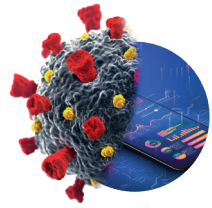


Küresel Salgın Sonrasında Ulusal Bilişim Güvenliği

Tolga Mataracıoğlu
Kerim Can Kalıpcıoğlu
Süleyman Muhammed Arıkan
Gökhan Işık
Yasemin Demiral
Derya Cincioğlu
Prof. Dr. Hacı Ali Mantar

Tolga Mataracıoğlu

2002 yılında İstanbul Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünden derece ile mezun olan Mataracıoğlu, 2006 yılında aynı üniversitenin Telekomünikasyon Mühendisliği bölümünü bitirmiştir. 2005 yılından bu yana TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nde çalışmakta olup aynı zamanda Siber Güvenlik Eğitimleri ve Çözümleri Biriminin yöneticiliğini yapmaktadır. Bilgi güvenliğiyle ilgili ulusal ve uluslararası pek çok makale sahibi olan Mataracıoğlu'nun çalışma konuları arasında sistem tasarımı ve güvenliği, işletim sistemi güvenliği, bilgi güvenliği yönetim sistemi, iş sürekliliği ve BT yönetişimi danışmanlığıyla sosyal mühendislik yer almaktadır.

Kerim Can Kalıpcıoğlu

Kalıpçıoğlu, 2017 yılında Yıldız Teknik Üniversitesi'nde lisans eğitimimi tamamlayarak Bursa Uludağ Üniversitesi Bilgisayar Mühendisliği anabilim dalında yüksek lisansa başladı. Mart 2018'de Eskişehir Osmangazi Üniversitesi Mühendislik Mimarlık Fakültesi Yazılım ana bilim dalında Bilgi Güvenliği alanında araştırma görevlisi oldu. Araştırma görevliliği süresince işletim sistemleri, sistem programlama, mikroişlemci sistemleri ve bilgi güvenliği konularındaki ders ve laboratuvarların yürütülmesine yardımcı oldu. Eylül 2019'dan beri TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nde Ar-Ge personeli olarak çalışmaktadır.

Süleyman Muhammed Arıkan

2015 yılında Pamukkale Üniversitesi Bilgisayar Mühendisliği bölümünden mezun olan Arıkan, 2019 yılında Gazi Üniversitesi Adli Bilişim bölümünde yüksek lisans derecesini almıştır. Eğitim hayatına Gazi Üniversitesi Adli Bilişim bölümü doktora programında devam etmektedir. 2016 yılında TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nde Araştırmacı olarak işe başlayan Arıkan, Uzman Araştırmacı olarak siber güvenlik teknolojileri geliştirme projelerinde görev yapmaktadır. Yazılım mühendisi olarak; web teknolojileri, veri tabanları, yazılım geliştirme, proje yönetimi, konfigürasyon yönetimi ve yazılım süreç iyileştirme konularında tecrübe sahibidir. Aynı zamanda TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü'nde enstitü kurulu üyesi olarak çalışan temsilcisi görevini sürdürmektedir.

Gökhan Işık

Işık, 2014 yılında Eskişehir Osmangazi Üniversitesi Bilgisayar Mühendisliği bölümünden mezun oldu. Aynı üniversitede Bilgisayar Mühendisliği ana bilim dalında yüksek lisans tez dönemindedir. 2016 yılından itibaren TÜBİTAK BİLGEM Bilgi Teknolojileri Enstitüsü Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı (B3LAB) biriminde araştırmacı olarak çalışmaktadır. 2019 yılından itibaren ise B3LAB biriminde bulut bilişim ve büyük veri altyapı ekip lideri sorumluğunu üstlenmiştir.

Yasemin Demiral

Demiral, 2014 yılında Anadolu Üniversitesi Bilgisayar Mühendisliği lisans ve 2019 yılında ise Gazi Üniversitesi Bilgisayar Mühendisliği yüksek lisans programından mezun olmuştur. 2016 yılından itibaren TÜBİTAK BİLGEM Bilgi Teknolojileri Enstitüsü Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı (B3LAB) biriminde araştırmacı olarak çalışmaktadır. 2018 yılından itibaren B3LAB biriminde bulut bilişim ve büyük veri altyapı ekibinde scrum master olarak görev almaktadır. B3LAB biriminde temel olarak sanallaştırma, konteyner, bulut bilişim teknolojileri, DevOps ve süreçlerin kesintisiz ve otomatik olarak gerçekleştirilmesi alanlarında çalışmaktadır.

Derya Cincioğlu

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsünde Başuzman Araştırmacı olarak görev yapan Derya Cincioğlu, Eskişehir Osmangazi Üniversitesi Endüstri Mühendisliği Bölümü mezunudur. Ortadoğu Teknik Üniversitesi'nde Endüstri Mühendisliği Bölümünde Yüksek Lisans eğitimini tamamlamıştır. Profesyonel kariyeri boyunca birçok uluslararası şirket ve kamu kuruluşunda Bilgi Güvenliği Yönetim Sistemi, Risk Yönetimi, BT Servis Yönetim Sistemi (ITIL ve ISO 20000) ve İş Sürekliliği Yönetim Sistemi konularında danışmanlık ve denetçilik yapmış, eğitimler vermiştir.

Prof. Dr. Hacı Ali Mantar

Prof. Dr. Hacı Ali Mantar, 1993'te İstanbul Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümü'nde lisans derecesini aldıktan sonra 1998'de New York ABD'de Syracuse Üniversitesinde yüksek lisansını yaptı ve akabinde 2003'te yine aynı üniversitede doktorasını tamamladı. Dr. Mantar 2010 yılında doçent ve 2015 yılında profesör unvanlarını aldı. Haberleşme ve Ağ Protokolleri, Kablolu ve Kablosuz Haberleşme Teknolojileri, Bilgisayar Ağları, Ağ Mimarileri, Bilgi Sistemleri, Yazılım Tanımlı Ağlar (SDN), Dağıtık Sistemler, Ağ Güvenliği ve Adli Bilişim konularında araştırmalar yapmıştır. Dr. Mantar birçok ulusal ve uluslararası akademik ve endüstriyel araştırma projelerini yürütmüştür. TÜBA üyesi olan Dr. Mantar, 2015'te TÜBİTAK BİLGEM Başkanlığı ve 2018'de HAVELSAN Yönetim Kurulu Başkanlığı görevlerine atanmıştır.

Tolga Mataracıoğlu

After graduating from the Electrical and Electronics Engineering department of İstanbul Technical University in 2002, Mataracıoğlu received MSc degree from the Telecommunications Engineering department of the same university in 2006. He has been working at TÜBİTAK BİLGEM Cyber Security Institute since 2005 and he is currently the manager of Cyber Security Trainings and Solutions Unit. Mataracıoğlu has written many national and international level papers about information security. His research areas include system design and security, operating systems security, information security management systems, business continuity, IT governance, and social engineering.

Kerim Can Kalıpcıoğlu

After getting his undergraduate degree in engineering in 2017, Kalıpçıoğlu applied to Bursa Uludağ University Department of Computer Engineering to further study computer security. In March 2018, he started as an information security research assistant at Eskişehir Osmangazi University Department of Computer Software. He assisted undergraduate courses in operating systems, microprocessor systems, and information security. Since September 2019, he works as R&D personnel at TÜBİTAK BİLGEM.

Süleyman Muhammed Arıkan

After graduating from Pamukkale University Computer Engineering Department in 2015, Arıkan received his MSc degree from Gazi University Graduate School of Informatics Computer Forensics Department in 2019. He continues his education at Gazi University Computer Forensics Department PhD Program. Arıkan, who started working as a Researcher at TÜBİTAK BİLGEM Cyber Security Institute

in 2016, currently works as a Senior Researcher in cybersecurity technology development projects. As a software engineer, he has experience in web technologies, databases, software development, project management, configuration management and software process improvement. At the same time, he is a member of the Institute Board at TÜBİTAK BİLGEM Cyber Security Institute as employee representative.

Gökhan Işık

Işık, graduated from Eskişehir Osmangazi University Computer Engineering department in 2014. Now, he is at thesis period in Computer Engineering MSc at same university. He has been working as a Researcher at TÜBİTAK BİLGEM Information Technologies Institute Cloud Computing and Big Data Research Laboratory (B3LAB) since 2016. He has been in charge of cloud computing and big data infrastructure team leader at B3LAB since 2019.

Yasemin Demiral

Demiral graduated from Anadolu University Computer Engineering undergraduate degree in 2014 and Gazi University, Computer Engineering MSc in 2019. She has been working as a researcher at TÜBİTAK BİLGEM Information Technologies Institute Cloud Computing and Big Data Research Laboratory (B3LAB) since 2016. Since 2018, she has been working as a scrum master in the cloud computing and big data infrastructure team at B3LAB. She has worked mainly in the fields of virtualization, container, cloud computing, big data, DevOps and continuous integration/continuous delivery technologies at B3LAB.

Derya Cincioğlu

Derya Cincioğlu, working as a Chief Senior Researcher at TÜBİTAK BİLGEM Cyber Security Institute, graduated from Industrial Engineering Department in Eskişehir Osmangazi University. She received her MS degree in Industrial Engineering from METU. Throughout her professional career, she participated as the Consultant and Project Manager for the design, implementation and certification of Information Security Management, Risk Management, IT Service Management (ITIL and ISO 20000) and Business Continuity Management Projects for several organizations.

Prof. Hacı Ali Mantar

Prof. Hacı Ali Mantar received undergraduate degree in Electronics and Communication Engineering Department at Istanbul Technical University (İTÜ) and continued his education in New York, United States. He completed his MSc in 1998 and PhD in 2003 at Syracuse University in the Department of Electrics and Electronics Engineering. Dr. Mantar took his Associate Professor title in 2010 and Professor title in 2015. Dr. Mantar studied and researched in the following fields: Communication and Network Protocols, Wired and Wireless Communication Technologies, Computer Networks, Network Architectures, Information Systems, Software Defined Networks, Distributed Systems, Network Security and Forensic Computing. He executed many national/international academic and industrial research projects. He is also TÜBA Member. Dr. Mantar is appointed as the President of TÜBİTAK BİLGEM in 2015 and as the Chairman of the Executive Board at HAVELSAN in 2018.

DOI: 10.53478/TUBA.2020.065

Küresel Salgın Sonrasında Ulusal Bilişim Güvenliği

Tolga Mataracıoğlu
tolga.mataracioglu[at]tubitak.gov.tr

Kerim Can Kalıpcıoğlu
can.kalipcioglu[at]tubitak.gov.tr

Süleyman Muhammed Arıkan
suleyman.arikan[at]tubitak.gov.tr

Gökhan Işık
gokhan.isik[at]tubitak.gov.tr

Yasemin Demiral
yasemin.demiral[at]tubitak.gov.tr

Derya Cincioğlu
derya.cincioglu[at]tubitak.gov.tr

Prof. Dr. Hacı Ali Mantar
ali.mantar[at]tubitak.gov.tr

TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM)

Özet

2020 yılı ile birlikte dünyamızı etkilemeye başlayan COVID-19, hem özel hayatımızda hem de iş yapış yöntemlerimizde köklü değişiklikler yaşanmasına sebep oldu. İçinde bulunduğumuz mevcut duruma uyum kapsamında, birçok kurum tarafından salgın sırasında çalışanlarının virüsten etkilenmemesi ve salgını oluşabilecek en az zararla atlatmak adına, uzaktan çalışma bağlamında dijital dönüşüm ve bulut bilişim güvenliği gibi birçok konuda etkin ve hızlı kararlar alındı. Uzaktan çalışma ile birlikte değişen gereksinimlere uyum sağlanması ve mevcut yapının hem güvenlik hem de sürdürülebilirlik açısından iyileştirilmesi çalışmalarının daha da önem kazanmasının yanında bilgi teknolojileri ile ilişkili riskler de beraberinde gelişmeye ve ilerlemeye devam etmektedir.

Salgının süregeldiği dönem içerisinde siber güvenlik risklerinin yönetimi ve gerekli önlemlerin zamanında ve etkin bir şekilde alınması kurumların mevcut gündemlerinden düşmemesi gereken maddeler olarak karşımıza çıkmaktadır. Bu makalede küresel salgın sonrasında ulusal bilişim güvenliği kapsamında mevcut durum değerlendirilmekte olup, değişen alışkanlıklar doğrultusunda alınan ve alınması gereken önlemler ile dijital dönüşüm süreci doğrultusunda yapılan çalışmalar aktarılmaktadır.

Anahtar Kelimeler

küresel salgın, bilişim güvenliği, siber tehdit, siber saldırı, COVID-19, uzaktan çalışma, dijital dönüşüm, bulut bilişim güvenliği

National IT Security After the Pandemic

Abstract
From 2020 onwards, ongoing pandemic of COVID-19 has been affecting our social and business lives by causing radical changes. Many companies have been planning and implementing effective and rapid actions in many areas including digital transformation and cloud computing security within the scope of remote working in order to prevent their employees from being affected by the virus during the pandemic and to survive from the pandemic with the least possible damage. Meanwhile, risks related to information technologies continue to evolve and progress along with the efforts conducted to adapt to changing requirements based on remote working and improve the existing infrastructure by taking security and business continuity into account.

Management of cyber security risks and taking appropriate actions in a timely and effective manner during the pandemic are at the top of current agendas of the companies. Current situation of national cyber security after the pandemic has been analysed within the scope of this article together with the security precautions based on changing conditions and studies conducted in accordance with digital transformation processes.

Keywords
pandemic, IT security, cyber threat, cyber attack, COVID-19, remote working, digital transformation, cloud computing security

Giriş

Değişen koşullar göz önünde bulundurulduğunda, kurumların mevcut bilgi teknolojileri altyapısı ve siber güvenlik faaliyetlerinin öneminin gün geçtikçe daha da artmakta olduğu gözlenmektedir. Gereksinimler doğrultusunda birçok kurum tarafından uygulanmaya başlayan uzaktan çalışma faaliyetleri; beraberinde güvenli iletişim ve depolama kanallarının oluşturulması ve sürdürülebilirliğinin sağlanması, bilgi güvenliği farkındalık faaliyetlerinin arttırılmasına yönelik uzaktan eğitim stratejilerinin değerlendirilmesi, iş sürekliliği çalışmaları ile birlikte bilgi teknolojileri altyapılarının devamlılığının herhangi bir aksaklık yaşanmadan devam ettirilmesi çalışmalarının yoğun bir şekilde devreye alınmasını sağladı.

COVID-19 ile birlikte bilgi teknolojilerinde yaşanan gelişmeler, depolanan ve taşınan bilgi boyutunun her geçen gün daha da artmasına imkân verebilir hale gelmiştir. Bu kapsamda her geçen gün daha fazla bilgi elektronik ortama aktarılmakta, depolanmakta, işlenmekte, hizmete sunulmakta ve taşınabilmektedir. Elektronik ortamlarının çeşitliliği ve kullanım kapasitesinde yaşanan artış bilişim güvenliğine ilişkin yeni riskler ve sorunları da beraberinde getirmektedir. Bu doğrultuda kurumların dijital platformlar, uzaktan erişim, alternatif iletişim kanalları, güvenli altyapının devamlılığı anlamında etkin risk yönetimi ve ilişkili risk indirgeme faaliyetlerini etkin bir şekilde yönetmeleri oldukça önem arz etmektedir. Bilişim güvenliği kapsamında kurumların en değerli varlığı olarak kabul edilen çalışanların kurumsal ve kişisel bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliği konularında farkındalık seviyeleri arttırılmalı ve güvenlik zincirinin en önemli parçasını oluşturdukları konusunda bilgilendirilmelidir. Daha önce de belirtildiği üzere, COVID-19 salgını süresince uzaktan çalışma kurumların iş yapış yöntemlerinin merkezinde yer almaktadır.

Dizüstü bilgisayarlar, akıllı telefonlar veya video konferans yazılımları gibi giderek yaygınlaşan iletişim araçları sayesinde, çalışanlar neredeyse her yerde

işlerini sürdürebilme imkânı bulmaktadır. Teknolojinin gelişmesiyle beraber, işler yalnızca ofis alanlarında değil, ofis dışındaki alanlarda da rahatlıkla yürütülebilmektedir. İster otel odasında veya ulaşım aracında olsun, isterse müşterinin yanında; ofisten bağımsız çalışma modeli, mesai saatleri, çalışma alanı ve görev dağılımı gibi iş hayatımızla ilgili birçok tanımı değiştirmektedir.

2016 yılında 6715 sayılı kanun ile uzaktan çalışmaya ilişkin 4857 Sayılı İş Kanunu'nun 14. maddesine hükümler eklenmiştir. Kanunda "Uzaktan çalışma", "İşçinin işveren tarafından oluşturulan iş organizasyonu kapsamında iş görme edimini evinde ya da teknolojik iletişim araçları ile işyeri dışında yerine getirmesi esasına dayalı ve yazılı olarak kurulan bir iş ilişkisidir" şeklinde tanımlanarak çerçevesi çizilmiştir.

Teknik altyapıları, insan kaynakları, politika ve prosedürleri ile iş yapış şekilleri bakımından uzaktan çalışma modeline uyumluluk gösteren kurum ve kuruluşlar, bu modeli uygulamada daha güvenli ve başarılı bir yerde konumlanırlar. Ayrıca müşteriler, tedarikçiler ve iş ortakları gibi diğer paydaşların da uzaktan çalışma modeline gösterdikleri uyum bu modelin güvenliğini ve başarısını etkiler. Paydaşların bu modeli uygulamada yaşadıkları uyum sorunları veya iş yapış şeklinden kaynaklanan bir takım doğal kısıtlar, uzaktan çalışma modeline geçiş sürecini olumsuz etkiler. Bazı sektörlerin yapısı gereği bu modeli uygulaması mümkün olmayabilir.

Uzaktan çalışma modeli ile birlikte iletişim altyapısına olan ihtiyaç artmaktadır, buna paralel olarak karşı karşıya kalınan siber risklerde de artış yaşanır. Birçok kurum ve kuruluş uzaktan çalışma için istekli olsa bile, çok azı uygun siber güvenlik politikalarına ve altyapısına sahiptir. Kimlik avı dolandırıcılığı ya da farklı yöntemlerle mevcut sistem açıklarından faydalanan saldırganlar; işlerini uzaktan sürdüren çalışanları herhangi bir açık ağ üzerinden hedef alabilirler.

Bu sebeple kurum ve kuruluşların uzaktan çalıma modelini uygulamaya koyarken dikkat edilmesi gereken konuları ele alan Uzaktan Çalışma Modeli Rehberi hazırlanmıştır. Rehber TÜBİTAK BİLGEM Yazılım Teknolojileri Araştırma Ensitüsü tarafından iç destekli olarak 2016 yılında başlatılan Dijital Olgunluk Değerlendirme Modeli ve Rehberlik (DİJİTAL-OMR) Projesi ile Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan, kurumsal dijital kabiliyetlerini bütüncül bir yapı üzerinden değerlendirmeyi sağlayan Dijital Olgunluk Değerlendirme Modeli ile uyumlu olarak hazırlanmış olup Rehber ile dijital kurumsal kapasitenin artırılması amaçlanmıştır. Bu sayede d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılması ile dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanmaktadır. 2017 yılında İşletim ve Bakım Rehberi, 2018 yılında BT Hizmetleri yetkinliği altında yer alan Veri Merkezi Rehberi, 2019 yılında aynı yetkinlik altında Kablosuz

Ağların Yönetimi Rehberi, Aktif Dizin Yönetimi Rehberi ve Sunucu Yönetimi Rehberi yayımlanmıştır. 2020 yılının hemen başında bunlara ek olarak İstemci Yönetimi Rehberi yayımlanmıştır. Uzaktan Çalışma Modeli Rehberi rehber ailesinin son üyesidir.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm Rehberlerin www.dijitalakademi.gov.tr platformu ile açık erişimi sağlanmakta ve Rehberlerin kullanımının yaygınlaşması amacıyla eğitim programları, toplantılar ve çalıştaylar düzenlenmesi ile Rehberlik Mekanizmaları hayata geçirilmektedir. Rehberde yer alan uzaktan çalışma modelinin yaşam döngüsüne ait bazı konu başlıkları aşağıdaki gibidir:

- *Uzaktan çalışma ortamının seçimi ve kullanımı: İş yerlerindeki verimli çalışmanın uzaktan çalışma modelinde de yakalanabilmesi, ortamın uygun şekilde düzenlenmesi gibi bazı gereksinimlere bağlıdır.*
- *Uzaktan çalışmanın usul ve esasları: Evden çalışma modeli (home office) gibi oluşturulan uzaktan çalışma ortamlarının uygunluğu ve güvenliği, kuruluşların kurumsal düzenlemelerine ve çalışanın aldığı önlemlere dayanır.*
- *Uzaktan çalışmanın yapılacağı alanlar için güvenlik politikası: İş ve ofis alanlarının dışındaki tüm çalışmalarda, hangi bilgilerin kuruluş dışında kullanılabileceğine dair prosedürlerin ve talimatların oluşturulması gerekmektedir. Bununla birlikte, çalışanların bu bilgilere dışarıdan erişim koşulları da yazılı ve açık bir şekilde tanımlanmalıdır.*
- *Güvenlik ve erişim kontrolü: Uzaktan çalışma modelinde çalışanların kullandığı BT sistemlerinin (ör. bilgisayar, telefon, tablet vs.) yanında, bu çalışmalar esnasında oluşturulan ve paylaşılan veriler de dikkatli bir şekilde ele alınmalıdır. Bu kapsamda, işveren tarafından verilen çalışma ortamına ilişkin düzenlemelere uyulmalı ve çalışma materyalleri güvenli şekilde kullanılmalıdır.*
- *Gizli verilerin imha edilmesi: Uzaktan çalışma sistemlerindeki verinin yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslara, kurum içi çalışma ortamına oranla daha çok dikkat edilmesi gerekmektedir.*
- *Uzaktan çalışma hakkında yasal düzenlemeler: Kuruluşlar, uzaktan çalışma esasları ile ilgili çeşitli iş kanunlarına ve iş güvenliği yönetmeliklerine uyum göstermelidirler.*
- *Bulut bilişim ortam güvenliği: Uzaktan çalışma modelinde kullanımı artış gösteren bulut bilişim ortamının güvenlik gereksinimleri ve alınacak önlemler tanımlanmalıdır.*

Uzaktan çalışma yönteminin yaygınlaşması ile birlikte bulut bilişim ortamlarının güvenliği ve operasyonel açıdan etkinliği de kurumlar tarafından değerlendirilmesi ve iş süreçlerinin aksamadan sürekliliğinin sağlanması aşamasında oldukça kritik bir öneme sahiptir.

Bulut bilişim; esnek olarak ölçeklendirilebilen hesaplama gücü, depolama, ağ gibi veri merkezi kaynaklarının ağ üzerinden bir bulut hizmetleri platformu

vasıtasıyla; gerektiği anda, self servis olarak kullandığın kadarını öde prensibiyle talep sahibine ölçülebilir, lokasyon bağımsız ve gerektiğinde çok kiracılı bir kullanım modeliyle kullandırılabilmesi imkanını sağlayan bir altyapı ve hizmet modeli olarak öne çıkmaktadır. NIST (National Institute of Standards & Technology)'e göre bulut sisteminin aşağıdaki özelliklere sahip olması gerekmektedir (Mell & Grance, 2011):

- ***İsteğe Bağlı Self Servis (On-demand Self-service):*** *İnsan etkileşimi olmadan bilgi işlem yetenekleri (hesaplama, ağ, depolama) sağlama yani sanal makine ve ağ oluşturma işlemlerini kapsar.*
- ***Geniş Ağ Erişimi (Broad Network Access):*** *Servisler ağ üzerinden kullanılabilir ve bu servislere standart mekanizmalarla erişilebilir.*
- ***Kaynak Havuzu Oluşturma (Resource Pooling):*** *Bilgi işlem kaynakları, çok kiracılı bir model kullanarak birden fazla müşteriye hizmet vermek üzere toplanır. Müşterinin kaynakların tam yeri hakkında genellikle bilgisi yoktur*
- ***Hızlı Esneklik (Rapid Elasticity):*** *Yetenekler esnek olarak sağlanabilir ve hızla ölçeklenebilir.*
- ***Ölçülen Hizmet (Measured Service):*** *Kaynak kullanımı izlenebilir, kontrol edilebilir ve raporlanabilir.*

Bulut bilişim, hem endüstride hem de akademik çevrede kaynakları yönetebilmek için uygun bir yol sağlar. Bulut sistemleri, sisteme sık sık bağlı veya bağlantısı kesilmiş sayısız kullanıcı, cihaz, ağ, kurum ve kaynak dikkate alındığında teknoloji dünyasında aktif bir sistemdir. Tercih edilecek bulut hizmeti modelinin belirlenmesi için esneklik, ölçeklenebilirlik, birlikte çalışabilirlik ve hizmetin kontrolü faktörleri dikkate alınır. Bulut bilişim ortamlarında tutulan verilerin ve kaynakların güvenli şekilde muhafaza edilebilmesi için kapsamlı bir kimlik doğrulama ve yetkilendirme mekanizması gerekmektedir. Etkili kimlik doğrulama ve yetkilendirme mekanizması eksikliği, bulut ortamında kimlik yönetimi, risk yönetimi, güven yönetimi, uyumluluk, veri güvenliği, gizlilik, şeffaflık ve veri sızıntısı gibi çeşitli problemler oluşturmaktadır. Bir bulut sisteminde, verilerin depolanması ve işlenmesi kurumlar tarafından veya üçüncü taraf hizmet sağlayıcıları yardımıyla yapılır. Servis sağlayıcı, bulutta depolanan verilerin ve uygulamaların korunmasının yanı sıra bulut altyapısının güvenli bir ortamda olmasını sağlamalıdır. Güvenlik sorunları ile karşılaşmamak için ağ yapıları en güncel güvenlik standartları ile yapılandırılmalıdır.

Her sistemde güvenlik problemi olduğu gibi, bulut bilişimde de doğası gereği hem bulut hizmet sağlayıcılarını hem de kullanıcılarını etkileyebilecek çeşitli güvenlik sorunları bulunmaktadır. Bu sorunlar öncelikle, veri erişimi (availability), veri bütünlüğü (integrity), veri mahremiyeti (privacy) ve veri gizliliği (confidentiality) gibi sorunlarla birlikte bulutta akan ve bulutta depolanan verilerin güvenliği ile ilgilidir. Bu çalışmada, bulut hizmet modelleri tanıtıldıktan sonra, bulut bilişim güvenlik konuları ve olası zararlı etkilerini iyileştirmek için endüstride kullanılan çeşitli yöntemlerden bahsedilerek, kapsamlı olarak bulutta veri güvenliği konusu ele alınmaktadır.

Küresel Salgın Sonrasında Ulusal Bilişim Güvenliği makalesi kapsamında öncelikli olarak ülkemizde bilişim güvenliği kapsamında yapılan çalışmalar aktarılmakta olup, ulusal siber güvenlik stratejileri ve eylem planlarının hazırlanması, USOM'un kurulması, kurumsal ve sektörel SOME'lerin kurulması ile kritik altyapıların belirlenmesine ilişkin yürütülen çalışmalara ilişkin bilgilere yer verilmektedir. Ulusal Bilişim Güvenliği mevcut durumu hakkında verilen bilgiler doğrultusunda, salgın sonrası bilişim güvenliğine yönelik tehditlerin sınflandırması ve eğilimlerine yönelik yapılan araştırmalar, COVID-19 döneminde gerçekleşen güvenlik olayları ve tedbir önerileri yaşanan örnekler ile anlatılmaktadır. Salgın sonrası bilişim güvenliği tedbirleri ve ulusal bilişim güvenliği kapsamında ele alınan uyum süreci; salgın sonrasında değişen alışkanlıklar ve dijital dönüşüm sürecine yönelik bilgilerin verilmesinin ardından bilgi ve iletişim güvenliği tedbirleri rehberi ve uzaktan çalışma, uzaktan bilgi güvenliği farkındalığı, bulut bilişimde veri güvenliği, uzaktan çalışma süresince dikkat edilmesi gereken siber güvenlik hususları başlıkları ile ele alınmaktadır.

Ülkemizdeki Bilişim Güvenliği Çalışmaları: Mevcut Durum Analizi

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Çalışmaları

Gelişen teknolojiler, toplumsal talepler ve kamu sektöründeki reform eğilimleri doğrultusunda, farklı kurumlar altında ayrı ayrı sürdürülen dijital dönüşüm (e-Devlet), siber güvenlik, milli teknolojiler, büyük veri ve yapay zekâ ile ilgili çalışmaların tek çatı altında toplanması amacıyla, 10 Temmuz 2018 tarihli ve 30474 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 1 Sayılı Cumhurbaşkanlığı Kararnamesi kapsamında T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kurulmuştur (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi İnternet Sitesi, 2020). Kararname kapsamında Dijital Dönüşüm Ofisinin hizmet birimleri;

1. *Dijital Dönüşüm Koordinasyon Dairesi Başkanlığı,*
2. *Dijital Teknolojiler, Tedarik ve Kaynak Yönetimi Dairesi Başkanlığı,*
3. *Dijital Uzmanlık, İzleme ve Değerlendirme Dairesi Başkanlığı,*
4. *Siber Güvenlik Dairesi Başkanlığı,*
5. *Büyük Veri ve Yapay Zekâ Uygulamaları Dairesi Başkanlığı,*
6. *Uluslararası İlişkiler Dairesi Başkanlığı,*
7. *Bilgi Teknolojileri Dairesi Başkanlığı,*
8. *Yönetim Hizmetleri Dairesi Başkanlığı,*
9. *Hukuk Müşavirliği olarak belirlenmiştir (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi İnternet Sitesi, 2020).*

Siber Güvenlik Dairesi Başkanlığı'nın görev ve sorumlulukları aşağıda listelenmiştir (Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı, 2020):

1. *Cumhurbaşkanınca belirlenen politikalar kapsamında kamu kurumları ve kritik altyapılara yönelik siber güvenlik stratejileri geliştirmek.*

2. *Ulusal siber güvenlik ve bilgi güvenliğini destekleyici projeler geliştirmek.*
3. *Siber güvenlik ile ilgili politika, strateji ve eylem planlarının ülke çapında etkin şekilde uygulanmasına yönelik gelişmeleri takip etmek.*
4. *Kritik altyapıların belirlenmesine yönelik çalışmalar yapmak.*
5. *Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşlar konusunda ilgili kurumlara önerilerde bulunmak.*
6. *Kamu, özel sektör ve üniversiteler arasındaki işbirliğinin artırılması suretiyle ulusal siber güvenlik ekosisteminin oluşturulmasına katkı sağlamak.*
7. *Özel sektörün kapasitesinin kritik alanlara yönlendirilmesi ve mükerrer yatırımların önlenmesi için öncelikli siber güvenlik alanlarını belirlemek.*
8. *Kritik altyapılar başta olmak üzere her alanda, yerli ve milli siber güvenlik ürünlerinin geliştirilmesine ve bu çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik çalışmalar yapmak.*
9. *Kritik teknoloji ve bilgi varlıklarını korumak amacıyla önleyici ve koruyucu faaliyetler konusunda çalışmalar yürütmek.*
10. *Kamu kurumlarında ve kritik altyapı işleten kuruluşlarda bilgi güvenliği yönetim sisteminin kurulup işletilmesi, teknik standartlar ile usul ve esasların belirlenmesi, uygulamanın izlenmesi ve yönlendirilmesi konularında çalışmalar yürütmek.*

Ulusal Siber Güvenlik Stratejileri ve Eylem Planlarının Hazırlanması

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı Siber Güvenlik Kurulu tarafından 21/12/2012 tarihli toplantıda kabul edilmiş ve Bakanlar Kurulu'nun 20/06/2013 tarihli ve 28683 sayılı kararı ile Resmi Gazetede yayımlanmıştır (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016). Akabinde "2016-2019 Ulusal Siber Güvenlik Stratejisi" ve "2016-2019 Ulusal Siber Güvenlik Eylem Planı" hazırlanmıştır. 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, kamu bilişim sistemlerine ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ilave olarak küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın ülkemiz ölçeğindeki bütün bileşenlerini kapsar (2016-2019 Ulusal Siber Güvenlik Stratejisi, 2016). 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlık çalışmaları devam etmektedir.

USOM'un Kurulması

Ülkemizin siber güvenliğine karşı siber ortamda ortaya çıkan tehditlerin belirlenmesi, muhtemel saldırı ve olayların etkilerini azaltılması veya ortadan kaldırılmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur (USOM Hakkımızda, 2020).

Başkanlık bünyesinde kurulan USOM, ulusal ve uluslararası seviyede siber ortamda ortaya çıkan tehditler ile ilgili kendisine ulaştırılan ihbarları da de-

ğerlendirerek, söz konusu tehditlerin tespit ve bertaraf edilmesi için Kamu Kurumları ve özel kişiler ile koordinasyonunu sağlamaktadır (USOM Hakkımızda, 2020). Bu itibarla gelen ihbar ilk aşamadan başlanarak, çözüm sürecine kadar takip edilerek değerlendirilmektedir (USOM Hakkımızda, 2020).

Diğer taraftan ulusal ve uluslararası siber güvenlik tatbikatları düzenlenerek kamu kurum ve kuruluşlarının siber saldırılara karşı farkındalığının ve hazırlığının arttırılması faaliyetleri ile bilinçlendirme ve yönlendirme faaliyetleri hâlihazırda devam etmektedir (USOM Hakkımızda, 2020).

Kurumsal ve Sektörel SOME'lerin Kurulması

Siber Güvenlik Kurulu'nun ilk toplantısında "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiş ve 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak yayımlanmıştır. 29 ana eylem ve 95 alt eylem maddesinden oluşan eylem planında, her eylem kapsamındaki çalışmaları sorumlu ve ilgili kuruluş olarak yürütecek kurum ve kuruluşlar belirlenmiştir (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2020). Söz konusu eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME, Sektörel SOME) oluşturulması öngörülmüştür (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2020). SOME'ler siber olayları bertaraf etmede, oluşması muhtemel zararları önlemede veya azaltmada, siber olay yönetiminin ulusal düzeyde koordinasyon ve işbirliği içerisinde gerçekleştirilmesinde hayati önemi olan yapılardır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2020). Bu bağlamda kurum ya da kuruluşların bünyesinde 7 etkin ve verimli bir Kurumsal SOME'nin kurulması, bu Kurumsal SOME'nin USOM ve varsa bağlı olduğu Sektörel SOME ile diğer Kurumsal SOME'lerle koordineli çalışması ve işbirliği halinde olması ulusal siber güvenliğimize katkı sağlayacaktır (Kurumsal SOME Kurulum ve Yönetim Rehberi, 2020).

Kritik Altyapıların Belirlenmesi

20.06.2013 tarih ve 2 sayılı Siber Güvenlik Kurulu kararı ile belirlenen kritik altyapılar aşağıda listelenmiştir:

1. *Enerji*
2. *Elektronik Haberleşme*
3. *Bankacılık ve Finans*
4. *Ulaştırma*
5. *Su Yönetimi*
6. *Kritik Kamu Hizmetleri*

Kritik altyapıların belirlenmesine yönelik çalışmalar yapma görevi 10 Temmuz 2018 tarihli ve 30474 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren 1 Sayılı Cumhurbaşkanlığı Kararnamesi kapsamında T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'ne verilmiştir (Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı, 2020).

Türkiye Siber Güvenlik Kümelenmesi Faaliyetleri

Misyonu ihtiyaçların tespiti ve yenilikçi yöntemlerle karşılanması için en üst

düzey iş birliği ve eşgüdümü ve sağlıklı rekabet koşullarını sağlayarak ekosistemi geliştirmek ve bunun sürekliliğini sağlayacak mekanizmaları oluşturmak, vizyonu da siber güvenlik alanında yetkin insan kaynağı ve markalaşmış yerli/milli çözümlerle global pazarda rekabetçi ve söz sahibi olmak olan Türkiye Siber Güvenlik Kümelenmesi, 2017 yılında ilgili tüm kamu kurum/kuruluşlar, özel sektör ve akademi temsilcilerinin katılımlarıyla ortaya çıkan, Savunma Sanayii Başkanlığı tarafından desteklenen ve SSTEK A.Ş. tarafından yürütülen bir projedir (Türkiye Siber Güvenlik Kümelenmesi, 2020). Kümenin uzun vadeli hedeflerinin belirlenmesi ve yönetilmesi Danışma Kurulu vasıtasıyla yapılır. Kümelenmenin günlük operasyonları SSTEK A.Ş. bünyesinde kurulan Koordinasyon Ofisi tarafından gerçekleştirilmektedir (Türkiye Siber Güvenlik Kümelenmesi, 2020). Siber Küme'nin hedefleri aşağıda listelenmiştir (Türkiye Siber Güvenlik Kümelenmesi, 2020):

- *Türkiye'deki siber güvenlik firmalarının sayısını artırmak,*
- *Üyelerinin teknik, idari ve finansal açılardan gelişimine destek olmak,*
- *Siber güvenlik ekosisteminin standartlarını geliştirmek,*
- *Üyelerinin ürün ve hizmetlerinin markalaşmasına yardımcı olmak,*
- *Üyelerinin ulusal ve global pazarda rekabet gücünü artırmak,*
- *Siber güvenlik alanındaki insan kaynağı sayısını artırmak, niteliklerini geliştirmek,*
- *Bütün toplumda siber güvenlik bilincini geliştirmek.*

Siber Küme'nin faaliyetleri ise aşağıda listelenmiştir (Türkiye Siber Güvenlik Kümelenmesi, 2020):

- *Küme üyelerinin kendi aralarında ve dış paydaşlarla iletişimini artırmak için teknik, sosyal etkinlikler düzenlemek,*
- *Üye firmaların ürün ve hizmetlerini kataloglamak,*
- *Yerli ürünlerin kullanımı için teşvik mekanizmaları oluşturmak,*
- *Yurt içi pazarda, büyük ölçekli müşteriler nezdinde üyelerinin tanıtımını yapmak, bilinirliklerini artırmak,*
- *Siber güvenlik konusuna ilgi duyan kişilerin kendilerini geliştirebileceği, kabiliyetlerini belgelendirebileceği eğitim, yarışma, grup çalışmaları gibi etkinlikler düzenlemek, eğitim tesisi kurmak, kurulmasına destek olmak,*
- *Sektörel her türlü bilgi, belge, rapor ve bu doğrultuda teknolojik ve sektörel haber ve bültenlerin paylaşımını yapmak,*
- *Firmaların yararlanabileceği destek, teşvik, proje gibi kaynakları tespit etmek ve üyelerin erişimini kolaylaştırmak amacıyla danışmanlık ve lobi faaliyetleri yapmak,*
- *Sektörün test ve geliştirmelerine altyapı imkânı sunan Test Ve Analiz Laboratuvarı kurmak,*
- *Sertifikasyon Laboratuvarı kurmak,*

- *Siber Güvenlik Akademisi kurmak,*
- *Teknoloji Yol Haritası oluşturmak, Siber Güvenlik Teknoloji Taksonomisini belirlemek, teknoloji yönetimi yapmak,*
- *Tatbikat Alanları kurmak/mevcutları değerlendirmek,*
- *Ulusal/Uluslararası konferans, eğitim, seminer, panel, fuar gibi etkinlikler düzenlemek,*
- *Yurtdışında temsilcilikler açmak ya da temsilci bulundurmak,*
- *Kümelere yönelik teşviklerden faydalanmak,*
- *Staj arz ve talep koordinasyonunu sağlamak,*
- *Ön lisans/lisans/lisansüstü programlarının açılmasına destek vermek,*
- *Siber güvenlik sektörüne girme niyetinde olan Türk veya Yabancı işletme ve yatırımcılara; mesleki, sosyal, teknik ve ekonomik yönlerden rehberlik etmek,*
- *İnsan Kaynağı/Talebi eşleştirmesi için ortam (web sayfası, kariyer günleri, vb.) düzenlemek.*

Salgın Sonrası Bilişim Güvenliğine Yönelik Tehditlerin Eğilimi

Koronavirüs salgınının siber olaylara etkileri dört sınıfta incelenebilir. Bunlardan ilki salgının sosyal mühendislik saldırılarına konu edilmesi ve bu şekilde etkilerinin arttırılmasıdır. Diğeri ise özel sektörde ve 2020/4 Sayılı Cumhurbaşkanlığı Genelgesi ile kamuda uygulanan uzaktan çalışma nedeniyle ortaya çıkan risklerdir. Bir başka etki de uzaktan eğitimde yaşanan siber güvenlik riskleri olarak karşımıza çıkmaktadır. Bu tür risklere örnek olarak katılımcının yerine başka birinin eğitime katılması, eğitim sonu sınavına girip eğitim sertifikası almaya hak kazanması gösterilebilir. Son olarak da salgın sonrası ortaya çıkan yeni saldırı türleri kaynaklı risklerdir. Salgın sonrası yeni dünyada ortaya çıkan bu tür risklere örnek olarak yapay zeka kullanarak ses ve görüntü taklidi ile başkasıymış gibi toplantılara katılmak örnek olarak gösterilebilir.

Koronavirüs döneminde evden çalışma yapılmasının getirdiği birden çok risk vardır. Bunlardan en önemlisi daha önceden İnternete kapalı olan sistemlerin uzaktan erişim amacıyla İnternete açılmasıdır. Özellikle İnternete kapalı olduğu gerekçesiyle güvenliği ihmal edilen ve bu süreçte ani şekilde uzaktan çalışma düzenine geçmek zorunda kalan işletmelerin bilgisayar sistemleri saldırılarla karşı karşıya kalmışlardır. Shodan arama motoru üzerinde yapılan analizde son dönemde Uzaktan Masaüstü Protokolü (RDP) erişimine açık sistem sayısının arttığı ve bunların önemli bir kısmının BlueKeep (CVE-2019-078) zafiyetini barındırdığı raporlanmıştır. Bunun yanında ev ortamında kullanılan bilgisayarların ve bağlantıların güvenliğinin sağlanması sorunu ortaya çıkmıştır.

Bu dönemde önemli risklerden biri de bireylerin bilgi alma ihtiyacı dolayısıyla sosyal mühendislik saldırılarına karşı daha savunmasız olmasıdır. Saldırganlar da bu gelişmeleri hazırladıkları Koronavirüs temalı sosyal mühendislik saldırılarıyla takip etmiş, böylece yanlış bilgilerin ve zararlı yazılımların yayılma-

sını sağlamaya çalışmışlardır. Unutmamak gerekir ki bu saldırılarda olağan zamanda kullanılan tekniklerden farklı bir teknik kullanılmamaktadır. Bu nedenle Koronavirüs döneminde de kullanıcıların her zaman takip etmesi gereken bilgi güvenliği politikalarına bağlı kalması gerekir.

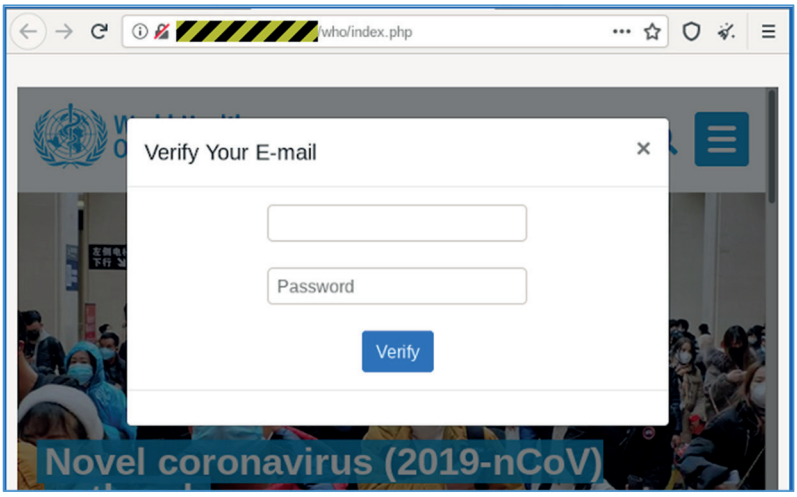
Koronavirüs Dönemindeki Güvenlik Olayları ve Tedbir Önerileri

Salgın döneminde güvenlik araştırmacıları tarafından belirlenmiş ve yayınlanmış güvenlik olayları aşağıda özetlenmiştir.

Dünya Sağlık Örgütü Oltalama E-postaları

Salgın döneminde önem kazanan sağlık örgütlerinden biri olan Dünya Sağlık Örgütü (DSÖ), Birleşmiş Milletler'e bağlı uluslararası bir kuruluştur. Saldırganlar da, Koronavirüs salgınının başından beri birçok kişinin DSÖ'den gelecek açıklamaları beklediğini bilmektedirler. Bu nedenle hazırladıkları oltalama e-postaları ile DSÖ'nün ismini kullanarak kullanıcı bilgilerini çalmayı amaçlamaktadırlar. Görsel 1'de oltalama e-postasında bulunan link aracılığıyla yönlendirilen sahte sayfa örneği verilmiştir.

Görsel 1. Oltalama e-postasında bulunan link aracılığıyla yönlendirilen sahte sayfa



Kaynak: *(sophos.com)*

Bu amaçla gönderilen e-postalarda, güvenlik önlemlerinin bulunduğu iddia edilen sahte sayfaya ait bir bağlantı bulunmaktadır. Arka planda gerçek DSÖ web sitesinin bulunduğu sayfada ek olarak kötü amaçlı bir pop-up bulunmaktadır. Form gönderildiği takdirde kullanıcılar DSÖ'ye ait www.who.int web sitesine yönlendirilmekte, girilen e-posta bilgileri ise saldırganların eline geçmektedir.

Koronavirüs Alan Adları

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'nin araştırmasına göre bu yıl Koronavirüs ile ilgili 4000 tane alan adının alındığı ve bunların 320'sinin zararlı web siteleri olduğu görülmüştür. Ulusal Siber Olaylara Müdahale Merkezi (USOM) zararlı alan adları listesinde ise 100'den fazla alan adının Koronavirüs ile ilgili sözcükler içerdiği görülmüştür. Bu alan adlarının özellikle Türkiye'de yaşayan kişileri ve kurumları hedef alması önemli bir noktadır. Aynı şekilde yabancı dillerde de dolandırıcılık amacıyla alan adlarının alındığı görülmektedir. Görsel 2'de USOM zararlı alan adları listesinde bulunan bazı alan adları listelenmektedir.

Görsel 2. USOM zararlı alan adları listesinde bulunan bazı alan adları

```
korona-iade.com
covid19bireyseliadeniz.com
covid19-apps.com
antivirus-covid19.site
covid19-guidelines.online
covidapp-19.space
canada-alert-covid19.com
covidapp-19.site
xn--covid19-gncelsalgnvakalar-nwc35l.com
```

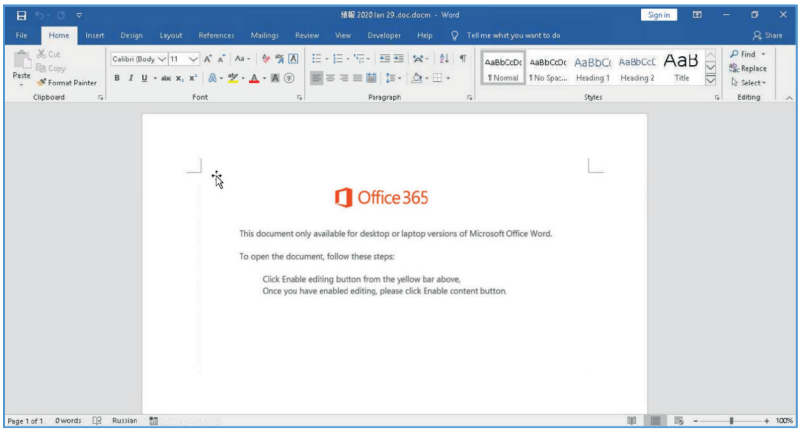
Özellikle salgın döneminde alışverişin yasal niteliği olan güvenilir web siteleri üzerinden yapılması gerekmektedir. İnternet üzerinden Koronavirüs ile ilgili herhangi bir amaçla para talep eden web sitelerine karşı dikkatli olunmalıdır. Bağış kampanyaları benzeri organizasyonlar için güvenilir kurumların web sitelerinden bilgi alınmalıdır.

Emotet

Koronavirüs temalı oltalama e-postaları ile zararlı yazılım dağıtımına dair birden çok vaka belirlenmiştir. Genelde uzaktan yönetim aracı ve truva atı tipinde olan bu zararlıların yanında bazı fidye yazılımlarının da bu şekilde dağıtıldığı araştırmacılar tarafından doğrulanmıştır. Bu girişimlerden biri de Emotet zararlısını yeniden yaymayı amaçlayan oltalama saldırılarıdır.

İlk olarak 2014 yılında görülmüş olan Emotet, öncelikli olarak bankacılık bilgilerini hedef almış bir truva atı yazılımıdır. E-posta yoluyla yayılan Emotet aynı zamanda solucan benzeri özellikler göstererek ağa bağlı bilgisayarlara da bulaşabilmektedir. Bunun yanında Emotet diğer zararlı yazılımların da sisteme bulaşmasına aracı olabilmektedir. Görsel 3'te zararlı kod içeren Word dokümanı örneği verilmektedir.

Görsel 3. Zararlı kod içeren Word dokümanı



Kaynak: *(xforce.ibmcloud.com)*

Word belgeleri aracılığıyla yayılan zararlı yazılım, belgenin düzenleme modunda açılmasına teşvik etmek için Office 365 logosu ile beraber hazırlanmış bir metin barındırmaktadır.

CovidLock: Android Fidye Yazılımı

Çevredeki Koronavirüs vakalarını izleyerek kullanıcıyı bilgilendirmeyi vadeden bir Android uygulaması olan CovidLock, aslında kullanıcı verilerini şifreleyerek 100 ABD Doları değerinde Bitcoin talep eden bir fidye yazılımıdır. Belirtilen süre içerisinde fidyenin ödenmesi için telefondaki verilerin silineceği ve sosyal medya hesaplarının "sızdırılacağı" gibi tehditlerde bulunan uygulama, Google Play Store harici kaynaklardan dağıtılmaktadır. Android Nougat ve sonrası sürümlerde ekran kilidi kullanıldığında ise işlevini yerine getirememektedir. Para karşılığı satın alınması istenilen parolanın, yazılımın içerisinde açık şekilde saklandığı güvenlik araştırmacıları tarafından keşfedilmiştir. Parola paylaşılarak fidye yazılımının ortaya çıkaracağı maddi zararın engellenmesi amaçlanmıştır. Görsel 4'te Koronavirüs Android fidye yazılımı örneği verilmektedir.

Görsel 4. Koronavirüs Android fidye yazılımı

Kaynak: *(domaintools.com)*

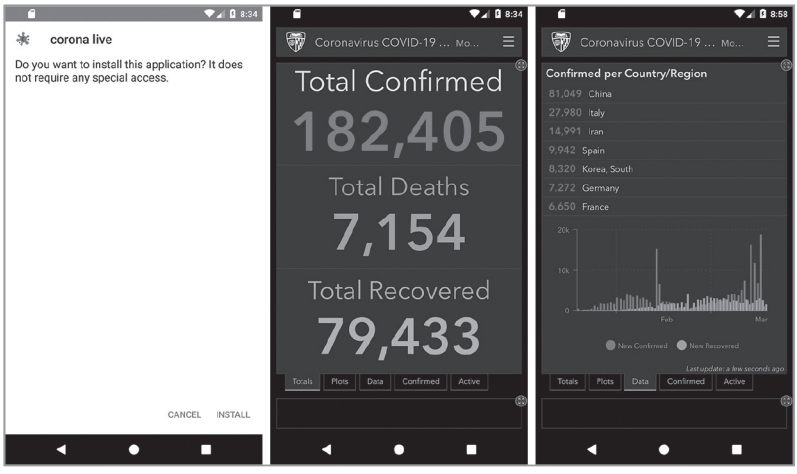
Kullanıcıların bu ve benzeri saldırılardan korunabilmesi için güvenilmeyen kaynaklardan uygulama yüklememesi ve uygulamalara gerekmeyen izinleri vermemesi gerekmektedir. Uygulamanın kalıcılığını sağlamasından dosya sistemine erişime birçok yetkiyi ek izinlerle elde ettiği düşünüldüğünde, şüpheli görülen izinlerin kısıtlanması ile zararlı uygulamaların vereceği zararın engellenebileceği görülmektedir. Bunun yanında güncellemelerin takip edilerek kısa sürede uygulanması ve ekran kilidi kullanılması önem arz etmektedir.

Android Casus Yazılımları

Yine benzer şekilde Koronavirüs salgını döneminde hastalıklarla ilgili istatistiksel bilgiler sağlayan zararlı bir uygulamanın Google Play Store harici kaynaklardan dağıtıldığı görülmüştür. John Hopkins Üniversitesi tarafından hazırlanan Koronavirüs haritasındaki bilgileri kullanıcılara yansıtan uygulama, arka planda SpyMax adlı uzaktan yönetim aracını (RAT) barındırmaktadır. Yapılan detaylı araştırmada benzer şekilde Koronavirüs temalı ve benzer yapıda Android uzaktan yönetim araçları barındıran birden çok uygulama olduğu belirlenmiştir.

Symantec firmasının yaptığı araştırmada ise SM-COVID-19 adlı uygulamayı taklit ederek yeniden paketlenmiş ve kötü amaçlı kod barından 11 tane uygulamanın olduğu raporlanmıştır. Bu uygulamalar Türkiye'yi hedef almadığı için ülkemizde kullanımı olmayacağı düşünülmekle beraber, bu tarz saldırılara karşı dikkatli olunması gerekmektedir. Görsel 5'te "corona live 1.1." adlı uygulamaya ait ekran görüntüsü verilmektedir.

Görsel 5. corona live 1.1. adlı uygulama

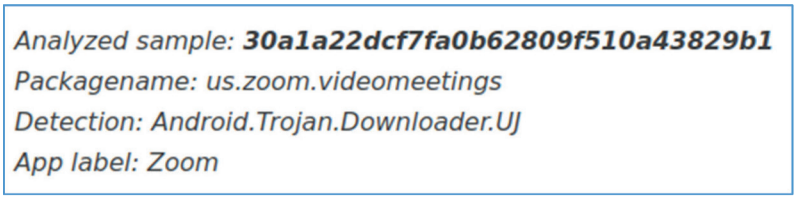


Kaynak: *(lookout.com)*

Zoom Uygulamaları

ABD merkezli Zoom Video Communications firması İnternet üzerinden görüntülü konuşma ve konferans yapılmasına olanak sağlayan servisler sunmaktadır. İnternet üzerinde görüşme ihtiyacının artmasıyla beraber yaygın bir şekilde kullanılan bu servislere ZOOM Cloud Meetings adlı Android uygulamasından da erişilebilmektedir. Uygulamalara olan yoğun talebi gören saldırganlar, bu uygulamaları yeniden paketleyerek kötü amaçlı yazılımlarını yaymak için kullanmaktadırlar. Genellikle reklam geliri elde etmek amacıyla yapılan bu saldırılar kullanıcıların gizliliğini tehlikeye atmaktadır. Görsel 6'da trojan downloader içeren bir Zoom uygulaması klonu görülmektedir.

Görsel 6. Trojan downloader içeren bir Zoom uygulaması klonu



Kaynak: *(labs.bitdefender.com)*

Bunun yanında yakın zamanda aynı servislere erişim için kullanılan Microsoft Windows ve macOS masaüstü uygulamalarında da kullanıcıların güvenliğini tehdit eden güvenlik zafiyetleri ve kullanıcı gizliliğini tehlikeye atan durumlar raporlanmıştır. Bu nedenle mümkün olduğunca farklı bir servis tercih edilerek internet üzerinden görüşme ihtiyacının karşılanması önerilmektedir. Görsel 7'de NIST NVD veritabanına kayıtlı güncel Zoom zafiyetleri yer almaktadır.

Görsel 7. NIST NVD veritabanına kayıtlı güncel Zoom zafiyetleri

Vuln ID	Summary	CVSS Severity
CVE-2020-11500	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key. **Published:** April 03, 2020; 09:15:13 AM -04:00	(not available)
CVE-2020-11470	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access. **Published:** April 01, 2020; 06:15:17 PM -04:00	V3.1: 3.3 LOW V2: 2.1 LOW
CVE-2020-11469	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process (with the user's privileges) to obtain root access by replacing runwithroot. **Published:** April 01, 2020; 06:15:17 PM -04:00	V3.1: 7.8 HIGH V2: 7.2 HIGH
CVE-2019-16273	DTEN D5 and D7 before 1.3.4 devices allow unauthenticated root shell access through Android Debug Bridge (adb), leading to arbitrary code execution and system administration. Also, this provides a covert ability to capture screen data from the Zoom Client on Windows by executing commands on the Android OS. **Published:** January 06, 2020; 03:15:11 PM -05:00	V3.1: 9.8 CRITICAL V2: 10.0 HIGH

Servisin kullanılması durumunda Android veya iOS sistemler için indirilen uygulamalar Google Play Store ve App Store üzerinden, masaüstü uygulamalar ise firmanın kendi web sitesi üzerinden indirilmeli ve güncellemeler takip edilmelidir.

Diğer Olaylar
Pulse Secure VPN yazılımında bulunan zafiyet kullanılarak birden çok firmaya REvil (Sodinokibi) fidye yazılımının bulaştırılmış olduğu tahmin edilmektedir. Aynı şekilde Palo Alto ve Fortinet VPN yazılımlarında da güncel zafiyetler olduğu görülmektedir. Bu nedenle kullanılan VPN yazılımlarının güncellemelerinin yapılması ve ek güvenlik önlemlerinin alınması gerekmektedir.

Emotet dışında, aralarında daha önce görülmemiş zararlıların da dahil olduğu bazı yazılımların e-posta ekleriyle yayıldığı gözlemlenmiştir. Bu zararlılar genellikle Microsoft Office tarafından kullanılan dosya tiplerinde olduğundan, bu tip belgelere dikkat edilmesi gerekmektedir. Gerekmediği durumlarda belgeler düzenleme modunda açılmamalıdır.

Salgın Sonrası Bilişim Güvenliği Tedbirleri ve Ulusal Bilişim Güvenliği

Değişen Alışkanlıklar ve Dijital Dönüşüm Süreci
Günümüzde, sosyal yaşantımızdan hijyen alışkanlıklarımıza kadar birçok alanda dönüşümlere sebep olan COVID-19, bilişim sektöründe de çeşitli konularda değişimi ve gelişimi gerekli kılmıştır. Salgının önlenmesi adına alınan tedbirler neticesinde uzaktan çalışma, uzaktan eğitim, uzaktan tedavi, çevrimiçi alışveriş gibi kavramlara ek olarak artırılmış gerçeklik teknolojisine dayanan sanal sporlar, çevrimiçi toplantı, konser, seminer ve konferans gibi ekinlikler hayatımızda daha geniş uygulama alanı bulmuştur. Alışkanlıkların değiştiği ve süreçlerin mümkün olduğunca dijital olarak yürütüldüğü bu dönemde, yaşanan değişimlere ve kazanılan yeni alışkanlıklara rağmen güvenliğin ödün vermeden devamlılığını sağlamak adına siber güvenlik de payına düşen değişimden ve gelişimden nasibini almıştır. Bu süreçte elde edilmiş kazanımlar, COVID-19'un ardından yeni normal dönemin temelini oluşturacaktır.

Özel sektörün ve özellikle kamu kurumlarının yıllarca yapma konusunda endişe duyduğu/tereddüt ettiği uzaktan çalışma yöntemi, iş sürekliliğini sağlamak adına zorunlu olarak uygulamaya geçmiştir. Bu durum; sonuç odaklı yaklaşımı beraberinde getirerek çalışma saati yerine çıktının esas olduğunu göstermiştir. Ayrıca, çevrimiçi olarak gerçekleştirilen toplantı faaliyetleri sayesinde konumdan bağımsız ve zaman kaybı yaşamadan çalışmalar yürütüldüğünden fiziksel toplantılara nazaran daha çok verim sağlanmıştır.

Salgından önce çevrimiçi katılıma nazaran fiziksel katılımın daha çok tercih edilmesine karşın bu süreç içinde eğitim ve konferans, seminer vb. etkinlikler için sanal ortamda katılıma yönelik empati artmış ve oldukça benimsenmiştir. Ayrıca, fiziksel katılım ile kayıt ücreti alan birçok organizasyon, çevrimiçi etkinlikleri ücretsiz olarak sunmuştur. Benzer şekilde bazı yayınevleri ise kitaplarının bir kısmını çevrimiçi olarak kullanıcıların hizmetine sunmuştur.

Salgın döneminde, insanların hastaneler veya klinikler üzerinden virüse maruz kalmasını engellemek ve sağlık sebebi ile dış dünya ile oluşacak iletişimi minimuma indirmek amacıyla, özellikle riskli grupta bulunan yaşlılara yönelik olarak, telefon ve/veya İnternet üzerinden muayene imkanı sunulmuştur. Bu durum, özellikle yaşlı insanların dijital ortamları kullanabilmesinin önemini bir kez daha gözler önüne sermiştir. Bu süreçte; telefon, bilgisayar gibi araçları kullanmayı öğrenmeye gayret gösterilmiş ve İnternet gibi teknolojilerin ihtiyaç dışı ve/veya lüks olduğu yanılgısı yenilmiştir.

Geniş bir kullanıcı kitlesine sahip olan ve sürekli gelişimini sürdürün çevrimiçi alışveriş, bu dönemde de kendinden beklenen ilerlemeyi göstermiştir. COVID-19 salgını sebebiyle; gıda, market, temizlik, dezenfektan, kitap ve oyuncak gibi kategorilerde e-ticaret sitelerinin satışları yüzde 200 artarken, kapanan mağazalar ve dükkanlar insanların evde olmasını ve İnternetten alışveriş yapmasını fırsata çevirerek İnternetten satış yapmaya yönelmişlerdir (5G ile İhracatçılar E-Ticarette Atağa Kalkıyor, 2020). Dolayısı ile bu süreçte çevrimiçi alışveriş, hem iş yerlerinin kapanmadan faaliyetlerine devam etmesine yardımcı olurken hem de kişilerin dış dünya ile etkileşimini en aza indirerek çeşitli ihtiyaçlarını evden gidermesine büyük katkı sağlamıştır.

Salgın döneminde uygulanan sokağa çıkma yasakları ve alınan izolasyon kararları neticesinde, insanlar spor, eğlence ve sosyal aktivitelerini çevrimiçi olarak sürdürmeye yönelmiştir. Bu kapsamda çevrimiçi konser ve sanal sporlar geniş katılımcı kitlesi bulmuştur. Sanatçılar, dinleyicilerine sosyal medya platformları üzerinden mini konserler sunarken birçok spor müsabakası sanal gerçeklikten faydalanarak çevrimiçi olarak yapılmıştır. Örneğin Formula 1, hayranların yarışları izlemeye devam etmelerini sağlamak amacıyla Sanal Grand Prix Serisi başlatmış ve salgın nedeniyle ertelenen her yarış, F1 pilotları tarafından bir bilgisayar oyunu üzerinden oynanarak yapılmıştır (Formula 1 launches Virtual Grand Prix Series to replace postponed races, 2020).

Bilişim sektöründe yaşanan tüm bu gelişmeler, hayatımızın hemen her alanının dijitalleşmesine sebep olurken siber tehditleri de beraberinde getirmiştir. Bazı tehdit aktörlerinin devlet destekli olması ve özellikle aşı ile ilaç şirketlerini hedef alması sebebiyle konunun ulusal tehdit çerçevesinde değerlendirilmesi ve önlemlerin alınması gerekmektedir (COVID-19 Salgını Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar, 2020). Ayrıca, kötü amaçlı yazılıma ve/veya oltalama saldırısına yönelik olan COVID-19 içerikli engellenmiş e-posta sayının günlük bazda 18 milyona kadar ulaşabildiği gözlemlenmiştir (Kumaran & Lugani, 2020). Buna ek olarak salgın süresince, COVID-19 ile ilişkili erişim adresine sahip çok sayıda İnternet sitesinin siber saldırılara zemin hazırlamak amacıyla açıldığı görülmüştür (COVID-19 Salgını Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar, 2020). Dünya Sağlık Örgütü, saldırganların pandemiden faydalanarak sosyal ağ uygulamaları mesajları veya e-posta iletileri üzerinden para veya hassas bilgileri elde etmek amacıyla gerçekleştirdiği saldırılara karşı kişileri uyarmıştır (Beware of criminals pretending to be WHO, 2020). Sonuç olarak, siber güvenliğin değişen ve gelişen bilişim sektörü karşısında ilerleme kaydetmesi zorunluluk halini almıştır.

Şirketlerin ve kurumların çalışma hayatına ve çalışma ortamına ilişkin en iyi uygulamaları (best-practice) çevrimiçi gerçekleştirilen faaliyetler neticesinde değişime uğrayarak, öğrenilen dersler doğrultusunda süreçlerin işletilmesinde ve güvenliğin sürdürülmesinde kullanılan yöntemler gelişme göstermiştir. İş sürekliliği planlarında oldukça kısıtlı yer bulan salgın hastalıkların bilinenden/beklenenden daha büyük olasılığa/etkiye sahip olduğu görüldüğünden yeni normal dönemde salgın hastalık riski ile uygulamaya alınacak aksiyonlar daha iyi analiz edilecektir. Salgın döneminde, organizasyon bünyesinde tutulan cihazların fiziksel güvenliklerine verilen öneme nazaran mobil cihazların güvenliği odak noktası olmuştur. Dolayısıyla mobil cihazlar için siber güvenlik kapsamında birçok tedbir/önlem geliştirilmiştir. Tüm bunlara ek olarak; özellikle uzaktan çalışma, uzaktan eğitim ve çevrimiçi alışveriş gibi faaliyetlerde son kullanıcı odaklı bilgi güvenliği eğitimlerine ve farkındalık için bilgilendirme çalışmalarına verilen önem artmıştır.

Yerli ve milli iletişim teknolojilerinin önemi bir kez daha anlaşılmıştır. Yabancı aktörlerin milli bilgileri ele geçirmesi, kullanması ve işlemesi olasılıklarına karşı kurumlar, yabancı kaynaklı çözümler yerine mümkün olduğunca yerli ve milli teknolojilere odaklanmış ve daha çok şirket içi (on-premise) çözümlere yönelmiştir. Buna ek olarak ilgili süreçte, çeşitli güvenlik hizmeti sunan firmaların da değişime uyum sağladığı ve ürün portföyünü uzaktan çalışma ortamına ve mobil cihazlara yönelik genişlettiği görülmüştür. Ayrıca bu dönemde, saldırganların/saldırı vektörlerinin hızlı tespit edilmesi ve ivedi aksiyon alınması için siber tehdit istihbaratının önemi kavranmıştır. Bu kapsamda, siber tehdit istihbaratının kullanımına ve üretilmesine ilişkin çalışmalara ağırlık verilmiştir.

Bilgi ve İletişim Güvenliği Tedbirleri Rehberi, Uzaktan Çalışma ve Videokonferans Güvenliği

Kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında genel olarak alması gereken tedbirleri belirlemek için 06.07.2019 tarih ve 30823 sayılı Resmi Gazetede "Bilgi ve İletişim Güvenliği Tedbirleri" konulu 2019/12 sayılı Cumhurbaşkanlığı Genelgesi yayımlanmıştır. Yayımlanan Genelge doğrultusunda T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi koordinasyonunda paydaşların katılımıyla bu Bilgi ve İletişim Güvenliği Rehberi hazırlanmaktadır.

Bilgi ve İletişim Güvenliği Rehberinin temel amacı; bilgi güvenliği risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilginin/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır.

Rehberde yer alan varlık gruplarına yönelik güvenlik tedbirleri başlıkları aşağıda listelenmiştir:

- *Ağ ve Sistem Güvenliği*
- *Uygulama ve Veri Güvenliği*
- *Taşınabilir Cihaz ve Ortam Güvenliği*
- *Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği*
- *Personel Güvenliği*
- *Fiziksel Mekanların Güvenliği*

Uygulama ve teknoloji alanlarına yönelik güvenlik tedbirlerinin aşağıda listelenen başlıklar halinde rehberde yer alması planlanmaktadır:

- *Kişisel Verilerin Güvenliği*
- *Mesajlaşma Güvenliği*
- *Bulut Bilişim Güvenliği*
- *Kripto Uygulamaları Güvenliği*
- *Kritik Altyapılar Güvenliği*

Bu başlıklar içerisinde uzaktan çalışmayla ilgili olarak ağ ve sistem güvenliği, fiziksel mekanların güvenliği ve mesajlaşma güvenliği başlıkları altında çeşitli tedbir maddelerinin yer alması planlanmaktadır.

Özellikle mesajlaşma güvenliği altında anlık mesajlaşma, e-posta ve video konferans güvenliği konularının ele alınması ve bu konularla ilgili güvenlik tedbirlerinin oluşturulması hedeflenmektedir. Bu konulardaki genel güvenlik tedbirleri başlıkları altındaki tedbir adlarının aşağıdaki gibi olması beklenmektedir:

- *Mesajlaşma uygulaması seçimi*
- *İletim ortamı güvenliği*
- *Mobil uygulamalar üzerinden gizlilik dereceli veri paylaşımı ve haberleşmenin engellenmesi*
- *Uçtan uca şifreleme*
- *Şifreleme anahtarlarının saklanması*
- *Yönetim arayüzüne erişim*
- *Cihaz üzerindeki verinin şifrelenmesi*
- *Kritik haberleşmenin güvenliği*

Uzaktan Bilgi Güvenliği Farkındalığı

COVID-19 sonrası bilgi güvenliği farkındalık oluşturma süreçlerinin uzaktan yapılması konusuna daha da odaklanılmıştır. Bu kapsamda çevrimiçi eğitim ve farkındalık portalleri önem kazanmaktadır.

Bilgi güvenliği farkındalığı konusunda www.bilgimikoruyorum.org.tr internet sitesi ulusal çapta hizmet vermektedir. "Bilgimi Koruyorum E-Öğrenme Projesi", bilgi güvenliği haberleşme ve ileri elektronik alanlarında çalışmalarda bulunan TÜBİTAK BİLGEM tarafından gerçekleştirilmiş olan bir projedir (Bilgimi Koruyorum, 2020). Görsel 8'de "Bilgimi Koruyorum" İnternet sitesi ekran görüntüsü yer almaktadır.

2005 yılında ülkemizin bilgi ve iletişim teknolojilerinden etkin olarak yararlanması ve bilgi toplumuna dönüşmesi ile ilgili uygulanacak stratejiler "Bilgi Toplumu Stratejisi" adlı çalışmada belirlenmiştir. Bilgi Toplumu Stratejisi'nin Eylem Planı'nın 88. Maddesi Ulusal Bilgi Sistemleri Güvenliği Programıdır ve bu maddenin sorumlusu olarak TÜBİTAK BİLGEM belirlenmiştir (Bilgimi Koruyorum, 2020).

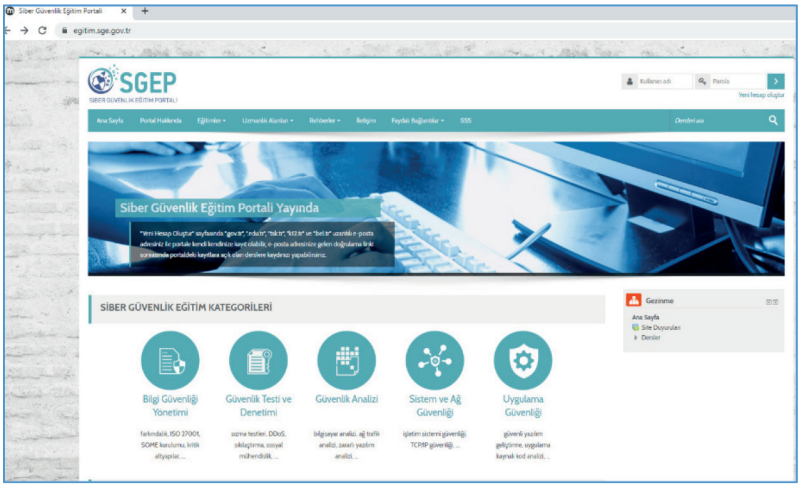
Görsel 8. "Bilgimi Koruyorum" İnternet sitesi

Çevrimiçi eğitim portali konusunda Siber Güvenlik Eğitim Portali isimli egitim.sge.gov.tr internet sitesi TÜBİTAK BİLGEM tarafından hizmet vermektedir.

Siber Güvenlik Eğitim Portali, Kalkınma Bakanlığı işbirliği ile TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü tarafından yürütülen Siber Güvenlik Eğitim ve Araştırma Merkezi Projesi - Siber Güvenlik Eğitim Altyapısı iş paketi kapsamında hayata geçirilmiştir (Siber Güvenlik Eğitim Portali, 2020). Görsel 9'da "Siber Güvenlik Eğitim Portali" İnternet sitesi ekran görüntüsü yer almaktadır. Siber Güvenlik Eğitim Portali ile;

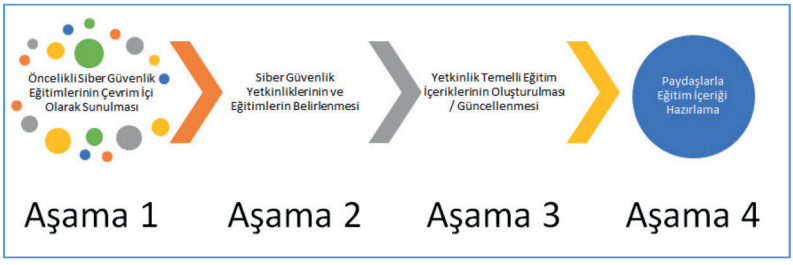
- *Toplumun siber güvenlik ile ilgili konularda farkındalığının artırılması,*
- *Yükseköğretim öğrencilerinin siber güvenlik teknolojileri konusunda teknik bilgi edinebilmeleri,*
- *Siber güvenlik alanında çalışan uzmanların yetkinliklerinin geliştirilmesi için ihtiyaç duyulan eğitimlerin çevrim içi olarak sunulması planlanmaktadır (Siber Güvenlik Eğitim Portali, 2020).*

Görsel 9. "Siber Güvenlik Eğitim Portali" İnternet sitesi



Hayata geçirilen portal aynı zamanda 2016-2019 Siber Güvenlik Stratejisi ile belirlenen hedeflerin gerçekleştirilmesine katkı sağlamaktadır. Siber Güvenlik Eğitim Portali içeriğinin Görsel 10'da belirtilen aşamalara göre tamamlanması ve yaygınlaştırılması hedeflenmektedir (Siber Güvenlik Eğitim Portali, 2020).

Şekil 10. Portal içeriği yaygınlaştırma aşamaları



".gov.tr", ".edu.tr", ".tsk.tr", ".k12.tr" ve ".bel.tr" uzantılı e-posta adresine sahip bir kullanıcının kayıt olabileceği Siber Güvenlik Eğitim Portali aşağıda listelenen 5 kategori bazında eğitimler sunmaktadır (Siber Güvenlik Eğitim Portali, 2020):

- *Bilgi Güvenliği Yönetimi*
- *Güvenlik Testi ve Denetimi*
- *Güvenlik Analizi*
- *Sistem ve Ağ Güvenliği*
- *Uygulama Güvenliği*

Portalde yer alan eğitimler sanal siber güvenlik laboratuvarı altyapısını kullanabilmekte, bu altyapı kullanıcıların eğitimlerden edindikleri bilgiyi beceriye

dönüştürebilmesinde anahtar rol oynamaktadır. Portalde çevrimiçi eğitimlerin yanısıra, aşağıda listelenen rehberler de tüm kullanıcıların erişimine açılmıştır:

- *Temel Siber Güvenlik Gereksinimleri*
- *Siber Güvenlik Teknoloji ve Ürün Taksonomisi*
- *Güvenli Yazılım Geliştirme Kılavuzu*
- *Kurumsal Uygulamalarda Kişisel Verilerin Korunması Rehberi*

Bulut Bilişimde Veri Güvenliği

Bulut bilişim güvenliği alanında en önemli güvenlik konuları veri erişilebilirliği, gizliliği ve bütünlüğü gibi sorunlarla birlikte bulutta akan ve bulutta depolanan verilerin güvenliği olarak sınıflandırılabilir. Bulutta veri güvenliği ile ilişkili olarak kimlik yönetim sistemlerinin güvenli bir şekilde geliştirilmesi ve uygulanması gerekmektedir. Bu bölümde veri güvenliği özellikleri, veri yaşam döngüsü ve veri güvenliği sağlama yöntemleri açıklanacaktır.

Veri Güvenliği Özellikleri

Bulutu kullanırken verilerle ilgili sağlanması gereken mahremiyet, gizlilik, bütünlük ve erişilebilirlik özellikleri bu bölümde açıklanmaktadır. Mahremiyet, bulut ortamlarındaki veri güvenliğinde ele alınması gereken en önemli konulardan birisidir. Mahremiyet, bir bulut kullanıcısının kimlik bilgilerinin yetkisiz kullanıcılara açılmamasını sağlamaktır. Bu özellik, özellikle hassas verilerle çalışan, bulut kullanıcıları için çok önemlidir.

Veri gizliliği, bulut kullanıcılarına ait verilerin yetkisiz taraflara ifşa edilmemesini sağlayan özelliktir. Bulut hizmet sağlayıcı, temel olarak bulut kullanıcılarının verilerinin güvenliğini sağlamaktan sorumludur. Çoklu kiracılık modeli veri güvenliğinin sağlanması konusunda karmaşıklığı arttıran bir etken olarak ortaya çıkmaktadır. Çünkü birden fazla müşteri bir bulut kullanıcısını verilerini depoladığı aynı donanıma erişebilir. Bazı bulut hizmet sağlayıcıları iş planlaması ve kaynak yönetimi tekniğini kullanırken, bazıları ise fiziksel donanımlarını verimli kullanmak için sanallaştırma tekniğini tercih etmektedir. Bu iki yöntemin, saldırganların aynı makinedeki bir hedef sanal makineden bilgi almak için ana bilgisayara ve o makinedeki diğer sanal makinelere yan kanal saldırılarına dayanıklı olması gerekmektedir

Verilerin bütünlüğü, bulutta depolanan verilerin, bulut kullanıcısı tarafından alınırken yetkisiz kişiler tarafından herhangi bir şekilde değiştirilmemesini ifade etmektedir. Bunu sağlamak için, bulut hizmet sağlayıcıları hiçbir üçüncü tarafın aktarılan veya depolanan verilere erişiminin olmadığını taahhüt etmelidir. Yalnızca yetkili bulut kullanıcıları verilerini değiştirebilmelidir.

Erişilebilirlik, bulut kullanıcılarının verilerine kesintisiz olarak erişmesini içermektedir. Meydana gelebilecek herhangi bir DDoS saldırısına karşı bulut ortamının dayanıklı olması gerekmektedir.

Veri Yaşam Döngüsü
Bir buluttan veri akışı çeşitli farklı aşamalardan geçer ve her aşama önceki özelliklerin bir veya daha fazlasının korunmasını gerektirir. Veri yaşam döngüsü, verinin üretilmesinden verinin imhasına kadar olan tüm süreci ifade eder. Veri yaşam döngüsü yedi kısma ayrılmaktadır (Chen & Zhao, 2012).

Veri oluşturma, veri sahipliği ile ilgilidir. Geleneksel bilgi sistemleri ortamında, genellikle kullanıcılar veya kurumlar verilere sahiptir ve bunları yönetir. Ancak eğer veriler buluta geçirilecekse, veri sahipliğinin nasıl korunacağı göz önüne alınmalıdır. Kişisel bilgiler için veri sahipleri hangi kişisel bilgilerin toplandığını bilme ve bazı durumlarda kişisel bilgilerin toplanmasını ve kullanılmasını durdurma hakkına sahiptir.

Geleneksel bilgi sistemlerinde veri iletimi genellikle şifreleme gerektirmez veya yalnızca basit bir veri şifreleme önlemine sahiptir. Bulut ortamlarında veri iletimi için, verilerin yetkisiz kullanıcılar tarafından kullanılmasını ve bunlara müdahale edilmesini önlemek için hem veri gizliliği hem de bütünlüğü sağlanmalıdır. Veri bütünlüğünün sağlanması için veri iletim protokollerinin hem gizlilik hem de bütünlüğü sağlaması gerekmektedir. Veri iletiminin gizliliği ve bütünlüğü, yalnızca kurumsal depolama ve bulut depolama arasında değil, aynı zamanda farklı bulut depolama hizmetleri arasında da sağlanmalıdır.

PaaS veya SaaS modelinde bulut tabanlı uygulamalar tarafından kullanılan statik veriler için, çoğu durumda veri şifreleme mümkün değildir. Veri şifreleme, dizin oluşturma ve sorgulama sorunlarına yol açacağından, bulut tabanlı uygulamalar tarafından kullanılan statik veriler genellikle şifrelenmez. Yalnızca bulutta değil, geleneksel bilgi teknolojileri ortamlarında da, işlenen veriler, ilgilenilecek herhangi bir program için şifrelenmez. Bulut bilişim modellerinin çok kiracılı özelliği nedeniyle, bulut tabanlı uygulamalar tarafından işlenen veriler diğer kullanıcıların verileriyle birlikte saklanır. İşlemdeki şifrelenmemiş veriler veri güvenliği için ciddi bir tehdittir. Hassas veri sahipleri, kişisel bilgi kullanımının bilgi toplama amaçlarıyla tutarlı olup olmadığına ve kişisel bilgilerin üçüncü taraflarla, örneğin başka bulut servis sağlayıcılarıyla paylaşılıp paylaşılmadığına odaklanmalı ve bunu HSS'de belirtmelidir.

Veri paylaşımı, verilerin kullanım durumunu genişletip veri izinlerini daha karmaşık hale getirmektedir. Veri sahipleri, başka bir tarafı, verisinin paylaşımı için yetkilendirebilir fakat verisini paylaştığı taraf, veri sahiplerinin rızası olmadan verileri başka bir tarafla paylaşabilir. Bu nedenle, veri paylaşımı sırasında, özellikle üçüncü bir tarafla paylaşıldığında, veri sahiplerinin üçüncü tarafın orijinal koruma önlemlerini ve kullanım kısıtlamalarını sürdürüp sürdürmediğini göz önüne alması gerekir.

Bulut depolarında depolanan veriler, diğer yerlerde saklanan verilerle benzer şekildedir ve bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik özelliklerinin sağlanması gerekmektedir. Veri gizliliği için ortak çözüm veri şifrelemedir. Şifrelemenin etkin olmasını sağlamak için, hem şifreleme algoritmasının hem

de anahtar gücünün kullanımını göz önünde bulundurmak gerekmektedir. Büyük miktarda veri iletimi, depolama ve işleme içeren bulut bilgi işlem ortamı olduğundan, işlem hızını ve hesaplamayı da göz önünde bulundurmak gerekir.

Verilerin arşivlenmesi, tesis dışında depolama ve depolama süresine bağlı olarak depolama ortamına odaklanır. Veriler taşınabilir bir ortamda depolanıyorsa ve ardından ortam kontrol dışı ise, verilerin sızıntı riski muhtemeldir. Bulut ortamında arşivleme amaçlı kullanılan görece ucuz katmanların güvenliğinin sağlanması veya çoklu ve hibrit bulut ortamlarında farklı alanlarda saklanan arşiv veri ile operasyonel verinin gerektiğinde güvenli entegrasyonlarının sağlanması gibi senaryolarda güvenli veri paylaşımı standartlarının sağlanması gerekir.

Verilere artık gerek kalmadığında, tamamen yok edilip edilmediğinden emin olunması gerekmektedir. Depolama ortamının fiziksel özellikleri nedeniyle, silinen veriler hala mevcut olabilir ve geri yüklenebilir. Bu, hassas bilgilerin yanlışlıkla ifşa edilmesine neden olabilir. Veri imha süreçlerinin net bir şekilde tanımlanması ve bulut hizmetleri altyapısının bu süreçlerle uyumlu bir şekilde yönetiliyor olması gerekir.

Veri Güvenliğini Sağlama Yöntemleri

Bulut bilişimde veri güvenliğinin sağlanmasında kimlik erişimi yönetimi (Identity Access Management) sistemlerinin önemli bir rolü bulunmaktadır. Kimlik erişim yönetimi, bulut uygulamalarının güvenliğini analiz etmek için en iyi uygulamalardan biridir. Kimlik erişim yönetimi bulut sistemleri için veri güvenliğinde etkin güvenlik sağlar. Kimlik erişim yönetimi sistemleri, bulut ortamında güvenlik sağlamak için kimlik doğrulama ve yetkilendirme sağlama gibi farklı işlemleri gerçekleştirir. Kimlik erişim yönetimi sistemi, bulut sistemlerinde doğru kişilere izin verilmesini sağlayarak bulut kullanıcılarının kimliklerinin ve özelliklerinin güvenliğini garanti eder. Kimlik erişim yönetimi sistemleri, doğru ayrıcalıklara sahip doğru kişinin bulut sistemlerinde depolanan bilgilere erişip erişmediğini kontrol ederek erişim haklarının yönetilmesine de yardımcı olur (Indu, Anand, & Bhaskar, 2018). Şu anda, birçok kurum bulut ortamında depolanan hassas bilgiler için daha fazla güvenlik sağlamak üzere kimlik erişim yönetimi sistemlerini kullanmaktadır. Bu bölümde veri güvenliğinin sağlanması konusunda kimlik erişim yönetim sistemlerinin kullandığı doğrulama ve yetkilendirme mekanizmaları ile ilgili temel bilgiler aktarılacaktır.

i. Kimlik Doğrulama (Authentication) Mekanizmaları

Kimlik doğrulama, bir varlığı başka bir varlık aracılığıyla onaylama işlemidir. Kişinin veya uygulamanın erişim veya hak talebinde bulunmaya uygun olup olmadığından emin olmak için kullanılır. Kimlik doğrulama işlemi genellikle bir yazılım veya bir yazılım parçası tarafından gerçekleştirilir. Ağ ortamındaki ortak kimlik doğrulama yöntemleri fiziksel güvenlik mekanizmaları ve dijital güvenlik mekanizmaları olarak iki kısma ayrılmaktadır. Fiziksel güvenlik me-

kanizmaları erişim kartları ve iris veya retina tanıma, parmak izi tanıma, yüz tanıma ve biyometrik kimlik doğrulama mekanizmaları olarak sınıflandırılabilir. Dijital güvenlik mekanizmalarına örnek olarak oturum açma kimlik bilgileri, SSH anahtarları, çok faktörlü kimlik doğrulama, Chip/PIN, SSO (Single Sign-On) protokolleri verilebilir. Bir bulut sistemi, yukarıda belirtilen kimlik doğrulama mekanizmalarının herhangi birini veya bir kombinasyonunu takip edebilir.

ii. Kimlik Yetkilendirme (Authorization) Mekanizmaları
Yetkilendirme, bir yetkilendirilmiş kullanıcının girişlerine bağlı olarak belirli bir kaynağa erişmesine izinin verilip verilmeyeceğinin karar verilmesidir. Yetkilendirme işlemi, hangi kullanıcının veya hangi uygulamaların sistem üzerinde çalışmasına izin verildiğine karar verir. Bulut ağı, her bir hizmet farklı bir hizmet sağlayıcıdan ve farklı güvenlik düzeylerine sahipken, tek bir kullanıcının farklı hizmet türlerine aynı anda erişebildiği farklı kira hizmeti sağlayıcıları ortamı içerir. Sosyal ağ kimlik bilgileri aracılığı ile bulut altyapısı üzerindeki uygulama yetkilendirildiğinde, sosyal ağ kimlik bilgilerini kullanan başka uygulamalar tarafından da erişilebilir hale gelir. Bulut ortamında yetkilendirme, erişim kontrol politikalarıyla sağlanır. Bulut servis sağlayıcıları, kaynaklara ve hizmetlere yalnızca yetkili kullanıcılar tarafından erişilecek şekilde erişim kontrol politikalarını tanımlar ve uygular. Merkezi erişim kontrolü mekanizmaları, hassas bilgilerin güvenliğini sağlamada, çeşitli yönetim ve güvenlik görevlerini azaltmada kuruluşlar için avantajlıdır. Kimlik yetkilendirme mekanizmalarını erişim kontrol mekanizmaları ve erişim kontrol yönetişimi olarak iki kısımda toplanabilir. Kimlik yönetim sistemlerinde kullanılan erişim kontrol mekanizmaları; zorunlu erişim kontrolü (mandatory access control), isteğe bağlı erişim kontrolü (discretionary access control), yetki/göreve dayalı erişim kontrolü (entitlement /task based access control), rol tabanlı erişim kontrolü (role based access control) ve öznitelik tabanlı erişim kontrolü (attribute based access control) olarak sınıflandırılabilir. Kimlik yönetim sistemlerinde kullanılan erişim kontrol yönetişimi ise sertifika ve risk puanı, yaşam döngüsü yönetimi ve görev ayrımı olarak sınıflandırabilir.

Uzaktan Çalışma Süresince Dikkat Edilmesi Gereken Siber Güvenlik Hususları
Uzaktan çalışma süresince dikkat edilmesi gereken siber güvenlik hususları, işletmelerin alabileceği önlemler ve bireysel olarak alınabilecek önlemler olarak iki başlıkta açıklanmıştır.

Kurumların Alabileceği Önlemler
Uzaktan çalışmak kurumlar için yeni risklerin ortaya çıkmasına neden olmaktadır. Ancak bu risklerin çoğu uzaktan bağlantı için kullanılan sistemlerin güvenliğinin sağlanmasıyla engellenebilir. Bu kapsamda iş sistemlerine dışarıdan erişilememesi ve uzaktan yapılan bağlantıların güvenliğinin sağlanması gerekmektedir.

Güvenli bir VPN uygulaması güçlü şifreleme ve çok aşamalı kimlik doğrulama mekanizmalarına sahip olmalıdır. Bu mekanizmaların kullanımı tüm kullanı-

cılar için geçerli olmalıdır. Özellikle iş yeri dışarısındaki bağlantı ortamlarının her türlü tehdidi barındırabileceği düşünüldüğünde, kullanıcı bilgisayarlarında gerekli görülen güvenlik ürünlerinin kullanılması önem taşımaktadır. Bununla beraber iş bilgisayarlarının kişisel işlerde kullanımının olabildiği ölçüde engellenmesi gerekmektedir. Kullanıcıların uzaktan çalışma döneminde karşı karşıya kalabileceği riskler ve özellikle sosyal mühendislik saldırıları konusunda bilgilendirilmesi uç noktadaki güvenlik için önemlidir.

Bu önlemlerle kullanıcı güvenliği büyük ölçüde sağlanmakla beraber, olağan durumda yapılan; oltalama e-postalarının, zararlı yazılımların ve alan adlarının takibi işlemlerine Koronavirüs dolayısıyla oluşabilecek riskler de düşünülerek devam edilmelidir. E-posta sunucularının güvenliğine önem verilmeli ve bu yolla gelen dosyaların anti-virüs taramasından geçirilmesi gibi genel önlemler uygulanmalıdır.

Uzaktan çalışmanın yaygın bir şekilde yapıldığı Koronavirüs salgını döneminde toplantıların yapılması için çalışanlara güvenli toplantı ortamı önerilmelidir. Üçüncü parti bir servis üzerinden bu toplantılar yapılacak ise bu servisin güvenilirliği denetlenmelidir. Mümkün olduğu durumda uçtan uca şifreleme kullanmayı garanti eden servisler tercih edilmeli veya toplantı altyapısı işletme tarafından sağlanmalıdır.

Farklı kaynaklardan alınan hizmetlerin kullanımı sırasında aktarılan kişisel verilerin, bu platformlarla etkileşimi düşünülerek, Kişisel Verilerin Korunması Kanunu kapsamındaki yükümlülüklerin yerine getirilmesine dikkat edilmelidir.

Bireysel Olarak Alınabilecek Önlemler

Çoğu saldırı vektörünün kullanıcıların bilgisayarına istenmeyen yazılımları yüklemek için kullanıldığı görülmektedir. Bu nedenle yüklenen yazılımların denetlenmesi ile çoğu saldırı tehdidine karşı savunma yapılabilir. Kullanılan yazılımlar konusunda aşağıdaki tedbirler dikkate alınmalıdır:

- Masaüstü uygulamalarının bilgisayara yüklenmesi yerine güvenilir kaynaktaki web servislerinin kullanılması, bu güvenilir kaynakların çoğunlukla arama motorlarında ilk sıralarda bulunabilmesi nedeniyle çoğu zaman daha kolay ve güvenlidir.
- Benzer şekilde Google Play Store veya App Store'da bulunan uygulama indirme sayıları önemli bir güvenilirlik göstergesidir.
- Uygulamaların işlevini yerine getirebilmesi için hangi izinlerin gerekebileceği düşünülerek izinler verilmelidir. Uygulamalara gereksiz yere yüksek yetkiler verilmemelidir.
- Özellikle İnternetle etkileşimimizde önemli bir araç olan İnternet tarayıcılarının güncel olması önemlidir. Mobil cihazlar da dahil olmak üzere yaygın olarak kullanılan tarayıcılar tercih edilmelidir.

İnternet erişimi ve bağlantının güvenliği için;

- *Aynı parola birden fazla yerde kullanılmamalı ve yeterli karmaşıklıkta olmalıdır.*
- *Bir web sitesinin neden başka bir web sitesinde kullanılan hesap bilgilerine ihtiyaç duyabileceği düşünülmeli ve hesap bilgileri farklı web siteleri ile paylaşılmamalıdır.*
- *Güvenli Wi-Fi erişimi sağlanmalıdır. Wi-Fi erişimi parola ile korunmalı ve erişimde güvenli şifreleme kullanılmalıdır.*

E-posta güvenliğinin önemi de oltalama saldırılarıyla beraber artmıştır. Ancak çoğu oltalama e-postasından korunmak için dikkat edilebilecek birkaç önemli nokta vardır. Örneğin yazım hataları bu e-postaları belirlemek için kullanılabilecek kolay bir yöntemdir. Saldırganlar çoğu zaman spam filtrelerini atlatmak için bu tarz yollara başvurmaktadırlar. Bunun yanında e-postalarda bulunan bağlantılara tıklamadan önce web adresine dikkat edilmesi gerekmektedir. Bağlantılar metin içerisinde görünen adrese işaret etmiyor olabilir. Bu nedenle şüpheli gelen bağlantılara tıklamak yerine, web sayfasının e-posta içerisinde bulunan ilgili sözcüklerle beraber arama motorlarından araştırılması sizi birçok yanıltmacadan koruyacaktır. Unutmayın ki e-posta güvenilir bir kaynaktan geliyor olsa dahi birçok nedenden dolayı yanlış bilgi, zararlı yazılım ve kötü amaçlı bağlantı içeriyor olabilir.

Bir e-postanın oltalama amacıyla gönderildiği fark edilirse, bu e-posta mümkün olan en az etkileşimle silinmelidir. Kurumsal hesaplara gelen oltalama e-postaları için ilgili kişiler bilgilendirilmelidir.

Son olarak Koronavirüs dolayısıyla oluşabilecek bilgi kirliliğini önlemek için yapılabileceklerden söz edilmelidir. Bunlardan en önemlisi güvenilir olmayan haber kaynaklarından ve mesajlaşma uygulamalarından elde edilen bilgilerin kaynağının araştırılmasıdır. Güvenilir kaynaklardan doğrulanamayan bilgilere ise itibar edilmemeli ve bu bilgiler başkalarıyla paylaşılmamalıdır. Bu süreci toplum sağlığına ve kamu düzenine zarar vermek için fırsat olarak gören kişilerin olabileceği de düşünülerek hareket edilmelidir. Bilgi edinmek için resmi kaynaklar ve güvenilirliği olan uluslarası kuruluşların web sayfaları ve e-posta listeleri takip edilebilir.

Sonuç

Küresel salgın sonrasında ulusal bilişim güvenliğine yönelik yapılan ve yapılması gereken çalışmalar hakkında bilgi vermek amacıyla hazırlanan bu çalışma kapsamında bilgi teknolojileri altyapısı ve siber güvenliğin, yaşanan bu süreçte en önemli konular arasında yer aldığı görülmektedir. COVID-19 tehdidi sürecinde alınan tedbirler ve sosyal yaşantıda görülen değişimler nedeni ile dijital platformlar, uzaktan erişim ve haberleşme sistemlerinin kapasitesi, performansı ve sürekliliği de çalışma modellerinin değişmesiyle birlikte yeniden ele alınmakta ve değerlendirilmektedir.

Dijital dönüşüm sürecini derinden etkileyen COVID-19 salgınına karşı hızlı yanıt verebilmek için, kurumların mevcut süreçlerini gözden geçirerek çevik ve esnek bir yapıya dönüşmek adına aksiyonlar alması gerektiği görülmekte olup; ağ ve sistem güvenliği, uygulama ve veri güvenliği, taşınabilir cihaz ve ortam güvenliği, nesnelerin interneti cihazlarının güvenliği, personel güvenliği, mesajlaşma güvenliği ve bulut bilişim güvenliği gibi kritik konularda kurumların ulusal bilişim güvenliğinin sağlanması doğrultusunda gerekli önlemleri zamanında ve etkin olarak almaları kritik öneme sahiptir.

Teşekkür

Makalenin hazırlanması aşamasında görüş ve yorumlarını esirgemeyip makalenin olgunlaşması sürecinde katkı veren TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü Müdürü Mustafa Dayıoğlu'na, Yazılım Teknolojileri Araştırma Enstitüsü Müdürü Cemil Sağıroğlu'na, Bilişim Teknolojileri Enstitüsü Müdür Yardımcısı Dr. Hamza Özer'e, Siber Güvenlik Enstitüsü yöneticileri Necati Ersen Şişeci'ye, Özgür Yürekten'e, Emre Özkök'e, Bilişim Teknolojileri Enstitüsü'nden Mustafa Evcimen'e ve Yazılım Teknolojileri Araştırma Enstitüsü Yetkinlik Uzman Grubuna teşekkürlerimizi borç biliriz. Ayrıca makalenin hazırlanma sürecinde koordinatörlüğünü üstlenen TÜBİTAK BİLGEM Başkan Danışmanı Abdullah Alpaydın'a da şükranlarımızı sunarız.

Kaynakça

2016-2019 Ulusal Siber Güvenlik Stratejisi. (2016). *T.C. Ulaştırma ve Altyapı Bakanlığı.* Erişim: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf (ET: 15.05.2020)

5G ile İhracatçılar E-Ticatette Atağa Kalkıyor. (2020). *TİMReport* (183), 62-63. Erişim: https://tim.org.tr/files/downloads/Timreport/TIMReport183.pdf (ET: 20.05.2020)

Beware of criminals pretending to be WHO. (2020). World Health Organization: Erişim: https://www.who.int/about/communications/cyber-security (ET: 20.05.2020)

Bilgimi Koruyorum. (2020). Erişim: http://www.bilgimikoruyorum.org.tr/ (ET: 15.05.2020)

Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *International Conference on Computer Science and Electronics Engineering, DOI:10.1109/ICCSEE.2012.193.*

(2020). *COVID-19 Salgını Esnasında Gerçekleşen Sağlık Sektörü Hedefli Siber Olaylar*. STM. Erişim: https://www.stm.com.tr/documents/file/COVID-19_saglik_sektoru_siber_g%C3%BCvenlik_olaylari_170420.pdf (ET: 10.05.2020)

Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı. (2020). Erişim: https://cbddo.gov.tr/hizmet-birimlerimiz/siber-guvenlik-dairesi-baskanligi/ (ET: 20.05.2020)

Formula 1 launches Virtual Grand Prix Series to replace postponed races. (2020). Formula 1 Web sitesi. Erişim: https://www.formula1.com/en/latest/article.formula-1-launches-virtual-grand-prix-series-to-replace-postponed-races.1znLAbPzBbCQPj1IDMeiOi.html (ET: 10.05.2020)

Indu, I., Anand, P., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an Internal Journal.*

Kumaran, N., & Lugani, S. (2020). *Protecting businesses against cyber threats during COVID-19 and beyond*. Google Cloud Blog. Erişim: https://cloudblog.withgoogle.com/products/identity-security/protecting-against-cyber-threats-during-COVID-19-and-beyond/amp/ (ET: 12.05.2020)

Kurumsal SOME Kurulum ve Yönetim Rehberi. (2020). *T.C. Ulaştırma ve Altyapı Bakanlığı.* Erişim: https://www.uab.gov.tr/uploads/pages/siber-guvenlik/kurumsal-some-reh-v1.pdf (ET: 15.05.2020)

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing, National Institute of Standards and Technology*, Information Technology Laboratory.

Siber Güvenlik Eğitim Portali. (2020). Erişim: https://egitim.sge.gov.tr/ (ET: 20.05.2020)

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi İnternet Sitesi. (2020). Erişim: https://cbddo.gov.tr/hakkimizda/ (ET: 15.05.2020)

Türkiye Siber Güvenlik Kümelenmesi. (2020). Erişim: https://siberkume.org.tr/About (ET: 10.05.2020)

USOM Hakkımızda. (2020). Erişim: https://www.usom.gov.tr/hakkimizda.html (ET: 20.05.2020)