**T.C.**
**MARMARA ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**İŞLETME ANABİLİM DALI**
**MUHASEBE DENETİMİ BİLİM DALI**

# İÇ DENETİMİN GELİŞEN VE DEĞİŞEN DÜNYASINDA: SİBER GÜVENLİK VE DENETİM

**Yüksek Lisans Tezi**

**HÜSEYİN SİNAN OCAK**

**İstanbul, 2021**

**T.C.**
**MARMARA ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**İŞLETME ANABİLİM DALI**
**MUHASEBE DENETİMİ BİLİM DALI**

# İÇ DENETİMİN GELİŞEN VE DEĞİŞEN DÜNYASINDA: SİBER GÜVENLİK VE DENETİM

**Yüksek Lisans Tezi**

**HÜSEYİN SİNAN OCAK**

**Danışman: Prof. Dr. NEJAT BOZKURT**

**İstanbul, 2021**

## GENEL BİLGİLER

İsim ve Soyadı: Hüseyin Sinan Ocak

Anabilim Dalı: İşletme

Programı: Muhasebe Denetimi

Tez Danışmanı: Prof. Dr. Nejat Bozkurt

Tez Türü ve Tarihi: Yüksek Lisans – Haziran 2021

Anahtar Kelimeler: İç Denetim, Risk, Siber Güvenlik, Siber Saldırı, Siber Güvenlik Denetimi.

## ÖZET

## İÇ DENETİMİN GELİŞEN VE DEĞİŞEN DÜNYASINDA: SİBER GÜVENLİK VE DENETİM

Günümüzde, teknoloji çok yaygın bir şekilde kullanılmakta ve işletmelere büyük avantajlar sağlamaktadır. Ancak sağladığı avantajlara karşı birçok tehdidi de bünyesinde barındırmaktadır. Tehditlerin başında siber saldırılar yer almaktadır. Siber saldırıların şirketlere maliyetleri çok farklı boyutlara doğru ilerlemektedir. Bu nedenle siber güvenlik kavramının bileşenlerini çok iyi bir şekilde anlamak ve yaşanmış saldırılardan gerekli dersleri çıkartmak gerekmektedir. Bilgilerin sistemlerde kaydedilmeye başlamasından itibaren depolanan verilerin güvenlikleri de önemli olarak görülmektedir. Şirketlerin, güvenlik önlemlerini alarak gelebilecek her türlü siber saldırıya karşı hazırlıklı olmaları gerekmektedir. Eğer daha önceden tedbir alınmadıysa çok büyük kayıplar verilmesi söz konusu olabilmektedir. Siber güvenlik kapsamında alınan veya alınabilecek önlemler için iç denetim departmanlarına önemli görevler düşmektedir. Bu çerçevede iç denetim birimleri riskleri değerlendirmeli ve üst yönetime bilgi vermektedir. Şirketler, güvenlikle ilgili önlemlerini alma aşamasında siber güvenlik denetimleri yaptırarak şirket içerisinde yer alan açıklıkları daha iyi görebilmeye imkanına olmaktadır. Bu doğrultuda da aksiyon planları oluşturulmaktadır.

Çalışmada; siber güvenlik, siber güvenlik ve iç denetim ve siber güvenlik denetimi, konu başlıklarına üzerinde durulmuştur. Çalışmanın son bölümünde ise yaşanmış bir siber saldırı olayının nasıl gerçekleştiği ve sonucunda ne gibi aksiyonlar alındığına yönelik bir uygulama yer almaktadır.

## GENERAL KNOWLEDGE

Name and Surname: Hüseyin Sinan Ocak
Field: Business Administration
Programme: Accounting Auditing
Supervisor: Prof. Dr. Nejat Bozkurt
Degree A warded ande Date: Master - May 2021
Keywords: Internal Audit, Risk, Cyber Security, Cyber Attack, Cyber Security Audit.

## ABSTRACT

## IN THE DEVELOPING AND CHANGING WORLD OF INTERNAL AUDIT: CYBER SECURITY AND AUDIT

Today, technology is widely used and provides great advantages to businesses. However, it contains many threats against the advantages it provides. Cyber attacks are at the top of the threats. The costs of cyber attacks to companies are moving towards very different dimensions. For this reason, it is necessary to understand the components of the concept of cyber security very well and to learn the necessary lessons from experienced attacks. Since the information is started to be recorded in the systems, the security of the stored data is also seen as important. Companies must be prepared against any possible cyber attack by taking security measures. If precautions have not been taken before, huge losses may incur. Important duties fall on the internal audit departments for the measures taken or can be taken within the scope of cyber security. In this context, internal audit units should evaluate the risks and inform the senior management. Companies have the opportunity to better see the openings in the company by having cyber security audits during the process of taking security-related measures. Action plans are prepared in this direction.

In the study; Cyber security, cyber security and internal audit, and cyber security audit, topics were emphasized. In the last part of the study, there is an application about how a cyber attack incident occurred and what actions were taken as a result.

# İÇİNDEKİLER

# TABLO LİSTESİ

# ŞEKİL LİSTESİ

# KISALTMALAR

**COBIT** Control Objective of Information Technology

**BS** Bilgi Sistemleri

**PUKÖ** Planla – Uygula – Kontrol Et – Önlem Al

**BGYS** Bilgi Güvenliği Yönetim Sistemi

**ISO** International Organization for Standardization - Uluslararası Standartlar Teşkilatı

**ISACA** Information Systems Audit and Control Association – Bilgi Sistemleri Denetim ve Kontrol Derneği

**ITIL** Information Technologies Infrastructure Library – Bilgi Teknolojileri Altyapı Kütüphanesi

**DDOS** Distributed Denial of Service – Dağıtılmış Hizmet Reddi

**DOS** Denail of Service – Servis Hizmet Reddi

**IP** Internet Protocol – İnternet Protokolü

**BT** Bilgi Teknolojileri

**IIA** Institute of Internal Auditors – Uluslararası İç Denetçiler Enstitüsü

**UMUÇ** Uluslararası Mesleki Uygulama Çerçevesi

**CIA** Certified Internal Auditor – Sertifikalı İç Denetçi

**BYOD** Bring Your Own Device – Kendi Cihazını Getir

# GİRİŞ

Gelişen ve değişen dünyayla birlikte şirketlerin kullandıkları sistemlerde farklı bir boyuta doğru ilerlemektedir. Teknolojinin kullanımı şirketler için çok büyük avantajlar sağlasa da belirli bir noktadan sonra güvenlik boyutunun da düşünülmesi gerekmektedir. Hiçbir şirket, bilgilerinin başkaları tarafından izinsiz bir şekilde ele geçirilmesini istemez. Şirketlerin bu durumda sistemlerinin güvenliğini sağlama konusunda daha dikkatli hareket etmeleri gerekmektedir. Nitekim COVID-19 salgın hastalığıyla birlikte bazı şirketlerin uzaktan çalışmaya geçtiği bilinmektedir. Bu süreçte uzaktan çalışmaya geçen şirketlerdeki artış ile siber saldırıya uğrayan şirketlerdeki artışın doğru orantılı olarak ilerlediği görülmüştür. Sistemlerin güvenlik boyutu mekân fark etmeksizin sağlanması gereken bir süreçtir.

Çalışmanın birinci bölümünde; siber güvenlik konusu geniş bir çerçeve üzerinde anlatılmıştır. Siber kavramlara, standartlara, saldırıların gerçekleşmesi sırasında kullanılan silahlara, saldırı türlerine ve global dünyada da bilinilirliği olan şirketlere çok büyük zararlar veren siber saldırı hikayelerine yer verilmiştir.

Çalışmanın ikinci bölümünde; iç denetim hakkında temel seviyede bilgi verilmiş ve iç denetimin ilgili olduğu güncel konulara yer verilmiştir. Daha sonrasında bu konulardan biri olan siber güvenliğin iç denetimle ilişkisi açıklanmıştır. İç denetçiler şirketin birçok alanında oluşabilecek risklere karşı üst yönetime güvence vermektedir. Gelişen ve değişen teknolojik dünyayla birlikte şirketlerde büyük boyutlarda zarara yol açabilecek siber saldırılara karşı güvenlik önlemlerinin alınması konusunda iç denetçinin yönetime farkındalık kazandırması gibi birçok görevleri bulunmaktadır.

Çalışmanın üçüncü bölümünde; siber güvenlik denetiminin önemine yer verilmiştir. Şirketler siber güvenlik denetimi yaptırarak sistemlerindeki zafiyetleri tam anlamıyla görebilmektedir. Daha sonrasında bu zafiyetlerin siber saldırganlar tarafından fark edilmeden önce kapatılması gerekmektedir. Şirketlerin birçok alanda verileri bulunmaktadır. Bunların yabancı kimseler tarafından ele geçirilmesi sonucunda hem itibar kaybı hem de maddi kayıplar ortaya çıkmaktadır. Bu sebeple belirli bir ölçeğe ulaşmış olan şirketlerin, üst yöneticilerin meydana gelebilecek saldırılara karşı şirketi

koruyabilmek veya zararı azaltmak adına siber güvenlik denetimi yaptırması gerekmektedir.

Çalışmanın son bölümünde; teknoloji dünyasının gelişmesiyle birlikte çok fazla yaygınlaşan bir siber saldırı örneğine yer verilmiştir. Özellikle, şirket personelleri üzerinden yapılan bir oltalama saldırısının gerçekleşme yöntemi, saldırının fark edilmesiyle birlikte şirket içerisindeki durum ve saldırı sonrasında alınmış ve alınabilecek önlemler hakkında inceleme yapılmıştır.

# 1. SİBER GÜVENLİK

## 1.1. Siber Kavramlar

### 1.1.1. Siber Güvenlik

Siber güvenlik kavramının çeşitli kaynaklarda birçok tanımı bulunmaktadır. Bunlardan bazılarına çalışmada yer verilmiştir.

Siber güvenlik; siber alanda kullanılan verilerin ve varlıkların gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak amacıyla kuruluşlar ve devletler tarafından izlenen güvenlik, risk yönetimi süreçleriyle ilgili eylemlerin tümüdür[1].

Siber güvenlik, işletmedeki faaliyetlerin etkinliği ve etkililiği, iç ve dış raporlamanın güvenilirliği aynı zamanda geçerli yasa ve düzenlemelere uygunluğuyla ilgili hedeflerini destekleyen sistemlerle ilgilidir[2].

Siber güvenlik hem siber bölgeyi hem de organizasyonu ve kullanıcıların varlıklarını herhangi bir tehdit unsuruna karşı savunmak amacıyla kullanılabilecek araçlar, politikalar, güvenlik sistemleri, risk yönetimi yaklaşımları, faaliyetler, eğitim, en iyi uygulamalar, güvence ve teknoloji bütününden oluşmaktadır[3].

Siber güvenlik, hem siber alanda yer alan bilişim sistemlerinin hem de bilginin gizlilik, bütünlük ve erişilebilirlik ölçülerinin korunmasını sağlamaktır. Saldırıların tespit edilmesinin ardından bunlara karşı önlemler alınması ve sonraki aşamada ise sistemlerin, saldırılar meydana gelmeden önceki durumlarına getirilmesi amaçlanmaktadır[4].

Bilgi sistemleri içerisinde işlenen, depolanan ve transfer edilen bilginin gizliliğinin ve mahremiyetinin korunması, veri bütünlüğünün ve bilgiye erişimin, erişim hız ve

---

[1] Daniel Schatz, Rabih Bashroush ve Julie Wall, **"Towards a More Representative Definition of Cyber Security"**, Journal of Digital Forensics Security and Law, Cilt.12, Sayı.2, 2017, s.66

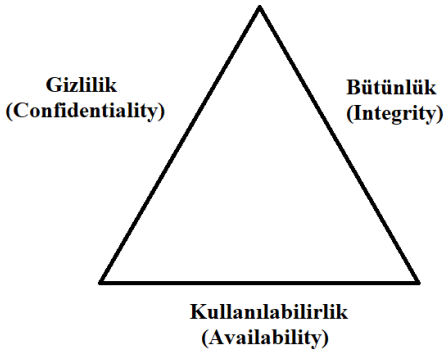
[2] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense"**, The Institute of Internal Auditors (IIA), 2016, s.5

[3] https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, (26.09.2020)

[4] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, **"2016-2019 Ulusal Siber Güvenlik Stratejisi",** s.8

kalitesinin korunması ile sistemin devamlılığının sağlanması hem bilgi güvenliğinin hem de siber güvenliğin temel prensipleri olarak kabul görülmektedir[5].

**Şekil 1:** Bilgi Güvenliği (CIA) Üçlüsü




**Kaynak:** Tony Flick ve Justin Morehouse, **Securing The Smart Grid Next Generation Power Grid Security**, 2011, s.35

Bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik (kullanılabilirlik) gibi özelliklerini koruyabilmek için birtakım standartları bulunmaktadır. Bu kavramları daha detaylı incelersek; gizlilik, bilgiye ve sisteme yetkisi olmayan şahısların erişiminin engellenmesi şeklinde tanımlanabilir. Bütünlük, bilginin yetki izni olmayan şahıslar tarafından değiştirilmesi, silinmesi veya herhangi bir şekilde zarar görmesi durumuna karşı içeriğinin muhafaza edilmesidir. Erişilebilirlik, kişilerin bilgiye ihtiyaçları olduğu zaman kullanıma hazır durumda olması demektir[6]. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir[7].

[5] Barış Çeliktaş ve Soner Çelik, **"Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar"**, Cyberpolitik Journal, Cilt.3, Sayı.5, 2018, s.122

[6] Mustafa Meral, **Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi**, Harp Akademileri Stratejik Araştırmalar Enstitüsü, Savunma Kaynakları Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2015, s.26

[7] http://www.belgelendirme.com.tr/iso-27001-2013-bilgi-guvenligi-belgesi.html, (28.09.2020)

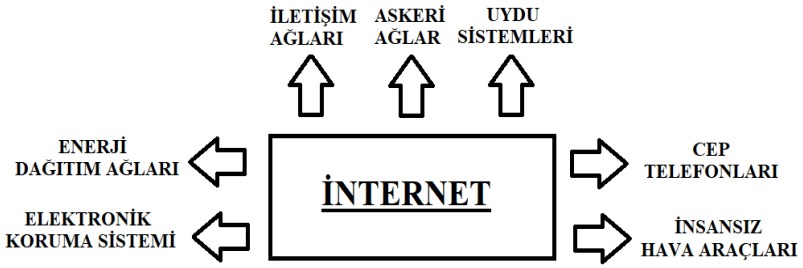
### 1.1.2. Siber Uzay

Literatüre baktığımızda siber uzay veya siber alan olarak her iki terimde kullanılmaktadır. Tanımlar, teknolojik gelişmelerle birlikte zaman içerisinde değişime uğramaktadırlar.

Verilerin depolandığı ve her durumda erişime açık, iletişimin kolaylıkla yürümesini sağlayan bilgisayar ve ağ bileşenlerinden oluşan sanal ortama, siber uzay adı verilmektedir[8]. Teknolojinin gelişimiyle birlikte internet, hayatımızda önemli bir rol almaktadır.

İnternet, siber uzayı meydana getiren bileşenlerin başında yer almaktadır. Siber uzayın diğer bileşenleri ise; iletişim ağları, dış dünyaya kapalı askeri ağlar, cep telefonları, uydu sistemleri, enerji dağıtım ağları, elektronik koruma sistemi, insansız hava araçlarıdır[9].

**Şekil 2:** Siber Uzayın Bileşenleri




**Kaynak:** Barış Çeliktaş, **Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme**, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi, Trabzon, 2016, s.6

### 1.1.3. Siber Savaş

Günümüz dünyasında neredeyse her alanda görülen teknolojik yeniliklerle birlikte siber ortam denilen bir kavram ortaya çıkmıştır. Siber ortam; şahıslar, işletmeler ve

[8] Haydar Çakmak ve Tamer Altunok, **Suç Terör ve Savaş Üçgeninde Siber Dünya**, Ankara: Barış Platin Kitabevi, 2009, s.27

[9] Uğur Akyazı, **"Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler"**, 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 2013, s.216

devletlerin yer aldığı bir bütün olarak düşünüldüğünde, çoğunlukla tehlikeye açık ve karmaşık bir yapıya sahiptir. Kimi zaman devletlerin kimi zaman ise şahısların karşı karşıya gelmesiyle birlikte siber alanda görülen bu mücadele adını siber savaşa vermiştir[10].

Siber savaş, bilgi teknolojilerini koruma amacıyla siber ortamda saldırılar gerçekleştirmek veya karşı taraftan gelebilecek müdahaleleri önleyebilmek için gerçekleştirilen faaliyetlerin tamamıdır[11].

Siber ortamda, bilgi teknolojilerini kullanarak bir kuruma veya bir ülkeye; sistemlerini kullanılamaz hale getirerek maddi ve manevi zararlar vermek amacıyla gerçekleştirilen saldırı çeşidine siber savaş adı verilmektedir[12]. Siber savaş, kargaşa çıkarmadan savaşma ve karşı tarafın kanını dökmeden rakibi yenme sanatı ve bilimidir[13].

### 1.1.4. Siber Suç

Bir suç eyleminin bilgisayar, cep telefonu, tablet vb. gibi elektronik cihazlar kullanılarak gerçekleştirilebilme durumu mevcut ise ya da sistemlerin içinde yapılacak eylem hukuki sınırlar içerisinde değilse bu tip suçlar siber suç olarak ifade edilmektedir[14].

Siber suçları diğer suçlardan ayıran en belirgin fark, suçun bir bilişim sistemi aracılığıyla işlenmiş olmasıdır. Aslına bakacak olursak suçları, bilgisayar ile işlenen suçlar ve bilgisayarsız işlenen suçlar olarak ikiye ayırmamız da mümkündür[15]. Siber suçlara örnek olarak kullanıcının izni olmadan sisteme girilmesi, yetki aşımı, verilerin

[10] Kamil Tarhan, **Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik,** Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Ana Bilim Dalı, Yüksek Lisans Tezi, Konya, 2018, s.38
[11] Steven A. Hildreth, **"Cyberware"**, Congressional Research Service, 2001, s.1
[12] Önder Şahinaslan, **Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma,** Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, Doktora Tezi, Edirne, 2013, s.4
[13] Jeffery Carr, **Inside Cyber Warfare: Mapping the Cyber Underworld,** 1.Baskı, 2010, s.2
[14] Ufuk Taşcı ve Ali Can, **"Türkiye'de Polisin Siber Suçlarla Mücadelede Politikası: 1997-2014"**, Fırat Üniversitesi Sosyal Bilimler Dergisi, Cilt.25, Sayı.2, 2015, s.230-231
[15] Çakmak ve Altunok, **a.g.e.**, s.26

değiştirilmesi, yok edilmesi, sistemin devamlılığını engellemek için yapılan yasa dışı eylemler verilebilir[16].

### 1.1.5. Siber Terörizm

Siber terörizm, siyasi bir motivasyonla geçmişte planlanarak, toplumlara zarar vermek amacıyla bilgisayar sistemlerinin el verdiği ölçüde, internet ağlarına yönelik gerçekleştirilen faaliyetlerin bütünüdür. Terörizm, siber alan içerisindeki internetten yararlanmaya odaklanmış durumdadır. Uzaktan kontrol edilebilmesi, bilgi akışındaki rahatlık, yakalanma olasılığının diğer saldırı yöntemlerine göre daha zor olması siber terörizmin tercih edilmesinin sebeplerinden bazılarıdır[17].

Tablo 1'te görüldüğü gibi dünyada internet kullanım oranı hızlı bir şekilde yükselmektedir. 2022 ve 2030 yıllarına gelindiğinde dünya büyük bir internet ağı ile birbirine bağlı duruma gelecektir. Bu durumla birlikte siber terör saldırılarına maruz kalacak kişilerin ve kurumların da artacağı düşünülmektedir. Dünyada önemli sektörler arasında yer alan finans, sağlık, kamu, ulaşım, üretim, gibi sektörler siber teröristlerin odaklandıkları yerlerdir[18].

**Tablo 1:** Dünyada İnternet Kullanımı

| Yıl | Nüfus | İnternet Kullanıcı Sayısı | İnternet Kullanımının Nüfusa Oranı |
|---|---|---|---|
| **2015** | 7,3 milyar | 1,8 milyar | 25% |
| **2017** | 7,6 milyar | 3,8 milyar | 50% |
| **2022-Tahmini** | 8 milyar | 6 milyar | 75% |
| **2030-Tahmini** | 8,5 milyar | 7,5 milyar | 88% |

**Kaynak:** Şeref Sağıroğlu ve Mustafa Alkan, **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık**, BGD Siber Güvenlik ve Savunma Kitap Serisi 1, 2018, s.266

[16] Hans Corell, **The Challenge of Borderless Cyber-Crime,** Symposium on the Occasion of the Signing of the Unıted Nations Convention Against Transnational Organized Crime, Palermo, 2000, s.3
[17] Çakmak ve Altunok, **a.g.e.**, s.38–39
[18] Şeref Sağıroğlu ve Mustafa Alkan, **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,** BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Grafiker Yayınları, 1.Baskı, Ankara, 2018, s.265

### 1.1.6. Siber Casusluk

Siber casusluk; siyasi, askeri ve ekonomik açıdan rakiplerine karşı daha önde olmak amacıyla bilişim sistemlerini yasaların izin vermediği şekilde kullanarak bir kuruluşa veya kişiye ait bilgilerin, sırların ele geçirilmesidir[19].

Siber casusluk kavramını, hareket alanı siber uzay olan bir tür bilgisayar korsanları olarak adlandırabiliriz. Siber casuslar, sistemlere sızıp içerisinde bulundukları sürece, arkalarında iz bırakmamaya çalışmaktadırlar[20].

### 1.1.7. Siber Caydırıcılık

Caydırıcılık stratejisini uygulayabilmek için iki temel unsur bulunmaktadır. Birincisi, her an karşı taraftan gelebilecek saldırılara karşı koyabilmek için güçlü bir savunma sistemine sahip olmak, ikincisi ise misilleme üzerine odaklanmaktır. Eğer, saldırganlar yaptıkları eylemlerden sonra ağır cezalara çarptırılırlarsa bu bir örnek olabilir ve diğer saldırganlar bu tip eylemlerde bulunmadan önce bir kez daha düşünebilirler[21].

Siber caydırıcılık ile ilgili bazı ünlü yazarların sözleri şu şekildedir; savaş stratejisti Sun Tzu: *''En iyisi savaşmadan baş eğdirmektir.''* Romalı Komutan Belisarius ise *"En mükemmel ve mutlu zafer şudur: Kendiniz bir zarar görmeden, düşmanı amacından vazgeçmek zorunda bırakmaktır.''* demiştir. Bu tanımlardan yola çıkarak siber caydırıcılık savaşa göre daha çok tercih edilebilmektedir[22].

Siber caydırıcılık, bilgi teknolojilerini hedef alan saldırı veya tehdit unsuru oluşturabilecek bir durumun engellenmesi ve önlenmesi olarak tanımlanmaktadır. Tanımdan yola çıkarak tüm bu saldırılar ve tehdit unsurlarından siber uzay kapsamında yapılan eylemler anlaşılmaktadır. Saldırıların nereden geldikleri tespit edilerek

[19] Eugene Nickolov, **Modern Trends in the Cyber Attacks Against the Critical Definitions of the Fundamental,** Regional Cybersecurity Forum, Sofia, 2008
[20] Haley Christopher, **"A Theory of Cyber Deterrence",** Georgetown Journal of International Affairs, 2013
[21] Christopher, **a.g.m.**, 2013
[22] Sağıroğlu ve Alkan, **a.g.e.**, s.207–208

uluslararası yargıda cezalandırılmaları durumun da siber caydırıcılığın önemli bir unsurudur. Siber caydırıcılığın bazı temel özellikleri şöyledir[23]:

- Daha az insan ile daha fazla tehdit oluşturulabilir. Ama önemli olan insan kaynağı değil bilgidir. Bilgi elde edilebilir olduktan sonra gelişime ve güncellemeye ihtiyaç duyar.
- Teknolojik olarak kendisini geliştirmiş ülkeler diğer ülkelere göre siber güvenlik konusunda daha hassastır.
- Saldırgan, farklı kişiler sorumluymuş gibi gösterebilmekte veya kendisini gizleyebilmektedir.
- Saldırılar bölümlerle ayrılmış şekilde gerçekleşebilir veya karşı saldırı olarak dönebilir.

### 1.1.8. Siber Hijyen

Siber saldırılara uğrayan şirketlere baktığımızda genel olarak güvenlik önlemlerinin yeterince sağlıklı olmadığını ya da önlemlerinin hiç olmadığını görmekteyiz. Saldırıyı gerçekleştirecekler, kurumu önceden analiz ederek açıkların nerede daha fazla olduğunu tespit etmektedirler.

Siber güvenlik ile ilgili temel bir ilke olan siber hijyen: siber tehditlerin barındırdığı riskleri minimize edebilmek için birtakım önlemler alınmasıdır. Siber hijyen aynı zamanda kişisel hijyenle de benzerlik göstermekte ve iyi bir şekilde uygulanırsa kurumların saldırılara uğrama riskini azaltmaktır[24]. Siber hijyen uygulamaları, saldırganların başarılı olmalarını zorlaştırmakta ve ortaya çıkabilecek hasarı azaltabilmektedir[25]. Siber hijyenin temel prensibi başkaları tarafından da bilinen zayıf noktalara odaklanarak, onları geliştirme ve değiştirme durumudur. İleriki dönemlerde siber hijyen kurumlar için çok önemli bir kavram haline dönüşecektir.

[23] Gaycken Sandro ve Martellini Maurizio, **Cyber Security: Deterrence and IT Protection for Critical Infrastructures,** 2013, s.3–4
[24] Enisa, **"Review of Cyber Hygiene Practices",** European Union Agency for Network and Information Security, 2016, s.6–14
[25] Murguiah Souppaya vd., **"Crıtical Cybersecurity Hygiene: Patching The Enterprise",** National Institute of Standards and Technology, 2018, s.4

Siber hijyenin sağlıklı bir şekilde oluşmasını sağlayan altı kontrol adımı bulunmaktadır[26]:

- 1. Kontrol: Donanım Varlıklarının Envanter ve Kontrolü

Ağda mevcut olan tüm donanım aygıtları yalnızca yetkili yerlere erişim imkanına sahip olacak şekilde etkin bir yönetim (envanterin izlenmesi ve düzeltilmesi) tarzıyla yetkisiz ve yönetilmeyen aygıtların bulunması ve erişilmesinin önlenmesi aşamasıdır. Bu sayede güvenlik tehdidi oluşturabilecek cihazların görünür olması sağlanmaktadır.

- 2. Kontrol: Yazılım Varlıklarının Envanter ve Kontrolü

Ağdaki tüm yazılımları, yalnızca yetkili yazılımın yüklenip çalıştırılabilmesi aynı zamanda yetkisiz ve yönetilmeyen yazılımların bulunması veya uygulanmaması için etkinleştirilmesi işlemidir.

- 3. Kontrol: Aralıksız Güvenlik Açığı Yönetimi

Doğru araçlarla desteklenen güvenlik açığı yönetim programı, kurumun kendi güvenliğini denetlemesini ve hem iç hem de dış tehditlerin sunduğu riskleri yönetmesini sağlar. Güvenlik açığı yönetimi sayesinde en güvenilir kurumların ağlarında da birtakım hata ve kusurlar ortaya çıkabilir.

- 4. Kontrol: Yönetimle ilgili Ayrıcalıkların Kontrollü Kullanımı

Bilgisayarlarda, ağlarda ve uygulamalarda yönetimsel ayrıcalıkların kullanımını, atanmasını, yapılandırılmasını izlemek, kontrol etmek, önlemek, düzeltmek için kullanılan işlemler ve araçlardır.

- 5. Kontrol: Mobil Cihazlarda, Dizüstü Bilgisayarlarda, İş İstasyonlarında ve Sunucularda Donanım ve Yazılım için Güvenli Yapılandırma

Saldırganların savunmasız hizmetlerden yararlanmalarını önlemek için, sıkı bir yapılandırma yönetimi ve kontrol süreci kullanarak mobil cihazların, dizüstü bilgisayarların, sunucuların ve iş istasyonlarının güvenlik yapılandırmasını oluşturmak, uygulamak ve etkin bir şekilde yönetmektir.

[26] **"Tripwire State of Cyber Hygiene Report"**, Foundatıonal Controls For Security Complıance & IT Operatıons, 2018, s.2–7

- 6. Kontrol: Denetimlerin İzlenmesi ve Analizi, Onarımı

Güvenlik önlemleri ve analizleri, BT ekiplerinin saldırganların yerlerini belirleyebilmelerine, kötü niyetli yazılımları tespit etmelerine ve zararsız makinelerde etkinlikleri izlemelerine yardımcı olabilir.

## 1.2. Siber Güvenlik Standartları

Siber güvenliğin etkili bir şekilde yönetilebilmesi için kurumların sahip oldukları bilgilerin standartlar aracılığıyla herhangi bir tehlikeye karşı korunması gerekmektedir. Bu standartlar teknolojilerin getirdiği yenilikler sayesinde sürekli olarak değişim ve gelişim göstermektedir[27]. Bu çalışmada uluslararası kabul görmüş ISO 27000 serisi ve COBIT standardına yer verilmiştir.

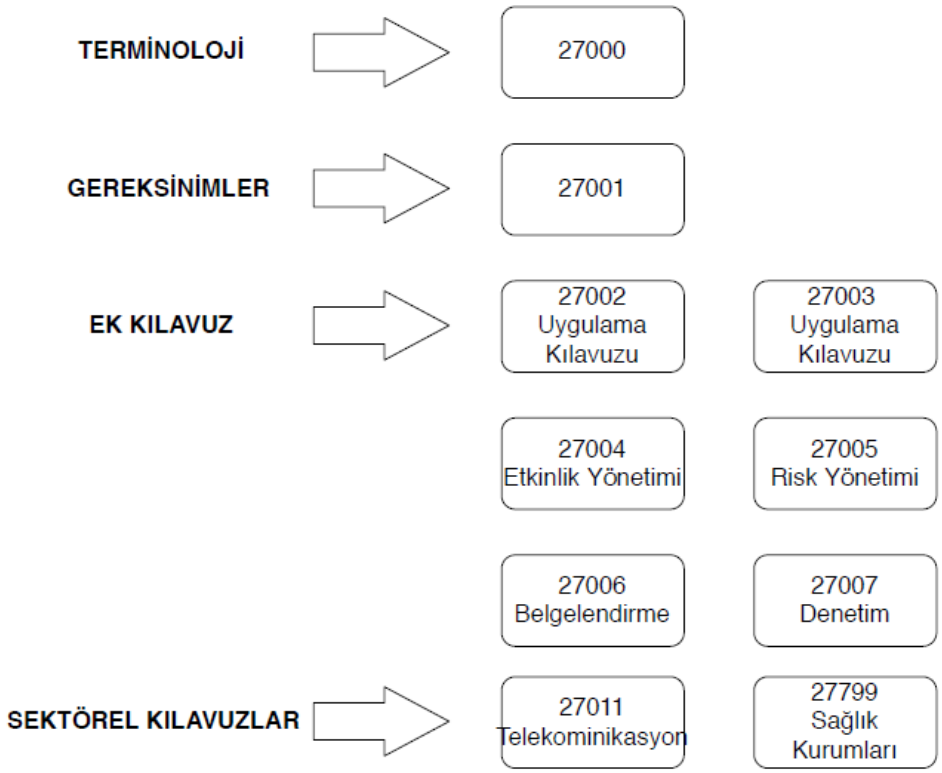
### 1.2.1. Uluslararası Standartlar Teşkilatı ISO 27000 Standartlar Serisi

ISO 27000 standardı, güvenlik riskini en aza indirmek veya güvenliğini tehdit eden durumlar karşısında yol gösterici olmak konumundadır. Bu standart, ISO 27000 ile ilgili kavramları ve bilgi güvenliğiyle ilgili temel bilgileri içerisinde barındırmaktadır[28].

[27] Şeref Sağıroğlu, **Siber Güvenlik ve Savunma Standartlar ve Uygulamalar,** BGD Siber Güvenlik ve Savunma Kitap Serisi 3, Grafiker Yayınları, 1.Baskı, Ankara, 2019, s.51

[28] Mustafa Özlü ve İzzet Gökhan Özbilgin, **"Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi"**, XII. Akademik Bilişim Konferansı Bildirileri, Muğla Üniversitesi, 10-12 Şubat 2010, s.224

**Şekil 3:** ISO / IEC 27000 Standardı Ailesi




**Kaynak:** Faruk Çubukçu, **Bilgi Güvenliği Yönetim Sistemi, ISO 27001:2013 Uygulama Kılavuzu**, 2018, s.24

### *1.2.1.1. ISO 27001*

İlk olarak 2005 yılında ortaya atıldığında BS 7799-2 olarak isimlendirilen bu standart daha sonra güncellenerek ISO 27001 ismini almıştır. ISO 27001 Standardının ortaya çıkma sebeplerinin başında dijital ortamda saklanan bilgilerin, başkaları tarafından ele geçebilecek durumda olmasıdır. Çalınan bilgiler daha sonra şirketler/kurumlar için büyük tehlikeler barındırabilir. Bu sebeple bilgilerin gizliliğinin sağlanması, bütünlüğünün korunması ve yetkisiz kişiler tarafından erişimin engellenebilmesi için bu standart ortaya çıkmıştır. ISO 27001 standardı kurumların bilgi güvenliğini sağlayabilmesi için uluslararası bir standarttır. Bu standardı kullanamaya en çok ihtiyacı

olan kurumların başında finans, kamu ve sağlık sektörleri gelmektedir. Çünkü bu tür kurumlarda başkalarına ait bilgiler saklanmaktadır[29].

ISO 27001 Standardının işletmelere/kurumlara sağladığı bazı faydalar şöyledir[30];

- Bilgileri koruyarak riskini en aza indirir.
- Kurumun daha verimli bir şekilde çalışmasına katkı sağlar.
- Bilgilerin doğru ve güvenilir bir biçimde korunmasına olanak sağlar.
- Şirketin/İşletmenin sahip olduğu tüm bilgilerinin gizli kalmasını sağlar.
- Şirkette bilgilerin korunmasına dair farkındalık ortaya koyar. Şirketin bilgi güvenliği konusundaki eksikliklerini ortaya çıkarmakla birlikte bu alanlarda daha yüksek güvenlik önlemi alınmasına olanak sağlar.
- Bilgilerin içeriğinin yetkisiz kişiler tarafından değişmesini engeller.
- Yasal olarak uyulması gereken ilkelerin yönetmeliğe uygun olmasını yardımcı olur.
- Şirketin kurumsal saygınlığını korur.
- Rakipleriyle rekabette daha avantajlı bir yerde olmasına yardımcı olur.

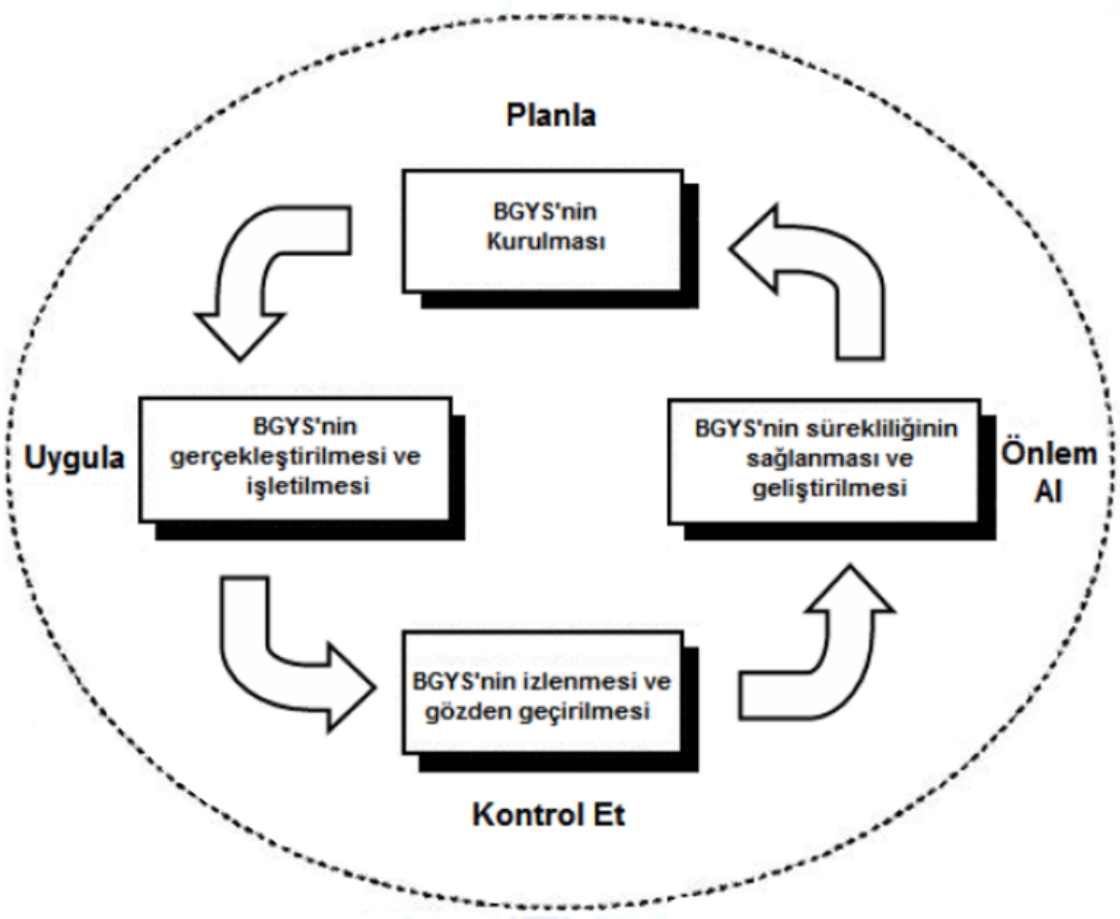
**Şekil 4***:* ISO 27001 Faydaları (%)


**Kaynak:** https://www.bsigroup.com/tr-TR/ISO-27001-Bilgi-Guvenligi-Yonetimi/ISOIEC-27001-Revizyonu/, (15.10.2019)

[29] Faruk Çubukçu, **Bilgi Güvenliği Yönetim Sistemi ISO 27001: 2013 Uygulama Kılavuzu,** Pusula 20 Yayıncılık, 1.Baskı,İstanbul, 2018, s.17–27
[30] Özbilgin ve Özlü, **a.g.m.**, s.1–8

İşletmeler ve kurumlar, PUKÖ kavramıyla birlikte daha etkili bir bilgi güvenliği sistemi uygulamayı ve yönetmeyi amaçlamaktadırlar. PUKÖ sayesinde BT risklerini en kısa zamanda kaldırmayı hedeflemekte ve daha iyi bir sistem için Planla, Uygula, Kontrol Et, Önlem Al (PUKÖ) modelini esas almaktadır[31].

**Şekil 5:** BGYS'nin PUKÖ Modeli




**Kaynak:** http://www.bilgiguvenligitr.com/bilge-adam-guvenlik-egitimleri/egitim-2-isoiec-27001-bilgi-guvenligi-yonetim-sistemi-uygulama-egitimi/, (17.10.2019)

BGYS aşamaları, Plan-Do-Check-Act[32]:

- Planlama (Plan): BGYS'nin amaç ve hedeflerinin belirlenmesi, politika ve prosedürlerin hazırlanması, üst yönetimin desteğinin alınması, kurumun mevcut

[31] Mustafa Yılmaz, **İşletmelerde Bilgi Güvenliği Uygulama Sorunları ve Çözüm Önerileri; Konya Örneği,** Karatay Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Yüksek Lisans Tezi, Konya, 2018, s.36-37
[32] Çubukçu, **a.g.e.,** s.93–101

olan eksikliklerinin belirlenmesi, işletmenin ihtiyacı olan yazılımların belirlenmesi, bilgi varlıkları temelinde risk analizi ve çalışmaları süreçlerini içermektedir.

- Uygula (Do): Bu süreçte planlama aşamasında belirlenen politikalar ve hedefler uygulanır. Bu aşamada seçilen kontrollerin uygulanması, performans analizi, bilgi güvenliği ihlaliyle karşılaşıldığında etkili müdahalede bulunulması, BGYS ekibi belirlenen riskleri gözden geçirme ve riskleri azaltmak için çalışmalar yapmaktadır.
- Kontrol Et (Check): Bu süreç BGYS'de hedeflenen performansın değerlendirilmesi ve raporlanmasını içerir. Sistemin iyileştirilmesi, kontrol etme sürecinin doğru bir şekilde yapılıp yapılmadığına bağlıdır. Belirli sürelerle iç denetimler yapılarak ortaya çıkan sonuçlar hakkında üst yönetimle görüşülmektedir.
- Önlem Al (Act): Tespit edilen durumlara göre düzeltici ve önleyici faaliyetlerde bulunulur.

PUKÖ modeli kısaca, ne yapılması gerektiğini, kararların uygulanmasını, sistemin çalışırlılığının kontrol edilmesini ve istenildiği gibi çalışmayan kontroller için önlemler alınmasını ortaya koymaktadır[33].

#### *1.2.1.2. ISO 27002*

Eski adı ISO 17799 olarak yer alan bu standart, 2007 yılında ISO 27000 serisi bilgi güvenliği standartlarına ait olduğu açıkça belli olması için içeriğinin aynı kalmasıyla birlikte ismi ISO 27002 olarak değiştirilmiştir. ISO 27001 Standardının uygulamasında yerine getirilecek hususlar ISO 27002 de yer almaktadır.

ISO 27002 standardına göre; bu standart, işletmelerdeki bilgi güvenliği ve risk yönetimini ön planda tutarak kontrollerin doğru seçilebilmesi, yönetilebilirliğini ve uygulanabilirliğini bir bütün olarak içerisinde bulunduran bilgi güvenliği uygulamaları için rehber niteliği kapsadığını ifade etmektedir[34].

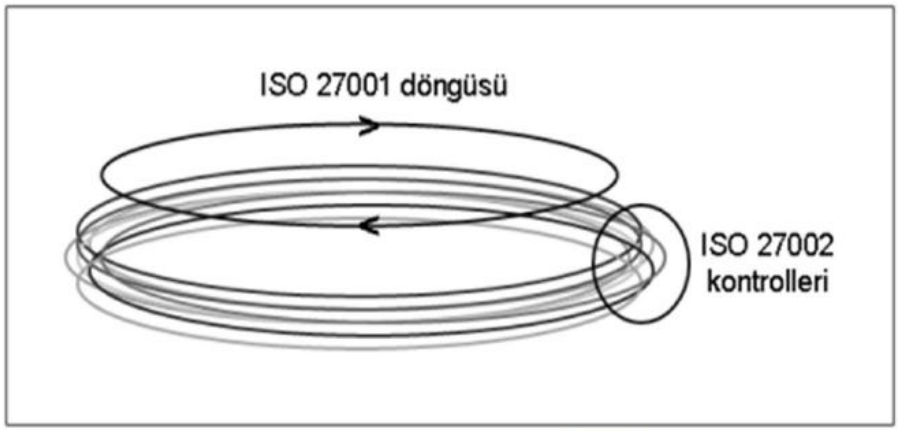
---

[33] M. Mahir Ülgü vd.(Editörler), **Bilgi Güvenliği Politikaları Kılavuzu Sürüm 2.1**, T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, Kuban Matbaacılık Yayıncılık, Ankara, 2019, s.19

[34] https://intweb.tse.org.tr/Standard/Standard/Standard.aspx?, (22.10.2019)

ISO 27001 ve ISO 27002 standartları arasındaki farklara bakmak gerekirse; ISO 27001 standardı, güvenilir bir sistem yönetimi ve bilgi güvenliği altyapısı oluşturmak için kullanılırken, ISO 27002 standardı ise bilgi güvenliği kontrollerini uygulamak için kullanılmaktadır. ISO 27001 standardı Bilgi Güvenliğindeki büyük resmi göstermekteyken bu standartta anlatılanları uygulayabilmek için ise ISO 27002 vb. standartlar incelenir[35].

**Şekil 6:** ISO 27001 Ailesi




**Kaynak:** Ahmet Bozgeyik, **Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi,** Hasan Kalyoncu Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Doktora Tezi, 2018

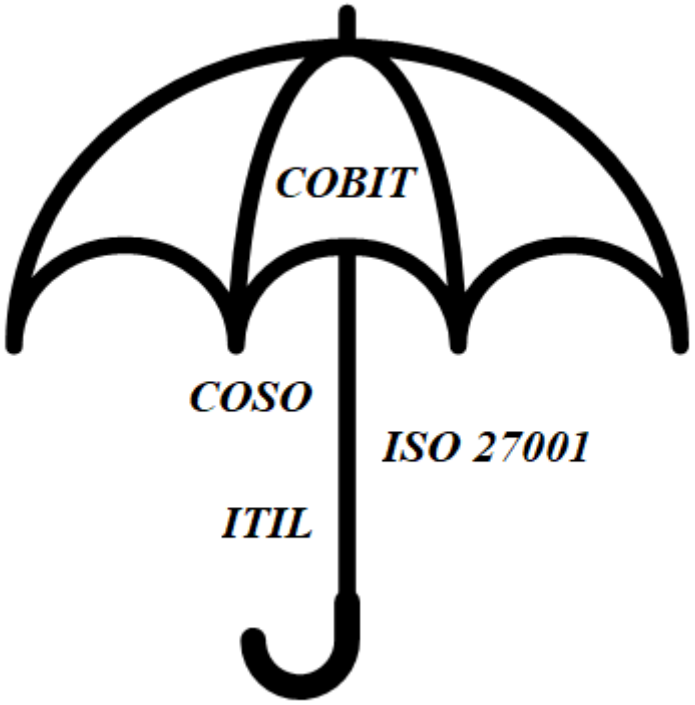
### 1.2.2. COBIT

COBIT, ISACA tarafından 1996 yılında Türkçe karşılığı Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri olan "Control Objectives for Information and Related Technology" kelimelerinden üretilmiş, BT Yönetimi için en iyi uygulamalar bütünüdür. COBIT, bilişimsel ve ilgili teknolojilerle ilişkisi olan bilgileri kontrol ederek yönetmeyi amaçlamaktadır[36]. COBIT'in ilk bölümünün yayınlanmasından sonra sürekli olarak güncellemelere tabi tutulmuştur. COBIT 1 ile başlayan uygulamanın son versiyonu COBIT 5 olarak kurumsal BT yönetişimi kavramını ön plana çıkarmıştır. COBIT'i ISO vb. diğer standartlardan ayıran temel özellik tüm BT fonksiyonlarını içerisine alan bir

[35] https://www.mshowto.org/iso-27000-ailesi-standartlari-nedir.html, (22.10.2019)
[36] Orhan Yılmaz, **ITIL ve COBIT Yönetim Standartları ve Bir Uygulama,** Beykent Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2014, s.31

çerçeve sunmasıdır[37]. COBIT, gelişen ve değişen teknolojinin getirdiği risklerin nasıl yönetileceğine ve sistemleri nasıl daha güvenilir duruma getirebiliriz sorusuna yanıt aramaktadır[38]. COBIT 5'ten bankacılık, sigorta, kamu, üretim, sağlık, enerji, telekomünikasyon, otomotiv sektörlerinden belirli bir ölçeğe ulaşmış olan işletmeler faydalanabilmektedir[39].

**Şekil 7:** COBIT Şemsiyesi




**Kaynak:** Fatih Akyol, **COBIT (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri) Uygulayan Şirketlerdeki Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçlere Etkileri,** Yüksek Lisans Tezi, 2013

COBIT'in bir kuruma sağladığı faydalardan bazıları şu şekilde ifade edilmiştir[40]:

a) Bilgi ve donanım varlıklarını kurum hedeflerine göre kullanır.

b) Stratejik hedeflere ulaşmak için etkin ve yenilikçi fayda sağlar.

[37] Fatih Güneş vd., **Bilgi Teknolojileri Denetimi ve COBIT'in Sektörel Uygulanabilirliği,** Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği, s.3–4
[38] Eliza Natasa Artinyan, **"Cobit Çerçevesi"**, Deloitte, s.1–2
[39] **COBIT 5: Ne kadar hazırsınız?,** Kurumsal Bilgi Teknolojileri Yönetişim Çerçevesi, Pwc, s.2–4
[40] Şahinaslan, **a.g.t.**, s.38

c) Siber risklere karşı güvenli ve verimli bir teknolojik ortam sunar.

d) Kabul edilebilir düzeyde tehdit riskini yönetir.

e) İşletme yönetimini, maliyetlerini ve hizmetleri iyi duruma getirir.

f) Süreçlerin ilgili bölümlerinde ilgili standart (ISO 9001/27001, ITIL, CMMI ve PMI vb.) yaklaşımları tavsiye eden çerçeve yapı sağlayan denetim aracı olarak katkı sağlar.

## 1.3. Siber Silahlar

Siber Silah, insanlara ve cihazlara fiziksel zarar verme ya da sabote etme amacıyla birtakım kimseler/kurumlar tarafından siber savaş sırasında siber saldırılarda kullanılan yazılımlar ve cihazlar olarak tanımlanmaktadır[41]. NATO Güvenlik Danışmanı Rex Hughes siber silahlarla ilgili şu cümleyi kullanmıştır: *"Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır"*[42].

### 1.3.1. Virüs

Kullanıcılar tarafından fark edilemeyerek sistemler üzerinde değişiklik yapıp onları bozabilen ve istem dışı görüntüleri ekrana yansıtabilen bir zararlı yazılım türüdür. Virüsler, gizlendikleri süre boyunca hedeflerine ulaşabilmekte ve sistem içerisindeki varlıklarını sürdürebilmektedirler. Sistemlere daha büyük zararlar verebilmek ve kullanılabilirliğini engellemek için sürekli yayılım eğilimindedirler[43]. Farklı boyutlarda tehditler içeren virüsler, son zamanlarda en çok kullanılan siber saldırıları araçlarından biri olarak yer almaktadır[44].

E-posta adresine gelen bir e-mailin okunmasıyla veya dosyanın açılması ile kullanıcı kişi virüsü yayabilir. Virüsler, istemeyerek de olsa kişilerin müdahalesi ile harekete geçmesi özelliği sayesinde diğer zararlı yazılımlardan ayrılmaktadır. Bu durumda

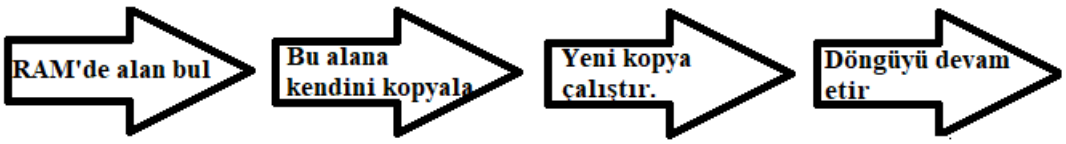
[41] Stefano Mele, **"Cyber-weapons: Legal and Strategic Aspects Version 2.0",** Italian Institute of Strategic Studies, 2013, s.10
[42] Mehmet Tutuş ve Özgür Ulusan, **"E-Devlet ve Siber Güvenlik Gelişmiş Siber Silahlar",** Türk Hava Kurumu Enstitüsü, 2013, s.5
[43] Sağıroğlu ve Alkan, **a.g.e.**, s.228
[44] Meral, **a.g.t.**, s.16

kullanıcıların uğrayabileceği zararları kısmen ya da tamamen ortadan kaldırabilmek için virüs koruma programları ortaya çıkmıştır[45].

### 1.3.2. Solucan

Bilgisayar kurtları olarak da bilinen solucanlar, e-mail, crack programlar, korsan oyun, Dvd ve Cd'ler yoluyla sisteminize sızabilmektedir. Sisteminizde sürekli olarak yerini değiştirebilen ve bununla birlikte çoğalabilen programlardır. Virüslerden farklı olarak sisteminizde girdiği andan itibaren kopyalama işlemini otomatik olarak gerçekleştirmektedir. Bununla birlikte bilgisayarınız içerisinde yer alan bir solucan kullanıcıdan bağımsız olarak herhangi bir komut olmaksızın çoğalmaya başlamaktadır. Bilgisayarınıza sızan solucanın ortaya çıkartabileceği en kötü durum bilgisayarın RAM'indeki kullanım alanın arttırarak kısa bir zamanda çalışmaz hale gelmesine ya da çökmesine sebep olmasıdır. Solucanların izlediklerin yol aşağıdaki şekilde görülmektedir[46].

**Şekil 8:** Solucanların İlerleme Aşamaları

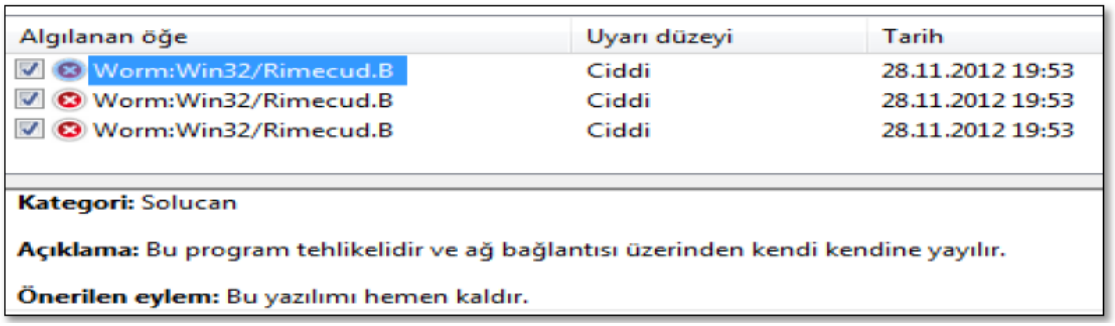



**Kaynakça:** https://www.tech-worm.com/worm-solucan-nedir/, (28.10.2019)

Solucanlar; ağ solucanı, e-posta solucanı, özel kod yapılı solucanlar ve mobil kod zararlılar olmak üzere ayrı şekilde görülmektedir. Bunların arasından ağ bağlantısı ile bulaşan ve sistem içerisinde kendi kendine çoğalma tehlikesi bulunan Worm.Win32/Rimecud.B bir solucan türünün sistem üzerinden kaldırılması için uyarı penceresi aşağıda görülmektedir[47].

[45] Gürol Canbek ve Şeref Sağıroğlu, **"Kötücül ve Casus Yazılımlar: Kapsamlı bir Araştırma",** Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt.22, Sayı.1, 2007, s.123
[46] https://www.tech-worm.com/worm-solucan-nedir/, (28.10.2019)
[47] Şahinaslan, **a.g.t.**, s.18–19

**Şekil 9:** Solucan Yazılımı Uyarısı




**Kaynak:** Önder Şahinaslan, **Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma,** Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi, 2013

### 1.3.3. Casus Yazılım

Casus yazılımların diğerlerinden farklı olan unsurları, sistemin içerisine sızdıktan sonra kopyalarını oluşturarak çoğalmaya gerek duymamalarıdır. Bu tür yazılımların amaçları, kişisel bilgileri kullanıcılar tarafından fark edilmeyerek ele geçirmektir. Daha sonrasında ise ele geçirilen bu bilgiler ticari amaçlar için kullanılmaktadır[48]. Kullanıcılar, internette gezerken istemeyerek bu tür yazılımların sistemlerine girmesine izin verebilmektedirler. Bu sebeple ilgi çekici reklamlara, indirim fırsatları adı altında gelebilecek çeşitli mesajlara inanmamalı ve dikkatli davranmaları gerekmektedir. Aksi taktirde istemeyerek de olsa sistem içerisindeki kurulumu veya onayı kullanıcılar kendileri gerçekleştirmektedirler[49].

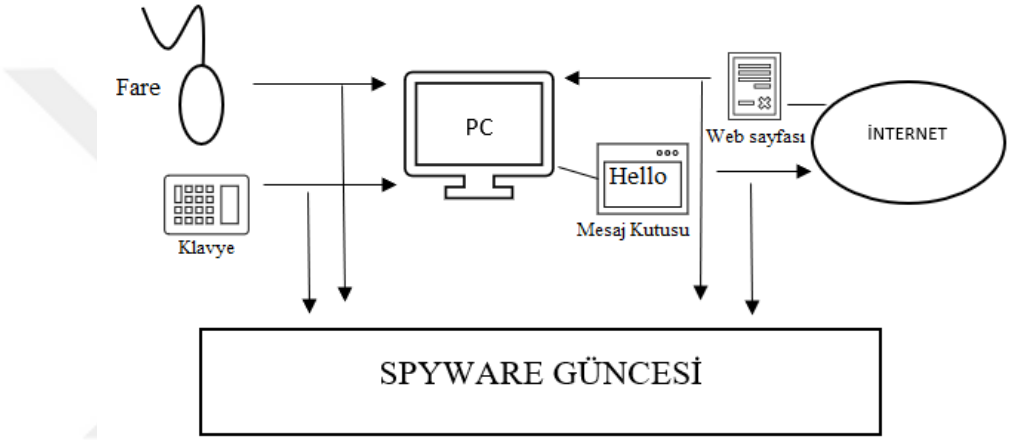
Spyware (casus yazılım), sistem içerisinde çalışmaya devam ederken bilgisayarınızda ve internette gerçekleştirdiğiniz işlemleri takip etmektedir. Örnek vermek gerekirse sisteminize bulaşan casus yazılımlar aşağıdaki işlemlerden bir kısmını yapıyor anlamına gelebilir[50]:

- Giriş yaptığınız Web sayfalarının adresini kaydetmek,
- E-posta üzerinden iletişime geçilen kişilerin bilgilerini kaydetmek,

[48] Resul Daş, Şahin Kara ve M. Zekeriya Gündüz, **"Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri",** s.1
[49] Hüseyin Akarslan, **Bilişim Suçları,** Seçkin Yayıncılık, Ankara, 2012, s.93
[50] Michael Miller, **PC Güvenliği ve Bilgisayar Virüsleri,** Alfa Basım Yayım, 2003, s.314

- Size ulaşan ya da sizin gönderdiğiniz maillerin içeriklerini kaydedilmesi,
- Bilgisayarınızı kullanırken klavyeye her bastığınız anda harflerin kaydedilmesi,
- Bilgisayarı kullanırken farenin sistem içerisindeki tüm hareketlerinin takip edilmesi,
- Tüm sohbet kanallarının içeriğini takip ederek kişisel verilere (isim, adres, fotoğraf) ulaşmak.

**Şekil 10:** Spyware sisteminizi nasıl izler ve bildirir?




**Kaynak:** Michael Miller, **PC Güvenliği ve Bilgisayar Virüsleri,** 2003

### 1.3.4. Truva Atı

Truva atından ismini alan trojanlar, sistemlere girerek çok iyi bir şekilde kendilerini gizleyebilmektedirler. Facebook, whatsapp, e-posta gibi uygulamalar yoluyla karşı tarafa ilgi çekici mesajlar iletilebilir ayrıca reklamlar verilebilirken bu tür aldatıcı bağlantılara tıklanmamalıdır. Tarafımıza ilgimizi çeken bir e-mail ulaştığında kimden geldiğini bilmediğimiz iletileri açtığımız taktirde trojanlar sisteme sızmaya başlayabilirler. Trojanlar çok daha tehlikeli hale de gelebilmektedir, bunlara örnek vermek gerekirse; bilgisayarınızdaki kameraya ulaşarak sizi izleyebilir ve mikrofonunuz aracılığıyla sizi dinleyebilir[51]. Truva atı bulaşmış bir bilgisayarın tehlike boyutunu anlatabilmek şu çerçevede daha iyi anlayabiliriz. Yukarıda da bahsettiğimiz gibi kişiler

[51] Olcay Büyükçapar, **Bilişim Teknolojileri ve Yazılım**, Kodlab Yayıncılık, İstanbul, 2018, s.57

genellikle tanıdığı kişilerden gelen e-mailleri açmakta ve linklere tıklamalıdır. Ancak e-mail gönderen kişi aslında karşı tarafın bilgisayarına sızmış bir truva atı olabilir. Çünkü bilgisayara sızmış olan truva atı kullanıcının e-mail bilgilerini ele geçirerek hatta içerisine sızarak e-mail kutusu içerisinde yer alan kullanıcılara, yakın arkadaşlarına e-mailler gönderebilir. E-Mail alan kişi, gönderen kişiyi tanıdığı için bu iletiyi rahat bir şekilde açmaktadır. Aslında e-mail bir truva atıdır ve artık kendi sistemine de bulaşmıştır. Sisteminizi bu tür tehlikeli yazılımlardan korumak için güçlü anti-virüs programları kullanarak sisteminizi her zaman güncel tutmak gerekmektedir[52].

Virüslerin çalışabilmesi için bir dış müdahale gerekirken, solucanlar ise sistem içerisinde girdikten sonra kendi kendilerine çoğalabilme özellikleri bulunmaktadır. Truva atları, kendi kendilerine çoğalamama özelliği sebebiyle virüsler ile benzerlik gösterse de faydalı bir program gibi gözükerek arka planda sisteme zarar verecek çalışmalar yürüten bir casus yazılımdır[53].

### 1.3.5. Arka Kapı

Arka kapı, sistem üzerinde istenildiği zaman ortaya çıkarılamayacak şekilde, kullanıcı adı ve şifre gibi kimlik doğrulama metotlarını devre dışı bırakarak yasadışı yöntemlerle sisteme ulaşma ve bilgilere erişme imkânı sağlayan bir yöntemdir[54].

Zaman zaman truva atları ve arka kapılar birbirine karıştırılmaktadır. Hem arka kapı hem de truva atları sisteme sızmayı amaçlayan zararlı yazılımlardandır. Ancak truva atı görünürde zararlı bir yapı gibi kendini ortaya vermezken, arka kapı yalnızca sistemin içerisine girmeyi hedefleyen gizli yapılar olarak bilinmektedir[55].

### 1.3.6. Mantık Bombası

Mantık bombaları, belirli bir sistemin içerisinde yer alan zararlı yazılımlar olarak karşımıza çıkmaktadır. Bu tür zararlı yazılımlar sistemlere sızarlarken kullanıcı kişiler

[52] Miller, **a.g.e.**, s.74–75
[53] Barış Çeliktaş, **Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme,** Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi, Trabzon, 2016, s.33
[54] Akarslan, **a.g.e.**, s.95
[55] Canbek ve Sağıroğlu, **a.g.e.**, s.126

tarafından fark edilmeleri çok zordur. En yaygın zararlı yazılımlar arasında bulunan mantık bombaları, sistemlere sızdıkları süreden itibaren verileri ortadan kaldırmaya çalışırlar. Etki alanları çok geniş bir kitledir[56].

### 1.3.7. Kök Kullanıcı Takımı

Kök kullanıcı takımları, bir saldırının başarılı olması durumunda sızılan sisteme eklenen yazılımlardır. Takım içerisinde bulunan araçlar, saldırganın izlediği yolu ve daha sonrasında sisteme girerken yakalanmaması için sistem içerisinde bıraktığı arka kapıları oluşturur. Bu sayede saldırgan sistem içerisinde rahat bir şekilde hareket edebilmektedir[57].

Kök kullanıcı takımlarının önemli iki unsuru bulunmaktadır. İlki giriş yaptıkları sistemde, herhangi bir yetki sınırlandırılması ile karşı karşıya kalmamak için ihtiyaç duyulan komutların girilmesidir. İkincisi ise sisteme sızan kişilerin, kendilerinden daha üstün yetkiye sahip olanlardan gizlenmeleridir[58].

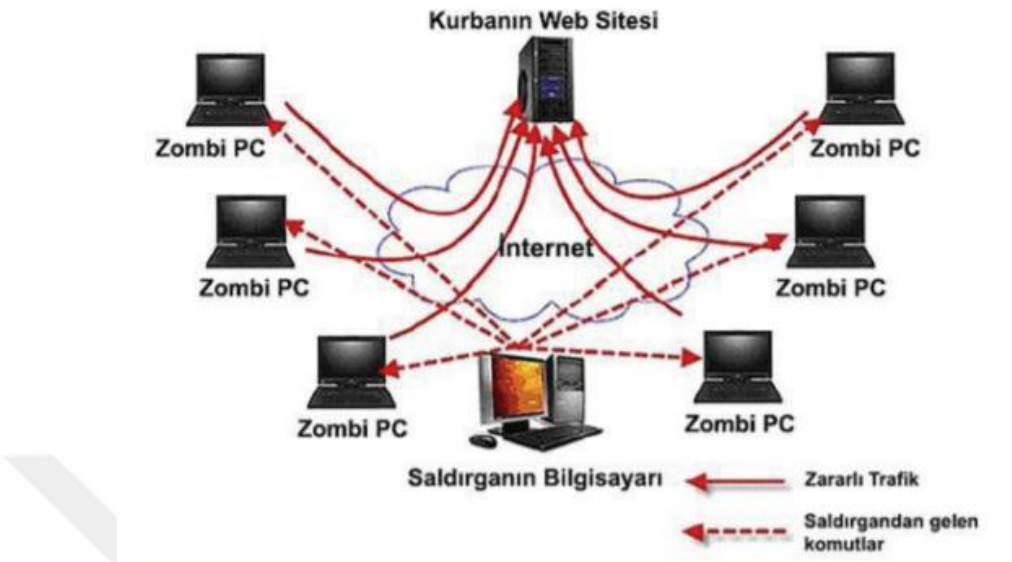
### 1.3.8. Köle Bilgisayarlar / Botnet / Zombi Bilgisayar

Zombi bilgisayarlar, kullanıcının haberi olmaksızın sistemine yüklenen zararlı yazılımın, sistem kontrolünün başkaları tarafından ele geçirilmesi ve bu sayede hedefteki sistemlere saldırılar gerçekleştirmek amacıyla kullanılan bilgisayarlara verilen isimdir. Botnetler, siber saldırıların en önemli alt yapı bileşenlerinden biridir. Botnet ağları, komuta ve kontrol sunucularından ve saldırıya katılan aynı zamanda uzaktan yönetilebilen çok sayıda virüslü bilgisayarlardan oluşmaktadır[59]. Zombi bilgisayarların artmasıyla birlikte siber saldırıların ortaya çıkartacağı boyutta da bir artış gerçekleşmektedir.

---

[56] Akarslan, **a.g.e.**, s.94
[57] Canbek ve Sağıroğlu, **a.g.e.**, s.127
[58] Akarslan, **a.g.e.**, s.94–95
[59] Louis Marinos, Adrian Belmonte ve Evangelos Rekleitis, **"Enisa Threat Landscape 2015",** European Union Agency For Network And Information Security, 2016, s.26

**Şekil 11:** Zombi Bilgisayarların Siber Saldırılarda Kullanılması




**Kaynak:** https://www.stm.com.tr/documents/file/Pdf/05-2_siber_tehdit_durumu_rapor_2016-08-03-10-57-17.pdf, (22.12.2019)

Zombi bilgisayar haline dönüşen bir sisteme yüklenen programlar sayesinde saldırganlar istedikleri zaman DDos komutlarını göndererek sistemleri aktif hale getirmekte ve gerçekleştirilecek olan siber saldırıya dahil etmektedir.[60] Mühendislik Teknoloji Danışmanlık dergisinin siber tehdit durum raporunda şu bilgilere yer verilmiştir[61]: 2016 yılında EMEA (Europe, Middle East and Africa) ülkeleri arasında yapılan bir araştırmada botnete bağlı cihazların sayısı tespit edilmiştir. Buna göre Türkiye ilk sırada yer almakta, şehirler olarak bakıldığında ise İstanbul ve Ankara botnetlere bağlı en fazla cihaz bulunan şehirler arasında birinci ve ikinci sırada yerlerini almaktadır.

### 1.3.9. Fidye Virüsü

Saldırganlar, sistemlere müdahalede bulunarak verilerin asıl sahibi olan kişilerin ulaşmasına engel olmaktadır. Daha sonra bu verilere sahip olan kişilerle iletişime geçerek belirli bir fidye karşılığında verileri, dosyaları erişime açmaktadır. Bu tür zararlı

[60] https://docplayer.biz.tr/12545187-Dos-ddos-zombi-bilgisayar-ve-botnet-nedir.html, (25.12.2019)
[61] **"2016 Ekim-Aralık Dönemi Siber Tehdit Durum Raporu",** STM Mühendislik Teknoloji Danışmanlık, s.12

yazılımlara fidye virüsleri ismi verilmiştir. Fidye yazılımlarını sistemlere bulaştıran saldırganlar, sistemlere bir ekran görüntüsü göndermekte ve bu şekilde kullanıcılarla iletişime geçmektedirler. İletişime geçerek fidye yazılımlar için banka yoluyla veya nakit olarak ödeme yapılırken saldırganlar genelde tespit ediliyordu ve onlar için büyük problemler ortaya çıkıyordu. Ancak Bitcoin vb. yeni ödeme yöntemleri türeyince ödemelerin takip edilmesi ve sisteme sızan kişilere ulaşmak artık daha zorlamıştır. Fidye yazılım saldırıları, bilgilerin çok kıymetli olmasıyla birlikte fidyelerinde yüksek seviyede istenildiği daha çok sağlık, finans ve telekomünikasyon şirketlerini hedef almaktadır. Fidye yazılımı saldırısının başarılı olması için gereken aşamaları şu şekildedir[62]:

- Sistemin ele geçirilmesi,
- Kullanıcının sistem içerisinde yer alan verilere erişimin engellenmesi,
- Veri sahibine ödeyeceği fidyenin ve ödeme şeklinin bildirilmesi,
- Veri sahibi tarafından yapılan ödemenin kabulü.
- Ödeme alındığında asıl kullanıcıya erişim izninin verilmesi.

## 1.4. Siber Saldırı Türleri

### 1.4.1. DoS ve DDoS Saldırıları / Hizmet Dışı Bırakma

Dos (Denial Of Service- Servis Hizmet Reddi) saldırılarında amaç kullanıcıların sistemlere ulaşmasını engellemektir. Her sistemin bir kapasitesi bulunmaktadır ve bu kapasitenin aşılması durumunda sistemlere ulaşmak çok zorlaşmakta ya da erişilemez hale gelmektedir. DDos saldıırları ise Dos saldırılarındaki gibi tek bir servis sağlayıcısıyla yapılmamaktadır. DDos saldırıları sırasında ne kadar çok zombi adı verilen bilgisayarlar kullanılırsa saldırının gücü de o oranda artmaktadır. Zombi bilgisayarlar, DDos saldırları öncesinde ele geçirilmiş ve istenilen zaman saldırıya katılabilir durum da ki sistemlerdir. DDos saldırıları ile Dos saldırılarını kıyasladığımızda, DDos saldırılarının boyutları daha büyük zararlar ortaya

[62] Çeliktaş ve Çelik, **a.g.m.**, s.108–109

çıkarmaktadır. Bu tip saldırılarda amaç sistemin içerisine sızmak değil, verilen hizmeti askıya/sekteye uğratmaktır[63].

Corero 2018 Yılı DDoS Trend Raporu'nda yayınlanan istatistiklere göre[64];

- 2018 yılında yapılan DDos saldırılarının %82'si düşük boyutlarda gerçekleşmiştir.
- Yüksek boyutlarda gerçekleştirilen saldırıların oranı toplam saldırıların %2'si olarak gözlenmiştir.
- 2018 yılında yapılan DDos saldırılarının %81'i 10 dakika veya daha kısa sürmüştür.
- DDos saldırılarının %96'sı 60 dakika veya daha kısa sürmüştür.
- 2017 yılında 10 dakikadan daha az süren saldırıların oranı %71 iken, 2018 yılında %81 olarak gerçekleşmiştir.

Q4 2017 Global DDoS Threat Landscape Raporu'ndaki istatistiklere göre; ABD %24, Güney Kore %10,3 ve Çin %8,7 oranlarıyla DDos saldırısı gerçekleştiren ülkeler listesinde en üst sıralarda yerlerini almıştır. Türkiye ise %2,1 ile en fazla DDos saldırısı gerçekleştiren 10 ülke arasında dokuzuncu sırada yerini almıştır[65].

### 1.4.2. Sosyal Mühendislik

Sosyal Mühendislik (Social Engineering), bireyleri aldatmayı hedefleyen ve ileri seviye teknoloji kullanılmasına gerek kalmadan gerçekleştirilen bir saldırıdır[66].

Sosyal mühendislik tipi saldırılardan korunmak amacıyla savunma sistemleri kurulmakta ve buna bağlı olarak da kurumların güvenlik prosedürleri daha iyi bir duruma gelmektedir. Sosyal mühendislik denetimleri yaptıran kurumlar, bu tip bir saldırıyla karşı karşıya kalma ihtimalleri diğer kurumlara göre daha azdır. Çünkü

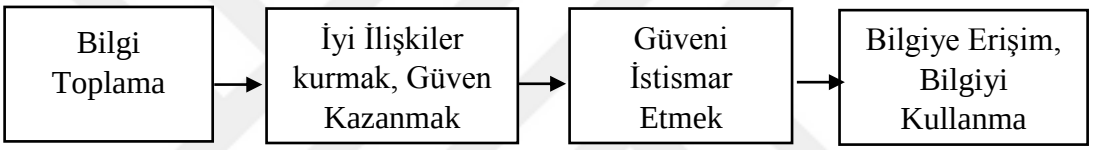
[63] https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html, (01.01.2020)
[64] Corero, **"Full Year 2018 DDoS Trends Report",** 2019, s.4–6
[65] Imperva, **"Global DDoS Threat Landscape Q4 2017",** 2018, s.8-17
[66] Gökhan Muharremoğlu ve Raif Berkay Dinçel, **"Sosyal Mühendislik",** Pwc, 2018, s.1

denetimlerin yapıldığını bilen şirket çalışanları, uyulması gereken güvenlik kurallarını iyi bilmekte ve ona göre kontrol eylemleri daha etkin bir şekilde çalışmaktadır[67].

Sosyal Mühendislik saldırılarının diğer saldırılara göre başarılı olmalarının temel sebepleri[68];

- İnsanlar kandırılabileceklerini asla düşünmemektedir.
- İşletmeler aldıkları güvenlik tedbirlerinin teknik olarak yeterli olduklarını düşünmektedir.
- Bilgi güvenliğinin aşılabilecek en zayıf noktası ‘‘İnsan’’ boyutudur.

**Şekil 12:** Sosyal Mühendislik Saldırı Planı




**Kaynak:** Alper Başaran ve Okan Yıldız, **Sosyal Mühendislik Saldırıları**

### 1.4.3. Yemleme-Oltalama Saldırıları

Oltalama (Phishing) tekniği kullanılarak yapılan saldırılarda, kullanıcıların kredi kartı bilgileri, kimlik bilgileri gibi özel bilgilerini ele geçirmek amaçlanmaktadır. Saldırganların en fazla tercih ettiği oltalama yöntemi, bir bankadan veya finans kurumları tarafından gönderilmiş gibi gözüken e-postalardır. E-Mailin içeriğinde genellikle bir form bulunmakta ve bu formda hesap numarası, şifre vs. gizli tutulması gereken bilgiler yer almaktadır. Zaman zaman kim oldukları belli olmayan kişiler bu sefer e-posta yoluyla değil de telefonla arayarak veya mesajla iletişime geçmekte ve bilgileri talep etmektedir[69].

[67] Hasan Bağcı, **“Sosyal Mühendislik ve Denetim”,** Denetişim Dergisi, Kamu İç Denetçiler Derneği, Sayı.1, 2016, s.48
[68] Okan Yıldız ve Alper Başaran, **“Sosyal Mühendislik Saldırıları”,** s.17
[69] https://www.eset.com/tr/phishing/, (10.01.2020)

### 1.4.4. IP Aldatmacası-Gizlenmesi

Bu saldırı türünde saldırgan, güvenilir bir sitenin internet protokolünü (IP) kullanarak herhangi bir kişinin sistemine bağlanmaktadır. Bu sayede saldırıyı gerçekleştirirken kendi kimlikleri ortaya çıkmamakta ve gizlenmektedirler[70].

IP aldatması (IP Spoofing), en fazla Dos saldırılarında görülmektedir. Saldırı başladığı andan itibaren gönderilen paketlerin hepsi farklı adreslerden geliyormuş gibi gözüktüğü için asıl saldırganın belirlenmesi mümkün olmamaktadır[71].

Ülkemizde Yüksek Öğretim Kurumuna (YÖK) yapılan saldırı buna bir örnektir. Sitede bulunan açıklardan yararlanarak YÖK'ün internet sitesini hacklemişlerdir. Ele geçirdikten sonra üniversiteler ile ilgili evrakları, YÖK'e gelen şikayetleri ve birçok gizli yazışmaları sosyal medya üzerinden paylaşmışlardır. Siber güvenlik uzmanları saldırganları yakalayabilmek için harekete geçseler de saldırı IP Spoofing yöntemi ile yapıldığından saldırıda yer alan bilgisayarların IP adreslerinin kamu kurumlarına ve ilgisiz kişilerin üzerine kayıtlı oldukları ortaya çıkmıştır[72].

### 1.4.5. Sıfırıncı Gün Saldırıları

Sıfırıncı gün(0-Day) saldırıları, yazılımlarda büyük zararlar verebilecek daha önceden bilinmeyen ve ortaya çıkartılmamış zafiyetlerin saldırganlar tarafından bulunmasıdır. Yazılımı yapanlar, uygulamanın herhangi bir kısmında zafiyet bırakmayacak duruma getirip bu aşamadan sonra kullanıma açmalıdır. Eğer kullanılan bir uygulamada zafiyet varsa da geliştirici en kısa sürede bir yama ortaya çıkartarak bunu düzeltmelidir. Eğer geliştirici buna dikkate almaz ve bazı kısımlarında açıklar bırakırsa sıfırıncı gün saldırılarına uğrayabilir[73]. Bireyler ve kurumlar da kendi sistemlerini sürekli güncel tutarak bu tür bir saldırıdan korunabilirler[74].

---

[70] Muharrem Gürkaynak ve Adem Ali İren, **"Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler",** Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt.16, Sayı.2, s.272

[71] https://tr.wikipedia.org/wiki/IP_spoofing, (11.01.2020)

[72] Su Dilara Alioğlu, **Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları,** İstanbul Bilgi Üniversitesi, Lisansüstü Programlar Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, 2019, s.32–33

[73] https://www.beyaz.net/tr/guvenlik/makaleler/zeroday_nedir.html, (15.02.2020)

[74] https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit, (15.02.2020)

## 1.5. Siber Saldırı Örnekleri

Siber saldırganlar, artık şirketleri hedef almaktansa şirkette çalışan personelleri hedef almaktadır. Kurumlar, çalışanlarına siber güvenlik eğitimleri vermeli ve farkındalığı sağlamalıdır. Aksi taktirde saldırganların bir numaralı hedefi haline gelmektedirler[75].

Siber saldırıların şirketlere verdiği zararlar her geçen gün artmaktadır. Kayıpları maddi anlamda büyük olmakla birlikte toplum içinde saygınlıklarını da büyük ölçüde yitirmektedirler. Bunun üzerine IBM'in CEO'su Ginni Rometty, ''*Siber suç, dünyadaki her şirket için en büyük tehdittir*.'' açıklamasını yapmıştır. Amerikalı iş adamı Warren Buffet ise *"Siber saldırıların, nükleer silahlardan bile daha kötü olduğunu söylemiştir*"[76].

### 1.5.1. RSA Securid Sızıntısı

Siber saldırıların farklı amaçları da olabilir. Her siber saldırıda direkt olarak maddi kazanç hedeflenmemekte hedefteki kurumun dolaylı yolla maddi zarar veya itibar kaybına uğraması da hedeflenebilir. 2011 yılında gerçekleşen veri sızıntısının detayları RSA tarafından tam olarak açıklanmasa da Securid iki faktörlü kimlik doğrulama sistemi ile ilgili bazı bilgilerin çalındığı belirtilmektedir. Saldırganlar bu saldırı sayesinde doğrudan maddi kazanç elde edememekle birlikte RSA'in ana şirketi olan EMC bu veri sızıntısı olayını kapatmak için 66 milyon USD harcamıştır. Saldırı RSA içerisindeki bazı çalışan gruplarına hedefli oltalama e-postası gönderilerek başlatılmıştır. Saldırının başarılı olmasının nedeni e-postaların ikna edici şekilde tasarlanmış olması ve adında "2011 İşe Alım Planı" olan ilgi çekici bir dosya içermesidir[77].

### 1.5.2. Target Firmasına Saldırı

Amerika'da bulunan ünlü perakende firması Target 2013 yılının Kasım ayında ağır bir siber saldırıya uğramıştır. Bu saldırı sonucunda 40 milyon kişinin kredi kartı bilgileri ve

[75] İsmail Saygılı, **Dünyayı Yöneten Güç-Bilgi Güvenliğinin En Zayıf Halkası İnsan Faktörü,** Siber Güvenlik Dergisi, Sayı.1, Mayıs 2017, s.56-58

[76] https://www.cybermagonline.com/rakamlar-ve-istatistikler-ile-2018-icin-en-onemli-5-siber-guvenlik-gercegi, (22.02.2020)

[77] Saygılı, **a.g.m.,** s.58

70 milyon kişinin adres bilgileri, telefon numaraları vs. gibi özel bilgiler ele geçirilmiştir Hackerler, alışveriş anında POS cihazına takılan kredi ve banka kartlarının arkasındaki manyetik şeritte depolanan bilgileri ele geçirmişlerdir. Şirketin güvenlik ve ödeme sistemlerine kötü amaçlı yazılımlar yükleyerek bu saldırıyı gerçekleştirmiş bulunmaktalar. Bloomberg Businessweek haberine göre saldırı başladığı anda dışarıdan hizmet veren bilgi güvenliği uzmanları saldırı olduğu yönünde uyarılarda bulunmuş ancak Target firmasının yöneticileri bu uyarıları dikkate almamıştır[78].

Target firması, müşterilerine ait bilgilerin sızdırılması sebebiyle 2017 yılındaki mahkeme sonucunda 18,5 milyon USD ödemek durumunda kalmıştır. Aslında firma kayba uğrayan müşterilerinin tüm kayıplarını ödemeyi kabul etse de bu cezayı almaktan kurtulamamıştır. Mahkemenin kararına göre Target etkin bir bilgi güvenliği sistemi yürütememiştir. Çok büyük kayıplara uğrayan firma bu yaşananlardan sonra güçlü bir siber güvenlik sistemi kuracak ve bilgi güvenliği işlerinde daha yetkin kişilere bünyesinde yer verecektir[79].

### 1.5.3. ICANN Firmasına Saldırı

Dünya genelinde internet alan adlarının yönetilmesinde söz sahibi olan ve internetin gelişimine ve değişimine ilişkin önemli kararların alınmasında yetkili kurumların başında gelen ICANN (Internet Corporation for Assigned Names and Numbers) 2014 yılında, 20 dakikalık süre boyunca hacklendiğini duyurdu. Hackerlar tarafından ICANN'den gönderilmiş süsü verilen e-postaların, ICANN çalışanları tarafından açılması ve yönlendirilen sahte sayfada çalışanların kişisel bilgilerini vermesi hackerların ICANN'in dahili sistemlerine ulaşmasını sağladı. Dahili sistemlere yönetim erişimi alan hackerlar bu bölgede çalışanların mail adresleri, telefon numaraları ve çeşitli bilgilerini ele geçirdi. Problemin farkedilmesi üzerine çalışanlara ait tüm mail hesaplarını iptal eden ve şifreleri yenileyen ICANN güvenlikle ilgili gerekli önlemleri aldı. ICANN Wiki sayfası, ICANN blog ile Whois sorgulama portalını 20 dakikalık sure ile ele geçiren korsanlar alınan güvenlik önlemleri ile problem büyümeden sistemden uzaklaştırıldı. Konu ile ilgili açıklama yapan ICANN yetkilileri *"Hack olayı*

[78] https://www.businessinsider.com/bloomberg-businessweek-publishes-brutal-interactive-cover-on-the-target-hack-2014-3, (25.02.2020)
[79] https://h4cktimes.com/veri-sizintilari/abdnin-dev-perakende-zinciri-targeta-sok-ceza.html, (26.02.2020)

*ile ilgili kamuoyunu bilgilendirmek ICANN'in önemle savunduğu şeffaflık ilkesinin bir gereğidir, ayrıca siber güvenlik konusunda paylaşılan bu bilgi diğer kurumların gerekli önlemleri almasında da rol oynuyor."* şeklinde açıklama yapmıştır[80].

### 1.5.4. Alman Çelik Fabrikasına Saldırı

Hackerler bu seferde 2014 yılında bir çelik fabrikasına siber saldırı düzenlemiştir. Almanya'da bulunan çelik fabrikası uğradığı siber saldırı sonucunda, saldırganlar tesisi ele geçirmiş ve maden eritme ocaklarının istenildiği zaman kapatılmamasına sebep olmuş ve tesislerde büyük zararlar ortaya çıkmıştır[81].

Saldırının gerçekleşme anı şu şekildedir[82]:

*"Karmaşık sosyal mühendislik ve spear phishing tekniklerini kullanan hackerlar, fabrikanın ofis ağına erişti. Spear phishing, saldırganların sanki bir organizasyondan geliyormuş gibi epostalar gönderdiği bir saldırı tipi. Bu tür e-postalar ile ofis ağına erişen saldırganlar, buradan da üretim ağına sızdı. Bu aşamadan sonra ise bazı bileşenler ve hatta bütün sistemler çökmeye başladı. Fabrikanın maden eritme ocaklarından biri kontrollü bir biçimde kapatılamadı ve BSI'a göre bu durum fabrikada devasa zararlara yol açtı. Saldırganların teknik yeteneklerinden ise "çok gelişmiş" olarak bahsedildi."*

### 1.5.5. Cathay Pacific Havayolu Şirketine Saldırı

Merkezi Hong Kong'da bulunan Cathay Pacific Havayolu şirketi 2018 yılında 9,4 milyon müşterisinin kişisel bilgilerinin, gerçekleşen bir siber saldırı sonucu çalındığını duyurmuştur. Bu saldırı sonucunda havayolu şirketinin hisselerin büyük düşüşler gerçekleşmiş ve yaklaşık olarak 201 milyon dolarlık bir değer kaybı yaşamıştır. Havacılık sektörünün en geniş kapsamlı siber saldırısı olarak tarihteki yerini almış bulunmaktadır. Bu olay saldırı gerçekleştikten yedi ay sonra ortaya çıkmış ve firma tarafından yapılan açıklamada; kişisel bilgilerin ele geçirildiği ancak bu bilgilerin

[80] **Siber Güvenlik Çağı,** Natro Hosting Dergisi, Sayı.3, Ocak 2015, s.15
[81] https://lepicallidus.com/teknoloji/almanyada-celik-fabrikasina-siber-saldiri, (27.02.2020)
[82] https://www.technopat.net/2014/12/23/hackerlar-almanyada-celik-fabrikasini-hackledi/, (05.03.2020)

herhangi bir yerde kullanılıp kullanılmadığı ile ilgili bir bilginin olmadığını söylemişlerdir[83].

# 2. SİBER GÜVENLİK VE İÇ DENETİM

## 2.1 İç Denetim

Türkiye İç Denetçiler Enstitüsü'nün tanımına göre[84];

*"İç denetim, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkililiğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur."*

İç denetim finansal işlemler ile ilgilendiği kadar aynı zamanda finansal olmayan işlemlere de odaklanmaktadır. Yapılan denetimler sayesinde yöneticiler ve çalışan kişiler yaptıkları işleri analiz ederek iç kontrol ile ilgili süreçleri değerlendirmektedir[85]. İç denetimin performansını değerlendirebilmek ve katma değerini ortaya çıkartabilmek için Uluslararası İç Denetçiler Enstitüsü (IIA) tarafından "Uluslararası İç Denetim Standartları" yayınlanmıştır. Denetim sırasında bu standartlara uymak gerekmektedir[86].

İç denetim, işletmelerin faaliyet alanı ile ilgili tüm süreçlerinin gözden geçirilerek değerlendirilmesini içeren bir denetim türüdür. Bu denetim sayesinde kontrollerin

[83] https://tr.sputniknews.com/asya/201810251035836450-cathay-pasific-havayollari-hacklendi-musteri-bilgileri-calindi/, (07.03.2020)
[84] https://www.tide.org.tr/page/26/Ic-Denetimin-Tanimi, (27.03.2020)
[85] Nuran Cömert, **"İşletmelerde Kontrol ve Denetim Kavramlarının Doğru Kullanılması amacına Yönelik Kavramsal Bir İnceleme",** Marmara Business Review, Cilt.1, Sayı.1, 2016, s.12
[86] Ali Kamil Uzun, **"İşletmelerde İç Denetim Faaliyetinin Rolü ve Katma Değeri",** Deloitte s.2

etkinliği ölçülmektedir. İç denetim görevini yerine getiren iç denetçiler, denetim sonucunda ortaya çıkan bulguları ve önerileri üst yönetim ile paylaşmaktadır. İşletme çalışanları, iç denetçilerin varlığını bilmesi durumunda kendilerinin işletme politikalarına ve planlarına ne derece uyum göstermiş oldukları ölçüleceği için davranışlarını ve faaliyetlerini daha dikkatli bir şekilde gerçekleştirmeye çalışacaklardır[87].

İç denetçilerin, sorumluluklarını yerine getirebilmeleri için gerekli olan bilgi ve beceriye sahip olması gerekmektedir. İç denetçilerin her alan hakkında uzmanlık seviyesin de bilgilerinin olması beklenmemektedir. Yetersiz olduklarını düşündükleri durumlarda dışarıdan uzmanlık desteği almaları gerekmektedir[88].

## 2.2 İç Denetimin Amacı ve Kapsamı

İç denetimin amacı; kurumların hedeflerine ulaşabilmesi ve karşı karşıya oldukları risklerin yönetilebilmesi için iç kontrol sistemine yönelik bağımsız ve tarafsız bir şekilde güvence hizmeti vermektir. İç denetim faaliyetini gerçekleştirenler, doğru bir risk yönetimiyle birlikte hem etkili hem de verimli kontrol ve kurumsal yönetim ile ilgili görüş ve öneriler vermektedir[89]. İç denetim sayesinde işletmeyi yönetmekle sorumlu olan kişiler görevlerini daha etkin bir şekilde yerine getirebilme fırsatına sahip olmaktadır. İç denetimin asıl amacı işletme yönetimine hizmet etmektir[90].

Bir işletmede hilenin ortaya çıkartılması iç denetimin esas amaçlarından bir tanesi olmasa da incelediği konular arasında yer almaktadır. Hilenin önlenmesi, caydırılması ve tespit edilmesi yönetimin sorumluluğu içerisindedir. İç denetim ekipleri yönetime, hile olaylarına karşı kontrollerin yeterli seviyede olup olmadığı konusunda güvence hizmeti sağlamaktadır[91]. Genel olarak iç denetimin kapsamı şunlardan oluşmaktadır[92]:

- İç kontrol sisteminin incelenerek değerlendirilmesi,
- Risk yönetim sisteminin bir bütün olarak incelenmesi,

[87] Ersin Güredin, **Denetim,** Beta Basım Yayım, 10.Baskı, İstanbul, 1998, s.15
[88] Davut Pehlivanlı, **Modern İç Denetim Güncel İç Denetim Uygulamaları,** Beta Yayınları, 2.Baskı, İstanbul 2014, s.18–19
[89] İstanbul Serbest Muhasebeci Mali Müşavirler Odası, **"İç Denetime Genel Bir Bakış",** 2015, s.14
[90] Hasan Gürbüz, **Muhasebe Denetimi,** Bilim Teknik Yayınevi, 4.Baskı, İstanbul, 1995, s.51
[91] Didem Doğmuş Yurdakul., **"Avrupa Birliği'nde İç Denetim Sistemi: Üye Ülke Uygulamaları",** H. Kıral içinde, İç Denetim, Ankara: İç Denetim Koordinasyon Kurulu, 2014, s.15
[92] Bayram Aslan, **"Bir Yönetim Fonksiyonu Olarak İç Denetim",** Sayıştay Dergisi, Sayı 77, s.68–69

- Yönetimin ve mali bilgi sisteminin incelenmesi,
- Muhasebe kayıtları ile mali tabloların doğruluk ve güvenilirlik açısından incelenmesi,
- İşletmenin her türlü faaliyetlerinin yasal mevzuata, standartlara ve belirlenen politika ve prosedürlere uygunluğunun incelenmesi,
- Değerlendirmelerin sonucunda rapor verilmesi ve önerilerde bulunulması,
- Raporlamadan sonra gereken izlemelerin yapılması.

## 2.3 İç Denetimin Unsurları

### 2.3.1 Bağımsızlık ve Tarafsızlık

Bağımsızlık; iç denetçilerin görevlerini yerine getirirken tarafsızlığını bozabilecek durumlardan uzak durmalarıdır. Tarafsızlık ise iç denetçilerin görevlerini, çalışmaların sonucuna dürüst bir şekilde inanacakları ve bu denetimin kalitesinden taviz vermeyecek şekilde yapmalarını sağlayan tarafsız bir zihinsel tutumdur. Tarafsız bir iç denetçinin karar alırken başkalarına bağlı kalmaması önemlidir[93].

İşletmenin birer çalışanı olarak iç denetim ekipleri veya dışarıdan denetim hizmeti veren ekipler, denetim alanı içerisindeki konularla ilgili verilecek kararlarda bağımsız ve tarafsız bir şekilde davranması gerekmektedir. Denetim sonucunda ortaya çıkacak bulguların ve verilecek önerilerin doğru olabilmesi için iç denetçilerin bağımsızlık ve tarafsızlıklarını kaybetmemeleri son derece önem arz etmektedir. Bu durumu etkileyecek sebeplere; kişisel ilgi, ekonomik ilgi, sosyal baskı, cinsiyet önyargısı gibi örnekler verilebilir[94].

İç denetçilerin bağımsız olabilmeleri için denetledikleri birimden daha üst bir yöneticiye karşı sorumlu olması gerekmektedir. ABD'de 317 işletmenin yer aldığı bir araştırma sonucuna göre iç denetçilerin 136'sı Muhasebe Müdürüne karşı sorumludur. Bu durum, iç denetçilerin muhasebe departmanıyla ilgili denetimlerini doğru bir şekilde gerçekleştirememelerine yol açmaktadır. Muhasebe müdürünün çalışmalarını

[93] Türkiye İç Denetim Enstitüsü, **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi (2007'deki Değişikliklerle),** 2008, s.35–39
[94] Pehlivanlı, **a.g.e.**, s.8

inceleyecek olan iç denetçi ancak üst yönetime karşı sorumlu olursa başarılı bir denetim gerçekleşmiş olacaktır. Aynı zamanda iç denetim ekiplerinin, denetim sırasında görevinin ne olduğunu bilmeleri, her türlü baskıya rağmen doğru bildiklerini yapması gerekmektedir. Bağımsızlığın tek başına yeterli olmadığı bu konuda tarafsızda olması gereken iç denetçilerin görevlerini yerine getirebilmeleri için kendi yaptıkları prosedürleri denetlemekten kaçınmaları gerekmektedir. Denetçiler hem yapan hem de denetleyen konumuna düşmemeye özen göstermelidir. İç denetçilerin bağımsız ve tarafsız olmaları bu şartlara uygun davranmalarına bağlıdır[95].

### 2.3.2 Güvence ve Danışmanlık Kavramı

Güvence Hizmetleri; İşletmenin risk yönetimi, kontrol ve yönetişim süreçlerine yönelik bağımsız bir değerlendirme esas alınarak sonuçların objektif olarak incelenmesidir. Güvence görevinin kapsamı ve niteliği iç denetçiler tarafından belirlenmektedir. Güvence hizmetlerinde genellikle üç tarafı bulunmaktadır[96]:

- Sistem veya ele alınan bir konunun doğrudan içinde olan kişi veya grup, süreç sahibi
- Değerlendirmeyi yapan kişi veya grup, iç denetçi
- Değerlendirmeyi kullanan kişi veya grup, kullanıcı

**Şekil 13:** Güvence Hizmetlerinin Tarafları


**Kaynak:** Emine Aktaş, **İç Denetim ve Risk Yönetimi İlişkisi,** İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Muhasebe ve Denetim Anabilim Dalı, Yüksek Lisans Tezi, 2015

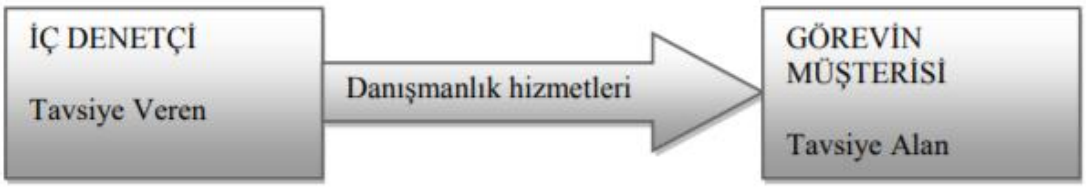
Danışmanlık Hizmetleri; işletme içerisinde idari bir görevde yer almamak şartıyla faaliyetlerini geliştirme ve değer katma hedefiyle yola çıkılan bir hizmettir. Bu hizmet çerçevesinde, önerilerde bulunmak ve işleri hem daha kolay hem de daha doğru bir

[95] Gürbüz, **a.g.e.**, s.52–53
[96] Türkiye İç Denetim Enstitüsü, **a.g.e.**, s.15

şekilde gerçekleştirebilmek üzerine görüşmeler yapılmaktadır. Danışmanlık hizmetlerinin genellikle iki tarafı bulunmaktadır[97]:

- Tavsiye veren kişi veya grup, iç denetçi
- Tavsiye talep eden ve alan kişi veya grup, görevin müşterisi

**Şekil 14:** Danışmanlık Hizmetinin Tarafları




**Kaynak:** Emine Aktaş, **İç Denetim ve Risk Yönetimi İlişkisi,** İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Muhasebe ve Denetim Anabilim Dalı, Yüksek Lisans Tezi, 2015

Bu iki hizmet çeşidi ile birlikte iç denetimin kapsamında genişlemektedir. İç denetim birimleri kontrol, risk yönetimi ve kurumsal yönetim konularında yönetime danışmanlık ve aynı zamanda güvence hizmetleri sağlamaktadır. İç denetimin gelişimi ve değişimi sonucunda çalışmalar pro-aktif olarak yürütülmeye başlanmıştır. Geleneksel denetimde olay gerçekleştikten sonra müdahale edilirken, kurumsal risk yönetimi temelli denetim anlayışıyla olayın gerçekleşme durumuna karşı iç denetim birimleri önlemlerini almaktadır. Bu sayede kurumların amaçlarına ulaşmalarına katkı sağlanmaktadır[98].

### 2.3.3 Kurumun Faaliyetlerinin Geliştirilmesi ve Değer Katılması

Değer Katmak, güvence ve danışmanlık hizmetleri yoluyla işletmenin hedeflerini gerçekleştirme fırsatlarını arttırmak ve faaliyetleri geliştirme imkânlarını belirleyerek riske maruz kalmasını azaltmaktır[99].

Sürekli olarak gelişen meslekler arasında iç denetim, işletmelerde çok önemli ve vazgeçilemez konumda olmasını sağlayan, onun işletmelere sağladığı katma değerden

[97] Türkiye İç Denetim Enstitüsü, **a.g.e.**, s.15
[98] Pehlivanlı, **a.g.e.**, s.8–9
[99] Türkiye İç Denetim Enstitüsü, **a.g.e.**, s.35

kaynaklanmaktadır[100]. İç denetçiler, yaptıkları işi yönetim kademesine çok iyi bir şekilde anlatabilmeleri gerekmektedir. Üst yönetim, iç denetimin işletmeye sağlayacağı katma değerin farkına varırsa, iç denetim sistemi daha etkili ve verimli bir şekilde çalışma fırsatına sahip olabilmektedir. İç denetimin değer katma rolü iyi anlaşılamadığı için yönetim kademesinin bütçede daralmaya gideceğinde ilk akla gelen alan olarak iç denetim görülmektedir. Geleneksel denetim yaklaşımını benimseyen iç denetim ekipleri genellikle bu durumla karşı karşıya kalmaktadır[101].

### 2.3.4 Sistematik ve Disiplinli Bir Faaliyet Olması

İç denetim faaliyetinin sistematik bir çalışma olmasının temelinde; iç denetim faaliyetinin işletme içerisinde oluşturulmasından iç denetçilerde bulunması gereken niteliklere, denetim faaliyetlerinin planlamasında nasıl bir yol izleneceğine yönelik tüm konuların detaylı bir şekilde standartlara bağlanmış olması yer almaktadır. İç denetimin tanımında yer alan hususlara, standartlarda detaylı olarak yer verilmiştir. İşletmeye değer katma, bağımsızlık ve tarafsızlık gibi önemli noktalar standartlarda ve UMUÇ'ta detaylı olarak bulunmaktadır. İç denetimin tanımı ile standartlar ve UMUÇ arasında tam bir anlam ve bütünlük vardır. Bu sayede iç denetim hem teorik açıdan hem de uygulama aşamasında tüm yönleriyle detaylandırılma imkanına sahip olmaktadır. Birbirleriyle uyum içerisinde olan bu süreçler, iç denetim mesleğinin etik kurallarının güçlü bir şekilde belirlenmesine ve sertifikalı iç denetçi (CIA) gibi iç denetçilerin niteliklerine yönelik düzenlemeler, iç denetimin disiplinli bir meslek olmasına katkı sağlamaktadır[102].

## 2.4 İç Denetimin Türleri

### 2.4.1 Mali Denetim

Mali denetim kavramı, literatürde aynı zamanda finansal tablolar denetimi ve mali tablolar denetimi ismi ile de geçmektedir.

Mali tablolar denetimi, işletmelere ilişkin finansal tabloların belirli muhasebe standartlarına uygunluğu, mali durumu ve faaliyet sonuçlarının gerçeği yansıtıp

[100] Ali Kamil Uzun, **"Denetim Hayattır",** Turcomoney Dergisi, Deloitte, 2014, s.3
[101] Ali Kamil Uzun, **"Değer Yaratan Denetim",** İç Denetim Dergisi, Deloitte, Sayı.14, 2006, s.1–2
[102] Çetin Özbek, **İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol,** 2012, s.106

yansıtmadığı konusunda bir görüşe varabilmek için yapılan denetimdir[103]. Mali denetimler büyük bir kullanıcı kitlesinin, ekonomik karar alma sürecinde önemli yer tutmaktadır. Mali denetim sonucunda, yöneticiler işletmenin kaynaklarının hangi ölçüde ve etkinlikte kullanıldığını görebilmektedirler[104].

İç denetimin, finansal tabloların denetimindeki rolü muhasebe kayıtlarının doğruluğunu ve güvenilirliğini araştırarak bu bilgilerin elde edilmesi aşamasın da yer alan kayıt ortamını ve raporlama sistemini kontrol etmektir. İç denetçilerin amaçları arasında işletme varlıklarının dışarıdan veya içeriden gelebilecek zararlara karşı korunup korunmadığını araştırmaktır. Finansal tablolar denetimi, hata ve hileleri ortaya çıkartma rolünün yanında önlenmesi için de koruma yöntemlerinin geliştirilmesine yardımcı olmaktadır[105]. Aynı zamanda iç denetimdeki önemlilik seviyesi bağımsız denetime göre daha düşüktür. Bu sebeple iç denetim sırasında daha fazla ayrıntıya girilmekte ve devamlılık gerektiren bir süreç olarak görülmektedir[106].

### 2.4.2 Uygunluk Denetimi

İşletmenin, faaliyetlerinin veya işlemlerinin belirli kurallara uygun olup olmadığının belirlenmesi amacıyla yapılan denetim türüdür. Bu kuralları belirleyen otorite işletmenin üst yönetiminde bulunan kişiler olabildiği gibi devlet kurumları da olabilmektedir. Bu denetim türünde asıl amaç mevzuata uygunluğun belirlenmesidir[107]. Bir üretim işletmesi dışarıdan hammadde alırken, depoya gelen malzeme için teslim alma tutanağının düzenlenip düzenlenmediği ya da üst yönetimin kasada nakit olarak bulunacak tutarın üç günü geçmeden bankaya yatırılması gerektiği yönündeki gibi kurallar bu denetim türüne bir örnek teşkil etmektedir.

---

[103] Şaban Uzay, Mehmet Özbirecikli ve Seval Kardeş Selimoğlu, **Bağımsız Denetim,** Nobel Akademik Yayıncılık, 2.Baskı, 2017, s.14

[104] Gürbüz Gökçen, Başak Ataman ve Cemal Çakıcı, **Türkiye Finansal Raporlama Standartları Uygulamaları,** Beta Yayıncılık, 2.Baskı, İstanbul, 2016, s.196

[105] Nihat Kırmızı, **İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Denetim Karar Sürecindeki Yeri,** Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2007, s.47

[106] Nejat Bozkurt, **Muhasebe Denetimi,** Alfa Yayıncılık, 7.Baskı, İstanbul, 2015, s.28

[107] Bozkurt, **a.g.e.**, s.28

Uygunluk denetiminin sonuçları, finansal tablolar denetimindeki gibi üçüncü şahıslara yönelik bilgi vermenin aksine işletmenin üst yöneticilerine rapor edilmektedir[108].

İşletmenin ana sözleşme hükümleri, meclis tarafından çıkartılan kanun, yönetmelik ve tüzük, işletme yönetiminin belirlediği politika ve prosedürler ve diğer kişiler ile yapılan anlaşmalar uygunluk denetiminde esas alınan kriterler arasındadır. Finansal tablolar denetiminden önce uygunluk denetiminin yapılmış olması gerekmektedir. Eğer uygunluk denetimi gerçekleştirilmediyse denetçinin görevi, ilk olarak denetlenecek konu üzerindeki muhasebe kayıtlarının incelenmesidir. Uygunluk denetiminin sonuçlandırılması finansal tablolar denetiminin gerçekleştirilmesi aşamasına yardımcı olmaktadır[109].

Uygunluk denetimi, işletmelerin vergi mevzuatı açısından uygun işlem yapıp yapmadıklarına da dikkat etmektedir. Vergi Usul Kanunu hükümleri ve vergi matrahı ile ilgili düzenlemeler uygunluk denetiminin ilgilendiği alanlardandır[110].

### 2.4.3 Faaliyet Denetimi

Faaliyet denetimi, performans denetimi ve başarım denetimi olarak da isimlendirilmektedir.

Faaliyet denetimi, işletmelerin büyüme ve kar oranları hakkındaki değerlendirmelerini ortaya koymaktadır. İşletmelerin amaçlarına ulaşabilmesi için faaliyetlerinin başarısını ölçmeye ve amaca ulaşırken karşılaşılabilecek engelleri yönetime düzenli bir şekilde bildirmektedir. Faaliyet denetiminin temelinde üç önemli kavram yer almaktadır. Birincisi etkenlik kavramı amaca ulaşmak, ikincisi etkinlik(verimlilik) kavramını amaca ulaşabilmek için sahip olduğumuz kaynaklardan verimli bir şekilde faydalanmak, üçüncüsü ise ekonomiklik tutumlu olmaktır[111].

Faaliyet denetimi gerçekleştirilirken denetçilerin sordukları sorular şunlardır[112]:

- İşletme faaliyetlerinde ne kadar başarılı?

[108] Güredin, **a.g.e.**, s.14
[109] Gürbüz, **a.g.e.**, s.12
[110] Uzay, Özbirecikli ve Selimoğlu, **a.g.e.**, s.14
[111] Uzay, Özbirecikli ve Selimoğlu, **a.g.e.**, s.15
[112] Sibel Uzun, **Bağımsız Denetimde İç Kontrol ve İç Denetimin Rolü,** Okan Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2016, s.14

- Hedeflere ne ölçüde ulaşılmıştır?
- İşletme faaliyetlerinin hedeflere etkisi ne ölçüde olmuştur?
- Faaliyetlerin verimliliğe etkisi ne kadar olmuştur?
- İşletme faaliyetlerini gerçekleştirirken ilkelere uygun davranmış mıdır?
- İşletmenin amaçlarına ulaşmak için izlediği yol nasıldır?

Faaliyet denetimlerini gerçekleştiren denetçiler arasından en uygunu iç denetçilerdir. Çünkü iç denetçiler diğer denetçilere göre kurumu daha yakından tanımaktadırlar[113]. Faaliyet denetiminin odak noktası kurumların örgüt yapısı, üretim yöntemleri, bilgi işlem faaliyetleridir. Bu sebeple faaliyet denetiminin gerçekleştirilmesi diğer denetim türlerine göre daha karmaşık bir yapıya sahiptir[114].

**Tablo 2:** Denetim Türleri Karşılaştırması

| | **Finansal Tablolar Denetimi** | **Uygunluk Denetimi** | **Faaliyet Denetimi** |
|---|---|---|---|
| **Denetimin Konusu** | Finansal Tablolar | Bireylerin yaptığı işlem ve faaliyetler | Örgütün veya bir birimin faaliyet sonuçları |
| **Ölçüt** | Genel Kabul Görmüş Muhasebe Kavram ve İlkeleri | Yetkili otoritelerin koyduğu yasa, kural veya politikalar | Etkinliği veya verimliliği ölçmek için önceden belirlenmiş performans göstergeleri |
| **Sonuçların İletilmesi** | Muhasebe bilgilerini kullanan tarafların tümü | Üst yönetim | Bir üst yönetim veya değerleme yapan birimin kendi yöneticileri |

**Kaynak:** Şaban Uzay, Mehmet Özbirecikli ve Seval Kardeş Selimoğlu, **Bağımsız Denetim,** Nobel Akademik Yayıncılık, 2017

[113] Murat Kiracı, **"Faaliyet Denetimi ile İç Kontrol İlişkisi",** Osmangazi Üniversitesi, Sosyal Bilimler Dergisi, Cilt.4, Sayı.2, 2003, s.68–69
[114] Bozkurt, **a.g.e.**, s.29

### 2.4.4 Bilgi Teknolojileri Denetimi

Sürekli değişen teknolojik gelişmelerle birlikte işletmeler faaliyetleriyle ilgili işlemlerin büyük bir kısmını sanal ortam üzerinden yürütmektedir. Sanal ortam üzerinden üretilen ve saklanan bilgiler daima riskler ile karşı karşıyadır. Bilgi teknolojileri denetimiyle birlikte sistemin güvenilirliğinin ve yeterliliğinin incelenmesi amaçlanmaktadır[115].

İç denetçiler; bilgi teknolojileri denetimi yaparak kurumun bilgi teknolojileri hedeflerine ulaşabilmesi için kontrollerin etkin şekilde çalışıp çalışmadığını test etmektedir. Denetimin kapsamı bilgi teknolojileriyle ilgili nesnel güvence verebilmek için sistemlerin incelenmesi, ilgili kanıtların toplanması, değerlendirilmesi ve sonuçların üst yönetime rapor olarak bildirilmesidir. İç denetim standartlarında yer alan etkinlik, gizlilik, bütünlük, erişilebilirlik, uygunluk ve güvenilirlik kavramları çerçevesinde bilgi teknolojileri denetimini gerçekleştirmektedirler[116].

İç denetçilerin gerçekleştirdikleri denetim sırasında karşılaştıkları bazı kontrol eksiklikleri şunlardır[117]:

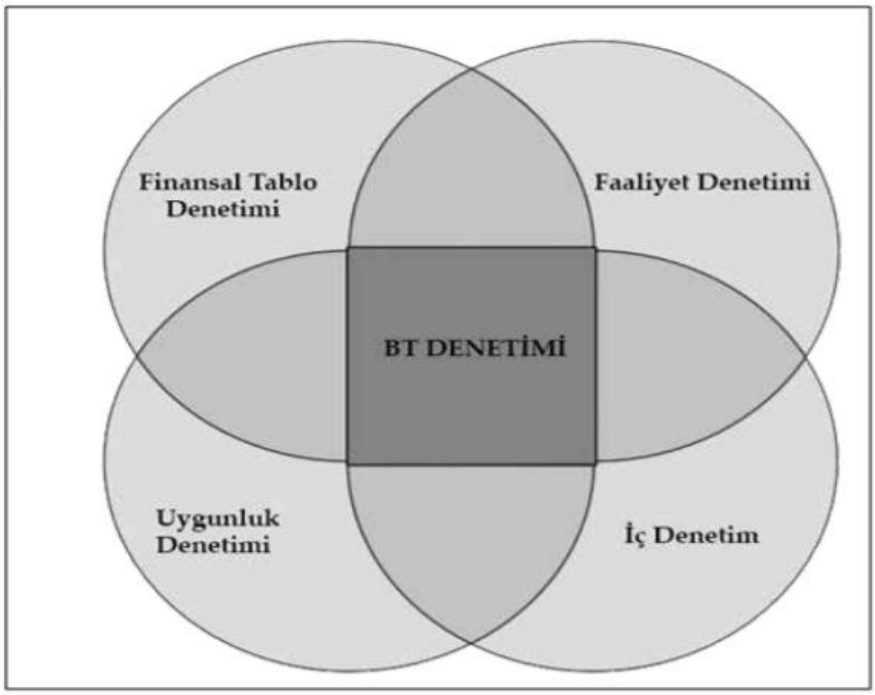
- İşletmenin bilgi teknolojileriyle ilgili politika ve prosedürlerinin olmaması ya da güncel tutulmaması,
- Görev, yetki ve sorumlulukların çalışanlara detaylı şekilde anlatılmaması,
- Aktif şekilde çalışmayan güvenlik ve saldırı tespit sistemi,
- Antivirüs programının olmaması,
- Parola ile ilgili kuralların bulunmaması,
- Güvenlik yamalarının sistemlere yüklenmemesi,
- Veri tabanı güvenliğiyle ilgili önlemlerin bulunmaması,
- Sistemlerde kullanıcı adı ve şifre giriş sayfalarının SSL ile yapılandırılmamış olması,
- İşletme için önem arz eden sunucuların güvenli yerlerde bulunmaması,

[115] Aslan, **a.g.m.**, s.76
[116] Mehmet Doğanyiğit, **"Pilot İç Denetimlerin Gerçekleştirilmesi Projesi",** Denetişim Dergisi, Kamu İç Denetçiler Derneği, Sayı.4, 2010, s.115
[117] Melike Sinem Uçum, **"BT Güvenliği Denetimi",** Denetişim Dergisi, Kamu İç Denetçiler Derneği, Sayı.16, 2015, s.76

Bilgi sistemlerindeki kontrollerin etkili bir şekilde çalışmaması durumunda işletmenin tüm kayıtları üzerinde büyük bir risk unsuru yer almaktadır. Örneğin; bilgi sisteminde yer alan bir kontrol zayıflığından dolayı üst yönetime giden bilginin yanlış veya eksik olması neticesinde yönetim tarafından verilen kararın etkisi ölçülemeyecek boyutlara ulaşabilir[118].

BT denetiminde diğer denetim türlerinde olduğu gibi mali kayıtları veya iş süreçlerini denetlemekten söz edilmemektedir. BT denetimi denildiğinde bilginin kalitesi ve güvenilirliği için kullanılan teknolojinin denetimi anlaşılmaktadır. Bu sebeple diğer denetim türlerinden ayrılmaktadır. Ancak denetim türlerinin hepsinde denetim ilkeleri, uygulama standartları, üst düzey süreçler ve faaliyetler ortak bir temele dayanmaktadır. Bu sebeple denetim türleri birbirleriyle sürekli olarak etkileşim içerisindedir. Şekilde görüldüğü gibi BT denetimi de diğer denetim türlerinin bir bileşenidir[119].

**Şekil 15:** BT Denetiminin Yeri




**Kaynak:** Stephen Gantz**, The Basıc of IT Audit Purposes Processes and Practical Information,** 2014

[118] Kırmızı, **a.g.t.**, s.54
[119] Stephen Gantz, **The Basics of IT Audit Purposes Processes and Practical Information,** 2014, s.2

### 2.4.5 Sistem Denetimi

Belirli büyüklüğe ulaşmış işletmelerin büyük bir kısmında iç kontrol sistemi güçlü veya zayıfta olsa bulunmaktadır. Sistem denetimiyle birlikte zayıf olan bu iç kontrollerin güçlü duruma getirilmesiyle, işletmenin daha etkili ve verimli bir şekilde çalışması amaçlanmaktadır[120].

Sistem denetimi, denetimi yapılan bölümün amaçlarına ulaşabilmesi doğrultusunda iç kontrol sisteminin etkin bir şekilde çalışıp çalışmadığının incelenmesidir. Denetim sırasında işletmenin iç kontrol sistemindeki eksikliklerin ortaya çıkartılması, kalitesinin ve uyguluğunun belirlenmesi, uygulanan metotların yeterliliğin ölçülmesi değerlendirme aşamasında esas alınan kriterlerdir[121].

## 2.5 İç Denetimin Güncel Başlıkları

İş dünyası ve dijital dönüşümün birbirine bağlı iki aktör olduğu görülmektedir. İşletmeler, faaliyetlerini daha etkili ve verimli bir şekilde yürütebilmek için teknolojik gelişmeleri takip etmektedir. Faaliyetlerine en uygun teknolojiyi seçmek için denetim ekiplerinin tecrübelerinden yararlanmaya ihtiyaç duyulmaktadır. Çünkü her bir yeni teknolojinin işletmelere getirdiği farklı türde risklerde yer almaktadır. İç denetçilerin, teknolojik gelişmeleri takip ederek ortaya çıkabilecek bu riskleri işletmenin üst yönetimiyle görüşmesi gerekmektedir. Teknolojik gelişmelerle birlikte iç denetçiler gelişmeli, değişmeli ve dönüşmelidir. Yeni düşüncelere kendilerini hazırlayarak işletmelerin ihtiyaçları doğrultusunda yardımcı olması beklenmektedir[122].

14. yıllık Küresel CEO Anketine katılan CEO'ların yaklaşık %70'i maliyetleri azaltmak ve daha verimli olmak için BT'ye yatırım yapmaktayken, %54'ü ise mobil cihazlarda, sosyal medyada ve daha farklı yeni teknolojiler de dahil olmak üzere girişimlere para aktarmaktadır. Ankette CEO'lar teknoloji olanaklarını araştırdıklarını ve bulut bilişimin risklerini ve faydalarını düşündüklerini belirtmişlerdir. Anket sonucunda; bulut bilişim, sosyal medya, mobil cihaz kullanımı ve siber güvenlik, iç

[120] Doğanyiğit, **a.g.m.**, s.114
[121] Kamu İç Denetim Rehberi, **İç Denetim Koordinasyon Kurulu,** Ankara, 2013, s.35
[122] **"Embracing the Next Generation of Internal Auditing",** Protiviti, 2019, s.3–17

denetim ekiplerinin dikkate alması gereken konular arasında olduğu görülmektedir. İç denetim yöneticilerine göre ilgili riskleri dikkate almak için iç denetim işlevlerinin iç ve dış konu uzmanlarıyla etkileşim içerisinde olduğu görülmektedir[123].

### 2.5.1 Bulut Bilişim ve İç Denetim

Bulut bilişim; verilerin, uygulamaların ve altyapının çevrimiçi olarak depolandığı ve uzaktan erişilebilme imkanını veren her türlü hizmeti ifade etmektedir. Şirketler bulut bilişim sayesinde fiziksel konum, iş gücü veya sermaye ile sınırsız kapasiteyi sunabilir duruma gelmektedir. Günümüzde yaşanan teknolojik gelişmeler, çoğu işletmeyi doğrudan etki altına almaktadır. İşletmelerin bulut bilişimi tercih etmelerinin en büyük sebepleri; zaman ve mekân sınırlamasının olmaması ve maliyetinin düşük olmasıdır[124]. Ancak bulut bilişim, sağladığı faydalar kadar bünyesinde güvenlik risklerini de barındırmaktadır. Bulut Bilişimde dikkat edilmesi gerekenler; risklerin belirlenmesi, risklerin nasıl azaltılabileceği ve bilgilerin nasıl daha etkin ve güvenli bir şekilde kullanılabileceği gibi konulardır[125].

İşletmeler, bulut bilişimi sistemlerine entegre edeceklerinde gereken eğitimi ve güvenlik önlemlerini dikkate almazlarsa istenilen faydayı veremeyebilir. Bununla birlikte operasyonel, finansal ve uyumlulukla ilgili risklerle karşı karşıya kalabilirler. Bu risklere örnek vermek gerekirse[126];

- Veri güvenliği ve düzenleyici risk: Halka açık bir bulutta depolanan veriler üçüncü bir tarafın yönetimine ve kontrollerine bırakılır.
- Operasyonel risk: İşletmede mevcut olan hizmetlerin bulut sistemiyle entegrasyonu pahalı ve zaman alıcı olabilir. Paylaşılan bulut hizmeti modelleri genellikle sınırlı özelleştirilebilirlik imkânı sağlayarak beklenilenden daha fazla entegrasyon riski ortaya çıkartabilir.

[123] Pwc, **"Lights, camera, action... scripting internal audit for a changed world",** 2011 State of The Internal Audit Profession Study, 2011, s.9
[124] Accenture, **"Technology Building Your Cloud Strategy With Accenture",** s.3
[125] Şeref Sağıroğlu ve Mustafa Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, 1.Baskı, Ankara, 2019, s.52–54
[126] KPMG, **"20 key risks to consider by Internal Audit before 2020",** 2018, s.7

- Finansal risk: Bulut hizmeti önemli bir yatırım gerektirirken, paylaşılan hizmetler zayıf planlama ve değişen iş gereksinimlerine bağlı olarak değişebilmektedir.

İç denetim, bulut bilişim ile ilgili risklerin değerlendirilmesi, yönetilmesi, kontrol edilmesi ve işletmelerin menfaatlerinin garanti altına alınmasına destek olmaktadır[127]. İç denetim, işletmelerin sistemlerini incelerken birtakım değerlendirmeler yaparak, üst yönetime tavsiye niteliğinde görüş bildirmektedir. Bulut bilişim konusunda iç denetçiler şu konularda yardımcı olabilmektedir[128]:

- Bulut platformları çalıştırmak için kullanılan mevcut yönetişim çerçevesinin bağımsız bir şekilde değerlendirmesini yapmak,
- İşletmeye uygun bulut bilişim sertifikalarının tanımlanması ve amaca uygun bir bulut bilişim yönetim çerçevesi oluşturmak için önerilerde bulunmak,
- Veri güvenliği risklerini tanımlamak için işletme adına üçüncü taraf bulut hizmet sağlayıcılarının bağımsız bir değerlendirmesini yapmak,
- İşletme ve bulut hizmeti sağlayıcısı arasında atanan rollerin ve sorumlulukların kapsamını değerlendirmek,
- Üçüncü taraf bulut bilişim hizmet sağlayıcıları ile Hizmet Seviyesi Anlaşmalarını (SLA) gözden geçirilmesi ve sözleşmeye uygunluğunun değerlendirilmesi,
- Bulut bilişim kurulumunun iç ve dış düzenlemelerle ilgili incelemesinin yapılması.

### 2.5.2 Büyük Veri ve İç Denetim

Büyük Veri (Big Data) kavramı 2005 yılında Roger Magoulas tarafından, büyüklüğü ve karmaşık yapısından dolayı geleneksel veri yönetimi araçlarını kullanarak yönetilememesi ve işlenememesinden dolayı büyük miktarlardaki veri kümeleri şeklinde tanımlanmıştır. Büyük verinin oluşumunda Çeşitlilik (Variety), Hız (Velocity),

[127] Pwc, **"İç Denetimin Gelişen Teknolojideki Yeni Rolü",** s.6
[128] KPMG, **a.g.m.**, s.7

Hacim (Volume), Değer (Value) ve Doğruluk (Veracity) olmak üzere 5 bileşen bulunmaktadır. Genellikle büyük verinin 5V'si olarak isimlendirilmektedir[129].

**Şekil 16:** Büyük Veride 5V


**Kaynak:** Ahmet Onay, **Büyük Veri Çağında İç Denetimin Dönüşümü,** Muhasebe Bilim Dünyası Dergisi, 2020

Çeşitlilik: Dünya genelinde Büyük Verinin artışıyla birlikte farklı tip ve özelliklerde görülmektedir. Bu çeşitlilik, denetim kanıtlarının çeşitliliğine de yansımaktadır. İç denetçiler veri ambarı içerisinde daha ayrıntılı çalışmalar yürütme durumunda kalmaktadır[130].

Hız: Veri hacmi sürekli artarak büyük boyutlara dönüşmektedir. Örneğin; bir giyim mağazasında genellikle satışlarla ilgili kayıtlar ön planda tutulmaktadır. Ancak müşterilerin, mağazanın internet sayfasındaki davranışları, incelediği ürünler, aynı ürünle ilgili sayfa da kaldığı süre gibi değişkenler müşterinin satın alma davranışını tahmin edebilmek için önemli bir gösterge olarak da görülebilmektedir. Bu sebeple bunlar belirlenerek müşteri, farklı alışveriş sitelerine yönelmeden önce ilgisini çekebilecek farklı hareketler sergilenebilir aksi taktirde müşteri vazgeçebilir. Bu durum ile karşılaşmamak için müşteri hareketleri ile eş zamanlı çalışan modeller geliştirilmesi gerekmektedir. Bu analizlerin kısa sürede yapılması gerekliliği büyük verideki hız

[129] Ümit Dülger, **"Büyük Veri Nedir?",** Yeni Türkiye Dergisi, Yeni Türkiye Stratejik Araştırma Merkezi, Sayı.89, 2016, s.503
[130] Ahmet Onay, **"Büyük Veri Çağında İç Denetimin Dönüşümü",** Muhasebe Bilim Dünyası Dergisi, Cilt.22, Sayı.1, 2020, s.142

kavramını tanımlamaktadır[131]. Büyük Verinin sağladığı yüksek hız, denetim kanıtlarının sık, tekrarlanabilir ve sürdürülebilir olması doğrultusunda sürekli denetime olanak sağlamaktadır. Büyük Veriyle bağlantılı olan teknoloji ve yazılımların geliştirilmesi, iç denetçilerin sürekli denetimi gerçekleştirebilmelerinin yolunu açmıştır[132].

Hacim: Verinin hacmi, verinin büyüklüğünü ve boyutunu yansıtmaktadır. Değişen ve gelişen teknolojiyle birlikte verilerin hacmi katlanarak artmaktadır. Örneğin; "*Dünya'da her bir dakikada 200 bin e-posta gönderilmekte, 300 bine yakın tweet atılmakta ve Facebook'a 150 binden fazla resim yüklenmektedir*." İç denetim yöneticileri, denetlenecek verinin hacmi arttıkça denetimin kapsamını da genişletmek durumuyla karşı karşıya kalmaktadırlar. Daha önceden yapılan denetimlerde örneklem yolu ile denetim tercih edilirken, bu dönemde ise verinin tamamı üzerinden denetim çalışmaları gerçekleştirilmektedir. Bu durumda makul güvence kavramı yerini daha yüksek seviyede bir güvenceye bırakmaktadır[133].

Doğruluk: Bilgi yoğunluğunun fazla olduğu büyük veride, verinin güvenilir veya doğru olması önem arz etmektedir. Verilerin doğru kişiler tarafından görünebilir ve gizli kalması, hangilerinin saklanması veya atılması gibi güvenlik önlemlerinin değerlendirilmesi gerekmektedir[134]. İç denetim ekiplerinin büyük veriden faydalanabilmesi için verinin doğru, tutarlı ve eksiksiz olması gerekmektedir. Bu şartların sağlanabilmesi için sistem yedekleme ve geri yükleme, veriyi kurtarma, erişim kontrolü vb. alanlarla ilgili olan BT denetimi önemli bir yer tutmaktadır. İç denetçilerin, doğru bilgiye ulaşabilmesi için öncelikle bu konularda etkin kontrollerin yer alması ve geliştirilmesi yönünde çaba göstermesi gerekmektedir[135].

Değer: Büyük verinin değeri, verinin kurumlar için ekonomik değer oluşturabilecek bir anlayışa dönüşmesiyle ortaya çıkmaktadır. Büyük verinin değeri, birbirleriyle ilişkili bireyler ve topluluklar hakkında ya da bilginin kendi yapısıyla ilgili veri parçaları arasında bağlantı kurularak ulaşılabilen sistemden elde edilmektedir. Büyük verinin iş süreçlerinde sağlayacağı maliyet, büyük veriden faydalanabilmek için işletmelerin

[131] Suat Atan, **"Veri, Büyük Veri ve İşletmecilik",** Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt.19, Sayı.35, 2017, s.13
[132] Onay, **a.g.m.**, s.142–143
[133] Onay, **a.g.m.**, s.134-135
[134] https://tr.wikipedia.org/wiki/Büyük_veri, (14.05.2020)
[135] Onay, **a.g.m.**, s.143

üstleneceği maliyetten daha fazla olması durumunda büyük veriyi daha değerli bir konuma getirecektir. Büyük verinin, karar verme süreçlerinde anlık olarak etki etmesi ve doğru kararı verebilmek için ulaşılabilir olması, değer bileşeni için önemli bir boyut olarak yerini almaktadır. COVID-19 salgını ile karşı karşıya kalan bir devletin, anlık olarak ülkedeki doktor sayısına, il ve ilçelere göre hasta sayısının dağılımını görebilmesi buna örnek olarak gösterilebilir[136].

Büyük hacme sahip işlemlerin geleneksel yöntemlerle denetlenmesi istenilen sonucu vermeyebilir. Daha verimli sonuçlar elde edebilmek için risk odaklı denetim modellerinin geliştirilmesi gerekmektedir. Bu model sayesinde işletme, mevcut yapısında gerçekleşebilecek hilelerle daha etkin bir şekilde mücadele edebilmektedir[137].

### 2.5.3 Mobil Teknolojiler ve İç Denetim

Bilgisayar teknolojisi ile programlanan ve kontrol edilen akıllı cihazlar iş gücün de "mobil çalışan" kavramına yeni bir anlam getirmiştir. Uzaktan çalışmak, bir zamanlar işletmeler tarafından sağlanan bir dizüstü bilgisayar aracılığıyla işletmenin ağına bağlanmakla sınırlıyken, bugünün seçeneklerindeyse işleri mobil bir şekilde yürütmek için telefonlar ve tabletler bulunmaktadır. Akıllı cihazlar işletmede çalışanlara, wi-fi veya hücresel hizmetin olduğu her yerde hem kişisel hem de iş yerinde kullanabilmek için tek bir cihaza sahip olma imkânı sağlar. Ancak bazı işletmeler çalışanlarına, şahsi olarak kullandıkları akıllı cihazları kullanmalarını -kendi cihazını getirme (BYOD)- söylerken bazıları ise çalışanlarına işletme adına ayrıca akıllı cihaz temin etmektedir. Her iki durumda da işletmeler, akıllı cihazların barındırdığı çok sayıda risk ile karşı karşıya kalmaktadır[138].

İş dünyasında birçok işletme, iş gereksinimlerini daha etkili bir şekilde karşılamak için mobil cihazlar kullanmaktadır. Ancak bu sistemi kurarken ortaya çıkabilecek

[136] Ertuğrul Aktan, **"Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu",** Bilgi Yönetimi Dergisi, Cilt.1, Sayı.1, 2018, s.6-7
[137] Şeref Sağıroğlu ve Orhan Koç, **Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar**, Grafiker Yayınları, 1.Baskı, Ankara, 2017, s.288
[138] GTAG, **"Auditing Smart Device: An Internal Auditor's Guide to Understanding and Auditing Smart Devices",** The Institute of Internal Auditors (IIA), 2016, s.3–4

riskleri de değerlendirmek gerekmektedir. İşletmelerin dikkate alması gereken risklerden bazıları şunlardır[139]:

- Artan bilgi kaybı riski: Çalışanlara teslim edilen akıllı cihazların çalınması ya da kaybolması durumlarda güvenlik riski artmaktadır.
- İzlenme: Günümüzde birçok cihazın karşı karşıya kalabileceği casus ve zararlı yazılımların, yeni nesil teknolojiyle birlikte artık mobil cihazlar için de yapılması riski artış göstermektedir.
- Farkındalık ve iletişim: Çalışanlara sürekli olarak güvenlik uygulamaları konusunda eğitimler vermek, örneğin mobil cihazlar için zayıf şifreler yerine daha güçlü ve güvenilirini kullanmak.
- BT çalışanlarının eğitilmesi: İşletmede çalışan BT çalışanları mobil cihazlar konusunda çok iyi olmayabilirler ve bu nedenle cihazların güncellenmesini takip edemeyebilirler.

İç denetimin, akıllı cihazlarla ilgili riskleri ve kontrolleri değerlendirme yaklaşımı, yeni cihazların da ortaya çıkmasıyla birlikte gelişmektedir. İç denetim faaliyeti, yönetimin akıllı cihazların kullanımıyla ilişkili olan bu riskleri azaltma da etkin bir rol oynamaktadır. Bu doğrultuda iç denetçilerin görevleri şunlardır[140]:

- İşletmenin akıllı cihaz stratejisini anlama,
- Akıllı cihaz teknolojisinin organizasyon üzerindeki etkisinin değerlendirilmesi,
- Akıllı cihaz ortamı için güvence sağlama.

Bu güvenceyi sağlayabilmek için akıllı cihazların kullanımından kaynaklanan risklerin belirlenerek değerlendirilmesi, yönetişim, risk yönetimi ve kontrol yeterliliğinin belirlenmesi ve cihazlarla ilgili kontrollerin etkinliğinin incelenmesi gerekmektedir[141].

[139] Pwc, **"İç Denetimin Gelişen Teknolojideki Yeni Rolü",** s.12
[140] GTAG, **"Auditing Smart Device: An Internal Auditor's Guide to Understanding and Auditing Smart Devices",** s.3–8
[141] GTAG, **"Auditing Smart Device: An Internal Auditor's Guide to Understanding and Auditing Smart Devices",** s.3

### 2.5.4 Sosyal Medya ve İç Denetim

Sosyal medyanın yaygın olarak kullanılmasıyla birlikte şirket çalışanları ve müşteriler arasındaki etkileşimin birçok avantajı bulunmaktadır. Sosyal medya üzerinden işletmeler, kendi reklamlarını herhangi bir ücret ödemeden yapabilme imkânına sahiptir. Ancak bu avantajların işletmelere getirdiği bazı riskleri de bulunmaktadır. İtibar ve marka riski, veri sızıntısı ve güvenlik ile ilgili riskler işletmeler için yüksek risk seviyesindedir. Bu riskler iyi bir şekilde yönetilirse, işletmeye düşük maliyetler ve yeni gelir kalemleri gibi avantajlar sağlamaktadır. Riskler şöyledir[142]:

- Markanın zarar görmesi: Sosyal ağ sayesinde müşteriler, şirketin ürünleri ve hizmetleri hakkındaki yorumlarını paylaşma olanağına sahip olmaktadır. Bu doğru bir şekilde yönetilirse herhangi bir sorun ortaya çıkmayacaktır. Ancak kötü bir şekilde yönetilmesi durumunda şirketin marka imajı zarar görebilir. Örneğin; uluslararası ünlü bir pizza zincirinde yiyecek hazırlama konusunda şaka yapan çalışanlar, Youtube'da bir video yayınlamıştır. Kısa bir zaman sonra video bir milyondan fazla kişi tarafından izlenmiş ve Google üzerinden arama da ilk 10 da görüntülenmiştir.
- Veri kaybı: İşletme çalışanlarının çok sayıda kişiyle bağlantılı olması nedeniyle önemlilik arz eden bilgilerin kaza ile veya kasıtlı olarak dışarıya sızma riski artmaktadır. Çoklu bağlantılar bilgisayar korsanlığı ile müşteri veri kaybına da yol da açabilmektedir.
- Kötü amaçlı yazılımların yayılımı: Sosyal ağlarla artan bağlantı nedeniyle bir sistemin hacklenmesi daha kolay duruma gelebilmektedir. Örneğin, twitter kullanıcılarının hareketleri kısa süre içerisinde popüler hale gelebilmektedir. Hackerlar bu bağlantılardaki URL'leri değiştirerek kullanıcıları kötü amaçlı web sitelere yönlendirmektedir.

PWC'nin Küresel Bilgi Güvenliği Durumu Araştırması'na göre çok az ayıda şirket bu tür risklere karşı yeterince hazırlıklıdır. Çoğu şirket (%60) henüz sosyal ağlar, bloglar gibi Web 2.0 değişimlerini destekleyen güvenlik teknolojileri uygulamamıştır. Ve hatta

[142] Pwc, **"Lights, camera, action... scripting internal audit for a changed world",** s.9–11

daha fazlası (%77) sosyal ağların veya Web 2.0 teknolojilerinin kullanımını ele alan güvenlik politikalarını belirlememiştir[143].

Sosyal medyada işletmelerin uğradığı kazalara bir örnek daha vermek gerekirse; 2017'de McDonald's hızlı bir şekilde kaldırılmasına rağmen retweet edilen ve 1.000'den fazla kez beğenilen bir Trump / Obama karşıtı mesajını tweetledi. Belki de saf bir şekilde, şirket Trump taraftarlarından ve müteakip #BoycottMcDonalds hashtag'inden kaçınılmaz bir tepki beklemiyordu. Bir özür yayınladı ve hesabının saldırıya uğradığını açıkladı. Sosyal medya platformlarından milyonlarca kişiye ulaşmak mümkündür bu sebeple önemli bir pazarlama aracı olarak da görülmektedir. İşletmeler McDonald's gibi olaylar ile karşılaşmamak için pazarlama ve iletişim stratejilerine özen göstermelidir[144].

Ülkemizin nüfusunun yarısından fazlasının internete erişimi bulunmakta ve online deneyimlerin müşterilerin kararlarını önemli ölçüde etkilemektedir. AdAge tarafından yapılan bir araştırmada sonuç olarak tüketicilerin satın alma kararlarında sosyal medyanın tıpkı televizyon reklamları kadar etkili olduğu görülmüştür[145].

İç denetiminin sosyal medya konusunda odaklanması gereken konular şunlardır[146];

- Belirli konulara yönelik politikaların geliştirilmesine yardımcı olmak, teknolojinin getirdiği fırsatları ve riskleri dengelemek,
- Mobil cihazlar için güvenlik politikalarının merkezden yönetilmesini ve uygulanmasını sağlamak ayrıca cihazların kaybolması veya çalınması durumunda cihazların kilitlenmesi veya cihaz içeriğinin silinmesini sağlamak,
- İşletmenin kullanacağı mobil antivirüs yazılımını belirlemek için risk değerlendirmesi yapmak,
- İşletmede bulunan BT politikalarına uyumun izlenmesi,
- Şirketin maliyetlerini en aza indirecek planların yapılmasını sağlamak.

[143] Pwc, **"Lights, camera, action... scripting internal audit for a changed world",** s.12
[144] **"Risk In Focus 2019 Hot Topıcs For Internal Auditors",** The Institute of Internal Auditors Netherlands, European Confederaiton of Institutes of Internal Auditing, 2018, s.24
[145] Accenture, **"Accenture Türkiye Dijitalleşme Endeksi",** 2016, s.22
[146] Pwc, **"Lights, camera, action... scripting internal audit for a changed world",** s.12

### 2.5.5 Siber Güvenlik ve İç Denetim

Teknolojinin yaygın olarak kullanıldığı bu dönemde siber güvenlik birçok kuruluşun odak noktasıdır. Siber güvenlik konusu, sürekli olarak yönetim kurulu gündeminin tepesinde bulunan konuların başında gelmektedir. Siber güvenliğin önemli bir konu haline gelmesini sağlayan bazı faktörler şunlardır[147];

- Veri ihlallerinin maliyetli sonuçlarından kaçınmak
- Müşteri verilerinin kaybolmasıyla ilgili olarak, kurumun itibar kaybının önlenmesi
- İşletme bilgilerinin güvenliğinin sağlanması
- Bilgisayar korsanları tarafından belirli bilgileri ve bireyleri hedef alan fidye yazılımların karmaşıklığı.

Bu bilgisayar korsanları faaliyetlerini doğrudan ağlar üzerinden değil aynı zamanda kilit tedarikçiler ve teknoloji ortaklarıyla bağlantılar sağlayarak gerçekleştirebilmektedir. Siber güvenlik ihlallerinin sonuçları bir kuruluşun karlılığı ve itibarı için çok ağır sorunlar ortaya çıkartabilmektedir. KPMG'nin İsviçre'de bulunan 60 şirkette yaptığı bir araştırma sonucunda şu istatistiklere ulaşılmıştır[148]:

- Siber saldırılara uğrayan şirketlerin %42'si sonuç olarak finansal kayıplara uğramıştır.
- Siber müdahale planlarının %82'si tedarikçilere veya iş ortaklarına yönelik saldırı olaylarını kapsamamaktadır.
- Araştırmaya katılanların işletmelerin yalnızca %28'inde siber sigorta bulunmaktadır.

İstatistiklerden de anlaşıldığı gibi siber saldırganlar dünya genelinde işletmelere çeşitli zararlar verebilmek için aktif olarak çalışmaktadır. Siber saldırılar; finansal sahtekarlık, bilgi hırsızlığı veya bilgiyi kötüye kullanma, bilgisayar sitemlerini çalışamaz duruma getirme, bir işletmenin faaliyet alanındaki altyapı sistemini bozma gibi çeşitli nedenlerle gerçekleştirilmektedir. Bu sebeple iç denetim yöneticileri siber riskleri doğru bir şekilde

[147] KPMG, **a.g.m.**, s.9
[148] KPMG, **a.g.m.**, s.9

belirlemeli ve yönetime destek vermelidir. İşletmelerle ilgili siber tehditleri anlamak için işletme dışındaki tarafların hangi bilgileri değerli gördüğü, işletmede bulunan süreçlerden hangisinin en önemli olduğu ve çalışmaması durumunda ortaya çıkabilecek sonuçları belirlemek önemlidir. Ayrıca hangi bilgilerin dışarıya sızması durumunda finansal veya rekabetçi kayıplara ya da itibar hasarının oluşacağının önceden belirlenmesi işletmeler için önem arz etmektedir. Bu durumların ortaya çıkmasında yer alan bazı bilgiler şunlardır; müşterilerin ve çalışanların verileri, tedarik zinciri, ürün kalitesi ve güvenliği, sözleşmelerin şartları ve fiyatlandırmaları, finansal veriler ve planlamalar[149].

İşletmelerin faaliyet alanları, siber tehditlerin belirlenmesinde önemli değişiklikler göstermektedir. Örneğin; perakendeciler müşteri verilerini korumaya ve müşteri hizmetlerinin kesintiye uğramamasına dikkat etmektedirler. Fikri mülkiyet araştırma ve geliştirmeye odaklanmış kuruluşlar için önemli bir endişe kaynağı olarak yer almaktadır. Üreticiler, üretim ve tedarik zinciri sistemlerinin güvenilirliği ve verimliliğinin yanı sıra ürünlerin kalitesi ve güvenliğine odaklanmaktadır. İç denetim yöneticileri, alana göre farklılıklar gösterebilecek bu riskleri belirleyebilmek ve gereken önlemleri alabilmek için sektörü iyi bir şekilde analiz ederek tanıması gerekmektedir[150].

İşletmeleri siber saldırılardan korumada siber güvenlik uzmanlarının çalışmaları kadar iç denetim ekiplerinin çalışmaları da rol oynamaktadır. Siber güvenlik riski, teknoloji riski olduğu kadar aynı zamanda bir iş riskidir. İç denetim departmanları bu riski yönetmede işletmenin temel yapıtaşı olarak görev almaktadır. İç denetim yöneticileri, işletmelerde siber güvenlik denetimlerinin planlandığı şekilde yürütülmesini sağlamakla birlikte ileriye yönelik ve stratejik düşünce liderliğini sunmaktadır. Siber güvenlik konusunda iç denetim ekiplerinin dikkati dört alanda bulunmaktadır[151]:

- Siber tehditlere karşı hazırlık ve müdahale konusunda güvence vermek,
- Yönetime, kurumun karşı karşıya olduğu risk seviyesini ve mevcut olan bu risklere karşı alınan aksiyonları bildirmek,

[149] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.3–5
[150] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.5–8
[151] **"Küresel Bakış Açıları ve Anlayışlar Yapay Zeka - İç Denetim Mesleğine İlişkin Dikkate Alınması Gerekenler",** The Institute of Internal Auditors, 2017, s.10

- Kuruma yönelik bir siber saldırı gerçekleşmesi durumunda etkili savunma ve müdahale mekanizmasının uygulanabilirliğine yönelik güvence vermek için BT departmanı ile ortak çalışma yürütmek,
- Kurumda mevcut olan risklerle ilgili çalışanlar arasında iletişimi ve iş birliğini sağlamak.

## 2.6 Siber Güvenlikte Üçlü Savunma Hattı

Üçlü savunma hattı, işletmelerin hedeflerine ulaşırken karşılaşabilecekleri risklerin etkili bir şekilde yönetilmesinde kilit rol oynamaktadır. Bu savunma hattının doğru bir şekilde ayrıştırılması ve etkin çalışması, iç denetim faaliyetinin siber güvenlikteki rolünü değerlendirmede önemli bir adım olarak görülmektedir[152]. Bu model işletmede bulunan tüm departmanların birbirleriyle uyum içerisinde çalışmalarını sağlamak bakımından önemli bir koordinasyon görevi üstlenmektedir. Risklere tam ve doğru bir şekilde karşılık verebilmenin ön koşulu bu koordinasyona bağlıdır. İşletmelerde risk yönetimi ve kontrol alanındaki sorumluluklar belirlenirken Üçlü Savunma Hattı modeli bir gösterge (benchmark) olarak kabul görmektedir. Modelin uygulandığı işletmelerde, görev-yetki-sorumlulukların net ve açık olarak belirlenmesi risk yönetimi ve kontrolüne katkı sağlamaktadır. Üçlü savunma hattı işletmelerde birer erken uyarı sistemi olarak görülmektedir[153].

[152] **"IIA Position Paper: The Three Lınes Of Defense In Effectıve Rısk Management And Control",** The Institute of Internal Auditors, 2013, s.2–5

[153] Murat Nail Uzel, Bülent Hasanefendioğlu, Cem Niyazi Durmuş, **"3'lü Savunma Hattının COSO İç Kontrol Sisteminin Etkinliğin Arttırılmasında Kaldıraç Etkisi",** Mali Çözüm Dergisi, İSMMMO, Sayı.136, 2016, s.199–204

**Şekil 17:** Üçlü Savunma Hattı


**Kaynak:** Federation of European Risk Management Associations & European Confederation of Institutes of Internal Auditing, **"At The Junction of Corporate Governance and Cybersecurity",** Cyber Risk Governance Report 2017, s.12

Bağımsız denetçiler, işletmenin yapısı dışarısında olmalarına rağmen kurumun yönetişim ve kontrol çevresinde önemli bir role sahiptirler. Kurumun dışarısında kalan bağımsız denetçiler ile işletme çalışanları arasında etkili ve verimli bir eşgüdüm sağlandığı taktirde üst yönetime ve ilgililere güvence sağlayarak ek bir savunma hattı da ortaya çıkabilmektedir[154].

### 2.6.1 Birinci Savunma Sistemi

Birinci savunma hattını oluşturan yöneticiler, işletmede mevcut olan riskleri üstlenir ve yönetirler. Aynı zamanda süreç ve kontroller ile ilgili eksiklikleri düzeltmeden sorumlu kişiler olarak yer almaktadırlar. Operasyonel yönetim, işletme içerisindeki politika ve prosedürlerin uygulamaya koyulmasında görev aldığı kadar faaliyetlerin işletmenin hedef ve amaçlarına ulaşması yolunda ortaya çıkartabileceği riskleri belirleme, değerlendirme, kontrol etme ve azaltma çabası içerisinde de bulunmaktadır. Yöneticiler, uygulamaya koyulan prosedürlere çalışan personellerin uyup uymadığını gözlemlemektedir. Eğer kontrol eksikliği veya yüksek risk barındıran bir durum ortaya

[154] **"IIA Position Paper: The Three Lınes Of Defense In Effectıve Rısk Management And Control",** s.8

çıkarsa kısa süre içerisinde giderilmeli aksi taktirde raporlanması gerekmektedir[155]. Denetim raporları genellikle birinci savunma hattındaki faaliyetleri incelemek için yapılan çalışmalardan oluşmaktadır[156].

Üçlü savunma hattını siber güvenlik açısından değerlendirdiğimizde: İşletmelerde teknoloji alanında çalışan genel müdür ve yardımcısı, bilgi güvenliği yöneticileri ve bilgi teknolojileri uzmanı olarak çalışanlar siber güvenlikte birinci savunma hattını oluşturmaktadır. Teknolojiden sorumlu genel müdür (CTO), teknolojik gelişmeleri takip ederek işletmenin misyonuna katkı sağlayacak şekilde yönlendirmektedir. Aynı zamanda fikri mülkiyetini koruma görevi de bulunmaktadır. Teknoloji departmanında çalışan diğer personeller ise işletme varlıklarının yeterli seviyede korunması yönündeki çalışmaların başında yer almaktadırlar. Teknoloji birimindekilerin, siber saldırılara karşı mücadele genel müdür ve diğer üst düzey yöneticilerle iş birliği içerisinde faaliyetlerini yürütmesi, siber risklerin belirlenmesinde önemli rol bir oynamaktadır. İşletmeler de birinci savunma hattına yönelik faaliyetler şunlardır[157]:

- Güvenlik prosedürlerinin yönetimi, eğitimi ve testi,
- Konfigürasyonun güvenli araçlarla gerçekleştirilmesi, güncel yazılımların kullanılması ve yamaların yapılması,
- Saldırı tespit sistemlerini kullanmak ve sızma testlerinin gerçekleştirilmesi,
- Ağ trafik akışını doğru şekilde yönetmek ve korumak için güvenilir ağ yapılandırması,
- Bilgi varlıklarının, teknolojik cihazların ve ilgili yazılımların envanteri,
- Verilerin korunması ve kayıpların önlenmesi için programlarının kullanılması,
- Yetki erişiminin doğru yönetilmesi,
- Gerektiğinde verilerin şifrelenmesi,
- İç ve dış taramalarla güvenlik açığı yönetimi uygulamaları,
- Sertifikalı BT, BT riski ve bilgi güvenliği yeteneklerine sahip kişilerin iş alımı.

[155] **"IIA Position Paper: The Three Lınes Of Defense In Effectıve Rısk Management And Control",** s.5
[156] https://www.misti.co.uk/internal-audit-insights/how-internal-audit-can-benefit-from-the-three-lines-of-defence-model, (29.05.2020)
[157] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.6–7

### 2.6.2 İkinci Savunma Sistemi

İkinci savunma hattı, yönetim tarafından belirlenen finansal kontrol, risk yönetimi, uyum kontrolleri, sistem güvenliği gibi fonksiyonlardan oluşmaktadır. Bu fonksiyonlar işletme içerisinde birinci savunma hattındaki risk ve kontrolleri oluşturmaya, gözden geçirmeye ve izlemeye yardımcı olan birimlerdir[158]. İkinci savunma hattı aynı zamanda siber güvenlikle ilgili yönetişim işlevlerinin çoğunun gerçekleştirilmesinden sorumludur. İkinci savunma hattının siber güvenliğe ilişkin sorumlulukları şunlardır[159]:

- Siber güvenlik ile ilgili riskleri değerlendirmek ve bu risklerin işletmenin risk iştihanı uygunluğunu belirlemek,
- Mevcut ve ortaya çıkabilecek riskleri izlemek, yasalardaki ve yönetmeliklerdeki değişiklikleri takip etmek,
- Uygun kontrol tasarımını sağlamak için birinci savunma hattı ile iş birliği içerisinde çalışmak.

Siber güvenlik riskleri, birçok risk türüne göre daha tehlikelidir. Bu nedenle zamanında karşılık verilmez ise işletmede ağır sonuçlar ortaya çıkabilir. İkinci savunma hattı, sürekli gelişen tehdit ortamına karşılık olarak işletmeyi yeterince hazırlamak ve güvence altına almak için kritik öneme sahiptir. Bu aşamada siber güvenlik riskleri ve kontrolleri hakkında yönetim kurullarına farkındalık sağlamak için birinci ve üçüncü savunma hatlarıyla birlikte çalışılması gerekmektedir. İkinci savunma hattında yaygın siber güvenlik faaliyetleri şunlardır[160]:

- Siber güvenlik politikaları, eğitimi ve testinin tasarlanması,
- Siber risk değerlendirmelerinin yapılması,
- Siber tehdit unsuru ile ilgili bilgilerin toplanması,
- Verilerin sınıflandırılması ve erişim izinlerin tasarlanması,
- Anahtar risk göstergelerinin izlenmesi ve gereken iyileştirmelerin yapılması,
- IT alanında sertifikalı kişilerin işe alınması ve devamlılığın sağlanması,

[158] Chartered Institute of Internal Auditors, **"Governance of risk: Three lines of defence",** 2019, s.2
[159] Federation of European Risk Management Associations & European Confederation of Institutes of Internal Auditing **"At The Junction of Corporate Governance and Cybersecurity",** Cyber Risk Governance Report 2017, s.11
[160] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.9–10

- Üçüncü taraflarla, tedarikçilerle ve hizmet sağlayıcılar ile ilişkilerin değerlendirilmesi,
- İş sürekliliği planlarının yapılması ve test edilmesi.

### 2.6.3 Üçüncü Savunma Sitemi

Üçüncü savunma hattı, bağımsız ve nesnel bir güvence sağlayıcısı olarak iç denetim işlevinden oluşmaktadır. İç denetimin amacı yönetişim, risk yönetimi ve iç kontrollerin etkinliğini sağlamaktır. Aynı zamanda birinci ve ikinci savunma hatlarının etkinliğinin değerlendirilmesi üçüncü savunma hattında bulunan iç denetimin görevlerinden biridir[161].

İç Denetçiler Enstitüsü (IIA) Uluslararası Mesleki Uygulama Çerçevesi kapsamında, İç Denetimin misyonu: "riske dayalı, nesnel güvence sağlayarak ve tavsiye ile öngörülerle kurumu geliştirmek ve korumaktır." Bu misyon kurumların siber güvenlik riski ile karşı karşıya kalmaları durumunda da aynı ölçüde uygulanabilmektedir. İç denetim, siber risk yönetim grubu ile koordineli olarak kurumların siber risk yönetim planlarının geliştirilmesi, uygulanması ve değerlendirilmesinde önemli bir rol oynamaktadır.[162] Üçüncü savunma hattı olarak iç denetim, siber güvenlik ile ilgili durumlar söz konusu olduğunda ikinci savunma hattıyla birlikte önemli bir rol oynamaktadır. İç denetim yöneticilerinin, siber güvenlikle ilgili değerlendirmeler yaparken göz önünde bulundurması gereken konulardan bazıları şunlardır[163]:

- Yönetim kurulu ve üst yöneticiler siber güvenlikle ilgili kilit risklerin farkındalar mı? İşletme, içerisinde siber güvenlik girişimleri yeterli destek ve öncelik alıyor mu?
- Yönetim, siber tehditlere veya güvenlik ihlallerine duyarlı varlıkları tanımlamak için bir risk değerlendirmesi yaptı mı ve potansiyel etki (finansal ve finansal olmayan) değerlendirildi mi?

[161] https://www.misti.co.uk/internal-audit-insights/how-internal-audit-can-benefit-from-the-three-lines-of-defence-model, (29.05.2020)
[162] Federation of European Risk Management Associations & European Confederation of Institutes of Internal Auditing, **a.g.m.**, s.18
[163] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.11–15

- Siber güvenlikle ilgili mevcut ve ortaya çıkabilecek olan risklerden, yaygın zayıflıklar ve siber güvenlik ihlallerine karşı güncel kalmak için birinci ve ikinci savunma hatlarıyla iş birliği yapılıyor mu?
- Siber güvenlik politikaları ve prosedürleri mevcut mu ve çalışanlar periyodik olarak siber güvenlik bilinci eğitimi alıyor mu?
- BT süreçleri siber tehditleri tespit etmek için tasarlanmış ve çalışıyor mu? Yönetimin yeterli izleme kontrolleri var mı?
- Üst yönetime ve yönetim kuruluna, işletmenin siber güvenlik programlarının durumu hakkında bilgi vermek için geri bildirim mekanizmaları çalışıyor mu?
- Siber saldırı veya tehdit durumunda yönetimin etkin bir yardım hattı veya acil durum prosedürü mevcut mu? Bunlar çalışanlar ve servis sağlayıcılara aktarıldı mı?
- İç denetim faaliyeti siber tehditleri azaltmak için süreçleri ve kontrolleri değerlendirebiliyor mu yoksa İç denetim yöneticilerinin siber güvenlik uzmanlığı için ek kaynaklar düşünmesi gerekiyor mu?
- İşletme, verileri harici olarak depolayanlar (BT sağlayıcıları, bulut depolama sağlayıcıları) dahil sistem erişimi olan üçüncü taraf hizmet sağlayıcılarının bir listesi tutuluyor mu? Hizmet kuruluşunun denetimlerinin siber güvenlik riski yönetimi programlarının bir parçası olarak etkinliğini değerlendirmek için bağımsız bir siber güvenlik incelemesi yapıldı mı?
- İç denetim, işletmenin karşı karşıya olduğu yaygın siber tehditleri yeterince tanımlamış mı ve bunlar iç denetim risk değerlendirmesine ve planlamasına dahil edilmiş mi?

İşletmeler bu konulara özen gösterdikleri taktirde kurumlarında güçlü yönetişimin temelleri atılmış sayılmaktadır. İç denetim yöneticileri yukarıdaki konuları dikkate alarak siber güvenlikle ilgili kırmızı bayrakları belirleyebilmektedirler. Yönetişim eksikliklerini gösteren kırmızı bayraklardan bazıları; birbirinden ayrılmış yönetişim yapısı, eksik strateji, siber güvenlik çabasının gecikmesidir[164].

[164] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.14

Bir iç denetçi, BT tarafından tanımlanan Penetrasyon testini yeniden yapmak yerine, testin ayrıntılarını gözden geçirerek sonuçlara güvenip güvenemeyeceğine karar verebilir. İç denetçi gerektiğinde, teknik personeli gözlemlemeli ve onlarla yüz yüze görüşmeler gerçekleştirmektedir. Bunun sonucunda siber güvenlik prosedürlerine dahil edilmesi gereken bulgular tespit edilebilmektedir[165]. İç denetim ekiplerinin üçüncü savunma hattındaki faaliyetleri şunlardır[166]:

- Siber güvenlik ile ilgili önleyici ve tespit edici önlemlerin bağımsız bir şekilde gerçekleştirilmesini sağlamak,
- Sorunlu internet adresleri, kötü amaçlı yazılımlar ve veri sızıntıları için erişimi kısıtlı olan kullanıcıların BT varlıklarını değerlendirmek,
- Gerekli olan iyileştirme tedbirlerinin takip edilmesi,
- Hizmet kuruluşlarının, üçüncü tarafların ve tedarikçilerin siber risk değerlendirmelerini gerçekleştirmek, birinci ve ikinci savunma hatları bu sorumluluğu paylaşmaktadır.

## 2.7 Siber Danışmanlar

Güvenilir birer danışman olarak görülen iç denetim yöneticilerinin, siber dünyadaki gelişmeleri ve mevcut riskleri takip etmesi gerekmektedir. İşletmelerin faaliyet alanlarına yeni katılan teknolojik cihazların güvenliğini sağlama konusunda iç denetim yöneticilerinin ekiplerini doğru şekilde yönlendirerek işletmeye destek vermesi beklenmektedir. Siber güvenlik riskinin sıfıra indirilmesi mümkün değildir. Ancak siber danışmanların görevi, bu riski minimum seviyeye indirme oyunu olarak görülmektedir. Saldırganların, "Saray Mücevherleri" olarak adlandırdıkları işletmenin gizli bilgilerine ulaşmasının engellenmesi siber danışmanların amaçlarından biridir[167].

Siber güvenlik riski, iç denetim birimlerinin çoğunun farkında oldukları risk kategorileri arasında bulunmaktadır. Ancak sadece küçük bir kısmı siber güvenlik konularıyla ilgili iç denetim hizmeti vererek bu tür bir riske karşı aksiyon almaktadır.

---

[165] GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** s.13

[166] Federation of European Risk Management Associations & European Confederation of Institutes of Internal Auditing, **a.g.m.**, s.19

[167] The Institute of Internal Auditors, **"Global Perspektifler ve Anlayışlar: Güvenilir Bir Siber Danışman Olarak",** Sayı.4, 2016, s.3–4

Global Nabız'ın anket verilerine göre siber güvenlik hizmeti ile ilgili bazı istatistikler şöyledir[168].

- Siber güvenlikle ilgili iç denetim hizmetlerinin yalnızca %16'sını iç denetim departmanları vermektedir.
- Siber güvenlikle ilgili iç denetim hizmetlerinin %42'sini iç denetim departmanları ve dış hizmet sağlayıcılarının ortak çalışmaları sonucunda ortaya çıkmaktadır.
- Siber güvenlikle ilgili iç denetim hizmetlerinin %16'sı dış hizmet sağlayıcılar tarafından sağlanmaktadır.
- Siber güvenlikle ilgili iç denetim hizmetlerinin %25'i işletmeye siber güvenlikle ilgili hiçbir iç denetim hizmeti vermemektedir.

İç denetim departmanlarının işletmelere, siber güvenlik denetimi hizmetini verememelerinin sebepleri şunlardır[169]:(Ankete katılanlar birden fazla cevap verebilmektedir)

- %65 oranla ilk sırada, iç denetçilerin siber güvenlikle ilgili becerilere ve bilgi birikimine sahip olmaması
- %55 oranla iç denetçilerin siber güvenliği denetlemek için gereken araçlara sahip olmamaları
- %26 oranla iç denetim ekiplerinin, siber güvenlikle ilgili riskleri değerlendirmemiş olmaları
- %22 oranla iç denetimin siber güvenliği denetleyecek zamanı olmaması
- %19 oranla yönetimin, siber güvenliğin denetlenmesi için gereken desteği iç denetime vermemesi

İç denetçilerin siber güvenlik konularından uzak olmalarının sebeplerinden ilki yetkinliklerinin olmamasından kaynaklanmaktadır. Ancak kendilerini bu alanda geliştirerek işletmeler için güvenilir siber danışmanlar konumuna gelmeleri söz konusu olabilir.

---

[168] The Institute of Internal Auditors, **"Global Perspektifler ve Anlayışlar: İç Denetimin Global Nabzı Kanalıyla Sunulan Yeni Trendler",** Sayı.5, 2016, s.13–14

[169] The Institute of Internal Auditors, **"Global Perspektifler ve Anlayışlar: İç Denetimin Global Nabzı Kanalıyla Sunulan Yeni Trendler",** s.15

# 3. SİBER GÜVENLİK DENETİMİ

## 3.1 Siber Güvenlik Denetimi Çerçevesi

Siber güvenlik denetiminin kapsamı[170];

- Şebeke, veri tabanı ve uygulamalara ilişkin veri güvenliği politikaları,
- Veri kaybı önleme tedbirleri,
- Uygulanan etkili ağ erişim denetimleri,
- Dağıtılan algılama / önleme sistemleri,
- Güvenlik kontrolleri (fiziksel ve mantıksal),
- Olaylara müdahale programlarından oluşmaktadır.

Siber güvenlik denetimi ile ilgili amaçlar aşağıdaki şekilde sınırlandırılabilir[171]:

[170] ISACA, **"Cyber Security Audit",** 2017, s.1

- Siber güvenlik politikaları ve prosedürleri ve bunların çalışma etkinliği hakkında bir değerlendirme yaparak yönetime güvence sağlamak.
- Güvenlik kontrollerindeki zayıflıklar nedeniyle kurum verilerinin güvenilirliğini, doğruluğunu ve güvenliğini etkileyebilecek güvenlik kontrolü sorunlarını tespit ederek yönetime rehberlik etmek.
- Yanıt verme ve kurtarma programlarının etkinliğini değerlendirerek kurumsal yaklaşımların içselleştirilmesinde yardımcı olmak.

Güvenlik yeteneklerinin sürdürülmesi ve iyileştirilmesi, siber tehditlerin azaltılmasına ve kuruluşu istenen siber güvenlik olgunluk düzeyine taşımaya yardımcı olabilir. İç denetim, kapsamlı bir siber risk değerlendirmesi gerçekleştirerek, denetim komitesi ve yönetim kurulu üyelerine objektif bakış açıları ve bulgular sunabilir. Ayrıca bu bulguları bir veya birden fazla sayıda kurum için siber risk alanlarını ele alan geniş bir iç denetim planı geliştirmek için kullanabilir[172].

Siber güvenlik denetimleri ve değerlendirme süreçleri, siber güvenliğin başarısında önemli bir rol oynamaktadır. Siber güvenlik denetimlerinin yürütücüleri olarak bilenen iç denetçiler, risk yönetim uzmanları ve işletme yönetimi konumunda olan taraflar detaylı olarak aşağıda açıklanmıştır[173].

a) Yönetim: İşletme hakkında son kararı her zaman yönetim vermektedir. Bu sebeple, işletme yönetimindekiler siber güvenlik kontrollerinin var olması ve etkin bir şekilde çalışması için önemli bir rol üstlenmektedir. Kararların, risk yönetimi süreçleri göz önüne alınarak doğru bir şekilde verilmesi gerekmektedir.
b) Risk Yönetimi: Risk değerlendirmeleri çoğu zaman işletmede bir güvenlik sorumlusunun rehberliğinde gerçekleştirilmektedir. Risk değerlendirmelerinde genellikle iki türlü amaç bulunmaktadır. Risk düzeyinin netleşmesi ve kolay bir şekilde anlaşılabilmesi için risk durumu hakkında toplantı yapılarak ortak bir yaklaşıma varılması önemlidir. İkinci olarak da mevcut olan risklerin ortadan kaldırılması için alternatif yolların belirlenmesi gerekmektedir. Bu sayede hem

[171] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,** s.352
[172] Deloitte, **"Cybersecurity and The Role of Internal Audit: An Urgent Call To Action",** 2017, s.4
[173] Mahmut Sami Öztürk, **"Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi",** Muhasebe ve Vergi Uygulamaları Dergisi, Ankara SMMMO, 2018, s.221–222

problem hem de çözüm yolları belirlenmekte ve işletmeye zarar vermesinin önüne geçilmektedir. Siber güvenlikte riskli alanlar sürekli değişime uğramaktadır. İşletmede güçlü bir siber güvenlik altyapısı oluşturmak için ise yönetim çerçevesine, tanımlanmış süreçlere ve yetenekli siber güvenlik kaynaklarına sahip olmak önemlidir.

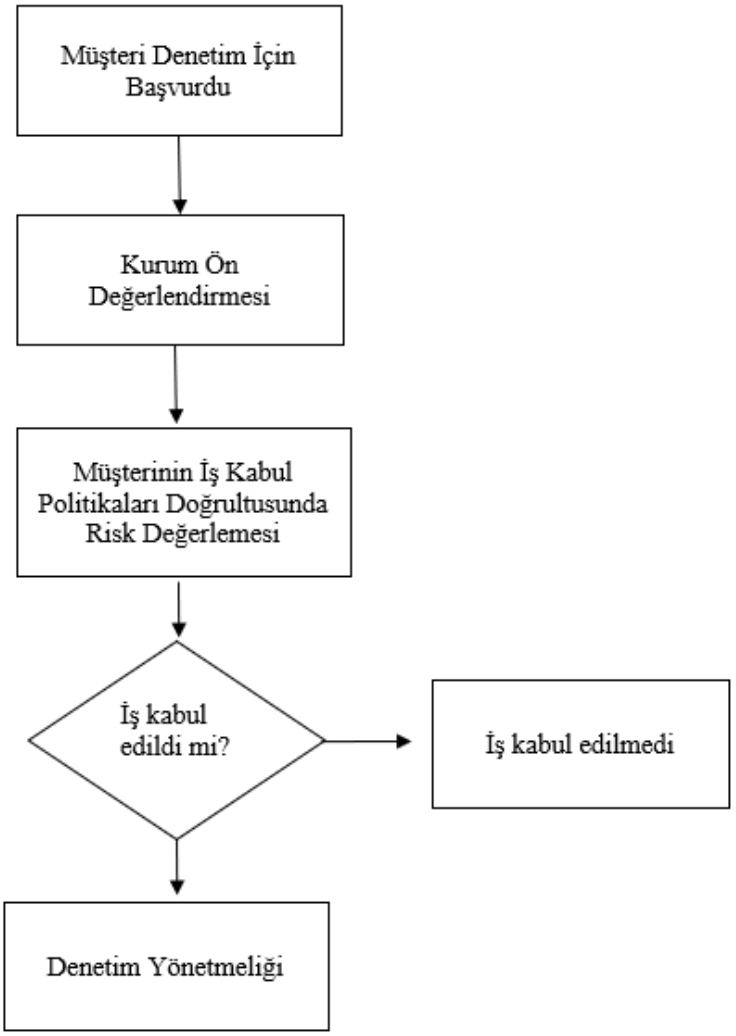
c) İç Denetim: Sürekli olarak gelişmekte olan dijital dünyada işletmeleri korumak kritik önem taşımaktadır. İç denetim departmanları, siber güvenlik denetimleri konusunda çok önemli bir rol oynamaktadır. Aynı zamanda denetim kuruluna işletmenin yönetim kurulu seviyesinde bağımsız bir görüş bildirilmesi için çapraz raporlama ilişkisine sahiptir. Çapraz raporlama ile yönetim kuruluna bilgi verilmekte ve bu doğrultuda denetim kuruluna rapor verilmektedir. Denetim sırasında kontroller objektif bir şekilde değerlendirilmekte ve iyileştirmeler için tavsiyelerde bulunulmaktadır. Aynı zamanda üst yönetim ile yönetim kurulunun siber riskleri anlamasına, bunlarla karşı aksiyon alınmasına yardımcı olmakta ve siber tehditleri yönetme konusunda işletmeye katkı sağlamaktadır.

## 3.2 Risk Değerlendirme Aşaması

### 3.2.1 Müşteri Kabulü

İşletme, sistemlerinin içerisinde yer alan güvenlik açıklarını bulabilmek ve bu doğrultuda aksiyon almak için siber güvenlik denetimi hizmeti veren bir kuruma başvurmaktadır. Siber Güvenlik Denetimi hizmetini verecek taraf, işletmeye yönelik ön inceleme yaparak risk boyutunu belirlemektedir. Hizmeti verecek firma, ön inceleme sonucunda denetimi kabul etmeme durumu söz konusu olabilmektedir.

**Şekil 18:** Denetim Başlangıcı




**Kaynak:** Kamu Gözetim Kurumu, **Müşteri Kabul Denetim Planlaması ve BDS'lerde Ele Alınan Önemli Bazı Alanlar,** s.3-4

Karşılıklı anlaşma sağlandıktan sonra sözleşmenin koşulları belirlenerek denetim sözleşmesi imzalanmaktadır. Taraflar arasından denetim hizmeti verecek şirketin bağımsız olması önem arz etmektedir[174].

### 3.2.2 Denetimin Planlanması

Kurumlar, denetimler yaptırarak etkin operasyonlar gerçekleştirmekte, idari ve yasal düzenlemelere uygunluğunun anlaşılmasına katkı sağlamaktadır. Denetimler sayesinde

[174] Uzay, Özbirecikli ve Selimoğlu, **a.g.e.**, s.143

meydana gelebilecek problemlere kısa sürede karşılık verilmektedir. Etkili bir denetim aynı zamanda kurumun mali operasyonel ve etik refahını korumaktadır. Siber güvenlik denetimleri kurumlardaki bilgi ve ilgili sistemlere odaklanarak tüm bu sonuçları desteklemektedir. Denetimin başarılı bir şekilde gerçekleştirilmesinin anahtarı doğru ve tam olarak planlanmasıyla mümkün olmaktadır. Denetimin kapsamını ve amacını her iki tarafta anlamalı ve kabul etmelidir. Amaç açıkça belirtildikten sonra denetim aşamasına geçmek için ilgili prosedürleri kapsayacak bir denetim planı hazırlanmaktadır. Denetim planının önemli bir bileşeni, çalışma programıdır. Denetim programı, kurumdaki kontrollerin etkinliğini test etmek ve doğrulamak amacıyla kullanılacak prosedürleri ve adımları belgelemek için sık sık kullanılmaktadır. Denetim sonuçlarının tutarlılığı ve kalitesi denetim programına doğrudan bağlıdır. Bu nedenle iç denetçilerin kapsamlı denetim programlarının nasıl geliştirileceğini iyi bir şekilde bilmeleri gerekmektedir. Plan ve program dahilinde siber güvenlik denetiminde, iç denetçilerin yapabilecekleri şöyle sıralanabilir[175]:

- Kurumda mevcut olan güvenlik politikasına, standartlarına, yönergelerine ve prosedürlere uyumun kontrol edilmesi,
- Politika, standartlar, kılavuzlar ve prosedürlerin etkinliğinin incelenmesi ve eksikliklerin tespit edilmesi,
- İlgili yasal, düzenleyici ve sözleşmeye bağlı gerekliliklerin belirlenmesi ve incelenmesi,
- Kurumdaki güvenlik açıklarını tanımlamak,
- Risk stratejisi konusunda tavsiyelerde bulunmak,
- Siber riskleri diğer risklere karşı bağımsız olarak değerlendirilmesi ve önceliklendirilmesi
- Siber riskleri azaltabilmek için kontrollerin etkili bir şekilde çalışmasına yardımcı olmak
- Sürekli değişime uğrayan siber risklerin takip edilmesi,
- Operasyonel, idari ve yönetimsel konulardaki mevcut güvenlik kontrollerinin izlenerek, güvenlik önlemlerinin etkin bir şekilde uygulanmasını sağlamak,

[175] Alptuğ Güler ve Ali Kasım Arkin, **"Siber Hijyenin Sağlanmasında İç Denetimin Rolü",** Denetişim Dergisi, Sayı.19, 2019, s.33

- İyileştirmeler için tavsiyelerde bulunmak.

### 3.2.3 Risklerin Belirlenmesi

Siber Güvenlik Denetimi doğru ve tam bir şekilde planlandıktan sonra denetim sırasında önemli konuların belirlenmesi gerekmektedir. Denetim gerçekleştirilirken kontrollerin nasıl uygulanacağı ve sisteme yönelik var olabilecek tehditler açıkça ortaya konulmalıdır. İşletmelerin kontrolleri sadece iyi bir şekilde tasarlamaları yeterli değildir. Tasarlanan bu kontroller ve araçların güncel olarak da takip edilmesi gerekmektedir. Kontrollerin olmadığı ya da var olan kontrollerin etkili bir şekilde çalışmadığı sistem, içeriden ve dışarıdan gelebilecek tüm tehditlere açık kapı bırakmaktadır[176].

Siber olayların yaşanması kurum içinde finansal, operasyonel, yasal ve itibar üzerinde değişiklik meydana getirmektedir. Kurumların kritik altyapıdaki rolü, bir internet sitesinin potansiyel etkisini de arttırabilir. Siber ihlalin yaşanması durumunda ortaya çıkabilecek olumsuz örneklerden bazıları şunlardır[177]:

- İtibar kaybıyla birlikte hisselerde düşüş,
- Fikri mülkiyet veya ticari sırların kaybedilmesi,
- Gizli veya tüketici kişisel bilgilerin kaybından veya suistimalinden kaynaklanan para cezaları, davalar
- Zaman ve verimlilik kaybı,
- Şirketin imajını düzeltebilmek için halkla ilişkiler kampanyası maliyetleri,

Dolayısıyla bir siber güvenlik denetiminde siber ihlallerin iş süreçlerine etkileri kapsamında risk değerlendirmesi yapılması büyük önem arz etmektedir. Kurumlarda risk stratejisinin belirlenmesi yönetime ait bir karardır. Risklere karşı uygulanan kontroller kurumsal varlıkların korunması yönünde olması gerekmektedir. İşletme yöneticilerinin, ilgili faaliyetini sürdürmesi için gerekli olan gizlilik, bütünlük ve erişilebilirlik kontrollerinin seviyesinin ne şekilde belirleneceği üzerine yönlendirilmesi gerekmektedir[178].

[176] Öztürk, **a.g.m.**, s.227
[177] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,** s.353
[178] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,** s.353–358

## 3.3 Sızma Testi

Sızma testleri, penetrasyon testi olarak da bilinmektedir. Güvenlik testleriyle kötü niyetli şahısların sistemlere yetkisiz erişmesini engellemek ve güvenlik açıkları belirlenerek bunların ortadan kaldırılması hedeflenmektedir. Kurumlar tarafından yapılan testlerin amaçları şunlardır[179]:

- Ortaya çıkabilecek yeni zafiyetlerin tespit edilmesi,
- Tasarım zafiyetlerinin belirlenmesi,
- Kurumun güvenilir olduğuna yönelik bir imaj göstergesi,
- Bilgi güvenliği politikalarının gözden geçirilmesi,
- Bilgi güvenliği sertifikasyonlarına uyumda sürekliliğin sağlanması,
- Etkili ve bilinçli güvenlik yatırımlarının gerçekleştirilmesi,
- Personellerin sorumluluğunun gözden geçirilmesi,
- Sistemlere yapılabilecek saldırı veya saldırılara karşı güvenliğin sağlanması.

Sızma testleri, güvenlik uzmanları tarafından gerçekleştirilmekte olup bilgisayar ağ cihazları, işletim sistemleri, iletişim araçları ve insan faktörü olmak üzere bütün bilişim altyapısını kapsayacak şekilde planlanmaktadır. Test sona erdiğinde sızılan sistemde bulunan zafiyetler ve çözüm önerilerinin bulunduğu sızma testi raporu oluşturulmaktadır. Bu rapor, kurumun sistemlerinin güvenliği hakkında tespitler barındırmakta ve ilgili kişilere iletilmektedir[180]. Rapor, sızma testini yaptıran firmaya 3 farklı rapor şeklinde teslim edilmektedir. Bu raporlar şunlardır[181]:

- Yönetim Raporu: Kuruma yönelik alınacak önemli kararları içeren özet şeklinde hazırlanmış rapordur. Yönetim raporu, başlangıçta yapılan sözleşmeye uygun şekilde tamamlanma durumunu, test sonuçları kapsamında işletmenin genel güvenlik düzeyini, tespit edilen açıklıklarla ilgili yatırımları, sistemde bulunan açıklıkların risk matrislerini içermektedir.
- Teknik Rapor: Tespit edilen açıklıklara yönelik teknik bilgiler içermekte olup çözüm üretmede tavsiyeler verilmektedir. Bu raporda; test sırasında ortaya çıkan

[179] Yılmaz Vural ve Şeref Sağıroğlu, **"Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler",** Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt.26, Sayı.1, 2011, s.91
[180] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** s.439–440
[181] Şahinaslan, **a.g.t.**, s.118–119

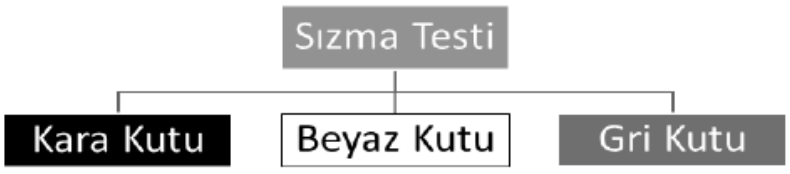
açıklar belirtilmekte olup nedeni, gelebilecek saldırı türü, alınması gereken önlemleri içeren profesyonel tavsiyeler bulunmaktadır. Ayrıca açıklıklara ait ekran görüntüleri, detaylı açıklamaları da yer almaktadır.

- İyileştirilmiş Dış Rapor: Yönetim raporunda ve teknik raporda yer verilen açıklıkların giderilmesi için güvenlik uzmanları iyileştirme çalışmaları yapmaktadır. İyileştirilmiş dış raporda; sızma testi sırasında tespit edilen açıklıkların giderildiğinin anlaşılması amacıyla aynı sistemlerde tekrar sızma testi uygulanmaktadır. Kısacası bu rapor, sistemlerin siber saldırılara karşı dayanıklı olduğunu ortaya koymaktadır.

### 3.3.1 Sızma Testi Türleri

Sızma testleri arasından hangisinin yapılacağına kurumun ihtiyaçlarına göre kurumun kendisi veya testi gerçekleştirecek güvenlik uzmanı karar vermektedir. Kurum yeni bir sistemi, geliştirme aşamasından üretim aşamasına taşıyorsa ve güvenlikle ilgili ayarların doğru bir şekilde yapılıp yapılmadığı konusunda bilgi almak istiyorsa beyaz kutu testini yaptırması yönünde karar çıkacaktır. Ancak güçlü bir güvenlik stratejisi bulunan ve sistemini gerçekleşebilecek her türlü saldırı açısından test ettirmek isteyen bir kurum ise siyah kutu sızma testini yaptırma kararı verilmektedir[182]. Sızma testleri şekil 19'da da görüldüğü gibi kara kutu, beyaz kutu ve gri kutu olmak üzere 3 şekilde gerçekleştirilebilir.

**Şekil 19:** Sızma Testleri




**Kaynak:** Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** s.443

[182] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** s.444

#### *3.3.1.1 Siyah Kutu*

Siyah kutu (Kara Kutu) testinde uzmanların, test edilecek sistem hakkında hiçbir bilgisi bulunmamaktadır. Bu aşamada test uzmanları, aynı birer saldırgan gibi düşünmekte ve hareket etmektedir. Sistemde yer alan güvenlik açıklarını kendi başlarına bulmak için çaba sarf etmektedirler[183]. Siyah kutu sızma testleri çok pahalı ve uzun zaman alacak bir test türüdür. Testin yapıldığı sırada sistemde aksama veya kalıcı hasarlar ortaya çıkabilmektedir. Bu sebeple testi yapacak güvenlik uzmanlarının dikkatli bir şekilde davranmaları gerekmektedir. Test sonucunda ortaya çıkan bulgular test yaptıran şirket için büyük önem taşımaktadır[184].

#### *3.3.1.2 Beyaz Kutu*

Güvenlik testini gerçekleştirecek uzmanlar, kurum içerisindeki yetkili kişiler tarafından bilgilendirilerek tüm sistemler hakkında bilgi sahibi olmaktadır. Beyaz kutu testiyle daha önceden kurumda çalışmış ya da çalışmakta olan şahısların sistemi uğratabilecekleri zararlar tespit edilmektedir. Beyaz kutu testlerinde uygulanan yöntemler, siyah kutu testlerine yaklaştıkça ortaya çıkan sonuçlar sistemin güvenlik açısından büyük bir sorun olduğunu göstermektedir[185].

#### *3.3.1.3 Gri Kutu*

Sızma testini gerçekleştirecek güvenlik uzmanları belirli alan için sistem, uygulama, donanım veya yazılım hakkında birtakım bilgilere sahip olmaları gerekmektedir. Gri kutu sızma testlerinde, ne siyah kutu sızma testindeki gibi hiçbir şey bilmeden ne de beyaz kutu sızma testindeki kadar çok bilgi sahibi olunmaktadır. Bu tür sızma testlerinde belirli bir güvenlik zafiyetini test etmek amaçlanmaktadır. Gri kutu sızma testlerinde, kurumun tamamına yönelik bir zafiyet analizi yerine bir bölgenin veya işlemin güvenlik testi yapılmaktadır[186].

---

[183] Aileen G.Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu ve Monique Joones, **"An overview of penetration testing",** International Journal of Network Security, Vol.3, No.6 2014, s.21

[184] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** s.443

[185] Narmin Mammadova, **Web Yazılımlarında Güvenlik Problemleri Üzerine Araştırma,** İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, 2017, s.24

[186] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** s.444

### 3.3.2 Sızma Testi Aşamaları

Sistemdeki açıklıkların bulunması ve bu açıklıkların kullanılması sonucunda sisteme sızılması hem sızma testini gerçekleştirecek uzmanlar için hem de sızma işlemini yapacak saldırganlar için aynı adımlar ile gerçekleştirilmektedir. İki eylem arasındaki fark ise bir tarafın sistemleri zarara uğratma hedefi varken diğeri ise sistem içerisindeki açıkları kapatmaktır. Sızma testlerinin yürütülmesi aşamasında uygulanması gereken adımlar bulunmaktadır[187].

#### *3.3.2.1 Bilgi Toplama*

Bu aşamada sızma testinin türüne göre bilgi sistemleri hakkında araştırmalar yapılmaktadır. Kurumun içerisinden veya dışarısından internet, intranet, haber siteleri, televizyon ve sosyal mühendislik saldırıları yoluyla detaylı bilgiler alınmaktadır. Kurum içi veya kurum dışından toplanabilecek bilgilere ait örneklerden bazıları şunlardır[188]:

- İnternet (Kurum Dışı): İletişim bilgileri, (Web Adresi, Posta Adresi, Telefon, Faks, E-posta)
- İntranet (Kurum İçi): Kullanılan ağ protokolleri, veri tabanlarının belirlenmesi, güvenlik yazılımlarının tespiti
- Sosyal Mühendislik (Kurum İçi ve Kurum Dışı): Telefon yoluyla ikna, e-posta yoluyla aldatmaca

#### *3.3.2.2 Zafiyet Taraması*

Sızma testlerinde hedefe ulaşabilmek için güvenlik açıklıklarının keşfedilmesi gerekmektedir. Sızma testini yapacak uzmanlar veya sızma işlemini gerçekleştirecek saldırganlar sistemdeki zafiyetleri bulabilmek için güvenlik açığı veri tabanlarını kullanmaktadır. Güvenlik açığı tarayıcıları doğru bir şekilde çalışmasına rağmen çoğu zaman yeterli olmamaktadır. Eleştirel bir tutum sergilenmesi amacıyla burada eylemi

[187] Tuncay Yiğit ve Muhammed Alparslan Akyıldız, **"Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi",** Süleyman Demirel Üniversitesi, Fen Bilimleri Enstitüsü Dergisi, Cilt.18, Sayı.1, 2014, s.15

[188] Vural ve Sağıroğlu, **a.g.m.**, s.9

gerçekleştiren kişinin yorumuna ihtiyaç duyulmaktadır. Bu sebeple zafiyet taraması otomatik olarak yapılabildiği kadar manuel analizi de bünyesinde barındırmaktadır[189].

#### *3.3.3.3 Erişimi Kazanmak ve Sürdürmek*

Güvenlik zafiyetleri belirlendikten sonra sisteme sızma eylemi gerçekleştirilmektedir. Bu aşamada güvenlik zafiyetini doğru bir şekilde istismar ederek hedef sistem içerisinde sürekli yer almak amaçlanmaktadır. Hedefin yalnızca eylemi gerçekleştirenlerin kontrolünde olduğu anlaşılınca sızma işlemi başarılı bir şekilde gerçekleştirilmiştir. Sızma işlemin yapan güvenlik uzmanları ya da saldırganlar bu süreçten sonra sistemde istedikleri gibi hareket edebilmektedir[190].

#### *3.3.3.4 İzleri Temizlemek*

Bu aşamada sızma işlemini yapan güvenlik uzmanları ya da saldırganlar sistem üzerinde yaptıklarının izlerini silmektedir. Güvenlik uzmanları, test süresi bittikten sonra açılan oturumların kullanılmasının önüne geçmek için saldırganlar ise yasal bir suçla karşı karşıya kalmamaları için log(iz) kayıtlarını ortadan kaldırmaktadır. Güvenlik uzmanlarının buradaki amacı sisteme saldırının hangi yöntemlerle ve araçlarla yapılabileceğini göstermek ve yöneticilere farkındalık sağlamaktır[191].

## 3.4 Riske Karşılık Verme

İşletmeler, güvenlik ihtiyaçlarına ve maliyetlerine göre riskleri kontrol altında tutmayı hedeflemektedir. Siber saldırı ve tehditler ile mücadele ederken ve siber savunma yöntemlerini uygularken savunma sistemlerinin efektif ve doğru bir şekilde kullanmaları gerekmektedir. Etkin bir savunma ve korunma mekanizmasının oluşmasını sağlayan siber savunma ve korunma sistemleri aşağıda açıklanmıştır[192].

[189] Georgia Weidman, **Penetration Testing: A Hands On Introduction To Hacking,** 2014, s.9-10
[190] Sağıroğlu ve Alkan, **Siber Güvenlik ve Savunma Problemler ve Çözümler,** s.451–452
[191] Şahinaslan, **a.g.t.**, s.116–117
[192] Çeliktaş, **a.g.t.**, s.47

### 3.4.1 Şifreleme

Dönemin en büyük sorunlarından biri olan güvenli veri alışverişi sırasında gizlilik çok önem taşımaktadır. İletilmek istenen bilgilerin başkaları tarafından kolay bir şekilde erişilmemesi için şifreleme yöntemleri kullanılmaktadır. Bu şifreleme yöntemine kriptoloji ismi verilmektedir. Kriptoloji kelimesi gizleme bilimi anlamına gelmekte ve şifreleme (kriptografi) ve şifre çözme (kriptanaliz) olmak üzere ikiye ayırmaktadır[193].

**Şekil 20:** Şifreleme (Kriptografi) Aşamaları


**Kaynak:** Ayşe Beşkirli, Durmuş Özdemir ve Mehmet Beşkirli, **Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme,** Avrupa Bilim ve Teknoloji Dergisi, 2019

Bilgi şifreleme işlemi yapıldıktan sonra başkalarının anlayamayacağı duruma dönüşmektedir. Şifreyi okuyabilmek için kişilerin elinde şifrenin anahtarları olmak zorundadır. Bu anahtarlar sayesinde şifreli metin düz metin haline dönüşmektedir[194].

Şifreleme işlemleri çok uzun yıllardır askeri ve diplomatik alanlarda iletişim sırasında kullanılmaktadır. Ancak son zamanlarda özel sektördeki işletmelerde şifreleme yoluyla iletişim kurma aşamasına gelmiştir. Sağlık ve finans alanındaki bilgilerin önem derecesi göz önüne alındığında güvenli ve gizli bilgi akışı şifreleme yöntemiyle daha güvenilir bir duruma dönüşmektedir[195].

### 3.4.2 Bal Küpü

Bal küpü (Honeypot), saldırganları üzerlerine çekmek için yöntem olarak kullanılmaktadır. Bal küplerinin asıl amacı saldırıyı gerçekleştirenleri durdurmak değildir. Buradaki görevleri sisteme yetkisiz girişlerin ya da saldırganın kullandığı

[193] Tarık Yerlikaya, **Yeni Şifreleme Algoritmalarının Analizi,** Trakya Üniversitesi, Fen Bilimleri Enstitüsü, 2006, s.2-3
[194] Ayşe Beşkirli, Durmuş Özdemir ve Mehmet Beşkirli,, **"Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme",** Avrupa Bilim ve Teknoloji Dergisi, 2019, s.285
[195] Yerlikaya, **a.g.t.**, s.3

metod ve araçlar hakkında bilgi edinmekte ve tuzak bir sunucu görevi görmektedir. Bal küpleri sayesinde işletmeye yönelik saldırıları gizli bir şekilde izleyerek kaydetmekte ve açıkların tespit edilmesine olanak sağlamaktadır. Bunları yaparken sistemin içerisindeki bilgileri tehdit edici davranışlardan kaçınmaktadır[196].

### 3.4.3 Uç Nokta Güvenliği Sistemi

Uç nokta cihazları, internet üzerinden ağa bağlanan tüm makineleri kapsamaktadır. Her işletmede olması muhtemel masaüstü ve dizüstü bilgisayarları, yazıcıları ve tarayıcıları, tabletleri, akıllı telefonları içerisinde barındırmaktadır. Uç nokta güvenliği sistemiyle ağdaki tüm uç nokta cihazlarının güvenliğinin sağlanması amaçlanmaktadır[197]. Bu sistemle birlikte işletme içerisindeki ağa bağlı cihazların, tek bir merkez üzerinden kontrol edilmesi sağlanarak yönetilebilirliğini kolay bir şekle dönüştüren bütünleşik bir güvenlik sistemidir[198].

### 3.4.4 Steganografi

Steganografi, bilgi gizleme yöntemlerinin önemli bir alt dalı olarak nesnelerin içerisine verinin gizlenmesi olarak tanımlanmaktadır. Ses, video ve resim görüntülerinin üzerine veri saklanabilmektedir. Görüntü dosyalarının içerisine gizlenmiş bir başka görüntü mevcut olmakta kısaca veri içerisine veri gömmektir. Günümüzde gelişen teknolojiyle ve bilginin önem derecesindeki artışla birlikte steganografi kullanımı da hızla yükselmektedir[199]. Steganografi, bilgi saklama sanatı olarak tanımlanmakta ve mesajı gizleyerek ilgili yerlere ulaştırma amaçlanmaktadır. Steganografi'nin kriptografi'den en önemli farkı saklanması istenen mesaj varlığının gizlenmesidir. Saklanan verinin varlığını yalnızca gönderici ve alıcı kişi fark edebilirken başka birisi tarafından anlaşılması mümkün değildir. Kriptografi'de ise verinin gizlendiğini herkes

---

[196] Süleyman Muhammed Arıkan ve Recep Benzer, **"Bir Güvenlik Trendi: Bal Küpü",** Acta Infologica Dergisi, Cilt.2, Sayı.1, 2018, s.2–3

[197] https://www.kaspersky.com.tr/resource-center/preemptive-safety/endpoint-security, (06.12.2020)

[198] Çeliktaş, **a.g.t.**, s.71

[199] Andaç Şahin, Ercan Buluş ve M.Tolga Sakallı, **"24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme",** Trakya Üniversitesi Fen Bilimleri Dergisi, Cilt.7, Sayı.1, 2006, s.17-18

görebilmekte ancak sadece anahtar çözücülerine sahip olan kişiler tarafından anlaşılmaktadır[200].

### 3.4.5 IP Adres Takip Sistemleri

İnternet protokolü (IP) adresi, İnternet'e erişen ağdaki bir bilgisayara veya başka bir cihaza atanan bir numaradır. Bu numara, onu kullanan bilgisayar hakkında genel bir konum hatta sahibinin adı gibi belirli bilgileri açığa çıkarabilmektedir. Suç işleyen suçlular tarafından kullanılan IP adreslerinin bilgi günlüklerini oluşturmak için izleme yazılımı kullanılabilir. IP adresleri gizlenebilmesinden dolayı bu yazılımı kullanmanın başarısı hem onu kullanan kişinin hem de saldırıyı yapan kişinin becerisine bağlı olarak değişmektedir[201].

### 3.4.6 Güvenlik Duvarı

Güvenlik duvarları ağ ortamında iletişimi sağlayan trafiğin istenildiği şekilde ilerlemesinin imkân veren cihazlardan oluşmaktadır. Bir güvenlik duvarı, paketlerin içerisindeki bilgilere bakarak uygun olmayan paketleri düşürür veya güvenliğini sağladığı yerel ağın erişime izin vermektedir. Güvenlik duvarları üzerindeki erişim kuralları sayesinde önceden belirtilen uygunluk kontrolleri test edilmektedir. Erişim kuralları ağ yöneticisi tarafından ihtiyaçlar doğrultusunda değiştirebilmektedir. Değişiklik yapılacağı sırada dikkatli bir şekilde davranılmaz ise gereksiz IP adresleri portlarının erişime açılmasına neden olabilmektedir. Bu durumda güvenlik açıkları meydana çıkmaktadır[202].

## 3.5 Raporlama

Siber güvenlik denetimi sonucunda ortaya çıkan sonuçlar bir denetim raporu ile ilgili kişilerle paylaşılmaktadır. Yapılan denetim neticesinde belirlenen bir güven aralığında güvence verilmektedir. Siber güvenlik denetim güvencesi kurumun siber güvenliğinin

---

[200] Ömer Kurtuldu ve Nafiz Arıca, **"İmge Kareleri Kullanan Yeni Bir Steganografi Yöntemi",** Journal Of Naval Science And Engineering, Vol.5, No.1, 2009, s.108

[201] Ajeet Singh Poonia, **"Audit Tools for Cyber Crime Investigation",** International Journal of Enhanced Research in Science Technology & Engineering, Vol.3, Issue.12, 2014, s.18

[202] Osman Ayhan Erdem ve Ramazan Kocaoğlu, **"Yeni Bir Ağ Güvenliği Yaklaşımı: Dinamik Zeki Güvenlik Duvarı Mimarisi",** Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt.29, Sayı.4, 2014, s.707

boyutu hakkında önemli bilgiler ortaya koymaktadır. Denetim güvencesi ne kadar iyi olursa işletmenin siber güvenlik politikalarının da o ölçüde etkili olduğundan bahsedilebilir. Aynı zamanda dış paydaşlara karşı işletmenin güvenilirliği, imajı ve şeffaflığı ile denetimin doğruluğu, kalitesi ve objektifliği hakkında da bilgi sunmaktadır[203].

Denetim sonuçlarının hızlı bir şekilde raporlanması, şirketin siber tehditlerle kısa süre içinde başa çıkmasına olanak tanımaktadır. Ancak siber saldırılara karşı kesin bir garanti bulunmamakla birlikte koruma düzeyi sadece teknoloji yatırımına bağlıda değildir. Mevcut kaynakları daha etkin bir şekilde kullanarak iç ve dış uzmanlar tarafından bir risk altyapısının geliştirilmesi, yönetimi ve düzenli test edilmesi kilit bir önceliktir. Bir siber güvenlik denetim raporuyla kurumun güvenlik ihlalleriyle karşı karşıya kalma olasılığını keşfetmenin maliyeti, gerçek bir saldırının neden olduğu potansiyel yönetişim, finansal ve itibarla ilgili olumsuz etkiden önemli ölçüde daha düşüktür[204].

[203] Öztürk, **a.g.m.**, s.229–230
[204] Seth Berman, **"Cyber Audits Prerequisite to Good Governance",** Issues.232, 2013, s.6

# 4. SİBER SALDIRI VE SONRASINDA ALINAN AKSİYONLARA YÖNELİK BİR UYGULAMA

Uygulama sırasında yer verilen bilgiler Türkiye'de siber saldırıya uğramış bir şirkete aittir. Gizlilik prosedürü kapsamında şirket hakkında detaylı bir bilgi yer almamaktadır.

## 4.1 Uygulamanın Amacı ve Kapsamı

Özellikle son dönemlerde çok fazla yaygınlaşan siber saldırıların şirketlere verdikleri zararın boyutu çok büyüktür. Bu uygulamayla birlikte bir siber saldırının gerçekleşmesi durumunda ortaya çıkacak zararın boyutlarını en aza indirebilmek için gerekli olan önlemlerin anlatılması amaçlanmıştır. Bu doğrultuda, değerlendirme tablolarında şirketin saldırı öncesi durumu, saldırı sonrası durumu ve mevcutta geliştirilebilecek olan aşamaları yer almaktadır.

Yaşanmış bir Oltalama (Phishing) saldırısı sonrası şirkette alınan aksiyonlara yönelik bir inceleme yapılmıştır. İnceleme sonrasında eksik olarak görülen konulara, öneri başlıkları altında yer verilmiştir.

## 4.2 Siber Saldırı Vakası

Bu konu başlığı altında, yaşanan siber saldırının detaylarına yer verilecektir.

Şirketin Kuruluş Tarihi: 21.06.2015

Siber Saldırı Tarihi: 11.01.2020

Şirkette Çalışan Toplam Personel Sayısı: 480

Şirketin Yer Aldığı Sektör: İlaç

Saldırının Gerçekleşme Yöntemi: Oltalama (Phishing)

Maddi Kayıp: 150.000 $

Şirketteki personellerin aralarında dosya paylaşımı yapabilmeleri, dosyaların muhafaza edilmesi ve mesaj yoluyla iletişim sağlayabilmeleri için bir dokümantasyon programı bulunmaktadır. Bu program içerisinde departmanların birbiriyle iletişimini

gösteren iş akışları, günlük olarak birbirleriyle yaptıkları dosya alışverişleri, şirket prosedürü, görev tanımları vs. tüm bilgiler yer almaktadır. Ayrıca bu bilgiler haricinde sektör gereği ilaçların yapım aşamasında kullanılan formüller, hammaddeler, ilaçların analiz sonuçları ve benzeri gizli dosyaların olduğu bilgilerde yer almaktadır. Dokümantasyon programındaki bu gizli bilgilere her departmanın ulaşabilmesi mümkün değilken biyoteknoloji departmanında çalışan personellerin görevleri gereği yetkileri mevcuttur.

Saldırının gerçekleştiği Biyoteknoloji departmanı, diğer ilaç üretimlerinden farklıdır. Biyoteknoloji departman, hücre bazlı ilaç üretimi yapmaktadır. Normal ilaçlardan farkı diğer ilaçlarda kimyasal hammaddeler kullanılırken Biyoteknolojik ilaçlarda bu mümkün değildir. Biyoteknolojik ilaçlara örnek vermek gerekirse SMA hastalarının kullandığı ilaçlar bu kategoriye girmektedir. Bu tip ilaçları temin edebilmek fiyatı sebebiyle normal ilaçlara göre çok daha zordur.

Saldırı Biyoteknloji departmanında beş ay önce işe başlayan uzman bir personel üzerinden yapılmıştır. Biyoteknoloji bölümünde çalışan personelin e-posta adresine bir mail gelmiştir. Bu mailin içeriğine bakıldığında; mevcutta kullanılan dokümantasyon programına bir güncelleme geldiği ve bu sebeple kullanıcının sistemden çıkartıldığı yazmaktadır. Sisteme tekrar giriş yapılabilmesi için linke tıklanarak tekrar giriş yapılması gerekmektedir. Aynı zamanda programda yapılan güncellemeyle birlikte gelen yenilikleri gösteren dosyanın da ekte olduğu belirtilmiştir. Personel işe de yeni başladığı için ve böyle bir güncellemenin olabileceğini düşünerekten linke tıklayarak kullanıcı adı ve şifresiyle programa girişini yapmıştır. Her zaman giriş yapılan ekran olduğu düşünülen bu sitenin alan adının başlangıcı aynıyken son kısmındaki farklılık dikkat çekmemiştir. Onun haricinde internet sayfasının görüntüsünde hiçbir farklılık bulunmamaktadır. Personel sisteme giriş yapmış ancak kullanıcı adı ve şifresi artık tuzak kuran siber saldırganların eline geçmiştir. Saldırganlar sistemin içine sızmış ve bütün dokümantasyonlara ulaşma imkanına sahip olmuştur. Ancak bu durum şirket içerisinde hemen farkına varılamamıştır. Saldırganlar program içerisinde yer alan tüm dokümanları kopyaladıktan sonra sistemi kullanılamaz durumda getirmişlerdir. Programda çalışan tek kısım olarak iletişim kurulabilmesi amaçlı mesaj kutusudur. Saldırganlar uzun süre sistem içerisinde kalmış ve şirketin içeride aldığı yedeklerin

tamamına da ulaşabilmiştir. Şirketin dışarısında bir yedek tutmamaları şirkete büyük zarar vermiştir.

Sistemin çökmesi sonucunda şirket bünyesinde çok büyük iki problem ortaya çıkmıştır. Birincisi gizli olan ilaç formüllerinin yayınlanması, diğeri ise ilaçların üretimine devam edilebilmesi için ihtiyaç olan formüllerdir. Bu formüller olmadan şirketin Biyoteknoloji departmanı tarafından üretilen hücre bazlı ilaçların üretilmesi mümkün değildir. Program çökertildikten sonra saldırganlar mesaj yoluyla şirket çalışanlarıyla iletişim kurmuştur. 150.000 $ karşılığında tüm dosyaların verileceği saldırganlar tarafından iletilmiştir. Verileri tekrar alabilmek için çeşitli yollar aransa da saldırganların dediğini yapmaktan başka çare olmadığı anlaşılmıştır. Bu süreçten sonra saldırganlar ile iletişime geçilmiş ve ödemenin yapılacağı bilgisi aktarılmıştır. Ancak bilgilerin tekrar alınabilmesi için bir garanti bulunmamaktadır. Bu sebeple saldırganlar biraz olsun iyi niyetli olduklarını gösterebilmek amacıyla bir kısım dosyaları program üzerinden erişime açmıştır. Ancak bu dosyalar ilaç formüllerin olduğu bilgileri kapsamamaktadır. Saldırganlar ödeme takibinin yapılamaması için kripto para ile ödemenin yapılmasını istemiştir. Bu durum saldırganların profesyonel bir şekilde çalıştıklarını göstermektedir. Sonuç olarak ödeme yapılmış ve iki gün içerisinde programdaki dosyalar şirkete iade edilmiştir. Ancak saldırganlarda bir yedeğin olup olmadığı ve herhangi bir zamanda bunu yayınlamayacakları bilgisi mevcut değildir. Bu sebeple şirket üretimine devam etse de üst yönetimdekilerin kafasında bir soru işareti olarak kalmıştır.

## 4.3 Durum Değerlendirme Tabloları

IT Bölümü ve İnsan Kaynakları Bölümü ile görüşülmüş olup firmadan alınan bilgiler tablolarda yer almaktadır. Saldırı gerçekleşmeden önceki ve gerçekleştikten sonraki duruma yönelik bilgileri aynı zamanda önerileri de gösteren tablolara aşağıda yer verilmiştir:

| **1. Çalışanlara siber güvenlik konusuyla ilgili bir farkındaklık eğitimi verildi mi?** | |
|---|---|
| **Saldırı Öncesi Durum** | Şirket personellerine yönelik çeşitli eğitimler verilse de siber güvenlik konusuyla ilgili bir eğitim içeriden veya dışarıdan verilmediği görülmüştür. |
| **Saldırı Sonrası Durum** | Siber olaylar ile nasıl mücadele edileceğine yönelik bir eğitim henüz verilmemiştir. IT Bölümü tarafından verilmesi düşünülmektedir. |
| **Risk ve Öneri** | Siber güvenlik riskine karşı personellerin farkındalık kazanması kurumun saldırıya uğrama riskini de azaltacaktır. Siber güvenlik her departmanı ilgilendiren bir konu olduğu için personellere farkındalık eğitimi verilmelidir. Bu doğrultuda üst yönetimin, personellerin yaptıkları işin önemlilik seviyesini düşünerekten hareket etmeleri gerekmektedir. |

| 2. Meydana gelebilecek siber saldırılara karşı sigorta bulunmakta mıdır? | |
|---|---|
| **Saldırı Öncesi Durum** | Siber saldırılara karşı bir sigorta yapılmamıştır. |
| **Saldırı Sonrası Durum** | Saldırı sonrasında yaşanılan kayıpların önüne geçebilmek amacıyla şirket bünyesinde bir siber güvenlik sigortası yaptırılmıştır. Ancak bu sigortanın kapsamı çok dar olarak ele alınmıştır. |
| **Risk ve Öneri** | Siber güvenlik sigortasının, verilerin kaybedildiğinde ortaya çıkabilecek zarardan daha yüksek bir maliyeti bulunmamaktadır. Bu doğrultuda yapılan siber güvenlik sigortasının kapsamı genişletilmeli ve tam ölçekli bir sigorta yaptırılmalıdır. |

| 3. Şirkette teknolojik açıdan zafiyetlerin görülebilmesi için sızma testi yapıldı mı? | |
|---|---|
| **Saldırı Öncesi Durum** | Daha önce şirkette böyle bir çalışma yapılmamıştır. |
| **Saldırı Sonrası Durum** | Şirketin üst yönetimi, bu hizmeti veren dışarıdan bir firma ile anlaşarak sızma testi yaptırmıştır. Yapılan sızma testleri sonucunda sistem içerisinde çok fazla zafiyet ortaya çıkmıştır. Ortaya çıkartılan bu zafiyetlerin büyük bir kısmı ortadan kaldırılırken bazıları ise beklemektedir. Bekleme sebebi olarakta zafiyetin ortaya çıkartacağı sonuçların çok büyük etki etmeyeceği düşünülmekte ve bazı şeylerin tamamen değişmesi bu doğrultuda da büyük maliyet ortaya çıkacağıdır. |
| **Risk ve Öneri** | Sızma testini yapan personellerin, sistemlerin içerisidenki zafiyetleri ortaya çıkarması sonucunda benzer saldırıların tekrar etmesini önlemek amaçlanmaktadır. Ortaya çıkartılan bu zafiyetlerin bir kısmı mevcut sistemler üzerinde beklemektedir. Siber saldırganlar sistemlerde yer alan en ufak bir zafiyetten dahi faydalanabilmektedir. Küçük denilen zafiyetler saldrıganlar tarafından tespit edilmesi durumunda beklenen etkiden fazlasını ortaya koyabilmektedir. Bu nedenle en kısa sürede tüm zafiyetler ortadan kaldırılmalıdır. |

| **4. Şirket içerisinde önemli bilgilere yönelik şifreleme politikaları uygulanmakta mıdır?** | |
|---|---|
| **Saldırı Öncesi Durum** | Önemli olduğu düşünülen tüm bilgiler dokümantasyon programında tutulmaktadır. Bu programa girebilmek için şifre ve kullanıcı adı girmek gerekse de ek olarak gizli dosyalara ait bir şifreleme politikası uygulanmamıştır. |
| **Saldırı Sonrası Durum** | Saldırı sonrasında güvenlik önlemleri arttırılsa da şifreleme politikalarına yönelik sistem üzerinde ek bir şey yapılmamıştır. Bunun yerine çok yüksek seviyede önemlilik arz eden bilgiler sistem üzerinde tutulduğu gibi manuel olarak dosyaların içerisinde de gizli bir alanda saklanmaktadır. |
| **Risk ve Öneri** | Şifreleme(Kriptografi) işlemi yapıldığında dosya içerisinde yer alan bilgiler başkalarının anlayamacağı bir şeye dönüşmektedir. Anlaşılmayacak duruma gelen bu dosyaların düzelebilmesi için dosyayı bozan kişilerin elindeki şifreleme anahtarlarının olması gerekmektedir. Bu anahtarlar sayesinde şifrelenen metin okunabilecek duruma dönüştürülebilmektedir. |

| 5. Beklenmedik bir durum ile karşılaşılması durumunda aksiyon planı mevcut mudur? | |
|---|---|
| **Saldırı Öncesi Durum** | Acil durum planı bulunmamaktadır. |
| **Saldırı Sonrası Durum** | Üst yönetim, saldırı sonrasında doğrudan IT Bölümü personellerinden bilgi almak istemiştir. IT Bölümü de durumu nasıl kurtarabileceği üzerine araştırmalar yapmakta ancak daha önceden nasıl bir yol izleneceğine yönelik bir planlama yapılmadığı için süreç olması gerekenden daha yavaş bir şekilde ilerlemiştir. |
| **Risk ve Öneri** | Acil durum nedeniyle işletme faaliyetleri olağan olmayan bir şekilde aksayabilir. Bu sebeple yazılı bir acil durum planı hazırlanması önerilmektedir.<br>- Yazılı acil durum planı tüm ilgili kişilere dağıtılmalıdır.<br>- Olağanüstü bir durumda hangi mekanlardaki hangi yedek sunucuların devreye gireceği belirlenmelidir.<br>- Planda yüksek riskli ve öncelikli alanlar olasılık, finansal etkiler ve diğer sonuçları yönlerinden tespit edilerek bu doğrultuda önlem alınmalıdır. |

| 6. İşletmede kullanılan programların tümünde log kayıtları tutulmakta mıdır? | |
|---|---|
| **Saldırı Öncesi Durum** | İşletme içerisinde kullanılan programların tamamında log kayıtları tutulmaktadır. |
| **Saldırı Sonrası Durum** | Saldırı sonrasında log kayıtlarına ulaşılarak saldırının nereden ve kim tarafından gerçekleştirildiği araştırılmaya çalışılmış ancak bir sonuca varılamamıştır. |
| **Risk ve Öneri** | Log analizleri sayesinde şirkete yapılan bir saldırı çok kısa süre içerisinde tespit edilebilir. Şirketlerin çoğunda log kayıtları tutulmakta ancak analizi yapılmamaktadır. Analizi de yapılmadığı için saldırı sonradan fark edilmiştir. Bu sebeple güçlü bir bilişim altyapısı kurulmalı ve log analizleri de yapılmalıdır. Aksi taktirde bir başka saldırı yaşanması durumunda tespit etmek yine mümkün olmayacaktır. |

| 7. Uzaktan çalışma ve uzaktan erişime ilişkin güvenlik prosedürleri belirlenmiş midir? | |
|---|---|
| **Saldırı Öncesi Durum** | VPN kullanımına yönelik prosedür belirlenmiştir. Dışarıdan bir firmadan VPN kullanımı için hizmet alınmaktadır. |
| **Saldırı Sonrası Durum** | Saldırı gerçekleştikten sonra bu konuyla ilgili herhangi bir aksiyon alınmamıştır. Dışarıdan hizmet alınmaya devam edilmektedir. |
| **Risk ve Öneri** | VPN kullanımı için dışarıdan bir hizmet alınmaktadır. Ancak bu hizmeti dışarıdan almak şirketi dışarıdan birilerine açmak anlamına da gelmektedir. VPN'e bağlandıktan sonra içeride yapılan işlemlerin ne kadarı takip edilmekte olup olmadığı çoğu zaman bilinememektedir. Bu nedenle şirket içerisinde yetkili bir personel tarafından şirketin kendi VPN ağı kurulması daha doğru olacaktır. Tüm kontrol şirket içerisinde bulunacak ve içerik olarak dışarıya bilgi çıkmayacaktır. |

| 8. Yedekleme ve kurtarma ile ilgili şirket içerisindeki durum nedir? | |
|---|---|
| **Saldırı Öncesi Durum** | Belirli sürelerle yedekleme yapılmaktadır. Aynı zamanda yedeklenen veriler düzenli aralıklarla kontrol edilmektedir. |
| **Saldırı Sonrası Durum** | Saldırı gerçekleştikten sonra şirket yetkilileri, verileri geri getirebilmek amacıyla İngiltere ve ABD'deki bazı firmalar ile iletişime geçmiştir. Gerekli görüşmeler yapılmış olsa da bir sonuca varılamamıştır. |
| **Risk ve Öneri** | Bilgilerin dışarıda bir yerde daha tutulmaması büyük bir sorun teşkil etmiştir. Bu nedenle en kısa süre yedeklenen verilerin dışarıda da muhafaza edilmesi gerekmektedir. Bir daha böyle bir saldırı yaşanması durumunda en azından dışarıdan verilerin geri getirilmesi sağlanabilir. |

| 9. Şirkette flash bellek kullanımına yönelik bir kısıtlama veya |
|---|

| yasaklamaya yönelik bir uygulama bulunmakta mıdır? | |
|---|---|
| **Saldırı Öncesi Durum** | Şirkette flash bellek kullanımıyla ilgili bir kısıtlama veya yasaklama uygulaması bulunmamaktadır. |
| **Saldırı Sonrası Durum** | Saldırı sonrasından flash bellek kullanımına yönelik bir sınırlandırma getirilmek istenmiştir. Ancak şirket içerisinde bazı işlerin hızlı bir şekilde ilerlemesini engelleyeceği yönünde görüş ortaya çıkmıştır. Bu sebeple de şirkette flash bellek kullanımına yönelik prosedür yayınlanmıştır. Prosedür içeriğine bakıldığın da: flash belleklerin bilgisayara takıldığında ilk olarak virüs taraması yapılması gerektiği, kime ait olduğu belli olmayan flash belleklerin bilgisayara takılmaması gerektiği, flash bellek içerisindeki dosyaların şifrelenmesi gibi kurallar yer almaktadır. |
| **Risk ve Öneri** | Saldırı sonrasında flash bellek kullanımıyla ilgili prosedür yayınlanmış olsa da bu kurallara uymayan personeller olabilmektedir. Bu durumu fark eden kötü niyetli kişi veya kişiler flash bellek aracılığıyla sisteme sızabilmektedir. Bu sebeple şirket içerisinde flash bellek kullanımı tamamen yasaklanabilir. Bilgisayar ortamında bir ortak alan oluşturularak departmanlar arası dosya paylaşımı oradan yapılabilir. Yalnızca ilgili kişilerin dosyaya erişimi istenmesi durumunda ise dosya şifrelenerek ilgili kişiyle şifresi mail yoluyla paylaşılabilir. Bu sayede flash bellek yoluyla şirketteki sistemlere dışarıdan bir sızma hareketi kesin olarak engellenmiş olur. Aynı zamanda bir önceki tabloda bahsedilen e-imza uygulamasıyla giriş yalnızca ilgili kişilerin ulaşabilmesi istenen dosyalar için de yapılabilir. |

# SONUÇ

Siber güvenlik geçmişte çok fazla gündem konusu olmazken günümüzde ise çok yaygınlaşmıştır. Bunun sebebi olarak da teknolojik gelişmeler görülmektedir. Bu doğrultuda şirketler siber güvenlik risklerini çok iyi bir şekilde anlamalı ve aksiyon planlarını ona göre yapmalıdır.

Gelişen ve değişen teknolojik dünya üzerinde iç denetçilerin görevleri de değişiklik göstermektedir. İç denetçiler, mesleki anlamda kendilerini geliştirebilmek adına güncel konuları takip etmelidir. Şirketlerin güvenilir danışmanları arasında görülen iç denetçilere duyulan saygı genellikle çok fazladır. Bunun en önemli sebebi olarak henüz gerçekleşmemiş olaylara karşı riskleri belirleyip şirketlerin aksiyon almalarını sağlamalarıdır.

Her ne kadar birçok üst yönetici tarafından siber güvenlik konusu önemli olarak görülmese de saldırıya uğradıktan sonra bu görüş değişiklik göstermektedir. Bu sebeple saldırı meydana gelmeden önce durumun farkına varılması gerekmektedir. Bu farkındalığı sağlamada en önemli aktör iç denetçilerindir. Şirketlerin karşı karşıya oldukları riskler analiz edilirken siber güvenlik çerçevesi de değerlendirilmelidir. Türkiye'deki iç denetçiler siber güvenlik konularına çok vâkıf değilken yurtdışında ise daha fazla söz hakkına sahiptir. Bunun sebebi Türkiye'deki birçok iç denetçinin siber güvenlik hakkında çok fazla bilgi sahibi olmamasıdır. Ancak ilerleyen süreçte Türkiye'de de bu durum değişecektir.

Türkiye'deki firmalara bakıldığında ya bünyesinde bir siber saldırı olayı yaşanmış ya da çevresinde yaşanmış olan şirketlerin güvenlik tedbirleri konusunda daha güçlü olduğu görülmüştür. Ancak saldırı gerçekleştiğinde şirketler hem itibar kaybına hem de maddi kayıplara uğramaktadır. Çok büyük boyutlarda maddi kayıplar verilmediği sürece şirketler genellikle faaliyetlerine devam ederken itibar kaybına uğrayan şirketlerde bu durum böyle değildir. İtibar kaybına uğrayan şirketlere olan güven sarsıldığında müşteri açısından eğer alternatif bir firma varsa oraya yönlenmektedir. Saldırıya uğrayan şirketlerin güçlü bir alt yapısı yoksa itibar kaybının getirdiği kazançtaki düşüş ile kısa sürede iflas etmektedir. Bu yüzden maddi kayıpların yeniden kazanılması yakın zamanda mümkünken itibar kaybı şirketlerin sonunu getirmektedir.

Yeterli seviyede güvenlik tedbiri alınmayan sistemlerin saldırganlar tarafından ele geçirilmesi çok kolaydır.

Şirketler siber güvenlik denetimi yaptırarak sistemlerinde mevcut zafiyetleri tespit etmelidir. Bu doğrultuda tespit edilen zafiyetlerin analizi yapılmalı ve en kısa süre içerisinde giderilmelidir. Daha önce sistemlerin güvenliğiyle ilgili bir analiz yaptırmayan şirketlerde birden fazla zafiyet ortaya çıkmaktadır. Bu zafiyetlerin giderilmesi kimi zaman maddi açıdan çok kolay olsa da büyük yatırım gerektiren zafiyetlerde vardır. Tespit edilen zafiyetler arasından yakın zamanda giderilmesi düşünülmeyenlerin siber saldırı sırasında verebileceği zarar düşünülmelidir. Genellikle siber saldırıların etkisi daha büyük sonuçlara yol açacağı düşünülse de üst yönetimdeki kişiler henüz gerçekleşmemiş ve gerçekleşme ihtimalini de düşük gördükleri için büyük maddi yatırımlar yapmaktan kaçınmaktadır. Ancak siber güvenlik denetimi ve önlemleri konusunda maddi yatırım yapmaktan kaçınan üst yöneticiler, şirketlerinde bir güvenlik ihlali yaşandığında ne kadar yanlış bir yol izlediklerini daha rahat görmektedir.

# KAYNAKÇA

***Kitaplar***


Akarslan, Hüseyin. **Bilişim Suçları,** Seçkin Yayıncılık, Ankara, 2012.

Bozkurt, Nejat. **Muhasebe Denetimi,** Alfa Yayıncılık, 7.Baskı, İstanbul, 2015.

Büyükçapar, Olcay. **Bilişim Teknolojileri ve Yazılım**, Kodlab Yayıncılık, İstanbul, 2018.

Flick Tony ve Justin Morehouse. "Threats and Impacts: Utility Companies and Beyond", **Securing The Smart Grid Next Generation Power Grid Security** içinde (35-48), 2011.

Carr, Jeffery. **Inside Cyber Warfare: Mapping the Cyber Underworld,** 1.Baskı, 2010.

Çakmak, Haydar ve Tamer Altunok. **Suç Terör ve Savaş Üçgeninde Siber Dünya,** Barış Platin Kitabevi, Ankara, 2009.

Çubukçu, Faruk. **Bilgi Güvenliği Yönetim Sistemi ISO 27001: 2013 Uygulama Kılavuzu**, Pusula 20 Yayıncılık, 1.Baskı, İstanbul, 2018.

Gantz, Stephen. **The Basics of IT Audit Purposes, Processes, and Practical Information,** 2014.

Gürbüz, Hasan. **Muhasebe Denetimi,** Bilim Teknik Yayınevi, 4.Baskı, İstanbul, 1995.

Güredin, Ersin. **Denetim**, Beta Basım Yayım, 10.Baskı, İstanbul, 1998.

Gökçen, Gürbüz, Başak Ataman, Cemal Çakıcı. **Türkiye Finansal Raporlama Standartları Uygulamaları,** Beta Yayıncılık, 2.Baskı, İstanbul, 2016.

Miller, Michael. **PC Güvenliği ve Bilgisayar Virüsleri,** Alfa Basım Yayım, 2003.

Özbek, Çetin. **İç Denetim Kurumsal Yönetim Risk Yönetimi İç Kontrol,** 2012.

Pehlivanlı, Davut. **Modern İç Denetim Güncel İç Denetim Uygulamaları,** Beta Yayınları, 2.Baskı, İstanbul, 2014.

Sağıroğlu, Şeref ve Mustafa Alkan. **Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık,** BGD Siber Güvenlik ve Savunma Kitap Serisi 1, Grafiker

Yayınları, 1.Baskı, Ankara, 2018.

Sağıroğlu, Şeref. **Siber Güvenlik ve Savunma Standartlar ve Uygulamalar,** BGD Siber Güvenlik ve Savunma Kitap Serisi 3, Grafiker Yayınları, 1.Baskı, Ankara, 2019.

Sağıroğlu, Şeref ve Mustafa Alkan. **Siber Güvenlik ve Savunma Problemler ve Çözümler,** BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, 1.Baskı, Ankara, 2019.

Sağıroğlu, Şeref ve Orhan Koç. **Büyük Veri ve Açık Veri Analitiği: Yöntemler ve Uygulamalar,** Grafiker Yayınları, 1.Baskı, Ankara, 2017.

Sandro, Gaycken ve Martellini Maurizio. **Cyber Security: Deterrence and IT Protection for Critical Infrastructures,** 2013.

Türkiye İç Denetim Enstitüsü. **Uluslararası İç Denetim Standartları Mesleki Uygulama Çerçevesi (2007'deki Değişikliklerle),** 2008.

Uzay, Şaban, Mehmet Özbirecikli, Seval Kardeş Selimoğlu. **Bağımsız Denetim,** Nobel Akademik Yayıncılık, 2.Baskı, 2017.

Yurdakul, Didem Doğmuş. **"Avrupa Birliği'nde İç Denetim Sistemi: Üye Ülke Uygulamaları",** H. Kıral içinde, İç Denetim, İç Denetim Koordinasyon Kurulu, Ankara, 2014.

Weidman, Georgia. **Penetration Testing: A Hands On Introduction To Hacking**, 2014.

***Süreli Yayınlar***

Akyazı, Uğur. **"Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler",** 6.Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 2013.

Aktan, Ertuğrul. **"Büyük Veri: Uygulama Alanları, Analitiği ve Güvenlik Boyutu",** Bilgi Yönetimi Dergisi, Cilt.1, Sayı.1, 2018.

Aslan, Bayram. **"Bir Yönetim Fonksiyonu Olarak İç Denetim",** Sayıştay Dergisi, Sayı.77

Atan, Suat. **"Veri, Büyük Veri ve İşletmecilik",** Balıkesir Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Cilt.19, Sayı.35, 2017.

Aileen G.Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Joones. **"An Overview of Penetration Testing",** International Journal of Network Security, Vol.3, No.4, 2014.

Bağcı, Hasan. **"Sosyal Mühendislik ve Denetim",** Denetişim Dergisi, Kamu İç Denetçiler Derneği, Sayı.1, 2016.

Beşkirli, Ayşe, Durmuş Özdemir, Mehmet Beşirli. **"Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme",** Avrupa Bilim ve Teknoloji Dergisi, 2019.

Canbek, Gürol ve Şeref Sağıroğlu. **"Kötücül ve Casus Yazılımlar: Kapsamlı bir Araştırma",** Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt.25, Sayı.1, 2007.

Christopher, Haley. **"A Theory of Cyber Deterrence"**, Georgetown Journal of International Affairs, 2013.

Cömert, Nuran. **"İşletmelerde Kontrol ve Denetim Kavramlarının Doğru Kullanılması amacına Yönelik Kavramsal Bir İnceleme",** Marmara Business Review, Cilt.1, Sayı.1, 2016.

Çeliktaş, Barış ve Soner Çelik. **"Güncel Siber Güvenlik Tehditleri: Fidye Yazılımlar",** Cyberpolitik Journal, Cilt.3, Sayı.5, 2018.

Doğanyiğit, Mehmet. **"Pilot İç Denetimlerin Gerçekleştirilmesi Projesi",** Denetişim

Dergisi, Kamu İç Denetçiler Derneği, 2010.

Doğu, Emin. **Siber Güvenlik Çağı,** Natro Hosting Dergisi, Sayı.3, Ocak 2015.

Dülger, Ümit. **"Büyük Veri Nedir ?",** Yeni Türkiye Dergisi, Yeni Türkiye Stratejik Araştırma Merkezi, Sayı.89, 2016.

Erdem, Osman Ayhan ve Ramazan Kocaoğlu. **"Yeni Bir Ağ Güvenliği Yaklaşımı: Dinamik Zeki Güvenlik Duvari Mimarisi",** Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt.29, Sayı.4, 2014.

GTAG, **"Assessing Cybersecurity Risk: Roles of the Three Lines of Defense",** The Institute of Internal Auditors (IIA), 2016.

GTAG, **"Auditing Smart Device: An Internal Auditor's Guide to Understanding and Auditing Smart Devices",** The Institute of Internal Auditors (IIA), 2016.

Güler, Alptuğ ve Ali Kasım Arkin. **"Siber Hijyenin Sağlanmasında İç Denetimin Rolü",** Denetişim Dergisi, Sayı. 19, 2019.

Gürkaynak, Muharrem ve Adem Ali İren. **"Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler",** Süleyman Demirel Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Dergisi, Cilt.16, Sayı.2, 2011.

Kurtuldu, Ömer ve Nafiz Arıca. **"İmge Kareleri Kullanan Yeni Bir Steganografi Yöntemi",** Journal of Naval Science and Engineering, Vol.5, No.1, 2009.

Kiracı, Murat. **"Faaliyet Denetimi ile İç Kontrol İlişkisi",** Osmangazi Üniversitesi, Sosyal Bilimler Dergisi, Cilt.4, Sayı.2, 2003.

Muhammed Arıkan, Süleyman ve Recep Benzer. **"Bir Güvenlik Trendi: Bal Küpü",** Acta Infologica Dergisi, Cilt.2, Sayı.1, 2018.

Onay, Ahmet. **"Büyük Veri Çağında İç Denetimin Dönüşümü",** Muhasebe Bilim Dünyası Dergisi, Cilt.22, Sayı.1, 2020.

Öztürk, Mahmut Sami. **"Siber Saldırılar, Siber Güvenlik Denetimleri ve Bütüncül Bir Denetim Modeli Önerisi",** Muhasebe ve Vergi Uygulamaları Dergisi, Ankara SMMMO, 2018.

Poonia, Ajeet Singh. **"Audit Tools for Cyber Crime Investigation",** International Journal of Enhanced Research in Science Technology & Engineering, Vol.3, Issue.12, 2014.

Saygılı, İsmail. **"Dünyayı Yöneten Güç – Bilgi Güvenliğinin En Zayıf Halkası İnsan Faktörü",** Siber Güvenlik Dergisi, Sayı.1, Mayıs 2017

Schatz, Daniel, Rabih Bashroush, Julie Wall. **"Towards a More Representative Definition of Cyber Security", Journal of Digital Forensics Security and Law.** Cilt.12, Sayı.2, 2017.

Şahin, Andaç, Ercan Buluş, M.Tolga Sakallı. **"24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme",** Trakya Üniversitesi Fen Bilimleri Dergisi, Cilt.7, Sayı.1, 2006.

Taşcı, Ufuk ve Ali Can. **"Türkiye'de Polisin Siber Suçlarla Mücadelede Politikası: 1997-2014",** Fırat Üniversitesi Sosyal Bilimler Dergisi, Cilt.25, Sayı.2, 2015.

Uçum, Melike Sinem. **"BT Güvenliği Denetimi",** Denetişim Dergisi, Kamu İç Denetçiler Derneği, Sayı.16, 2015.

Uzun, Ali Kamil. **"Denetim Hayattır",** Turcomoney Dergisi, Deloitte, 2014.

Uzun, Ali Kamil. **"Değer Yaratan Denetim",** İç Denetim Dergisi, Deloitte, Sayı.14, 2006.

Uzel, Murat Nail, Bülent Hasanefendioğlu, Cem Niyazi Durmuş. **"3'lü Savunma Hattının COSO İç Kontrol Sisteminin Etkinliğin Arttırılmasında Kaldıraç Etkisi",** Mali Çözüm Dergisi, İSMMMO, Sayı.136, 2016.

Vural, Yılmaz ve Şeref Sağıroğlu. **"Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler",** Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt.26, Sayı.1, 2011.

***Tez***

Aktaş, Emine, **İç Denetim ve Risk Yönetimi İlişkisi,** İstanbul Ticaret Üniversitesi, Sosyal Bilimler Enstitüsü, Muhasebe ve Denetim Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2015.

Akyol, Fatih, **COBIT (Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri) Uygulayan Şirketlerdeki Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçelere Etkileri,** Beykent Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Yönetimi Analim Dalı, Yüksek Lisans Tezi, İstanbul, 2013.

Alioğlu, Su Dilara, **Siber Saldırılar ve Ülkelerin Siber Güvenlik Politikaları,** İstanbul Bilgi Üniversitesi, Lisansüstü Programlar Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Porgramı, 2019.

Bozgeyik, Ahmet, **Gaziantep'te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi,** Hasan Kalyoncu Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Doktora Tezi, Gaziantep, 2018.

Çeliktaş, Barış, **Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme**, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi, Trabzon, 2016.

Kırmızı, Nihat, **İşletmelerde İç Kontrol Sistemini İncelemenin Bağımsız Denetim Karar Sürecindeki Yeri,** Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2007.

Mammadova, Narmin, **Web Yazılımlarında Güvenlik Problemleri Üzerine Araştırma,** İstanbul Aydın Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, 2017.

Meral, Mustafa, **Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi,** Harp Akademileri Stratejik Araştırmalar Enstitüsü, Savuma Kaynakları Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 2015.

Şahinaslan, Önder, **Siber Saldırılara Karşı Kurumsal Ağlarda Oluşan Güvenlik Sorunu ve Çözümü Üzerine Bir Çalışma,** Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, Doktora Tezi, Edirne, 2013.

Tarhan, Kamil, **Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik,** Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Ana Bilim Dalı, Yüksek Lisans Tezi, Konya, 2018.

Uzun, Sibel, **Bağımsız Denetimde İç Kontrol ve İç Denetimin Rolü,** Okan Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı, Yüksek Lisans Tezi, İstanbul, 2016.

Yerlikaya, Tarık, **Yeni Şifreleme Algoritmalarının Analizi,** Trakya Üniversitesi, Fen Bilimleri Enstitüsü, 2006.

Yılmaz, Mustafa, **İşletmelerde Bilgi Güvenliği Uygulama Sorunları ve Çözüm Önerileri; Konya Örneği,** Karatay Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Ana Bilim Dalı, Yüksek Lisans Tezi, Konya, 2018.

Yılmaz, Orhan, **ITIL ve COBIT Yönetim Standartları ve Bir Uygulama,** Beykent Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 2014.

***İnternet Kaynakları***

https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (26.09.2019)

http://www.belgelendirme.com.tr/iso-27001-2013-bilgi-guvenligi-belgesi.html (28.09.2019)

https://www.bsigroup.com/tr-TR/ISO-27001-Bilgi-Guvenligi-Yonetimi/ISOIEC-27001-Revizyonu/ (15.10.2019)

http://www.bilgiguvenligitr.com/bilge-adam-guvenlik-egitimleri/egitim-2-isoiec-27001-bilgi-guvenligi-yonetim-sistemi-uygulama-egitimi/ (17.10.2019)

https://intweb.tse.org.tr/Standard/Standard/Standard.aspx? (22.10.2019)

https://www.mshowto.org/iso-27000-ailesi-standartlari-nedir.html (22.10.2019)

https://www.tech-worm.com/worm-solucan-nedir/ (28.10.2019)

https://www.stm.com.tr/documents/file/Pdf/05-2_siber_tehdit_durumu_rapor_2016-08-03-10-57-17.pdf (22.12.2019)

https://docplayer.biz.tr/12545187-Dos-ddos-zombi-bilgisayar-ve-botnet-nedir.html (25.12.2019)

https://www.beyaz.net/tr/guvenlik/makaleler/dos_ve_ddos_nedir.html (01.01.2020)

https://www.eset.com/tr/phishing/ (10.01.2020)

https://tr.wikipedia.org/wiki/IP_spoofing (11.01.2020)

https://www.beyaz.net/tr/guvenlik/makaleler/zeroday_nedir.html (15.02.2020)

https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit (15.02.2020)

https://www.cybermagonline.com/rakamlar-ve-istatistikler-ile-2018-icin-en-onemli-5-siber-guvenlik-gercegi (22.02.2020)

https://www.businessinsider.com/bloomberg-businessweek-publishes-brutal-interactive-cover-on-the-target-hack-2014-3 (25.02.2020)

https://h4cktimes.com/veri-sizintilari/abdnin-dev-perakende-zinciri-targeta-sok-

ceza.html (26.02.2020)

https://lepicallidus.com/teknoloji/almanyada-celik-fabrikasina-siber-saldiri (27.02.2020)

https://www.technopat.net/2014/12/23/hackerlar-almanyada-celik-fabrikasini-hackledi/ (05.03.2020)

https://tr.sputniknews.com/asya/201810251035836450-cathay-pasific-havayollari-hacklendi-musteri-bilgileri-calindi/ (07.03.2020)

https://www.tide.org.tr/page/26/Ic-Denetimin-Tanimi (27.03.2020)

https://tr.wikipedia.org/wiki/Büyük_veri (14.05.2020)

https://www.misti.co.uk/internal-audit-insights/how-internal-audit-can-benefit-from-the-three-lines-of-defence-model (29.05.2020)

https://www.kaspersky.com.tr/resource-center/preemptive-safety/endpoint-security (06.12.2020)

***Diğer Yayınlar***

T.C. Ulaştırma Denizcilik Ve Haberleşme Bakanlığı, **"2016-2019 Ulusal Siber Güvenlik Stratejisi"**, s.8.

Hildreth, Steven A, **"Cyberware",** Congressional Research Service, 2001.

Enisa, **"Review of Cyber Hygiene Practices",** European Union Agency For Network And Information Security, 2016.

Souppaya, Murguiah vd., **"Crıtıcal Cybersecurıty Hygıene: Patchıng The Enterprıse",** National Institute of Standards and Technology, 2018.

**"Tripwire State of Cyber Hygiene Report"** Foundatıonal Controls For Security Complıance & IT Operatıons, 2018.

Artinyan, Natasa Eliza, **''Cobit Çerçevesi'',** Deloitte.

**COBIT 5: Ne kadar hazırsınız?,** Kurumsal Bilgi Teknolojileri Yönetişim Çerçevesi, Pwc.

Mele, Stefano, **"Cyber-weapons:Legal and Strategic Aspects Version 2.0",** Italian Institute of Strategic Studies, 2013.

Marinos, Louis, Adrian Belmonte, Evangelos Rekleitis, **"Enisa Threat Landscape 2015",** European Union Agency For Network And Information Security, 2016.

Corero, **"Full Year 2018 DDoS Trends Report"**, 2019.

Imperva, **"Global DDoS Threat Landscape Q4 2017",** 2018.

İstanbul Serbest Muhasebeci Mali Müşavirler Odası, **"İç Denetime Genel Bir Bakış",** 2015.

**"Embracing the Next Generation of Internal Auditing",** Protiviti**,** 2019.

**"Lights, camera, action... scripting internal audit for a changed world",** 2011 State of The Internal Audit Profession Study, Pwc, 2011.

Accenture, **"Building Your Cloud Strategy With Accenture"**.

KPMG, **"20 key risks to consider by Internal Audit before 2020",** 2018.

Pwc, **"İç Denetimin Gelişen Teknolojideki Yeni Rolü",** 2015.

**"Risk in Focus 2019 Hot Topıcs For Internal Auditors",** The Institute of Internal Auditors Netherlands, European Confederaiton of Institutes of Internal Auditing, 2018.

Accenture, **"Accenture Türkiye Dijitalleşme Endeksi",** 2016.

**"Küresel Bakış Açıları ve Anlayışlar Yapay Zeka - İç Denetim Mesleğine İlişkin Dikkate Alınması Gerekenler",** The Institute of Internal Auditors, 2017.

Chartered Institute Of Internal Auditors, **"Governance of risk : Three lines of defence",** 2019.

Federation of European Risk Management Associations & European Confederation of Institutes of Internal Auditing, **"At The Junction of Corporate Governance and Cybersecurity",** Cyber Risk Governance Report 2017.

The Institute Internal Auditors, **"Global Perspektifler ve Anlayışlar: Güvenilir Bir Siber Danışman Olarak",** Sayı.4, 2016.

The Institute Internal Auditors, **"Global Perspektifler ve Anlayışlar: İç Denetimin Global Nabzı Kanalıyla Sunulan Yeni Trendler",** Sayı.5, 2016.

The Institute of Internal Auditors, **"IIA Position Paper: The Three Lınes Of Defense In Effectıve Rısk Management And Control",** 2013.

ISACA, **"Cyber Security Audit",** 2017.

Deloitte, **"Cybersecurity and The Role of Internal Audit: An Urgent Call To Action",** 2017.

Hans Corell, **The Challenge of Borderless Cyber-Crime,** Symposium on the Occasion of the Signing of the Unıted Nations Convention Against Transnational Organized Crime, Palermo, 14 December 2000.

Nickolov, Eugene, **Modern Trends in the Cyber Attacks Against the Critical Definitions of the Fundamental**, Regional Cybersecurity Forum, Sofia, 7-9 October 2008.

Özlü, Mustafa, İzzet Gökhan Özbilgin, **"Yazılım Geliştirme Süreçleri ve ISO 27001 Bilgi Güvenliği Yönetim Sistemi",** XII. Akademik Bilişim Konferansı Bildirileri, Muğla Üniversitesi, 10-12 Şubat 2010.

Ülgü, M.Mahir vd.(Editörler), **Bilgi Güvenliği Politikaları Kılavuzu Sürüm 2.1,** T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, Kuban Matbaacılık Yayıncılık, Ankara 2019.

Güneş, Fatih vd., **Bilgi Teknolojileri Denetimi ve COBIT'in Sektörel Uygulanabilirliği,** Beykent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği.

Tutuş, Mehmet, Özgür Ulusan, **"E-Devlet ve Siber Güvenlik Gelişmiş Siber Silahlar",** 2013.

Daş, Resul, Şahin Kara, M. Zekeriya Gündüz, **"Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri Ve Çözüm Önerileri"**.

**"2016 Ekim-Aralık Dönemi Siber Tehdit Durum Raporu",** STM Mühendislik Teknoloji Danışmanlık.

Muharremoğlu, Gökhan, Raif Berkay Dinçel, **"Sosyal Mühendislik",** Pwc, 2018.

Yıldız, Okan, Alper Başaran, **"Sosyal Mühendislik Saldırıları"**.

Uzun, Ali Kamil, **"İşletmelerde İç Denetim Faaliyetinin Rolü ve Katma Değeri",** Deloitte.

**Kamu İç Denetim Rehberi,** İç Denetim Koordinasyon Kurulu, Ankara, 2013.

Kamu Gözetim Kurumu, **Müşteri Kabul Denetimin Planlanması ve BDS'lerde Ele Alınan Önemli Bazı Alanlar**.

Berman, Seth, **"Cyber Audits Prerequisite to Good Governance",** Issues.232, 2013.