BİLGİSAYAR BİLİMLERİ VE TEKNOLOJİLERİ DERGİSİ
JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGIES
http://dergipark.org.tr/tr/pub/bibted

Derleme Makalesi

Yönetim Bilgi Sistemlerinde (YBS) Siber Güvenliğin Önemi

Hakan Aydın*

**İstanbul Topkapı Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, İstanbul / Türkiye*

Anahtar Kelimeler:
Siber Güvenlik
Yönetim Bilişim Sistemleri
Bilgi Güvenliği

ÖZ

İçinde bulunduğumuz Bilgi Çağında işletmelerin faaliyetlerini gerçekleştirirlerken Yönetim Bilişim Sistemlerini (YBS) yoğun olarak kullanmaları YBS için Siber Güvenliği (SG) bir zorunluluk getirmiştir. Siber tehdit ve saldırılar neticesinde YBS sistemlerinde oluşabilecek siber güvenlik olayları işletmelerde kullanılan YBS sistemlerinin hizmet dışı kalmasına, işletmelerde ekonomik zararın oluşmasına, işletmelere ait kurumsal, kişisel, sağlık, fikri mülkiyet gibi farklı verilerin zarar görmesine neden olabilecektir. Hatta bu SG olayları ulusal güvenliğin ihlaline kadar etki gösterebilecektir. Bu çalışmada, öncelikle SG ile ilgili kavramların genel çerçevesi çizilmiş, siber güvenlik kapsamında YBS güvenliği araştırılmış, bu çerçevede YBS siber güvenliğinin mevcut farkındalığın artırılmasına ilişkin öneriler getirilmesi amaçlanmıştır. Araştırmada elde edilen sonuçlar, bilgi güvenliği kural ve tedbirlerini almayan işletmelerin siber tehdit ve saldırıları riskleri ile karşı karşıya olduklarını, bu nedenle YBS sistemlerinde bilgi güvenliğine ilişkin kural ve tedbirlerinin dikkate alınarak uygulanmasının hayati derecede öneme sahip bir konu olduğunu ortaya koymaktadır. Çalışma neticesinde ayrıca YBS sistemlerinin bilgi güvenliğinin sağlanmasında yerli ve milli bilişim teknolojilerinin kullanımının önemi vurgulanmıştır.

The Importance of Cyber Security in Management Information Systems (MIS)

Keywords:
Cyber security
Management Information Systems
Information Security

ABSTRACT

In the Information Age we are in, the intensive use of Management Information Systems (MIS) while carrying out their activities has made Cyber Security (SG) a necessity for MIS. Cyber security incidents that may occur in MIS systems as a result of cyber threats and attacks may cause the MIS systems used in enterprises to be out of service, economic damage to enterprises, and damage to different data such as corporate, personal, health, intellectual property belonging to enterprises. In fact, these SG incidents can have an effect as much as a violation of national security. In this study, first of all, the general framework of the concepts related to SG was drawn, MIS security was researched within the scope of cyber security, and it was aimed to make suggestions for increasing current awareness of MIS cyber security in this framework. The results obtained in the research reveal that the implementation of the rules and measures regarding information security in MIS systems is a vital issue. As a result of the study, the importance of the use of domestic and national information technologies in ensuring the information security of MIS systems was emphasized.

***Sorumlu Yazar**
*(hakanaydin@topkapi.edu.tr) ORCID ID 0000-0002-0122-85

e-ISSN: 2717-8579

Geliş Tarihi: 30/06/2022; Kabul Tarihi: 05/10/2022

1. GİRİŞ

Yönetim Bilişim Sistemleri (YBS) küçük, orta ve büyük ölçekli kurum, kuruluş, organizasyon ve şirketler için doğru verinin toplanarak anlamlı bilgiler haline getirilmesinde, planlanmasında, ilgili birimler ile güvenli olarak paylaşılmasında ve koordine edilmesinde ve nihai olarak da etkin kararlar alınmasında yönetim, yöneylem, bilişim, bilgisayar, yazılım gibi bilim dallarını içeren disiplinler arası bir alandır. YBS alanı küçük, orta ve büyük ölçekli kurum, kuruluş, organizasyon ve şirketler için doğru verinin toplanarak anlamlı bilgiler haline getirilmesinde, planlanmasında, ilgili birimler ile güvenli olarak paylaşılmasında ve koordine edilmesinde ve nihai olarak da etkin kararlar alınmasında hayatın hemen her alanında kullanılmaktadır.

YBS, bir organizasyonun operasyonlarının omurgasını oluşturan donanım ve yazılımdan oluşan bilgisayar sistemleridir (Tecim, 2020). Organizasyonlar için YBS'yi karar verme sürecinin en önemli bileşenlerinden birisi olup gerekli süre ve deneysel çabaların azaltılarak karar verme sürecinin daha güvenli, doğru ve kolay olmasını sağlar (Wassef Hijazeen ve diğ., 2022). Siber Güvenlik (SG), bilgi veya verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayan bir dizi faaliyettir (2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı). SG alanı, bilişim sistemlerinin siber tehdit, saldırı ve olaylardan korunmasını hedefleyen bir disiplindir.

Günümüzde YBS teknolojilerinin giderek artan oranlarda ve yoğun olarak kullanılması bilgi güvenliğini bir zorunluluk haline getirmiştir. Bilgi güvenliği, en değerli kaynaklarından biri olan veri ve bilginin gizliliği, mahremiyeti, bütünlüğü ve kullanılabilirliği ile ilgilendiğinden, kuruluşların yönetiminde kilit bir rol oynar (Antunes ve diğ., 2021). Siber tehditler içinde bulunduğumuz dijital çağda her işletmenin bir gerçeğidir (Akhtar ve diğ., 2021). İşletmeler için siber olaylardan zarar görebilecek varlıklar arasında kişisel veya kurumsal olarak tanımlanabilir bilgiler, sağlık bilgileri, fikri mülkiyet, çok farklı veriler, hükümet ve özel sektör verileri gibi daha pek çok varlık sayılabilir. İşletmeler bilgi güvenliğine ilişkin tehditlere yönelik olarak gerekli tedbirleri almak ve bu tehditler ile başa çıkma için gayret göstermektedirler. Siber tehdit ve saldırıları karşısında YBS sistemlerinde oluşabilecek bilgi güvenliği zafiyetleri YBS sistemlerinin hizmet dışı kalmasına, ekonomik zararın oluşmasına ve hatta kamu düzeninin bozularak ulusal güvenlik zafiyetlerine kadar etkilere neden olabilecektir. Siber güvenlik konusu özellikle son yıllarda iş dünyasında ticari anlamda bilgi yönetimi için öok önemli bir etmen haline gelmiştir (Chan ve diğ., 2019). Artan sayıda siber güvenlik olayıyla birlikte işletmeler, özellikle de küçük ve orta ölçekli işletmeler (KOBİ'ler) giderek daha fazla ekonomik zayıflama riskiyle karşı karşıyadır (Schwieger ve Ladwig, 2022). Küçük işletmeler özellikle siber suçlular için çekici hedefler haline geliyor, ancak büyük işletmelerin rutin olarak uyguladığı siber güvenlik önlemlerini uygulamakta zorlanıyor ve bu nedenle iş gücünün önemli bir bölümünü istihdam eden küçük işletmeler için etkili ve uygun siber güvenlik çözümlerine acilen ihtiyaç duyulmaktadır (Tam ve diğ., 2021). Küçük ve orta ölçekli işletmeler (KOBİ'ler) birçok ülke ekonomisinin büyük bir bölümünü oluşturmaktadır, ancak literatüre göre KOBİ'ler siber güvenliği yeterince uygulamıyor ve bu da onları siber saldırılara açık hale getiriyor (Chidukwani ve diğ., 2022). Bu çalışmada, öncelikle SG ile ilgili kavramların genel çerçevesi çizilmiş, siber güvenlik kapsamında YBS güvenliği araştırılmış, bu çerçevede YBS siber güvenliğinin mevcut farkındalığın artırılmasına ilişkin öneriler getirilmesi amaçlanmıştır.

Çalışmanın ikinci bölümünde araştırmanın metodolojisi açıklanmıştır. Üçüncü bölümünde YBS ve dördüncü bölümünde ise SG konularına yer verilmiştir. Beşinci bölümde YBS için SG'in önemi araştırılmıştır. Altıncı bölümde YBS'ye yönelik olası siber saldırı türü ve yöntemleri araştırılmıştır. Yedinci bölümde YBS sistemlerinde bilgi güvenliği araçları araştırılmıştır. Çalışmanın yedinci ve son bölümünde araştırmada elde edilen bilgiler doğrultusunda sonuç ve önerilere yer verilmiştir.

2. YÖNTEM

Betimleme Yöntemi, olayların, grupların, kurumların vb. çeşitli alanların ne olduğu ve bu sırada gerçekleşen eylemleri daha iyi anlayabilme, aktarabilme adına aralarındaki ilişkinin açıklandığı bir unsurdur (Kaptan, 1995). Araştırmada betimleme yöntemi kullanılmıştır. Araştırma soruları aşağıdaki şekilde belirlenmiştir:

- YBS bağlamında hangi temel siber güvenlik kavramlarından söz edilebilir?
- İşletmelerde kullanılmakta olan YBS sistemlerine yönelik siber tehdit ve saldırılar nelerdir?
- İşletmeler için YBS'nin siber güvenliğinin sağlanmasının önemi nedir?
- Araştırma neticesinde elde edilen bilgiler kapsamında hangi sonuç ve öneriler getirilebilir?

3. YÖNETİM BİLİŞİM SİSTEMLERİ (YBS)

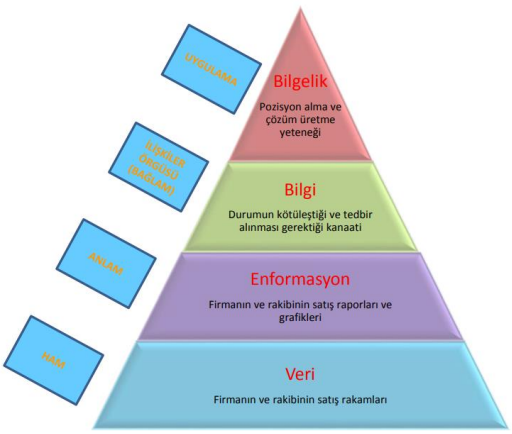
YBS, kurum, kuruluş, organizasyon ve şirketlerin operasyonlarının belkemiği olarak işlev gören, verinin toplanarak anlamlı bilgiler haline getirilmesinde, planlanmasında, ilgili birimler ile güvenli olarak paylaşılmasında ve koordine edilmesinde ve nihai olarak da etkin kararlar alınmasında teknik ve davranışsal yaklaşımları içeren, donanım ve yazılımdan oluşan bilgisayar sistemleridir. YBS ile herhangi bir organizasyonun işleyişi, yönetimi ve karar vermesi için bu bilgi sistemlerinden bilgi desteği alınır. YBS bilgisayar donanımı, yazılımı, yapay zekâ, karar modeli ve veri

tabanı gibi bilişim teknolojilerini içerir. YBS, işletme ve bilgisayarın kesiştiği bir yerdir (Damar ve Coşkun, 2017). YBS için bilgi doğru ve etkin karar vermenin temel öğesidir. Disiplinler arası bir alan olan YBS birçok bilim dalının entegre olarak kullanıldığı bir alandır. Bu bağlamda YBS'ye ilişkin yaklaşımlar Şekil 1'de gösterilmektedir.

Şekil 1. YBS'de Davranışsal ve Teknik Yaklaşımlar. Kaynak: (Tecim, 2020)

YBS'nin temel özellikleri arasında ilişkisel veri tabanlarının kullanılması, yöneticilerin bilgiye kolay ve zamanında erişebilmeleri, esneklik, sistem güvenliği, Günlük operasyonlarla ilgilenmemesi, yapısal kararlara yönelik olması, ihtiyaç duyulan raporların üretilmesi ve organizasyon içi işlemlere yönelik olması sayılabilir (Özen, 2014).

Şekil 2'de yer alan bilgi piramidinde en altta veri vardır. Bunu sırasıyla yukarıya doğru enformasyon izlemektedir. Bir sonraki adım bilgidir. Piramidin en tepesinde ise bilgelik kavramı bulunmaktadır.



Şekil 2. Veri, Enformasyon, Bilgi ve Bilgelik Kavramları Kaynak: (Özen, 2014)

YBS bilgi sistemlerini doğası gereği etkin olarak kullanır. YBS'de kullanım alanı bulan bilişim sistemleri teknoloji tabanlı bilgi sistemleridir. YBS sistemlerini kullanan işletmeler bu sistemlerin sahip oldukları yetenekleri kullanmak suretiyle işlevlerini bilgi çağının gereklerine ve kullanıcıların elektronik bilgi hizmetleri beklentilerine uygun olarak işlevlerini yerine getirmek istemektedirler. Gizliliği, bütünlüğü ve erişilebilirliğiz sağlamayan veri/bilginin bilgi güvenliğinden söz edilemez. Dolayısıyla bu tür verinin işletmeler içinde bir önemi olmayacaktır.

Bilgi güvenliğinde bilginin gizliliğini, bütünlüğünü ve erişebilirliğini sağlamak esastır. Gizlilik, bütünlük ve erişebilirlik ağ güvenlik sistemlerindeki üç önemli güvenlik hizmetidir (Simmonds ve diğerleri, 2004). Gizlilik, bütünlük ve erişebilirlik ilkeleri her ağ güvenlik sisteminin sağlaması gereken hizmetlerdir (Stallings ve Brown, 2008). Tablo 1'de YBS'ye ilişkin olarak gizlilik/bütünlük ve erişebilirlik sorularının cevapları yer almaktadır.

Tablo 1. YBS'de Gizlilik/Bütünlük ve Erişebilirlik Kavramları

YBS açısından Gizlilik nedir?	YBS sistemlerinde gizlilik ilkesi, bilgiye siber uzayda YBS aktörlerinin ulaşması, yani başkaca hiç kimsenin ulaşamaması olarak tanımlanabilir.
YBS açısından "Bütünlük" nedir?	YBS sistemlerinde bütünlük ilkesi, bu sistemlerde üretilen her türlü YBS sistemlerine ait verinin/bilginin değiştirilememesi, bozulamaması ve yok edilememesi olarak tanımlanabilir.
YBS açısından "Eriebilirlik" nedir?	YBS sistemlerindeki siber uzay aktörlerinin istedikleri anda, yetkilerine uygun olarak veri/bilgiye erişilebilmelerine ilişkin hususlar olarak tanımlanabilir.
YBS açısından "Gizlilik" nedir?	YBS sistemlerinde gizlilik ilkesi, bilgiye siber uzayda YBS aktörlerinin ulaşması, yani başkaca hiç kimsenin ulaşamaması olarak tanımlanabilir.

İşletmelerde farklı problemlerin çözümünde doğru ve sağlıklı kararların alınmasında farklı seviyelerdeki yöneticiler için farklı bilişim sistemlerine ihtiyaç vardır. Bu durum Şekil 3'de sunulan YBS Bilgi Piramidi yapısında sunulmuştur.

Şekil 3. Yönetim Bilişim Sistemleri (YBS) Piramidi. Kaynak: (Tecim, 2020)

İşletmeler hem etkin olarak YBS'den yararlanmak ve hem de doğru veri/bilgilere erişmek istemektedirler. Böylelikle bilgi güvenliği sağlayarak doğru bilgilere

ulaşabilecek ve işletmeleri için doğru ve etkin kararlar verebileceklerdir. Van Thuy (2022) tarafından yapılan çalışmada internet teknolojisi olmadan bankaların daha fazla pazar payı kazanmalarının ve pazarlama stratejilerini genişletmelerinin çok zor olduğu belirtilmektedir.

4. SİBER GÜVENLİĞİN TANIMI, TEMELLERİ VE İLKELERİ

Günümüzde bilişim teknolojilerinin ve özellikle de İnternetin işletmelerin hemen her alanında yoğun olarak kullanılması siber güvenliği zorunlu kılmıştır. İşletmelerin en değerli bilgi kaynaklarının elektronik ortamlara taşındığı, veri/bilgilerini bilgisayar ortamında kayıt ve muhafaza altına aldığı, bilgi hizmetlerini bilgisayar ağları üzerinde paylaştığı bir çağda yaşadığımız bir gerçektir. İşletmeler için her türlü bilgi hizmeti ve faaliyeti artık fizikî sınır ve kuralların bulunmadığı bir boyut olan siber uzayda gerçekleşmektedir. Bilgi güvenliği, bilişim güvenliği ve siber güvenlik gibi kavramlar günümüzde işletmeler en önemli ve öncelikli konuları hâline gelmiştir.

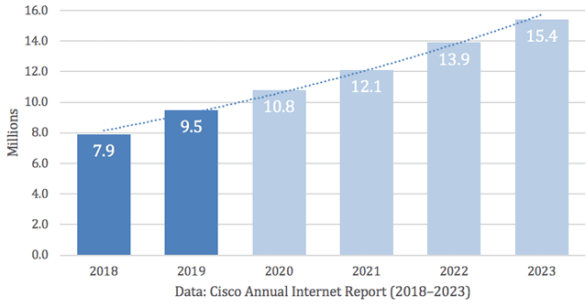
Siber güvenlik yazılımdan donanıma, ağlardan uygulamalara kadar pek çok bilgi teknolojileri varlıkları ile ilgilenir. Siber güvenlik, yalnızca bilgi kaynaklarının değil, diğer varlıkların da korunmasını kapsadığından, geleneksel bilgi güvenliğinin sınırlarının ötesine geçmiştir (Von Solms and Niekerk, 2013). Siber güvenlik konuları hakkında önemli sorular Tablo 23.1'de yer almaktadır.

Tablo 2. Siber Güvenlik Kavramları

Siber Savaş	Elektronik ortamda gerçekleşen bir savaş şeklidir (Boyd, 2009; Johnson, 2015).
Siber Terörizm	Sanal ortamda gerçekleşen terörizm faaliyetleridir.
Siber Savunma	Siber ortamda gerçekleşen savaşlar, saldırılar, terörizm, zararlı yazılımlar gibi durumların olumsuz etkilerine karşı alınan tedbirler ve yürütülen faaliyetlerdir.
Gizlilik	Bilginin yetkisiz kişilerin eline geçmemesi.
Bütünlük	Bilginin/verinin doğruluğunu ve tamlığını koruma özelliğidir.
Erişilebilirlik	Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olması.
Siber Uzay	Özellikle başta İnternet olmak üzere elektronik ortamlara bağlı sistem ve hizmetler.
Bilgi Varlığı	Bilginin/verinin taşındığı, saklandığı, aktarıldığı veya işlendiği her türlü sistemlerdir.
Siber Olay	Bilginin/verinin gizliliğinin, bütünlüğünün, erişilebilirlik durmunun ihlali.
Siber Risk	Bilgi varlıklarında zarar oluşturma potansiyelidir.
Siber Zafiyet	Siber tehdit ve saldırılara maruz kalabilecek olası zayıflıklardır.
Siber Suç	Bilişim teknoloji ve sistemleri ile gerçekleştirilen suçlardır.

Siber saldırılar bilginin gizlilik, bütünlük ve erişebilirlik özelliklerini hedef alırlar. Siber saldırı amaçları arasında siber ortamda yer alan bilgilerin istismar edilmesi, bozulması, değiştirilmesi, sistemlere erişimin engellenmesi ya da zarar verilmesi sayılabilir. Siber saldırılar neticesinde bilişim sistemleri tarafından işlenen verilere zarar verilmesi durumu söz konusudur. Siber saldırılar bir ülkenin stratejik olarak büyük önem taşıyan haberleşme ve bilgisayar sistemlerini, enerji kaynaklarını, enerji ulaşım ağlarını, askeri komuta ve kontrol sistemlerini, ekonomik sistemlerini, kritik altyapılarını zarara uğratacak büyüklükte etkiye neden olabilirler. İşletmelerin bilgi sistemlerine yönelik siber saldırıların giderek arttığı bir gerçektir. Ancak tüm siber saldırılar başarılı olarak sonuçlanmayabilir. Bu saldırılar sadece çok gizli veya özel bilgileri değil, aynı zamanda diğer tüm bilgileri de hedef olarak seçebilirler.

Siber saldırılar veri gizliliği ve bütünlüğünde ciddi kayıplara neden olarak sistemlere erişimi engelleyebilir ve sistemleri hizmet veremez duruma getirebilir. Saldırının düzeyine, tekniğine ve elde edilen bilgilerin türü gibi çeşitli kriterlere göre siber saldırılar değişen önemde kayıplarla veya tamamen işlevsiz hale gelme ile sonuçlanabilirler. Siber saldırılardan sonra saldırıya uğrayan sistemlerin kurtarılma ve eski hallerine getirilme maliyetleri çok yüksek olabilir. Bilgi güvenliği kapsamında, bir bilgisayar sistemine veya ağ güvenliğine yapılan saldırı tipleri, en iyi şekilde, bilgisayar sisteminin bilgi sağlarken fonksiyonunu gözlemleyerek karakterize edilebilir. Siber saldırıların ulusal güvenliğe kadar uzanan sonuçları olabilir. Siber saldırılara örnek olarak DDoS saldırıları örnek olarak verilebilir. Cisco'nun raporunda toplam DDoS saldırı sayısının 2023 yılına kadar 7,9 milyondan (2018 verisi) 15 milyonun üzerine çıkacağı tahmin edilmektedir (Şekil 4).



Şekil 4. DDoS toplam saldırı tahmini Kaynak: (Cisco Annual Internet Report, 2018–2023)

SG konusundaki bu tanımlarda öne çıkan önemli bir husus, siber savaşın devletlerarası cereyan eden bir faaliyet olduğudur. Söz konusu tanımlarda yer alan siber terörizmin ise kritik milli altyapıları devre dışı bırakmayı, bir devleti boyun eğdirmeyi veya sivil toplumu korkutmayı amaçladığı görülmektedir. İnternet ve bilgisayar sistemleri aracılığıyla hedeflenen sistemleri bozmak siber terör saldırılarının amaçları arasında yer almaktadır (Zanini vd., 2001).

5. YÖNETİM BİLİŞİM SİSTEMLERİNDE SİBER GÜVENLİĞİN ÖNEMİ

İçinde bulunduğumuz Bilgi Çağında işletmeler tarafından YBS'nin yoğun olarak kullanılması, YBS için SG konularının farkındalığını bir zorunluluk gelmiştir. Bilgi Sistemleri (IS) güvenliği, günümüzde çoğu organizasyonel faaliyet büyük ölçüde bilgi ve iletişim teknolojilerine bağlı olduğundan, modern işletmeler ve kuruluşlar için büyük bir endişe haline gelmiştir (Belsis ve diğ., 2005). Siber tehdit ve saldırıları karşısında YBS sistemlerinde oluşacak bilgi güvenliği zafiyetleri YBS sistemlerinin hizmet dışı kalmasına, ekonomik zararın oluşmasına ve hatta kamu düzeninin bozularak ulusal güvenlik zafiyetlerine kadar etkilere neden olabilir. Li ve diğ. (2021) tarafından yapılan çalışmada bilgi teknolojileri güvenlik yatırımlarının daha az dijitalleştirilmiş kuruluşlarda güvenlik ihlallerini azalttığı, ancak yüksek düzeyde dijitalleştirilmiş kuruluşlar için güvenlik ihlallerini artırdığı, bu bağlamda anti-virüs ve saldırı tespit sistemleri gibi teknik ağ kontrol güvenlik sistemlerine yatırım yapmanın harici güvenlik ihlallerini azalttığı belirtilmektedir. İşletmeler için bilginin güvenli bir şekilde oluşturulması ve bu bilginin yine güveni bir şekilde paylaşılması ve kullanılması yöneticilerin etkin ve anlamlı kararlar almalarında hayati öneme haizdir. Bilişim sistemlerinin siber olay, savaş, terörizm, tehdit ve saldırılara karşı korunması için bu aktivitelerin tespit edilmesi, durdurulması ve önlenmesi gereklidir.

SG alanı YBS gibi çok paydaşlı ve disiplinler arası bir konudur. Bilişim sistemlerini hedefleyen siber tehdit ve saldırı çeşitliliği ve sayısında bir artış olduğu bir gerçektir. Bu durum YBS'de kullanılmakta olan bilişim sistemleri için de geçerlidir. Siber saldırılar veri gizliliği ve bütünlüğünde ciddi kayıplara neden olarak sistemlere erişimi engelleyebilir ve sistemleri hizmet veremez duruma getirebilir. Mevcut iş ortamında, bir firmanın bilgi sistemleri güvenliği artık endüstrinin daha geniş güvenlik ortamından bağımsız değildir (Jeong ve diğ., 2019). Saldırının düzeyine, tekniğine ve elde edilen bilgilerin türü gibi çeşitli kriterlere göre siber saldırılar değişen önemde kayıplarla veya tamamen işlevsiz hale gelme ile sonuçlanabilirler. Siber saldırılardan sonra saldırıya uğrayan sistemlerin kurtarılma ve eski hallerine getirilme maliyetleri çok yüksek olabilir. Değerlendirme kontrolleri veri güvenliği açısından değerlendirme kontrolleri veritabanı sisteminin doğru yapılandırılıp yapılandırıldığını, güncelliğini, doğru kullanımını, kullanıcı ayrıcalıklarının yönetimini, hassas verileri, verilere erişim yetki ve seviyeleri gibi kontrolleri içerir (Oracle, 2022).

YBS sistemlerinde Bilgi ve İletişim Teknolojilerinin (BİT) ve özellikle İnternet'in yaygın ve yoğun kullanımı YBS sistemlerinde güvenlik risklerinin ve belirsizliklerinin oluşması durumunu beraberinde getirmektedir. YBS sistemlerinde gizlilik ilkesi, bilgiye yalnız ve yalnız bu bilgi sistemlerindeki YBS aktörlerinin ulaşabilmelerini ifade etmektedir. YBS sistemlerinde bütünlük ilkesi bu sistemlerde üretilen her türlü verinin/bilginin değiştirilememesi, bozulamaması ve yok edilememesi olarak tanımlanabilir. YBS sistemlerinde erişilebilirlik ilkesi bu sistemlerdeki siber uzay aktörlerinin istedikleri anda, sahip oldukları yetki hiyerarşisi içerisinde doğru bilgiye erişilebilmelerine ilişkin hususlar olarak tanımlanabilir.

6. YBS SİSTEMLERİNE YÖNELİK OLASI SİBER SALDIRI TÜRÜ VE YÖNTEMLERİ

YBS bilgi sistemlerine yönelik olası siber saldırı türü ve yöntemleri arasında aşağıda yer alan siber saldırı türü ve yöntemleri sayılabilir.

- **Virüsler:** Virüsler, diğer programları değiştirerek zarar veren kötücül programlardır. Kullanıcının bilgisi ve isteği olmadan bilgisayara yüklenir ve kendilerini kopyalamak suretiyle diğer sistemlere ve dosyalara yayılırlar.
- **Solucanlar:** Bunlarda aynı virüsler gibi kötücül programlardır. Ancak virüslerden farkları kendi başlarına kendini bir cihazdan başkasına kopyalamak üzere tasarlanmış olmalarıdır. Solucanlar bilgisayar ağlarını da kullanmak suretiyle bilgisayardan bilgisayara kopyalayarak kendilerini çoğaltabilirler.
- **Truva Atları:** Yapı itibari ile zararlı fonksiyonlar içeren ve bilişim güvenliğine zarar veren casus yazılımlardır. Bu programlar tarihte düşman kalelerini içeriden fethetmek için kılık değiştirerek kalelere gizlice sızan askerlere benzetilebilir.
- **Mantık Bombaları:** Belirli bir programın içerisine, genellikle de hedef alınan bilgisayar veya ağ sistemlerinde yer alan veri/bilgileri silmek ve değiştirmek amacıyla kasıtlı olarak zararlı ve kötücül bir kod yerleştirilmesi işlemi olarak tanımlanırlar. Aktif hale geldiklerinde kendilerine verilen kötücül görevi yerine getiriler.
- **İstem Dışı Elektronik Postalar:** Çoğunluğu reklam maksadıyla gönderilen ve genelde spam olarak da biline e-postalardır.
- **Klavye İşlem Kayıt Ediciler:** Kullanıcılar tarafından yapılan klavye işlemlerini kaydeden kötücül programlardır. En temel işlevleri arasında kullanıcıların klavye ile yatıkları işlemleri

yakalayarak bunları yetkisiz kişilere göndermek vardır.

- **Casus Yazılımlar:** Veri ve bilgileri kullanıcı bilgisi dışında kopyalayarak yetisiz kişilere transfer edilmesini sağlayan kötücül yazılımlardır. Genel olarak programların bedava deneme sürümlerinin içerisine enjekte edilmektedirler.
- **DDoS Saldırıları:** Bu siber saldırıların amacı, ağ iletişimini engelleyerek veya hizmetlere erişimi engelleyerek kaynakları tüketmektir (Darwish vd., 2013). Bu saldırı türünde büyük miktarda karışık veya karşılanamaz verileri bilgisayar ağlarına veya İnternet'e bağlı sunucular gibi bilişim cihazlarına göndererek zarar vermek amaçlanır. Tıpkı virüslerde olduğu gibi yeni DoS siber saldırıları da sürekli olarak geliştirilmekte ve siber saldırganlar tarafından yenileri oluşturulmaktadır. Flooding saldırıları, protokol saldırıları ve uygulama katmanı saldırıları, DDoS saldırılarının üç tipik kategorisidir (Singh ve diğerleri, 2017). Flooding saldırıları, bulut sistemlerinin kullanılabilirliğini, gizliliğini ve bütünlüğünü etkileyen yaygın saldırılar arasındadır (Modi ve diğerleri, 2013). Bu saldırılar, en önemli güvenlik tehditleri arasında yer alan erişebilirliğe dayalı saldırılardır (Fakeeh, 2016). DDoS saldırıları, COVID-19 döneminde ilk on siber güvenlik tehdidi arasındadır (Khan ve diğerleri, 2021).
- **Sosyal Mühendislik:** Sosyal mühendislik, özel ve gizli bilgilerin yetkisiz kişiler tarafından erişimi ve elde edilmesi için insan hatalarından yararlanan bir manipülasyon tekniğidir. Bu tür siber saldırıları çevrimiçi, yüz yüze ve diğer etkileşimler yoluyla gerçekleşebilir. Bilgisayar korsanları kullanıcıların bilgi eksikliğinden yararlanmaya çalışabilirler.
- **Diğer Saldırı Türleri:** Siber saldırganların kullandıkları diğer yöntemler yukarıda yer alan siber saldırı türlerinden çok daha fazladır. Ayrıca her geçen gün yeni siber tehdit ve saldırılarında gerçekleştirildiğini göz önünde bulundurmak gerekir.

7. YBS SİSTEMLERİNDE BİLGİ GÜVENLİĞİ ARAÇLARI

YBS bilgi güvenliği kapsamında aşağıda açıklanan teknik ve yöntemler siber tehdit ve saldırılara karşı siber karşı koyma tedbir ve yöntemleri kullanılabilir.

- **Şifreleme:** Şifreleme, teknik anlamda, insan tarafından okunabilen düz metinlerin, şifreli metin olarak da bilinen anlaşılmaz metne dönüştürülmesi işlemidir. Şifreleme işlemi sonrasında yalnızca yetkili tarafların bilgiler anlaşılabilmektedir. Şifreleme işlemlerinde genellikle bir şifreleme anahtarı kullanılır. Şifreleme işlemlerinde kullanılan anahtarlar şifreli bir mesajın hem göndericisinin hem de alıcısının ortak kararlaştırdığı bir dizi matematiksel değerdir.
- **Antivirüs Yazılımları:** Virüs ve virüs çeşitlerinin bilgisayar sistemlerine girmesini önleyerek, önceden bulaşmış olan virüsleri tespit etmeyi amaçlayan, virüsleri tespit işlemi eğer başarılı olursa virüsleri tanımlayarak tüm formlarını yok etmeyi amaçlayan, bu bağlamda virüs tehdidine karşı geliştirilmiş olan yazılımlardır.
- **Güvenlik Duvarı (Firewall):** Bilgisayar ağları arasına, ağların birbirlerinden izole edilmesi maksadıyla yerleştirilen ve ağlardan gelen ve/veya giden geçişleri kontrol edip, ağları güvenlik politikalarına göre denetleyerek ağ trafiğinin bilinen protokollere göre aktığını garanti eden sistem ya da sistemlerdir.
- **Sayısal İmza:** Sayısal imzalar bir elektronik dokümanları gönderenleri ve alanları doğrular. Yani sayısal olarak imzalanmış olan bir belgeyi gönderen kişi, onu yolladığını, alıcı da onu aldığını inkâr edemez. Sayısal imzalar mesajdan mesaja değişiklik gösterirler. Böylelikle bir bilgisayar ağı üzerinde gönderilen ve alınan dokümanın orijinal olup olmadığı ile güvenilir olup olmadığı mümkün kılınmış olur.
- **Özel Sanal Ağlar:** Bu ağlar ya da diğer adıyla VPN'ler özel ağlar ve açık ağlar arasında bulunan geçit kapıları olup, İnternet üzerinden şifrelemeyi ve özel iletişimi sağlamak için kullanılan, kuruma ait bilgi ve verilerin, sanal bir ağ oluşturularak bilgisayar ağları üzerinden aktarılmasını sağlayan bir teknolojidir.
- **Vekil Sunucular (Proxy):** Vekil Sunucular ya da bilinen adıyla Proxy'ler, bir yardımcı geçiş sistemi olup İnternet üzerindeki bir makine ile iç ağdaki bir makine arasında direk alışverişe izin vermeyerek, bu alışverişin arasına giren bir servistir.
- **Saldırı Tespit Sistemleri:** Saldırı Tespit Sistemleri ya da bilinen genel anlamı ile IDS'ler, sistem üzerindeki aktiviteleri analiz ederek, güvenlik zaafları ve açıklıklarını tespit eden, sistem yöneticilerine alarm vererek durumu bildiren sistemlerdir. Bu sistemler her türlü siber saldırının tespiti ve bertaraf edilmesi için geliştirilmiş sistemlerdir. Bu sistemlerin kullanımı ile bilgisayar sistemine yönelik saldırılar veya saldırı hazırlıklarını belirlemek amaçlanır. Kaynaklara yönelik tehdit oluşturan eylemleri fark etmeyi hedefleyen sistemler olarak tanımlanabilirler.
- **Zayıflık İnceleme Araçları:** Zayıflık inceleme araçları, bilgi güvenliğini sağlamak maksadıyla bir bilgisayar sistemi veya bir ağın savunma mekanizmasının zayıf ve hassas taraflarını, değişik analiz araçları kullanarak ortaya çıkarmayı amaç edinen araçlardır. Bu araçlar ile bir bilgisayar sistemi veya bir ağın güvenliğine metodolojik olarak bakılarak bu bilgisayar sistemi veya ağın potansiyel olarak zayıflıkları ortaya konur ve sınıflandırılır.

8. SONUÇ VE ÖNERİLER

Yönetim Bilişim Sistemleri (YBS), kurum, kuruluş, organizasyon ve şirketlerin operasyonlarının belkemiği olarak işlev gören, verinin toplanarak anlamlı bilgiler haline getirilmesinde, planlanmasında, ilgili birimler ile

güvenli olarak paylaşılmasında ve koordine edilmesinde ve nihai olarak da etkin kararlar alınmasında teknik ve davranışsal yaklaşımları içeren, donanım ve yazılımdan oluşan bilgisayar sistemleridir. Siber güvenlik faaliyetleri bilgi sistemlerinin siber tehdit, saldırı ve olaylardan korunmasını hedefleyen faaliyetler bütünüdür.

YBS sistemlerinde veri yönetiminde bilgi güvenliği konu, kural ve tedbirlerinin dikkate alınarak uygulanmasının özellikle yöneticilerin karar mekanzmalarında önemli rolü vardır. Bilgi güvenliği YBS için kritik öneme haiz bir konudur. Organizasyonlar için veri güvenliği iş sürekliliğini sağlamak, veri ihlallerinin önlemek ve yetkisiz erişimlerin önüne geçmek açısından önemlidir. Günümüzde iş dünyasının özellikle İnternetin de yaygın kullanımı ile büyük oranda dijitalleşmektedir. Bu anlamda veri güvenliği şirketlerin en mühim gündemlerinden birisi olmalıdır.

İşletmeler finansal kayıp yaşamamak, faaliyetlerini yürütmek ve güven oluşturabilmek için siber riskler karşısında doğru önlemler almak zorundadır. Herhangi bir organizasyon Veri güvenliği ile ilgili saldırı ve tehditleri en aza indirgemek, veri ihlali riskini azaltmak ve yasal uyumluluğun sağlanmasına yardımcı olmak için siber güvenlik konularının farkında olmalıdır. Veriler, organizasyonlar için en önemli varlıklar olduklarından dolayı her türlü yetkisiz erişime karşı korunmaları önemlidir. Veri güvenliği problemleri ve ihlalleri, başarısız denetimler ve yasal gerekliliklere uyulmaması, organizasyonların işlevlerini yerine getirememelerine, itibarlarının zarar görmesine, marka değerlerinin kaybına ve hatta idari ve para cezaları almalarına neden olabilir. Bu nedenle YBS kapsamındaki tüm hassas veriler korunmalıdır.

YBS sistemleri için bilgi güvenliğinin sağlanmasında Ulusal SG testlerinden geçirilmiş, yerli ve milli bilişim teknolojilerinin kullanılması hayati öneme haiz bir konudur. YBS sistemlerinin siber tehdit ve saldırıların odağında olması durumu, YBS sistemlerine yönelik siber tehdit, saldırı ve olayların tespit edilerek durdurulmasını, önlenmesini ve karşı koyma tedbirlerinin alınmasını bir zorunluluk haline getirmektedir. Araştırılan istatistikler, İşletmelerin sürekli gelişen siber tehdit ve saldırı ortamlarına uyum sağlamalarının hayati öneme haiz olduğunu ortaya koymaktadır.

SG, siber varlıkların tehdit, saldırı ve olaylardan korunmasını, gizlilik, bütünlük ve erişilebilirliğin sağlanmasını kapsayan faaliyetler bütünüdür. Günümüzde küçük, orta ve büyük ölçekli dahil organizasyonlar karar alma, kâr payı vb. nedenler ile YBS'ni yoğun olarak kullanmaktadırlar. Ancak günümüzde YBS sistemlerinin bilişim teknolojilerini ve özellikle de İnternet teknolojilerini yoğun olarak kullanması bu sistemleri siber güvenlik endişelere ile karşı karşıya bırakmış ve YBS sistemlerinde bilgi güvenliğinin önemini arttırmıştır. YBS sistemlerini hedef alan siber saldırılar işletmelerin bilgi hizmetlerini durdurabilir, aksatabilir.

Araştırmamız kapsamında aşağıdaki sonuçlara ulaşılmıştır.

- İşletmelerin YBS sistemlerinde giderek artan oranlarda bilişim teknolojileri ve özellikle de İnternet kullanılmaktadır. Bu durum beraberinde hayati öneme haiz bilgi güvenliği risk ve tehditlerini de getirmektedir.
- İşletmeler tarafından kullanılan YBS, günümüzde siber tehdit ve saldırıların odağı haline gelmiştir.
- İşletmeler için YBS'nde bilgi güvenliğinin sağlanması işletmelerin faaliyetlerini yürütmesinde hayati derecede öneme sahiptir.

Ulaşılan bu sonuçlara dayanarak şu öneriler getirilebilir:

- İşletmeler YBS kullanımında bilgi güvenliğini bir güvenlik politikası olarak değerlendirmelidirler.
- İşletmeler YBS bilgi güvenliği konusunda farkındalığı artırmak için gerekli çalışmaları yapmalıdırlar.
- İşletmeler aktif kullandıkları YBS'ne yönelik olası siber tehdit ve saldırılara karşı proaktif davranış sergilemeli, bu konuda işletme çalışanlarını kapsayan eğitim, tatbikat vb. Faaliyetler planlanmalı ve icra etmelidirler.
- İşletmeler faydalandıkların farklı YBS'ni bütüncül bir güvenlik bakış açısıyla değerlendirmelidirler.
- İşletmeler kullandıkları YBS'nin yazılım kaynak kodlarını tedarikçi firmalardan temin edilmelidirler. Ayrıca bu sistemleri yetkilendirme seviyelerine göre farklı güvenlik seviyesine sahip ağlar üzerinde ve bu sistemleri birbirinden ayrıştırarak çalıştırmalıdırlar.
- İşletmeler özellikle yerli ve milli olmayan YBS donanım ve yazılımlarını düzenli yazılım güvenliği testlerine tabi tutmalıdırlar.
- YBS sistemlerini kapsayan AR-GE çalışmaları teşvik edilmelidir.
- İşletmeler için yerli ve milli bir YBS ekosistemi oluşturulmalıdır. Bu kapsamda yerli ve milli YBS donanım ve yazılımlar kullanılmalıdır. Ayrıca bu durumu teşvik edecek işletmeye has politika ve stratejiler geliştirilmelidir.

KAYNAKÇA

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219-238.

Akhtar, S., Sheorey, P. A., & Bhattacharya, S. (2021). Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward. International Journal of

Business Intelligence Research (IJBIR), 12(1), 82-97.

Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. Information Management & Computer Security.

Boyd, B. L. (2009). Cyber warfare: Armageddon in a Teacup?. Army Command and General Staff Coll Fort Leavenworth KS.

Chan, L., Morgan, I., Simon, H., Alshabanat, F., Ober, D., Gentry, J., Cao, R. (2019, June). Survey of AI in cybersecurity for information technology management. In 2019 IEEE technology & engineering management conference (TEMSCON) (pp. 1-8). IEEE.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. IEEE Access.

Cisco Annual Internet Report, 2018–2023 (https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html) [Erişim Tarihi: 30.06.2022]

Damar, M., & Coşkun, E. (2017). Üniversitelerde bilgi işlemden yönetim bilişim sistemlerine geçiş: Mevcut durum ve beklentiler. Bilişim Teknolojileri Dergisi, 10(1), 21.

Darwish, M., Ouda, A., & Capretz, L. F. (2013, June). Cloud-based DDoS attacks and defens-es. In International Conference on Information Society (i-Society 2013) (pp. 67-71). IEEE.

Fakeeh, K. A. (2016). An overview of DDoS attacks detection and prevention in the cloud. International Journal of Applied Information Systems (IJAIS), 11(7).

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. Information & Management, 56(5), 681-695.

Johnson, T. A. (Ed.). (2015). Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. CRC Press.

Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic.

Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. Journal of Management Information Systems, 38(1), 222-245.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of network and computer applications, 36(1), 42-57.

ORACLE. (2022). Veri Güvenliği Konuları, Erişim Tarihi: 27.04.2022, https://www.oracle.com/tr/security/database-security/what-is-data-security/(Checkpoint, 2022) [Erişim Tarihi: 30.06.2022]

Özen, Ü. (2014). Bilgi Sistemlerine Giriş: Temel Kavramlar. Atatürk Üniversitesi AOF Yayınevi.

Singh, K., Singh, P., & Kumar, K. (2017). Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. Computers & security, 65, 344-372.

Simmonds, A., Sandilands, P., & Van Ekert, L. (2004, October). An ontology for network security attacks. In Asian applied computing conference (pp. 317-323). Springer, Berlin, Heidelberg.

Schwieger, D., & Ladwig, C. (2022). Cyber Insurance Concepts for the MIS and Business Curriculum. Informatıon Systems Education Journal, 20(5), 5.

Stallings, W., & Brown, L. (2008). Computer Security Principles and Practicessecond edition.

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses. Computers & Security, 109, 102385.

Tecim, V. (2022). Yönetim Bilişim Sistemleri (YBS). Erişim Tarihi: 27.04.2022, https://vahaptecim.com.tr/yonetim-bilisim-sistemleri/ [Erişim Tarihi: 30.06.2022]

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023). Erişim Tarihi: 27.04.2022, http://www.sp.gov.tr/tr/temel-belge/s/202/Ulusal+Siber+Guvenlik+Stratejisi+ve+Eylem+Plani+ 2020-2023 [Erişim Tarihi: 30.06.2022]

Van Thuy, N. (2022). Applications of IOTS, Internet Data, and Artificial Intelligence in Building Better Management Information System (MIS) in Banking Activities in Vietnam. In Advances in Computational Intelligence and Communication Technology (pp. 195-201). Springer, Singapore.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. com-puters & security, 38, 97-102.

Wassef Hijazeen, O., Ghazi Alshanty, A., & Abuhamdeh, M. (2022). Management Information System For Effective And Efficient Decision Making: Case Study Five-And Four-Stars Hotel In Jordan. Webology (ISSN: 1735-188X), 19(2).

Zanini, M., & Edwards, S. J. (2001). The networking of terror in the information age. Networks and netwars: The future of terror, crime, and militancy, 32.