



T.C.

TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

İŞLETME ANABİLİM DALI

MUHASEBE FİNANSMAN BİLİM DALI YÜKSEK LİSANS PROGRAMI

**İÇ DENETİMİN SİBER GÜVENLİKTEKİ ETKİNLİĞİ ÜZERİNE
ETKİSİ: İÇ DENETÇİLERİN ALGILARI**

YÜKSEK LİSANS TEZİ

Ebru TÜZEMEN

Danışman: Doç. Dr. Mihriban COŞKUN ARSLAN

TOKAT-2023

ETİK SÖZLEŞME

Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü tez yazım kılavuzuna göre, Doç. Dr. Mihriban COŞKUN ARSLAN danışmanlığında hazırlamış olduğum “**İç Denetimin Siber Güvenlikteki Etkinliği Üzerine Etkisi: İç Denetçilerin Algıları**” adlı Yüksek Lisans tezinin bilimsel etik değerlere ve kurallara uygun, özgün bir çalışma olduğunu, aksinin tespit edilmesi halinde her türlü yasal yaptırımını kabul edeceğimi beyan ederim.

26/04/2023

Ebru TÜZEMEN

JÜRİ KABUL VE ONAY

Ebru Tüzemen Tarafından hazırlanan “**İç Denetimin Siber Güvenlikteki Etkinliği Üzerine Etkisi: İç Denetçilerin Algıları**” adlı tez çalışmasının savunma sınavı 26/04/2023 tarihinde yapılmış olup aşağıda verilen Jüri tarafından Oy Birliği ile Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü İşletme Anabilim Dalı’nda Muhasebe Finansman Programı Yüksek Lisans Tezi olarak kabul edilmiştir.

Jüri Üyeleri (Unvanı, Adı Soyadı)

İmzası

Üye (Başkan) :.....

.....

Üye :

...

Üye :

....

ONAY

...../...../.....

Lisansüstü Eğitim Enstitüsü Müdürü

ÖZET

İÇ DENETİMİN SİBER GÜVENLİKTEKİ ETKİNLİĞİ ÜZERİNE ETKİSİ: İÇ DENETÇİLERİN ALGILARI

TÜZEMEN, Ebru

Yüksek Lisans, İşletme Bilim Dalı

Tez Danışmanı: Doç. Dr. Mihriban COŞKUN ARSLAN

Nisan 2023, xi + 134 sayfa

Dijital altyapının gelişmesi ile internet, bilgisayar sistemleri, yazılımlar, donanımlar gibi unsurlardan oluşan ve siber alan olarak ifade edilen bu ortamda bilginin depolanması, işlemlerin yapılması ve raporların hazırlanması gerçekleştirilmektedir. Bu durum fırsatları ön plana çıkarsa da siber saldırı risklerini de beraberinde getirmektedir. Siber saldırılar ciddi maliyetlere neden olduğu için önlemlerin alınması ve etkilerinin azaltılması gerekmektedir. Bu bağlamda, organizasyonların yönetimine ve yönetim kuruluna organizasyonun risk yönetimi ve iç kontrollerinin etkili olduğu konusunda güvence vermesine yardımcı olan iç denetim, özellikle siber saldırılara karşı önlemler alınması ve etkilerinin azaltılması açısından büyük önem arz etmektedir.

Bu çalışma Türkiye’de devlet ve vakıf üniversitelerinde görev yapmakta olan iç denetçilerin gözünden üniversitelerde iç denetimin siber güvenlikteki etkinlik algısını ortaya koymak üzere nicel bir araştırma olarak yürütülmüştür. Üniversitelerde iç denetimin mevcut durumunun belirlenmesi ve iç denetim ve siber güvenlik konularındaki eksiklerin tespit edilmesi çalışmanın önemini oluşturmaktadır. Araştırma verileri online anket aracılığıyla toplanmıştır.

Çalışmada tanımlayıcı faktör analizi yapılmış ve “İç Denetim ve Siber Güvenlik Algısı”, “Üniversite Yönetimi ve Siber Güvenlik Algısı”, “İç Denetim ve Siber Güvenlik Algısı”, “Siber Güvenlik Bilgi Düzeyi Algısı” ve “Siber Risk Yönetimi ve Siber Tehditler Algısı” faktörleri elde edilmiştir.

Çalışma sonucunda bilgi güvenliği, siber güvenlik ve iç denetim ile ilgili gerekli eğitim ve denetimi arttırmanın siber risklere karşı iç denetimin sağlanmasında önemli birer faktör olduğu tespit edilmiştir. Yine BT sistem ve araçlarının, süreçleri ve görevleri otomatikleştirerek, risk yönetimini ve iç kontrolleri iyileştirerek, organizasyonların

yasalara, yönetmeliklere ve endüstri standartlarına uymasına yardımcı olarak iç denetime yardımcı olabileceği tespit edilmiştir.

Anahtar Kelimeler: Bilgi Teknolojileri, Siber Güvenlik, İç Denetim



ABSTRACT

THE EFFECT OF INTERNAL AUDIT ON EFFECTIVENESS IN CYBER SECURITY: PERCEPTIONS OF INTERNAL AUDITORS

TÜZEMEN, Ebru

Master's Thesis Degree , Business Scientific

Advisor: Doç. Dr. Mihriban COŞKUN ARSLAN

January 2023, xi + 134 pages

With the development of digital infrastructure, information is stored, transactions are made and reports are prepared in this environment, which is expressed as cyberspace, which consists of elements such as the internet, computer systems, software, and hardware. Although this situation brings opportunities to the fore, it also carries risks of cyber attacks. Since cyber-attacks cause serious costs, taking precautions and reducing their effects is necessary. In this context, internal audit, which helps organizations to provide assurance to the management and board of directors that the organization's risk management and internal controls are effective, is of great importance, especially in terms of taking precautions against cyber attacks and reducing their effects.

This study was carried out as quantitative research to reveal the perception of the effectiveness of internal audit in cyber security in universities from the eyes of internal auditors working in state and foundation universities in Turkey. Determining the current state of internal auditing in universities and identifying the deficiencies in internal audit and cyber security constitute the importance of the study. Research data were collected through an online questionnaire.

In the study, descriptive factor analysis was performed and the factors of “Internal Audit and Cyber Security Perception”, University Administration and Cyber Security Perception”, “Internal Audit and Cyber Security Perception”, “Cyber Security Knowledge Level Perception” and “Cyber Risk Management and Cyber Threats Perception” has been obtained.

As a result of the study, it has been determined that increasing the necessary training and auditing related to information security, cyber security, and internal audit is an essential factor in providing internal audits against cyber risks. It has also been found that IT

systems and tools can assist internal auditing by automating processes and tasks, improving risk management and internal controls, and helping organizations comply with laws, regulations, and industry standards.

Key Words: Information Technologies, Cyber Security, Internal Audit



1.5.3. Performans Denetimi	23
1.5.4. Sistem Tabanlı Denetim.....	23
1.5.5. Bilgi Teknolojisi Denetimi.....	24
1.6. KAMUDA İÇ DENETİM VE İŞLEYİŞİ	25
1.7. ÜNİVERSİTELERDE İÇ DENETİM VE İŞLEYİŞİ.....	26
1.8. İÇ DENETİM MESLEĞİ VE ULUSLARARASI İÇ DENETİM MESLEĞİ DÜZENLEMELERİ	30
2. BÖLÜM: SİBER GÜVENLİK VE İÇ DENETİM FAALİYETLERİ	34
2.1. SİBER RİSK KAPSAMI	34
2.1.1. Siber Risk Kavramı.....	35
2.1.2. Kullanılan Analiz Yöntemleri.....	36
2.1.3. Siber Risklerin Haritalandırılması	38
2.1.4. Siber Risk Sigortası.....	39
2.2. SİBER SUÇLAR, SİBER TEHDİTLER VE SİBER SALDIRILAR... 41	
2.2.1. Siber Suçların Kapsamı.....	41
2.2.2. Siber Tehditlerin Kapsamı ve Siber Silahlar.....	43
2.2.3. Siber Saldırıların Kapsamı	45
2.2.3.1. Siber Saldırı Çeşitleri	46
2.2.3.2. Dünya’da ve Türkiye’de Siber Saldırı Örnekleri	49
2.2.3.3. Dünyada Siber Saldırı Örnekleri	49
2.2.3.4. Türkiye’de Siber Saldırı Örnekleri.....	56
2.3. SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ.....	58
2.3.1. Bilgi Güvenliği.....	59
2.3.2. Siber Güvenlik	60
2.4. SİBER GÜVENLİK KAVRAMLARI.....	63
2.4.1. Siber	63
2.4.2. Siber Zorbalık	64

2.4.3. Siber Uzay	64
2.4.4. Siber Tehdit	64
2.4.5. Siber Hijyen	65
2.4.6. Siber Suç	65
2.4.7. Siber Terörizm	65
2.4.8. Siber Casusluk	66
2.4.9. Siber Caydırıcılık	66
2.5. SİBER GÜVENLİK RİSK YÖNETİMİ	66
2.6. SİBER GÜVENLİK OLGUNLUK MODELİ	72
2.7. SİBER GÜVENLİK STANDARTLARI	73
2.8. SİBER GÜVENLİK AÇISINDAN DENETİM SÜREÇLERİ	74
2.9. SİBER GÜVENLİKTE İÇ DENETİMİN ROLÜ	76
2.10. ÜÇLÜ SAVUNMA HATTI MODELİ	80
2.10.1. Birinci Hat Modeli	81
2.10.2. İkinci Hat Modeli	81
2.10.3. Üçüncü Hat Modeli	82
3. BÖLÜM: İÇ DENETİMİN SİBER GÜVENLİKTEKİ ETKİNLİĞİ ÜZERİNE ETKİSİ: İÇ DENETÇİLERİN ALGILARI UYGULAMASI	83
3.1. ARAŞTIRMANIN AMACI	83
3.2. ARAŞTIRMANIN ÖNEMİ	84
3.3. LİTERATÜR TARAMASI	85
3.4. ARAŞTIRMANIN HİPOTEZLERİ	90
3.5. ARAŞTIRMANIN ANAKÜTLESİ VE ÖRNEKLEMİ	91
3.6. VERİ TOPLAMA ARACI	91
3.7. ARAŞTIRMANIN YÖNTEMİ VE KISITLARI	92
3.8. BULGULAR	92
SONUÇ VE ÖNERİLER	109

KAYNAKÇA.....	113
EKLER	129
ÖZGEÇMİŞ	134



TABLolar LİSTESİ

Tablo No.....	Sayfa No
Tablo 2.1: Siber Güvenlik Olgunluk Modeli.....	73
Tablo 4.1: Demografik Verilerin Frekans Tablosu.....	93
Tablo 4.2: Denetçi Özellikleri Frekans Tablosu.....	94
Tablo 4.3: Üniversite İç Denetim Yetkinliği Frekans Tablosu.....	95
Tablo 4.4: Siber Risk Yönetimi Açısından Üniversitenin Yaşadıkları Zorlukların Önem Derecesi Frekans Tablosu.....	96
Tablo 4.5: İç Denetim Ve Bilgi Güvenliği Personel Sayısı Tanımlayıcı İstatistikleri.....	97
Tablo 4.6: Faktör Analizi Sonuçları.....	98
Tablo 4.7: Öğrenim Durumları İtibariyle Farkları Gösteren ANOVA Tablosu.....	99
Tablo 4.8: Öğrenim Durumları Arasındaki Farkı Gösteren Scheffe Testi Sonuçları.....	100
Tablo 4.9: Katılımcıların İç Denetçi Olarak Üniversitede Çalıştıkları Süre İtibariyle Farklarını Gösteren ANOVA Sonuçları.....	102
Tablo 4.10: İç Denetçi Olarak Mesleki Tecrübeleri İtibariyle Farklarını Gösteren ANOVA Sonuçları.....	102
Tablo 4.11: Katılımcıların Siber Güvenlik Ve Bilgi Teknolojileri Konularındaki Bilgi Düzeyleri İtibariyle Farklarını Gösteren ANOVA Sonuçları.....	103
Tablo 4.12: Katılımcıların Siber Güvenlik Ve Bilgi Teknolojileri Konularındaki Bilgi Düzeyleri Arasındaki Farkı Gösteren Scheffe Testi Sonuçları.....	104
Tablo 4.13: Katılımcıların Mevcut Durumlarının İstatistik Tablosu.....	105

ŞEKİLLER LİSTESİ

Şekil No.....	Sayfa
Şekil. 2.1: Siber Güvenlik Risk Değerlendirme Çerçevesi.....	68
Şekil 2.2: Üçlü Savunma Hattı Modeli.....	80



KISALTMALAR

AEK	Ağ Erişim Kontrolü
AV	Antivirüs
BGYS	Bilgi Güvenliği Yönetim Sistemi
BT	Bilgi Teknolojisi
ECIIA	Avrupa İç Denetim Enstitüleri Konfederasyonu
ERP	Kurumsal Kaynak Planlaması
IDC	International Data Corporation
IDS-IPS	İzinsiz Giriş Tespit-Önleme Sistemleri
IIA	İç Denetim Enstitüsü
IP	İnternet Protokolü
IPPF	Mesleki Uygulama Çerçevesi
ISRAM	Bilgi Güvenliği Risk Analizi Metodu
İDKK	İç Denetim Koordinasyon Kurulu
MBS	Muhasebe Bilgi Sistemi
MRP II	Üretim kaynakları planlaması
MRP	Malzeme İhtiyaç Planlama
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü
TC	Türkiye Cumhuriyeti
TİDE	Türkiye İç Denetim Enstitüsü
www	World Wide Web

GİRİŞ

Son yıllarda, küreselleşme ve bilgisayarlaşma, endüstrinin, siyasetin, kültürün ve sosyal düzenin yeniden tanımlanmasına yol açmıştır. Bu değişimler, bilgi teknolojisinin ekonomik ve kültürel entegrasyonu mümkün kılmasıyla ortaya çıkmıştır ve küreselleşmeye büyük katkılar sağlamıştır. Teknolojik devrim sayesinde, küresel bilgisayar ağları aracılığıyla mal, bilgi ve insanların sınırları aşarak serbestçe hareket etmesi daha kolay hale gelmiştir.

İç denetim, bir organizasyonun risk yönetimi, yönetişimi ve iç kontrol sistemlerinin bağımsız bir şekilde değerlendirilmesidir. İç denetimin temel amacı, organizasyonun operasyonlarının etkili, verimli ve yasalara, yönetmeliklere ve politikalara uygun olduğuna dair güvence sağlamaktır. İç denetim birimleri genellikle kuruluşun yönetim kurulu veya denetim komitesine rapor sunmakta ve organizasyonun BT ve siber güvenlik kontrollerini gözden geçirmekte ve değerlendirme yetkisine sahip olabilmektedir. Bu şekilde, iç denetim departmanları, organizasyonun risk yönetimi ve uyumluluk süreçlerine katkıda bulunarak işleyişin güvenilirliğini ve etkinliğini artırmaktadır.

İç denetim, herhangi bir organizasyon için oldukça önemli bir konumdadır, ayrıca iç denetim, muhasebe sistemlerinin uygulanmasında kilit unsur olarak kabul edilir ve bu da departmanın çalışmalarının değerlendirilmesine yardımcı olur. Mali raporlar iç denetim departmanının kalitesini yansıttığından, iç denetimin etkinliği şirketin çalışmasını geliştirmeye yardımcı olur. Ayrıca, iç denetim, bir organizasyondaki Kurumsal Yönetim (KY) yapısının önemli bir parçasıdır. İç denetim, organizasyon hedeflerine ulaşılmasına ve bu hedeflere ulaşmak için stratejilerin uygulanmasına büyük katkı sağlar.

İç denetim, tüm yönetim seviyelerinde uygun iş kararlarının dayandığı farklı organizasyon birimlerinden gelen finansal ve operasyonel bilgilerin güvenilirliğini, gerçekliğini ve bütünlüğünü belirler. İç denetim görevlerinin başarılı bir şekilde yürütülmesi, bağımsız olmaları gerektiği anlamına gelir; bu, şirket yönetiminin çalışmalarından, bilgilerinden, sonuçlarından ve değerlendirmelerinden hiçbir şekilde etkilenmemesi gerektiği anlamına gelmektedir. Bu şekilde iç denetim raporu, iç denetim

ve yönetim arasında bir iletişim aracı ve şirketin başarılı yönetimi için önemli bir rehber haline gelir.

Birçok sistem, organizasyonda kontrol amacıyla rutin olarak kullanılır ve sınırlı karar vermeyi gerektirir. Bazı sistemlerin çıktıları bir program veya stratejinin parçası olarak kullanılabilir. Sistemin kendisi, müşteri sipariş sürecini basitleştirmek gibi bir kurumsal strateji uyguluyor olabilir. Bir sistem, yöneticilerin karar vermesine yardımcı olabilir.

Çoğu organizasyon kararlarını iç denetim bölümünün tavsiyelerine göre almaktadır. İç denetçiler, denetim komitesine kıyasla üst yönetime rapor verirken daha az objektiftir. Ayrıca iç denetim departmanı üst yönetime rapor verirse, objektiflikleri bozulacağı için önerileri yönetimin tercihiyle daha tutarlı olacaktır.

Siber güvenliğe bütünsel ve kapsamlı bir yaklaşım sağlamak için iç denetimin siber güvenlikten sorumlu tek kişi olmaması, bunun yerine BT güvenliği, BT operasyonları ve BT yönetimi gibi diğer departmanlarla yakın çalışması gerektiğini belirtmek gerekir.

Kısacası, iç denetim uzmanları siber güvenliğe önem vermelidir çünkü siber tehditler ve saldırılar organizasyon üzerinde önemli bir etkiye sahip olabilir ve etkin risk yönetimi ve iç kontroller, organizasyonu bu tehditlerden korumak için çok önemlidir. İç denetim, kurumun etkili yönetişime, risk yönetimine ve yasa ve yönetmeliklere uyum dahil olmak üzere siber güvenlikle ilgili iç kontrollere sahip olmasını sağlamada ve riski azaltmak için önerilerde bulunmada önemli bir rol oynayabilir.

Siber güvenlik, bilgisayar sistemlerini, ağları ve diğer dijital varlıkları yetkisiz erişim, kullanım, ifşa, kesinti, değişiklik veya imhadan koruma uygulamasıdır. Bilgisayar korsanlığı, kimlik avı ve kötü amaçlı yazılım gibi siber tehditlere karşı koruma sağlamak için güvenlik önlemlerinin ve kontrollerinin uygulanmasını içerir.

Siber güvenlik ile herhangi bir toplum veya herhangi bir kullanıcı kritik verilerini bilgisayar korsanlarından koruyabilir. Siber güvenlik, dolaylı olarak, sık kullanıcıların internet veya ağ üzerinden iletişim kurabileceği diğer kişilerin de güvenliğini gerektirir.

Tüm organizasyonun ticari kaybı ve mali kaybının korunmasının yanı sıra daha da önemli olan itibar zedelenmesinin önüne geçmek için güvenlik korkularını hafifletmeye yönelik bir prosedür olarak tanımlanabilir. Ancak, bilgi korumasıyla ilgili en önemli gerçek, bunun tek parça bir prosedür değil, sürekli bir süreç olmasıdır. Bilgi

teknolojisi yöneticilerinin tehlikeyi en aza indirmek için kullanılan araç gereçleri modernize etmeleri gerekmektedir.

Siber güvenlik açısından denetim süreci, bir organizasyonun güvenlik açıklarını tespit etmesine ve bu açıkları çözmesine yardımcı olur. Bu süreç, organizasyonun bilgi sistemlerini korumak için alınması gereken önlemlerin belirlenmesine yardımcı olup, potansiyel riskleri azaltır.

Siber güvenlikte denetim süreci aynı zamanda, siber saldırılar ve diğer güvenlik tehditlerine karşı koruma sağlamak için önemlidir. Denetim süreci, organizasyonların siber güvenlik politikalarını, prosedürlerini ve teknolojilerini değerlendirir ve bu politikaların ve prosedürlerin etkililiğini test eder. Bu süreç, organizasyonların siber güvenlik stratejilerini geliştirmelerine ve iyileştirmelerine yardımcı olur.

Bilgi güvenliği, tehditleri ortadan kaldırmakla değil de daha çok riski anlamak ve yönetmekle ilgilidir. Her işlevsel bilgi işlem cihazı aynı zamanda ağ bağlantılı bir bilgi işlem cihazı olduğunda, mutlak güvenli bir bilgi sistemi diye bir durum olmamaktadır. Daha güvenli sistemler, organizasyonlar için kendi tür riskleriyle birlikte gelir, güvenlik ile serbest bilgi akışı arasındaki fiili dengenin her gün kontrol edilmesi gerekir.

Herhangi bir sistem veya süreçteki gerçek bilgi güvenliği açıkları, teknolojik açıklar değil insan kaynaklı açıklardır. İnsanların öngörülemeyen ve bazen de açıklanamayan şekillerde davranma alışkanlığı vardır. Bilgisayar korsanlarının bilgi güvenliğindeki insan sorununu istismar etmede sosyal mühendislik kavramı dillendirilmektedir. Sosyal mühendislik, genellikle erişimi olan veya olması gereken biriymiş gibi davranarak birisinin parolalarını, erişim ayrıntılarını veya gizli bilgilerini ifşa etmesi için kandırma sürecidir.

Günümüzde bir organizasyonun rekabet avantajı, tekrarlayan görevleri otomatik hale getirmek, raporlamayı iyileştirmek ve stratejik karar vermeyi geliştirmek için verilerden yararlanmak için teknolojiyi ne kadar iyi kullanabileceğine bağlıdır. Bununla birlikte, bir organizasyon BT'ye ne kadar çok güvenirse, kurumsal BT ekosistemindeki güvenlik açıklarını bulma konusunda ün salan kötü niyetli uzmanların neden olduğu güvenlik ihlallerine karşı o kadar savunmasızdır.

Siber güvenlik olaylarının çoğalması, kurumsal kuruluşların karşılaştığı en büyük risk olabilir. İhlalin maliyetine ek olarak, arıza süresi ve itibarın zarar görme potansiyeli, olayın felaket durumuna gelmesi durumunda bir şirketi iflasa zorlayacak kadar ciddidir.

Geçmiş yıllarda sadece virüsten koruma yazılımı ve güvenlik duvarları kullanmak yeterli olabilirdi. Ancak son yıllarda, bu durum geçerliliğini kaybetmiştir. Artık organizasyonlar, saldırıları engellemek için riskleri erken aşamada başarılı bir şekilde tanımlamalı ve azaltmalıdır.

Siber güvenlik risk yönetimi, organizasyonların veya devletlerin bilişim sistemlerinin güvenliğini sağlamak için alınan önlemleri içerir. Bu önlemler, bilişim sistemlerine yönelik tehditlerin belirlenmesi, risklerin değerlendirilmesi ve uygun güvenlik önlemlerinin alınması için bir süreç halinde yürütülür.

Siber güvenlik risk yönetimi süreci, risk değerlendirme, risk yönetimi ve risk izleme ve değerlendirme olmak üzere üç aşamadan meydana gelir. Siber risk yönetimi, siber güvenlik tehditlerinin tespit edilmesi ve değerlendirilmesi, risklerin analizi ve değerlendirilmesi, mevcut riskler için alınan önlemleri sürekli kılmayı içeren bir döngüdür. Bu döngü siber güvenliğini sağlamak ve iş sürekliliğini korumak için birçok organizasyonun uyguladığı bir risk yönetim şeklidir. Özellikle siber güvenlik olaylarının sık yaşandığı bu günlerde siber risklere karşı daha dirençli bir organizasyon oluşturmak için bu yönetim şekli kritik bir öneme sahiptir.

İç denetim, siber güvenlik risklerini belirlemek, değerlendirmek ve kontrol etmek için önemli bir araçtır. İç denetim departmanları, organizasyonun bilgi sistemlerinin güvenliğini ve siber risk yönetimini değerlendirmektedir. Bu değerlendirme süreci, organizasyonun bilgi sistemlerinin güvenlik açıklarını belirlemek, uygun güvenlik önlemlerini uygulamak ve potansiyel tehditlere karşı koruma sağlamak için açısından önemli bir rol oynamaktadır.

İç denetim birimleri, siber güvenlik politikalarının, prosedürlerinin ve kontrollerinin etkinliğini gözden geçirmekte, siber saldırılara karşı önlemlerin yeterli olduğunu değerlendirmekte ve gerektiğinde iyileştirmeleri önermektedir. Ayrıca, siber güvenlik olaylarına müdahale süreçlerini ve etkinliğini değerlendirerek, organizasyonun siber saldırılara karşı hazırlıklı olma durumunu artırmaya yönelik çalışmalar yürütmesi gerekmektedir.

BT, siber güvenlik ve iç denetim yakından ilişkilidir ve organizasyonların karşılaşılabilecekleri siber risklerin etkili bir şekilde yönetilebilmesi için birlikte çalışmaları gerekmektedir. İç denetim, organizasyonların yasalara ve düzenlemelere

uyumunu sürdürmelerine ve dijital varlıklarını korumalarına yardımcı olmak için organizasyonun BT ve siber güvenlik kontrollerinin değerlendirilmesinde, test edilmesinde ve iyileştirme önerileri sağlanmasında kritik bir rol oynar.

Bu çalışmanın amacı, iç denetimin siber güvenlikteki etkinliğinde iç denetçi algısının ölçülmesidir. Türkiye’deki üniversiteler çalışmanın anakütlesini oluşturmaktadır. Üniversitelerde iç denetimin nasıl sağlandığı ve siber risklerle nasıl baş edildiğinin tespit edilmesi çalışmanın alt amaçlarını oluşturmaktadır.

Yukarıdaki bilgiler ışığında literatüre katkı sağlamak amacıyla yürütülen bu çalışmada dört tane hipotez yer almaktadır. Bunlar;

H1: Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının öğrenim durumlarına göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

H2: Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının iç denetçi olarak üniversitede çalıştığı süreye göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

H3: Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının mesleki deneyimine göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

H4: İç denetçilerin siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyine göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

Türkiye’deki devlet ve vakıf üniversitelerinin bünyelerinde oluşturulmuş olan “İç Denetim” birimlerinde çalışan bütün iç denetçiler çalışmanın anakütlesini (evrenini) oluşturmaktadır. Bu amaç doğrultusunda devlet ve vakıf üniversitelerindeki toplam 168 iç denetçinin iletişim bilgilerine, çalıştıkları üniversitelerin resmi internet sayfalarındaki birim adreslerinden ulaşılmıştır. Sanal ortamda hazırlanan ölçek formu 168 iç denetçinin tamamının e-posta adresine online olarak doldurulması için gönderilmiştir. Gönderilen e-postalardan 42 tanesi için hatalı e-posta gönderimi uyarısı alınmıştır. Hatalı olmayan gönderimlerden toplam 56 geri dönüş sağlanmıştır. Eksik ve kayıp verilerin elenmesinden sonra 52 katılımcı ile uygulama yapılabilmektedir. Bu rakam, tam sayım yaptığımız ama geri dönüşü tam alamadığımız çalışmamız için yeterli bir örneklem miktarıdır.

Üniversitelerde görev yapmakta olan iç denetçi özellikleri ile iç denetim algıları arasında benzer ve farklı noktalar tespit edilerek literatüre katkıda bulunmak bu

alışmanın önemi ni ortaya koymaktadır. Aynı zamanda üniversitelerde iç denetimin mevcut durumunun belirlenmesi ve iç denetim ve siber güvenlik konularındaki eksiklerin tespit edilmesi alışmanın önemi ni oluşturmaktadır.

alışmanın birinci bölümünde; iç denetim kavramı, kapsamı, amacı, özellikleri, tarihsel gelişimi, türleri ve standartları hakkında detaylı bilgi verilmiştir. alışmanın ikinci bölümünde siber güvenlik ve iç denetim faaliyetleri hakkında detaylı bilgi verilmiştir. Üçüncü bölümde ise uygulamaya yer verilmiş ve Türkiye’deki Devlet ve Vakıf Üniversitelerinde çalışan iç denetçiler ile yapılan araştırmanın sonuçları aktarılmıştır. Sonuç bölümünde değerlendirmelere ve önerilere yer verilmiştir.



1. BÖLÜM: İÇ DENETİM

İç denetim, bir organizasyonun yönetimi ve iç kontrol yapısının değerlendirilmesinde ve amaçlarına kritik bir rol oynayan bir işlemdir. Bu, bir organizasyon stratejisinin sürdürülmesi için yönetim ve çalışanların uygun şekilde yönlendirilip yönetildiği ve risklerin etkili bir şekilde yönetilmesini sağlamak için bir dizi faaliyeti içermektedir. Bu faaliyetler organizasyonların tüm bölümlerini kapsamakta ve sonuçları yönetime raporlanmaktadır. Hazırlanan bu raporlar organizasyon yöneticilerinin karar almalarında kullanılmakta ve süreçlerdeki iyileştirmelerin yapılmasında yardımcı olmaktadır. Bu bölümde iç denetim kavramı, amacı, özellikleri, tarihsel gelişimi, türleri ve çalışmanın amacı doğrultusunda üniversitelerde iç denetim kavramı açıklanmaktadır.

1.1. İÇ DENETİM KAVRAMI

İç denetim mesleğinin geliştirilmesine ve iç denetim faaliyetlerinin dünya çapında kabul edilmesine yönelik olarak çalışmalar yürüten İç Denetim Enstitüsü'nün (Institute of Internal Auditors - IIA) uluslararası kabul görmüş iç denetim tanımına göre; iç denetim, organizasyonun tüm faaliyetlerini izlemek, geliştirmek, iyileştirmek, değer katmak gibi nedenler için bağımsız ve tarafsız bir danışmanlık ve güvence hizmeti sağlamaktadır. İç denetçiler, risk yönetimi, yönetim ve iç kontrol süreçlerinin etkinliğini ve verimliliğini değerlendirip geliştirmek için sistematik yaklaşımlar geliştirerek bir organizasyonun hedeflerine ulaşmasına yardımcı olmaktadır (Korkmaz, 2007:4).

Daha geniş anlamda iç denetim; kontrol, yönetim ve risk yönetimi süreçlerinin etkinliğini sistematik ve disiplinli bir yaklaşımla değerlendirip, geliştirerek, organizasyonların hedeflerine ulaşmalarına yardımcı olan ve gerek özel sektörde gerekse kamu sektöründe yönetim faaliyetlerinin neredeyse vazgeçilmez bir işlevi haline gelmiş bir disiplindir (Pickett, 2010:96).

İç denetim, özünde, organizasyonun kararlaştırılan hedeflere ulaşmadaki etkinliğini ölçüp, değerlendirerek, kontrol, yönetim ve risk yönetimi hakkında kurum başkanına bağımsız ve tarafsız bir görüş sağlamaktadır. Ayrıca, iç denetim tavsiyeleri ve bulguları, denetlenen alanlarda süreç yönetimine fayda sağlamaktadır. Risk yönetimi, kontrol ve yönetim; hedeflere ulaşılmasını, risklerin düzgün bir şekilde değerlendirilmesini, iç ve dış raporlama ve hesap verebilirlik süreçlerinin güvenilir

olmasını, yürürlükteki yasa ve yönetmeliklere uygunluğu ve bunun için belirlenen davranışsal ve etik standartların sağlanmasını sağlamak için oluşturulmuş politikalar, prosedürler ve faaliyetleri içermektedir (Korkmaz, 2007:4).

Bir organizasyon için etkin bir iç denetim sistemi, sadece işletmenin varlıklarını korumakla kalmayıp aynı zamanda işletme için katma değer sağlayacak faaliyetler sunmalıdır. Bu nedenle, iç denetimin bağımsız ve tarafsız bir şekilde gerçekleştirilmesi, mesleki yeterliliğe ve deneyime sahip iç denetim uzmanları tarafından yapılması gerekmektedir. İç denetim, işletmenin olağan güvence faaliyetlerini yerine getirmenin yanı sıra süreçlerini iyileştirerek işletmeye etkinlik ve verimlilik açısından değer katmaktadır. Bu nedenle, işletmenin hedeflerine ulaşması için etkili bir iç denetimin varlığı çok önemlidir. İç denetim yapısının, iç denetim planlamasının, güçlü stratejik iletişimin, yönetim becerilerinin ve iç denetçinin mesleki niteliklerinin ve deneyiminin işletmeye özgü dinamiklere göre belirlenmesi, iç denetimin etkinliğini etkileyen kritik faktörlerdir (Hazaee, vd., 2020: 869).

Sonuç olarak iç denetim organizasyonların yönetim ve kontrol sistemlerinin değerlendirilmesinde ve yapısında kilit rol oynamaktadır. Bu rolde organizasyonları gözlemleyip değerlendirmeler yapmaktadır. Böylelikle risk profili, iş süreçleri ve kontrol süreçleri hakkında ayrıntılı bilgi sunmuş olmaktadır. İç denetim aynı zamanda, organizasyonların finansal tablolarının doğruluğunu belirlemeye yardımcı olmaktadır. Bu sayede organizasyonların itibarını korumasına yardımcı olmaktadır (Zorlu, 2014:12).

1.2. İÇ DENETİMİN AMACI VE ÖZELLİKLERİ

Her organizasyonun, kurumun iç kontrollerini ve iç denetim programının kapsamını ve iç denetim bulgularının gözden geçirilmesi ve ayrıca tespitler doğrultusunda yapılması gerekenler hakkında görüş bildirmekten sorumlu bir iç denetim komitesine sahip olması gerekmektedir (Hoos vd., 2018:153-156). Bu iç denetim komitesinin belli başlı amaç ve özellikleri mevcuttur.

1.2.1. İç Denetimin Amacı

İç denetimin temel amacı; organizasyonun hedef ve amaçları doğrultusunda üst yönetim tarafından oluşturulmuş kontrollerin etkinliğinin ve yeterliliğinin incelenmesi, işletme varlıklarının her türlü zarara karşı korunup korunmadığının, faaliyetlerin işletme politikaları ile uyum içerisinde yürütülüp yürütülmediğinin ve mali tablolara temel

oluşturan muhasebe bilgilerinin doğruluk ve güvenilirliğinin araştırılmasıdır. İç denetim, amaçlarını gerçekleştirirken üst yönetimin de sorumluluklarını yerine getirmesine katkı sağlamaktadır (Ceyhan; 2010: 37-38).

İç denetim, yönetim kuruluna ve/veya üst yönetime risk yönetimi süreçlerinin eksiksiz, etkin ve verimli olduğuna dair nesnel bir güvence sağlamaktır. Bu görevin bir parçası olarak iç denetim fonksiyonu, üst yönetime görev ve sorumluluklarını yerine getirmeleri konusunda tavsiyelerde bulunmakta, rehberlik etmekte ve işlerin yapılması için fırsat sunmaktadır.

Geleneksel anlamda iç denetimin amacı; her türlü riski bulup, ortadan kaldırmaktır. Diğer bir ifadeyle iç denetim birimi, organizasyonlarda faaliyetlerin önceden belirlenmiş standart, politika ve hedeflere uygun olarak yürütülüp yürütülmediğini denetleyen birim olarak tanımlanmaktadır. İç Denetim ayrıca üst yönetime danışmanlık/danışmanlık hizmetleri sağlamakta ve yönetimin bilgiye dayalı kararlar almasını sağlamaktadır. İç denetim raporlarında faaliyetlerin verimliliği ve etkinliği inceleyerek bu konuda yönetime önerilerde bulunmaktadır (Aslan, 2010:72).

Sonuç olarak iç denetimin temel amacı, organizasyonların misyon ve vizyonlarına ulaşmaları için risk yönetimi, kontrol yönetimi ve bu yönetim süresinde bir rehberlik ve danışmanlık hizmeti sunmaktır. İç denetim, işletme finansal kaynakları, yasal uyumluluk, güvenlik ve stratejik yönetim gibi yerlerde güvenilir bir iç kontrol ortamına yardımcı olmaktadır.

1.2.2. İç Denetimin Özellikleri

Organizasyonların faaliyetlerini, iş süreçlerini, finansal raporlamalarını ve risk yönetimini değerlendirmek amacıyla gerçekleştirilen bir faaliyet olan iç denetim, bağımsız bir güvence ve danışmanlık hizmeti sunmaktadır. İç denetim süreci, organizasyonların hedeflerine ulaşmak için uyguladığı risk yönetimi, kontrol ve yönetim süreçlerinin etkinliğini değerlendirerek, iş süreçlerinin ve finansal raporlama sistemlerinin etkinliği, verimliliği ve uygunluğunu da denetler.

İç denetimin temel özellikleri, organizasyonların amaçlarına ulaşmada etkili bir şekilde katkıda bulunmakta ve iç denetim faaliyetlerinin etkinliğini artırmak için önem arz etmektedir. Bu noktada iç denetimin temel özellikleri aşağıdaki gibi sıralanmaktadır (Arcagök ve Erüz, 2006: 192):

- Fonksiyonel bağımsızlık,

- Kuruma değer katma,
- Risk Odaklı Denetim ve Yönetişim Süreçlerine Katkı Sağlama
- Güvence ve Danışmanlık Hizmeti Sağlama
- Standartlara Uygunluk

1.2.2.1. Fonksiyonel Bağımsızlık

Bağımsızlık ve Tarafsızlık Politikası, yönetim sistemi denetimlerini yürütürken tarafsızlık son derece önemli noktada bulunmaktadır. Bağımsızlık ve Tarafsızlık Politikası, yönetim sistemlerinin denetimine ilişkin Uluslararası Standartlar Teşkilatı (International Organization for Standardization - ISO) tarafından somutlaşan tarafsızlık ilkelerine tamamen bağlıdır. Bağımsızlık ve Tarafsızlık Politikası, denetim hizmetlerinin uygulanmasında bağımsızlığını ve tarafsızlığını sağlamak ve tüm denetimlerin açık, bağımsız ve tarafsız bir şekilde yürütülmesini sağlamak için prosedürler sunmaktadır. Bağımsızlık ve Tarafsızlık Politikası, denetim faaliyetleriyle ilgili olarak alınan kararlar ve bulgular için yetki ve sorumluluğu elinde tutmaktadır (Türkiye İç Denetim Enstitüsü, 2008: 36-37). Denetimin bağımsızlık ve tarafsızlık politikasına yönelik özellikleri aşağıdaki gibi sıralanmıştır:

- İç denetim birimi direkt üst yöneticiye bağlıdır.
- Denetim faaliyeti, idarenin mevcut işlemlerinden, yönetimin faaliyetlerinden ve günlük işlerden bağımsızdır.
- İç denetçiler, idari ve mali işlemlerin hazırlanmasında, karar alınmasında ve uygulanmasında görev almamaktadır.
- İç denetçiler, iç kontrol sisteminin tasarlanmasına veya uygulanmasına ve iç kontrol önlemlerinin seçimine katılmamaktadır.
- İç denetçilere, ilgili mevzuatta öngörülen iç denetim faaliyetleri dışında görev verilmemektedir.
- İç denetimin bağımsızlığı, kalite güvence ve iyileştirme programının bir parçası olarak İç Denetim Koordinasyon Kurulu tarafından düzenli olarak değerlendirilmektedir (Birimi, 2017: 15).

1.2.2.2. Kuruma Değer Katma

İç denetim mesleği uzun zamandır hizmet verdiği organizasyonlara değer katmayı kendine görev edinmiştir. Bu sadece denetimler yapmak, kontrolleri test etmek ve

raporları yayınlamakla ilgili değildir. İç denetimin, tek tek parçaların ve parçaların toplanmasını almak ve şirketin kapsamlı bir görünümünü oluşturmak için organizasyon içindeki benzersiz konumunu kullanması ve organizasyonun güçlü yönler, zayıf yönler, tehditler ve fırsatlar hakkında rehberlik etmesi beklenmektedir. İç denetime değer katan çeşitli faktörler şu şekilde sıralanabilir (Türkiye İç Denetim Enstitüsü: 15).

- Uluslararası iç denetim standartlarını temel almak
- İş Zekasını Geliştirin ve Değerlendirin
- Meslekte Değere Odaklanmak
- İlişkileri kuvvetlendirmek ve bilgiye dayalı hareket etmek
- Duyurulanları ve planlananları uygulamak.

1.2.2.3. Risk Odaklı Denetim ve Yönetişim Süreçlerine Katkı Sağlama

Risk odaklı denetim, mali ve idari riskleri, hataları ve eksiklikleri belirleyerek ve en iyi uygulama örneklerini yaygınlaştırarak sistemlerin iyileştirilmesine yönelik, mevzuata uygun yönetim standartları ile iç denetime katkı sağlayan bir iç denetim özelliğidir. Bu yüzden iç denetim birimi denetim süresi itibarıyla karşılaşılan riskler üzerine yoğunlaşmaktadır (Demirbaş, 2005: 176-177).

Geleneksel denetim planları, halihazırda organizasyonların potansiyel risklerine odaklanmaktadır. Riske dayalı iç denetimler ise şirketlerin karşı karşıya olduğu yapısal riskleri inceleyerek başlar ve daha sonra hangi risklerin en acil ve en yüksek kayıp potansiyeline sahip olduğunun analizini yapıp kontrol ve düzenlemelerini yeniden sağlamaya çalışmaktadır. Bu bakış açısıyla risk odaklı denetim, geleneksel denetim metodolojisinde olduğu gibi organizasyonu departman yerine bir bütün olarak incelediği için Kurumsal Risk Yönetimi yaklaşımıyla daha uyumludur (Abidin, 2017: 361-371).

1.2.2.4. Güvence ve Danışmanlık Hizmeti Sağlama

Hem organizasyon yönetimi hem de organizasyonla ilişkisi olanlar için etkin bir iç denetim sistemine sahip olunması; iç kontrol sistemi, risk yönetimi ve işlem süreçlerinin etkin bir şekilde çalıştığı; ortaya çıkan bilgilerin doğruluğu ve eksiksizliği, varlıklarının korunduğu; faaliyetlerin verimli, ekonomik, etkin ve kurum politikasına uygun olarak yürütüldüğüne dair makul bir güvence sağlamaktadır (İDKK, 2006).

İç denetim biriminin temin ettiği güvence hizmeti mutlak bir güvence değildir. Çünkü tüm organizasyon eylemlerine nüfuz etmenin imkânsız olması ve geleceğin bir

çok belirsizlik içermesi, mutlak güvencenin sağlanmasını imkansız kılmaktadır. İç denetim faaliyetlerinin iç denetim standartlarına uygun olarak yürütülmesi ve bu faaliyetleri yürüten denetçilerin mesleki etik çerçevesinde hareket etmesi durumunda iç denetimin makul güvence sağladığı genel olarak kabul edilmektedir (Aslan, 2010: 74).

İç denetim, organizasyona güvence sağlamanın yanı sıra, kurumun amaçlarına ulaşması için kurum faaliyetlerinin ve operasyonel süreçlerin sistematik ve düzenli bir şekilde değerlendirilmesi ve geliştirilmesi için tavsiyelerde bulunmaktadır.

Önerilen tavsiyelere, denetim faaliyeti neticesinde hazırlanan denetim raporunda yer verildiği gibi, doğrudan iç denetim biriminden talep edilen danışmanlık faaliyeti kapsamında hazırlanan raporlarda da yer verilmektedir (Aslan, 2010: 74).

1.2.2.5. Standartlara Uygunluk

Standartlara uygunluk denetimleri, bir organizasyonun kurumsal tüzükler, kontroller ve politikalar gibi yasal gereklilikleri veya dahili yönergeleri karşıladığından emin olmak için uygulanan kontrollerdir. Bir denetim raporu, denetim boyunca uyumluluk hazırlıklarının, güvenlik politikalarının, risk yönetimi prosedürlerinin ve kullanıcı erişim kontrollerinin gücünü kapsayacaktır (Duncan ve Whittington, 2014: 78).

Standartlara uygunluk programları, mevcut kurallar güncellendiği ve yeni düzenlemeler getirildiği için sürekli bir değişim halindedir. Denetim, düzenlemelere ve gereksinimlere uygunluğu sağlamak için değiştirilmesi veya iyileştirilmesi gereken dahili iş süreçlerinin bir taslağını sağlamaktadır. Dikkate alınması gereken kilit alanlar; hassas verilerin güvenliği, finansal raporlama, bordro, İnsan Kaynakları politikaları, yönetim standartları, sağlık ve güvenliktir (Joshi vd., 2010: 260).

1.3. İÇ DENETİMİN TARİHSEL GELİŞİMİ

Tarihçiler, iç denetimin kökenlerinin çok eski zamanlara kadar uzandığını ve tüccarların M.Ö. yüzyıllarda tahıl ticareti için kullanılan makbuzlarının doğrulanması gibi faaliyetlerin varlığına dair kanıtlar olduğunu dile getirmişlerdir. Ancak iç denetim kavramının ve mesleğinin mesleğin gerçek anlamda büyümesi, 19. ve 20. yüzyıllarda kurumsal ticaretin yaygınlaşmasıyla ortaya çıkmıştır. Birçok yerde faaliyet gösteren ve binlerce çalışanı olan şirketler, kontrol sistemlerine olan talebin artmasıyla iç denetim uygulamalarına ağırlık vermişlerdir (www.theiia.org.a). İç denetimin tarihsel gelişimi bu başlık altında dünyada ve Türkiye’de olmak üzere ayrı ayrı açıklanmıştır.

1.3.1. Dünyada İç Denetimin Gelişimi

İç denetimin tarihi incelendiğinde, büyük İtalyan ticaret merkezleri olan Venedik, Milano ve Floransa gibi şehirlerde 13. yüzyılda ortaya çıktığı bilinmektedir. Ancak, kıta Avrupa ülkelerinde denetim ve iç denetim konuları, akademik olarak 1900'lü yıllarda tartışılmaya başlamıştır. Yani, iç denetim kavramı İtalya'da 13. yüzyılda başlamış olsa da, kıta Avrupası'nda akademik tartışmaları 1900'lü yıllarda başlamıştır (Polat, 2016:6). Aynı zamanda İngiliz tüccarlarının dünya ticaretinde önem kazandığı 1800'lerin ortalarında, mallarının kayıtlarının doğruluğunu kontrol etmek için kendi çalışanlarını görevlendirmeleriyle birlikte, iç denetim kavramının ortaya çıktığı bilinmektedir (Cangemi ve Singleton, 2003: 7).

Modern örgütsel organizasyonlarda ise iç denetimin bir işlev olarak ortaya çıkışı 1940'lara denk gelmektedir. Özellikle, 1941 yılında merkezi Amerika'nın Lake Mary, Florida eyaletinde bulunan İç Denetçiler Enstitüsü'nün (IIA) kurulması, dünya çapında iç denetim mesleğinin gelişmesinde ve örgütlenmesinde önemli bir rol oynamıştır. IIA'nın kuruluş belgesi 17 Kasım 1941'de sunulmuştur ve 9 Aralık 1941'de, ilk yıllık toplantısının yapıldığı New York'ta yapılmıştır. Toplantıda 24 kurucu üye üyeliğe kabul edilmiş ve ilk başkan olarak, John B. Thurston görevlendirilmiştir. 2023 yılı itibarıyla IIA tarafından, kuruluşun 230.000'den fazla üyesinin olduğu açıklanmıştır. (Zorlu, 2014:50; Spraakman, 2001:19-41, www.theiia.org:a).

IIA, iç denetim mesleğinin dünya genelindeki en önemli kurumudur ve bu alanda saygın otorite, lider ve savunucudur. Aynı zamanda, IIA üyeleri iç denetim, risk yönetimi, kurumsal yönetişim, iç kontrol, bilgi teknolojileri denetimi, eğitim ve güvenlik gibi konulara odaklanarak çalışmaktadır. IIA, iç denetim mesleğinin dünya çapındaki temsilcisi ve üyeleri için bu alanda etkili bir eğitim ve bilgi kaynağı olarak kabul edilir. IIA'nın amacı, dünya genelindeki iç denetim mesleğine liderlik etmektir. Bu amacı gerçekleştirmek için, aşağıda sıralananlarla sınırlı kalmayacak şekilde temelde şu faaliyetleri yürütmektedir (www.theiia.org:a)

- İç denetim uzmanlarının organizasyonlara sağladığı değeri destekleyerek ve teşvik ederek katkılarını arttırmak,
- Kapsamlı mesleki eğitim ve gelişim fırsatları, standartlar, uygulama kılavuzları ve sertifikasyon programları sunarak iç denetçilerin yeteneklerini geliştirmelerine yardımcı olmak,

- İç denetim, kontrol, risk yönetimi ve yönetişimde uygun rolü araştırmak, yaymak ve uygulayıcılara ve paydaşlara teşvik etmek,
- İç denetimdeki en iyi uygulamalar konusunda uygulayıcıları ve diğer ilgili tarafları eğitmek,
- Tüm dünyadan iç denetçileri bir araya getirerek bilgi ve deneyimlerini paylaşmak.

IIA, 1944 yılında Toronto'da ve 1948 yılında Londra'da olmak üzere Amerika dışındaki ilk iki birliğini kurmuştur. İç denetim, 1990'lardan itibaren kamu sektöründe Amerika, Kanada ve bazı Avrupa ülkelerinde uygulanmaya başlamıştır (www.icisleri.gov.tr).

İç denetimin uygulamaya alınmasının ilk yıllarında, ilgi alanlarının muhasebe ve mali konularla sınırlı olduğu görülmektedir. 1978'de İç Denetçiler Birliği tarafından onayladığı yeni tanımla birlikte iç denetimin alanı iç kontrollerin ve işletme faaliyetlerinin denetimini de kapsayacak şekilde genişletilmiştir. Bugün modern anlamda iç denetim 'risk odaklı denetim' şeklinde anılmaktadır. (Gramling ve Ramamoorti, 2003: 97-113; Türedi vd., 2015: 4).

Risk odaklı iç denetimin gelişim süreci şu şekilde özetlenebilir:

- 1950'lerde varlık koruması
- 1960'larda işletme bilgilerinin bütünlük ve güvenilirliğinin sağlanması,
- 1970'lerde uygunluk denetimi,
- 1980'lerde İşletme etkinliğinin (Performans) denetimi
- 1990'larda iş hedeflerine ulaşılmasının denetimi
- 2000'lerde risk bazlı denetimler yapmak (Özer, 2008: 43).

Avrupa'daki iç denetim mesleğinin ortak sesini temsil etmek üzere 1980 yılında Portekiz, Almanya, Fransa, İngiltere & İrlanda, Norveç ve Benelüks ülkeleri ile resmi bir yapı olarak "Avrupa İç Denetim Enstitüleri Konfederasyonu" (European Confederation of Institutes of Internal Auditing - ECIIA) kurulmuştur. Enstitü; Avrupa Birliği (AB) ve üye ülkelerdeki iç kontrol uzmanlarının konumunu desteklemek; IIA'nın tüm kamu ve özel sektördeki tüm iç denetim faaliyetlerine uygulanmasını teşvik etmek amacıyla kurulmuştur. Ayrıca enstitü; AB Parlamentosu, Komisyonu ve diğer Avrupa düzenleyicileri ve dernekleri gibi önemli paydaşlarla ilişki kurarak iyi kurumsal yönetişim ve iç denetimin önemine destek olmaktadır. ECIIA, Avrupa'da iç denetimin

mesleki uygulamalarını teşvik ederek kurumsal yönetişimi geliştirme rolüne sahiptir. ECIIA'nın üyeleri, Avrupa'nın farklı ülkelerindeki ulusal iç denetim enstitüleri tarafından temsil edilmektedir. Bu enstitüler, özel ve kamu sektörlerinde en iyi uygulamaları geliştirmek, paylaşmak ve teşvik etmek için çalışmaktadır. 2001 yılında tüzel kişilik ECIIA, merkezi Brüksel'de bulunan Uluslararası Kâr Amacı Gütmeyen Kuruluş olarak oluşturulmuştur. ECIIA'nın üye sayısı 2023 yılı itibariyle 48.500'dür (www.eciia.eu).

1.3.2. Türkiye’de İç Denetimin Gelişimi

Türkiye’de İç denetimin gelişim süreci, bu alanda Türkiye’deki önemli bir meslek profesyoneli olan Uzun (1998) tarafından üç aşamada açıklanmaktadır:

Birinci aşama: Cumhuriyetin ilanından sonra, özel sektörün oldukça az olduğu, devletin kontrolü altında olan bir dönemdir. Merkezi hükümet, yetkilerini paylaşmak yerine kamu kurumlarını ve yerel yönetimleri doğrudan kontrol altında tutmak için merkezden atanmış memurlar aracılığıyla sürekli bir denetim politikası izlenmiştir. Bu nedenle, İç Denetim bu aşamada siyasi otoritenin bağımlılığı altında yürütülmektedir.

İkinci aşama: Bu dönemde, özel girişimlerin yaygınlaşması ve sermaye birikiminin artması, üretim ve ticaret hacminin büyük ölçüde artmasına sebep olmuştur. Ancak bu süreç, büyük şirketler ve bankaların yönetimindeki organizasyon ve yönetim sorunlarını da beraberinde getirmiştir. Şirketlerin tek bir merkezden yönetilmesi zorlaştı ve bu nedenle İç Denetim birimi, bu büyük şirketlerin ve bankaların iç kontrolünü sağlamak amacıyla doğrudan yönetimlerine bağlı olarak ortaya çıkmaya başlamıştır. İç Denetim birimi, bu dönemde öncelikle yönetsel amaçlı ve kurum yönetimine bağımlı bir şekilde faaliyet göstermektedir.

Üçüncü aşama: 1980'lerin sonrasında, ülke dışına açılmaya başlanması ticaret hacmini arttırmıştır. Yabancı yatırımlar arttı ve şirketler, halka açılarak çok ortaklı hale gelmiştir. Bu değişimle birlikte, şirketlerin yönetimi de değişerek ve aile şirketi olmaktan çıkmıştır. Profesyonel yönetim anlayışının benimsenmesiyle birlikte, şirket sahipleri ve yöneticileri arasında farklılaşma yaşanmıştır.

Bu dönemde, şirketler daha verimli ve rekabetçi olmak için çalışmalar yürütmüşlerdir ve bu süreçte etkinlik, verimlilik analizleri, performans değerlendirmeleri gibi kavramlar büyük önem kazanmıştır. Bu gelişmeler, İç Denetim kavramının daha da önem kazanmasına neden olmuştur ve artık İç Denetim fonksiyonu yalnızca yönetsel kaygılarla sınırlı kalmamış, ekonomik nedenlerle de şekillenmeye başlamıştır. Bu sebeple

de İç Denetim, organizasyonlar için oldukça kritik rol üstlenmesi kaçınılmaz hale gelmiştir.

Türkiye'de iç denetim uygulamaları, “Türkiye İç Denetim Enstitüsü (TİDE)” ve Hazine ve Maliye Bakanlığı’na bağlı “İç Denetim Koordinasyon Kurulu” gibi kuruluşlar tarafından yürütülmektedir.

TİDE 'nin kuruluşuna yönelik ilk çalışmalar Aralık 1994'te başlatılmıştır. Bu tarihte dört meslek profesyoneli ile IIA Batı Avrupa direktörü arasında yapılan görüşme TİDE'nin kuruluşu için atılan ilk adımdır. 1995 yılında dört profesyonel tarafından başlatılan bu girişim, 47 kurucu üyenin çalışmaları sonucunda "İç Denetim Enstitüsü" adıyla bir meslek örgütüne dönüşmüştür. Bu süreçte, Ali Kamil UZUN başkanlık görevini üstlenmiştir. Kuruluşun ardından ilk Uluslararası İç Denetim Sempozyumu gerçekleştirilerek, sempozyum kitabı yayınlanmıştır. 1996 yılına gelindiğinde ise enstitü, IIA ve ECIIA üyeliğine kabul edilmiştir. Her iki uluslararası örgütün de çalışma komitelerinde yönetim organları ile aktif görev almaktadır. Vizyonunu; “Meslekte küresel gelişim ve mükemmelliğin paydaşı olmak” üzerine kuran TİDE, şirketlerin yönetim kurulları, denetim komiteleri, icra kurulu başkanları, üst düzey yöneticiler ve iç denetçiler, kamu kurum ve kuruluşları, düzenleyici kurumlar, üniversiteler ve akademisyenlere sunduğu hizmetler ile kalıcı değer yaratma misyonunu sürdürmektedir (www.tide.org.tr:a).

TİDE, yaklaşık 1.035 kurumu temsil eden ve 3.159 üyesi olan bir enstitüdür. Enstitü, meslek mensuplarının eğitim ve iletişimini güçlendirmek için kongreler, TİDEX profesyonel söyleşiler, mesleki toplantılar düzenlemekte ve yeni kitaplar çıkartmaktadır. Ayrıca, enstitü yurtdışında yapılan "iç denetçi sertifikası" sınavının Türkçe olarak ülkemizde yapılmasını sağlamaktadır. Böylece TİDE, mesleğin örgütlenmesi için de çaba harcamaktadır (www.tide.org.tr:b, 2021:18)

TİDE, iç denetim mesleğinin gelişimini uluslararası standartlara ulaşmasını amaçlamakta aynı zamanda hem kamu kurum ve kuruluşlarındaki hem de finans ve reel sektör şirketlerindeki mesleğin profesyonellerine; kurumsal yönetim kalitesi ve mesleki yeterlilikler için akademik gelişimlerini sağlayacak çeşitli hizmetler sunmaktadır. Bu bağlamda mesleki gelişim ve yetkinlik eğitimlerinin yanı sıra profesyonel meslek erbaplarına küresel yetkinlik belgesi ile sertifikasyonun artırılmasında destek olmakta aynı zamanda da sürekli profesyonel gelişim konusunda öncülük etmektedir. Bu kurum,

iç denetim biriminde çalışanların yetkinliklerini, özel sektör ile kamu kurum ve kuruluşların yönetsel kalitelerini, iç denetim mesleğinin akademik ilerlemesini geliştirmek için çeşitli hizmetler sunmaktadır. Türkiye İç Denetim Enstitüsü sunduğu servisler ile iç denetim çalışanlarına ve Türkiye iş dünyasına; günceli yakalamak, ilerleme ve büyümenin ana partneri olmakla ilgili çeşitli olanaklar sunmaktadır.

Türkiye'nin 1999'da Helsinki konferansında Avrupa Birliği'ne resmi olarak aday gösterilmesinden sonra mali yönetim, iç denetim ve kontrol alanındaki olması gereken kanuni düzenlemelerin AB standardıyla uyumlu hale getirilmesi açısından gerekli çalışmalar başlatılmıştır. Bu çalışmalar sonucunda kamuda yer alan iç denetim gereksinimlerinin farkına varılmış ve ilk önce TC Merkez Bankası 2002'de İç Denetim Genel Müdürlüğü'nü kurup faaliyete geçirmiştir ([http:// www.icdenetim.net](http://www.icdenetim.net), 2022). İç denetim, kuruluş ve paydaşları için tarafsız, bağımsız ve nesnel hizmetler sunduğu için hem özel hem de kamu kuruluşlarında kurumsal yönetimin önemli bir parçası olarak tanımlanmaktadır (Davidson vd., 2013: 44). Bu yaklaşım, 2004 yılında Türkiye'de kamu sektöründe 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun kabulü ile benimsenmiştir. Daha sonra iç denetim, iç kontrol ve risk yönetimi uygulamaları AB direktifleri dikkate alınarak uluslararası standartlarla uyumlaştırılmıştır (Çevikbaş, 2011: 49).

24.12.2003 tarihli ve 25326 sayılı Resmi Gazetede çıkan ve tüm maddeleriyle 01.01.2006 tarihinden başlayarak yürürlüğe giren ve daha önce de tanımlanan 5018 sayılı “Kamu Mali Yönetim ve Kontrol Kanunu”; düzenleyici ve denetleyici kurumlar dahil olmamak şartıyla, genel yönetim içindeki kamu kurum ve kuruluşlarında iç denetimin kurulmasını hedeflemektedir. Düzenlenen Kanun içerisinde, iç denetim faaliyetinin doğru olarak yürürlüğe girmesini ve kamu kurum ve kuruluşlarında işletilebilmesi için gerekli araştırmalar yapılmış ve hem idari hem de yasal düzenlemenin oluşturulması temelinde oldukça önemli işlemler gerçekleştirilmiştir (<http://www.icdenetim.net>, 2022).

Diğer taraftan, bu kanun sürekli gözden geçirilmekte ve Avrupa Birliği uygulamalarına uygun olup olmadığı yeniden değerlendirilmektedir. Dünyada hızla artan ve etkin bir biçimde uygulanan “medeni” bir denetim sistemi olan iç denetim yaklaşımı, ülkemiz bakımından taze bir yaklaşım olmasının yanı sıra, halen kamu kurumlarınca içselleştirilme, benimsenme ve ilerletilme sürecindedir. Bu sistem hem kullanılan kaynakların etkinliği ve verimliliği, hem de bilginin güvencesi, performans kontrolü ve

şeffaflık ilkeleri bakımından hızla önemli hale gelmektedir. İç denetimin özünde bir güvence işlevi vardır. Çünkü iç denetim faaliyeti sonucunda organizasyona ve organizasyon dışındaki ilgili taraflara tarafsız bir güvence verilmektedir. Bu güvence, üretilen bilgilerin doğruluğunu ve eksiksizliğini içerir; faaliyetlerin etkin, ekonomik, verimli ve mevzuata uygun olarak işletilip işletilmediğini; organizasyonlarda nerelerde ve hangi işlemlerin denetlenip veya denetlenmediğini göstererek tarafsız bir denetim raporu sunmaktadır (Çevikbaş, 2011: 49-50).

Türkiye’de İç denetim 5018 sayılı kanunun 63. maddesindeki bir tanımlamada şu şekilde tanımlanmış ve belirginleştirilmiştir; “kamu idaresinin çalışmalarına değer katmak ve geliştirmek için kaynakların ekonomiklik, etkinlik ve verimlilik esaslarına göre yönetilip yönetilmediğini değerlendirmek ve rehberlik yapmak amacıyla yapılan bağımsız, nesnel güvence sağlama ve danışmanlık faaliyetidir. Bu faaliyetler idarelerin yönetim ve kontrol yapılarıyla mali işlemlerin risk yönetimi, yönetim ve kontrol süreçlerinin etkinliğini değerlendirmek ve geliştirmek yönünde sistematik, sürekli ve disiplinli bir yaklaşımla ve genel kabul görmüş standartlara uygun olarak gerçekleştirilir.” (Bütçe ve Mali Kontrol Genel Müdürlüğü, 2004: 452).

T.C. Hazine ve Maliye Bakanlığı tarafından kurulan İç Denetim Birimi Başkanlığı Türkiye’deki en üst makamdır. Bu birim 5018 sayılı Kanuna dayanarak, şu şekilde resmiyet kazanmıştır; “İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmeliğin 13’üncü maddesi ve İç Denetim Koordinasyon Kurulu’nun (İDKK), İç Denetçi Atamalarında Uyulacak Esas ve Usuller Hakkında Tebliği (Sıra No 1) gereğince Bakanlığımız İç Denetim Biriminin kurulması ve Başkanın görevlendirilmesine dair Müsteşarlık Makamının 24.04.2007 tarihli Onayı, Üst Yönetici ve iç denetçilerce imzalanan İç Denetim Birimi Yönergesi uyarınca Bakanlığımız İç Denetim Birimi Başkanlığı faaliyetlerine başlamıştır”. Bakanlıkta 35 iç denetçi kadrosu vardır ve kuruluş sırasında, daha önce merkez denetim elemanı sayılanlar içinden 17 iç denetçi göreve atanarak, hâlihazırda Başkanla beraber 7 iç denetçi görev yapmaktadır. İç Denetim Birimi’nin genel yönetim yapısı ve görevleri şu şekilde sıralanmaktadır (www.hmb.gov.tr):

- Birim, Yönetimsel olarak direkt Müsteşara bağlıdır ve yönetsel faaliyetlerden farklı bir işleve sahip olduğundan dolayı Bakanlığın diğer birimleriyle hiyerarşik bir ilişkisi yoktur.

- İç Denetim Birimi suçla ilgili ihbar ve şikayetleri takip eden bir birim değildir. Ancak, görev alanına giren risklerin değerlendirilmesi, suiistimallerin önlenmesi, gerekli incelemeler ve Üst Yöneticinin talebi üzerine İDKK tarafından belirlenen limitler dahilinde ihbar ve şikayetler hakkında soruşturmalar yürütebilir. İnceleme ve denetimler sırasında suça konu teşkil eden eylemler soruşturulmak üzere Kıdemli Yönetici 'ye bildirilmektedir.
- İç Denetim Birimi, teftiş, soruşturma ve dış denetim faaliyetlerini yürüten diğer birimlerle rekabete girmez, suiistimallerin önlenmesi ve suç teşkil eden fiillere ilişkin belge ve bilgilerin sağlanması konularında bu birimlerle işbirliği yapmaktadır.
- İç denetim birimi faaliyetlerinin standartlara uygunluğu ve kalitesi ölçüldüğü için denetim faaliyetleri ve denetçiler ile ilgili şikayet ve görüşlerin İç Denetim Birimi'ne ve İDKK'ya iletilmesi mümkündür.

Türkiye'de iç denetim konusunda ayrıca, Sermaye Piyasası Mevzuatı, Bankacılık Kanunu, Sigortacılık Mevzuatı, Kamu Mali Yönetim Kanunu ve Yeni Türk Ticaret Kanunu Tasarısı gibi hukuki düzenlemeler bulunmaktadır. Bu düzenlemeler, iç denetimin yasal çerçevesini oluşturmakta ve şirketlerin, finansal kuruluşların ve kamu kurumlarının iç denetim faaliyetlerini yönetmelerini sağlamaktadır.

1.4. ULUSLARARASI İÇ DENETİM STANDARTLARI

Bugünün iş dünyasında, verimli ve etkili bir iç denetim fonksiyonuna sahip olmak çok önemlidir. İç denetim, sağlıklı bir kurumsal yönetişimin temel taşıdır ve kurumsal yapı için kritik bir öneme sahip olduğundan, yönetim kurulu, iç denetçilerin etkili bir şekilde hizmet etmesini sağlamakla sorumludur. Bunun için de Uluslararası İç Denetim Standartları önemli bir araçtır. Standartlar, organizasyondaki iç denetçilerinin hizmetlerini tutarlı, doğru ve uygun maliyetli bir şekilde sağlamak ve kurumsal değeri korumaktadır. Standartlar ayrıca şunları sağlar ([www.theiia.org:b](http://www.theiia.org/b)):

- Geniş bir değer artırıcı iç denetim yapmak için bir çerçeve sunar.
- İç denetimin uygulamasını temsil eden temel prensipleri belirler.
- İç denetim performansının değerlendirilmesinin temelini oluşturur.
- İyileştirilmiş kurumsal süreçlerin ve işlemlerin oluşmasını destekler.

İç denetim işlevlerinin kapsamını belirleyen standartlar IIA tarafından yayımlanmaktadır. Standartlar iç denetimin rolü ve sorumluluklarını özetlemek amacıyla

oluşturulmuş, daha sonra bu standartlar, "İç Denetim Mesleği Uygulama Standartları" adı altında bir araya getirilerek yürürlüğe girmiştir. IIA, Mesleki Uygulama Çerçevesi adı verilen iç denetim kılavuzunun kavramsal çerçevesini belirleyerek, iç denetim standartlarının anlaşılmasını ve uygulanmasını kolaylaştırmaktadır. Bu çerçeve, iç denetim faaliyetleri için farklı yaklaşımların sürekli olarak güncellenmesini sağlamaktadır. Ayrıca, IIA, iç denetçilerin eğitimine yönelik sertifikasyon programları sunarak, profesyonel olarak iç denetim faaliyetlerinin yürütülmesine yardımcı olmaktadır. Yönetim Kurulu tarafından kabul edilen bu standartlar, iç denetim mesleğinin en saygın otoriteleri tarafından belirlenmiştir.

IIA'nın 2003 yılında güncellediği iç denetim standartları, o dönemdeki risk yönetimi ve kurumsal yönetim gereksinimlerine uygun olarak şekillendirilmiştir. Standartlar, iç denetçilerin sadece danışmanlık faaliyetleri yürütmelerine değil, aynı zamanda görev sonuçlarının da paylaşılmasına odaklanmalarını öngörmektedir. Bu şekilde, iç denetim faaliyetlerinin değer yaratan bir rol oynaması ve organizasyonların hedeflerine ulaşmasına katkı sağlaması amaçlanmaktadır. Bu standartlar, 2004 yılından itibaren tüm IIA üyeleri ve Uluslararası İç Denetçiler (Certified Internal Auditor -CIA) için zorunlu hale getirilmiştir (Kalender, 2008: 100).

Uluslararası İç Denetim Standartları, nitelik ve performans olmak üzere iki temel kategoriye ayrılmaktadır. Nitelik standartları, iç denetim faaliyetinin yönetmeliklerle ilgili yönlerini kapsarken, aynı zamanda bağımsızlık ve objektiflik, mesleki yeterlilik, özenli çalışma, sürekli mesleki gelişim, kalite güvence ve geliştirme programlarını da içermektedir. Performans standartları ise iç denetim faaliyetinin yönetimi, görev planlaması, icra edilmesi, sonuçların raporlanması, takibi ve risk yönetimi ile ilgili bilgiler sağlamaktadır. Standartlar, iç denetim faaliyetinin sağlıklı bir şekilde yürütülmesi ve mesleki standartların korunması için önemlidir. Bu standartlar, uygulama önerileriyle birlikte iç denetçilere rehberlik etmek için tasarlanmıştır.

IIA tarafından belirlenen standartlar ilke odaklı olarak hazırlanmıştır. Standartlar, iç denetimi gerçekleştirmek ve teşvik etmek için bir çerçeve sağlamaktadır. Standartların doğru bir şekilde anlaşılması ve uygulanması için hem ifadelerin hem de yorumların dikkate alınması gerekmektedir. Standartların bir parçası olan sözlükte belirtilen özel anlamlar verilen terimler kullanılarak standartların daha iyi anlaşılması sağlanmaktadır (www.theiia.org:c).

Uluslararası İç Denetim Standartları, diğer standart koyan kuruluşların standartları ile birlikte kullanılabilir şekilde tasarlanmıştır ve iç denetim raporlarında bu standartlara gerektiğinde referans verilebilir. Bununla birlikte, eğer IIA standartları ile diğer kuruluşların standartları arasında bir tutarsızlık veya uyumsuzluk varsa, iç denetim faaliyeti ve iç denetçiler IIA Standartlarına uyum sağlamak zorundadır. Bu, iç denetim faaliyetinin niteliğini, objektifliğini ve uygunluğunu sağlamak amacıyla IIA'nın standartlarına uygun bir şekilde uygulanması gerektiği anlamına gelir (ECIIA, 2005: 21-22).

1.5. İÇ DENETİM TÜRLERİ

İç denetim, organizasyonun faaliyetlerinin etkinliğini, verimliliğini ve uygunluğunu değerlendiren bir süreçtir. İç denetim, bir organizasyonun risklerini yönetmesine, iş süreçlerini kontrol etmesine ve yönetim yapısını geliştirmesine yardımcı olur. Ayrıca iç denetim faaliyetleri, organizasyonun hedeflerine ulaşmasına katkıda bulunarak, yönetim sürecinin daha etkin ve verimli bir şekilde yürütülmesine destek olur. Bu sayede işletme, operasyonel risklerini minimize edebilir, kaynaklarını doğru şekilde kullanarak daha iyi sonuçlar elde edebilir ve yönetim ekibi karar alırken daha güvenilir bilgilere sahip olabilir. İç denetim faaliyetleri ile organizasyonun süreçlerindeki ve dahili kontrol ortamındaki zayıflıklar tespit edilerek, organizasyona zarar verebilecek durumlar mümkün olan en kısa sürede düzeltilebilir. Bir organizasyon için iç denetim planı, en büyük risk alanlarının tespiti ve yönetimi için tasarlanmalıdır. Plan aynı zamanda organizasyonun hedefleri ve stratejik ihtiyaçları doğrultusunda şekillendirilmelidir. Bu şekilde iç denetim faaliyetleri, organizasyonun iş süreçlerinin etkinliğini artırarak riskleri azaltabilir ve hedeflerine ulaşmasına yardımcı olabilir.

Bir organizasyonun performansını veya bir sürecin yürütülmesini bir dizi standart, politika, ölçü veya düzenlemeye göre değerlendirmek için iç denetimden yararlanılmaktadır. Bu denetimler, organizasyonların ihtiyaçlarına ve yapısına göre farklılaşabilmektedir. Bu farklılaşma sonucunda iç denetim türleri; mali denetim, uygunluk denetimi, performans denetimi, sistem tabanlı denetim ve bilgi teknolojisi denetimi olmak üzere beş başlık altında açıklanabilmektedir. Daha farklı iç denetim türleri de ihtiyaçlar noktasında kullanılabilmektedir.

1.5.1. Mali Denetim

Mali denetim, mali tabloların ve tabloların dayanağını oluşturan muhasebe kayıtlarının gözlenmesi ve raporlanmasını kapsamaktadır. Mali denetim, bu raporlara dayanak oluşturan kayıtlar, belgeler ve diğer bilgiler üzerinde yapılan çalışmalara dayanan ve işletmenin finansal tablolarının genel hükümlere uygun olarak hazırlanıp hazırlanmadığını belirlemek amacıyla yapılan bir denetim türüdür. Kabul edilen muhasebe ilkeleri ve işletmenin yasal statüsüne uygun olarak sonuçların bir denetim raporunda özetlenmesinin yanı sıra sistematik bir incelemesini de oluşturmaktadır.

Mali denetimde, genellikle denetime esas alınan mali tablolar; bilanço, gelir tablosu, birikmiş karlar tablosu ve nakit akış tablosu. Ayrıca satışların maliyet tablosu, nakit akım tablosu, kar dağıtım tablosu ve öz kaynaklar değişim tablosu olup bilanço ve gelir tablosu dip not ve ekleri ile birlikte ana mali tabloları oluşturup diğerleri ise ek mali tabloları oluşturmaktadır (Aslan, 2010: 75-76).

1.5.2. Uygunluk Denetimi

Uygunluk denetimi, bir organizasyonun mali işlemlerinin ve diğer faaliyetlerinin belirli yöntem, kural ve mevzuata uygunluğunun gözlenmesidir (Koçak, 2010: 125). Denetimlerin yapılması, kanıtların toplanması, değerlendirilmesi, sonuçların oluşturulması ve denetim sürecinin belgelenmesi, denetlenebilir organizasyonlarla iletişim kurulması ile ilgilidir ve bir denetim stratejisi ile planının tamamlanmasından sonra başlamaktadır. Planlama aşamasında denetçiler, denetim kanıt toplamaya başlamadan önce uygunsuz durumları önlemek, tespit etmek ve düzeltmek için iç kontrolleri ve kurumsal düzenlemeleri gözden geçirmektedir. Uygunluk denetiminin adımlarını şu şekilde sıralanabilmektedir: (Slobodanyk vd., 2018: 322).

- Denetçiyle görüşükten sonra organizasyon, denetçinin uzmanlığının uygun olup olmadığına karar verilir.
- Bir ön toplantıda denetçi, denetim yönergelerini ve nelerin gerekli olduğunu açıklar. Denetçi, müşterinin hazırlaması için denetim kontrol listeleri oluşturmaktadır.
- Organizasyon, denetim anketlerini doldurup denetçiye gerekli belgeleri sağladıktan sonra, denetçi, belgeleri görüntülemek, çalışma alanlarında gezinmek, altyapı ve güvenlik özelliklerini incelemek ve yönetim ve çalışanlarla görüşmek için yerinde çalışabilmektedir.

- Rapor nispeten kısa sürede teslim edilmelidir. Son toplantıda denetçi raporu tartışıp ve risk alanlarını ele almak için tavsiyelerde bulunmaktadır. Düzenleyici bir süreç içinde faaliyet gösterebilir veya göstermez, organizasyonların düzeltici eylemleri tamamlamalarını sağlamak için genellikle orta vadede eksiklikleri gidermeleri gerekmektedir. Bazen denetim firmaları, organizasyonların riskleri veya eksiklikleri düzeltmelerine yardımcı olmak için takip desteği sağlamaktadır. Denetçiler daha sonra bu önlemlerin karşılanıp karşılanmadığını kontrol etmektedir (Slobodanyk vd., 2018: 322-325).

1.5.3. Performans Denetimi

Performans denetiminde organizasyonun önceden belirlenmiş amaç ve hedeflerine ulaşıp ulaşılmadığı ölçülmeye çalışılmaktadır. Bu yönden performans denetimi, bir organizasyonun faaliyetlerini yürütmek için kullandığı kaynakların etkililik, ekonomiklik, verimlilik ve etkinlik açısından denetlenmesidir. Performans denetiminin faaliyet bazında gerçekleştirilmesi halinde, faaliyet denetimi olarak da ifade edilmektedir (Aslan, 2010: 76)

Uluslararası Yüksek Denetim Kurumları Standartlarının (ISSAI-1) ilgili kısmında, Denetçinin, performans denetiminde, kaynakların elde edilip kullanılmasındaki tutumluluk, verimlilik ve amaçlara ulaşmadaki etkinliğinin rapor edileceğini ifade eder. Bu tür raporlar kapsam ve nitelik bakımından önemli ölçüde farklı olabilir. Örneğin kaynakların sağlıklı şekilde kullanılıp kullanılmadığını kapsayabilir; program ve politikaların etkisi konusunda yorum yapabilir ve iyileştirmeye yol açacak değişiklikler tavsiye edebilir (www.sayistay.gov.tr, s.163).

1.5.4. Sistem Tabanlı Denetim

Sistem tabanlı denetim, iç kontrol sisteminin işleyişinin ve etkinliğinin ayrıntılı bir şekilde incelenmesidir. İç kontrolün ciddi bir parçası olan iç denetim, aynı zamanda iç kontrol sisteminin hedefine uygun olarak işlediğine dair güven sağlamak ve karşı karşıya olduğu riskleri en aza indirmektedir. Bu sonuca ulaşmak, bir sistem denetimi veya sistem tabanlı bir denetimin gerçekleştirilmesine bağlıdır (Arcagök ve Erüz, 2006: 204-205).

1.5.5. Bilgi Teknolojisi Denetimi

Bilgi teknolojileri denetimleri oldukça detaylı ve önemli bir süreçlerdir. Bu süreçlerin doğru ve eksiksiz bir şekilde yürütülebilmesi için denetimin yeterli teknolojik bilgiye sahip denetçiler tarafından gerçekleştirilmesi veya denetim sırasında bilgi teknolojileri konusunda uzmanlardan destek alınmalıdır. Bu sebeple bilgi teknolojilerinde denetim faaliyetlerinden bahsedebilmek için öncelikle bilgi teknolojileri denetçilerinin yetiştirilmesi ve bilgi teknolojileri denetim eğitimleri ve seminerleri düzenlenmelidir (Özbilgin, 2003: 127).

Sürekli değişen teknolojik gelişmeler sayesinde işletmeler faaliyetleri ile ilgili işlemlerin büyük bir kısmını sanal ortamda gerçekleştirmektedir. Sanal ortamda oluşturulan ve saklanan bilgiler her zaman risklidir. Bilgi teknolojileri denetimi ile birlikte sistemin güvenilirliğinin ve yeterliliğinin test edilmesi amaçlanmaktadır (Ocak, 2021: 41-42)

İç denetçiler; bilgi teknolojisi denetimi yaparak organizasyonun bilgi teknolojisi hedeflerine ulaşabilmesi için kontrollerin etkin bir şekilde çalışıp çalışmadığını kontrol etmektedir. Bir denetimin kapsamı, sistemleri incelemek, ilgili kanıtları toplamak ve değerlendirmek ve bilgi teknolojisi ile ilgili objektif güvence sağlamak için sonuçları üst yönetime raporlamaktır. İç denetim standartlarında yer alan gizlilik, etkinlik, bütünlük, kullanılabilirlik, uygunluk ve güvenilirlik kavramları çerçevesinde bilgi teknolojilerini denetimi uygulanmaktadır.

İç denetçiler denetim sırasında kontrol bazlı bazı eksiklerle karşılaşmaktadır. Bunlar:

- Organizasyonun bilgi teknolojileriyle ilgili politika ve prosedürlerinin güncellenmemesi veya olmaması,
- Görev, yetki ve sorumlulukların personele yeterince aktarılamaması,
- Saldırı tespit ve güvenlik sisteminin aktif çalışmaması,
- Antivirüs programının olmaması,
- Şifre ve kodlarla ilgili kuralların bulunmaması,
- Güvenlik açıklarının sisteme yüklenmemesi,
- Veri tabanı güvenliği ile ilgili tedbirlerin alınmaması,
- Sistemlerde kullanıcı adı, şifre gibi tanımlı işlemlerin giriş sayfalarında SSL ile yapılandırılmamış olması,

- Organizasyon için önemli olan sunucuların güvenli alanlarda olmaması.

Bilgi sistemlerindeki kontroller etkin bir şekilde çalışmıyorsa, organizasyonun tüm kayıtları için büyük bir risk faktörü vardır. Örneğin; üst yönetiminin aldığı yanlış bir karar, bilgi sistemindeki kontrol zayıflığı nedeniyle bu kararın etkisi ölçülemez boyutlara varabilmektedir.

BT denetimleri, diğer denetim türlerinde olduğu gibi mali kayıtların veya iş süreçlerinin denetiminden bahsetmez. BT denetimi söz konusu olduğunda, bilginin kalitesini ve güvenilirliğini sağlamak için kullanılan teknolojilerin denetimi akla gelmelidir. Bu nedenle diğer denetim türlerinden farklıdır fakat birbirleriyle sürekli etkileşim halindedirler. Çünkü denetim türlerinin hepsinde denetim ilkeleri ve uygulama standartları bir temele dayanmaktadır (Ocak, 2021: 41-42).

1.6. KAMUDA İÇ DENETİM VE İŞLEYİŞİ

İç denetimin kamu yönetimi tarafından tanımı, olası ihlalleri, hataları ve boşa giden eylemleri en aza indirmek amacıyla, kurumu oluşturan tüm sistem ve süreçleri izlemek ve değerlendirmekle yönetimin görevlendirdiği birim tarafından yürütülen kurum içindeki bir dizi faaliyetlerdir (Bayrakçı ve Demirel, 2017: 54).

Uluslararası camiada çağdaş denetim yaklaşımı olarak kabul edilen iç denetimin kamuda başarıyla uygulanabilmesi, sürdürülebilmesi ve kuruma değer katabilmesi için üst yönetimin yanı sıra iç denetçilerin de bilgi birikimi ve temel yetkinliklerle donatılması büyük önem taşımaktadır. Risk temelli bir yaklaşımla katma değer oluşturan iç denetim faaliyetlerinin oluşturulması, üst yönetim ile denetlenen birimler arasında farkındalığın artırılmasına ve risk yönetimi süreçlerinin iyileştirilmesine bağlıdır. İç denetim birimleri risk yönetimi ve kurumsal yönetim süreçlerini doğru bir şekilde tasarlayıp ilgili konularda değerlendirmeler yaparak üst yöneticilere hesap verme sorumluluklarını yerine getirme esnasında karar verirken önemli rol oynamaktadır (Uysal, 2018: 36).

Buradaki en önemli nokta, kurumsal risk yönetimi alanında karar verme yetkisine sahip olan üst yönetimde iç denetim birimi veya elemanının söz sahibi olamaması, sadece tavsiyelerde bulunabilmesidir. Aksi halde iç denetçi; sağlayacağı güvence hizmetleri ile ilgili olarak bağımsızlığını kaybedebilir (Türedi vd., 2015: 12).

Türkiye'de kamu mali yönetimi ve kontrol sisteminin eksikliklerini gidermek amacıyla Avrupa Birliği ile uyumlu hale gelmek için denetim faaliyetleri alanında çalışmalar yapılmıştır. Bu doğrultuda hazırlanan kanun Türkiye Büyük Millet

Meclisi'nde 10.12.2003 tarihinde 5018 sayı ile kabul edilmiş, 24.12.2003 tarihli Resmi Gazete'de yayımlanarak kısmen yürürlüğe girmiştir. Kanunun adı: 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'dur. Bu düzenleme, denetim faaliyetlerinin mevcut kriterlere uygun hale getirilmesine ve daha etkili bir şekilde yapılmasına olanak tanımaktadır. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanununun 64. Maddesine göre iç denetimin görevleri aşağıdaki gibidir:

- Objektif bir risk analizine dayalı olarak kamu idarelerinin yönetim ve kontrol yapılarının değerlendirilmesi.
- Kaynakların verimli, ekonomik ve etkili kullanımına yönelik çalışmalar yapılması ve önerilerde bulunulması.
- Bir ödeme sonrası uyumluluk denetiminin gerçekleştirilmesi.
- Mali işlemlerle ilgili idari giderlerin, kararların ve tasarrufların, politika ve hedeflere, programlara, kalkınma planına, stratejik planlara ve performans programlarına uygunluğunun izlenmesi ve değerlendirilmesi.
- Mali yönetim ve kontrol süreçlerine ilişkin sistematik bir denetim gerçekleştirilmesi ve sorunlar hakkında önerilerde bulunulması.
- Denetim sonuçları neticesine göre geliştirmelere dair tavsiyelerde bulunulması.
- Denetim esnasında veya denetim neticesine göre soruşturma açılacak bir durumla karşılaşıldığında üst yönetim amirine bildiride bulunulması

İç denetçi bahsedilen bu görevleri yerine getirirken, İç Denetim Koordinasyon Kurulunca belirlenen ve uluslararası kabul görmüş kontrol ve denetim standartlarına uymalıdır (Korkmaz, 2007: 10-11).

1.7. ÜNİVERSİTELERDE İÇ DENETİM VE İŞLEYİŞİ

1982 Anayasası'na göre, üniversitelerin kuruluş amacı ülkenin ihtiyaçlarına yönelik nitelikli insan kaynağı yetiştirmek, bilgi üretmek ve topluma faydalı hizmetler sunmaktır. Üniversiteler, 2547 sayılı Yükseköğretim Kanunu uyarınca bilimsel özerkliğe ve kamu tüzel kişiliğine sahip olan kurumlardır. Bu kurumlar, fakülteler, enstitüler, yüksekokullar ve benzeri birimlerden oluşmaktadır. Yükseköğretim kurumları, yüksek kalitede eğitim-öğretim, bilimsel araştırma, yayın ve danışmanlık hizmetleri sunarak topluma katkıda bulunmaktadır (<https://www.mevzuat.gov.tr>, 2023).

Kamu tüzel kişiliği olan üniversiteler için iç denetim ihmal edilemez bir yönetim faaliyetidir. Bu yüzden iç denetim faaliyetlerinden iç denetçiler, mali, yönetsel ve iç kontrol süreçlerinin işleyişinden de üst yönetim sorumludur. 5018 sayılı kanun gereği Yükseköğretim Kurulunun (YÖK) sorumluluğu, Yükseköğretim yıllık ana program ve ana stratejik planlarını yapmasıdır. Aynı zamanda üniversitelerin hazırlamış olduğu plan ve programların Yükseköğretimin kendisinin hazırlamış olduğu ana plana uygunluk seviyesini gözlemleyip denetlemesidir.

Üniversitelerde iç denetim işlemlerinin gerçekleştirilebilmesi için ulusal ve uluslararası standartlara uygunluğun sağlanması gerekmekte olup, bu nedenle üniversitelerin kamu kurumu niteliği taşıması sebebiyle üst yönetimle ilgili bir birim oluşturulması gerekmektedir. Bu birimler, iç denetim faaliyetlerinin yapılabilmesi için iç denetim birimlerinin kurulmasını zorunlu kılmaktadır (Aydın, 2021: 12).

5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu'nun yürürlüğe girmesiyle birlikte kamu mali yönetiminde önemli adımlar atılmıştır. Bu adımların biri de üniversitelerde iç denetim birimlerinin oluşturulmasıdır. İç denetim birimleri tarafından yapılan sistemli çalışmalar, raporlama ve iyileştirme çabaları sayesinde kamusal kaynakların kullanımı daha düzenli hale getirilmiştir. Bu uygulamanın sonuçları da olumlu yönde görülmüştür.

Üniversitelerin, ortaya çıkabilecek risklerden korunabilmesi ve yönetimin standartlara uygun hareket edip etmediğinin bilinebilmesi için etkili bir iç kontrol ve iç denetim sistemi kurulması gerekmektedir. Bu sayede üniversitelerde gerçekleşen tüm olaylar ve gelişmeler izlenebilir ve denetlenebilir hale gelir. İç denetim sistemi, üniversitelerin özerkliği göz önünde bulundurularak, önemli bir mekanizma olarak karşımıza çıkmaktadır. Bu mekanizmanın etkin bir şekilde işletilmesi, üniversitelerin karşılaşılabileceği riskleri minimize etmesine yardımcı olacaktır (Zorlu, 2014: 2,157).

Üniversitelerdeki tüm birimler ve bu birimlerde yürütülen faaliyetlerin denetlenmesi, iç denetim faaliyetlerinin kapsamına girmektedir. Rektörlük, fakülteler, yüksekokullar, araştırma merkezleri, daire başkanlıkları, enstitüler, işletme müdürlükleri, tüm finansal ve önemli sistemlerin yanı sıra okullar ve diğer alt birimler, iç denetim biriminin faaliyetleri, süreçleri veya projeleri ile değerlendirilmektedir. Denetim kapsamı, iç denetim birimi tarafından belirlenir ve faaliyetler, süreçler veya projelerin

değerlendirilmesini içermektedir. Bu bağlamda üniversitelerin iç denetime konu olan faaliyetleri Öz (2015:107-108) tarafından 12 başlık altında toplanmıştır:

a) Yüksek Okul, Meslek Yüksek Okulları ve Fakülteler

- Bakım, onarım, yenileme ve satın alma işlemleri,
- Öğrenci ödemeleri ve harcırah giderleri,
- İçerik ve web site işlemleri,
- Akademik işlem raporları, bölüm ve fakülte raporları,
- Personel işlemleri ve bütçe hazırlanması,
- Erasmus projeleri gibi öğrenci kayıt işlemleriyle alakalı olarak öğrenciler için tahsis edilen bütçenin takibi,
- Alt yapı olanaklarının belirlenmesi, onarılması ve inşa edilmesiyle alakalı ihale, proje ve planların kurulan komisyonlar aracılığıyla kabulü,
- Yıl sonu tablolarının hazırlanması.

b) Yapı İşleri Birimi

- Yatırım programlarının hazırlanması,
- Yeni projelerin inşası, binaların bakım ve onarımı,
- Yeni kabul görülen yönetmeliklerin belirlenmesi

c) Bilgi İşlem Birimi

- BT birimi tarafından alınan donanım ve yazılımlar,
- Bilgi işlemin güvenliğinin izlenmesi,
- Mal ve hizmet edinimleri,
- Bilgisayar işlemleri.

d) Sağlık Kültür ve Spor Birimi

- Sağlık, spor ve kültür birimi aracılığı ile öğrencilerin barınma ve beslenme giderlerinden elde edilen gelirin bütçelenmesi.

e) Mali ve İdari İşlemler Birimi

- Yatırım bütçesinin teklifi,
- Makine-donanım ve sistem hizmeti edinimlerinin teklifinin hazırlanması,
- İdari ve akademik personelin maaş işlemleri.

f) Kütüphane Birimi

- Kütüphane işlemleri,

- Kullanıcı hizmetleri,
- Danışmanlık hizmetleri,
- Kategori etme ve kataloglama işlemleri,
- Elektronik kütüphanecilik işlemleri.

g) Personel Daire Başkanlığı

- İdari ve akademik personel alımları,
- Yurt dışı ödenekleri,
- Taşınır eşya işlemleri,
- Yurtdışı eğitim İşlemleri
- Personel emeklilik işlemleri,
- Ek ödeme, e-bütçe tazminat işlemleri,
- İstatistiki bilgiler ve faaliyet raporları

h) Strateji Geliştirme Birimi

- Birimin hazırlamış olduğu stratejik planlar,
- Bütçenin mali programının hazırlanması

i) Hukuk Müşavirliği Birimi

- Birim tarafından kurumun lehine veya aleyhine sonuçlanan davalar için idari yargı işlemleri,
- Yüksekokullarda öğrencilerden alınması gereken ödemelerin alınamaması durumunda icra takibinin başlatılması,
- İcra işlemleri süreciyle ilgili takip işlemleri.

j) Araştırma ve Uygulama Merkezleri

- Bilimsel projeler için ayrılan ödenekler ve diğer organizasyonlarda yapılan ortak projeler ve araştırmacılara ayrılan ödenekler.

k) Döner Sermaye Faaliyet Müdürlüğü

- Döner sermaye ihale süreci, bütçe ve muhasebe işlemleri ile gelir işlemleri.

l) Arşiv Ve Şube Müdürlüğü'ne Yapılan Evrak Kayıt Ve O Üniversite Biriminde Gerçekleştirilen Yazışmalar

- YÖK işlemleri,
- Fen, Eğitim ve Sosyal Bilimler Enstitüsü ve diğer enstitüler tarafından gerçekleştirilen mezuniyet ve tez bitirme işlemleri,

- Doktora ve yeterlilik işlemleri,
- Ek ders ödemeleri
- e-mail süreçleri

Üniversitelerin hedeflerine ulaşmalarına yardımcı olmak için, üniversite kaynaklarının etkin, verimli ve ekonomik bir şekilde kullanılmasını sağlamak için bir iç denetim sistemi kurulması gerekmektedir. Üniversitelerde iç denetim süreci, öncelikle denetlenecek birim ve alanların belirlenmesiyle başlar. Daha sonra risklerin tanımlanması ve önceliklendirilmesi, kaynakların tahsis edilmesi, planlama ve onaylama ile iç denetim programının hazırlanması adımlarından geçer. Program onaylandıktan sonra, denetimi yapacak iç denetçilere görev yazısı gönderilir. İç denetçiler görevlendirildikten sonra, denetlenecek birime bildirim yazısı gönderilir ve denetim süreci başlatılır. Bu süreç, üniversitelerin kaynaklarının etkili bir şekilde kullanılmasını ve amaçlarına ulaşmalarını sağlamak amacıyla önemlidir.

1.8. İÇ DENETİM MESLEĞİ VE ULUSLARARASI İÇ DENETİM MESLEĞİ DÜZENLEMELERİ

Organizasyonların işleyiş süreçlerini analiz edip raporlamasını yapan kişilere “iç denetçi” denilmektedir. (İenstitü, 2021). Bugün iç denetim mesleğinin önemi önceki dönemlere göre organizasyonlara sağladığı katkılar nedeniyle daha fazladır. Bu yüzden iç denetimin uygulanması hayati önem taşımaktadır. Denetçi, organizasyonların görevlerini idam etmeleri için maliyet kontrolleri, risk değerlendirme ve olası risklerle karşılaşılması durumunda etkisinin azaltılması için alınacak tedbirler konusunda tavsiyelerde bulunmakla sorumludur.

Uluslararası İç Denetçiler Enstitüsü, iç denetim mesleğinin standartlarını oluşturur ve yayınlar. Bu alanda yapılan araştırma ve geliştirme çalışmalarıyla, uluslararası işbirliği sağlanır. İç denetim meslek mensupları, Etik Kurallar ve İç Denetim Mesleki Uygulamalarına Dair Uluslararası Standartlar gibi belirli davranış kurallarına uymakla yükümlüdürler. Bu standartlar, iç denetim mesleğinin etik kurallarına uygun olarak faaliyet göstermesini ve iç denetim süreçlerinin objektif, mesleki özen gösteren ve yüksek kaliteli olmasını sağlamayı amaçlamaktadır.

1999 yılında IIA tarafından Mesleki Uygulama Çerçevesi olarak yayınlanan ve daha sonra geliştirilerek Uluslararası Mesleki Uygulama Çerçevesi (IPPF), 2002 yılında yürürlüğe konulmuştur. 2007 yılında onaylanan ve 01.01.2009 tarihinde uygulamaya

giren bu çerçeve, iç denetçilerin yüksek kaliteli iç denetim hizmetleri sunmalarına yardımcı olmak üzere tasarlanmış olup, mevcut ve gelecekteki iç denetim uygulamalarını kapsamaktadır.

Uluslararası Mesleki Uygulama Çerçevesi, iç denetçilerin faaliyetlerini uygun ve etik kurallara uygun bir şekilde gerçekleştirmelerini sağlayacak standartlar içermektedir. İç Denetimin Tanımı, Etik Kurallar ve Uluslararası İç Denetim Mesleki Uygulama Standartları gibi konular, çerçevenin birinci bölümünde yer almaktadır. İkinci bölümde ise, durum bildirileri, uygulama önerileri ve kılavuzlar gibi materyaller sunulmaktadır. Bu materyaller, iç denetim uygulamalarının geliştirilmesine ve daha da iyileştirilmesine yardımcı olmak için tasarlanmıştır. Uygulama önerileri ve kılavuzlar, iç denetim faaliyetlerinin işin özüne uygun bir şekilde gerçekleştirilmesini kolaylaştırır ve daha etkili hale getirir. Durum bildirileri, iç denetçilerin sorumluluklarını belirleyerek önemli yönetim, risk veya kontrol sorunlarını anlamalarına yardımcı olurken, uygulama önerileri, Standartların yorumlanmasında veya belirli iç denetim ortamlarında uygulanmasında denetçilere yardımcı olan uygulamaları içermektedir. Uygulama kılavuzları ise iç denetim faaliyetlerinin yürütülmesinde ayrıntılı rehberlik sağlayarak, iç denetimde kullanılan araç, teknik, yaklaşım, süreç, prosedürler ve programlara ait uygulama örneklerini sunmaktadır (www.theiia.org:d).

İç denetçiler görevlerini yerine getirirken IIA sertifikalı iç denetçiler ve tüm üyeleri için yayınlamış olduğu yasa ve yönetmeliklerin gerekliliklerinin ötesinde bir iç disiplin sorumluluğunu ortaya koyan uluslararası İç Denetim Mesleki Etik Kurallarına tam uyum göstermelidir. IIA'nın Etik Kuralları, iç denetim mesleğinde etik kültürünü geliştirmeyi amaçlamaktadır. Bu kuralların geliştirilmesi, risk yönetimi, kontrol ve yönetimle ilgili çalışmaların güven temelli olması nedeniyle gereklidir. Kuralların iki ana bölümü vardır:

- 1) İç denetim mesleği ve uygulaması ile ilgili ilkeler (Dürüstlük, Objektiflik, Gizlilik, Yetkinlik)
- 2) İç denetçilerden beklenen davranış ilkeleri (Dürüstlük, Objektiflik, Gizlilik, Yetkinlik ilkelerine yönelik davranış ilkeri)

İyi bir iç denetçi, teknik yetenek ve organizasyondan her seviyede çalışan ile iletişim kurabilmek gibi yüksek standartlara sahip, aynı zamanda iç denetçinin bu

alandaki temel eğitim programlarını tamamlamış olup mesleki gerekli sertifikaları edinmeye özen göstermiş olmalıdır (Eşkazan, 2003: 1-2).

657 sayılı Devlet Memurları Kanunun 48. Maddesine göre iç denetçi olarak atanacakların aşağıdaki şartları barındırması gerekmektedir:

- Başvurulacak kamu idaresinin kendi özellikleri de dikkate alınarak İç Denetim Koordinasyon Kurulu tarafından belirlenen alanlarda en az dört yıllık yüksek öğrenimi tamamlamış olmak.
- En az 5 yıl olacak şekilde kamu idarelerinde denetim elemanı olarak veya en az 8 yıl olacak şekilde İç Denetim Koordinasyon Kurulunca belirtilen alanlarda görev yapmış olmak.
- Ehliyet ve temsil yeteneğine sahip olmak.
- İç Denetim Koordinasyon Kurulunca gerekli görülen diğer şartları barındırmak.

Kamu iç denetçilerin barındırması gereken belli başlı mesleki ahlak kuralları vardır. Bunlar; dürüstlük, gizlilik, nesnellik (objektiflik) ve yetkinliktir (Çevikbaş, 2011: 56-60). İç denetçilerin, yürütmüş olduğu denetim işini yerine getirirken bazı özelliklere sahip olmaları gerekmektedir. Bunlar (İenstitü, 2021):

- Bireysel çalışabilme beceresini barındırmak ve aynı zamanda ekip çalışmalarında başarılı olmak.
- Gerektiğinde inisiyatif kullanabilme becerisini barındırmak.
- Görevli olduğu kurumun süreçlerine hakim olmak.
- Detaycı ve dikkatli, olmak.
- Sözlü, sözsüz ve yazılı iletişim becerisini barındırmak.
- Etkin bir şekilde soru sorup dinleyebilme becerisine sahip olmak.
- Vakti etkin kullanabilmek.
- Analitik düşünebilme becerisini barındırmak.
- Disiplinli olmak.
- Sorumluluklarını yerine getirebilme yeteneğine sahip olmak.
- Denetim yapacağı birimlerin teknik bilgilerine sahip olmak.
- Tespit edici, düzeltici ve önleyici faaliyet konusunda rehberlik edebilme yeteneğine sahip olmak.
- Akıcı ve anlaşılır bir diksiyona sahip olmak.

- Çalışanları Kalite Yönetim Sistemlerine aktif olarak katılmaları için motive edebilme yeteneğine sahip olmak

Türkiye’de “İç Denetçilerin Çalışma Usul Ve Esasları Hakkında Yönetmelik” 28/10/2021 tarihli ve 31642 sayılı Resmî Gazete’de yayımlanan 27/10/2021 tarihli ve 4653 sayılı Cumhurbaşkanı Kararı uyarınca yeni Yönetmelik Cumhurbaşkanlığı Yönetmeliği bölümüne eklenmiştir.

İç denetim birimi başkanı, pozisyonun gereklerine uygun olarak iç denetim birimini yönetmek zorundadır. Baş denetim görevlisi, iç denetim fonksiyonunun amacını, yetkisini ve sorumluluğunu gösteren bir belgeye sahip olmalıdır. İç denetim başkanı, iç denetim fonksiyonunun sorumluluklarını yerine getirmesi için planlar hazırlamalıdır. Denetim fonksiyonunun başkanı aynı zamanda denetim personeline rehberlik sağlamak için yazılı politikalar ve prosedürler sağlamalıdır. Başkan, iç denetim fonksiyonunun performansını değerlendirmek için bir kalite güvence programı geliştirmeli ve sürdürmelidir.

2. BÖLÜM: SİBER GÜVENLİK VE İÇ DENETİM FAALİYETLERİ

İç denetim, organizasyonların siber risklere karşı güvende kalmasında önemli bir rol oynamaktadır. Siber güvenlik açısından denetim süreçleri, organizasyonların bilgi sistemlerinin korunmasına yardımcı olmak için önemli bir araç konumundadır. Bu süreçler, potansiyel güvenlik tehditlerine karşı savunmasızlıkları belirlemek, riskleri tespit etmek ve uygun önlemleri almak için bir çerçeve sağlamaktadır. Denetim süreçleri, organizasyonların siber güvenlik politikalarının etkinliğini değerlendirmeye, siber güvenlik kontrollerinin uygunluğunu test etmeye ve organizasyonun siber güvenlik stratejisinin uygulanmasını takip etmeye yardımcı olur. Bu nedenle, iç denetim, organizasyonların siber güvenliği sağlama konusunda önemli bir rol oynamaktadır. Bu bilgi doğrultusunda çalışmanın ikinci bölümü bu iki konu arasındaki ilişkinin önemi neticesinde yazılmıştır.

2.1. SİBER RİSK KAPSAMI

Son on yılda küresel ekonomi, geleneksel sermaye mallarına (toprak, sermaye, emek) dayalı bir ekonomiden, bilgi ve elektronik veri işlemeye dayalı iş modelinin önemli olduğu dijital bir ekonomiye dönüşmektedir. İleri teknolojilerin geliştirilmesi, bulut çözümleri, 5G iletişimi, Nesnelerin İnterneti ve yapay zekânın yanı sıra otomatik üretim süreçlerinde robot kullanımı, her yerde bulunan İnternet iletişimi ve mobil cihazlar sayesinde büyük miktarda verinin (büyük veri) oluşturulması dijital ekonominin genişlemesine katkıda bulunmaktadır. Ekonominin ve sosyal ilişkilerin dijitalleşmesi, büyük gelişme fırsatlarının ve yeniliklerin tek kaynağı değildir, aynı zamanda ciddi ve tamamen yeni tehditlerin de ortaya çıkmasına neden olmaktadır. Dijital bilgiler, hem kazara hem de kasıtlı olarak gerçekleşen siber tehditlerin bir sonucu olarak kullanılabilirlik, bütünlük ve gizlilik kaybına maruz kalmaktadır. Bilgi teknolojileri (BT) güvenlik harcamalarındaki sürekli artış, siber tehditlerin daha etkili bir şekilde azaltılması anlamına gelmemektedir. Sistemlerde insan hala en zayıf halkadır. Dikkatsizlik, acelecilik, yanlış bilgilendirme, sosyal mühendislik hilelerine yatkınlık, kimlik avı kampanyalarının yüksek oranda yaygınlaşmasını sağlayan insan tutumlarıdır. Yukarıda belirtilen koşullar, siber riskin odak noktasını oluşturmaktadır (Strupcewski, 2021: 1).

2.1.1. Siber Risk Kavramı

Siber risk, bir organizasyonun BT sistemlerine veya dijital varlıklarına yönelik tehditleri ifade etmektedir. Siber saldırılar, kötü amaçlı yazılımlar, kimlik avı (phishing), kötüye kullanım ve hatalar gibi faktörler, organizasyonun siber riskle karşı karşıya kalmasına neden olmaktadır. Siber saldırılar, organizasyonların iş sürekliliğine engel olup finansal kayıplara yol açabilir. Ayrıca, müşteri güvenini zedeleyerek itibar kaybına neden olabilmektedir (Jung vd., 2023: 6-7).

Siber saldırılar, son yıllarda daha karmaşık ve sofistike hale gelmiştir öyle ki saldırganlar, organizasyonların hassas bilgilerine erişmek için daha akıllı taktikler kullanmaktadırlar. Birçok organizasyonun iş sürekliliği, dijital varlıklarının güvenliği ve müşterilerinin güveni siber risk yönetimi stratejilerine bağlı olduğundan siber riskin önemi her geçen gün artmaktadır. Örneğin, bir şirketin veri tabanına yapılan bir saldırı sonucunda, müşteri bilgileri çalınabilir ve bu da şirketin itibarını zedeleyebilir. Ayrıca, çalınan müşteri bilgileri kötüye kullanılabilir ve bu da müşterilerin finansal kayıplar yaşamasına yol açabilir.

Siber risklerin tespiti ve değerlendirilmesi, faaliyet alanı, sektör beklentileri, olgunluk seviyesi ve üst yönetimin sahipliği gibi çeşitli faktörlerden etkilenir. Türkiye'de risk yönetimi, organizasyonlar içinde daha fazla önem kazanırken, siber riskler genellikle ayrı bir kategori olarak ele alınmıştır. Farklı sektörlerin farklı risk algıları ve siber güvenlik olgunluk seviyeleri vardır ve bu da siber risklerin algılanışını ve değerlendirilmesini etkiler. Ayrıca, üst yönetim tarafından siber risklerin yönetilmesine ilişkin sahiplik, bu risklerin organizasyon genelinde ne kadar ciddiye alındığını da etkiler. Bu nedenle, siber risklerin tespiti ve değerlendirilmesi, farklı etmenlerin bir araya gelmesiyle oluşan karmaşık bir süreçtir ve organizasyonların bu sürece öncelik vermesi önemlidir.

Son yıllarda siber risklerin tespiti, yönetimi ve riskin azaltılması konusunda organizasyonlar tarafından pek çok önlem alınmaktadır. Ancak, şirketlerin öncelikli odağı genellikle riskleri azaltıcı faaliyetler olmuştur. Özellikle, sistemlere erişim, cihaz ve bağlantı güvenliğinin sağlanması, şirketlerin öncelikli risk azaltma önlemleri arasındadır. Bu amaçla, şirketler siber güvenlik ürünlerine daha fazla yatırım yapmakta ve danışmanlık hizmetleri almaktadır. Bu önlemler, şirketlerin siber güvenlik açıklarını kapatmalarına ve siber saldırılara karşı daha dirençli hale gelmelerine yardımcı olur.

Ancak, siber güvenlikte sadece önleyici tedbirler yeterli değildir. Organizasyonların siber saldırıların gerçekleşmesi durumunda hazırlıklı olmaları ve saldırıların etkilerini minimize etmek için acil durum planlarına sahip olmaları da önemlidir. Dolayısıyla, şirketlerin siber güvenlik konusunda hem önleyici hem de müdahale edici stratejilere yatırım yapmaları gerekmektedir. Siber risk yönetiminin iyileşebilmesi adına yapılabilecek işlemler aşağıda sıralanmaktadır:

- Kamunun süreçleri sektörel farklılıkları göz önünde bulundurarak daha belli bir biçimde tarif etmesi ve şekillendirmesi önemlidir.
- Siber risk yönetimine bakış açısında bütüncül bir değişiklik gerekmektedir. Bu değişikliğin gerçekleşebilmesi için eğitim ve bilgi gereklidir. Siber risk eğitimlerinin şirket oryantasyonunun bir parçası olduğu ve bilinçlendirme yöntemlerinin şirketlerin tüm iş birimlerine bağlantılı yapılar oluşturulmalıdır.
- Siber riskin organizasyonların sahip olduğu diğer tüm riskler gibi vizyon ve misyonlarında yer almaları ve konumlandırılması önem arz etmektedir.
- Siber risk yönetiminin etkinliği için organizasyonel değişim ve insan kaynakları yönetimi önemlidir.
- İnsan Kaynakları (İK), operasyonlar, hukuk ve diğer iş birimlerinden yetkililer dahil olmak üzere her şirkette siber risk geliştirmek ve strateji belirlemek için özel bir siber güvenlik komitesi oluşturmak ve düzenli bir toplantı takvimi ile irtibat kurmak etkili olabilir (www.tusiad.org).

2.1.2. Kullanılan Analiz Yöntemleri

Organizasyonlar, siber risklerin tespit ve analiz edilmesinde tercihlerini, seri ve yapısal yaklaşımlardan yana kullanmaktadırlar. Organizasyonların siber risklere karşı önleyici tedbir almaları ve bu riskleri ortadan kaldırmak için ilk olarak kendi kurum kültürlerine ve varlıklarına elverişli risk profilleri oluşturmaları daha etkin ve uygulanabilir tekniklerin iyileştirilmesine imkan sağlamaktadır. Bu sebeple, organizasyonların iç ve dış çevresi, faal olduğu alanlar, dijital ağlara olan sadakati, değer zinciri dahilindeki amaçları, teknik ve insan kaynaklı emniyet fireleri, siber riskler devamındaki toparlanma evresinin durumu, herhangi bir siber saldırı neticesinde işlerin rutin düzeyine gelme periyodu ve siber güvenlik çatısı altındaki yasal gereksinimleri giderme yeteneği risk profilinin ortaya konulmasında önemsenmesi gereken konulardır.

Ortaya koyulan bu risk profili doğrultusunda organizasyonun kabul edebileceği risk düzeyi de belirlenerek siber güvenlik ölçümleri yapılır. Fakat hiçbir şartta ve süreçte %100 güvenlik sağlanamayacaktır ve hep makul seviyede bir risk altında olacaktır (Selimoğlu ve Saldi, 2019: 7-8). Siber tehditlere karşı önleyici tedbir almak amacıyla riskler analiz edilmeye çalışılmaktadır. Risk değerini tahmin etmek için temel olarak kantitatif (nicel) ve kalitatif (nitel) yöntemler uygulanmaktadır.

Nicel risk analizi yönteminde riski ifade etmek için istatistiksel ve matematiksel yöntemler kullanılır. Nitel risk analizi yönteminde ise riski ifade etmek için matematiksel ifadeler yerine az-çok, büyük-küçük, yüksek-düşük gibi ifadeler kullanılmaktadır (Rot, 2008: 2-3; Kıran ve Soğukpınar, 2021: 17).

Yoğun nicel ölçümler kullanılan bu nicel risk analizi yöntemi, modern bilgi güvenliği risk analizi için uygun değildir. Geçmiş yıllardan farklı olarak, modern bilgi sistemleri karmaşık bir yapıya ve geniş bir uygulamaya sahiptir. Bu yüzden, karmaşık ortamlar için riski modellemek adına kullanılan yoğun istatistiksel ölçümler bu süreci daha da karmaşık hale getirmektedir.

Nitel ölçümler için kullanılan nicel risk analizi yöntemi, modern bilgi güvenliği risk analizi için daha uygundur. Bununla beraber, bu yöntemin göz ardı edilemeyecek bir dezavantajı; çelişkili sonuçlar veren doğasıdır. Nitel yöntemler riski modellemek adına matematik ve istatistik gibi araçlara başvurmduğundan, yöntemin sonucu büyük ölçüde risk analistlerinin görüşlerine bağlıdır. Niteliksel risk analizi yöntemleri kullanılırken subjektif sonuç alma riski vardır.

Nicel ve nitel risk analizi yöntemlerinin bahsedilen bu eksik ve açıklarına istinaden bilgi güvenliği risk analizi metodu (Information Security Risk Analysis Method - ISRAM) yöntemi geliştirilmiştir. ISRAM, niceliksel, anket tabanlı bir risk analizi yöntemidir.

ISRAM'ın risk modeli, temel risk formülü olan aşağıdaki formüle dayanmaktadır:

$$\text{Risk} = \text{Güvenlik ihlali meydana gelme olasılığı} * \text{Güvenlik ihlali meydana gelmenin sonucu}^1 \quad (1)$$

¹ Risk= Probability of occurrence of security breach * Consequence of occurrence of security breach

Formül (1)'den çıkarılan ISRAM'ın risk modeli formül (2)'de verilmektedir. Formül (2), formül (1)'deki iki temel parametrenin izdüşümleri olan iki ana bölümden oluşur.

$$Risk = \left(\frac{\sum_m [T_1 (\sum_i w_i p_i)]}{m} \right) \left(\frac{\sum_n [T_2 (\sum_j w_j p_j)]}{n} \right) \quad (2)$$

i : Oluşma olasılığı araştırması için soru sayısı;

j : Olayın sonuçlarının araştırılması için soru sayısı;

m : Gerçekleşme olasılığı anketine katılan katılımcı sayısı;

n : Olayın sonuçları anketine katılan katılımcı sayısı;

w_i, w_j : “ i ” (“ j ”) sorusunun ağırlığı ;

p_i, p_j : “ i ” sorusu (“ j ”) için seçilen cevap seçeneğinin sayısal değeri;

T_1 : Oluşma olasılığı anketi için risk tablosu;

T_2 : Olayın sonuçlarının araştırılması için risk tablosu;

ISRAM, temel olarak organizasyondaki güvenlik risklerini analiz etmek için bir anket hazırlama ve yürütme sürecidir. Formül 2'deki iki risk parametresi için ayrı ve bağımsız iki araştırma süreci yürütülür. Anketin hazırlanması ve yürütülmesi ve dolayısıyla sonuçlarının analizi, iyi tanımlanmış risk tanımlama aşamalarına göre belirlenir. Formül 2 bu adımları matematiksel olarak temsil eder (Soğukpınar ve Karabacak, 2005: 147-159).

2.1.3. Siber Risklerin Haritalandırılması

Bir bilgi teknolojisi sisteminin herhangi bir siber riske maruz kalması ve bu riskten kurtarma yeteneğinin var olması, sisteminin tehditlere karşı dayanıklılığını veya bağışıklığını göstermektedir. Siber dayanıklılık veya bağışıklık kavramı İngilizce’de ‘cyber resilience’ olarak adlandırılmaktadır. Bu kavram, sistemlerin siber riskler karşısında iyileşme sürecini metrik değişkenler bazında analiz yapmayı sağlamaktadır. Örneğin, aynı özelliklere sahip A ve B olmak üzere iki eşit sistem olduğunun varsayımı yapılsın. Aynı siber saldırıya maruz kalan bu iki sistemin hedef performans düzeyine A sistemi t_1 , B sistemi ise t_2 süresi sonunda ulaşsın. $t_1 < t_2$ ise, sistem A'nın “siber dayanıklılık” düzeyi sistem B'den daha iyi olduğu algılanmaktadır.

Genel olarak risk değerlendirilirken kullanılan formül “risk=tehdit*güvenlik açığı*sonuç” şeklinde belirlenmiştir. Risk analiz edilebilir ve uygun yöntemlerle

yönetilebilirse, sistem güvenli bir duruma gelebilmektedir. Ayrıca sistemlerin karşılaştığı öngörülemeyen olaylar sonucunda tekrar optimum performansa ulaşmak için gereken yetkinlik, riskleri yönetme becerisini de göstermektedir. Sonrasında sistem performansı ile sistem esnekliği arasındaki ilişki siber riskin nasıl kontrol edilebileceğini göstermektedir (Selimoğlu ve Saldı, 2019: 12).

Siber risklerin haritalandırılmasında riski değerlendirmek için bir organizasyonun kültürüne özgü risk ve dayanıklılık modeli geliştirilmek adına gerekli faaliyetleri tanımlayan bir siber risk yol haritası geliştirmek amaçlanmaktadır. Siber risk yol haritasının amacı, organizasyondaki merkezi risk komitesine siber riske maruz kalma durumunu yorumlamak ve dayanıklılık faaliyetlerinin etkinliğini ölçmek için bir model sunmaktadır. Siber risk yol haritasında üç aşama mevcuttur (Amin, 2019: 32-43):

1. Aşama: Organizasyonun bugün nerede olduğunun tespit edilmesiyle başlamaktadır. Siber risk çoğunlukla organizasyonun kendine özgü doğasına ve siber dayanıklılığına bağlıdır. Bu nedenle ilk aşamada organizasyonun siber güvenlik ortamının, siber vakaları önleme, saldırıları tespit etme, tespit edilen saldırılara müdahale etme, kopuklukları en aza indirme ve bunları bertaraf etme yeteneğinin ortaya konulması gerekmektedir.

2. Aşama: Organizasyonun siber güvenlik açısından gelecekte nerede olması gerektiği saptanmalıdır. Bu saptanışa göre ne tür bir siber yönetim kültürü oluşturulmak isteniyor ve ne düzeyde bir siber dayanıklılık geliştirilmesi gerekmektedir? sorularının yanıtları aranmaktadır.

3. Aşama: Bu adımda organizasyonun şu an bulunduğu yerden gelecekte olması gereken yere giden rota çizilmelidir. Siber risklerin tam potansiyel büyüklüğünün ve organizasyon üzerindeki finansal etkilerinin değerlendirilmesinde ve alternatif risk azaltma stratejilerinin karşılaştırılmasında ve değerlendirilmesinde kullanılacak modeller sağlanmaktadır.

2.1.4. Siber Risk Sigortası

Siber saldırılardan kaynaklanabilecek en kötü senaryolar arasında veri kaybı, işin durdurulması, üretimin durdurulması, şantaj, çalınan bilgilerin ifşa edilmesiyle ilgili tehditler ve itibar kaybına sebep olabilir. İtibar kaybı burada en büyük risk olarak kabul edilir. Organizasyonların ve şahısların siber saldırı neticesinde doğabilecek kötü sonuçlardan korunma yöntemlerinden birisi siber risk sigortasıdır. Yukarıda bahsedildiği

gibi pek çok kurum günümüzde siber saldırıya uğrayabilmekte veya hali hazırda siber saldırıya uğramış bulunmaktadır. Bu kapsamda siber risk sigortası, diğer bir adı ile veri güvenliği sigortasının önemi ön plana çıkmaktadır (Altuntaş vd., 2018: 11).

Siber sigortalar, bilgi ihlalleri sonucunda oluşabilecek zararlar ve savunma masraflarını kapsayan bir sigorta türüdür. Bu zararlar arasında, üçüncü taraf verilerine bulaşan virüsler, sigortalayanın yetkisi dışında üçüncü taraf verilerine erişilmesi, sistem kodlarının çalınması, donanımların çalınması ve çalışanların bilgilerinin ifşa edilmesi gibi riskler yer almaktadır. Ayrıca, siber sigortalar ile ağ kesintilerinden kaynaklanan gelir kayıpları, güvenlik tehditlerinin ortadan kaldırılması için üçüncü taraflara yapılan tehdit ödemeleri ve elektronik bilgilerin ihmali sonucu oluşan zararlar da kapsama alınabilir. Bu sigortalar, organizasyonların siber riskler karşısında finansal olarak korunmasına yardımcı olur ve siber güvenlik önlemlerinin maliyetlerini azaltır. Ancak, siber sigortaların teminat kapsamı ve fiyatlandırması şirketten şirkete değişebilir ve her zaman her tür siber saldırıyı kapsamayabilir, bu nedenle sigorta şirketi ile ayrıntılı bir görüşme yapmak önemlidir (www.broadcom.com). Siber sigortalar riski azaltmakta ve saldırılara karşı koruma sağlamaktadır. Ancak siber saldırıların gerçekleşmeyeceğine dair bir güvence verilmemektedir. Siber sigorta, gizliliği haiz ve korunma ihtiyacı duyulan verilerin hukuka aykırı yollarla ortaya çıkması ile oluşacak hasara karşı yapılan sigorta poliçesi olarak ifade edilmektedir (Çotak, 2019: 16).

Bir başka tanımda siber risk sigortası, belirli bir gizlilik düzeyine sahip ve korunması gereken verilerin ortaya çıkması, çalınması veya kullanılması sonucu yaşanabilecek zararlara karşı işletme, kurum veya kuruluşları koruyan sigorta poliçesidir şeklinde ifade edilmektedir (www.sigortamedya.com.tr).

Siber risk sigortasının gelişim sıralamasına bakıldığında, siber risk sigortası ürünleri ilk olarak 1990'ların sonlarında ABD'de ortaya çıkmış ve 2000'li yılların başında Avrupa'da siber risk sigortası kapsamı sunulmaya başlanmıştır. Türkiye'de ise ilk kez 2010 yılında siber risk sigortasına ihtiyaç olduğu görüşü hakim olmaktadır.

Başlangıçta, siber riskler yabancı sigorta şirketleri tarafından teminat altına alınırken, daha sonra Türkiye'deki sigorta şirketleri de bu alanda hizmet vermeye başlamıştır. Ancak, ilk başlarda siber risklerin önemi yeterince anlaşılamamıştır ve sadece veri kayıpları siber riskler olarak kabul edilmiştir. Fakat zamanla, ortaya çıkan siber zararlar, veri kayıplarından daha kapsamlı ve ciddi olduğunu göstermiş ve sigorta

şirketlerinin verilen teminatları da buna paralel olarak genişletmesi gerektiğini ortaya çıkarmıştır. Gelecekte, siber risk sigortalarına olan ihtiyacın artması beklenmektedir.

Siber risk sigortası, diğer sigorta türlerinden farklıdır çünkü sigorta kapsamında yer alan değerlerin maddi bir değeri yoktur. Sigortalanan şey, verinin kaybolması, silinmesi ya da çalınması değil, bu olayların 3. şahısların talebi sonucunda ortaya çıkabilecek zararlarıdır. Siber risk sigortasının diğer bir farklı özelliği de, gerçekleşen riskin etkisinin önceden tahmin edilmesinin zor olmasıdır. Bu sebeple, sigorta şirketleri bu alanda ürünlerini yaygınlaştırmak ve uygun fiyatlı poliçeler sunmakta zorlanabilirler. Siber risk sigortası poliçeleri, sigortalının ihtiyaçlarına göre özelleştirilebilen ek teminatlar içerebilir ve internet kullanımı veya elektronik veri gibi birçok riski kapsar (Altuntaş vd., 2018: 8-22).

2.2. SİBER SUÇLAR, SİBER TEHDİTLER VE SİBER SALDIRILAR

Teknolojinin yaygınlaşması ve internet kullanımının artması, beraberinde çeşitli siber riskler de getirmektedir. Bu riskler, insanların kişisel bilgilerinin çalınması, veri kaybı, siber saldırılar ve ağ kesintileri gibi problemlere neden olabilmektedir. Siber risk terimi, bilgisayar sistemleri, ağlar ve diğer teknolojik varlıkların güvenliğini tehdit eden riskleri tanımlamakta, siber alan ise, bu sistemlerin birbiriyle iletişim halinde olduğu soyut veya somut alanı ifade etmektedir. Siber alanlarda ortaya çıkan siber suç, siber tehdit ve siber saldırı kavramları bu bölümde açıklanmaktadır.

2.2.1. Siber Suçların Kapsamı

Günümüzde teknolojinin hızla ilerlemesi, bilgi ve iletişim teknolojilerindeki gelişmeler, siber suçlar ve siber saldırılar gibi dijital suçların artmasına neden olmuştur. Siber suçlar, internet ortamında bilgisayar, cep telefonu gibi elektronik cihazlarla gerçekleştirilen her türlü yasadışı faaliyeti kapsamaktadır (Ocak, 2021: 6).

Genellikle bilgisayar suçu olarak bilinen siber suç, bir bilgisayarın dolandırıcılık, çocuk pornografisi, fikri mülkiyet hakları, kimlik hırsızlığı ve mahremiyet ihlali gibi cezai suç teşkil eden amaçlarla işlenmektedir. Bilgisayarlar, ticaret, eğlence ve resmi kamusal işler için temel hale geldikçe ve özellikle internetin yaygınlaşmasıyla siber suçların tespitinin önemi daha çok artmıştır (Türk ve Şenyuva, 2021).

Siber suçlar Türkiye iç mevzuatında ilk kez, 1991 yılında 765 sayılı Türk Ceza Kanununda, (TCK) 3756 sayılı kanunla Md. 525/a, b, c ve d maddeleriyle eklenen Bilişim

Alanında Suçlar bölümüyle konu olmuştur. 2004 yılında çıkarılan 52373 sayılı yeni TCK'da siber suçlar, siber suçların güncel gelişimi göz önüne alınarak oldukça ayrıntılı şekilde tanımlanmıştır. 5237 sayılı yeni TCK'da bilişim alanında suçlar hali hazırda;

- Hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu (m.243),
- Bilişim sisteminin isleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu (m.244/1-2),
- Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m.244/4),
- Banka veya kredi kartlarının kötüye kullanılması suçu (m.138) olarak belirlenmiştir.

Ayrıca özel hayata ve hayatın gizli alanına karşı suçlar bölümündeki siber suçları;

- Kişisel verilerin kaydedilmesi (m.135),
- Kişisel verileri hukuka aykırı olarak verme veya ele geçirme (m.136),
- Verilerin yok edilmemesi suçları (m.138) olarak belirlenmiştir (Taşçı ve Ali, 2015: 232-233).

Siber suçlar, ulusal sınırları aşır uluslararası sınırlara ulaşmıştır. Bu suçlarla mücadelede çok büyük zorluklar yaşanmaması için dünya çapında elbirliğiyle etkin bir mücadele yürütülmesi gerekmektedir. Bu zorlukları bertaraf edebilmek adına devletlerin aynı farkındalıkta ve hassasiyette olması, hukuki mevzuatlar arasında uyumluluk sağlanması gerekmektedir. Siber suçlarla mücadele edilebilmesi, dünya çapında elbirliğiyle etkin bir mücadele yürütülmesi halinde anlam kazanabilecektir. Aksi halde içinden çıkılmaz bir siber suç örneği ile karşı karşıya kalınmaktadır. Örneğin Norveç'de suç kabul edilmeyen bir eylem Türkiye'de suç kabul etmekteyse, fail saldırıyı Norveç'den gerçekleştirdiği takdirde Türk yetkililerin Oslo devletinin rızası olmadıkça soruşturma yürütememektedir.

Siber suçlarla ilgili sınırlar ötesinde ortaya çıkan bu durumların çözümüne uluslararası adımların atılması zorunluluk haline gelmiştir. Bu adımların en önemlisi Türkiye'nin de taraf olduğu "Avrupa Konseyi Siber Suç Sözleşmesi(ASSSS)"dir (Aliusta ve Benzer, 2018: 37). Avrupa Konseyi'nin 1996 yılında Suç Sorunlarına dair Avrupa Komitesi'ne (SSAK European Committee on Crime Problems) siber suçlarla ilgili bir uzman komitesi kurma tavsiyesiyle başlayan süreç, Şubat 1997'de Avrupa Konseyi Bakanlar Komitesi tarafından "Siber-Uzay Suçları Uzman Komitesi"nin kurulmasıyla

devam etti. Bu komite, sözleşme taslağını hazırladı ve SSAK tarafından Haziran 2001'de onaylandı. Daha sonra Avrupa Konseyi Bakanlar Komitesi tarafından 8 Kasım 2001 tarihinde kabul edildi. 23 Kasım 2001'de Budapeşte'de imzaya açılan Siber Suç Sözleşmesi, 1 Temmuz 2004'te yürürlüğe girdi ve uluslararası arenadaki ilk antlaşma oldu. Türkiye'de, sözleşmeyi 2010 yılında imzaladı ve 2 Mayıs 2014'te 6533 sayılı Kanunla kabul ederek yürürlüğe koydu. Sözleşme, 48 maddeden oluşmakta ve dört ana başlık altında düzenlenmektedir. İmza yerine atfen Budapeşte Sözleşmesi olarak da bilinir ve Türkiye'nin iç hukukunun bir parçasıdır, dolayısıyla uygulanması zorunludur (Aköz, 2018: 2, 44-45, 48-49).

2.2.2. Siber Tehditlerin Kapsamı ve Siber Silahlar

Siber tehditler artık sadece bilgisayar sistemlerine zarar vermekle sınırlı değildir. Bunun yanı sıra, bir ülkenin kritik olarak kabul edilen haberleşme, enerji, ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verme potansiyeline sahiptir. Bu tür saldırılar, asimetrik bir harp türü olarak da kabul edilmektedir. Bu nedenle, siber tehditlerin gelecekte de önemli bir tehdit olarak varlığını sürdüreceği ve tüm dünya tarafından bu gerçeğin kabul edildiği bir gerçektir (Aslay, 2017: 25).

Geleneksel tehdit kavramı, askeri nitelikli tehditler ve sınırlar arası tehditler gibi belirli özelliklere sahip olan tehditleri kapsarken, günümüzde uluslararası terörizm, organize suç örgütleri, siber terör, devletler arası saldırılar, konvansiyonel ve kitle imha silahlarının yaygınlaşması gibi çok boyutlu, kaynağı ve şekli önceden tahmin edilmesi zor tehditler ortaya çıkmıştır. Bu tehditler, fiziksel varlığa doğrudan etki edebilen tehditler grubuna girmektedir (Erdoğan, 2013: 265).

Siber suçların artmasıyla birlikte, siber silahlar da ortaya çıkmıştır. Siber silahlar, bir ülkenin veya organizasyonun diğer bir ülke veya organizasyona karşı siber saldırı gerçekleştirmek için kullandığı bir tür teknolojik silahtır. Siber silahlar, bilgisayar sistemlerini bozmak, ağları felç etmek, gizli bilgileri çalmak veya diğer zararlı faaliyetlerde bulunmak için kullanılabilir.

Siber silahlar, uluslararası ilişkilerde önemli bir rol oynamaktadır. Birçok ülke, siber silahlarla ilgili araştırma ve geliştirme (Ar-Ge) faaliyetleri yürütmekte ve siber silahların kullanımını denetlemek için yasal düzenlemeler getirmektedir.

Elektronik ortamda savunma ve saldırı amaçlı kullanılan her türlü araç siber silah olarak tanımlanmaktadır. NATO, kötü amaçlı kod veya yazılım olarak da ifade edilen

siber silahları, “saldırı yeteneğine sahip olan ve karşıya zarar veren yazılım veya kod parçasıdır” şeklinde tanımlamıştır (Sağıroğlu, 2018: 25).

Rid (2013:36) siber silahları iki kategoriye ayırmaktadır. İlk kategoride, "Genel Ama Düşük Potansiyelli Araçlar" adını verdiği siber araçlar bulunmaktadır. Bu araçlar gerçek silahlara benzer, hedef belirleme gerektirmeden kullanılabilir ve kolayca elde edilebilirler. Ancak, bu araçlarla yapılan saldırılar sonucunda hedefin vurulduğu ve saldırının izlerinin görülebildiği bir şekilde gerçekleşir. Bankaların web sitelerine yönelik DDoS saldırıları bu kategoriye örnek olarak verilebilir.

İkinci kategori ise "Spesifik ve Yüksek Potansiyelli Silahlar" adı verilen silahlardan oluşmaktadır. Bu silahlar, adından da anlaşılacağı gibi, gerçek silahlara daha yakındır. Ancak, tek kullanımlık ve sadece belirli hedeflere yönelik olarak tasarlanmışlardır. Bu nedenle, uzun istihbarat çalışmaları sonucunda geliştirilirler. Stuxnet örneği de bu tür silahlara bir örnektir (Rid, 2013:36; Varlık, 2016a).

Bazı akademisyenler "siber silahların" iki ana kategorisi olduğuna inanmaktadır: hedef bilgisayar sistemlerine doğrudan erişim gerektirmeyenler (örneğin, İnternet üzerinden yayılan virüsler) ve hedef bilgisayar sistemlerine doğrudan erişimi olanlar ise (örneğin, SCADA sistemlerine sızabilen ve dolaylı kinetik etkiler oluşturabilen siber ajanlar) kategorisinde yer almaktadır. Bu yaklaşıma göre, olası bir silahsızlanma veya silah kontrolü rejimine tabi olacak unsurlar belirlenecektir.

Siber silahların herhangi bir uluslararası denetim rejimine tabi olabilmesi için askeri ve siyasi çevrelerin kitle imha silahları veya balistik füzeler gibi 'stratejik silahlar' bağlamında ele alması önemlidir. Konuyla ilgili yapılan araştırmalar, 'stratejik silahlar' segmentinde askeri amaçlarla kullanılan siber becerilerin değerlendirilmesinin ilk ve en önemli koşulunun, bir ülkenin kritik ulusal altyapısına yıkıcı zararlar vermesi olduğunu belirtiyor. Şimdiye kadar, siber silahların nükleer silahlara eşdeğer bir yıkıcı geliştirdiğine dair somut bir kanıt bulunamamıştır. Öte yandan, özellikle kritik ulusal altyapılarını ve ekonomilerini bilgisayar ağlarına taşıyan ülkeler için böyle bir tehdit göz ardı edilmemiştir. Nükleer silah rejimi bu silahların kullanılmaması üzerine kuruluyken, siber silahlar barışçıl durumlarda bile kullanılabilir. Ayrıca saldırıya uğrayan bir devlet, kendi egemenliğine saldıran bir aktörü tespit edemez. Bu nedenle, uluslararası topluluklarda genellikle siber silahlar kullanılmaktadır (Erendor ve Tamer, 2018: 61).

2.2.3. Siber Saldırıların Kapsamı

Son yıllarda, siber saldırı vakalarındaki endişe verici bir artış, siber güvenliği dünya genelindeki ülkeler için önemli bir endişe haline getirmiştir. Mevcut değişken sosyo-politik ortam ve terör vakalarındaki büyük artış göz önüne alındığında, devlet kurumlarının terör örgütleri ve devlet aktörleri tarafından normal yaşam biçimini bozmak için siber alan istismarı olasılığını hızla fark etmesi gerekmektedir. Siber terörizmin tehdit düzeyi hiçbir zaman bugünkü kadar yüksek olmamıştır ve bu durum çok fazla güvensizlik ve korku yaratmıştır (Albahar, 2019: 993).

Günümüz siber saldırılarının dinamiklerini tam olarak kavrayabilmek için siber uzayın kendine özgü boyutlarını anlamak önemlidir. Siber uzay ortamı herhangi bir geleneksel sınır veya hudutla sınırlı olmadığından, gizli siber saldırılar inanılmaz hızlarda binlerce mil öteden taşınabilir. Bu tür saldırılar, yerde büyük bir fiziksel orduya ihtiyaç duymadan, bilgisayarları olan bir kişi veya bir grup tarafından, oturma odalarında güvenle oturarak kolayca gerçekleştirilebilir. Bu tür siber saldırıların verdiği hasar, herhangi bir konvansiyonel savaş kadar ölümcül olabilir. Dünya çapında siber saldırı tehditlerindeki büyük artışa katkıda bulunan çeşitli yönler veya faktörler vardır ve en belirgin olanı İnternet'in her yerde bulunabilmesidir (Albahar, 2019: 993).

Siber alanda, çeşitli kaynaklar tarafından, bireysel kullanıcılardan büyük organizasyonlara, terör örgütlerinden devletlere kadar hedef sistemlerin bozulması ve işlevsiz hale getirilmesi için birçok saldırı gerçekleştirilmektedir. Bu saldırılar genellikle "siber saldırı" olarak adlandırılır ve "Siber alan içindeki bilgileri istismar etmek, bozmak, değiştirmek, sistemlere erişimi engellemek veya zarar vermek amacıyla gerçekleştirilen faaliyetlerdir" şeklinde tanımlanabilir. Başka bir tanımda ise siber saldırı, "Saldırganlar tarafından bilgi sistemlerinin çalışmaz hale getirilmesi, bilgi sistemlerinin güvenliğinin veya güvenilirliğinin riske atılması, bozulması veya çalınması" olarak tanımlanabilir (Şafak, 2020:133-134).

Siber saldırı, bir bilgisayar sistemi, ağ veya diğer dijital cihazlara yönelik kötü niyetli girişimlerdir. Siber suçlular, bilgi çalmak, hasar vermek, itibarlarını zedelemek, para kazanmak veya diğer hedeflere ulaşmak için siber saldırılara başvurabilirler. Saldırıları, farklı amaçlar doğrultusunda çeşitli teknik ve yöntemler kullanılarak gerçekleştirilir.

Siber saldırılar, hedeflerine ve kullanılan tekniklere bağılı olarak farklı şekillerde gerçekleştirilebilir.

Saldırganlar siber saldırılarla, siber ortamdaki fiziksel veya sanal yapıyı, yazılım, donanım ve alt yapı sistemlerini, genellikle de bu sistemler üzerindeki bilgiyi ve kullanıcıları hedef alarak eylemlerini gerçekleştirirken, temel olarak üç prensibe göre hareket etmektedirler.

- Birinci Prensip: Gizli bilgilerin elde edilmesi veya bilginin gizliliğinin açık edilmesi,
- İkinci Prensip: Bilgiye zarar verilerek değiştirilmesi yani bütünlüğünün bozulması,
- Üçüncü Prensip: Bilgiye kullanıcıların erişiminin engellenmesi yani kullanılabilirliğinin önlenmesidir (Şenol, 2017: 2-3).

2.2.3.1. Siber Saldırı Çeşitleri

Siber saldırı terimi, modern çağın gelişmiş bilgi ve iletişim teknolojilerinin yeteneklerinden yararlanarak gerçekleştirilebilecek çeşitli kötü niyetli faaliyetleri kapsamaktadır. Siber alanda gerçekleştirilen ve gün geçtikçe artan popülerliğe sahip olan siber saldırı türleri arasında şunlar yer almaktadır (Öztürk, 2018: 211-214; Çakır ve Uzun, 2021: 360-361; Hekim ve Başbüyük, 2013: 137-140; Avcı vd., 2021: 6-7; Gökçe vd., 2014: 216-217; Demircan, 2021: 32-35; Şafak, 2020: 138-139; Ahmetoğlu ve Daş, 2019; Acar ve Zoray, 2021)

- I. **Kötücül Yazılım (Malware):** Siber dünyanın en yaygın tehditlerinden biridir. Bu tür yazılımlar, bilgisayarlara veya diğer cihazlara bulaşarak kişisel bilgileri çalmak, sistemleri kilitlemek veya bozmak gibi çeşitli zararlı faaliyetler gerçekleştirir. Malware, virüsler, solucanlar, trojanlar, fidye yazılımları ve casus yazılımlar gibi farklı türlerde olabilmektedirler.
- II. **Oltaama Saldırıları (Phishing):** Kişisel veya finansal bilgileri ele geçirmek amacıyla sahte web siteleri veya e-postalar kullanarak kullanıcıları kandırma yöntemidir. Phishing, siber suçluların en sık kullandığı yöntemlerden biridir ve dolandırıcılık amaçlı kullanılmaktadır.
- III. **Hizmeti Engelleme (DoS/DDoS) Saldırıları:** İnternet servislerini hedefleyen bir tür siber saldırıdır. Bu tür saldırılar, birçok cihazın aynı anda hedefi yüklemesiyle gerçekleştirilir ve hizmetlerin çökmesine neden olabilmektedir.

- IV. **Kimlik Avı (Identity Theft):** Kişisel bilgilerin ele geçirilerek kötüye kullanılmasıdır. Bu tür saldırılar genellikle sahte web siteleri veya sahte e-postalar yoluyla gerçekleştirilmektedir.
- V. **Güvenlik Açıkları:** Bir cihazın veya yazılımın güvenlik duvarını aşarak saldırganların cihaza veya yazılıma erişim sağlamasına izin veren açıklar olarak tanımlanabilir. Bu tür açıklar, siber suçluların hassas bilgilere erişim sağlamasına neden olabilmektedir.
- VI. **İçerik Filtreleme:** Siber suçluların, internet trafiğini izleyerek bilgiye erişim sağlama yöntemidir. Bu tür saldırılar, şifreleme veya diğer güvenlik önlemlerinin kullanılmaması durumunda gerçekleştirilmektedir.
- VII. **Sosyal Mühendislik:** Kişilerin psikolojik zayıflıklarını veya güvenlik korkularını aşmak için kullanılan bir taktiktir. Bu tür saldırılar, kişilerin güvenliğini kazanmak için sosyal medya veya diğer iletişim platformlarını kullanabilmektedir. Örneğin, bir saldırgan, bir kişinin şifresini veya diğer hassas bilgileri elde etmek için onunla güven kurarak sahte bir hesap kullanabilmektedir.
- VIII. **Zombi Ağı (Botnetler):** Birçok cihazı kontrol etmek için kullanılan bir ağıdır. Botnetler, bilgisayarları veya diğer cihazları ele geçirerek bir saldırganın kontrolü altına alınabilir ve saldırganlar tarafından yasa dışı faaliyetler için kullanılabilir.
- IX. **Siber Zorbalık (Cyberbullying):** Kişilerin internet veya diğer dijital ortamlarda saldırgan veya rahatsız edici davranışlar sergilemesidir. Bu tür saldırılar, özellikle sosyal medya kullanımının yaygınlaşmasıyla birlikte artmıştır.
- X. **Endüstriyel Siber Casusluk:** Bir ülkenin veya şirketin diğer ülkelerin veya rakiplerinin siber faaliyetlerini izlemek veya çalmak için kullanılan bir taktiktir. Bu tür saldırılar, ekonomik casusluk veya diğer ulusal güvenlik tehditleri için kullanılabilir.
- XI. **Truva Atı (Trojan):** Bilgisayar sistemlerine zarar vermek için kullanılan bir siber saldırı türüdür. Bu saldırı türü, kötü niyetli bir kişi veya grup tarafından, normal bir dosya veya program gibi görünen bir kötü amaçlı yazılım hedef bilgisayar sistemini ağırlıyor. Bu saldırı çeşidi, birçok farklı amaç için kullanılabilir. Örneğin, bilgisayarınızı uzaktan kontrol etmek, kişisel bilgileri çalmak, spam e-postaları kaldırmak veya diğer kötü amaçlı yazılımları yüklemek için kullanılabilir.

Bu nedenle, şifreleme antivirüs yazılımı kullanımı ve internet güvenliği önlemlerine dikkat etmek önemlidir.

- XII. **Fidyeleme (Ransomware):** Truva atları ve solucanlar sayesinde kişilerden veya organizasyonlardan para sızdırmak amacıyla tasarlanmış siber saldırı yazılım türleridir. Fidyeleme saldırı uygulanan sistem üzerinde gerçekleştirmiş olduğu değişiklikler ile kişinin verilerini şifrelemekte veya kullanıcının sisteme erişimini kısıtlayarak bir ödeme talebinde bulunmaktadır. Kişi veya organizasyon ödemeyi yaptığında sisteme veya verilere erişim sağlanacağı düşünülse de bunun oranı %30 civarındadır.
- XIII. **Kırma (Cracking):** Genel olarak kişilerin finansal bilgilerini çalmak için kullanılmaktadır. Bu yöntem bir program içerisine yerleştirilmiş ek programlar sayesinde kişisel bilgisayarların güvenlik sistemini aşarak bir arka kapı oluşturmaktadır. Kırma işleminin yayıldığı bir diğer durum halka açık alanlarda kullanılan kablosuz ağlardır. Koruması düşük olan ağlara bağlanmak hackerlar için kolay hedef durumuna düşmek anlamına gelmektedir.
- XIV. **Ortakdaki Adam (Man In The Middle):** Burada kurban ve kurbanın bağlanmak istediği sunucu arasında çeşitli dinleme işlemleri yapılmaktadır. Saldırganın kurbandan çalmak istediği verilerin ele geçirilmesi bu yolla sağlanmaktadır. Bu gibi şifrelenmemiş ağlara bağlanmak ve dinleme işlemini gerçekleştirmenin birden fazla yolu bulunmaktadır. Ortadaki adam saldırısı modeli Bazı saldırı çeşitlerinde kurban yani istemci gerçek siteye ulaşmadan önce saldırgan tarafından yapılmış sahte sayfaya ulaşmaktadır. Böylece ulaşmak istediği siteye giriş yapmak için kullanıcı bilgilerini saldırgana teslim etmiş olmaktadır. Bir başka saldırı yönteminde ise kurban erişim sağlamak istediği siteye verilerini yollar ancak arada bulunan saldırgan bu verilerin aktarımını çeşitli programlar sayesinde kendisine aktarmaktadır.

Sonuç olarak, siber tehditlerin kapsamı oldukça geniş ve çeşitlidir. Bu tehditler, bireysel veya kurumsal olarak herkesi etkileyebilir ve ciddi sonuçlar doğurabilir. Bu nedenle, internet ve diğer dijital ortamlarda güvenliği sağlamak için alınan önlemler son derece önemlidir. İyi bir siber güvenlik planı, güçlü şifreler, yazılım güncellemeleri ve bilinçli internet kullanımı gibi önlemleri içermelidir.

2.2.3.2. Dünya’da ve Türkiye’de Siber Saldırı Örnekleri

İnternetin, ağların ve gelişmiş cihazların yaygınlaşmasıyla birlikte çevrimiçi güvenlik önemini her geçen gün arttırmaktadır. Dünya çapında yaşanan bazı siber saldırı örnekleri aşağıda verilmiştir.

2.2.3.3. Dünyada Siber Saldırı Örnekleri

Check Point Research² firmasının raporuna göre, 2022 yılında küresel siber saldırılar %38 arttı ve bu artışta evden çalışmanın yaygınlaşması, uzaktan bağlanma güvenlik açıkları ve online eğitimlerin COVID-19 sonrası eğitim kurumlarında yaygınlaşması etkili oldu. Bu artıştan faydalanmak isteyen küçük korsan çeteleri, siber saldırılarda öncülük etti ve son dönemde sağlık sektörüne de ilgi gösterdiler. Check Point Research, yapay zeka teknolojisinin gelişmesi ile birlikte 2023'te siber saldırı sayısındaki artışın devam edeceği konusunda uyarıda bulundu. Sağlık sektörü, diğer sektörlerle kıyasla artış oranında ilk sırayı almaktadır. Bu bölümde dünyadaki siber saldırı örnekleri yer almaktadır.

Irak Vakası

1992 yılında, ABD ve Irak arasında gerçekleşen bir siber saldırı örneği dünya gündemine oturmuştur. ABD, Irak'ın tüm iletişim sistemlerini ele geçirerek bu durumu kendi çıkarları doğrultusunda kullanmıştır. 2003 yılına gelindiğinde, Irak'ı işgal etmeyi planlayan ABD, Irak Savunma Bakanlığı'nın veri tabanını ele geçirmiş ve çalışanlarına bir mesaj göndermiştir. Mesajda, savaşın başlayacağı ve halkın evlerine gitmesi gerektiği belirtilmiştir. Mesajı dikkate alan Iraklı çalışanlar ve askerler yerlerini terk ederek, ABD'nin işgaline hazırlıksız yakalanmışlardır. Bu olay sonucunda, ABD'nin siber saldırısı Irak'a büyük bir dezavantaj sağlamış ve işgal planları kolaylıkla gerçekleştirilmiştir. (Karakuş, 2011: 146). Bu vaka ile teknolojinin ve internetin hayatlara dahil olmasıyla savaş stratejilerinde de değişimler yaşandığı görülmektedir (Tunca, 2019: 5).

² Check Point Research, müşterilerine ve daha geniş bir siber güvenlik topluluğuna son derece gelişmiş tehdit istihbaratı sunan bir siber güvenlik araştırma ekibidir. Dünya genelinde işletmeler ve kuruluşlar için siber güvenlik çözümleri sağlayan önde gelen bir şirket olan Check Point Software'nin bir parçasıdır. Araştırma ekibi, yeni ortaya çıkan siber tehditleri tespit etmek ve analiz etmek için sürekli çalışır, bulgularını ve görüşlerini müşterileri ve daha geniş güvenlik topluluğuyla paylaşır.

Solar Sunrise Vakası

ABD Savunma Bakanlığı ağı Şubat 1998'de bir dizi saldırıya maruz kaldı. Saldırıda UNIX tabanlı bir işletim sistemi olan Solaris'teki bir güvenlik açığı kullanıldı. Saldırganlar ilk olarak sistemde bu zafiyetin varlığını kontrol etti ve var olduğunu anlayınca bu zafiyetten yararlanarak sisteme bilgi toplama saldırısı başlattı. Programı kurdular ve topladıkları bilgileri almak için geri döndüler. 1-26 Şubat 1998 tarihleri arasında gerçekleşen saldırılarda aynı saldırı yöntemini kullandı (www.globalsecurity.org):

- Herhangi bir güvenlik açığının olup olmadığının tespiti için gerekli araştırmaları yapmak,
- Tespit edilen bu güvenlik açığından faydalanmak,
- Sniffer programını veri toplamak için kullanmak,
- Toplanan bu verileri almak için tekrar geri dönmek.

Ay Işığı Labirenti (Moonlight Moze)

Mart 1998'de başlayan ve "Ay Işığı Labirenti" olarak bilinen bir siber saldırı operasyonunda, ABD'nin NASA, ABD Enerji Bakanlığı, Pentagon ve üniversitelerin araştırma ve geliştirme sırları, askeri tesislerin haritaları, askeri tesislere ait bilgiler de dahil olmak üzere pek çok hassas bilgi ele geçirilmiştir. Bu saldırıyı diğerlerinden ayıran en önemli şey, rastgele değil, organize edilmiş olmasıdır. Saldırı sırasında sınıflandırılmamış bilgilere sahip bilgisayarlara erişildiği bildirilirken, hassas bilgilerin bir bütün olarak sistemlere dahil edilmiştir. Saldırıların takibi, saldırıların Moskova'ya 20 mil uzaklıkta bulunan ve Rusya Bilimler Akademisi ile yakın bağları olan bir servis sağlayıcı aracılığıyla gerçekleştirildiğinin ortaya çıkarılması iki sene gibi uzun bir zaman almıştır. Zira saldırı hakikatte 1996 senesinde şekillenmeye başlamış, 1998 senesinde ise ABD sızıntıyı tespit edebilmiştir. ABD gibi bir süper gücün dahi bu saldırının siber güvenlikte tehditlerle karşı karşıya kalılabileceğini ve bu tehditlerin ebatlarının ne denli ağır olabileceğini göstermesi dolayısıyla çok önemlidir (Yılmaz, 2018: 26-27).

ABD, yıllar boyunca ve milyonlarca dolar harcayarak edindiği tecrübeyi kaybettiği bir operasyonla karşı karşıya kalmıştır. Bu operasyon, hesaplanamayacak bir ekonomik kayba neden olmuş ve ABD'nin tüm askeri altyapısını yeniden inşa etmek zorunda kalmıştır. Çünkü düşman, askeri tesislerin yerleri, karargahların koordinatları ve stratejileri gibi gizli bilgilere erişmiştir.

Kosova Vakası

NATO-Kosova Krizi (1999), 1990'larda İnternet'in hızlı büyümesinden sonra gerçekleştirilmiştir. Kosova Savaşı sırasında NATO uçaklarının Sırbistan'ı bombalamaya başlamasından sonra, Kara El (Black Hand) gibi Sırp yanlısı ve Batı karşıtı hacker grupları NATO'nun internet altyapısına saldırmaya başlamışlardır. Siber saldırıların Yugoslavya Federal Cumhuriyeti silahlı kuvvetlerinin çıkarları doğrultusunda gerçekleştirilip gerçekleştirilmediğinin tespiti mümkün olmamakla birlikte, NATO askeri operasyonlarını aksatmaya yönelik olduğu anlaşılmıştır. Kara El (Black Hand) hacker grubu, adını Birinci Dünya Savaşı'nın başlamasına yol açan pan-Slav gizli cemiyetinden almıştır. Savaş sırasında Kara El (Black Hand) hacker grubunun NATO'nun en önemli bilgisayarlarını ele geçirdiği ve bilgisayarlardaki tüm verileri sildiği iddia edilmiştir. Bu durum NATO'nun, Kosova Savaşı'nda her ne kadar amacına ulaşmış olduğu kabul edilse de siber saldırılar karşısında yetersiz kaldığını ortaya koymuştur (Özkan, 2019:120; Sertçelik, 2018:33).

Avustralya Atık Sistemi Scada Vakası

2001 yılında kanalizasyon arıtma tesisine içeriden sızmalar sonucu yazılım geliştirme ekibinin eski bir çalışanı, şirketin otoparkından wifi'na bağlanarak Queensland kanalizasyon arıtma tesisini tam 46 defa hacklemiş ve yaklaşık 264.000 galon ham lağımı yakındaki parklara ve nehirlerle salmıştır. Kanalizasyon arıtma tesisinin tekrar çalışması için harcanan para vakanın ilk ekonomik etkisidir. Tesisin çalışmaması sonucu civardaki nehirlerle atık su boşaltması nedeniyle nehirler kirlenmiştir. Dolayısıyla buradaki ekosistem tehlikeli hale gelmiştir. Bu sorunun giderilmesi için de epeyce para harcanmıştır. Bu tesis vakası aynı zamanda balıkçılık ve turizm sektörünün de olumsuz etkilemiştir. Firma vaka sonucu yaşadığı bu sıkıntılardan sonra siber güvenlik yatırımlarını arttırmak zorunda kalmıştır (<https://ciip.wordpress.com>).

ABD ve Kanada Elektrik Kesintisi

14 Ağustos 2003 tarihinde Kanada'nın Ontario eyaleti ve ABD'nin birçok eyaletinde elektrik kesintileri meydana gelmiştir. Ontario'daki elektrik kesintisi, yaklaşık bir hafta boyunca devam eden ve 50 milyon kişiyi etkileyen, ABD tarihindeki en büyük elektrik kesintisi olarak kaydedilmiştir. Bu kesintinin ABD için maliyetinin 4 ila 10 milyar dolar arasında olduğu söylenmektedir. Ontario'da ise üretimin aksaması nedeniyle kesintinin 2,3 milyar Kanada doları maliyeti olduğu tahmin edilmektedir. Yaşanan bu

olay, Kanada ve ABD'nin gelecekte benzer bir durumun yaşanmaması için ekstra önlemler alması gerektiğini göstermiştir (Özkan, 2019: 127-128).

Yahoo Vakası

2013 ve 2014 yıllarında gerçekleşen iki ayrı siber saldırı sonucu, 3 milyar kullanıcının kişisel bilgileri ele geçirildi. Saldırganlar, kullanıcıların isimleri, e-posta adresleri, telefon numaraları ve şifreleri de dahil olmak üzere çeşitli bilgilere erişti.

2014'ün sonlarında, öncü İnternet şirketi Yahoo tarihteki en büyük veri ihlallerinden birini yaşadı. Bu saldırıda toplam 500 milyon Yahoo kullanıcısının güvenliği ihlal edildi. Kurbanların, saldırıda kimlik bilgileri, parolaları ve güvenlik sorularının yanıtları çalındı.

Ayrıca Yahoo, 2016 yılına kadar bu ihlalleri bildirmemiş ve Menkul Kıymetler ve Borsa Komisyonu (SEC) Yahoo'ya zamansız raporlama için 35 milyon \$'lık 40'tan fazla toplu dava açmıştı. Olaylar ayrıca şirketin satış fiyatını yaklaşık 350 milyon \$ düşürmüştü (Tsukayama, Timberg, ve Fung, (2016).

Ec-Council'in Vakası

23 Şubat 2014'te Eugene Belford adlı bir hacker, profesyonel etik hackerlar için bir Amerikan sertifika organizasyonu olan E-Commerce Consultants'ı (EC-Coincil) hacklemiştir. Konseye kayıtlı 60.000'den fazla etik hacker'ın kimlik bilgileri yayınlanmıştır. Kimlik bilgileri kamuoyuna açıklanan BT uzmanları arasında ABD Ordusu, FBI, Birleşmiş Milletler ve NSA üyelerinin de bulunduğu belirtilmiştir. Hackerlar, ele geçirdikleri kimlik bilgilerini, hackledikleri siteleri kaydettikleri zone-h sitesinde "Sertifikalı etik olmayan yazılım güvenliği uzmanına aittir." başlığıyla yayınlamıştır (Özkan, 2019: 120).

ABD Sermaye Piyasasına Saldırı Vakası

2014 yılında gerçekleşen bir dolandırıcılık davası, Vadim Ermolovich adlı bir Ukraynalı hackerın üç ekonomi dergisine ve özel finansal bilgilere erişmek ve bunları ticari amaçlarla kullanmakla suçlandığı davaydı. Bu bilgileri borsa oyuncularına satarak, piyasaların manipüle edilmesine neden oldu ve elde edilen bu bilgilerle 30 milyon dolarlık bir soygun gerçekleştirildi. Amerikan Adalet Bakanlığı, 28 yaşındaki Ermolovich'in elektronik dolandırıcılık, kimlik hırsızlığı ve hackerlık suçlamalarıyla tutuklandığını açıkladı. Bu, 2014'ün en büyük menkul kıymet dolandırıcılığı olarak kabul edildi (Varlık, 2016b).

Siber Saldırı Altındaki Ukrayna

2016 yılından itibaren Rusya'nın Ukrayna üzerinden yoğun bir şekilde siber saldırı gerçekleştirdiği ve hatta siber silahlarının test edilmesi için Ukrayna'yı bir test sahası olarak kullandığı bilinmektedir. Rusya, 2014 yılında Kırım'ı ilhak ettikten sonra Ukrayna'ya yönelik siber saldırılarını arttırmıştır. 2015-2016 yıllarında Ukrayna'daki ana elektrik santralinde gerçekleştirilen bir dizi siber saldırı neredeyse çeyrek milyon Ukraynalı'nın elektriksiz kalmasına sebep olmuştur. Saldırıları öncelikle Ukrayna hükümeti, finans ve enerji sistemlerini hedef almıştır. Kullanılan kötü amaçlı yazılımın kontrolden çıkması, hızla yayılmasına neden olmuştur ve bu da Batılı ve hatta Rus şirketlerinin milyarlarca dolar zarar etmesine neden olmuştur.

Rusya tarafından 24 Şubat' 2022'de başlayan Ukrayna işgali sırasında, Rusya Ukrayna askeri ve devlet kurumlarına yönelik çevrimiçi saldırılarını yüzde 196 artırmıştır. Rus askeri istihbarat örgütü GRU, Şubat 2022'de Ukrayna web sitelerine karşı bir dizi DDoS saldırısı başlatmış, bu saldırılar Ukrayna bankacılık ve savunma web sitelerini hedef aldı. Rus destekli gruplar, "DanaBot" adlı bir malware-as-a-service platformunu kullanarak Ukrayna Savunma Bakanlığı web sitelerine yönelik DDOS saldırılarına devam etmiştir. Rusya ayrıca, 24 Şubat'ta "IsaacWiper" adlı bir wiper yazılımıyla Ukrayna hükümet sistemlerine saldırmıştır.

WannaCry Vakası

Küresel bir etki yaratan WannaCry fidye yazılımı saldırısı, Mayıs 2017'de gerçekleşti. Fidye yazılımı, birçok organizasyonun sistemlerini kilitleyerek kurbanların dosyalarını şifreledi ve Bitcoin cinsinden fidye talep etti. Saldırganların saldırıda başarılı olmasının nedeni, bazı bilgisayar sistemlerinin güncelliğini yitirmiş olması ve yazılım güncellemelerinin yapılmamış olmasıdır. Saldırının etkisi küresel boyutta hissedildi ve birçok organizasyonun iş sürekliliğini etkiledi. Saldırganlar, ABD Ulusal Güvenlik Kurumu tarafından geliştirildiği iddia edilen bir ele geçirme yöntemini kullanarak Microsoft Windows işletim sistemindeki bir zayıflıktan faydalanarak saldırıyı gerçekleştirmeye karar verdi.

WannaCry fidye yazılımı saldırısında, saldırganlar önce 300 dolar değerinde bitcoin talep etmiş, daha sonra ise fidye miktarını 600 dolarlık bitcoin'e çıkarmıştı. Saldırı kurbanlarına, üç gün içinde fidyeyi ödemezlerse dosyalarının kalıcı olarak silineceği tehdidi yapılmıştı. Ancak verilerin geri verilmesi konusunda kesin bir güvence olmadığı

için kurbanlar, fidye ödemeye pek sıcak bakmamıştı. Saldırı sırasında kullanılan kod hatalı olduğundan, fidye ödemesi yapıldığında saldırganlar hangi kurbanın hangi bilgisayarı için ödeme yaptığını görememişti. Bu nedenle, kurbanların verilerinin geri getirilip getirilmediği hala kesin bir şekilde bilinmiyordu.

Dünyanın ilk "fidye solucanı" (fidye yazılımı kripto solucanı) olan WannaCry, 150 ülkede Windows ile çalışan 230.000 bilgisayarı etkilemiştir. Etkilenen şirketlerden biri İspanyol operatör şirketi Telefónica olmuştur. Birleşik Krallık'taki binlerce NHS hastanesi ve ameliyatı vakadan etkilenmiştir. Bu yüzden ambulanslar yanlış yönlendirilmiş ve acil tıbbi müdahaleye ihtiyacı olan insanlar mağdur olmuştur. Saldırı sonucunda 19.000 randevunun iptal edilmesi nedeniyle NHS'nin 92 milyon sterlin kaybettiği tahmin edilmiştir (www.kaspersky.com.tr).

Dünya Kupası Vakası - Phishing (Kimlik Avı) Saldırı Örneğini

2018'deki Dünya Kupasında Inc tarafından derlenen verilere göre Dünya Kupası kimlik avı dolandırıcılığında futbol taraftarlarına e-mailler iletilmiştir. Bu spam e-maillerle, Dünya Kupasına ev sahipliği yapan Moskova'ya asılsız gezi düzenleyen dolandırıcılarla taraftarlar kandırılmaya çalışılmıştır. Bu e-maillere girip linke tıklayanların kişisel verileri ele geçirilmiştir (www.cyberartspro.com).

Harris Federasyonu Vakası

Mart 2021'de, Londra merkezli Harris Federasyonu bir fidye yazılımı saldırısına maruz kalmış ve yönettiği 50 ikincil ve birincil akademinin tamamının aygıtlarını ve e-maillerini "geçici olarak" devre dışı bırakmak mecburiyetinde kalmıştır. Bu, 37.000'den fazla çocuğun derslerine ve sanal ortamdaki sohbetlerine ulaşamamasıyla neticelenmiştir (www.cyberartspro.com).

Kosta Rika'da Conti saldırısı

2022 yılında Conti grubu, Kosta Rika gibi küçük bir Güney Amerika ülkesine karşı büyük bir saldırı gerçekleştirerek, ülkenin hükümeti tarafından "siber terörizm" olarak nitelendirilen bu şok edici saldırının ardından ulusal acil durum ilan edilmiştir. Conti grubu, muhtemelen başka projelere odaklanarak veya tamamen yeni bir isimle ortaya çıkarak, RaaS saldırılarının genellikle emniyet güçlerinin ve hükümetlerin denetiminden kaçtığı için bu saldırının ardından kaybolmuştur.

Lapsus\$ Şantaj Grubu

2022 yılında ortaya çıkan Lapsus\$ adlı şantaj grubu, yüksek profilli veri hırsızlıkları gerçekleştirerek kurumsal kurbanlarından zorla ödeme almaya çalışmıştır. Microsoft, Samsung, Nvidia, Ubisoft, Okta ve Vodafone gibi şirketler de bu kurbanlar arasında yer almıştır. Grup, rüşvet vermek gibi yöntemler kullanarak hedeflerine ulaşmıştır. Bir süre sessiz kalmış olan grup, yılın sonunda Rockstar Games'in geliştiricisi olduğu Grand Theft Auto'ya saldırarak tekrar gündeme gelmiştir. Grubun birkaç üyesi Birleşik Krallık ve Brezilya'da tutuklanmıştır.

2022 yılının başlarında Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'nin (STM) kendi Honeypot³ verileri, dünya genelinde en fazla siber saldırının gerçekleştirildiği ülkeleri belirledi. 2022'nin ilk üç ayında, Honeypot sensörleri üzerinden toplam 6 milyon 137 bin 330 saldırı tespit edildi. Hindistan, 1 milyon 308 bin saldırı sayısı ile en çok saldırı yapan ülke oldu ve ABD 632 bin saldırıyla ikinci sırada yer aldı. Bu ülkeleri sırasıyla Vietnam, Rusya, Çin, Meksika, Pakistan, İran, Japonya ve Brezilya takip etti. Rusya'nın saldırı sayısı önemli ölçüde arttı ve 467 bin saldırı gerçekleştirdiği kaydedildi. Raporda, bu artışın nedeni olarak Rusya'nın Ukrayna'yı işgal girişimiyle birlikte Rus tehdit aktörlerinin eylemlerini artırması gösterildi.

2023 yılında da siber saldırıların artarak devam edeceği kaçınılmaz bir gerçektir. Özellikle; yapay zeka tabanlı uygulamalar, elektrikli araçlar, metaverse, devletler arası siber saldırılar ve blockchain teknolojileri gibi alanlarda siber saldırılar artabilir.

Latitude Financial Vakası

Avustralya'da bir finans şirketi olan Latitude Financial'ın 330.000 müşterisinin kişisel verileri, bir siber saldırı sonucunda bilgisayar korsanları tarafından ele geçirildi. Avustralya Menkul Kıymetler Borsası aracılığıyla yapılan saldırıyı duyuran şirket, 16 Mart 2023'te yaklaşık 330.000 müşterinin kişisel verilerinin çalındığını söyledi. 3 milyon civarında müşterisi olduğu söylenen şirket, çalınan gizli bilgiler arasında 100 bin ehliyetin de yer aldığını belirtti.

³ Honeypot: Saldırganların çalışma yöntemlerini ve çeşitli tehdit türlerini araştırmak için tasarlanmış bir güvenli ve kontrol edilebilir bir ortamdır. Bu ortam, saldırganların gerçek hedeflerine zarar vermeden önce, onların kullanacakları yöntemleri ve teknikleri anlamak ve anlamak için kullanılır. Bu sayede savunma ekipleri, gerçek dünya saldırılarına karşı daha iyi hazırlanabilir ve savunma stratejilerini geliştirebilirler.

Yaşanılan bu siber saldırıyla ilgili müşterilerini bildirmek isteyen şirket, ilgililere e-mailler gönderdi ve sosyal medya hesaplarının şu anda daha fazla güvenlik tehdidinden kaçınmak için kullanılmadığını söyledi. Aynı zamanda şirket, korsanların kendilerinden fidye talep edip etmediğine dair bir açıklamada bulunmadı.

Bu siber saldırı olayının ardından hükümet, 1,7 milyar dolarlık siber güvenlik planlarını duyurdu ve gelişip yenilenen stratejileriyle İçişleri Bakanlığı bünyesinde ulusal siber güvenlik ofisi kurulacağı belirtti (www.trthaber.com).

2.2.3.4. Türkiye’de Siber Saldırı Örnekleri

2022’de Türkiye’de kötü amaçlı yazılım saldırıları bir önceki yıla göre % 61 artarak 1.015.810’a yükselmiştir. Yayınlanan araştırmalara göre her saat 116 yeni siber saldırı gerçekleşmektedir (www.haberturk.com). Türkiye’de ortaya çıkan siber saldırılar genellikle, kredi kartı dolandırıcılığı, DDoS saldırıları, mobil tehditler, fidye yazılımları ve ortalama saldırılarıdır (www.rasyotek.com.tr).

RedHack, 1997 yılında kurulan bir grup olup, Marksist ve sosyalist eğilimleri benimsemektedir. Grup, ülkemizdeki sivil direniş konuları ve olayları hakkında çeşitli bilgi, video, fotoğraf ve yorumları hem ulusal hem de uluslararası kamuoyuyla paylaşarak duyurmayı amaçlamaktadır. Grubun, ülkemize yönelik gerçekleşen birçok saldırının arkasında olduğu düşünülmektedir. Bu sebeple, RedHack üyelerine karşı geniş çapta operasyonlar düzenlenmiş ve birçok hukuki işlemle karşı karşıya kalmışlardır. Ancak grup, yayınladığı içerikler ve eylemleriyle özellikle sosyal medyada geniş bir takipçi kitlesine sahip olmuştur.

Anonymous, dünya genelinde faaliyet gösteren ve çeşitli siyasi olaylar karşısında protesto etmek için devlet kurumlarına siber saldırılar düzenleyen bir hacker grubudur. Türkiye’de de birçok kurumu hedef almış ve saldırılar gerçekleştirmiştir. İlk zamanlarında eğlence odaklı bir çevrimiçi topluluk olarak tanınan Anonymous, 2008 yılından itibaren uluslararası internet saldırıları ve protestolar ile anılır hale gelmiştir.

RedHack, Anonymous ve diğer kaynaklarla ilgili yaşanan siber saldırılardan bazıları şöyledir:

Telekomünikasyon İletişim Başkanlığı (TİB) Saldırısı

Uluslararası siber-aktivistler grubu Anonymous, Türkiye’de internet sitelerinin sansürlenmesine yönelik yapılan "filtre" iddialarına tepki göstererek, temel hak ve özgürlüklerin ihlal edileceği gerekçesiyle 9 Haziran 2011 tarihinde siber saldırılar

düzenlemeye başlamıştır. Bu saldırılar, TİB'e bağlı web sitelerine yönelik DDoS saldırıları ile gerçekleştirilmiştir. Ancak TİB'in siber güvenlik önlemleri sayesinde, Anonymous üyeleri istedikleri sonuca ulaşamamışlar, bunun üzerine grup, bazı kamu kurumları ve siyasi partilerin web sitelerine saldırmıştır.

Kızıl Hackerlar (RedHack) Ankara Emniyet Müdürlüğü Vakası

Kızıl Hacker'lar olarak bilinen bir grup, 4 Mart 2012'de Polis Ağı (POLNET) ve Ankara Emniyet Müdürlüğü sunucularına izinsiz olarak erişim sağlamış ve burada yer alan birçok bilgiyi ele geçirmiştir. Bu bilgiler arasında şikayet dilekçeleri, ihbarlar ve yazışmalar gibi hassas ve mahremiyeti korunması gereken veriler de bulunmaktadır. Kızıl Hackerlar daha sonra bu bilgileri internet üzerinde yayınlamıştır. Bu olay vatandaşlar arasında önemli endişelere yol açmıştır, çünkü kişisel bilgilerin ifşa edilmesi ve mahremiyetin ihlal edilmesi gibi ciddi güvenlik riskleri ortaya çıkmıştır.

Kızıl Hackerlar (RedHack) Türk Hava Yolları (THY) Vakası

29 Mayıs 2012 tarihinde havacılık sektörü için getirilen grev yasağına karşı çıkan THY çalışanları grev yapmıştır. THY'nin o tarihte yaptığı açıklamaya göre grev nedeniyle 100 uçuş iptal edilmiş ve Atatürk Havalimanı'ndan kalkacak seferlerde gecikmeler yaşanmıştır. THY, grevin kanunsuz olduğunu belirtmiş ve greve katılan personellerini bildirimsiz işten çıkarma kararı almıştır. Bu karar RedHack adlı bir grup, THY web sitelerini hack'leyerek grevi desteklediklerini açıklamıştır. RedHack, Twitter hesabından yaptığı açıklamada, THY'nin emekçilerinin haklarını savunduklarını ve seyahat şirketiyle ilgili sorunun çalışanlar değil, yönetim olduğunu belirtmiştir.

Turkcell Vakası

15 Aralık 2014 tarihinde, Turkcell'in müşteri hizmetleri resmi Twitter hesabı, bir siber saldırı sonucu hacklenmiştir. Turkcell'in ana sayfasından yapılan açıklamada, saldırganların hesaba erişim sağlayarak yanıltıcı mesajlar gönderdikleri belirtilmiştir. Turkcell, hızlı bir şekilde olayı doğrulayarak, kullanıcıları bu mesajlara itibar etmemeleri konusunda uyarıda bulunmuştur.

14 Aralık 2015 – 24 Aralık 2015 '.tr' Vakası

2015 yılında 14 Aralık'ta başlayan ve yaklaşık 10 gün süren bir siber saldırı, özellikle ".tr" uzantılı alan adlarının yönetildiği sunucuları hedef almıştır. Bu saldırı sonucu birçok banka, noter ve devlet kurumunun internet sitesi ve mobil uygulamaları

erişilemez hale gelmiştir. Bu saldırılar, dünya üzerinde yaşanmış en yoğun siber saldırılardan biri olarak kabul edilmiştir ve internet trafiğini büyük ölçüde etkilemiştir.

Demirören Vakası

25 Mart 2018 tarihinde Demirören Grubu'nun Doğan Yayın Holding'i satın almasının ardından Kızıl Hackerlar tarafından Demirören Grubu'na bir saldırı gerçekleştirilmiştir. Saldırgan, Demirören Holding'e ait tüm internet sitelerini hacklemiştir.

TRT Çocuk Vakası

29 Nisan 2018 tarihinde TRT'nin TRT Çocuk web sitesi ele hacklendi. Hedefi <https://www.trtcocuk.net.tr/> web sitesi olan hackerlar, "Boğaziçi Üniversitesi kendi düşüncelerini savunduğu için susturuldu biz de buna kayıtsız kalmayacağız ne mutlu insanım diyebilene" şeklinde paylaşımda bulundular. Aynı zamanda bu hackerlar, 1 mayısta provokasyon amacıyla toplanma çağrısında bulundular (www.cybermagonline.com).

N11 Vakası

Kişisel Verileri Koruma Kurumu, 26 Aralık 2019 tarihinde Türkiye'nin önde gelen e-ticaret sitelerinden biri olan n11.com'a üye olan 832 müşterinin e-posta adreslerinin çalındığını açıklamıştır. Bu durum, online alışverişler sırasında kullanıcıların cep telefonu numaraları, ev adresleri ve diğer özel bilgilerinin istendiği düşünüldüğünde büyük bir veri sızıntısı olduğunu göstermektedir (www.memurlar.net).

2.3. SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ

Siber güvenlik ve bilgi güvenliği, günümüzde önemli bir konu haline gelmiştir. İnternet kullanımının artması, dijital dönüşüm sürecinin hızlanması ve siber suçların artması, siber güvenliğin hayati bir konu haline gelmesine neden olmuştur. Siber suçlar, siber casusluk, fidye yazılımları, kimlik hırsızlığı ve veri ihlalleri gibi birçok tehdit içermektedir. Bu tehditler, hem bireysel kullanıcıları hem de organizasyonları hedef almaktadır (Güngör ve Güney, 2017: 138). Bu tehditlerle baş ederken siber güvenlik ve bilgi güvenliği birlikte hareket ettiği için bu iki kavramın birbiri ile karıştırıldığı tespit edilmiştir. Bu sebeple siber güvenlik ve bilgi güvenliği konularının derinlemesine açıklanması gerekmektedir.

2.3.1. Bilgi Güvenliđi

Bilgi güvenliđi kavramının ortaya çıkışı 1990'lı yıllarda gerçekleşmiştir. Teknoloji konusundaki iyileşmeler, bilgi ve bilgi tabanlı sistemlerin popülerize olması ve internet kullanımının artması gibi olgular bilginin sakınılması hususundaki ehemmiyetini ortaya çıkarmaktadır (Akdoğan vd., 2018).

Bilgi güvenliđi, herhangi bir bilginin istenmeyen kişilerce elde edilmesini engelleme girişimidir. Bilgilere, yetkisi olmayan kişilerin ulaşılıp bu bilginin kullanılması, ortaya çıkarılması, silinmesi, değıştirilmesi veya zarar verilmesi kısaca kişisel veya kurumsal mahremiyeti, bütünlüğü ve ulaşılabilirliđi ihlal eden olguların öne geçilmesi halinde bilgi güvenliđi sağlanmış olmaktadır (Aldemir ve Kaya, 2020). Bilgi güvenliđi, sadece edinilen bilginin kötüye kullanılmamasını deđil, edinildiđi kaynağın yasal olması, iletim aşamasındaki kanalların güvenli olması ve gerektiđi zaman güvenli bir şekilde yok edilmesi unsurlarını da kapsayan bir sürecin ifadesidir (Taner ve Kılıç, 2019).

Hemen hemen her şey internet üzerinden yapılabildiđi için insanlar artık daha verimli bir şekilde çalışabilmektedirler. Ancak bu kolaylığın bir sonucu olarak, bilgileri korumak yani bilgi güvenliđini sağlamak konusu daha da önem kazanmıştır. Bu güvenliđi sağlamak için organizasyonların ve bireylerin bazı önlemler almaları gerekmektedir. Bu önlemlerden bazıları aşağıda sıralanmaktadır:

1. **Güçlü Parolalar Kullanımı:** Parola oluşturulurken en az 8 karakterin kullanılması ve oluşturulan parolanın sayı, harf ve sembol kombinasyonu içermesi önemlidir. Aynı zamanda bu parolaların düzenli olarak değıştirilmesi ve aynı şifrenin birden fazla hesap için kullanılmaması önemlidir.
2. **Antivirüs Yazılımı Kullanımı:** Bilgisayarları zararlı yazılımlardan korur ve herhangi bir virüs tehlikesine karşı güvenlik önlemleri alır. Güncellemeleri takip etmek ve antivirüs yazılımı düzenli olarak güncellemek son derece önemlidir.
3. **Ağ Güvenliđi:** Kurumsal ağlar ve kablosuz ağlar, güvenli olmayan bir şekilde yapılandırıldığında, potansiyel saldırganlar için açık bir davetiye haline gelir. Ağı korumak için güçlü bir şifreleme kullanmanın yanı sıra güncellemelerin düzenli olarak yapılması ve yalnızca güvenilir cihazlar kullanılması önemlidir.
4. **E-posta Güvenliđi:** E-postaların çođu, herhangi bir önlem alınmadan, açık bir şekilde gönderilir. E-posta şifrelemesi kullanılarak gönderilen iletiler, e-postaların

alıcısının yalnızca şifreli bir şekilde gönderiyi açabilmesini sağlar. Ayrıca, herhangi bir eki açmadan önce, e-posta'nın güvenilir olduğundan emin olunması güvenlik için önemlidir.

- 5. Düzenli Yedekleme:** Bilgi kaybını önlemek için yedekleme yapmak önemlidir. Yedekleme işlemi, verilerin güvenli bir şekilde saklanmasını sağlar ve bir güvenlik ihlali yaşanması durumunda veri kayıplarını en aza indirir.

Bilginin tam anlamıyla korunması adına tüm ögeler titizlikle gözden geçirilip lazım olan tüm destekler sağlansa dahi, insan unsurunun bu sürecin en zayıf halkası olduğu unutulmamalıdır. Bilgi güvenliği ile alakalı gerekli tüm eğitimler hem özel hem de kamu kurumları tarafından çalışanlara verilmeli, tedbirler üst seviyede tutularak yaşanabilecek maddi ve manevi kayıplar önlenmeye çalışılmalı, kurum içerisinde istihdam edilen personelin hatalı davranışları ve ihlalleri yüzünden bilgi güvenliğinin sektöre uğraması engellenmelidir (Vural ve Sağıroğlu, 2013).

2.3.2. Siber Güvenlik

Teknolojinin hızla gelişmesiyle birlikte, internetin kullanımı da yaygınlaşmış ve korsanlığın bir parçası haline gelmiştir. Ancak, internetin ulaşım kolaylıklarının avantajlarının yanı sıra, dezavantaj olarak siber suçlar da artmaktadır. Siber güvenlik, bu siber suçlara karşı korunmak için gerekli önlemleri almak adına ortaya atılan bir kavramdır. Siber güvenlik ilk olarak 1990'ların başında bilgisayar bilimcileri tarafından ağ tabanlı platformlarda bir dizi siber güvensizliğe dikkat çekmek için kullanılmıştır (Helen, 2005).

Siber güvenlik, bilişim sistemlerinin, ağların, cihazların ve verilerin kötü amaçlı saldırılardan korunması ile ilgilenen bir disiplindir. Siber güvenlik, herhangi bir siber suçtan korunmak için alınan önlemlerin tamamını kapsamaktadır. Bunun yanı sıra, siber güvenlik, veri güvenliği, ağ güvenliği, uygulama güvenliği, kullanıcı güvenliği ve fiziksel güvenlikleri de içermektedir. Siber güvenlik, siber saldırıları etkilerini en aza indirmek için son derece önemlidir (Akyazı, 2019).

Siber saldırılar, kötü niyetli kişi veya kişilerin, bilgisayar sistemlerine ve dijital cihazlara sızarak, çeşitli zararlı amaçlarda bulunmalarıdır. Siber saldırılar, kişisel veri hırsızlığı, kimlik avı, fidye yazılımları, kötü niyetli yazılımlar ve diğer zararlı faaliyetleri içermektedir. Siber güvenlik, sadece bireysel kullanıcılar için değil, aynı zamanda işletmeler ve devlet kurumları için de büyük bir endişe kaynağıdır. Çünkü bir siber saldırı,

bir bilgi müşteri verilerini, finansal bilgileri veya ticari sırlarını çalabilir ve bu durum, müşterilerin itibarını ciddi şekilde zedeleyebilir. Benzer şekilde, bir devlet kurumuna yapılan bir siber saldırı, önemli stratejik verilerin çalınmasına veya kritik altyapıların hedef alınmasına neden olabilir (Aldemir ve Merve, 2020)

Siber güvenlik uygulamaları siber suçlardan korunmak için kullanılan önlemlerdir. Bunlardan bazıları şöyledir (Liang ve Kim, 2022; Özkan, 2011; Liao, Richard Lin, Lin ve Tung, 2013; Bace ve Mell, 2001; Raiyn, 2014; Dolan ve Widayanti, 2022; Öztürk, 2018):

1. Güvenlik Duvarı: Ağdaki trafiği kontrol eden ve istenmeyen trafiği engelleyen bir yazılımdır. Güvenlik duvarları, ağa erişmek için belirli protokollerin veya IP adreslerinin kullanılmasını engelleyebilir ve saldırganların ağa erişmesinin önlemektir.
2. Kimlik doğrulama: Kullanıcıların kimliklerinin doğrulanması için kullanılan bir yöntemdir. Kimlik doğrulama, kullanıcıların parola, biyometrik veri veya çift faktörlü kimlik doğrulama gibi yöntemlerle kimliklerini doğrulamaktadır. Bu, kullanıcıların hesaplarına yetkisiz erişimi önlemektir.
3. Şifreleme: Verileri bir anahtarla şifreleyen bir yöntemdir. Şifrelenmiş veriler, yalnızca doğru anahtara sahip kişiler tarafından okunabilmektedir. Bu, verilerin kötü niyetli kişiler tarafından ele geçirilmesini önler ve gizliliği sağlamaktadır.
4. Güncelleme yönetimi: Güvenlik açıklarını düzeltmek için yazılımın ve işletim sisteminin güncellenmesini içermektedir. Bu, saldırganların sistemlere erişmesini ve kontrol etmesini önlemektir.
5. İzleme: Bir organizasyondaki güvenlik olaylarının izlenmesi, analizi ve yönetimi için kullanılan bir yöntemdir. Bu, olay günlüklerinin toplanması, analizi ve raporlanması, siber saldırıların tespiti ve müdahale edilmesi ve güvenlik olayları hakkında duyarlılık yaratılması gibi konuları kapsamaktadır.
6. Saldırı tespit sistemleri: Ağda belirli faaliyetleri tespit etmek için kullanılan bir yöntemdir. Bu sistemler, zararlı yazılım, saldırılar ve diğer güvenlik risklerini tespit etmek için kullanılmaktadır.
7. Sızma testi: Bir organizasyonun güvenlik zafiyetlerini tespit etmek için kullanılan bir testtir. Bu testler, saldırganların kullanabileceği yöntemleri taklit ederek ağ güvenliği açısından zayıf noktaları tespit etmek için gerçekleştirilmektedir.

8. Güvenlik politikaları: Bir organizasyonun güvenlik stratejisini ve hedeflerini belirleyen belgelerdir. Bu politikalar, organizasyonun güvenlik ihtiyaçlarını karşılamak için belirli yönergeler ve prosedürler içermektedir.
9. Veri kurtarma: Bir organizasyonun verilerinin kaybolması veya zarar görmesi durumunda verileri kurtarmak için kullanılan bir yöntemdir. Bu, verilerin kaybolması veya zarar görmesi durumunda organizasyonun iş sürekliliğini sağlamaktadır.
10. Güvenlik yazılımı: Bir organizasyonun bilişim sistemlerinin güvenliğini sağlamak için kullanılan yazılım araçlarıdır. Örnek olarak, antivirüs yazılımları, güvenlik duvarları ve saldırı tespit sistemleri gibi araçlar sayılabilmektedir.
11. Güvenlik eğitimi: Bir organizasyondaki çalışanların bilinçli ve güvenli bir şekilde çalışmalarını sağlamak için verilen eğitimidir. Bu eğitim, çalışanların güvenlik tehditlerini tanıyabilmesi, güvenli şifreler oluşturabilmesi ve e-posta dolandırıcılığı gibi saldırıları tanıyabilmesi gibi konuları kapsamaktadır.
12. Bulut güvenliği: Bir organizasyonun bulut bilişim hizmetleri kullanırken güvenlik ihtiyaçlarını karşılamak için kullanılan bir yöntemdir. Bu, bulut sağlayıcısının güvenlik önlemleri, verilerin şifrelenmesi, kullanıcı erişim kontrolü ve bulut uygulamalarının güvenliği gibi konuları kapsamaktadır.
13. Ağ güvenliği: Bir organizasyonun ağını korumak için kullanılan bir yöntemdir. Bu, ağ trafiğinin izlenmesi, güvenlik duvarları ve saldırı tespit sistemleri gibi araçlar kullanılarak ağa giren ve çıkan trafiğin kontrol altında tutulması, ağa güvenli erişim sağlanması gibi önlemleri içermektedir.
14. Siber güvenlik eğitimi: bir organizasyonun çalışanlarına siber güvenlik bilincini kazandırmak için kullanılan bir yöntemdir. Bu, siber güvenlik tehditlerinin tanıtılması, güvenli davranışların teşvik edilmesi, güvenlik politikalarının açıklanması ve eğitimlerin sürekli olarak yenilenmesi gibi konuları kapsamaktadır.
15. Fiziksel güvenlik: Bir organizasyonun fiziksel varlıklarını, çalışanlarını ve ziyaretçilerini korumak için kullanılan bir yöntemdir. Bu, bina erişim kontrolü, video gözetimi, güvenlik personeli, kapı ve pencere kilitleme sistemleri ve alarm sistemleri gibi konuları kapsamaktadır.

16. Yedekleme ve kurtarma: Bir organizasyonun verilerinin güvenliğini sağlamak için kullanılan bir yöntemdir. Bu, verilerin yedeklenmesi, yedeklerin düzenli olarak test edilmesi, felaket kurtarma planlarının hazırlanması ve yedeklerin güvenli bir şekilde saklanması gibi konuları kapsamaktadır.
17. Dış kaynak kullanımı: Bir organizasyonun güvenliğini etkileyebilecek dış kaynakların yönetilmesi için kullanılan bir yöntemdir. Bu, dış kaynakların siber güvenlik yeterliliğinin değerlendirilmesi, sözleşme yapılması, düzenli güvenlik denetimleri yapılması ve dış kaynakların güvenli bir şekilde kullanılması gibi konuları kapsamaktadır.
18. Web güvenliği: Bir organizasyonun web sitelerinin ve uygulamalarının güvenliğini sağlamak için kullanılan bir yöntemdir. Bu, web uygulama güvenliği testleri, güvenli yazılım geliştirme, web sunucusu güvenliği, web tarayıcı güvenliği ve web uygulaması güvenliği için en iyi uygulamaların takip edilmesi gibi konuları kapsamaktadır.

Sonuç olarak, siber güvenlik ve bilgi güvenliği, günümüzde hayati bir konu haline gelmiştir. Siber suçların artması ve internet kullanımının artması nedeniyle, siber güvenlik ve bilgi güvenliği, herkes için önemli hale gelmiştir. Organizasyonlar ve bireyler, siber güvenlik ve bilgi güvenliği konusunda bilinçlenerek, alınması gereken önlemleri uygulamalıdır. Bu sayede, siber suçların etkisi azaltılabilir ve güvenli bir dijital dünya oluşturulabilir.

2.4. SİBER GÜVENLİK KAVRAMLARI

Siber güvenlik, bir organizasyonun ya da kişinin bilgisayar, ağ ve internet gibi dijital sistemlerini, cihazlarını ve verilerini tehditlerden korumak için alınan önlemlerdir. Siber güvenliğin alanına giren bir dizi kavram vardır. Bunlardan çoğu aşağıdaki gibi sıralanmıştır.

2.4.1. Siber

Siber terimi, kökenini sibernetik biliminden almaktadır. Sibernetik, canlılar ve makineler arasındaki iletişimi inceleyen bir disiplindir ve bu terim ilk olarak 1958 yılında sibernetiğin öncüsü kabul edilen Louis Couffignal tarafından kullanılmıştır. Sibernetik, insan davranışlarının yanı sıra mekanik ve elektronik sistemlerin de çalışma prensiplerini inceler ve bu prensipleri birbirleriyle etkileşim içinde olan tüm sistemler için

uygulanabilir kılmayı hedeflemektedir (www.wikipedia.org:a). Siber kavramı, internet, bilgisayarlar, dijital cihazlar ve diğer teknolojik sistemler gibi dijital ortamlarla ilgili anlamlarda kullanılan bir sıfattır. Günümüzde sanal alan olarak anlaşılsa da (Yılmaz, 2018) siber ve sanal ayrı kavramlardır. İnternet, yarattığı ortam açısından sanalken, iletişim yöntemi açısından siberdir (www.wikipedia.org:b).

2.4.2. Siber Zorbalık

İnternet, sosyal medya veya diğer dijital platformlar aracılığıyla bir kişi ya da grubun kuruma karşı kötü muamele, taciz veya zarar verme eylemlerini ifade eder. Bu tür zorbalık, kişisel bilgilerin ifşa edilmesi, hakaretler, tehditler, aşağılama, iftira, yönlendirme ve diğer benzeri işlemler şeklinde olabilir. Siber zorbalık, hem çocuklar hem de yetişkinler arasında yaygın bir sorundur ve ciddi sonuçlar olabilir, özellikle de kurbanların psikolojik sağlığı üzerinde olumsuz etkileri vardır (Heirman ve Walrave, 2008:1-2).

2.4.3. Siber Uzay

Siber uzay kavramı 1982 yılında William Gibson tarafından kaleme alınan Burning Chrome adlı yayında ilk olarak ele alınmıştır. Gibson, Neuromancer adındaki bilim kurgu romanında siber uzayı tanımlamıştır. Siber uzay, elektromanyetik dosyada oluşturulan bilgilerin, dünyanın dört bir yanına farklı sistemler kanalıyla gönderilmesi ve bu bilgilerin erişildiği sanal ortamların tamamıdır (Polat, 2020:137). Siber güvenlikte kullanılan bir terim olan siber uzay, internet üzerindeki tüm dijital sistemleri ifade eder. Aynı zamanda, bilgisayarlar, sunucular, ağlar, veritabanları, yazılımlar, mobil cihazlar ve diğer dijital sistemleri de içerir.

Siber uzayda, siber saldırganlar, kötü niyetli yazılımlar ve diğer tehditler, dijital varlıkları hedef alarak veri hırsızlığı, kimlik avı, fidye yazılımı ve diğer siber suçları gerçekleştirebilirler. Bu nedenle, siber güvenlik uzmanları, siber uzaydaki sistemlerin sınırlarını elde etmek için sürekli olarak tehditleri izlemeli ve önlem almalıdırlar (Yılmaz, 2018:28).

2.4.4. Siber Tehdit

İnternet ve diğer dijital sistemler üzerinden düşmanca kötü niyetli veya zararlı davranışlar “siber tehdit” olarak ifade edilmektedir. Bu tehditler, siber suçlular tarafından

bilgisayar ağıları, web siteleri, yazılımlar, cihazlar ve diğer dijital sistemlere saldırılar yaparak gerçekleştirilebilmektedir. Siber tehditlerin amaçları arasında, veri hırsızlığı, kimlik avı, fidye yazılımları, kötü amaçlı yazılımlar, hizmet reddi saldırıları (DDoS), casus yazılım ve diğer zararlı saldırganlar yer alabilmektedir. Siber tehditler, işletmeler, hükümet kurumları ve bireyler için ciddi riskler barındırmaktadır ve bu risklerden korunmak için siber güvenlik önlemleri alınması gerekmektedir (Yılmaz, 2018:29-30). Siber uzaydaki tehditler asimetrik tehditlerdir. Tehditlerin asimetrikliğine katkı yapan en önemli iki unsur anonimlik ve elde edilebilirliktir (Karabacak, 2011:3).

2.4.5. Siber Hijyen

Dijital dünyada güvenlik ve koruma sağlamak için alınan önlemlerin tümü “Siber Hijyen” olarak adlandırılmaktadır. Bu terim, kötü amaçlı yazılımlar, bilgisayar korsanları ve siber saldırılar gibi tehditlere karşı koruma amaçlı uygulamalar, politikalar ve korumaları kapsamaktadır.

Siber hijyen uygulamaları, bilgisayar cihazlarını ve cihazlarını korumak için kullanıcıların takip etmesi gereken belirli önlemleri içermektedir. Bu bölümler arasında güçlü parolalar kullanma, düzenli olarak yazılım tutma yapmak, siber saldırılara karşı koruyucu yazılımlar kullanma, dolandırıcılık ve kimlik avı saldırılarına karşı dikkatli olmak gibi önlemler yer almaktadır.

Siber hijyeni, bireysel kullanıcılar kadar organizasyonlar da sağlamalıdır. Özellikle işletmeler, müşteri bilgileri ve finansal veriler gibi hassas bilgileri sakladıkları için siber hijyene önem vermelidir (Ocak, 2021).

2.4.6. Siber Suç

Bilgisayar, internet ve diğer dijital teknolojileri kullanarak işlenen suçları ifade eder. Siber suçlar, özellikle son yıllarda giderek artan bir trenddir ve birçok farklı şekilde gerçekleştirilebilir. Siber suçlar arasında kimlik avcılığı (phishing), fidye yazılımı (ransomware), zararlı yazılımların (kötü amaçlı yazılım) kullanımı, bilgisayar korsanlığı (hacking), taciz izleme (örneğin çocuk istismarı), kimlik hırsızlığı ve siber zorbalıklar bulunmaktadır (egm.gov.tr).

2.4.7. Siber Terörizm

Bilgisayar korsanlığı ve siber saldırılar yoluyla, bir kişi ya da grup tarafından bir ülke veya kuruma karşı saldırgan, yıkıcı veya şiddet içeren eylemler için kullanılan bir

terimdir. Siber terörizm, siber güvenlik açıklarını kullanarak devletler, şirketler veya kişilere karşı saldırılar gerçekleştiren kişiler tarafından gerçekleştirilebilir. Bu tür saldırılar, bilgisayar korsanları tarafından finansal kaynakların çalınması, kişisel bilgilerin ele geçirilmesi, hizmetlerin sınırlandırılması, dış algısını etkilemek veya hatta bir ülkedeki ulusal rakipler için kullanılabilir. Siber terörizm, fiziksel terörizm gibi son derece ciddi bir tehdit olabilir ve bu nedenle uluslararası ciddiyetle ele alınması gereken bir şeydir (Ocak, 2021).

2.4.8. Siber Casusluk

Genellikle bilgisayar ağları, internet ve diğer dijital sistemler aracılığıyla bilgi toplama, izleme ve buralardaki siber altyapılarına yetkisiz erişim sağlama eylemleri “siber casusluk” olarak ifade edilir. Bu tür bir casusluk, siber yürütücüler, devlet destekli aktörler, hacker grupları veya diğer kötü niyetli aktörler tarafından gerçekleştirilebilir. Siber casusluk, ticari sırları çalmak, stratejik askeri bilgileri elde etmek, siyasi amaçlar için bilgi toplamak gibi amaçlarla gerçekleştirilebilir. Bu nedenle, siber güvenlik önlemleri, özellikle de kurumsal ve devlet merkezli, siber casusluk eylemlerine karşı önemli bir savunma sistemleridir (Ocak, 2021).

2.4.9. Siber Caydırıcılık

Bir organizasyonun siber saldırılara karşı kendini savunmak ve potansiyel saldırganları caydırmak amacıyla yürüttüğü bir dizi faaliyet “siber caydırıcılık” olarak ifade edilir. Siber güvenlik faaliyetleri, özellikle finansal kurumlar ve devlet kurumları gibi büyük ve kompleks organizasyonlar için hayati önem taşır. Çünkü siber saldırıların hem maliyeti hem de etkisi oldukça yüksektir. Siber caydırıcılık faaliyetleri, bu kurumların siber saldırılara karşı savunma kabiliyetlerini artırarak, maliyetli veri kayıplarını önleme ve itibar kaybını azaltma gibi ciddi risklerin önüne geçme konusunda önemli bir rol oynar. Siber saldırganlar, çalınacak veriler, şantaj yapacakları bilgileri veya sistemlerine zarar verecek virüsleri hedefleyerek organizasyonları hedef alabilmektedirler (Ocak, 2021).

2.5. SİBER GÜVENLİK RİSK YÖNETİMİ

Siber risk yönetimi organizasyonların güvenli bir şekilde iş yapmalarını sağlamak için, siber tehditleri tanımlayarak risklerini yönetmelerine ve bunları azaltmaya yardımcı olan bir süreçtir. Siber risk yönetimi aşağıdaki kullanımları içermektedir:

Siber Tehditlerin Değerlendirilmesi: Siber tehditlerin tanımlanması ve analiz edilmesi, risk yönetiminin temel aşamalarından biridir. Siber risk değerlendirmesi, organizasyonların karşılaşılabilecekleri tehditlerin türünü, olası saldırı senaryolarını, siber saldırıların etkisini ve bu saldırılardan finansal zararlarını tahmin etmelerine yardımcı olur. Bu değerlendirmeler, organizasyonların siber güvenlik stratejilerini oluşturmak ve kaynaklarını doğru bir şekilde tahsis etmek için kritik öneme sahip olmaktadır (www.nist.gov).

Siber Güvenlik Politikaları ve Prosedürleri: Organizasyonlar siber güvenliği sağlamak için siber güvenlik politikaları ve prosedürleri geliştirmelidir. Kurumun siber güvenlik alanındaki vizyonu ve misyonu doğrultusunda gelecek dört yıla ilişkin hedef ve politikalarının konu aldığı ve daha önceki eylem planlarından elde edilen ilerlemenin bir adım daha ileri gitmesi gerektiği ifade edilmektedir. Bu politikaların uygulanması, siber risk yönetiminde önemli bir rol oynamaktadır (Çakır ve Arınmış Uzun, 2021: 369).

Eğitim ve Farkındalık: Organizasyonların siber güvenlik farkındalığı oluşturmak ve çalışanları siber güvenlik konusunda eğitmek için düzenli eğitim programları uygulaması gerekmektedir. Eğitimler, çalışanların siber tehditleri tanımlama ve siber saldırı karşı korunma konusunda yetkin hale gelmelerine yardımcı olur. Bu sayede organizasyonlar çalışanlarının güvenlik davranışlarını iyileştirebilir ve siber riskleri en aza indirebilir (Efe, 2021: 160).

Güvenlik Denetimi ve Sürekli İzleme: Güvenlik denetimleri, organizasyonların siber güvenlik politikalarının ve prosedürlerinin uygun bir şekilde uygulanıp uygulanmadığını doğrulamak için düzenli olarak yapılması gereken bir faaliyettir. Organizasyonlar, siber saldırının tespit edilmesi için ayrıca sürekli izleme yapmalıdır. Bu izleme sayesinde organizasyonlar, saldırıları tespit edebilir, kaynaklarını doğru bir şekilde yönlendirebilir ve saldırılardan etkilenen sistemleri hızla kurtarabilir (Acar vd., 2016: 1561-1562).

Kriz yönetimi: Siber risklerin gerçekleşmesi durumunda organizasyonların hızlı ve etkili bir şekilde tepki vermesi gerekmektedir. Kriz yönetimi, organizasyonların siber saldırılara ve diğer olağandışı durumlara karşı hazırlıklı olmalarına yardımcı olur. Kriz yönetimi planları, siber risk yönetiminde kritik bir rol oynamaktadır. Bu planlar, siber saldırılara karşı acil önlemler, kriz iletişimi stratejileri ve yedekleme planlarını içermelidir (Korucu, 2021: 53).

Yönetişim, Risk ve Uyum: Yönetişim, risk ve uyum, organizasyonların siber risklerini yönetmek için birçok standart ve yönergeyi izlemesi gerekmektedir. Bu kapsamda organizasyonların ISO/ 27001 ve NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) Cybersecurity Framework gibi standartları ve siber güvenlik risk yönetimi gibi yönergeleri takip etmeleri önemsenmektedir. Bu standartlar ve yönergeler, organizasyonların bilgi güvenliği politikalarını, prosedürlerini ve uygulamalarını belirlemelerine yardımcı olmaktadır. Yönetişim, risk ve uyum, ayrıca siber risklerin yönetimi için gözetim, denetim ve raporlama süreçlerini de içermektedir (Onay, 2020: 208-211). Bu kullanımlar, organizasyonların siber riskleri yönetmelerine yardımcı olmaktadır ve siber güvenliklerini güçlendirmelerine olanak sağlamaktadır.

Siber güvenlik yönetimi, stratejik yön sağlayan, hedeflere ulaşılmasını sağlayan, riski uygun şekilde yöneten, kurumsal kaynakları sorumlu bir şekilde kullanan ve bir kurumsal güvenlik programının etkinliğini izleyen kurumsal bir stratejidir. Siber güvenlik yönetiminin birbiriyle ilişkili Şekil 2.1’de yer alan altı bileşeni vardır. Bu altı bileşen, yönetimin siber güvenlik yönetişiminin tasarımı ve çalışma etkinliğini değerlendirmek için kullanılmaktadır. Bileşenlerin herhangi birindeki bir eksiklik siber güvenliğin genel etkinliğini etkilediğinden birlikte çalışmaktadırlar. Aksi takdirde, organizasyonun siber tehditleri veya riskleri değerlendirmeye hazır olmadığı kabul edilmektedir (GTAG, 2016: 17; Güler ve Arkın, 2019:29).

Şekil. 2.1 Siber Güvenlik Risk Değerlendirme Çerçevesi



Kaynak: GTAG, 2016: 17; Güler ve Arkın, 2019:29).

1. Siber Güvenlik Yönetiřimi

İç denetim birimi, organizasyonun siber güvenlik yönetiřiminin farkında olmalıdır. 2100 numaralı IIA Standardı: İřin nitelięi, iç denetim faaliyetinin yönetiřim, risk yönetimi ve kontrol süreçlerini deęerlendirmesini ve iyileřtirmeye katkıda bulunmasını gerektirir. Yönetiřim, rollerin ve sorumlulukların açıklıęa kavuřturulmasını, hesap verebilirlięin oluřturulmasını, çok yıllık bir stratejinin benimsenmesini ve birden fazla paydařla stratejik iřbirlięini içerecek řekilde eylem planlarına öncelik verilmesini içerebilir (GTAT, 2016:17).

Güçlü siber güvenlik yönetiřimi için:

- Risk toleransını belirlemek.
- Kesinti durumunda iř süreklilięi ve felaket durumlarında kurtarma için planlamalar yapmak.
- Organizasyonu etkileyebilecek tehditlere dayalı siber güvenlik riskleri hakkında iřbirlięi yaparak veri ve bilgi toplamak.
- Siber güvenlik tehdit ve riskleri konusunda bir farkındalık kültürü oluřturmak.
- Güvenlik ihlallerine karřı anında müdahale etmek.

Etkili yönetiřim ayrıca tanımlanmıř politikalar, yeterli personel ve doęru eğitim programları ile gerçekteřtirilmektedir (GTAG, 2016:18; Güler ve Arkin, 2019:29).

2. Bilgi Varlıkları Envanteri

BT departmanı, tüm bilgi varlıklarının güncel bir envanterini tutmalı ve kurumsal hedeflere ulaşmak ve operasyonları sürdürmek için en önemli olanlara öncelik vermelidir. Bu varlıklar, stratejik kurumsal hedeflere ve giriřimlere ulaşmak için birden fazlasına ihtiyaç duyar. Geleneksel genel BT denetimleri ve periyodik incelemeler. Etkinlięin süreklilięini saęlamak için, en deęerli varlıkları korumak için tasarlanmıř önleyici ve operasyonel kontroller sürekli olarak izlenmelidir.

BT departmanı, tüm bilgi varlıklarının güncel bir envanterini tutmalı ve organizasyonun hedeflerini ilerletmek ve operasyonları sürdürmek için en önemli olanlara öncelik vermelidir. Stratejik kurumsal hedeflere ve giriřimlere ulaşmak için bu varlıklar birden fazlasına ihtiyaç duyar. Geleneksel BT genel kontrolleri ve periyodik deęerlendirmeler. En deęerli varlıkları korumak için tasarlanan önleyici ve tespit edici

kontrollerin sürekli etkinliği sağlamak için sürekli olarak izlenmesi gerekmektedir (Güler ve Arkın, 2019:30).

Organizasyonun bilgi varlıklarını değerlendirirken aşağıdakiler dikkate alınmalıdır:

➤ Veri

- Türler (ör. işlemsel, BT yapılandırması, yapılandırılmamış)
- Sınıflandırma (standartlaştırma ve önceliklendirme sağlar)
- Ortamlar (ör. veri ambarları, önemli veri tabanları)

➤ Teknoloji varlıklarının altyapı deposu

- Sunucular
- Ağ cihazları
- Depolama
- Son kullanıcı cihazları (ör. dizüstü bilgisayarlar, mobil cihazlar)

➤ Uygulamalar

➤ Dış ilişkiler

- Üçüncü taraflarca barındırılan ortamlar
- Veri dosyalarının harici kuruluşlarla paylaşılması (örneğin satıcılar, düzenleyici kurumlar, hükümetler)

Bir ağda hangi yazılımların ve cihazların etkileşime girdiğini belirleme yeteneği, siber tehditlere karşı korunmak için çok önemlidir. Bir organizasyon, bilinmeyen aygıtlar ve yazılımlar kullanılarak yapılan ağ saldırılarına karşı savunma yapamamaktadır. Çalışanların kendi cihazlarını getirmelerine izin veren organizasyonlar, kurumsal ağ üzerinden verilere erişen çok sayıda ve çeşitli cihaz ve yazılımlarla karşı karşıya kalmaktadır. Çalışan cihazlarını ve ağ bağlantısını yönetmek, üst yönetimin odak noktası olmalıdır. Gün geçtikçe daha fazla çalışanın kurumsal bilgilere 7/24 erişmesi gerekmektedir. Bilinmeyen cihazları keşfetme, doğrulama ve dökümanını çıkarma yeteneği, bir organizasyonun genel siber güvenlik stratejisinin etkili olmasını sağlamak için bu cihazlardaki değişiklikleri izlemesine, kontrol etmesine ve ölçmesine olanak tanımaktadır (GTAG, 2016: 18-19; Güler ve Arkın, 2019:30).

3. Standart Güvenlik Yapılandırmaları

Cihazlar, uygulamalar ve işletim sistemlerinde temel oluşturmak ve devam ettirmek için merkezileştirilmiş otomatik yapılandırma yönetimi yazılımı kullanılmalıdır.

Yönetim yazılımını kullanmak, sistemleri manuel olarak veya standart dışı bir şekilde yönetmekten daha verimlidir. Bilgi güvenliği ve iç denetim faaliyetleri, riske dayalı ortamın uygun şekilde değerlendirilmesini sağlamak için temelleri gözden geçirmelidir. Sektörde tehditler hakkında yeni bilgiler ortaya çıktığında, yazılım ve donanım güncellemelerinin yanı sıra korumalı yapılandırmaları güncel tutmak için gerekli yamalar uygulama süreçlerine dahil edilmelidir (GTAG, 2016: 19; Güler ve Arkın, 2019:31).

4. Bilgi Erişim Yönetimi

Yönetim, iş sorumluluklarına göre kullanıcılara erişim verme ve onaylama süreci gibi proaktif kontrolleri uygulamaya eklemeyi dikkate almalıdır. İç denetim faaliyetleri, erişim düzeylerinin mevcut roller için gerekçelendirildiğinden emin olmak için kritik verilere ve sistemlere olan kullanıcı erişimi uygulamasını gözden geçirmelidir. Bilgiye erişme ve bilgiyi yayınlama becerisine sahip kullanıcılar, siber güvenlik riskine karşı en savunmasız olanlardır. Kullanıcılar, kimlik avı girişimlerinin bir sonucu olarak parolalarını yanlışlıkla ifşa ederek veya kötü amaçlı yazılım yükleyerek, yetkisiz erişimi önlemek için tasarlanmış sistematik denetim katmanlarını atlayabilmektedir. Erişimi olan kişiler, organizasyonun içinde veya dışındadır; bu nedenle, veriler dahili veya harici olarak barındırılıyorsa, hassas verilere erişimi olan çalışanlara, danışmanlara ve tedarikçilere karşı dikkatli olunmalıdır. Erişim vermek ve iptal etmek ve ayrıcalıklı kullanıcıların gizliliğini değerlendirmek için proaktif kontrollerin gözden geçirilmesi, bir organizasyonun siber güvenlik programının etkinliğinin önemli bir göstergesidir (GTAG, 2016: 19-20; Güler ve Arkın, 2019:32).

5. Ani Cevap ve İyileştirme

Güçlü bir siber güvenlik politikasının gerçekleştirilebilmesi için olası risklerin hızlı bir şekilde tespit edilip aynı hızla cevap verilip iyileştirme süreçlerinin başlaması gerekmektedir. Herhangi bir organizasyonun, riskleri anında iletme ve iyileştirme yeteneği, programın etkinliğini ve olgunluk seviyesini göstermektedir. Etkin programlar, yönetimin yanıt verme süresini hızlandırmaktadır. Bu bileşenin rolleri:

- İyileştirmenin kabul edilmesi,
- Önemli risklerin anında bildirilmesi,
- Tespit edilen sorunların ortadan kaldırılana kadar takip edilmesi,
- Organizasyonda çözüm odaklı eğitim ve rapor verilmesidir (GTAG, 2016: 20).

6. Devam Eden İzleme Bileşeni

Siber güvenlik risk değerlendirme çerçevesinin son bileşeni olan devam eden izleme, yukarıda açıklanan beş bileşenin her birinin devam eden denetimi, riskin nasıl yönetildiği ve düzeltici eylemlerin ne kadar iyi yürütüldüğünü belirlemeye yardımcı olmaktadır. Etkili bir risk değerlendirme programı, basit bir kontrol listesinden daha fazlasını gerektirmektedir (GTAG, 2016: 20-21; Güler ve Arkın, 2019:32).

2.6. SİBER GÜVENLİK OLGUNLUK MODELİ

Günümüzde siber güvenlik gün geçtikçe daha ciddi bir sorun haline gelmektedir. Organizasyonlar, veri ihlallerine ve siber saldırılara karşı güvende kalmak için çeşitli güvenlik tedbirleri almaktadır. Ancak, bu tedbirler ve stratejiler ne kadar etkili olursa olsun, ne kadar güçlü olduğuna dair bir endişe hep vardır.

Siber güvenlik olgunluk düzeyi, önceden tanımlanmış bir siber güvenlik olgunluk modeli yardımıyla ölçülmektedir. Siber güvenlik olgunluk modeli, Tablo 2.1’de özetlenen beş olgunluk seviyesine dikkat çekmektedir. Bir organizasyonun 3. 4. veya 5. seviyelerine ulaşması için ilk olarak önceki olgunluk seviyelerinin tüm kıstaslarını karşılamış olması gerekmektedir (Güler ve Arkın, 2019: 22-23).

Siber Güvenlik Olgunluk Modeli, organizasyonların güvenlik stratejilerini geliştirmelerine ve uygulamalarını değerlendirmelerine katkı sağlayan bir araçtır. Bu model, bir organizasyonun siber güvenlik uygulamalarının olgunluk düzeyini belirlemek için kullanılmaktadır. Yine siber güvenlik olgunluk modeli, organizasyonun güvenlik uygulamalarının ne kadar iyi olduğunun değerlendirilmesine yardımcı olmaktadır. Modelin oluşturulması için, en iyi uygulamaları temel alan ve çeşitli kaynaklardan faydalanan bir yaklaşım benimsenmiştir (www.nist.gov).

Tablo 2.1’de görüldüğü gibi geliştirilen bu olgunluk modelinin amacı, siber güvenliği ele almak ve siber güvenlik risklerini yönetmek için etkili bir yaklaşım oluşturmaktır. Üye Kuruluşlar yerinde bir siber güvenlik olgunluk seviyesine erişmek için, en az 3. olgunluk seviyesinde veya üzerinde faaliyet göstermelidir (SAMA, 2017:10; Güler ve Arkın, 2019:24).

Tablo 2.1 Siber Güvenlik Olgunluk Modeli

Olgunluk Seviyesi	Tanım ve Kriterler	Açıklama
0 (Mevcut Değil)	- Herhangi bir dökümantasyon yoktur. - Bazı siber güvenlik kontrolleri için farkındalık veya dikkat yoktur.	Siber güvenlik kontrolleri yerinde değildir. Belirli bir risk alanı hakkında herhangi bir farkındalık olmayabilir veya bu siber güvenlik kontrollerini uygulamak için mevcut planlar olmayabilir.
1 (Geçici)	- Siber güvenlik kontrolleri tanımlanmamış veya kısmen tanımlanmıştır. - Siber güvenlik kontrolleri tutarsız bir şekilde gerçekleştirilmektedir. - Siber güvenlik kontrolleri tam olarak tanımlanmamıştır.	- Siber güvenlik kontrol tasarımı ve uygulaması ilgili bölüme veya kuruma göre değişir. - Siber güvenlik kontrol tasarımı, tespit edilen riski sadece kısmen azaltabilir ve uygulama tutarsız olabilir.
2 (Tekrarlanabilir ancak gayri resmi)	Siber güvenlik kontrolünün yürütülmesi, standartlaştırılmış olsa da, gayri resmi ve yazılı olmayan bir uygulamaya dayanmaktadır.	- Tekrarlanabilir siber güvenlik kontrolleri yerindedir. Bununla birlikte, kontrol hedefleri ve tasarımı resmi olarak tanımlanmamış veya onaylanmamıştır. - Yapılandırılmış bir gözden geçirme veya kontrolün test edilmesi konusunda sınırlı bir değerlendirme vardır
3 (Yapısal ve resmileştirilmiş)	- Siber güvenlik kontrolleri, yapılandırılmış ve resmileştirilmiş bir şekilde tanımlanır, onaylanır ve uygulanır. - Siber güvenlik kontrollerinin uygulanması gösterilebilir.	- Siber güvenlik politikaları, standartları ve prosedürleri oluşturulmuştur. - Siber güvenlik belgelerine uyum, yani politikalar, standartlar ve prosedürler, tercihen bir yönetim, risk ve uyum (GRC)3 aracı kullanılarak izlenir. - Uygulamanın değerlendirilmesi için kilit performans göstergeleri tanımlanır, izlenir ve raporlanır
4 (Yönetilebilir ve ölçülebilir)	- Siber güvenlik kontrollerinin etkinliği periyodik olarak değerlendirilir ve gerektiğinde geliştirilir (iyileştirilir). - Bu periyodik ölçüm, değerlendirmeler ve iyileştirme fırsatları belgelenmiştir.	- Siber güvenlik kontrollerinin etkinliği ölçülmekte ve periyodik olarak değerlendirilmektedir. - Siber güvenlik kontrollerinin etkinliğini belirlemek için temel risk göstergeleri ve trend raporlaması kullanılmaktadır. - Ölçme ve değerlendirme sonuçları, siber güvenlik kontrollerinin iyileştirilmesine yönelik fırsatları belirlemek için kullanılır.
5 (Uyarlanabilir)	Siber güvenlik kontrolleri sürekli bir iyileştirme planına tabidir.	- Kurumsal çapta siber güvenlik programı, siber güvenlik kontrollerinin sürekli uyumu, etkinliği ve iyileştirilmesine odaklanmaktadır. - Siber güvenlik kontrolleri, kurumsal risk yönetimi çerçevesi ve uygulamaları ile entegredir. - Siber güvenlik kontrollerinin performansı, emsal ve sektör verileri kullanılarak değerlendirilir.

Kaynak: (SAMA, 2017:10; Güler ve Arkin, 2019:23)

2.7. SİBER GÜVENLİK STANDARTLARI

Siber güvenlik standartları, siber güvenliği sağlamak için belirli bir seviyede güvenlik ve korumayı gerektiren kurallar, prosedürler ve korumalardır. Siber güvenlik standartları, bir organizasyonun bilgi yapısının altyapısını korumak ve siber saldırılardan korumak için uygulanan önlemlerdir.

Pek çok farklı siber güvenlik standardı mevcuttur ve bunlar genellikle endüstri standartları olarak adlandırılır. ISO 27001 genel olarak en sık karşılaşılan bilgi güvenlik yönetim sistemleri için bir standart olarak kabul edilmektedir.

ISO 27001, Bilgi Güvenliği Yönetim Sistemi (BGYS) için uluslararası bir standarttır. Bu standart, bir organizasyon bilgi varlıklarının (örneğin, müşteri verileri, finansal bilgiler, çalışan verileri) gizliliğini, verilerini ve erişilebilirliğini korumak için gerekli olan en iyi uygulamaları belirlemektedir. ISO 27001, bir organizasyonun bilgi güvenliği yönetim sistemi kurmasını ve çalışmasını sağlamaktadır. Bu sistemi oluşturmak için, bir organizasyon risk analizi yapılmalı, güvenlik kontrolleri belirlemeli ve uygulanmalıdır. ISO 27001 ayrıca, bir organizasyonun iş sürekliliği yönetimini de kapsayan bir standarttır.

Bu standart, birçok farklı sektördeki organizasyonlar için uygulanabilir olup, küçük ve büyük yoldan tüm organizasyonlar tarafından kullanılabilir. ISO 27001 sertifikası, bir organizasyonun bilgi güvenliği yönetim sisteminin gerçekleştirmeye uygunluğunu doğrulayan bağımsız bir sertifikadır.

Siber güvenlik standartları, cihazlar için rehber niteliğinde olup, uygulamalarının siber güvenliği nasıl iyileştirebileceği konusunda yol gösterici olmaktadır. Bunun yanı sıra, bir yapının herhangi bir siber zarar görmesi durumunda, uygun siber güvenlik standartlarının uygulanmamış olması, hukuki ve maddi yükleri de beraberinde getirecektir (Bozgeyik, 2018: 60-65)

2.8. SİBER GÜVENLİK AÇISINDAN DENETİM SÜREÇLERİ

Siber güvenlik denetimleri, bir organizasyonun siber güvenliğiyle ilgili sorunları tespit etmek ve incelemek için yapılan bir uygulamadır. Bu denetimler, bilgisayar ağları, sunucular, yazılımlar ve diğer bilişim sistemleri gibi siber denetimleri elde etmek için yapılmaktadır. Siber güvenlik denetimleri, bir örgütün siber saldırılara karşı korunmasını sağlamak için kritik bir öneme sahiptir.

Siber güvenlik denetimleri, organizasyonun siber güvenlik açısından eksiklikleri ve zayıflıkları tespit etmek amacıyla yapılan bir dizi işlemi içermektedir. Bu işlemler, organizasyon bilişim sistemleri ve ağlarının güvenliği için yapılan araştırma ve analizleri kullanmaktadırlar.

Bilgi Sistemleri Denetimi ve Kontrol Kurumu (ISACA) tarafından yayınlanan raporda siber güvenlik denetimlerinin kapsamı aşağıdaki gibi olmalıdır:

- Şebeke, veritabanı ve uygulamalara dair veri güvenliği politikaları,
- Veri kaybına karşı alınan önlemler,
- Uygulanan etkili ağ erişim denetimleri,
- Dağıtılan algılama / önleme sistemleri,
- Güvenlik kontrolleri (fiziksel ve mantıksal),
- Olaylara müdahale programlarıdır.

Siber güvenlik denetim ve kontrolleri konuları aşağıdaki bilgileri barındırmalıdır:

- Hassas verilerin ve fikri mülkiyet haklarının korunması,
- Çoklu bilgi kaynağının bağlı olduğu ağların korunması,
- Cihazların ve bu cihazların içerdiği verilerin sorumluluğu ve hesap verebilirliğidir.
- Fiziksel ve çevresel güvenlik,
- Hesapların ve şifrelerin yönetimi,
- Hassas verilerin gizliliği,
- İşletme sürekliliği yönetimi,
- Güvenlik konusunda bilinçlilik ve eğitim,
- Vaka yönetimi,
- Erişim kontrolleri,
- Varlık yönetimi,
- Değişim yönetimi,
- Uygunluk,
- Gizlilik ilkeleri,
- Sistemler ve verilerin korunması,
- Sigorta işlemleridir.

Siber güvenlik denetimleri, genellikle siber güvenlik açısından yüksek risk taşıyan organizasyonlar için gereklidir. Bu organizasyonlar, finansal kuruluşlar, devlet kurumları, sağlık hizmetleri ve büyük işletmeler gibi çeşitli amaçlara yönelik faaliyet gösterenleri içermektedir. Siber güvenlik denetimleri, bir örgütün siber saldırılara karşı korumalarını ve olası güvenlik tehditlerini önleme için gerekli önlemleri almalarını sağlamaktadır.

Siber güvenlik denetimleri, iki ana türde olabilir. Bunlar iç denetim ve dış denetim. İç denetim, organizasyonun kendi personeli tarafından yapılırken, dış denetim, üçüncü taraf bir denetim şirketi tarafından yapılır. Dış denetimler, organizasyona siber güvenlik hakkında bir bakış açısı sağlar ve organizasyonun siber güvenlik konusundaki muhafazasını bir üçüncü taraf bakış açısı sunmaktadır.

Siber güvenlik denetimleri, organizasyon bilişim sistemleri ve ağlarının elde edilmesini sağlamak için önemli bir araçtır. Bu denetimler, organizasyonun siber izinlerini geliştirme ve güvenliğe yönelik olası riskleri azaltmak için gerekli tedbirlerin alınmasına yardımcı olmaktadır. Siber güvenlik denetimlerinin düzenli olarak yapılması, bir organizasyonun siber güvenlik açısından etkin bir şekilde yol almasını sağlamaktadır (Öztürk 2018: 216-222).

2.9. SİBER GÜVENLİKTE İÇ DENETİMİN ROLÜ

Organizasyonların dahil olduğu dijital dönüşüm sürecinde, üst yönetimin aklındaki en önemli risklerden biri siber güvenlidir. İç denetçilerin siber güvenlik risklerine karşı güvence ve danışmanlık hizmetini etkin bir şekilde sağlamak ve organizasyonun katma değerini arttırmak için bu alandaki teknik bilgi ve deneyimlerini sürekli iyileştirmeleri gerekmektedir.

Günümüzde siber güvenlik risklerinin boyutları ve etkisi devamlı değişmektedir. Çünkü siber güvenliğe yönelik saldırılar, bireysel eylemlerin ötesine geçerek organize eylemler haline gelmektedir. Saldırıların şiddeti sadece maddi kayıplara neden olmakla kalmaz, organizasyonların itibarını ve sürekliliğini de etkilemektedir. Yeni nesil teknolojilerin gelişmesi siber güvenlik açısından yeni çözümler getirdiği gibi yeni riskleri de beraberinde getirmektedir.

Siber alandaki büyük kayıplar göz önüne alındığında, organizasyonların siber saldırılara karşı daha savunmasız hale geldiği veya saldırıların erken tespit edilememesi, güvenlik açıklarının ve boşlukların zamanında kapatılmaması nedeniyle önemli yatırımlara rağmen organizasyonların bu teknolojileri etkin bir şekilde kullanmadığı zamanlar vardır. Bu gibi durumlarda iç denetim fonksiyonunun odaklanması gereken ana alanlar şu şekilde sıralanabilir:

➤ Yönetişim

Organizasyonların siber risklere karşı dayanıklı hale gelebilmesi için önceliklerinden biri de üst yönetim seviyesinde siber güvenlik farkındalığı yaratmaktır.

İşte her iş biriminin kurumsal siber güvenlik risklerine karşı dayanıklı olması için atması gereken adımlar. Üst yönetim düzeyinde iç denetim tarafından değerlendirilmesi gereken siber güvenlikle ilgili konular aşağıdaki gibi özetlenebilir.

- Üst yönetici için, kurumun amaç ve hedefleri ile stratejik planlarının siber güvenlik açısından değerlendirilmesi,
- Kurumun mevcut hizmet sunumu ve operasyon modelinin içerisine siber güvenlik katmanının entegre edilmesi,
- Siber güvenlik açısından kurumun mevcut mevzuat ve prosedürlerinin gözden geçirilmesi,
- Olası siber güvenlik zararları ve kayıplara karşı yeterli sigorta ve güvence planlamalarının gerçekleştirilmesi,
- Mevcut teknolojinin gelişen siber güvenlik saldırılarına karşı ne kadar etkin olduğunun sürekli olarak izlenmesi ve değerlendirilmesi,
- Dijital dönüşüm sürecinin getirdiği risklerin siber güvenlik gözüyle değerlendirilmesi, • Siber güvenliğin, üçlü savunma mekanizması ile nasıl entegre edileceğinin değerlendirilmesi,
- İç denetimin siber güvenliğe yönelik odaklanmasının planlanması,
- Siber güvenlik ile ilgili teknoloji yatırımının yanında insan kaynağı yatırımının da gerçekleştirilmesi,
- Siber güvenliğe yönelik organizasyon seviyesinde farkındalığın oluşturulması.

Üst yönetimin yukarıdaki sorulara doğru cevaplar verebilmesi ve etkin şekilde aksiyon alabilmesi için ilk etapta yapması gerekenler ise;

- Siber güvenliğe ilişkin risk toleransının belirlenmesi ve onaylaması,
- Siber risklerin ölçülmesi ve değerlendirilmesi,
- Siber risklere yönelik daha şeffaf ve dinamik bir raporlama yapısının tesis edilmesi,
- Üst yönetim seviyesinde, siber güvenliğe ilişkin yetkilendirme ve görevlendirmelerin gerçekleştirilmesi,
- Kurum siber güvenliğe yönelik farkındalığın artırılmasına destek verilmesi olarak belirtilebilir.

➤ **Temel Kontrol Aktiviteleri**

Siber saldırılara karşı güvende kalma adına kurumlarda uygulanan ve iç denetimin değerlendireceği temel kontrol aktiviteleri aşağıdaki gibidir:

- Bilgi teknolojileri genel kontrolleri ile mevcut sistemlerin verinin gizlilik, tamlık ve doğruluk açısından mevcut mevzuat ve prosedürler ile uyumlu olup olmadığının değerlendirilmesi,
- Erişim ve yetkilerin yönetimi ile yönetici yetkileri dâhil olmak üzere tüm yetkilerin izlenebilmesi, erişime ilişkin şifre ve diğer gerekliliklerin güncel ihtiyaçlara göre sürekli gözden geçirilmesi,
- İzleme ile mevcut sistemlerin, yetkisiz erişim ve diğer boyutları ile sürekli olarak izlenebilmesi,
- Dijital varlık yönetimi mekanizmalarının geliştirilmesi,
- Kişisel verilerin korunması kapsamında gerekli yasal ve uygulama bazlı kontrollerin ve işlemlerin gerçekleştirilmesi.

➤ **Üçüncü Taraf Risk Yönetimi**

Organizasyonların hizmet aldığı üçüncü taraf hizmet sağlayıcıların siber güvenlik riskleri açısından zafiyetleri çoğu zaman organizasyonlar için önemli risk alanları arasında yer almaktadır. Çünkü bu tür üçüncü taraf hizmet sağlayıcılarla veri paylaşımı ve sistem entegrasyonu gerektirmektedir. Bu nedenle bir organizasyon içinde alt yüklenici, hizmet sağlayıcı, taşıyon veya yüklenici olarak çalışan tüm tarafların, kurumun siber güvenlik süreçleriyle uyumlu bir kontrol ortamına sahip olması gerekir.

Bu açıdan değerlendirildiğinde, üst yönetim ve iç denetim için öncelikli sorular aşağıdaki gibi sıralanabilir:

- Organizasyon, hizmet sunumu veya mevcut operasyonları içerisinde yer alan tüm üçüncü taraf hizmet sunucularına ilişkin bir envantere sahip midir?
- Üçüncü taraf hizmet sağlayıcılar ile paylaşılmış ve siber güvenlik risklerine karşı alınacak aksiyon ve beklentileri içeren açık ve net bir prosedür bulunmakta mıdır?
- Üst yönetim ve organizasyon üçüncü taraf hizmet sağlayıcılarından kaynaklı olarak oluşabilecek risklerin farkında mıdır? Bu riskler etkin şekilde ölçülmekte ve izlenmekte midir?

➤ **Sürdürülebilirlik**

İş sürdürülebilirliği, günlük operasyonlardan siber güvenlik riskleriyle ilgili kurumsal önceliklere kadar birçok alanda kritik öneme sahiptir. Direnç, hizmet sunumunda hedeflenen bir düzeyi sürdürmek veya değişen koşullara ve saldırılara çok hızlı yanıt vererek bu düzeye mümkün olan en kısa sürede ulaşmak olarak ifade edilebilir.

Faaliyetlerin sürdürülebilirliği için yönetim ve iç denetim tarafından göz önünde bulundurulması gereken öncelikli hususlar şu şekilde özetlenebilir:

- Siber güvenlik gözüyle sürdürülebilirliği etkileyebilecek alanların yönetimi ve zafiyetlerin ortadan kaldırılmasına yönelik sürekli iyileştirme çalışmaları,
- Sürdürülebilirlik risklerinin etkin şekilde izlenmesi ve değerlendirilmesi,
- Sistemlere yönelik sürdürülebilirlik risklerinin tespit edilmesi ve bilgi teknolojileri mimarisinin bu açıdan incelenmesi,
- Üçüncü taraf ve diğer bağımlılıkların siber güvenlik gözüyle değerlendirilmesi,
- Saldırıların tespit edilmesi ve sürekli raporlanması,
- Sistemlerin geri dönüş planlamalarının sürekli olarak test edilmesi.

➤ **Siber Risk Yönetimine Yönelik Bakış Açısının Günümüz İhtiyaçlarına Göre Gözden Geçirilmesi**

Sürekli gelişen ve karmaşılaşan siber güvenlik risklerine karşı organizasyonlarda yeni bir bakış açısının geliştirilmesi gerekmektedir. Yeni bakış açısının temel bileşenleri aşağıdaki gibi özetlenebilir:

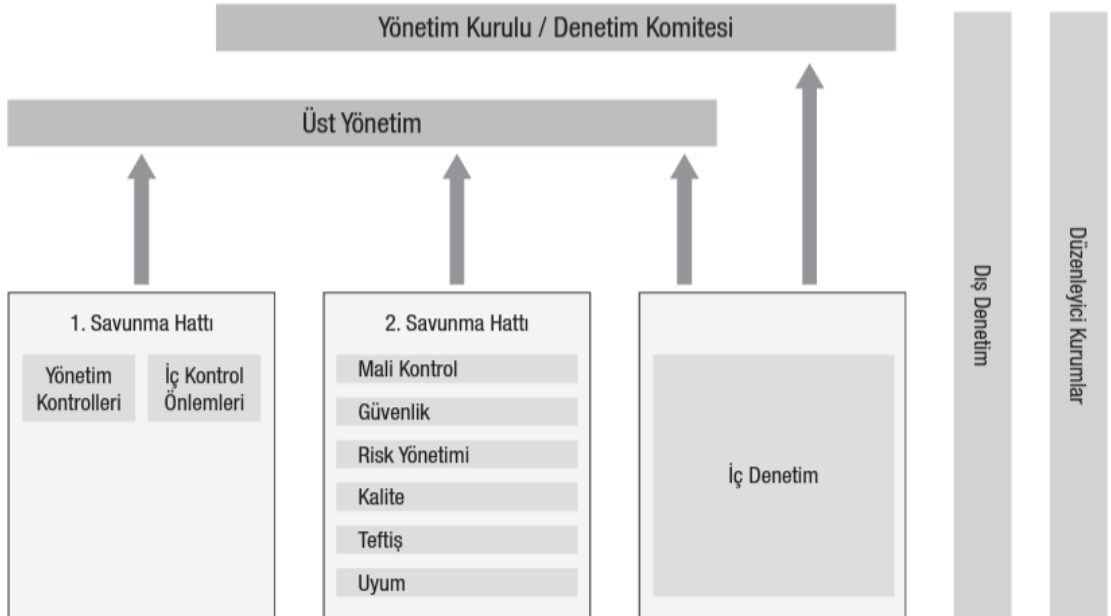
- Siber güvenlik risklerinin ve bu risklere ilişkin kontrol faaliyetlerinin statik olarak ve organizasyonun operasyonundan ayrı bir yapı ile izlendiği ve uygulandığı bir yaklaşımdan ziyade siber güvenlik risklerini organizasyonun yönetişimi içerisinde değerlendirmek ve siber güvenlik risklerinin organizasyonun operasyon modeline ve hizmet sunumuna etkilerini bir bütün olarak ele almak gerekmektedir.
- Siber güvenlikte odağın mevzuata uyumun ötesinde, yönetişim ve uygulamaya kaydırılması gerekmektedir.
- Siber güvenliğe ilişkin risklerin birbirinden kopuk ve çoğu zaman mükerrer kontroller gerçekleştiren yapılar yerine, ortak hizmet merkezi olarak çalışan siber güvenlik operasyonları merkezi tarzında yapılar ile yönetilmesi gerekmektedir.
- Mevcut durumda organizasyonların maruz kaldıkları siber saldırılara ilişkin aksiyonlar alınırken, küresel eğilimler ve değişen saldırı yöntemleri sürekli izlenerek

gelecekte organizasyonların siber saldırılara dayanıklı olmalarını sağlayacak aksiyonlar da ihmal edilmemelidir (Akmeşe, 2020).

2.10. ÜÇLÜ SAVUNMA HATTI MODELİ

Organizasyonlarda operasyonel faaliyet ve risklerin daha etkin, etkili ve ekonomik çerçevede yönetilmesi için üçlü hat modeli uygulanmaktadır. Bu model, organizasyon içindeki tüm departmanların ve kademelerin verimli ve uyumlu çalışmasını sağlamak için üç ana hat üzerinden kontrol ve koordinasyon görevini yerine getirirken entegre çalışmayı esas alan bir modeldir.

Ortaya çıkışının nedeninin spor ve ordu olduğu yönünde görüşlere sahip olan 3'lü Savunma Hattı, organizasyonların hedeflerine ulaşmada karşılaştıkları riskleri etkin bir şekilde yönetmeye ve operasyonel verimliliği artırmaya yardımcı olması açısından son yıllarda popüler hale gelmiştir. Üçlü savunma hattı, uygulandığı organizasyonda görev, sorumluluk ve yetkilerin çalışan/bölüm/hat bazında açık ve net bir şekilde tanımlayarak ve faaliyetlerin verimli ve etkin bir şekilde yürütülmesi için koordinasyon sağlayarak risk yönetimi ve kontrolüne önemli katkı sağlamaktadır. Model, kurumsal yönetim sisteminde ve değer yaratmada mutlak rol oynamaktadır (Hasanefendioğlu, 2020; bulenthasanefendioğlu.blogspot.com).



Şekil 2.2. Üçlü Savunma Hattı Modeli

Kaynak: www.icas.com

Çeşitli uluslararası özel ve kamu kurumları tarafından benimsenen ve risk yönetimi ve kontrolünde önemli bir yere sahip olan "Üçlü Savunma Hattı" modeli, IAA tarafından geliştirilmiştir. Bu model, kurum içinde oluşturulan üç savunma hattı ile birlikte üst yönetim kademesi ve dış denetim ve düzenleyici kurumlardan oluşan bir yapıya sahiptir. Şekil 2.2.'de gösterilen bu model, kurumların risk yönetimi ve kontrol süreçlerinde etkili bir araç olarak kullanılmaktadır.

2.10.1. Birinci Hat Modeli

Siber güvenlik birinci hat modeli, bir organizasyonun bilgilerini korumak için kullandığı ilk savunma hattını ifade eder. Bu model, yönetim kontrollerinden meydana gelmektedir. Birinci hat modeli, temel olarak ağ koruması, kullanıcı hesapları ve kimlik doğrulama, saldırı sınırlaması ve engelleme, zararlı yazılımların etkileri, ağ yönetiminin denetimi gibi konuları kapsar. Bu model, ayrıca ağa bağlı cihazların ve yazılımlarının güncel bilgilerini, zayıf noktalarının tespit edilmesini de içermektedir.

Birinci hat modeli, bir organizasyonun siber güvenlik stratejisinin en temel ayağıdır. Bu modelin doğru bir şekilde muhafaza edilmesi ve uygulanması siber saldırılara karşı daha iyi korumayı sağlar ve muhtemel güvenliklerinin erken tespit altına alınmasına yardımcı olmaktadır.

2.10.2. İkinci Hat Modeli

"Siber Güvenlik İkinci Hat Modeli" genellikle, bir organizasyonun finansal kontrol, kalite yönetimi ve risk yönetimi gibi güvenlik fonksiyonlarından meydana gelmektedir. İkinci Hat Modeli, bir organizasyonun güvenlik sisteminde ikinci savunma hattıdır ve birinci hat (ilk savunma hattı) olarak yönetici temel güvenlik önlemlerine ek olarak kullanılır. Bu model, birinci hat savunma önlemlerinin aşıldığı veya atlatıldığı başlıca organizasyonların savunmasını yürütmek için tasarlanmıştır.

Bu model, ikinci savunma hattı olarak hareket eden bir grup veya ekip tarafından yürütülmektedir. Bu ekip, birinci savunma hattının (örneğin, güvenlik duvarları, antivirüs yazılımları, spam filtreleri vb.) zayıf yönlerine müdahale etmektedir. İkinci Hat Modeli, siber saldırılara karşı daha etkili bir koruma sağlamak için, siber güvenlik ekiplerinin etkili bir şekilde çalışmasını gerektirir. Bu model, siber saldırıların özelliklerini, tespit edilmesini, müdahale edilmesini ve raporlanmasını içerir.

2.10.3. Üçüncü Hat Modeli

Üçüncü savunma hattı olarak iç denetim faaliyeti üst yönetime ve yönetim kuruluna yönetişim, risk yönetimi ve kontroller konusunda bağımsız ve objektif bir güvence sağlar. Bu, siber güvenlik risklerini ve tehditlerini yönetme ve azaltmada birinci ve ikinci savunma hattının gerçekleştirdiği faaliyetlerin genel etkinliğinin değerlendirilmesini içerir. İç denetim faaliyeti aşağıdaki konularla ilgili danışmanlık yapabilir:

Siber güvenlikte üçüncü hat modeli, iç denetim faaliyetleri sonucu üst yönetime güvence sağlamaktadır. Bu hat, birinci ve ikinci hat modelinin etkinliğinin yeterince sağlanıp sağlanmadığının raporunu oluşturmaktadır. İç denetimin buradaki rolü danışmanlık sağlamasıdır.

İç denetim, bir organizasyonun siber güvenlik politikaları, denetimleri ve kontrolleri ile uyumunu değerlendiren ve zayıflıklarını ve eksikliklerini tespit eden bir danışmanlık faaliyetidir. İç denetim ayrıca, siber güvenlik politikalarının, yönetiminin ve kontrollerinin etkili değerlendirmesini sunmaktadır.

İç denetim aynı zamanda, siber saldırılara karşı bir organizasyonun direnişini artırmak siber güvenlik kontrolleri gerçekleştirmektedir. Bu, kontrollerin doğru şekilde yapıldığını, güncel olduğunu ve uygun bir şekilde yapıldığını ispatlamalıdır. Ayrıca, iç denetim, bir organizasyonun siber güvenlik politikalarının doğru bir şekilde yürütüldüğü konusunda emin olmak için üstlenmiş olduğu sorumluluğundan ötürü düzenli olarak denetimler yapmaktadır (Selimoğlu ve Altunel, 2019: 11-12).

3. BÖLÜM: İÇ DENETİMİN SİBER GÜVENLİKTEKİ ETKİNLİĞİ ÜZERİNE ETKİSİ: İÇ DENETÇİLERİN ALGILARI UYGULAMASI

İç denetim, organizasyonların siber güvenlik politikalarını ve prosedürlerini değerlendirmekte, güvenlik kontrollerinin etkinliğini gözden geçirmekte ve siber riskleri tanımlamak için önleyici ve tespit edici önlemler almaktadır. Ayrıca, iç denetim, siber saldırılara karşı koruma mekanizmalarının düzgün çalıştığından emin olmak için kontrolleri test etmekte ve zayıf noktaları belirlemektedir. Siber güvenlik, iç denetimin tespit ettiği riskleri ele almakta, uygun güvenlik önlemlerini uygulamakta ve siber saldırılara karşı korumayı sağlamaktadır.

Bu şekilde, iç denetim ve siber güvenlik birlikte çalışarak organizasyonun bilgi varlıklarını korur, siber riskleri yönetir ve uygun güvenlik önlemlerini hayata geçirir. İç denetim, siber güvenlik süreçlerini değerlendirirken, siber güvenlik ise iç denetimin risk değerlendirmelerine dayanarak organizasyonun siber saldırılara karşı direncini artırır. Bu işbirliği, organizasyonun siber güvenlik açıklarını tespit etme, düzeltme ve gelecekteki tehditlere karşı savunma yeteneklerini güçlendirme konusunda önemli bir rol oynar. Bu bölümde iç denetim ve siber güvenlik arasındaki ilişki ve önemin üniversitelerdeki iç denetçiler açısından ölçülmesine yönelik yapılan araştırma sonuçları yer almaktadır.

3.1. ARAŞTIRMANIN AMACI

İç denetim ve siber güvenlik birlikte çalışarak, organizasyonların siber risk yönetimini daha etkin bir şekilde gerçekleştirmelerine yardımcı olurlar. İç denetim, organizasyonun siber güvenlik stratejilerini gözden geçirir ve güvenlik kontrollerinin etkinliğini değerlendirir. Siber güvenlik ise, iç denetimin risk analizlerini ve önerilerini dikkate alarak uygun güvenlik önlemlerini uygular. Bu işbirliği, organizasyonların siber saldırılara karşı daha güçlü bir savunma yapabilmesini sağlar ve siber güvenlik risklerini azaltmada etkili olur.

Bu araştırmanın temel amacı, üniversitelerdeki iç denetim süreçlerinin, iç denetçilerin algısı açısından siber güvenlikteki etkinliklerinin ölçülmesidir. Bu çalışmanın alt amaçları ise, üniversitelerde iç denetimin nasıl gerçekleştirildiğinin ve siber risklerle nasıl başa çıkıldığının belirlenmesidir.

3.2. ARAŞTIRMANIN ÖNEMİ

Organizasyonlar için, siber güvenlik uygulamaları fiziksel güvenlik kadar önemlidir. Bilgi güvenliği ve siber güvenliğin işletmelerde uyumlu bir şekilde sağlanması, işletmelerin öncelikli odak noktası olmalıdır. Bu durum dijital çağın en önemli gerekliliklerinden biridir. Teknoloji ve dijitalleşme ile birlikte iş süreçlerinde, organizasyon faaliyetlerinde ve kontrol ortamlarında, varlıkların her türlü zarar ve saldırı risklerine karşı korunması için iç denetçilere büyük görevler düşmektedir. İç denetçiler, bu risklere karşı alınacak tedbirlerin planlanması, uygulanması ve süreçlerde yeniden yapılanmanın bir parçası olarak önemli bir rol üstlenmektedir. Organizasyonların siber güvenlik faaliyetleri, yönetiminin sorumluluğundadır ve bu faaliyetlerin yürütülmesinde en büyük destekçi iç denetim birimleridir.

Üniversitelerde iç denetim ve siber güvenlik, önemli bir alan olarak kabul edilmektedir. Çünkü üniversiteler, birçok hassas veriyi depolayan, bilimsel araştırmalar yapan ve geniş bir bilgi ağına sahip kurumlardır. Bu nedenle, iç denetim ve siber güvenlik, üniversitelerin işleyişi ve varlıklarının korunması açısından büyük önem taşımaktadır.

İç denetim, üniversitelerde yönetim süreçlerinin değerlendirilmesi, iç kontrollerin etkinliğinin değerlendirilmesi ve yasal uyumluluk kontrollerinin gerçekleştirilmesi gibi görevleri yerine getirmektedir. Üniversitelerde iç denetim, risk yönetimi ve iş süreçlerinin iyileştirilmesine odaklanırken, aynı zamanda siber güvenlik konularında da rol oynamaları gerekmektedir. İç denetim birimleri, üniversitelerin bilgi sistemlerinin güvenliğini ve siber risk yönetimini değerlendirmeli, uygun güvenlik kontrollerini önerir ve mevcut politika ve yönetmeliklere uyumu denetlemelidir.

Siber güvenlik ise üniversitelerin dijital varlıklarını, bilgi sistemlerini ve verilerini korumak için gerekli önlemleri almayı içermektedir. Üniversiteler, öğrenci ve personel bilgileri, araştırma sonuçları, mali bilgiler ve diğer önemli verileri içeren bir dizi hassas bilgiye sahiptir. Bu bilgilerin güvenliğini sağlamak, siber saldırılara karşı koruma önlemleri almak ve veri güvenliği politikalarını uygulamak, üniversitelerin sorumluluğundadır.

Üniversitelerde iç denetim ve siber güvenlik arasındaki işbirliği siber risklerin belirlenmesi, etkin güvenlik kontrollerinin uygulanması ve uyumluluk sağlanması konularında önemli bir rol oynamaktadır. Bu işbirliği üniversitelerin siber saldırılara karşı

daha güçlü bir savunma yapmasını sağlamakta ve bilgi varlıklarının güvenliğini sağlamada etkili bir yöntem olarak kabul edilmektedir.

Bu bağlamda üniversitelerde görev yapmakta olan iç denetçilerin, iç denetim sürecinde siber güvenlik uygulamalarının etkinliğinin ölçülmesi amaçlanan araştırmanın anakütlesinin Türkiye’de faaliyet gösteren devlet ve vakıf üniversitelerinden oluşması araştırma sonuçları açısından önem arz etmektedir. Ayrıca, üniversitelerde görev yapmakta olan iç denetçi özellikleri ile iç denetim algıları arasında benzer ve farklı noktalar bu araştırma kapsamında tespit edilerek literatüre katkıda bulunmak çalışmanın bir diğer önemli noktasıdır. Aynı zamanda üniversitelerde iç denetimin mevcut durumunun belirlenmesi ve iç denetim ve siber güvenlik konularındaki eksiklerin tespit edilmesi de çalışmanın önemini oluşturmaktadır.

3.3. LİTERATÜR TARAMASI

İç denetim ve siber güvenlik alanında yapılan araştırmalar ve araştırma sonuçları bu bölümde kısaca özetlenmiştir.

Gönen ve Çelik (2005) çalışmasında, iç denetim ve insan kaynakları fonksiyonları arasındaki stratejik ortaklığın bir işletmenin rekabet avantajı üzerindeki etkisini incelemiştir. Gelişen rekabet ortamı, yönetimi denetimle desteklemenin önemini beraberinde getirdiği için iç denetim ve insan kaynakları ortaklığının toplumsal yaşamda önemli bir yer işgal eden işletmelere rekabet avantajı sağladığını tespit etmişlerdir.

Demirbaş (2005), iç denetimin kapsamı gereği ‘güvence ve danışma’ faaliyeti sağlar ifadelerinin iç denetimin değerlendirme fonksiyonunu genişletmekte ve aynı zamanda risk yönetimi ve idareyle iletişim kavramlarının birlikte anılmasını sağladığına vurgu yapmıştır.

Abdioğlu (2007) çalışmasında, İMKB-100 endeksinde yer alan şirketlerde kurumsal yönetimde iç denetimin rolü üzerine bir çalışma yapmıştır. Bu çalışmanın sonuçlarına dayalı olarak, iç denetimin kurumsal yönetim yaklaşımının uygulanmasında olumlu ve önemli bir rol oynadığı tespit edilmiştir.

Memiş (2007) yaptığı çalışmada Türkiye’deki iç denetim profilinin belirlenmesi adı küresel örneklerle tespitler yaparak yerel temelde kıyaslamalar yapmıştır.

Uzay ve Tanç (2008) yaptıkları çalışmada Türkiye’de iç denetimin tarihsel gelişiminden ve artan öneminden bahsetmişlerdir.

Ceyhan (2010), işletmelerde iç kontrol ve iç denetim sisteminin, şirket kurumsallaşmasına yaptığı katkıyı araştırmaya çalışmıştır. Araştırma sonuçlarına göre iç denetim faaliyetlerinin, şirket faaliyetlerinin sürdürülebilir kıldığı, şirket kaynaklarının verimli ve etkin kullanılmasını sağladığı, kurumsal yönetim anlayışının benimsenmesinde, şirketlerin amaçlarına ulaşmasını kolaylaştırmada etkin bir rol oynadığı tespit edilmiştir. Böylece iç denetim faaliyeti, şirketlerin performanslarını istikrarlı bir şekilde artırmaları ve başarısız duruma düşmemeleri için önemli bir araç niteliği kazanmaktadır. İç denetim faaliyeti ayrıca risk yönetimi ve kurumsal yönetim gibi konularda şirketlere güvence sağlamada ve sorunları önlemede yönetim kurullarına yardımcı olmaktadır.

Aslan (2010), iç denetimin organizasyonların sürdürülebilirliğini ve amaçlarına ulaşmasını sağlama yolunda gereksinim duydukları temel unsur haline geldiğini tespit etmiştir. Bu yüzden iç denetimin günümüzde, uluslararası standartlara uygun olarak yürütülen bir yönetim disiplini haline geldiğini vurgulamıştır.

Tosunoğlu (2010), işletmelerde denetim fonksiyonunun mevcut yapısının tespitine ve mevcut durumun şekillenmesinde etkili olan faktörlerin belirlenmesine yönelik olan bu tezinde, işletmelerin kuruluş yılı, faaliyet alanı ve çalışan sayıları gibi yapısal değişiklikleri de kapsayan yapılandırılmış bir anket çalışmasıyla yürütülmüştür. Çalışma sonuçlarına göre, iç denetim biriminin organizasyondaki yönetim fonksiyonlarından biri olan planlamanın düzenli bir şekilde uygulanmasında oldukça önemlidir. Ayrıca iç denetim fonksiyonunun kurumdaki operasyon ve faaliyetleri iyileştirdiği ve işletmeye katma değer sağladığı ortaya çıkmıştır. Aynı zamanda organizasyonun hedeflerine ulaşmalarını engelleyecek tehdit ve zayıflıkların veya hedeflerine ulaşmalarını sağlayacak fırsatların tespit edilmesi yine iç denetimin risk değerlendirmesi ile sağlanacağı tespit edilmiştir.

Akyel (2010) yönetim temelinde iç denetim ve dış denetim etkinliklerinin birbirleriyle ilişkilerini açıklamıştır. Sonuç olarak tüm denetim kontrollerinin birbirleriyle uyumlu hale getirecek çeşitli adımların atılması gerektiğini vurgulamıştır.

Bezirci ve Karasioğlu (2011) bu çalışmada bağımsız denetimler temelinde atılan adımların Türkiye tarafını özetlemişlerdir. Yapılabilecek denetimlerle beraber hırsızlığın, yolsuzluğun ve muhasebe temelli düzensizliğin büyük ölçüde ortadan kaldırılabileceğini vurgulamışlardır.

Çevikbaş (2011) çalışmasında Türkiye’de iç denetim temelinde atılan yasal düzenlemelerin olmasına karşın gelecekte ortaya çıkabilecek denetim sorunlarını ortadan kaldırmak için geleceğe yönelik adımların atılmasını belirtmiştir.

Cengiz (2013) çalışmasında, işletmelerin kurumsal yönetişimi çerçevesinde iç denetimin yerini ve önemini belirlemeyi amaçlamıştır. Bu amaç kapsamında ayrıca kurumsal yönetim ve iç denetim ilişkisi tanımlanmaya çalışmıştır. Sonuç olarak ise kurumsal yönetim ve iç denetimin birbirinden ayrılamayacak kadar yakın ilişki içerisinde oldukları görülmüştür.

Akçay (2013), çalışmasında kamu kurumlarındaki iç denetimin etkin bir şekilde işleyip işlemediğinin tespit etmeyi amaçlamıştır. Bu amaç doğrultusunda kamu kurumlarının iç denetim sürecindeki faaliyet sonuçlarını incelemiştir. Gerçekleştirilen bu çalışma sonucunda, ulaşılması gereken hedef ve amaçlara göre risklerin ortaya konulamadığı ve dolayısıyla ortaya konulamayan bu risklerin analizinin yapılamadığı tespit edilmiştir. Aynı zamanda iç denetim birimlerine personel alımı yapılırken mesleki yeterliliklerinin yeterince dikkate alınmadığı bunun da bilgi eksikliğine neden olduğu ve iç denetimin kurumun ast ve üst personeli tarafından yeterince benimsenmediği tespit edilmiştir.

Akçay (2013) bu çalışmada Türkiye’de kamu kurumlarının iç denetim kontrollerinin nasıl etkilediğini araştırmıştır. Bunun için anket çalışmasına örnek bir belediyede yapmıştır. Sonuç olarak iç denetim sürecinin kamu kurumları içinde önemli derecede etkili olduğunu tespit etmiştir.

Kartal (2013) yaptığı çalışmada Türkiye’de kamu ve özel sektörlerde iç denetim faaliyetlerinin öneminden bahsetmiştir. Özellikle Türk Bankacılık sisteminde iç denetim sürecinin temelini ve yapılış biçimini ortaya koymuştur.

Tufan ve Görün (2013) bu çalışmada Türkiye’de benimsenen iç denetim sisteminin kamu kurumlarındaki algılanma düzeyi ile uygulamasının hangi seviyede olduğunun incelenmesini hedeflemişlerdir.

Duncan ve Whittington (2014), BT’nin ilişkilerinin karmaşıklığın kabul edilmesi gerektiğini ve bu nedenle tüm tarafların çıkarlarının açıkça belirlenip yönetilmesi gerektiğini belirtmişlerdir.

Zorlu ve Tanç (2014) çalışmalarında, kar amacı gütmeyen bir devlet üniversitesinde iç kontrol ve iç denetim bölümünün üniversiteyi nasıl denetlediği, bu

denetim ve kontrollerle hangi sonuçlara ulaşıldığı, hangi iç denetim ve iç kontrol faaliyetlerinin uygulandığını incelenmişlerdir. Çalışmanın sonuçlarına göre kamu mali yönetimi bölümünde uzman personel noksanlığı neticesiyle birçok kamu kurumunda bu sistemi oluşturmanın oldukça güç olduğunu ve epeyce zaman aldığını vurgulamıştır.

Türedi vd. (2015) çalışmalarında, risk odaklı iç denetim konusunda standart belirleyen organizasyonların yayınları ve genel kabul görmüş uygulama ilkeleri üzerine bir literatür taraması yaparak risk esaslı iç denetimin kavramsal çerçevesini açıklamışlardır. Bunu yaparken de risk esaslı iç denetimin gelişimi ve kurumsal yönetimi ile ilişkisini özetlemişlerdir.

Gök (2015) Türkiye’de kamu yönetimlerinde yapılmakta olan iç denetim sürecinin yapısal özellikleri ve performansı, İç Denetim Koordinasyon Kurulu tarafından 2008-2013 dönemleri ile alakalı açıklanan raporlardaki veriler temelinde incelemeler yapmıştır.

Özdoğan ve Öncü (2016) bu çalışmada Türkiye’de aktif olan iç denetçiler temelinde yapılan anket çalışmalarında iç denetim mesleğinin son durumunu tespit etmek ve geliştirilmesi gereken alanların saptanmasını sağlamayı hedeflemişlerdir.

Güvemli vd., (2016) çalışmalarında Türkiye’de iç denetimin ve Türk Ticaret Kanununun olumlu ve olumsuz yönlerini ortaya koymuşlardır. Sonuç olarak da ekonomik gelişmelerin iç denetimi doğrudan etkilediğini tespit etmişlerdir.

Ünlü (2018) çalışmasında, internet bankacılığının avantajları olduğu kadar dezavantajlarının da olduğunu vurgulayarak, internet bankacılığı kullanan tüketicilerin karşılaşacağı saldırılara karşı çözüm önerileri getirmeyi amaçlamıştır. Bu doğrultuda önlemin hem bankacılar hem de kullanıcılar tarafından alınması gerektiğini ve bu alanda yeni kuralların belirlenip, benimsenmesi gerektiğini belirtmiştir. Ayrıca internet bankacılığı düzenlemelerinin sürekli güncellenmesi ve olası siber risklere karşı yeni yöntemler alınması gerektiğinin önemini vurgulamıştır.

Hoos vd. (2018), iç denetçilerin yansızlığına dokunabilecek iki faktörü araştırmak için yola çıkmıştır. Bunun için 79 tecrübeli iç denetçiyi deneye dahil etmişlerdir. Araştırma sonuçlarına göre, ilk olarak iç denetim fonksiyonunun bir yönetim eğitimi zemini olarak kullanıldığında, iç denetçilerin risk değerlendirmelerinin yönetim tercihleriyle uyumlu hale geldiği tespit edilmiştir. İkinci olarak yine iç denetim fonksiyonunun bir yönetim eğitimi zemini olarak kullanıldığında, iç denetçilerin daha

uygun yatırım tavsiyesinde bulundukları tespit edilmiştir. Üçüncü olarak ise, iç denetçilerin beklenmedik durumlarda denetim komitesine yönetimden daha uygun tavsiyede bulundukları ortaya konulmuştur.

Uysal (2018) araştırmasında, Türkiye'de kamu kurumlarında görev yapan iç denetçilerin kurumsal risk yönetimi ve risk odaklı iç denetim konusundaki farkındalıklarını belirlemeyi amaçlamıştır. Araştırma sonucunda kamudaki iç denetçilerin iç denetim faaliyetlerini riske dayalı olarak yürüttükleri ve risk yönetimi alanındaki sorumlulukları konusunda yeterli bilgiye sahip oldukları tespit edilmiştir. Ayrıca kamu idarelerindeki risk yöneti olgunluğunun yeterince oturmadığı saptanmıştır.

Altuntaş vd. (2018) çalışmalarında, Avrupa Birliği uyum sürecini takip eden ve 2007 yılından bu yana bu süreci başarıyla yöneten Türk sigortacılık sisteminin siber risklere karşı koruma sağlama etkinliğini test etmeyi amaçlamışlardır. Çalışmanın sonucuna göre, Türkiye ve AB sigortacılarının risk algıları ve riski değerlendirme bakış açıları arasında çok büyük farklılıklar olmamasına rağmen Türkiye'deki siber risklerin yaratacağı olası sorunlara ilişkin işletmelerin farkındalığının AB'den farklılık göstermiştir.

Selimoğlu ve Saldı (2019) çalışmalarında, siber risklerin iç denetim perspektifinden analiz edilmesi, haritalanması ve değerlendirilmesi için hangi yöntemlerin uygulanacağı ve kullanılacağı ele alınacağını açıklanmaya çalışmışlardır. Çalışma sonucuna göre, teknolojinin gelişmesiyle birlikte iç denetimin iş hayatındaki önemi ve rolü değişirken, operasyonel ve yönetim süreçlerindeki kapsamının da genişlediği tespit edilmiştir. Bu nedenle, siber risklere karşı önlem alınmasında iç denetimin rolünün, bilgi teknolojilerinin rolü kadar önemli olduğuna vurgu yapmıştır.

Mollaoğulları ve Öncü (2020) yaptıkları çalışmada iç denetim birimi yöneticilerinin algıları içinden denetim komitesinin, iç denetim birimi sorumluları ile olan etkileşimi incelemişlerdir.

Karaman, Turan ve Aydın, (2020) bir bilgisayar ağına uygulanan saldırıyı belirlemek ve saldırı modelinin sisteme zarar verip vermeyeceğini tespit etmek için yapay sinir ağı tabanlı bir sistem geliştirmişlerdir. Araştırmalarında DDOS, Botnet, DOS, BruteForce saldırı türlerini incelemişler ve DDOS ve BruteForce saldırılarının inceledikleri veri setindeki diğer iki türe göre daha yüksek frekansta gerçekleştiğini

bulmuşlardır. Oluşturdukları sistemin başarısının %99,26 gibi yüksek bir orana sahip olduğu gözlemlenmiştir.

Ocak (2021) çalışmasında, siber güvenlik, siber güvenlik ile iç denetim ilişkisi ve siber güvenlik denetimi konularını açıklamaya çalışmıştır. Ayrıca gerçek bir siber saldırı olayının nasıl gerçekleştiği ve bunun sonucunda hangi işlemlerin yapıldığına dair bir uygulamaya yer vermiştir.

Aydın (2021) çalışmasında, üniversitelerde uygulanmakta olan iç denetim faaliyetlerinin etkin ve amacına uygun işleyip işlemediğini tespitini yapmak, ayrıca iç denetim faaliyetlerinin uygulanmasından doğan misyonu yerine getirmek, kararlar almak ve çözüm önerileri getirmeyi amaçlamıştır. Aydın, üniversitelerdeki denetimin güvenilir ve doğru bir şekilde ilerleyebilmesi için gerekli şartların (alt yapı, fiziki imkânlar güven ortamı gibi) sağlanması gerektiğine vurgu yapmıştır. Bunun için ilk olarak yönetim tarafından kurumsal yönetimin önemi ve gerekliliği konusunda bir anlayış olmalıdır. Bu anlayış ile üniversitenin misyon ve vizyonuna değer katmak amacıyla rektörün iç denetime ve iç denetçiye güveninin ve desteğinin tam olması gerektiğini belirtmiştir.

Kıran ve Soğukpınar (2021) çalışmalarında uluslararası standartlardan yararlanarak kritik altyapıların korunması, risk analizi ve yönetiminin yapılmasına yönelik bir çatı önermişlerdir. Ayrıca bilişim altyapısındaki risklerin kritik altyapılara ve diğer kritik altyapıları ne denli zarara uğratabileceği açıklanmıştır.

3.4. ARAŞTIRMANIN HİPOTEZLERİ

Üniversitelerdeki iç denetim birimlerinde çalışan iç denetçilerin gözüyle iç denetimin siber güvenlik üzerine etkilerinin araştırılmasının amaçlandığı bu çalışma kapsamında aşağıdaki hipotezler test edilmek üzere oluşturulmuştur:

H₁: Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının öğrenim durumlarına göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

H₂: Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının iç denetçi olarak üniversitede çalıştığı süreye göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

H₃: Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının mesleki deneyimine göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

H4: İç denetçilerin siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyine göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır.

3.5. ARAŞTIRMANIN ANAKÜTLESİ VE ÖRNEKLEMİ

Türkiye’deki devlet ve vakıf üniversitelerinin bünyelerinde oluşturulmuş olan “İç Denetim” birimlerinde çalışan bütün iç denetçiler çalışmanın anakütlesini (evrenini) oluşturmaktadır. Bu amaç doğrultusunda devlet ve vakıf üniversitelerindeki toplam 168 iç denetçinin iletişim bilgilerine, çalıştıkları üniversitelerin resmi internet sayfalarındaki birim adreslerinden ulaşılmıştır. Sanal ortamda hazırlanan ölçek formu 168 iç denetçinin tamamının e-posta adresine online olarak doldurulması için gönderilmiştir. Gönderilen e-postalardan 42 tanesi için hatalı e-posta gönderimi uyarısı alınmıştır. Hatalı olmayan gönderimlerden toplam 56 geri dönüş sağlanmıştır. Eksik ve kayıp verilerin elenmesinden sonra 52 katılımcı ile uygulama yapılabilmektedir. Bu rakam, tam sayım yaptığımız ama geri dönüşü tam alamadığımız çalışmamız için yeterli bir örneklem miktarıdır (Saruhan ve Özdemirci, 2018:199).

3.6. VERİ TOPLAMA ARACI

Araştırma sorularına yanıt bulabilmek için oluşturulan anket formu için öncelikle literatürden faydalanılmıştır. Konu ile alakalı olarak toplanan bilimsel bilgiler ışığında Tokat Gaziosmanpaşa Üniversitesi İç Denetim biriminde çalışmakta olan birim çalışanları ve Bilgi İşlem biriminde çalışan birim elemanları ile süreç ve işleyiş hakkında görüşmeler yapılmıştır. Bu görüşmeler neticesinde anket soruları ilk halini almıştır. Ardından yapılan ikinci görüşmede bu sorular üzerine yine görüşler alınmış ve bir test grubu oluşturulup ölçeğin geçerliliği ve güvenilirliği test edilmiştir. Yapılan nitel görüşmeler ardından anket formu son halini almıştır. Anket formunun uygulanması için anakütleyi oluşturan üniversitelerin iç denetim birimindeki görevlilere e-posta yoluyla iletilmeden önce Tokat Gaziosmanpaşa Üniversitesi Etik Kurulundan gerekli izinler alınmıştır⁴.

Araştırmanın veri toplama aracı dört bölümden oluşmaktadır. Birinci bölümde katılımcıların siber güvenliğe ilişkin, mevcut durum bilgilerine on soru ile ulaşılmaya çalışılmıştır. Bu bölümdeki sorular kapalı uçlu sorulardır. Veri toplama aracının ikinci kısmında katılımcıların siber güvenlik açısından; üniversite yönetimi ve iç denetim

⁴ Etik Kurul Raporu çalışmanın Ek 2 kısmında yer almaktadır.

doktora seviyesinin ise (%7,7) olduğu görülmüştür. Katılımcıların üniversitelerde çalışma sürelerine bakıldığında %40,4'ünün 11-15 yıl, %48,1'inin 6-10 yıl, %9,6'inin 16-20 yıl, %1,9'unun ise 1-5 yıl kadar çalıştığı görülmüştür. Mesleki tecrübeye bakıldığında ise katılımcıların %21,2'sinin 16-20 yıl, %46,2'sinin 11-15 yıl, %30,8'inin 6-10 yıl, %1,9'unun ise 1-5 yıllık deneyime sahip oldukları görülmektedir

Tablo 4.1 Demografik Verilerin Frekans Tablosu

Değişken	Kategori	n	%
Cinsiyet	Kadın	8	15,4%
	Erkek	44	84,6%
Yaş	25 Yaş ve altı	0	0,0%
	26-35 Yaş	0	0,0%
	36-45 Yaş	20	38,5%
	46-55 Yaş	21	40,4%
	56 Yaş ve üstü	11	21,2%
Öğrenim Durumu	Lisans	36	69,2%
	Yüksek Lisans	12	23,1%
	Doktora	4	7,7%
İç Denetçi Olarak Üniversitede Çalışılan Süre	1-5 Yıl	1	1,9%
	6-10 Yıl	25	48,1%
	11-15 Yıl	21	40,4%
	16-20 Yıl	5	9,6%
	21-25 Yıl	0	0,0%
	25 Yıl ve üstü	0	0,0%
İç Denetçi Olarak Mesleki Tecrübe	1-5 Yıl	1	1,9%
	6-10 Yıl	16	30,8%
	11-15 Yıl	24	46,2%
	16-20 Yıl	11	21,2%
	21-25 Yıl	0	0,0%
	25 Yıl ve üstü	0	0,0%

Çalışmada yer alması elzem olan denetçi özellikleri Tablo 4,2'de yer almaktadır. Buna göre, katılımcıların siber güvenlik ve bilgi teknolojileri konularında %42,3'ünün "eğitim aldım ancak kendimi çok yetkin olarak görmüyorum" dediğinin %38,5'inin "yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum" dediğini, %19,2'sinin ise "eğitim aldım ve yeterli bilgiye sahibim" dediğini görülmektedir. Alınan sertifikalara baktığımızda katılımcıların %26,9'unun CGAP (Certified Government Auditing Professional) sertifikasına sahip olduğunu, %19,2'sinin Kamu İç denetçi sertifikasına sahip olduğunu, %17,3'ünün İç Tetkikçi sertifikasına sahip olduğunu, %7,7'sinin Mali Müşavir sertifikasına sahip olduğunu, %5,8'inin Bağımsız Denetçi sertifikasına sahip olduğunu, %5,8'inin Muhasebe Yetkilisi sertifikasına sahip olduğunu, %17,3'ünün ise herhangi bir sertifikasyona sahip olmadığı görülmektedir. Katılımcıların sahip olduğu

sertifika derecelerinin yoğunluğu ise sırayla A2 (%37,2), A4 (30,2), A1 ve A3 derecelerinin ise %16,3 olarak yer aldığı görülmektedir.

Tablo 4.2 Denetçi Özellikleri Frekans Tablosu⁸²

Değişken	Kategori	n	%
Siber Güvenlik ve Bilgi teknolojileri Konularında	Eğitim aldım ve yeterli bilgiye sahibim	10	19,2%
	Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	22	42,3%
	Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	20	38,5%
Alınan Mesleki Sertifikasyonlar	Yok	9	17,3%
	İç Tetkikçi	9	17,3%
	CGAP (Sertifikalı Devlet Denetim Uzmanı)	14	26,9%
	Kamu İç Denetçi	10	19,2%
	Muhasebe Yetkilisi	3	5,8%
	Bağımsız Denetçi	3	5,8%
	SMMM	4	7,7%
Sertifika Derecesi	A1	7	16,3%
	A2	16	37,2%
	A3	7	16,3%
	A4	13	30,2%

Çalışmanın bir diğer önemli kümesi üniversitelerin iç denetim yetkinlikleridir. Katılımcılar hakkındaki bilgileri Tablo 4.3’de görmek mümkündür. Tabloyu incelediğimizde üniversitelerin siber güvenlik konularında %51,9 oranında hizmet satın aldıklarını, %48,1 oranında kendi siber güvenlik departmanlarının bulunduğunu görmekteyiz. Katılımcılara “İç denetim birimi, siber güvenlik süreçlerini ve kontrollerini değerlendirebilecek yetkinlikte mi?” diye sorduğumuzda %38,5 hayır ve kısmen dediklerini, %23,1 oranında ise evet dediklerini görmekteyiz.

Son bir yıl içerisinde siber güvenlik ile ilgili konuların üniversite yönetim kurulunda %44,2 oranında hiç gündeme alınmadığını, %28,8 oranında bir def gündeme alındığını, %26,9 oranında ise birkaç toplantıda gündem olarak konuşulduğunu görmekteyiz. Katılımcılara ‘İç denetim birimi tarafından üniversitenin karşı karşıya gelebileceği yaygın siber tehditler (ör. Suçlular, bilgisayar korsanları, ağa bağlı sistemler, bulut sağlayıcıları, tedarikçiler, sosyal medya sistemleri, kötü amaçlı yazılım) belirlendi mi?’ diye sorduğumuzda, %80,8 oranında hayır, %19,2 oranında evet dediklerini görmekteyiz. Evet, yanıtını veren katılımcılar %60,0 oranında belirlenen siber tehditler iç denetim risk değerlendirme ve planlama süreçlerine dâhil edildiğini %40,0 oranında ise kısmen dâhil edildiğini söylemektedir.

Tablo 4.3 Üniversite İç Denetim Yetkinliği Frekans Tablosu

Değişken	Kategori	n	%
Siber Güvenlik Konularında Üniversitemiz	Hizmet satın almaktadır	27	51,9%
	Kendi departmanı bulunmaktadır	25	48,1%
İç Denetim Birimi Siber Güvenlik Süreçlerini ve Kontrollerini Değerlendirebilecek Yetkinlikte Mi?	Evet	12	23,1%
	Hayır	20	38,5%
	Kısmen	20	38,5%
Son Bir Yıl İçerisinde Siber Güvenlik İle İlgili Konular Üniversite Yönetim Kurulunda Gündem Olarak Yer Aldı Mı?	Bir defa gündem olarak konuşuldu	15	28,8%
	Birkaç toplantıda gündem olarak konuşuldu	14	26,9%
	Sık sık toplantılarda gündem olarak konuşuldu	0	0,0%
	Bütün toplantılarda gündem olarak konuşuldu	0	0,0%
	Hiç gündeme alınmadı	23	44,2%
İç Denetim Birimi Tarafından Üniversitenin Karşı Karşıya Gelebileceği Yaygın Siber Tehditleri Belirledi Mi?	Evet	10	19,2%
	Hayır	42	80,8%
	Kısmen	0	0,0%
Belirlenen Siber Tehditler İç Denetim Risk Değerlendirme ve Planlama Süreçlerine Dâhil Edildi Mi?	Evet	6	60,0%
	Hayır	0	0,0%
	Kısmen	4	40,0%

Tablo 4.4'te yer alan Siber risk yönetimi açısından üniversitelerin yaşadıkları zorlukların önem derecesi frekans tablosuna bakacak olursak, nitelikli bir siber güvenlik uzmanının işe alımının zor olması ifadesine önem derecesine göre ilk sırada yer verenler 10 kişinin katılımıyla %19,2 oranındadır. Önem derecesine göre son sırada yer verenlerin ise toplam 7 kişinin katılımıyla %17,3 oranında olduğu görülmektedir.

Kurumda standart/ortak bir siber risk yönetim anlayışı olmaması ifadesine önem derecesine göre ilk sırada yer verenlerin 11 kişinin katılımıyla %21,2 oranında olduğu ve en çok katılımın 12 kişinin katılımıyla %23,1 oranında 3. derece yoğunlaştığı görülmektedir. Önem derecesine göre ifadeye son sırada yer verenlerin ise 3 kişinin katılımıyla %5,8 oranında olduğu görülmektedir.

Sektörel ve operasyonel olarak siber tehditlerin neler olduğuna yönelik yönetim seviyesinde bir takip ve farkındalık olmaması ifadesine önem derecesine göre ilk sırada yer verenlerin sadece 1 kişinin katılımıyla %1,9 oranında olduğu ve en çok katılımın 12 kişinin katılımıyla %23,1 oranında 5. derecede yoğunlaştığı görülmektedir. Önem derecesine göre ifadeye son sırada yer verenlerin ise 6 kişinin katılımıyla %11,5 oranında olduğu görülmektedir.

Tablo 4.4 Siber Risk Yönetimi Açısından Üniversitelerin Yaşadıkları Zorlukların Önem Derecesi Frekans Tablosu

Soru	Önem	1	2	3	4	5	6	7
Nitelikli Bir Siber Güvenlik Uzmanının İşe Alımının Zor Olması	Sıra	10	6	7	10	5	5	9
	Oran	19,2%	11,5%	13,5%	19,2%	9,6%	9,6%	17,3%
Kurumda Standart/Ortak Bir Siber Risk Yönetim Anlayışı Olmaması	Sıra	11	3	12	5	10	8	3
	Oran	21,2%	5,8%	23,1%	9,6%	19,2%	15,4%	5,8%
Sektörel ve Operasyonel Olarak Siber Tehditlerin Neler Olduğuna Yönelik Yönetim Seviyesinde Bir Takip ve Farkındalık Olmaması	Sıra	1	7	7	10	12	9	6
	Oran	1,9%	13,5%	13,5%	19,2%	23,1%	17,3%	11,5%
Çalışanlara Bilgi Güvenliği Konusunda Eğitim Verilmemesi	Sıra	8	5	7	10	12	5	5
	Oran	15,4%	9,6%	13,5%	19,2%	23,1%	9,6%	9,6%
Kurumun Bu Konuya yeterli Bütçe Ayırmaması/Yatırım Yapılmaması	Sıra	9	17	6	7	3	3	7
	Oran	17,3%	32,7%	11,5%	13,5%	5,8%	5,8%	13,5%
Yeni Siber Tehditlere Karşı Önlem Alınmaması	Sıra	6	8	8	2	4	14	10
	Oran	11,5%	15,4%	15,4%	3,8%	7,7%	26,9%	19,2%
Kurumda Siber Güvenlik Konusunun Net Bir Sahibinin Olmaması	Sıra	7	6	5	8	6	8	12
	Oran	13,5%	11,5%	9,6%	15,4%	11,5%	15,4%	23,1%

Çalışanlara bilgi güvenliği konusunda eğitim verilmemesi ifadesine önem derecesine göre ilk sırada yer verenlerin 8 kişinin katılımıyla %15,4 oranında olduğu ve en çok katılımın 12 kişinin katılımıyla %23,1 oranında 5. derecede yoğunlaştığı görülmektedir. Önem derecesine göre ifadeye son sırada yer verenlerin ise 5 kişinin katılımıyla %9,6 oranında olduğu görülmektedir.

Kurumun bu konuya yeterli bütçe ayırmaması/yatırım yapılmaması ifadesine önem derecesine göre ilk sırada yer verenlerin 9 kişinin katılımıyla %17,3 oranında olduğu ve en çok katılımın ise 17 kişiyle %32,7 oranında 2. derecede yoğunlaştığı görülmektedir. Önem derecesine göre ifadeye son sırada yer verenlerin ise 7 kişinin katılımıyla %13,5 oranında olduğu görülmektedir.

Yeni siber tehditlere karşı önlem alınmaması ifadesine önem derecesine göre ilk sırada yer verenlerin 6 kişinin katılımıyla %11,5 oranında olduğu ve en çok katılımın 14 kişinin katılımıyla %26,9 oranında 6. derecede yoğunlaştığı görülmektedir. Önem derecesine göre ifadeye son sırada yer verenlerin ise 10 kişinin katılımıyla %19,2 oranında olduğu görülmektedir.

Kurumda siber güvenlik konusunun net bir sahibinin olmaması ifadesine önem derecesine göre ilk sırada yer verenlerin 7 kişinin katılımıyla %13,5 oranında olduğu, ifadeye en çok katılımın olduğu ve aynı zamanda son sırada yer verenlerin 12 kişinin katılımıyla %23,1 oranında olduğu görülmektedir.

İç Denetim Ve Bilgi Güvenliği Personel Sayısı Tanımlayıcı İstatistikleri Tablo 4.5'te verilmiştir. İlgili tablo incelendiğinde, iç denetim biriminde en az 1 ile en fazla 7 çalışan arasında personel olduğu belirtilmiştir. Üniversitelerde çalışan iç denetim personel sayısının ortalaması ise yaklaşık 3,2 olarak elde edilmiştir.

Bilgi güvenliğinden sorumlu çalışan sayılarına bakıldığında en az 1 en fazla 5 çalışan olduğu görülmektedir. Ortalama ise 3,1 olarak elde edilmiştir.

Tablo 4.5 İç Denetim Ve Bilgi Güvenliği Personel Sayısı Tanımlayıcı İstatistikleri

Descriptive Statistics					
	N	Minimum	Maximum	Aritmetik Ortalama	Standart Sapma
İç Denetimde Çalışan Personel Sayısı	52	1,000	7,000	3,212	1,500
Bilgi Güvenliğinden Sorumlu Personel Sayısı	52	1,000	5,000	3,154	1,319
Valid N (listwise)	108				

Veri toplama aracının ikinci kısmında yer alan ölçeğin yapı geçerliliğini test etmek amacıyla açıklayıcı faktör analizi yapılmıştır. Analiz sonucunda 2 ifade binişiklik sebebiyle ölçekten çıkartılmıştır. Elde edilen nihai çözümde beş faktör vardır. Bu beş faktör toplam varyansın %78,900'ünü açıklamaktadır. KMO değeri %0,823, Bartlett test sonucu anlamlıdır. Bu bulgular ışığında örnek hacminin yeterli ve veri setinin faktör analizi için uygun olduğu söylenebilir.

Aşağıdaki Tablo 4.6'da açıklayıcı faktör analizi sonuçları özetlenmektedir. Faktör analizi neticesinde birinci faktör altında toplanan ifadelerin katılımcıların bilgi güvenliği denetlemesi algısını ölçen ifadeler olduğu görülmüştür. Bu sebeple birinci faktör "**İç Denetim ve Siber Güvenlik Algısı**" olarak isimlendirilmiştir. İkinci faktör altında toplanan ifadelerin katılımcıların üniversite yönetimi ve siber güvenlik algısını ölçen ifadeler olduğu görülmüştür. Bu sebeple ikinci faktör "**Üniversite Yönetimi ve Siber Güvenlik Algısı**" olarak isimlendirilmiştir. Üçüncü faktör altında toplanan ifadelerin katılımcıların İç Denetim ve Siber Güvenlik Algısını ölçen ifadeler olduğu görülmüştür. Bu sebeple üçüncü faktör "**İç Denetim ve Siber Güvenlik Algısı**" olarak isimlendirilmiştir.

Tablo 4.6 Faktör Analizi Sonuçları

Faktör 1: Bilgi Güvenliği Denetlemesi Algısı	Faktör Yüğü	Öz Değer	Açıklanan Varyans	Cronbach Alfa
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde kimlik ve erişim yöntemleri kontrol edilir.	0,805	11,249	20,112	0,935
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde sistem izlemesi yapılır.	0,800	3,678		
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde güvenlik duvarı incelenir.	0,763	2,425		
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde genel güvenlik protokollerine uygunluk kontrol edilir.	0,762	1,344		
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde şifreleme ilkeleri kontrol edilir	0,762	1,029		
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde ağa bağlanan cihazlar incelenir.	0,761	,789		
İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde yedekleme prosedürleri kontrol edilir.	0,695	,656		
İç denetim birimi siber güvenlik denetlemelerinde iş planı ve acil durum planlarını kontrol eder.	0,560	,581		
Faktör 2: Üniversite Yönetimi ve Siber Güvenlik Algısı				
Üniversite yönetimi siber güvenlik konusunun önemine inanmaktadır.	0,822	,510	17,932	0,905
Üniversite yönetimi siber güvenlik konusunda proaktif yaklaşım sergilemektedir.	0,775	,415		
Üniversite yönetiminin siber güvenlik konusundaki beklentileri son yıllarda artış göstermiştir.	0,731	,395		
Üniversite yönetimi tarafından siber güvenlik konusunda yeterince kaynak aktarımı yapılmaktadır.	0,668	,341		
İç denetim birimi siber güvenlik konusunda daha fazla sorumluluk almalıdır.	0,664	,322		
Üniversite yönetimi siber güvenlik konusunda ilgili personellerle düzenli iletişim kurmaktadır.	0,618	,246		
Faktör 3: İç Denetim ve Siber Güvenlik Algısı				
İç denetim birimi siber güvenlik konusundaki eksiklikleri belirler ve raporlar.	0,803	,169	15,167	0,891
İç denetim birimi üniversitedeki siber güvenlik uygulamalarına katkı sağlar.	0,784	,160		
İç denetim birimi siber güvenlik konusundaki güncel konuları takip eder.	0,750	,143		
İç denetim birimi siber güvenlik konusunda yeterince bilgi sahibidir.	0,669	,123		
Faktör 4: Siber Güvenlik Bilgi Düzeyi Algısı				
Üniversitede siber güvenliğe yönelik kurum kültürü gelişmiştir.	0,804	,090	13,190	0,837
Üniversitede tüm çalışanlar siber güvenliğe ilişkin yükümlülüklerini tam olarak bilmektedir.	0,779	,084		
İç denetim personeli üniversitedeki bilgi işlem faaliyetleri hakkındaki yeterli bilgi sahibidir.	0,658	,068		
İç denetim personeli ile bilgi güvenliği personeli ya da bilgi işlem personeli arasında yardımlaşma vardır.	0,584	,063		
Faktör 5: Siber Risk Yönetimi ve Siber Tehditler Algısı	Faktör Yüğü	Öz Değer	Açıklanan Varyans	Cronbach Alfa

Siber risk yönetimi ile ilgili olarak siber tehditleri değerlendirme ve ölçme konusunda üniversitenin uygulamalarını yeterli buluyorum.	0,892	,052	12,499	0,890
Siber risk yönetimi ile ilgili olarak siber saldırılara müdahale etme konusunda üniversitenin uygulamalarını yeterli buluyorum.	0,829	,043		
Siber risk yönetimi ile ilgili olarak siber saldırıları önleme konusunda üniversitenin uygulamalarını yeterli buluyorum.	0,828	,024		
Toplam Varyans			78,900	

Dördüncü faktör altında toplanan ifadelerin katılımcıların Siber Güvenlik Bilgi Düzeyi Algısını ölçen ifadeler olduğu görülmüştür. Bu sebeple dördüncü faktör “**Siber Güvenlik Bilgi Düzeyi Algısı**” olarak isimlendirilmiştir. Beşinci faktör altında toplanan ifadelerin katılımcıların Siber Risk Yönetimi ve Siber Tehditler Algısını ölçen ifadeler olduğu görülmüştür. Bu sebeple beşinci ve son olan faktör “**Siber Risk Yönetimi ve Siber Tehditler Algısı**” olarak isimlendirilmiştir.

Katılımcıların öğrenim durumlarına göre iç denetimde siber güvenlik algılarının farklılaşp farklılaşmadığı tek yönlü varyans analizi ile test edilmiştir. Analiz sonuçları Tablo 4.7’de gösterilmiştir.

Tablo 4.7 Öğrenim Durumları İtibariyle Farkları Gösteren ANOVA Tablosu

		Sum of Squares	df	Mean Square	F	Sig.
Bilgi Güvenliği Denetlemesi Algısı	Gruplararası	6,910	2	3,455	4,524	,016
	Gruplar içi	37,418	49	,764		
	Toplam	44,328	51			
Üniversite Yönetimi ve Siber Güvenlik Algısı	Gruplararası	12,391	2	6,195	9,010	,000
	Gruplar içi	33,692	49	,688		
	Toplam	46,083	51			
İç Denetim ve Siber Güvenlik Algısı	Gruplararası	5,424	2	2,712	3,368	,043
	Gruplar içi	39,451	49	,805		
	Toplam	44,875	51			
Siber Güvenlik Bilgi Düzeyi Algısı	Gruplararası	6,231	2	3,115	4,670	,014
	Gruplar içi	32,688	49	,667		
	Toplam	38,918	51			
Siber Risk Yönetimi ve Siber Tehditler Algısı	Gruplararası	2,557	2	1,278	2,073	,137
	Gruplar içi	30,219	49	,617		
	Toplam	32,776	51			

Tablo 4.7’deki ANOVA sonuçları incelendiğinde birinci, ikinci, üçüncü ve dördüncü faktör açısından öğrenim durumları arasında anlamlı farklılık olduğu görülmektedir. Beşinci faktör açısından öğrenim durumu birbirinden farklılaşmamaktadır.

Öğrenim durumunun “Bilgi Güvenliği Denetlemesi Algısı” faktörü ile arasında anlamlı fark vardır. Öğrenim durumunun “Üniversite Yönetimi ve Siber Güvenlik Algısı” faktörü ile arasında anlamlı fark vardır. Öğrenim durumunun “İç Denetim ve Siber Güvenlik Algısı” faktörü ile arasında anlamlı fark vardır. Öğrenim durumunun “Siber Güvenlik Bilgi Düzeyi Algısı” faktörü ile arasında anlamlı fark vardır. Farkın yönünü görmek için yapılan Scheffe testi sonuçları Tablo 4.8’de verilmiştir.

Tablo 4.8 Öğrenim Durumları Arasındaki Farkı Gösteren Scheffe Testi Sonuçları

Dependent Variable	(I) Öğrenim Durumu	(J) Öğrenim Durumu	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
						Lower Bound	Upper Bound
Bilgi Güvenliği Denetlemesi Algısı	Lisans	Yüksek	-,76042 *	,29129	,041	-1,4958	-,0251
		Lisans Doktora	,48958	,46056	,572	-,6731	1,6523
	Yüksek Lisans	Lisans	,76042 *	,29129	,041	,0251	1,4958
		Lisans Doktora	1,25000	,50452	,055	-,0237	2,5237
	Doktora	Lisans	-,48958	,46056	,572	-1,6523	,6731
		Yüksek Lisans	-1,25000	,50452	,055	-2,5237	,0237
Üniversite Yönetimi ve Siber Güvenlik Algısı	Lisans	Yüksek	-,84722 *	,27640	,014	-1,5450	-,1494
		Lisans Doktora	1,05556	,43703	,064	-,0477	2,1589
	Yüksek Lisans	Lisans	,84722 *	,27640	,014	,1494	1,5450
		Lisans Doktora	1,90278 *	,47875	,001	,6942	3,1114
	Doktora	Lisans	-1,05556	,43703	,064	-2,1589	,0477
		Yüksek Lisans	-1,90278 *	,47875	,001	-3,1114	-,6942
İç Denetim ve Siber Güvenlik Algısı	Lisans	Yüksek	-,42361	,29910	,374	-1,1787	,3315
		Lisans Doktora	,90972	,47291	,168	-,2842	2,1036
	Yüksek Lisans	Lisans	,42361	,29910	,374	-,3315	1,1787
		Lisans Doktora	1,33333 *	,51805	,045	,0255	2,6412
	Doktora	Lisans	-,90972	,47291	,168	-2,1036	,2842
		Yüksek Lisans	-1,33333 *	,51805	,045	-2,6412	-,0255
Siber Güvenlik Bilgi Düzeyi Algısı	Lisans	Yüksek	-,75000 *	,27225	,029	-1,4373	-,0627
		Lisans Doktora	,37500	,43047	,686	-,7117	1,4617
	Yüksek Lisans	Lisans	,75000 *	,27225	,029	,0627	1,4373
		Lisans Doktora	1,12500	,47155	,068	-,0654	2,3154
	Doktora	Lisans	-,37500	,43047	,686	-1,4617	,7117
		Yüksek Lisans	-1,12500	,47155	,068	-2,3154	,0654
Siber Risk Yönetimi ve Siber Tehditler Algısı	Lisans	Yüksek	-,35185	,26177	,412	-1,0127	,3090
		Lisans Doktora	-,71296	,41390	,237	-1,7578	,3319
	Yüksek Lisans	Lisans	,35185	,26177	,412	-,3090	1,0127
		Lisans Doktora	-,36111	,45340	,730	-1,5057	,7835
	Doktora	Lisans	,71296	,41390	,237	-,3319	1,7578
		Yüksek Lisans	,36111	,45340	,730	-,7835	1,5057

Tablo 4.8’deki Scheffe testi sonuçları incelendiğinde öğrenim durumu yüksek lisans olan katılımcıların “Bilgi Güvenliği Denetlemesi Algısı” öğrenim durumu lisans olan katılımcılardan fazla olduğu görülmektedir.

Öğrenim durumu yüksek lisans olan katılımcıların “Üniversite Yönetimi ve Siber Güvenlik Algısı” öğrenim durumu lisans olan katılımcılardan fazla olduğu görülmektedir. Yine öğrenim durumu yüksek lisans olan katılımcıların “Üniversite Yönetimi Ve Siber Güvenlik Algısı” öğrenim durumu doktora olan katılımcılardan fazla olduğu görülmektedir.

Öğrenim durumu yüksek lisans olan katılımcıların “İç Denetim ve Siber Güvenlik Algısı” öğrenim durumu doktora olan katılımcılardan fazla olduğu görülmektedir.

Öğrenim durumu yüksek lisans olan katılımcıların “Siber Güvenlik Bilgi Düzeyi Algısı” öğrenim durumu lisans olan katılımcılardan fazla olduğu görülmektedir.

Katılımcıların iç denetçi olarak üniversitede çalıştıkları süreye göre iç denetimde siber güvenlik algılarının farklılaşıp farklılaşmadığı tek yönlü varyans analizi ile test edilmiştir. Analiz sonuçları aşağıdaki Tablo 4.9’da verilmiştir.

Tablo 4.9 Katılımcıların İç Denetçi Olarak Üniversitede Çalıştıkları Süre İtibariyle Farklarını Gösteren ANOVA Sonuçları

		Sum of Squares	df	Mean Square	F	Sig.
Bilgi Güvenliği Denetlemesi Algısı	Gruplararası	,468	2	,234	,262	,771
	Gruplar içi	43,859	49	,895		
	Toplam	44,328	51			
Üniversite Yönetimi ve Siber Güvenlik Algısı	Gruplararası	1,477	2	,738	,811	,450
	Gruplar içi	44,606	49	,910		
	Toplam	46,083	51			
İç Denetim ve Siber Güvenlik Algısı	Gruplararası	,005	2	,003	,003	,997
	Gruplar içi	44,870	49	,916		
	Toplam	44,875	51			
Siber Güvenlik Bilgi Düzeyi Algısı	Gruplararası	1,401	2	,700	,915	,407
	Gruplar içi	37,518	49	,766		
	Toplam	38,918	51			
Siber Risk Yönetimi ve Siber Tehditler Algısı	Gruplararası	,264	2	,132	,199	,820
	Gruplar içi	32,511	49	,663		
	Toplam	32,776	51			

Tablo 4.9'daki ANOVA sonuçları incelendiğinde, katılımcıların İç Denetçi olarak üniversitede çalıştıkları süre ile tabloda yer alan beş faktör arasında farklılaşma olmadığı görülmektedir.

Katılımcıların iç denetçi olarak mesleki tecrübelerine göre iç denetimde siber güvenlik algılarının farklılaşıp farklılaşmadığı tek yönlü varyans analizi ile test edilmiştir. Analiz sonuçları aşağıdaki Tablo 4.10'da verilmiştir.

Tablo 4.10 İç Denetçi Olarak Mesleki Tecrübeleri İtibariyle Farklarını Gösteren ANOVA Sonuçları

		Sum of Squares	df	Mean Square	F	Sig.
Bilgi Güvenliği Denetlemesi Algısı	Gruplararası	,459	2	,229	,256	,775
	Gruplar içi	43,869	49	,895		
	Toplam	44,328	51			
Üniversite Yönetimi ve Siber Güvenlik Algısı	Gruplararası	4,158	2	2,079	2,430	,099
	Gruplar içi	41,924	49	,856		
	Toplam	46,083	51			
İç Denetim ve Siber Güvenlik Algısı	Gruplararası	3,852	2	1,926	2,301	,111
	Gruplar içi	41,023	49	,837		
	Toplam	44,875	51			
Siber Güvenlik Bilgi Düzeyi Algısı	Gruplararası	4,258	2	2,129	3,010	,058
	Gruplar içi	34,660	49	,707		
	Toplam	38,918	51			
Siber Risk Yönetimi ve Siber Tehditler Algısı	Gruplararası	,804	2	,402	,616	,544
	Gruplar içi	31,972	49	,652		
	Toplam	32,776	51			

Tablo 4.10 incelendiğinde katılımcıların iç denetçi olarak mesleki tecrübelerine göre iç denetimde siber güvenlik algıları farklılaşmamaktadır.

Katılımcıların siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyine göre iç denetimde siber güvenlik algılarının farklılaşıp farklılaşmadığı tek yönlü varyans analizi ile test edilmiştir. Analiz sonuçları aşağıdaki Tablo 4.11’de gösterilmiştir.

Tablo 4.11’deki ANOVA sonuçları incelendiğinde üçüncü ve beşinci faktör açısından katılımcıların siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyleri arasında anlamlı farklılık olduğu görülmektedir. Birinci, ikinci ve dördüncü faktör açısından katılımcıların siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyleri birbirinden farklılaşmamaktadır. Katılımcıların siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeylerinin “İç Denetim ve Siber Güvenlik Algısı” faktörü ile arasında anlamlı bir fark vardır. Yine siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyleri “Siber Risk Yönetimi ve Siber Tehditler Algısı” faktörü ile arasında anlamlı bir fark vardır.

Tablo 4.11 Katılımcıların Siber Güvenlik Ve Bilgi Teknolojileri Konularındaki Bilgi Düzeyleri İtibariyle Farklarını Gösteren ANOVA Sonuçları

		Sum of Squares	df	Mean Square	F	Sig.
Bilgi Güvenliği Denetlemesi Algısı	Gruplararası	,501	2	,251	,280	,757
	Gruplar içi	43,827	49	,894		
	Toplam	44,328	51			
Üniversite Yönetimi ve Siber Güvenlik Algısı	Gruplararası	1,145	2	,573	,624	,540
	Gruplar içi	44,938	49	,917		
	Toplam	46,083	51			
İç Denetim ve Siber Güvenlik Algısı	Gruplararası	8,182	2	4,091	5,463	,007
	Gruplar içi	36,693	49	,749		
	Toplam	44,875	51			
Siber Güvenlik Bilgi Düzeyi Algısı	Gruplararası	4,114	2	2,057	2,896	,065
	Gruplar içi	34,805	49	,710		
	Toplam	38,918	51			
Siber Risk Yönetimi ve Siber Tehditler Algısı	Gruplararası	4,149	2	2,074	3,551	,036
	Gruplar içi	28,627	49	,584		
	Toplam	32,776	51			

Farkın yönünü görmek için yapılan Scheffe testi sonuçları aşağıdaki Tablo 4.12’de gösterilmiştir.

Tablo 4.12’teki Scheffe testi sonuçları incelendiğinde katılımcılardan eğitim aldım ve yeterli bilgiye sahibim diyenlerin yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum diyenlere kıyasla “İç Denetim ve Siber Güvenlik Algısının” daha fazla olduğu görülmektedir. Benzer şekilde eğitim aldım ancak kendimi çok yetkin olarak görmüyorum diyen katılımcıların da yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum diyen katılımcılara kıyasla “İç Denetim ve Siber Güvenlik Algısının” daha fazla olduğu görülmektedir.

Tablo 4.12 Katılımcıların Siber Güvenlik Ve Bilgi Teknolojileri Konularındaki Bilgi Düzeyleri Arasındaki Farkı Gösteren Scheffe Testi Sonuçları

Dependent Variable	(I)	(J)	Mean Difference	Standard Error	Sig.	Lower Bound	Upper Bound
İç Denetim ve Siber Güvenlik Algısı	Eğitim aldım ve yeterli bilgiye sahibim	Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	,09091	,33003	,963	-,7423	,9241
		Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	,87500*	,33515	,041	,0289	1,7211
	Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	Eğitim aldım ve yeterli bilgiye sahibim	-,09091	,33003	,963	-,9241	,7423
		Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	,78409*	,26736	,019	,1091	1,4590
	Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	Eğitim aldım ve yeterli bilgiye sahibim	-,87500*	,33515	,041	-1,7211	-,0289
		Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	-,78409*	,26736	,019	-1,4590	-,1091
Siber Risk Yönetimi ve Siber Tehditler Algısı	Eğitim aldım ve yeterli bilgiye sahibim	Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	,45455	,29151	,305	-,2814	1,1905
		Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	,78333*	,29603	,038	,0360	1,5307
	Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	Eğitim aldım ve yeterli bilgiye sahibim	-,45455	,29151	,305	-1,1905	,2814
		Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	,32879	,23615	,387	-,2674	,9249
	Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum	Eğitim aldım ve yeterli bilgiye sahibim	-,78333*	,29603	,038	-1,5307	-,0360
		Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum	-,32879	,23615	,387	-,9249	,2674

Katılımcılardan eğitim aldım ve yeterli bilgiye sahibim diyenlerin yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum diyenlere kıyasla “Siber Risk Yönetimi ve Siber Tehditler Algısının” daha fazla olduğu görülmektedir.

Üniversitelerde iç denetimin uygulanış şeklinin ve bazı eksiklerin belirlenmesine dair iç denetçilere belli başlı bazı sorular sorulmuştur. Katılımcıların mevcut durumlarına ait istatistik Tablo 4.13’te gösterilmiştir.

Tablo 4.13 Katılımcıların Mevcut Durumlarının İstatistik Tablosu

Sorular	Evet	Hayır	Kısmen	Fikrim Yok
Siber Güvenliğe İlişkin Önemli Varlık Grupları Belirlenmiştir	14 26,90%	13 25,00%	5 9,60%	20 38,50%
Siber Güvenliğe İlişkin Önemli Varlık Gruplarının Kritiklik Derecesi Belirlenmiştir	14 26,90%	12 23,10%	5 9,60%	21 40,40%
Siber Güvenliğe İlişkin Önemli Varlık Gruplarının Mevcut Durum Ve Boşluk Analizleri Yapılmıştır	8 15,40%	17 32,70%	5 9,60%	22 42,30%
Siber Güvenliğe İlişkin Önemli Varlık Grupları İle İlgili Neler Yapılacağına Ait Rehber Uygulama Yol Haritası Belirlenmiştir	8 15,40%	16 30,80%	10 19,20%	18 34,60%
Siber Güvenliğe İlişkin Önemli Varlık Gruplarının Değişimi Söz Konusu Olduğunda Değişiklikler Rehberine Uygun Olarak Yönetilmektedir	8 15,40%	17 32,70%	8 15,40%	19 36,50%
Cumhurbaşkanlığı Dijital Dönüşüm Ofisi’nin Yayınladığı Bilgi Ve İletişim Güvenliği Rehberine Uygun Olarak Denetimler Yapılmaktadır	10 19,20%	24 46,20%	7 13,50%	11 21,20%
Cumhurbaşkanlığı Dijital Dönüşüm Ofisi’nin Yayınladığı Bilgi Ve İletişim Güvenliği Rehberi Yol Haritasının İzlemesi Ve Kontrolü Yapılmaktadır	8 15,40%	20 38,50%	11 21,20%	13 25,00%
Üniversitemizde Siber Güvenliğe İlişkin Kurallar Ve Politikaların Bulunduğu Kılavuz Mevcuttur	6 11,50%	25 48,10%	9 17,30%	12 23,10%
Üniversitelerdeki İç Denetim Birimlerinde Bilgi Teknolojileri Konusunda Uzman Personelin De Çalışması Gerekmetedir	20 38,50%	13 25,00%	3 5,80%	16 30,80%
Son Yıllarda Siber Güvenlik Açısından İç Denetimin Rolü Artmıştır’ Sorusuna 6 Katılımcının Kısmen	23 44,20%	13 25,00%	6 11,50%	10 19,20%

Katılımcılardan “siber güvenliğe ilişkin önemli varlık grupları belirlenmiştir” sorusuna 5 katılımcının kısmen, 13 katılımcının hayır, 14 katılımcının evet ve 20 katılımcının en yüksek oranla (%38,50) fikrim yok dediği görülmektedir.

Katılımcılardan “siber güvenliğe ilişkin önemli varlık gruplarının kritiklik derecesi belirlenmiştir” sorusuna 5 katılımcının kısmen, 12 katılımcının hayır, 14

katılımcının evet ve 21 katılımcının en yüksek oranla (%40,40) fikrim yok dediği görülmektedir.

Katılımcılardan “siber güvenliğe ilişkin önemli varlık gruplarının mevcut durum ve boşluk analizleri yapılmıştır” sorusuna 5 katılımcının kısmen, 8 katılımcının evet, 17 katılımcının hayır ve 22 katılımcının en yüksek oranla (%42,30) fikrim yok dediği görülmektedir.

Katılımcılardan “siber güvenliğe ilişkin önemli varlık grupları ile ilgili neler yapılacağına ait rehber uygulama yol haritası belirlenmiştir” sorusuna 8 katılımcının evet, 10 katılımcının kısmen, 16 katılımcının hayır ve 18 katılımcının en yüksek oranla (%34,60) fikrim yok dediği görülmektedir.

Katılımcılardan “siber güvenliğe ilişkin önemli varlık gruplarının değişimi söz konusu olduğunda değişiklikler rehberine uygun olarak yönetilmektedir” sorusuna 8 katılımcının evet, 8 katılımcının kısmen, 17 katılımcının hayır ve 19 katılımcının en yüksek oranla (%36,50) fikrim yok dediği görülmektedir.

Katılımcılardan “Cumhurbaşkanlığı Dijital Dönüşüm Ofisi’nin yayınladığı Bilgi ve İletişim Güvenliği Rehberine uygun olarak denetimler yapılmaktadır” sorusuna 7 katılımcının kısmen, 10 katılımcının evet, 11 katılımcının fikrim yok ve 24 katılımcının en yüksek oranla (%46,20) hayır dediği görülmektedir.

Katılımcılardan “Cumhurbaşkanlığı Dijital Dönüşüm Ofisi’nin yayınladığı Bilgi ve İletişim Güvenliği Rehberi yol haritasının izlemesi ve kontrolü yapılmaktadır” sorusuna 8 katılımcının evet, 11 katılımcının kısmen, 13 katılımcının fikrim yok ve 20 katılımcının en yüksek oranla (%38,50) hayır dediği görülmektedir.

Katılımcılardan “üniversitemizde siber güvenliğe ilişkin kurallar ve politikaların bulunduğu kılavuz mevcuttur” sorusuna 6 katılımcının evet, 9 katılımcının kısmen, 12 katılımcının fikrim yok ve 25 katılımcının en yüksek oranla (%48,10) hayır dediği görülmektedir.

Katılımcılardan “üniversitelerdeki iç denetim birimlerinde Bilgi Teknolojileri konusunda uzman personelin de çalışması gerekmektedir” sorusuna 3 katılımcının kısmen, 13 katılımcının hayır, 16 katılımcının fikrim yok ve 20 katılımcının en yüksek oranla (%38,50) evet dediği görülmektedir.

Katılımcılardan “son yıllarda siber güvenlik açısından iç denetimin rolü artmıştır” sorusuna 6 katılımcının kısmen, 10 katılımcının fikrim yok, 13 katılımcının hayır ve 23 katılımcının en yüksek oranla (%44,20) evet dediği görülmektedir.



SONUÇ VE ÖNERİLER

İç denetim organizasyonların işleyiş amaçlarını yerine getirirken hesap verme yükümlülüklerini eksiksiz yerine getirebilmek için önemli bir konum oluşturmaktadır. İç denetim ile üst yönetime raporlar hazırlanarak yönetim fonksiyonunun yerine getirilmesine yardımcı olunurken, güçlü ve stratejik kararların alınmasında da yol gösterici olunabilir. Organizasyonlar, verilerinin güven altında ve aynı zamanda ilgili kişiler tarafından ulaşılabilir olmasını istemektedir. Organizasyon verileri kurumsal hafızayı oluşturur.

Dijital çağın bütün nimetlerini kullanan organizasyonlar aynı zamanda bilgi teknolojilerinin olumsuz taraflarına da maruz kalırlar. Siber güvenlik açıkları, organizasyonları, önemli verilerin ve bütün sistemin ele geçirilmesi gibi bir sürü sorunla karşı karşıya bırakmaktadır. Bu sorunu gidermek için de iç denetim, BT ve siber güvenlik birlikte çalışmalıdır.

BT sistemleri ve araçları, süreçleri ve görevleri otomatikleştirerek, risk yönetimini ve iç kontrolleri iyileştirerek, organizasyonların yasalara, yönetmeliklere ve endüstri standartlarına uymasına yardımcı olarak iç denetime yardımcı olabilir. Yönetiminin kurumsal düzeyde almaları gereken siber güvenlik tedbirleri aşağıdaki gibi sıralanmıştır:

- Kurumlarda bilgi güvenliğini sağlamak için profesyonel bir ekip oluşturarak güvenli bir sistem kurulmalıdır.
- Oluşturulan ekip ile sistem yöneticilerinin sorumlu oldukları bilgi güvenliği ile ilgili gerekli eğitimlerin alınmasına destek olunmalı ve yaygın kabul gören güvenlik sertifikasyonlarının alınması sağlanmalıdır.
- Üniversitelerin ağları ve sistemlerine düzenli olarak denetimler yapılmalı ve saptanan eksiklerin giderilmesi adına faaliyete geçilmelidir.
- Sistemin yaptığı kayıtlar düzenli olarak incelenmeli ve saldırı tespiti için gerekli yazılımlar kullanılmalıdır.
- Antivirüs yazılımının etkin olarak kullanılması sağlanmalıdır.
- Üniversitedeki tüm bilgisayarlar merkezi bir antivirüs sunucu üzerinden güncellenmelidir.
- Kullanıcıların erişim hakları belirlenmelidir.

- Üniversite personeline düzenli aralıklarla sosyal mühendislik ve bilgi güvenliği bilinçlendirme eğitimleri verilmeli ve konferanslar ve toplantılar yapılmalıdır.
- Bilgi güvenliği, bilgi işlem, hukuk ve halkla ilişkiler birimleri koordineli çalışmalıdır.
- IP adreslerinin dağılımı, kullanıcı hesaplarının oluşturulması, ortak hesapların kullanımdan kaldırılması ve görevler ayrılığı prensibinin uygulanışı sık sık incelenmelidir.
- Kablosuz erişimlerin sağlandığı noktalar sürekli denetlenmelidir.
- Üniversitelerdeki Güvenlik Duvarı ve Saldırı Tespit Sistemi doğru yapılandırılmalıdır.
- Üniversitelerde yaşanabilecek hizmet kesintilerinden asgari düzeyde etkilenmek için gerekli önlemler alınmalıdır.
- Üniversitelerde yaşanan yoğun bilgi üretiminden dolayı, ulusal düzeyde siber güvenlik politikalarının oluşturulması için gerekli bilimsel ve teknolojik araştırma ve geliştirme proje ve programlarının oluşturulması adına öğretim elemanlarına ve öğrencilere destek olmalıdır.
- Üniversitelerde siber güvenlik uzmanlarının yetiştirilmesi için ilgili lisansüstü programlar geliştirilmelidir.
- Siber saldırılara karşı her kişi veya organizasyon gibi risk altında olan üniversiteler için özellikle üniversite yönetiminin durumun ciddiyetinin farkına varması ve gerekli tedbirleri alması gerekmektedir.

Araştırma, Türkiye’de devlet ve vakıf üniversitelerinde görev yapmakta olan iç denetçilerin gözünden üniversitelerde iç denetimin siber güvenlikteki etkinlik algısını ortaya koymak üzere nicel bir çalışma olarak yürütülmüştür. Araştırmanın verileri online anket aracılığıyla toplanmıştır. Toplanan verilerle analizlere başlanmıştır. 27 ifadeden oluşan ölçeğe yapılan açıklayıcı faktör analizi sonucunda beş faktör elde edilmiştir. Bu faktörler “İç Denetim ve Siber Güvenlik Algısı”, “Üniversite Yönetimi ve Siber Güvenlik Algısı”, “İç Denetim ve Siber Güvenlik Algısı”, “Siber Güvenlik Bilgi Düzeyi Algısı” ve “Siber Risk Yönetimi ve Siber Tehditler Algısı” olarak isimlendirilmiştir.

Elde edilen faktörler bağımlı değişkenler olarak alınarak fark testleri gerçekleştirilmiştir. Fark testleri sonucunda öğrenim durumu yüksek lisans olan

katılımcıların “Bilgi Güvenliği Denetlemesi Algısı” öğrenim durumu lisans olan katılımcılardan fazla olduğu tespit edilmiştir. Öğrenim durumu yüksek lisans olan katılımcıların “Üniversite Yönetimi ve Siber Güvenlik Algısı” öğrenim durumu lisans olan katılımcılardan fazla olduğu tespit edilmiştir. Yine öğrenim durumu yüksek lisans olan katılımcıların “Üniversite Yönetimi Ve Siber Güvenlik Algısı” öğrenim durumu doktora olan katılımcılardan fazla olduğu tespit edilmiştir. Öğrenim durumu yüksek lisans olan katılımcıların “İç Denetim ve Siber Güvenlik Algısı” öğrenim durumu doktora olan katılımcılardan fazla olduğu tespit edilmiştir. Öğrenim durumu yüksek lisans olan katılımcıların “Siber Güvenlik Bilgi Düzeyi Algısı” öğrenim durumu lisans olan katılımcılardan fazla olduğu tespit edilmiştir.

Katılımcıların, İç Denetçi olarak üniversitede çalıştıkları süre ile elde edilen beş faktör farklılaşmamaktadır. Yine katılımcıların iç denetçi olarak mesleki tecrübelerine göre iç denetimde siber güvenlik algıları farklılaşmamaktadır.

Katılımcıların Siber Güvenlik ve Bilgi Teknolojileri Konularında eğitim aldım ve yeterli bilgiye sahibim diyenlerin yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum diyenlere kıyasla “İç Denetim ve Siber Güvenlik Algısının” daha fazla olduğu tespit edilmiştir. Benzer şekilde eğitim aldım ancak kendimi çok yetkin olarak görmüyorum diyen katılımcıların da yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum diyen katılımcılara kıyasla “İç Denetim ve Siber Güvenlik Algısının” daha fazla olduğu söylenebilir.

Katılımcıların mevcut durumlarına değindiğimizde, siber güvenlikte üniversite yönetiminden genelde fikirlerinin olmadığı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi’nin Yayınladığı Bilgi Ve İletişim Güvenliği Rehberine Uygun Olarak Denetimlerin ve kontrollerin yapılmadığı söylenebilir. Yine katılımcıların Üniversitelerdeki İç Denetim Birimlerinde Bilgi Teknolojileri Konusunda Uzman Personelin de Çalışması Gerekmemektedir dediği ve siber güvenlik açısından iç denetimin rolünün arttığının farkında oldukları söylenebilir.

Uygulama neticesinde ‘Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının öğrenim durumlarına göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır’ olan H_1 hipotezi ve ‘İç denetçilerin siber güvenlik ve bilgi teknolojileri konularındaki bilgi düzeyine göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır’ olan H_4 hipotezleri kabul edilmiştir.

Yine uygulama neticesinde ‘Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının iç denetçi olarak üniversitede çalıştığı süreye göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır’ olan H₂ hipotezi ve ‘Türkiye’deki üniversitelerde görev yapmakta olan iç denetim elemanının mesleki deneyimine göre iç denetimde siber güvenlik algısı arasında anlamlı bir fark vardır’ olan H₃ hipotezleri reddedilmiştir.

Çalışmanın kısıtları göz önüne alındığında nitel araştırma yöntemleri ile desteklenmesi daha farklı sonuçlar ortaya koyabilecektir. Ayrıca çalışmanın ikinci ayağında sadece iç denetçilerle değil kurumlardaki bilgi işlem personelleriyle de görüşmeler yapılarak ölçek yeniden test edilebilir.

KAYNAKÇA

MAKALELER

- ABİDİN, N. H. Z. (2017). Factors Influencing the Implementation of Risk-Based Auditing. *Asian Review of Accounting*, 25(3), 361-375.
- ACAR, D., ÖZTÜRK, M. ve USUL, H. (2016). Dijital Ortamda Denetim: Sürekli Denetim. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Muhasebe Denetimi Özel Sayısı, 1561-1571. <https://dergipark.org.tr/en/pub/sduibfd/issue/53164/706430>
- AKÇAY, S. (2013). Türkiye’de İç Denetim Sürecinin Kamu Kurumlarının Faaliyet Sonuçları Üzerindeki Etkinliği: Belediyeler Üzerine Bir Uygulama. *Afyon Kocatepe Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*. 15(1), 57-77.
- AKMEŞE, S. (2020). Kamuda Dijital Dönüşümün Siber Güvenlik ve Dijital Güvence Boyutları ve İç Denetimin Rolü. *Denetişim*, 0(20), 108-119.
- AKSOĞAN, M., BAYER, H., GÜLADA, M. O. ve ÇELİK, E. (2018). İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği. *Kesit Akademi Dergisi*, (13), 271-288.
- AKYAZI, A. (2019). Mahremiyetin Dönüşümü: Ünlülerin Instagram Paylaşımları Üzerine Bir Araştırma. *Gaziantep University Journal of Social Sciences*, 18(1), 197-216. DOI:10.21547/jss.431086.
- AKYEL, R. (2010). Yönetimde İç Kontrol, İç Denetim Ve Dış Denetim Fonksiyonlarının Birbirleri İle İlişkileri Ve Türk Kamu Yönetiminde Uygulanmalarının Değerlendirilmesi. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 19(3), 1-21.
- ALBAHAR, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Sci Eng Ethics*. 25, 993–1006. <https://doi.org/10.1007/s11948-016-9864-0>
- ALDEMİR, C. ve KAYA, M. (2020). Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları, *Kamu Yönetimi ve Politikaları Dergisi*, 1(1), 6-27. <https://dergipark.org.tr/en/pub/kaypod/issue/56116/726431>.

- ALİUSTA, C. ve BENZER, R. (2018). Avrupa Siber Suçlar Sözleşmesi Ve Türkiye'nin Dahil Olma Süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), 35-42. DOI: 10.18640/ubgmd.512829.
- ALTUNTAŞ, E., KARA, E., SOYLU, A. B. ve KIRKBEŞOĞLU, E. (2018). Siber Sigortalar: Son Gelişmeler, Uygulamalar ve Sorunlar. *Bankacılık ve Sigortacılık Araştırmaları Dergisi*, (12), 8-22. <https://dergipark.org.tr/en/pub/bsad/issue/41804/393332>
- ASLAN, B. (2010). Bir Yönetim Fonksiyonu Olarak İç Denetim. *Sayıştay Dergisi*, (77), 63-86. <https://dergipark.org.tr/en/pub/sayistay/issue/61532/919029>
- AYDIN, S. K. (2021). Üniversitelerde İç Denetim ve Misyon Sorunu. *Ünye İktisadi ve İdari Bilimler Fakültesi Dergisi*, 4(2), 9-22. <https://dergipark.org.tr/en/pub/uiibfd/issue/66218/959212>
- BAYRAKÇI, E. ve DEMİREL, A. (2017). İç Denetimin Yapısal Ve İşlevsel Sorunlarının Türkiye'deki Üniversiteler Bağlamında Analizi. *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi*, 19(33), 52-60. DOI: 10.18493/kmusekad.400150
- BEZİRCİ, M., & KARASİOĞLU, F. (2011). Türkiye'de Denetimin Tarihsel Gelişimi. *Sosyal Ekonomik Araştırmalar Dergisi*, 11(21), 571-592. <https://dergipark.org.tr/en/pub/susead/issue/28414/302397>
- CENGİZ, S. (2013). İşletmelerde Kurumsal Yönetim Kapsamında İç Denetimin Yeri Ve Önemi: Borsa İstanbul'da Bir Araştırma. *Afyon Kocatepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 15(2), 403-448. <https://dergipark.org.tr/en/pub/akuiibfd/issue/1618/20271>
- ÇAKIR, H. ve ARINMIŞ UZUN, S. (2021). Türkiye'nin Siber Güvenlik Eylem Planlarının Değerlendirilmesi. *Ekonomi İşletme Siyaseti ve Uluslararası İlişkiler Dergisi*, 7(2), 353-379. <https://dergipark.org.tr/en/pub/kkujebpir/issue/67132/1007557>
- ÇEVİKBAŞ, R. (2011). Türkiye'de İç Denetim Kurumu. *Türk İdare Dergisi*, 83(471-472), 47-67.
- DEMİRBAŞ, M. (2005). İç Kontrol ve İç Denetim Faaliyetlerinin Kapsamında Meydana Gelen Değişimler, *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi*, 7, 167-188.

- DOLAN, E. ve WIDAYANTI, R. (2022). Implementation of Authentication Systems on Hotspot Network Users to Improve Computer Network Security. *International Journal of Cyber and IT Service Management*, 2(1), 88–94. <https://doi.org/10.34306/ijcitsm.v2i1.93>
- EFE, A. (2021). Yapay Zekâ Odaklı Siber Risk ve Güvenlik Yönetimi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 5(2), 144-165. DOI:10.33461/uybisbbd.972206
- ERENDOR, M. E. ve TAMER, G. (2018). The New Face Of The War: Cyber Warfare. *Cyberpolitik Journal*, 2(4), 57-74.
- EŞKAZAN, A. R. (2003), İç Denetimin Değişen Dünyasında İç Denetçiler. *İç Denetim Dergisi*, Kış, Sayı: 6, 32-33.
- GÖK, M. (2015). Türkiye’de Kamu İç Denetim Sistemi: Yapı Ve Performans Açısından Bir Değerlendirme. *Yönetim Ve Ekonomi Araştırmaları Dergisi*, 13(3), 482-502.
- GÖNEN, S. ve ÇELİK, M. (2005). Rekabet Üstünlüğü Sağlamada İç Denetim Ve İnsan Kaynakları Yönetiminin Stratejik Ortaklığı. *Ege Academic Review*, 5(1), 41-46.
- GÜLER, A. ve ARKIN, A. K. (2019). Siber Hijyenin Sağlanmasında İç Denetimin Rolü. *Denetişim*, (19), 17-40.
- GÜNGÖR, U. ve GÜNEY, O. (2017). Uluslararası İlişkilerde Güvenliğin Dönüşümü Çerçevesinde Bilgi Güvenliği ve Siber Savaş. *Karadeniz Araştırmaları*, 14(55), 131-146. <https://dergipark.org.tr/en/pub/karadearas/issue/68461/1069983>.
- GÜVEMLİ, B., ŞANLI, N., TORAMAN, C. ve YAZ, D. A. (2016). The Evolution Of The Auditing Profession In Turkey: The Union Of Chambers Of Cpa’s And Sworn-In Cpa’s (Turmob) History And Background. *Muhasebe Ve Finans Tarihi Araştırmaları Dergisi*, (11), 5-48. <https://dergipark.org.tr/en/pub/muftad/issue/30118/324939>.
- HEIRMAN, W. ve WALRAVE, M. (2008). Assessing Concerns And Issues About The Mediation Of Technology In Cyberbullying. *Cyberpsychology*, 2(2), 1-12.
- HOOS, F., MESSIER Jr, W. F., SMITH, J. L. ve TANDY, P. R. (2018). An Experimental Investigation Of The Interaction Effect Of Management Training Ground And Reporting Lines On Internal Auditors’ Objectivity. *International Journal of Auditing*, 22(2), 150-163.

- JOSHI, PL, DESHMUKH, A. ve AJMI, JA (2010). A Study Of Compliance With International Auditing Standards By Auditors In Bahrain. *International Journal of Applied Decision Sciences*, 3 (3), 259-279. <https://doi.org/10.1504/IJADS.2010.036102>.
- JUNG, K., ELING, M. ve JAEHUN, C. (2023). Spatial Loss Clusters and Socio-Economic Drivers of Cyber Risks. *SSRN*, <https://ssrn.com/abstract=4363817>.
- KALENDER, İ. (2008). Türk Kamu İdaresinin Yeni Yönetim ve Denetim Sistemleri. *Türk İdare Dergisi*, 87-103.
- KARAMAN, M. S., TURAN, M. ve AYDIN, M. A. (2020). Yapay Sinir Ağı Kullanılarak Anomali Tabanlı Saldırı Tespit Modeli Uygulaması. *Avrupa Bilim ve Teknoloji Dergisi*, Ejosat Ek Özel Sayı (HORA), 10-17. DOI: 10.31590/ejosat.1115825
- KARTAL, F. (2013). Türkiye’de Kamu Ve Özel Sektörde İç Denetim Uygulamaları. *Maliye Ve Finans Yazıları*, 1(99), 8-36. <https://dergipark.org.tr/en/pub/mfy/issue/16281/170764>.
- KIRAN, E. ve SOĞUKPINAR, İ. (2021). Kritik Altyapılarda Siber Risk Analizi ve Yönetimi. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi*, 14(1), 15-33. DOI: 10.54525/tbbmd.649913
- KOÇAK, S. Y. ve KAVAKOĞLU, T. (2010). İl Özel İdarelerinde İç Denetim Sisteminin Değerlendirilmesine İlişkin Bir Araştırma. *Sayıştay Dergisi*, (77), 119-148. <https://dergipark.org.tr/en/pub/sayistay/issue/61532/919040>.
- KORKMAZ, U. (2007). Kamuda İç Denetim. *Bütçe Dünyası Dergisi*, 2(25), 4-15.
- KORUCU, O. (2021). Yeni Normal Dünya Düzeninin Siber Güvenlik Ve Bilgi Güvenliğine Etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44-60. <https://dergipark.org.tr/en/pub/ybs/issue/63606/908082>.
- LIAO, H., RICHARD LIN, C., LIN, Y. ve TUNG, K. (2013). Intrusion Detection System: A Comprehensive Review. *Journal of Network and Computer Applications*, 36(1), 16-24. <https://doi.org/10.1016/j.jnca.2012.09.004>
- MEMİŞ, M. Ü. (2007). Türkiye’deki İç Denetim Profiline Belirlenmesine İlişkin Bir Araştırma. *Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 16(1), 461-478.
- MOLLAOĞULLARI, B. ve ÖNCÜ S. (2020). Denetim Komitesinin İç Denetim Birimi Çalışmalarına Etkisi: Türkiye’de İç Denetim Birimi Yöneticilerinin Algısı

- Araştırması. *Yönetim Ve Ekonomi: Celal Bayar Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*, 27(3), 405-424. DOI: 10.18657/yonveek.600904
- NISSENBAUM, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, 7, 61–73. <https://doi.org/10.1007/s10676-005-4582-3>
- ONAY, A. (2020). Yönetişim-Risk-Uygunluk Yru Yaklaşımı Açısından İç Denetim Fonksiyonunun Sorumlulukları ve İlişkili Taraflara İlişkin Bir Araştırma. *Muhasebe ve Denetime Bakış*, 19(59), 187-212.
- ÖZBİLGİN, İ. G. (2003). Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar. *Sayıştay Dergisi*, 49, 123-128.
- ÖZDOĞAN, B. ve ÖNCÜ S. (2016). Türkiye’de İç Denetim Mesleğinin Güncel Durumu: Bir Araştırma. *Yönetim Ve Ekonomi: Celal Bayar Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*, 23(1), 19-33. DOI: 10.18657/yecbu.50513.
- ÖZTÜRK, M. S. (2018). Siber Saldırıları, Siber Güvenlik Denetimleri Ve Bütüncül Bir Denetim Modeli Önerisi. *Journal of Accounting and Taxation Studies*, Special Issue of the 10th Year, 208-232. DOI: 10.29067/muvu.340848
- POLAT, D. (2020). NATO’nun Yeni Operasyon Alanı: Siber Uzay. *Güvenlik Bilimleri Dergisi*, Uluslararası Güvenlik Kongresi Özel Sayısı, 135-158. DOI: 10.28956/gbd.695973
- POLAT, K. (2016). Türkiye Büyük Millet Meclisinde İç Denetim Faaliyetleri. *Denetişim*, (14), 5-17. <https://dergipark.org.tr/en/pub/denetisim/issue/22467/240300>.
- RAIYN J. (2014). A Survey Of Cyber Attack Detection Strategies. *International Journal of Security and Its Applications*, 8(1):247–256
- SELİMOĞLU, S. K. ve SALDI, M. H. (2019). İşletmelerde Siber Risklerin Analizinde, Haritalanmasında ve Değerlendirilmesinde İç Denetimin Rolü. *Muhasebe ve Denetime Bakis*, 19(57).
- SELİMOĞLU, S. ve ALTUNEL, M. (2019). Siber Güvenlik Risklerinden Korunmada Köprü ve Katalizör Olarak İç Denetim. *Denetişim*, (19), 5-16. <https://dergipark.org.tr/en/pub/denetisim/issue/46331/585512>.
- SERTÇELİK, A. (2018). Siber Olaylar Ekseninde Siber Güvenliği Anlamak. *Medeniyet Araştırmaları Dergisi*, 2(3), 25-42. <https://dergipark.org.tr/en/pub/mad/issue/35779/443816>

- SHAH, S. ve MEHTRE, B.M. (2015). An Overview Of Vulnerability Assessment And Penetration Testing Techniques. *Journal of Computer Virology and Hacking Techniques* 11, 27–49. <https://doi.org/10.1007/s11416-014-0231-x>
- SLOBODIANYK, Y., SHYMON, S. ve ADAM, V. (2018). Compliance Auditing In Public Administration: Ukrainian Perspectives. *Baltic Journal of Economic Studies*, 4(5), 320-331.
- SOĞUKPINAR İ. ve KARABACAK B. (2005). ISRAM: Information Security Risk Analysis Method. *Computer & Security*, 24(2), 147-159. <https://doi.org/10.1016/j.cose.2004.07.004>.
- SPRAAKMAN, G. (2001). Internal Audit At The Historical Hudson's Bay Company: A Challenge To Accepted History. *Accounting Historians Journal*, 28(1), 19-41. <https://doi.org/10.2308/0148-4184.28.1.19>
- STRUPCZEWSKI, G. (2021). Defining Cyber Risk. *Safety Science*, 135, 105143. DOI: 10.1016/j.ssci.2020.105143
- ŞAFAK, E. (2020). Uluslararası Hukukta Değişen Güvenlik Algısı ve Saldırı Suçu Bağlamında Siber Saldırıları. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, 28(1), 127-160. DOI: 10.15337/suhfd.640029
- ŞENOL, M. (2017). Türkiye’de Siber Saldırlara Karşı Caydırıcılık. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3 (2), 1-9. DOI: 10.18640/ubgmd.373193
- TANER, E. ve KILIÇ, İ. (2019). Güvenlik Güçlerinin Bilgi Güvenliği Farkındalığını Belirlemeye Yönelik Bir Araştırma. *Güvenlik Bilimleri Dergisi*, 8(2), 253-269. DOI: 10.28956/gbd.646321.
- TAŞCI, U. ve CAN, A. (2015). Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 25 (2), 229-248. DOI: 10.18069/fusbed.25089
- TUFAN, M. ve GÖRÜN, M. (2013). Türkiye’deki Kamu İç Denetim Sisteminin Uluslararası İç Denetim Standartları Çerçevesinde İncelenmesi. *Sayıştay Dergisi*, (89), 115-135.
- TÜREDİ, H., ZOR, Ü. ve GÜRBÜZ, F. (2015). Risk Odaklı İç Denetim. *Muhasebe ve Finansman Dergisi*, (66), 1-20. DOI: 10.25095/mufad.396528

- TÜRK, B. ve ŞENYUVA, G. (2021). Şiddet Sarmalı İçinden Siber Zorbalık: Bir Gözden Geçirme. *İBAD Sosyal Bilimler Dergisi*, (10), 462-479. DOI: 10.21733/ibad.901032
- UYSAL, M. C. (2018). Kamu Kurumlarında Kurumsal Risk Yönetimi Ve Risk Odaklı İç Denetim: İç Denetçiler Üzerine Bir Araştırma-II. *Denetişim*, (18), 35-44. <https://dergipark.org.tr/en/pub/denetisim/issue/43464/530197>
- UZUN, A. K. (1998). İç Denetimin Toplam Kalite Yönetimindeki Yeri. *Mali Çözüm Dergisi*, 43, 19-23.
- ÜNLÜ, U. (2018). İnternet Bankacılığı Sisteminde Tüketicilerin Karşılaşacağı Olası Saldırıları Ve Çözüm Önerileri. *Bankacılar Dergisi*, 104, 82-96.
- VURAL, Y. ve SAĞIROĞLU, Ş. (2013). Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(2). <https://dergipark.org.tr/en/pub/gazimmfd/issue/6676/88512>.
- YILMAZ, O. (2018). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı Ve Siber Güvenlik. *Cyberpolitik Journal*, 2(4), 22-43. <https://dergipark.org.tr/en/pub/cyberj/issue/35147/389915>

KİTAPLAR

- ARCAGÖK, M. S., ERÜZ, E. (2006). *Kamu Mali Yönetimi ve Kontrol Sistemi*, İstanbul: Hesap Uzmanları Derneği Yayınları.
- CANGEMI, P. M. ve SINGLETON, T. (2003). *Managing The Audit Function: A Corporate Audit Department Procedures Guide*, 3. Baskı, New Jersey: John Wiley and Sons Inc.
- GRAMLING, A. A. ve RAMAMOORTI, S. (2003). *Research Opportunities In Internal Auditing*. Institute of Internal Auditors.
- GTAG, (2016). *Assessing Cybersecurity Risk: Roles of the Three Lines of Defense*, The Institute of Internal Auditors. <https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservice/s/downloadabledocuments/cybersecurity/gtag-assessing-cybersecurity-risk.pdf>, (Erişim Tarihi: 15.12.2022).
- HASANEFENDİOĞLU, B. (2020). *Yöneticinin E-Kitabı: 3 - BDDK ve Basel Bankacılık Komitesi Düzenlemelerine Göre 3'lü Savunma Hatı Modeli*, Technology Development Group, <https://technologydevelopmentgroup.net/contact/> (Erişim Tarihi: 13.03.2023).
- İÇ DENETİM KOORDİNASYON KURULU (2006). *İç Denetçilerin Çalışma Usul ve Esasları Hakkında Yönetmelik*, Ankara: İç Denetim Koordinasyon Kurulu Yayını.
- ÖZEREN, B. (1999). *İç Denetim Meslekleri Uygulama Standartları ve Yönlendiren İlkeler*, Ankara: Sayıştay Araştırma/İnceleme/Çeviri Dizisi: 3.
- PICKETT, K. S. (2010). *The Internal Auditing Handbook*. John Wiley & Sons.
- RID, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press, USA.
- SAĞIROĞLU, Ş. (2018). *Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık*. Ankara: Grafiker Yayınları.
- SARUHAN, Ş. C. ve ÖZDEMİRCİ, A. (2018). *Bilim, Felsefe ve Metodoloji*. 5. Baskı. İstanbul: Beta Basım Yayım Dağıtım A.Ş.

BİLDİRİLER

- ACAR, S. ve ZORAY, M. T. (2021). Ortadaki Adam Saldırısının Teknik Yönden İncelenmesi. *VII. Uluslararası TURKCESS Eğitim ve Sosyal Bilimler Kongresi*. (ss.278). Girne, Cyprus (KKTC).
- AHMETOĞLU H. ve DAŞ R. (2019). Derin Öğrenme İle Büyük Veri Kümelerinden Saldırı Türlerinin Sınıflandırılması. *Uluslararası Yapay Zekâ ve Veri İşleme Sempozyumu (IDAP)* (ss.1-9), Malatya, Türkiye. Doi: 10.1109/IDAP.2019.8875872.
- DUNCAN, B. ve WHITTINGTON, M. (2014). Compliance With Standards, Assurance And Audit: Does This Equal Security?. *In Proceedings of the 7th International Conference on Security of Information and Networks* (pp.77-84).
- LIANG, J. ve KIM, Y. (2022). Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall. *IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp.0752-0759), Las Vegas, NV, USA, doi: 10.1109/CCWC54503.2022.9720435.
- KARABACAK, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri. *Siber Güvenlik Çalıştayı*, Bilgi Güvenliği Derneği, 29 Eylül 2011.
- ROT, A. (2008). IT Risk Assessment: Quantitative And Qualitative Approach, *In Proceedings of the World Congress on Engineering and Computer Science (WCECS 2008)*, San Francisco, CA, USA, October 2008.
- UZAY, Ş. ve TANÇ, A. (2008). Internal Auditing in Turkey: The Historical Development. *In 12th World Congress Of Accounting Historians*. İstanbul.

TEZLER

- ABDİOĞLU, H. (2007). *İşletmelerde Kurumsal Yönetim Anlayışı Kapsamında İç Denetimin Rolü Ve İMKB-100 Örneği*. (Yayınlanmamış Doktora Tezi). İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.
- AKÖZ, B. C. (2018). *Türk Ceza Kanunu Kapsamında Bilişim Suç Ve Cezaları İle Örnek Yargısal Kararların Analizi Ve Mevzuat Önerileri*. (Yayınlanmamış Bilişim Uzmanlığı Tezi). Ankara: Bilgi Teknolojileri ve İletişim Kurumu. BTK Yayın No: 0255.
- BOZGEYİK, A. (2018). *Gaziantep'te Faaliyet Gösteren Orta Ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi*. (Yayınlanmamış Doktora Tezi). Gaziantep: Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü.
- CEYHAN, İ. F. (2010). *İç Denetim ve Kurumsallaşma*. (Yayınlanmamış Yüksek Lisans Tezi). Kırıkkale: Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü.
- ÇOTAK, A. (2019). *Sigortacılık Sektöründe Siber Güvenliği, Dünyada ve Türkiye'deki Gelişmelerin İncelenmesi*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul: Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü Anabilim Dalı.
- OCAK, H. S. (2021). *İç Denetimin Gelişen Ve Değişen Dünyasında Siber Güvenlik ve Denetim*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul: Marmara Üniversitesi.
- ÖZ, M. (2015). *Üniversitelerde İç Denetimin Etkinliğinin Arttırılmasına Yönelik Bir Alan Araştırması*. (Yayınlanmamış Yüksek Lisans Tezi). Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.
- ÖZER, A. (2008). *Risk Odaklı İç Denetim ve Bir Uygulama*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü.
- ÖZKAN, İ. (2011). *Güvenli Ağ Erişimi Ve Kimlik Doğrulama*. (Yayınlanmamış Yüksek Lisans Tezi). İstanbul: Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü.
- TOSUNOĞLU, B. (2010). *İç Denetimin İşletmelerin Yönetim Fonksiyonları Ve Performansları Üzerindeki Etkilerine Yönelik Bir Araştırma*. (Yayınlanmamış Yüksek Lisans Tezi). Tokat: Gaziosmanpaşa Üniversitesi Sosyal Bilimleri Enstitüsü.

ZORLU, M. (2014). *Kâr Amacı Gütmeyen Organizasyonlarda İç Kontrol Ve İç Denetim: Bir Devlet Üniversitesinde Uygulama*, (Yayınlanmamış Yüksek Lisans Tezi), Nevşehir: Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü.



İNTERNET KAYNAKLARI

- 2022 Yılında Bilgisayar Korsanları Fazla Mesai Yaptı! (2023), <https://www.haberturk.com/siber-saldirilar-1-milyonu-asti-3554879-teknoloji> (Erişim Tarihi: 02.03.2023).
- A Shortlist of Reported SCADA Incidents, (2009), <https://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/> Erişim Tarihi: 01.03.2023
- Ankara Emniyet Müdürlüğü'nü Hacklediler, (2012), <https://www.cnnturk.com/guncel/ankara-emniyet-mudurlugunu-hacklediler> (Erişim Tarihi: 03.03.2023)
- ARSLAN, R. (2015). “Türkiye’ye siber saldırının 10 günü: Ne oldu?”, https://www.bbc.com/turkce/haberler/2015/12/151224_siber_saldiri_arslan (Erişim Tarihi: 03.03.2023)
- Avustralya'da Bir Finans Şirketinin 330 Bin Müşterisinin Verileri Siber Saldırıyla Çalındı, (2023), <https://www.trthaber.com/haber/dunya/avustralyada-bir-finans-sirketinin-330-bin-musterisinin-verileri-siber-saldiriyla-calindi-754116.html> (Erişim Tarihi: 30.03.2023).
- BRUCE, S. (2017). “Internal Audit: Three Lines Of Defence Model Explained”, <https://www.icas.com/professional-resources/audit-and-assurance/internal-audit/internal-audit-three-lines-of-defence-model-explained> (Erişim tarihi: 18.03.2023).
- Cybersecurity Framework, <https://www.nist.gov/cyberframework> (Erişim Tarihi: 18.03.2023).
- History Of The IIA, <https://www.theiia.org/en/about-us/about-internal-audit/history-of-the-ii/>, (Erişim Tarihi: 01.03.2023). - a
- <https://www.mevzuat.gov.tr>. (Erişim Tarihi: 18.03.2023).
- Internal Auditing Standards: Why They Matter, <https://www.theiia.org/en/standards/why-standards-matter/>, (Erişim Tarihi: 08.03.2023). - b
- International Standards for the Professional Practice of Internal Auditing, <https://www.theiia.org/en/standards/what-are-the-standards/mandatory-guidance/standards/>, (Erişim Tarihi: 05.03.2023) - c

- IŞIK, İ. (2021). “İç Denetçi Nedir? Ne İş Yapar?”, <https://www.iienstitu.com/blog/ic-denetci> (Erişim Tarihi: 21.03.2023).
- İç Denetim Birimi Başkanlığı, İç Denetimin Tarihsel Gelişimi, <https://www.icisleri.gov.tr/icdenetim/ic-denetimin-tarihsel-gelisimi>, (Erişim Tarihi: 01.03.2023).
- İç Denetim*, <https://www.hmb.gov.tr/ic-denetim-nedir>, (Erişim Tarihi: 24.12.2022).
- KARAKUŞ, C. (2011). “Sayısal Haberleşme Teknikleri ve Ağ Teknolojileri”, <http://www.ckk.com.tr/ders/communication.pdf> (Erişim Tarihi: 01.03.2023)
- KVKK, *Bazı N11.com Müşterilerinin Eposta Adresinin Ele Geçirildiğini Duyurdu*, (2019). <https://www.memurlar.net/haber/875838/kvkk-bazi-n11-com-musterilerinin-eposta-adresinin-ele-gecirildigini-duyurdu.html> (Erişim Tarihi: 21.03.2023).
- QUINN, S., IVY, N., BARRETT, M., WITTE, G. ve GARDNER, R. (2022). “Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight”, <https://csrc.nist.gov/publications/detail/nistir/8286c/final> (Erişim Tarihi: 03.03.2023)
- Redhack Bu Kez TBMM'yi Hackledi*, (2014), <https://www.odatv4.com/guncel/redhack-bu-kez-tbmmyi-hackledi-1001141200-51300> (Erişim Tarihi: 21.03.2023).
- Redhack Demirören'i Hackledi*, (2018), <https://www.odatv4.com/guncel/redhack-demiroreni-hackledi-25031855-135591> (Erişim Tarihi: 21.03.2023).
- Siber Güvenlik Tehdit Kategorileri ve Yeni Nesil Siber Suçlar*, (2021). <https://cyberartspro.com/siber-guvenlik-tehdit-kategorileri-ve-yeni-nesil-siber-suclar/> (Erişim Tarihi: 03.03.2023)
- Siber Suç Nedir?* (2019), <https://www.egm.gov.tr/siber/sibersucnedir> (Erişim Tarihi: 02.03.2023).
- Siber Uzay*, (2020). https://tr.wikipedia.org/wiki/Siber_uzay - a (Erişim Tarihi: 03.03.2023)
- Siber*. (2022). <https://tr.wikipedia.org/wiki/Siber> - b (Erişim Tarihi: 03.03.2023)
- Sigortamedya, (2019). “Siber Risk’ler Sigortacıların Radarına Girdi”, <https://www.sigortamedya.com.tr/siber-riskler-sigortacilarin-radarina-girdi-2/> (Erişim Tarihi: 25.02.2023)

- Solar Sunrise*, <https://www.globalsecurity.org/military/ops/solar-sunrise.htm> (Erişim Tarihi: 02.03.2023).
- Teknoloji Çağı Ve Son 10 Yılın Siber Saldırıları*, (2021). <https://rasyotek.com.tr/blog/teknoloji-cagi-ve-son-10-yilin-siber-saldirilari/> (Erişim Tarihi: 03.03.2023)
- The History of ECIIA*, <https://www.eciia.eu/the-history-of-eciia/>, (Erişim Tarihi: 02.03.2023).
- The IPPF: The Framework for Internal Audit Effectiveness*, <https://www.theiia.org/en/standards/international-professional-practices-framework/>, (Erişim Tarihi: 09.03.2023). - d
- THY'nin Resmi Sitesi Hacklendi*, (2014), <https://www.cnnturk.com/teknoloji/thynin-resmi-sitesi-hacklendi> (Erişim Tarihi: 03.03.2023)
- TRT Çocuk Hacklendi!*, (2018), <https://www.cybermagonline.com/trt-cocuk-hacklendi> (Erişim Tarihi: 03.03.2023)
- TSUKAYAMA, H., TIMBERG, C. ve FUNG, B. (2016). “Yahoo Data Breach Casts ‘Cloud’ Over Verizon Deal”, <https://www.washingtonpost.com/news/the-switch/wp/2016/09/22/report-yahoo-to-confirm-data-breach-affecting-hundreds-of-millions-of-accounts/?noredirect=on> (Erişim Tarihi: 01.12.2022)
- Turkcell'e Yapılan Siber Saldırıda Hacker Şoku*, (2014), haberler.com/teknoloji/turkcell-e-yapilan-siber-saldirida-hacker-soku-6787638-haberi/ (Erişim Tarihi: 24.12.2022).
- Türkiye İç Denetim Enstitüsü 2021 Faaliyet Raporu*, (2021), <https://www.tide.org.tr/file/documents/pdf>, (Erişim Tarihi: 03.03.2023). - b
- Türkiye İç Denetim Enstitüsü*, <https://tide.org.tr/page/1/Hakkimizda>, (Erişim Tarihi: 03.03.2023). - a
- VARLIK, E. (2016a). “Asimetrik Savaş Ve Siber Silahlar”, <https://siberbulten.com/stratejik-siber-guvenlik-ders-notlari/asimetrik-savas-ve-siber-silahlar/> (Erişim Tarihi: 15.02.2023)
- VARLIK, E. (2016b). “‘Basın Bülteniyle Borsa Vurguncusu’ Hacker Hakim Karşısında”, <https://siberbulten.com/siber-guvenlik/basin-bulteniyle-borsa-vurguncusu-hacker-hakim-karsisinda/> (Erişim Tarihi: 15.02.2023)

WannaCry fidye yazılımı nedir?, <https://www.kaspersky.com.tr/resource-center/threats/ransomware-wannacry> (Eriřim Tarihi: 21.02.2023).



RAPORLAR

- BACE R., MELL P. “Intrusion detection systems, National Institute of Standards and Technology (NIST)”, *Technical Report 800-31*, 2001.
<http://cs.uccs.edu/~cchow/pub/ids/NISTsp800-31.pdf>
- ECIIA- Avrupa İç Denetim Enstitüleri Konfederasyonu, *Avrupa’da İç Denetim Durum Raporu*, Şubat-2005.
- Gebze İleri Teknoloji Enstitüsü İç Denetim Birimi, *İç Denetim*,
https://www.academia.edu/download/57856556/GYTE_IC_DENETIM_SUNU_MU2.pdf, 2008. (Erişim Tarihi: 25.10.2022).
- Marsh ve Tusiad, *2020 Türkiye Siber Risk Algı Araştırması*
https://tusiad.org/tr/yayinlar/raporlar/item/download/9428_0ff86134737e19b44a7425cb059f44f8, 2020. (Erişim Tarihi: 25.12.2022).
- Saudi Arabian Monetary Authority (SAMA), *Cyber Security Framework*: <https://kr-labs.com.ua/books/SAMA%20Cyber%20Security%20Framework.pdf>, 2017. (Erişim Tarihi: 21.03.2023).
- Symantec, *Internet Security Threat Report*, <https://docs.broadcom.com/doc/istr-21-2016-en>, 2016. (Erişim Tarihi: 12.01.2023).

EKLER

EK 1: İç Denetimin Siber Güvenlikteki Etkinliği Üzerine Etkisi: İç Denetçilerin Algıları Anket Formu

Sayın İlgili;

Bu anket formu Tokat Gaziosmanpaşa Üniversitesi Lisansüstü Eğitim Enstitüsü İşletme Anabilim Dalı Muhasebe Finansman Programında yürütülmekte olan yüksek lisans tez çalışması için yapılmaktadır. Sizlerden edinilecek bilgiler tamamen bilimsel amaçlı olarak kullanılacaktır. Katkılarınız bizim için önemlidir. Şimdiden değerli katkılarınızdan dolayı teşekkür ederiz.

Doç. Dr. Mihriban COŞKUN ARSLAN

Ebru TÜZEMEN

BÖLÜM 1: MEVCUT DURUM

Lütfen aşağıda yer alan ifadelere katılım düzeyinizi belirtiniz.

No	İfadeler	Evet	Hayır	Kısmen	Fikrim Yok
1	Siber güvenliğe ilişkin önemli varlık grupları belirlenmiştir.				
2	Siber güvenliğe ilişkin önemli varlık gruplarının kritiklik derecesi belirlenmiştir.				
3	Siber güvenliğe ilişkin önemli varlık gruplarının mevcut durum ve boşluk analizleri yapılmıştır.				
4	Siber güvenliğe ilişkin önemli varlık grupları ile ilgili neler yapılacağına ait rehber uygulama yol haritası belirlenmiştir.				
5	Siber güvenliğe ilişkin önemli varlık gruplarının değişimi söz konusu olduğunda değişiklikler rehberine uygun olarak yönetilmektedir.				
6	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayınladığı Bilgi ve İletişim Güvenliği Rehberine uygun olarak denetimler yapılmaktadır.				
7	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin yayınladığı Bilgi ve İletişim Güvenliği Rehberi yol haritasının izlemesi ve kontrolü yapılmaktadır.				
8	Üniversitemizde siber güvenliğe ilişkin kurallar ve politikaların bulunduğu kılavuz mevcuttur.				
9	Üniversitelerdeki iç denetim birimlerinde Bilgi Teknolojileri konusunda uzman personelin de çalışması gerekmektedir.				
10	Son yıllarda siber güvenlik açısından iç denetimin rolünün artmıştır.				

BÖLÜM 2: DEĞERLENDİRME

Lütfen aşağıda yer alan ifadelere katılım düzeyinizi belirtiniz.

(1: Kesinlikle Katılmıyorum 2: Katılmıyorum 3: Ne Katılıyorum Ne Katılmıyorum 4: Katılıyorum 5: Kesinlikle Katılıyorum)

No	İfadeler	1	2	3	4	5
1	Üniversite yönetimi siber güvenlik konusunun önemine inanmaktadır.					
2	Üniversite yönetiminin siber güvenlik konusundaki beklentileri son yıllarda artış göstermiştir.					
3	Üniversite yönetimi siber güvenlik konusunda proaktif yaklaşım sergilemektedir.					

4	Üniversite yönetimi tarafından siber güvenlik konusunda yeterince kaynak aktarımı yapılmaktadır.					
5	Üniversite yönetimi siber güvenlik konusunda ilgili personellerle düzenli iletişim kurmaktadır.					
6	Üniversitede tüm çalışanlara düzenli olarak bilgi güvenliği ve siber güvenlik eğitimleri verilmektedir.					
7	Üniversitede tüm çalışanlar siber güvenliğe ilişkin yükümlülüklerini tam olarak bilmektedir.					
8	Üniversitede siber güvenliğe yönelik kurum kültürü gelişmiştir.					
9	Üniversitede, siber riskler ve bu risklere yönelik alınan siber güvenlik önlemleri önemsenmektedir.					
10	İç denetim personeli üniversitedeki bilgi işlem faaliyetleri hakkındaki yeterli bilgi sahibidir.					
11	İç denetim personeli ile bilgi güvenliği personeli ya da bilgi işlem personeli arasında yardımlaşma vardır.					
12	İç denetim birimi siber güvenlik konusunda yeterince bilgi sahibidir.					
13	İç denetim birimi siber güvenlik konusundaki güncel konuları takip eder.					
14	İç denetim birimi siber güvenlik konusundaki eksiklikleri belirler ve raporlar.					
15	İç denetim birimi üniversitedeki siber güvenlik uygulamalarına katkı sağlar.					
16	İç denetim birimi siber güvenlik konusunda daha fazla sorumluluk almalıdır.					
17	İç denetim birimi siber güvenlik denetlemelerinde iş planı ve acil durum planlarını kontrol eder.					
18	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde kimlik ve erişim yöntemleri kontrol edilir.					
19	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde sistem izlemesi yapılır.					
20	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde güvenlik duvarı incelenir.					
21	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde ağa bağlanan cihazlar incelenir.					
22	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde şifreleme ilkeleri kontrol edilir.					
23	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde yedekleme prosedürleri kontrol edilir.					
24	İç denetim birimi tarafından yapılan bilgi güvenliği denetlemelerinde genel güvenlik protokollerine uygunluk kontrol edilir.					
25	Siber risk yönetimi ile ilgili olarak siber tehditleri değerlendirme ve ölçme konusunda üniversitenin uygulamalarını yeterli buluyorum.					
26	Siber risk yönetimi ile ilgili olarak siber saldırıları önleme konusunda üniversitenin uygulamalarını yeterli buluyorum.					
27	Siber risk yönetimi ile ilgili olarak siber saldırılara müdahale etme konusunda üniversitenin uygulamalarını yeterli buluyorum.					

BÖLÜM 3: BİLGİLER

Lütfen size uygun cevabı işaretleyiniz.

1) Üniversiteniz;

Devlet Üniversitesi () Vakıf Üniversitesi ()

2) Cinsiyet:

Kadın () Erkek ()

3) Yaş:

25 ve altı () 26-35 () 36-45 () 46-55 () 56 ve üstü ()

4) Öğrenim Durumu:

Lisans () Yüksek Lisans () Doktora ()

5) İç Denetçi Olarak Üniversitede Çalışılan Süre:

1-5 yıl () 6-10 yıl () 11-15 yıl () 16-20 yıl () 21-25 yıl () 25 yıl ve üstü ()

6) İç Denetçi Olarak Mesleki Tecrübeniz:

1-5 yıl () 6-10 yıl () 11-15 yıl () 16-20 yıl () 21-25 yıl () 25 yıl ve üstü ()

7) Siber Güvenlik ve Bilgi Teknolojileri konularında;

Eğitim aldım ve yeterli bilgiye sahibim ()

Eğitim aldım ancak kendimi çok yetkin olarak görmüyorum ()

Yeterli bilgimin ve tecrübemin olduğunu düşünmüyorum ()

8) Alınan Mesleki Sertifikasyonlar;

CPA (Sertifikalı Kamu Denetçisi) ()

CIA (Sertifikalı İç Denetçi) ()

Diğer

Yok ()

9) Varsa sertifika Dereceniz hangisidir;

A1 () A2 () A3 () A4 ()

10) İç Denetimde çalışan personel sayısı:.....**11) Siber Güvenlik konularında üniversitemiz;**

Hizmet satın almaktadır. ()

Dışarıdan danışmanlık almaktadır. ()

Kendi departmanı bulunmaktadır. ()

12) Bilgi güvenliğinden sorumlu personel;

Bilgi İşlem Daire Başkanlığında çalışmaktadır. ()

İç Denetim Birimi Başkanlığında çalışmaktadır. ()

Diğer

13) Bilgi güvenliğinden sorumlu personel sayısı:.....**14) İç denetim birimi, siber güvenlik süreçlerini ve kontrollerini değerlendirebilecek yetkinlikte mi?**

Evet () Hayır () Kısmen ()

15) Son bir yıl içerisinde siber güvenlik ile ilgili konular üniversite yönetim kurulunda gündem olarak yer aldı mı?

Bir defa gündem olarak konuşuldu ()

Birkaç toplantıda gündem olarak konuşuldu ()

Sık sık toplantılarda gündem olarak konuşuldu ()

Bütün toplantılarda gündem olarak konuşuldu ()

Hiç gündeme alınmadı ()

16) İç denetim birimi tarafından üniversitenin karşı karşıya gelebileceği yaygın siber tehditler (ör. suçlular, bilgisayar korsanları, ağa bağlı sistemler, bulut sağlayıcıları, tedarikçiler, sosyal medya sistemleri, kötü amaçlı yazılım) belirlendi mi?

Evet () Hayır () Kısmen ()

17) Yukarıdaki soruya evet veya kısmen cevabı vermişseniz bu soruya cevap veriniz.

Belirlenen siber tehditler iç denetim risk değerlendirme ve planlama süreçlerine dahil edildi mi?

Evet () Hayır () Kısmen ()

18) Siber risk yönetimi açısından üniversitenin yaşadığı en büyük zorlukları önem derecesine göre sıralayınız.

() Nitelikli bir siber güvenlik uzmanının işe alınmasının zor olması.

() Kurumda standart/ortak bir siber risk yönetim anlayışı olmaması.

() Sektörel ve operasyonel olarak siber tehditlerin neler olduğuna yönelik yönetim seviyesinde bir takip ve farkındalık olmaması.

() Çalışanlara bilgi güvenliği konusunda eğitim verilmemesi.

() Kurumun bu konuya yeterli bütçe ayırmaması/yatırım yapılmaması.

() Yeni siber tehditlere karşı önlem alınmaması.

() Kurumda siber güvenlik konusunun net bir sahibinin olmaması

EK 2: Etik Kurul Kararı

T.C.
TOKAT GAZİOSMANPAŞA ÜNİVERSİTESİ
SOSYAL VE BEŞERİ BİLİMLER ARAŞTIRMALARI
ETİK KURULU KARARLARI

KARAR TARİHİ	OTURUM NO	KARAR SAYISI
16.12.2021	26	01-11

Üniversitemiz Sosyal ve Beşeri Bilimler Araştırmaları Etik Kurulu Başkan Prof. Dr. Eren YÜRÜDÜR Başkanlığında toplandı.

KARAR 26.04- Lisansüstü Eğitim Enstitüsü Müdürlüğünün 03.12.2021 tarih ve 105327 sayılı yazısı görüşüldü.

Aşağıda bilgileri yer alan araştırmacıların yapmak istediği uygulamaların ve kullanacağı veri toplama araçlarının etik açıdan uygunluğuna oy birliği ile karar verildi.

ÇALIŞMANIN TÜRÜ	Yüksek Lisans Tezi
BAŞLIK	İç Denetimin Siber Güvenlikteki Etkinliği Üzerine Etkisi: İç Denetçilerin Algıları
TEZ YÜRÜTÜCÜSÜ/ YAZARI	Ebru TÜZEMEN (İşletme Anabilim Dalı)
RAPORTÖR GÖRÜŞÜ	OLUMLU

Prof. Dr. Eren YÜRÜDÜR
Etik Kurul Başkanı
(İmza)

Doç. Dr. Mehmet KARGÜN
Başkan Yardımcısı
(İmza)

Prof. Dr. Mehmet Serkan UMUZDAŞ
Üye
(İmza)

Doç. Dr. Emine ÖĞÜK
Üye
(İmza)

Doç. Dr. Yücel EROL
Üye
(İmza)

Doç. Dr. Fatih YAZICI
Üye
(İmza)

Dr. Öğr. Üyesi Şevki BABACAN
Üye
(İmza)