YÖNETİM BİLİŞİM SİSTEMLERİ DERGİSİ
http://dergipark.gov.tr/ybs

Yayın Geliş Tarihi: 01.04.2021
Yayına Kabul Tarihi: 16.06.2021
Online Yayın Tarihi: 07.07.2021

Cilt:7, Sayı:1, Yıl: 2021, Sayfa: 44-60
ISSN: 2148-3752

YENİ NORMAL DÜNYA DÜZENİNİN SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİNE ETKİLERİ

Onur Korucu, M.Sc., LL.M

Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, İstanbul Bilgi Üniversitesi, İstanbul, Türkiye

ÖZET

Hızla değişmekte olan dünya teknoloji sahası, Dünya Sağlık Örgütü'nün (DSÖ) 30 Ocak 2020 tarihinde küresel pandemi olarak ilan ettiği Covid-19 salgını ile yeniden şekillenmiştir. Yaşanan pandemi, teknoloji başta olmak üzere sosyal, sağlık, eğitim, ekonomi, güvenlik, gıda, tedarik zinciri, iletişim ve ulaşım vb. birçok sektörleri kritik seviyede etkilemekte, küresel ve ulusal ölçekte sıra dışı boyutta değişimlere sebebiyet vermektedir. Yeni normal düzende, bilinen siber güvenlik ve veri hırsızlığı saldırılarına farklı bilişim platformlarında yaşanan veri güvenliği ihlalleri eklenmiştir. Dijital ortamlarda veri güvenliğinin sağlanması, tüm iş modellerinin ve mevzuatlarla uyumluluğun merkezinde yer almaktadır. Veri güvenliğinin sağlanması hususunda denetim ve kontrol fonksiyonlarının sağlanabilmesi için birbirinden farklı yaklaşımlar kullanılmaktadır.

Veri güvenliği ancak, veri güvenliğinin bozulmasına sebep olan ya da olabilecek risk ve tehditlerin tayin edilmesi ve yönetilmesi ile mümkündür. Sürekli izlenebilir ve ölçümlenebilir veri güvenliği, kurumsal risk yönetimi modeli ile belirlenmiş risklerin yönetimi ve yeni tehditlerin öngörümlenebilmesi ile sağlanmalıdır. Yapılan çalışmada 2000'ler sonrasında şekillenen teknoloji sahasının, yaşanan olağan üstü şartlarda yeni dünya düzeni kuralları ile nasıl etkilendiği ele alınmış olup, daha dirençli bilgi güvenliği ve siber güvenlik yaklaşımlarına ilişkin öneriler sunulmaktadır.

Anahtar Kelimeler: Siber Güvenlik, Bilgi Güvenliği, Siber Dayanıklılık, Risk Yönetimi, Dijital Dönüşüm

EFFECTS OF THE NEW NORMAL WORLD ORDER TO CYBER AND INFORMATION SECURITY

ABSTRACT

The fast-changing world's technology concept reshaped by the Covid-19 virus when World Health Organization (WHO) declared it as a global pandemic. The pandemic critically affected many different sectors particularly technology and others such as social, health, education, economic, security, food, logistics, communication, transportation, etc. It caused global and national unorthodox and critical changes. New data security violations are added to the known cybersecurity and data theft attacks in new normal. All business models and compliance practices with the regulations point out data security within a digital environment as a root action. When it comes to data privacy different approaches provide the same output using audit and control functions.

Data security can only be maintained by identifying risks and threats that can exploit data and manage them. A continuously monitored and measured data security practice with corporate risk management model, can only be increased by the management of identified risks and forecasting new threats. This study provides suggestions in relation to more robust and consolidated information security and cyber security approaches by addressing how does the 2000's technology shaped with the new extraordinary conditions and the regulations of this new world.

Keywords: Cyber Security, Information Security, Cyber Resilience, Risk Management, Digital Transformation

GİRİŞ

Yaşanmakta olan pandemi etkilerinin yoğun şekilde hissedildiği bir yılı aşkın süreçte teknolojinin hızla değişip gelişmesi ile ortaya çıkan kişisel, kurumsal, ulusal ve uluslararası bilgi güvenliği ve siber güvenlik ihtiyaçları hususunda geleneksel güvenlik çözümlerinin yetersiz kaldığı görülmüştür. Bireyler, kurumlar ve devletler bir güvenlik ihlali ile karşılaşılıp karşılaşmayacağı endişesini geçtiğimiz yıllarda terk etmiş olup, yeni dünya düzeninde, bu ihlallerle ne zaman karşılaşacağı ve buna hazır olup olmadığı endişesini yaşamaktadır. Bununla birlikte, siber alanda yaşanan ilerlemeler bilginin niteliğini de değiştirmiş ve bilgi, siber ortamın en temel metalarından biri haline gelmiştir. Bilginin kullanılması, erişilmesi, saklanması 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).

Dijital devrimin yaygınlaşması ile iş hayatında lokasyon bağımsız hareket edebilme kabiliyeti artmıştır. Ancak dijital dönüşümün yararlarının yanısıra, özellikle kurumsal hayat için yeni güvenlik ihtiyaçları ortaya çıkmıştır. Kurumlar tarafından sağlanan geleneksel yaklaşımlı güvenlik önlemleri pandemi öncesinde yeterli olarak değerlendirilse dahi, kurumlara ait önemli bilgi varlıkları dijital dönüşümün etkisinde yepyeni tehditler ile karşılaşmaktadır. Önce cep telefonları daha sonra sosyal medya ve bulut teknolojilerinin hayatımıza girişi ile işletmelerin geleneksel sınırları her geçen gün genişlemekte hatta internet kullanımının yaygınlaşması ile sınırsız hale gelmektedir. Dijital dönüşümün bir parçası olan sektör bağımsız küçük, büyük ölçekte tüm organizasyonlar siber tehditlerin hedefindedir (Deloitte, 2020).

Dünya genelinde pandemi sebebi ile yaşanan benzeri görülmemiş kriz süreci, küresel ekonomide kaosa neden olurken, teknoloji dünyasında tedarik zincirlerinin bozulmasına, kurumsal sistem zafiyetlerinin su yüzüne çıkmasına sebep olmuş ve ortaya çıkan ihtiyaçlar neticesinde toplumsal bazda dijital dönüşüm adımları hızla atılmıştır. Yeni dünya düzeninde kaçınılmaz şekilde değişen kurumsal iş modelleri ile iş yapış yöntemleri her zamankinden daha hızlı dönüşüm içinde olmakla birlikte yaşanan krizde önceden hazırlıklı olunmayan iletişim ve aksiyon zorunluluklarını sağlamak hususunda kurumlar varoluşsal bir hayatta kalma mücadelesi vermektedir.

Covid-19 salgının ortaya çıkması ile birlikte küresel düzeyde bir internet bağımlılığı ve buna bağlı dijital ekonomi değişkenlerinin hakim olduğu teknoloji sahası oluşmuş, normal düzende yılları alması beklenen dijital dönüşüm yapılanması birçok üst düzey teknoloji yöneticisinin yapamadığı şekilde aylar içinde gerçekleşmiştir. İçinde bulunulan durum, kurumların ve devletlerin iç sistemlerinde yaşanan dijital altyapının mimarisi sorunlarına dikkat çekerken, özellikle ekonomik parametreler, jeopolitik konum ve veri güvenliği gibi önemli konularda alınacak yeni önlemleri su yüzüne çıkarmıştır. Ortaya çıkan dijitalleşme risklerinin bütüncül olarak ele alınması, kurumların küresel işlevlerini ve endüstri ekosistemlerini etkileyecek tehlikeli bir domino etkisinden kaçınmak için mecburi bir eylem niteliğindedir.

Yaşanan pandemi sürecinde ortaya çıkan dijitalleşme zorunluluğunun yıllar içinde olgunlaşarak gelişen bir bilişim ortamı yeterliliğinde sağlanamaması sebebi ile kurumlar uzaktan erişim ve bilişim kabiliyeti gibi yeteneklerini acil durum yöntemleri ile sağlayabilmişlerdir. Sağlanan dijitalleşme çok hızlı ve güvenlikten ziyade işlev odaklı olarak gerçekleşmiştir. Değişen teknoloji ekosistemine uyum sağlanması amacı ile gerçekleştirilen ancak yeterli güvenlik yaklaşımı tasarlanmamış her türlü karar ve aksiyon sonrasında yepyeni bilişim riskleri ve siber tehditler oluşmaktadır.

Uzaktan erişimin büyük oranda benimsenmesi ile evden çalışmayı mümkün kılan bulut hizmetlerine dayalı dijital uygulamaların kullanılması mecburi bir ihtiyaç haline gelmiştir. Dijital dönüşüm hareketinin en önemli oyuncularından olan bulut bilişimin kişisel veriler olarak nitelendirilen hassas verilerin korunmasına yönelik yerel ve küresel hukuki düzenlemelerden etkilenmesi ve kullanım sahası bulması tartışmalı süreçlerin ortaya çıkmasına sebep olmuştur. Bu bağlamda dijital

dönüşüm bakış açıları ve kurumsal altyapı mimarileri yeniden şekillenmekte, artan risklere ilişkin siber güvenlik farkındalığı kurumsal düzeyde artmaktadır.

Bu itici güçlerin birleşmesi kritik operasyonlar ve geniş endüstri ekosistemleri üzerinde küresel olarak büyük etki yaratmıştır.

- Uzaktan çalışmanın yaygınlaşması ile kişisel ve kurumsal cihazlara, herhangi bir güvenlik katman yapısı bulunmayan ev internet ağlarına, mobil uygulamalara vb. gerçekleştirilen siber saldırı girişimleri katlanarak arttırmıştır.
- Uzaktan çalışma ortam şartları sebebi ile güvenlik farkındalığı azalan ve kurumsal güvenlik adımlarını benimsememiş kurum çalışanları üzerinde sosyal mühendislik yönelimlerinin etkisi artmıştır.
- Birbirine bağlı tedarik zinciri yapısı ile çalışan, iç içe geçmiş kurumsal bilişim yapılarında yüksek düzeyde siber güvenlik dayanıklılığı sağlamak daha zor bir hale gelmiştir.
- Kullanılmakta olan bulut tabanlı yeni hizmetlerin hızlı dağıtımı ve kurumsal ağ mimarisindeki değişiklikler, önemli risk güvence adımlarının bypass edilmesine ve daha geniş kapsamlı teknolojik ekosistem etkilerine sebep olmaktadır.
- Kritik varlıklar ve iş fonksiyonlarının, ulusal bazda artan güvenlik zafiyetlerinden ötürü siber saldırılara maruz kalma oranı yükselmiştir.
- Hastanelerin ve sağlık kurumlarının teknolojik altyapıları başta olmak üzere temel kritik altyapı hizmetleri, sürekli değişen formda karşımıza çıkan fidye yazılımı (ransomware), kimlik avı dolandırıcılığı (phishing scams) vb. saldırılardan büyük ölçüde etkilenmiştir.

Kurumların teknoloji yöneticilerinin, mevcut şartlar altında iş sürekliliğini sağlayabilmeleri için teknolojik ekosisteme uygun stratejik kararları alabilmeleri ve yeni düzenin içinde en verimli iş modelini yeknesak bir yaklaşımla kurum kültürü olarak benimsetmeleri büyük önem arz etmektedir.

Siber güvenlik dayanıklılığı, farklı disiplinlere uyumluluğun sağlanması ve her katmanda dijitalleşebilme kabiliyetlerinin kazandırılması ile mümkün olacaktır. İş sürekliliğinin sağlanması açısından internetin ve dijital kanalların kullanımının yaygınlaşması, bir operasyonel risk olan siber güvenliğe daha büyük bir önem kazandırmıştır.

Yapılan çalışmada yaşanan pandemi sürecinde değişmekte olan teknoloji sahasında, bilgi güvenliği ve siber güvenlik yaklaşımlarına dair kurumların alması gereken önlemlere ilişkin faydalı olacağına inanılan bilgiler paylaşılmış, sektörel analizlere yer verilmiştir.

PANDEMİ SÜRECİNDE SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ KAVRAMI

Siber kavramı, bilişim ortamları ve bilişim ağlarını içeren varlıkları tanımlamak için kullanılır. Siber uzay (cyber space) kelimesi de birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır (National Cyber Security Framework Manual, 2018). Siber saldırı ise "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" şeklinde tanımlanmıştır.

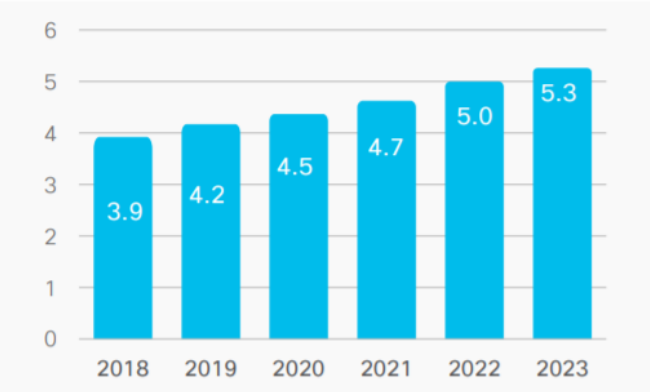
Siber ortamlar dinamik yapıları gereği beklenmedik durumların gerçekleşebileceği risk yüzdeliği yüksek ve çeşitli saldırılara maruz kalabilecek yapıdadır. Bilgi teknolojileri (BT) sistemlerinin; fiziksel güvenlikten haberleşme güvenliğine, yayınım güvenliğinden bilgisayar güvenliğine, ağ güvenliğinden bilgi güvenliğine, cihaz güvenliğinden sistem güvenliğine, yazılım güvenliğinden donanım güvenliğine, bulut ortamlarının güvenliğinden siber güvenliğe kadar birçok tedbirin alınması gerektiği bilinmeli ve korunacak olan siber varlıkların sınıfına, ortamına veya değerlerine göre gerekli güvenlik seviyeleri belirlenmeli ve koruma sağlanmalıdır (Sağıroğlu vd., 2012).

Pandemi sürecinde bilinen siber güvenlik ve bilgi güvenliği kavramları güncellenmiş ve bu kavramlara küresel çapta yaşanan ekonomik kriz ortamında yeni anlamlar yüklenmiştir. Pandemi sürecinde artan dijital faaliyetler çerçevesinde, siber güvenlik ve bilgi güvenliği konseptinde göze çarpan güncel yaklaşımlar, iş sürekliliğinin sağlanabilmesi için yaşanan ikilemin önemli göstergelerindendir. Pandemi sürecinde iş sürekliliğinin sağlanması, ekonomi çarklarının dönmesi ve

arz talep dengesinin sağlanabilmesi için birincil yöntem olan uzaktan çalışma modeli siber saldırılara tam anlamıyla bir davetiye çıkarmıştır. Uzaktan çalışma modeline, bilişim altyapısı ve bilgi güvenliği sistematiği perspektifinden hazır olmayan birçok kurum, bu yönteme hızlı bir geçiş yaparak, uzun süredir siber güvenlik açısından zaten var olan zorlukları daha da gün yüzüne çıkartmıştır. Sanal özel ağ (virtual private network-VPN) kullanmayan kurum çalışanları tarafından güvenli olmayan yollarla, kritik verileri trafiği yaşanması, mevcut risklerin azaltılması yaklaşımlarının uygulanmasında büyük ölçüde tutarsızlık yaratmıştır. İş faaliyetlerinin sağlanması konusunda kurumların göze aldıkları risk etkileri, kurumların belirledikleri siber güvenlik ve bilgi güvenliği risk iştahlarının çok üzerinde kalmıştır. Yaşanan siber vakalar, kurumların siber güvenlik, bilgi güvenliği, bilgi teknolojileri vb. iş birimlerinde uzaktan çalışma sistemlerini daha güvenli bir hale getirmeleri için aşırı efora sebebiyet vermiş, kurumların teknoloji yönetimi hususunda zayıf olduğu yönleri açığa çıkarmıştır. Kurum çalışanlarının internete bağlanabilen her türlü mobil cihaz ve bilişim kanalı aracılığı ile kritik altyapılara bağlanabilmeleri, kurumsal güvenlik kriterlerinin kriz koşullarına uygun hale getirilmesi ihtiyacını belirlemiştir.

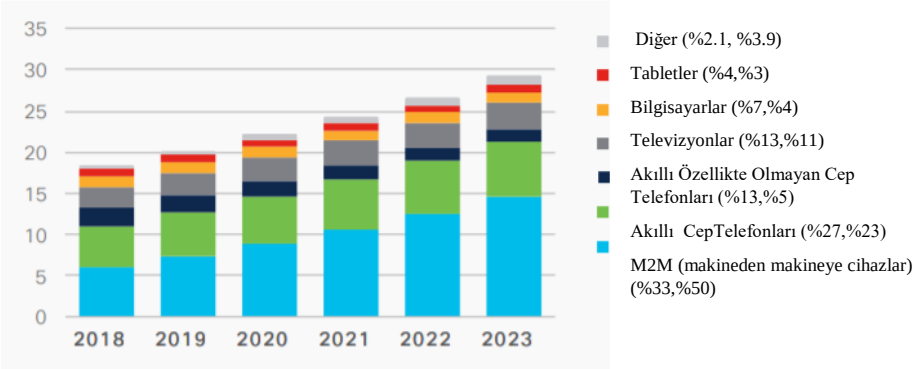
Günümüzde siber güvenlik ve bilgi güvenliği kavramları, dijital herhangi bir platformun, uygulamanın, bilişim yönteminin kullanıldığı her türlü faaliyetin bir parçası olmuştur. Değişen teknoloji kapasitesinin her geçen gün artması yeni güvenlik risklerini beraberinde getirmektedir. Uluslararası araştırmalar göstermektedir ki, küresel nüfusun yaklaşık üçte ikisi 2023 yılına kadar internet erişimine sahip olacaktır. 2018'de 3,9 milyardan (küresel nüfusun %51'i) 2023 yılına kadar 5,3 milyar toplam internet kullanıcısı (küresel nüfusun %66'sı) olması beklenmektedir (Cisco Annual Internet Report, 2020).

Tablo1. 2018-2023 Dünya Genelinde İnternet Kullanımı (milyar)



İnternet kullanımındaki artış, ağ bağlantılı çalışan ortalama cihaz sayısındaki artışı hızlandırırken, hane ve kişi başına bağlantı sayısında da büyük artışlar görülmektedir. Her geçen yıl farklı form faktörlerinde çeşitli yeni cihazlar artan dijital yetenekleri ile piyasaya tanıtılmaktadır. Yapılan değerlendirmelere göre, özellikle M2M (makineden makineye) kablolu ve kablosuz dahil herhangi bir iletişim kanalı kullanan cihazlar arasında doğrudan iletişim modelleri, akıllı sayaçlar, video gözetimi, sağlık izleme, ulaşım ve paket veya varlık takibi gibi cihazların ve bağlantıların artmasına büyük ölçüde katkıda bulunmaktadır. 2023 yılına kadar M2M bağlantıları toplam ağ bağlantılı cihazların ve bağlantıların %50'si kadar kadar artarak 14,7 milyar bağlantıya ulaşacaktır. Akıllı telefonların kullanımı yüzde 7'lik, ağ bağlantılı televizyonlarınkullanımı ise yaklaşık %6'lık artış göstererek 2023'e kadar 3,2 milyara ulaşacaktır. 2018'de 18,4 milyar iken, 2023'e kadar 29,3 milyar ağ bağlantılı cihaz olacağı öngörülmektedir. 2019 da dünyada günlük alınan ve gönderilen e-posta sayısı ortalaması 293,6 milyar ve bu sayının 2022'de 333,2 milyar olması beklenmektedir (Cisco Annual Internet Report, 2020).

Tablo 2. Dünya Genelinde Ağ Bağlantılı Cihaz Kullanımı (milyar)



Yaşanan sosyal mühendislik vakaları Covid-19 salgını süresince ciddi şekilde artış göstermiştir. Saldırganlar, gerçek kullanıcıları kandırarak kurumların mevcut güvenlik önlemleri ile güvenliğini sağladıkları sistemlerden bilgi ve para çalmaya ya da sistemlere erişim kazanmaya çalışmaktadır. Yaşanan en yaygın sosyal mühendislik vaka örnekleri, saldırganların uzaktan çalışma şartlarında oluşan kullanıcı zafiyetlerini kullanıp şirketlerin destek hatlarını arayarak "text phishing" ("yazılı oltalama saldırıları"), "voice phishing" ("sesli oltalama saldırıları")gibi teknikler vasıtası ile kendilerini çalışan gibi tanıtarak gizli bilgilere ve sistemlere erişim sağlamaya çalışmalarıdır. Yaşanan bu durum açıkça ortaya çıkarmıştır ki, teorik güvenlik yaklaşımları, iş süreçlerinin bir parçası olarak bilgi güvenliği yönetim sistemleri ile kurumsal yapılara uçtan uca nüfuz etmedikçe ve tüm kurum çalışanları bu güvenlik gereksinimlerini benimsemedikçe işlevsel ve uygulanabilir değillerdir. Pandemi süreci, kurumlara güvenlik farkındalık seviyelerini değerlendirebilmeleri için bir bilanço çıkarmıştır. Web ve e-posta güvenliği için filtreleme teknolojilerinin kullanılması ve bu tip siber saldırılardan kaynaklı hasarı azaltmak adına özelleştirilmiş kuralların devreye sokulması alınabilecek güvenlik önlemlerindendir. Özellikle hastaneler, sağlık kuruluşları ya da kritik altyapıya sahip kurumlarda güncel beyaz uygulama listeleri (white-list) kullanılması insan hatası riskini azaltmak için tercih edilmektedir.

Saldırganlar, pandemi öncesi süreçte olduğu gibi pandemi sürecinde de kötü amaçlı yazılımları kurumsal sistemlere aktarabilmek için zayıf güvenliğe sahip web sitelerini kullanmaktadırlar. Salgın ile savaşmak ya da salgın ile ilgili bilgi paylaşmak kandırmacası ile oluşturulan kötü amaçlı yeni internet siteleri ve domainleri, saldırganların bu yeni web siteleri üzerinde zayıf noktaları bularak sürücü indirmeleri yolu ile kötü amaçlı yazılımlarını kullanıcılar arasında yaygınlaşmasına fırsat sağlamaktadır. Kurum çalışanlarının kritik kurumsal bilişim ortamları ve verilere erişimi olan iş bilgisayarları veya mobil cihazları vasıtası ile meraklarına yenik düşerek güvenlik gereksinimlerini sorgulamadan eriştikleri internet adresleri, çalışanların iş bilgisayarlarına kötücül yazılım, virüs vb. veya zafiyet yaratabilecek çeşitli siber tahribatın oluşmasına sebep olmaktadır.

Salgın süresince siber tehditler kamu sektörü üzerinde de büyük bir baskı yaratmıştır. Dünyanın farklı bölgelerinde devletler tarafından kamuoyuna sunulan açık veri kanallarının saldırıya uğraması, ulusal bazda hizmet veren sağlık kuruluşlarının işlemlerinin askıya alınması ve BT ağlarının kapatılarak, bakım gerektiren hastaların başka bir tesise taşımasına sebebiyet vermesi, kritik devlet departmanlarının altyapılarının fidye yazılımlar tarafından şifrelenmesi ve yetkililerin bilgi paylaşımı ve dosyalara erişiminin engellenmesi gibi birbirinden tehlikeli siber saldırılar yaygın hale gelmiştir.

PANDEMİ SÜRECİNDE SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ GELİŞMELERİ

Covid-19 salgını sebebiyle kurumların mevcut teknoloji stratejileri ve bununla birlikte siber güvenlik yaklaşımları da değişmektedir. Teknoloji dünyasının bu değişimi ülkelerin hukuki uyum bakış açılarını da yeniden şekillendirmeye sevk etmektedir. Özellikle ülkemizde son yıllarda yaşanan hukuki yansımalar ve güncellenen mevzuatlar da artık bilişim güvenliğinin önemini farklı sektörler

perspektifinde açık ve net olarak ortaya koymaktadır. Başta bankacılık, elektronik haberleşme vb. dijital dönüşüme öncülük eden sektörlerde, pandemi gölgesinde geçen 2020 yılında yürürlüğe giren yasal düzenlemeler güvenlik konusuna verilen önemin ne denli kıymetli olduğunu göstermektedir.

Covid-19 pandemisinin yaşanmakta olduğu günümüzde, dünya genelinde küresel ekonomiyi etkileyen dinamikleri ve dünya nüfusunun genelini etkileyen dijital güvenlik ihtiyaçlarını güncel konjonktürleri göz önünde bulundurarak anlamak çok önem kazanmıştır. Kurumların teknoloji yatırımları hususunda yaptıkları planlamaları büyük oranda etkileyen siber suçların mekanizmalarını ve bu tehditlerin yayılmasında rol oynayan etkenleri doğru analiz etmek çok önemli bir hale gelmiştir. Dünya genelinde literatürde konuya ilişkin farklı yaklaşımlarla bu tür olayların nasıl ortaya çıktığı değerlendirilmekte, siber suçların sistemik yaklaşımları tanımlanmakta ve bu tehditler için birçok çözüm yöntemi önerilmektedir (Kotenko vd., 2013; Hindy vd., 2018). Bu süreçte başta sağlık sektörü olmak üzere kritik sistem altyapılarının hedef alındığı siber saldırılar konusunda dünyada yaşanan gelişmelere bakıldığında, 8 Nisan 2020 tarihinde Birleşik Krallık Ulusal Siber Güvenlik Merkezi (NCSC), Amerika Birleşik Devletleri İç Güvenlik Bakanlığı (DHS), Siber Güvenlik ve Altyapı Güvenliği Ajansı (CISA) ortaklığında bir rapor yayınlamış ve raporda, pandemi sürecinde siber suçluların gelişmesinin önüne nasıl geçileceği, gelişmiş siber tehditlere (advanced persistent threat-APT) karşı nasıl önlemler alınması gerektiği konusunda bilgilendirmeler yapmıştır (UK's National Cyber Security Centre vd., 2020). Yayınlanan raporda kimlik avı, oltalama, kötü amaçlı yazılım ve iletişim platformlarının (Zoom, Microsoft Teams, Google Hangouts, Skype vb.) kötü niyetli kullanımı konularına odaklanılmıştır (Lallie, 2006). Devletlerin yayınladığı raporlar ve sektörel siber güvenlik durum değerlendirmeleri gibi farklı kaynaklardan edinilen geri bildirimlerde, kontrol edilmesi ve sınıflandırılması zor, aynı zamanda farklı tipte siber saldırıların gerçekleştiği görülmektedir. Yaşanılan siber güvenlik vakalarına olan yaklaşımlar kurumların iç dinamikleri ve iş sürekliliği çevikliği, ülke regülasyonları ve ekonomik dinamiklere göre birbirinden farklı yöntemlerle çözümlenmektedir.

Pandemi sürecinde tecrübe edilen siber vakalar, tespit edilen siber vakalarda ülkelerin birbirinden farklı siber güvenlik dayanıklılıklarını ön plana çıkmaktadır. Her ülke siber güvenlik dayanıklılığını güçlendirebilmek için farklı yaklaşımları benimsemektedir. Farklı ülkelerin küresel siber güvenlik endeksi ve siber güvenlik taahhüdü sıralamalarına bakıldığında ABD her iki endekste de ilk sıralarda yer aldığı, Birleşik Krallık ve Fransa'nın ise endekslerde üst sıralarda yer aldığı görülmektedir. Türkiye siber güvenlik endeksi sıralamasında Rusya ve İtalya'dan önde 20. sırada yer alırken, Siber Güvenlik Taahhüdü sırlamasında ise 40. sırada yer alarak sadece Meksika ve Endonezya'nın önünde bulunmaktadır. Bu kapsamda genel olarak Türkiye'nin uzaktan çalışmaya ilişkin siber güvenlik veri ve ağ yönetimi konularındaki yetkinliğinin gelişime açık olduğu değerlendirilmektedir. Pandemi sürecinde karşılaşılan yeni tip siber saldırıların yanı sıra bilinen tip siber saldırılara karşı birçok kurumun güvenlik kanallarının hazırlıksız oldukları ve birçok kurum çalışanının güvenlik hususunda yeterli farkındalık seviyesinde olmadıkları görülmüş ve bu durum ortaya olumsuz sonuçlar çıkarmıştır. Pandemi öncesi ve sonrası gerçekleşen siber saldırılara ilişkin hazırlanacak kümülatif raporlar, dünya genelinde sektörel ve lokasyon bazlı dağılımın görülmesini sağlayabilecektir (Kolomiyets vd., 2012; Van Heerden vd., 2016; Horton vd., 2018).

Yaşanan pandemi sürecinde evden çalışma yüzdesinin önemli bir oranda arttığı görülmektedir. Özellikle bazı ülkeler dönüşümlü çalışma yöntemini uygularken, başta bazı Avrupa Birliği (AB) ülkeleri olmak üzere birçok ülkenin gerek görmedikleri sektörler için tamamen evden çalışma modelini uyguladıkları bilinmektedir (BBC, 2021). Kurumsal kritik kaynaklara uzaktan erişimin güvenli ve izole şekilde sağlanabilmesi şirketler için en önemli ihtiyaçlardan birisi haline gelmiştir. Uzaktan erişim yöntemleri, gerekli güvenlik gereksinimlerini karşılamadığı hallerde önemli riskler barındırmaktadır. Pandemi sürecinde uzaktan erişim ve iletişim ihtiyaçları için dijital çözüm platformları sağlayan firmalar birçok siber saldırının hedefi haline gelmiştir. Özellikle her türlü iş operasyonunun konu olduğu toplantıların gerçekleştirildiği bu dijital iletişim platformlarında geniş yetkili erişimlerin düzenli olarak izlendiğinden emin olunması ve sistem yöneticisi (admin) seviyesindeki kullanıcıların ya da hassas veriye erişimi olan personelin olası şüpheli işlemlerini tespit etmek adına davranışsal analitik araçlar kullanılması kritiktir.

Kurumsal güvenlik yaklaşımının yeknesak bir şekilde sağlanmasında kurumların tercih ettiği önemli güvenlik önlemlerinden biri VPN uygulamalarıdır. VPN uygulamaları, kullanıcıların izole

ağlar üzerinden, kurumsal bilişim sistemlerine uzaktan bağlanıp kullanabilmelerini sağlayan, sanal özel ağlar olarak tanımlanabilir. VPN, uzaktan erişim sağlayan kurum çalışanları ile kurum ağı arasındaki iletişimin şifreli olarak gerçekleştirilmesi ve kullanıcı IP adresinin gizli tutulması gibi güvenlik hizmetlerini kurum çalışanlarına sunmaktadır. VPN'in en büyük avantajı, kullanıcı ile kurumun izole ağı arasında güvenli, müdahale edilemeyen bir tünel oluşturarak, hassas verilere sahip olan kurumların siber saldırılardan korunmasına yardımcı olmasıdır. Bir diğer avantajı ise kullanıcının IP adresini gizleyip sadece özel ağın IP adresini görünür hale getirerek kullanıcıların internet üzerindeki aktivitelerinin üçüncü taraflarca izlenmesi zorlaştırmasıdır. Bu teknoloji çözümleri ile kurumların kendilerine özel oluşturulmuş iletişim hattı tahsis edilmesi yerine aynı hizmeti daha düşük maliyete herkes tarafından paylaşılan altyapıdan temin edebilmeleri sağlanabilmektedir. Ayrıca, birden fazla doğrulama yöntemi kullanılarak daha güvenli erişim sağlanması, ISO / IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Standardı, ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi / The Information Technology Infrastructure Library), COBIT (Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler-Control Objectives for Information and related Technology) gibi ülkemizde sıklıkla bilgi teknolojileri güvenliğinin sağlanması amacı ile kullanılan uluslararası standartların da önemli kontrol noktalarından biridir. VPN kullanımında, ağ cihazları ve uzaktan çalışmayı mümkün kılan her tip cihazın güncel yama ve güvenlik konfigürasyonlarına sahip olması için güncellemeler yapılması ve tüm VPN bağlantılarında çok faktörlü kimlik doğrulama (multi factor authentication) kullanılması, eğer bu mümkün değilse uzaktan çalışan personelin güçlü parolalar kullandığından emin olunması önemli güvenlik kontrollerindendir. VPN kapasitesinin BT güvenlik ekiplerince test edilmesi ve daha fazla bant genişliğine ihtiyacı olan kurum çalışanlarına bu imkanı verebilmek adına kısıtlamalara ilişkin politikalar oluşturulması ise güvenlik zorunlulukları arasındadır (Falliere vd., 2011; Yılmaz vd., 2020).

3 Aralık 2020 tarihinde 13'üncüsü düzenlenen Siber Güvenlik, Güvenli Veri Paylaşımı ve Transferi" temalı Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (ISC Turkey 2020)'nda yapılan açıklamalara göre, Türkiye'yi hedef alan ve engellenen siber saldırıların sayısı 2018'de 73 bin iken, 2019'da 150 bine çıkmıştır. 2020 yılında gerçekleşen ve engellenen saldırı sayısı ise 102 bini aşmıştır. Belirlenen bu sayılar ile Türkiye, dünyanın en çok atak alan ülkeleri arasında yerini almaktadır.

Pandemi sürecinde karşılaşılan siber güvenlik vakalarına sebep olan birçok etmen bulunmaktadır. Yeterli güvenlik altyapısı bulunmayan uzaktan masaüstü cihazların kullanımının %40 artması bu etmenlerden biridir. Pandemi sürecinde milyonlarca kurum çalışanının işlerine uzaktan çalışma yöntemi ile devam etmeleri, bulut bilişime bağlı uzaktan çalışma imkanı sunulan RDP (uzak masaüstü protokolü) ile yönetilen masaüstü cihazların sayısını artırmıştır. Yeterli bilgi güvenliği altyapısının ve kriptografik gereksinimlerin sağlanmadığı bu cihazların sayısındaki artış, masaüstü bilgisayarlara erişim sağlamak için brute force saldırılarının (kaba kuvvet saldırıları) düzenlenmesini kolaylaştırmıştır. Kompleks olmayan şifreleri kırmak için geliştirilen yazılımlara dayalı bu siber saldırılar, masaüstü bilgisayar aracılığı ile herhangi bir ağa sızılmasına olanak tanımaktadır. 2020 yılında RDP brute force saldırıları %400 oranında artmıştır. Bu saldırılardaki ciddi artışın iki temel sebebi masaüstü cihazların çok fazla işlem için kullanılması ve güvenlik önlemlerinin gerektiği gibi alınmamasıdır.

Pandemi sürecinde sıkça karşılaşılan bir diğer siber saldırı tipi, Covid-19 temalı e-posta dolandırıcılıklarıdır. Bu saldırı tipindeki örneklerin 2020 yılının Mart ayında dahi %667 oranında artmış olduğu belirlenmiştir. Covid-19 temalı dolandırıcılık vakaları, küresel alanda birçok ülkenin karantina ilan ettiği Mart ayında ciddi ölçekte artış göstermiştir. Covid-19 içerikli oltalama (phishing) saldırıları, hedefledikleri kişilerin kullanıcı ve kişisel verilerini ele geçirmeyi amaçlamaktadır. Pandemi sürecinde ilgi çekici anahtar kelimeler belirlenerek, hedef alınan kitleyi kandırabilmek için çeşitli bağlantılar ve tıklama ikonları oluşturularak gerçekleştirilmektedir. Pandemi sürecinde dijital verilerin paylaşımının artması, birçok kişinin resmi olmayan e-postaları kullanmasına neden olurken, sahte e-postalardaki bağlantılara veya yönlendirdikleri sahte web sayfalarına erişmek en sık gerçekleştirilen güvenlik ihlalleri arasındadır. Kurumsal iş bilgisayarları üzerinden, kişisel e-postalar aracılığı ile sağlanan veri paylaşımları, özellikle günümüzün hassas konularından kişisel veri ihlal vakalarının yaşanması ile neticelenebilmektedir. Covid-19 salgını sürecinde hedef kitle niteliğindeki

kullanıcıların tuzağa düşürülmesi amacı ile gerçekleştirilen oltalama saldırılarında "COVID", "coronavirus", "test", "quarantine" ve "vaccine" gibi anahtar kelimeler kullanılmaktadır.

İnternet arama motorlarında 2020 yılının başında "Covid-19" aramasına karşılık yaklaşık 6,1 milyon sonuç elde edilirken, bu sayı 2020 yılı sonunda 5 milyara ulaşmış durumdadır. Bu bağlamda, siber dolandırıcıların Covid-19 konseptini kullanarak çok çeşitli saldırı ortamları hazırladıkları görülmektedir. Bilgi güvenliği hususunda farkındalık sahibi olmayan kişiler ya da kurum çalışanları bu saldırı tiplerinden kolayca etkilenmektedir. Covid-19 konseptli sayısız web sayfası üzerinden gerçekleştirilen oltalama ve kötü amaçlı yazılım saldırıları ile siber suçlular, tuzaklarına düşen kişilere sahte ödemeler yaptırmakta, sahte Covid-19 tedavileri, malzemeleri hatta aşılar için ödeme yapmaya ikna etmektedir.

2020 yılı Aralık ayının başında teknoloji devi şirketlerin Covid-19 aşılarının dağıtımı için gerekli olan "soğuk zincir", yani aşının dağıtımı için kullanılan lojistik ağ alanında faaliyet gösteren bazı kurumların küresel ölçekli ve hedef odaklı bir oltalama saldırısı ile hedef alındığını açıklanmıştır. Yapılan geribildirimlere göre bu saldırılarda amaç, kullanıcı bilgilerine erişerek geleceğe yönelik erişim yetkisini ele geçirmektir. Bu sayede saldırganlar, geliştirilen aşının dağıtımı için metot, süreç, iç iletişim gibi konularda bilgi toplamaya çalışmaktadırlar. Benzer şekilde 2020 yılı Kasım ayı içerisinde, Covid-19 virüsüne karşı aşı geliştiren kurum çalışanlarına Linkedin ve Whatsapp üzerinden sahte iş teklifleriyle sosyal mühendislik saldırısı yapıldığı raporlanmıştır (Trendmicro, 2020). Bu çerçevede hükümetler, ilaç tedavisi ve aşı araştırmalarından, aşı dağıtım faaliyetlerine kadar içinde bulunduğumuz kriz dönemi süresince siber güvenlik anlamında tetikte olmalıdırlar.

Pandemi sürecinin en çok beklenen çıktısı olan aşı geliştirme faaliyetlerinde üretilen kıymetli bilgiye ek olarak, kişisel sağlık bilgileri ve hasta veriler de en değerli veriler arasındadır. Bu çerçevede, bu bilgiler siber saldırganlar tarafından sıkça hedef alınmaktadır. Dijital dönüşüm adımlarının sağlık sektöründe yaygınlaşması ile siber güvenliğin sağlık hizmetleri ve sağlık verileri için giderek büyüyen bir risk faktörü olduğu görülmüştür. Bu alanda araştırma yapılan araştırmalara göre, sağlık kuruluşlarını en çok etkileyen ilk beş risk aşağıdaki gibi tanımlamaktadır:

- Zararlı network trafiği
- Oltalama (phishing) saldırıları
- Operasyon sistemi zafiyetleri
- Ortadaki Adam Saldırıları (man in the middle)
- Zararlı yazılımlar

Uzaktan çalışma modeli ile iş dünyasında kullanılan iletişim platformlarının artışı ile en popüler video konferans uygulamalardan birisi olan Zoom, salgının başlangıcında birçok güvenlik skandalına maruz kalmıştır. 2020 güvenlik sektörü raporuna göre, ele geçirilen kötü amaçlı dosya ve kodlardan oluşan fidye yazılım örnekleri salgının başlangıcından bu yana %72, yaşanılan fidye yazılım saldırıları ise %105 artmıştır (Skybox Security, 2020; Sonicwall, 2020).

Yaşanan pandemi süresince %148 oranında artan uzaktan çalışma iş modeli, kurumsal bilgisayarların özel amaçlarla kullanımını da artırmıştır. Bu bilgisayarlardan, internetin en riskli alanlarından yetişkin içeriklere erişen çalışanların sayısı ise %600 artış göstermiştir. Covid-19 ile mobil cihaz zafiyetleri ise %50 artmıştır. Bu istatistikler, bireysel cihazların karşı karşıya olduğu büyük riski ortaya koymaktadır (Netskope, 2020). Tecrübe edilen güvenlik vakarının tekrar yaşanmasını önlemek için uzaktan çalışma modelinde kullanılan her tip kurumsal mobil cihazın diğer hane halkı tarafından kullanımına izin verilmemesi, kişisel bir cihaz üzerinden iş yapmak gerekirse antivirüs vb. güvenlik önlemlerinin alındığından emin olunması, alınabilecek önlemler arasındadır.

2020 yılında profesyonel hizmetler sağlayan denetim ve danışmanlık firmalarının hazırladığı raporda, 83 ülkedeki teknoloji devi şirketlerden 4 bin 200'den fazla CIO ve teknoloji yöneticisi katılımı ile gerçekleştirdiği CIO araştırmasına göre; pandeminin başında verilen küresel karantina alarmında şirketler teknolojiye ayırdıkları bütçelerin üzerine çıkmıştır. Teknoloji liderlerinin %86'sı iş gücünün önemli bölümünü uzaktan çalışmaya kaydırmış, %43'ü pandemiden sonra, mevcut ekiplerinin yarısından fazlasının uzaktan çalışmasını beklemektedir (KPMG, 2020). Uzaktan güvenli çalışma şartlarını sağlamak için haftada fazladan 15 milyar dolar harcanmıştır. Araştırmaya katılan her 10 bilgi teknolojileri (BT) liderinden dördü şirketlerinin siber saldırıya uğradığını belirtmiştir. Bu

saldırıların %83'ü oltalama-kimlik avı (phishing), %62'si uzaktan çalışma modelinde güvenlik zafiyetlerinden yararlanmak isteyen kötü amaçlı yazılım olarak sınıflandırılmıştır. Pandemi sürecinde teknoloji harcamaları büyük ölçüde artsa da, teknoloji bütçelerinin 2021'de daha fazla baskı altında olacağı beklenmektedir. Covid-19'dan önce BT liderlerinin %51'i 2021 yılı için ayırılması planlanan teknoloji bütçesinde artış beklenmekteyken, pandemi sırasında gerçekleşen aşırı harcamalar sebebi ile bu oran %43'e düşmüştür. Güvenlik ve gizliliğe yapılan yatırımların oranı %47 olarak tespit edilirken, altyapı ve bulut sistemlere yapılan yatırımlar Covid-19 sırasındaki en büyük üçüncü yatırım alanı olmuştur. BT liderlerinin neredeyse yarısı Covid-19'un, dijital dönüşümün parçası olan yapay zeka, makine öğrenimi, blockchain ve otomasyonun benimsenmesini hızlandırdığı görüşünde birleşmiştir.

Pandemi sürecinde gözlemlenen siber güvenlik yaklaşımları dönemsel olarak değerlendirilirse; çalışanların uzaktan çalışma modeline geçiş yaptığı ve herkesin yeni çalışma yöntemine uyum sağladığı pandeminin ortaya çıktığı ilk üç aylık süreçte, iş sürekliliği açısından güvenli uzaktan bağlantı ve ortak çalışma sistemleri devreye alınmıştır. Kurumsal kaynaklar iş gücünün yanı sıra, kritik varlıklara erişimin sağlanması ve bu varlıklarla ilgili erişimlerin izlenmesine ayrılmıştır. Özellikle bu süreçte kurumsal firmalar ani gelen beklenmedik salgın sürecinin yükümlülükleri karşısında kritik stratejik kararları endoğru şekilde almaya çalışmışlardır. 2020'nin ortalarına gelindiğinde altyapı güvenliği, kişisel verilerin güvenliği ve markaların itibarı yaşanan siber güvenlik tehditlerine karşı korunmaya çalışılmıştır. Artan siber güvenlik tehditlerine karşı, kurumların siber güvenliği sağlamak için ayırdıkları bütçelerin artırılması gündeme alınmıştır. 2020 yılı son çeyreğinde kurumlar siber güvenlik stratejilerini işlerin sürekliliği için pandemi şartlarına uygun olarak düzenlemiş, altyapı mimarilerine ilişkin değerlendirmelerini gereğinden çok daha kısa sürede gerçekleştirmiştir. Siber güvenlikte otomasyon kullanımı sağlayan kurumsal şirketler iş sürekliliği konusunda ilk dalga etkisinden az da olsa sıyrılmıştır. 2021 yılının ilk çeyreğine gelindiğinde ülkeler pandemiye karşı farklı çalışma modelleri belirlemiş, uzaktan çalışma pratiğinde eksik kalan adımlar profesyonel destek alınarak giderilmeye çalışılmıştır. 2020 yılında yaşanan siber vakalardan tecrübe edinen kurumlar özellikle çalışanlarına güvenlik konseptinin benimsenmesi ve uzaktan uygulanabilmesi için farkındalık eğitimleri vermiştir. Ancak pandemi sürecinde yaşanan belirsizlik ekosistemi, kurumların özellikle uzun vadeli teknolojik strateji planlarının güncellenmesi zorunluluğunu ortaya çıkarmış, tercih edilen siber güvenlik ürünleri ülkelerin yerel yasalarına uyumun sağlanması için daha çok talep görmüştür. Farklı coğrafyalarda hizmet veren kurumların dijital altyapılarını desteklemek için büyük yatırımlar yapması kaçınılmaz olmuştur.

Bu bağlamda, kurumsal şirketlerin bilgi güvenliği ve siber güvenlik yaklaşımları açısından gereksinimlerini doğru analiz etmeleri ve mevcut güvenlik risklerini belirlemeleri, verileri ve sistemleri korumak için büyük önem taşımaktadır. Kurumların teknoloji liderlerinin siber güvenlik için sistemik ve bütüncül bir yaklaşımı benimsemeleri dijital dönüşüm perspektifinde iş sürekliliğinin sağlanmasını kolaylaştıracaktır.

Devletler, kurumlar ve bireyler yaşanan pandemi sürecinden zarar görmüşlerdir. Ancak pandemi sonrası ekonomi ekosistemi, siber teknoloji sahasını en iyi yönlendiren kurumlar tarafından belirlenecektir.

PANDEMİ SÜRECİNDE İŞ SÜREKLİLİĞİNİN SAĞLANMASI

Kurumlara yönelik olası iş kesintilerinin etkilerini önceden tespit eden ve ilgili tüm paydaşların çıkarlarını, marka değerini ve değer oluşturma faaliyetlerini koruyan, olası tehditlere karşı esneklik kazandırmak için bir altyapı sağlayan bütünsel bir yönetim süreci, iş sürekliliği yönetimi olarak ifade edilir (ISO, 2019). Kurumlarda iş sürekliliğinin sağlanması hususunda en bilinen uluslararası standart ISO 22301:2019 İş Sürekliliği Yönetim Sistemi Standardıdır. ISO 22301 standardı, kurumları kesintiye uğratacak olaylar meydana geldiğinde bu durumlara karşı hazırlıklı olunması, cevap verilebilmesi ve geri dönülebilmesi için belgelenmiş bir yönetim sitemine ilişkin gereksinimleri belirler. Bu bağlamda özellikle pandemi sürecinde iş sürekliliği yönetim sistemine ilişkin alınmış önlemlerin değeri ve sertifika kontrol gereksinimlerinin uygulamadaki realitesi net bir şekilde yaşanarak anlaşılmıştır.

Dünya genelinde yaşanmaya devam eden pandemi süreci farklı sektörlerden kurumların iş sürekliliğinin aksamasına, karşılanamayan kritik ihtiyaçlar ülke ekonomileri üzerinde olağanüstü olumsuz etkilerin ve belirsizliklerin ortaya çıkmasına sebep olmuştur.

2021 yılı öngörümleme çalışmalarında olduğu gibi Covid-19 salgınının küresel ekonomik büyüme eğrisi ciddi şekilde aşağı çekilmiştir. Etkin bir kriz yönetimi gerektiren bu ortamda kurumlar ve yöneticiler, salgının stratejik hedeflerin tutturulması ve tüketici talebinin karşılanması üzerinde yarattığı etkilerin yönetilebilir olması için farklı yöntemlere başvurmuşlardır. Kurumların kriz ortamında, alması gereken acil aksiyonlardan kaynaklanacak orta ve uzun vadeli sonuçların yöneticiler tarafından iyi değerlendirilmesi gerekmektedir.

İş sürekliliği kavramı pandemi öncesi dönemde her ne kadar kurumlar tarafından uyum çalışmalarının bir parçası olarak değerlendirilmiş olsa bile, hazırlanan iş sürekliliği planlarının büyük bir çoğunluğu bu denli küresel bir krize sebep olabilecek pandemi durumunu bir risk etmeni olarak yeterli kapsamda ele almadığından günümüzde yaşanmakta olan sürece hazırlıksız yakalanmışlardır. Bu bağlamda farklı sektörden birçok kurumun iş süreklilik planlarını gözden geçirmeleri ve pandemi durumunu göz önünde bulunduran güncel bir iş süreklilik planı oluşturmaları gereği ortaya çıkmıştır (ISACA, 2020).

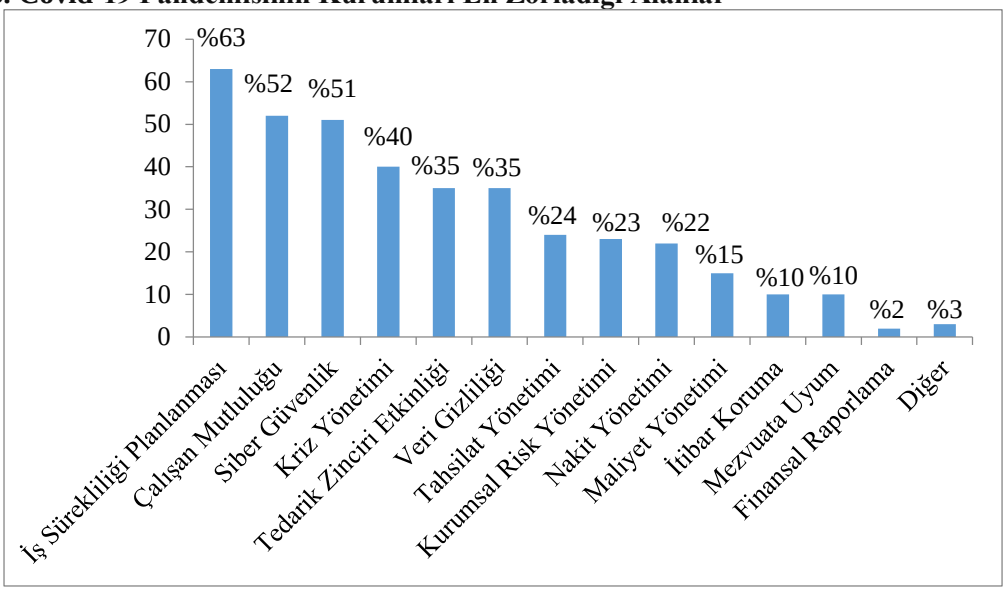
İş sürekliliği konseptinin en önemli çıktılarından biri kriz yönetimidir. Kurumların kriz yönetimlerini sağlamaları noktasında önceden hazırlanmış politika ve prosedürlere sahip olması özellikle pandemi sürecinde rekabet açısından belirleyici faktörlerden biri olmuştur. Kurumların ulaşmayı hedefledikleri güvenlik olgunluk seviyelerini gerçekleştirebilmeleri için, her türlü risk ve tehdidi en detaylı şekilde değerlendirerek gerekli önleyici faaliyetleri hazırlamış ve iletişim taraflarını belirlemiş olmaları gereksinimi önemlidir.

İş operasyonlarının sürdürülmesini sekteye uğratabilecek, yerel doğal afetlerden küresel salgınlara kadar birçok faktör, iş sürekliliği planlaması (BCP) ile bertaraf edilebilmektedir. Bir kurum için ortaya çıkabilecek tehditlerin önlenmesi ve zararın ortadan kaldırılması için bir sistem yaratma süreci olan iş sürekliliği planlaması, personelin ve varlıkların korunduğunu ve bir kriz anında hızla yeniden işlevsel olmalarını sağlamaktadır.

Kriz yönetiminde bir diğer önemli konu, tepki hızıdır. Her acil durum farklıdır ve doğası gereği farklı müdahaleler gerektirebilmektedir. Pandemi sürecinde yüksek sayıda kurum çalışanının uzaktan çalışma modeline geçmesi de bunlardan yalnızca bir tanesidir. Bu noktada veri merkezlerinde yaşanabilecek sorunlar ya da kapasite kısıtlılıklarına karşı, bazı iş yüklerini bulut sistemlerine paylaştırmak kriz durumlarında sistemin rahatlamasını sağlayacaktır.

Kriz durumlarının yönetilmesi BT liderlerinin doğru kararları zamanında alabilmeleri ve küresel analizlerinin ulusal pazarda etkinliği ile sağlanacaktır. Uluslararası profesyonel hizmet firmaları tarafından yayınlanan, pandemi sürecinde yaşanan gelişmeleri analiz etmek amacıyla birçok farklı kurumdan ve sektörden teknoloji lideri ile gerçekleştirilen ankette pandemi sürecinde kurumların hangi konularda yeterli etkinliği gösteremedikleri araştırılmıştır.

Tablo 3. Covid-19 Pandemisinin Kurumları En Zorladığı Alanlar



Ankete katılan teknoloji liderlerinin %63'ü iş sürekliliği planlamasının Covid-19 sürecinde karşılaştıkları eksikliklerden biri olduğunu belirtmiştir. %52'si çalışan mutluluğunun korunmasını, %51'i ise kriz yönetimi faaliyetlerini pandemi döneminde karşılaşılan zorluklar arasında değerlendirmiştir. İş sürekliliği planlaması; kurumlara ait kritik aktivitelerin zamanında yerine getirilmesine, kriz etkisinde olayların etkin bir şekilde çözümlenmesine, tehditlerin ve güvenlik açıklarının tespit edilerek risklerin minimize edilmesine, tedarik sürecinin devamlılığına katkıda bulunmaktadır. Hazırlanan raporda teknoloji liderlerinin %58'inin çalışmakta olduğu kurumun iç denetim planlarında iş sürekliliği bulunmazken, %63'ü bu süreçte kurumların zorlandığını belirtmiştir. İş sürekliliği konusunda zorluk çeken katılımcıların %61'i iş sürekliliği/kriz yönetimi alanlarında danışmanlık sağlayacak yetkin kaynakları olmadığını belirtmiştir (E&Y, 2020)

Günümüzde, kurumların yaşanan siber olaylara hızla yanıt verme çevikliğine sahip olmaları iş sürekliliği açısından önem taşımaktadır. Sorunlara çözüm bulmak, iş akışını sağlamanın yanı sıra sorunların sebeplerinin hızlıca analiz edilip ortadan kaldırılmasını da içerir. Kurumların acil durum ve kriz yönetimi yetkinliklerinin yaşanan pandemide yetersiz kalınan noktalar dikkate alınarak güncellenmesi, kurumların sistem ve veri yedeklerinin düzenli alınması ve kontrol edilmesi önemli çıktılar arasındadır.

Süregelen zaman içerisinde gözlemlendiği üzere, az miktarda devlet ve kurum dışında, pandemi sürecini öngörerek etkin iş sürekliliği planı yapan kurum sayısı neredeyse bulunmamaktadır. Birçok kurum pandemi durumunu iş süreklilik planlarında oluşabilecek bir risk etmeni olarak değerlendirmemiş veya es geçmiştir. Yaşanan Covid-19 salgını sonucunda, kurumların öngörmedikleri bu riskin, gelirlerini, müşterilerini ve çalışanlarını ne boyutta olumsuz etkilemiş olduğu ortaya çıkmıştır. Bu nedenle, oluşabilecek tüm riskleri olasılıklarıyla birlikte değerlendirerek proaktif bir iş süreklilik planının oluşturulması, belirlenen senaryoların test edilmesi ve uygulanması, ilgili kurumu küresel bir pandemiden korumak adına daha hazırlıklı kılacaktır (Marsh, 2020).

PANDEMİ SÜRECİNDE ALINMASI GEREKEN SİBER GÜVENLİK VE BİLGİ GÜVENLİĞİ ÖNLEMLERİ

Siber Dayanaklılık Kültürünün Teşvik Edilmesi

Siber risk yönetimi, her kurumun uçtan uca değerlendirmesi gereken bir unsurdur. Kurumların üst yönetimlerinin her türlü iş faaliyetlinde hesap verebilirlik ilkesini baz alarak gerekli risk unsurlarını şeffaf bir şekilde çalışanları ile paylaşması, kurumsal güven ortamını ve izlenebilir risk yönetimini sağlamaktadır. Şirketlerin yasal temsilcisi ve nihai karar mekanizması niteliğindeki yönetim kurullarının yaşanabilecek siber olayların kurumlarına vereceği zararı, hem hukuki hem de

itibar kaybı sonuçlarını çok iyi anlamaları ve gerekli önlemlerin alındığından emin olmaları gerekmektedir. Bu anlamda siber güvenlik dayanıklılığı gereksinimlerinin sağlanabilmesi için kurumlardaki ilgili tüm paydaşları süreçlere dahil ederek çok disiplinli ve entegre bir yaklaşım benimsenmelidir. Siber dayanıklılık bir kurumun içeriden veya dışarıdan gelen, bilinçli veya bilinçsiz sebep olunan her türlü tehdide uyum sağlama ve bunlara karşı koyma yeteneğini tanımlamaktadır. Siber dayanıklılık kavramı ile ifade edilen dayanıklılık sadece sistemlerin değil, insanların da olumsuz durumlara karşı gösterdiği duygusal direnci tanımlamak için kullanılır. Siber dayanıklılık, kurumlar için kritk verilerin ve hizmetlerin gizliliğinin, bütünlüğünün ve erişebilirliğinin korunmasıyla ölçülür ve bu koruma görevi en başta tüm kurum çalışanlarına aittir. Olası siber güvenlik senaryolarına karşı proaktif şekilde planlama ve hazırlık yapmak, kurumların potansiyel güvenlik açıklarının ve maruz kalınabilecek tehditlerin geç kalınmadan tespit edilmesini sağlamaktadır. Ayrıca siber saldırılara yönelik önceden verilen eğitim ve tatbikatlar kurumların siber dayanıklılığını artırmaktadır.

Siber dayanıklılık, kurum kültürü ve stratejisini belirleyen ana unsurlardan biridir. Covid-19 krizi sadece siber güvenliğe odaklanmanın dijitalleşme gereksinimlerinin karşılanması için yeterli olmayacağını aynı zamanda sürdürülebilir siber dayanıklılık yapısının şart olduğunu göstermiştir.

Kurumların siber dayanıklılık konusunda adım atmaları, büyük ölçüde dijitalleşme ve teknoloji yönetimi yaklaşımlarındaki değişime dayanmaktadır. Bu değişimde insan kilit bir rol oynamaktadır. Yapılan değerlendirmelerin geneli incelendiğinde insan faktörünün tüm veri ihlallerinin %90'ında kilit bir rol oynadığı görülmektedir. Siber dayanıklılığın sağlanabilmesi, dijital alanda atılacak doğru adımlarda kurum teknoloji liderleri ve çalışanlarının birlikte yürüyebilmesi ve doğru siber güvenlik yatırımlarının sağlanması ile mümkündür.

Siber dayanıklılık mevcut düzenlemelere uyum amacı ile yapılacak tek seferlik bir kontrol listesi üzerinden geçme eylemi (check-the-box) değildir. Siber güvenlik sahası çok hızlı değişim göstermektedir. Özellikle pandemi sürecinde kurumların iş sürekliliği, yaşanan siber vakalara yanıt verebilme kabiliyeti, çevik aksiyon alabilme ve riski giderme yaklaşımı hiç olmadığı kadar büyük önem kazanmıştır. Bu anlamda siber dayanıklılığın sağlanması kurumların sadece düzeltici değil aynı zamanda önleyici faaliyetlerini sağlamaları ve hızlı reaksiyon verebilen yapılar kurabilmeleri ile mümkün olacaktır.

Kritik Varlıkların ve Hizmetlerin Korunmasına Odaklanılması

Pandemi sürecinin en büyük olumsuz etkileri kurumların kritik hizmetleri, verileri ve varlıkları üzerinde hissedilmiştir. Kurum liderlerinin yaşanan kriz durumunun yarattığı olumsuz etkilerin çalışanlarını, müşterilerini ve iş ortaklarını ne boyutta etkilediğini değerlendirmeleri sürdürülmesi zorunlu operasyonların sağlanabilmesi için en önemli adımlardandır.

Uzaktan çalışma modellerinde veri güvenliğinin korunması ve siber güvenlik dayanıklılığının sağlanması uçtan uca güvenlik modelleri ile desteklenmelidir. Kurum çalışanları kurumların en önemli bilgi güvenliği belirleyicileridir. Bilgisayarlar ve mobil cihazlarda kullanılan yazılımların sürekli güncel tutulması, mobil uygulamalar ve diğer yazılımların yalnızca güvenilir platformlardan indirilmesi, bilgisayarlar veya mobil cihazlara belli aralıklarla düzenli virüs taramaları yapılması gibi kolay önlemler kurum çalışanlarının hatalarının yol açacağı siber vakaların önüne geçecektir. Kurumlarda kayıt yönetiminin otomatize edilebilmesi için Security Information and Event Management (SIEM) sistemleri kullanılması, sistemler ve ağlar üzerinde belirlenen senaryolar doğrultusunda anomalilerin tespitinin Güvenlik Operasyon Merkezi (Security Operation Center-SOC) ekipleri tarafından tespit edilmesi ve gereken yanıt verme çeviklikleri kurumlara ait kritik varlıkların ve hizmetlerin korunması açısından tercih edilen teknoloji çözümleri arasındadır.

Kurumlara ait kritik varlıkların ve hizmetlerin korunabilmesi öncelikle bu varlık ve hizmetlerin sınıflandırılarak, kritiklik seviyelerine uygun önlemlerin alınması ile mümkündür. Bu anlamda kurumların korumaları gereken her türlü hizmet, veri, sistem, personel vb. her türlü kritik varlığı güvenlik gereksinimlerine göre önceliklendirmeleri ve bu varlıkların risk analizlerinin yapılması bir kurumsal yönetim zorunluluğudur. Belirlenen güvenlik koşulları çerçevesinde her türlü kritik varlık kimlik ve erişim yönetimi mekanizmaları ile korunmalıdır. Güçlü kimlik doğrulama

prosedürleri ve gerekli hallerde yetkilerin kısıtlanması kriz durumlarında belirleyici önlemler arasındadır.

Uzaktan erişilebilir sistemlerin güvence altına alınması, kurumların veri sızıntılarını önlemek ve şüpheli durumları tespit etmek için katmanlı savunma sistemleri ile mümkündür. Uzaktan bağlanan uç noktalardaki kontrolü sağlamanın en doğru yöntemi çok faktörlü kimlik doğrulama kullanılan VPN yöntemleridir.

Kurum çalışanlarına ait tüm cihazlarda denetim izlerinin takip edilmesi ve sistemlerde karşılaşılan anomalilerin tespit edilmesi kurumlarda olası veri sızıntısı vakalarını önleyebilir. Kayıtlarnı gözden geçirilmesi, saldırıların tespiti ve analizi, olay müdahale ve kurtarma ekiplerinin eğitilmesi gibi siber güvenlik faaliyetlerine daha fazla önem gösterilmesi kurumları birçok siber saldırıdan koruyabilir.

Mevcut dijital dönüşüm adımları sonrasında kurumlar, sınırlı kaynakları akıllıca tahsis etmek zorundadır. Yapay zeka (AI), makine öğrenimi (ML) ve büyük veri gibi sıradan siber güvenlik süreçlerini otomatikleştiren ve insan hatası riskini en aza indiren teknolojilere yatırım yapmak kurumların siber geleceğini güçlendirecektir.

Kriz Sürecinde ve Sonrasında Riske Dayalı Kararların Dengelenmesi

Siber risk yönetimi ve risk transferi konusunda gereken aksiyonların alınmaması, marka ve itibar zararlarına, veri ihlallerine, regülasyon uyumsuzluklarına, müşteri memnuniyetsizliğine ve mali kayıplara neden olabilmektedir. Bu sebeple kurum yönetim kurulları başta olmak üzere tüm yöneticilerinin kurumların kriz süreçlerinde risk iştahlarını doğru belirlemeleri ve sektörel konumlarına göre risk profillerini çok iyi tanımaları gerekmektedir.

Kurum liderleri Covid-19 pandemi sürecinde teknoloji bütçelerini belirlerken kritik iş süreçlerinin güvenliğinin sağlanması için yatırım önceliklendirmesini doğru belirlemelidir. Ortaya çıkan kriz ortamında oluşan yeni zafiyetler, teknoloji risklerinin hızla büyümesine sebep olmaktadır. Bu sebeple yapılacak güvenlik yatırımları hem bugün bilinen hem de teknoloji liderlerinin görüşleri ile belirlenecek yarın oluşabilecek risk unsurlarına yönelik olmalıdır.

Etkin siber güvenlik dayanıklılığının kurumsal çerçevede sağlanması tüm risk etkenlerinin ve olasılıklarının değerlendirilmesi ile mümkündür. İyi bir siber güvenlik risk analizinin yalnızca metrik ölçülerle kantitatif raporlara dönüştürülmesi yeterli değildir. Bununla birlikte kurumsal stratejilere ve hedeflere entegre olmuş nitelikte olması şarttır. Aksi takdirde risk değerlendirme yaklaşımları iyi birer araştırma dokümanı olarak kalacak ve iş optimizasyonu için hayata geçemeyecektir.

Yeni Normale Geçiş Surecinde Süreklilik Planlarının Güncellenmesi ve Test Edilmesi

Kriz yönetimi bütün iş sürekliliği planlarının önemli bir parçasıdır. Bir tehdidin ya da vakanın yalnızca ortaya çıkma olasılığı değil aynı zamanda ne zaman ortaya çıkabileceği de ele alınmalıdır. Sadece bilinen riskleri analiz etmeye ve önlemeye yönelik çalışan bir kurum kriz yönetimi açısından iyi bir durumda olmayabilir. Bu yüzden, iş birimleri arası bir kriz yönetimi takımı kurmak ilk adım olmalıdır. Yaşanmakta olan pandemi gibi kriz durumlarında, kurum içindeki birbirinden farklı rol ve sorumlulukları olan çalışanları ortak bir hedef ve aksiyona doğru yönlendirmek konusunda detay içeren bir eylem planı çevik reaksiyonların alınabilmesi için yönlendirici olacaktır. Oluşturulacak kriz yönetim planları kurumu bütünüyle ele alarak, siber güvenlik faaliyetleri ve iş süreçlerini, birbirlerine bağlılıkları ile değerlendirmelidir.

Yöneticiler, siber saldırı ve pandemi senaryolarını da dahil ederek kurumu kriz süreçlerine hazır hale getirmek için olay yönetimi, felaket kurtarma ve iş sürekliliği planlarını test etmeli sürekli iyileştirmelidir. Bu planlar kriz süresince ve sonrasında iş sürekliliğini sağlamak için hazırlanmalı ve koruma sağlayabilir durumda olmalıdır. Hazırlanan planlar olay müdahale ve kurtarma konularını da içermelidir. Kurumlar, tüm iş birimlerinin katılımı ile risk yönetim yaklaşımlarının etkili ve etkin olduğunu değerlendirmelidir.

Pandemi ile benimsenen uzaktan çalışma modeli, artık kurumların işletme maliyetlerini düşürmek açısından sürekli olarak uygulayacağı bir çalışma sekline dönüşmektedir. Bu nedenle

kurumlar, güvenli uzaktan erişim altyapısını çalışanlarına sunmaya devam etmelidirler. Pandemi boyunca, kurumlar dijital mimarilerini ve mevcut teknolojilerini emsaline rastlanmamış bir hızla değiştirmeye çalışarak dijital dönüşüme ayak uydurmuşlardır. Bu dijital dönüşüm, yapay zeka (AI), bulut bilişim ve nesnelerin interneti (IoT) gibi teknolojilerle desteklenmekte, varlıklar, kişiler ve veriler arasında bağlantı kurulmasını sağlamaktadır. Siber risk yönetimi, bahsedilen yeni iş yapış modellerine hızlı bir şekilde uyum sağlamalı ve kurumun stratejik öncelikleri dikkate alınarak belirlenmiş kurumsal risk kabul seviyeleri, tüm çalışanların katılımını sağlayacak şekilde işbirliği içinde olmalıdır.

İş Ekosistemi Genelinde İşbirliğinin Güçlendirilmesi

Hem kamu ve özel sektör liderleri mevcut kriz durumu şartlarında karşılaşılan siber güvenlik saldırıları ve güvenlik zafiyetlerini tanımlamalı ve tecrübe edilen çıkarımlar ilgili sektörler ve makamlar ile paylaşmalı, gereken önleyici aksiyonların sağlandığından emin olmalıdır.

Kurumlar güvenlik beklentilerini birlikte çalıştıkları iş ortakları ve tedarikçileri ile paralel olacak şekilde iş birliğine gitmelidir. Bu sayede hukuki düzenlemeler ortak beklenti ile teşvik edilerek üçüncü taraf güvence hizmeti alınması sağlanabilir. Ülkemizde 2020 yılında özellikle bankacılık sektöründe güncellenen bankacılık bilgi sistemleri ve elektronik bankacılık düzenlemelere buna en doğru örnek niteliğindedir.

Dijital ekosistemin dağınık yapısı tek bir kurum üzerinden siber saldırı tiplerinin etkili bir şekilde tanımlanmasına olanak sağlamamaktadır. Siber saldırıların önlenmesi ve zamanında yanıtlanması için sektörlerin kolektif yaklaşımla gerçek zamanlı ve şeffaf siber güvenlik verilerini yansıtmaları şattır. Uygulanacak ulusal siber güvenlik politikalarında sektörler tarafından paylaşılan gerçek zamanlı veriler çok önemli yer tutacaktır.

Birbirine bağlı çalışan her bir cihaz bir siber saldırının giriş ve zıplama noktaları olabilir. Bu nedenle kurumsal düzeyde etkin bir sonuca ulaşmak ancak risk bazlı hazırlanmış güvenlik stratejilerinin uygulanması ile mümkün olacaktır.

SONUÇ

Yaşanmakta olan pandemi süreci göstermiştir ki, dijitalleşme, iş sürekliliği ve siber dayanıklılık kavramları bilinen bilgi güvenliği ve siber güvenlik kavramları içerisinde büyük bir öneme sahiptir.

Yaşanan siber güvenlik vakaları, kurumsal organizasyonlarda iş modelleri ve yasal mevzuatlara uyum çerçevesinde uygulanan güvenlik kontrollerinin, yeni çalışma ortamı olan evlerde ya da küçük ölçekli işletmelerde uygulanmasına sebep olmuştur. Pandemi öncesi önemi göz ardı edilen güvenlik konuları, uzaktan çalışma modeli ile herkes için daha yakınsanmıştır.

Güvenlik zincirinde kırılması en kolay halka olarak görülen insan kaynaklı hatalardan faydalanan siber saldırganlar, ev ve işyerlerindeki cihazları ele geçirmenin yeni yollarını aramaktadırlar. Çoğu zaman bu cihazlar kurumsal cihaz yönetimi kapsamının dışında bırakıldığından mevcut pandemi şartlarında etkisi büyüyen riskler olarak karşımıza çıkmaktadır.

Pandemi süreci ile yaşanan gelişmeler değişen iş modellerinin, teknolojik gelişmeler ve siber güvenlik önlemleri çerçevesinde yeniden gözden geçirilmesi gerektiğini işaret etmiştir. Covid-19 salgınının hayatımıza getirmiş olduğu hızlı ve yeni değişiklikler nedeniyle, iş gücünün büyük bir kısmı dijitalleşmeyi benimsemiş ve bu yolda küçük de olsa adımlar atmaya başlamıştır. Birçok kurum pandemi ile gelen bu hızlı değişimin ardından, var olan ve potansiyel siber zafiyetlerine karşı kendine geçici korunma önlemleri edinmiştir. Ancak, bu geçici çözümlerin farkına varan siber saldırganlar siber güvenlik politikalarını zorlayarak, siber saldırılarına devam edebilecekleri yeni kurumsal zafiyetler tespit etmeyi sürdürmektedirler.

Pandemi sürecinde sistemlerin neredeyse tamamen dijital sistemlere taşınması bilgi güvenliği üzerinde oldukça önemli bir baskıyı da beraberinde getirmiştir. Yaşanan siber saldırı olayları analiz edildiğinde saldırganların özellikle kötü niyetli e-posta saldırıları ve kullanıcıların kimlik bilgilerine

yapılan saldırılara odaklandıkları görülmektedir. Siber saldırılara karşı siber dayanıklılık kazanmak için bazı kurumsal güvenlik stratejilerini izlemek mümkündür.

- Kurumların güvenlik kültürünün önemi pandemi sürecinde kurum çalışanlarının kriz durumlarındaki davranışlarında belirleyici olmuştur. Kuruluşların, gerekli bilgi güvenliği ve siber güvenlik eğitimlerini tüm çalışanlarına vermeleri en büyük öncelik konusudur. Güvenlik farkındalığı, çalışanların iş hayatlarındaki yaklaşımlarını olumlu yönde değiştirecek, tehditlerin gerçek ve her zaman olası olduğunu unutmamalarını sağlayacak kurumsal güvenlik bakış açısı oluşturmalarını sağlayacaktır.
- Uzaktan çalışma iş modeline geçiş ile mobil cihazlara yönelik siber riskler daha da artmıştır. Dünya genelinde olduğu gibi her sektörden kurum çalışanları artan bir hızla mobil cihazlar kullanmaktadır. Bu bağlamda, mobil cihazları da varlık yönetimi ve risk değerlendirme mimarilerinin içinde değerlendirmek gerekmektedir. Mobil cihazlarda MDM (mobile device management-mobil cihaz yönetimi) uygulamalarının kullanılması ve kriptografik koruyucu önlemlerin alınması kurumsal bilgi güvenliği mimarisinin bir parçası olmalıdır.
- Kurumsal ağ yapısı üzerinden internete bağlı her cihaz için anti virüs programı kullanılması ve bu programların güncelliğinin düzenli olarak kontrol edilmesi zorunlu bir siber güvenlik aksiyonudur.
- Teknoloji dünyasında değişen ve gelişen dijitalleşme akımında siber uzay doğası gereği beklenmeyeni planlamak yani olası senaryoları önceden belirlemek ve belirsizlikleri azaltmak oldukça önemli bir rekabet gücü haline gelmiştir. Bu sebeple etkin ve etkili iş sürekliliği planlarının hazırlanması pandemi döneminin en önemli kurumsal ödevlerindendir.
- Uluslararası standart ve çerçevelerin önerdiği, teknoloji denetimlerinin en önemli kontrol noktalarının başında gelen şifre/parola güvenliği yetersizliği, pandemi döneminde kurum çalışanlarının siber saldırılarla karşı karşıya kalmalarına sebep olmuştur. Yeni dönem siber saldırganların kabiliyetleri düşünüldüğünde kompleks şifrelerin dahi kısa süreler içinde kırılabileceği bir gerçektir. Bu nedenle kurum çalışanlarının üzerine düşen önemli güvenlik uygulamalarından biri, kişisel amaçlı kullanılan internet hizmetleri (sosyal medya, e-posta, e-ticaret vb.) için kullanılan şifrelerin kurumsal uygulamalarda aynı sıra ve içerik ile kullanılmaması, kompleks yapıda oluşturulan şifrelerin/parolaların uzun ve tahmin edilemez yapıda oluşturulmasıdır. Şifrelerin periyodik değiştirilmesi eski BT denetim kontrolleri arasındayken yeni trend kontrollerde tercih edilen şifrelerin/parolaların uzun ve önceki versiyonlarından farklı olması öncelikli güvenlik beklentisidir.
- Kurumların mevcut sistemlerinde kurulacak yazılım veya uygulama gibi yeni veri işleme platformları gerekli kod kontrolleri gerçekleştirilerek, test ortamlarında gerekli analiz sağlanması sonrasında kullanılmaya başlanmalıdır.
- Çalışmada bahsedilen uzaktan çalışma modelinde kontrollü bir ağ yapısı VPN kullanımı ile sağlanmalı, katmanlı güvenlik ağı yapısı teknoloji liderleri tarafından bir güvenlik kalite unsuru olarak değil bir zorunluluk olarak uygulanmalıdır.
- Kurumsal kritik verilerin çalınması için tek zafiyet noktası siber ortamlar değildir. Her tip kurumsal cihazın çalınması ya da ele geçirilmesi veri ihlallerinin yaşanmasına sebebiyet verebilir. Bu çerçevede, korunan bilgileri içeren bilgisayar ve diğer türden elektronik cihazların, güvenli olduğu düşünülen alanlarda tutulması gerekmektedir.
- Pandemi sürecinde teknoloji yöneticilerini zorlayan diğer bir konu hukuki düzenlemelerde bilgi güvenliği ve veri güvenliği çerçevesinde gerçekleştirilen güncellemelerdir. Siber saldırıların günümüzde en büyük hedefi kişisel veriler olmaktadır. Bu anlamda teknoloji liderlerinin ulusal ve uluslararası düzenlemeleri mevcut yapılarında doğru şekilde entegre etmeleri ve uyum çalışmalarını bir kağıt üstü çalışma değil, güvenlik sistemlerinin güçlenebileceği bir destek kuvvet olarak kurumsal mimariye kazandırmaları gerekmektedir.

Pandemi kavramı henüz hayatımıza girmemişken de bilgi güvenliği ve siber güvenlik kavramları gelişen iş dünyasının en kritik unsurlarından biri konumundaydı. Ancak yaşanan pandemi sonucunda teknoloji ve internet bağımlı iş modelleri bir mecburiyet olmuştur. İş hayatında operasyonel hızı artırmak, teknoloji gereksinimlerini etkin bir şekilde sağlamak isteyen her kurumun siber güvenlik alanında yatırım yapması kaçınılmazdır. Siber saldırıları hızlı bir şekilde tespit etmek

ve siber güvenlik vakalarında ihtiyaçlara en kısa sürede yanıt vermek gelişmiş teknolojilerin kullanımı ile etkili olacaktır. Kurumların teknoloji liderlerinin siber güvenlik bütçelerini belirlerken profesyonel servisler ve teknoloji dünyası öncüleri tarafından pandemi sonrası oluşan siber ekosistemi değerlendiren raporları titizlikle incelemeleri ve teknolojinin sürekli değişen ve gelişen perspektifinde proaktif yaklaşımlarla doğru yatırımlar yapmaları bundan sonraki süreçte rekabeti belirleyen faktörlerin başında yer alacaktır.

KAYNAKÇA

Bayraktar, G. (2015). Siber savaş ve ulusal güvenlik stratejisi. İstanbul: Yeniyüzıl Yayınevi.

Deloitte, Global siber güvenlik yönetici bilgilendirme raporu (2020). https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/tr-web-kuresel-siber-guvenlik-yonetici-bilgilendirme-raporu.pdf, (25.03.2021).

NATO CCDCOE, National cyber security framework manual (2018). https://www.ccdcoe.org/uploads/2018/10/NCSFM_0.pdf, (26.03.2021).

Sağıroğlu, Ş. ve Alkan, M. (2012). Siber güvenlik siber savaşları, TBMM İnternet Komisyonu.

Cisco Annual Internet Report (2018-2023) White Paper (2020), https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html, (26.03.2021).

Kotenko, I. ve Chechulin, A. (2013). A cyber attack modeling and impact assessment framework, 5. International Conference on Cyber Conflict, CYCON 2013, IEEE, 1–24, 2013.

Hindy, H., Brosset, D., Bayne, E., Seeam, A., Tachtatzis, C., Atkinson, R. ve Bellekens, X. (2018). A taxonomy and survey of ıntrusion detection system design techniques, network threats and datasets, arXiv:1806.03517, vol. 1, no. 1, Article, 2018.

UK's National Cyber Security Centre (NCSC), the US' Department of Homeland Security (DHS) Cybersecurity, Infrastructure Security Agency (CISA), (2020). Advisory: COVID-19 exploited by malicious cyber actors. https://www.ncsc.gov.uk/news/Covid-19-exploited-by-cyber-actors-advisory, (25.03.2021).

Lallie, H. S., Shepherd, L.A., Nurse J. R. C., Erola, A., Epiphaniou, G., Maple, C., ve Bellekens, X. (2020). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic, arXiv:2006.11929v1, cs.CR, (21.03.2021).

Kolomiyets, O., Bethard, S. ve Moens, M. F. (2012). Extracting narrative timelines as temporal dependency structures, proceedings of the 50th annual meeting of the association for computational linguistics: long papers-Association for Computational Linguistics, vol:1, 88–97.

Van Heerden, R., Von Soms, S. ve Mooi, R. (2016) Classification of Cyber Attacks in South Africa", IST-Africa Week Conference, IEEE, 1–16, 2016.

Horton N. ve DeSimone, A. (2018) Sony's Nightmare Before Christmas: North Korean Cyber Attack on Sony and Lessons for us Government Actions in Cyberspace, JHUAPL, Tech. Rep., United States, 2018.

Falliere, N., Murchu, L. O. ve Chien, E. (2011) W32. Stuxnet Dossier,", Security Response, 5 (6): 29.

Yılmaz, Ö., Cömert, C. K. ve Güler, V. (2020) Havelsan Siber Güvenlik Bülteni, Siber Güvenlik Direktörlüğü.

Stubbs, J.(2020) Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources, Reuters, https://uk.reuters.com/article/uk-healthcare-coronavirus-astrazeneca-no/exclusive-suspected-north-korean-hackers-targeted-Covid-vaccine-maker-astrazeneca-sources-idUKKBN28719Y, (24.03.2021).

2020 Vulnerability and Threat Trends, Skybox Security, https://www.skyboxsecurity.com/wp-content/uploads/2020/07/2020-VT_Trends_Executive_Summary.pdf, (24.02.2021).

2020 Sonicwall Cyber Threat Report, Cyber Threat Intelligence for Navigating the New Business Normal, https://www.sonicwall.com/resources/2020-cyber-threat-report-mid-year-update-pdf/, (26.03.2021).

Cloudy with a Chance Of Malice, Forecasting the New Era of Cloud-Enabled Threats, Netskope, https://resources.netskope.com/cloud-threat-report/cloud-and-threat-report-february-2021, (26.03.2021).

KPMG (2020) https://home.kpmg/tr/tr/home/medya/press-releases/2020/12/sirketler-teknolojiye-haftada-fazladan-15milyar-dolar-harcadi.html, (26.03.2021).

ISO 22301:2019, Business Continuity Management System, Social Security, 3-4.

Snedaker (2021) Information Technology Executive, United States, 3, Business Continuity–Pandemic Preparation, https://www.isaca.org/resources/news-and-trends, (20.03.2021).

Ernst&Young LLP (2021) COVID-19'un İç Denetim Fonksiyonu Üzerine Etkileri Araştırma Sonuçları, Ernst&Young LLP, https://www.ey.com/en_gl/consulting/how-chief-audit-executives-areresponding-to-Covid-19-in-the-next, (21.03.2021).

Trendmicro (2020) Injecting Deception Mid-Pandemic: Covid-19 Vaccine Related Threats, https://www.trendmicro.com/en_us/research/21/c/injecting-deception-covid-19-vaccine-related-threats.html (14.06.2021)

BBC (2021) Remote working: Is Big Tech going off work from home?, https://www.bbc.com/news/technology-56614285 (14.06.2021)