin kullanılması
- Finansal destek/ Ekonomik genişlik
- Müşteri memnuniyeti (Demirtaş, 2013).

BGYS kurumlarda olumlu katkılar sağlamaktadır. Kaliteli bir süreç yönetilmektedir. İş süreçlerinde, teknolojik gelişmelerde, insan kaynakları kısmında o şirkete katkısı büyük olmaktadır. Bilgi güvenliği yönetim sistemini anlayıp uygulamak riskleri analiz etmeye ve tedbirler geliştirmeye yol açmaktadır. En başta yapılması gereken bilgi güvenliği için farkındalık oluşturmak ve çalışanların bilgi sahibi olmasını sağlanmalıdır. Kurum kültüründe herkesin alması gereken eğitimler olmalıdır. Bunlara örnek:

- E-posta Güvenliği
- Şifre Güvenliği
- İnternet Kullanımı
- Cihaz Güvenliği/Mobil cihaz
- Siber Tehditler ve Türleri
- Sistem Güvenliği
- Sızma Testi Eğitimleri
- Ağ Güvenliği Eğitimleri
- BGYS Eğitimi
- Risk Analizi

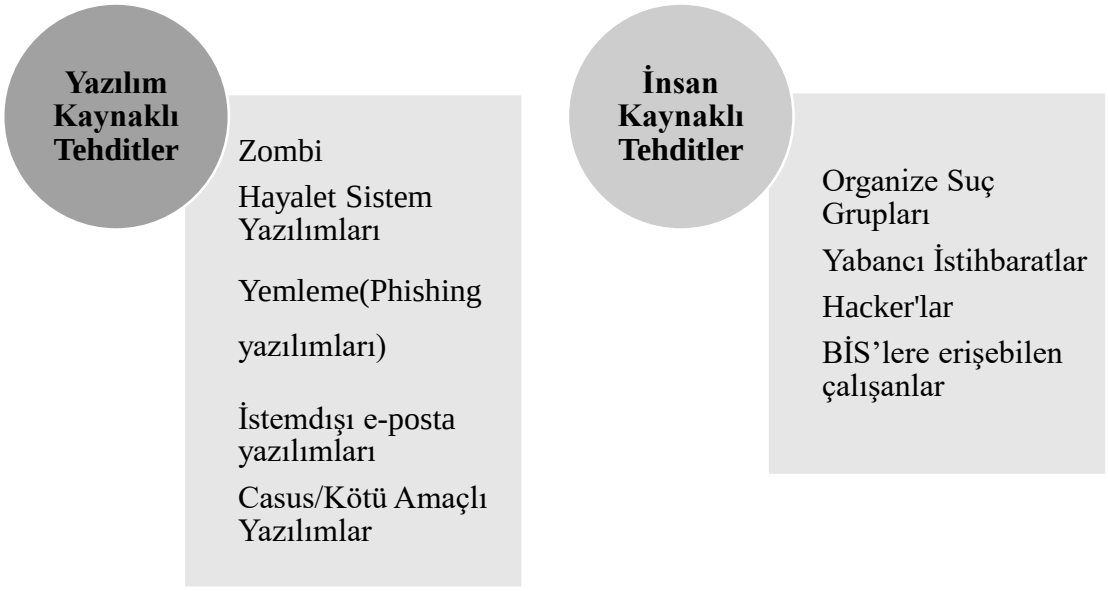
Bu eğitimler dışında kurum kültürüne ve amacına uygun eğitimler de eklenebilir ve kurum çalışanları bilgi güvenliği konusunda daha profesyonel çalışması sağlanabilir (Tuğal vd., 2021). Güvenliğin en zayıf halkası insandır. Bu sebeple eğitimlerin verilmesi çalışanların bilgi güvenliği konusunda kültürlenmesine sebep olur. Çalışanların bilgi güvenliği konusunda uzmanlaşmaları da bu süreçten sonra daha sık görülmektedir.

2.2. Bilgi Güvenliği Tehditleri/Tedbirleri

Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemine bir önceki bölümlerde bahsedilmiştir. Bilgi güvenliği sağlanırken bazı zamanlarda olumlu olumsuz yaşanabilecek durumlar vardır. İç tehdit ve dış tehditler olmak üzere ikiye ayırmak mümkündür. Solmaz'ın (2023) çalışmasından yola çıkılarak hazırlanan ve Şekil 6'da yer aldığı üzere; iç tehditlerde yazılım kaynaklı olabilecek sorunlar ele alınırken dış tehditlerde insan kaynaklı sorunlar ele alınmıştır.

Şekil 6

Bilgi güvenliği tehditleri



Yazılım Kaynaklı Tehditler

Yazılım kaynaklı tehditler, yazılım sistemlerinin güvenliğini, bütünlüğünü, kullanımını ve erişilebilirliğine tehdit oluşturabilecek tehditlerdir. Bu ve benzeri tehditler, yazılım geliştirme sürecindeki hatalar, güvenlik açıkları, kötü amaçlı yazılımlar ve kullanıcı hatalı gibi sebeplerden oluşabilmektedir (Kahya, 2007).

a. Zombi/Hayalet Sistem Yazılımları; bir bilgisayara kullanıcısının anlamayacağı ama çok farklı yollarla bulaşabilir. Bulaşma yöntemlerinin çoğu hedef olan bilgisayarlardaki açıklıklardır. İşletim sistemlerinin eski sürüm olması, yazılımların yetersiz kalması, bilinçsiz kullanıcının olması sebebiyle daha çabuk ve kolay bulaşabilmektedir. Hayalet sistem, genellikle bilgisayar korsanlarının kullandığı yazılım türüdür. Bu yazılım kullanıcıların bilgisayarına sızarak uzaktan kullanıcının hiç fark etmeyeceği şekilde yönetilebilir. Sinsi ve adından da anlaşılacağı üzere hayalet virüs olarak adlandırılmıştır (Canbek & Sağıroğlu, 2007).

b. Hayalet sistem yazılımları, e-postalarda yaygın görülebilmektedir. Kötü amaçlı yazılım yaymalarda kullanılarak da yazılım dünyasına zarar vermektedir. Gizli erişim sebebiyle gizli veri toplama yapılabilmekte ve hassas bilgilere erişimi sağlayarak gizlilik ilkesini çiğnemiş duruma gelebilmektedir. Bu yazılım türlerine örnek verilirse; botnetler, rootkitler ve RATs'lerdir. Botler, ele geçirilen bilgisayarlar anlamına gelir. Bir komuta karşılık vererek kontrol sunucusundan gelen emirleri yerine getirir (Ünver vd., 2011). Rootkitler, işletim sistemlerinde değişiklikler yaparak o işletim sistemini ele geçiren programlardandır. İşletim sisteminin her açılması sonucu etkinleşir ve gizli olması sebebiyle de fark edilmesi çok zordur. Rootkitler bilgisayarı, klavyeyi, ağ bağlantılarını engelleyebilir özelliktedir. RATs, Saldırganlara uzaktan erişim ve kontrol imkânı sağlar (Ünver vd.,2011). Dosya kaydetme, ekran kaydı, klavye girdilerinin kaydedilmesi gibi işlemleri yaptırabilir. Olduğundan farklı ve tehlikesiz gösterebilir. Zararlı bir programdır.

c. Yemleme yazılımları (phishing yazılımları), kullanıcıları kandırarak kişisel verilerini, hassas verilerini ifşalamak için yazılmış bir programdır. Phishing (Oltalama), kötü niyetli kişilerin sosyal mühendislik yaparak sahte veya yanıltıcı e-postalar, mesajlar veya web siteleri aracılığıyla kullanıcıların kişisel veya finansal bilgilerini çalmayı amaçlayan bir siber saldırı türüdür (Bilişim Academy, 2024). Kullanıcının güvendiği bir kurum veya işletme gibi tanıtıp güven kazanarak işlemlerini yaparlar

d. İstemdışı e-posta yazılımları, kullanıcıların istemedikleri, çoğunlukla zararlı ve istenmeyen e-postaları almalarına neden olan yazılımlardır. Bu yazılım spam e-postaları gönderebilmek için kullanılmaktadır. Adware, Phishing yazılımları, spam botları gibi istem dışı e-posta yazılımları spam filtrelerini kullanarak istenmeyen bir durum ortaya çıkarır.

e. Casus/kötü amaçlı yazılımlar, bilgisayarlara zarar vermek, bilgi hırsızlığı yapmak, kullanıcıların sistemlerini ele geçirerek zarar vermek amacıyla tasarlanmış yazılımlardır. Kullanıcının bilgisayarla olan etkileşimine engel olan veya kısmi olarak bu etkileşimin kontrolünü ele geçiren ve kullanıcının bilgisayarına gizlice yüklenen programdır (Ünver vd., 2011). Kötü amaçlı yazılım türleri vardır. Bunlara örnek olarak; Truva atları, solucanlar, Adware, Spyware, virüsler, Keylooger'lar verilebilir. Kötü amaçlı yazılımlar, faydalı yazılım gibi görünerek kullanıcıları kandırıp bilgisayarları ele geçirmeyi hedeflemişlerdir. Zarar vererek bilgi hırsızlığı ile tavizler oluşturmak, bilgi açıklığından yararlanmak kötü amaçlı yazılımların özelliklerindendir (Canbek & Sağıroğlu, 2007).

İnsan Kaynaklı Tehditler

Bilgi güvenliği tehditlerinde insan kaynaklı tehditler, kurumları tehlikeye atan insan hataları, kötü niyetli yazılımların kullanılması, dikkatsizlik ve bilinçsizlikler sonucu ortaya çıkmaktadır. Bilgi teknolojilerinin de beraberinde getirdiği yeniliklerle birlikte güvenlik açıkları da oluşmaktadır. Bu eksikliklerden en önemlileri de insan kaynaklı olanlardır. Tüm personelin bilinçlendirilmesi gerektiği gibi bir de insan kaynaklı bazı tehditler de göz önündedirler. Bunlar:

a. Organize suç grupları, giderek artan bir tehdittir. Bu gruplar ülke genelinde kurumları hedef edinerek kazanç elde edebilmek için örgütlenen gruplardır. Veri çalarak çaldıkları verileri ilgili olabilecek farklı firmalara fark ettirmeden satılmasıyla uğraşarak kar elde etmeye çalışmaktadırlar. Bu grup fidye talep etmekten, hizmetleri kesintiye uğratmaya kadar büyük tehdit oluşturabilmektedirler. Kurumlar için bu gruplar oldukça tehlikeli saldırıları oldukça ciddidir. Profesyonelce yaklaşımları sayesinde çalışan personellerin güvenini kazanarak yollarına devam edebilirler. Böyle bir durumda da personellerin bilinçlendirilmesi şarttır. Bankacılık yazılımlarında daha çok menfaatleri doğrultusunda daha çok vakit geçirmektedirler. Bu saldırılarda bilgisayarları, kurum cihazlarını, kurum ağını erişilmez hale getirerek kontrolü tamamen ellerine alabilir hale getirebilirler. Bu tehditlere karşı kurumların ve bireylerin savunma stratejileri geliştirmeleri ve bunun uygulanması için çalışma yapmaları kritik önem arz eder.

b. Yabancı istihbarat örgütleri, bilgi güvenliği alanında büyük tehdit oluşturmaktadır. Bu gibi örgütlenmeler ülkenin her türlü alanından avantaj sağlamak amacıyla hareket ederler. Siber casusluk olarak da adlandırılan bu saldırılar ulusal güvenliği de tehdit altında bırakabilir. Yabancı istihbarat örgütleri en güncel gelişmeleri toplayarak saldırılarını da ona göre düzenlemektedirler. Bu örgütler, ulusal tehdit oluşturur, ekonomik ve ticari zarar verebilir, finansal kayıplar oluşabilir, hizmetlerde kesintiler yaşanabilir, veri gizliliği ihlali oluşturabilir, şirketlerin rekabet avantajlarını yitirmelerine sebep olabilirler. Bilgi teknolojilerin sunduğu imkânlardan yararlanarak siber uzayın kullanılmasını sağlamışlardır. Bu durum da devletler arasındaki siber savaşları tetikleyebilmektedir. Gelişmiş ülkelerde siber güvenlikle toplu mücadele için Siber Güvenlik Ajansları kurulmuştur (Şeşen & Kuzucuoğlu, 2021). Yenilenen teknolojiyle ve yeni dünya düzenindeki saldırmaların da türü değişmiştir. Siber saldırılara teşvik eden gelişmiş ülkelerin farkındalığı daha fazladır.

c. "Hackerler, bilgisayar sistemlerine çeşitli amaçlarla giren ve izinsiz erişim sağlayan bireylerdir. İnşa edici yanları ile diğer bilgisayar suçlularından, özellikle

de yıkıcı olarak nitelendirilen “cracker”lardan ayrılan “hacker”ların eylemlerinin ana karakteristikleri ise; basitlik, hâkimiyet (üstünlük) ve kanuna aykırılık olarak çizilmektedir” (Kaya, 2010). Amaçları veri çalmak, sistemleri bozmak, finansal kazanç elde etmek, bilgiye erişmek ve savunma mekanizması olarak kullanmaktır. Bilgi güvenliğinde ciddi tehditler oluştururlar. Hacker türleri vardır. Bunlar; beyaz şapalı hackerlar, siyah şapkalı hackerlar ve Gri şapkalı hackerlardır. Beyaz şapkalı hackerlar etik hackerlardır. Etik hackerlar, siber güvenlik alanında kendini geliştiren ve firmaların güvenlik zafiyetlerini tespit etmek için çalışan kişilerdir. Bu kişiler, kötü niyetli bir hacker bakış açısı ile sistemleri analiz ederek sistemleri hacklenmekten korumaya çalışırlar (Deloitte,2024). Bu hackerlar şirketlerin ya da kurumların güvenlik açıklarını kapatmak, kurumun gizliliğini korumak amacıyla giriş sağlarlar. Daha çok güvenlik danışmanı rolündedirler ya da sızma testi yapan personeldirler. Siyah Şapkalılar, kötü niyetlidirler. Yasa dışı, illegal durumlar içindedirler. Siber suçlu olarak sayılacak olan bireylerdir. Amaçları veri çalmak, veri satmak, fidye istemek, kişisel verilere zarar vermektir. Siber terörist de denilmektedir. Gri şapkalı hackerlar izinsiz sızma yaparlar fakat genellikle amaçları zarar vermek değildir. Güvenlik açıklarını tespit etmek ve bazen de ilgili kişilere bildirmek için yapan kişilerdir. Güvenlik açıklarını bildiren kişilerdir.

d. BİS’lere erişebilen çalışanlar, kurumların bilgi güvenliği stratejisi açısından kritik bir konumdadırlar. Bu çalışanlar kurum içi ve kurum dışı işlerde aktiflerdir. Erişim sağlayabildikleri veri kaynakları yelpazesi geniştir. Dolayısıyla bu erişimlere yakın olan bireylerin denetlenmesi, göz önünde olması güvenlik açığı oluşturabilmektedir. Bilgi güvenliği riskleri oluşan bu durumlarda en az risk oranına dönüştürene kadar kurum çalışmalarını sürdürür. Risk analizlerini değerlendirir. Bu personellere yönetici erişimi imkânı verilebilir, uygulama erişimleri verilebilir, kullanıcı erişimi açılabilir. Sızıntı olabileceği gibi kötü amaçlı faaliyetlerle veri sızdırılması ve sistemlerin kitlenmesi gerçekleşebilir. Uygun şifre kuramama, sınırsız erişimler, iç tehditler gibi sebeplerden ötürü siber saldırı gerçekleşebilir ve bilgi güvenliği sağlanamayabilir. Bu da bilgi güvenliği ilkelerinin yerine gelmemesi anlamına gelmektedir.

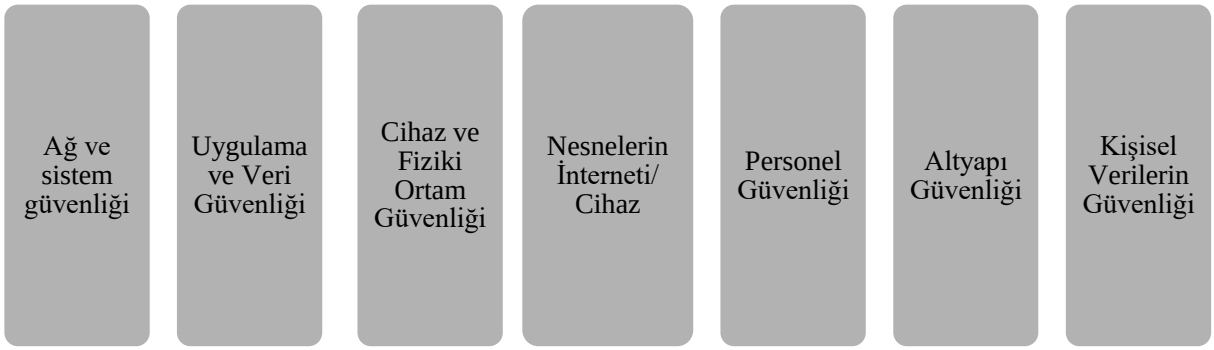
Bilgi güvenliğinde oluşabilecek tehditler yukarıdaki bölümde verilmiştir. Zaman zaman tehditlerin şekil ve yöntemleri değişse de çoğunluğu kurumlara ve işleyişlere zarar vermek amacıyladır. Kurumların bilgilerini elde ederek fayda sağlamak bunu satışa koyarak kar elde etmeye çalışan bu kitleler risk içermektedir. Saldırı risklerinin artmasında bilgi güvenliğinin yeterli olmaması, kurumların denetim güçlerinin olmaması, altyapıların eksikliği, yazılım ve bilgi teknolojilerinin yetersizliği, bilinçsiz çalışanlar, kötücül yazılımlara karşı savunmasız olmaları gibi birçok sebep vardır. Kötücül yazılımlardan sonra dolandırıcılık, kandırma, kara para aklama gibi kötü süreçler olabilmektedir. Buna ek olarak da sosyal mühendislik yöntemini de kullanarak kandırma işlemi gerçekleştirilebilir. Örneğin; kurumda işe yeni başladığını söyleyen ve kullanıcı adı ve şifresi talep eden bir bireye, o kurumdaki yetkili olabilecek kişinin kullanıcı adı ve şifre vermesinden sonra erişim imkânı sağlanmış olur. Böylelikle kurum yetkilisi tarafından verilen şifre ile kurumun bilgilerine erişebilen saldırgan figürleri ortaya çıkmış olur. Bu gibi durumlarda çalışanların farkındalık ve bilinçlenmesi sağlanmalıdır. Kurumsal bilgi güvenliğindeki en önemli faktöreler, çalışanların bilgi güvenliği farkındalıkları ve bilinç düzeyleridir. Kurumsal bilgi güvenliğinin sağlanmasında yapılacak olan teknolojik gelişmelerin bilgi güvenliği risklerine uygun personellerin yetiştirilmesi gerekmektedir (Yılmaz, 2014).

Tedbirler

Bilgi güvenliği tedbirlerinden ilk adımı bilgi güvenliği alanında çalışanların bilgi sahibi olmasını sağlamak ve farkındalıklarını artırmak, ikinci adımda bilgi güvenliği ve bilgi güvenliğinin önemi konusunda toplumu bilinçlendirme çalışmaları, üçüncü olarak da yetkilendirmelerin yapılmasıdır. Bu durumla bilgi toplumu düzeninin gerekliliklerine bağlı olarak dijitalleşmenin, teknolojik gelişimlerin güvenlik önlemlerinde de değişim yapılması gerekliliğini ortaya koymaktadır. Teknolojik gelişimler sonucunda güvenlik önlemlerindeki söz konusu değişim kimi zaman ağ güvenliğinde kimi zaman kullanılan yazılımlarda kimi zaman altyapı güvenliğindedir. Buna örnek olarak aşağıdaki Şekil 7'de verilmiştir. Bunun üzere bilgi güvenliği tedbirleri detaylandırılmıştır.

Şekil 7

Bilgi güvenliği tedbirleri



a. Ağ ve Sistem Güvenliği, bilgi yönetimi alanında kritik bir rol üstlenir. Bilgi varlıklarını dış tehditlere karşı koruyarak önlemler alınmasıdır. Ağ güvenliği, güvenlik duvarları oluşturarak veri kaybını önlemek amacıyla kurulmuş setlerdir. Bazen yazılım bazen bir uygulama bazen ise internet ortamındaki bir uzantı olabilmektedir. Yetkisiz erişime imkân tanımayan bir düzendir. Kötü amaçlı yazılımlardan korumak ve veri hırsızlığına karşı ağın gizliliğini, bütünlüğünü ve erişilebilirliğini koruyan sistemlerdir. Bunun yanında sistem güvenliği; ağ üzerinde çalışan ve kötü amaçlı yazılımlardan koruyabilmek, uygulamaların güvenilirliğini sağlamak amacıyla alınan önlemlerden oluşmaktadır. Ağ güvenliği denilince de akla sadece güvenlik duvarı gelmemelidir. Bilgi güvenliğindeki esasların sağlanması için bütün olarak ele almak gerekmektedir. Bilgisayar ağlarını, cihazları, yazılımları ve kurulumunu bütünleşmiş bir sistem yapmak gerekmektedir. Dışarıdan gelebilecek bir saldırıya karşı savunma mekanizması uygulanırken içerdeki personelden bu saldırının gelebileceği daha az düşünülmektedir. Ağların ve sistem odasına erişebilen personellerin de kontrollü ve yetkilendirilmesi gerekmektedir. Ağ güvenliğinin tam sağlanması için; internet bağlantı güvenliğinin sağlanması gerekmektedir. Saldırıları tespit etmesi için bazı uygun sistemlerin kurulumunun yapılması gerekmektedir. Veri güvenliğinin sağlanması için şifreleme ve koruma yöntemlerinin geliştirilmesi gerekmektedir. Kötü amaçlı yazılımlardan korunmak için antivirüs uygulamalarının olması

gerekmektedir. Kurumların güvenliğinde son zamanlarda oldukça önemsenen yedeklemelerin olması gerekmektedir.

VPN (Virtual Private Network - Sanal Özel Ağ) güvenliğine de dikkat edilmesi gerekmektedir. VPN güvenli ve şifreli erişimler sağlarken kullanıcıların veri trafiğini de gizleyerek koruma sağlamaktadır. Güvenli ve çevrimiçi erişimi sunmuş olur (Kahya, 2007). Eğer özel ağ kullanılacaksa özel ağ ile internet arasına bir güvenlik duvarı kurulması gerekir. Güvenlik duvarı, bir ağın veya bilgisayar sisteminin güvenliğini sağlamak amacıyla kullanılan bir donanım veya yazılım bileşenidir. Güvenlik duvarları, gelen ve giden ağ trafiğini denetleyip filtreler yapar ve daha önce belirlenmiş kurallara göre izin verir veya engeller.

b. Uygulama güvenliği, yazılım uygulamalarının geliştirilmesinde, dağıtılmasında ve işletilmesi sürecinde güvenliği sağlamadır. Bu süreç, uygulamalarda yetkisizlikten korur. Saldırılarda veri ihlallerinden korunmasını amaçlamaktadır. Veri güvenliği, verilerin yetkisiz erişime, tahribat ve hırsızlığa karşı korunmasını sağlayan önlemleri içerir. Veri güvenliğinde fiziksel güvenliğin de sağlanması gerekmektedir. Akıllı kartlar, şifreleme yöntemleri, tek kullanımlık parolalar, doğrulama kodları ile daha güvenli hale getirilmektedirler. Şifreleme yapılırken de eğer farklı birimler varsa kurumda her bir birim için şifre belirlenmelidir ve birimler kendi arasında şifre paylaşımı yapmamalıdır. Bireysel yönetmeler söz konusu ise bireyler şifrelerini belirleyip kullanmalıdırlar. Hazır şifreler kullanılmamalıdır. Şifre belirlerken de dikkat edilmesi gereken unsurlar ekstra önemsenmelidir.

c. Cihaz ve Fiziki Ortam Güvenliği, bilgi varlıklarını fiziksel tehditlerden korunması için alınan önlemlere denir. Bu güvenlik önlemleri, cihazların ve verilerin fiziksel olarak güvende tutulmasını amaçlamaktadır. Cihaz güvenliği ve fiziki ortam güvenliği, bilgi güvenliğinin kritik bileşenlerinden olmuştur. Cihaz güvenliğinin sağlanabilmesi için, biyometrik kimlikler olmalıdır. Cihazlarda şifre belirleme yapılmalı ve çok faktörlü kimlik doğrulamalar yapılmalıdır. Fiziki ortamların

erişimlerinde kartlı geçişlerle kontrollü geçişler yapılmalıdır. Kamera, kilitli kapılar, biyometrik veriler isteyen sistemlerin kullanılması gerekmektedir (Çubukçu, 2018). Cihaz güvenliği denilince günümüzde en çok kullandığımız artık her işimizi onunla yaptığımız bilgisayarlarımız akla gelmektedir. Bilgisayar güvenliklerinde kişisel veya kurumsal bilgisayarlarda önemsenmesi artık zorunluluk haline gelmiş bazı uygulamalar vardır. Bunlar:

- Bilgisayarlara şifrelerin konulması
- Parolaların zorluk derecesinin en zor olarak seçilmesi
- Parolaların belli aralıklarla değiştirilmesi ve tahmin edilebilirliğinin zor olması
- Kötü yazılımları için koruyucu antivürüs uygulamalarının yüklenmesi
- Önemli verilerin düzenli olarak yedeklenmesi
- İnternet kullanımının ve erişilen sitelerin kontrolünün sağlanması
- E-postalara gelen eklere dikkat edilmesi, gönderirken de güvenli uzantılarla gönderilmesi
- İşletim sistemlerinin en güncel olması cihaz ve teknik anlamda alınması gereken önlemler arasındadır (BBS Belgelendirme, 2024).

d. Nesnelerin İnterneti (loT)/ Cihaz Güvenliği, internet üzerinden birbirine bağlı cihazların oluşturduğu bağlı bir ağ düzenidir. IoT (Nesnelerin İnterneti) son zamanlarda ortaya çıkan Bluetooth, Zigbee, GSM ve WiFi gibi çeşitli haberleşme çözümleri sunan nesnelerin ve cihazların birbiriyle bağlantısını ifade eden bir bilgisayar paradigmasıdır (Taş & Kiani, 2021). IoT'lar internet aracılığıyla cihazların daha geniş iletişim kurmasını sağlar. IoT cihazların güvenliği, cihazların hem bireysel hem de ağ seviyesinde korunmasını ifade eder. Veri gizliliğini ve cihazların doğru çalışıp çalışmadığını öngören bir çalışmadır. Bu cihazlar genellikle sensörler, yazılımlar ve diğer teknolojilerle donatılmışlardır. Veri toplamak, paylaşmak ve analiz etmek amacıyla internete de bağlı olmaları gerekmektedir. loT cihazları genellikle sensörlerle donatılmıştır. Bu sensörler, sıcaklık, nem, ışık, hareket gibi çevresel verileri toplar. Bu veri toplama paylaşma evresi de bilgi güvenlik risklerine karşılık tedbirleri de beraberinde getirir.

Şekil 8

Nesnelerin internetinden etkilenen bazı alanlar

Saldırganların servislerine karşılık savunma mekanizması geliştiren IoT, bilgi girişi yapılan nesnelerde verilerin filtrelerden geçerek alınması gerekmektedir. Sorgu veri tabanına düşmeden giren veriler için şifrelemeler yapılmalı ve sızıntı oluşturabilecek veri açıklarını kapatılması için önlemler alınmalıdır. Web servislerinde veri alışverişi yapılırken doğrulama yapılmalı ve şifrelenerek yapılmalıdır. Zaman damgası kullanımı yapılmalı ya da paket kimlik doğrulaması ile kontrol tam manada saldırgana verilmeyeceği gösterilmelidir. Ağlarda dolaşan kötü niyetli yazılımların tespitini yapan uygulamalar edinerek ve ağ trafiğinin kontrolü sağlanarak şüpheli her şey ağdan uzaklaştırılabilir. IoT güvenliği için, kimlik doğrulamalar, yetkilendirmeler, veri şifrelemeleri, güncellemeler, cihazların fiziksel olarak yetkisiz erişimlere karşı korunmalarının yapılması, ağ güvenliğin sağlanmasına oldukça dikkat edilmelidir. Cihaz seçimlerinde de milli yazılım ve donanım ürünleri olanların tercih edilmesi daha doğru olacaktır. Milli olmayanlarda güvenlik açıkları daha fazla olma ihtimali vardır.

e. Personel Güvenliği, bir kurum veya kuruluşlarda çalışan personelin fiziksel, psikolojik ya da bilgi güvenliklerini sağlamak amacıyla kurulan önlemlerdir. Çalışanların güvenli bir ortamda çalışmasını sağlamak için yapılan bazı önlemler vardır. İş sağlığı ve güvenliği ile alakalı olan bu alanı kapsamaktadır. Personel güvenliği unsurları; fiziksel güvenlik, psikolojik güvenlik, bilgi güvenliği, eğitim ve farkındalık, politika ve prosedürlerdir. Fiziki güvenlikte yangın alarmları, yangın çıkışları, kameralara dikkat edilmesi ve kontrollerinin yapılması gereklidir. İlk yardım ve acil durumlarda müdahale planlarının hazırlanması ve personele duyuruların yapılması önemlidir. İş kazalarını önlemek amacıyla da gerekli donanımların bulundurulması gereklidir. Çalışanların psikolojik olarak rahat ve güvende hissedebilmeleri için psikolojik güvenlik geliştirilmelidir. Mobbing ve taciz gibi durumlarda politikalara bağlı kalınarak işlem yapılmalıdır. Bilgi güvenliği tedbirlerinden en önemli olan personelin bilgi güvenliği, kurum çalışanlarının veri güvenliği konusunda bilinçlendirilmesi gerekmektedir. Veri koruma politikalarının ve prosedürlerinin uygulanması için personele bilgilendirme yapılmalı ve farkındalık çalışmaları yapılmalıdır. Personelin çalışma planlarına uygun güvenlik ve bilgi güvenliğiyle alakalı eğitimler düzenlenmelidir. Personel başkaları tarafından yapılabilecek saldırılara karşı nasıl savunma yapması gerektiğini bilmeli ve tehditlerin belirlenmesinde rol almalıdır. Tüm personelin bilgi güvenliğiyle alakalı (tehditler, yenilikler, saldırılar) yöntem ve tekniklere dair eğitim alması gerekli ve elzemdir.

f. Altyapı Güvenliği, bilgi sistemlerindeki ağlar ve fiziksel altyapıların iç ve dış tehditlere karşı korunmasını amaçlayan önlemlerdir. Bu güvenlik önlemleri, veri ihlallerini, yetkisiz erişimleri, siber saldırıları önlemek amacıyla tasarlanmıştır. Altyapı güvenliği unsurları; ağ güvenliği, fiziksel güvenlik, depolama güvenliği, bulut güvenliği, siber güvenliktir. "Ağ ölçeklenebilirliği, yönetilebilirliği, güvenliği ve sürekliliği yüksek standartlara ulaştırılmak üzere sanallaştırılır. En doğru şekilde bilgi işleme, veri depolama ve ağ çözümlerinin onaylı tasarımlar kapsamında bir araya getirilmesi ile kurulum sürelerinin hızlandırılması, performansının artırılması ve yönetiminin kolaylaştırılması sağlanır" (Ard Bilişim Yazılım Teknolojileri , 2024). Altyapı güvenliği için alınması gereken önlemler

vardır. Güvenlik denetimleri ve testlerinin düzenli olarak yapılması gereklidir. Yapan kişilerin de bu denetimleri şifreli ve kontrollü yapması gerekmektedir. Güvenlik politikalarının ve prosedürlerinin belirlenmesi ve bu prosedürlerin uygulanması gereklidir. Bu prosedürlerin çalışanlarla paylaşılması ve çalışanların farkındalığı için çalışmalar yapılması gerekmektedir.

g. Kişisel Verilerin Güvenliği, bireylerin özel bilgilerinin izinsiz erişim ve kullanımına karşı korunmasını sağlayan prosedürlerdir. Bu uygulamalar kişilerin mahremiyetini korumayı ve veri ihlallerine karşılık güvence sağlamayı amaçlamıştır. Kişisel veriler, kişinin kimlik yapısını ortaya koyan ve kişiye özel bilgiler olarak tanımlanabilir. Kişisel veriler, bir kişiyi doğrudan veya dolaylı olarak tanımlayabilecek her türlü bilgiyi kapsar ve isim, adres, telefon, e-posta, kimlik numarası, finansal bilgiler ve daha fazlasını içermektedir. Bu yüzden kişisel verilerin korunması önem arz etmektedir. Bu durum sadece kişinin kendisi ile alakalı değildir. Kişinin çalıştığı kurum ve kurum bilgilerini de alakadar eder bir durumdur. 29677 Sayılı Kişisel Verilerin Korunması Kanunu'nda da bahsedildiği üzere amaç kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. "*Veri güvenliğine ilişkin yükümlülüklerde; kişisel verilerin uygunsuz olarak işlenmesini, kişisel verilere hukuka uygun olmayacak şekilde erişilmesini, kişisel verilen korunmasını, muhafaza edilmesini, uygun güvenlik tedbirleriyle her türlü teknik ve idari süreçleri yönetmek zorunludur*" (T.C. Cumhurbaşkanlığı Resmi Gazete, 2016).

Bilgi iletişim teknolojilerinin gelişmesiyle birlikte daha fazla internet kullanımı ve veri paylaşımı olmaktadır. Sosyal mecralarda kullanıcılar kendilerine dair bilgileri paylaşarak, tasvirlerle, resimlerle de bunlara destek vermektedirler. Bu bilgilerin paylaşımıyla da üçüncü kişilerin erişebilmesi hatta aleyhte kullanılabilirliği artmaktadır. Bu süreçlerin korunması ve kişilerin haklarının savunuculuğunu ise KVKK'lar yapmaktadır. Bunlara ek olarak güvenlik ve gizliliğe dikkat edilmesi gerekir. BTK, bu konuda neler yapılması gerekliliği üzerinde durulmuştur. Yapılan çalışmalarda:

- Bilinen ve güvenilir sitelerden alışveriş yapılmalıdır.
- İnternet ve sosyal ağlarda çok fazla konum, adres, özel olabilecek bilgiler paylaşılmamalıdır.
- İnternet alışverişlerinde sanal kart ya da limit belirleme yöntemi uygulanmalıdır.
- Harici belleklerin virüs ve kötü amaçlı yazılımlardan arındırılmış olduğundan emin olunmalıdır.
- Lisanssız yazılım ve uygulamalar kullanılmamalıdır.
- Akıllı telefonlarda uygulama indirmelerinde daha dikkatli olunmalıdır.
- Gerek iş yerinde gerekse kişisel bilgisayarlarda kullanılan şifrelerin zorluk derecesi artırılmalı ve tahmin edilebilir olmamalıdır (Bilgi Teknolojileri ve İletişim Kurumu, 2024).

Risklerin olması teknolojik imkânlardan gelişmişliklerden kaçınılarak değil, yeni teknolojilerin sisteme dâhil olması ile birlikte gelebilecek tehditlerden sakınmayı gerektirir. Bunun için yapılabilecek veri açıklarını yok edebilecek altyapıları sağlamak ve kurum ya da kuruluşlar için risk analizleri yapılması gerekmektedir. Bilgi işlem, iletişim ve altyapıların sürekli kontrol edilmesi ve güvenlik açıklarının oluşmaması için önlemler alınmalıdır.

Ülkemizde kamu ve özel sektörde bilgi yönetim sisteminin 2003 yılında Başbakanlık Genelgesi oluşturulması ile birlikte bilgi güvenliği tedbirlerinde daha genel bir gelişme gözlemlenmektedir (Demirtaş, 2013). Bu genelgenin yanında elektronik dönüşümler de desteklenerek basılı olan bilgi düzeninin elektronik ortamlara aktarılması durumu yaygınlaşmıştır.

3. SİBER GÜVENLİK

Siber güvenliği anlamak için öncelikle siber uzayın da ne olduğunu bilinmesi gerekmektedir. Siber uzay, geniş bir bilgi ortamıdır. İçerisinde bilginin çevrimiçi saklandığı, paylaşıldığı, iletildiği, bilgisayar ağları ile bireylerin arasındaki kısımdır. Siber uzay, sadece sanal ortam anlamına da gelmez. Verileri saklayan bilgisayarların yanında bilgi akışının olmasını sağlayan sistemlerin, altyapıların fiziksel ortamda bulunmasını da sağlamaktadır (Singer & Friedman, 2018). İnternet ortamında olan hem sanal hem fiziki durumlar siber uzayın bir parçası olmuştur. "Siber uzay; dünyada ve uzayda yer alan bilişim sistemlerinin ve ilgili ağların oluşturduğu ya da bağımsız bilgi sistemlerinde bulunan sayısal ortama denilmektedir" (Kurnaz & Önen, 2019). Siber uzay değişen toplumun içerisinde sürekli evrim geçiren bir yapıdadır. Teknoloji ve teknoloji kullanıcıları tarafında her geçen gün bir yenilik olmakta, teknik ve dijital değişimler yaşanmaktadır. "21'inci yüzyılın yaşam ve teknik düzenin egemen platformu" Siber uzay olacaktır diyen Wired dergisinin editörü Ben Hammersry akla gelmektedir (Singer & Friedman, 2018). Büyük ülkelerin özellikle de gelişmiş ülkelerin yöneticilerinin de bilgi güvenliğine önem veren cümleleri olmuştur. Rusya Devlet Başkanı Vladimir Putin de 2017'de Moskova'da düzenlenen Ulusal Bilgi Forumu'nda da siber güvenliğin 21. Yüzyılda yaşam ve teknik düzenin temeli olacağından bahsetmiştir. Bu denli önemsenen durumlarda da korunma ve saldırılara karşı savunma stratejilerin geliştirilmiş olması beklenmektedir. Siber güvenlik, bilgisayar sistemleri, ağlar, cihaz ve programlar ve dijital saldırılardan korunmak amacıyla düzenlenen uygulamalar, teknolojiler ve süreçleri içeren bir düzendir. "Siber güvenlik; siber uzayda oluşan bilişime yönelik saldırılardan korumak, bilişim sistemindeki bilgiyi/verinin gizliliğini, bütünlük ve erişilebilirliği güvenceye almak, saldırıları ve siber güvenlik olaylarını tespit etmek ve bununla ilgili mekanizmaları devreye almak ve sistemleri siber saldırı öncesine döndürmektir" (Kurnaz & Önen, 2019). Siber güvenlik, bilginin korunması ve kötüye kullanımına yönelik tedbirlerin alınmasıdır. Bu kavram hem bireysel hem kurumsal bakış açısıyla önemsenen ve incelenmesi gereken bir konu olmuştur. Değişen ve gelişen bilgi toplumu kavramıyla birlikte de siber güvenlik kavramı hayatımıza girmiştir. Dijital imkânların kurum, devlet gibi ortamlarda kullanılmasıyla birlikte bilginin korunmasından kullanılmasına sağlanmasından saklanmasına kadar olan süreçte alınması gereken tedbirler bütünüdür.

Solmaz'ın(2023) çalışmasından yola çıkarak; siber güvenliğin ortaya çıkması bilgisayar teknolojilerinin yaygınlaşmasına bağlı kalmaktadır. 1980'lerde kişisel bilgisayarların artmasıyla birlikte kötü amaçlı yazılımlarda artışlar görülmektedir. İnternetin ilk büyük saldırısı Morris Solucanı ile yapılmıştır ve birçok bilgisayarı ve ağları ele geçirilmiştir. Bu olayla birlikte bilgi güvenliğine karşı farkındalık oluşmaya başlamıştır. Önlemlerin geliştirilmesi gerçeği ortaya çıkmıştır ve 1990'larda internetin yaygınlaşması ve bilgisayarların artmasıyla birlikte siber güvenlik tehditleri de artmaya başlamıştır. Web siteleri, sosyal ağlar güvensiz hale gelmiştir. Bunun için güvenlik yazılımları oluşturulmuştur. 2000'ler ve sonrasında siber saldırılar daha karmaşık hale gelmiştir. Bilginin güç olduğu bilinci tam oturduğundan veri ihlalleri ve fidye yazılımları artmıştır. Buna karşılık olarak da siber güvenlik bir disiplin haline gelmiştir. Şirketler ve kurumlar siber stratejilerini gözden geçirerek daha gelişmiş hale getirmek için çabalamışlardır. 2010'larda nesnelerin interneti, mobil erişimler, bulutlar yaygınlaşarak siber güvenlik alanında farklı fırsatlarla birlikte zorlukları da beraberinde getirmiştir.

Şekil 9

Güvenlik ilişkisi

Microsoft'un açıklamalarında iki milyar insan internet kullanmaktadır. 2025 yılına kadar iki katından fazla olması beklenmektedir. Bu durumda kullanıcı sayısı bir ağ üzerinde ne kadar artarsa güvenlik önlemlerinin de o denli artması gerekmektedir. Dolayısıyla Siber güvenlik gerekliliği ortaya çıkmıştır (Yılmaz ve diğer.,2015). Teknolojik gelişmelere paralel

olarak da sistemlerin kalabalık oluşu ve güvenlik tedbirleri bu sebeple artışa geçmiştir. Zararlı kodların ortaya çıkmasıyla yıllar geçtikçe siber güvenlik süreçlerinde değişiklikler olmuştur. TÜBİTAK'ın yaptığı açıklamalarda siber saldırıya maruz kalan sistemler; bilgi sistemleri, iletişim sistemleri, denetleme ve kontrol merkezleri, veri toplama sistemleri, dağıtık kontrol sistemleridir. Bakıldığında bireysel veya kurumsal verilere yönelik saldırılar görülmektedir. Bu durumu özetleyen bir kavram vardır. Bu kavram siber tehdittir (TÜBİTAK, 2024).

Siber tehdit, bilgi sistemlerine veya ağlara karşı gerçekleştirilen kötü niyetli eylemleri tanımlayan bir kavramdır. Siber tehditleri diğer tehditlerden ayıran özellik siber uzayda da karşılaşılacak olmasıdır. Siber uzayda ortaya çıkan bir saldırının tahmin edilmesi, bulunması ve önlem alınması oldukça zordur. Buna rağmen siber güvenlik kapsamındaki çalışmalar ve yasal düzenlemeler yapılmakta ve yaygınlaştırılmaktadır.

Siber güvenlikle birlikte işletmelerin finansal bilgi sistemlerinin korunması da sağlanmıştır. Denetim sağlayan kurumların denetim yaptıkları bilgilerin de uygun ortamlarda saklanması ve güvenliğinin sağlanması gerekmektedir. Bu bilgilerin siber güvenlik ihlallerine uğramaması için kontroller yapılmıştır. Bu ve benzeri çalışmalar siber güvenlikte uluslararası çalışmaların politikalarında da gelişmeler olduğunun habercisi olmuştur. Uluslararası ilişkilerde siber alanda yapılan gelişmeler küresel anlamda da ilerlemelerin olduğu anlamına gelmektedir. Uluslararası politikaların tekrar ele alınması ve geliştirilmesi için gerek hukuksal gerek akademik çalışmalar ile daha da detaylandırılmıştır. Bu çalışmalar sonucunda siber güvenliğin daha iyi anlaşılabilmesi için; sibernetik gibi siber terörizm gibi siber caydırıcılık gibi siber savaşlar gibi kavramların ilişkilendirilmesi gerekmektedir. Sibernetik, canlı ve yapay sistemlerin kontrol ve iletişim süreçlerini inceleyen disiplinler arası bir bilim dalıdır. Bu bilim dalı organizmalardan makineye kadar farklı sistemlerin bilgi işleme ve kontrollerinin nasıl yapıldığıyla ilgilenir. Sibernetik yönetimlerde gelişmiş bir bilgi ağı içinde karar alma, bilgi aktarımı, bilişsel unsurlar olarak hepsini ele alabilen interdisipliner bir yapıdadır. Sibernetik bilginin, bilgi teknolojileri ile daha kapsamlı hale gelmesi ve karar alıcıların siber güvenlik çerçevesinde yönetmelerine katkı sağlamaktadır (Güntay, 2017).

Siber güvenlik her alanla etkileşim içinde olması bilginin her yerde yönetilmesi gerekliliğiyle bağlantılıdır. Siyasette, ideolojik hedeflerde kasıtlı ve zarar vermek amacıyla yapılan kapsamlı sistemlere siber terörizm denmektedir. Siber terörizm bilgisayar ağlarını bozmaya yönelik kasıtlı eylemlerdir. Saldırı denilince akla gelen geniş anlamda can ve mal tehdidine ek olarak sosyal, dini, ideolojik, politik veya başka amaçlarla bilgisayar ağlarına yapılan saldırılar siber terörizm kapsamına girmektedir (Güntay, 2017). Siber terörizmin asıl amacı, sistemlere sızarak kontrolü ele geçirmek, veri hırsızlığı yaparak manipülasyonu artırmak, fiziksel zarar vermek ve uluslararası gerginliklere sebep olmaktır. Siber terörün klasik terörden farkı aşağıdaki tabloda belirtilmiştir. Siber terör daha çok gizlilik ve zarar veren yazılım odaklı çalışmalardır. Ağ güvenliklerindeki sorunlar, yazılım güncellemelerindeki sorunlarla birlikte daha ulusal ve uluslararası çalışmaları destekler niteliktedir.

Tablo 2

Klasik Terör-Siber Terör Farkı

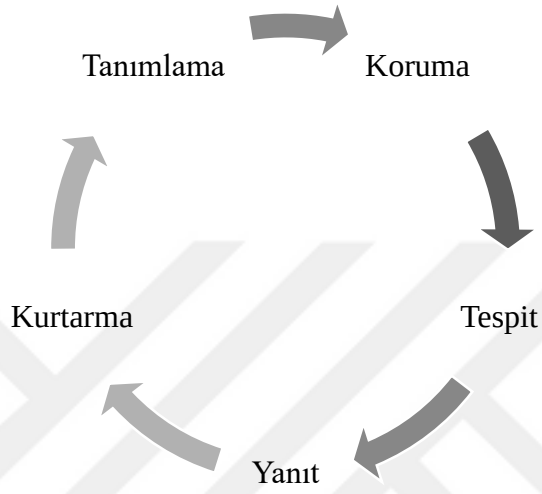
Klasik Terör	**Siber Terör**
Fiziksel şiddet kullanılarak gerçekleştirilir.	Dijital ve sanal ortamda gerçekleştirilir.
Fiziksel saldırı araçları (silahlar, bombalar, kimyasal maddeler) kullanılır.	Bilgisayar korsanlığı, kötü amaçlı yazılım, fidye yazılımı, DDoS(Dağıtık Hizmet Reddi Saldırıları) saldırıları, phishing ve sosyal mühendislik gibi dijital teknikler kullanılır.
Saldırıyı yapan gruplar yaşamsal risk altındadır.	Yaşamsal riski bulunmadan uzaktan etkili bir saldırı yapılabilir.
Terörü kontrol etmek, uzaklaştırmak, izlemek kısmen mümkündür.	Siber teröristleri tespit etmek, kontrol altında tutmak, yok etmek imkânsıza yakın zordur.
Güvenlik güçleri, istihbarat ajansları, askeri operasyonlar ve terörle mücadele yasaları gibi yöntemlerle mücadele edilir.	Siber güvenlik önlemleri, ağ güvenliği, yazılım güncellemeleri, eğitim ve farkındalık artırma, ulusal ve uluslararası işbirlikleri ile mücadele edilir.
Fiziksel şiddet kullanılarak gerçekleştirilir.	Dijital ve sanal ortamda gerçekleştirilir.
Fiziksel saldırı araçları (silahlar, bombalar, kimyasal maddeler) kullanılır.	Bilgisayar korsanlığı, kötü amaçlı yazılım, fidye yazılımı, DDoS(Dağıtık Hizmet Reddi Saldırıları) saldırıları, phishing ve sosyal mühendislik gibi dijital teknikler kullanılır.
Saldırıyı yapan gruplar yaşamsal risk altındadır.	Yaşamsal riski bulunmadan uzaktan etkili bir saldırı yapılabilir.

Siber caydırıcılık, siber saldırıları önlemek veya azaltmak amacıyla çeşitli strateji ve politikaların uygulanmasıdır. Amacı, potansiyel saldırıları ve saldırganları siber saldırıdan vazgeçirmek ve önlem almaktır. "Caydırıcılık bir devlet veya topluluğun, başka bir devlet veya topluluğun aleyhine olabilecek hareketlerden sakınması için gerekli tedbirleri almasıdır" (Güntay, 2017). Siber caydırıcılık, hem teknik hem stratejik önlemler içerir. Caydırıcılık amaçları için bilgisayardaki işlemleri ve yapan kişiyi tespit etmek sadece yeterli gelmeyebilir. Bunun için titiz bir araştırma, hukuki bir deneyim ve sorumlu olan kişilerin tespiti çok önemlidir. Bu kısımda da zamanlama ön plana çıkmaktadır. Siber güvenlik sağlanması için eş zamanlı olunmasına gerek yoktur. Her an her dakika kontrollü olmak gerekmektedir. Bu durumlarda değerlendirildiğinde siber tehditler değişirken siber güvenlik çeşitleri de oluşmaktadır. Değişkenlikler olurken siber caydırıcılıklarda hedefler aynı kalmaktadır. Bu durum da dezavantajlıdır. Saldırının ne denli büyük olabileceği, yıkıcılığı öngörülemeyecek derecede olabilir. Caydırıcılıklarda da değişik hedeflerin belirlenmesi daha avantajlı olacaktır (Singer & Friedman, 2018).

Siber savaşlar, devletler arsında gerçekleşen, bilgisayar ağları, düzeni ve dijital altyapılar üzerinde yürütülen saldırı odaklı çalışmalara denilir. Siber savaşın amaçları, bilgi sistemlerini ele geçirmek, iletişim ve ekonomik altyapıları bozmak ve hasar vererek yok etmektir. Ulusal ve uluslararası veri akışlarında artık bu durum oldukça yaygındır. Güntay(2017), makalesinde siber savaş hakkında bazı değerlendirmelerde bulunmuştur. Siber savaşlar gerçektir. Siber savaşlar artık ışık hızı kadar hız kazanmıştır. Saldırının etkisi düşünüldüğünden daha fazladır. Geleneksel savaş anlayışından daha hızlı ve önce gelmektedir. Siber savaşlar bilgi teknolojilerindeki gelişmeyle birlikte bugünkü küreselliğini korumaktadır. Siber savaşların gerçekleşmesiyle birlikte de siber suçlar daha yaygınlaşmıştır. Bilgi savaşlarıyla siber savaşların kesişimi daima siber zorbalıklar, siber savaşlar, siber terörizmler olmuştur.

Şekil 10

Siber güvenlik döngüsü



Yukarıdaki şekilde de siber güvenlik döngüsü ele alınmıştır. Siber güvenliğin bilgi güvenliği çerçevesinde değerlendirilmesi, tasarlanması, uygulamaya geçirilmesi, denetim uygulanması adımlarıyla bir döngü içinde olması tamamen bilgi sistemlerinin ve bilgi güvenliğinin sağlanması içindir. Bu sebeple siber güvenlik süreci yorumlanarak yukarıdaki şekil oluşturulmuştur. Veri akışında risklerin ve güvenlik açıklarının belirlenmesiyle başlayan siber güvenlik döngüsü, güvenlik duvarları, koruyucu yazılımlar, şifreleme, erişim kontrolleri gibi önlemler alınarak devam edilir. Güvenlik protokollerinin oluşması ve protokoller için çaba gösterilir. Veri kullanıcıları ve kurum çalışanları bilgilendirilir ve eğitim verilir. Olası ihlallere karşı saldırı sistemlerini algılayabilecek sistemler kurulmalıdır. Güvenlik tehditlerinin sürekli izlenerek hızlı bir şekilde yanıt verecek uygulamalar olmalıdır. Güvenlik ihlallerine müdahale edilerek hızlı aksiyon alabilmek bu konuda mühimdir. Kurtarma planlarının da olması gerekir. Siber güvenlik prosedürleri ve politikaları güncellenerek gözden geçirilmelidir.

3.1. Siber Güvenliğin Önemi/Gerekliliği

Her devlet, bilişim ağlarını, tüm bilişim sistemlerini siber saldırılardan muhafaza etmek ve elinde bulunan verilerin güvenliğini sağlamak için bir siber güvenlik stratejisi geliştirmek durumundadır. Siber güvenlik, dijital dünyayla birlikte işletmelerin, devletlerin, kurum ve kuruluşların bilgi ve dijital sistemlerini koruması için önemlidir. Günümüzde finansal işlemler, kişisel iletişim, devlet altyapıları ve daha birçok işlemler dijital platformda gerçekleşmektedir. Bu platformların güvenliği, erişilebilirliği ve bütünlüğünü sağlamak önemlidir ve gereklidir. Siber saldırılar sadece ekonomik zararlara uğratmaz. Aynı zamanda da ülkelerin itibar kaybına da sebep olmaktadırlar. Dolayısıyla ulusal güvenlik risklerine yol açmaktadır. Güçlü bir siber güvenlik politikası ve altyapısıyla saldırılara karşı tedbirler alarak, tehditler önlenerek bireylerin ya da kurumların güven faaliyeti göstermeleri sağlanabilmektedir. Sürdürülebilir ve inovasyonlara açık olan siber güvenlik alanı başarıyı yakalaması için varlığını sürdürmesi gerekmektedir.

Kişiselden devlet boyutuna, güvenlik ihtiyacının daha fazla hissedildiği bir dünyada güçlü ve bağımsız bir devlet olabilmenin önemli şartlarından bir tanesi, çevresindeki siyasi, askeri, ekonomik vb. gelişmeleri yakından takip edebilmektir. Bunlara karşılık harekete geçmek ve teknolojik gelişmelerin getirisi olan sanal dünyaya, ağ yapılarına, sistemsel olan her şeye hâkim olmaktır (Özdemirci & Torunlar, 2018). Günümüzde güvenliğin, bağımsızlığın, özgürlüğün, güçlülüğün rakip ağlarda nelerin olduğu nelerin dolaştığı ve nelere ilgi duyulduğu ile alakalıdır. Bilgileri toplamak için ağlar, internetin olduğu her ortam uygun ortamlardır. Bu durumda da küreselleşen düzende siber güvenliğin erişilebilir ilkesine dayanarak bilgilerin kullanımına izin verilirken kontrol edilerek de güvenliğinin sağlanması gerekliliği ortaya çıkmaktadır. Bu yüzden siber güvenlik, dijital dünyada güvenliği sağlamak için gereklidir. İnternet ve teknolojinin hayatımızda yer edinmesiyle birlikte kişisel ve kurumsal bilgilerin, ulusal bilgilerin sınırları vardır. Bunların korunması için belirlenen sınırlar çerçevesinde güvenlik sistemlerinin olma zorunluluğu ortaya çıkmıştır. Dijital teknolojilerin artmasıyla birlikte tehditlerdeki artış ve karmaşıklık da artmaktadır. Yapılan siber saldırılar kritik altyapıları, ulaşım, sağlık, bilgi merkezlerinde hizmetin kesintiye uğramasına sebep olmaktadır. Bu durumda siber güvenlik önlemleri alındığında toplumun ve ekonominin güvenli, sürdürülebilir bir şekilde ilerlemesini sağlamaktadır.

Siber güvenlik, dijital verilerin ve sistem güvenliğini sağlamayı amaçlayan bir disiplindir. Şirketler veya bireyler hassas olabilecek bilgilerini dijital ortamda saklarken dikkat edilmesi gereken kurallar vardır. Bu kurallar siber güvenlik kapsamına girmektedir. Siber güvenlik, kişisel verilerin gizliliğini sağlamak için gereklidir. Kimlik hırsızlığına karşı korunmak için siber güvenlik gereklidir. Şirketlerin ticari sınırlarının ve yenilikçi fikirlerinin çalınması, rekabet ortamlarını kaybetmelerine neden olan saldırılara karşılık bu tür bilgilerin güvenliğini sağlamak için gereklidir.

Ulusal güvenliğin sağlanması için ve ulusal savunma stratejilerinde siber güvenlik öncelikli konulardandır. KTÜ'nün yapmış olduğu bir araştırmada özellikle bu konulara değinilmiştir. Araştırmada üniversite öğrencilerine yapılan anketler sonucunda şimdiye kadar siber sorun yaşayan kişilerin oranı %86 çıkmıştır. Bakıldığında çok büyük olan bu oran siber güvenliğin sağlanamadığı ve önlemlerin yeterli olmadığını ortaya çıkarmıştır. Buna ek olarak Buna ek olarak siber güvenlik kavramının kullanıcılarda korku ve endişeye sebep olduğu da gözlenmiştir. Siber algının tam manada yerleşmemesi ve buna ek olarak eğitimlerin yapılması gerekliliği ortaya çıkmıştır. Siber güvenliğin önemli bir konu olup olmadığına dair sorularda ise; %96 oranında önemli görüldüğü ortaya çıkmıştır (Eroğlu vd., 2018). Araştırma sonucunda daha geniş bir siber güvenlik çalışması yapılarak farkındalık oluşturulması gerekliliği ortaya çıkmıştır.

Siber güvenlik, şirketlerin, devletlerin, bireylerin dijital dünyada güvenli bir şekilde faaliyet gösterebilmeleri için vazgeçilmez bir uygulamadır. Bilgi çağında siber tehditlerin artması, siber saldırıların sayısının artması ile birlikte siber güvenlik alanına yapılan yatırımlar da artmıştır. Bu sebeple de siber güvenliğe verilen önem de artmıştır.

3.2. Siber Güvenlik Protokolleri

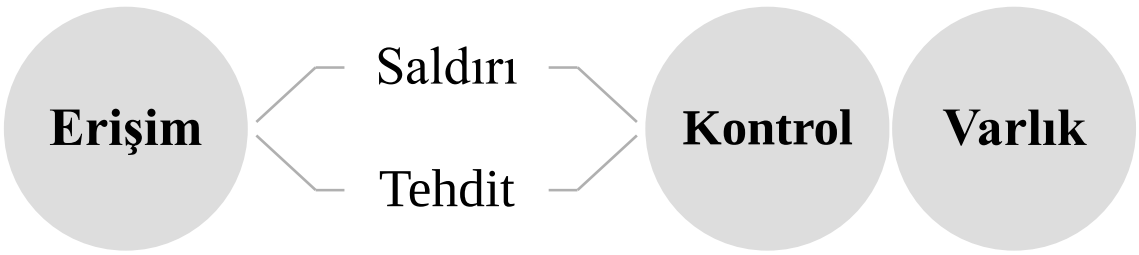
Siber güvenlik protokolleri, bilgi sistemlerinin korunması amacıyla geliştirilen kurallar, standartlar, prosedürler ve yöntemler bütünüdür. Bu belirlenen prosedürler, protokoller siber güvenlik uzmanları tarafından kullanılıp uygulamaya geçirilir. Siber

güvenlik protokollerinden bazıları; ağ güvenlik protokolleri, kimlik doğrulama ve yetkilendirme protokolleri, veri şifreleme protokolleri, ağ erişim kontrol protokolleri, güvenli bilgi ve onay yönetimi, e-posta güvenliği protokolleri, veri yedekleme protokolleridir. Protokol seçimi ve uyumluluk için; kurumun, işletmelerin kendi ihtiyaçlarına ve risk profillerine uygun protokoller seçilmeli ve uygulanmalıdır. Siber güvenlik tehditleri sürekli değişime uğramasından protokollerdeki güvenlik önlemlerinin de düzenli olarak incelenmesi ve güncellenmesi gerekmektedir. Tek bir güvenlik protokolüne bağlı kalmadan çok katmanlı olabilecek güvenlik yaklaşımı benimsendiğinde daha az risk barındırır.

Acil durumlarda da risk yönetimi için acil durum ve kurtarma planları yapılmalıdır. Bu protokollerin uygun şekilde seçilmesi kritik öneme sahiptir. Siber güvenlik protokollerinin etkin bir şekilde kullanılmasına ve organizasyonların siber tehditlere karşı daha dirençli olmasına yardımcı olur. Bu kullanımın etkin olabilmesi için, risk değerlendirmesi ve yönetiminin gerçekleştiriliyor olması gerekmektedir. Yazılım ve donanım güncellemelerinin düzenli yapılıyor olması gereklidir. Bir siber saldırı durumunda hızlı ve etkili bir şekilde müdahale edebilmek için olay müdahale planlarının hazırlanması ve olaylara müdahale ekiplerinin eğitilmesi beklenmektedir. Mevcut yasal düzenlemelere ve sektör standartlarına uyumluluğun sağlanması için düzenli olarak iç denetim ve dış denetim gerçekleştirilmesi gerekmektedir. Ayrıca siber güvenlik protokollerinde etkin kullanımın nasıl olması gerektiği bilgisi de Şekil 11' de belirtilmiştir. Protokollerden verim alabilmek için bazı şartlar vardır.

Şekil 11

Siber güvenlik protokollerinin etkin kullanımı



Erişim yönetimi, belirli kullanıcıların kullandığı sistemlere ve bilgi erişim süreçlerini denetler. Erişim kontrol protokolleri, kimlik doğrulama yaparak hangi kaynaklara nasıl erişileceğini belirler. Bu protokoller kullanıcıların ve cihazların ağ ve sistemlere erişim haklarını belirleyen politikalar oluşturur. Erişim yönetimi, kullanıcıların ve sistemlerin doğru verilere erişimini sağlamak için kullanılırken, siber güvenlik protokolleri bu erişimin güvenli bir şekilde sağlanmasını ve verilerin korunmasını garanti eder. Bu iki alanın entegrasyonu, hem kimlik doğrulamanın hem de veri iletiminin güvenli bir şekilde gerçekleşmesini sağlamaktadır.

Varlık yönetimi, şirketlerin, kurum ve kuruluşların sahip olduğu donanımları, yazılımları ve sistemlerin güvenliğini sağlar. Korunması gereken cihazların envanter listesi tutulur ve bunlara uygun güvenlik politikaları oluşturulur. "Varlık yönetimi, bir organizasyonun sahip olduğu tüm bilgi teknolojileri varlıklarının (donanım, yazılım, veri, ağ cihazları vb.) envanterini çıkarır ve takip eder" (Karayel & Akbıyık, 2023). Bu envanterler, güvenlik protokollerinin hangi varlıklara uygulanacağını belirlemek için gereklidir. Her varlığın güvenlik gereksinimleri farklı olabilir, bu nedenle varlık yönetimi ile güvenlik önlemlerinin uyumlu hale getirilmesi önemlidir.

Saldırı tespiti ve yanıt protokolleri, sistemlere yapılan saldırıların tespitini yapmak ve yanıt vermek için kullanılan protokollerdir. Saldırı tespiti ve önleme bu saldırılara karşı savunma sağlamaktadır. Bu protokoller, sistem ve ağ güvenliğini sağlamak için kullanılmaktadır. Saldırı tespiti ve yanıt protokolleri, bir kuruluşun siber saldırılara karşı savunma yeteneklerini artırmak için kritik öneme sahiptir. Bu protokoller, potansiyel tehditlerin erken tespit edilmesini ve bu tehditlere etkili bir şekilde yanıt verilmesini sağlamaktadır.

Kontrol, sistemlerin güvenliğini sağlamak için alınan teknik ve idari önlemlerdir. Risklerin azaltılması için gerekli bir adımdır. Aynı zamanda kontrol, kullanıcıların ve sistemlerin kaynaklara erişim haklarını yönetir. Kontrol aşaması, siber güvenlik

protokollerinin uygulanmasında kritik bir rol oynar. Bu aşama, güvenlik önlemlerinin etkinliğini değerlendirir, denetler ve gerektiğinde iyileştirme sağlar.

Tehdit yönetimi, bir organizasyonun karşılaşabileceği potansiyel siber tehditleri tanımlamak, analiz etmek, önlemek ve yanıtlamak için kullanılan süreçler ve stratejilerdir. Olası güvenlik tehditlerini tanımlamak, analiz etmek ve yönetmek için kullanılır. Tehditlerin azaltılması ve yönetilmesi sürecidir. Bunun için uyun stratejiler geliştirir. Her bir kavram, siber güvenliğin farklı bir yönünü ele alarak genel güvenlik stratejisinin bir parçası olarak hizmet eder. Tehdit yönetimi, potansiyel tehditleri tanımlamak ve onlara karşı önlemler geliştirmek için geniş bir yaklaşımı ifade ederken, siber güvenlik protokolleri bu tehditlere karşı koruma sağlayan spesifik teknikler ve standartlardır. Tehdit yönetimi sürecinde kullanılan protokoller, organizasyonların karşılaştığı tehditlere karşı daha etkili bir savunma oluşturur ve bu iki alanın entegrasyonu bilgi güvenliğini artırır.

Siber güvenlik protokollerinin etkin bir şekilde uygulanabilmesi için çeşitli gereksinimlerin karşılanması gerekir. Bu gereksinimler, teknolojik altyapıdan insan faktörlerine kadar geniş bir yelpazede ele alınmalıdır. “Güvenlik protokollerinin etkin kullanımı için gerekli olan ana unsurlar; güçlü bir altyapı, yazılı güvenlik politikaları, erişim kontrolü, çok faktörlü kimlik doğrulama, çalışan eğitimleri, tatbikatlar ve eğitimler, veri şifreleme, yedekleme, ağ güvenliğidir” (Solmaz, 2023). Eğitimler, kimlik avı (phishing) gibi temel tehditlerle başa çıkma ve güvenli internet kullanımı konularında bilinç oluşturmaya yönelik olmalıdır. Ayrıca; teknoloji tarafında, güncel antivirüs yazılımları, güvenlik duvarları ve veri şifreleme gibi teknolojik önlemler alınmalı ve yazılım güncellemeleri düzenli olarak yapılmalıdır. Erişim kontrolü ve kimlik doğrulama süreçlerinin güçlendirilmesi, sistemlere yalnızca yetkili kişilerin erişmesini sağlar. Siber güvenlik olaylarına hızlı yanıt verebilmek için etkili bir acil durum planı ve olay müdahale süreci oluşturulmalı, bu süreçler düzenli olarak test edilmelidir. Bu adımların tamamı, siber güvenlik protokollerinin etkin bir şekilde uygulanmasını ve kurumun siber tehditlere karşı sağlam bir savunma hattı oluşturmasını sağlar.

4. BİLGİ GÜVENLİĞİ ve SİBER GÜVENLİĞİ ARASINDAKİ İLİŞKİ

Dijital çağda, bilgi güvenliği ve siber güvenlik, bilgi teknolojilerinin korunması ve saklanması açısından önem taşımaktadır. Bu iki kavram birbiriyle yakından ilişkilidir. Bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenli bir şekilde iletilmesi bilgi güvenliğidir (Demirtaş, 2013). Günümüzün vazgeçilmez parçası olan bilgi işlemlerinde bilginin işlenmesi, gizliliği, özgünlüğü, bütünlüğü daima risk altındadır. Bu risklerin analizinden korunma yöntemlerine kadar uygulanan politikalar, süreçler bütünü olan bilgi güvenliğidir. Bilgi sistemlerini, ağları, programları verileri ve veri yönetim sürecini dijital dünyanın risklerine karşı korumayı hedefleyen teknik kontroller barındıran savunma mekanizmaları da siber güvenliktir.

Bilgi güvenliği, her türlü bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlamaktadır. Bu durum hem dijital hem de fiziksel bilgi varlıklarının korunmasını içermektedir. Siber güvenlik ise daha spesifik olarak dijital ortamlarda, özellikle internet üzerinden gelen tehditlere karşı sistemlerin korunmasıyla ilgilenmektedir. "Bilgi güvenliği, bir kurumun sahip olduğu tüm verilerin korunmasını hedeflerken, siber güvenlik bu verilerin internet gibi dış kaynaklı tehditlerden korunmasına odaklanmaktadır" (Yılmaz vd.,2015). Bu bağlamda, siber güvenlik, bilgi güvenliğinin bir alt kümesi olarak düşünülebilir çünkü dijital tehditlere karşı savunma sağlar. Örneğin, bir şirketin sunucularını fiziksel ve dijital tehditlere karşı koruma stratejileri bilgi güvenliğine girerken, bu sunuculara yapılabilecek siber saldırılara karşı alınan önlemler siber güvenliğin kapsamına girmektedir

Bilgi güvenliği ve siber güvenlik arasındaki ilişki ise aşağıdaki tabloda karşılaştırmalı olarak ele alınmıştır. Sağıroğlu ve Akleylek'in (2022) siber güvenlik ve tehdit bilgisine dair yapmış olduğu bölümde bilgi güvenliği ve siber güvenlik üzerine detaylıca durulmuştur. Ayrıca ISO 27001 Standardından da yola çıkılarak aşağıdaki tablodaki karşılaştırma incelenebilir.

Tablo 3

Bilgi Güvenliği-Siber Güvenlik Karşılaştırması

	Bilgi Güvenliği	**Siber Güvenlik**
Kapsamı ve Odak Noktaları	Daha geniş bir kapsamı vardır. Tüm bilgi türlerinin korunmasını sağlar. Her türlü bilgi varlığı bu kapsamda değerlendirilir.	Dijital olabilecek tüm bilgi varlıklarının ve sistemlerinin korunmasına odaklanır. Bu nedenle de bilgi güvenliğinin bir alt kümesindedir denilebilir.
Yaklaşımlar ve Stratejiler	Uyumluluk, risk yönetimi, politika geliştirme ve eğitim gibi geniş bir strateji sürecini içerir. İnsan faktörü ve organizasyon olabilecek süreçlere odaklanır.	Teknik ve savunma mekanizmaları üzerinde yoğunlaşır. Güvenlik duvarları, koruyucu yazılımlar, kontrolsüz girişleri engellemek için çözümler kullanır.
Tehdit ve Risk Yönetimi	Her türden tehdide odaklanır ve değerlendirir. Fiziksel, insan kaynaklı ve dijital riskler olabilir. Bunun için risk yönetim süreçleri ve politikalar geliştirir.	Dijital tehditlere odaklanır. Siber saldırılar, kötü amaçlı yazılımlar, veri ihlalleri, siber tehditler gibi süreçleri tespit edip önlenmesini sağlamak ve yöntemler geliştirmektir.
Uyumluluk ve Düzenleyici Çerçeveler	Bilgi koruma yasalarına, prosedürlere, ve standartlara uyumu sağlar.	Özel olarak siber güvenlik yasalarına ve düzenlerine uyumu sağlar.

Bilgi güvenliği ve siber güvenlik, modern organizasyonların bilgi ve teknoloji varlıklarını korumak için kritik öneme sahip iki farklı disiplindir. Bilgi güvenliği, genel bir koruma stratejisi sunarken, siber güvenlik, dijital dünyadaki spesifik tehditlere karşı savunma sağlar. Bilgi güvenliği söz konusu olduğunda, güvence altına alınacak varlıklar, teknolojiler ve bilgidir. Her iki alanın entegrasyonu, bütüncül ve etkili bir güvenlik stratejisi oluşturmak için gereklidir. Bu nedenle, organizasyonlar hem bilgi güvenliği hem de siber güvenlik önlemlerini benimsemeli ve uygulamalıdır. Bu şekilde riskler kontrol edilebilir hale getirilir, iş sürekliliği sağlanır, yasal kriterler belirlenmiş olur. Kurumsal güven ve saygınlık kazanılmış olur.

Kurumların elektronik ortamdaki verdikleri hizmetlerle değişime uğraması bilgi toplumunun gerekliliklerinden olan elektronik ortamlar yaygın hale gelmektedir. Geleneksel devlet anlayışından e-devlet anlayışına geçişler görülmektedir. "E-devletten yüz yüze görüşerek dilekçe yazma, form doldurma, evrak tamamlama gibi faaliyetleri içerirken e-devlette elektronik ortamda yapılabilmektedir" (Yılmaz vd., 2015). Bu verilen hizmet lerin güvenliği sağlanırken kurum kültürü haline gelerek de daha deteylı güvenlik sistemlerinin ve prosedürlerinin oluşması için siber güvenlik gerekliliği ortaya çıkmaktadır. Bu sebeple doğan her bilgi ihtiyacı bilginin güvenliğini gerektirdiği gibi siber güvenlik önlemlerini de gerektirmektedir.

4.1. Bilgi Güvenliğinde Siber Güvenliğin Gerekliliği

"Bilgi güvenliği, elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür" (Demirtaş, 2013). Bilginin işlenmemiş ama yönetilmesinde gereklilik görülen veri ve güvenliği için; "Veri güvenliği ancak, veri güvenliğinin bozulmasına sebep olan ya da olabilecek risk ve tehditlerin tayin edilmesi ve yönetilmesi ile mümkündür. Sürekli izlenebilir ve ölçümlenebilir veri güvenliği, kurumsal risk yönetimi modeli ile belirlenmiş risklerin yönetimi ve yeni tehditlerin öngörülebilmesi ile sağlanmalıdır" (Korucu , 2021).

Bilginin günümüzde dijital ortamlarda yaygınlaşması ve bilişim sistemleriyle oldukça fazla paylaşılması, bilginin maruz kaldığı riskleri artırmakta ve bilgi güvenliği kavramına yeni bir boyut kazandırmaktadır. Bu süreç bilginin bir taraftan erişilebilir olmasını mesafelerin ve mekân kavramlarının ortadan kaldırılarak hizmet verilmesini sağlarken buna karşılık bilginin güvenliğini de sağlamak zorlaşmaktadır. Zorlaşan bu durumda da siber güvenliğin gerekliliği de ortaya çıkmaktadır. Dijital dünyanın değişim ve gelişiminde güvenlik önlemlerinde de değişimler olmuştur. Yenilikler yeni saldırı türelerini yeni tehditleri de beraberinde getirdiklerinden tüm organizasyonlar büyük ya da küçük ölçeklerde siber tehdit altındadır. Bu organizasyonların tehditlerine uygun tedbir almaları da şarttır.

Uzaktan erişimli çalışmalarda, bulut bilişimlerin yaygın olarak kullanımının olduğu organizasyonlarda veri güvenliği ve korunması zaruri haline gelmiştir. Bunun sebebi de kişisel verilerin yaygın olarak kullanılması, şifreleme işlemlerinin yapılması, kontrollerin de dijital ortamda yapılıp bulut yardımıyla erişime sunulması gibi süreçler bilgi güvenliğinin korunması ilkesine dayanarak siber güvenlik önlemlerini almak zorunluluk haline gelmiştir. "Uzaktan çalışma ortam şartları sebebi ile güvenlik farkındalığı azalan ve kurumsal güvenlik adımlarını benimsememiş kurum çalışanları üzerinde sosyal mühendislik yönelimlerinin etkisi artmıştır" (Korucu , 2021).

Bilgi güvenliğinin siber güvenlik tedbirleriyle birlikte sağlanması için yapılması gereken bazı değerlendirmeler vardır. Bu değerlendirmeler:

- Saldırılar neticesinde hukuki olarak da tedbirler alınmalıdır.
- Kurumların siber güvenlik alanından sorumlu çalışanlarının olması gereklidir. Görev ve yetkilendirmeler yapılmalı ve ihtiyaç duyulan bilgi eksikliklerinde de eğitimler verilmelidir.
- Zamanın teknolojik gelişimine ayak uydurarak teknik manada gelişim gösterilmeli ve donanımların güncellenerek en son sürümlerin olması gerekmektedir.
- Kapsamlı bir risk değerlendirmesi yapılarak risk yönetimi için planlar yapılmalı ve risk karşısında alınacak tedbirlerin belirlenmesi gerekir.
- Siber güvenlikle alakalı en güncel kaynakları ve uygulamaları takip ederek kurumların siber güvenlik uygulamalarına entegre etmek gerekir.
- Siber güvenlikle alakalı eylem planları hazırlandığında kurumda olan tüm çalışanlarla bu planlamaların paylaşılması gerekmektedir (Güngör & Güney, 2017).

Bu değerlendirmelerle birlikte bilgi güvenliği daha nitelikli olurken siber güvenliğin de bunu desteklemesi gereklidir. Bu duruma bütüncül bakış açısıyla bakmak önemlidir. Organizasyonlar bu bakış açısıyla yaklaştıklarında bilgi varlıklarını ve dijital altyapılarını en etkili şekilde koruyabilirler. Siber güvenliğin yaşayan bir süreç olarak ele alınması kurumlarda başarı getirecektir. Bu süreçte siber güvenlik oldukça önemlidir. Çünkü bilgi yönetimi, kurumların ve bireylerin değerli, hassas bilgilerini içermektedir. KVKK'ya göre

de belirli prosedürlerle bu bilgilerin saklanması ve korunması gereklilikleri vardır.

4.2. Bilgi Yönetim Sürecinde Siber Güvenlik Kullanımı

Bilgi yönetim sürecinde siber güvenlik kullanımı, bilgilerin toplanması, depolanması, işlenmesi ve paylaşılması sırasında ortaya çıkabilecek tehditlere karşı koruma sağlamak için alınan önlemleri ifade eder. Bilgi yönetim sürecinde; bilgi toplama, bilgi depolama, bilgi işleme, bilgi paylaşımı, bilginin imhası vardır. Bu süreçlerin siber güvenlik ile bütünleşmesi ise; veri gizliliğinin sağlanması, veri bütünlüğünün sağlanması, erişilebilir bir veri ve veri izlenebilirliğinin olmasını sağlamaktır. Veri izlenebilmesi, bilgi yönetim süreçlerinin şeffaf ve denetlenebilir olmasını sağlamaktır.

Bilgi yönetiminde siber güvenliğin amacı, kurumların dijital varlıklarını koruyarak bilgi güvenliğini sağlamak ve işletme sürekliliğini garanti altına almaktır (Özdemirci, 2019). Bu durum, siber tehditlere karşı savunma mekanizmaları oluşturarak veri ihlallerini önlemeyi ve bilgiye yalnızca yetkili kişilerin erişmesini sağlamayı içerir. Aynı zamanda, siber güvenlik, veri ihlallerini engelleyerek bilgilerin doğruluğunu korur ve sistemlerin kesintisiz çalışmasını sağlayarak iş süreçlerinin aksamasını önler. Böylece, siber güvenlik uygulamaları, bilgi yönetiminde hem güvenilirliği artırır hem de kurumsal itibarın korunmasına katkıda bulunur.

Bilgi yönetim sürecinde siber güvenlik, bilgilerin güvenliğini sağlamak için kritik bir rol oynar. Bu süreçte kullanılan siber güvenlik önlemleri, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korur. Bilgi toplama sürecinde, verilerin güvenli bir şekilde elde edilmesi ve toplanan bilgilerin güvenli bir şekilde depolanması önemlidir. Bu süreçte kullanılan siber güvenlik önlemleri şifreleme ve kimlik doğrulama gibi önlemler olabilir. Bilgi işleme sürecinde, bilgilerin güvenli bir şekilde işlenmesi ve analiz edilmesi güvenlik duvarları oluşturmak ve süreçlerin izlemesi yapılarak denetlenir. Bilgi dağıtımı sürecinde, bilgilerin güvenli bir şekilde iletilmesi ve dağıtılması önemlidir. Bu süreçte kullanılan siber güvenlik önlemleri veri şifreleme ve ağ güvenliğidir.

Verilerin evrimleşmesinde yönetim ve saklanmasında, işlenmesi ve aktarılmasında bağlı verileri bir değere dönüştürmek, veriyi kullanılabilir hale getirebilmek anlamına gelmektedir. Bu durum veriyi ekonomik manada da değerli hale getirmektedir. Sürecin bu şekilde ekonomik getiri olarak ilerlemesi ise ekstra kontrollere ve siber güvenlik protokollerinin uygulanmasını gerektirmektedir.

> Günümüz teknolojisi düşünüldüğünde bilgi ağlarının yapısı sadece bilgisayarlarla sınırlı kalmamakta, çeşitli sensörler ve gömülü bilgisayarlarla sınırlı kalmamakta, çeşitli sensörler ve gömülü elektronik sistemler de siber uzayın bir paydaşı olarak ortaya elektronik sistemler de siber uzayın bir paydaşı olarak ortaya çıkmaktadır. Bunun en güzel örneklerinden biri internete bağlı olan çıkmaktadır.(Ünal , 2018,s.385)

Siber güvenliğin internet ile bağlantısının, bilgi teknolojileri alanının gelişimiyle de paralel olduğu görülmektedir. Bilgi yönetim sürecinde siber güvenlik kullanımı, sadece teknolojik önlemlerle sınırlı olmayıp, aynı zamanda kurumsal politikalar, prosedürler ve insan faktörünü de içeren geniş kapsamlı bir yaklaşımdır. Bu nedenle, etkili bir bilgi yönetimi için kapsamlı ve bütünleşik bir siber güvenlik stratejisinin benimsenmesi gerekmektedir. Bilgi yönetiminde siber güvenlik uygulamaları bu süreçte gerekli olan adımlardır. Risk değerlendirmesi, potansiyel risklerin belirlenip değerlendirilmesini sağlar, Güvenlik politikalarının belirlenmesi, kurum içi bilgi güvenliği politikalarının oluşturulması ve uygulanmasını sağlamaktadır. Denetimler ve testler, bilgi yönetim süreçlerinin ve siber güvenlik önlemlerinin düzenli olarak denetlenmesi ve test edilmesini sağlamaktadır. Olay müdahale planlarında, olası siber durumlarına uygulanacak acil durum planlarının hazırlanması sürecidir.

Bilgi yönetiminde siber güvenliğin gerekliliği, sadece verilerin korunması değil, aynı zamanda iş sürekliliğinin sağlanması, yasal düzenlemelerin de yerine getirilmesi ve itibarın korunması açısından da kritik öneme sahiptir. Bilgi yönetim sürecinde siber güvenliğin sağlanması için kapsamlı stratejiler benimsenmelidir. Güvenli bir siber güvenlik stratejisi

sadece bilgi varlıklarını korumakla kalmaz, aynı zamanda bilgi yönetim sürecini de nitelikli hale getirir. Ayrıca, siber güvenlik, olası tehditleri önceden tespit ederek hızlı müdahale imkânı sunar, bu da bilgi yönetiminde proaktif bir yaklaşım geliştirilmesine yardımcı olur. Bilgi güvenliğinin sağlanması için siber güvenlik politikalarının ve en iyi uygulamaların hayata geçirilmesi gerekmektedir.

5. BİLGİ YÖNETİMİNDE SİBER STRATEJİLER

Bilgi yönetiminde siber stratejiler, bilgilerin güvenli, verimli ve etkin olmasını sağlamak için geliştirilmiş yaklaşımlardır. Bu stratejiler siber tehditleri ve önlemlerinin nasıl alınması gerektiğini kapsamaktadır. Temel stratejilerden bazıları; risk yönetimi, erişim kontrolü, siber farkındalık, izleme ve denetleme gibi stratejilerdir. Bu stratejiler, bilgi yönetiminde siber güvenliği sağlamak için bir araya getirilen kapsamlı bir yaklaşımdır. Bilgi yönetimi süreçlerinin her aşamasında siber güvenlik önlemlerinin alınması, verilerin korunması ve iş sürekliliğinin sağlanması açısından kritik öneme sahiptir. "Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür" (Baykara vd., 2013).

Bilgi güvenliği politikaları her kurum için aynı değildir. Her kurumun işleyişine göre güvenlik önlemleri, amaç ve hedefleri, kurallar ve uygulamalar değişik şekillerde belirlenir ve uygulanır. İyi bir siber güvenlik stratejisi kullanıcıların işini zorlaştırmaz ve uygulanabilir olmasıyla daha yaygındır. Buna bağlı olarak, bilgi organizasyonlarında atılan adımlar ve yenilenen hizmet anlayışıyla birlikte siber bağımlılık oranları artmaktadır. Siber güvenliğin sağlanması içim öncelikle bazı adımların sistemli olarak ilerlemesi gerekmektedir. Aksi takdirde siber risklerin boyutu büyür ve önlenemez hale gelebilir. Bunun için;

- Teknik tedbirlerin artırılması gerekir.
- Koruma yazılımlarının kurulması gerekir.
- Kurumsal yapılanmaların belirlenmesi gerekir.
- Farkındalık çalışmalarının artırılması ve oluşturulması gerekir.
- Yasal çerçevenin oluşturulması gerekir.
- Politika kapsamında çalışan tüm yetkililere sorumluk verilmeli ve yetkilendirmeler net bir şekilde yapılmalıdır.
- Ulusal ve uluslararası politikalar ve stratejilerin belirlenmesi gerekir.
- Uluslararası işbirliği ve uyum çalışmalarının yapılması gerekir (Yılmaz vd.,2015)

Bu yapılması gerekenlerin yanında siber güvenlik sürekli gelişim ve değişim içerisinde olduğundan denetlemelerin yapılması ve alınan önlemlerde de güncelleme

yapılması gerekmektedir.

5.1. Ulusal ve Uluslarası Siber Güvenlik Strateji ve Politikaları

Ulusal siber güvenlik strateji ve politikaları, bir ülkenin dijital varlıklarını ve altyapısını siber tehditlere karşı korumak amacıyla belirlenen genel çerçeveleri ve spesifik önlemleri kapsar. Bu strateji ve politikalar, hükümetlerin, kamu kurumlarının, özel sektörün ve toplumun genelinde güvenliği sağlamak için bir rehber niteliğindedir.

Dünya savaşlarından sonra bazı ülkeler savaş yöntemlerinde farklılık olması gerektiğini araştırmış ve soğuk savaş dönemi ile birlikte Amerika Birleşik Devletleri (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) kıyasıya rekabet oluşturmuştur. 1982'de ABD'nin SSCB'ye açtığı savaşla siber savaş boyut kazanmış ve siber savaşlar ortaya çıkmaya başlamıştır. Karşılıklı olarak kötü kaynaklı casus yazılımlarla ülkeler birbirinin ağlarına zarar vermeye veri açığı yakalamaya ve ifşalar oluşturmaya çalışmıştır. O günden bugüne de siber saldırı düzeyleri değişkenliğe uğramış ve hatta günümüzde sosyal medyanın etkisiyle, sanal paraların artmasıyla, Meta ve sanal ortamların artmasıyla da siber zorbalık ve siber saldırıların olduğu görülmektedir. Siber saldırılara karşılık ABD tedbirlerini de geliştirmiş ve uygulamaya almıştır. ABD aldığı önlemlerle birlikte ABD'nin sürekli değişen siber tehdit ortamına karşılık güvende kalabilmek için yaklaşım sergilemiştir. Siber güvenlikte uluslararası yelpazede bir diğer başarılı ülke de İsrail'dir. Coğrafi konumu ve çevre ülkelerle olan gerginlikleri sebebiyle de hedef haline gelmiştir. Faklı ülkeler İsrail'in teknolojik gelişimlerine karşılık sınırlar koymak istediklerinden siber saldırılar daha sıklıkla olmaktadır. Fakat bu saldırılara karşılık geliştirilen savunma planları, siber güvenlik stratejileri onları güçlü kılar (Arslan, 2023).

AB, ülkeler arasında varlığını sürdürürken siber güvenliğe olan ilgisini de artırmıştır. AB, dijital ekonomisini ve vatandaşlarının güvenliğini korumak için kapsamlı ve koordineli bir siber güvenlik politikası benimsemiştir. AB'nin siber güvenliğe bakış açısı, üye devletler arasında işbirliğini artırmak, siber tehditlere karşı ortak bir savunma mekanizması oluşturmak ve dijital altyapının güvenliğini sağlamak üzerine odaklanmıştır. Bazı siber

güvenlik yaklaşımları vardır. Bunlardan biri Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı/European Union Agency for Cybersecurity (ENISA)'dır. AB'nin siber güvenlik politikalarının geliştirilmesi ve uygulanması konusunda merkezi bir rol oynamaktadır. Ajans, üye devletlere, AB kurumlarına ve özel sektöre siber güvenlik konusunda teknik destek sağlar ve kapasite geliştirme faaliyetlerini yürütür. AB'nin siber güvenliğe bakış açısı, koordineli ve kapsamlı bir yaklaşımı yansıtarak hem ulusal hem de uluslararası düzeyde güçlü bir siber güvenlik ekosistemi oluşturmayı amaçlar. Bu strateji, teknolojik bağımsızlık, operasyonel kapasite, küresel işbirliği ve sürekli yenilikçilik üzerine kuruludur.

Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization/NATO)'nün soğuk savaş döneminden sonra üye ülkeleri tehditlere karşı korumak amacıyla birçok politika ve strateji geliştirmiştir. NATO'nun siber güvenlik stratejilerinin ana hatlarını; Siber Savunma Politikası ve Stratejisi, NATO Bilgisayar Olaylarına Müdahale Ekibi (NCIRC), Siber Savunma Eğitim ve Tatbikatları gibi çalışmalar oluşturmaktadır. NATO'nun siber güvenlik stratejileri, ittifakın dijital dünyadaki güvenliğini sağlamak için kapsamlı ve çok yönlü bir yaklaşım benimser. Bu stratejiler, siber tehditlere karşı proaktif savunma, üye devletler arasında işbirliği ve bilgi paylaşımı, kritik altyapıların korunması ve uluslararası işbirliğini teşvik etmeyi hedefler. Bu sayede, NATO'nun kolektif savunma kabiliyeti ve üyelerinin siber güvenlik kapasiteleri sürekli olarak geliştirilmektedir (Güntay, 2016).

5.2. Türkiye'nin Siber Güvenlik Strateji ve Politikaları

Türkiye'nin Siber Güvenlik Strateji ve Politikaları, ülkenin dijital varlıklarını ve altyapısını siber tehditlere karşı korumak, siber güvenlik farkındalığını artırmak ve ulusal siber savunma yeteneklerini geliştirmek amacıyla oluşturulmuştur. Bu strateji ve politikalar, çeşitli kurumlar ve düzenlemeler aracılığıyla uygulanmaktadır. Siber güvenlik politikalarının geliştirilmesi ve uygulanmasında, kamu ve özel sektör iş birliğinin de büyük bir önemi bulunmaktadır. Bunun yanında Türkiye dijital gelişimini, teknolojik adımlarını hızlandırmakta ve jeopolitik konumundan dolayı da siber tedbirlerini geliştirmek zorundadır.

Türkiye'nin siber güvenlikle ilgili belirlediği strateji ve politikalar önleyici ve tepkisel

yaklaşımlıdır. Türkiye'nin siber güvenlik politikasının bazı temellere dayandırıldığı görülmüştür. Bu alanlar; kritik altyapının korunması, Farkındalık ve eğitim, Araştırma ve Geliştirme, Uluslararası Normlar ve Standartlar olmak üzere dört tanedir (Arslan, 2023). Bu strateji ve planların verimli bir şekilde uygulanabilmesi için organizasyonlar gereklidir. Bu amaçla koordine edecek bazı kurum ve kuruluşlar oluşmuştur. Bu kurumlar BTK, TÜBİTAK'dır (Arslan, 2023). Siber güvenlik kapsamındaki çalışmalar, 2012 yılına kadar Bilim Teknoloji ve İletişim Kurumu (BTK) tarafından yürütülmüştür. BTK siber alanda düzenleyici ve denetleyici rol alır. Bu kapsamda siber güvenlikle alakalı mevzuatın oluşturulması, uygulanması, denetlenmesi BTK' nın hizmetleri arasındadır. Kurum genellikle sektörde faaliyet gösteren şirketlerin siber güvenlik standartlarına uyumlu olup olmadıklarını kontrol eder. BTK, siber güvenlik farkındalığını artırmak ve insan kaynaklarını geliştirmek amacıyla eğitim programları ve farkındalık kampanyaları düzenler. Siber güvenlik konusunda bilinçlendirme çalışmaları yaparak farkındalıkları artırır. BTK Akademi gibi eğitim platformlarında da eğitimlerini tamamlayan bireylere sertifika vererek eğitime teşvik eder.

BTK, Türkiye'nin siber güvenlik alanında düzenleyici, denetleyici ve koordinasyon sağlayıcı bir rol üstlenir. Kurum, siber güvenlik politikalarının geliştirilmesi, siber olaylara müdahale, bilgi paylaşımı, eğitim, standartların belirlenmesi, uluslararası işbirliği, araştırma ve geliştirme faaliyetleri ve kritik altyapıların korunması gibi çeşitli alanlarda önemli görevler yürüterek Türkiye'nin dijital ve siber güvenlik kapasitesine destek olunmaktadır.

> Ulusal siber güvenlik kapasitesinin arttırılmasına yönelik çalışmalar gerçekleştirmek amacıyla kurulan Siber Güvenlik Enstitüsü(SGE) 1997 yılında Bilişim Sistemleri Güvenliği (BSG) Birimi adıyla TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) çatısı altında faaliyetlerine başlamıştır. 2012 yılı itibariyle yoluna TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak devam eden Siber Güvenlik Enstitüsü, temel olarak siber güvenlik alanında ülkemize teknoloji kazandırmak üzere yürüttüğü Ar-Ge faaliyetleri ile ülkemizin ulusal güvenliğine hizmet vermektedir. (TÜBİTAK, 2024)

Siber Güvenlik Enstitüsü (SGE) ulusal siber güvenliğin sağlanması ve bu konuda ülkemizin kendi ayakları üzerinde durması misyonu doğrultusunda TÜBİTAK BİLGEM çatısı altında kurulmuştur. Türk Silahlı Kuvvetlerinin bilişim sistemleri güvenliği altındaki ihtiyaçları karşılamak için projeler üretmektedir. TÜBİTAK BİLGEM SGE (2024), siber konulu faaliyetlerini üç ana başlıkta toplamaktadır. Bunlar;

- İleri Siber Güvenlik Araştırma Geliştirme Çalışmaları
- Siber Güvenlik Stratejisi Belirleme Çalışmaları
- Siber Güvenlik Çözüm Projeleri

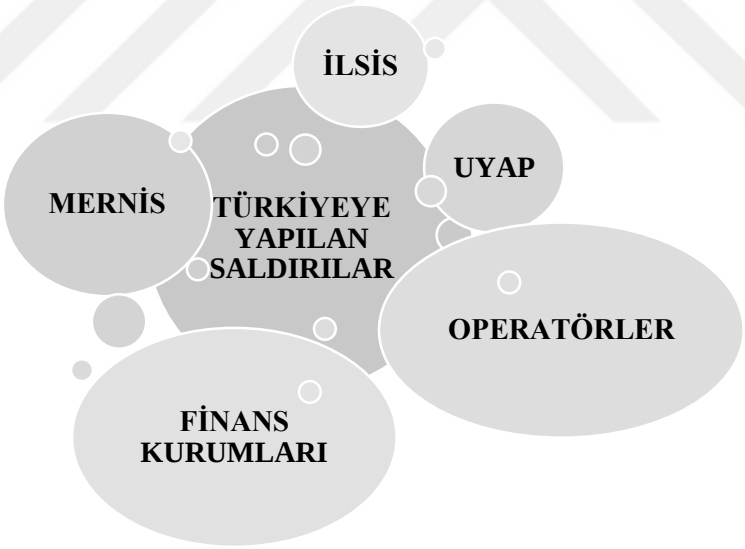
Bu üç alanda çalışmalarını yapmakta ve siber güvenlik hassasiyetini ülkede oluşturmaktadırlar. Aynı zamanda SGE yerli ve milli uygulamalar geliştirmeyi, yazılımları milli bir bilinçle yapmayı hedeflemektedir. ORION Veri Güvenlik Platformu da bunlara örnektir. ORION Veri Güvenlik Platformu; ortak yönetim paneli, ağ ve uç nokta ortamlarında kurulan ajan yazılımları ile hassas verilerin olası izinsiz erişimi, kullanımı veya paylaşımı senaryolarına karşı çözüm sunan bir veri kaçağı önleme sistemidir. SGE'nin bir diğer çalışması da SİBERLAB-Sanal Siber Güvenlik Laboratuvarı'dır. Gelişen siber güvenlik teknolojileri; uygulama odaklı eğitimler, tatbikatlar ve analiz laboratuvarları için kullanıcıları hızlı ve kolay tasarlanabilir sanal ortamlara yönlendirmektedir. Sanal Siber Güvenlik Laboratuvarı Altyapısı ile ağ cihazları ve bilgisayarları içeren topolojiler tasarlanabilmekte ve kullanıcının tasarıma uygun ortamlara tarayıcı üzerinden (herhangi bir kaynak gereksinimi olmadan) hızlı bir şekilde erişebilmesi sağlanmaktadır (TÜBİTAK, 2024).

Türkiye'de bu yapılan yeniliklerin yanında dijitalleşen her sisteme ayrı ayrı saldırıların olduğu bilinmektedir. Teknik gelişimlerin olumsuzluklarından gelişen ve bilgi yüklü her sistem hedef olarak gösterilerek tehdit altında kalmaktadır. Bu sistemlerden bazıları Şekil 12'de bahsedilmiştir. Merkezi Nüfus İdare Sistemi(MERNİS) 2016 yılında önemli bir saldırıya maruz kalmıştır. Bu saldırıyla birlikte birçok kişinin kişisel verilerinin sızdırıldığı ortaya çıkmıştır. Bu olayla birlikte Türkiye 'de siber güvenlik konusunun ne kadar önemli olduğu gerçeği ortaya çıkmıştır. Türkiye'de Ulusal Yargı Ağı Projesi (UYAP) de yine 2016 yılınsa saldırıya uğramış ve bazı hizmetlerin aksamasına sebep olmuştur. Saldırı sonrası, Adalet Bakanlığı ve diğer ilgili kurumlar, sistemin güvenliğini artırmak için

çeşitli önlemler almış ve altyapıyı güçlendirmiştir. Türkiye'de İl Milli Eğitim Müdürlüğü Bilgi Sistemleri(İLSİS), 2007'de siber saldırıya uğramıştır. İLSİS, Milli Eğitim Bakanlığı tarafından kullanılan ve öğrenci, öğretmen ve okul bilgilerini içeren bir bilgi yönetim sistemidir. Bu saldırı, İLSİS sisteminde ciddi kesintilere ve veri kayıplarına yol açmıştır. Ayrıca Türkiye'deki büyük bankalar, zaman zaman fidye yazılımları, phishing (oltalama) saldırıları ve DDoS saldırılarıyla karşı karşıya kalmaktadır. İletişim teknolojilerinin yaygın olduğu verilerin kuvvetli olduğu operatörlerde de zaman zaman ciddi saldırılar olmuştur. Bu tür olaylar, dijitalleşen kamu- özel hizmetlerinin siber güvenlik açısından ne kadar kritik olduğunu ve bu alanda sürekli olarak güncellenen ve güçlendirilen güvenlik önlemlerine ihtiyaç duyulduğunu ortaya koymuştur.

Şekil 12

Türkiye'ye yapılan saldırılar



Yönü ve saldırının türü değişen siber güvenlik durumlarında Türkiye'de siber saldırılara karşı savunma sağlayan çeşitli sistemler ve mekanizmalar bulunmaktadır. Bu sistemler, hem devlet kurumları hem de özel sektör tarafından geliştirilmiş ve uygulanmıştır. Bu sistemler: Siber Güvenlik Kurulu, Ulusal Siber Olaylara Müdahale Merkezi, Kamu Güvenliği Ağı (Kamu-Net)'dır.

a. Siber Güvenlik Kurulu

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar gereğince; Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır. (Bilgi Teknolojileri ve İletişim Kurumu, 2024).

Kurulun; siber güvenlikle alakalı politikalar belirlemek, strateji ve yelem planları çıkarmak, uygulanması için gereken kararları almak, altyapı çalışmaları için kararlar almak, siber güvenliğin sorumlu tutulacağı kurum ve kuruluşları belirlemek, istisna olacak kurumlara karar vermek gibi görevleri vardır.

Kurul, siber güvenlik konusunda bireysel, kurumsal ve ulusal farkındalık için eğitimler düzenlemektedir. Eğitimlerde, bilgi güvenliğine, siber güvenlik ve tehditlerine, genel güvenlik önlemlerine, bilgi güvenliği politikalarına, mobil cihazların güvenliğine, mevzuat ve çalışmalarına değinilmektedir. Ayrıca siber güvenlik konularına ait makale, sunum, rapor çalışmaları da yapılmaktadır.

Siber Güvenlik Kurulu**,** Türkiye'de de ilk kez 20 Haziran 2013 tarihli ve 28683 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı hazırlamış ve yayımlamıştır. Bu plana göre kritik alt yapılar; "*işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları*" şeklinde ifade edilmiştir (Ünal, 2018). Eylem planının amacı; bilgi teknolojileri üzerinden sağlanan her türlü hizmette kullanılan sistemlerin güvenliğinin sağlanmasını, kritik altyapıların oluşturulmasını ve güvenliğinin sağlanmasını, siber güvenlik olaylarının etkilerinin düşürülmesini, oluşan adli süreçlerde daha detaylı araştırılmasını sağlamaktır. Daha detaylı incelemeler yapılarak ortaya çıkarılan planı ise 2016-2019 Ulusal Siber Güvenlik Stratejisi'dir.

2016-2019 Ulusal Siber Güvenlik Eylem Planı, Türk hükümetinin ülkenin kritik altyapısını siber tehditlerden koruma stratejisini özetleyen bir belgedir. Bu dönemde belirlenen risklere karşılık güncelleme yapılmıştır. Belirlenen riskler, kurumlar arası iletişim sorunu, toplumun sosyal ve sanal ortamlara bağımlılığı, siber casusluklar ve saldırıların boyutu, personel yetkinliklerindeki yetersizlik, siber farkındalık için ayrılan bütçe ve ekonomik kaygılardır. Bu risklere karşılık alınacak önlemler belirlenerek 2016-2019 Ulusal Siber Güvenlik Stratejisi için güncelleme yapılmıştır. Alınan önlemler ise; kritik altyapı için güçlendirme ve savunma çalışmaları, siber suçlarla mücadele, farkındalık çalışmaları, insan kaynağı sağlama, siber güvenlik süreçlerini geliştirme, siber güvenlik ile bilgi güvenliği ve milli güvenliği entegre edebilecek çalışmalar geliştirmektir. Bu planın ardından da eksiklikleri tamamlamak amacıyla 2020-2023 Ulusal Siber Güvenlik Stratejisi Eylem Planı oluşturulmuştur.

b. Ulusal Siber Olaylara Müdahale Merkezi (USOM)

BTK bünyesinde faaliyet gösteren USOM, Türkiye'de siber güvenlik olaylarına hızlı ve etkili bir şekilde müdahale etmek amacıyla kurulmuştur. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı kapsamında kurulan USOM, siber tehditlere karşı uyarılar yayınlar, olaylara müdahale ederek ve çeşitli sektörlerdeki kurumlarla işbirliği yapmaktadır. 7/24 çalışma planıyla çalışmalarda tespit edilen siber tehditlerle mücadele etmektedir. Siber tehditlere maruz kalan bilişim sistemlerine yönelik koruyucu tedbirlerin alınması konusunda faaliyetlerde bulunmaktadır. USOM, ülkemizdeki kamu kurum ve kuruluşları, internet servis sağlayıcıları, özel sektör kuruluşları ve diğer internet aktörleri ile birlikte gerekli çalışmaları yapmaktadır. Siber güvenlik farkındalık faaliyetleri kapsamında Sektörel ve Kurumsal Siber Olaylara Müdahale Ekibi(SOME), üniversitelere, siber güvenlik topluluklarına yönelik olarak siber güvenlik eğitimi faaliyetlerinde bulunmaktadır. Siber olaylara hızlı ve etkili bir şekilde müdahale etmektedir. Kurumlar arasında koordinasyonu sağlar ve olay sonrası toparlanma süreçlerini yönetmektedir. Siber güvenlik olaylarına hızlı müdahale, tehditlerin erken tespiti ve kurumlar arası koordinasyon konularında önemli bir rol oynamaktadır. Aynı zamanda, siber güvenlik farkındalığını artırarak hem kamu hem de özel sektörde daha güvenli bir dijital

ortamın oluşturulmasına katkıda bulunmaktadır (USOM, 2024).

c. Kamu Güvenliği Ağı (Kamu-Net)

Kamu kurumlarının güvenli iletişim sağlaması için oluşturulan bir ağdır. Bu ağ, kamu kurumları arasındaki veri trafiğini güvenli hale getirmek amacıyla şifreleme ve diğer güvenlik önlemleri kullanır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile Siber Güvenlik Kurulu Kararları uyarınca Kamu-Net'in oluşturulması çalışmaları Ulaştırma ve Altyapı Bakanlığınca yürütülmektedir. Kamu-Net, siber güvenlik tehditlerine karşı güçlü koruma sağlar. Güvenlik duvarları, izinsiz giriş tespit sistemleri ve diğer güvenlik önlemleri ile kamu kurumlarının verileri ve sistemleri korunur. Ağın yönetimi merkezi olarak gerçekleştirilir ve bu sayede ağın güvenliği, performansı ve verimliliği sürekli olarak izlenir ve optimize edilir. Bu projeyle; siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi amaçlanmaktadır. (UAB, 2024). Kamu-net projesine hâlihazırda 53 kamu kurumu dâhil edilmiştir (Özbilen & Çağlar, 2020).

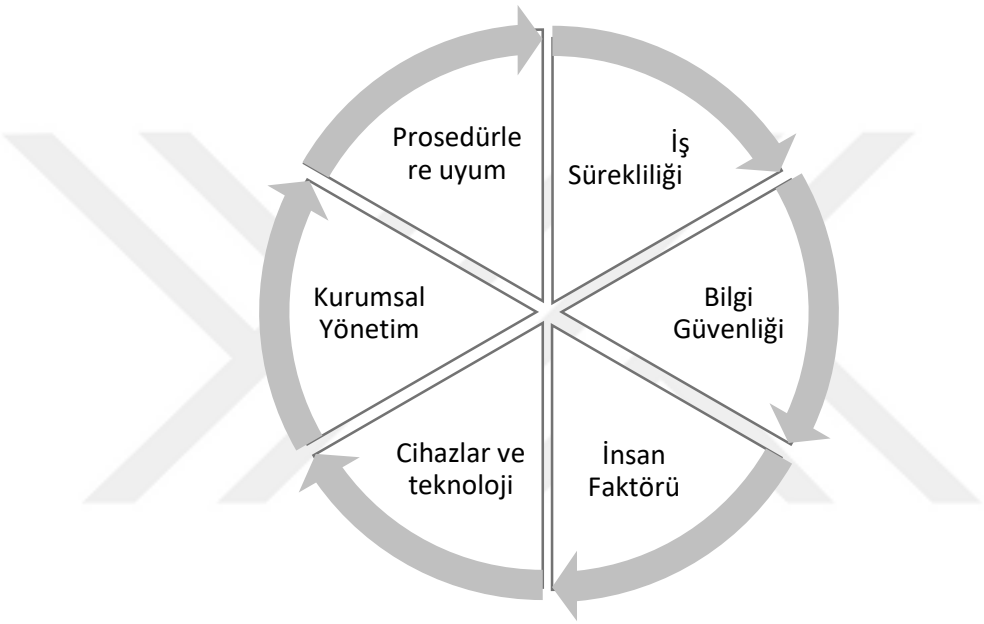
Kamu-Net üzerinden iletilen tüm veriler, gizlilik prensiplerine uygun olarak işlenir ve saklanır. Kamu kurumlarının hassas bilgileri, üçüncü tarafların erişimine karşı korunur. Türkiye'deki kamu hizmetlerinin dijital dönüşümünü destekleyen kritik bir altyapıdır. Bu ağ, kamu kurumları arasındaki veri alışverişinin güvenli ve kesintisiz olmasını sağlar, böylece vatandaşlara sunulan hizmetlerin kalitesini ve güvenliğini artırır. Ayrıca, siber güvenlik tehditlerine karşı güçlü bir savunma mekanizması sunarak, kamu kurumlarının bilgi güvenliğini korur (CBDDO, 2024).

Türkiye'nin siber güvenlik stratejisi, dinamik bir yapıya sahiptir. Sürekli güncelleme isteyen sürekli gelişimlere karşılık tedbirlerini almaya çalışan bir düzen vardır. Teknolojik gelişmelere ve siber tehditlere karşı da değişim şarttır. Türkiye'nin siber stratejileri siber tehditlere karşı direnci artırmayı ve siber güvenliği teşvik etmeyi amaçlamıştır. Siber güvenlik yaklaşımının yeterli olup olmadığı konusunda da

araştırmalar yapılarak yetersiz görülen kısmın geliştirilerek siber güvenlik stratejilerine uygun hale getirilir. Siber güvenlik olgunluğunun olup olmaması da aşağıdaki şekilde verilen boyutlar incelenerek karar verilir.

Şekil 13

Siber olgunluk için bakılması gereken boyutlar



Siber olgunluk, prosedürlere uyum sonucu yapılacak olan sürecin sürekliliğini ele alır. Bilginin güvenliği için tüm çalışmalar yapılırken süreçte yer alan insan faktörü de en önemli faktörler arasındadır. Bireylerin siberi yönetme ve uygulama sürecinde teknik aletlerin, cihazların yeterli ve nitelikli olması da diğer bir etkendir. Bunlara ek olarak da siber süreci destekleyen yönetimlerin olması gerekliliği ortaya çıkar ve siber süreci iyi yöneten bir yönetici grubu başarıyı elde edebilmektedir. Kurumlardaki siber uygulamalarının başarılı sonuçlar elde edebilmesi için gerekli faktörleri adım adım izlemek gerekmektedir.

6. BİLGİ ve BELGE YÖNETİMİNDE SİBER GÜVENLİK

Günümüz dünyasında internetin yaygın kullanımı, teknolojik faaliyetlerin gelişmesi ve kullanımı ile birlikte bilgi yönetimi şekillerindeki değişim artmıştır. Teknolojinin hızla ilerlediği bu dönemde, Bilgi ve Belge Yönetimi alanındaki hizmetlerde de değişiklikler olmuştur. Geleneksel manadaki hizmet anlayışından yenilikçi hizmet anlayışına geçişler gözlemlenmektedir (Bayter & Yıldırım, 2023). Bu gibi hizmetlerin yenilenmesi güvenlik önlemlerindeki değişiklere bütünleşmiş bir şekilde olmalıdır. Çünkü dijital çağda, BBY, kurumların etkinlik ve verimliliklerini artırmak için kritik bir rol oynamaktadır. Bilgi ve belge yönetimi, kurumların bilgilerini ve belgelerini toplama, düzenleme, saklama ve dağıtma süreçlerini içeren bir disiplindir. Bu süreçler, dijital ortamda gerçekleştirildiğinde daha hızlı ve etkin hale gelir, ancak siber güvenlik risklerini de beraberinde getirir. BBY süreçlerinde siber güvenlik önlemlerinin alınmaması, veri ihlalleri, bilgi kaybı ve kurum itibarının zedelenmesi gibi ciddi sonuçlar doğurabilir. Buna istinaden siber güvenlik, bilgi ve belge yönetiminde bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için vazgeçilmezdir.

Bilgi ve Belge Yönetimi alanında en temel alanlardan biri de kütüphanelerdir. Bu bilgi merkezlerinin, kütüphanelerin bilgi yönetim süreci içinde mekânsal olarak ya da hizmet kapsamında ele alınması gerekmektedir. Kütüphanelerde verilen hizmetlere ve elektronik ortama yansıyan hizmetlerde siber güvenlik gereklilikleri vardır. Bilgi yönetim sürecinde siber güvenlik bilgi hizmetleri ile de aşağıdaki bölümlerde ele alınmaktadır.

6.1. Bilgi Hizmetlerinde Siber Güvenlik

Kütüphanelerde Erişim Kontrolü ve Kimlik Doğrulama

Bilgi ve belgelere yetkisiz erişimlerin engellenmesi için güçlü erişim kontrolü ve kimlik doğrulama mekanizmaları kullanılmalıdır. Kullanıcılar için birden fazla doğrulama yöntemi kullanılması gerekmektedir. Ayrıca kullanıcıların rollerine göre yetkilerinin belirlenmesi ve erişim kontrollerinin de role dayalı erişim kontrolü olması gerekmektedir. Yetkilere göre veri şifreleme yöntemlerinin yapılması da kritik öneme sahiptir.

Ağ üzerindeki iletilerin ve depolanan verilerin şifrelenerek kontrol altında tutulması da siber güvenlik önlemlerindendir. Verilerin korunması ve bilgi ve belge yönetim sistemlerinin dış tehditlere karşı korunması için güvenlik duvarları ve saldırı tespit/önleme sistemleri kullanılmalıdır. Böylelikle güvenlik duvarları, izin verilen ve reddedilen ağ trafiğini belirleyerek sistemleri koruma altına alır ve ağ trafiğini izleyerek olası saldırıları tespit eder ve önler (Aldemir & Kaya, 2020). Veri kaybı oluşturabilecek her türlü riski geride bırakıp yedekleme ve kurtarma planları prosedürlerde yer almalıdır ve bilgi ve belgelerin kaybolması durumunda hızlı bir şekilde geri yüklenmesi için düzenli yedekleme ve felaket kurtarma planları uygulanmalıdır.

Bilgi ve belge yönetiminde siber güvenlik, bilgilerin ve belgelerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için kritik bir öneme sahiptir. Erişim kontrolü, veri şifreleme, güvenlik duvarları, yedekleme ve kurtarma, izleme ve denetim ile eğitim ve farkındalık programları gibi siber güvenlik hizmetlerinin etkin bir şekilde uygulanması, BBY süreçlerinin güvenliğini artıracaktır. Kurumlar, bu hizmetleri entegre ederek bilgi ve belgelerini koruma altına almalı ve siber güvenlik risklerine karşı hazırlıklı olmalıdır.

5070 Sayılı Elektronik İmza Kanunu'nda elektronik imza (e-imza) tanımı: "elektronik imza, bilginin orijinalliğini ve tarafların kimliğini güvence altına alan bir teknolojidir" şeklindedir. Buna ek olarak Yılmaz'ın (2024) yorumu; "kimlik doğrulama, neredeyse bütün hukuki işlemlerin gerçekleştirilmesinde ilk adımı oluşturmaktadır. Bu nedenle elektronik hizmet sunumunda kimlik doğrulama araklarından sağlıklı olanlar tercih edilmelidir. Elektronik imza; bilginin, orijinalliği bozulmadan, tarafların kimliğini de belirleyebilecek şekilde elektronik ortamda karşı tarafa aktarılmasını garanti eden bir teknolojidir" şeklinde olmuştur.

Bilgi ve belge yönetiminde belgelerin elektronik ortamda kullanılmasıyla birlikte e-imza düzeni kolaylık sağlamıştır. Elektronik imzalar, siber saldırılara karşı bir güvenlik katmanı sağlar. Örneğin, bir saldırganın bir belgeyi değiştirip yeniden imzalaması zordur, çünkü imza anahtarı sadece imzalayan kişide bulunur. Bu da, veri sızıntıları, kimlik

sahtekârlığı ve veri ihlalleri gibi tehditlere karşı ek bir koruma sağlar. Bu nedenle, elektronik imzalar, dijital dünyada kimlik doğrulama, veri bütünlüğü, gizlilik ve yasal güvence sağlamak için hayati bir araç olarak siber güvenliğin önemli bir parçasıdır.

E-Arşivler

E-Arşivler ile siber güvenlik arasındaki ilişki, dijital verilerin güvenli bir şekilde saklanması, işlenmesi ve iletilmesi üzerine odaklanır. E-Arşivler, işletmelerin ve devlet kurumlarının dijital belgeleri uzun vadeli olarak sakladıkları, erişilebilir hale getirdikleri ve düzenlemelere uygun şekilde arşivledikleri sistemlerdir. Bu belgeler, finansal kayıtlar, sözleşmeler, fatura belgeleri ve daha birçok önemli veri türünü içerebilir.

E-Arşiv sistemi süreçleri teknik altyapı gerektirir. Kurumlarda iş süreçleri bilgi sistemleri aracılığıyla yürümektedir. Elektronik platformlarda yürütülen arşiv süreçlerinde değişen teknoloji ile birlikte de gelişim yaşanmaktadır. Geçmişi ve bugünü geleceğe taşımak için arşivleri bugünün şartlarına uygun hale getirmek gerekmektedir (Özdemirci, 2019).

E-Arşivlerde saklanan belgelerin gizliliğinin korunması, yetkisiz kişilerin erişimini engellemek için şifreleme yöntemleri ve güvenlik protokolleri kullanılır. Ayrıca, veri bütünlüğünün korunması, verilerin değiştirilmesini veya manipüle edilmesini önlemek için de önemlidir. Kimlerin hangi verilere erişebileceği konusunda sıkı kontroller yapılması gereklidir. Kullanıcı kimlik doğrulama sistemleri (örneğin, iki faktörlü kimlik doğrulama) ve rol tabanlı erişim kontrolleri bu amaçla kullanılır. E-Arşiv sistemlerine yapılan tüm erişimler ve işlemler izlenmeli ve kaydedilmelidir. Bu denetim kayıtları, olası güvenlik ihlallerini tespit etmek ve bu ihlalleri araştırmak için kritik öneme sahiptir. E-Arşivlerde saklanan verilerin güvenli bir şekilde yedeklenmesi ve olası veri kaybı durumlarında hızlı bir şekilde kurtarılabilmesi için yedekleme ve felaket kurtarma planlarının uygulanması gereklidir. Birçok sektörde, verilerin nasıl saklanacağı, kimlerin erişim sağlayabileceği ve ne kadar süreyle saklanacağı gibi konularda yasal düzenlemeler mevcuttur. Siber güvenlik, bu yasal gerekliliklere uygun bir e-arşiv yönetimi sağlanmasını güvence altına alır. Bu nedenlerle, e-arşiv sistemleri için güçlü bir siber güvenlik yapısı oluşturmak, verilerin

güvenliği ve organizasyonun genel bilgi güvenliği duruşu açısından hayati önem taşır.

E-Kaynaklar

Elektronik kaynaklar, bilgisayarlar, sunucular, ağlar, veri depolama sistemleri, yazılımlar ve dijital platformlar gibi dijital bilgilere erişim sağlanan tüm araçları kapsamaktadır. Siber güvenlik ise bu elektronik kaynakların güvenliğini sağlamayı amaçlamaktadır. Bu hizmetlerin güvenliği ve erişilebilirliği, siber güvenlik önlemleriyle sağlanmalıdır. Kullanıcıların internet bağlantısının olduğu her yerden çevrimiçi olarak erişebilecekleri ağlarla mümkün olan bu hizmet bu durumla birlikte de erişim güvenlik önlemlerinin gereklilikleri ortaya çıkmaktadır. E-kaynak hizmetleri kapsamında sunulan dijital içeriklerin güvenliği, bu materyallerin yetkisiz erişimden, veri sızıntılarından korunmasıyla sağlanmaktadır. Bu nedenle, şifreleme teknikleri, erişim kontrolleri ve veri güvenliği standartları gibi siber güvenlik önlemleri uygulanmaktadır.

Siber güvenlikte en zayıf halka genellikle insan faktörüdür. Bu nedenle, e-kaynak hizmetlerini kullanan kullanıcıların siber güvenlik konularında eğitilmesi ve farkındalıklarının artırılması önemlidir. Kullanıcıların güçlü şifreler kullanmaları, güvenli internet bağlantıları tercih etmeleri ve şüpheli e-postalardan kaçınmaları gibi konularda bilinçlendirilmesi gerekmektedir. E-kaynak hizmetleri sağlayan dijital kütüphaneler, kullanıcıların güvenli bir şekilde dijital içeriklere erişmelerini sağlamak için güçlü siber güvenlik önlemleri uygulamaktadırlar. Bu önlemler, kullanıcıların verilere güvenle erişmelerini ve kütüphane hizmetlerinden en iyi şekilde yararlanmalarını sağlamaktadır.

Dijital Kütüphaneler

> Dijital kütüphaneler ve sosyal medya, bilgi paylaşımı ve erişiminde önemli bir rol oynamaktadır. Bu iki alanın sentezi de bilgiye erişimi ve paylaşımını daha hızlı, kolay ve etkileşimli hale getirmektedir. Günümüz dünyasında her geçen gün hızla değişen teknolojik ve toplumsal yapı, kütüphanelerin de dönüşüm sürecine girmesine neden olmuştur. (Bayter & Yıldırım, 2023,s.185)

Dijital kütüphaneler geleneksel anlamdaki kütüphane mantığından dışarı çıkarak yenilikçi bakış açısıyla gelişim göstermektedirler. Dijital kütüphanelerde yeni hizmet modelleri oluşmuştur. Teknolojinin gelişmesiyle birlikte hizmetlerdeki değişimde göz ardı edilemeyecek seviyelerdedir. Dijital Kütüphane hizmetleri; çevrimiçi kataloglar, çevrimiçi eğitimler, sosyal medya, dijital arşivler, sanal gerçeklik gibi değişimlerle birlikte sunulmaktadır. Bu yenilikler, kullanıcı deneyimini iyileştirmeyi, bilgilere daha kolay erişim sağlamayı ve dijital içeriğin daha verimli bir şekilde yönetilmesini hedeflemektedir. Örneğin; dijital kütüphaneler bilimsel ve akademik içeriklerin açık erişimle sunulmasına olanak tanıyan platformlar haline gelmiştir. Açık erişim, araştırma sonuçlarının herkes tarafından erişilebilir olmasını sağlayarak bilginin yayılmasını hızlandırmaktadır (Aydın, 2024).

Sanal ve artırılmış gerçeklik teknolojileri, dijital kütüphanelerde yenilikçi öğrenme ve keşif deneyimleri sunmak için kullanılmaktadır. Bu süreçte de dijital ürünlerin kullanıldığı mobil erişim ve uygulamaları yaygın görülmüştür. Mobil cihazların yaygınlaşmasıyla birlikte dijital kütüphaneler, kullanıcıların her yerden erişim sağlaması için mobil uyumlu hale getirilmiştir. Dijital kütüphaneler, bulut tabanlı hizmetler kullanarak verilerin depolanması, işlenmesi ve sunulmasını kolaylaştırmaktadır. Bulut teknolojileri, kütüphanelerin büyük veri kümelerini yönetmesini ve kullanıcıların istedikleri bilgilere hızlı bir şekilde erişmelerini sağlamaktadır. Bu yenilikçi yaklaşımlar, dijital kütüphanelerin daha erişilebilir, etkileşimli ve kullanıcı dostu hale gelmesini sağlamaktadır. Aynı zamanda, bu kütüphaneler bilginin demokratikleşmesini, bilime ve kültüre daha geniş kitlelerin ulaşmasını desteklemektedir.

Dijital kütüphaneler genellikle büyük miktarda dijital içeriği depolayan ve erişilebilir kılan sistemlerdir. Bu içerikler, kitaplar, makaleler, resimler, müzikler ve diğer türden kültürel ve akademik materyaller olabilir. Siber güvenlik, bu dijital kütüphaneler için önemli bir konudur; çünkü bu platformlar da diğer dijital sistemler gibi çeşitli siber tehditlere maruz kalınabilir. Dijital kütüphanelerde saklanan ve sunulan verilerin güvenliği büyük önem taşımaktadır. Bu verilerin yetkisiz erişime karşı korunması, şifreleme teknikleri kullanılarak sağlanabilir. Ayrıca, veri depolama ve iletim süreçlerinde güvenlik protokolleri ve

standartlarına uygunluk da büyük önem taşımaktadır. Dijital kütüphanelerde, farklı kullanıcı gruplarının farklı düzeylerde erişim hakkına sahip olması gerekebilir. Örneğin, kamu erişimi olan içeriklerle sadece üyelere veya araştırmacılara özel içerikler arasında ayrım yapılabilir. Bu nedenle, rol tabanlı erişim kontrolleri gibi yöntemler kullanılarak veriye erişim sınırları belirlenmelidir.

Dijital kütüphaneler, siber saldırıların hedefi olabilir. Bu saldırılar, veri sızıntıları, hizmet dışı bırakma (DDoS), fidye yazılımları ve kimlik hırsızlığı gibi çeşitli formlarda olabilir. Bu tür saldırılara karşı korunmak için güçlü ağ güvenliği önlemleri, güvenlik duvarları, saldırı tespit sistemleri (IDS) ve saldırı önleme sistemleri (IPS) gibi teknolojiler kullanılabilir. Dijital kütüphanelerdeki verilerin yedeklenmesi ve felaket kurtarma planlarının oluşturulması önemlidir. Veri kaybını önlemek için düzenli olarak yedekleme yapılmalı ve olası bir felaket durumunda verilerin hızlı bir şekilde kurtarılabilmesi için planlar hazırlanmalıdır. Dijital kütüphaneler genellikle kullanıcıların kişisel verilerini de içerebilecekleri için ilgili yasal düzenlemelere uyum sağlamak önemlidir. Özellikle veri koruma yasaları, telif hakları ve erişim hakları gibi konular dikkate alınmalıdır. Dijital kütüphaneler siber güvenlik açısından çeşitli tehditlere karşı korunmalı ve güvenli bir ortam sağlanmalıdır. Bu, kullanıcıların güvenle içeriklere erişebilmesini ve kütüphane işletmecilerinin de veri güvenliğini sağlar (Karataş, 2015). Siber güvenlik hizmetleri, bilgi merkezlerinin verilerini ve sistemlerini korumak, yetkisiz erişimleri önlemek ve siber tehditlere karşı dayanıklılığı artırmak için gereklidir. Bilgi merkezleri, bu hizmetleri titizlikle uygulayarak, bilgi güvenliğini en üst düzeyde tutmalı ve sürekli olarak gelişen tehditlere karşı hazır olmalıdır.

Kütüphanelerde MERNİS Bilgileri Kullanımı/ KVKK

Kütüphaneler, kullanıcılarına çeşitli hizmetler sunarken kişisel verileri toplar ve işlemektedir. Bu veriler, 6698 sayılı KVKK ve MERNİS bilgilerinin kullanılması bağlamında büyük bir öneme sahiptir. KVKK, kişisel verilerin korunması ve işlenmesi konusunda net kurallar koymaktadır. Kütüphaneler, üyelik süreçlerinde veya çeşitli hizmetler sunarken kullanıcıların isim, adres, T.C. kimlik numarası gibi kişisel verilerini

toplamaktadır. Bu verilerin korunması, KVKK ile uyumlu olmayı gerektirmektedir. KVKK, kişisel verilerin güvenli bir şekilde saklanması, yetkisiz erişime karşı korunması ve sadece gerekli durumlarda işlenmesi gerektiğini belirtir (Çakmak & Şişkin , 2020).

MERNİS, Türkiye'deki nüfus bilgilerini içeren merkezi bir sistemdir ve kamu kurumları tarafından kullanılmaktadır. Kütüphaneler, üyelik işlemlerinde doğrulama yapmak veya kullanıcı bilgilerini güncellemek amacıyla MERNİS verilerini kullanmaktadır. Ancak bu verilerin kullanımı, sadece yasal yetkiler çerçevesinde ve KVKK hükümlerine uygun olarak yapılmalıdır. KVKK ve MERNİS bilgilerinin siber güvenlik açısından korunması, kütüphaneler için yasal bir zorunluluğun ötesinde, kullanıcıların güvenine dayalı bir sorumluluktur. Olası veri ihlalleri, hem hukuki yaptırımlar hem de kullanıcı güveninin kaybı gibi ciddi sonuçlar doğurabilir. Bu nedenle, kütüphaneler siber güvenlik stratejilerini, KVKK ve MERNİS bilgilerinin korunmasını öncelikli hale getirmelidir.

Kütüphanelerdeki kişisel veriler, kimlik hırsızlığı, veri sızıntısı veya siber saldırılar gibi çeşitli tehditlerle karşı karşıya kalabilir. Bu tehditlere karşı risk yönetimi stratejileri geliştirilerek veri ihlallerinin önlenmesi hedeflenmelidir. Bu kapsamda, sızma testleri, güvenlik açıklarının düzenli olarak gözden geçirilmesi ve acil durum planlarının oluşturulması gibi önlemler alınabilir. Ayrıca alınacak tedbirler:

- Kütüphanelerde saklanan kişisel veriler, yetkisiz erişimi engellemek amacıyla güçlü şifreleme yöntemleriyle korunmalıdır.
- Kişisel verilere erişim, yalnızca yetkili kişilerle sınırlandırılmalı ve erişim kayıtları düzenli olarak izlenmelidir.
- Kütüphanelerin bilgi sistemleri, dışarıdan gelebilecek siber saldırılara karşı güvenlik duvarları ve güncel antivirüs yazılımlarıyla korunmalıdır**.**
- Yazılım ve sistemler, bilinen güvenlik açıklarına karşı düzenli olarak güncellenmeli ve yeni tehditlere karşı korunmalıdır.
- Kütüphane personelinin siber güvenlik konusunda eğitilmesi, olası siber saldırıların etkilerini en aza indirmek için kritik öneme sahiptir (Kavak & Odabaş, 2023).

6.2. Bilgi Merkezlerinde Siber Güvenlik Önlemleri

Bilgi merkezlerinde siber güvenlik önlemleri, dijital verilerin korunmasını sağlamak ve bilgi sistemlerinin güvenliğini artırmak için bir dizi stratejik adım içermektedir. Türkiye'deki bilgi merkezlerindeki gözlem ve araştırmalara bakılarak siber güvenlik önlemlerine bazı örnekler verilebilir. Bunlar;

1. Erişim kontrol sistemlerinde, kullanıcıların bilgi sistemlerine ve verilere erişimini kontrol etmek amacıyla kimlik doğrulama (şifreler, biyometrik sistemler) kullanılmaktadır. Türkiye'deki üniversite kütüphanelerinde, akademik veri tabanlarına erişim için öğrenciler ve personel, üniversitenin sağladığı kimlik doğrulama sistemlerini kullanmaktadırlar. Halk kütüphanelerinde ise e-devlet girişi ile doğrulama yapılmaktadır.

2. Veri şifrelemede, hem depolanan hem de aktarılan verilerin şifrelenmesi, bilgilerin yetkisiz kişiler tarafından okunması önlenmektedir. Türkiye'deki çeşitli devlet kurumları, kritik bilgileri şifrelemek için milli şifreleme yazılımlarını kullanmaktadır. Buna örnek olarak da; TÜBİTAK tarafından geliştirilen "Kamu Sertifikasyon Merkezi" aracılığıyla güvenli iletişim sağlanır (TÜBİTAK, 2024).

3. Güvenlik duvarları ve antivirüs yazılımlarında, bilgi merkezleri siber tehditlerden korumak için güvenlik duvarları ve antivirüs yazılımları kullanılmaktadır. Milli yazılımlar daha çok tercih sebebi olmaktadır. Kütüphanelerde kullanılan sistemlerde, kütüphane otomasyon sistemlerinde de buna dikkat edilmektedir. Bu duruma örnek olarak Türkiye'deki birçok bilgi merkezi ve kütüphane, dışarıdan gelen tehditlere karşı ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi) tarafından sağlanan güvenlik hizmetlerinden yararlanmaktadır (ULAKBİM, 2024).

4. Yazılım güncellemelerinde, güvenlik açıklarını kapatmak için bilgi merkezlerinde kullanılan tüm yazılımların ve sistemlerin düzenli olarak güncellenmesi sağlanmaktadır. Türkiye'deki kamu kurumları, BTK tarafından

yayınlanan siber güvenlik yönergelerine uygun olarak yazılım güncellemelerini düzenli olarak gerçekleştirmektedir.

5. Yedekleme ve kurtarma planlarında, veri kaybını önlemek ve sistem arızalarında verileri geri yüklemek için düzenli yedekleme ve kurtarma planları oluşturulmaktadır. Prosedürlere uygun yazılır ve kurum geneline duyuru yapılır. Türkiye'deki büyük veri merkezlerinde, verilerin belirli aralıklarla yedeklenmesi ve olası bir siber saldırı ya da doğal afet durumunda acil kurtarma planlarının devreye alınması yaygın bir uygulamadır. Örneğin, e-devlet kapısı hizmetleri, veri yedekleme ve kurtarma konusunda ileri düzey güvenlik önlemleri ile korunmaktadır (Özdemirci, 2019).

6. Personel eğitimi ve farkındalık çalışmalarında, siber güvenlik farkındalığını artırmak için personel ve kullanıcılar düzenli olarak eğitilir. Bu eğitimlere katkı sunan Turkcell, Vodafone gibi telekomünikasyon şirketleri ücretsiz eğitimlerle desteklemektedir. Buna ek olarak devlet kurumlarında eğitimcilerin çağrılmasıyla farkındalıklar oluşturulmaktadır. En detaylı ve sistemli olarak da BTK Akademi, Türkiye genelinde bilgi merkezleri çalışanları için siber güvenlik farkındalık eğitimleri sunmaktadır. Bu eğitimler, bilgi güvenliği politikalarının etkili bir şekilde uygulanmasına katkıda bulunur.

7. "Ağ güvenliği ve tehdit tespitinde, sürekli ağ izleme ve anormal faaliyetlerin tespit edilmesi, potansiyel tehditleri önceden belirlemeye yardımcı olur" (Kahya, 2007). Türkiye'deki birçok devlet kurumunda belirlenen kurallar çerçevesinde bilgi sistemleri izlenir ve olası tedbirler raporlanır. Bu uygulamada en düzenli gerçekleştirenler bankalardır.

Bu önlemler, Türkiye'deki bilgi merkezlerinin siber tehditlere karşı korunmasını ve dijital varlıklarının güvenliğini sağlamada kritik rol oynamaktadır. Türkiye'deki bilgi merkezlerinde uygulanan siber güvenlik önlemleri, dijital varlıkları koruma konusunda önemli bir adım olsa da sürekli gelişim ve uyum gerektiren bir alandır. Teknolojik yeniliklerin takibi, personel eğitiminin sürekliliği ve yerel çözümlerin daha da geliştirilmesi,

bu önlemlerin etkinliğini artırabilir. Ayrıca, düzenleyici çerçevenin sadeleştirilmesi ve uyum süreçlerinin kolaylaştırılması, bilgi merkezlerinin siber güvenlik önlemlerini daha etkin bir şekilde uygulamalarına yardımcı olabilir.

7.DEĞERLENDİRME

Siber güvenlik bakış açısı, yapılan çalışmalarla birlikte ulusal ve uluslararası çalışmalar temelinde yeni bir boyut haline gelmiştir. Çalışmada bilgi yönetim sürecinden ve gerekliliklerinden siber güvenlik ilişkisine kadar incelendiğinde siber güvenlik önlemlerinin bir prosedür haline getirilerek kullanılmasının daha uygun ve sistematik olacağı öngörülmüştür. Daha stratejik davranılarak siber güvenlik alanında uzun vadeli planlamaların yapılmasını gerektirmektedir. Verimli bir sonuç elde edileceği ve bilgi güvenliğini başından sonuna daha nitelikli hale geleceği öngörülerek bazı güvenlik şirketlerinin ve kurumların bu sorumluluğu yerine getiriyor olması da bilgi güvenliğine karşı bilinçlenmelerin olduğunu göstermektedir. Bazı kurumların bu anlamda çalışma yaptığı fakat yaygın tasarım olmadığı buna ilave olarak kurumlarda bilgi güvenliği ve siber güvenlik alanlarında farkındalık oluşturabilecek çalışmalar gerekli görülmüştür. 27001 ISO'ya göre kurumlarda standardın sağlanması gerekmektedir.

Bilgi ve belge yönetimi alanında bilgi güvenliği politikasını inceleyen doktora ve yüksek lisans çalışmasının yapılmadığı ortaya çıkmıştır. Farklı alanlardaki bilgi güvenliği politikası incelenerek siber stratejilerdeki eksiklikler gözlemlenmiştir. Bilgi yönetimindeki siber stratejilerin daha uygun hale getirilmesi için finansal desteğin olması ve üst yönetimin desteğinin olması önemli faktör olarak görülmektedir. Bunlara ek olarak teknolojik cihazlarda son teknoloji kullanmanın önemli olduğu ve çalışanların farkındalığının olması gerekliliği ortaya konulmaktadır. Bilgi güvenliği yönetim süreci içerisinde de çalışanlar için ve siber güvenliğin anlaşılması için eğitimlerin yapılması ve eğitim içeriklerinin daha siber odaklı olmasına özen gösterilmesi gerektiği ortaya çıkmıştır.

Türkiye'de siber güvenlikle alakalı strateji ve politikalarda çalışmalarını sürdüren BTK, TÜBİTAK, SGE gibi kurumların siber güvenliği daha duyulur hale getirmeleri gerekli görülmektedir. Alternatif kurumların da oluşması bu alanın daha çok gelişeceğini göstermektedir. Bunlara ek olarak SOME' nin siber olaylara müdahalesiyle birlikte siber caydırıcılığa katkısının olduğu görülmüştür. Buna benzer oluşumların artması da siber saldırılara karşı caydırıcı olabileceği düşünülmektedir.

Siber saldırılara maruz kalan bilgi merkezlerinin de hazırlıklı olması gerektiği ortaya konulmaktadır. Kütüphanelerde kontrollü erişimlerle ve kimlik doğrulama işlemleriyle önlemler alınmaya çalışılmaktadır fakat bu önlemlerin artması bilgi merkezlerini daha güvenli hissettirecektir. Bu sebeple verilen hizmetlerde ve siber güvenlik önlemlerinde daha fazla hedefler belirlenmesi beklenmektedir. Dijital ortamdaki her bilginin de güvenli olmasını sağlamak gerekmektedir.

Bu çalışmada bilgi yönetim süreci ve siber güvenlik gereklilikleri ele alınmıştır. Araştırma sürecinde yapılan literatür taraması, bilgi yönetiminin stratejik yaklaşımını, nasıl kullanıldığını ve bilgi akışının etkin olabilmesi için ne denli önemli olduğunu ortaya koymuştur. Tezde bilgi yönetim uygulamalarını, ulusal ve uluslararası siber güvenlik önlemlerini ve bilgi yönetiminde siber güvenliğin kullanımının önemine değinilmiştir. Özellikle günümüz çağında doğru bilgiye erişimin sağlanması, işletmelerin başarıya ulaşmasında belirleyici bir faktördür.

Bilgi yönetim sürecinde bilgi merkezlerinin yeri ve önemi ve bilgi yönetiminde siberin nerelerde yer alabilirliği üzerinde de durulmuştur. Araştırma sonucunda, bilgi yönetimi sürecinin daha etkin hale getirilebilmesi için bazı önerilerde bulunulmuştur. Bu öneriler, bilgi teknolojilerinin kullanımı, siber güvenlik eğitim programları ve bilgi yönetiminde dikkat edilmesi gerekenler, merkezlerinde siber güvenlik kullanımı kapsamaktadır. Özellikle bilgi organizasyonlarındaki iletişimin güçlendirilmesi siber güvenlik bilinçlendirilmesi bilgi yönetimi uygulamalarının başarısını artıracaktır.

8. SONUÇ VE ÖNERİLER

Bilgi kavramının ne zaman güç olduğu anlaşıldıysa o günden bugüne bilgiye verilen önem artmıştır. Bilgi kavramının gelişmesinin beraberinde olgunlaşan bilgi toplumu düzeni de önemlilik sırasını korumaktadır. Gelişen ve yaygınlaşan bu toplum düzeninde bilgi teknolojileri kullanımında ciddi artışlar olmuştur. Bilim ve teknolojinin gelişmesiyle birlikte bilgisayar ve internetin hayatımıza çok büyük katkısı olmuştur. Bu sebeple dünyada pek çok alanda internet kullanımı yaygınlaşmıştır. Bilgi teknolojilerindeki bu ilerlemelerin sonucu olarak da bilgi yönetim yaklaşımlarında da farklı bakış açıları oluşmaktadır. Bilgi yönetimine genel bir bakış açısı olsa da değişen ve gelişen dünyada bilgi yönetim şekillerinde de gelişme gözlemlenmiştir. Elektronik ortama aktarılan bilgilerin yönetimi teknik manada olmaktadır. Bilginin üretilmesi, aktarılması, sağlanması ve kullanılması her anlamda elektronik ortamdadır. Bu süreç kapsamında göz ardı edilmemesi gereken en önemli unsurlardan biri de bilgi güvenliğidir. Bu durumda bilgi güvenliğinde zafiyet olması sebebiyle birçok tehlikeyi de beraberinde getirmektedir. Bilgi güvenliği teknolojik boyutuyla bakıldığında küresel etki bırakan bir yapıdadır fakat sadece teknik değildir. Bilgi güvenliğinin sağlanmasında bireyler, kurumlar ve hatta ülkeler de etkilidir. İnsan faktörü de bu halkada en zayıf olan halkadır. Bu nedenle bilgi yönetimini sağlamak için uyulması gereken yazılı prosedürlerin olması ve bilinçlendirme yapılması gerekmektedir.

Teknoloji ve bilgi teknolojilerinin günlük hayatımızın vazgeçilmez birer parçası haline gelmesinin yanında, kamu ve özel sektör tarafından sunulan hizmetlerin de büyük bir kısmı bilgi güvenliği ilkelerine uygun olarak elektronik ortama aktarılmıştır. Bu süreçte siber güvenlik ve emniyet ilkelerine de dikkat edilmiştir. Bilgi güvenliği ile siber güvenliği ile birbirinden ayırmak mümkün değildir. Bütünleşmiş bir yapıda olan bu güvenlik düzeni sürdürmek bireylerin, kurum ve kuruluşların, devletlerin lehine bir durum olmuştur. Belirlenen siber güvenlik kurallarına uyulması, siber stratejilerin düzenlenmesi ve geliştirilmesi siber gelişim için fayda sağlamıştır. Aynı zamanda bilgi yönetiminde siber güvenliğin de kullanılıyor olması veri güvenliği, iş sürekliliği, yasal düzenlemeler açısından faydalı bir çalışmadır. Bu çalışma; etkili bir siber güvenlik stratejisinin, sadece teknolojik önlemlerle sınırlı kalmaması gerektiğini, aynı zamanda insan faktörünü ve örgütsel yapıyı da dikkate alması gerektiğini göstermiştir. Siber güvenlik önlemlerinin başarısı, çalışanların

farkındalığı ve eğitimi ile doğrudan ilişkilidir. Ayrıca, sürekli güncellenen ve test edilen güvenlik politikalarının, bilgi yönetim süreçlerinin bütünlüğünü ve güvenliğini sağlamak için kritik olduğu gerçeği de ortaya çıkmıştır. Bu sebeple de kurumlarda ve bilgi merkezlerinde çalışan personelin ve kullanıcıların siber güvenlik farkındalığını sürekli kılmak için düzenli eğitimler ve bilinçlendirme programları artırılmalıdır. BTK Akademi gibi platformlar üzerinden interaktif eğitimler ve görsel sunumlar yapılabilir. Ayrıca, siber güvenlik tehditlerine yönelik güncel gelişmeleri içeren bültenler, çalışanlara düzenli olarak gönderilmelidir.

Bu çalışma kapsamında bilgi yönetimi süreçlerinde siber güvenlik risklerinin doğru bir şekilde tanımlanması ve yönetilmesinin, kurumlar için rekabet avantajı yaratabileceği sonucuna varılmıştır. Bu bağlamda, kurumların siber güvenlik stratejilerini geliştirirken; kapsamlı risk değerlendirmeleri yapılması gerekmektedir. Düzenli olarak güvenlik taramaları ve sızma testleri yapılmalı, zafiyet yönetimi yazılımları kullanılarak sistemlerdeki güvenlik açıkları hızla giderilmelidir. Kurumlar, bilgi varlıklarını ve bu varlıkların karşı karşıya geldikleri tehditleri düzenli olarak değerlendirmelidir. Bu değerlendirmeler, kurumların zayıf noktalarını belirlemelerine ve gerekli önlemleri almalarına yardımcı olacaktır. Çalışan eğitimi ve farkındalığı için eğitimler ve projeler düzenlenmelidir. Çünkü siber güvenlik, sadece teknik bir mesele değil, aynı zamanda insan faktörünü de içeren bir süreçtir. Çalışanların siber tehditlere karşı bilinçlendirilmesi ve düzenli eğitimlerle güncel kalmalarının sağlanması, güvenlik açıklarının minimize edilmesinde kritik rol oynamaktadır. Siber güvenlik alanında siber saldırılara karşı en büyük kalkan siber güvenlik eğitimleridir. Özellikle de kurumlarda siber yetkililerine siber saldırı olması durumunda nasıl hareket edilmesi gerektiği öğretilmelidir. Bu tür saldırılara karşılık kullanılacak yazılım ve donanımların yeterli olması ve yerli olmasına dikkat edilmelidir. Siber saldırılara karşı siber dayanıklılık kazanmak için bazı kurumsal stratejiler izlenmelidir.

Örnek olarak;

- Siber uzay gereği beklenmeyen siber saldırıyı planlamak ve nasıl savunma gerektireceği üzerinde kafa yormak olabilir.
- Kurumsal ağ yapısı üzerinden antivirüs programlarının yüklenmesi sağlanmalıdır.
- Uzaktan çalışma modeline geçiş yapan kurumlarda siber güvenliğin üst seviyede

olması gereklidir ve elzemdir.

- Kurumların mevcut sistemlerine ek olarak siber güvenlik performansını artıracak yazılımların geliştirilmesi gereklidir.
- Kuruluşların siber güvenlik eğitimlerini sadece yetkilendirilen personele değil tüm personele verilmesi gereklidir.

Bu ve benzeri detaylar kurumların siber saldırılara karşı direncini artırmakta ve siber güvenliğin bilgi yönetim sürecindeki gerekliliği daha belirgin ortaya çıkmaktadır.

Teknolojinin hızla geliştiği bir dönemde, siber tehditler de sürekli değişmektedir. Bu nedenle, kurumların en güncel teknolojik cihazları, güvenlik teknolojilerini ve yazılımlarını kullanmaları gerekmektedir. Güvenlik duvarları, antivirüs yazılımları, şifreleme teknikleri ve çok faktörlü kimlik doğrulama gibi çözümler, bilgi yönetim süreçlerinde güvenliği artıran önemli unsurlardır. Bu unsurlara da dikkat edilerek çalışmalar gerçekleştirilmelidir. Siber güvenlik stratejileri, dinamik ve sürekli güncellenen bir yapıda olmalıdır. Tehditlerin ve teknolojilerin değişkenliği göz önünde bulundurularak, kurumların güvenlik politikalarını ve protokollerini düzenli olarak gözden geçirmeleri ve güncellemeleri gerekmektedir. Denetleme düzeninin de olması gereklidir. Siber süreçleri denetleyip uygun olmayan taraflarını tespit eden ve güncellenmesi için çaba gösteren bir organizasyonun da gerekliliği ortaya çıkmıştır.

Siber güvenlik sürecini yürüten ulusal ve uluslararası çalışan yönetimler vardır. Bunların varlığı siber güvenliğin ilgili kurumlarda uygulanabilirliğini artırmaktadır. Ulusal siber güvenlik stratejileri de ülkeleri siber tehditlerden korumak amacıyla oluşturulmaktadır. Bu stratejiler siber güvenliğin nasıl uygulanması gerektiğine dair rehber niteliğindedir. Kurumlarda yılda en az bir kez tam kapsamlı felaket kurtarma tatbikatları düzenlenmeli ve sonuçlar detaylı bir şekilde analiz edilerek planlar güncellenmelidir. Kurumlarda yaşanan olumsuzluklara rağmen "*Tüm bu olumlu/olumsuz potansiyellerden korunabilmek amacıyla bilgi güvenliğine önem vererek çalışmalarına devam eden devlet kuruluşları ve/veya özel işletmelerde, özellikle yerli ve milli güvenlik yazılımı programları kullanılmalı, veri güvenliği açısından yerli kriptolama programlarının sürekli güncelleştirilmesi*

sağlanmalıdır" (Şeşen & Kuzucuoğlu, 2021) gibi bir çıkarım yapmak mümkündür. Buna örnek olarak **"***Ülkemizde son yıllarda, 'Türkiye Siber Güvenlik Kümelenmesi' organizasyonu ile bu konuda 'Siber Güvenlik Fikir Yarışması' düzenlenmiş olup çeşitli alanlarda yerli ve milli ürünler üretilmesi konusunda önemli adımların atılmakta olduğu görülmektedir"* (Özbilen & Çağlar, 2020)**.** Bu uygulamalar sayesinde siber güvenlik alanında ülkemizde yeniliklere yol açılmıştır. Çünkü bu yarışma; siber güvenlik alanındaki yetenekleri ve yenilikçi çözümleri teşvik etmek amacıyla düzenlenen bir etkinliktir. Bu tür yarışmalar genellikle üniversite öğrencileri, genç profesyoneller ve siber güvenlik uzmanları arasında düzenlenir ve çeşitli kategorilerde siber güvenlik sorunlarına yaratıcı çözümler geliştirmeyi hedefler.

Türkiye'de de siber güvenlik stratejilerini belirlemek için siber güvenlik stratejileri ve politikaları üzerinde çalışılmıştır. Siber tehditlerden korumak, siber güvenlik farkındalıklarını artırmak amacıyla oluşturulan politikalar ilgili kurumlardan uygulanması istenmektedir. Türkiye'de siber güvenlik kapsamındaki çalışmaları yürüten kurumlar çalışmalarıyla göz önünde olmayı başarmışlardır. Bu kurumlar ve yaptıkları çalışmalar; BTK, TÜBİTAK, TÜBİTAK BİLGEM, SGE, Siber Güvenlik Kurulu, USOM ve Kamu-Net'tir. Türkiye'nin siber stratejilere ve siber tehditlere karşı tedbirleri ve uygulamaları bu kurumlar yapmaktadır. Türkiye'nin siber stratejileri güncel ve dinamik bir yapıdadır. Bu dinamikliği devam ettirebilmek için Türkiye'nin siber güvenlik politikalarının sürekli olarak gözden geçirilip güncellenmesi ve iyileştirilmesi, siber güvenlik alanında elde edilecek başarının kalıcı ve sürdürülebilir olmasına katkı sağlayacaktır. Bu sebeple TÜBİTAK, BTK ve üniversiteler aracılığıyla siber güvenlik konusunda Ar-Ge faaliyetleri teşvik edilmeli, yerli teknoloji üreticileri ve bilgi merkezleri arasında işbirlikleri geliştirilmelidir.

Türkiye'nin Küresel Güvenlik Endeksi (Global Security Index) sıralaması, ülkenin siber güvenlik kapasitelerini ve tehditlere karşı hazırlık seviyesini gösteren önemli bir göstergedir. Uluslararası Telekomünikasyon Birliği (ITU) tarafından yayımlanan bu endeks, ülkelerin yasal, teknik, organizasyonel kapasitelerini, siber güvenlik eğitimi ve iş birliği alanındaki performanslarını değerlendirmektedir. Türkiye'nin Küresel Güvenlik Endeksi'nde başarılı bir şekilde yer alması için tüm kurum personellerine bazı eğitimler

vererek daha temkinli daha nitelikli personel kitlesi oluşturmalıdır. Bu eğitimlerin içeriği:

- Bilgisayar yönetimi
- Şifre oluşturma ve yönetme
- Güvenli kod değişimi
- Antivirüs uygulamaları
- Veri kaybına karşılık yedekleme
- E-posta yönetimi
- Risk yönetimi
- Değişiklik ve güvenlik yönetimi
- Dosya yönetimi
- Donanım ve yazılım
- Yenilik Yönetimi
- Siber güvenlik kalkanı oluşturma ve daha birçok belirlenecek konularla personeli bilinçlendirmek için gereklidir.

Türkiye'nin siber bağımlılığını azaltmak için ENISA'nın (European Union Agency for Cybersecurity) bünyesine katılması uygun olabilir. ENISA Avrupa Birliği'nin siber güvenlik ajansıdır ve AB üye ülkelerine siber güvenlik konusunda destek sağlamak, rehberlik etmek ve politika geliştirmekle sorumludur. ENISA, bilgi güvenliği, siber tehditler ve risk yönetimi konularında araştırmalar yapar ve en iyi uygulamaları teşvik eder. Bu durumda Türkiye siber güvenlik açıklarını kapatabilecek güce ve bilgiye sahip olabilir. Ayrıca ENISA'ya üyelik yasal altyapı ve güveni sağlayacağından siber caydırıcılığı da üst seviyede olacaktır. Bu durum, "Türkiye'nin siber tehditlere karşı direncini artırarak hem bireylerin hem de kurumların dijital dünyada daha güvende olmalarını sağlayacaktır" (Arslan, 2023).

Bilginin yönetimi uygulanması ve yönetiminin olduğu bilgi merkezlerinde bilgiye verilen önem en üst seviyede olmalıdır. Bilgi merkezlerindeki bilgi güvenliği önlemleri;

- Kütüphanelerde dijital verilere ve sistemlere erişim, yalnızca yetkili personel ve kullanıcılarla sınırlandırılmalıdır.

- Kullanıcı adı ve güçlü şifre gibi kimlik doğrulama yöntemleri kullanılabilir. Hem depolanan verilerin hem de ağ üzerinden aktarılan bilgilerin şifrelenmesi, yetkisiz erişim durumunda verilerin korunmasını sağlar.
- Kütüphane ağlarını ve bilgisayarlarını dış tehditlerden korumak için güvenlik duvarları ve güncel antivirüs yazılımları kullanılmalıdır.
- Kütüphaneler, veri kaybı riskine karşı düzenli yedeklemeler yapmalı ve acil durumlarda verilerin geri yüklenmesi için kurtarma planları geliştirmelidir.
- Kütüphane personeli ve kullanıcılarına bilgi güvenliği konusunda düzenli eğitimler verilerek, olası siber tehditler ve güvenlik ihlalleri konusunda farkındalık kazandırılmalıdır.
- Kütüphanelerde kullanılan tüm yazılımlar ve sistemler, güvenlik açıklarını önlemek için düzenli olarak güncellenmelidir.
- Kütüphanelerde bilgi ve veri saklanan cihazların fiziksel olarak güvenli ortamlarda tutulması önemlidir. Bu, yetkisiz kişilerin donanımlara erişimini engelleyebilir.
- Kullanıcıların kütüphane sistemlerine kaydettiği kişisel bilgilerin korunması yasal düzenlemelere uyumlu şekilde gerçekleştirilmelidir.

Bilgi politikalarının değişim sürecinde, siber güvenlik standartlarında, stratejilerinde bilgi merkezlerinde bilgi uzmanlarına verilen değerin daha fazla olması gerekmektedir. Zeynep Akdoğan(2022)'ın yaptığı çalışmada %5 oranında ankete katılan BBY uzmanı olan bireylerin, çalıştıkları kurumda bilgi politika değişikliklerinden haberdar oldukları gerçeği ile bilginin güncellendiği, yedeklendiği evrede BBY uzmanlarının olmadığı gerçeği ortaya çıkmıştır. Aksine diğer meslek gruplarından olan bireylerden daha çok bilgi yönetimine, bilgi güvenliğine ve bilgi güvenliği politikalarına aşinadırlar. Bu sebeple de bilgi uzmanlarının bilgi yönetim süreçlerinde, siber güvenlik süreçlerinde bulunması daha yaygınlaştırılmalıdır.

Sonuç olarak, bilgi yönetimi süreçlerinde siber güvenliğin sağlanması, sadece kurumların operasyonel verimliliğini artırmakla kalmaz, aynı zamanda itibarı ve müşteri güvenini de korur. Bilgi yönetiminde etkili bir siber güvenlik uygulaması, sadece tehditleri

tespit etmek ve yanıtlamakla sınırlı kalmamalıdır. Aynı zamanda, sürekli risk değerlendirmesi ve güvenlik açıklarının yönetimini gerektirir. Bu, bilgi sistemlerinin güvenlik seviyesini sürekli olarak iyileştirmek ve ortaya çıkan yeni tehditlere karşı proaktif bir yaklaşım benimsemek anlamına gelir. Bilgi yönetimi süreçlerinde siber güvenlik, dijital ortamda güvenli ve verimli bir bilgi yönetimini sağlamanın temel unsuru olarak öne çıkar. Kurumların siber güvenlik stratejilerini ve uygulamalarını güçlendirmeleri, bilgi güvenliğini artırmakla birlikte, operasyonel riskleri minimize eder ve uzun vadeli başarıyı destekler. Bu bağlamda, siber güvenliğin bilgi yönetimi süreçlerinin ayrılmaz bir parçası olarak ele alınması, bilgi varlıklarının korunması ve organizasyonel sürdürülebilirliğin sağlanması açısından kritik öneme sahiptir.

Günümüz dünyasında da onca yapay zekâ, teknolojik gelişmelerin olması güvenlik önlemlerinde de sürekli gelişimi takip etmeyi gerektirmektedir. Siber güvenlik önlemlerinin anlaşıldığı ve standartlaşmış programlarla uygulandığı süreçlerin daha yaygın hale getirilmesi gerekmektedir. Kurumların özelinde siber gelişime daha fazla bütçe ayrılmalıdır ve daha fazla önlemler alınmalıdır. Veri kayıplarının sonucunda kurumların telafisi olmayan çıkmaza girmesi durumunda kullanabilecekleri bir risk yönetimleri hazırda bulunması gerekli ve elzemdir. Süreçleri yönetenlerin belirlenmesi ve olası saldırılarda korunabilmesi için süreç yönetimi de yazmaları daha uygun olacaktır. Hayata geçirilecek siber güvenlik uygulamalarının mutlaka test aşamasından geçmesi ve sonrasında uygulanması gerekmektedir. Kurumların siber saldırı ile karşılaşmaları durumunda uygulayacakları stratejiler kesinlikle belirlenmelidir.

Son olarak bu çalışma, bilgi yönetim süreçlerinin güvenliğinin sağlanmasının, bütünsel bir yaklaşımla ele alınması gerektiğini ve bu yaklaşımın kurumlara uzun vadeli faydalar sağlayacağını göstermektedir. Bu bağlamda, siber güvenliğin bilgi yönetimi süreçlerine entegrasyonu, gelecekte de araştırma ve uygulama alanında önemli bir konu olarak kalacaktır.

Singer’in (2015) şu sözü ile siber güvenlik dünyasına farklı bir akış açısı eklenebilir. “Eskiden nasılsa, gelecekte de öyle olacaktır. Bu dünyanın -hem çevrim içi hem de gerçek- risklerini kabul etmeli ve yönetmeliyiz, çünkü her şeye burada ulaşabiliriz. Ve bu da gerçekten herkesin bilmesi gerekendir” (Singer & Friedman, 2018).

9. KAYNAKÇA

ADL Uluslararası Belgelendirme ve Eğitim. (2020). ISO27001. https://www.adlbelge.com/iso-27001-bilgi-guvenligi-risk-yonetim-proseduru/adresinden 6 Haziran 2024 tarihinde alınmıştır.

Akdoğan, Z. (2022). *Kamu Kurumlarında Bilgi Güvenliği Yönetim Sistemleri İçin Politika Geliştirme Metodolojisi.*[*Doktora Tezi,* Ankara Üniversitesi].YÖK Tez Merkezi.

Akyön, F. V. (2001). Bilgi Kavramı ve Yönetimi. *Öneri Dergisi, 4*(15), 167-172. https://doi.org/10.14783/maruoneri.735506

Alaca, E. (2021). *Türkiye'deki Halk Kütüphanesi Yönetim ve Hizmet Yapısının Yenilikçi Örgüt Kültürü Açısından Değerlendirilmesi*. [*Doktora Tezi*, Ankara]. YÖK Tez Merkezi.

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

Ard Bilişim Yazılım Teknolojileri . (2011). https://www.ardbilisim.com.tr/bilisim-altyapisi-ve-veri-guvenligi-cozumleri/ 7 Temmuz 2024 tarihinde alınmıştır.

Arslan, S. F. (2023). *21. Yüzyılda Ulusal Ve Uluslararası Siber Güvenlik:Türkiye'nin Siber Güvenlik Strateji ve Politikaları.*[Yüksek Lisans Tezi, İstanbul]. YÖK Tez Merkezi.

Arşiv Hizmetleri Hakkında Yönetmelik. (2024). Mevzuat Bilgi Sistemi. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=9189&MevzuatTur=7&MevzuatTertip=5 adresinden 06 Haziran 2024 tarihinde alınmıştır.

Atan, S. (2020). Bulut Bilişim ve Geleneksel Alternatiflerinin Karşılaştırılması: İşletmeler için Avantajlar, Riskler ve Geçiş Önerileri. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 22(3), ss. 747-759.

Avcı, U., & Avcı, M. (2004). Örgütlerde Bilginin Önemi ve Bilgi Yönetim Süreci. *Mevzuat Dergisi*(74), ss. 1-14. https://www.mevzuatdergisi.com/2004/02a/01.htm

Aydın , H., Barışkıran, M. A., & Çetinkaya, A. (2021). Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi. *Güvenlik Bilimleri Dergisi,, 10*(1), ss. 151-174.

https://doi.org/10.28956/gbd.941801

Aydın, S. (2024). *Bilgiye Erişimin E-hali: Dijital Kütüphaneler*. https://www.zdergisi.istanbul/makale/bilgiye-erisimin-e-hali-dijital-kutuphaneler-634 adresinden 09.10.2023 tarihinde alınmıştır.

Balcılar, H. (2008). *Türkiye'nin Bilgi Toplumu Olma Yolunda Bilgi Teknolojilerinden İnternetin Kullanımı:Muş İlindeki İnternet Kafe Kullanıcılarının Amaçları Üzerinde Bir Araştırma*.[Yüksek Lisans Tezi, Konya].YÖK Tez Merkezi.

Barutçugil , İ. (2002). *Bilgi Yönetimi*, Kariyer Yayıncılık.

Baykara, M., Daş, R., & Karadoğan, İ. (2013,Mayıs 20-21). *Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi.* [1st International Symposium on Digital Forensics and Security].

Bayter, M. (2015). *Bilgi Merkezleri ve Kaynakları Tarihi*[Ders Notları]. Ankara.

Bayter, M., & Yıldırım, K. (2023). Dijital Kütüphaneler ve Sosyal Medyanın Sentezi: Bilgi Paylaşımında Yenilikçi Güç. *Library Archive and Museum Research Journal*, 4(2), 185-200. https://doi.org/10.59116/lamre.1328838

BBS Belgelendirme. (2024). BBS Belgelendirme Eğitim ve Gözetim Hizmetleri: https://www.bbsas.com.tr/iso-27001-2022-bilgi-guvenligi-yonetim-sistemi/ adresinden 11.10.2024 tarihinde alınmıştır.

Bedük, A. (2008). Türkiye'nin Bilgi Toplumu Olma Yolunda Bilgi Teknolojilerinden İnternetin Kullanımı: Muş İlindeki İnternet Kafe Kullanıcılarının Amaçları Üzerinde Bir Araştırma. [*Yüksek Lisans Tezi*, Konya]. YÖK Tez Merkezi.

Bıçakcı, S., Çelikpala, M., Han, A. K., Kasapoğlu, C., & Ergun, D. (2016). *Türkiye'de Siber Güvenlik ve Nükleer Enerji.* Araştırma, EDAM. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/ _siber_guvenlik_raporu.pdf adresinden 23.11.2023 tarihinde alınmıştır.

Bilgi Teknolojileri ve İletişim Kurumu . (2024). BTK. https://www.btk.gov.tr/siber-guvenlik-kurulu adresinden 24.12.2023 tarihinde alınmıştır.

Bilgi Teknolojileri ve İletişim Kurumu. (2024). BTK. https://internet.btk.gov.tr/kisisel-veriler-ve-kisisel-bilgi-guvenligi adresinden 24.12.2023 tarihinde alınmıştır.

B. Yılmaz , & F. Özdemirci.(10-11 Ekim 2022). Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv- eDevlet- Bulut Bilişim-Büyük Veri- Yapay Zekâ. *Bilgi Yönetimi ve Bilgi Güvenliği.* [E-BEYAS].

Bilişim Academy. (2024). Bilişim Academy: https://bilisimacademy.com/blog/phishingoltalama-nedir/ adresinden 17.06.2023 tarihinde alınmıştır.

BTK Akademi. (2024). *Bilgi Güvenliği Yönetim Sistemleri Dersi*. https://www.btkakademi.gov.tr/portal/course/bilgi-guvenligi-yonetim-sistemi-9633 adresinden 06 01, 2024 tarihinde alınmıştır.

CBDDO. (2024, 07 15). *Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi*. KamuNet Projesi: https://cbddo.gov.tr/projeler/kamu-net/ adresinden 14.06.2023 tarihinde alınmıştır.

Çakır, H., & Arınmış Uzun, S. (2021). Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi. Ekonomi İşletme Siyaset Ve Uluslararası İlişkiler Dergisi, 7(2), 353-379.

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

Şişkin, D. Ş., & Çakmak, T. (2020). Üniversite Kütüphanelerinde Kişisel Veriler: Ankara'daki 15 Üniversite Kütüphanesindeki Uygulamaların Analizi. Türk Kütüphaneciliği, 34(3), 458-484. https://doi.org/10.24146/tk.754346

Çelik, K. (2021). Bulut Bilişim Teknolojileri. Bartın Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi, 12(24), 436-450. https://doi.org/10.47129/bartiniibf.1019898

Çetin, H. (2014). Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. Akdeniz İİBF Dergisi, 14(29), 86-105.

Çoban , H. (1997). *Bilgi Toplumuna Planlı Geçiş.* İstanbul: İnkılap Kitabevi.

Çubukçu, F. (2018). *Bilgi Güvenliği Yönetim Sistemi: ISO 27001:2013 Uygulama Kılavuzu.* Pusula Yayıncılık.

Çuhacı, A. (2012). Ulrıch Beck'in Risk Toplumu Kuramı. İstanbul University Journal of Sociology, 3(14), 129-157.

Darıcılı, A. B. (2019). Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler. *TESAM Akademi Dergisi*, 6(2), 11-33. https://doi.org/10.30626/tesamakademi.613517

Davenport, T., & Prusak, L. (1998). *Working Knowledge: How Organizations Manage What They Know*. Harvard Business School Press.

Deloitte . (2024). Deloitte: https://www2.deloitte.com/tr/tr/pages/risk/articles/ethic-hackers.html adresinden 03.17.2024 tarihinde alınmıştır.

Demirel, F. T. (2023). Araştırmalarda Kullanılan Yöntem ve Teknikler: Sosyoloji Araştırmaları Dergisi İçerik Analizi. *Veche*, 2(1), 30-43.

Demirtaş, H. (2013). *Bilgi Güvenliği Yönetiminin Gerekleri ve Başarı Dayanakları: Bir Uygulama Örneği*.[Yüksek Lisans Tezi,Sakarya].YÖK Tez Merkezi.

Dhillon, G., & Backhouse, J. (2002). The Role of Information Security in the Organization. *Communications of the ACM, 44*(9), 125-128. doi:10.1145/382205.382282

Kanunlar: 5809 sayılı Elektronik Haberleşme Kanunu, R.G.T. 5/11/2008, S.27050.

Kanunlar: 5070 sayılı Elektronik İmza Kanunu, R.G.T. 15/1/2004, S. 25355.

Eroğlu Yalın, B., & Şahin Başfırıncı, Ç. (2018). Cybersecurity Perceptions Of University Students In Turkey. Karadeniz Teknik Üniversitesi İletişim Araştırmaları Dergisi, 8(2), 2-14.

Yılmaz, E. N., Gönen, S., Şanoğlu, S., Karacayılmaz, G., vd. (2021). Endüstri 4.0'ın Gelişim Sürecinde Unutulan Bileşen: Siber Güvenlik. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 9(4), 1142-1158. https://doi.org/10.29130/dubited.905340

Güçlü, N., & Sotirofski, K. (2006). Bilgi Yönetimi. Türk Eğitim Bilimleri Dergisi, 4(4), 351-373.

Güngör, U., & Güney, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. Karadeniz Araştırmaları, 14(55), 131-146.

Güntay, V. (2016). *Uluslararası İlişkiler Temelinde Siber Güvenlik : Mikro Siber İttifak Teorisi (Micro-CAT)*.[Doktora Tezi,Trabzon]. YÖK Tez Merkezi.

Güntay, V. (2017). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu;

Siber Savaş Örneği. Güvenlik Bilimleri Dergisi, 6(2), ss. 81-108. https://doi.org/10.28956/gbd.354150

ISO27001: Bilgi Güvenliği İhlal Prosedürü . (2016).

ISO27001: Bilgi Güvenliği Risk Yönetimi Prosedürü. (2016).

Kahya, E. (2007,31 Ocak-2 Şubat). *Bilgisayar Ağ Sistemleri Güvenliği*. Akademik Bilişim'07 - IX. Akademik Bilişim Konferansı Bildirileri, Kütahya, 279-288.

Karaoğlan Yılmaz, D. F. G., Yılmaz, D. R., & Sezer, B. (2014). Üniversite Öğrencilerinin Güvenli Bilgi ve İletişim Teknolojisi Kullanım Davranışları ve Bilgi Güvenliği Eğitimine Genel Bir Bakış. Bartın University Journal of Faculty of Education, 3(1), 176-199.

Karasoy, H. A., & Babaoğlu, P. (2021). Türkiye'de Siber Güvenlik: Yasal Ve Kurumsal Altyapı. *Yasama Dergisi*(44), 123-155.

Karataş A., E. (2015). Dijitalleştirme Süreci Ve Dijital Kütüphane Uygulamalarına Bir Bakış. *Journal of Turkish Studies*, 10(10), ss. 561-574.

Emre Kaya, A. E. (2010). Enformasyon Toplumunun Suçluları: "Hacker"lar. Marmara İletişim Dergisi(16).

Koçak, H., & Memiş, K. (2018). Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu. Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi, 20(3), ss. 1-10. https://doi.org/10.32709/akusosbil.484559

Korucu, O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik ve Bilgi Güvenliğine Etkileri. Yönetim Bilişim Sistemleri Dergisi, 7(1), ss. 44-60.

KPMG. (1982). KPMG: https://kpmg.com/tr/tr/home/gorusler/2016/11/siber-guvenlikte-en-yaygin-bes-yanilgi.html adresinden 01.06.2024 tarihinde alınmıştır.

Kurnaz, S., & Önen , M. (2019). Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security*, 1(2), ss. 82-103.

M. Murugesan, P. Balamurugan, J. Santhosh, & G. Arulkumaran. (2020). Threats and Emerging Developments in Cyber Security. *Webology*, 17(2), ss. 587-598.

Özbilen, T., & Çağlar, A. (2020). Türk Kamu Sektöründe Bilgi Ve Bilişim Güvenliği. *Kamu Yönetimi ve Teknoloji Dergisi*, 2(1), ss. 72-94.

Özdemirci , F. (2019). *Kurumlar için EBYS ve e-Arşiv Sistemi İdari Yapılanma ve Yönetim Süreci: Bileşenler ve Entegrasyonlar.*Yalçınkaya B.,Ünal M.Altay, Yılmaz B.,Özdemirci F.(Ed.), Bilgi Yönetimi ve Bilgi Güvenliği. Bilgi Yönetim Sistemleri Belgelendirme ve Bilgi Güvenliği Merkezi (BİL- BEM).

Özdemirci, F., & Torunlar, M. (2018). Bilgi-Değişim-Siber Güvenlik-Bağımsızlık. *Bilgi Yönetimi*, 1(1), 78-83.

Özdemirci, F. (2019). Milli e-Arşiv Bilgi Sistemi Ağı ve Veri Merkezi Yapılanma Önerisi: Yenilikçi Teknolojiler-Yeni Nesil Arşivciler-Yapay Zekâ ve Ötesi . Bilgi Yönetimi, 2(2), 169-176.

Özdemir, E. G., Karalı, H., & Çiçek, İ. (2022). Tapu Ve Kadastro Genel Müdürlüğünde Dijital Dönüşüm: E-Arşiv. Arşiv Dünyası, 9(2), ss. 157-189. https://doi.org/10.53474/ad.1158549

Parvin, S., Sadoughi, F., Karimi, A., Mohammadi, M., & Aminpour, F. (2019). Information Security from a Scientometric Perspective. *Webology*, 196-209.

REISSWOLF. (2021). https://reisswolf.com.tr/cozumler/dokuman-yonetimi?gad_source=1&gclid=Cj0KCQjwhb60BhClARIsABGGtwh8hhYEeV_lhRh4oeZUBznuwkQ9nIQymkryJ_3iUArNA5tn2Sj8-EaAol2EALw_wcB# adresinden 04.11.2023 tarihinde alınmıştır.

Sayyarer, E., Kınacı, B. F., & Güven , E. Y. (2023). *Bilgi ve Bilişim Sistemleri Güvenliği.* Nobel Bilimsel Eserler. https://turkviewer.libraryturk.com/webviewer.php?doc=446049 adresinden 04.11.2023 tarihinde alınmıştır.

Sebetci, Ö. (2018). G. Dönük, D. G. Öztürk, E. Güler, M. C. Hanaylı, M. B. Günay, P. Gayret, A. Dilek.Sebetci S. (Ed.): *Bilgi Teknolojileri ve Yönetim Bilişim Sistemleri* (ss. 2-46). Kodlab.

Selvi, Ö.Ö. (2012). Bilgi Toplumu, Bilgi Yönetimi ve Halkla İlişkiler. *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 1(3), 192-214.

Singer, P. W., & Friedman, A. (2018). *Siber Güvenlik ve Siber Savaş.* Buzdağı.

Singh, B., & Singh, N. (2020). MoLaBSS: Server-Specific Add-On Biometric Security Layer Model to Enhance the Usage of Biometrics. *Information*, 2-23.

Solmaz, S. B. (2023). Siber Güvenlik Tarihindeki Dönüm Noktaları: Tehditlerin evrimi ve savunma stratejileri. *Orta Doğu Ve Orta Asya-Kafkaslar Araştırma Ve Uygulama Merkezi Dergisi, 3*(1), 1-9.

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *SciVerse Science Direct*, 97-102.

Sümer, B. (2007). Bilgi Toplumuna Dönüşüm Sürecinin Avrupa Birliği ve Türkiye'de İstihdam Yaratmaya Etkisi.[Doktora Tezi, Dokuz Eylül Üniversitesi]. YÖK Tez Merkezi.

Şeşen, Y., & Kuzucuoglu, A. H. (2021). Veri ve Bilgi Güvenliği Bağlamında İstihbarat Faaliyetleri. *Library Archive and Museum Research Journal*, 2(2), 93-110. https://doi.org/10.29228/lamre.51218

T.C. Cumhurbaşkanlığı Resmi Gazete. (2016, Nisan 7). *Kişisel Verilerin Korunması Kanunu, 57(29677).* Kişisel Verileirn Korunması Kanunu. https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm adresinden alınmıştır.

Taş, O., & Kiani, F. (2021). Nesnelerin İnterneti (IoT) ve Kablosuz Algılayıcı Ağların Güvenliğine Yapılan Saldırıların Tespit Edilmesi ve Önlenmesi. *Politeknik Dergisi*, 24(1), 219-235. https://doi.org/10.2339/politeknik.627825

Taşbaş Ustaoğlu, E., & Mayatürk Akyol, E. (2021). Bilgi Yönetimine İlişkin Kavramsal ve Kuramsal Bir İnceleme. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 16(1), 23-37.

TDK. (1932). *Türk Dil Kurumu Sözlükleri*. https://sozluk.gov.tr/ adresinden 24.08. 2024 tarihinde alındı

Tonta, Y. (1996). Internet, Elektronik Kütüphaneler ve Bilgi Erişim. *Türk Kütüphaneciliği,* 10(3), ss. 215-230.

Torunlar, M., & Özdemirci, F. (2019). *Bilginin Bilgiyle Savaşı.* Ankara Üniversitesi BİL-BEM.

Tuğal, İ., Almaz, C., & Sevi, M. (2021). Üniversitelerdeki Siber Güvenlik Sorunları ve Farkındalık Eğitimleri. Bilişim Teknolojileri Dergisi, 14(3), 229-238. https://doi.org/10.17671/gazibtd.754458

Tunca, S. (2019). Modern Çağda Siber Güvenlik Kavramı. Dumlupınar Üniversitesi İİBF Dergisi(3-4), 1-7.

TÜBİTAK. (2024). *TÜBİTAK BİLGEM*. SGE: https://bilgem.tubitak.gov.tr/sge-kurumsal/ adresinden 24.07.2024 tarihinde alınmıştır.

TÜBİTAK. (2024). *TÜBİTAK BİLGEM Kamu Sertifikasyon Merkezi Kurumsal Şifreleme Sertifika Uygulama Esasları*.Kamu SM: chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://kamusm.bilgem.tubitak.gov.tr/BilgiDeposu/KSM_SIFRELEME_SUE/KSM_SIFRELEME_SUE_v7.pdf adresinden 24.07.2024 tarihinde alınmıştır.

Türkiye İstatistik Kurumu. (2024). İstatistik Veri Portalı. https://www.tuik.gov.tr/ adresinden 23.07.2024 tarihinde alınmıştır.

Türkiye İstatistik Kurumu.(2024). İstatistik Veri Portalı: https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim Arastirmasi-2023-49407 adresinden 08.13.2024 tarihinde alınmıştır.

UAB. (2024). *T.C. Ulaştırma ve Altyapı Bakanlığı*. KamuNet: https://hgm.uab.gov.tr/kamu-net adresinden 06.09.2023 tarihinde alınmıştır.

Uğur, S. (2020). Büyük veri, nesnelerin interneti, sosyal ağlar, sanal kimlikler ve siber güvenlik. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 6(1), 4-7.

ULAKBİM. (2024). *Ulusal Akademik Ağ ve Bilgi Merkezi* . https://ulakbim.tubitak.gov.tr/ adresinden 21.05.2024 tarihinde alınmıştır.

USOM. (2024). *Ulusal Siber Olaylara Müdahele Merkezi*. USOM: https://www.usom.gov.tr/hakkimizda adresinden 21.05.2024 tarihinde alınmıştır.

Ünal, A. N. (2018). Bilgi Yönetim Sistemleri Ve Siber Güvenlik. *International Journal of Social Inquiry*, 11(2), 375-394.

Ünal, H. (2019). *Dijitalleştirme ve Kurumsal Elektronik Arşiv Yönetimi Sistemlerinin Yapılandırılması.[Yüksek Lisasns Tezi,*Ankara].YÖK Tez Merkezi.

Ünver, M., Canbay, C., & Günaydın, Y. (2011). *Köle Bilgisayar ve Köle Bilgisayar Ağları (Zombi ve Botnetler)* . Ankara. BTK.

Wazida, M., Kumar Das, A., Chamola, V., & Parkd, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, 313-321.

Yazıcıoğlu, O., Varol, K., & Borat, O. (2011). *Bilgi Yönetimi. İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 10(20), 15-32. https://doi.org/10.18521/ktd.04379

Yel, T., & Atasoy, A. (2021). Dijitalleşmenin Bağımsız Denetime Yansımalarının Siber Güvenlik Yönünden Değerlendirilmesi. *Muhasebe ve Finansman Dergisi*, ss.439-458. https://doi.org/10.25095/mufad.982624

Yılmaz, B., Cibaroğlu, M., Yalçınkaya, B., & Özdemirci , F. (2022, Ekim 10-11). Bildiri Özetleri. *e-Beyas 2022 Sempozyumu Metaverse ve Bilgi Yönetimi*. chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://2022.ebeyas.org/wp-content/uploads/2022/10/ebeyas_bildiri_ozetleri-1.pdf

Yılmaz, E., Ulus, H., & Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. Bilişim Teknolojileri Dergisi, 8(3), 133. https://doi.org/10.17671/btd.87028

Yılmaz, H. (2016). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. Denetişim(15), 45-59.

Vural, Y., & Sağıroğlu, Ş. (2013). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,* 26(1).

Zaim, H. (2010). Türkiye'de Bilgi Yönetimi Uygulamaları. Journal of Social Policy Conferences(50), 761-782.

Zeng, Y. (2022). AI Empowers Security Threats and Strategies for Cyber Attacks. *Science Direct* , 170-1 ADL Uluslararası Belgelendirme ve Eğitim. https://www.adlbelge.com/iso-27001-bilgi-guvenligi-risk-yonetim-proseduru adresinden 07.06.2024 tarihinde alınmıştır.

10. LİNKLER

https://www.kaspersky.com.tr/resource-center/threats/spyware

https://www.kaspersky.com.tr/resource-center/definitions/stealth-virus

https://www.isbank.com.tr/blog/zararli-yazilim-turleri-nelerdir

https://bilisimacademy.com/blog/phishingoltalama-nedir/

https://www2.deloitte.com/tr/tr/pages/risk/articles/ethic-hackers.html

https://www.bilimnetbilisim.com/altyapi-guvenligi/

https://www.adlbelge.com/

https://hgm.uab.gov.tr/kamu-net

https://cbddo.gov.tr/projeler/kamu-net/

https://www.usom.gov.tr/

https://www.btk.gov.tr/siber-guvenlik-genel-bilgi

https://tubitak.gov.tr/tr

https://bilgem.tubitak.gov.tr/

https://bilgem.tubitak.gov.tr/sge-kurumsal/

https://www.btk.gov.tr/siber-guvenlik-kurulu

https://www.mevzuat.gov.tr/

https://www.resmigazete.gov.tr/

11. STANDARTLAR

TS EN ISO 9000 (2004), “Kalite Yönetim Sistemleri- Temel Esasları ve Terimler ve Tarifler”, Türk Standardları Enstitüsü, Ankara.

TS ISO IEC 17799 (2006), “Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri”, Türk Standardları Enstitüsü, Ankara.

TS ISO IEC 27001(2006), “Bilgi Teknolojisi – Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimleri”, Türk Standardları Enstitüsü, Ankara.

TS ISO/IEC TR 18044 (2007), “Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği ihlal olayı yönetimi,” Türk Standardları Enstitüsü, Ankara.75.