SİBER GÜVENLİK RİSKLERİNİN VE COVID-19 SALGININ UZAKTAN DENETİM ÜZERİNDEKİ ETKİLERİ

(THE EFFECTS OF CYBER SECURITY RISKS AND COVID-19 OUTBREAK ON REMOTE AUDITING)

Mehmet ATAKAN*

ÖZ

Teknolojik gelişmeler ve küreselleşme, dünya genelinde bir çok sistemi entegre hale getirmiş bulunmaktadır. Bu süreçte bilgi kaynaklarının da bağlantılı hale gelmesi, birçok ülkede hizmetlerin siber ortamda sunulması gibi hususlar, güvenlik algısı ve anlayışının değişmesine sebebiyet vermiştir. Siber risklerin ve tehdit faaliyetlerinin, söz konusu değişimin etkisiyle arttığı açıkça görülmektedir. Günümüzde devletler ve şirketler artık sanal alanda da tehdit edilebilmektedir. Bu nedenle siber güvenliğe olan ilgi her geçen gün artarken, dünyada siber politikalar artık daha karmaşık bir hal almıştır. Siber güvenlik alanında yenilikleri doğru okuyabilmeyi ve gerekli güvenlik politikaları oluşturabilmeyi başarabilmek, siber alanda doğru strateji oluşturma noktasında olumlu bir etki yapacaktır. Bütün bu parametrelerin etkisiyle, dünya genelinde yeni yönetim ve denetim tekniklerinin yanı sıra denetimde etkililiğin ve yaygınlığın sağlanabilmesi için uzaktan denetimin daha fazla tercih edilmeye başlandığı bir sürece girilmektedir. Ayrıca, tüm dünyada etkisini gösteren COVİD-19 salgınının teknolojik gelişmeleri hızlandıracağı ve siber güvenlik politikaları üzerinde de etkili olacağı düşünüldüğünde, siber güvenliğe ilişkin denetimlerin yaygın ve etkili şekilde gerçekleştirilebilmesi önem kazanmaktadır.

Bu makalede, siber güvenlik, siber tehdit ve siber saldırı gibi alanlarda COVİD-19 salgını etkisiyle görülen gelişmeler ile bunlara ilişkin olumsuzlukları kontrol etmek üzere ön plana çıkan "uzaktan denetim" alanında beklenen değişimler anlatılmaya çalışılmaktadır.

Anahtar Kelimeler: Siber Güvenlik, Siber Güvenlik Riski, Siber Güvenlik Denetimi, Uzaktan Denetim, Covid-19

JEL Kodları: M42, D81

ABSTRACT

Technological developments and globalization have integrated many systems around the world. In this process, issues such as the connection of information sources and the provision of services in cyberspace in many countries have caused a change in security perception and understanding. It is clearly seen that cyber risks and threat activities have increased with the effect of this change. Nowadays, states and companies can be threatened in virtual space. Therefore, while the interest in cyber security increases day by day, cyber policies in the world have become more complex. Being able to read the innovations in the field of cyber security correctly and to create the necessary security policies will have a positive effect on creating the right strategy in the cyber field. With the effect of all these parameters, a period in which remote auditing is becoming more preferred is being entered in order to ensure effectiveness and prevalence in auditing as well as new management and auditing techniques worldwide. In addition, considering that the COVID-19 epidemic, which has an impact all over the world, will accelerate technological developments and will have an impact on cyber security policies, it is important to carry out widespread and effective cyber security inspections.

This article tries to explain the developments in areas such as cyber security, cyber threat and cyber attack with the effect of the COVID-19 outbreak and the expected changes in the field of "remote auditing ", which has come to the fore in order to control the negativities related to them.

Keywords: *Cyber Security, Cyber Security Risk, Cyber Security Auditing, Remote Auditing, Covid-19*

JEL Classification: *M42, D81*

* İç Denetçi/Müfettiş, PTT A.Ş. Genel Müdürlüğü, Ankara, Orcid Id: 0000-0003-0329-0624, mehmet.atakan@ptt.gov.tr,
Yazı Gönderim Tarihi: 26.05.2020, Yazı Kabul Tarihi: 14.10.2020

1. GİRİŞ

Bilgi teknolojilerindeki hızlı ilerlemeye bağlı olarak, bilgisayarlar ve internet alanındaki yenilikler yaşamın bir parçası haline gelmiştir. Teknolojideki bu hızlı gelişmeler, insan hayatını değiştirmenin yanı sıra siber alanda büyük ilerlemelere neden olmuştur. Özellikle internet kullanımı yaşam tarzını da değiştirmiş olup, siber alanda tüm kesimler üzerinde birçok açıdan etkisini göstermiş ve alışkanlıkların değişimine neden olmuştur.

Öte yandan, siber alanda yaşanan ilerlemeler bilginin niteliğini de değiştirmiş ve bilgi siber ortamın en temel metalarından biri haline gelmiştir. Bilginin çoğaltılması, erişilmesi ve paylaşılması siber ortamın yaygınlaşmasıyla beraber oldukça kolay hale gelmiştir. Fakat her dönemde değerli olan bilginin günümüzde elektronik hale gelmesi ve bilişim sistemleri ile yoğun bir şekilde paylaşılması, maruz kaldığı riskleri artırmakta ve bilgi güvenliği kavramına yeni bir boyut kazandırmaktadır. Bir taraftan her türlü bilgiye erişim konusunda sınırların, mesafelerin, mekân ve zaman kısıtlamalarının ortadan kalktığı bir ortam oluşurken, buna karşın bilginin güvenliğini sağlamak zorlaşmakta, bilginin bulunduğu ve iletildiği siber ortam güvenliği de giderek önem kazanmaktadır (Bayraktar, 2015).

Bilgi teknolojilerinde meydana gelen gelişmeler ve siber alanda oluşan yenilikler, 2020 yılı itibari ile hayatımızda yer edinen COVID-19 ile birlikte yaşam tarzlarını değişime uğratmış ve yeni bir düzen oluşmaya başlamış bulunmaktadır. COVID-19 salgınının dünya üzerinde olumsuz etkileri devam etmekte ve yaşamın her alanında yeniden alışkanlıkların değişimine neden olacağı anlaşılmaktadır. Yaşam tarzının değişimi teknolojik değişimler ile beraber siber alanın da toplum hayatı üzerinde etkisini giderek artırmaktadır. Bu bağlamda, yönetim ve denetim tekniklerinde de değişiklikler görülmekte, denetim yöntemi olarak özel sektörün öncülüğünü yaptığı ve kamu kesiminde de son yıllarda giderek önemli bir yere sahip olan uzaktan denetimin bu dönemde bilgi güvenliği ve siber alanda karar alma süreçlerinin vazgeçilmez bir parçası olacağı anlaşılmaktadır. Bu çalışmada, siber güvenlikle ilgili gelişmeler analiz edilerek, COVID- 19 ile birlikte denetim tekniklerinde ve özellikle uzaktan denetim üzerinde oluşturduğu etkiler üzerinde durulmaktadır. Konuyla ilgili literetür taraması yöntemi ile derlenen bilgiler değerlendirilerek, içinde bulunulan süreçte uzaktan denetim fonksiyonunda ortaya çıkan ve/veya ortaya çıkması beklenen değişimler belirlenmeye çalışılmıştır.

2. KAVRAMSAL ÇERÇEVE

Bilgi teknolojileri alanındaki gelişmeler birey dahil şirket, kuruluşlar ve devlet üzerinde etkileri yadsınamayacak kadar yer edinmiştir. Bu alandaki gelişmeler hem olumlu hem olumsuz anlamda birçok değişimi de beraberinde getirmiştir. Teknolojik anlamda gelişmeler tüm toplum üzerinde değiştirici ve dönüştürücü bir rol oynamıştır ve tüm unsurlar bundan etkilenmiştir.

Özellikle elektronik ticaret (e-ticaret) ve sosyal medya ağları, internet kullanıcılarının en fazla rağbet gösterdiği kullanım alanlarının başında gelmektedir. Küresel e-ticaret hacmi 2017 yılında bir önceki yıla göre 400 milyar dolar artış göstererek 2,3 trilyon dolara yükselmiş olup, bu rakamın 2021 yılında 4,5 trilyon dolar seviyesine ulaşması beklenmektedir (Orendorff, 2017). Çin 682 milyar dolar ile en büyük e-ticaret pazarına sahiptir. Çin'in ardından 438 milyar dolar ile ABD ve 196 milyar dolar ile de İngiltere gelmektedir (Ecommerce Foundation, 2017). E-ticaret yoluyla gerçekleştirilen satışların toplam satışlar içerisindeki payının en yüksek olduğu ülke ise İngiltere'dir. Bu ülkede tüm satışların %23'ü internet üzerinden gerçekleşirken, Almanya %11,7 ile ikinci ve Avustralya da %8,9 ile üçüncü sırada yer almaktadır (BCG, 2016, s. 9).

Bunların yanı sıra finansal işlemler, bilgi paylaşımı, eğlence, reklamcılık, haber, araştırma vb. birçok alanda da internet teknolojilerinden yoğun bir şekilde yararlanılmasına bağlı olarak, internetin ekonomi içerisindeki payı gün geçtikçe büyümektedir. İnternete dayalı ekonomik faaliyetlerin GSYİH içerisindeki payı 2010-2016 yılları arasında gelişmiş ülkelerde %4,3'ten %5,5'e, gelişmekte olan ülkelerde de %3,6'dan %4,9'a yükselmiştir. (BCG, 2016: 8-9).

Hal böyle olunca, günümüzde bilgi teknolojileri sürecinin değiştirici ve dönüştürücü özelliklerinin yadsı-

namaz gerçekliği ile birlikte siber alandaki gelişmeler de bu değiştirici ve dönüştürücü özelliklerin bir parçası olmuştur. Özellikle siber güvenlik konusu tüm alanlarda etkisini fazlaca hissettirmeye başlamıştır. Siber güvenlik alanında meydana gelen bu gelişmeler, özellikle özel ve kamu kuruluşlarının yanı sıra devletler açısında da oluşabilecek risklerin önceden tespiti ve bu risklere karşı alınabilecek tedbirlerin belirlenmesi hususunda denetim olgusunu hayati önem noktasına getirmiştir. Diğer taraftan, tüm dünyayı saran COVID-19 salgını ile birlikte çalışma şartları dahil birçok alanda değişim başlamıştır ve bu durum uzaktan denetim üzerinde de olumlu bir etki göstereceğe benzemektedir.

Çalışmanın ilerleyen bölümlerinde uzaktan denetim tekniğinin gelişimine yol açan, siber uzay, siber tehditler, siber güvenlik, bilgi güvenliği kavramlarının ve COVID-19 etkeninin açıklanmasında yarar görülmektedir.

2.1. Siber Uzay

Siber uzay; bilgisayar ağları ve bu ağlar vasıtasıyla ulaşılabilen her türlü veri kaynağını kapsayan alan olarak tanımlanmaktadır (Karaçay, 2017).

Siber uzay ya da siber ortam genellikle internetle birlikte ve bağlantılı bir kavram olarak düşünülse de siber uzay internetten çok daha fazlasını ifade etmektedir. Çünkü gerçek dünyada meydana gelmesi mümkün olmayan bir işlem, siber uzayda meydana gelebilir. Örneğin basit bir çipteki hesaplama dahi bir siber uzay olayıdır ki bunun yapılması sırasında herhangi bir internet bağlantısı da gerekmemektedir (Fentz,.2005). Siber uzay, insanoğlunun ortak bir mirasıdır ancak; ne yazık ki, bazı kişilerin bu ortak mirası kötü olarak kullanmaları sebebiyle siber uzay artık farklı bir suç ortamı haline gelmiştir. Siber güvenlikle ilgili her türlü riskin tanımlanmasına zemin hazırlayan bir ortamı ifade etmesi dolayısıyla siber uzay konumuz açısından önemli bir kavramdır.

2.2. Siber Tehdit

Siber tehdit, kişisel ve kurumsal verilerin gizliliğini yasal olmayan yöntemlerle aşarak bunlara ulaşmak veya tahrip etmek amacıyla yapılan her türlü siber saldırı ve saldırı girişiminin genel adıdır. Siber tehditlere örnek olarak; sunucu web servis hizmetlerini durdurma, virüsler veya trojanler sayılabilir (Şahinaslan, 2003).

Gelişen bilişim sistemleriyle beraber hem devlet hem de devlet dışı aktörler için yeni tehditler ortaya çıkmaktadır ki bu tehditlerin soyut alandan geliyor olması, tespit edilebilme özelliğinin az olması gibi etkenler, tehditlerin sonuçları açısından bir öngörülmezlik durumunu doğurmaktadır. Bir diğer taraftan bu tehditlerin merkezi bir yapıya sahip olmaması da belirsizliğini arttırmaktadır. Bu anlamda tehdidin kaynağı tek bir birey (hacker), birey toplulukları (hacker grupları), terör örgütleri veya bizatihi devletler de olabilmektedir (Kurnaz, 2016). Siber saldırıları ve saldırı girişimlerini, siber güvenliği en fazla tehdit eden faktörler olarak ifade edilebiliriz.

2.3. Siber Güvenlik

Siber ortamda var olan bilişim sistemlerini saldırı ve tehditlerden korumak, bu ortamda korunmak istenen bilginin gizliliğini sağlamak, bu tehdit ve saldırıların mahiyetini ve kaynaklarını tespit etmek, bu müdahalelere karşı müdahaleler ve hamleler geliştirmek amacıyla oluşturulmuş olan ulusal hukuk, uluslararası hukuk ve insan haklarına uygun her türlü önlem ve sistemler, siber güvenlik olarak tanımlanmaktadır (Kara, 2013).

Bir diğer benzer tanıma göre siber güvenlik; siber uzayda kullanıcıların ve kurum kuruluşların güvenliklerini sağlamak amacıyla kullanılan araçlar, güvenlik politikaları, kılavuzlar, eğitimler, uygulamalar, güvenlik teminatları ve her türlü teknolojik altyapılanmadır (Yılmaz, 2017).

Siber risk ise, bir kuruluşun bilgi teknolojisi sisteminin bir tür başarısızlık nedeniyle finansal kayıp, işleyişini durdurma veya itibar kaybına sebep olan tüm riskleri kastetmektedir. Böyle riskler aşağıdaki sınıflandırılmış eylemler sonucu ortaya çıkmaktadır (The Institute of Risk Management, 2014, s. 8):

- Casusluk, dolandırıcılık veya para sıkıntısı sebebiyle bilgi sistemlerine erişmek için kasıtlı veya yetkisiz güvenlik ihlalleri,

- Kasıtsız veya kazara güvenlik ihlali,
- Zayıf sistem bütünlüğü ve diğer faktörlerden dolayı operasyonel BT riskleri.

Farklı yönetim kontrolleri yanı sıra denetim fonksiyonu da siber güvenliği sağlama yolunda önemli bir araçtır. Denetim estrümanının etkin kullanımı siber güvenlik seviyesinin artırılmasına doğrudan katkı sağlamaktadır. Bu aşamada, siber güvenliğin önemli bir alt bileşeni olarak bilgi güvenliği ve ilişkili konular üzerinde kısaca durmakta fayda görülmektedir.

2.4. Bilgi Güvenliği ve Sosyal Mühendislik

Bilgi güvenliğinin sağlanması bakımından, güvenlik altyapısının ve politikalarının doğru belirlenmesi, korunacak bilginin analiz edilmesi ve yönetim fonksiyonlarının çok yönlü şekilde gerçekleştirilmesi gerekir. Siber saldırıların elektronik ortamda tanımadığımız kötü niyetli kişilerden gelebileceği gibi, arkadaş grupları veya tanıdık kişilerden de gelebilir. Bu tür durumlar sosyal mühendislik alanında incelenmektedir (Canbek & Sağıroğlu, 2006).

Sosyal mühendislik yöntemleri, davranışlardaki önyargılar üzerine inşa edilir. Bu yönüyle önyargılar adeta insanın sistem açıklarını ifade etmektedir. Sosyal mühendislik yöntemlerini kullanan dolandırıcılar, haksız çıkar elde etmek amacıyla ve çeşitli yollarla kişi ve kurumlara ait bilgi ve sistemleri ele geçirmektedir. Dolandırıcılığın yaşam döngüsü; ayak izini takip et, güven yarat, manipüle et, hedefi terk et şeklinde ifade edilmektedir (Türkiye Bankalar Birliği, 2015).

Alınan güvenlik önlemleri ile birlikte siber riskler ve tehditler yok edilebilmekte yahut etkilerini azaltılabilecek önlemler alınmaktadır. Güvenlik önlemleri almanın yanı sıra belirlenen siber güvenlik politikaları doğrultusunda denetimler gerçekleştirilmesi de gerekmektedir.

3. SİBER GÜVENLİK DENETİMLERİ ve UZAKTAN DENETİM

Telekomünikasyon ve bilgi teknolojilerindeki gelişmeler sonucunda artık iletişim sınırlar ve mesafe tanımamaktadır. Bilgisayar ve internet, bütün dünyayı siber uzay denilen global bir köy haline dönüştürmüştür. İnternetin de gelişmesiyle beraber dünyada teknolojik etkileşim önemli derece artmıştır. Bu nedenle internete bağlantılı bilgisayar sisteminin veya ağının başka bilgisayar sistemleri veya ağlarına karşı yapmış olduğu siber saldırı sonucunda bilginin açığa çıkarılması, erişilebilirliğinin kesintiye uğraması gibi riskler, siber güvenlik politikalarının gözden geçirilmesini ve denetimini daha da önemli kılmaktadır.

Bilgi sistemleri teknolojilerindeki son gelişmeler, kurumlarda farklı alanlardaki birçok uygulamada otomasyona geçilmesine sebebiyet vermiştir. Günümüz iş ortamıında, hem kamu hem de özel sektörde işlemlerin gerçekleştirilmesi için dijital bir alt yapıya sahip oldukları ve bu kapsamda bilginin depolandığı işlemlerin yapıldığı ve raporlamanın elektronik ortamda gerçekleştiği görülmektedir. Bu dijital alt yapı internet, bilgisayar sistemi, yazılım, donanım ve hizmetler yani dijital ortamın tamamı **siber alan** olarak ifade edilmektedir. Dolayısıyla siber alan, dünyanın herhangi bir yerinden gelebilecek saldırılara açık durumdadır ve bu saldırıları yapanın belli olmaması ve bunu ispat edecek kanıtların olmaması siber güvenliği sağlamayı iyice zorlaştırmaktadır (Türkiye'nin Siber Güvenlik Politikası, 2015).

Aynı şekilde siber saldırılara maruz kalınması ve siber saldırılar sonucu sistemlerin işlemez hale gelmesi, tüm sektörlerin bu riskleri önceden belirleyebilmesi ve yönetebilmesi için politikalar geliştirilmesini ve denetimleri yaygınlaştırmasını zorunlu hale getirmektedir. Oluşturulan politikalar içerisinde de riskli alanların belirlenip önem derecesine göre öncelik verilerek denetlenmesi, denetim sonucunda elde edilen bulguların raporlanması gerekmektedir. Bu süreçte etkili denetim yöntemlerinin geliştirilmesi ve denetim tekniklerinin gelişen koşullara uyarlanabilmesi başlı başına önemli bir konu haline gelmektedir. Bu noktada, denetimin odaklanacağı konuların detayı (siber alan değişkenleri) üzerinde önemle durulması, denetim tekniklerinin geliştirilebilmesi bakımından uygun bir strateji olacaktır.

Teknolojik alt yapı, faaliyetlerin gerçekleştirilmesinde büyük fırsatlar sağlamasına karşın büyük riskleri de beraberinde getirmektedir. İşletmelerde verilerin çok

önemli bir kaynak haline dönüşmesinden dolayı, verilere erişim, verilerin paylaşımı, verilerden bilgilerin oluşturulması ve bilgilerin kullanılması önemli bir ihtiyaç niteliği taşımaktadır. Verilere ve bilgi yönetimine yönelik talebin artmasının yanında, veri tabanlarının, uygulamaların ve **bilgi sistemleri**nin güvenliğinin tesis edilmesi çok kritiktir. En az yolsuzluklar kadar yetkisiz erişimlere karşı da verilerin ve bilgilerin korunması gerekmektedir. İnternetin hızla yayılması neticesinde, bu bilgi ve verilere birçok kişinin erişim imkânı bulunmaktadır. Dolayısıyla verilerin ve uygulamaların korunması için etkili mekanizmalara gereksinim duyulmaktadır (Kumar, vdğr. 2005).

Günümüzde bilginin saklanması ve paylaşılması açısından büyük kolaylıklar sağlayan bilişim teknolojileri, daha önce değinildiği üzere şirketler için önemli maddi ve itibar kaybına neden olabilecek bazı **siber güvenlik riskleri**ni ve tehditlerini de beraberinde getirmektedir. Şirketler maliyetlerine bakmaksızın en üst düzey güvenlik teknolojilerinden faydalanarak sistemler geliştirse de bu tür teknik güvenlik önlemleri yeterli olmamaktadır. Çünkü güvenlik teknolojilerinin geliştirilmesi, saldırganları teknik açıdan zorlaşan yapıdaki insan faktörünün zayıflıklarından yararlanmaya yöneltmiştir. Bu durum ise insan faktörünü güvenlik anlamında en zayıf halka haline getirmektedir. Kurum içerisinde insan faktörüne bağlı oluşabilecek bilgi güvenliği riskleri tamamen ortadan kaldırılamasa da en aza indirilebilmesi için gerekli farkındalık faaliyetlerine önem verilmesi gerekmektedir. Ayrıca sadece dışarıdan gelebilecek saldırılara odaklanmayıp kurum içerisinden gelebilecek saldırıları da göz önünde bulundurarak insan ilişkilerine önem verilmesi gerekmektedir.

Öte yandan; siber güvenlik politikalarının yetersizliği ile birlikte artan siber suçlar neticesinde şirketlerin de ciddi oranda para ve itibar kaybına uğradıkları görülmektedir. İnternet, çeşitli alanlarda bireylere, işletmelere ve ülkelere büyük fırsatlar sunarken diğer taraftan yeni bir suç türü olan **siber suçlar**ın doğmasına neden olmuştur. Siber suçlar dünya çapında trilyonlarca dolar finansal kayba sebebiyet vermektedir. Ancak birçok kişi veya kurum bu suçun büyüklüğünden ve etkilerinden haberdar değildirler (Verma & Bajaj, 2008). Bununla birlikte, birçok ülke siber güvenlik politikalarının içerisinde önemli bir yer tutan siber suçlara yer vermeye başlamıştır. Artık günümüzde şirketler sanal dünya ile beraber büyümesi sebebiyle, siber suçlar alanına büyük yatırım yaparak bu alanda çalışacak insanlar istihdam etmektedir.

Bilgi güvenliğine yönelik **bilişim suçları** da bu risklerden kaynaklanmaktadır. Bilişim sistemleri üzerindeki bilgisini, gizli verilere ulaşmak veya ağlar üzerinde zarar verici işler yapmak için kullanan kişilere, internet bilgi hırsızı veya korsanı denir. İnternette bilişim suçunun gerçekleşebilmesi için ilk olarak kullanıcıların bilgisayarına bir takım casus yazılımların kurulması gerektiği ifade edilmektedir ve hiçbir casus program kendi kendine bilgisayar sistemlerine kurulamamaktadır (Türkiye Bankalar Birliği, 2015, s. 13). Devletler bilişim suçuyla mücadele için hukuk sitemleri içinde düzenlemeler yapmakta, özel ve ceza muhakemesi hukuk kuralları ile siber suçları önlemeye çalışmaktadır. Devletlerin kendi içinde aldığı önlemler etkili görünse de çoğu zaman etkisiz kalabilmekte ve bazı suçlar uluslararası bir ağ içinde gerçekleşebilmektedir. Siber suçlarda, çok az sayıda ülkenin mevzuatında düzenlemelerin yer alması, siber suçlular için büyük bir avantaj ortaya çıkarmaktadır (Özbek, 2015). Bu gelişmelere paralel olarak, yaşanan mağduriyetlerin çokluğu Türk ceza yargısında da "Bilişim Suçu" kavramının gündeme alınmasına sebep olmuştur.

Siber tehditler ve çeşitleri hızla gelişmekte olan teknolojiler ve evrim geçiren operasyonel uygulamalar ve gereksinimler, hem özel hem de kamu sektöründeki işletmeleri, birbirine son derece bağlı ve teknolojik açıdan yakınsayan bilgi ağlarına yönlendirmektedir. Patentli bilgi işleme çözümleri ve ayrı ayrı veri depolayan veri tabanları, birleştirilmiş entegre sistemlerin kullanımına sebebiyet vermekte ve böylece iyi planlanan tek bir ağ ihlali, veri hırsızlığı veya hizmet engelleme saldırısının potansiyel etkisini önemli ölçüde artırmaktadır. Bu nedenle, ticari işletmelerin ve kamu kurumlarının, yeni saldırı stratejilerine ve taktiklere hızla cevap verebilen veya bunlara yönelik öngörülerde bulunabilen **ağ savunma sistemleri**ni geliştirmeleri son derece önem taşımaktadır (Colbaugh & Glass, 2011).

Siber ortamda birçok siber saldırılar meydana gelmektedir. Tüm bu saldırılara örnek olarak; açık artır-

ma dolandırıcılıkları, işletmedeki fırsatlara ve işlere yönelik dolandırıcılıklar, bağış dolandırıcılığı, çocuk istismarı, telif hakkı ihlalleri, sıkıştırmalar, kredi kartı hileleri, kredi dolandırıcılığı, sanal zorbalıklar, siber tacizler, siber soygunlar, siber medikal dolandırıcılıklar, siber terörizm, evlenme, boşanma ile ilgili dolandırıcılıklar, eğitim dolandırıcılıkları, kumar dolandırıcılığı, hacking, kimlik hırsızlığı, göç dolandırıcılığı, yatırım hileleri, laptop hırsızlığı, borç ve bağış dolandırıcılığı, organize suçlar, e-mail dolandırıcılığı, satış hileleri, istek dışı e-postalar (spam), seyahat dolandırıcılığı, virüsler, solucanlar (worms), truva atları (trojans), casus yazılımlar (spyware) verilebilmektedir (Milhorn, 2007). Siber saldırılar, güvenlik ihlallerinin işletme üzerinde yıkıcı etkilere sahip olabileceğinden ötürü, siber güvenlik günümüz organizasyonlarındaki en büyük risklerden birisi olarak belirlenmektedir. Siber suçluların daha sofistike bir yapıya bürünmesinden ve siber saldırıların çok daha fazla yaygınlaşmasından dolayı bir siber saldırının önemli boyuttaki finansal, operasyonel ve itibarsal zararı; yönetilmesi gereken çok kritik bir risktir (City of Vancouver, 2016). Bu nedenle meydana gelebilecek her türlü siber tehdit ve siber saldırı çeşitlerinin çok iyi analiz edilerek işletmeler tarafından gerekli güvenlik önlemlerinin alınması, alınan önlemlerin denetlenmesi hayati önem taşımaktadır.

İşletmelere yönelik yapılan bir araştırmada, işletmelerin bilgi teknolojileri üzerinde en çok aşağıdaki güvenlik ihlallerinin meydana geldiği ortaya konulmuştur (Statista. 2015):

- Bilgi teknolojilerinin veya iletişim araçlarının çalınması,
- Çalışanları etkileyen sosyal mühendislik vakaları,
- Hassas dijital belgelerin çalınması,
- Bilgi teknolojileri sistemleri veya süreçlere yönelik sabotajlar,
- Hassas fiziksel belgelerin veya parçaların çalınması,
- Elektronik iletişime yönelik gerçekleştirilen casusluklar,
- Toplantıların veya telefon konuşmalarının gizlice dinlenmesidir.

Ayrıca, **sosyal ağlar** da siber tehditler açısından önemli bir alan teşkil etmektedir. Günümüzde sosyal ağlar, ergenler ve yetişkinler tarafından daha sık kullanılmaktadır (Grant, N. 2008). Yeni yetişen gençler Myspace, Facebook ve Youtube gibi sosyal ağ sitelerini günlük hayatının bir parçası olarak görmektedir. Özel yaşamlarını paylaşma ve tanımadığı diğer kişilere kendini tanıtma amacıyla sosyal ağları kullanmaktadır (Özmen, v.dğr., 2011).

Sosyal ağlar; "bireylerin toplum içerisinde kendilerini tanımlayarak, aynı kültürel seviyede rahatlıkla anlaşabilecekleri insanlarla internet iletişim metotları ile iletişime geçmek ve aynı zamanda normal sosyal yaşamda yapılan çeşitli jestleri simgeleyen sembolik hareketleri göstererek insanların oluşturduğu sanal ortamlarda sosyal iletişim kurmaya yarayan araçlar" olarak tanımlanmaktadır (Yavanoğlu, vdğr., 2012). Ayrıca sosyal ağ siteleri, kullanıcının bilgilerinin bir kısmının diğer kullanıcılara açık olduğu, arkadaşlık istekleri gönderip iletişimde bulunduğu ve çeşitli sosyal medya paylaşımlarının olduğu web tabanlı hizmetleri içerisinde barındırmaktadır (M.Boyd & Ellison, 2007). Ara yüzlerinin ve üyeliğin kolay ve anlaşılır olması, sosyal ağların birçok kullanıcıya hitap etmesini sağlamaktadır. Günümüzde gerçek kimlikleri ile sosyal ağlarda yer alan birçok kullanıcı bulunmaktadır. Bu sayede sosyal ağ kullanıcısı kendi hayatlarında olup bitenleri, güncel olayları, ilgi alanlarını rahat bir şekilde arkadaşı olduğu birçok insanla paylaşabilir, fikirlerini belirtebilir. Ayrıca video, resim gibi sosyal içerik paylaşımlarında bulunabilir, başkalarının paylaştıklarından haberdar olabilir (Gülbahar, vd. 2010.). Sosyal ağlardaki güvenlik açıklıklarının temel nedenleri; bu ağların kuruluş amaçları nedeniyle, mahremiyetin korunmaması ve kullanıcıların kişisel bilgilerini paylaşarak kendilerini bu ortamda hedef haline getirmeleridir (ISACA).

Yukarıda bahsedilen değişkenlerle ilgili siber risklerin artması sonucu hizmetlere ilişkin tüketici güveninin azalma eğilimine başlaması halinde bu riskler olağanüstü harcamalara neden olacaktır. Bu nedenle, siber güvenlik risklerinin analizi, önceden tespiti ve güvenliği için denetim hayati önem taşımaktadır.

Siber güvenlik denetimleri, siber güvenlik denetimlerinin kapsamı ve hangi güvenlik ve kontrol noktala-

rından oluştuğu, Bilgi Sistemleri Denetimi ve Kontrol Kurumu (ISACA) tarafından yayınlanan raporda şu şekilde belirlenmektedir:

Siber güvenlik denetimleri için **birincil güvenlik ve kontrol konuları** (ISACA: 1);

- Hassas verilerin ve fikri mülkiyet haklarının korunması,
- Çoklu bilgi kaynağının bağlı olduğu ağların korunması,
- Cihazların ve bu cihazların içerdiği bilgilerin sorumluluğu ve hesap verebilirliğidir.

Siber güvenlik denetiminin kapsamı ise (ISACA, s. 1);

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

Siber güvenliğin amacı bilgi ve bilgi sistemlerinin korunmasıdır. Siber güvenlik kontrolleri aşağıdaki konuları bünyesinde barındırmaktadır:

- Çalışanların güvenliği,
- 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 işlemleri.

Bilgi teknolojilerindeki gelişmeler, siber alanda oluşan tehdit ve saldırılar nedeniyle denetim son derece önemli hale gelmiştir. Siber güvenlik tehditlerine maruz kalınması, ülkeleri tehdit eden bir boyut aldığından denetim, siber suçlarla ilgili yasal konular açısından da önemli bir boyut kazanmıştır. Yakın zamanda yaşanan önemli siber saldırılar göz önünde bulundurulduğunda ciddi zararlara ve maliyetlere sebep olmuştur. Bu nedenle hem özel sektörde hem de kamu sektöründe siber saldırılara karşı önlemlerin alınması ve etkilerinin azaltılması gerekmektedir. Ayrıca denetim sırasında, siber güvenlik sorunlarına yol açan risk faktörleri ve bu faktörlerin nedenleri daha titizlikle değerlendirilmelidir.

Bu minvalde üçlü savunma hattının siber riskleri kapsayacak şekilde tasarlanması ve uzaktan denetim biriminin oluşturularak siber güvenlik risklerine yönelik çalışmalar yürütmesi, siber güvenlik risklerinin azaltılmasında etkili olacaktır. Özellikle uzaktan denetim, yukarıda izah edildiği üzere mesafelerin artık sonlandığı, işlemlerin anlık gerçekleştiği bir dünya düzeninde daha da önemli bir yapıya bürünmüştür.

Uzaktan denetim, yerinden denetimin ayrılmaz bir parçasıdır. Yerinden denetim, fiziki olarak işlemlerin yerinden incelenmesi ve risklerin değerlendirilmesidir. Uzaktan denetimde, veri havuzunda bulunan bilgiler değerlendirilir; alınan önlemler takip ve izlemeye alınır; riskler öncelik sırasına konularak değerlendirilir ve üst birime raporlanır.

Yerinden denetimde, denetim sırasında incelenen alanlar veya işlemler ile ilgili raporlama yapılırken, uzaktan denetim veri havuzundaki veriler kullanarak tüm süreçlerin risklerini öncelik sırasına göre derecelendirerek değerlendirilme ve raporlama yapılmaktadır. Bu anlamda uzaktan denetim, yerinden denetime rakip, yerinden denetimin ikamesi olmamakla birlikte yerinden denetimin tamamlayıcısı konumundadır.

4. COVID-19 ve UZAKTAN DENETİM ÜZERİNDEKİ ETKİLERİ

Günümüzde küreselleşmenin getirmiş olduğu iş dünyasındaki rekabet, teknolojik değişim ve gelişmeler, siber hile ve hırsızlıklar yeni iş yapış modelleri oluşturmakta, birçok alanda hızla değişim ve dönüşüm sürecini getirmektedir. Bahsedilen gelişmeler ile birlikte COVID-19 salgını doğrultusunda üretimin

yavaşlaması, durdurulması, seyahatlerin sınırlanması, yasaklanması, kontrollerin güçlendirilmesi gibi durumlarla karşılaşılmaktadır. Özellikle COVID-19 virüs salgını nedeniyle hayata evde devam etmek zorunda kalındığından, e-ticaret müşterilerinin internet üzerinden yaptıkları işlemlerde de artarak devam etmektedir. Öte yandan, internet bankacılığı, banka ve kredi kartı kullanımları ve e-ticaret, çevrimiçi ödeme sisteminin müdahalelere maruz kalan temel bileşenleridir.

Koronavirüs küresel çapta eğilimleri büyük ölçüde değiştirmiştir. İnsanların davranışı, ticaretin doğası, iş dünyası ve hatta yaşam biçimi değişmiştir. Örneğin Birleşik Krallık'taki tüketicilerin % 40'ı koronavirüs salgını nedeniyle eğlenceyle ilgili harcamaları azaltarak daha fazla para biriktirmeyi planladığını belirtmiştir (Harris Interactive, 2020). Ayrıca bu süreçte insanlar dijital ortamlardan haberleşmeye ağırlık vermeye başlamıştır. Örneğin koronavirüs salgını sırasında, ABD'li yetişkinlerin % 51'i sosyal medyayı daha fazla kullanmıştır (Williamsion, 2020). Koronavirüsün bir pandemi olarak kabul edilmesi ve daha fazla insanın evden çalışmaya başlamasından dolayı internet kullanımı %50 artmıştır (Harris Interactive, 2020). Bu değişim şirketlerdeki değişimi tetiklemiştir. Amerika Birleşik Devletleri'nde Walmart, perakende satışın düşmesiyle Amazon Prime gibi yıl boyunca ücretsiz kargo hizmeti sunmak için yapılanmaya gitmiştir (O'Brien, 2020).

COVID-19 salgınında sosyal hayatın değişime uğraması ve evde kalmak, tüketicileri çevrimiçi alışverişe yöneltmiştir. Adobe Analytics raporlarına göre, ABD'deki toplam çevrimiçi satışlar bir önceki yıla göre % 76,2 artışla 73,2 milyar ABD dolarına ulaşmıştır (Kesten, 2020). Amazon açıkladığı ikinci çeyrek sonuçları raporunda işletme nakit akışının, son on iki ayda % 42 artarak 51,2 milyar dolara yükseldiğini belirtmiştir (Amazon, 2020). Ev eşyaları satışı yapan B&Q and Screwf perakende mağazalarının sahibi Kingfisher açıklamasında kendin yap markalarının çevrimiçi satışların koronavirüs salgını sırasında %183 oranında arttığını belirtmiştir (Denton, 2020). Emarketers araştırmasına göre de koronavirüs salgınının ABD ekonomisini büyük oranda kötü etkilemesine rağmen e-ticarette %18,0 büyümeye olacağını, bunun da dijital değişimin bir başka kanıtı olduğunu savunmuştur (Samet, 2020).

2020 yılının başlarında ortaya çıkan ve kısa sürede küresel bir yayılım gösteren COVİD-19 virüs salgını nedeniyle, ülkeler seyahat ve çalışma kısıtlamaları getirmek zorunda kalmıştır. Çok yönlü etkilerinin olacağı ilk gün itibarıyla belli olan COVID 19 virüsüne karşı kuruluşların kurumsal yönetim ilkeleri doğrultusunda mevcut yönetişim modellerini, iş sürekliliği planlarını güncellemeleri ve salgına özel modeller oluşturmaları gerekli olmaktadır. O nedenle kuruluşların mevcut iş planlarını ve kriz yönetimi planlarını değerlendirmeleri ve bulundukları sektöre özel yaklaşımlar oluşturmaları önem arz etmektedir. Nitekim salgın dolayısıyla birçok kuruluşun çeşitli tedbirler aldığı görülmektedir. Bu süreçte denetim mekanizmasının önemi her geçen gün artmakla birlikte, COVİD-19 salgını nedeni ile uzaktan denetimin daha da etkin bir şekilde yapılması elzem bir konu olarak karşımıza çıkmaktadır. Bilhassa e- ticaret şirketlerinin bu dönemde daha da çok uzaktan denetime ihtiyaç duydukları görülmektedir. Öte yandan, uzaktan çalışma konusu, dünyayı etkisi altına alan ve tüm kesimleri etkilemeyi başaran COVID-19 sonrası dönemde devam edecek önemli bir değişim olacaktır. Uzaktan çalışma ile birlikte uzaktan denetim de yeni düzeninin değişmez bir parçası olacağa benzemektedir. Bu nedenle, yönetim kurullarının şimdiden çalışanların bu konudaki görüşlerini ve önerilerini almaları yararlı olacaktır.

COVID-19 salgınına bağlı gelişmeler, kuruluşlar için siber güvenlik açısından çok önemli riskler doğurabilecektir. Dolayısıyla COVİD-19 salgını nedeniyle öngörülemeyen birçok etkiyi barındıran bu durum, kurumsal yönetimin bir bileşeni olan denetimin, önemini bir kez daha ortaya koymuştur. Etkin bir uzaktan denetim bu dönemde güncel denetim prosedürleri ile birlikte yeni uzaktan denetim prosedürlerini de içermelidir. Yaşanmakta olan salgın durumu karşısında uzaktan denetim özellikle siber tehditler karşısında daha etkili ve verimli olması açısından, periyodik kontrollerin de sayısının arttırılması gerekecektir. Bununla birlikte; uzaktan denetim ile elde edilen/edilecek verilerin güvenliği önem arz edecektir. Veri güvenliği politikasındaki eksikler nedeni ile bilgile-

rin mahremiyetinin tehlikeye düşmesi durumunda telafisi imkânsız sonuçlar oluşmaktadır. Bu nedenle iç kontrollerin yürütülmesi zorlaşacak, iç kontrollerde önemli değişiklikler olabilecek ve tüm bu gelişmeler kuruluşun iç kontrol ortamını önemli ölçüde etkileyecektir. Ayrıca, bu süreçte yönetim kurulu ve icra kuruluna kısa periyotlarla temel performans göstergelerine ve COVID-19 risklerine ilişkin raporlama yapılmalıdır. Yönetim kurullarının da COVID-19'un ortaya çıkardığı yeni risk ve konuların gözetimine daha fazla zaman ayırması beklenmektedir.

COVID-19 salgınının kısa ve orta vadede etkilerin öngörülememesi nedeniyle kuruluşların tüm departmanlarına önemli görevler düşmektedir. Yönetişim ve organizasyon yapısını, karar alma ve iletişim mekanizmalarını, sızma test analizlerini, süreçlerini ve kurtarma yöntemlerini tekrar gözden geçirmelidirler. Bunlar yapılırken denetim birimlerinin de bu dönemde uzaktan denetim faaliyetlerini sürdürme noktasında gerekli önlemleri almaları ve kuruluşların gelecekte alacakları kararlara yardımcı olmaları önem arz etmektedir.

Siber güvenlik denetimlerindeki en önemli birimler, İç Kontrol, Risk Yönetim ve İç Denetim Birimleridir. İç Denetim Birimi siber saldırılara karşı iç denetim mekanizmasının oluşturulmasında, güvenlik önlemlerinin alınmasında, siber güvenlik denetimlerinin icra edilmesinde ve yönetimle bağlantı kurulmasında anahtar rol üstlenmektedir. Kontrol mekanizmalarının sağlıklı bir şekilde işlemesi için iç denetim fonksiyonunun yeterli ve etkili bir şekilde yürütülmesi gerekir. Denetim türlerinde dolayısıyla iç denetimde başarı ve etkinliğin sağlanabilmesi için bazı koşullar vardır. Öncelikle yönetimin iç denetimin sağlayacağı faydaları kavraması ve iç denetimi sahiplenmesi gerekir. Ayrıca yönetim, iç denetçiler için sağlıklı bir çalışma ortamı oluşturmalıdır. Kurumun tüm birimlerinde sağlıklı çalışmalar yapılabilmesi için iç denetim biriminin diğer tüm birimlerince tanınması gereklidir (Memiş, 2008).

İç denetim en sade ifadeyle, bağımsız ve tarafsız bir güvence ve danışmanlık faaliyetidir. Etkili bir iç denetim fonksiyonunun hem üstlenmesi ve hem de üstlenmemesi gereken roller vardır. Bu bağlamda, iç denetimin temel görevi; bir kurumdaki önemli risklerin uygun şekilde yönetilmesini ve iç kontrol sisteminin etkili şekilde işlev görmesini sağlama konusunda yönetime tarafsız güvence sağlamaktır. İç denetimin rolü çerçevesinde, yürütülen görevin; iç denetimin bağımsızlık ve tarafsızlığını olumsuz etkileyip etkilemeyeceği hususu ile yürütülecek faaliyetin kurumun risk yönetimi süreçlerinin geliştirilmesine katkı sağlayıp sağlamayacağı hususuna özellikle dikkat edilmesi gerekmektedir (Madendere, s. 6.)

Etkili bir iç kontrol sisteminin oluşturulmasında danışmanlık rolüne sahip olan iç denetim, işletme faaliyetlerinin incelenmesi ve etkili bir değerlendirme işleviyle işletme içinde organize edilmiş, bağımsızlığı tartışma konusu yapılmayan bir değerlendirme mekanizmasıdır (Pickett, 2000).

Siber güvenlik denetim faaliyetleri; COVID-19 salgını nedeni ile saha çalışmalarının yürütülemeyeceği de dikkate alındığında siber saldırılarla ilgili riskleri azaltmaya yönelik olarak, denetlenecek alanlarda sürekli kontroller yapılarak ve riskler düzenli olarak izlenerek uzaktan denetime yöneltilmelidir. Uzaktan yapılan denetimler neticesinde iç kontrolün etkinliğine yönelik makul güvence verilmesinin sağlanması açısından, COVID-19 salgını ortamında siber saldırılar da göz önünde bulundurularak çok hızlı yeni ve kritik kontrol noktaları belirlenmeli ve bu kontrollerin yeterliliği ve etkinliği periyodik olarak gözden geçirilmelidir. Olağanüstü bir dönem olan bu süreç daha önce hiç yaşanmadığından iç kontrol noktalarının yaşanan değişimler ışığında hızlı ve etkili bir şekilde güncellenmesini sağlanmalıdır. Bu dönemde kontroller açısından kuruluşların etkin ve kritik kontrol noktalarının belirlenmesi çok faydalı olacaktır. Geliştirilecek olan yapay zeka yazılımlarının her alanda olduğu gibi iç kontrol ve iç denetim alanında da iş yükünü azaltacağı ve çok daha geniş alanları kontrol edebileceği aşikardır.

Teknoloji firmaları tarafından basit ve tekrarlayan görevlerde yapay zeka kullanımı için çözümler sunulmaya başlanmış bulunmaktadır. Hesaplama sürecinde yardımcı olan, konuşarak iletişim kuran, işlemler sırasında yönlendiren bir yapay zeka formunun geldiği sinyaller verilmektedir. Aynı zamanda çok ama çok büyük verileri analiz edip suiistimallerin önüne geçecek sisteme geçme konusunda çalışmalar devam

etmektedir. Tekrarlanan ve hata bedeli düşük işlerde yapay zekanın insan çalışanlardan daha başarılı olduğu, süreç boyunca hata oranı insanınkine denk bile olsa yapılan hatanın sonucunda çok küçük bir zarar oluştuğu gerçektir. İnsan yerine yapay zeka kullanmak bütçeler açısından fark yaratmadığı gibi, insanı daha verimli olabileceği başka görevlere aktarmak mümkün olabilecektir.

Yakın gelecekte ileri teknoloji uygulamaları ile uzaktan denetim uygulamalarında kaçınılması mümkün olmayan bir dönüşümün gerçekleşmesine neden olacaktır. Bilgisayarlar ve yazılımlar uzaktan denetim mensuplarının işlerini kuşkusuz kolaylaştıracağı gibi aynı zamanda işlerinin bir kısmını da ellerinden alacaktır. Yapay zekanın kontrol ettiği bilgisayar sistemleri ile yapılan işler meslek mensuplarının işlerini azaltacaktır. Uzaktan denetim denetçinin işlerini akıllı yazılımlar ile gerçekleştireceğine göre, uzaktan denetim için bu dönüşüm yolculuğunda hızlıca geleceğe yönelik adımlar atılması gerekmektedir. Teknolojik dönüşüm uzaktan denetimin işlerini zorlaştırmak bir yana stratejik karar desteği olma yolunda daha güçlü bir rol almaları konusunda kapıları aralayabilecektir. Öğrenen makineler rutin işleri yaparken uzaktan denetimin gelecekte kritik karar destek danışmanlığına odaklanması gerekecektir. İç denetçide aranan en önemli vasıf olarak günümüzde mesleki bilgi yeterli olurken gelecekte analitik düşünce yeteneği, iletişim yetkinliği, iş zekası, endüstriye özgü bilgi, bilgi teknolojilerine hakimiyet, aranacak önemli özellikler haline gelecektir. Aynı şekilde, bilgi teknolojileri, siber güvenlik, kurum kültürü, yönetişim, veri analitiği gibi alanlarda gerçekleştirilen çalışmalarla üst yöneticilere karar verme aşamasında destek olmak ve danışmanlık yapmak iç denetimin işleyişindeki dönüşüm sonucu uzaktan denetimin görevi haline gelecektir.

Dünyada ve ülkemizde etkisini gösteren COVID-19 salgını ile değişim ve gelişmeye bağlı olarak birçok alanda olduğu gibi uzaktan denetim alanında da inovasyon ön planda olmalıdır. Teknolojik gelişmeler ve dijital dünyadaki değişim hızı sonucu elektronik fatura, elektronik defter gibi kavramların gündemde olması ile zamanında düzgün bir biçimde ve doğru şekilde veri girişi uzaktan denetimin başarısını etkilemektedir. Salgın ile birlikte denetimin de etkilenmemesi kaçınılmaz olacağı gerçeğinden hareketle başarı oranın arttırılması ya da en azından bulunduğu konumu koruması açısından zamanın gerisinde kalmamak ve değişen koşullar altında başarı, uzaktan denetimin felsefi olarak yenilikçi bir yaklaşımı benimsemesiyle mümkün olacaktır.

Uzaktan denetimin bugünün ve geleceğin beklentilerini karşılayabilmesi için, iş modellerindeki değişime paralel şekilde dönüşüme uğraması kaçınılmaz görülmektedir. Dünya genelinde meydana gelen salgınla birlikte tetiklenen teknolojik gelişmeler, diğer meslekleri zorladığı gibi uzaktan denetim alanında da etkisini göstermektedir. Büyük veri analizleri, bulut bilişim, yapay zeka uygulamaları, blokzinciri (blokchain) gibi teknolojik gelişmeler ve tüm bu teknolojik başarıları harmanlayan gelecekteki **dijital denetim** günümüzdeki uzaktan denetimin yerini alacak gibi görünmektedir.

5. SONUÇ

Dünyada bilgi teknolojileri uygulamaları her geçen zaman diliminde yeni gelişmeler ile birlikte tüm kullanıcıların faaliyetlerini etkilemeyi başarmış bulunmaktadır. Yeni teknolojik gelişmelerin olumlu etkilerinin yanında olumsuz etkilerinin ve beraberinde getirdiği risklerin siber güvenliği tehdit etmesi kaçınılmaz olmuştur. Bu bakımdan, siber güvenlik özellikle finansal işletmeler, devletler ve hatta bireyler için hayati önem taşıyan bir alan konumuna gelmiştir. Siber politikalar oluşturulurken bilgi teknolojilerinde yaşanan bu gelişmeler uzaktan denetimin etkinliğini artırma stratejilerini de ön plana çıkarmıştır. Bu stratejiler sayesinde uzaktan denetim faaliyetleri geleneksel denetim yaklaşımından, yoğun bilgi teknolojilerine dayalı denetim yaklaşımlarına doğru yönelmiştir. Ayrıca, bilgi teknolojilerinde görülen gelişmelerin yanı sıra tüm dünyada etkisini gösteren COVID-19 salgınının zorladığı çalışma tarzı değişiklikleri, iç denetçilerin risk yönetimi ve iç kontrol sisteminin etkililiğini değerlendirme misyonlarıyla ilgili bilgi ve becerilerini geliştirme gereksinimini arttırmaktadır.

Bu çalışmada, siber güvenlik konuları ile COVID-19 salgınının uzaktan denetim üzerindeki etkileri ve bu süreçte denetiminin uzaktan denetim biçimde

yapılması ile ilgili hususlar açıklanmaya çalışılmıştır. Salgın nedeni ile tüketici alışkanlıklarında meydana gelen değişimler tüm sektörler tarafından dikkatle takip edilmekte, hatta ülkeler yeni sosyal ve ekonomik modelleri tartışılmaktadır. Siber riskler ve siber saldırılar karşında siber güvenliğin sağlanması kapsamında uzaktan denetim yöntemlerinin yeniden gözden geçirilmesi, denetimin uzaktan gerçekleştirilmesi prosedürlerinin oluşturulması gerekmektedir. Diğer taraftan, COVID-19 salgını gibi nedenlerle denetim saha çalışmalarının bu dönemde yapılamamasından dolayı uzaktan denetim çalışmalarında daha çok veri ve bilgiye ihtiyaç olacaktır. Elde edilen verilerin korunması ve güvenliğinin artması yönünde daha çok kontrol ve güvenlik politikalarına ihtiyaç duyulacaktır. Bu dönemde yapılan işlemleri denetleyecek denetçilerin daha dikkatli olması gerekmektedir. COVID-19 salgını ile birlikte ülkelerin çoğunda evden çalışma, kısmi çalışma gibi yöntemleri tercih etmek suretiyle değişikliğe gittiği görülmektedir. Bu nedenle veri güvenliğinde oluşacak aksamalar veya veri analizi programlarında oluşabilecek kesintiler uzaktan denetim çalışmalarının aksamasına neden olacak, denetim faaliyetlerinin sonuçlanmasını ve raporlanmasını geciktirecektir. Oluşabilecek bir siber saldırıyı engelleme faaliyetlerinde de iç kontrol sisteminin etkinliğinin ve etkililiğinin de zayıflama ihtimali ortaya çıkması halinde telafisi imkansız zararlar oluşacaktır.

Belirtilen durumlar karşısında iç kontrol ve risk yönetim sistemleriyle birlikte denetim mekanizmalarının beklenen fonksiyonu etkili şekilde yerine getirebilmesi için yapay zeka teknolojilerinden de yararlanarak uzaktan denetim tekniklerinin geliştirilmesi önem taşımaktadır. Özellikle artan siber tehditlere yönelik siber güvenlik denetimlerinde uzaktan denetimin etkin şekilde uygulanabilmesi için yönetim (kurulları) desteğiyle birlikte iç denetim birimlerine büyük görev düşmektedir. İç denetim faaliyetinin risk yönetim ve iç kontrol faaliyetleri ile birlikte bir bütün olarak ama birbirinden de bağımsız bir şekilde yürütülmesi gerektiği unutulmamalıdır. Riskler belirlenmeden, riskleri azaltıcı önlemlerin tespiti noktasında yapılacak bir iç kontrol faaliyeti etkin olmayacak ve bu durum yürütülecek iç denetim faaliyetlerinden etkin sonuç alınamamasına yol açacaktır. Bu nedenle, öncelikli olarak; yürütülen kamu veya özel sektör faaliyetlerine yönelik riskler belirlenmeli, riskleri en aza indirgeyecek iç kontrol faaliyetleri oluşturulmalıdır. Akabinde, bu faaliyetlerin etkinliğini ve verimliliğini denetleyecek bağımsız bir iç denetim sistemi oluşturulmalı ve tüm faaliyetlerin yeterli düzeyde bilgi ve veri havuzu ile desteklenerek değerlendirilebilmesi için her türlü sonucu alabilecek düzeyde yazılımlar ile entegre uzaktan denetim birimi oluşturulmalıdır. Uzaktan denetimin, emek yoğun çalışmadan ziyade teknoloji yoğun çalışma sistemleri kullanılarak dijitalleştirilmesi halinde verimli ve etkili bir şekilde oluşturulup uygulanması sağlanabilecektir. Bunun yanı sıra iş modellerindeki değişimler gözetilerek ve sürdürülebilir inovasyon felsefesiyle uzaktan denetim tekniklerinin geliştirilmesine devam edilmelidir.

Sonuç olarak, teknolojik yeniliklerle çeşitlenen siber güvenlik riskleri ve tüm dünyada etkisini gösteren COVID-19 salgını sonrasında tüm şirketlerin ve kamu kurumlarının siber güvenliği sağlamak için uzaktan denetim prosedürlerinin yeterliliği ile ilgili yeniden bir değerlendirme yapmaları beklenmektedir. COVID-19 salgını etkisini sürdürdükçe, iç denetim birimlerinin özellikle siber güvenlik riskleri başta olmak üzere ortaya çıkan riskler ve iş sürekliliğine ilişkin konularda yönetime hızlı, sürekli değerlendirme ve önerilerde bulunmalarına ilişkin beklenti daha da artacaktır.

Kaynakça

Bayraktar & Gökhan (2015). *Siber savaş ve ulusal güvenlik stratejisi*. İstanbul: Yeniyüzıl Yayınevi.

BCG (2016), The ınternet economy in the G-20: The $4.2 trillion growth opportunity. *Boston Consulting Group*, Boston.

Boyd, D.M. & Ellison, N.B. "*Social network sites: Definition, history and scholarship", Journal of ComputerMediated Communication*, *13*(1), 2007, article 11, 210-230.

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

Colbaugh, R. & Glass, K. (2011). Proactive defense for evolving cyber threats. *IEEE International Conference on Intelligence and Security Informatics,* 10-12 Temmuz 2011, Beijing, China.

Denton, J. (2020, 22 Temmuz). B&Q owner Kingfisher saw online sales surge over 225% in June and bucks the trend for dismal retail news with profit forecast boost. *This is money.* https://www.thisismoney.co.uk/money/markets/article-8547787/B-Qowner-Kingfisher-saw-online-sales-surge-225-June.html adresinden alındı. (Erişim Tarihi, 06.08.2020).

Fentz, S. (2017). Viyana Üniversitesi Web Sitesi. [Çevrimiçi] 2005. http://www.univie.ac.at/frisch/isegov/ aushaengUniWien/CyberpaceSecurity_Fenz.pdf (Erişim Tarihi, 30.11.2017).

Grant N. (2008). On the usage of social networking software technologies in distance learning education. In K. McFerrin et al. (Eds.), *Proceedings of society for* ınformation *technology and teacher education*, *International Conference* (3755-3759), Chesapeake, VA: AACE.

Gülbahar, Y., Kalelioğlu, F. & Madran, O. (2010). Sosyal ağların eğitim amaçlı kullanımı. *XV. Türkiye'de İnternet Konferansı* (1-6). İstanbul: İstanbul Teknik Üniversitesi.

Harris Interactive. (2020). Global barometer: Consumer reactions to COVID-19. https://harrisinteractive.co.uk/wp-content/uploads/sites/7/2020/06/wave-4_media-amp-entertainment_global-barometer.pdf.___adresinden alındı.

Kara, M. (2013*). Siber saldırılar-siber savaşlar ve etkileri* (Basılmamış yüksek lisans tezi). İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Karaçay, T. (2017). Başkent Üniversitesi Web Sitesi. [Çevrimiçi]. http://www.baskent.edu.tr/ tkaracay/etudio/agora/bt/siber.html._adresinden alındı.

Kesten, G. (2020). As online prices ıncrease, consumers' purchasing power declines*, Adobe Blog,* https://theblog.adobe.com/as-online-prices-increase-consumers-purchasing-power-declines/ adresinden alındı. (Erişim tarihi, 3/08/2020).

Kumar, V. Srivastava, J. & Lazarevic, A. (2005). Managing cyber threats: issues, approaches, and challenges. *Springer.*

Kurnaz, İ. (2016). Siber güvenlik ve ilintili kavramsal çerçeve. *Siber Politikalar Dergisi*, *1*, (1). [Çevrimiçi]. http://cyberpolitikjournal.org/wpcontent/uploads/2017/02/Journal_Dergi_pdf.pdf (Erişim Tarihi: 01.12.2017).

Milhorn, H.T. (2007). Cybercrime how to avoid becoming a victim. *Universal Publishers*, Boca Raton, Florida.

Memiş, M. Ü. (2008). Etkin ve başarılı bir iç denetim için gerekli koşullar. *Mali Çözüm Dergisi*, (85), 75-91.

Madendere, M. A. (2005) *Kurumsal risk yönetiminde iç denetim rolü* (Çeviri/Derleme). (Yayımlanmamış TİDE Dökümanı), 8-9.

O'Brien, M. (2020). Walmart coming soon, cheaper alternative to amazon prime. *Multichannel Merchant,* https://multichannelmerchant.com/operations/walmart-coming-soon-cheaper-alternative-amazon-prime/ adresinden alındı. (Erişim tarihi, 6/08/2020).

Orendorff, A. (2017), *Global Ecommerce Statistics [Infographic] and 10 International Growth Trends You Need to Know,* https://www.shopify.com/enterprise/global-ecommerce-statistics, (10.03.2018).

Özmen, F., Aküzüm, C., Sünkür, M. & Baysal, N. (2015). Sosyal ağ sitelerinin eğitsel ortamlardaki işlevselliği (Functionality of Social Networks in Educational Settings). International Advanced Technologies Symposium (IATS'11), 16-18 May 2011, Elazığ. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 1*(1), 1-10, (9) 42-47.

Özbek, M. (2015). *The* ımpacts *of european cybercrime convention on Turkish criminal law.* http://www.goksusafiisik.av.tr/Articletter/2015_Summer/GSI_Articletter_2015_Summer_Article6.pdf. adresinden alındı. (Erişim Tarihi, 12.05.2017).

Pickett, K.H. (2000*). The* ınternal *auditing handbook*, JohnWiley&Sons, Reprinted, England.

Samet, A. (2020). US Ecommerce will rise 18% in 2020 amid the pandemic, Emarketer. https://www.emarketer.com/content/us-ecommerce-will-rise-18-2020-amid-pandemic?ecid=NL1001 adresinden alındı. (Erişim tarihi: 3/08/2020).

Şahinaslan, Ö. (2003). *Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma* (Basılmamış doktora tezi). 2-8. Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Türkiye Bankalar Birliği. (2015). *Dolandırıcılık eylemleri ve korunma yöntemleri*. https://www.tbb.org.tr/Content/Upload/Dokuman/7328/TBB-Dolandiricilik-Eylemleri-veKorunma-Yontemleri.html. adresinden alındı. (Erişim Tarihi, 12.05.2017).

Verma, A. & Bajaj, S.K. (2008). Cyber fraud: a digital crime. *IADIS International Conference Information Systems.*

Williamson, D. A. (2020). Uptick in US adults' social media usage will likely normalize post-pandemic,

EMarketer. https://www.emarketer.com/content/uptick-us-adults-social-media-usage-will-likely-normalize-post-pandemic?ecid=NL1001 adresinden alındı. (Erişim tarihi, 2/08/2020).

Yavanoğlu, U., Sağıroğlu, Ş. & Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi*, *15*,(1), 15-27.

Yılmaz, O. (2017*).* Küreselleşme sürecinde dönüşen güvenlik algısı ve siber güvenlik. *Siber Politikalar Dergisi (Cyberpolitik Journal), 2*.

The Institute of Risk Management. (2014). *Cyber risk executive summary.*

İnternet Kaynakları

Amazon. (2020). *Amazon.com.* Announces second quarter results. https://s2.q4cdn.com/299287126/files/doc_financials/2020/q2/update/Q2-2020-Amazon-Earnings Release.pdf adresinden alındı.

City of Vancouver. (2016). *Internal audit summary report*. http://vancouver.ca/files/cov/internal-audit-cybersecurity.pdf adresinden alındı.

Ecommerce Foundation (2017), *Global Ecommerce Report 2017, http://mazarsusa.com/wp-content/ uploads/2017*/11/Global-Report-2017-1.pdf adresinden alındı. (Erişim Tarihi, 10.03.2018).

ISACA (Information Systems Audit and Control Association). (Mart 2015). Cyber security audit İnternet, *Türkiye'nin Siber Güvenlik Politikası.* http://www.ankarastrateji.org/ haber/turkiye-nin-siber-guvenlikpolitikasi-991/ adresinden alındı.

Statista. (2015). *Types of cyber crime in companies in Germany* 2015. https://www.statista.com/statistics/429635/cyber-crime-in-companiesgermany adresinden alındı.