KTO KARATAY ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI
TEZLİ YÜKSEK LİSANS PROGRAMI

KURUMLAR İÇİN BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN OLUŞTURULMASI

Ömer Şaban FİDANCI

Yüksek Lisans Tezi

KONYA
Haziran 2022

KURUMLAR İÇİN BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN OLUŞTURULMASI

Ömer Şaban FİDANCI

KTO Karatay Üniversitesi
Lisansüstü Eğitim Enstitüsü
Adli Bilişim Mühendisliği Anabilim Dalı
Tezli Yüksek Lisans Programı

Yüksek Lisans Tezi

Tez Danışmanı: Doktor Öğretim Üyesi Ali ÖZTÜRK

Konya
Haziran 2022

BİLDİRİM

Enstitü tarafından onaylanan Yüksek Lisans tezimin tamamını veya herhangi bir kısmını basılı veya dijital biçimde arşivleme ve aşağıda belirtilen koşullar dahilinde erişime açma iznini KTO Karatay Üniversitesine verdiğimi bildiririm. Bu izinle, Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak ve gelecekteki çalışmalar (makale, kitap, lisans, patent vb.) için tezimin tamamının veya bir bölümünün kullanım hakları yalnızca bana ait olacaktır.

Tezimin bütünüyle kendi çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Telif hakkı bulunan ve sahiplerinden yazılı izinle kullanılması zorunlu olan kaynakları, yazılı izin alarak kullandığımı ve istenildiğinde izinlerin suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayımlanan "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" kapsamında, tezim, aşağıda belirtilen koşullar haricince, YÖK Ulusal Tez Merkezi ve KTO Karatay Üniversitesi Açık Erişim Sisteminde erişime açılır.

☐ Enstitü / Fakülte Yönetim Kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir.[1]

☐ Enstitü / Fakülte Yönetim Kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren … ay …ertelenmiştir.[2]

☐ Tezimle ilgili gizlilik kararı verilmiştir. 34

Haziran 2022

Ömer Şaban FİDANCI

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

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

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

[4] MADDE 7(2) Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

ETİK BEYAN

KTO Karatay Üniversitesi Lisansüstü Eğitim Enstitüsü Tez Hazırlama ve Yazım Kurallarına uygun olarak Dr. Öğr. Üyesi Ali ÖZTÜRK danışmanlığında tarafımdan üretilen bu tez çalışmasında; sunduğum tüm veri, enformasyon, bilgi ve belgeleri bilimsel etik kuralları çerçevesinde elde ettiğimi, tüm değerlendirme, analiz, bulgu ve sonuçları bilimsel usullere uygun olarak sunduğumu, tez çalışmasında yararlandığım kaynakların tümüne bilimsel normlara uygun biçimde atıfta bulunarak kaynak gösterdiğimi, tezimin kaynak gösterilen durumlar dışında özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

15.06.2022

_____

Ömer Şaban FİDANCI

TEŞEKKÜR

Yüksek lisans tezimi uzun süreler boyunca emek ve özveri ile hazırlayıp tamamlamanın heyecanını ve gururunu yaşıyorum. Bu bölüme kaydolmamda beni teşvik eden Semih YUMUŞAK hocama, öğrenim boyunca yardımlarını esirgemeyen katkılarından dolayı Adli Bilişim Mühendisliği Bölümü hocalarıma, tez aşamasına gelmemde destek olan ve emeği geçen Sayın Prof. Dr. Novruz ALLAHVERDİ hocama, tez konusu ve araştırmalarımda desteğini esirgemeyen tez danışmanım Sayın Dr. Öğr. Üyesi Ali ÖZTÜRK'e, manevi desteğini esirmeyen aileme teşekkürlerimi sunarım.

15 Haziran 2022 Ömer Şaban FİDANCI

ÖZET

Ömer Şaban FİDANCI

Kurumlar için Bilgi Güvenliği Yönetim Sisteminin Oluşturulması

Yüksek Lisans Tezi

Konya, 2022

Günümüzde bilgi güvenliği ile sıkça anılan diğer iki önemli konu da siber güvenlik ve kişisel verilerin korunması alanlarıdır. Bilgi teknolojilerindeki gelişmelerle birlikte, bilgi güvenliğinin sağlanmasına yönelik gereksinimler gittikçe daha karmaşık ve kapsamlı hale gelmiştir. Sınırlı bütçe ve personel kaynakları ile kapsamlı bir bilgi güvenliği çalışması yapılması için daha sistematik ve yönetsel sistemlerin uygulanması zorunluluk haline gelmiştir. ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardında belirtilen madde baslıkları dikkate alınarak, etkin bir BGYS tesis edilmesi için siber güvenlik ile ilgili teknik tedbirlere ilave olarak yönetsel tedbirlerin de alınmasını zorunlu kılmıştır. Ayrıca kurumlarda farkındalık eğitimleri ile kurum kültürünün değiştirilmesi güvenlik önlemlerinin etkinliğini artıracak unsurlardır. Bilgi güvenliği yönetimi sistemlerinin oluşturulması amacıyla uluslararası standartlar ve Cumhurbaşkanlığı güvenlik rehberi incelenerek araştırmanın kurumlara rehber olmada katkı sunacağı tahmin edilmektedir.

Anahtar Kelimeler

Kurumlarda bilgi güvenliği, siber güvenlik, BGYS, ISO 27001, sızma testi, SIEM

ABSTRACT

Ömer Şaban FİDANCI

Creation of an Information Security Management System for Organizations

Master's

Konya, 2022

Two other critical issues that are frequently mentioned with information security today are the fields of cyber security and the protection of personal data. With the developments in information technologies, the requirements for ensuring information security have become increasingly complex and comprehensive. It has become a necessity to implement more systematic and managerial systems to conduct a comprehensive information security study with a limited budget and personnel resources. Considering the article titles specified in the ISO 27001 Information Security Management System (ISMS) standard, administrative measures and additional technical measures related to cyber security will be obliged to establish an effective ISMS. Additionally, changing the corporate culture with awareness training in institutions are factors that will increase the effectiveness of security measures. It is presumed that this research will contribute to guide institutions by examining international standards and the security guide of the Presidency in furtherance of establishing information security management systems.

Keywords

Information security in institutions, cyber security, ISMS, ISO 27001, penetration test, SIEM

İÇİNDEKİLER

KISALTMALAR DİZİNİ

Kısaltma	Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
SOME	Siber Olaylara Müdahale Merkezi
SMB	Server Message Block
KVKK	Kişisel Verileri Koruma Kanunu
GDPR	General Data Protection Regulation
CVE	Common Vulnerabilities and Exposures
PCI DSS	Payment Card Industry Data Security Standard
SIEM	Security İnformation and Event Management
FISMA	Federal Information Security Management Act
ABD	Amerika Birleşik Devletleri
FBI	Federal Bureau of Investigation
HIBAA	Health Insurance Portability and Accountability Act
COBIT	Information Systems Audit and Control Association
DDos	Distributed Denial of Service
PUKÖ	Planla-Uygula-Kontrol Et-Önlem Al

ŞEKİLLER LİSTESİ

ÇİZELGELER LİSTESİ

1. GİRİŞ

Bilgi, günümüzde kurumların elektronik ortam içerisinde en önemli varlıklarından biri haline gelmiştir. Bu yönü ile kurumların bilginin gizlilik, bütünlük ve erişebilirlik fonksiyonlarının koruma altına alınması hayati önem kazanmıştır. Bilişim teknolojilerinin ve iletişim araçlarının kullanımının artması ile kurumlar hizmetlere ilişkin sistemlere daha fazla bağımlı hale gelmişlerdir. Farklı kurum ve kuruluşlar enerji, haberleşme, bankacılık hizmetleri vb. sektörler de bilişim ve iletişim sistemlerini yoğun kullanmaktadırlar. Bilişim sistemlerinin kurumlarda yoğun kullanılması kaliteli ve hızlı bir hizmet anlayışını beraberinde getirdiğinden kurumlar arasında rekabetin her geçen gün artarak kurumsal bilgiler dijitalleştirilmiş, bu dijitalleşme beraberinde bilişim sistemlerinin gelişmesine neden olmuştur. Her geçen gün gelişen bilişim sistemlerinde siber güvenlik riskleri ve zafiyetler bilişim sistemleri altyapılarında oluşmakta ve siber saldırıların yoğunlaşarak artmasına sebep olmaktadır. Kurumlar siber tehditlere karşı çok büyük risk altındadırlar. Bilişim sistemlerinde mevcut güvenlik zafiyetleri, bu sistemlerin çalışamaz hale gelmesine, suça aracılık etmesine, can ve mal kayıplarına, toplum ve kamu düzeninin bozulmasına, güvenlik ihlallerine kadar birçok şeye neden olabilecektir.

Bilgi güvenliği kurumlar için stratejik bir öneme sahiptir. Kurum hem kendi organizasyonuna bilginin kendi kontrolünde olduğunu hem de paydaşlarına bilginin güvenilirliğini sağladığının kanıtı olarak sunabilecektir. Kurumlar işleyişlerini daha güvenli hale getirmeleri için uygulayacakları standartlar ve bilgi güvenliği yönetim sistemleri uygulamaları kurumların itibarını ve rekabet gücünü artıran bir unsur olarak da karşımıza çıkmaktadır. Bu yüzden bilgi güvenliği standartları ve bilgi sistemlerinin uygulanması konusunda gerek kurum gerek devlet gerekse kurumlara büyük bir vazife düşmektedir. Dijitalleşen çağımızda bilginin ne kadar önemli ve korunmasının gerekli olduğu göz önünde bulundurulduğunda güvenlik önlemlerinin alınması kaçınılmazdır. Bu önlemlerin uygulanmasında yasalarda desteklenmiş ve kurumların zorunlu uygulaması gereken hususlar kanunlarla da belirtilmiştir. Ayrıca Cumhurbaşkanlığı tarafından yayınlanan “Bilgi ve İletişim Güvenliği Rehberi”, kurumların bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması, kritik verinin güvenliğinin sağlanması için minimum güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için

yürütülecek faaliyetlerin tanımlanmasını amaçlayan bir rehberdir (Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2022).

Bu tez çalışması kurumların bilgi varlıklarının korunması ve karşılaşabileceği riskleri minimize etmesi ve iş sürekliliğinin sağlanması, bilgi güvenliğinin Bilgi Güvenliği Yönetim Sistemlerinin (BGYS) kurumlarda uygulanmasıyla mümkün olacağının savunulduğu ve tüm süreçlerdeki kritik bilgilerin işlendiği, depolandığı ve saklandığı bilgi işlem merkezlerinde karşılaşılabilecek siber güvenlik tehditlerinin incelenmesi ve bundan hareketle, kurum ve kuruluşlarda güvenlik standardı oluşturup bu standarda göre kurumsal bir yapı kurmak isteyenlere yönelik bir kaynak doküman olması düşüncesiyle hazırlanmıştır.

Ayrıca bu çalışmada kurumsal bilgi güvenliği ile ilgili akademik ve gerçek saha tecrübeleri araştırılarak kapsamlı incelendiğinden, kurumsal bilgi güvenliği bilincinin geliştirilmesi, yüksek seviyede farkındalık oluşturulması, mevcut ve yeni standartlar hakkında bilgi içermesi bakımından literatüre özgün değer olarak katkı sağlayacağı düşünülmektedir.

Bu tez çalışması literatürdeki kaynaklar incelendiğinde yapılan çalışmaların oldukça sınırlı sayıda bulunduğu ve yerli literatürün çok az sayıda bulunması sebebiyle, bu çalışmayı baz alıp kurumsal bilgi güvenliği ve standartlarını uygulayacak kurumların bilgi merkezlerinde kendi özgün sistemlerini kurup yönetebilecekleri içeriği sağlayacağından, ulaşılacak sonuçların katma değeri büyük önem arz etmektedir.

Bu çalışma kapsamında öncelikle ilgili literatürde bulunan araştırmalar incelenerek konumuz ile ilgili bir literatür taraması yapılmış ve ikinci bölümde sunulmuştur. Ardından bilgi kavramı, bilgi güvenliği ve oluşturan unsurlar, bilgi güvenliğinin kurumlar açısında önemi ve siber güvelik kavramları ile ilgili kurumsal bir çerçeve çizilerek üçüncü bölümde sunulmuştur. Araştırmanın dördüncü bölümünde; kurumsal bilgi güvenliği ve bilgi güvenliği yönetim sistemi konuları ve beşinci bölümde ise siber güvenlik tehditleri ve güvenlik zafiyetleri konuları incelenmiştir. Son bölümde ise araştırmanın sonucu ve önemine ilişkin görüşler ve öneriler bildirilmiştir.

2. LİTERATÜR TARAMASI

Konu ile ilgili literatür yurt içinde ve yurt dışında yapılmış çalışmalarda genel olarak incelendiğinde bilgi, bilgi güvenliği ve siber olaylar ile siber güvenlik kavramlarının incelenmesinin konunun önemine binaen son yıllarda oldukça popüler olduğu ve halen araştırmacılar tarafından merak edildiği görülmektedir. Ancak araştırmalarda bu seviyede ilgi gören bu alan ile ilgili kurumların hassasiyeti bulunmasına rağmen halen açık bir hedef olduğu ve bir takım güvenlik zafiyetlerinin bulunduğu görülmektedir. Kurumların bilgi güvenliği ve siber güvenlik konularında yaptıkları engelleme stratejileri aldıkları önlemler ve işe koştukları sitemler merak edilmekte ve bazı araştırmalarda incelenmektedir. Ancak konu oldukça karmaşık ve sürekli yeni gelişmelerle güncellenmekte ve bu da yeni araştırmaların yapılmasının gerekliliğini ortaya koymaktadır. Aşağıda ilgili yazında bilgi güvenliği ve siber güvenlik konularında yapılmış bazı araştırmalar ve bu araştırmaların değindikleri kilit noktalar ile ulaştıkları sonuçlar sunulmuştur.

KURT KAYA tarafından yapılan araştırmada; bilgi güvenliği ve siber güvenlik kapsamında bakanlık uygulamaları için güvenli yazılım geliştirme metodolojisi önerisi sunulması amaçlanmıştır. Araştırma kapsamında güvenli uygulama geliştirme metodolojisi araştırılmış ve yapılan saha ziyaretleri sonucunda yazılım geliştiriciler ile bu konuda bir anket çalışması yapılarak araştırma grubunun düşünceleri araştırılmıştır. Araştırmanın sonunda, 2016-2019 Ulusal Siber Güvenlik Eylem planında ifade edilen amaçlar kapsamında, Çevre ve Şehircilik Bakanlığının kurumsal yapısı ve potansiyel durumu ile uyumlu bir güvenli uygulama yazılımı geliştirme metodolojisi önerilmiş, güvenli yazılım geliştirme politikası ve kontrol listesi hazırlanarak sunulmuştur (Kurt Kaya, 2017).

VURAL, tarafından yapılan araştırmada; bilgi güvenliği için risk oluşturan tehdit ve tehlikeler analiz edilmiş, web ortamlarında büyük risk meydana getiren SQL enjeksiyon açıklıkları, sızma testleri genel itibariyle ayrıntılı olarak irdelenmiş ve alınması ihtiyaç olan tedbirler sunulmuştur. Bilgi güvenliğini sağlamaya dair yapılan sızma testlerinin beşerî kaynaklara ve teknolojik kaynaklara etkisi incelenmiş, ardından çözüm önerileri verilmiştir (Vural, 2007).

GÜNGÖR “ulusal bilgi güvenliği: strateji ve kurumsal yapılanma” isimli çalışmasında ulusal bilgi güvenliğini internet teknolojilerinin getirdiği bilgi güvenliği algısındaki değişimleri de içeren bir kavramsal çerçevede incelemek, ülkelerin ve uluslar üstü kuruluşların bu kapsamda geliştirdiği stratejiler ve rehber ilkeler ışığında ülkemizin ihtiyaçlarına cevap verecek bir ulusal bilgi güvenliği stratejisinin ve yasasının temel elemanlarını belirlemeyi amaçlamıştır. Bu kapsamda araştırma için bilgi güvenliği konusunda yapılmış araştırmalar, raporlar ve eserler incelenmiş ve bir takım çözüm önerileri sunulmuştur. Bu temel çözüm önerileri şöyledir;

- Türkiye’de henüz tamamlanmamış olan bilgi güvenliği yasal altyapısının tamamlanması,
- Kamu kurumları ve kritik altyapı işletmecisi özel sektör kuruluşlarında bilgi güvenliği yönetim sistemlerinin teşkili,
- Bilgi güvenliği kültürünün geliştirilmesi,
- Ulusal bilgi güvenliğinin sağlanması için oluşturulan karar alma mekanizmalarında kamu ve özel sektörün karşılıklı iş birliğini sağlayacak kurumsal altyapının teşkili,
- Stratejik düzlemde bilgi güvenliğinin ulusal kalkınma hedefleriyle uyumlaştırılması ve bu kapsamda kamu kurumlarının stratejik planlarında bilgi güvenliğine vurgu yapılmasının sağlanması,
- Veri koruma ve siber suçlar alanında gerekli düzenlemelerin hayata geçirilmesidir (Güngör, 2015).

VURAL ve SAĞIROĞLU tarafından yapılan araştırmada kurum ve kuruluşların veri güvenliğinin oluşturulması ve sürdürülmesi için güvenlik sistemlerinin güncelliğinin korunması, ihtiyaç olan eğitimlerin alınması, potansiyel ve olası güvenlik açıklarının belirlenip rutin aralıklarla bu iş ve fiillerin tekrar edilmesinin önemi vurgulanmıştır. Bunun yanında bilgi güvenliğini sağlamak adına yalnızca teknik yeterlilikler öne çıkarılmaması gerektiği, aynı anda teknik bir yapı içermeyen ve o nitelikte sayılmayan personelin rehberliği ve eğitimi, kurumsal etik, fiziki güvenlik tedbirlere de dikkat edilmelidir (Vural ve Sağıroğlu, 2010).

CANBEK ve SAĞIROĞLU, “Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme” adlı araştırmalarında bilgi olgusunu geniş bir açıdan ele almış, veri, bilgi, öz bilgi kavramlarına değinmiştir. Bilişim teknolojilerinin bilgi üstündeki etkileri ve boyutları ortaya konulduktan sonra bilgi güvenliği kavramı üzerinde bir inceleme gerçekleştirilmiştir. Sonuç olarak araştırmada, bilgi güvenliğine yapılan saldırıların, zaman içerisinde hem nicelik hem de nitelik ve çeşitlilik yönünden arttığı bir ortamda etkili bir bilgi güvenliği meydana getirebilmek adına ihtiyaç olan, güvenlik süreçleri verilmiştir. En sonda ise açıklanan, incelenen, irdelenen ve özetlenen hususlar genel olarak değerlendirilmiştir (Canbek ve Sağıroğlu, 2006).

EMİNAĞAOĞLU ve GÖKŞEN çalışmasında bilgi güvenliği konularını incelemeyi ve Türkiye’de bilgi güvenliği sorunları ve çözüm önerilerini sunmayı amaçlamıştır. Bu doğrultuda, çalışma kapsamında dünyadan ve ülkemizden en güncel istatistiksel bilimsel verilerle mevcut durum ortaya koyulmuş ve bilgi güvenliğinde ortak yapılan en yaygın yanlışlara dikkat çekilmiştir. Ardından bu durumlara yönelik kısa ve uzun vadede toplum geneline ve kurumlara uygulanabilecek etkin çözüm önerileri tavsiye edilmiştir (Eminağaoğlu ve Gökşen, 2009).

AKTAŞ, çalışmasında BGYS standartları içerisinde uluslararası geçerliğe sahip olan uluslararası standart organizasyonu ISO 27001 bilgi güvenliği yönetim sistemi (BGYS) kapsamında yer alan erişim kontrol protokolünün şirketler için önem düzeyinin, şirketlerin bilgi güvenliğinin sağlanmasındaki etkileri incelemiştir. Araştırmada kullanılan anket eğitim ve finans gibi farklı sektörde görev yapan 343 farklı seviyelerde çalışan bireye uygulanmış ve elde edilen veriler analiz edilmiştir. Araştırma sonucunda BGYS belgesi bulunan firmaların erişim kontrol politikalarının ve düzenlemelerinin bilgi güvenliği ile ilgili olan risk ve tehditlerin minimuma indirildiği bildirilmiştir (Aktaş, 2020).

ARDA, “Siber uzay ortamında saldırı tehditlerinin farkındalığı, tespiti ve önlenmesi üzerine bir gerçek-zaman sistem önerisi” isimli çalışmasında bilgi ve siber güvenlik kavramlarını incelemiş, ardından çalışmasında öneri olarak sunduğu sistem ile güvenli bir ortamda siber tehditlerin anlatılması ve etkilerinin gösterilmesini sağlamak istemiştir. Bunun yanında araştırması sayesinde yeni güvenlik tekniklerinin denenmesine de imkân tanımayı amaçlamıştır (Arda, 2020).

AKPINAR, “Veri merkezli katmanlı güvenlik tasarımı ile etkin olay analizi ve yönetimi” isimli çalışmasında siber risklere karşı veri merkezi güvenliğinin sağlanmasına yönelik güvenlik yaklaşımları ve veri merkezlerinde SIEM çözümlerinin etkin kullanımına yönelik inceleme gerçekleştirmiştir. Araştırmacı veri merkezlerinin Bilgi Güvenliği ve Olay Yönetimi anlamına gelen SIEM (Security Information and Event Management) çözümlerini kullandıklarını ve doğru yönetilemeyen SIEM çözümlerinde, çok sayıda log kaçırma, yanlış alarmların oluşması, siber tehditleri gözden kaçırma gibi risklerle karşı karşıya kalındığını ve güvenlik tasarımı doğru yapılmayan, doğru güvenlik ürünleri kullanılmayan veri merkezlerinin siber tehditlere karşı savunmasız hale geldiğini vurguladığı çalışmasında yaptığı incelemeler sonucunda, incelmelerin kamuya bağlı bir veri merkezinde yapılan SIEM uygulamasıyla desteklendiğini bildirmiştir (Akpınar, 2020).

SANTANAM, “Cyber security, cybercrime and cyber forensics: applications and perspectives” isimli eserinde siber güvenlik, siber adli tıp ve siber suç kavramlarını derinlemesine incelemiş ve siber güvenlik konusunda uygulamalar ve perspektifleri ele almıştır. Santanam eserinde siber tehdit yüzeylerinin bilgisayarlarda uygulamalara saldıranların erişimi olan kısmi hedef oluşturduğunu belirtmektedir. Kodun bir bölümü veya uygulamanın bir bölümü dış dünyaya ara yüzler aracılığıyla açık olabilmekte ve bu açık bölümler saldırıların hedefi haline gelebildiği bildirilmektedir. Uygulamanın siber tehdit yüzeylerinin dört bileşenden meydana geldiğini ifade eden araştırmacı, bunları; kullananların eriştiği kod, ara yüzey, servis ve protokoller olarak sıralamıştır (Santanam, 2010).

ŞAHİNASLAN, “Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma” isimli doktora tezinde ise; kurumların siber güvenlik temelinde çok katmanlı bir ağ mimarisi oluşturmasında, sahibi olduğu değerli bilgi ve sistem kaynakları üzerinde var olabilen zafiyetleri tespit etmede kullanılabileceği bir sızma test yöntem kılavuzu meydana getirmiştir. Bunun yanında ilgili yöntemin uygulanması neticesinde varlıklar üstünde saptanan zafiyetleri kullanabilecek tehditlere karşı alınacak tedbirlerin bir arada tanımlanıp yönetilebildiği siber önlem sistemi(SOS) adı verilen uygulama geliştirmiştir (Şahinaslan, 2013).

WİLLİAMS, DAVİS, COTHREN, WHİTE VE CONKLİN çalışmasında bilgisayar güvenliği ilkelerini incelemiş ve CompTIA Security+ ve ötesine atıfta bulunmuştur. İnternet erişiminin yaygınlaşması ve insanların verilere ulaşımının kolaylaşmasından dolayı genişleyen siber tehdit yüzeylerinin büyük bir saldırı tehditi altında cazip bir hedef olduğunu belirtmiştir. Araştırmacı, devlet aktörleri adı verilen unsurların da devreye girmesiyle siber tehditlerin kurumlar için büyük bir tehdit oluşturduğunu savunmaktadır. Bu noktada araştırmacı siber saldırıda bulunan saldırganların bunu yapmasında iki farklı maksadının olduğunu dile getirmiştir. Bunlar;

i. Bilgisayar mekanizmasını, yazılımlarını ve sistemi devre dışına itmek.

ii. Edindikleri sistemleri kullanarak maddi kazanç elde etmektir (Williams vd.,2018) .

YILMAZ, ULUS ve GÖNEN, "bilgi toplumuna geçiş ve siber güvenlik" adlı makalesinde teknolojinin gelişmesiyle birlikte küreselleşmeye bağlı güvenlik kaygılarının ortaya çıkışı, Türkiye'de uygulanan bilgi toplumu stratejisi, ülkemiz ve dünyada bilgi toplumuna geçiş süreci, bilgi teknolojileriyle oluşturulan kritik altyapı sistemleri, bu sistemlere karşı siber tehditler ve bu sistemlerin risk analizini incelemeye amaçlamıştır. Araştırmacı ülkemizde siber güvenliğin henüz tam anlamıyla anlaşılmadığını, önlem alınamadığını ve yeterli olgunluğa erişmediğini vurguladığı çalışmasında, bu alanda mevcut güvenlik güçlerinin imkân ve kabiliyetleri ile yetişmiş personel sayısının yetersiz olduğunu ve internet ortamında işlenen suçlara müdahalede uluslararası rollerin de eklenmesiyle bu sayının daha da yetersiz kaldığını bildirmektedir. Son dönem siber saldırıların sayılarında büyük bir artışın meydana gelmesiyle bu konuda olumlu çalışmaların arttığını ve bunlardan bazılarının;

- Siber Güvenlik Eylem Planları,
- Ulusal Bilgi Güvenliği Programı,
- Ulusal Bilgi Güvenliği Kapısı,
- Yasal Çalışmalar,
- Siber Olaylara Müdahale Ekipleri ve Birimleri,
- Siber Güvenlik Tatbikatları,

- Konferanslar,
- Çalıştaylar ve
- TSK bünyesinde icra edilen faaliyetler ve oluşumlar olduğunu ifade etmiştir (Yılmaz vd., 2015).

Görüldüğü üzere bilgi güvenliği ve siber güvenlik konuları ile ilgili yapılan yukarıdaki araştırmalardan bazıları kuramsal bir araştırma şeklinde hazırlanırken bazıları ise anket, görüşme ve gözlemlere dayalı incelmeler ortaya koymuşlardır. Her birinin araştırma deseni ve veri elde etme teknikleri farklı olsa da ulaşmak istedikleri amaç bilgi güvenliği ve siber güvenlik konularının daha detaylı bir şekilde tanıtılmasının sağlanmasıdır. Bu araştırmada ise bilgi güvenliği ve siber güvenlik konularının derinlemesine incelenmesi amaçlanmıştır. Bu doğrultuda internet ortamında ve diğer gerçek ortamlar kullanılarak ulaşılabildiği kadar çok dergi, kitap, rapor ve mevzuat incelenmiş ve gerekli veriler toplanmıştır. Elde edilen veriler araştırma planı ve süreci kapsamında kullanılarak yorumlanmış ve ardından bu araştırmanın sonuçlarına ulaşılmıştır.

3. GENEL BİLGİLER

Çalışmanın bu bölümünde bilgi güvenli kavramları kapsamında; bilgi ve bilgi güvenliği kavramları, bilgi güvenliğini oluşturan unsurlar ve bilgi güvenliğinin kurumlar açısından önemi ile siber ve siber güvenlik kavramları konusunda kavramsal bir çerçeve oluşturulmuştur.

3.1. Bilgi Güvenliği Kavramları

Bilgi, teknoloji ve iletişim çağı olarak adlandırılan içinde bulunduğumuz 21. Yüzyılda, internet iş ve sosyal yaşantılarımızın her alanına dahil olmuştur. Mesajlaşma, sosyal medya, alışveriş yapma, bankacılık vb. pek çok sahada hemen hemen her saniye bir işlem yapılmakta ve farklı içerikler üretilerek kullanıcılara sunulmaktadır. Online bağlantının sağladığı küresel iletişim dünyasında virüsler, korsanlar, dolandırıcılar, izinsiz dinleme ve erişim gibi pek çok tehdit de bulunmaktadır. Bu tehdit ve risklerin oldukça fazla olması bilgi güvenliği konusuna atfedilen önemi daha da çok ön plana çıkarmıştır. Bu nedenle bilgi güvenliği kavramının ve bilgi güvenliğinin kurumlar için öneminin daha iyi anlaşılması ve içselleştirilmesi gerekir. Bilgi ve bilgi güvenliği kavramları, bilgi güvenliğinin unsurları ve kurumlar için önemi aşağıda yer alan başlıklar altında özetlenerek sunulmuştur.

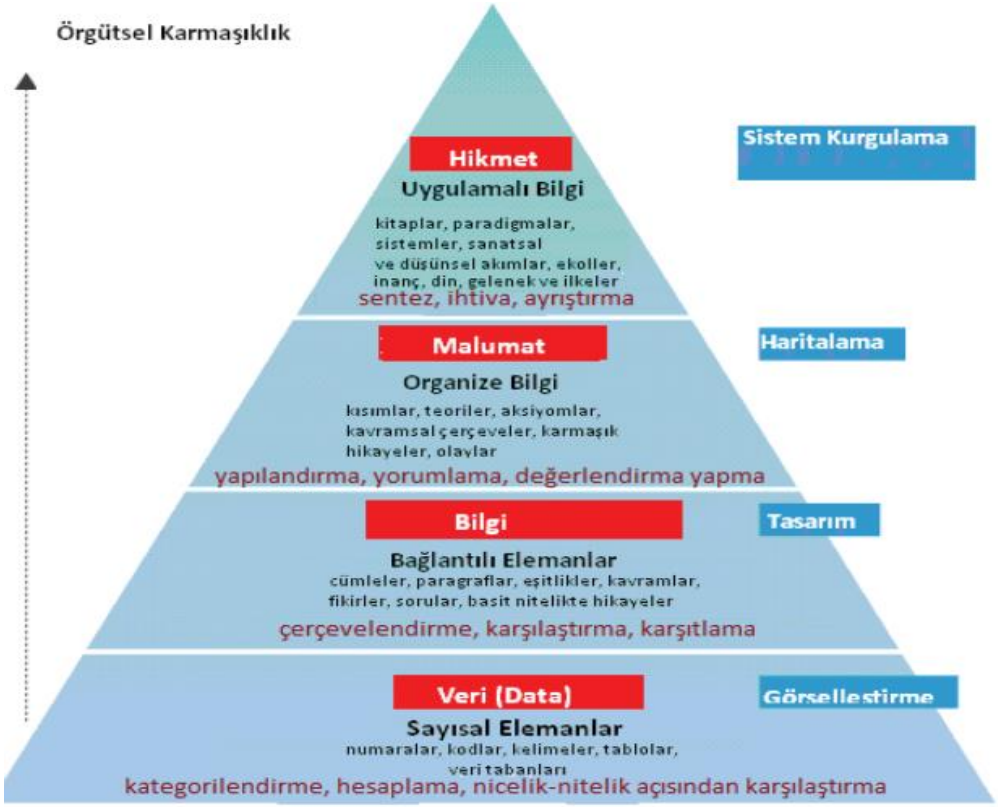
3.1.1. Bilgi Nedir?

İngilizcede bilgiye ilişkin kullanılan (data, information, knowledge) kavramlarının hepsinin Türkçe karşılığı bilgi olarak bilinmektedir. Bu terimlerin dilimizde karşılıkları olarak veri, bilgi, malumat kavramlarının ayrı ayrı bilinmesi ve kullanılması daha doğru bir yaklaşımdır (Canbek ve Sağıroğlu, 2006). Bilgi kavramını açıklamadan önce bilgi kavramı ile karıştırılan bazen de onun yerine kullanılan veri kavramını açıklamak ve bunların bilgi ile ilişkisini incelemek gerekmektedir (Güngör, 2015).

Veri (data), birbirleriyle ilişkisi kurulmamış sayısal setlere verilen isimdir (Canbek ve Sağıroğlu, 2006). Bilgi oluşumunda veri ve ilişkili olduğu konu oldukça önemlidir. Veri ve ilişkili olduğu konu, bilgi üretecek şekilde bir araya getirilir. İşlenmiş veri olarak da ifade edilebilecek bilgi, Shannon tarafından “bir konu hakkında var olan belirsizliği azaltan bir kaynak” olarak tanımlanmıştır. Kısaca, veri üzerinde yapılan uygun bütün

işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, vs.) çıktısı, bilgi olarak ifade edilebilir (Canbek ve Sağıroğlu, 2006). Malumat (knowledge) tecrübe etme, öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların ya da bilginin farkında olunması ve anlaşılması olarak tanımlanmaktadır (Güngör, 2015) (Canbek ve Sağıroğlu, 2006).

Bir organizasyonun bilgi üretme yolculuğunda verinin girdi olarak kullanılması yeterli olurken karmaşık yapıdaki örgütlerin ürettiği gelişmiş bilgi varlıklarının üretilebilmesi için malumattan ve hatta hikmetten faydalanılmaktadır.



Şekil 1. Bilgi piramidi

Kaynak: Güngör (2015)

Literatürde bilgi ile ilgili birçok disiplinde tanımlar yapılmış, araştırmacılar bu konuda birçok farklı ifadede buluşmuşlardır. Bu doğrultuda yapılan tanımlardan yola çıkarak bilgi ve özellikleri ile ilgili bir özetleme yapılacak olunursa, bilgi;

- İnsan yaşantısındaki en hassas ve önemli varlıklardan birisi, kişi, örgüt ve toplumlar için edinilmesi güç, aynı anda elde tutulması da oldukça zor bir meta şeklinde tanımlanabilir (Canbek ve Sağıroğlu, 2006).
- Bilgi, verilerin belirli bir anlam teşkil edecek biçimde düzenlenmiş durumudur (Eminağaoğlu ve Gökşen, 2009).
- Bir başka ifadeyle bilgi bir sorunun yanıtıdır. Bilgiye yapılan araştırmalar ve deneylerle ulaşılacağı gibi gözlemleme ya da iletişim etkinlikleri vasıtasıyla da bilgi edinilebilir. Belirsizlikleri ortadan kaldırarak davranışlara, alınacak kararlara veya neticelere etki edebilir (Kurt Kaya, 2017).
- İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat (Türk Dil Kurumu [TDK], 2022).
- Öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, vukuf (Türk Dil Kurumu [TDK], 2022).
- Bilişim disiplinine göre; kurallardan yararlanarak kişinin veriye yönelttiği anlam (Türk Dil Kurumu [TDK], 2022).
- Felsefe bilimine göre ise; genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşüncelerdir (Türk Dil Kurumu [TDK], 2022).

3.1.2. Bilgi Güvenliği

Bilgi güvenliği, bir ülkenin bilgi varlıklarının, kritik altyapılarının, bilgi ve iletişim teknolojileri altyapısının, işletme ve vatandaşların iş ve işlem güvenliğinin sağlandığı sosyo-kültürel yönü olan bir kavramdır (UNESCAP, 2022). Bilgi güvenliği, sayısal ortamdaki bilginin saklanması ve taşınması esnasında bilginin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi saklama ve işleme platformu oluşturma çabalarının tümüdür (Canbek ve Sağıroğlu, 2006)

Aslında bilgi güvenliği yeni bir olgu değildir. Bilginin yazılı bir biçimde saklanabilir olmaya başladığı ilk çağlardan itibaren bilgi korunabilir ve elbette çalınabilir, yok edilebilir bir metadır. Tarih boyunca insanlar farkında olmasalar da sakladıkları önemli bilgilerin güvenliğini sağlamak için tedbirler almak durumunda kalmışlardır (Güngör, 2015).

Bilgi güvenliği, bilgilerin izinsiz olarak kullanılmasından, ilan edilmesinden, paylaşılmasından, ortadan kaldırılmasından, üzerlerinde değişiklik yapılmasından ve bilgilere zarar verilmesinden muhafaza etme ve bilgilere yapılabilecek izinsiz erişmeleri engelleme iş ve işlemleridir (Eminağaoğlu ve Gökşen, 2009).

Bilgi güvenliği uluslararası standardizasyon örgütü tarafından yapılan tanımlamaya göre ise bilgi güvenliği; bilgilerin gizlilik, bütünlük ve erişilme niteliklerinin muhafaza edilmesidir. Bunun yanında özgün olma, hesap verebilme, reddedilemezdik ve güvenilir olma gibi başka nitelikleri de bulunmaktadır (ISO, 2013).

Amerika Birleşik Devletleri Kongresi (USC) 2002 yılında çıkardığı "Federal Bilgi Güvenliği Yasası (FISMA)"nda Bilgi güvenliğini şöyle ifade etmektedir; bilginin korunduğu bilgi sistemlerinin ve sistemin içerdiği bilginin yetkisiz erişimine, kullanımına, ifşa edilmesine, değiştirilmesine, incelenmesine, hasar verilmesine veya yok edilmesine karşı korunması ve buna ilişkin tedbirlerin bütünüdür ([USC], 2022).

Ulusal Güvenlik Komitesi (CNNS)'ye göre; gizlilik, erişebilirlik ve bütünlük oluşturmak için bilgi ve mekanizmalarının yetki olmadan erişmeye, kullanmaya, açıklamaya, tahrip olmaya, değişiklik yapılmaya karşı korunabilmesi şeklinde tanımlanmaktadır (Kurt Kaya, 2017).

İngilizce' de "information security" kavramı bilgi güvenliği olarak dilimize çevrilmektedir. "Information assurance" kavramının Türkçe karşılığı olarak bilgi güvencesi kavramının kullanılması daha uygun olacaktır. Bilgi güvencesinde, bilgi sisteminde bilgi güvenliğini sağlamak için gerekli olan teknik ve süreçsel gereksinimler daha stratejik düzeyde ele alınırken bilgi güvenliği kavramı ise daha taktik düzeyde bir anlam içermektedir (Güngör, 2015). Şekil.2'de bu kavramların kapsamları ve arasındaki farklar sunulmuştur.

Şekil 2. Bilgi güvenliği ve güvencesi kavramlarının farkları

Kaynak: Güngör (2015)

3.1.3. Bilgi Güvenliğini Oluşturan Unsurlar

Bilgi güvenliği için amaçlanan iş ve işlemleri somutlaştıran ve etkili bir bilgi güvenliği sağlamak için birtakım belirleyiciler bulunmaktadır. Bilgi güvenliğini oluşturan bu üç önemli unsur aşağıda belirtilmiş ve unsurların birbirleriyle etkileşimi Şekil.3'te sunulmuştur (Güngör, 2015);

i. Gizlilik (Confidentiality): Bilginin yetkisiz kişilerin veya sistemlerin erişimine kapalı olması ya da bilginin yetkisiz kişilerce açığa çıkarılmasının engellenmesidir.

ii. Bütünlük (İntegrity): Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır. Bütünlük için kısaca kazara veya kasıtlı olarak bilginin bozulmaması olarak da ifade edilebilir.

iii. Erişebilirlik/ Kullanılabilirlik (Availability): Bilginin ihtiyaç duyulduğu anda kullanıma hazır durumda olması anlamına gelmektedir. Bilginin korunduğu bilgi

sistemiyle ilgili bir sorunun veya sisteme yönelik bir riskin ortaya çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde olmalıdır. Kullanılabilirlik ilkesinin odağı kullanıcılar olup her kullanıcı erişim hakkının bulunduğu bilgi sistemine, yetkili olduğu zaman diliminde mutlaka erişebilmelidir.

Şekil 3. Bilgi güvenliğini oluşturan temel unsurlar (CIA üçlüsü)

Kaynak: Singh vd. (2014)

Singh, Vaish ve Keserwani tarafından tasarlanan ve bilgi güvenliğinin üçlüsü olarak tanınan Şekil 3'te görülen unsurlar zaman geçtikçe yetersiz olarak görülmüş ve bazı araştırmacılar tarafından yeniden gözden geçirilerek yeni unsurlar dahil edilmiştir (Stallings, 2011). Bu düzenlemeyi yapan ve oldukça popüler olan araştırmacılardan birisi de D. B. Parker'dir. Parker yukarıda ifade edilen bilgi güvenliği üçlüsünün yalnızca teknolojik açıdan riskleri içerdiğini ancak insan odaklı faktörlerin de bilgi güvenliği için önemli bir tehdit oluşturduğunu varsayarak bilgi güvenliği unsurlarını güncellemiştir. Araştırmacı 1988'de "Parker Altılısı" adı ile tanınan yeni bir model ortaya koymuştur. Bu model bilgi güvenliğinin üç temel unsuru üzerine inşa edilmiş ve bu unsurlara dahil edilmiş unsurları kapsamaktadır. İfade edilen bu altı unsur ile bilgi güvenliği daha kapsamlı ve detaylı ele alınmaktadır. Bu model tehlikelere karşın

koruma için genellikle kimlik doğrulama ve şifreleme yöntemine işaret etmektedir (Kurt Kaya, 2017). Aşağıda yer alan Şekil 4'te ilgi güvenliğinin yeni ve kapsamlı unsurları olarak tanınan Parker altılısı sunulmuştur.

Şekil 4. Bilgi güvenliğini oluşturan altı temel unsur (Parker altılısı)

Kaynak: Kurt Kaya, (2017)

Bu modelde bilgi güvenliliğinin üç temel unsuruna yararlılık, özgünlük ve sahiplik/kontrol olmak üzere üç boyut (ilke) eklenmiştir. Bu ek boyutlar incelendiğinde (Kurt Kaya, 2017) (Kabay vd.,2022);

- Özgünlük: Bu boyut gerçek olmak, doğrulanabilir olmak ve güvenilir olmak özellikleri ile alakalı bir boyuttur. Gönderilen mesajın ve gönderen kişinin geçerliğine güvenin oluşmasında gerekli bir ilkedir. Bu durum sisteme giren her kişinin güvenilir bir kaynak olduğunu doğrulamakla alakalıdır.
- Yararlılık: Maksadına uygunluğu anlatan ilkedir.
- Sahiplik/Kontrol: Bilgi ile fiziki temasın engellenme işlemi, kopyasının alınması ya da yetkisi olmadan kullanılmasını önleme işlemidir.

3.1.4. Bilgi Güvenliğinin Kurumlar Açısından Önemi

Günümüzde bilişim teknolojilerinin yaygınlaşması ve günlük hayatımızda yapmış olduğumuz iş ve işlemlerin elektronik ortamlarda hızla yapılmaya başlanması, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir (Canbek ve Sağıroğlu, 2006). Bilgi güvenliği, her kurumun sürekliliğinin sağlanmasında büyük önem taşır ve kurumun başta elektronik olmak üzere, çeşitli ortamlardaki kritik bilgilerinin ve diğer bilgi varlıklarının korunmasını sağlar. Sadece büyük şirketler, bankalar değil bunun yanı sıra tüm kamu kurumları veya kâr amacı gütmeyen herhangi bir kurum, okul, vb. de bilgi güvenliği sorunları ve risklerini farklı düzeylerde de olsa sürekli yaşamaktadır. Bu gerçek, dünya genelinde olduğu gibi ülkemizde de sürekli artan boyutlarda ortaya konan bir olgu haline gelmektedir (Eminağaoğlu ve Gökşen, 2009). Bu bağlamda kurumların bilgi güvenliği yönetimi; uluslararası standartlar, ölçümleme yöntemleri, ilgili ulusal veya uluslararası yasalar, ticari yükümlülükler, gelişen teknolojiler ve değişen iş süreçlerine paralel olarak sürekli değişen ve önemi artan riskleri de kapsayacak şekilde büyük önem kazanmakta ve hem bilişim hem de iş dünyasındaki en öncelikli konulardan birisi haline gelmektedir (Eminağaoğlu ve Gökşen, 2009).

İşin niteliği veya sürecin yapısı ne olursa olsun, teknoloji bağlantılı olmayan süreçlerin yönetiminde bile, bilgi güvenliğinin de etkin, sürekli ve başarılı bir şekilde sağlanarak yönetilmesi çok önemli bir gereksinim olmaktadır. İşlerin ve süreçlerin sağlıklı yönetimi aynı zamanda ilgili bilgi güvenliği süreçlerinin de sağlıklı yönetimini zorunlu kılmaktadır. Bilgi güvenliği stratejileri ve bunları yönetecek uygun yöntemleri olmayan kurumlar, sadece güvenlik açısından değil, operasyonel ve diğer her türlü iş süreçlerinin yönetimi açısından da ciddi sıkıntılar, maddi ve/veya manevi kayıplarla yüzleşmektedir (Tipton ve Krause, 2007).

Bilgi yönetimindeki en önemli unsurlardan birisi de bilginin güvenliği ve özellikle korunabilmesidir. Zira güvenli olarak saklanamayan her bilginin yönetimi de sıkıntı teşkil etmektedir. Bilgiye erişen kişilerin güvenli kaynaklardan olması ve bunu güvenli bir şekilde kullanması yapılması gereken tedbirlerden biri olarak ortaya çıkmaktadır. Bu noktadan değerlendirildiğinde erişim işlevinin kontrol altında tutulması ve erişimin denetlenmesi işlemlerinin istenilen şekilde yapılamaması kurumları, özel ve tüzel kişileri ve ilgili paydaşları mali ve manevi zararlara uğratabilir. Bu doğrultuda

gerçekleştirilen bazı çalışmalar bu konunun önemini daha iyi vurgulamaktadır (Aktaş, 2020).

Örneğin 2008 tarihinde gerçekleştirilen CSI ve FBI kurumlarının Amerika'da 522 kurum (devlet veya özel) genelinde yaptıkları incelemenin bulgularına göre; kurumların %42 sinde mobil cihaz, cep bilgisayarları çalınmış; %49'unda solucan, virüs, truva atı gibi zararlı kod saldırıları gerçekleşmiş; %44 ü şirket personeli tarafından internet ve diğer yetkileri ve erişimleri suiistimal edildiği raporlanmıştır. İfade edilen bu 522 kurum yıl içerisinde 156 Milyon ABD doları zarara uğramış ve maddi kayıplar yaşamıştır (Richardson ve Director, 2008).

2017 yılında gerçekleştirilen başka bir çalışmaya göre 965,6 milyon bilgi sızıntısı olayının 1505'i bireysel olduğu ortaya koyulmaktadır. %32,2'si harici gelen art niyetli saldırılardan ve %65,4'ü ise şirket personelinden meydana gelmektedir. Kişisel veriler ve mali bilgiler %90,8 oranla en fazla saldırı altındaki alanlardan olduğu görülmektedir. Ağ bağlantıları %45,6 ile bilgi sızıntısının en fazla yapıldığı kanaldır. Bilgi sızıntısı en büyük miktarda ticaret bazlı firmalarda yapılmakta ve saldırılar için en çok tercih edilen finansal sektörler ise yüksek teknoloji, ticaret ve ulaşım sektörleri olarak görülmektedir. Ulaşım, ticaret ve yüksek teknoloji firmalarının verileri genellikle kurum dışından gelen saldırılara maruz olurken; finans, tıp ve eğitim sektöründeki firmalar ise genellikle kurum içi bir yapıdan saldırıya maruz olmaktadır. Bilgisayar korsanlarının kaynakları, koruma sistemleri çalışmayan veya etkili olmayan kontrol edilmeyen kanallardan oluşmaktadır (Marjanovic, 2017).

Bilgi güvenliği, bir bilgi sisteminin faaliyetlerini yerine getirirken kesintisiz, kaliteli ve güvenli bir hizmet sunumunun sağlanmasını hedeflemektedir. Diğer yandan kurumsal imaj ve güvenirliğin sağlanması, eldeki bilgi varlıklarının korunumu ve yetkisiz erişimlerin önlenmesi de bilgi güvenliğinin temel amaç ve öncelikleri arasındadır. Burada dikkat edilmesi gereken husus, bilgi güvenliği kavramının aslında kullanılan teknolojiden bağımsız bir şekilde ele alınması gerekliliğidir. İster kâğıt tabanlı ortamda olsun isterse bilgi sistemlerinde sayısal bir halde bulunsun, bilgi kendisine yönelen tehditlere karşı bu bilgiyi tutanlar ve kullananlar tarafından her zaman korunmaya muhtaçtır. Zaten bilgi güvenliğinin ilk kullanım alanları gizlilik ve sır kavramının oldukça önemli olduğu diplomatik ve askeri konulardır. İlk dönemlerde bilgi güvenliği

sadece istihbarata karşı koyma ve kritik bilgiyi koruma ekseninde ele alınmış ve bu noktada alınması gereken tedbirler bütünü olarak algılanmıştır. Ancak bilgi ve iletişim teknolojilerinin gelişimiyle bilginin sayısallaşarak sistemlerde tutulur ve saklanır hale gelmesi neticesinde bilgininin güvenli bir biçimde saklanması, korunması ve gerektiğinde kullanılması sorunu artık bilgi sistemlerine sahip herkesin ortak meselesi haline gelmiştir. Bilgi toplumuna dönüşüm süreciyle beraber kişisel bilgisayardan en karmaşık bilgi altyapılarına kadar tüm bilgi sistemleri bilgiyi bünyesinde saklar olmuş ve bu nedenle de bilgi güvenliği olgusu sayısallaşma ile birlikte önem kazanmıştır (Güngör, 2015).

Bilginin ve teknolojinin iç içe olduğu ve teknolojinin baş döndürücü bir hızla gelişen ve yayılan elektronik ortamları desteklemesi, her zaman yanı başımızda olacak bilgisayar korsanı gibi kötü niyetli kişilerin veya bu tür kişilerin yazdığı casus yazılımların, sistemlerin açığını bulmada bu açıkları kullanıp sistemlere izinsiz erişmede ve sistemlere ve sistemi kullanan kişilere, kişisel veya kurumsal zarar vermede hemen hemen her yolu denemeye çalıştıkları tespit edilmektedir. Kurumlar için bu derece önemli olduğu yukarıda da ifade edilen bilgi güvenliği ve bilginin korunması konusunda; bu saldırı ve tehditlere karşı her türlü önlemin alınması ve bunun sürdürülebilir olması için bu tür yazılımların ve kullanılan teknik ve stratejilerin rutin olarak incelenmesi gerekmektedir (Canbek ve Sağıroğlu, 2006).

3.2. Siber ve Siber Güvenlik Kavramları

Siber, meydana getirilen, depo edilen ve paylaşılan dijitalleştirilmiş verilerden meydana gelen bir bilgi ortamıdır. Siber kavramı bütün dijital ağları içine alan oldukça geniş bir kavramdır. "Siber" terimi etimolojisi incelendiğinde İngilizce dilindeki "Cyber" sözcüğünden uyarlanıp birçok dilde kullanılmaya başladığı görülmekte ve "Bilgisayar ağlarına ait olan", "İnternete ait olan", "Sanal gerçeklik" anlamlarına geldiği bilinmektedir (Rouse, 2022). Ayrıca siber sözcüğünün “sibernetik” kökünden geldiği ve Sibernetik kelimesinin ise “kendi kendine denge kurarak kontrol etme ve yönetme anlamında kullanıldığı belirtilmektedir. İnsan yaşamı ile makinelerin yönetişimi şeklinde birbirleri ile bilgi alış-verişi olarak “Siber” terimi tanımlanabilir (Ünaldı, 2003). Yani genel olarak internet ile alakalı her şey siber kategorisinde incelenebilir

(Rouse, 2022). Siber zamanımızda sanal erişim veya sanal yaşam olarak daha çok kullanılmaktadır.

Siber güvenlik, bilgi güvenliğinin alt bileşeni olan ağ ve bilgisayar güvenliği kavramının internetin gelişimi ve yaygınlaşmasından sonra dönüştüğü yeni kavramsal çerçeve olarak tanımlanabilir. Her ne kadar siber güvenlik, bilgi güvenliğinin alt bir dalı olsa da son zamanlarda ortaya çıkan ulusal strateji metinlerinde bilgi güvenliği yerine siber güvenlik kavramının da kullanılabildiği görülmektedir (Güngör, 2015). Siber uzayın güvenliğini oluşturmak ve muhafaza etmek için yapılan faaliyetlerin bütününe siber güvenlik adı verilmektedir (Kurt Kaya, 2017). Siber güvenlik kavramının daha iyi anlaşılması için birtakım terimlerin kavramsallaştırılması ve tanımlanması şarttır. Bu kavramlar içinde; siber uzay, siber silah, siber saldırı, siber savaş, siber suç sayılabilir.

Siber uzay: ABD Savunma Bakanlığı'nca "internetin bulunduğu, telekomünikasyon ağlarını ve bilgisayar sistemlerini de kapsayan, birbirine bağlı bilgi teknolojisi altyapılarının olduğu küresel bir alan" olarak tanımlanıyor. Şöyle bir tanımlama da var: "İnsanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan, birbirine bağlı olma durumu" (Emre,2012).

Siber saldırı: Hedef olarak belirlenen organizasyon ve bireylerin bilgi sistemlerinin işlem yapmasını önlenmesi, hasar görmesi, değiştirilmesi yönetimleriyle; iş, yönetim ve sosyal yaşam üstünde olumsuz etkiler meydana getirilmesidir (Kurt Kaya, 2017).

Siber silah: Siber saldırıları yapmak için tercih edilen siber ortam araçları olarak tanımlanmaktadır (Emre , 2012).

Siber savaş: Bir ülkenin başka bir ülkenin bilgisayar mekanizmalarını ya da ağlarını zarara uğratmak veya kesintiler oluşturmak adına gerçekleştirdiği sızma işlemleridir (Kurt Kaya, 2017). Düşman olarak belirlenen hedefe siber saldırıda bulunmak, saldırılara karşı savunma yapmak, istihbarat verisi toplamak siber savaş faaliyetlerini oluşturuyor. Siber savaşların ana hedefi ülkelerin güvenlik, sağlık, enerji, ulaşım, haberleşme, su, bankacılık, kamu hizmetleri gibi kritik sektörlerinin bilgi sistemi altyapılarıdır (Emre ,2012).

Siber suç: Siber uzayda işlem ve hizmetlerin bir suç için kullanılması ya da siber uzayın bir suçun kaynağı, vasıtası, amacı olduğu suç etkinlikleridir (Kurt Kaya, 2017). Basit bir tanımlamayla ise siber suç, bilişim suçlarının internet üzerinden işlenen özel bir türüdür (Güngör, 2015).

Siber güvenlik: kişisel bilgilerin, kritik altyapı ve bilgi sistemlerinin saldırı ve tehditlere karşı korunması anlamına gelir (Fumudoh ve Viswanathan, 2014). Siber güvenlik, bilişim sistemlerinin ve işlenen bilgilerin gizlilik, bütünlük veya erişebilirliğinin güvence altına alınması, siber saldırıların tespit edilmesi ve bu tespitlere karşı tepki mekanizmalarının devreye alınması olarak da ifade edilmektedir. Siber âlemde kurum kuruluş ve kullanıcıların mağduriyetini, imajını, özel gizli bilgilerin çalınmasını, ele geçirilmesini veya saldırıya uğramasını korumak için kullanılan güvenlik prosedürleri, risk analizleri, kontrol mekanizmaları, fiziksel ve çevresel güvenlik vb. uygulamaların tamamıdır (Ercan, 2015).

ISO 27032 ise siber güvenliği; organizasyonların ve kullanıcıların varlıklarını sürdürebilmeleri adına işe koşabilecekleri araçları, politikaları, güvenlik terimlerini, önlemleri, yönergeleri, risk yönetim anlayışlarını, fiilleri, eğitim ve rehberlikleri, güvence ve teknolojik ürünlerin bütününü kapsamaktadır (ISO, 2012).

Siber uzaydan gelebilecek saldırılara ve tehditlere karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan politikalar, güvenlik kavramları, risk yönetimi yaklaşımları siber güvenliği oluşturuyor (Emre, 2012).

Siber güvenlik, ulusal ve uluslararası güvenliği tehdit ettiği için devlet güvenliğinde bir boyut olarak görülmektedir. Devletin kendisini ve kurumlarını tehditlere, casusluğa, sabotaj, suç ve sahtekarlığa, kimlik hırsızlığına ve diğer yıkıcı online işlemlere ve etkileşimlere karşı koruması siber güvenlik çatısı altında ifade edilebilir (Choucri, 2012). Devletlerin siber güvenliğe bakış açıları farklılık göstermektedir.

Çizelge 1'de bazı devletlerin siber güvenlik tanımlamaları arasındaki farklılıkları ortaya koymaktadır.

Çizelge 1. Ülkelerin Siber Güvenlik Tanımları

Ülkeler	Siber Güvenlik Tanımları
Avusturalya	Ülkenin genel olarak terörle mücadele etme gayretlerinin bir parçasıdır.
Avusturya	Esas itibariyle veri koruma alanıdır.
Kanada	Acil durumlara hazırlıklı olma gayretleridir.
Finlandiya	Veri güvenliği konusu ve ekonomik öneme sahip bir konu
Fransa	Hem yüksek teknoloji ürünü bir suç alanı hem de bilgi toplumunun gelişimini engelleyen bir problemdir.
İtalya	Bilgi toplumunun ilerlemesinin önemli bir parçasıdır.
Yeni Zelenda	Kritik altyapıların muhafaza edilmesidir.
Türkiye	Tüzel ve özel kişilerin varlıklarını sürdürmelerinde kullanacakları her türlü teknolojik güvenlik araçlarının ve yönetmelerinin bileşimidir.

Kaynak: (ISO, 2012) (Cavelty, 2008)

Siber savunma: Ülkelerin siber saldırılara karşı yaptıkları engelleme gayretlerine denilmektedir. Siber tehlikeler bilgi kaynaklarına karşıdır. Bu sebepten ötürü savunmanın ilk basamağı muhafaza edilmesi gereken yapı ve olguların bir listesinin yapılmasıdır. Bu doğrultuda yönetimler siber savunma niyetiyle stratejik ve kritik alt yapılarını tespit ederler. Hasara uğraması ve yok edilmesi halinde halk düzeninin ve devlet hizmetlerinin sürdürülmesinde zorluk oluşturacak; fonksiyonlarını yapamadığında toplumun sağlığına, güvenliğine ve iktisadi ferahına negatif etkide bulunacağı düşünülen bu kritik ağ, sistem ve yapılar şöyle sıralanabilir (Alkan vd., 2013) (Ünver vd., 2010).

- Bilgi ve iletişim kurumları ve kaynakları
- Enerji kurumları ve kaynakları
- Mali Kurumlar
- Medya ve Kültür
- Sağlık Kurumları

- Gıda ve Su Kaynakları Sektörleri
- Ulaşım Sektörü
- Savunma Sektörü
- Kamu Hizmetleri Altyapıları ve Kamu Güvenliği
- Nükleer, Biyolojik, Kimyasal Kaynak ve Maddelerdir.

Yukarıda ifade edilen bu kritik ve stratejik yapıların belirlenmesi yapıldıktan sonra diğer basamaklar işe koşulmaktadır. Çizelge 2 Siber savunma adımlarını göstermektedir.

Çizelge 2. Siber Savunma Adımları

Adım	**Yapılacak İşlem**
1. Adım	Sitemin zayıf ve eksik unsurlarını tespit etmek
2. Adım	Tespit edilen güvenlik zafiyetlerine ve açıklarına dair tehlike ihtimalini analiz etmek.
3. Adım	Her tehlikenin başarılı bir biçimde yönlendirilmesi durumunda oluşabilecek neticelerin değerlemesinin yapılması
4. Adım	Bütün saldırıların maliyetlenmesinin yapılması
5. Adım	Mevcut karşıt tedbirlerin maliyetlemesinin hesabının yapılması
6. Adım	Güvenlik mekanizmalarının ve sistemlerinin maliyet- yarar hesaplamaları yapılarak belirlenmesi.

Kaynak : Alkan vd. , (2013)

4. KURUMSAL BİLGİ GÜVENLİĞİ VE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Çalışmanın bu bölümünde kurumsal bilgi güvenliğine yönelik tehditler, alınabilecek önlemler bilgi güvenliği yönetim ve önleme sistemleri kapsamında kurumların gözetmesi ve uyması gereken kanun ve standartlar konusunda kavramsal bir çerçeve sunulmuştur. Bu kapsamda SIEM ve çözümlerinde temel bileşenler, etkin SIEM ve LOG yönetimi, 5651 sayılı Kanun, Kişisel Verileri Koruma Kanunu ve bu kanun kapsamında kurumlarda uyulması gereken zorunluluklar, İSO/IEC 27001 bilgi güvenliği standartları, BGYS kurulumunda yapılması gerekenler, PSI güvenlik standartları konseyi, COBIT ve FISMA konusunda bilgiler verilmiştir.

4.1. Kurumsal Bilgi Güvenliğine Yönelik Tehditler

Kurumların sahip oldukları ve faaliyetleri kapsamında kullandıkları bilgilerin kurum tarafından korunması ve saklanması oldukça gerekli ve süreklilik arz eden bir durumdur. Çünkü kurumların sahip olduğu bu bilgiler karşı taraf olarak adlandırılan kişiler tarafından birtakım amaçlar doğrultusunda ele geçirilmek ve kullanılmak istenebilir. Özellikle bilgi ve teknoloji çağı olarak adlandırılan günümüz koşullarında kurumlar veya ülkeleri zarara uğratmak ve bu zararın yanında birtakım kazançlar elde emek isteyen karşı taraflar, bunun hedef kurumun bilgi güvenliğini tehdit ederek sağlamaya çalışmaktadır. Bu nedenle kurumların özellikle kritik alt yapılarının bilgi güvenliğine yönelik tehditler ve saldırılar her geçen gün şiddetini artırarak kendini göstermeye çalışmaktadır.

Kurumsal bilgi güvenliğinde, karşı taraf, kötü niyetli şeklinde karakterize edilen korsan ya da saldırgan bireyler ve bu bireylerin gerçekleştirdikleri saldırılardır. Şahsi veya resmî kurumlarda bulunan bilgi ve bilgisayar güvenliği ve koruma sistem duvarlarını aşmak ya da bu mekanizmayı atlatmak, zafiyet yaratmak, hedefte olan kişileri dolaysız veya dolaylı şekilde zarara uğratmak, bilişim mekanizmalarına zarar vermek, sistemlerin işlerliğini engellemek, durdurmak, çökertmek ya da yok etmek gibi kötü amaç ve niyetlerle bilişim sistemleri ile alakalı gerçekleştirilen işlemler saldırı veya atak şeklinde ifade edilmektedir. Saldırganlar, hedefledikleri maksatlarına erişmek için pek çok farklı yöntem ve teknikleri kapsayan saldırılar planlamakta ve

gerçekleştirmektedirler. Saldırı çeşitlerinin bilinmesi, doğru bir biçimde değerlendirilerek analizinin yapılması, kanunlar ve stratejiler kapsamında gerekli önlemlerin belirlenmesi, kurumların bilgi güvenliği çalışmalarında büyük rol oynayan önemli faaliyetlerdir (Canbek ve Sağıroğlu, 2006).

4.2. SIEM (Security Information and Event Management) Anatomisi ve Gerekliliği

Zamanımız teknolojisi gelişim gösterdikçe bilgi ve verilerin hacmi daha da genişlemektedir. Böylece bilgilerin depo edilmesi ve işlenmesi gereksinimi her geçen gün daha da artmaktadır. Sahip olunan verilerin ve bilginin artış göstermesi ise bunların depo edilmesi için kaynak alanına durulan ihtiyacı ortaya çıkarmıştır. Ayrıca veri artışı demek ağ trafiğinin artışı demektir. Çoğalan ağ trafiğinin güvenli bir şekilde ve kesinti olmadan sürdürülebilmesi için ağ ve güvenlik araçlarının miktarı da artmaktadır. Bu nedenle büyük verilerin işlenmesi ve depo edilmesi için veri merkezlerine büyük iş düşmektedir. İfade edilen bu veri merkezleri, kurumların veri ve uygulamalarını toplu bir şekilde bünyesinde bulundurduğu için karşı taraf olarak bilinen siber korsanların hedefi haline dönüşmüştür. Bu doğrultuda veri merkezlerinde güvenliğin sağlanabilmesine her zamanki koşullardan daha da büyük önem atfedilmektedir (Akpınar, 2020).

Bilgi güvenliği kapsamında büyük bir görevi olan ve "güvenlik bilgileri ve tehdit/olay yönetimi" anlamını taşıyan "SIEM (Security Information and Event Management)" çözümlerinin bu kapsamda oynadığı rol önemlidir. Gerçek zamanlı rapor alma ve güvenlik tehditi analizi ile ağa dair tehditleri saptamaktadır. Bilgi güvenliğine yönelik tehditlerin her geçen gün türünün ve gücünün artması ise güvenlik önlemlerini ve yönetimini zorlaştırmaktadır. Bununla birlikte ağlara dahil olan cihaz miktarının artması nedeniyle bu cihazların yönetimi de güçleşmekte ve bu doğrultuda saldırganların ağa sızma ara yüzleri çoğalmaktadır. SIEM, birden çok kaynaktan edindiği verilerin analizini yaparak, aksiyon planlarının ortaya koyulmasında önemli bir rol oynar. Aynı zamanda saldırıların saptanması, dijital delillerin saklanması, bütünsel güvenlik analiz raporu ve güvenlik tehlikelerini gerçek zamanlı izleme şeklinde avantajları bulunan SIEM, kritik değere sahip bilişim teknolojileri unsurlarının nasıl bir saldırı ile karşı karşıya olduğu ve olabileceği hususunda ayrıntılı rapor üretebilmektedir (Akpınar, 2020).

SIEM, güvenlik olay/tehdit yönetimi olarak bilinen “SEM” ve güvenlik bilgi yönetimi yazılımı olan “SIM” teknolojilerinin birleşiminden meydana gelmiştir. SIM, günlük verilerin toparlanmasının otomatik hale dönüştürülmesini sağlayan bir programdır. SEM ise, bir yazılım, sistem ya da bilişim teknolojileri ortamında güvenlikle alakalı tehditleri adlandırma, toparlama, izlem ve rapor etme işlemidir. Güvenlik duvarları, ağ takımları ve sunuculardan alınan tehdit verileri, güvenlik zafiyetleri, tehlike ya da riskleri saptamak için ilgili algoritmalar ve istatistiksel yöntemlerle analiz edilmektedir. Kısaca SEM, tehdit olaylarının kaydının tutulmasını ve değerlemesini sağlamaktadır (Başaranoğlu, 2016). SIEM çözümleri pasif engelleyici, aktif izlem sistemleri olarak bilinmektedir. Geleneksel bir SIEM teknolojisinin bir saldırıyı önleme becerisi bulunmamaktadır. Ancak korelasyon motoru ve başka güvenlik araçlarıyla entegrasyonunun sağlanmasıyla bu saldırıların engellenmesini ve bir ihlal olduğunda yöneticilere bilgi vermeyi sağlamaktadır. Aktif izlem ekranı sayesinde de tehdit durumlarını anlık şekilde seyretme olanağı sunmaktadır. SIEM hatasız bir biçimde yapılandırıldığında, içten ve dıştan gelecek tehdit olaylarını belirleme ve yakalama, sistemde yetkili personelin hareket ve erişim haritasını ortaya koyma, rapor etme, sistem problemi veya saldırı sonrasında hata ayıklama hususunda yardım etmek gibi katkılar sunabilir (Akpınar, 2020).

4.3. SIEM Çözümlerinde Temel Bileşenler

Genellikle olması gereken standart bir SIEM yapısı, Şekil 5.’de sunulduğu üzere altı farklı bileşenden meydana gelmektedir. Bu unsurlar, kaynak cihaz, log toplama, günlüklerin ayrışması veya normalleştirilmesi olarak bilinen normalizasyon, kural ve korelasyon motoru, log depolama ve izleme ekranlarıdır. Bu unsurlardan her birisi diğer bileşenden özerk olarak iş görebilir. Ancak hepsi bir arada çalışmadan, SIEM bir bütün şeklinde işlem yapamayacaktır (Akpınar, 2020).

Şekil 5. SIEM çözümlerinin temel bileşenleri

Kaynak: Akpınar (2020)

Bazı kurumlarda ve kritik altyapılarda işe koşulan SIEM çözümü ile küçük ölçekli işletmelerin tercih edeceği çözümler farklılık yaratabilmektedir. Kritik altyapıların maruz kalacağı siber saldırı türleri, sistem sorunları daha kompleks olabileceği için tercih edilecek SIEM mimarisinin daha gelişmiş korelasyon becerilerine sahip olması kurumlar için öncelikli olmalıdır (Cyberdefenses INC, 2019).

4.4. Etkin SIEM Yönetimi

Kurumlar ve işletmelerin kullanacağı bir SIEM mimarisinde proje sürecinin başlangıcından itibaren planlanacak her adımı büyük önem arz etmektedir. Hatalı yapılandırılan, planlama süreci doğru yönetilemeyen bir işlemin neticesinde performans sıkıntıları, logların yığılması, log kaçırma ve tehditleri analiz etmede zorlanma gibi sorunlar yaşanabilmektedir. Veri merkezleri için SIEM projesine start verilmesinde planlama çok mühimdir. Oluşturulacak olan sistemin gereksinimi olan kaynakların ve kapasitenin hesabının yapılması da planlama aşamasının kritik faaliyetlerinden biri olarak görülmelidir. Kritik işlemlerin yapıldığı bir veri merkezinde etkin SIEM yönetiminde korelasyon, arama hızı, log kaçırma gibi odaklanılması gereken bir takım önemli parametreler bulunmaktadır. SIEM teknolojisini tipik bir log yönetimi ekipmanından ayıran en belirgin özelliklerin başında korelasyon özelliği gelmektedir. Korelasyon, veriler arasında bir ilişkinin olup olmadığını belirlemek için kontroller yaparak, eğer bir ilişki varsa bu ilişkinin etkisini ve gücünü inceleme olayıdır (Akpınar, 2020) ve SİEM teknolojisinin önemli bir avantajı olarak görülmektedir.

4.5. Kayıt (Log) Yönetimi

Log, bütün sistem ve ağ donanımlarında oluşan olay kaydıdır. Bu logların her birisi bir log girişinden meydana gelmektedir ve bu girişlerin tümü belli bir olayı içermektedir.

En önemlileri ise güvenlik loglarıdır. Kurulumu yapılan pek çok log bilgisayar güvenliği ile alakalıdır. Gelişmiş Teknolojiler Escal Enstitüsüne (SANS) göre loglar, güvenlik personeli için, belli bir araç ya da uygulama için bir olayın kim, ne, ne zaman, nerede ve neden konusundaki bilgilerin kaydını yapmak için tercih edilmektedir (Allen, 2020). Bu bilgisayar güvenlik logları virüsten koruma programı, güvenlik duvarları ve izinsiz girişleri belirleme ve önleme mekanizmaları gibi güvenlik yazılımları, sunucular, iş istasyonları ve ağ takımlarındaki işletim sistemleri ve uygulamalardan meydana gelmektedir (Kent ve Souppaya, 2006). Büyük log yönetimi harekât süreçlerinin karakteristik olarak gündelik kaynaklarını yapılandırmayı ve analizlerini hazırlamayı, tespit edilen tehditlere karşı cevap sürecini başlatmayı ve uzun süreli belleği yönetmeyi kapsamaktadır. Bunun yanında, günlük yönetimi logların gizliliğini, bütünlüğünü ve kullanılabilirliğini muhafaza etmeyi kapsamaktadır (Miller vd.,2011).

Log yönetimine çağımız şartlarında hiç olmadığı kadar büyük değer atfedilmektedir. FISMA, COBIT, HIBAA, SOX, ISO 27001 gibi uluslararası kural, standart ve prensipler etkili log yönetimini zorunlu hale dönüştürmüştür. PCI veri güvenliği standartları da log yönetimine zorunluluk getiren ilkelere başka bir örnek olarak verilebilir. PCI DSS standardı altı başlık altında temel 12 ihtiyaç maddelendirmektedir. Bu maddelerden biri de log yönetimine ait olgulardır. Aslında kanunlar, prensipler ve standartlar tüm yaptırımlara göre daha etkin bir rol oynamaktadır. Bunun yanında Mayıs 2007'de 5651 sayılı kanunda internet suçlarını önlemeye yönelik kurumların log yönetimi konusunda yükümlülükleri ve sorumlulukları ifade edilmiştir. Log yönetimi log toplama, normalleştirme ve indexleme, korelasyon, filtreleme/rapor etme ve alarm yönetimi bölümlerinden oluşmaktadır. Log yönetimiyle alakalı bazı stratejik adımlar aşağıdaki gibi sıralanabilir (Akbaş, 2013).

- Logların merkezi bir noktada toplanması
- Logların saklanması
- Verilere hızlı erişimi ve gösteriminin sağlanması
- Çok sayıda log formatının desteklenmesi
- Veri analizinin yapılması
- Kayıtların saklanması

- Arşivleme ve arşivlenen logları geri getirme
- Verilerin yetkiler ve ilişkiler seviyesinde erişimi
- Veri bütünlüğünün sağlanması

Daha önce de ifade edildiği üzere yukarıda belirtilen maksatlarının haricinde logların depolanması ve güvenliğinin ifa edilmesi belli kanun ve standartlar kapsamında yapılmaktadır (Akpınar, 2020).

4.6. Kurumsal Bilgi Güvenliğine Yönelik Alınabilecek Önlemler

Kurumsal bilgi güvenliğinin etkin bir şekilde sürdürülmesinde üst düzey yönetimin maddi ve manevi destek sağlayarak güvenlik süreçlerini benimsemeleri önemlidir. Bilgi güvenliği düzenlemelerinin firmalarda üst yöneticilerden başlayıp daha alttaki personele kadar yaygınlaşarak ulaşması ve kurumsal bir farkındalığın oluşturulması çok büyük önem arz etmektedir. Bu sürecin uygulanması esnasında ISO 27001 ve başka bilgi güvenliği yönetim stratejilerinin alt yapısının kullanılmasında büyük avantaj vardır. Güvenlik aşamalarının sürekli geliştirilen, denetlenebilen ve güncellenen bir yapıya kavuşturulması lazımdır. Veri güvenliğinin yalnızca bilgi teknolojisi güvenliği olmadığı kuralının benimsenmesi de büyük öneme haizdir. Kurumlarda bilgi güvenliği ek bir maliyet, gereksiz bir masraf ya da bir yük olarak düşünülmemeli, örgütün ticari misyonu ve iş gelişim vizyonu kadar değerli ve belirleyici bir pozisyonda konuşlandırılmalı, bir örgüt kültürü haline dönüşmelidir (Tipton ve Krause, 2007).

Veri sorumlularının; kişisel verilerin hukuka aykırı şekilde işlenmesini engellemek, bu verilere izinsiz erişimi önlemek ve hukuka uygun şekilde korunmasını ifa etmek gayesiyle alınabilecek teknik ve idari tedbirler bulunmaktadır. Kurumların ifa etmesi gereken bu önlemleri saptarken, kişisel verilerin özellikleri ve korunması gereken ortam dikkate alınmalıdır (KVKK, 2019).

Çizelge 3'te veri sorumluları tarafından alınabilecek teknik ve idari tedbirler gösterilmiştir.

Çizelge 3. Teknik ve İdari Tedbirler

Teknik Tedbirler	İdari Tedbirler
Yetki Matrisi ve Yetki Kontrol Erişim Logları Kullanıcı Hesap Yönetimi Ağ ve Uygulama Güvenliği Şifreleme Sızma Testi Saldırı Tespiti ve Önleme Sistemleri Log Kayıtları Veri Maskeleme ve Veri Kaybı Önleme Yazılımları Yedekleme Güvenlik Duvarları ve Güncel Anti-Virüs Sistemleri Silme, Yok Etme ve Anonim Hale Getirme Anahtar Yönetimi	Kişisel Veri İşleme Envanteri Hazırlanması Kurumsal Politikalar (Erişim, Bilgi Güvenliği, Kullanım, Saklama ve İmha vb.) Sözleşmeler (Veri Sorumlusu - Veri Sorumlusu, Veri Sorumlusu - Veri İşleyen Arasında) Gizlilik Taahhütnameleri Kurum İçi Periyodik ve/veya Rastgele Denetimler Risk Analizleri İş Sözleşmesi, Disiplin Yönetmeliği (Kanuna Uygun Hükümler İlave Edilmesi) Kurumsal İletişim (Kriz Yönetimi, Kurul ve İlgili Kişiyi Bilgilendirme Süreçleri, İtibar Yönetimi vb.) Eğitim ve Farkındalık Faaliyetleri (Bilgi Güvenliği ve Kanun) Veri Sorumluları Sicil Bilgi Sistemine (VERBİS) Bildirim

Kaynak : KVKK (2019).

Kurumsal bilgi güvenliği konusunda alınacak önlemlerden öncelikli olarak kurumun bir risk değerlemesi yapıp, olası risklerin kuruma etkilerinin neler olduğu, maddi kayıplara yol açıp açmadığı ve hangi risklerin giderilmesinin önemli olduğu sorularının cevaplanarak çözümlerin planlanması ve işe koşulması gerekir. Yani kurumsal bir risk ölçümü ve değerlemesi yapılmalıdır. Bu noktada uygun ölçüm yöntemlerinin ve doğru yazılımların kullanılması önemlidir. Çünkü riskin azaltılması için yapılacak işlemlerin bir maliyeti vardır ve maliyetleme gereklidir (Eminağaoğlu ve Gökşen, 2009). Risk azaltıcı teknolojik ve süreç içerikli çözümlerin yanında iş yapma biçimini düzenleyecek tüm prosedür, politika ve ilkeler kuruma tam entegre olacak şekilde uygulatılmalıdır. Bu doğrultuda kurumda çalışan tüm personel ve kurum paydaşı olan tüm tüzel kişiler ile gerekli gizlilik sözleşmeleri yapılmalı, önemli cezai sorumluluklar sözleşmelerde bulunmalıdır. Ayrıca bilgi gizliliği, ticaret sırlarının muhafazası hususlarına ilişkin yükümlülük ve sorumlulukların bildirildiği bilgi güveliği belgesi çalışanlara

imzalatılmalıdır. Kurumlarda, yöneticiler başta olmak üzere tüm çalışanların eğitilmesi ve bilgi güvenliğini sahiplenerek farkındalık yaratılması önemlidir. Bu nedenle sadece cezalar ve caydırıcı uygulamalar değil bilgi güvenirliği konusunda hassas davranışlar sergileyen personelin ödüllendirilmesi de gerekmektedir (Eminağaoğlu ve Gökşen, 2009).

Kurumsal bilgi güvenliğine yönelik öneriler içerisinde teknoloji boyutunda da yapılabilecek birçok önlem bulunmaktadır. Bunlar; ilgili her türlü ağ, iletişim, bilgisayar, elektronik kayıt, arşiv, yedek ve ayrıca yazılı belgeler, yazıcı, faks, vb. araçların kullanılmasında mümkün olduğunca en güncel kimlik doğrulama ve yetkilendirme teknolojileri seçilmelidir. Buna ilaveten, belirli noktalarda, cihazlara kaydı yapılan ve/veya ağlar üstünden gönderilen bilgiler için şifreleme teknolojilerinin de mutlak suretle yapılması gerekmektedir. Bunun sağlanmasında yetkin personelin iç denetlemeler yapması ve ayrıca kurum dışından güvenlik danışmanları vasıtasıyla dış denetlemeler gerçekleştirmesi kurum tarafından sağlanmalıdır. Ayrıca kurumların istihdam edeceği personeli işe alırken özellikle ticaret sırları ve gizil evrakları yoğun olarak kullanacak çalışanların adli sicil kayıtları, güvenlik kontrolleri, referansları, kişilik testleri vs., uygulamalar gerçekleştirilmelidir. En küçük kurumdan en büyüğe varıncaya kadar tüm örgütlerde ve devlet kurumlarında bilgi güvenliği konusunda farkındalık yaratacak bilinçlendirme ve eğitim etkinlikleri, projeleri düzenlenerek çalışanların bilgi güvenliği konusunda bilgilendirilmesi gerekmektedir (Eminağaoğlu ve Gökşen, 2009).

Aşağıda belirli ilke ve standartlar doğrultusunda kurumların bilgi güvenliğini ifa etmesinde takipte olmaları gereken ulusal ve uluslararası stratejiler kısaca sıralanmıştır. Yüksek düzeyde kurumsal bir bilgi güvenliğinin sağlanabilmesi adına (Sağıroğlu, 2019);

- Kurumların ve diğer tarafların bilgi güvenliği standartlarını bilmesi, uygulaması, hazırlanan politikalar doğrultusunda denetlemelerin yapılması ve karşılaşılan sorunların giderilmesi gerekir.
- Standartlar bağlamında hazırlanan politikaların üst düzey yöneticiler vasıtasıyla desteklenmesi, bütün personel ve paydaşlar tarafından taviz verilmeden

uygulanması, siber güvenlik yönetiminin dinamik bir süreç olduğunun farkına varılması ve ortaya çıkan risklerin yönetimi gerekmektedir.

- Kurumların standartlara uyduğunu belgelendirmeleri, uluslararası sahada geçerli sertifikasyonlarının bulunmaları, yüksek düzeyde bir bilinçliliğin yaratılması adına gereklidir.
- En zayıf halka kadar güvende olunacağı ihtimalini göz önünde bulundurarak gerekli tedbirlerin alınması gerekliliği fark edilmeli ve uygulanmalıdır.
- TSE 15408 ortak kriterler doğrultusunda hem kullanılan program ve uygulamaların sertifikalandırılması hem de sertifikalı ekipmanların kullanılmasının özendirilmesi gerekmektedir.

Neticede standartlar yüksek düzeyli bir güvenliği garanti etmiş olsa da bazı durumlarda standartlarında yetersiz olabileceği düşünülmeli ve bu doğrultuda bilgi ve siber güvenliğe daha geniş bir açıdan bakılması ve tedbirlerin çok boyutlu alınması gerektiği de akıldan çıkarılmamalıdır (Sağıroğlu, 2019).

4.7. 5651 Sayılı Kanun

Mayıs 2007 tarihinde yürürlüğe giren "İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi" yasasına göre, mevzuatta belirtilen trafik bilgileri yine mevzuatta belirtilecek süre kadar yani en az altı ay, en çok 2 seneye kadar saklanması gerekliliği ve bu bilgilerin doğruluğu, gizliliği ve bütünlüğünün ifa edilmesi gerekliliği ifade edilmiştir. Bu noktada ifade edilen trafik bilgileri, bilişim sistemlerinden alınan log kayıtlarıdır. Bu kayıtlar adli vaka kapsamı için delil özelliği taşımaktadır. 5651 Sayılı yasada; "kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişiler" tanımlamasına karşılık gelen devlet kurumları, internet sağlayıcıları vd. 6 aydan 2 seneye kadar log kayıtlarını saklamakla yükümlüdür (Akpınar, 2020).

5651 Sayılı yasanın gereklerine uymak mecburiyetinde olan kurumlar; otel, alışveriş merkezi, yüksek öğretim kurumları, kafe, internet Cafer, küçük ve orta ölçekli firmalar, fabrikalar gibi interneti toplu şekilde kullanılmasına izin veren ve halka açan yapılardır. Bu yasanın kapsamına, mekanların müşterilerine verdiği ücretsiz internet servisi ve şirketlerin personeline kurum içinde sunduğu internet hizmeti de dahildir. 5651 Sayılı

kanun doğrultusunda birtakım yükümlülükler bulunmaktadır. Bunlar (Resmi Gazete, 2007);

- İç IP adres dağıtım logları (Dynamic Host Configuration Protocol - DHCP)
- Web erişim logları
- Web erişimlerinde içerik tabanlı filtrelemenin gerçekleştirilmesi
- Logların zaman damgası ile saklanması ve gizlilik temininin sağlanması

İfade edilen bu yükümlülükler irdelendiğinde tercih edilen SIEM ürününün bu yükümlülükleri karşılaması beklenir (Akpınar, 2020).

4.8. Kişisel Verileri Koruma Kanunu

Kişisel verilerin dikkatsizce işlenmesi, yetkisiz bireylerin ulaşımına açılması, ifşası, kötüye kullanımı ya da maksat dışı kullanılması neticesinde kişisel hakların ihlal edilmesinin engellenmesi için ilgili yasa yürürlüğe girmiştir. Anayasa Mahkemesinin Nisan 2014 tarihli kararında; "Kişisel verilerin korunması hakkı, kişinin insan onurunun korunmasının ve kişiliğini serbestçe geliştirebilmesi hakkının özel bir biçimi olarak, bireyin hak ve özgürlüklerini kişisel verilerin işlenmesi sırasında korumayı […]" hedeflediği belirlenerek, "kişisel bilgilerin ticari firmalar için kıymetli bir varlık özelliği kazanması neticesinde, özel sektör unsurlarınca ortaya koyulan risklerin daha yaygın ve önemli boyutlara erişmesi, terör ve suç örgütlerinin kişisel bilgileri elde etme yönündeki çalışmalarının artması gibi faktörler" nedeniyle kişisel bilgilerin geçmiş dönemde olduğundan çok daha fazla muhafaza edilmeye ihtiyacı olduğuna işaret edilmiştir (KVKK, 2019).

6698 Kişisel Verileri Koruma Kanunun amacı, "özel hayatın gizliliği olmak üzere kişisel veriler işlenirken kişinin temel hak ve özgürlüklerini korumaktır. Aynı zamanda kişisel verileri işleyecek olan gerçek ve tüzel kişilerin yükümlülüklerini belirtirken aynı zamanda bu kişilerin uyacakları usul ve esasları düzenlemektir". Kanun 1. Bölümünde yer alan 2. Maddesinde yasanın kapsamı ifade edilirken, 3. Maddede tanımlar yer almıştır. İkinci bölümde kişisel verilerin işlenmesi konularına değinilmiştir. Bu doğrultuda kişisel verilerin işlenmesi için gereken ilkeler, işlenme şartları, özel nitelikli kişisel verilerin işlenme şartı, verilerin silinmesi, yok edilmesi ve anonim hale

getirilmesi ve kişisel verilerin aktarılmasının şartlarından bahsedilmektedir. Kanun 3. Bölümünde ise haklar ve yükümlülüklere yer verilmektedir. Bu kısımda veri sorumlusunun aydınlatma yükümlülüğünden, kişisel veri sahibinin haklarından ve veri güvenliğine dair yükümlülüklerden bahsedilmiştir. Veri güvenliğine ilişkin yükümlülüklerin yer aldığı madde olan 12. Maddenin kapsamı şöyledir; veri sorumlusunun verileri, güvence altına almak, hukuka uygun olarak işlenip işlenmediğini kontrol edip, erişimini önlemek ve bu amaçlar doğrultusunda güvence altına almak için tedbirleri almak zorundan olduğunu, üçüncü kişilerle paylaşımının mümkün olmadığını ve bu bilgilerin istenmeyen olaylar sonucunda başkalarının eline geçtiğinde yapması gerekenleri bildirir. Dördüncü bölümde başvuru, şikâyet ve veri sorumlusu sicili sunulurken, beşinci bölümde veri sorumlusu tarafından kişisel verileri silinmeyen veya anonim hale getirilmeyen kişilerin yaptıkları şikayetler doğrultusunda sorumlu için verilecek cezaların bulunduğu suçlar ve kabahatler konuları yer almaktadır. Altıncı bölümde ise kişisel veriler koruma kurumu ve teşkilatı çalışanlarının görevleri ve yükümlülükleri açıklanmaktadır (KVKK, 2020).

KVKK'nın 12. Maddesinde bulunan veri sorumlusunun kişisel verileri saklama ve koruma konusundaki yükümlülük ifadeleri (KVKK, 2019) ile kanun koyucu tarafından verilerin güvenliğini sağlamak amacıyla veri sorumlularının çok fazla idari ve teknik yükümlülüklerinin olduğuna vurgu yapılmaktadır. Ayrıca veri sorumlularının edindikleri kişisel verilere dair sır saklama yükümlülüklerinin bulunması ve vazifelerinden çekilseler bile bu sorumluluklarının devam etmesi oldukça önemlidir. Bilgi güvenliği açısından belki de en fazla karşı karşıya kalınan olaylardan biri bilgilerin sızdırılması mevzularının kamuoyundan saklanmasıdır. Yasa koyucu bunu öngörü olarak belirlemiş ve veri sorumlusunu; işlenen verilerin hukuka aykırı olarak başkaları vasıtasıyla elde edilmesi durumunda ilgilisine ve Kurul'a bildirme konusunda sorumlu tutmuştur. Bu konuda bildirim yapma yükümlülüğü ile sızıntı nedeniyle meydana gelecek zararın minimalize edilmesi ve ileride olma ihtimali bulunan sızıntıların önüne geçilmesi yönünde adımların atılması hedeflenmiştir (Küzeci, 2019).

4.9. KVKK Kapsamında Kurumlarda Uyulması Gereken Zorunluluklar

Türkiye'de faaliyetlerini sürdüren tüm kuruluşların Kişisel Verileri Koruma Kanunu hükümlerine bütünleşmiş şekilde çalışmalarını yapması bir mecburiyettir. 6698 Sayılı

yasa, gündelik yaşamda farklı farklı sistemlere bir biçimde kaydı yapılmış bulunan kişisel bilgilerin kullanılmasına bir standart sunmaktadır. Bu standart, kişisel bir bilginin izin verilenden daha farklı maksatlarla işlem yapılmasını engellemek ve bu bağlamda önemli yaptırımları ortaya koymaktadır (KVKK, 2019).

KVKK Yasası kapsamında kurumlardan uyulması istenilen beklentileri aşağıda sıralanmıştır (Kişisel Verileri Koruma Kurumu, 2017) (Barış, 2018):

- Kişisel bir verinin alınıp kaydedilmesi için açık rıza almak gereklidir.
- Bilgi saklanırken verilen taahhüt ve alınan açık rızanın ifade edildiği anlaşmayı kanuni otoritenin istediği bir durumda onlarla paylaşılmalıdır.
- Açık rıza ile verileri elde edilen bir ferde, arzu ettiği herhangi bir zamanda, bu bilgilerin yok edilmesini ya da güncellenmesini yapabileceği yollar ifade edilmeli ve bu yollar devamlı açık olmalıdır.
- Açık rıza ile elde edilen veriyi iletirken ve korurken gerekli güvenlik tedbirlerinin alınması ve bu bilgilere erişim hakkı bulunmayan kişi ve kuruluşların eline geçmesi engellenmelidir.
- Firmanın sistemine sadece SIEM eklemesi yeterli olmamaktadır. Alınan SIEM'in ilgili Kanun ile entegre olması şarttır.

Veri sorumlusu personelin ve kurumun bilişim sistemleri genellikle hem içten hem de dıştan gelen saldırılara, siber tehditlere veya kötü niyetli yazılımlara maruz olmaktadır ve bazı belirtilerine rağmen bu sorun uzun zaman anlaşılamamakta ve önlemek için geç kalınmaktadır. Bu sorunu önlemek için (KVKK, 2019);

a. Bilişim sistem ağında hangi yazılım, program ve servisin iş gördüğünün kontrolünün yapılması,
b. Bilişim sistem ağında sızma ya da istenmeyen bir durumun olup olmadığının tespit edilmesi,
c. Tüm kullanıcıların işlem hareketleri kaydının rutin olarak saklanması (log kayıtları vb.),
d. Güvenlik problemlerinin olabildiğince çabuk biçimde rapor edilmesi,

e. Personelin sistemdeki güvenlik zafiyetlerini veya bunları kullanan tehlikeleri bildirmesi için resmi bir raporlama prosedürünün hazırlanması gerekli ve önemlidir.

4.10. Bilgi İşlemde İSO/IEC 27001 Bilgi Güvenliği Standartları

1906'da "Uluslararası Elektroteknik Komisyonu", 1947'de ise "Uluslararası Standartlar Organizasyonu" uluslararası platformda ticaret ve elektroteknik standartların sağlanabilmesi için, İsviçre'nin Cenova kentinde hayata geçirilmiştir. ISO ve IEC beraber teknik çalışma ekipleri meydana getirerek (Joint Technical Committee-JTC) ve Bilimsel Komiteler (SC) koordinasyonunda bütün dünyada genel geçer görecek standartları hazırlamaktadır. ISO vasıtasıyla bilgi teknolojileri güvenlik standartları ile ilgili faaliyetler JTC–1 BT Komitesine bağlı SC-27'ye bağlı olarak faaliyet yürüten Bilgi Teknolojileri Güvenlik Teknikleri Alt Komisyonunda incelenmektedir (Sağıroğlu, 2019). Bu komisyonun görev ve sorumlulukları aşağıda sıralanmıştır:

- Bilişim teknolojileri sistemleri güvenlik hizmetlerinin ve gereksinimlerinin tanımlanması,
- Güvenlik yöntemleri ve yapılarının gelişimi,
- Güvenlik rehberlerinin gelişiminin sağlanması ve
- Yönetim destek raporları ile standartların hazırlanmasıdır (Sağıroğlu, 2019).

Bilgi ve bilişim sistemlerinin güvenliğini önemseyen, ilgili yazında kabul edilen anlayışları geliştiren ya da bu hususlara profesyonel şekilde ele alan İngiliz Standartlar Enstitüsü, bu konudaki ilk faaliyetlerini hazırlamış, geliştirdiği ilkeleri BS7799 standarttı adı ile 1995 yılında yayınlamıştır. BS7799:V1 ise bunun ilk versiyonu olarak bilinmektedir. 1999 yılında ise aynı standardın 2. bölümü olan BS7799:V2 standardını yayınlamıştır. Tüm çevrelerin bu hususlara ayrı özen göstermesi, başka ülkelerin gerçekleştirdiği faaliyetlerden de yararlanılarak, BS7799:V1 standardı 2000'de birtakım düzeltmeler ve küçük güncellemelerle ISO tarafından ISO/IEC 17799 ismiyle uluslararası ISO standardı haline dönüştürülmüştür. ISO vasıtasıyla daha sonra ise ISO 27001:2005 ismiyle dünya genelinde "bilgi güvenliği standardı" olarak kabul edilmiştir. Türkiye'de de AB uyum programında da ifade edilen bu standartların işe koşulması hususunda yapılan faaliyetler kapsamında, ISO 27001:2005 standardı Türkçeye

çevrilmiştir. Bu doğrultuda TSE tarafından TS ISO/IEC 27001 "Bilgi Güvenliği Yönetim Sistemi (BGYS)" standardı isminde yayımlanmış ve belgeleme işlemlerine başlanmıştır. BGYS; bireyleri, süreçleri ve bilişim sistemlerini kapsayan ve üst düzey yönetim tarafından destek gören bir yönetim mekanizmasıdır. İlerleyen yıllarda ise bilgi güvenliği standartları ailesi olarak 27xxx serisi şeklinde kabul edilmiş, mevcut standartlar ise zaman içerisinde sırayla bu ailenin birer üyesi haline getirilmiştir (Sağıroğlu, 2019).

ISO 27001, Nisan 2007 tarihinde Türkiye'de alınan kararlar neticesinde BGYS'nin belgelendirilmesi için ihtiyaç olan standartları kapsayan, kurumsal bilgi güvenliğinin ne şekilde yapılabileceğini ifade eden bir dokümandır (Şen ve Yerlikaya, 2013). BGYS kurum ve organizasyonların mühim bilgilerini yönetme, koruma ve güvenceye alma hedefiyle hazırlanan bir mekanizmadır. Bilgi güvenliği yönetimine organize bir şekilde yaklaşılması ve bir sisteminin geliştirilmesi hem kurumsal hem de toplumsal düzeyde kurumların güvenliği yönünden büyük önem ihtiva etmektedir (Aktaş, 2020). ISO 27001, organizasyonların yapılarına uygun politikalar, prosedürler ve planlar hazırlamasına katkı sağlayan uluslararası alanda genel geçer bir yapısal metodoloji sunmaktadır. Bunun yanında ISO 27001 sertifikasına sahip olan kurumlar bilgi güvenliğine dikkat ettiğinin ve bu konuya hassas yaklaştığının mesajını verir (Özbilgin ve Özlü, 2019).

4.11. BGYS Kurulumunda Yapılması Gerekenler

BGYS'nin kurulması, uygulanması ve yönetilmesi sürecinin aşamalarının oluşturulmasında; literatürde bulunan araştırmalar ve ISO 27001 bilgi güvenliği yönetim sistemi standardında yer alan maddelerden 11 adım aşağıda sıralanmıştır (Aktaş, 2020) (Koç, 2008) (Yılmaz , 2014).

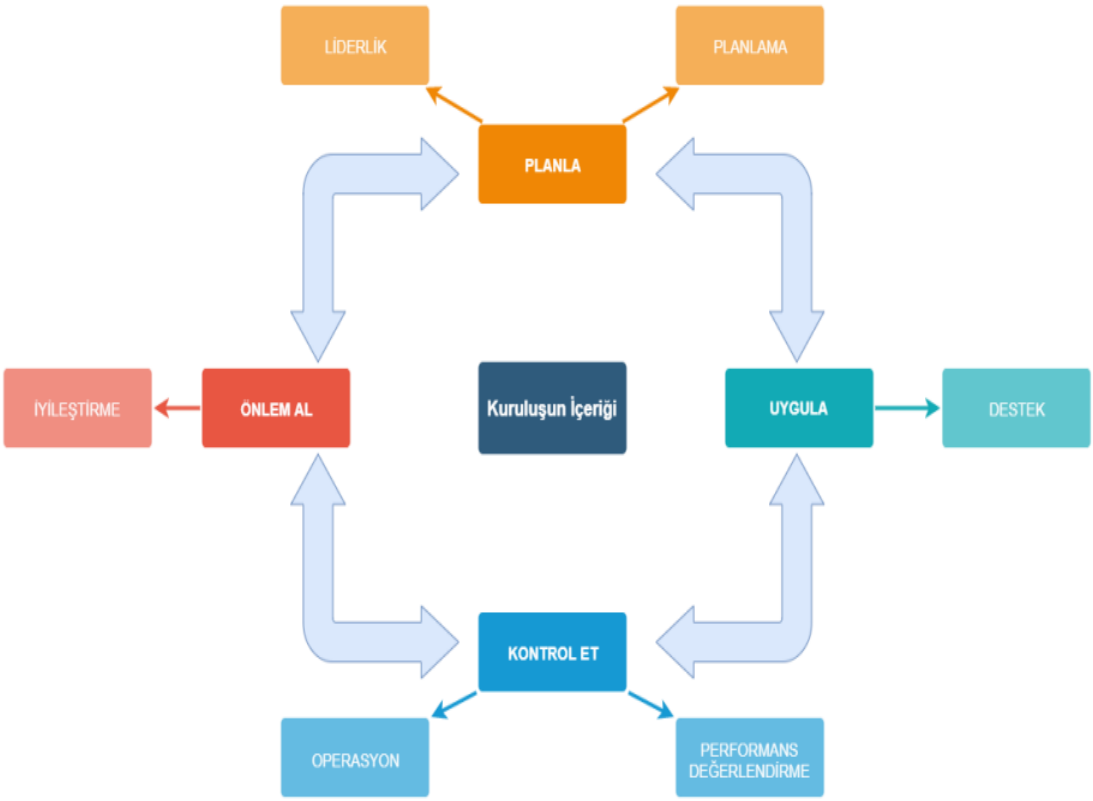
- Üst yönetimin fonksiyonlarını ve sorumluluklarını yerine getirmesi,
- Bilgi güvenliği takımının oluşturulması,
- İçeriğin tespit edilmesi,
- BGYS yol haritasının hazırlanması,
- Varlık envanterinin ve kaynakların belirlenerek oluşturulması,

- BGYS'nin gerçekleştirilmesi ve uygulamanın yapılması,
- Risklerin tespiti, analizi, değerlemesi ve yönetişim,
- Uygulanabilirlik bildirgesi,
- İç denetimin yapılması,
- Yönetimin gözlenerek kontrol edilmesi,
- Belgelendirme ve dış denetimin gerçekleştirilmesi
- Eğitim ve farkındalık çalışmalarının yapılması,

Neticede; sistemin kurulumu, varlık envanterinin hazırlanması, risk ve tehlikelerin saptanması, gereksinimler noktasında güvenlik politikalarının hazırlanması ve bunların denetiminin yapılıp uygulamanın kontrol edilmesi, kontroller neticesinde kullanılan sistemin yeniden güncellenerek geliştirilmesi şeklinde birbirini takip eden bu faaliyetlerin aşama aşama yapılması anlamını taşımaktadır (Yılmaz , 2014). Yapılan bu faaliyetlerin sonucunda da ISO 27001 standartına başvuru işlemi sağlanır.

BGYS'nin kurulmasında PUKÖ modeli olarak bilinen basamaklar oldukça önemli adımlardır. Bunlar hedefe ulaşmak için planların hazırlanması basamağı olan planla; politika ve mevzuata uygun oluşturulan planın işe koşulması aşaması olan uygula; performansın etkinliğini gözleme ve denetlemenin yapıldığı kontrol et ve BGYS'nin sürdürülebilirliği ve iyileştirme aşamalarında düzeltme ve tedbirler alma işlemlerini kapsayan önlem al basamaklarıdır (Aktaş, 2020) (Şen ve Yerlikaya, 2013).

Şekil 6 kurumlarda PUKÖ döngüsünü özetlemektedir.



Şekil 6. Kurumlarda PUKÖ döngüsü

Kaynak: Emir Erdoğan (2020)

4.12. PCI Güvenlik Standartları Konseyi

"PCI (Payment Card Industry) Güvenlik Standartları Konseyi" ödeme sistemlerinde bilgi güvenliği için standartların tanımlanması, fark edilmesi, gelişimi, yaygınlaştırılması ve tüm sektörün bütünleşmesi için hazırlanmış global bir forum olup, "Ödeme Kartı Endüstrisi Güvenlik Standartları'nı sağlama, muhafaza etme, geliştirme ve teşvik etme konularında faaliyetler yürütmektedir (PCI Güvenlik Standartları Konseyi, 2021). Bunun yanında, değerleme ve tarama karakteri, öz değerlendirme ölçekleri, eğitim, öğretim ve ürün sertifikasyon programları gibi standartların işlemesi için gerekli kritik donanımı sağlar. Konseyin kurucuları; "American Express, Discover Financial Services, JCB International, MasterCard ve Visa Inc." veri güvenliği bütünleşmiş programlarının her biri için mekanik ihtiyaçların bir parçası olarak PCI Veri Güvenliği Standardı (PCI DSS) hazırlatılmıştır. PCI konseyi vasıtasıyla sunulan

"Qualified Security Assessor (QSA)" sertifikasına sahip olan denetimciler sayesinde yapılan çalışmaların denetimleri yapılabilmektedir (Sağıroğlu, 2019).

PCI DSS, her bir alanda çok sayıda özel ihtiyaçlara sahip 12 ayrı kontrol alanını kapsayan bir güvenlik spesifikasyonunu bünyesinde barındırmaktadır (Simpson, 2017):

- Sistemler güvenlik duvarı vasıtasıyla muhafaza edilmelidir.
- Güçlü parola sistemi ve yapılandırma tanımlamaları işe koşulmalı ve öngörülebilen şifreler kullanılmamalıdır.
- Başta kart bilgileri olmak üzere depolanan kişisel bilgiler ve veriler doğru bir şekilde muhafaza edilmelidir.
- Kişisel ve kart bilgilerinin açık ve genel ağlar üstünden transfer edilmesi şifreli olmalıdır.
- Virüsten koruma programı kullanılmalı ve bunlar rutin şekilde güncellenmelidir.
- Oldukça güvenli sistemler ve uygulamalar hazırlanmalı ve bunlar sürdürülebilir olmalıdır.
- Kart sahibi bilgilerine erişimi, kurumun bilmesi gerekenlerle sınırlandırılmalıdır.
- Bilgisayar erişimi bulunan her kullanıcıya benzersiz bir kimlik ataması yapılmalıdır.
- Kart sahibi bilgilerine fiziki erişme olanağı minimuma indirgenmelidir.
- Ağ sistemine ve kart sahibi bilgilerine bütün erişimler takip edilmelidir.
- Güvenlik mekanizmaları ve süreçleri rutin şekilde test edilmelidir.
- Personel ve yükleniciler için bilgi güvenliğine yoğunlaşan sürdürülebilir bir program benimsenmelidir.

4.13. COBIT

COBIT, "Control Objectives for Information and Related Technology" nin kısaltılmış şeklidir. COBIT'in Türkçe karşılığı ise "Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri" şeklinde bilinmektedir. Bu ifade, COBIT'in maksadını anlatması yönünden önemli bir karşılıktır. COBIT, bilişim teknolojileri yönetiminde kurumların erişmesi

gerektiği hedefleri ve vizyonu ortaya koyar. COBIT'i, ITIL, CMMI ve ISO standartlarından ayıran en büyük özelliği tüm bilişim teknolojileri fonksiyonlarını kapsayan bir çerçeve sunmasıdır. Bu sebepten ötürü yukarıda ifade edilen diğer standartlardan farklı olarak, COBIT bireysel ya da grup halinde bilişim teknolojisi süreçlerinden ziyade bu teknolojilerin yönetilmesine yoğunlaşır (Tutu, 2010).

COBIT, ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından 1996'da hazırlanmış, işletmelerin ve kurumların bilgi teknolojileri yönetimi ve yönetişimi konusunda stratejiler işe koşmasına, düzenlemelerine ve uygulamalarına fayda sağlamak için oluşturulmuş bir bilişim teknolojileri yönetim planıdır (Beyaz. Net, 2020) (TETRA, 2020). Bilişim teknolojileri yönetişiminde (IT Governance) erişilmesi gereken hedefleri ortaya çıkarır. COBIT üst düzey yönetime, denetim yapanlara ve bilişim teknolojisi kullanıcılarına çalışma amaçlarının bilgi işlem amaçlarına evrilmesini, bu amaçlara varmak için lazım olan kaynakları ve yapılan aşamaları bütünleştirirken, aynı anda bilişim teknolojileri alt yapılarını da verimli kullanmayı sağlar (Beyaz. Net, 2020).

COBIT tüm paydaşların gereksinimlerini karşılayan, kurumları uçtan uca kapsayan, tek bir bütünleşmiş çerçeve uygulayan, bütünleşik bir model sergileyen ve yönetişim ile yönetimi birbirinden ayırabilen beş önemli etki alanına sahiptir (TETRA, 2020). COBIT aşağıdaki genel özellikleri gösterir (Tutu, 2010) (Şahinaslan , 2010):

- Bilişim teknolojilerinin kurumun iş (ticari) gayelerine hizmet etmesi gerekliliğini benimser,
- Bilişim teknolojisi ile iş stratejisinin entegrasyonunu oluşturmaya çalışır,
- Bu özellikleriyle çağdaş bilişim teknolojileri yönetiminin genel kabul görmüş ilkelerini kapsar,
- Teknolojisi siber tehlikelere karşı güvenlilik ve verimlilik arz eder,
- Kabul edilebilir seviyede tehlike ihtimalini yönetir,
- Başka bilişim teknolojisi yönetim standartları ile (ISO, ITIL, CMMI, MOF, vb.) entegredir,
- Her sektörden ve her ölçekteki firmalar tarafından kullanılabilir,

- Denetleme, süreç iyileştirme ve yönetimi, ölçüm, kıyaslama vb. farklı kullanım gayeleri bulunur.
- Süreçlerin ilgili kısımlarında ilgili standart (ISO 9001/27001, ITIL, CMMI ve PMI vb.) anlayışlarını tavsiye eden çerçeve bir yapı oluşturan denetim aracı şeklinde fayda sağlar.

COBIT çalışma oryantasyonu, bilişim teknolojileri süreçleri ile bağlantılı iş ödevlerini saptarken başarıyı ölçebilen farklı olgunluk modelleri ve metrikleri sağlayarak iş amaçlarını teknoloji altyapısıyla ilişkilendirmeyi kapsar. COBIT'in merkez noktası, aşağıda ifade edilen dört temel alanda gruplanan 34 süreçten meydana gelmekte ve bu süreçler birçok kurum ve işletmenin BT işlevlerinin tümünü içinde barındırır. COBIT bu nedenle süreç tabanlı bir model benimsemektedir. Bu temel alanlar şöyledir (Tutu, 2010) (Beyaz. Net, 2020):

- Planlama ve organizasyon,
- Edinim ve kurulum,
- Hizmet, teslim ve destek,
- İzlem ve değerleme.

4.14. FISMA

Federal Bilgi Güvenliği Yönetim Yasası (FISMA), 2002'de hayata geçirilen bir Amerika Bilgi Güvenliği Federal Yasasıdır (IS). Bu kanun mecburi bilgi güvenliği risk yönetimi standartlarının gelişim gerekliliği de dahil olmak üzere Federal Hükümet bilgi güvenliğini güçlendirmeye dair çıkarılmış bir yasadır. FISMA'nın genel karakteri arasında federal yapılar için politika hazırlama, risk yönetme ve BS farkındalık eğitimi bulunmaktadır. FISMA, E-Devlet Yasası olarak da tanınmaktadır (FISMA, 2022). FISMA kurumlar için siber güvenliğin önemine dikkat çekerek ve açık olarak düşük maliyetlemeyle etkin güvenlik için risk temelli bir politikayı savunmaktadır. FISMA özellikle, bilişim teknolojisi güvenlik tehlikelerini kabul edilebilir bir seviyeye düşürmek için her örgüt başkanının doğru maliyetlemeyle politika ve prosedürleri işe koşmasını gerektirmektedir. FISMA'ya göre "bilgi güvenliği" kavramı, bütünlük, gizlilik ve kullanılabilirlik ilkelerini yerine getirmek için bilgi ve bilgi mekanizmalarına

yetkisiz ulaşma, kullanma, ifşa etme, kesintiye uğratma, değişiklik yapma veya imha etmeden korumak anlamını taşır (FISMA, 2022).

FISMA ayrıca kamu kurumlarının güvenlik yönetimi planlarında müteahhitlerin çalışmalarını da kapsamasını ortaya koymaktadır. FISMA işlem kılavuzlarının hazırlanmasında sorumlu olan "Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)", FISMA ile beraber aşağıdaki etkili bilgi güvenlik programını ve adımlarını önermektedir. Bu program aynı anda kurumlara dair bir siber saldırıların önlenmesi için siber güvenliğe yardım eder (Securitynotes, 2017) (Taylor, 2006):

- Muhafaza edilmesi gereken bilgi varlıkları gruplandırılır,
- Asgari seviyede ana güvenlik denetimleri seçilir,
- Bir risk değerleme prosedürü işe koşularak kontroller sınırlandırılır,
- Sistem güvenlik programında ifade edilen kontroller belgelenir,
- Bilgi sistemlerine dair doğru güvenlik kontrolleri uygulanır,
- Uygulama neticelerinin etkinliğinin denetimi yapılır ve değerlenir,
- Çalışmanın amaçlarına ve misyonuna uygun risk seviyesi saptanır,
- Bilgi ağlarında olması gereken yetkilendirmeler ifa edilir,
- Güvenlik kontrollerinin rutin şekilde izlemi yapılır.

5. SİBER GÜVENLİK TEHDİTLERİ VE GÜVENLİK ZAFİYETLERİ

Araştırmanın bu bölümünde siber güvenlik tehditleri ve güvenlik zafiyetleri genel bir bakış açısı ile incelenmiş, siber güvenlik tehditlerinin özellikleri, tarafları, türleri, tespiti ve kurumlara etkileri özetlenmiştir. Ayrıca kurumları etkileyen siber güvenlik tehdit ve zafiyetleri konusunda tehdit önleme güvenlik sistemleri, penetrasyon (sızma) testi uygulamaları, siber güvenlik zafiyet analizleri, kurumların güvenlik önlemleri için tavsiyeler, kurumlarda son kullanıcı farkındalığı ve siber güvenlik sigortası konularından bahsedilerek kavramsal bir çerçeve sunulmuştur.

5.1. Siber Güvenlik Tehditlerin Özellikleri ve Amaçları

Siber güvenlik tehditleri maddi fayda sağlamak için gerçekleştirileceği gibi siyasi, askeri veya kişisel fayda sağlamak gibi maddi olmayan farklı nedenlerle de yapılabilmektedir. Siber güvenlik tehditlerinin maksadının ne olduğu mühimdir ve bilinmesi gerekir. Fakat gayesi ne olursa olsun siber korsanlar her daim yüksek bir güdülenmeyle bilişim sistemlerindeki ara yüz açıklarını tetkik ederler ve yeni zafiyetler buldukları an sistemi işlemez hale dönüştürmekten geri durmazlar (Güngör, 2015).

Kurumların, firmaların, ülkelerin ve bireylerin önemli bilgilerini kanuni olmayan yöntemlerle elde etmek, gasp etmek, başka taraflarla paylaşmak ya da silmek, bu bilgilerin depo edildiği ve işlendiği mekanizmaları iş göremez hale getirmek siber güvenlik tehditlerinin birincil hedefleri arasında bulunmaktadır (Adır, 2019).

Siber güvenlik saldırıları çağımız koşullarında global ölçekte önemli maddi zarara neden olan ve neredeyse bütün toplumların ortak problemi haline dönüşmüş bir güvenlik saldırısı türüdür. Siber güvenlik tehditlerinin özellikleri aşağıdaki gibi sıralanabilir (Güngör, 2015):

a. Sonuçları büyük hasarlara neden olur ve neticeleri yıkıcıdır. Özellikle internet temelli iş yapan bir bilgi sistemini güvenlik tehditinin özelliğine göre bütünüyle işlem yapamaz hale sokabileceği gibi belli bir zaman zarfında hizmet dışı kalmasına sebebiyet verebilir.

b. Maddi olarak ucuz bir saldırı tekniğidir. Maddi açıdan oldukça masraflı konvansiyonel silahlarla karşılaştırılamayacak kadar ucuza mal edilebilir. Saldırı

için askeri bir hava gücü inşa etmenin bir yönetime maliyeti oldukça yüksekken bir siber saldırı için zamanımızda düşük bir sunucu maliyeti kadar bir finansal kaynak yeterli olmaktadır.

c. Düzenlenen saldırının kim tarafından gerçekleştirildiğini belirlemek oldukça güç ve hatta bazen olanaksızdır. Birçok coğrafi bölgeden katılım kolaylığı sebebiyle izlemek son derece zorlaşmaktadır. Hatta dağıtık hizmet çökertme olayları (DDoS) ile milyonlarca bilgisayar, sahiplerinin izni olmadan saldırı aşamalarına kötücül yazılımlar vasıtasıyla dâhil edilebilmektedir.

d. Siber güvenlik tehditlerinin bilişim sistemlerinde meydana getirdiği etkileri zaman geçtikçe farklılaşmakta ve çoğalmaktadır. Daha etkin saldırıların zamanla daha az bilgisi ve deneyimi olan saldırganlar tarafından yapılabilmesi kolaylaşmaktadır.

e. Bir siber güvenlik saldırısı ardından internet vasıtasıyla ulaşılan e-devlet, dijital bankacılık gibi hizmetler servis dışı olabildiği gibi e-posta yoluyla yapılan haberleşme kesilebilir ve internet temelli iş yapan kritik altyapılar çökebilir.

f. Bir toplumun düşman bir ülkede finansal kayıp meydana getirme ve toplumsal kargaşaya yol açmasının en kolay, masrafsız ve kompleks yöntemi kritik altyapılarını hedef alınarak siber güvenlik saldırıları düzenlemesidir. Siber tehditler klasik askeri güç kullanımı kapsamı dışındaki bir asimetrik savaş tekniği olduğu için hem saldırıyı yapan ülkeye karşı uluslararası hukukun verdiği savunma hakkının kullanılması oldukça zordur, hem de saldırı düzenleyen toplumun bu saldırıyı sevk ve organize ettiğini kanıtlamak olanaksız bir durumdur.

5.2. Siber Güvenlik Tehditlerinin Tarafları

Siber güvenlik tehditlerinin tarafları tehditin türü, amacı ve yapılış şekline göre değişebilmektedir. Karşı taraf olarak adlandırılan siber saldırganlar hedefteki taraf yani saldırıya uğrayan ilgili tarafı farklı şekillerde zarar verirken bu zarar ilgisi olmayan kişiler tarafından da hissedilmekte ve birçok mağduriyet yaşanabilmektedir. Siber güvenlik tehditleri, siber uzayda yer alan ve kişisel ve tüzel kullanımı olan yazılım, program, donanım ve altyapıları hedef alırlar. Maksatları, saldırı teknikleri ve motive

olma şekilleri oldukça farklı aktörler bulunmaktadır ve bu karşı taraf aktörleri merak, hırs, intikam almak, menfaat sağlamak, maddi kazanç sağlamak, siyasi ve politik görüş, ideolojik, dinsel içerik ve benzeri nedenlerle saldırıyı gerçekleştirmek için güdülenirler (Adır, 2019).

Gayeleri ilgilendikleri hedef sistemleri zarara uğratmak ya da iş göremez hale dönüştürmek, mental baskı oluşturmak, kötü propagandaya sebep olmak ve bu sistemler kapsamında işlem yapılan ve korunan hassas ve önemli bilgileri elde etmek, tahrip etmek, gasp etmek ya da yok etmektir. Siber güvenlik tehditlerini organize eden karşı taraf aktörleri; çalışanlar, genç ve deneyimsiz meraklılar, Bot-Net (zombi bilgisayar ağı) Operatörleri, suç örgütleri, zararlı program yayımcıları, siber suçlular, siber korsanlar, rakip işletme ve kuruluşlar, organize suç örgütleri, hackerler, devlet ya da istihbarat grupları, terör örgütleri, tabi afetler ve devletler şeklinde oldukça geniş bir yelpazesi bulunmaktadır (Güngör, 2015) (Başaran, 2017).

5.3. Siber Güvenlik Tehditlerinin Türleri

İlgili literatürde siber güvenlik tehdit türlerinin belirlenmesinde farklı gruplandırmalar yapılmaktadır. Bunlar (Güngör, 2015);

a. Kaynağına göre siber güvenlik tehdit türleri (bireyler, Hacktivist oluşumlar, bilgisayar korsanlığı platformları, siber suç örgütleri, işletmeler, ülkeler),

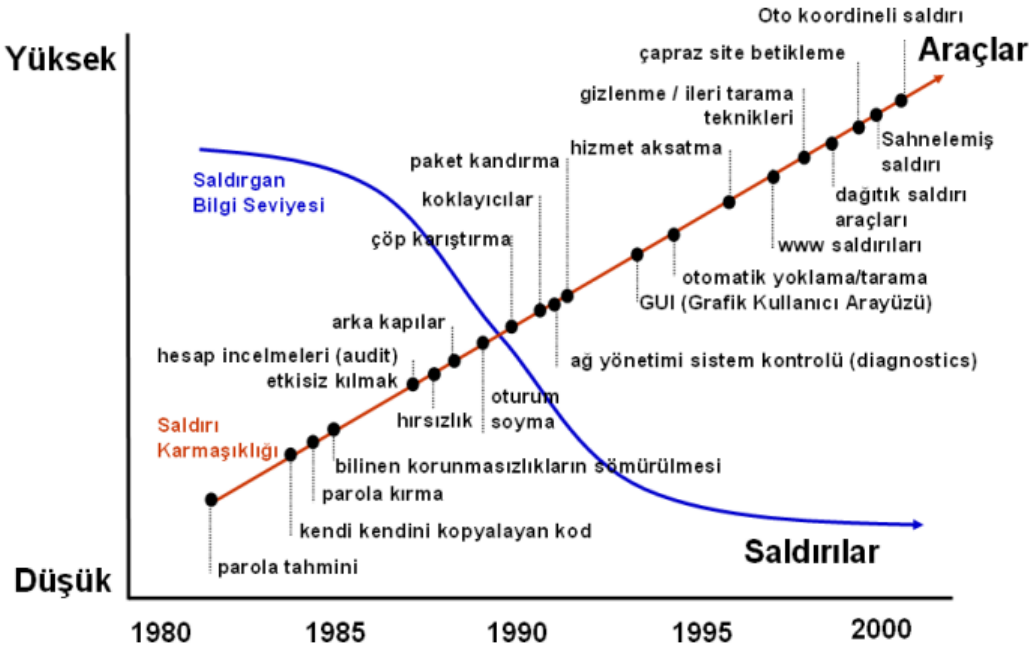
b. Saldırı hedefine göre siber güvenlik tehdit türleri (kişisel kullanıcılar, işletme ve firmalar, siyasi oluşumlar, devlet kurumları),

c. Kazanım amacına göre siber güvenlik tehdit türleri (siyasi, askeri, kişisel, maddi),

d. Elde edilen neticeye göre siber güvenlik tehdit türleridir (siber korsanlık, siber casusluk, eylemci saldırılar, siber terör, siber sabotaj, siber savaş),

e. Bilişim sistemindeki hasara göre siber güvenlik tehdit türleridir (gizlilik öğesine yönelik saldırılar, bütünlük öğesine yönelik saldırılar, erişebilirlik öğesine yönelik saldırılar).

Şekil 7'de yıllara göre gelişen saldırı türleri ve saldırgan teknik bilgisi gösterilmiştir.



Şekil 7. Saldırı türleri, karmaşıklığı ile saldırgan teknik bilgisi

Kaynak: Allen (2001)

Şekil 7'de siber güvenlik saldırıları teknolojinin gelişmesiyle yıllara göre oldukça farklılaşmış ve karmaşık hale gelmiştir. Parola tahmini yapma veya kurumlarda notların atıldığı çöpleri takip etme gibi oldukça basit saldırı türleri, artık yerini daha kapsamlı ve kompleks bir hal alan çapraz site betikleme, oto koordineli, dağıtık ve sahnelenmiş siber saldırılara devretmiştir. Özellikle 21. Yüzyıla gelindiğinde siber saldırılar veya saldırılarda tercih edilen araçlar, teknik yönden gittikçe kompleks bir duruma gelirken, bu saldırıyı organize edecek saldırganın gereksinim duyduğu bilginin düzeyi azalmış, deneyimi gittikçe düşmüştür. Bu durum tehdit ve saldırgan miktarını, saldırılar neticesinde meydana gelecek zararları çoğaltırken, saldırıyı engellemek için yapılması gereken işlemleri de güçleştirmiştir (Canbek, 2005).

Siber uzayda, siber güvenlik profesyonellerinin bilgisayar sistemlerini muhafaza etmelerini gerektirecek çok fazla siber saldırı silahı ve saldırı türü yer almaktadır. Mesela trojan atları, virüsler, solucanlar, mantık bombaları, dağıtık veya normal hizmet dışı bırakma, sosyal mühendislik faaliyetleri, oltalama saldırıları vd., gibi. Karşı taraf olan korsanlar bu saldırı türlerini kullanarak sızdıkları bilgisayar sistemleri veya ağlarına değiştirici, hasar verici, hizmet aksatıcı veya bilgileri ele geçirerek sızdırma

şeklinde birçok zarar açabilmektedir. Bu saldırılar kurum ya da işletmelerde mali zararlara sebep olabileceği gibi imaj ve saygınlığın azaltılması şeklinde de zararları bulunabilmektedir (Ulusal Siber Olaylara Müdahale merkezi [USOM TR-CERT], 2014).

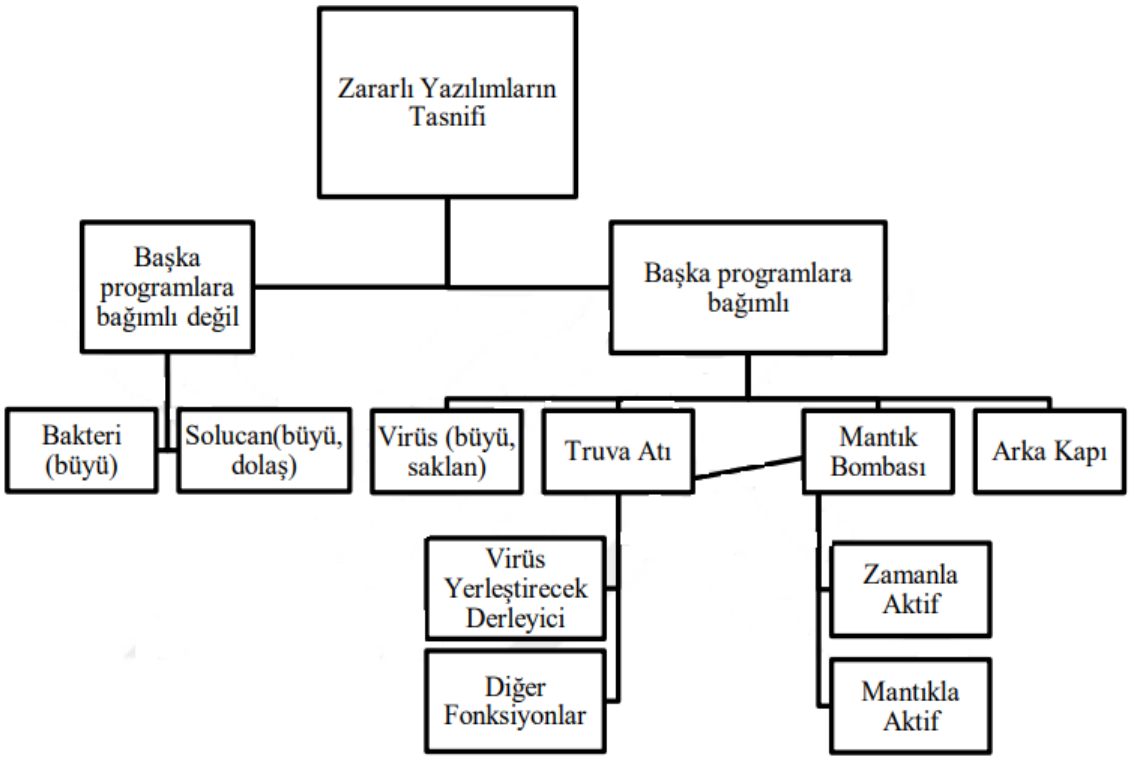
21. yy'da kullanımı en çok tercih edilen siber silahlar ve saldırı türlerini tetkik ettiğimizde ise karşımıza; zararlı yazılımlar (malware), yemleme saldırısı ve sistemleri etkilemeye yönelik hizmet dışı bırakma saldırıları ve sosyal mühendislik atakları gibi sözdizimsel ve popülaritesini sürekli koruyan saldırı silahları ve türleri özetlenmiştir (Emir, 2020).

Zararlı Yazılımlar (Malware): En genel anlamıyla bilgisayar sistemlerini kötü niyetle kullanmak için sistem bilgilerine ulaşmaya katkı sağlayan veya bilişim sistemlerine oldukça büyük zararlar açan kötücül bilgisayar programlarıdır (Ulusal Siber Olaylara Müdahale merkezi [USOM TR-CERT], 2014). Son zamanlarda, bilişim sistemlerinde bilgi güvenliği hususunda zafiyet meydana getiren ve her biri farklı amaçlara yönelik değişik teknikler kullanan çok farklı türde kötü niyetli yazılımın bulunduğu bilinmektedir (Canbek, 2005). Malware genel bir üst kavram olup virüsler, solucanlar, truva atları, rootkitler ve casus yazılımlar bu sınıfın kapsamında kendine yer bulabilmektedir. Bu yazılımların kişilere, süreçlere ya da teknolojilere karşı kullanımı tercih edilebilir. Bu konudaki temel ve en kritik nokta ise malware'nin maksadının sistemlere izinsiz erişme hakkını elde etmek ya da değerli-hassas bilgilerin elde edilmesini sağlamaktır (Ulusal Siber Olaylara Müdahale merkezi [USOM TR-CERT], 2014).

Aşağıda kötücül yazılımlar kapsamında bulunan yazılım türlerinin yapmış olduğu işlemlerin genel bir listesi verilmiştir (Özarpa vd., 2021);

- Bilgisayar sistemini uzaktan yönetebilirler (remote control-uzaktan kumanda)
- Kişisel verileri sistemden tek tek toplayarak elde ederler (spyware-casus yazılım)
- Bilgisayarda tuş kullanımını kaydederler (keyloggers-tuş kayıtçıları)
- Sisteme sessizce girip bütünüyle ele geçirirler (rootkit-trojan)

Zararlı yazılımlar farklı programlarla bağlantılı olup olmamasına göre sınıflandırmış ve Şekil 8'de olduğu gibi bu ayrım şematize edilerek gösterilmiştir (Çifci, 2017).



Şekil 8. Zararlı yazılımların sınıflandırılması

Kaynak: Çifci (2017)

Yemleme (Phishing): diğer bir adıyla oltalama olarak bilinen bu zararlı uygulama, kanun dışı yöntemlerle kullanıcıların herhangi bir yerde kullandıkları kullanıcı adı, şifre, kimlik bilgileri, kredi kartı bilgileri gibi verilerin elde edilmesidir (Wikipedia, 2022). Türkçe karşılığı yemleme olan "Phising" kelimesi İngilizce kelimelerden türetilmiş olup password (şifre) ve fishing (balık avlamak) kelimelerinin bileşiminden meydana gelmiştir. "Yemleyici/oltalayıcı" diye ifade edilen bu şifre avcıları, genellikle e-posta atarak bireylere ulaşmakta ve kredi kartı bilgisi gibi bazı önemli bilgilerini sanki resmi bir yapıymış gibi ister. Bu şekildeki e-postaları cevaplayan kişilerin de hesapları, şifreleri vb. önemli bilgileri çalınabilmektedir (Ulusal Siber Olaylara Müdahale merkezi [USOM TR-CERT], 2014).

Hizmet Dışı Bırakma (Denial of Service)/Dağıtık Hizmet Dışı Bırakma (DoS/ DDoS): Bu saldırı şekli isminden de anlaşılacağı üzere hedefteki sistemin işlem

yapmasını engellemek ve rutin yaptığı hizmetleri aksatma ve bozma niyetiyle gerçekleştirilmektedir. Bu şekilde kullanıcıların erişmek istediği kaynak ve sistemleri kullanması engellenmiş olmaktadır. Hizmet dışı bırakma saldırıları tek bir kaynaktan yapılabildiği gibi dağıtık şekilde de gerçekleşebilmektedir. Bu saldırılar üç farklı biçimde gerçekleşebilir: (i) Bir ağa taşma girişimi yapılarak meşru ağ trafiği engellenebilir, (ii) İki araç arasındaki bağlantılar hasara uğratılabilir ve bu şekilde bir hizmete ulaşım önlenmiş olur ve (iii) belli bir kişinin, belli bir hizmete ulaşımı engellenebilir (Keleştemur, 2015).

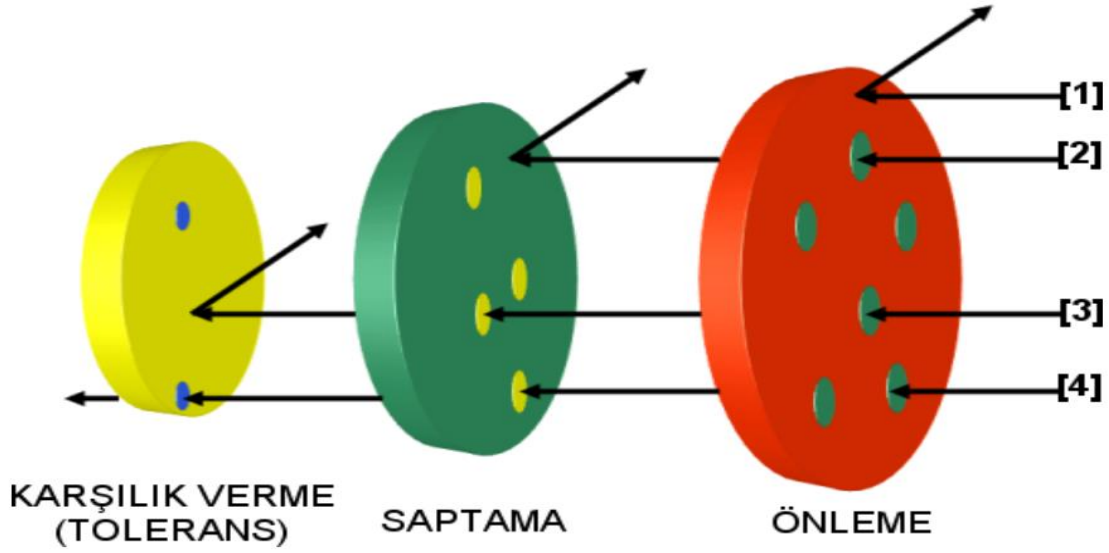
Sosyal Mühendislik: Bu faaliyetler temel anlamda bilgisayar veya bilgisayar ağlarındaki açıklıklardan yararlanılarak sistemi zarara uğratan saldırıların tersine "sosyal mühendislik" atakları ile kişilerin iletişim, etkileşim, düşünce şekli, güven veya kısaca insani zaaflarından yararlanarak siber güvenlik aşamalarının etkisiz duruma dönüştürülmesi veya atlatılması olarak yapılmaktadır. Siber saldırı olarak sosyal mühendislik teknikleri; farklı yalanlar ile sahte senaryolar oluşturmak, hedefteki tarafa kendini güvenilir bir kaynak olarak göstermek veya basit ödüllendirme yollarıyla bilgi sızdırmak olarak sıralanabilir (Bican, 2008).

5.4. Siber Güvenlik Tehditlerinin Tespiti

Güvenlik, yalnızca önleme ile yapılabilecek bir mevzu değildir. Mesela bir müzedeki eserlerin iyi bir şekilde korunmasını sağlamış olmak, müzenin etrafının çitlerle ve duvarlarla çerçevelendirilmesi, kapıların kapalı ve kilitli bulunması ve bir bekçinin bulunmasını engellemez. Aynı biçimde bilişim sistemlerinde de siber güvenlik tehdit girişimlerini tespit edecek çeşitli tekniklerin de kullanılması gerekir. Siber tehditleri önleme, saldırıları zorlaştıran (ama olanaksız hale dönüştürmeyen) ya da saldırı yapacakların cesaretini kıran (ama yok etmeyen) bir engel mimarisidir. Tespit etmek ve karşılığını vermek olmadan önlemenin ancak kısıtlı bir katkısı dokunur. Yalnızca önleme ile yetinilmiş olunsaydı, pek çok siber güvenlik tehditinden haberdar olunamayacaktı. Tespit etme ile daha önceden tanınan veya yeni meydana çıkmış saldırılar raporlanır ve bu saldırılara uygun cevaplar verilebilir. Saldırıların tespitini yapmada birincil ve en temel adım, sistemin tüm durumunun ve hareketinin izlemi ve bu iz bilgilerinin kaydedilmesidir. Böylece, saldırı ardından analiz yapmak için veri ve delil de toplanmış olacaktır. "Güvenlik duvarları, saldırı tespit sistemleri (intrusion

detection system), ağ trafiği izleyiciler, kapı (port) tarayıcılar, bal çanağı (honeypot) kullanımı, gerçek zamanlı koruma sağlayan karşı virüs ve casus yazılım araçları, dosya sağlama toplamı (checksum) kontrol programları ve ağ yoklayıcı (sniffer) algılayıcıları, tespit etme sürecinde tercih edilen en popüler teknikler arasında yer almaktadır (Canbek ve Sağıroğlu, 2006).

Şekil 9'te siber güvenlik süreçlerine bir örnek sunulmuştur.



Şekil 9. Güvenlik süreçleri ve siber tehditlerin tespiti

Kaynak: Canbek ve Sağıroğlu, (2006)

Şekil 9'te 1 ve 4 rakamlarıyla kodlanan 4 farklı saldırı gösterilmektedir. 1 kodlu saldırı, hemen önleme aşamasında engellenirken; 2, 3 ve 4 kodlu saldırılar bu aşamada önlenememiştir. Önleme aşamasını geçen bu saldırılardan 2 kodlu saldırı, saptama olarak ifade edilen aşamada tespit edilmiş ve yok edilmiştir. 3 ve 4 kodlu saldırılar, tespit edilemeden bu aşamayı atlatmışlardır. Belirlenen tolerans ile hazırlanmış son süreç olan karşılık verme aşamasında 3 kodlu saldırı engellenirken; tüm safhaları atlatıp geçen 4 kodlu saldırı ise sistemi zarara uğratmıştır (Canbek ve Sağıroğlu, 2006).

Aşağıda bulunan Çizelge 4'te literatürde bulunan bazı siber güvenlik tehditlerinin tespit ve önleme teknikleri sunulmuştur.

Çizelge 4. Siber Güvenlik Tehditlerin Tespiti ve Önlenmesi

Siber Güvenlik Tehditleri	Siber Tehditleri Tespit Etme	Önleme Teknikleri
GPS Yanıltma	Sinyalin yüksek çözünürlükte dijitalleştirilmesi ve analizi	Anti Jammer kullanmak
Araya Girme Saldırısı	Bağlantılarda beklenmedik kopmalar ve tanımlı olmayan lokasyonlar üstünden bağlantı	HTTPS üstünden internet kullanımı ve çoklu kimlik doğrulama tekniği
Bellek Taşması	Veri yığını depolayan hücrelerin denetimi	Değişikliklerin düzeltilmesi
Kötücül Yazılım	Anti-virüs program kullanımı	Anti-virüs programlarının kullanımı, işlemcinin formatlanması
ARP Yanıltma	Açık kaynaklı paket analizi gerçekleştiren yazılımlar	Yeni ARP paketleri belirlemek ya da HTTPS ve SSH ile kanal şifrelemek
Vekil Sunucu Saldırısı	IP bağlantılarının taranmasında benzer veya bilinmeyen IP bağlantısının tespiti	Kaynak yönlendirme opsiyonlarının inaktif olması ya da ağda IP değiştirmenin kaldırılması
Hizmet Kesintisi Saldırıları	Sistemin sitelerle olan bağının beklenmedik biçimde kopması ve değişim izni vermesi	Sistemin bağlanılacağı sitenin alternatiflerine geçiş yapılabilmesi
Siber Atak	Sistemde yoğunluğun bulunmadığı bilindiği halde fazla yoğunluğun olması	Sensörlerden iletilen bilgilerin işlemci vasıtasıyla görmezden gelinmesi

Kaynak : ENISA (2017); Muratoğlu (2020).

Nmap, Maltego ve Metasploit saldırı tespit araçları kullanılarak IP'lere bağlı portların taranması ile port açıklıkları konusunda bilgi sahibi olunarak, sistemin IP yollarında

bağlı olduğu bağlantı noktalarının haritalaması çıkarılarak ve veri tabanında yer alan sistem dinleme yolları ile sisteme bağlanacak yolları dinleme yöntemleri kullanılarak tehdit ile ilgili veri ve zafiyetlere ulaşılabilir (ENISA, 2017) (Muratoğlu, 2020).

5.5. Siber Güvenlik Tehditlerinin Kurumlara Etkileri

Bilişim teknolojilerinin özellikle de online bağlantı ve internetin, yaşamımızın her alanında olduğu zamanımız şartlarında, ifade edilen bu teknolojiler ve araçlar insanlara, kurumlara ve ülkelere her yönden katkı sağlamış ve sunduğu hizmetlerle önemli şekilde hayatı kolaylaştırmıştır. Ancak her geçen gün kullanımı artan bu teknolojik sistemler ve uygulamalar; kişileri, kurumları ve devletleri bu altyapılara bağımlı hale dönüştürmüştür. Bilişim teknolojilerinin hasar alması, tehditlere uğraması ya da işlem yapmasında yaşanan sorunlardan dolayı hizmet dışı kalması halinde çok mühim sıkıntılar doğuracak risklere maruz bırakabilecek, toplum düzenini baltalayacak hatta ulusal güvenliği tehlikeye sokabilecek altyapılar haline evirilmiştir. Zira bilişim teknolojilerinden bu derece yoğun şekilde istifade edilmesi neticesinde; bireyler nezdinde siber bağımlı insanlar, daha genel manada da toplum ve ulus olarak da siber bağımlı toplum ve ulus olma yolunda çok çevik adımlar atılmakta ve değişimler görülmektedir. Bu bağımlılığın başını ise bilgi toplumuna geçiş süreci çekmektedir. Bu dönüşümde, daha çok önemli bilgilerimizi dijital platforma aktarma sürecinde başarı kaydedilmiş, fakat bunun akabinde bu bilgilerin güvenliğini ifa edecek düzenlemeler hususunda aynı başarı kaydedilememiştir (Yılmaz vd., 2015).

Türkiye'de ve diğer dünya ülkelerinde görülen bütün bu bilgi toplumu haline dönüşüm süreci ile beraber, bu sürece zıt şekilde kişisel, ticari, maddi ve siyasi güdüler barındıran kötücül yazılımların miktarında büyük artışlar yaşanmıştır. Bu doğrultuda devletlerin kurumları ve işletmeler siber güvenlik tehditlerinin hedefi haline gelmiştir. Bu önemli sorunun her geçen gün örneklerinin arttığı da gözlenmektedir. Kötü niyetli yazılımların neden olduğu maddi hasarlar milyar dolarları bulmuştur. Kötücül yazılımlardan geçmişten bazı örnekler verilecek olunursa (Ünver ve Canbay, 2022);

- "I Love You" isimli virüsün dünya çapında yaklaşık olarak 45 milyon bilgisayar sistemine bulaştığı ve yaklaşık 10 milyar dolar zararın açıldığı bilinmektedir.

- “Nimda” kurtçuğunun dünya çapında yaklaşık 3 milyar dolar, “Love Bug”ın ise 10 milyar dolar zarara neden olduğu bilinmektedir,
- “MyDoom” isimli truva atının 4,8 milyar dolar civarında zarara neden olduğu bilinmektedir.
- “Sapphire/Slammer” solucanının 2003 yılında online olan bilgisayarların %90’ına 10 dakika içinde bulaştığı bilinmektedir.
- 2005 yılının ilk altı ayında zarara uğrayan bilgisayar miktarı bir önceki seneye göre %63 arttığı hesaplanmıştır.
- Amerikalı tüketicilerin son iki senede bilgisayarların tamir edilmesi ve yenilemesi için 7,8 milyar dolar harcadığı saptanmıştır.
- 2008’de geliştirilen siber casusluk maksadıyla kullanılan “Regin Virüsü” 2014’te fark edilmiş ve Rusya, Sudi Arabistan, İrlanda, Belçika, İran gibi birçok ülkeye yayılım göstermiştir (Ünver ve Canbay , 2022).

Zamanımızda ise Türkiye’de önemli kritik alt yapılardan olan e-devlet uygulamalarına yönelik siber güvenlik tehditleri o kadar çoğalmıştır ki, siber güvenlik önlemleri maalesef yetersiz kalmıştır. Bu durumun örnekleri; yakın tarihte gerçekleşen TEİAŞ sistemlerine yetkisiz erişim, Ankara kentindeki vatandaşların tapu bilgilerinin gasp edilmesi, HSBC Bankasının 2.7 milyon müşterisinin banka verilerinin ele geçirilmesi olaylarıyla gözlenmektedir (Yılmaz vd.,2015).

Ulusal ve uluslararası boyutta gerçekleşen çalışmalar, kurumlarda gelecek dönemlerde görülecek en önemli risklerin bilişim sistemlerine yönelik siber güvenlik tehditlerinin olacağını bildirmektedir. Bu düşünce ve varsayım kapsamında bir siber güvenlik tehditinin kurumsal bir yapıya maddi, manevi birçok zarar vereceği ve kurumun itibar, güven, imaj ve tarafları ile yapılan iş hukukunda birtakım güçlükler ve yaptırımların yaşanmasına sebebiyet vereceği aşikardır. Siber güvenlik tehditlerinin kurumsal etkilerini aşağıdaki gibi özetleyebiliriz (Şahinaslan , 2013);

- Bilgi güvenliği ihlalleri, manevi ve güven kayıpları
- Marka ve imaj kaybı,
- Kritik alt yapıların işlevsiz hale gelmesi,

- Paydaş ve müşteriler üzerinden güven kayıpları,
- Kurumsal hatta ülkesel boyutta güvenlik açıkları,
- Maddi ve manevi kayıplar,
- Kanuni yasal yükümlülüklerden dolayı kurumun davalara maruz kalmasıdır.

5.6. Penetrasyon (Sızma) Testi

Bilişim sistemlerindeki aksaklıkları ve açıklıkları ortaya koymanın en etkili tekniklerinden olan penetrasyon (sızma) testleri, potansiyel siber güvenlik tehditleriyle ilgili risklerin değerlenmesi amacıyla, erişim, yetkilendirme ve işlevsellik özellikleriyle sistemlere herhangi bir zarar verilmeden yapılan gerçek saldırıların simülasyonu olarak bilinmektedir. Penetrasyon testleri sayesinde bilgi güvenliği maksadıyla alınan tedbirlerin yeterli olup olmadığı, zafiyet ve eksikliklerin tehditlere açık yüzü olup olmadığı saptanarak belirlenen güvenlik açıklarının rapor edilmesi ve giderilmesi hedefiyle faaliyetler yapılır. Siber saldırılar tetkik edildiğinde saldıranların genel olarak sistemde bulunan açıklıklardan sızarak saldırılarını yaptığı gerçeği, penetrasyon testlerine daha çok önem atfedilmesine işaret etmektedir. Penetrasyon testleriyle bilişim güvenliği ile ilgili problemlerin gerçek bir saldırı yapılmadan önce tespit edilerek nasıl düzeltileceği ve olası güvenlik zafiyetlerine karşı ne şekilde tedbirler geliştirileceği konusunda planlar yapılması sağlanır (Vacca, 2013). Penetrasyon testleri, uzman güvenlik personeli vasıtasıyla, hedeflenen bilişim ağı, sistemi veya uygulamalar konusunda bilgi sahibi olunmadan veya azami bir bilgiye sahibi olarak, içeriden ya da dışarıdan gerçekleştirilebilir. Bu testler; bilişim sistemi, uygulamalar, bilgisayar ağ donanımı, işletim sistemleri, iletişim araçları, fiziki güvenlik ve çalışan faktörü olmak üzere tüm bilişim altyapısını çerçeveleyecek şekilde planlanmalıdır. Penetrasyon testinin neticesinde, testin gerçekleştirildiği hedef sistemin ve sistemde bulunan eksikliklerin ve çözüm önerilerinin olduğu penetrasyon test raporu hazırlanır. Penetrasyon testleri esnasında, metodolojik bir safhalar zinciri kullanılır ve test safhasının her adımında saptanan zafiyetlere göre, çözüm üretilmesi şarttır. Saptanan her bir zafiyet için geliştirilen çözüm planı da raporu tutularak, testi yaptıran kuruma verilmelidir (Vural, 2007).

Yüksek düzeyde bilgi güvenliğinin ifa edilmesinde önemli bir rolü bulunan penetrasyon testleri kişisel verilerin korunması ile alakalı kanuni mevzuatlar kapsamında önemli bir husus olarak güvenlik konularında yerini almıştır. Gerek Türkiye'de kullanılmakta olan 6698 Sayılı KVKK gerekse Avrupa'da kullanılmakta olan Genel Veri Koruma Tüzüğü (GDPR) doğrultusunda veri sorumluları güvenliğin sağlanması konusunda idari ve teknik önlemleri almakla yükümlüdür. Bu yasal mevzuatların en önemli taraflarından birisi, bilgi güvenliğinin sağlanamaması neticesinde ortaya çıkabilecek olası bir ihlal sonucunda, veri sorumlularının, saldırganların ve kişisel verileri koruyamayan kurum ve işletmelerin önemli cezalar ödemeye mecbur bırakılmalarıdır. Bu doğrultuda penetrasyon testlerinin, kişisel verilerin kaydının tutulduğu ve saklandığı sistemlerin güvenliğinin sağlanmasına dair risk ve tehditlerin yönetilebilmesi maksadıyla bilişim sistemlerinin değerlemesinin yapılması ve güvenlik kontrollerinin etkililiğinin rutin olarak test edilmesi yönünden önemli bir misyonu bulunur (Tekerek ve Vural, 2019).

Penetrasyon testleri ile bilişim sistemindeki en zayıf olan güvenlik noktaları saptandıktan sonra, doğru yerlere yatırım gerçekleştirilerek tehditlerin yaşanması engellenebilir ya da etkileri minimuma çekilebilir. Penetrasyon testlerinin bir başka önemli avantajı ise siber güvenliğin dışarıdaki bir uzman tarafından başka bir bakış açısı ile test edilmesiyle mevcut uzmanların geliştirmesi gerekli olan özelliklerini ve deneyimlerini de meydana çıkarmakta ve bu şekilde verilmesi gereken eğitim ve seminerler sağlıklı bir şekilde seçilebilmektedir (Johansen vd., 2016). Penetrasyon testlerinin kapsamı teknolojiye, sisteme ve uygulamalara göre farklılık gösterebilmektedir. Bütün bilişim sistemlerinin test edilmesine ilave olarak kuruma has kritik konulara (Ağ, Mobil Uygulama, Web Uygulama, Bulut ve Sosyal Mühendislik Testleri) ayrıca yoğunlaşabilir. Penetrasyon testlerinin türüne göre kapsam ya da araç ekipmanları farklı olsa da hepsinin ortak bir metodolojiyi paylaştığı bilinmektedir. Penetrasyon testleri "kara kutu", "beyaz kutu" ve bu iki tekniğin birleşimi olan "gri kutu" şeklinde adlandırılan üç farklı test tekniğinden meydana gelir. Kör test şeklinde de tanınan kara kutu penetrasyon testleri konuyla ilgili temel bilgisi ve ulaşım izni bulunmadan sıradan bir kullanıcı yetkisiyle gerçekleştirilebilir. Beyaz kutu penetrasyon testinde ise, işlemi yapan uzmanlara güvenlik bilgileriyle alakalı test öncesi bazı önemli bilgiler sunulmalıdır. Gri kutu penetrasyon testinde ise işlemi gerçekleştirecek uzmanlar bazı konularla ilgili bilgi sahibi olurken bazı konularda bilgi sahibi olmaları gerekmez.

Bilgi alınacak konular, yapılan planlama dahilinde süre ve mali sınırlılıklara göre işleme başlamadan önce düzenlenmiştir (Johansen vd., 2016).

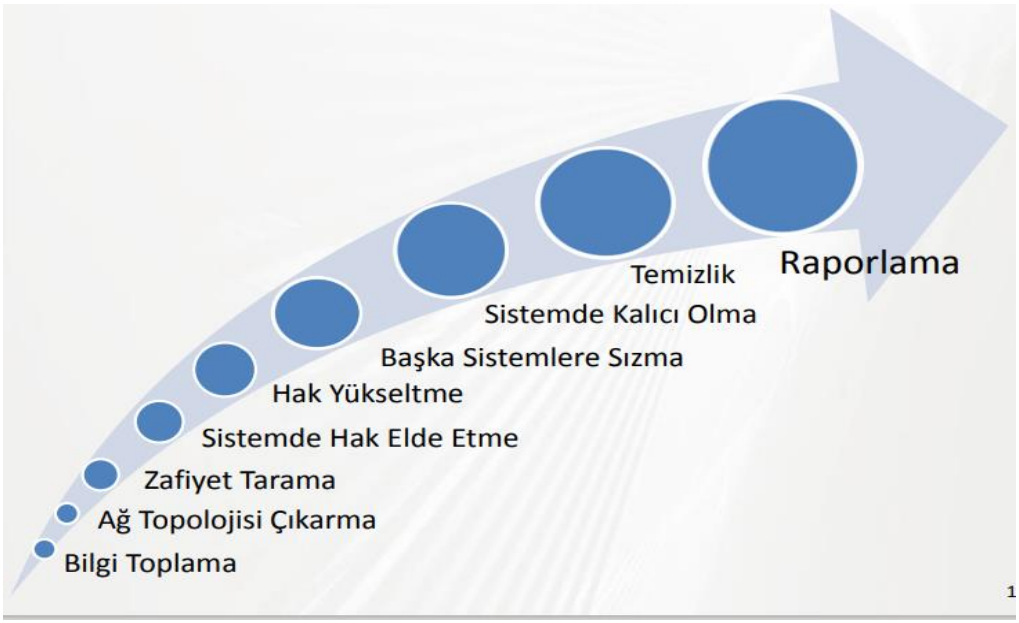
Penetrasyon testlerinin gerçekleştirildiği konumların seçimi de kritik olup, içte veya dışta bulunan bir konumda yapılabilir. Dışarıdan bir noktadan yapılan penetrasyon testlerinde web sitesi ve harici ağ sunucuları gibi dış konumdaki sistemler test edilirken bazı zamanlarda ise testler uzak bir konumdan organize edilebilir. İçteki lokasyondan gerçekleştirilen testler ise bilgi sistemlerinin bulunduğu dahili konumlardan yapılır. Bu tür bir test, özellikle vazifesini kötüye kullanan veya kimlik gaspına maruz kalmış bir personelin güvenlik sistemine ne derece zarar verebileceğinin ortaya çıkartılmasında büyük katkı sağlar. Bilgi güvenliğinin sağlanmasında önemli bir adım olarak görülen penetrasyon testleri düzenli aralıklarla veya şartlar yenilendiğinde tekrar edilmelidir (Tekerek ve Vural, 2019). Penetrasyon testleri ile güvenlik konusundaki eksiklikler, zafiyetler ve ihlaller belirlenerek kurumların güvenlik potansiyelleri ve güçleri saptanır. Bu şekilde güvenlik açısından zayıf ara yüzlere yönelik doğru yatırımların yapılabilmesi sağlanır. Penetrasyon testleri ile hassas sistemler üstünde hatalı yapılanmalar bulunur, IEC/ISO 27001, PCI DSS, COBIT, FISMA vb. gibi bilgi güvenliği sertifikaları ve düzenlemelerine duyulan ihtiyaç test edilmiş olunur (Akbaş, 2013).

Penetrasyon testleri, yazılım programlarıyla otomatik hale dönüştürülebilir ya da manuel şekilde elle de yapılabilir. Her iki kullanım şeklinde de test işleminde farklı aşamalar bulunmaktadır. Bunlardan ilk önce hedef sistem ile alakalı bilgilerin elde edilmesi (keşif yapılması) ve olası giriş yüzlerinin saptanması, test işlemi ve bulguların geri bildirilmesi süreçleri bulunur. Penetrasyon testleri bir kurumun ve firmanın güvenlik politikasının verimliliğini test etmek, personelin güvenlik konusundaki bilincini sınamak, bir kurum veya firmanın siber güvenlik tehditlerine cevap verme becerisini sınamak ve güvenlik düzeyinin analiz edilerek değerlemesi maksadıyla pek çok ticari ya da açık kaynak donanımlar kullanılarak gerçekleştirilir (Whitaker ve Newman, 2005).

Penetrasyon testini bir standarda oturtmak için 2010 tarihinde hayata geçirilen "Penetration Testing Execution Standard (PTES)" standardında penetrasyon testleri yedi (7) temel basamak şeklinde aşamalandırılmıştır (Adır, 2019):

1. Katılım öncesi etkileşim,
2. İstihbarat toplama,
3. Tehdit modelleme,
4. Zafiyet analizi,
5. İstismar (Penetrasyon süreci),
6. İstismar sonrası,
7. Raporlamadır.

Şekil 10'te ise sızma testi süreci daha kapsamlı aşamalarla şematize edilmiştir.



Şekil 10. Sızma testi süreci

Kaynak: Tübitak Bilgem (2015)

5.7. Kurumları Etkileyen Siber Güvenlik Zafiyetleri

Yazılım kodunda veya bilişim sisteminin herhangi bir alanında meydana gelen hatalar virüs, solucan, truva atı gibi kötücül yazılımların veya yetkisiz bir bireyin istismara uğrayabileceği güvenlik açıklıklarının ortaya çıkmasına sebebiyet verebilmektedir. Güvenlik zafiyetleri bilinçli veya bilinçsiz şekilde oluşabilmektedir (Gül, 2018).

1. Bilinçli zafiyetler: Bilinçli zafiyetler, sistemin mevcut güvenlik yapısını ihlal ederek bilişim sistemine ya da şifrelenmiş verilere saldırı yapılması maksadıyla yapılan arka kapılardır.

2. Bilinçsiz zafiyetler: Bilinçsiz zafiyetler kurum veya işletme içerisinde işe koşulan yazılımlardan, işletim sistemlerinden veya kişiler vasıtasıyla meydana gelebilmektedir. Bilinçsiz zafiyetler; sistem zafiyetleri, personel hatası zafiyetleri şeklinde iki grupta tetkik edilebilir.

a. Sistem zafiyetleri: Sistem zafiyetleri faaliyetteki uygulamalardan veya işletim sistemlerinden kaynaklı ortaya çıkan güvenlik zaaflarıdır. 1998'den zamanımıza kadar işlem yapan işletim sistemleri açıklıkları "CVE (Common Vulnerabilities and Exposures)"nin (CVE, 2022) sitesinde güncel şekilde yayımlanmaktadır. Son zamanların en fazla bilinen saldırısı 2017 tarihinde yapılan ve Windows işletim sistemlerini hedefe alan "WannaCry ransomware" kötücül yazılımıdır. Bu saldırı "SMB (Server Message Block)" portundaki ara yüzü kullanarak bilişim sistemindeki bilgileri şifrelemekte ve şifrenin kaldırılması için fidye istemektedir (Gül, 2018).

b. Personel hatası zafiyetleri: Personel hataları kurum veya işletme içerisinde çok önemli açıklıkların ortaya çıkmasına sebebiyet verebilmektedir. Kurum kapsamındaki haberleşme ağının SSH şifreli ağ yerine Telnet açık ağ üzerinde oluşturulması, ulaşım yetkilerinin doğru tanımlanamaması ve yeterli sürelerde güncelleştirilmemesi, hassas bilgilerin güvenlikli bir sunucu yerine kullanıcı cihazları üzerinde tutulması, kullanıcıların çok basit seviyede veya tahmini yapılabilen şifreler koyması gibi hatalar tehditlerin kolayca yapılabilmesine sebep olmaktadır. Bu personel hatalarının minimalize edilebilmesi için iş görenlerin siber güvenlik konularında eğitimden geçirilmeleri elzem bir ihtiyaçtır (Gül, 2018).

5.8. Kurumlarda Tehdit Önleme Güvenlik Sistemleri

Siber tehdit önleme süreci, güvenlik mekanizmalarının en çok odaklandığı ve çalıştığı bir safhadır. Bir konutun bahçesine duvar örmek, çelik kapı taktırmak gibi gündelik yaşamda tercih edilen emniyet tedbirleri gibi, bilişim sistemlerine yapılan tehdit ve saldırılara karşın, sistemin izole edilmesi için farklı tedbirler uygulanabilmektedir. Kişilere ait bilgisayarların güvenliği ile alakalı, anti-virüs yazılımlarının kurulmuş

olması, bu yazılımların ve işletim sistemi hizmet paketlerinin ve yanlış düzeltme ve güncelleştirmelerin rutin şekilde yapılması, bilgisayarda şifreli ekran koruyucu bulunması, bilgisayar başından uzun zaman ayrı kalındığında sistemden otomatik çıkılması, koyulan şifrelerin tahmin edilmesinin güç olacak biçimde belirlenmesi, bu şifrelerde gizlilik ilkesine uyulması ve düzenli olarak değiştirilmesi, disk paylaşımı yapılırken hassas davranılması, online olarak indirilen ya da e-posta ile alınana dosyaların gözden geçirilmesi, hassas evrakların parola ile muhafaza edilmesi veya şifreli şekilde depolanması, gizli veya hassas bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yöntemlerle iletilmemesi, kullanılmadığında internet erişiminin bulunmaması, hassas bilgi ve verilerin rutin olarak yedeklerinin kopyalanması gibi tedbirler, basit gibi görülen ancak güvenlik açısından hayat kurtarabilecek tedbirlerden sayılabilir. Kurumsal alanlarda bilişim sistemi güvenliğinde yapılması gereken önleme adımları daha geniş ve komplekstir. Siber güvenlik konusunda uzmanlaşmış bireylerin çalıştığı bu tür sistemlerde, tehdit önleme ile alakalı atılan adımlardan bazıları (Canbek ve Sağıroğlu, 2006):

- İşletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin rutin olarak düzenli aralıklarla tetkik edilmesi,
- Kullanıcı haklarının asgari düzeyde tutulması, kullanılmayan protokol, servis, bileşen ve proseslerin işlem yapmaması,
- Veri iletişiminde şifreleme yöntemlerinin, Güvenli tarayıcıların, Sanal Özel Ağ (Virtual Private Network) tercih edilmesi,
- Açık Anahtar Altyapısı ve e-imza kullanımı,
- Biyometrik temelli sistemlerin kullanılması şeklinde sayılabilir.

Gerçekte güvenlik süreçlerinin önleme safhasında tespit edilen işleyiş mükemmel olabilseydi, daha ilerdeki safhalara hiç gereksinim olmayacaktı. Gerçekleşen tüm siber saldırılar ilk etapta engellenmiş olurdu. Ancak hiçbir güvenlik aracı kusursuz veya hatasız değildir. Bununla birlikte, neredeyse her gün, işletim sistemleri, internet servisleri, bilişim teknolojileri ve güvenlik işlemlerinde farklı zafiyetler saptanmaktadır. Bu yönden değerlendirildiğinde tespit etme ve karşılık verme süreçlerini daha etkin kullanmak oldukça önemlidir (Canbek ve Sağıroğlu, 2006).

5.9. Siber Güvenlik Zafiyetleri Analizleri

Siber güvenlik zafiyetlerini analiz etmek ve değerlemek için pek çok açık kaynak metodoloji bulunmaktadır. Bilgi sistemi ne derece büyük ya da kompleks olursa olsun, zafiyet analiz etme ve değerleme metodolojileri işe koşularak sistem daha güvenli hale getirilebilir. Birtakım metodolojiler güvenlik analizlerinin teknik tarafına yoğunlaşırken, bazıları ise yalnızca yönetimsel ölçütleri odağa almaktadır. Bu güvenlik analizi metodolojilerini kullanmanın maksadı, bir bilişim sisteminin güvenlik zafiyetlerini doğru ve verimli biçimde değerleyebilmektir. Önemli güvenlik zafiyet analizi metodolojilerinden bazıları aşağıda sunulmuştur (Robinson vd., 2018);

- Açık Kaynak Güvenlik Test Metodolojisi Kılavuzu (Open Source Security Testing Methodology Manual - OSSTMM)
- Bilgi Sistemleri Güvenlik Testi Çerçevesi (Information Systems Security Assessment Framework - ISSAF)
- Açık Web Uygulama Güvenliği Proje Test Kılavuzu (Open Web Application Security Project Testing Guide - OWASPTG)
- Web Uygulama Güvenliği Konsorsiyum Tehdit Sınıflaması (Web Application Security Consortium Threat Classification - WASCTC)
- Sızma Testi Yürütme Standardı (Penetration Testing Execution Standard - PTES)

Siber güvenlik zafiyeti analiz yöntemleri güvenlik uzmanlarına, kurumların güvenlik ihtiyaçlarına uygun en iyi test stratejisini belirleme hususunda fayda sağlarlar. OSSTMM ve ISSAF analiz yöntemleri, neredeyse tüm kurumsal bilgi kaynaklarına yönelik ilkeler ve güvenlik testi politikaları önermektedir. OWASPTG ve WASCTC vasıtasıyla hazırlanan zafiyet analiz testi kılavuzu, bir uygulamanın güvenlik zafiyetlerini saptamak için çözümler üretmektedir. PTES ise her türlü analiz testi girişimi mevzusunda rehberlik sunabilmektedir. Güvenlik konusu kendi içerisinde bir süreçtir, analiz ve testler sayesinde bilişim sistemlerinin güvenlik zafiyetleri ve eksiklikleri ile ilgili mühim çözümler ortaya koyar. Analiz ve testler esnasında bilgi sistemlerinde oluşturulacak bir küçük değişiklik, güvenlik analiz sürecinin tümünü etkileyebilir ve neticeleri de hatalara neden olabilir. Tek bir analiz tekniği kullanmak,

güvenlik zafiyeti değerlemesi noktasında yeteri kadar ayrıntılı bir çözüm önerisi veremeyebilir. En iyi analiz tekniğinin seçimi, hedef kurumun karakterine göre ve analizleri yapacak uzmanların düşüncelerine göre değişiklik gösterebilir (Vural, 2007) (Johansen vd.,2016) (Whitaker ve Newman, 2005). Pek çok siber güvenlik analiz metodolojisi içinden, masraf ve etkili olma açısından en doğrusunu tercih etmek için, seçim sürecine özen göstermek önemlidir. Doğru bir siber güvenlik zafiyet analizinin saptanması, hedef kurum, kaynak durumu, güvenlik uzmanı bilgi ve deneyimi, çalışma hedefleri, bilgi sistemi teknik ayrıntıları gibi birçok parametreye bağlıdır (Tekerek ve Vural, 2019).

5.10. Kurumların Güvenlik Önlemleri İçin Tavsiyeler

Bilgisayar ve internetin her geçen gün kullanımının çoğaldığı ve yaşantımızı zaman geçtikçe daha da çok etkileyen, değiştiren ve yönlendiren sanal dünyanın avantajlarının, yararlarının, katkılarının ve üstünlüklerinin yanında, eğer ciddiye alınmazsa kişisel ve kurumsal işleyişi sekteye uğratacağı, verimliliği azaltacağı, büyük oranlarda zararlara neden olacağı, hatta çok önemli yerel veya global bir kaosa sebebiyet vereceği de bilinmelidir (Canbek ve Sağıroğlu, 2006).

Türkiye Bilimsel ve Teknik Araştırma Kurumu olan TÜBİTAK'ın Yönlendirme Kurulu, gerçekleştirmiş olduğu "Bilim ve Teknoloji Strateji Belgesi" araştırmasında (Türkiye Bilimsel ve Teknik Araştırma Kurumu, 2004), Türkiye'nin 2023'e ışık tutacak bilimsel, teknolojik ve yenilik vizyonunu ortaya koyarken, bilgi toplumuna geçiş için, teknoloji altyapısının daha da güçlendirilmesi hedefi doğrultusunda belirlenen stratejiler arasında bilgi güvenliğinin göz ardı edilmeyip farklı prensiplerinin ifade edilmesi oldukça ümit vericidir (Canbek ve Sağıroğlu, 2006).

Gittikçe dijitalleşen her türlü altyapı, bilişim ağları üstünden sunulan hizmetler ve kullanıcıların bizzat kendisi; dağıtık hizmet aksattırma saldırısı, kimlik hırsızlığı gibi farklı tehdit girişimleri, gizli dinleme, bilişim korsanlığı, sazan avlama, bilgisayar solucanları, virüsler, ileti sağanakları gibi tehditler tarafından ortaya koyulan geniş çeşitlilikte risklere maruzdur. Bu tehditler vasıtasıyla meydana gelen risklere karşı koymak için kullanıcılar, klasik olarak tehditlerden etkilenme ihtimalini azaltan, virüs koruma ve sağanak önleme yazılımları, güvenlik duvarları, saldırı tespit sistemleri ve diğer siber savunma araçlarına başvurmaktadır (Canbek, 2019).

Bilgi teknolojilerinin birlikteliğinde gelen tehlike ve risklerden korunmak için tamamlanması ihtiyaç olan eksikler ve açıklıklar bulunmaktadır. Bu aksaklıkların giderilmesinde atılacak adımlar aşağıdaki gibi maddelendirilebilir (Yılmaz vd.,2015):

- Siber güvenlik konusunda kritik olan yerlerde çalışan personelin bilişim teknolojilerindeki gelişimlere paralel olacak şekilde kurum içerisinde tazeleme eğitim programlarının yapılması,
- Toplumun bilgi güvenliği, siber güvenlik ve önemi hususunda farkındalıklarının yükseltilemesi,
- Yetkilendirme ilkelerine dikkat edilmesi gerekir. Oluşturulan kullanıcı adı ve etkin şifreleme teknikleri aracılığıyla bütün personelin her bilgiye erişimi engellenmelidir.
- Kurumlara açık anahtar altyapısı kurulmalı, belgelerin yetkisi olmayan kişiler tarafından erişimi veya kopya edilmesi önlenmelidir.
- Yazılımları test eden ile kullananlar arasında ayrıma gidilmeli, yazılımlar için yerleştirilecek açık kapıların, hataların, kusurların ve zafiyetlerin belirlenmesi kolaylatırmalıdır.
- Kritik pozisyonda iş görenlerin yedekli çalıştırılmasının sağlanması ve personelin kontrolünün yapılması.
- Milli bilgi sistem yazılım ve donanım ürünlerinin üretilmesi. Üniversite sanayi iş birliği işe koşularak yerli yazılım ve donanım ürünleri üretilmelidir.
- Kurumların kendilerine özgü, sürdürülebilir ve devamlı yenilenen dinamik bir risk analizi yapması. Özellikle kritik alt yapıların risk analizi aşamasında değerlendirilmeleri oldukça önemlidir.
- Yeni teknolojik olanakların getirdiği tehdit ve zafiyetlerden sakınmak. Bunun için güvenlik analizlerinin ve testlerin yapılması gerekir.
- Uzaktan erişim için tercih edilen VPN, DMZ ve firewall yazılım ve donanımları devamlı güncelleştirilmeli, dış ortamlardan gelecek saldırılara karşı uyarı (IDS, IPS) sistemleri ilave edilmelidir.

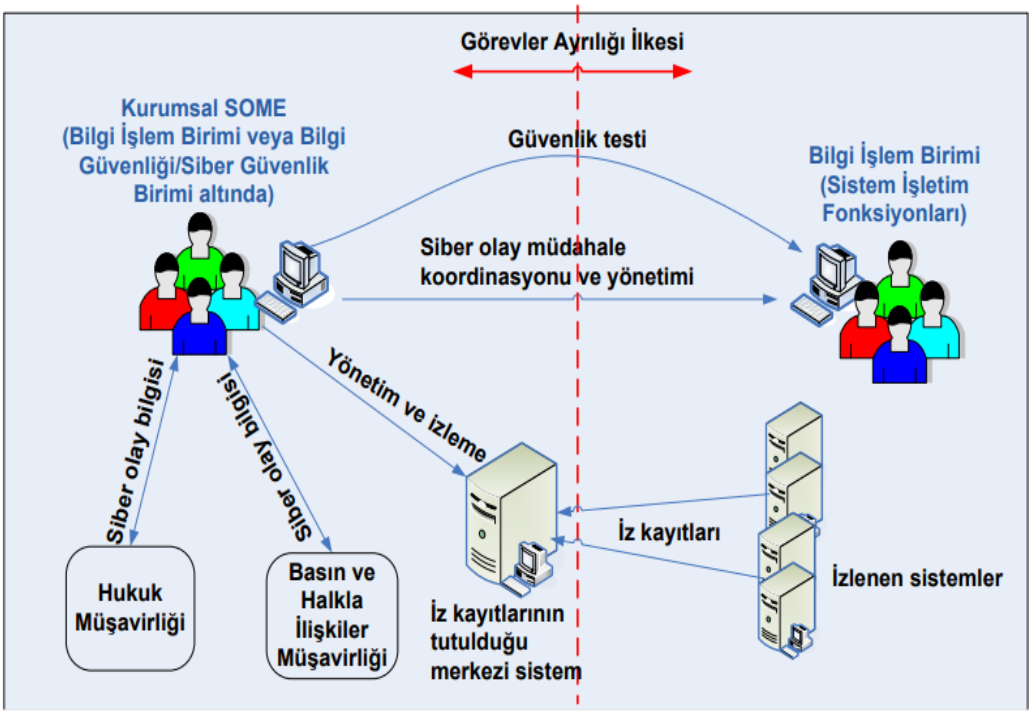
- Uzaktan erişim yapan kullanıcılar için çoklu şifreleme/ güvenlik mekanizmaları meydana getirilmelidir. Özellikle kritik alt yapıların güvenliği için akıllı kart, biyometrik okuyucu, sms ile şifrelendirme, katmanlı şifre yapısı gibi uzaktan erişimi güçleştirici önlemeler alınmalıdır.
- Bilgilerin yedeklenmesi, çıktıların alınması, dosyalanması ve bu bilgilerin olduğu bilişim sistemlerinin harici ağlardan bağımsız olmasının sağlanması,
- Hukuki yapılanma için gerekli adımların atılması. Kanun maddelerinin yeniden düzenlenmesi, caydırıcı cezaların işe koşulması gibi önlemlerin güncellenmesi.
- Ülkenin siber savaş kabiliyetinin yükseltilmesi. Bunun için siber saldırı, siber bağımlılık ve siber savunma bileşenlerini gözden geçirmesi gerekmektedir.

Daha önce ifade edildiği gibi engelleyici siber güvenlik önlemlerinin tek olarak önemli ve hassas verileri koruyamadığı bilinmektedir. Zira güvenlik duvarları ve oturum açma izinleri en başta kullanılması gereken iyi bir ilk savunma hattı olarak görülmelidir. Fakat ihlallerin de kaçınılmaz şekilde meydana gelebileceği akıldan çıkarılmamalıdır. Bu nedenle içeriden kaynaklanan siber güvenlik tehditleri sebebiyle artan bir ihlalin meydana gelme yüzdesi göz önünde bulundurularak, kurumlarda siber güvenlik riskini etkili bir biçimde yönetmenin yolları geliştirilmelidir. Bunlar (Efe ve Bensghır, 2019):

- Yukarıdan en aşağıya kadar siber güvenlik tehditlerini yönetmek için bütünsel ve dinamik bir plan haritası geliştirilmelidir.
- Mevcut uygulamaların durumu analiz edilmeli ve güvenlik açıkları saptanmalıdır.
- Teknik güvenlik hususları önemli çalışma paydaşlarının anlayabileceği koşullara dönüştürülmelidir.
- Müşterilere ve yatırımcılara gerekli ihtimam gösterilmeli ve güven aşılanmalıdır.
- Bütün bilişim teknolojileri ve iş uygulamaları için politikalar merkezi olarak yönetilmelidir.
- Bütün bilişim teknolojileri ve iş uygulamalarında fonksiyonlar arasında risk ve uyumluluk ihtiyaçları birleştirilmeli ve güvenlik prosedürleri standart hale dönüştürülmelidir.

- Siber güvenlik standartları iç denetimler ve faaliyetlerle hizalanmalı ve bir vizyon geliştirilerek problemlerin çözülmesiyle alakalı gelişmeler şeffaf bir şekilde ifade edilmelidir.
- Siber güvenlik sınırları, yetkileri, mevzuatı ve ilgili değişim yönetim süreçleri otomatik ve sürdürülebilir olmalıdır.
- Bütün bilişim teknolojileri ve iş uygulamalarında siber güvenlik prosedürleri standart olmalıdır.
- Siber güvenlik tehditleri, içeriden öğrenen riskler ve veri ihlalleri analiz edilmeli ve istisnalar departmanlara göre kontrol edilmelidir.
- Çalışma etkilerine göre müdahale etme ve iyileştirme işlemleri öncelikli hale dönüştürülmelidir.
- Problemin bir siber tehdit olamayacağı bir anda güvenlik durumu ile ilgili güvence verilmeli, ancak ne zaman olabileceği konusunda senaryolar ve bunlara göre tedbirler belirleyici olmalıdır.

Kurumların bilgi güvenliği ve siber güvenlik tehditlerine yönelik etkili bir güvenlik sistemi oluşturmaları ve bu güvenlik unsurlarını rutin olarak yenileyebilmeleri için kurum içerisinde siber olaylarla müdahale organizasyonu (SOME) kurmaları oldukça önemli bir adımdır. Zira Kasım 2013 tarihli 28818 sayılı Resmî Gazete ’de yayınlanan Siber Olaylarla Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ” doğrultusunda bazı kurumlara kurumsal SOME kurma yükümlülüğü getirilmiştir. Kurumsal SOME’ler bilgi işlem birimi kapsamında ya da bilgi işlem harici bir departmanda oluşturulabilir. Oluşturulan kurumsal SOME’ler siber olay öncesinde, sırasında ve sonrasında siber güvenliği yönetmek maksadıyla bilgi işlem birimleri, hukuk, basın ve halkla ilişkiler departmanları ve diğer paydaşlarla bir etkileşim içeresinde çalışmalıdır. Şekil 11’te kurumsal SOME’nin kurum içerisinde paydaşları ve ilişki ağları gösterilmiştir (Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, 2014).



Şekil 11. Kurumsal SOME'nin kurum bünyesindeki paydaşları ve temel işlevleri

Kaynak: Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü, (2014)

Şekil 11 incelendiğinde kurumsal SOME siber harekât öncesi, bilişim sistemleri üstünde düzenli ve rutin güvenlik testi işlemleri yapar ve yaptırılmasını sağlar. Kayıt yönetimi sistemi ara yüzünden sürekli olacak şekilde iz kayıtlarını izler ve inceler. Siber olay esnasında ise, bilgi işlem biriminin hazırladığı müdahaleleri yönetir ve bu departmandaki ilgili çalışanların koordineli bir şekilde iş görmesine katkıda bulunur.

5.11. Kurumlarda Son Kullanıcı Farkındalığı

Kurumlarda ortak kullanılan ağlarda son kullanıcı farkındalığı büyük önem arz etmektedir. Çünkü bünyesinde birçok teknolojik açıklıkların bulunmasının yanında personel tutum ve davranışlarından dolayı ortaya çıkan zafiyetleri de barındırmaktadır. Tüm dünyada internet kullananların miktarı son 5 senede iki kat artmış ve nerdeyse 2,5 milyara ulaşmıştır. İnternet kullanan insanların büyük bir bölümü ise bir çalışma ortamında iş görürken bir kurumsal ağa bağlanarak internetten faydalanmaktadır. İnternet kullanılarak sesli, görüntülü, yazılı haberleşme ve iletişim, sosyal ağ

platformları, bankacılık ve mali işlemler, devlet hizmetleri, e-eğitim, e-ticaret ve alışveriş gibi faaliyetler çalışanlar tarafından aktif şekilde yapılmaktadır (Şahinaslan, 2013).

Şekil 12. Son kullanıcı güvenliği alt parametreleri

Kaynak: Şahinaslan (2013)

Kurumlarda kurumsal ağlara bağlanan son kullanıcı tarafından muhafaza edilmesi gereken bilgiler aşağıdaki gibi maddelendirilebilir (Şahinaslan, 2013);

a. Kişisel bilgiler ve dokümanlar,
b. Banka ve mali bilgiler,
c. E-posta hesapları ve üyelik bilgileri,
d. Gizli web kamera ve şahsi görüntüler
e. Skype/Teams/Online konuşma verileri,
f. Ortam dinleme ve ses kayıt donanımları,
g. Facebook, Twitter gibi sosyal ağ platformlarında açık ve kontrolsüz paylaşımlardır.

Kurumlarda bilgi güvenliği yönetimi mimarisinde oldukça önemli bir adım olan Şekil 12'de görülen son kullanıcı güvenliğidir. Siber tehlikelere karşı sorumlu personel ve diğer çalışanlar en başta kendi güvenliklerini sağlamalı ve siber tehditlere karşı farkında olmalıdır. Daha sonraki aşamada ise çalıştığı kurumun bağlandığı ağın güvenli olmasına dikkat etmeli ve bu konuda hassas davranışlar sergilemelidir. Ayrıca son kullanıcılara farkındalık eğitimleri verilerek sorumlu olduğu verilerin güvenliğine odaklanmaları

sağlanmalıdır. Kurumlarda son kullanıcı farkındalığını benimsemek için; kişisel yazılım güvenliğine, kişisel donanım güvenliğine, kablosuz erişim güvenliğine, güvenilir şifreli bağlantı, sosyal ağ kullanım güvenliği ve anti-virüs, anti-spam, anti-spyware yazılımları ile koruma duvarı güvenliği konularına odaklanılmalıdır.

5.12. Kurumlarda Siber Güvenlik Sigortası

Siber güvenlik sigortası, kurumları ve bireysel kullanıcıları internet temelli tehlikelerden ve daha genel anlamda, bilişim teknolojisi altyapısı ve işlemleri ile alakalı tehditlerden muhafaza etmek için kullanılan yeni bir sigorta ürünüdür. Daha önceki zamanlarda siber uzaydaki bu tehlikeler, klasik ticaret işlemlerindeki genel yükümlülük poliçelerinde bulunmaz ya da en azından klasik sigorta ürünlerinde belirgin bir biçimde ifade edilmezlerdi (Canbek, 2019).

Siber sigorta poliçelerince bildirilen teminat çerçevesi genel olarak aşağıdaki konuları kapsamaktadır (Canbek, 2019):

- Veri hasarı, gaspı, hırsızlığı, bilgi korsanlığı ve DDos saldırıları gibi kayıplar ve zararlara karşı birinci taraf teminat (first-party coverage)
- Kusurlar ve ihmal nedeniyle bilgi ve verilerin muhafaza edilememesi ya da karalama ve itibar dezenformasyonu (defamation) gibi başka taraflara karşı kayıplar için şirketleri tazmin eden yükümlülük teminatı (liability coverage)
- Rutin güvenlik denetlemeleri, siber saldırı sonrası halkla ilişkiler, soruşturma harcamaları ve oluşan bilişim suçu ile alakalı ödül koyma fonlarıdır.

KVKK ile güncel bir hale dönüşen sayısal mahremiyet sigortacılık kapsamında değerlemesinin yapılması gereken başlıca hususlar arasında bulunmaktadır. Zira, klasik yükümlülük poliçelerinin özellikle kişisel verilerin toplandığı iş ve işlemler için önemli bir yarar sağlamadığı bilinmektedir (Wagner, 2015). Siber sigortalamanın bu doğrultuda önemli katma değer yaratacağı temel güdü açısından göz önünde tutulmalıdır. Genel bir değerlendirmeyle; siber güvenlik sigortasının, bilgi güvenliğini geliştirmeye direkt katkısının olmasının yanısıra; büyük çaplı bir güvenlik sorununda oldukça büyük katkılar sunacağı aşikardır. Genel itibariyle siber güvenlik sigortası, • Büyük kapsamlı zararlardan geri dönmede, • Faaliyetlerin normale çevrilmesinde ve •

Kamu desteğine olan gereksinimin minimalize edilmesinde daha pürüzsüz ve verimli bir fonlama sistemi sağlamaktadır.

Türkiye'de zamanımızda yaşandığı gibi, pek çok toplumda siber güvenlik sigortası pazarı, başka bilinen sigorta türlerine göre oldukça yeni ve henüz küçük çaplı bir işlem hacmine sahiptir. Bu nedenle siber güvenlik sigortasının gelişebilecek siber tehlikeler açısından bütünüyle etkisini ölçmek ve analizlerini yapmak tek başına bir siber olaya odaklanıldığında bile oldukça zordur. Fakat; siber risk ve tehditlerin, bireylere ve kurumlara etkisi, sigorta teminatlarının sağladığı koruma kapsamına nazaran daha da genişlemeyi sürdürdükçe, sigorta firmaları, hizmetlerini artırmaya ve daha çok tanınmaya devam edeceği düşünülebilir. Sigorta şirketleri, siber saldırılar sebebiyle meydana çıkan kayıp ve zararları karşıladıkça ve tehlikeler de gelişip değiştikçe; mevcut bulunan bilişim teknolojisi güvenlik hizmetleri ile sigorta ürünleri de popüler bir biçimde satın alınmaya başlayacaktır (Canbek, 2019).

6. SONUÇ

Kurumlarda bilgi güvenliği yönetim sisteminin oluşturulması amacıyla yapılan bu çalışmada; bilgi güvenliği kapsamında ulusal ve uluslararası alanda düzenlenmiş ve uygulanmaya çalışılan kanun, standart, strateji, ilke ve görüşler incelenmiş ve kurumsal bir bilgi ve siber güvenlik yönetim metodolojisinin çerçevesi hazırlanmıştır. Bu doğrultuda araştırmada sadece bilgi güvenliği süreçlerine değil güvenliğin etkin ve verimli şekilde yönetilmesine de odaklanılmıştır. Bu nedenle kurumsal bilgi güvenliği yönetiminde temel yapıtaşları olan kavramlar açıklanmış, bilgi güvenliği için kurumların uyması gereken ilkeler ve zorunluluklar standart ve yasalarla temellendirilmiştir. Özellikle zamanımız bilgi ve teknoloji toplumunda kurumların büyük siber tehditlere maruz kalması ve kurumsal siber güvenlik zafiyetlerin önlenmesinde yaşanılan aksaklıklar nedeniyle oldukça önemli bir hale gelen bilgi ve siber güvenlik konusunda sürdürülebilir bir yönetim anlayışının geliştirilmesi önemli bir zorunluluk olmuştur. Bu noktada kurumların kişisel ve kurumsal olarak bilgi güvenliği konusunda teknik ve idari tedbirleri alması, kanunların öngördüğü hükümleri uygulaması, bilgi güvenliği standartlarını geliştirmesi ve tüm kurum olarak güvenlik konusunda stratejik bir farkındalık anlayışı benimsemesi gerekmektedir.

Zamanımızda bilişim teknolojilerinin ve uygulamalarının yaygın hale gelmesi ve gündelik yaşamımızda yapılan iş ve işlemlerin dijital platformlarda hızlı ve kolay şekilde yapılmaya başlanması, bilgi güvenliğine duyulan ihtiyacı ve bu güvenliğin sağlanmasını daha çok zorunlu kılmaktadır. Kurumsal güvenliğin etkin bir şekilde sağlanmasında, bilginin değerinin farkına varılması, gerçekleşen iş ve işlemlerde bu araştırmada tetkik edilen güvenlik basamaklarını, parametrelerini, politikalarını ve unsurlarını işe koşmak, büyük oranda karşı karşıya kalınacak sorunları ve tehditleri minimalize edecek, işgücü, vakit ve finansal kayıpları engelleyecek, internetten gelebilecek kötücül yazılım, uygulama ya da program saldırılarına karşı kişisel ve kurumsal bilgi güvenliğinin oluşturulmasında büyük fayda sağlayacaktır.

Başarılı ve etkili bir bilgi ve siber güvenlik yönetimi; üst düzey yöneticilerin desteği ve bilinçli davranışları, çeşitli seminerler ve idari düzenlemelerle bütün personelde farkındalık yaratmak, kurum için öncelikli tehditler ve bu tehditleri minimuma düşürecek uygun çözümlerin saptanması, bu çözümlerin kurumun özellikleri

ve hedeflerine en uygun biçimde icra edilmesi, bu işlemlerin periyodik şekilde denetimden geçirilmesi ve bunların neticesinde ihtiyaç olan iyileştirmelerin ve düzenlemelerin gerçekleştirilerek sürekli gelişme ve değişme neticesinde sağlanabileceği unutulmamalıdır.

Kurumlarda yüksek düzeyli bir siber güvenlik sisteminin sağlanabilmesi için bu süreçlerin yanında, somut şekilde kurumsal bilgi güvenliği standardı olan TSE 17799'de ifade edilen durumların, KVKK kapsamında kurumlarda uyulması gereken zorunlulukların, PCI güvenlik standartları konseyinin ilkelerinin, COBIT ve FISMA politika önlemlerinin ve ISO/IEC 27001 bilgi güvenliği standartlarının bilinmesi, etkin bir SIEM ve log yönetiminin yapılması ve uygulanması gerekmektedir. Ancak bu şekilde yüksek düzeyde bir koruma sağlayan bir bilgi güvenliği yönetim modeli oluşturulabilir. İlgili literatür incelendiğinde, bilgi güvenliği ve siber güvenlik konularıyla alakalı pek çok çalışma bulunsa da "kurumlarda bilgi güvenliği yönetiminin" akademik çevrede yeterli şekilde tartışılmadığı ve konuya gösterilmesi gereken hassasiyetin fazlaca gösterilmediği bilinmektedir. Bu çalışmanın bulgularının akademik gündeme taşınarak farklı çalışmaların bulgularıyla desteklenmesi, çalışmanın katma değerini daha çok artıracağı öngörülmektedir.

Ülkemizde bilgi ve siber güvenlik konularının henüz tam manasıyla anlaşılamayan, yeterince tedbir alınamayan ve kurumsal olarak yeterli olgunluğa ulaşılamayan bir konu olduğu bilinen bir gerçektir. Özellikle bu sahada potansiyel güvenlik uzmanlarının ve güçlerinin olanak ve deneyimleriyle yetişmiş uzman sayısı istenilen düzeyde değildir. Siber ortamda işlenen suç içerikli fiillere müdahalede uluslararası roller de ilave edilince bu sayı oldukça yetersiz kalabilmektedir. Yakın tarihte siber güvenlik tehditlerinde büyük bir yükselişin ortaya çıkmasından dolayı bu alanda olumlu ve ümit verici faaliyetlere daha çok yoğunlaşıldığı görülmektedir. Bu faaliyetlere örnek verilecek olunursa; "Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Olaylara Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar, Çalıştaylar ve Konseyler tarafından ifa edilen faaliyetler ve oluşumlardır (Yılmaz vd., 2015). Ayrıca kurumların güvenlik zafiyetlerinin olup olmadığı, varsa nasıl önlemler alınması gerektiği konusunda önemli bir rehber olan penetrasyon testleri sayesinde IEC/ISO 27001, PCI DSS, COBIT vb. gibi bilgi güvenliği sertifikaları ve politikalarının ihtiyaçları da test

edilebilmektedir. Böylece oldukça kapsamlı bir güvenlik testi ile kurum olarak geniş bir siber güvenlik analiz ve değerlendirmesi gerçekleştirilmiş olunmaktadır.

Kurumlarda bilgi güvenliğinin statik değil dinamik bir süreç olduğu, muhafaza etme ve sağlamlaştırma işlemlerinin öncül adımlar olduğu, mutlak bir hazırlık aşamasına gereksinim duyulduğu, tehditlerin tespit edilmesinden sonra ivedilikle müdahalelerin yapılması gerektiği ve bilişim sistemlerindeki güvenlik zafiyetlerinin düzenli olarak analiz edilerek değerlenmesi ve sürekli iyileştirmelerin yapılması gerektiği bilinmelidir. Bundan dolayı; bilgi güvenliği konusunda özenli bir planlama, kontrol, denetim, özel sektör ve devlete ait kurumlar arasında koordinenin sağlanması, uluslararası alanda iş birliği ve standartlara entegre olma, farkındalık geliştirme, eğitim ve politik çözümler önemli siber sorunlar ile karşılaşmadan ciddiye alınması gereken hususlardan bazılarıdır. Özellikle kritik altyapıların bulunduğu kurumlarda bilginin oldukça değerli ve önemli bir varlık olduğu ve bilgiyi elde tutmanın bir güç olarak sayıldığı günümüz koşullarında, bilginin edinilmesi kadar, muhafaza edilmesinin de hayati önem taşıdığı, bu nedenle yukarıda ifade edilen tedbirlerin alınması gerektiği düşünülmektedir. Bilişim teknolojilerinin kullanımının her geçen gün çoğaldığı ve yaşamımız üzerinde her geçen gün daha da çok etkide bulunan ve yönlendiren sanal alemin var olduğu gerçeği ışığında; bu sanal alemin faydalarının, avantajlarının ve kazanımlarının olduğu gerçeğinin yanısıra, eğer ciddiye alınmazsa kişisel ve kurumsal açıdan pek çok zarara ve hasara neden olabileceği de unutulmamalıdır.

Bu araştırmanın ortaya koyduğu bulguların siber tehditlere karşı kurumları daha dayanıklı hale dönüştürme yolları ve stratejilerinin yanı sıra kurumsal bilgi güvenliğinin icra edilmesi ve sürdürülebilirliğine dair aşağıda ifade edilen katkıları sunmaktadır:

- Kurumsal ve kişisel imaj, itibar ve saygınlığın muhafaza edilmesine,
- Bilgi güvenliği ve siber güvenlik politikalarının etkin bir şekilde uygulanmasına,
- Kurumlarda bilgi kaynakları üstündeki siber tehditlerin öngörülmesine,
- Kurumlarda etkili bir güvenlik için etkin SIEM ve Log yönetiminin yapılması gerekliliğine,
- Kurumlarda ulusal ve uluslararası güvenlik sertifikasyonlarının temin edilmesine,

- Kurumsal bir güvenlik yönetimi için PCI standartları, FISMA ve COBIT standartlarının uygulanmasına,
- Kişisel Verileri Koruma Kanun kapsamında gerekli kurumsal düzenlemelerin yapılmasına,
- Gerçekleştirilen güvenlik sistem yatırımlarının finansal açıdan doğru şekilde ve miktarlarda yapılmasına,
- Kurumlarda bilgi güvenliği farkındalığının artırılması ve bilincinin gelişmesine,
- Kurumların önemli bilgi ve verileri üstündeki kapanan ya da halen süren siber tehditlerin izlenmesine,
- Kurumlarda bilgi işlem ve veri sorumlularının güvenlik odaklı işlemler yapmasına,
- Etkin bir siber güvenlik yönetimi için yılda en az iki 2 kez penetrasyon testi yapılması gerektiğine,
- Siber güvenlik tehditlerini önleme basamaklarına önem verilmesine,
- Siber güvenlik zafiyetlerinin analiz edilerek değerlendirilmesine,
- Son kullanıcı farkındalığı konusunda yetkili personel ve yöneticilerde farkındalık oluşturulmasına,
- Siber güvenlik sigortalarının öneminin farkına varılması ve bu sigortalama süreçlerinden faydalanılmasına yarar sağlayarak ilgililere gerekli düzenlemelerin yapılması adına katkı sağlamakta ve rehberlik etmektedir.

KAYNAKÇA

[USC], U. S. (2002). *Federal Information Security Management Act of*. 11 04, 2022 tarihinde pp.48-62, (online): https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma adresinden alındı

Adır, A. (2019). *Kurumlar için siber güvenlik laboratuvarı altyapısının oluşturulması.* Konya: Yüksek Lisans Tezi, KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü.

Akbaş, E. (2013). *Bilgi Güvenliği ve Log Yönetimi Sistemlerinin Analizi*. 05 20, 2022 tarihinde https://www.slideshare.net/anetertugrul/ertugrul/ adresinden alındı

Akpınar, A. (2020). *Veri merkezli katmanlı güvenlik tasarımı ile etkin olay analizi ve yönetimi.* Kırşehir: Yüksek Lisans Tezi. Kırşehir Ahi Evran Üniversitesi Fen Bilimleri Enstitüsü.

Aktaş, K. (2020). *Bilgi Güvenliği Yönetim Sistemi: Erişim Kontrol Politikası Üzerine Bir İnceleme.* İstanbul: Yüksek Lisans Tezi. Doğuş Üniversitesi Lisansüstü Eğitim Enstitüsü.

Alkan, M., Akkaya, M. U., İnceefe, M. A., & Kesen, M. (2013). *Siber Güvenlik Standardizasyon Kitapçığı.*

Allen, J. (2001). The CERT® Guide to System and Network Security Practices, Addison-Wesley. *Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme (9(3))*, 165-174. (G. Canbek, & Ş. Sağıroğlu, Dü) Politeknik Dergisi, (2006).

Allen, S. (2020). *Importance of Understanding Logs from an Information Security Standpoint.* 05 10, 2022 tarihinde https://www.sans.org/reading-room/whitepapers/logging/paper/200 adresinden alındı

Arda, E. (2020). *Siber Uzay ortamında saldırı tehditlerinin farkındalığı, tespiti ve önlenmesi üzerine bir gerçek-zaman sistem önerisi.* Ankara: Yüksek Lisans Tezi,Başkent Üniversitesi Fen Bilimleri Enstitüsü.

Barış, K. (2018). *Kişisel Verileri Koruma Kanunu nedir, şirketlerin ne yapması gerekiyor.* 05 17, 2022 tarihinde https://medium.com/peoplebox-ats/kisisel-verileri-koruma-kanunu-kvkk-nedirsirketlerin-ne-yapmasi-gerekiyor-cd8c4b93a235/ adresinden alındı

Başaran, A. (2017). *Siber Savaş Cephesinden Notlar.* İstanbul: Arıon Yayınevi.

Başaranoğlu, E. (2016). *Bilgi Güvenliği unsurları.* 05 20, 2022 tarihinde Siber Portal, Information Security: https://www.siberportal.org/white-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/ adresinden alındı

Beyaz. Net. (2020). *COBIT nedir? 25 Mart 2020 Güvenlik makaleleri*. 05 20, 2022 tarihinde https://www.beyaz.net/tr/guvenlik/makaleler/cobit_nedir.html adresinden alındı

Bican, C. (2008). *Sosyal Mühendislik Saldırıları, Ulusal Bilgi Güvenliği Kapısı*. 05 15, 2022 tarihinde http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari3.htm adresinden alındı

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

Canbek, G. (2019). *Siber Güvenlikte Sigortalama. (Ed. Şeref Sağıroğlu ve Mustafa Şenol) İçinde: Siber Güvenlik ve Savunma (1. Baskı), s.328-372.* Ankara: Grafiker Yayınları.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi, 9(3)*, 165-174.

Cavelty, M. D. (2008). *Cyber-Security and Threat Politics: US efforts to secure the information age.* Zurich: Oxon: Taylor and Francis.

Choucri, N. (2012). Cyberpolitics in International Relations. *MIT Press*.

CVE. (2022). 05 27, 2022 tarihinde https://cve.mitre.org/ adresinden alındı

Cyberdefenses INC. (2019). 05 15, 2022 tarihinde What is SIEM and how to choose the right tool: https://cyberdefenses.com/what-is-siem-and-how-to-choose-the-right-tool/ adresinden alındı

Çifci, H. (2017). H. Çifci içinde, *Her Yönüyle Siber Savaş* (s. 168). Ankara: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu.

Efe, A., & Bensghır, T. (2019). *Siber Güvenlik İçin Siber Yönetişim. (Ed. Şeref Sağıroğlu ve Mustafa Şenol) İçinde: Siber Güvenlik ve Savunma (1. Baskı)., s.328-372.* Ankara: Grafiker Yayınları.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir? Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11 (4)*, 1-15.

Emir Erdoğan, S. (2020). Bilgi güvenliği yönetim sisteminin oluşturulması, IEC/ISO 27001 standartının bir sivil havacılık kurumunda hayata geçirilmesi. *Yüksek Lisans Tezi. İstanbul Kültür Üniversitesi Lisansüstü Eğitim Enstitüsü*, 27.

Emir, B. (2020). *Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi.* Trabzon: Yüksek Lisans Tezi. Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü.

Emre, B. (2012). *5. Boyutta Savaş: Siber Savaşlar-1- Ulusal Bilgi Güvenliği Kapısı.* Ankara: Tübitak Bilgem.

Emre, B. (2012). Tükiye' de Siber Güvenlik. Siber Güvenlik Enstitüsü, TÜBITAK BİLGEM SGE. *Bilim ve teknik dergisi,Kasım 2012 Sayısı*, 13-15.

ENISA. (2017). *Cyber security and resilience of smart cars. Good practices and recommendations.* 05 15, 2022 tarihinde Security, European Union Agency for Network and Information: https://doi.org/10.2824/87614 adresinden alındı

Ercan, M. (2015). *Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri.* Gebze: Yüksek Lisans Tezi, Sosyal Bilimleri Enstitüsü,Gebze Teknik Üniversitesi.

FISMA. (2022). *2002 Federal Bilgi Güvenliği Yönetimi Yasası*. 05 21, 2022 tarihinde https://stringfixer.com/tr/FISMA adresinden alındı

FISMA. (2022). *Federal Bilgi Güvenliği Yönetim Yasası (FISMA) - Tectopedia nedir?* 05 21, 2022 tarihinde https://tr.theastrologypage.com/federal-information-security-management-act adresinden alındı

Fumudoh, S., & Viswanathan, U. (2014). *Exploring the Relationship between Online Privacy on Cyber Security, Yüksek Lisans Tezi, Lulea University of Technology.*

05 20, 2022 tarihinde Digitala Vetenskapliga Arkivet,Sweden: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1026488&dswid=8569 adresinden alındı

Gül, A. (2018). *Ağ davranış modeli ile kurum içi saldırıların belirlenmesi.* İstanbul: Yüksek Lisans Tezi. İstanbul Teknik Üniversitesi Bilişim Enstitüsü.

Güngör, M. (2015). *Ulusal bilgi güvenliği: Strateji ve kurumsal yapılanma.* Ankara: Uzmanlık Tezi. T. C. Kalkınma Bakanlığı Bilgi Toplumu Başkanlığı.

ISO. (2012). ISO 27032 Information Technology-Securty techniques- Guidelines for cybersecurity. *25021:11*.

ISO. (2013). *TS ISO/IEC 27001 Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler* (s. 112). içinde

Johansen, G., Allen, L., Heriyanto, T., & Ali, S. (2016). *Kali Linux 2-Assuring Security by Penetration Testing.* Packt Publishing Ltd.

Kabay, M., Whyne, E., & Bosworth, S. (2009). *Bilgi güvenliği için yeni bir çerçeveye doğru*. 05 05, 2022 tarihinde Bilgisayar Güvenliği El Kitabı, Beşinci Baskı: https://www.oreilly.com/library/view/computer-security-handbook/9780471716525/12_chap03.html adresinden alındı

Keleştemur, A. (2015). *Siber İstihbarat.* İstanbul: Level Kitap.

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management.* United States of America: National Institute of Standards and Technology.

Kişisel Verileri Koruma Kurumu. (2017). *Açık Rıza.* 05 2022, 17 tarihinde https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf adresinden alındı

Koç, F. (2008). *BGYS-Varlık Envanteri Oluşturma ve Sınıflandırma Kılavuzu.* TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü).

Kurt Kaya, G. (2017). *Bilgi güvenliği ve siber güvenlik kapsamında bakanlık uygulamaları için güvenli yazılım geliştirme metodolojisi önerisi.* Ankara: Uzmanlık Tezi. T.C. Çevre ve Şehircilik Bakanlığı.

Küzeci, E. (2019). E. Küzeci içinde, *Kişisel Verilerin Korunması* (s. 358). Ankara: Turhan Kitapevi .

KVKK. (2019). *6698 Sayılı Kişisel Verileri Koruma Kanunu*. 05 2022, 10 tarihinde https://www.kvkk.gov.tr/Icerik/5480/2019-14 adresinden alındı

KVKK. (2019). *KVKK Veri Güvenliği Rehberi*. 04 25, 2022 tarihinde https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf adresinden alındı

KVKK. (2020). 05 2022, 05 tarihinde https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2fe0ea-41e0-bf0b-bc9e43dfb57a.pdf adresinden alındı

Marjanovic, M. (2017). Leaking of Confidential Personal Information. *7 No. 21 Int'l J. Econ. & L.*, 133.

Miller, D., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2011). *Security Information and Event Management Implementation.* United States of America: The McGraw-Hill Companies, ISBN: 978-0-07-170108-2.

Muratoğlu, O. (2020). Akıllı Araçlar İçin Bulanık Mantık Temelli Siber Güvenlik Risk Modeli. *Journal of Visual Languages & Computing, 11(3)*, 55.

Özarpa, C., Avcı, İ., & Kara, S. (2021). Otonom araçlar için Siber güvenlik risklerinin Araştırılması ve Savunma Metotları. *Avrupa Bilim ve Teknoloji Dergisi, 31*(ek sayı 1), 242-255.

Özbilgin, İ. G., & Özlü, M. (2019). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve Ağ Yönetimi Politikası.* 15 05, 2022 tarihinde https://www.academia.edu/31607289/ISO_27001_Bilgi_G%C3%BCvenli%C4%9Fi_Y%C3%B6netim_Sistemi_ve_A%C4%9F_Y%C3%B6netimi_Politikas%C4%B1 adresinden alındı

PCI Güvenlik Standartları Konseyi. (2021). 04 25, 2022 tarihinde https://tr.pcisecuritystandards.org/index.php adresinden alındı

Pender-Bey, G. (2012) The Parkerian Hexad: The CIA Expanded:4-20. *Aktaran: Kurt Kaya, G.D. (2017). Bilgi güvenliği ve siber güvenlik kapsamında bakanlık uygulamaları için güvenli yazılım geliştirme metodolojisi önerisi.* Ankara: Uzmanlık Tezi. T.C. Çevre ve Şehircilik Bakanlığı.

Resmi Gazete. (2007). 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.

Richardson, R., & Director, C. S. (2008). CSI computer crime and security survey. *Computer security institute,1*, 1-30.

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). *Developing Cyber Peacekeeping: Observation, Monitoring and Reporting.* arXiv preprint arXiv:1806.02608.

Rouse, M. (2022, 05 02). *Siber Güvenlik*. webopedia: https://www.webopedia.com/definitions/cyber-crime/ adresinden alındı

Sağıroğlu, Ş. (2019). Siber Güvenlik ve Savunma (Ed. Şeref Sağıroğlu). Ş. Sağıroğlu içinde, *Siber güvenlik standartları* (1. Baskı b., s. 51,85). Ankara: Grafiker Yayınları.

Santanam, R. (2010). *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives.* Hershey, PA, USA: Information Science Reference.

Securitynotes. (2017). *Federal Information Security Management Act. Bilgi güvenliği notları*. 05 21, 2022 tarihinde http://securitynotes.org/federal-information-security-management-act/ adresinden alındı

Simpson, M. (2017). *PCI DSS Requirement 12: Leverage Policy To Improve Security*. 04 25, 2022 tarihinde https://www.securitymetrics.com/blog/pci-dss-requirement-12-leverage-policy-improvesecurity/ adresinden alındı

Singh, A., Vaish, A., & Keserwani, P. K. (2014). İnformation Security: Components and tehniques. *International Journal of Advancede Resarch in Computer Science and Software Engineering, 4(1)*, 2277-2288.

Stallings, W. (2011). *Cryptography and Network Security Principles and Practice 5. Baskı.* 139 Network.

Şahinaslan, E. (2010). *Standartlara dayalı bilgi güvenliği risk analiz ve ölçümleme metodolojisinin bankacılık sektörüne özgü modellenmesi ve uygulama*

yazılımının geliştirilmesi. Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Şahinaslan, Ö. (2013). *Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma.* Edirne: Doktora Tezi. Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. *XV. Akademik Bilişim Konferansı Bildirileri*, 719-723.

Taylor, L. (2006). *Matthew Slepherd, FISMA Certification & Accreditation Handbook.* 05 21, 2022 tarihinde http://www.fismacenter.com adresinden alındı

Tekerek, A., & Vural, Y. (2019). Sızma Testleri. (Ed. Şeref Sağıroğlu ve Mustafa Şenol) İçinde: Siber Güvenlik ve Savunma. s.439-453, (1. Baskı),Ankara: Grafiker Yayınları.

TETRA. (2020). *COBIT nedir?* 05 20, 2022 tarihinde https://www.tetrabilisim.com.tr/tr/modul/blog/cobit-nedir adresinden alındı

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

Tutu, İ. (2010). *COBIT nedir?* 05 20, 2022 tarihinde https://www.cozumpark.com/cobit-nedir/ adresinden alındı

Tübitak Bilgem. (2015). *Sızma Testleri ve Güvenlik Denetimleri, Siber Güvenlik Enstitüsü. 2 Şubat 2015 sunumu.* Ankara: Tübitak.

Türk Dil Kurumu [TDK]. (2022, 05 07). Türk Dil Kurumu Sözlüğü: https://sozluk.gov.tr/ adresinden alındı

Türkiye Bilimsel ve Teknik Araştırma Kurumu. (2004). Ulusal Bilim ve Teknoloji Politikaları, 2003-2023 Strateji Belgesi. *Versiyon 19 (2 Kasım 2004)* (s. 1-137). içinde Ankara: TÜBİTAK.

Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2022, 05 02). *Bilgi ve İletişim Güvenliği Rehberliği*. Türkiye Cumhuriyeti Cumhurbaşkanlığı Dijital Dönüşüm Ofisi: https://cbddo.gov.tr/sss/bilgi-iletisim-guvenligi-rehberi/ adresinden alındı

Ulaştırma Denizcilik ve Haberleşme Bakanlığı Haberleşme Genel Müdürlüğü. (2014). *Kurumsal SOME kurulum ve yönetim rehberi. Temmuz. Sürüm 1.* . Ankara.

Ulusal Siber Olaylara Müdahale merkezi [USOM TR-CERT]. (2014). *Siber Güvenliğine İlişkin Temel Bilgiler.* Ankara: Bilgi teknolojileri ve İletişim Kurumu. Temmuz.

UNESCAP. (2008). *UNESCAP*. 05 01, 2022 tarihinde Information Security for Economic and Social Development: https://www.unescap.org/sites/default/d8files/knowledge-products/wp-09-03.pdf adresinden alındı

Ünaldı, A. (2003). Netizen İnternet Vatandaşı. *Alt kitap yayınları,* Cilt No:1, s.10.

Ünver, M., & Canbay, C. (2022). *Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik.* 05 15, 2022 tarihinde Bilgi Teknolojileri Kurumu: http://www.btk.gov.tr/bilgi_teknolojileri/siber_guvenlik/d okumanlar/siber_guvenlik.pdf. adresinden alındı

Ünver, M., Canbay, C., & Özkan, H. (2010). *Kritik Altyapıların Korunması.* Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı,Mayıs 2010.

Vacca, J. (2013). *Managing information security.* Elsevier.

Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri.* Ankara: Yüksek Lisans Tezi, Gazi Üniversitesi. Fen Bilimleri Enstitüsü.

Vural, Y., & Sağıroğlu, Ş. (2010). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler. *Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi 26(1)*, 89- 103.

Wagner, W. (2015). *Cyber Insurance: Why You Need It If Your Organization Collects Consumer Data.* Privacy & Data Security Insight.

Whitaker, A., & Newman, D. P. (2005). *Penetration testing and network defense.* Cisco Press.

Wikipedia. (2022). *Phishing*. 05 22, 2022 tarihinde https://tr.wikipedia.org/wiki/Yemleme adresinden alındı

Williams, D., Davis, R. L., Cothren, C., White, G., & Conklin, A. (2018). *Principles of Computer Security: CompTIA Security+ and Beyond, 5th Edition.* NY, USA: McGraw-Hill.

Yılmaz, E., Ulus, H., & Gönen, S. (2015). Bilgi toplumuna geçiş ve siber güvenlik. *Bilişim Teknolojileri Dergisi, 8(3)*, 133.

Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi. *Dergipark*, 45-59.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Ömer Şaban FİDANCI

EĞİTİM DURUMU

Lisans Öğrenimi : 2014, Anadolu Üniversitesi, İşletme Fakültesi, İşletme

Yüksek Lisans Öğrenimi : 2022,KTO Karatay Üniversitesi, Fen Bilimleri Enstitüsü, Adli Bilişim Mühendisliği

Bildiği Yabancı Diller : İngilizce

İŞ DENEYİMİ

Çalıştığı Kurumlar :

2022, Ağ ve Bilgi Güvenliği Yöneticisi, Sanovel İlaç A.Ş.

2021, Ağ ve Bilgi Güvenliği Kıdemli Uzmanı, Kadir Has Üniversitesi

2019, Ağ ve Bilgi Güvenliği Uzmanı, Turkish Bank A,Ş.

2016, Sistem ve Network Uzmanı, KTO Karatay Üniversitesi

2012, Sistem ve Network Uzmanı, İttifak Holding

Tez Savunma Tarihi : 27/07/2022