2024

6(1), 36-56

2022 Yılında Yaşanan Gelişmeler Doğrultusunda Bilgi Güvenliğinde Risk Yönetiminin Artan Önemine İlişkin Bir Değerlendirme

Merve Tunçbilek*[1]

Anahtar Sözcükler

Risk yönetimi
Bilgi güvenliği
Siber güvenlik
BGYS
ISO 27001

Makale Hakkında

Gönderim Tarihi
12 Nisan 2023
Kabul Tarihi
07 Haziran 2024
Yayın Tarihi
30 Haziran 2024

Makale Türü
Araştırma Makalesi

Öz

Güvenlik olaylarının etkilerini minimize etme, bilgi varlıklarını koruma, müşteri güveni ve işin sürdürülebilirliğini temin etmek üzere tasarlanan bilgi güvenliği yönetim süreci bilgi ve iletişim teknolojilerinde yaşanan gelişmelerle önemi giderek artan bir noktaya gelmiştir. Bu sistematik yaklaşım; bilgi güvenliğini kurma, uygulama ve işletme, izleme ve gözden geçirme, sürdürme ve iyileştirme süreçleri ile kurumsal hedeflere ulaşmayı kolaylaştırmaktadır. Sistemin yönetimi hedeflerin belirlenmesi, gerekliliklerin analizi, kontrollerin geliştirilmesi ve kontrollerin sürekli değerlendirilerek iyileştirilmesi çerçevesinde bütüncül bir yaklaşım ile sağlanmalıdır. Gizlilik, bütünlük ve erişilebilirlik unsurları kapsamında bilgi güvenliği risk temelli bir yönetim anlayışının benimsenmesini gerekli kılmaktadır. Bu kapsamda rehber olarak uluslararası ISO 27001 standardı kullanılabilmektedir. ISO 27001, uygun bir bilgi güvenliği yönetim sisteminin uygulaması hakkında bir dizi ilkeleri belirlemektedir. Çalışmada 2022 yılında yaşanan bilgi güvenliği olayları ışığında etkin bir bilgi güvenliği risk yönetim sürecinin işletilmesinin gerekliliği tartışılmıştır. Doküman analizi yöntemi ile yayımlanmış makaleler, bildiri ve tezler, web sayfa içerikleri ve sektör raporları analiz edilerek kurumsal ve bireysel ölçekte alınabilecek önlemlere de yer verilmiştir.

An Evaluation of the Increasing Importance of Risk Management in Information Security in Line with the Developments in 2022

Keywords

Risk management
Information security
Cyber security
ISMS
ISO 27001

Article Info

Received
April 12, 2023
Accepted
June 07, 2024
Published
June 30, 2024

Article Type
Research Paper

Abstract

The information security management process, designed to minimize the effects of security incidents, protect information assets, ensure customer trust and business sustainability, has become increasingly important with the developments in information and communication technologies. This systematic approach; It facilitates the achievement of corporate goals with the processes of establishing, implementing and operating information security, monitoring and reviewing, maintaining and improving. The management of the system should be provided with a holistic approach within the framework of determining the targets, analyzing the requirements, developing the controls, and constantly evaluating and improving the controls. Within the scope of confidentiality, integrity and accessibility, information security requires the adoption of a risk-based management approach. In this context, the international ISO 27001 standard can be used as a guide. ISO 27001 specifies a set of principles on the implementation of an appropriate information security management system. In the study, the necessity of operating an effective information security risk management process in the light of information security events in 2022 is discussed. The measures that can be taken on an institutional and individual scale are also included by analyzing the articles, papers and theses, web page contents and sector reports published with the qualitative analysis method.

Atıf: Tunçbilek, M. (2024). 2022 yılında yaşanan gelişmeler doğrultusunda bilgi güvenliğinde risk yönetiminin artan önemine ilişkin bir değerlendirme. *Bilgi ve İletişim Teknolojileri Dergisi, 6*(1), 36-56. https://doi.org/10.53694/bited.1282138

Cite: Tuncbilek, M. (2024). An evaluation of the increasing importance of risk management in information security in line with the developments in 2022. *Journal of Information and Communication Technologies, 6*(1), 36-56. https://doi.org/10.53694/bited.1282138

*Sorumlu Yazar/Corresponding Author

[1] Dr., Devlet Hava Meydanları İşletmesi Genel Müdürlüğü, Ankara/Türkiye, merveguven@yahoo.com, https://orcid.org/0000-0002-7579-5157

Extended Abstract

Introduction

The digital transformation process, which manifests itself with the rapid change in information and communication technologies in the world and in our country, has caused radical changes in many business lines. While developments such as big data and artificial intelligence that accompany the digital transformation process show themselves in sectors that show rapid development and growth; serious reform trends in the public sector have led to the entry into the process.

It is possible to say that "security" threats come first among the determining factors in the public reforms shaped by the effects of the developments. Primitive security measures applied in the past have been replaced by modern applications with the development of technology, and thus the concept of information security has gained even more importance.

When it comes to information security, three basic elements come to mind. These elements ensure that the information system operates in an accessible, secure and unharmed operating environment and that information assets are protected, and are considered as confidentiality, integrity, availability (Gollman, 1999; Harris, 2002; Jonsson, 1996).

Information security management is a continuous improvement process designed to minimize the effects of security incidents, protect information assets, ensure customer trust and business sustainability. An information security management system is a systematic approach to establishing, implementing and operating, monitoring and reviewing, maintaining and improving information security to achieve organizational goals. ISMS, the confidentiality, integrity and accessibility of information; It maintains the risk management process by applying and assures the relevant parties that the risks are managed correctly. The management of the system should be provided with a holistic approach within the framework of determining the targets, analyzing the requirements, developing the controls, and constantly evaluating and improving the controls (Ma, Schmidt & Pearson, 2009).

In this study, the importance of the information security management system in organizations will be evaluated in terms of the events experienced in 2022. The questions to be asked in the study can be listed as follows:

- Why has a risk-based security approach become important?
- What are the most important events in the cyber world in the past year?
- What are the studies that need to be done to ensure Information Security?

Method

In the research, document analysis, one of the qualitative analysis methods, was preferred. This method was preferred in order to be able to handle and interpret the research topic in its own context with an interdisciplinary perspective (Altunışık, Coşkun, Bayraktaroğlu ve Yıldırım, 2010).

Information was collected by examining the written documents without the need for interviews and observations about the investigated phenomena and events related to the research subject. This saves resources and time. The examined documents generally consist of published articles, papers and theses, web page contents and sector reports. In this context, a detailed literature review was made and the subject was analyzed.

Conclusion

The wave of digital transformation experienced in the world and in our country has brought some difficulties along with the convenience it provides in the way of doing business. In the new order, public and private sector organizations are faced with a wide variety of information threats. The protection of information technology infrastructures of institutions against cyber attacks is becoming a more important and challenging task day by day. While organizations invest in numerous security measures to protect their sensitive data from outside threats, they remain vulnerable to malicious insiders with privileged access and in-depth knowledge of organizational assets.

Information security is not considered to be fully ensured only by the fulfillment of technological measures. Organizations should consider technological and administrative measures as a whole, and it should not be forgotten that the human factor is also an important factor. Information security is a complex process that includes all these factors.

Organizations that manage critical systems that can cause loss of life, large-scale economic damage, national security vulnerabilities or disruption of public order, loss of trust and reputation when the confidentiality, integrity or accessibility of the processed information/data are compromised should operate an effective information security risk management process as the first priority.

Giriş

Dünyada ve ülkemizde, bilgi ve iletişim teknolojilerinde yaşanan hızlı değişim ile kendisini gösteren dijital dönüşüm süreci birçok iş kolunda köklü değişikliklere neden olmuştur. Dijital dönüşüm süreci beraberinde yaşanan büyük veri ve yapay zekâ gibi gelişmeler hızlı bir gelişme ve büyüme gösteren sektörlerde kendisini gösterirken; kamu sektöründe ciddi reform eğilimleri sürecine girilmesine neden olmuştur.

Yaşanan gelişmelerin etkisiyle şekillenen kamu reformlarında belirleyici unsurların başında "güvenlik" tehditlerinin geldiğini söylemek mümkündür. Geçmişte uygulanan ilkel güvenlik tedbirleri teknolojinin gelişmesiyle, yerini modern uygulamalara bırakmış ve bu sayede bilgi güvenliği kavramı daha da önem kazanmıştır.

5809 sayılı Elektronik ve Haberleşme Kanunu ve beraberinde Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 6698 sayılı Kişisel Verilerin Korunması Kanunu, 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu T.C. Cumhurbaşkanlığı Genelgesi ve beraberinde Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi gibi yasal düzenlemeler, bilgi güvenliği konusuna verilen önemin birer göstergesi olarak değerlendirilebilir.

Ülkemiz yukarıda anılan yasal düzenlemeler ile aynı zamanda kuruluşlara kapsamlı bir Bilgi Güvenliği Yönetim Sistemi (BGYS) süreci benimsemelerini de zorunlu hale getirmiştir. Bilgi varlıklarının ve hizmet süreçlerinin güvenliğinin sağlanmasına verilen önemin bir göstergesi olarak kuruluşların kendi BGYS'lerini uluslararası kabul görmüş TS ISO/IEC 27001 standardı seviyesinde kurup, işletmeleri gerektiği vurgusu yapılmaktadır.

BGYS, bir risk temelli yönetim yaklaşımı olup; kuruluşların uygun bir risk yönetimi plan ve programı belirleyerek uygulamaları ve potansiyel tehditlerin etkilerini kontrol altına almalarını sağlamaktadır.

Bilgi Güvenliği Yönetim Sistemi

Bilgi güvenliği kavramını daha iyi anlaşılabilmesi için öncelikle bilgi ve iletişim teknolojilerinin temel girdisi olan bilginin tanımının yapılması gereklidir. Sözlük anlamıyla bilgi; öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, malumat ve kavrayışın tümüdür. Bilgi güvenliği alanında, varlıklar genellikle yalnızca bilginin kendisini değil bilgi varlıklarını ve bilgi yönetimini kolaylaştırmak için kullanılan kaynakları içerir (Oscarson, 2003).

Bilgi güvenliği denildiğinde akla üç temel unsur gelmektedir. Bu unsurlar bilgi sisteminin erişilebilir bir vaziyette güvenli ve bütünlüğüne zarar gelmemiş bir faaliyet ortamında işlemesini ve bilgi varlıklarının korunmasını temin etmekte olup gizlilik (confidentiality), bütünlük (integrity), erişilebilirlik (availability) olarak kabul edilmektedir (Gollman, 1999; Harris, 2002; Jonsson, 1996).

Bilgi güvenliği yönetimi, güvenlik olaylarının etkilerini minimize etme, bilgi varlıklarını koruma, müşteri güveni ve işin sürdürülebilirliğini temin etmek üzere tasarlanmış sürekli gelişim sürecidir. Bilgi güvenliği yönetim sistemi, kurumsal hedeflere ulaşmak için (1) bilgi güvenliğini kurmak, (2) uygulamak ve işletmek, (3) izlemek ve gözden geçirmek, (4) sürdürmek ve iyileştirmek için benimsenen sistematik bir yaklaşımdır. BGYS, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini; risk yönetimi sürecini uygulayarak muhafaza eder ve ilgili taraflara risklerin doğru bir şekilde yönetildiğine dair güvence verir. Sistemin yönetimi hedeflerin belirlenmesi,

gerekliliklerin analizi, kontrollerin geliştirilmesi ve kontrollerin sürekli değerlendirilerek iyileştirilmesi çerçevesinde bütüncül bir yaklaşım ile sağlanmalıdır (Ma ve diğerleri, 2009).

Kamuoyunun bilgi güvenliği ihlallerine karşı duyduğu endişeden dolayı ISO 27001 standardına uygunluk sertifikasyonu, yöneticinin bilgi süreçlerini değerlendirmesini ve sürecinin uluslararası bir standarda uygun olduğunu göstermektedir. ISO 27001, uygun bir bilgi güvenliği yönetim sisteminin uygulaması hakkında bir dizi ilkeleri belirlemektedir (Hsu, Wang & Lu, 2016). Bu kapsamda bilgi güvenliği standardı, uygulanmak üzere bu ilkeleri özetleyen bir kılavuzdur (Soysal, 2023).

Risk Yönetimi

Bilgi güvenliği alanında dikkate alınması gerekli bir diğer kavram risktir. Risk, doğrudan güvenlikle bağlantılı olmamakla birlikte güvenlik mekanizmalarındaki zafiyetler riskleri artıracaktır (Hsu ve diğerleri, 2016).

Risk bir zarara, bir kayba, bir tehlikeye yol açabilecek bir olayın oluşma olasılığı olarak tanımlanabilir (Cains, Taber, King, & Henshel, 2022). Risk için belirsizlik durumu, riskin gerçekleşeceği varlık ve bu varlığın bulunduğu bir ortam olmalıdır. Risk, gelecekte gerçekleşebileceği değerlendirilen koşulları ilgilendiren bir kavram olup iki kısımdan oluşmaktadır ve aşağıdaki denklemle ifade edilmektedir (Hsu ve diğerleri, 2016):

R=L*P

R: Risk

L: Potansiyel Kayıp

P: Olasılık

Bilgi güvenliği riskini daha spesifik olarak tanımlamak gerekirse; bilgi güvenliği riski, bir varlığın veya varlık grubunun güvenlik açıklarını kuruluşa zarar vermek için belirli bir tehdit olarak kullanma olasılığıdır (Kuzminykh, Ghita, Sokolov, & Bakhshi, 2021).

Kurumlar hedeflerine ulaşmaya çalışırken birtakım riskler ile karşılaşırlar. Bu süreç boyunca karşılaşılan riskleri analiz etme ve yönetme amacıyla sistematik bir yaklaşım benimsenmektedir. Her kurumun kabul edilebilir risk ile risk yönetimi yaklaşımı farklılık gösterebilir. Karşılaştıkları riskleri kabul edebilir ya da seviyesini kabul edilebilir düzeye indirmek için gerekli kontroller ve önlemler uygulayabilirler. Belirtilen bu yönetim süreci kısaca “risk yönetimi” olarak adlandırılır (Kuzminykh ve diğerleri, 2021).

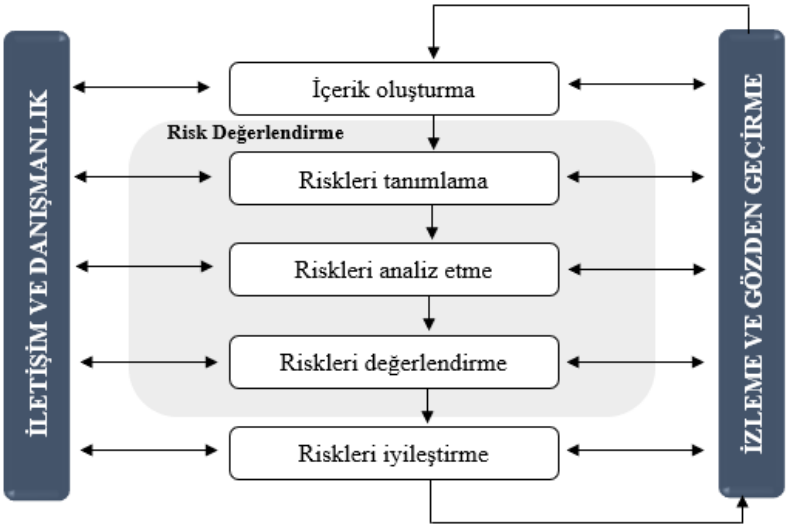
Risk yönetim çerçevesi Şekil1’de yer alan temel modelleri içerir (Bodrožić, 2018):

- İletişim ve danışmanlık – ilgili tüm taraflarla gerçekleştirilir
- İçerik oluşturma – temel risk parametrelerinin oluşturulmasıdır

Uygulama alanı ve risk değerlendirme kriterleri;

- Riskleri tanımlama – riskin kaynağını bulma, potansiyel sonuçların ortaya çıkma durumları
- Riskleri analiz etme – istenmeyen bir olayın olasılığının ve bu olayın neden olduğu hasarın ölçülmesi
- Riskleri değerlendirme - riskin en aza indirilmesi konusunda karar alınması
- Riskleri iyileştirme - olası olumsuz bir olayın nedenini ortadan kaldırmayı veya kontrol etmeyi ve sonuçlarını sınırlamayı amaçlayan bir dizi önlem, prosedür

- İzleme ve gözden geçirme - risk yönetimi sürecindeki tüm faaliyetlerin tutarlılığını ve belgelenmesini sağlar.



Şekil 1. Risk Yönetimi Süreci

Bilgi güvenliği kurumlar için oldukça önemli olup tehditlere karşı korunması gerekmektedir. Risklerini yönetmek, bilgi güvenliği sürecinin ana faaliyetlerinden biri haline gelmiştir. Kurumlar maddi ve manevi açıdan zarara uğramamak, kendilerine yönelen tehditleri ve sistemlerini etkileyecek riskleri gözden geçirmek için bir bilgi güvenliği politikası oluşturmak durumundadır. Bu doğrultuda işletilecek risk yönetimi süreci her kurumun kendi yapısına, kurumsal bağlılıklar ile yasal mevzuatları dikkate alan, bilgi güvenliği alanındaki ulusal/uluslararası standartları destekleyen, aynı zamanda kurum yönetiminin onaylayıp destekleyeceği bir yöntem olmalıdır.

Risk yönetim sürecinde tek bir doğru olmamakla birlikte, günümüzde uygulanan birçok risk yönetim metodolojisi bulunmaktadır. Her metodolojinin doğruluğu, karmaşıklığı, kaynak tahsisinin sağlanması gibi hususlarda üstünlük ve zayıflıkları bulunmaktadır. Kuruluşlar ulusal veya uluslararası mecrada kabul görmüş standartları benimseyerek bir risk yönetimi yaklaşımı benimseyebilir ya da kendi ihtiyaçlarına özel yöntemlerini geliştirebilirler.

Siber Dünyada Güvenliğin Tarihçesi ve Saldırı Yöntemleri

İnternet ve yeni ağ teknolojilerinin doğuşuyla dünya birbirine daha bağlı hale gelmiş, bu ağ altyapıları üzerinde büyük miktarda kişisel, ticari, askeri ve devlet bilgisi bulunur hale gelmiştir.

Bu gelişimi izlemek adına internetin ve dolayısıyla siber güvenlik unsurlarının gelişimine kısaca değinmek faydalı olacaktır (Daya, 2013):

1930'larda Enigma'nın şifresi kırılmış ve 1960'larda ilk "hacker" terimi ortaya atılmıştır. ARPANET'in 1969 yılında Savunma Bakanlığı tarafından ağ araştırmaları için görevlendirilmesiyle internetin doğuşu gerçekleşmiştir. INWG (InterNetworking Working Group) büyüyen ARPANET ağını yönetmek için standartları belirleyen ilk kuruluştur. İlk Başkanı Vinton CERF "İnternetin Babası" olarak tanınmaktadır. 1970'lerde Telnet protokolünün gelişmesi ve 1980'lerde internet bilgisayarlarının ortak dili olan TCP/IP'nin geliştirilmesi ile bugün bildiğimiz internet doğmuştur. 1990'larda internet halka açılmaya başlanmış ve world wide web (www) doğmuştur.

Günümüzde ise internet ortamında artık insanlar birden fazla ekranı aynı anda görüntülemekte ve sosyal medya platformlarında ışık hızında değişimler gerçekleştirmektedir. Bunun en çarpıcı yansımasını Nisan 2021'de yayınlanan bir dakikada internette yaşanan gelişmelerden anlamak mümkün olacaktır (Lewis, 2020):

Böylesine aktif kullanılarak sürekli veri akışının sağlandığı bir internet ortamında siber saldırılar da kaçınılmaz bir hale gelmiştir. Bilgi güvenliğinin temel prensiplerini ihlal edebilecek bu yöntemler; gizli dinleme (saldırganın hedef ve kaynak arasındaki bilgiyi okuması), hackleme (izinsiz erişim), oltalama (sahte e-posta ya da bölge adları kullanma), DoS (hizmet aksattırma), IP sahteciliği (IP kandırma ile yeni ağ paketi ekleme), virüs, solucan ve Truva atları gibi kullanıcının izni dışında sistem yapılandırması üzerinde değişiklik yapan saldırılar olarak sıralanabilir (Canbek ve Sağıroğlu, 2007). Bilgi güvenliği unsurlarına yönelik saldırı yöntemlerini genel itibari ile Tablo 1'de görmek mümkündür.

Tablo 1. Mevcut İnternet Protokolü Üzerinden Gerçekleşen Saldırılar

Bilgisayar Güvenliği Özellikleri	Saldırı Yöntemleri	İnternet Güvenliği Teknolojisi
Gizlilik	Gizli Dinleme, Hackleme, Oltalama, DoS, IP Sahteciliği	IDS, Güvenlik Duvarı, Kriptografik Sistemler, IPSec, SSL
Bütünlük	Virüsler, Solucanlar, Truva Atları, Gizli Dinleme, DoS, IP Sahteciliği	IDS, Güvenlik Duvarı, Anti-Malware Yazılım, IPSec, SSL
Erişilebilirlik	DoS, E-posta Bombardımanı, Spam Gönderme, Sistem Önyükleme Kaydı Bulaştırıcıları	IDS, Güvenlik Duvarı, Anti-Malware Yazılım
Mahremiyet	E-posta Bombardımanı, Hackleme, Spam Gönderme, DoS ve Çerezler	IDS, Güvenlik Duvarı, Anti-Malware Yazılım, IPSec, SSL

Bu kapsamda bu çalışmada, kuruluşlarda bilgi güvenliği yönetim sisteminin önemi 2022 yılında yaşanan olaylar nezdinde değerlendirilmeye çalışılacaktır. Çalışmada sorulması gereken sorular aşağıdaki gibi sıralanabilir:

- Risk temelli bir güvenlik yaklaşımı neden önemli hale gelmiştir?
- Siber dünyada geçtiğimiz yılda yaşanan en önemli olaylar nelerdir?
- Bilgi Güvenliğinin sağlanabilmesi için yapılması gereken çalışmalar nelerdir?

Yöntem

Araştırmada nitel bir veri analiz yöntemi olan doküman analizi tercih edilmiştir. Doküman analizi, yazılı belgelerin içeriğini titizlikle ve sistematik olarak analiz etmek için kullanılan bir nitel araştırma yöntemidir (Wach & Ward, 2013). Disiplinler arası bir bakış ile araştırma konusunu kendi bağlamında ele alıp yorumlayabilmek için bu yöntemin tercih edildiği bilinmektedir (Altunışık, Coşkun, Bayraktaroğlu ve Yıldırım, 2010).

Araştırma konusu ile ilgili incelenen olgu ve olaylar hakkında görüşme ve gözlem yapmaya gerek kalmadan yazılı belgelerin incelenmesi ile bilgi toplanması sağlanmıştır. Bu sayede kaynak ve zamandan tasarruf sağlanmaktadır. İncelenen dokümanlar genel olarak yayımlanmış makaleler, bildiri ve tezler, web sayfa içerikleri ve sektör raporlarından oluşmaktadır. Siber güvenlik konusunda inceleme yaparken siber güvenlik uzmanları, araştırma

kuruluşları ve güvenlik firmaları tarafından yayımlanan raporların incelenmesinde fayda olacağı değerlendirilerek; 2022 yılına ilişkin bir değerlendirmenin yer aldığı, internet ortamında erişime açık olan raporlar tercih edilmiştir. Elde edilen raporlar içerisinde siber güvenlik firmalarından kendi sensörleri ile bilgi toplayarak analiz raporu çıkaran kuruluşlara öncelik verilmiştir. Uluslararası kuruluşlar ile Türkiye'de siber güvenlik konusunda ekosistemin yürütücüsü konumda olan ve alanda faaliyet gösteren sektörel kuruluşlar ve birliklerin raporlarına da bu kapsamda yer verilmiştir. Bu kapsamda detaylı bir literatür incelemesi yapılarak konu analiz edilmiştir.

Bulgular

Bilgi Güvenliğinde 2022 Yılında Yaşanan Gelişmeler ve Olaylar

Teknolojik gelişmelerin etkisiyle her geçen gün değişen ve gelişen tehditler yalnızca bilgi ve bilişim güvenliğini değil; kişisel güvenlik, ekonomi güvenliği, doğal kaynakların güvenliği gibi birçok alanda da kendisini göstermektedir. Bu tehditler gelişen kötü amaçlı yazılımlar ile saldırganlar için çok fazla teknik bilgi gerektirmeden gerçekleştirilebilmekte ancak genellikle gözle görülür bir şekilde ilerlemediklerinden tespit edilmeleri oldukça zor bir hale gelmektedir.

Güvenlik tehditlerinin en çok görüldüğü siber uzayda sıklıkla ve etkisi yıkıcı şekilde ortaya çıkan olayları genellikle siber güvenlik olayları olarak ele almak mümkündür çünkü siber güvenlik, tüm güvenlik tehditlerinin merkezinde yer almaktadır (Sertçelik, 2015).

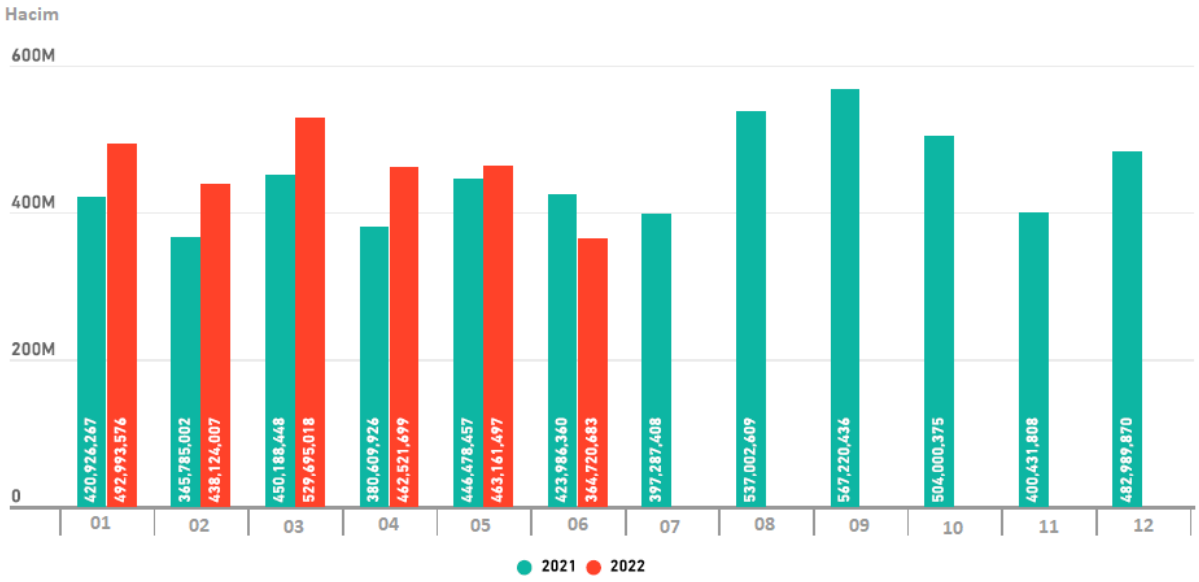
2022 yılında başlayan Rusya – Ukrayna savaşı artık ülkelerin savaş tehdidi olarak askeri çatışma yöntemlerinin yanında siber saldırıları da eşgüdümlü olarak kullanmakta olduğunu gözler önüne sermiştir. Savaşın siber boyutunda 50'den fazla CVE (Common Vulnerabilities and Exposures-*Ortak Zafiyetler ve Açıklıklar*) kullanıldığı ve 70'e yakın hükümet web sitesinin saldırıya uğradığı görülmüştür (Tübitak Bilgem, 2022). Siber savaşta ülke varlıklarına ayrım gözetmeksizin saldırı düzenlendiği görülmektedir (Kaspersky, 2022). Jeopolitik güçlerin yeniden yapılandırmayı hızlandırmasıyla dünyanın siber cephe hatlarında, sunulan gerçek tehlike tehdit aktörleri tarafından ön plana çıkarılmaktadır ve 2022 yılı pek çok kişi için güvenli ülke ve güvenli sektör olmadığı konusunda bir uyanış çağrısı haline gelmektedir (SonicWall, 2022). Her geçen yıl siber saldırı yöntemleri değişim göstermekle birlikte 2022 yılında 4.9 milyon şifrelenmiş tehditler (+%132) ile en çok artış gösteren saldırı biçimi olurken onu 57 milyon IoT zararlı yazılımı (+%77) takip etmektedir. 236.1 milyon ransomware saldırısı %23'lük bir oran ile azalış göstermiştir (SonicWall, 2022).

Kaspersky tarafından açıklanan 2022 yılı istatistiklerine göre;

- Siber saldırganlar kullanıcılara günlük 400.000 yeni kötü amaçlı dosyayla saldırdı (2021'e göre %5 daha fazla), 2022 yılı içerisinde toplam tespit edilen kötü amaçlı dosya sayısı 122 milyon olmuştur.
- Günlük olarak karşılaşılan fidye yazılımı (ransomware) payının 2021'e kıyasla %181 artarak günde 9.500 şifreleme dosyasına ulaştığı keşfedildi.
- Kötü amaçlı yazılımların yeni versiyonlarının cihazlara yüklenmesini sağlayan virüs sayısında %142'lik bir büyüme görüldü.
- Yayılan tüm kötü amaçlı dosyalardan %85'i Windows'u hedef aldı.
- Microsoft Office formatlarında dağıtılan kötü amaçlı dosyaların payının günlük olarak iki katına çıktığı (büyümenin %236'sı) keşfedildi.

2022 yılında yaşanan gelişmeler ışığında, artık daha fazla zararlı yazılım saldırısı ile karşılaşıyor olmanın iki sebebi olacağı değerlendirilebilir. Bunlardan ilki pandemi sonrası artık daha fazla kişinin iş ortamına dönmüş olması ve kurumsal ağlara gerçekleşecek saldırı miktarlarındaki artış, diğeri ise piyasada artık gerçekten daha fazla zararlı yazılımın geliştirilmiş olmasıdır.

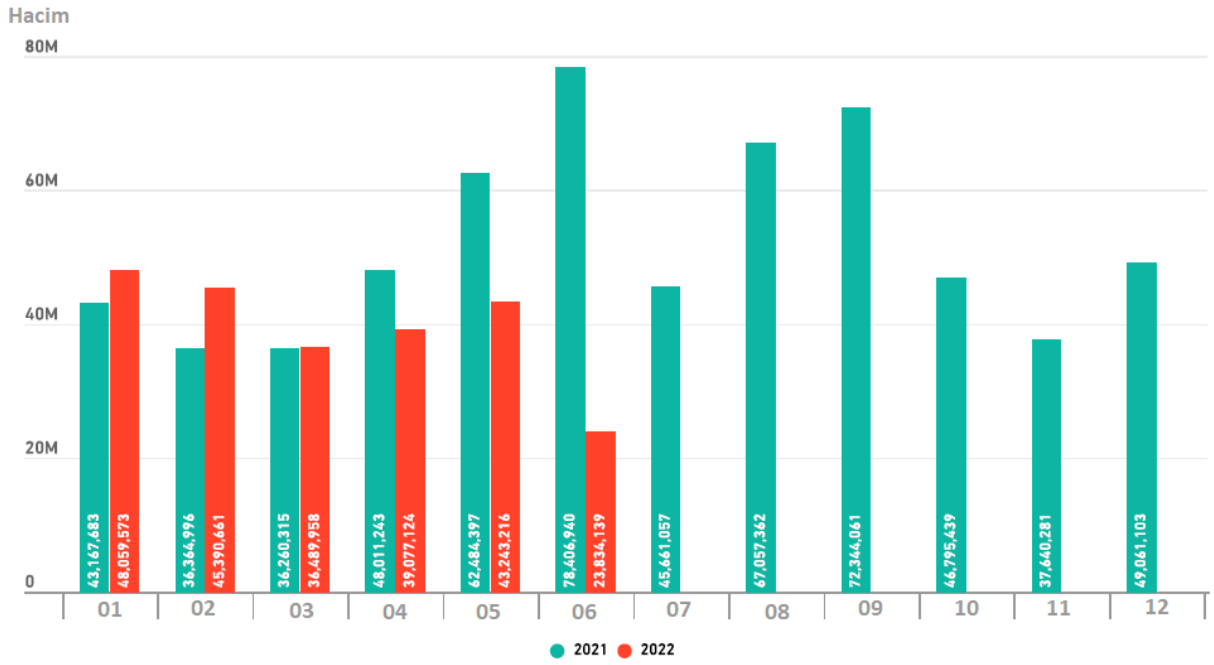
Şekil 3'te 2022'nin ilk yarısında dünya çapında Sonicwall tarafından tespit edilen kötü amaçlı yazılım miktarları hacimsel olarak gösterilmektedir. Haziran ayında yaşanan azalış eğilimi, piyasada daha fazla zararlı yazılım gerçekleşmesi yönündeki yorumu kuvvetlendirmektedir (SonicWall, 2022). 40'tan fazla ülkeden 190'dan fazla sensör ile veri toplayan Brandefence Siber İstihbarat aracının yayınladığı çalışmalar da bu görüşü destekler niteliktedir. Gelecek tehditleri önceden tahmin ederek olay yaşanmadan aksiyon alınmasını sağlayan siber istihbarat çalışmalarında 2022 yılında tespit edilen 142 güvenlik ihbarı, 450 adet güvenlik haberinin olduğu görülmektedir. 2021'de bu rakamlar 160 ihbar ve 791 haber şeklindedir (Brandefence, 2022). Bu durum siber güvenlik saldırı modellerinden ziyade zararlı yazılım çeşitlerinin geliştiği çıkarımı yapılmasını sağlamaktadır.



Şekil 2. Küresel kötü amaçlı yazılım (malware) hacmi

2022 yılı ilk yarısında fidye yazılım miktarında düşüş görülse de bu miktar 2017, 2018 ve 2019'un tüm yıl toplamlarını gölgede bırakarak pandemi öncesi seviyelerin çok üzerinde bir seviyeye ulaşmıştır (SonicWall, 2022).

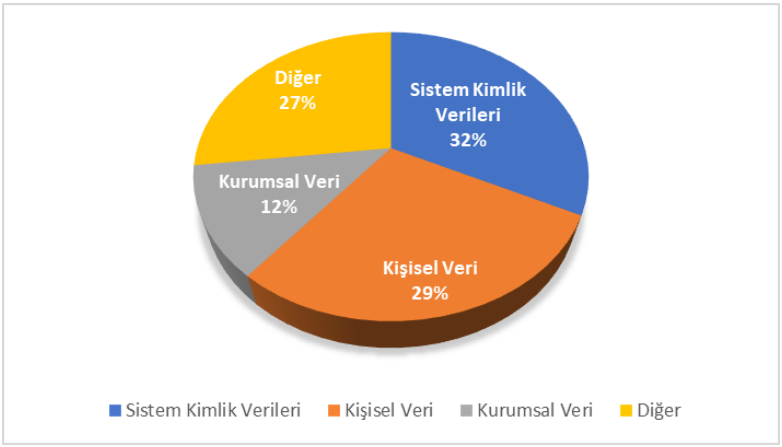
Virustotal tarafından yayınlanan rapora göre fidye yazılımı saldırıları 2022 yılında 2021 yılına göre %19 artış göstermiştir. Bu saldırıların %93'ü Windows işletim sistemine sahip cihazlara yapılmış olup çoğunlukla hatalı sistem konfigürasyonu, hedefli oltalama, zafiyet yönetiminin yapılamaması ve Stealer Malware (Kimlik Hırsızı Zararlı Yazılımı) gibi sebeplerden dolayı gerçekleştiği bilinmektedir (Siber Güvenlik Kümelenmesi, 2022).



Şekil 3. Küresel fidye yazılımı (ransomware) saldırı hacmi

2022 yılında kötü amaçlı yazılımlarda en çok %21.4'lük oranla eğitim sektörünün, ardından %19.3 ile kamu sektörünün hedef alındığı raporlanmaktadır (SonicWall, 2022).

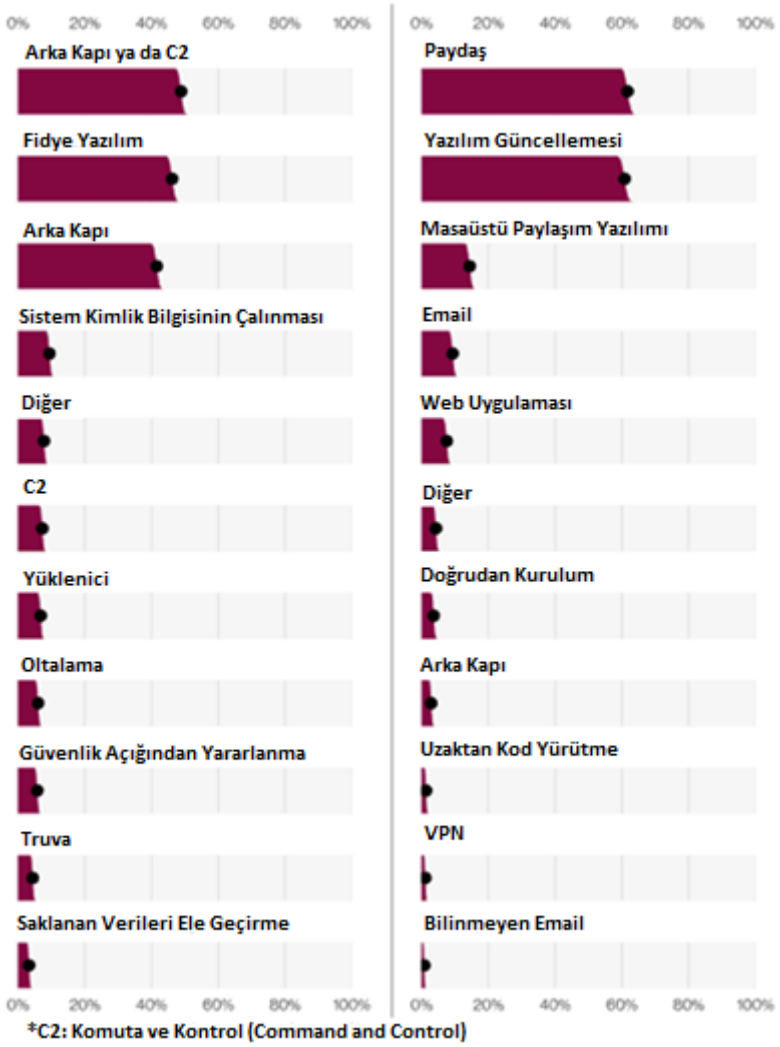
Gelişmiş kalıcı tehdit (APT) grupları veya kötü amaçlı yazılım dağıtmak gibi daha karmaşık bilgisayar korsanlığı gerçekleştiren aktörler tarafından sistemlere izinsiz giriş saldırılarına ilişkin veriler incelendiğinde, 2022 yılı içerisinde 7.013 olay ve 1.999 doğrulanmış veri ifşasının gerçekleştiği anlaşılmaktadır. Saldırıların %98'inin dış, %2'sinin iç tehdit aktörleri tarafından gerçekleştiği görülmektedir. Veri güvenlik ihlallerinin türlerine göre dağılımı ise Şekil 5'te verilmektedir (Verizon, 2022).



Şekil 4. Veri güvenlik ihlallerinin türlerine göre dağılımı (2022)

Siber güvenlik olay çeşitleri ile vektörlerine ilişkin yapılan analizler 2022 yılı içerisinde en çok arka kapılar (backdoor) ve fidye yazılım saldırılarının uygulandığını; vektörler konusunda da paydaşlar (iş ortakları) üzerinden

gelen ya da yazılım güncellemelerinin eksikliğinden faydalanılan saldırıların yoğunlukta olduğunu göstermektedir (Verizon, 2022).



Şekil 5. Siber güvenlik olay çeşitleri ile vektörleri, 2022

Bal küpü (honeypot), bir tuzak bilgisayar sistemi olup, saldırganlara hedef olarak sunularak saldırı tipleri ile ilgili araştırma yapılmasını sağlamaktadır (Nawrocki, Wählisch, Schmidt, Keil, & Schönfelder, 2016). STM Teknolojik Düşünce Merkezi'nin bal küpü sensörlerine 2022 yılı Temmuz, Ağustos ve Eylül aylarında toplamda 6.137.330 saldırı geldiği; en çok saldırı gelen ülke Hindistan (1.046.654 saldırı) olurken Türkiye'nin (120.273 saldırı) ülkeler sıralamasında 10. olduğu rapor edilmiştir. Aynı çalışmada, en çok saldırının sırasıyla SMB, RDP, SMTP ve SSH servisinin kullandığı portlara geldiği ve SSH ve RDP bal küpleri üzerinde en çok denenen kullanıcı adının "root", en çok denenen parolanın "admin" olduğu raporlanmıştır.

Tablo 2. 2022 Yılı SSH ve RDP Bal Küpleri Üzerinde En Çok Denenen Parolalar ve Deneme Sayıları

Denenen Parola	Denenme Sayısı
admin	7.846
123456	3.566
(Boş)	2.475
nproc	2.437
password	1.470
12345	1.048
123	964
1234	950
0	720
root	647

Tablo 3. 2022 Yılı SSH ve RDP Bal Küpleri Üzerinde En Çok Denenen Kullanıcı Adları ve Deneme Sayıları

Denenen Kullanıcı Adı	Denenme Sayısı
root	24.152
admin	9.607
sh	6.148
nproc	2.437
support	2.259
user	2.064
(Boş)	1.918
Test	1.804
guest	1.487
default	1.307

Analiz sonuçlarına bakıldığında birçok yönetim arayüzünün standart olarak kullandığı parolaların kurulum ve testler tamamlandıktan sonra güçlü parolalar ile değiştirilmesi, sıklıkla kullanılan servis ve yönetim paneli kullanıcı adlarının ise en kısa zamanda tahmini zor isimlerle değiştirilmesi gerektiği anlaşılmaktadır.

2022 yılı içerisinde gerçekleşen veri ihlallerinin %82'sinde kilit faktörün insan olduğu tespit edilmiştir (Verizon, 2022). Kimlik avı, her şekil ve büyüklükteki kuruluşun karşılaştığı hiç bitmeyen bir zorluktur ve hiçbir kuruluş veya çalışan saldırılara karşı yeterli farkındalık seviyesinde değildir. Sosyal mühendislik saldırıları ile gerçekleştirilen kötü amaçlı yazılım ve çalınan kimlik bilgileri, bir sosyal saldırı aktörünü kapıdan içeri sokulmasından sonra büyük bir ikinci adım sağlar ve bu da güçlü bir güvenlik farkındalığı programına sahip olmanın önemini vurgular.

Özellikle kamu çalışanlarının güvenlik farkındalığının daha yüksek seviyede olması gerektiğini Virustotal'in 2022 analiz çalışmasında yaptığı çıkarımlardan anlamak mümkündür. Bahse konu çalışmaya göre saldırganlar devlet altyapısını kötüye kullanma eğilimindedirler. Bunun sebebi kamu kurumlarının alan adlarının (.gov) koşulsuz güvenilir bulunmasıdır, dolayısıyla kötü amaçlı yazılım dağıtımı için kullanma eğilimindedirler. 50'den fazla

bölgede kötü amaçlı yazılım dağıtan 1700'den fazla URL ve kamu kurumlarına ait 400 alan adı bulunduğu da yine aynı çalışmada aktarılmaktadır (Virustotal, 2022).

Bilgi güvenliği risk yönetimi süreçlerinde BT yöneticilerinin faydalanması amacıyla, veri ihlallerinin artan maliyetlerine değinerek riskleri azaltmaya yardımcı faktörlere yönelik öneriler sunan "Bir Veri İhlalinin Maliyeti 2022" raporu IBM tarafından yayınlanmıştır. Çalışmada Mart 2021 ve Mart 2022 arasında veri ihlalinden etkilenen 550 kuruluşun 17 farklı ülkeden, 17 farklı sektörden olduğu, kuruluşların %83'ünün birden fazla ihlale maruz kaldığı, %60'ının veri ihlallerinin maliyetini müşterilere fiyat artışı ile yansıttığı, %19'unda ihlalin iş ortakları üzerinden geldiği ve bir veri ihlalinin ortalama maliyetinin 4,35 milyon dolar (kritik altyapılar için 4.82 milyon dolar) olduğu raporlanmıştır (IBM Security, 2022).

ISO 27001 standardı ve BGYS kuruluşların müşteri ve çalışan bilgilerini koruma, bilgi güvenliği risklerini etkili bir şekilde yönetme, yasal düzenlemelere uyum sağlama, güven sağlama ve itibarı koruma, bilgi güvenliği hedefleri geliştirme ve uygulama gibi konularda kılavuzluk eden ve bilgi güvenliği konusunda en yaygın kullanılan standarttır (Talib, El Barachi, Khelifi, & Ormandjieva, 2012). Bu kapsamda 2021 yılı için açıklanan ISO 27001 standardına sahip ülke ve sektör bilgileri incelendiğinde; tüm Dünya'da toplam 58.687 adet ISO IEC 27001:2013 sertifikasının, toplamda 99.755 yer (site) için verildiği görülmektedir. Türkiye'de toplam 706 sertifika 1169 yer için verilmiş durumdadır. Sertifika, müşteri standarda uygunluğunu kanıtladıktan sonra bir belgelendirme kuruluşu tarafından verilen belge ve "yer" ise bir kuruluşun iş yürüttüğü veya bir hizmet sağladığı kalıcı bir konum olarak ifade edilmektedir (ISO Survey, 2021).

Sektörlere göre ISO IEC 27001:2013 sertifika dağılımlarına bakıldığında en çok bilgi teknolojisi, ardından taşıma depolama ve iletişim sektörünün geldiği görülmektedir.

Tablo 4. Sektörlere Göre ISO 27001 sertifika sayıları (2021)

Sektör	Sayı
Diğer	43.488
Bilgi Teknolojisi	10.644
Taşıma, depolama ve iletişim	6.909
Finansal aracılık, emlak, kiralama	645
Mühendislik hizmetleri	630
Havacılık	21

2022, siber güvenlik mesleği için oldukça biçimlendirici bir yıl olmuştur. Jeopolitik ve makroekonomik çalkantılarla şekillenen ve tanımlanan modern siber güvenlik ortamında iş gücünde kararlılık kendini göstermektedir. Büyüyen küresel siber güvenlik tehditleri ile iş gücünde kritik görevleri üstlenecek profesyonellerdeki boşluk da artmaktadır. Siber güvenlik iş gücü araştırmaları, alandaki iş gücünün tahminen 4.7 milyon kişiden oluştuğunu (2021 yılına göre %11,1'lik artış ile) ancak kuruluşları günümüz tehditlerinden korumak ve savunmak için ilave 3.4 milyon kişiye ihtiyaç olduğunu göstermektedir (ISC^2, 2022).

Son olarak 2022 yılında gerçekleşen ve en çok ses getiren siber olaylara değinerek durumun ciddiyeti ve önemini vurgulamakta fayda vardır (Siber Güvenlik Kümelenmesi, 2022; Security Magazine, 2022; Cyber Security Hub, 2022):

- Google, saniyede 46 milyon istek ile bugüne kadar yapılmış en büyük HTTPS DDoS saldırısını engelleyerek rekor kırdı.
- 20 Mart 2022'de Microsoft, Lapsus$ adlı tehdit aktör grubu tarafından hedef alındı. Grup, Telegram'da Microsoft'u hackliediklerini ve bu süreçte Cortana, Bing ve diğer birkaç ürüne ait verileri ele geçirdiğini belirten bir ekran görüntüsü yayınladı. 22 Mart'a kadar Microsoft, saldırı girişimini hızla durdurduğunu ve yalnızca bir hesabın güvenliğinin ihlal edildiğini duyurdu. Microsoft ayrıca hiçbir müşteri verisinin çalınmadığını da belirtti. Lapsus$ grubu daha önce Nvidia, Samsung ve diğer pek çok şirketi hedef almıştır.
- Conti fidye yazılımı çetesi, yüksek profilli bir siber saldırıda Kosta Rika hükümetini ihlal etti. Tehdit grubu hükümetin sistemlerine girdi, çok değerli verileri çaldı ve 20 milyon dolar talep ederek Orta Amerika hükümetini olağanüstü hâl ilan etmeye zorladı.
- 2022 yılının haziran ayında öğrenci kredisi hizmeti veren Nelnet Serviceing'de gerçekleşen veri ihlal vakası 2,5 milyondan fazla kullanıcının gizli bilgilerinin sızdırılmasına neden oldu. Sistemindeki bir güvenlik açığı nedeniyle ad, soyad, ev ve e-posta adresleri, telefon numaraları ile sosyal güvenlik numaralarını içeren öğrenci kredisi hesabı kayıt bilgilerinin kimliği belirsiz bir üçüncü şahıs tarafından erişilebilir olduğu tespit edilmiştir.
- 27 Temmuz 2022 tarihinde BreachForums isimli darkweb forumunda "devil" isimli kullanıcı 5,4 milyon Twitter kullanıcısına ait ayrıntı içeren verileri yayınladı. İlgili sızıntının, Twitter'a 1 Ocak 2022 tarihinde bildirilen zafiyetin sömürülerek elde edildiği düşünülürken, Twitter ilgili zafiyeti 5 Ağustos 2022 tarihinde onayladı.
- 15 Eylül'de, bir yüklenicinin cihazının zararlı yazılım ile enfekte olmasının ardından kullanıcı bilgileri darkweb üzerinde satılmış ve buradan Uber'in dahili sunucularına erişilmiştir. Saldırgan, bu sayede yanal olarak ilerleyerek diğer Uber kullanıcı bilgilerini ele geçirmiş ve şirket genelindeki bir Slack kanalına bir mesaj göndererek bazı dahili siteler üzerinden çalışanlara bir grafik görüntü gösterecek şekilde DNS ayarlarını yeniden yapılandırmıştır.
- Ekim 2022'de kripto para platformu olan Binance tarafından desteklenen BNB zincirinin yer aldığı BSC Token Hub' da bulunan zafiyetin saldırganlar tarafından kullanılmasından dolayı Binance 570 milyon dolar değerinde BNB Token kaybetti.
- Crypto.com'a yönelik 17 Ocak'ta kripto hırsızlığı gerçekleştirilerek 500 kişinin kripto para cüzdanları hedef alındı. Saldırı ile yaklaşık 18 milyon dolar değerinde Bitcoin ve 15 milyon dolar değerinde Ethereum ve diğer kripto para birimleri çalındı.
- Avustralya'nın en büyük sağlık sigortası sağlayıcılarından biri olan Medibank Private Ltd, 1.8 milyon uluslararası müşteri dahil olmak üzere 9,7 milyon eski ve mevcut müşteriye ait verilere yetkisiz bir tarafça erişildiğini doğruladı.
- Birçok platformda parola kasası olarak hizmet sunan ve adından 2022 yılında birçok kez bahsettiren LastPass isimli firma veri ihlaline uğrayarak Aralık 2022 tarihinde müşterilerine ait bütün bilgiler saldırganlar tarafından ele geçirildi.
- Çalıntı kredi kartı bilgilerinin de yer aldığı illegal platform olan "BidenCash" isimli forumda 1,2 milyon adet ve son kullanma tarihlerinin 2023 ve 2026 tarihleri olduğu dikkat çeken kredi kartı ücretsiz olarak yayınlandı.

- Honda araçlarda kilit sistemini ve aracı uzaktan yönetmeye yarayan Rolling Pwn isimli kritik bir zafiyet bulundu.
- 1,5 milyondan fazla araçta kullanılan MiCODUS MV720 GPS cihazlarında aracı uzaktan yönetebilen bir güvenlik zafiyeti bulundu.
- Yandex Taksi hacklenerek Moskova'da bulunan tüm taksilerin aynı noktaya yönlendirilmesi büyük bir trafik sıkışıklığına yol açtı.
- 34 farklı Rus hacker grubunun, zararlı yazılımlar ile 50 milyondan fazla parola çaldığı tespit edildi.
- Dünya çapında yaygın olarak kullanılan Spring isimli Java Web Framework'ünde, sistem üzerinde uzaktan kod çalıştırabilen kritik bir güvenlik zafiyeti bulundu.
- Intel'in 12. nesil işlemcisi Alper Lake'in kaynak kodları sızdırıldı.
- FBI, kiralık DDoS hizmeti sunan platformlara yaptığı operasyon sonucunda 48 alan adını ele geçirdi.

Tartışma

Yapılması Gereken Çalışmalar

Günümüz teknoloji çağında, özellikle işlediği bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılara sahip kuruluşların internete bağlı şekilde sistemlerini yönetmeleri kaçınılmazdır. Güvenlik tehditlerinin yaygınlaşması ile birlikte kurumlar artık internete bağlı ancak aynı zamanda internetten korunan "intranetler" oluşturmak için güvenlik duvarları, şifreleme ve kimlik doğrulama mekanizmalarının kombinasyonlarını kullanmaktadır. Sanallaştırma teknolojileri bu kapsamda kurumların güvenlik endişelerini giderecek bir yaklaşım olarak ele alınmakta, artık farklı lokasyonlarda bulunan intranet ağları için ayrı hatlar kiralamak yerine, daha yeni bir yaklaşım olan VPN (Virtual Private Network) bağlantılarından yararlanılmaktadır. Kurumsal güvenlik yaklaşımında benimsenen önemli güvenlik önlemlerinden biri olan bu bağlantılar iletişimin şifreli tutulması ve kullanıcı IP bilgisinin gizli tutulması gibi imkanlar sayesinde ISO 27001, ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi), COBIT (Bilgi için Kontrol Hedefleri ve İlgili Teknolojiler-*Control Objectives for Information and related Technology*) gibi uluslararası önemli standartların da önemli kontrol noktalarından birini oluşturmaktadır (Korucu, 2021). Bu bağlantı tipinde veri sızıntısı önleme ve şüpheli aktiviteleri tespit edebilme amacıyla katmanlı savunma sistemleri kurulmalı ve çok faktörlü kimlik doğrulama mekanizması aktif edilmelidir (Korucu, 2021).

Geniş çaplı veri paylaşımları için ağları internete açık tutarken dikkat edilmesi gereken hususlardan bazıları; izinsiz girişleri tespit eden ve raporlayan güvenlik duvarları, güvenlik duvarında gelişmiş virüs kontrolü, tüm bağlantılar ve veri transferleri için şifreleme, senkronize şifreler veya güvenlik sertifikaları ile kimlik doğrulama, çalışanların e- posta ve eklerini açmasında zorunlu kurallar tanımlama olarak tanımlanabilir (Daya, 2013).

Bunların dışında kuruluşlar öncelikli olarak sistemlerini sürekli izlemeyi sağlayacak bir Güvenlik Operasyonları Merkezini (SOC) kendi bünyelerinde kurmalı, güncellemelerini Sandbox'lar üzerinde izledikten sonra entegre etmeli, düzenli sızma testleri gerçekleştirerek zafiyet tespiti gerçekleştirmeli ve gerekli önlemlerini hızla almalıdır (İçişleri Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü, 2021). SOC merkezleri, kritik varlık ve hizmetlerin korunması noktasında olası senaryolar üzerinden olay tespiti ve yanıt verme çevikliğini artırma yönüyle tercih

edilen bir teknoloji çözümüdür (Korucu, 2021). Daha profesyonel olarak ise kuruluşlar, tüm cihazlarda yazılımları güncel tutmalı, davranış tabanlı algılama ve anormallik kontrolü yetenekleriyle donatılmış bir uç nokta güvenlik çözümü devreye almalı, EDR (Endpoint Detection and Response) ve MDR (Managed Detection and Response) ile güçlendirilmiş etkili uç nokta koruması, tehdit algılama ve yanıt ürünlerinden faydalanmalı ve tehdit istihbarat verilerini alabilecekleri hizmetlerden yararlanmalıdır (Kaspersky, 2022). Saldırganların artık geleneksel saldırı yöntemleri yerine kurum, şirket ve devletler özelinde, hedef odaklı saldırılar yapıyor olması davranış analizi yaparak önceden tanımlı kurallar doğrultusunda saldırganların yaptığı ya da yapabileceği atakları tespit edebilmeyi gerekli kılmaktadır (Bozkus, 2021).

Güvenlik teknolojisi çoğunlukla yazılım tabanlıdır, ayrıca birçok yaygın donanım cihazı kullanılmaktadır. Birçok küçük ve karmaşık cihaz internete bağlanabilmektedir. Güvenlik geliştirmeleri genellikle, mevcut güvenlik teknolojisi setinde yapılan küçük ayarlamalardan oluşmaktadır. Mevcut güvenlik algoritmalarının çoğu yoğun hesaplama ve önemli miktarda işlem gücü gerektirir. Bu nedenle, halen güvenlik algoritmalarının tasarlanmasına ihtiyaç vardır. Bu alandaki araştırmalar halen devam etmektedir (Daya, 2013).

Yapılması gereken iş adımlarının temelinde mevcut güvenlik önlemlerinin sıkılaştırılması çalışmalarının yattığı anlaşılmaktadır. Buradan bahisle, bahse konu sıkılaştırma tedbirlerinin tespiti ve güvenlik algoritmalarının geliştirilmesi için risk temelli bir güvenlik anlayışının benimsenmesi gerekmektedir. Risk temelli yaklaşım stratejik bilgi güvenliği hedeflerinin tespitine de yardımcı olacak, bütünsel bir yaklaşımın benimsenmesini garanti edecektir. Bu konuda kurum ortamına derinlemesine bakılarak mevcut risklerin tespiti ve hangi stratejiler ile azaltıcı faaliyetlerin yürütüleceğinin anlaşılır hale getirilmesi gerektiği görüşü mevcuttur (Güler ve Arkin, 2019).

Bilgi güvenliğine yönelik tehditlerin seviyesini azaltmak, riskleri bertaraf edebilmek için kuruluşta bütün çalışanların katılımını sağlayıcı politikalar geliştirilmelidir. Bu politikalardan değersiz gibi görülen ancak önleyici tedbir olarak uygulanması gereken hususlara da dikkat etmek gerekmektedir. Sürekli aktif olarak faaliyet gösteren sistemlerde artan tehditlere karşın etkin bir koruma sağlamanın yolu kurumun birleştirilmiş bir çaba sarf edebilmesidir (Sunde, 2017). Siber güvenlik bir bütün olarak ele alınması gereken bir husustur ve tüm paydaşların aktif katılımını gerektirmektedir (Çakır ve Uzun, 2021).

Kuruluşlar için önemli bir öncelik, tuttukları veri ve bilgilerin ne kadar güvenli olduğudur. Fidye yazılımı gibi yüksek profilli veri ihlalleri ve siber güvenlik saldırıları nedeniyle kuruluşların veri ve bilgilerini en yüksek standartta işlemesi, güvenliğini sağlaması ve depolaması gerekmektedir. ISO 27001, kuruluşun elinde bulundurduğu bilgi ve verilerin güvenliği ile ilgili riskleri yönetmeye yönelik uluslararası bir standarttır. Standart, müşteri ve çalışan verilerinin güvenli bir şekilde saklanmasını ve GDPR gibi yasal gerekliliklere uygunluğu sağlamaktadır. Olası bilgi güvenliği kaynaklı zararları minimum seviyeye indirerek mali sonuçlar ile kurumsal imajı olumlu yönde etkileyecektir (Yılmaz, 2014). Bilgi güvenliği yönetim sisteminin (BGYS) kurulması, uygulanması, işletilmesi, izlenmesi, sürdürülmesi ve iyileştirilmesi için süreç bazlı bir yaklaşımın benimsenmesini sağlamaktadır (Certification Europe, 2022). ISO 27001'e dayalı bir BGYS'nin güvenlik ihlallerinin maliyetini ve bilgi teknolojileri arızalarını azaltacağını öngörüldüğü aktarılabilir (Hsu ve diğerleri, 2016).

Anlaşıldığı üzere, risk yönetimi ve dolayısıyla BGYS süreç yönetiminin etkinliği kuruluşlara dikkate değer bir katma değer sağlayacaktır. Etkili bir bilgi güvenliği yönetimi için, bilgi güvenliği stratejilerinin organizasyonel stratejilerle uyumlu olması sağlanmalıdır. Bu kapsamda stratejiler belirlenirken iş stratejileri, kurumsal kültür, insan kaynakları yapısı, IT güvenlik kaynakları, tedarikçiler, müşteriler, düzenleyici kurumlar vb. dikkate alınarak

yönetsel ve teknik kontroller değerlendirilmelidir. Yönetsel olarak; iç ve dış faktörler analiz edilmeli, paydaşlar belirlenerek ekipler oluşturulmalı, rol ve sorumluluklar tayin edilmeli, iletişim yöntemleri belirlenerek kılavuzlar oluşturulmalıdır. Teknik kontrol olarak; izleme sistemlerinin dizaynı, kimlik doğrulama kontrolü, erişim kontrolü, olay tespit mekanizmalarının kurulumu gibi çalışmalar gerçekleştirilmelidir (Ma ve diğerleri, 2009).

Bireysel Olarak Alınacak Önlemler

Bireysel olarak alınması gerekli önlemler aşağıdaki gibi sıralanabilir (Kaspersky, 2022):

- Güvenilmeyen kaynaklardan uygulama indirip kurmamalı
- Bilinmeyen kaynaklardan gelen bağlantılara veya şüpheli çevrimiçi reklamlara tıklanmamalı
- Güçlü ve benzersiz parolalar oluşturmanın yanı sıra iki faktörlü kimlik doğrulama mekanizmaları etkinleştirmeli
- Kritik güvenlik sorunlarını çözen güncellemeler vakit kaybetmeden yüklenmeli
- Güvenlik sistemlerini devre dışı bırakmayı isteyen mesajlar yok sayılmalı
- Lisanslı güvenlik çözümleri kullanılmalı
- Güvenilir olmayan ağ bağlantılarına erişim saplanmamalı
- Güvenilir olmayan bağlantılar üzerinde alışveriş ve bankacılık gibi işlemler gerçekleştirilmemelidir.

Sonuç

Dünyada ve ülkemizde yaşanan dijital dönüşüm dalgası iş yapış şekillerinde sağladığı kolaylıklarla beraber birtakım zorlukları da beraberinde getirmiştir. Yeni düzende kamu ve özel sektör kuruluşları çok çeşitli bilgi tehditleriyle karşı karşıya kalmaktadır. Kurumların bilgi teknolojileri altyapılarının siber saldırılara karşı korunması gün geçtikçe daha önemli ve zorlu bir görev haline gelmektedir. Kuruluşlar, hassas verilerini dış tehditlerden korumak için çok sayıda güvenlik önlemine yatırım yaparken, ayrıcalıklı erişim ve kuruluş varlıkları hakkında derinlemesine bilgi sahibi olan kötü niyetli içeriden kişilere karşı savunmasız kalırlar.

Bilgi güvenliği sadece teknolojik önlemlerin yerine getirilmesi ile tam olarak sağlanmış sayılmamaktadır. Kuruluşlar teknolojik ve idari önlemleri bir bütün olarak düşünmeli, bunların yanında insan faktörünün de önemli bir unsur olduğu unutulmamalıdır. Bilgi güvenliği tüm bu etkenleri içinde barındıran karmaşık bir süreçtir.

İşlenen bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına, güven ve itibar kaybına yol açabilecek kritiklikte sistem yöneten kuruluşların birinci öncelik olarak etkin bir bilgi güvenliği risk yönetim süreci işletmesi gerekmektedir.

Yayın Etiği Bildirimi / Research Ethics

Yazar araştırmanın etik dışı bir sorunu olmadığını, araştırma ve yayın etiği konusunu gözlemlediğini beyan etmektedir. / The author declares that the research has no unethical problem and observes the research and publication ethics.

Araştırmacıların Katkı Oranı / Contribution Rate of Researchers

Çalışmanın her aşamasına yazar katkı sunmuştur. / The author provides the contribution rates to each stage of the study.

Çıkar Çatışması / Conflict of Interest

Çalışmada herhangi bir çıkar çatışması bulunmamaktadır. / The study has no conflict of interest.

Fon Bilgileri / Funding

Bu çalışmada herhangi bir fon kullanılmamıştır. / There is no funding for this study.

Etik Kurul Onayı / The Ethical Commitee Approval

Etik kurul kararı: Bu araştırmada, tüm araştırmacılara açık, uluslararası veri tabanında yer alan veriler kullanıldığından etik kurul kararı gerektirmemektedir. / The Ethical Committee Approval: This research does not require an ethics committee decision, since data in an international database open to all researchers are used.

Kaynakça / References

Altunışık, R., Coşkun, R., Bayraktaroğlu, S. ve Yıldırım, E. (2010). *Sosyal bilimlerde araştırma yöntemleri: SPSS uygulamalı.* Sakarya yayıncılık.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 97-104).

Bodrožić, A. (2018). *Analiza rizika u intermodalnom transportu* (Doctoral dissertation, University of Zagreb. Faculty of Transport and Traffic Sciences. Division of Intelligent Transport Systems and Logistics. Department of Intelligent Transport Systems).

Bozkus, A. Y. (2021). Development of Cyber Threat Intelligence Tool (No. 5674). *EasyChair. International Conference on Cyber Security and Digital Forensics (ICONSEC'21)*, June 4-5, 2021, Yalova, TURKEY

Brandefence (2022). Security News. https://brandefense.io/security-news/ adresinden alındı.

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis, 42*(8), 1643-1669.

Canbek, G. ve Sağıroğlu, Ş. (2007). Bilgisayar sistemlerine yapilan saldirilar ve türleri: Bir inceleme. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi, 23*(1), 1-12.

Certification Europe (2022). https://www.certificationeurope.com/certificate/iso-27001/ adresinden alındı.

Cyber Security Hub (2022). The biggest data breaches and leaks of 2022. https://www.cshub.com/attacks/articles/the-biggest-data-breaches-and-leaks-of-2022 adresinden alındı.

Çakır, H. ve Uzun, S. A. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset ve Uluslararası İlişkiler Dergisi, 7*(2), 353-379.

Daya, B. (2013). Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering, 4.*

Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics, 2*(5), 544-554.

Güler, A. ve Arkin, A. K. (2019). Siber hijyenin sağlanmasında iç denetimin rolü. *Denetişim,* (19), 17-40.

Harris, S. (2002). All-in-one CISSP certification exam guide. McGraw-Hill/Osbourne.

Hsu, C., Wang, T., & Lu, A. (2016). The impact of ISO 27001 certification on firm performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE.

ISC^2 (2022). Siber Güvenlik İşgücü Araştırması. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf?rev=1bb9812a77c74e7c9042c3939678c196 adresinden alındı.

IBM Security (2022). Cost of a data breach report. https://www.ibm.com/reports/data-breach adresinden alındı.

İçişleri Bakanlığı Bilgi Teknolojileri Genel Müdürlüğü (2021). 2021 yılı öne çıkan siber güvenlik olayları. https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/bilgiteknolojileri/Haberler/2022/02/siber_bulten_subat_2022.pdf adresinden elde edildi.

Jonsson, E. (1996). *A quantitative approach to computer security from a dependability perspective.* Chalmers University of Technology.

Kaspersky (2022). Güvenlik Bülteni. https://www.kaspersky.com/about/press-releases/2022_cybercriminals-attack-users-with-400000-new-malicious-files-daily---that-is-5-more-than-in-2021 adresinden alındı.

Korkmaz, İ. ve Dalkılıç, M. E. Öncül parola denetimi yöntemiyle parola seçim sistemi: Türkçe parolalar için bir araştırma. *Akademik Bilişim, 10*, 206.

Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri. *Yönetim Bilişim Sistemleri Dergisi, 7*(1), 44-60.

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). *Information Security Risk Assessment. Encyclopedia, 1*(3), 602-617.

Lewis, L. (2020). Infographic: What happens in an internet minute 2020. All Access. Recuperado de: https://bit. ly/3bz7D9N [Consultado el 25 de junio 2020].

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business, 30*(1).

Nawrocki, M., Wählisch, M., Schmidt, T. C., Keil, C., & Schönfelder, J. (2016). A survey on honeypot software and data analysis. *arXiv preprint arXiv:1608.06249.*

Oscarson, P. (2003). Information security fundamentals: graphical conceptualisations for understanding. In *Security Education and Critical Infrastructures: IFIP TC11/WG11. 8 Third Annual World Conference on Information Security Education (WISE3) June 26–28, 2003, Monterey, California, USA 3* (pp. 95-107). Springer US.

Security Magazine (2022). 2022'nin en büyük 10 veri ihlali. https://www.securitymagazine.com/articles/98716-the-top-10-data-breaches-of-2022 adresinden alındı.

Sertçelik, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. *Medeniyet Araştırmaları Dergisi, 2*(3), 25-42.

Siber Güvenlik Kümelenmesi (2022). 2022 Yılında Gerçekleşen Siber Vakalar, https://siberkume.org.tr/NewsDetail/a2traEMvVHlJYXdmckFlemp3amdIN0t1aGNBSFk0Zklqc2tCem1aT1YrQWlkb0tVWEFaMjloNWZpdXU1ZXhkT2tJNXRCLzYzd1pDalNOMFhuU09Za3YrZ2JPakMrSlBndUpxaHZKemdxRXdiWjlHOTRQZHkxZGFzMEY5RXJwbDA1 adresinden alındı.

Sonicwall (2022). Siber Güvenlik Raporu. https://www.sonicwall.com/2022-cyber-threat-report/ adresinden alındı.

Soysal, H. (2023). *ISO/IEC 27001 kapsamında bilgi güvenliği yönetim farkındalığının değerlendirilmesi: Ankara ili sağlık kurumları bilgi işlem birimi çalışanları örneği* (Master's thesis, Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü).

STM Teknolojik Düşünce Merkezi (2022). Siber tehdit durum raporu Temmuz – Eylül 2022. https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-temmuz-eylul-2022 adresinden alındı.

Sunde S. J., (2017). *Assurance and Cyber Risk Management, The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities*, Ed.: Domenic Antonucci, John Wiley & Sons, Inc.: Hoboken, New Jersey.

Talib, M. A., El Barachi, M., Khelifi, A., & Ormandjieva, O. (2012). Guide to ISO 27001: UAE case study. *Issues in Informing Science and Information Technology, 7,* 331-349.

Tübitak Bilgem, (2022). Rusya-Ukrayna Siber Savaş Tehdit Araştırma Raporu, https://bilgem.tubitak.gov.tr/sites/images/tubitak_bilgem_sge_rusya_ukrayna_siber_savas_tehdit_arastirma_raporu.pdf adresinden alındı.

Verizon (2022). Veri İhlalleri İnceleme Raporu. https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/ adresinden alındı.

Virustotal (2022). https://blog.virustotal.com/2022/11/deception-at-scale-how-attackers-abuse.html adresinden alındı.

Wach, E., & Ward, R. (2013). Learning about qualitative document analysis.

Yılmaz, H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. *KİDDER Kamu İç Denetçileri Derneği, 15*(1), 45-59.