T.C.
NEVŞEHİR HACI BEKTAŞ VELİ
ÜNİVERSİTESİ SOSYAL BİLİMLER
ENSTİTÜSÜ

TURİZM İŞLETMECİLİĞİ
ANABİLİM DALI

KONAKLAMA İŞLETMELERİNİN SİBER GÜVENLİK YÖNETİM YAKLAŞIMLARININ DEĞERLENDİRİLMESİ

Yüksek Lisans Tezi

Cem ALKAN

Danışman
Doç. Dr. Eda ÖZGÜL KATLAV

Nevşehir Nisan, 2022

BİLİMSEL ETİĞE UYGUNLUK

Bu çalışmadaki tüm bilgilerin, akademik ve etik kurallara uygun bir şekilde elde edildiğini beyan ederim. Aynı zamanda bu kural ve davranışların gerektirdiği gibi, bu çalışmanın özünde olmayan tüm materyal ve sonuçları tam olarak aktardığımı ve referans gösterdiğimi belirtirim.

Tezi Hazırlayan
Cem ALKAN

TEZ YAZIM KILAVUZUNA UYGUNLUK

'Konaklama İşletmelerinin Siber Güvenlik Yönetim Yaklaşımlarının Değerlendirilmesi' adlı Yüksek Lisans, Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü Lisansüstü Tez Yazım Kılavuzu'na uygun olarak hazırlanmıştır.

Tezi Hazırlayan	**Danışman**
Cem ALKAN	Doç. Dr. Eda ÖZGÜL KATLAV

Turizm İşletmeciliği Ana Bilim Dalı Başkanı

Doç. Dr. Duygu EREN

KABUL VE ONAY

Doç. Dr. Eda ÖZGÜL KATLAV danışmanlığında Cem ALKAN tarafından hazırlanan ‘Konaklama İşletmelerinin Siber Güvenlik Yönetim Yaklaşımlarının Değerlendirilmesi’ adlı bu çalışma, jürimiz tarafından Nevşehir Hacı Bektaş Veli Üniversitesi Sosyal Bilimler Enstitüsü Turizm İşletmeciliği Ana Bilim Dalı’nda Yüksek Lisans Tezi olarak kabul edilmiştir.

…… /…... / …..

JÜRİ **İMZA**

Danışman: Doç. Dr. Eda ÖZGÜL KATLAV

Üye: Doç. Dr. Duygu EREN

Üye: Dr. Öğr. Üyesi Neşe ÇULLU KAYGISIZ

ONAY: Bu tezin kabulü Enstitü Yönetim Kurulunun ….. /….. / ….. tarih ve …… sayılı Kararı ile onaylanmıştır.

….. /…... / …..

Enstitü Müdürü

KONAKLAMA İŞLETMELERİNİN SİBER GÜVENLİK YÖNETİM YAKLAŞIMLARININ DEĞERLENDİRİLMESİ

Cem ALKAN

Nevşehir Hacı Bektaş Veli Üniversitesi, Sosyal Bilimler Enstitüsü

Turizm İşletmeciliği Ana Bilim Dalı, Yüksek Lisans, Haziran, 2021

Danışman: Doç. Dr. Eda ÖZGÜL KATLAV

ÖZET

Bu çalışmanın amacı İzmir'deki 4 ve 5 yıldızlı konaklama işletmelerinin günümüzün ciddi tehditlerinden biri haline gelen siber saldırılara karşı nasıl önlem aldıkları, herhangi bir saldırı girişimde hangi yolları kullanarak karşı savunma yaptıkları ve oluşan saldırılardan sonra nelerde değişiklik yaptıkları hakkında bilgi edinmektir. Bu amaç doğrultusunda Japonya Ticaret ve İnovasyon Bakanlığı'na bağlı Japonya Bilgi Teknolojileri Özendirme Ajansı'nın (IPA) Bilgi Güvenliği Yöntemi Kıyaslama Sistemi tarafından geliştirilen anket formu kullanılmış ve İzmir ilinde faaliyet gösteren 4 ve 5 yıldızlı konaklama işletmelerinin bilişim teknolojileri bölümü sorumlularına ya da çalışanlarına anket uygulanarak veri toplanmıştır.

Araştırma sonucunda araştırma verileri non parametrik testlerle analiz edilmiştir. Analiz sonuçlarına göre konaklama işletmelerinin tamamının siber saldırılara karşı önlem aldıkları, büyük bir bölümünün ticari faaliyetlerini bilişim sistemlerine bağlı olarak yürüttükleri, bu sistemlerde oluşabilecek 24 saatlik bir erişim probleminde konaklama işletmelerinin satışlarında ve mevcut misafir hesaplarını kontrol etme konularında sıkıntılar yaşanacağı görülmüştür. Son olarak yapılan analizler sonucunda işletmelere karşı oluşabilecek siber saldırıların o işletmelerde büyük bir güven kaybı ve imaj eksikliği yaratacağı sonucuna varılmıştır.

Anahtar Kelimeler: Siber güvenlik, siber saldırı, konaklama işletmeleri.

EVALUATION OF CYBER SECURITY MANAGEMENT APPROACHES OF ACCOMMODATION BUSINESSES

Cem ALKAN

Nevşehir Hacı Bektaş Veli University, Institute of Social Sciences

Tourism Management , Master of Science Thesis, June 2021

Supervisor: Assis. Prof. Dr. Eda ÖZGÜL KATLAV

ABSTRACT

The aim of this study is to learn about how 4 and 5-star accommodation businesses in Izmir are taking precautions against cyberattacks that have become one of the serious threats of today, what means they are counter-defending against any attack attempt, and what they have changed since the attacks that occurred. For this purpose, the questionnaire developed by the Information Security Method Benchmarking System of the Japan Information Technology Incentive Agency (IPA) affiliated with the Ministry of Commerce and Innovation of Japan was used and data was collected by surveying the information technology department managers or employees of the 4 and 5 star accommodation enterprises operating in Izmir.

As a result of the research, research data were analyzed with non-parametric tests. According to the results of the analysis, it was observed that all accommodation enterprises take precautions against cyberattacks, most of them carry out their business activities depending on their information systems, and in a 24-hour access problem that may occur in these systems, there will be difficulties in the sales of accommodation enterprises and controlling existing guest accounts. As a result of the latest analysis, it has been concluded that cyberattacks against businesses will cause a great loss of trust and lack of image in those enterprises.

Keywords: Cyber security, cyber attack, accommodation businesses.

TEŞEKKÜR

Bu tez çalışmasının tamamlanmasında benden desteğini hiçbir zaman esirgememekle birlikte akademik alanda benimsemiş olduğum düşünceleri nasıl dile getirebilme ve bu düşünceleri akademik bir şekilde yazıya dökebilme konularında katkıda bulunan değerli tez danışmanım Doç. Dr. Eda ÖZGÜL KATLAV' a ve tez savunmam sırasında jüri olarak katılım sağlayan Sayın Doç. Dr. Duygu EREN ile Dr. Öğr. Üyesi Neşe ÇULLU KAYGISIZ' a en samimi duygularımla teşekkürlerimi sunarım.

İçerisine ilk girdiğim andan itibaren gerek akademik gerekse insanlık bakımından desteklerini eksik etmeyen Nevşehir Hacı Bektaş Veli Üniversitesi Turizm Fakültesi'nin bütün hocalarına ayrı ayrı teşekkürlerimi sunarım.

Araştırmaya katkıda bulunan İzmir İlindeki 4 ve 5 yıldızlı konaklama işletmelerinin ilgi bölüm yöneticilerine, bütün hayatım boyunca arkamdan hiçbir zaman eksik olmayan ağabeyim Uğur ALKAN' a, tez yazım süresince yanımda olan ve destek veren bütün arkadaşlarıma teşekkürlerimi sunarım.

İÇİNDEKİLER

TABLOLAR LİSTESİ

BİRİNCİ BÖLÜM

GİRİŞ

Bu bölümde araştırmanın problemi, amacı, konusu, önemi, varsayımlar ve sınırlılıkları ifade edilmektedir.

1.1. Araştırmanın Problemi

Boyutu devasa biçimde olan ilk bilgisayar ENIAC'IN üretiminden, akıllı telefonların insanların gündelik yaşantısına dâhil olmasına kadar geçen sürede bilgi teknolojilerinde gerçekleşen gelişimler oldukça büyük bir hız sergilemiştir (Değirmenci,2002).

Günümüzde bir kibrit kutusundan daha küçük ölçülerde olabilen sabit ve taşınabilir veri depolama cihazlarında bir kütüphanenin sahip olduğu içeriği saklamak mümkündür. Kamu kuruluşları, özel kurumlar ve kişiler bilgilerini elektronik ortamda muhafaza etmektedirler. Elektronik dünyanın insanlara sunmuş olduğu en faydalı olanaklardan birisi de internet hizmetleridir. İnternet hizmetlerinin kullanımı kamusal hizmetlerde, askeri alanda, eğitim alanında, bilimsel araştırmalarda, sağlık sektörlerinde, ekonomide, ticarette ve haberleşmede büyük önem taşımaktadır. Sağlamış olduğu bütün kolaylıklara karşın bilgi teknolojilerinde gerçekleşen bu gelişim bazı risk ve güvenlik zafiyetlerini de beraberinde getirmektedir. Küresel bir alanı barından internet ortamında bulunan bütün aletlerde (tablet, kişisel bilgisayarlar, akıllı cihazlar ve çevrimiçi bağlantısı olan tüm aletler) bulunan bilgiler, farklı yollarla risk altına girmiş ve internet ortamında güvenlik açıkları meydana gelmeye başlamıştır. Bahsi geçen bu güvenlik açıkları; bilgileri ele geçirme, imha etme, bütünlüğünü bozma ya da farklı amaçlar doğrultusunda kullanma amacı güden şahıslar, kuruluşlar ve hatta devletler nezdinde bir silah haline gelmiştir. Bu durumlardan yola çıkarak; siber güvenlik, siber savaş ve siber saldırı gibi kavramlar oluşmuştur. Bilgi güvenliğini sağlama gereksinimi de bu gelişmelerle eş zamanlı olarak kavranmaya başlanmıştır (Kurgun, 2006).

Siber saldırıların gün geçtikçe arttığı ve bu saldırıların konaklama işletmelerinde ciddi bir sorun haline geldiği görülmektedir. Özellikle zincir konaklama işletmelerinin geniş veri tabanı ağlarına sahip olduklarından dolayı ilk hedef olarak görüldükleri de kaçınılmaz bir gerçek olmakla beraber misafirler açısından da ödeme

esnasında kredi kartı kullanımı, konaklama işletmelerinin sadakat programlarına katılım ve kendi akıllı cihazları ile konaklama işletmelerinin çevrimiçi bağlantı ağlarına katılmaları esnalarında düşündürücü bir etkendir (Chen ve Fiscus, 2018).

Turizm hizmet ve ürünlerinin üretiminde ve pazarlanması alanında küresel dağıtım sistemlerinden (GDS/Global Distrubition System) ve bilgisayarlı rezervasyon sistemlerinden (CRS/Computer Reservation System) yoğun şekilde faydalanılmaktadır. Hizmet sektörlerinde müşterilerin memnuniyetlerine yönelik müşteriler ile ilgili bilgilerin muhafaza edildiği veri tabanına sahip olmak işletmeler için büyük önem taşımaktadır. Saklanan bu bilgiler ileride müşterilere yönelik pazarlama stratejilerin de kullanılmaktadır. Bu nedenlerden dolayı işletmelerin elinde bulundurduğu bu bilgiler işletmelerin kendilerine ait mahrem bir alanı ifade etmektedir. İşletmeler haricindeki kişilerce ele geçirilen bilgiler, işletme aleyhine kullanılabilir ya da rakip işletmelerin eline geçen bilgiler işletmenin pazardaki rekabet etme gücünü kaybetmesine sebep olabilir (Buhalis, 2020).

Konaklama işletmelerine karşı gerçekleştirilecek siber saldırıların amaçları nelerdir? Konaklama işletmelerinde alınan siber güvenlik önlemleri nelerdir? Konaklama işletmelerine yönelik olaşabilecek herhangi bir saldırı anında kriz planları yapılmakta mıdır? Siber saldırılara karşı çalışan personeller ne derecede bilgilendirilmektedir.

Bu çalışmasının amacı konaklama işletmeleri yöneticilerinin siber güvenlik yönetim yaklaşımlarının incelenerek değerlendirilmesidir.

1.2. Araştırmanın Konusu ve Önemi

İçerisinde bulunduğumuz bilgi çağı, teknolojik gelişmelerden dolayı hızlı bir şekilde gelişmekte ve bu gelişime şahıslar ve örgütlerde aynı hızla adapte olabilmektedirler. Hızlı bir gelişim gösteren teknolojik olaylar beraberinde teknolojik ürünlere yönelik artan talepleri de beraberinde getirmiştir. Bu gelişim gösteren bilişim sistemleri organizasyonların ve bireylerin işlerini daha kolay bir şekilde yapmalarını sağlamakta, beşeri iş gücünü azaltarak zaman ve maliyet konularında tasarruf etmekle birlikte işlemlerin makineleşme yöntemiyle daha az hata payının çıkmasını da sağlamaktadır. Bu olaylar işletmelerin siber dünyaya geçişlerinin yolunu açmıştır (Canbek ve Sağıroğlu, 2006). Bu sayede artık kişiler, organizasyonlar ve hatta devletler zaman ve mekân bağımsızlığı içerisinde sorumluluklarının büyük bir kısmını yerine getirebilecek esnekliği kazanmışlardır (Canbek ve Sağıroğlu, 2006).

Günümüzde insanlar sahip oldukları akıllı cihazlar sayesinde bankacılık işlemlerini, fatura ödeme işlemlerini, sanal market uygulamalarına girerek alışverişlerini yapabilir, yemek sipariş verebilir ya da işletmelerindeki gelişimleri akıllı cihazlarıyla anlık olarak takip edebilir konuma gelmiştir. Bununla birlikte işletmeler arasındaki iletişimin kolay hale gelmesi, yöneticilerin ihtiyaç duydukları bilgilere bulundukları yerden akıllı cihazlarıyla ulaşabilmeleri, veri analizi programları kullanarak sistem içerisinde bulunan tüketici bilgi ve istatistiklerine göre sadece istenilen tüketici grubuna yönelik reklam faaliyetleri gerçekleştirebilmeleri de işletmeler için büyük bir kolaylık, avantaj ve maddiyat yönünden tasarruf sağlamaktadır (Karabıyık ve Armağan, 2017).

Bilişim sistemlerinin gelişmesiyle hem ülke hem de özel sektör organizasyonu olsun ülkenin ya da firmanın gizli bilgileri, kişisel verileri, devlet ve şirket sırları, askeri stratejik dokümanlar, kritik altyapı ve devlet fonksiyonları daha kolay ve daha kullanışlı olduğu için bu bilişim sistemleri içerisinde depolanmaya başlanmıştır. Bu bilişim sistemlerindeki bilgiler koruma altına alınması gereken önemli bilgilerdendir. (Çakmakçı, 2012).

Siber güvenlik yönetim modeline paralel olarak verilen kararlar her ülkenin veya organizasyonun siber saldırılara karşı tutumunu göstermektedir. Bu durumda en önemli olay sistemlerin çalışabilmesi adına gerekliliklerin yerine getirilmesi ve risklerin de bu bağlamda değerlendirilmesidir. Bu çerçeveden bakıldığı zaman yalnız bir siber güvenlik yönetim modelinin olmamasıyla birlikte, her devlet veya organizasyon önemli bilgilerini bilinçli bir şekilde yönetme ve koruma gereksiniminin bilincindedir. Siber dünyanın gelişimi ve siber saldırıların sonuçlarının ağırlık düzeyinin artmasıyla birlikte etkili bir siber güvenlik yönetim modeli araştırmaları da hız kazanmıştır. Turizmin en önemli kollarından birisi olan konaklama işletmelerinde ise bilgi güvenliği konusunda risk teşkil eden alanlar, bilgi teknolojilerinden yoğun bir şekilde faydalanılan alanlar olarak saptanmıştır (Canbek ve Sağıroğlu, 2006).

Ülkemizde siber güvenlik konusu ile ilgili olarak ilk hukuki atılımlar 2000'li yıllarda başlamış olsa da bu atılımlar üzerinde çok fazla durulmamıştır. Bu atılımlar varlığını 2012 yılından sonra gösterebilmiştir. Çalışmalar sonucunda faaliyet gösteren birimlere siber güvenlik konusunda yeni tanımlamalar yapılmış olup bu birimlere ek

olarak yeni görevler üstlenecek Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Ekibi (SOME) birimleri kurulmuştur (Göçoğlu, 2018). Konaklama işletmelerinin faaliyetlerinde kolaylık sağlamaları açısından kullandığı internet bağlantılarının ve paket programlarının istenmeyen kişiler tarafından ele geçirilmesi gibi bazı risklerle karşı karşıya kalmaktadır. Konaklama işletmelerinin faaliyetlerinin zararsız bir şekilde yürütmesi açısında bilgi güvenliğini sağlaması büyük bir önem taşımaktadır. Bu doğrultuda yapılan bu çalışmanın konaklama işletmelerdeki bilgi işlem bölümü yöneticilerinin bilgi güvenliğini sağlayabilmeleri açısından önem arz edeceği düşünülmektedir.

1.3. Varsayımlar ve Sınırlılıklar

Araştırma kapsamında anket yöntemiyle farklı şirket özellikleri bulunan 4 ve 5 yıldızlı konaklama işletmelerinin bilgi işlem yöneticilerinin anket sorularına doğru yanıt verdiği varsayılmıştır. Araştırma anket yöntemiyle İzmir ilinde 2021 yılının Ocak-Şubat aylarında faaliyet gösteren ve Covid-19'a rağmen işletme faaliyetlerini sürdürebilen farklı şirket özellikleri bulunan 4 ve 5 yıldızlı konaklama işletmelerinin bilgi işlem bölümünde çalışan 47 kişinin vermiş olduğu yanıtlar ile sınırlandırılmıştır.

İKİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

2.1. Veri ve Bilgi Kavramı

Veri (Data) kelimesinin kökeni Latince' den gelmektedir. Kelimenin Latince karşılık bulan tekil hali "datum" sözcüğüdür. Türk Dil Kurumu Sözlüğü'nde veri; bir tartışmanın, bir araştırmanın, bir muhakemenin temeli olan esas öğe, done, muta, olgu, komut ya da kavramların iletişim, yorum ve işlem bakımından elverişli gösterimi olarak ifade edilmektedir (TDK, 2010). Veri, kayıt edilmeye, işlenmeye değer bulunan her türlü olay, düşünce, işitsel ya da görsel iletilerdir (Tutar, 2010).

Veri, olaylar ile ilgili objektif gerçekleri açıklar ve aynı zamanda veri yorum yapılmamış gözlemler ve üzerinde işlem yapılmamış gerçekleri ifade etmektedir (Barutçugil, 2002). Sürecin temel maddesi olarak farklı rakam, sembol, harf ve işaretlerle betimlenen, üzerinde hiçbir işlem yapılmamış gerçekler ya da izlenimlerdir. Veri, tecrübe ve araştırma sonucunda ortaya çıkmaktadır. Baz olarak hesap ya da torum yapılması maksadıyla kullanılmaktadır. Bu nedenle bilgisayara kaydedilmesi ya da bilgisayar aracılığı ile üzerinde işlem yapılması mümkün görünen her türlü fotoğraf, resim ve sesler de veri olarak kabul görmektedir. İşlenmemiş bilgi olarak da ifade edilen veri, üstbilgi ile özelleşmiş bilgidir (Sarıhan, 1998).

2.2. Bilgi Yönetimi ve Süreçleri

Literatürde bilgi yönetimi çeşitli araştırmacılar tarafından farklı yönlerden incelense de benzer şekillerde ifade edilmiştir. Bilgi yönetimi, bilgiyi bir bütün olarak ele alıp çeşitli davranışlarını gözlem altında tutmaktadır (Şencan, 2013). Bilgi yönetimi değişik bakış açıları elde etmek ve ulaşılmak istenen hedef bağlamında çeşitli şekillerde ifade edilmektedir.

Barutçugil (2002)'e göre bilgi yönetimi, koordineli hedeflerin daha etkili biçimde sağlanabilmesi için kişilere, gruplara ve organizasyonun bütününe bilginin kolektif ve sistemli şekilde oluşturulması, paylaşımı ve uygulanmasını mümkün kılan bir disiplindir. Şencan (2013) ise bilgi yönetimini, hızlı bir şekilde kurumsal karar alınmasını sağlamak, iş ve çalışmakta olan personel performansını arttırmak ve organizasyonel verimliliğe katkıda bulunmak maksadıyla gerekli her çeşit bilginin

üretimi, depolanması, örgütte paylaşılması ve uygulanmasına olanak sağlayarak örgütte paylaşılmasını ve kullanımını sağlayan bir bilim dalı olarak ifade edilebilir.

Özetle bilgi yönetimi, organizasyonun hedeflerine ilişkin bilginin oluşturulması, dağıtılması, değerlendirilmesi ve aynı zamanda etkin şekilde kullanılmasıyla alakalı bütün süreçlerin idare edilmesi manasını taşımaktadır. Zaim (2005), bilgi yönetiminin hedefleri ise, bilgi yönetimini, bilgiyi bulup, anlayarak kullanma ve değer yaratmak adına kullanılan sistemli bir yaklaşım olarak ifade eder. Celep ve Çetin (2003), bilgi yönetiminin amaçları örgütlerin içerisinde bulundukları çevrelerde gelişen teknolojik ve akademik ilerlemeler ile kavramsal ilerlemelerden haberdar olunması ve bilgilere örgüt tarafından uyum sağlanmasından bahsedilmektedir. Bununla birlikte, bilgilerin muhafaza edilmesini sağlayarak bilgiye erişimi kolaylaştırmak, bilgi ortamını arttırmak ve bir servet olarak bilgiyi yönetmek hedeflerini de ifade etmektedir.

Bilgi yönetiminin hedeflerinden birisi Yeniçeri ve İnce (2005) tarafından şu şekilde ifade edilmiştir; öğrenme eğrisine hız kazandırmak, daha hızlı geliştirme elde etmek, doğru bilginin doğru bireylere doğru zamanda erişmesini kolay hale getirmek, hızlandırılmış dönüşüme olanak sağlamaktır. Bilgi yönetiminin esas hedefi olarak ise, bilgi aktarımını desteklemek ve bilgi paylaşımını sağlamaktan bahsetmektedirler.

Zaim (2005)'e göre ise bilgi yönetiminin uygulanma gayeleri içinde başka açıklamalara yakın olarak, örgütlerin mevcut bilgi potansiyellerinden yüksek seviyede faydalanmak, bilgi varlıklarını etkin şekilde kullanarak üst düzey verim elde etmek bulunmaktadır. Bilgi yönetimi, örgütlerin sürekliliği ve varlığı hususunda oldukça önemlidir.

Calep ve Çetin (2003)'e göre bilgi yönetiminde rekabet artışı, müşteri isteklerinin farklılaşması ve iş çevresinin değişikliğe uğraması önemli unsurlarken Zaim(2005)' e göre bilgi yönetiminin artmasında teknolojik gelişmelerin olduğu ifade edilmiştir.

Bilgi yönetiminin örgütlere edindireceği faydalar dört esas unsurda açıklanabilmektedir;

- Bilgi işçilerinin bilgi ile ilgili farkındalığının artması
- Bilginin erişilebilirliği
- Bilginin kullanılabilirliği
- Bilgi edinmeye dair etkili zamanlama.

Bunlara erişmek ise bilgi sisteminin yapılandırılmasından bilgi işçilerinin kabiliyetlerine kadar farklılaşan çoğu faktöre bağlıdır (Offsey,1997). Bilgi yönetiminde amaçlanan neticelere erişilmesi, uyulması gerekli olan bir takım prensiplere bağlıdır. (Şencan, 2013) bu prensipleri aşağıdaki gibi sıralamıştır;

- Bilgi dinamik bir sosyal süreçtir: Bilginin oluşması birlikte çalışan kişilerin ortak manalarda buluşacakları şekilde etkileşimde olmaları ile meydana gelmektedir.
- Bilgi yalnızca kullanıldığı zaman değer kazanır: Bilginin değerini koruyabilmesi için dinamik olması gereklidir. Durgun bilgi değer yitireceği için devamlı tartışılması değerini yükseltmektedir.
- Bilgi karmaşıktır: Bilginin en geniş sosyal ortamda, dünya çapında çevrede bulunması bilgi faktörlerini belirleme bağlamında yapılan herhangi bir teşebbüsü tabiatı gereği karışık duruma getirmektedir.
- Bilgi kendi kendini organize eder: Örgütlerde üretilen, korunan, yenilenen ve yitirilen bilginin kendine has bir hayat süreci mevcuttur. Böylece bilgi kendi kendini organize eden bir varlık olarak ifade edilebilmektedir.
- Bilgi dil yoluyla taşınır: Bilginin her yönü, kişilerin tecrübelerinin ve bildiklerinin çoğalmasına olanak tanıyan değişik bir dil vasıtasıyla aktarılmaktadır.
- Bilgi değişimi elde tutar: Bilgi modelleri zaman içerisinde değişim gösterdiklerinden dolayı bilgi yönetiminde kesin bir çözüm mümkün değildir. En faydalı yaklaşım sürekliliği sağlayan yaklaşımdır ve dolayısıyla bilgi değişimi elde tutmaktadır (Bayraktar,2006).

Literatürde yönetiminin tanımlanmasındaki gibi içinde de bulundurduğu evrelerle alakalı olarak da değişik isimlendirmelerle benzer yaklaşımların olduğu görülmektedir. Celep ve Çetin (2003)'e göre, kişiler, süreçler, ürünler ve hizmetlerin kaynağında, açık ve örtük bilginin ifade edilmesi ile haberleşme sürecine alınması olarak ifade edilen bilgi yönetimi, bilgi oluşturma, bilgiyi geçerli kılma, bilgi sunumu, bilgiyi paylaşma ve uygulamadır.

Bilgi yönetimi, bilginin üretilip toplanması, düzenli hale getirilerek değerlendirilmesi, personellerin erişimine açılması, erişimi açılan bilginin kullanılarak verimli hale getirilmesi, verimlilikten kaynaklanan bilginin tekrardan

bilgi haznesine aktarılması, yaratılan sitemin değerlendirilmesi gibi birçok evrenden oluşan bir evredir. Bu evre içinde herhangi bir alanda aksaklık yaşanması diğer evreleri de etkilediğinden bütün evrelerin doğru ve düzgün şekilde işletilmesi oldukça önem arz etmektedir. Bu sürecin içinde bulunan evreler; gerekli olan bilginin tespit edilmesi, erişebilir haldeki bilginin seçilmesi, bilgi geliştirme, bilgi edinimi, bilgi iletim yolu meydana getirme, bilgi paylaşımının mümkün kılınması, bilgiden faydalanma ve faydalanılan bilgiyi doğru kullanma şeklinde de ifade edilebilir (Beijerse, 2000). Şencan (2013) bilgi yönetimi sürecinin aşamalarını aşağıdaki gibi ele almıştır:

- **Bilginin Üretilmesi:** Bilginin sistemli ve bilinçli bir şekilde oluşturulması bilgi yönetimi bakımından oldukça önemlidir. Bilginin oluşturulması ilk olarak bilgi edinilmesini gerektirir. Yeni bilginin edinilmesi araştırma ve geliştirme faaliyetleri ve bilginin ortak olarak oluşturulması yolu ile gerçeklemektedir. Bilgi oluşturulması ise işletmelerin taklit etme, satın alma ve kiralama yöntemlerinin yanında yeni bilginin oluşturulmasıyla da mümkündür (Davenport ve Prusak, 2000).
- **Bilginin Sınıflandırılması ve Depolanması:** Bilginin gruplandırılması, bilgi yönetiminin bilginin doğru birey tarafından doğru şekilde ve zamanda kullanılması hedefine hizmet eden önemli evrelerdendir. Bu evreni hedefi, bilgiyi kolay ve talep edilen herkesçe ulaşılabilir ve uygulanabilir bir şekle girdirmektedir. Bilgi örgütlerde depolanabilmesiyle birlikte hizmetlerde, bireylerde ve süreçlerde de depolanabilmektedir (Davenport ve Prusak, 2000).
- **Bilginin Paylaşılması:** Davenport ve Prusak (2000) örgütler içerisinde bilgilerin paylaşılmasının önemini şu şekilde belirtmektedir; "şeffaflık bilgi yönetiminin elzem şartıdır. Ulaşılamayan ya da kurum içinde dolaşmayan bilgiyi kurumsal bilgi birikimi veya kurumsal sermaye şeklinde değerlendirmek olanaksızdır". Dolayısıyla dokümanların, belge veri tabanlarının, intranetin, internet olanaklarının ve her çeşit grup haberleşme olanaklarının örgüt üyelerine iletilmesinde en önemli kanallar buradaki görevliler ve yapılan yüz yüze toplantılardan meydana gelmektedir.
- **Bilginin Kullanılması:** Edinilen bilginin sadece korunması ve saklanması bir örgütün hayatı için yeterli değildir. Bir bilginin etkili şekilde

kullanımı ve uygulanması örgüte rekabet fırsatı kazandırmaktadır (Kalkan,2006).

- **Bilginin Değerlendirilmesi ve Ölçülmesi:** Bilginin değerlendirilmesi ve ölçülmesi bilginin örgüte nasıl katkıda bulunduğunu hesaplamak demektir. Zaim(2005)' nin ifade etmiş olduğu gibi bilginin değeri üç şekilde ölçülebilir:
  - Stratejik değerlendirme
  - Paydaşlar bakımından değerlendirme
  - Bilginin ve organizasyonların geliştirilerek rakiplere karşı üstünlük kurması açısından değerlendirilmesi

Bu maddelerin yapılabilmesi için, bilgi yönetiminin liderlik, teknoloji, kültür ve ölçüm olarak dört esas faktöründen bahsedilmektedir (Celep ve Çetin, 2003). Bu faktörler içinde teknoloji ayağı, teknoloji, haberleşme ve bilgi işlem merkezi altyapısını da içerecek şekilde örgütün bütün enformasyonun toplayan, işleyen, arttıran ve dağıtımını yapan platform olarak açıklanmaktadır (Barutçugil, 2002). Bilhassa intranet ve internet teknolojilerinde gözlemlenen hızlı değişim ve bu değişim firmalar tarafından aynı hızda kabul edilmesi örgütlerin teknolojiye özel önem vermelerine neden olmuştur. Şu an da enformasyona erişmek gelişmiş bilişim teknolojileri sayesinde kolay ve ucuz hale gelmiştir.

2.3. Bilgi Yönetimi Modelleri ve Yaklaşımları

1990 senelerinden bugüne kadar literatürde gelişme gösteren bilgi yönetimi terimine dair birçok model ortaya atılmıştır. Bu modeller kayıpların ve bilgi boşluklarının engellenerek örgüt çerçevesinde hızlı ve doğru kararlar alınmasın katkı sağlamaktadır. Ortaya konulan modeller bilginin elde edilmesi evresinden yeni bilgilerin oluşturulmasını sağlayacak bir sitem oluşturulmasına uzanan süreçteki etkinlikleri içermektedir.

Literatürde bilgi yönetim modellerinin de çeşitli gruplandırmaları bulunmaktadır (Kurgun,2006). Çeşitli modellerin tercihi örgütlerin amaçlarına göre farklılık içermektedir. Celep ve Çetin'in (2003) de ifade ettiği model bir örgütte bilginin yapılanmasına odaklanmaktadır. Bilginin yapılandırılması ise bilimsel girdilerle sınırlı kalmayıp yapılandırılmış bilginin örgüt içinde sonrada da açık programların yanında toplumsal farklılık süreciyle de somutlaştırıldığını varsaymaktadır (Calep ve Çetin 2003).

Nonaka'nın Bilgi Yönetim Modeli bilgi yönetim modelleri içinde en fazla bilinenlerden birisidir. Bu model, bilginin kaynağına dayalı türlerinden örtülü ve açık bilginin ve kendi aralarındaki dönüşümleri üzerine kurulan bir bilgi türü modelini ifade etmektedir. Örtük ve açık bilginin aldığı duruma göre meydana gelen dönüşüm süreçlerini içermektedir (Şencan,2013). Bu modele göre ise örtük bilgi toplumsallaştırma süreciyle aktarılabilmekte ve dışsallaştırma süreciyle de açık bilgi haline getirilebilmektedir. Bu varsayım kapsamında aynı zamanda açık bilgi içselleştirme yöntemiyle başka bilgilere dönüştürülebilmekte ve birleştirme aracılığıyla da açık bilgiye dönüştürülebilmektedir.

Önemli olan ve en fazla bilinen diğer bir model ise Wiig'in *Bilgi Yönetim Modeli*'dir. Bu model üç bölümden oluşan bu bilgi yapısı, bilgiyi ve bilginin uygunluğunu araştırmak, bilginin değerini bulmak, bilgi hareketini yönetmek gibi yöntem ve yaklaşımlardan meydana gelmektedir (İpçioğlu ve Zafer, 2004). Bilinen diğer bir model ise entelektüel sermayenin ölçülmesi için İsveç sigorta işletmesi Skandia tarafından geliştirilen Skandia Navigator Modeli'dir. Bu model yönetim ve raporlama modeli olarak ifade edilse de diğer bir yönden entelektüel sermayenin gelişiminde, bilgi yönetiminin rehberi olarak geliştirilen eylemlerin, yönetim etkinliklerinin ve çalışma sürecinin rehberi durumuna gelmiştir (Barutçugil, 2002). Amerikan Verimlilik ve Kalite Merkezi (APQR) tarafından organizasyonların bilgi yönetim süreçlerinin karşılaştırılmasını mümkün kılmak üzere geliştirilmiş bir bilgi yönetim modeli vasıtasıdır (İpçioğlu ve Erdoğan, 2004). Bu model dinamik bir sistemde temel bilgi yönetimi faaliyetleri ve bunları sağlayan etmenleri birlikte göstermektedir.

Bilgi yönetim sistemi modelleri içinde son olarak Awad ve Ghazırı'nın (2004) ifade ettiği ait olan modelden bahsetmek gerekmektedir. On adımdan meydana gelen bu model dört temel bölüme tahsis edilmiştir; alt yapı değerlemesi, bilgi yönetim sisteminin çözümlenmesi, tasarımı ve geliştirilmesi, bilgi yayma ve performans değerleme modelinin meydana getirilmesidir. Her bölüm kendi içinde çeşitli etkinliklerin yapılması ile birbirine geçiş sağlamakta ve bir bütünlük içinde ele alınmaktadır. Bu modelde de örtük bilgiden açık bilgiye geçiş mümkündür. Böyle oluşturulan bilgi sistemi modeline göre teknik bilginin ve kişilerin zihinlerinde gömülü olarak bulunan bilginin etkinliklerde kullanılacak dokümanter edilmiş şekilde bir bilgiye dönüşümüyle bireyin algılama ve zihinsel modellerle

zenginleştirdiği örtük bilgi diğer çalışanların faydalanabileceği yeni bir şekle aktarılmaktadır. Bu dönüşüm sürecinde de açık ve örtük bilgi devamlı olarak faaliyetlere rehberlik eden ve kolay karar vermeyi sağlayan bilgi oluşumuna katkı sağlamaktadır.

Bilgi yönetimi sistemlerinin hedefi bilgiyi insanlar örgüt içindeyken edinmektir. Bilgi yönetimi modellerinin yaklaşık hepsi bilgiyi haritalama, görünür hale getirme ve bir altyapı yaratma hedeflerini barındırmaktadır (Davenport ve Prusak, 2000).

Birbirine bağlı olan bu amaçları içeren çeşitli bilgi yönetimi yaklaşımlarından da bahsetmek mümkündür. Bu yaklaşımlarda, bilginin hem örtük hem de açık halini dikkatli bir şekilde inceleyen dinamik bilgi yönetimi yaklaşımı; örtük bilginin vurgulandığı ve bilgi yönetiminin bu bilgiye sahip olan birey üzerinden olduğu insan yönelimli bilgi yönetimi yaklaşımı; açık bilginin ön planda olduğu, bilgi yönetimini sağlayan yöntemlerle bu bilginin edinilmesi, saklanması, dağıtımı ve kullanımının vurgulandığı sistem yönelimli bilgi yönetimi yaklaşımı; örgütsel bilgiyi kontrol etmeyi ve teknolojiyi kullanmayı hedefleyen süreç yaklaşımı; örgütsel bilginin çoğunluğunun örtülü olduğunu varsayarak resmi kontroller, süreçler ve teknolojilerin bu tür bilgiyi aktarmak için uygun olmadığını varsayan ve bu bağlamda bilgi yönetimi için bilgi paylaşımını sağlayacak sosyal çevreler veya uygulama grupları kuran uygulama yaklaşımı; pek çok örgüt süreç ve uygulama yaklaşımlarının karışımını kullanan karma yaklaşım; en etkin örgütlerin çeşitli işlevlerini işletmek ve yönetmek için kullandıkları etkinlik ve yöntemlerden oluşan en iyi uygulamalar yaklaşımı; kodlanmış örgütsel bilginin depolandığı ve geri çağrıldığı bilgi havuzlarını kullanan bilgi havuzları ve geliştirilmesi yaklaşımı bulunmaktadır (Şencan, 2013).

Bu bilgi yönetimi yaklaşımları ve modellerinin yanında temel bilgi yönetim stratejileri de mevcuttur. Barutçugil ’in (2002) de ifade ettiği, organizasyonel farklılık ve yenilik süreci üzerine oturtulmuş bu stratejiler, yeni bilgilerin oluşturulması, paylaşımı ve uygulanması ile sürekli olarak yenilik yapmayı amaçlamaktadır ve uygulanma süreci, bilginin oluşturulması, depolanması, paylaşılması ve uygulanmasına dair süreçleri içermektedir. Bu kapsamda kişiselleştirme ve kodlama olarak iki temel bilgi yönetimi stratejisi yer almaktadır. Kişiselleştirme stratejisi bir örgütte bulunan kişilerin belli bilgilerinin depolanarak merkezi hale getirilmesini ifade ederken, kodlama stratejisi ise örgütsel bilgi akışının

gerçekleştirilmesi için örtük bilginin açık bilgiye dönüştürülmesini ve örgütün bilgi birikimini sistematize ederek depolanmasını ifade etmektedir (Şencan, 2013).

Özetle bilgi yönetimi, örgütlerde problem çözme, dinamik öğrenme, stratejik planlama ve karar alma gibi faaliyetler için önemli olan bilginin elde edilmesi, seçilmesi, örgütlenmesi, yayılması ve aktarılmasına yardımcı olan bir süreçtir. Otel yönetiminde de işletmenin diğer şirketlerle rekabet etmesine katkı sağlayacak, organizasyonda bilginin depolanması, örgütlenmesi ve aktarımını sağlayarak başarısına katkı sağlayacak bir vasıta olmaktadır.

2.4. Bilgi Güvenliği

Bilgi güvenliği; bilgilerin veya verilerin, depolanması ve taşınması esnasında, bütünlüğünün zarar görmeden, izinsiz erişimlerden korunması adına gösterilen çabalar bütünü veya bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaç ile ve doğru biçimde faydalanılarak, her türlü ortamda istenmeyen kişiler tarafından ele geçirilmesinin önlenmesi olarak da ifade edilebilmektedir (Canberk ve Sarıoğlu: 2006).

Sürekli gelişim içerisinde olan bilişim teknolojileri, bilgilerin işlenmesi, aktarılması ve muhafaza edilmesi gibi hususların işletmelere sağladığı yararlar göz önünde bulundurulduğu zaman işletmelerin bu sistemlere sürekli bir şekilde yatırım yaptıkları görülmektedir. İşletmeler kullandıkları yazılım programları ile daha az zaman harcayarak daha fazla verim aldıkları için bu yazılım programlarına kısmi olarak bağımlı hale gelmişleridir. Bütün faaliyetlerini bilişim teknolojileri üzerinden yürüten işletmelerin bu faaliyetlerini yürüttükleri bilişim sistemlerinin güvenliklerini sağlamaları son derecede önemlidir. Sadece bilgiye ulaşması gereken kişilerin erişiminin sağlanması, bilginin herhangi bir şekilde bozulmadan, değiştirilmeden, yetkisiz bireylerce tahrip edilmeden ve bilginin yetkisi olmayan kullanıcılar tarafından erişimine izin verilmeyerek gizliliğinin korunması bilgi güvenliği olarak ifade edilebilir (Pfleeger, 1997).

Gelişen bilişim teknolojileri, işletmelere sağladığı faydalıklar ile birlikte bazı riskleri de yanında getirmektedir. Bilginin güvenliği, bilginin gizliliğine, bilginin bütünlüğüne ve bilginin erişilebilirliğine karşı oluşabilecek zararları engelleyerek gerçekleştirilir. Bilgi güvenliğini oluşturan temel üç ana faktöre ilave olarak inkâr edememe, güvenirlilik ve kimlik yönetimi de alt faktörler olarak eklenebilir. Bu ana

faktör küçük ölçekli işletmelerde kolay bir şekilde oluşturulmaktadır. Ancak, büyük ölçekli işletmelerde çok sayıda çalışan bulunması, faaliyet gösteren cihaz sayısının fazla olması, farklı konumlarda kullanılan cihazların bulunması bilgi güvenliğinin sağlanmasını zor bir hale getirmektedir. Bu sebeplerle, bilgi güvenliği yalnızca bilgi güvenliği çalışanlarının sorumluluğunda değil, bilişim sistemlerini kullanan bütün çalışanlarda olmalıdır. Bilginin güvenliği yalnızca bilgi işlem personelinin sorumluluk alanında değil, tüm çalışanların sorumluluk alanında olmalıdır. Bilgi güvenliği, işletmelerde tüm çalışanlar tarafından dikkate alınırsa sağlanabilmektedir (Johnson ve Goetz, 2007). Bilgi güvenliğini tehdit eden saldırılar yalnızca işletme dışındaki kaynaklar tarafından değil işletme içerisinde bulunan kaynaklar tarafından da olabilmektedir. Bilişim sistemlerine giriş yetkisi bulunan personellerin sakıncalı işlem ve davranışlar sergilemesi bilişim sistemleri içerisinde bulunan gizli bilgilerin güvenliğini tehdit altına almaktadır (Thomson, Solms ve Louw, 2006). Siber güvenlik araştırmaları ve uygulamaları alanında çalışmalar gerçekleştiren bir firmanın yapmış olduğu araştırma sonuçlarında 2018 yılında meydana gelen siber saldırıların %46'sı kurum içerisinde çalışan personellerin haklarının sömürülmesiyle işletmede çalışan personeller tarafından başlamaktadır.

Bilgi güvenliğinin sağlanmasındaki en önemli etkenlerin başında işletme içerisinde çalışan personellerin bilgi güvenliğinin çok önemli bir konu olduğunun farkında olmalarıdır. Bilişim sistemlerine karşı tehdit unsuru bulundurun hususların göz ardı edilmesi, gerekli tedbirlerin alınmaması ya da yanlış önlemlerin alınması sonucu meydana gelen olumsuz sonuçlar bilişim sistemlerinin güvenliğinin sağlanılamadığını göstermektedir (Siponen, 2000). Maslow' un ihtiyaçlar hiyerarşisinde güvenlik ihtiyacı ikinci sırada yer alsa da, bilgi güvenliği konusunda çoğu kuruluş bu sıralamaya uyum göstermemektedir. Bu durumlarda işletmeler bilgi güvenlik tehditlerinin meydana gelmesinden sonra bilgilerinin ele geçirilmesi, hırsızlık, bilgilerin zarar görmesi gibi olumsuz sonuçları öngörmekte eksik kalmaktadırlar (Siponen, 2000).

Gizlilik, bütünlük ve kullanılabilirlik bilgi güvenliğinin en önemli başlıklarıdır. Bu ana başlıklara ek olarak bilgi güvenliğinin gerçekleştirilebilmesi için yardımcı başlıkların da sağlanması gerekmektedir. Kayıt tutma, güvenilirlik, kimlik doğrulaması ve yetkilendirme etkenleri de bilgi güvenliğinin sağlanmasında yardımcı olan etkenlerdir. Bu etkenlerin hepsinin eksiksiz bir şekilde yerine getirilmesi ile

bilgi güvenliği anlamıyla sağlanmış olacaktır. Bu etkenlerin bir ya da birkaçının yerine getirilmemesi, bilgi güvenliğinde eksiklikler gösterecektir (Baykara, Daş ve Karadoğan, 2013).

- **Gizlilik:** Yetkisi olmayan şahısların bilgiye erişmesinin önlenmesi temel amaçtır. Bilgi depolanırken, işlenirken ya da aktarımı gerçekleştirilirken yetkisi olmayan personellerin bilişim sistemlerine giriş yapmalarına izin verilmemelidir. İşletmelere karşı tehdit sayılabilecek birimler, şirkete zarar verme ve siber casusluk gibi saldırılarla hedef aldıkları işletmelerin bilişim sistemlerine sızmayı hedeflemektedir. Bu sebeple, bilginin gizliliğini sağlamak işletmenin bilgi güvenliği bakımından çok önemlidir. McCumber modelinde kurumların bilgi güvenliğini sağlamak amacıyla bilgilerin aktarılması ve depolanması evrelerinde şifreli giriş yöntemlerini kullanmasını önermektedir (McCumber, 2004).
- **Bütünlük:** Bilginin erişim yetkisi olamayan kişilerce değiştirilmesinin, tahrip edilmesinin ve bozulmasının engellenmesi manasına gelmektedir. Bilgi varlığının bütünlüğü, aktarılması sırasında ya da muhafaza edildiği yer içerisinde siber casuslarca bozulabilmektedir. İçinde bulunduğumuz bilgi çağında programlanan birçok virüs ve solucan adı verilen zararlı yazılımlar bilginin bütünlüğünü bozmayı amaçlamaktadır. Bu nedenle, bilgi varlığının bütünlüğünü korumak adına gerekli güvenlik önlemlerinin alınması kaçınılmazdır. Bilgi varlığının bütünlüğünün korunması için kullanılan en yaygın yöntem dosya özet değerinin hesaplanması yöntemidir. Uyumlu bilgisayar algoritmaları kullanılarak depolanan dosyaların özet değerleri çıkartılır. Özet değerleri çıkartılan dosyalar üzerinde yapılacak bütün değişikler aynı şekilde çıkarılan özet değerlerinde de değişikler meydana gelecektir. Eğer bu değişiklikler işletme tarafından bilinçli bir şekilde yapılmamışsa dosyanın bütünlüğünün siber saldırılar sonucunda bozulduğu anlaşılmaktadır (Whitman and Mattord, 2011).
- **Erişilebilirlik:** Yetkili kullanıcıların ya da sistemlerin istedikleri zamanda herhangi bir engel ile karşılaşmadan bilgiye erişimlerinin sağlanmasına verilen isimdir. Saldırganlarca kullanılan devre dışı bırakma

saldırısı gibi saldırılar bilgiye erişimin engellemesini amaçlamaktadır. Bu ve bunun gibi saldırılar sonucunda kurumlar veri kaybı, finansal zararlar ve temel hizmetlerin aksaması nedeniyle sektörde güven kaybı ve imaj zedelenmesi gibi problemler ile karşı karşıya kalmaktadırlar. Bu sebeple bilgiye erişebilirliğin sağlanması bilgi güvenliğinin temel unsurlarından birisidir (Gülmüş, 2011).

Bilgi güvenliğinin yerine getirilebilmesi için yukarıda açıklanan ana unsurlara ek olarak kayıt tutma, güvenirlik, kimlik doğrulaması ve yetkilendirme unsurları şu şekilde açıklanmaktadır (Gülmüş, 2011).

- **Kayıt Tutma:** Bilişim sistemlerinde yapılan bütün işlemlerin kayıtları sistemlerin kendi üzerinde ya da merkezi yönetimleri tarafından tutulmalıdır. Bu kayıtlar, sistemlere giriş yapan kişilerin yaptıkları tüm işlemlere ait bilgileri, erişim yaptıkları zaman bilgisi, sisteme nereden ve nasıl erişim yapıldığına yönelik bilgileri bulundurmaktadır. Özellikle, siber olaylara müdahale ekipleri bu kayıtlar üzerinde inceleme yaparak saldırıyı gerçekleştiren kişi veya kişilere yönelik izleri takip edebilmektedirler. Bilgi güvenliği bakımından kayıt tutma özelliği önemli bir yere sahiptir. Saldırı tespit, saldırı inceleme, mevzuatlara uyumluluk gibi sebeplerden dolayı kurumlar bütçelerinde kayıt tutma sistemlerine de yer vermektedirler (Gülmüş, 2011).
- **Güvenilirlik:** Kurumların bilişim sistemlerinde bulunan cihazların ve bilginin transferi için faydalanılan sistemlerin tasarımlarına ve kurumun hazırlamış olduğu şartnamenin maddelerine bağlı kalarak çalışması yöntemine verilen isimdir. Güvenilirlik algısına bağlı kalınması bilgi güvenliğinin unsurlarının önemli bir parçasıdır (Gülmüş, 2011).
- **Kimlik Doğrulaması:** Kullanıcılardan bilişim sistemlerine giriş yaparken ve bilişim sistemleri içerisindeki bilgilere ekleme veya bilgilerde değişiklik yapacakları zaman işletmeler tarafından kullanıcılara tanımlanan parola ya da biyometrik (bireyleri tanımak adına yapılan biyolojik ölçüm) doğrulama ile giriş yapmaları talep edilir, sistem üzerindeki kayıt ile eşleşmesi durumunda sisteme giriş ve sistem içerisinde değişiklik yapma hakkı verilmesidir (Gülmüş, 2011).

- **Yetkilendirme:** Bilişim sistemlerine erişim yetkisine sahip kullanıcıların sistem içerisinde hangi bilgilere ulaşabilme yetkisi ve hangi bilgilere ulaşımının engellenmesi işletmeler tarafından tanımlanmalıdır. Kullanıcıların sadece kendi iş tanımlarına yönelik bilgilere ulaşım ve o bilgiler üzerinde değişiklik yapma hakkına sahip oldukları sistemlerdir bilişim sisteminin güvenliğinin sağlanması için kullanıcılara ihtiyaçları dışarısındaki bilgilere erişim yetkisi verilmemelidir (Gülmüş, 2011).

Bilgi teknolojilerinde yaşanan gelişme sonucunda internet hayatımıza girmiştir. Tüketiciler otel rezervasyonları, yemek siparişi verme, market alışverişi, bankacılık işlemleri, vb gibi günlük işlemleri çevrimiçi ortamlarda yapabilmekte ve burada birçok veri birikmektedir. Ancak internet ortamında veri güvenliğinin sağlanması ve korunması konusunda bazı sorunlar bulunmaktadır. Bu noktada siber güvenlik kavramları ortaya çıkmıştır

2.5. Siber Alan Kavramı

Bilişim sistemlerinin gelişmesiyle birlikte gündelik dilimize yeni terimlerde giriş yapmıştır. Bunlardan bir tanesi olan siber uzay olgusu İngilizce'de "cyberspace" olarak ifade edilmekte ve dilimize siber ortam, siber alan olarak da çevrilebilmektedir. İlk kez 1982 yılında bilim kurgu romanları ile ünlü yazar William Gibson tarafından "Burning Chrome" isimli kitapta karşımıza çıkmıştır (Wired, 2009).

Farklı şekilde açıklanan siber uzay kavramları incelendiğinde;

- Amerika Birleşik Devletleri hava kuvvetleri için hazırlanmış olan kitapta siber uzay beşinci boyut olarak tanımlanmıştır. Siber uzay, karada, havada, denizde ve hatta uzaydan bağımsız ve iletişim altyapılarını kullanan sanal bir ortam olarak açıklanmıştır (Libicki, 2009).
- Bilgisayar ağlarının ortaya çıkardığı, üzerinde iletişim sağlanabildiği kavramsal ortamdır (Oxford Dictionaries, 2018).
- İnternet, iletişim ağları, bilgisayar sistemleri, sabit işlemci ve kontrol mekanizmalarını kapsayan, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağlı ağların oluşturduğu bilgi ortamındaki küresel bir alandır (Altıner ve Çakır, 2017).

İncelenen tanımlar doğrultusunda siber uzayın aslında hala büyüme gösteren, insanların yaşamlarında her türlü elektronik veriye erişim kolaylığı sağlayan yeni bir boyut olarak ifade edilebilir. Siber uzayla birlikte insanların bilgiye ulaşması için çizilen sınırlar yok edilmiş, insanlar arasında bilgisayar ve haberleşme sistemleri kullanılarak bağlantılar sağlanmaktadır.

Yukarıda incelendiği gibi siber uzay ile alakalı birden fazla tanımlama yapılmıştır. Bu tanımlar incelendiği zaman siber uzay ile alakalı aşağıdaki çıkarımlar yapılabilecektir:

- Siber uzay insan zihninde oluşan gerçekliğin ve sanalın birleşiminden meydana gelen bir sanal boşluktur. Fiziksel olarak gerçek bir alana sahip değildir. Siber uzay dünya için dijital tamamlayıcı bir kavram olarak değerlendirilebilmektedir.
- İnsanlar, siber uzaya fiziksel cihazların yapay işletim sistemlerini kullanarak erişim sağlamaktadırlar. Bu sebeple kullanılan cihazlar siber uzayın sınırı veya siber uzaya açılan pencere olarak değerlendirilebilmektedir. Meydana gelen bu etkileşimler ve kurulan iletişimler zaman ve boşluk kavramlarından bağımsız bir şekilde gerçekleşmektedir.

Siber alan kavramı beraberinde siber güvenlik konusunu gündeme getirmiştir. Siber alanda toplanan verilerin güvenliğinin nasıl sağlanacağı önemlidir. Siber alanda toplanan verilerin korunamaması ve güvenlik zafiyetleri işletmelerin ve tüketicilerin mağdur olmasına neden olabilmektedir. Bu kavram bir sonraki başlıkta detaylı bir şekilde açıklanacaktır.

2.6. Siber Güvenlik

Siber güvenlik olgusu bilişim sistemlerinin içerisinde barındırdığı bilgileri hedef alan her türlü saldırılara karşı sürekli bir şekilde koruma sistemleri olarak ifade edilebilmektedir (Cavelty,2010).

Birleşmiş Milletler' in haberleşme, bilgi ve iletişim teknolojileri alanındaki yetkili birimi Uluslararası Telekomünikasyon Birliği tarafından yapılan tanımda siber güvenlik, siber uzayda var bulunan örgüt ve organizasyonların varlıklarını korumak ve sürdürmek amacı ile kullandıkları araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eğitimler, eylemler, uygulamalar ve teknolojiler bütünü olarak ifade etmektedir. Siber uzayda organizasyon ve

kullanıcıların varlıklarını, kişiler, bilgi işlem donanımları, altyapılar, uygulamalar, hizmetler, haberleşme sistemleri ve siber uzayda iletilen ve/veya depolanan bilgiler meydana getirmektedir (Eltem,2021).

Bir diğer ifadeyle siber güvenlik, TAG-Cyber firmasının kurucusu ve yönetim kurulu başkanı olan Edward Amoroso tarafından Siber Güvenlik isimli kitabında "siber güvenlik, zararlı atakların sistemlerde, bilgisayarlarda ve ağlarda oluşturabileceği risklerin en aza indirgenmesini kapsamaktadır. Bu kavram virüslerin tespiti ve engellenmesi, kötü amaçlı erişimlerin engellenmesi, sistemlere sızmaların tespiti, şifrelenmiş iletişimin aktif edilmesi ve kimlik doğrulamanın zorunlu hale getirilmesine imkân sağlayacak araçları kapsamaktadır." şeklinde ifade etmiştir (Amoroso, 2006).

Uluslararası Telekomünikasyon Birliği tarafından da kabul edildiği gibi güvenliğin ana hedefi, bilişim sistemlerinde depolanan verilerin gizliliğini, bütünlüğünü ve kullanabilirliğini sürekli olarak sağlamaktır. Güvenlik alanında gizlilik, bütünlük ve kullanılabilirlik temel üç bileşenidir ve bu üç bileşen birbiri ile iç içe olacak şekilde ele alınmalıdır (Eldem,2021).

Endüstri 4.0 karamı ile birlikte sistemler gerçek zamanlı bağlantı, iletişim ve anlık tanımlamalar yapmaya başlamışlardır. İnsan ve makine birleşimiyle meydana gelen Endüstri 4.0 işletmelerin müşterilerinin özel istek ve zevklerine yönelik ürünler sunabilmeye yönelik gelişmeler kaydetmiştir. Bu gelişmelerle birlikte üreticilerde akıllı üretim tesisleri sistemlerine yatırımlar yapmaya başlamışlardır. Bu akıllı üretim tesisleri müşterilere ürünlerin ilk halinden son haline kadar geçen eveleri takip edebilme olanakları sağlamıştır (Fırat ve Fırat, 2017). Akıllı üretim tesisleri içerisindeki kullanılan cihazların hepsinde farklı yazılımlar kullanılmaktadır. Bu yazılım sistemlerinin üretimin aksamaması adına güvenliklerinin sağlanması işletme açısından büyük bir önem taşımaktadır (Fırat ve Fırat, 2017).

Siber saldırı riski olan sistemler sadece akıllı üretim tesisleri değil, bilişim sistemlerinin kullanıldığı çevrimiçi bağlantı sağlayarak faaliyetlerini sürdüren bünyesinde ülkelerin, işletmelerin ve bireylerin maddi ve manevi bilgilerini bulunduran bütün örgütler siber saldırı riskleriyle karşı karşıyadır. Örgüt büyüklüğü ne kadar artarsa örgüt siber saldırı riski ve örgüt içerisinde hizmet veren kişi sayısı da aynı derecede artmaktadır. İnsan unsurunun olduğu yerde hata payı da

bulunmaktadır. Çalışan personel sayısının artmasıyla sistemde oluşabilecek siber açıklıklarda artmaktadır (Ünver 2012).

Dünya Ekonomik Formu'nun 2018 senesinde yayınladığı Küresel Risk Raporunun, tezin ana unsurları olan siber güvenlik, siber saldırılar, veri hırsızlıkları kısacası tezin ana fikri ile tamamen örtüştüğü görülmektedir. Yayınlanan raporda ilk beş küresel risk raporunun dünyada meydana gelen iklim değişikliğinden mali dengesizliklere, doğal afetlerden ekonomik krizlere kadar uzanacak şekilde değerlendirildiği düşünülürse siber atakların ilk kez 2012 yılında olabilirlik bakımından ilk beş küresel risk kategorisine girmesi ve bundan sonraki yedi senede siber olaylar ile alakalı beş başlığın rapora dahil edilmesi, daha önce de belirtildiği gibi siber güvenlik olgusunun ne kadar önemli olduğunu ve riskin her gün teknolojik gelişmeler ile arttığı veriler ile saptanmıştır (Ilgar ve Erdoğdu 2018).

2.6.1. Siber Saldırı

İnternet ve bilgisayar kullanımının dünya çapında daha da yaygınlaştırılması kullanıcılara belli kolaylıklar sunmakta iken kendisiyle birlikte tehditler de getirmektedir. Kurumların ve ülkelerin siber saldırılarla karşılaşması bunların ilkleri olarak sayılabilir. Siber güvenlik ile bağlantılı diğer terimler gibi siber saldırının da üstünde tam anlamıyla uzlaşmayla varılan bir tanım bulunmamaktadır. Var olan farklı tanımlamalardan sonra genel olarak kabul edilen bir tanımda siber saldırı, siber casusların kullandığı bilgisayar sistemlerinin hedef aldıkları bilişim sistemlerine sızmak, hedef sistemlerdeki mevcut bilgileri ele geçirmek, bozmak veya silme amacıyla kısa ve uzun süreler boyunca bilinçli olarak gerçekleştirdiği saldırılar olarak tanımlanmaktadır. Bir siber saldırı hedef aldığı sistemlerin ya da ağların hedef için kullanışlı olmayan duruma gelmesine ve güvenilmez olmasına yol açtığı için önem taşımaktadır (Lin, 2010:63).

Uluslararası kuruluşların ve hükümetlerin, siber saldırıların neden olduğu risklerin etkilerini anlamak için girişmiş olduğu tanımlama gayretlerinin öneli olan iki örneğinden birisi Amerika Birleşik Devletleri' ne, diğeri ise Şangay İşbirliği Örgütü'ne ait olmaktadır. Amerika Birleşik Devletlerin' de Birleşik Devletler Siber Komutanlığı kurulduktan sonra 2011'de komutanlığın siber operasyonlarda kullanılmak üzere yayımlamış olduğu sözlükte siber saldırı tanımı şöyledir; Bilgisayarın ve bilgisayarlarla alakalı ağların veya sistemlerin kullanımı aracılığıyla

hedef faktörün kritik siber sistemlerinin, mal varlığımı, işlevlerini bozma veya tahrip etme maksatlı düşmanca hareket şeklinde ifade edilmektedir. Bu tanımlamanın esas özelliği siber saldırıları, kritik siber sistemlere zarar vermesi, düşünülen düşmanca eylemlerle kısıtlanmasıdır (Hathaway vd.,2012).

Çetin, Gundak ve Çetin(2015) siber saldırıyı bilişim sistemlerinde yaşanan gelişimler, internet altyapısının her geçen gün büyümesi siber uzay ile toplumsal hayatta yeni bir boyut açmış ve yaşamın bir parçası haline gelmiştir. İçeriğinde sürekli artan bilgiyi bulunduran ve büyüyen bu boyut hırsızlığın, dolandırıcılığın, casusluğun, şiddetin, istismarın da hedef alanı olduğu olarak tanımlarken Kurnaz ve Önen 2016-2019 Ulusal Siber Güvenlik Stratejisi (2016)'ye göre siber saldırı, ulusal siber uzayda yer alan bilgi ve iletişim teknolojilerinin gizlilik, bütünlük ya da ulaşılabilirliğini yok etmek maksadıyla, siber uzayın herhangi bir yerindeki kişi ya da sistemler tarafından kasıtlı olarak gerçekleştirilen işlemdir şeklinde tanımlamaktadır.

Fiziksel suç ve saldırılardan farklı olarak siber saldırgan için teknik bilgi gerekmektedir. Ancak gelişmelerin olumsuz bir yönü olarak da nitelendirebileceğimiz, ihtiyaç duyulan teknik bilginin her geçen gün azalması bilinçsiz kullanıcılar tarafından da saldırı gerçekleştirilmesine imkân tanımaktadır. Siber ortamda bir saldırı yapmak için ihtiyaç duyulan envanterler genellikle bir ağ bağlantısı ve bilgisayardan ibaret olacak kadar ucuz ve erişimi kolay olabilirken bu mağdur taraf bakımından yüksek bedeller ortaya çıkarabilmektedir (Gürkaynak ve İren, 2011).

Bir siber saldırının gerçekten ne olduğunu ifade edebilmek için ilk olarak gerçekleştirilen saldırının geleneksel saldırıdan ayrılan yönleri belirlenmelidir. Genellikle siber saldırılar çok hızlı bir şekilde meydana gelmekte ve bazen saldırıya uğrayan taraf henüz ne olduğunu anlamadan saldırı ile karşılaşmaktadırlar. Neredeyse ışık hızında meydana gelen siber saldırılarda kinetik silahlar yerine dijital aletler kullanılmaktadır. Kullanılan araçlar önemlidir çünkü bu yolla siber saldırılar, geleneksel saldırıların olağan fiziği ile sınırlandırılamaz duruma gelmektedir. Fiziki sınırlardan bağımsız bir hale gelmesi aynı anda birden fazla konumda gerçekleşebileceğinin de kanıtıdır. Yani aynı siber saldırı birden fazla hedef için yapılabilmektedir (Singer ve Friedman, 2014).

Bununla birlikte bazı siber saldırıların neticeleri, kitle imha silahları içeren saldırıların neden olduğunu yıkım ile benzerlik göstermektedir. Ek olarak geleneksel

saldırıların maliyetine oranla siber saldırıların maliyeti çok daha düşük olmaktadır. Aynı zamanda, siber uzayın kendisine özgü karakterini meydana getiren atfetmenin zorluğu siber saldırıların arkasında bulunan aktörün bulunmasını zor hale getirmekte ve saldırının kaza ile mi bilinçli olarak yapıldığı hususunda karar vermeyi daha zor bir hale getirmektedir. Siber saldırılarda öncelikle hedef bir bilgisayarı ve içerisindeki verileri hedef almaktır. Saldırının neticeleri fiziksel hasar durumu meydana getirse de hasar ilk olarak dijital ortamdaki bir olaydan ibarettir (Singer ve Friedman, 2014).

Geleneksel ve siber saldırı metotları arasındaki bu farklılıklardan hareketle siber saldırı konusunda daha genel bir tanım oluşturma çabalarını karşılayan dört genel özellik olduğu söylenebilir. Bu özelliklerden birincisi "bir siber saldırı bir bilgisayar ağının işlevlerini siyasal ya da ulusal güvenlik maksadıyla baltalamak için yapılan herhangi bir eylemdir" biçiminde ifade edilebilir. İkinci özellik "bu terim, eylemin aktif olarak yürütülmesi gerektiğini ifade etmektedir: saldırı ya da aktif savunma". Aktif savunma, saldırı yapan bilgisayar sistemlerine saldırmak ve mevcut siber saldırıları durdurmak için tasarlanmış elektronik karşı tedbirleri içermektedir. Belirtmek gerekir ki hükümetlerin hem aktif hem de pasif savunmaları kullanması muhtemeldir ve ikisi birlikte çalışacak biçimde tasarlanmaktadır. Üçüncü özellik saldırının yöntemi ve hedefini de barındıran "bir siber saldırı etkisiz hale getirme, mantık bombaları, kesme vb. gibi yöntemlerle gerçekleştirilebilir fakat bir bilgisayar ağının fonksiyonunu baltalamayı ya da bozmayı amaçlıyor olması gerekmektedir" şeklinde ifade edilebilir. Dördüncü özellik ise siyasal veya ulusal güvenlik çerçevesinde hedefe yöneliktir ve "siyasi veya ulusal güvenlik amacı, siber saldırıyı basit bir suçtan ayırmaktadır" şeklinde ifade edilmektedir. Eylemin tanımının diğer tüm unsurları yerine getirildiği durumlarda bir aktörün siber alanda gerçekleştirdiği herhangi bir saldırgan eylem, ulusal güvenliği etkilediğinden bir siber saldırıdır. Bu durum devlet dışı bir aktör tarafından gerçekleştirilse de aynı durum geçerli olmakta ve işlenen siber suç, siber saldırı kategorisinde değerlendirilmektedir (Hathaway vd., 2012).

2.7. Konaklama İşletmelerinde Bilgi Yönetimi ve Güvenliği

Konaklama işletmelerinde bilgi güvenliğinin kapsamı, işletmenin bilgi varlıklarını ve o bilgilerin bulundukları alanları kapsamaktadır. Aynı zamanda, bilişim

teknolojilerinin konaklama işletmelerindeki kullanım alanlarının artışı ile verilerin güvenliğinin kapsamı bu işletmelerde daha da genişlemektedir. Bu nedenle, ilk olarak konaklama işletmelerinde bilgi teknolojilerinin kullanım alanlarından bahsedilmektedir. Bilişim teknolojilerinin konaklama endüstrisinde kullanımı öncelikle ön büro biriminde başlamıştır. Misafirlerin giriş işlemleri, kayıt, rezervasyon, misafir sicil kayıtlarının depolanması, odalar ile alakalı işlemler, kasa işlemleri, istatistik çıkarma, raporlama ve santral hizmetleri gibi ön büro bölümünde yapılan işlemler, bilgisayar yardımıyla çok daha hızlı, pratik ve doğru biçimde yerine getirilmektedir (Çakmakçı, 2012).

Elektronik danışma hizmeti müşterilere gereksinim duydukları zaman doğru ve geçerli bilgileri elde etmeye yarayan hizmetler olarak bu konuya örnek gösterilebilir. Bilgiler TV ekranında gösterilebilmekte ve hava durumlarını kontrol etme, restoranların yerini bulma, ziyaret yerlerinin seçimi ve hatta bir tur haritası çıkarmak için menüden seçim yapabilme imkânına sahip olmaktadır. Bilgi teknolojileri, akıllı otel odasının oluşturulmasını ve tasarımında sıklıkla kullanmaktadır. Akıllı sistemler sayesinde müşteriler; oda sıcaklığı, hava temizliği, ışıklar ve sesleri kendi zevk ve isteklerine göre düzenleyebilmektedir (Pelit, 2009).

Bilişim teknolojisinin yoğun olarak kullanıldığı alanlar; muhasebe uygulamaları, enerji tasarruf sistemleri, mini bar kontrol sistemleri, kartlı kapı sistemleri, otomatik santral uyandırma, sesli mesaj sistemi, kablolu ve kablosuz internet bağlantısı, oda içi mültivizyon ve eğlence sistemleri gibi hizmetlerdir (Çakmakçı, 2012).

Bilgi teknolojilerinin yoğun olarak kullanıldığı alanlar, konaklama işletmelerinde bilgi güvenliği bakımından risk oluşturan alanları meydana getirmektedir. İşletmelerin bilgi güvenliğini riske atacak unsuları iç kaynaklı ve dış kaynaklı tehdit unsurları olmak üzere iki kategoride inceleyebiliriz.

Dış kaynaklı tehdit faktörleri, siber saldırılar, firmanın müşterilerinin sebep olduğu güvenlik açıkları, işletmenin kendi içerisinde gideremediği bir takım işleri dış kaynak kullanımı yoluyla çözmeye çalışması gibi unsurlar meydana getirmektedir. İç kaynaklı tehdit unsurları ise, işletme personelinin bilgi güvenliği hususunda bilgisiz olması, işletmede kullanılan otomasyonları ve yazılımların yeterli güvenlik yapısına sahip olmaması, donanımsal olarak eksikliklerin olması, işletmede lisanssız programların kullanılması gibi etkenlerdir. Konaklama işletmelerinde internet altyapısının satış ve rezervasyon için kullanılmaya başlanmasıyla birlikte elektronik

alanlarda güvenlik riskleri de oluşmaya başlamıştır. Konaklama işletmelerinde bilgi teknolojileri konusunda çalışanlara eğitim verilmesi faydalı olacaktır (Çakmakçı, 2012).

Turistik bölgelerde faaliyetlerini sürdüren konaklama işletmeleri çoğunlukla belirli sezonlarda hizmet vermektedirler. Bu sebeple personel devir hızı yüksek düzeydedir. Personel devir hızının yüksek seviyede olması işletme adına bir riski kendisiyle getirmektedir. Sezon içinde çalışmış ve işletme ile sorun yaşan bir personel, ayrılırken müşterilere ait bilgileri ya da işletmenin özel yazışmalarını ve anlaşmalarını ifşa edebilir bu sayede işletmenin zarar görmesini sağlayabilir (Çakmakçı, 2012).

Elektronik faaliyet gösteren işletmeler, faaliyetlerini elektronik ortamda yürütebilmek için bir web sitesine gereksinim duymaktadır. Web siteleri elektronik ortamda bir tanıtım aracı, iletişim platformu, mağaza ya da bir pazarlama aracı olarak kullanılmaları gibi pek çok fonksiyonlara sahiptir. Web sitesi kurulumu ve tasarımı ayrı bir uzmanlık gerektirdiğinden işletmeler çoğunlukla bu gereksinimi kendi bünyelerinde gideremekte ve dış kaynak kullanımı yapmaktadırlar. Bu kullanımda işletmeler özel bilgilerini dışarıdaki bir işletme ya da bireye vermek zorunda olduğundan bu hususta bir güvenlik riski meydana gelmektedir. Diğer bir şekilde, işletmelerde teknik bölüm mevcut değilse arızalanan bilgisayarlar ve elektronik aygıtlar için de dış kaynak kullanımı yapılmaktadır. Bu yolla işletmelerin cihazları başkalarının eline geçmekte ve kötü niyetli kişiler ya da işletmeler tarafından barındırdıkları bilgilerin çalınmasına, bütünlüğünün bozulmasına sebep verebilmektedir (Yeşilyurt, 2015).

Ödeme sistemleri işletmeler adına en önemli güvenlik konularının başında gelmektedir. Kredi kartı ile ödeme sistemleri, müşterileri otellerin farklı bölümlerinde yapmış oldukları harcamaların sisteme girilmesi, bu harcamaların ön büro müşteri hesaplarında anında görüntülenebilmesi ve işletme içerisinde koordinasyonu sağlamaktadır. Sanal POS sistemi ise internet üzerinden talimat verilerek bir ürün ya da hizmetin, alıcı ve satıcının bir araya gelmesinin güç olduğu durumlarda satın alım işlemini mümkün kılan bir yazılım sistemidir. Müşterilerin kredi kartı ya da nakit kartı bilgilerini sisteme girerek çevrimiçi olarak elektronik ortamda ödeme yapmalarına imkân sunmaktadır. Bu işlem esnasında fiziki bir cihaza ihtiyaç duyulmamaktadır. Müşterilerin kart bilgilerinin kopyalanmaması ve

çalınmaması adına işletmelerin hem fiziki hem de elektronik ortamlarda ödeme sistemlerini güvenli bir hale getirmeleri gerekmektedir. Elektronik ortamda bu işlemlerin güvenliği için 3D güvenli ödeme sistemi kullanılmaktadır (Yeşilyurt, 2015).

Konaklama işletmelerinde internet ağları, lobide ve odalarda sunulmaktadır. Burada bir ortak ağ kullanımı söz konusu olduğundan tüketicilerin bilinçsiz ya da kötü niyetleri internet hizmetleri kullanımı işletme adına risk teşkil etmektedir. Ortak ağdan gerçekleştirilecek bilinçsiz işlemler, kullanılan ağı saldırılara karşı savunmasız hale getirebilmekte ve işletmelerin bilgi sistemlerinin zarar görmesine neden olabilmektedir. Pek çok konaklama işletmesinde müşterilere verilen kablosuz ağ şifresi ortak bir şifre olmaktadır. Böylece otelden çıkış yapan müşterinin şifreyi dışarıda paylaşması söz konusu olabilmekte ve bu durum da bir güvenlik açığı riskini ortaya çıkarmaktadır.

Konaklama işletmelerinde bilgi güvenliği açığı meydana getirebilecek başlıca alanlar; personellerden kaynaklanan açıklar, misafirlerden kaynaklanan açıklar, yazılım ve donanım problemlerinden ileri gelen açıklar, dış kaynaklardan gelen açıklardır. Bilgi güvenliğinde en önemli faktör, en zayıf halka olmaları sebebiyle kullanıcılar yani insanlardır. Fakat gözlemlendiğinde güvenlik açıklarını saptamaya ve bu açıklara dönük tedbirler almaya yetkili olan insanlar yöneticilerdir. Yöneticiler personelleri bu açıklar konusunda bilgilendirecek ve yönetecek olan kişilerdir. Bu sebeple yöneticilerin bilgi güvenliği farkındalığına sahip olması konaklama işletmeleri adına büyük önem ifade etmektedir (Şahinaslan,2013).

2.8. Konaklama İşletmelerinde Siber Güvenlik Yaklaşımları

Bir konaklama işletmesinin, siber riskleri en aza indirgemek adına yürütebileceği pek çok yaklaşım bulunmaktadır. Siber güvenliğin sorumluluğunun yalnızca bilişim teknolojileri bölümüne devredilmesi, sınırlı bir başarıyı getirecektir. Bilişim teknolojisi güvenliğinin en iyi uygulamalarını kullanmak dahi -bu yaklaşım bütün olası saldırıların riskini kapsamadığından mevcut ihtiyaçların karşılanmasında olası bir durum olmamaktadır. Daha kapsamlı bir yaklaşım, bütün işletme genelinde bütünsel bir güvenlik programı yürütmektir. Bu yaklaşım ile başarıya ulaşılması daha olası bir durumdur (https://www.guvenlikonline.com/).

Siber güvenlik uygulamaları işletmedeki personellerin tamamının dikkatini çekmeli ve sadece genel farkındalık eğitimi yoluyla değil, aynı zamanda her bir pozisyon ve bölüm için özel bilgi ve yöntemleri de barındırmalıdır. Pek çok kuruluşun türüne göre destek sağlayacak önerilerden bazıları şöyledir;

- **Personel Eğitimi Düzenlenmesi:** İşletmenin her bir üyesi temel siber güvenlik eğitimi ve farkındalık eğitimi almış olmalıdır. Pek çok başarılı ağ ihlali, kötü amaçlı yazılımı yükleyen bir bağlantı barındıran 'sosyal olarak tasarlanan' bir e-posta ile başlamaktadır. Aynı şekilde, kimlik avı e-postalarını da anlamış olmalıdırlar (Şahinaslan,2013).
- **İyi Parola Yönetimi Uygulamaları Benimsenmesi:** Şifrelerin düzenli bir şekilde değiştirildiğinden ve varsayılan parolaların tekrar kullanılmadığından emin olmak adına bir parola yönetim ilkesi oluşturulmalı ve uygulanmalıdır. En iyi parola uygulamaları karmaşıklık üzerinden uzunluğa vurgu yapmaktadır ve daha uzun şifreler her durumda daha iyidir. Aynı zamanda, başarısız giriş girişimleri bir günlüğe kaydedilmeli ve sınırlandırılmalıdır (Şahinaslan,2013).
- **Yazılımlar Güncel Tutulmalıdır:** Her ne kadar basit bir şey olarak görülse de, ürün yazılımını da dâhil olmak üzere bütün yazılımların her zaman güncellenmesini yapmak oldukça önemlidir. Mümkünse bu işlem otomatik bir hale getirilmelidir (Şahinaslan,2013).
- **Erişim Ayrıcalıkları Yönetilmelidir:** Her bir ağ kullanıcısı – idareciler, operatörler, kullanıcılar, sıradan kullanıcılar ve ziyaretçiler de dâhil olmak üzere- atanan fonksiyonlar için gereken haklara ve ayrıcalıklara sahip olmalı ve daha fazla erişim yetkisi tanınmamalıdır (Şahinaslan,2013).

Bu önerilerin tamamı, siber riskleri hafifletmek için bütün organizasyonlarda uygulanabilecek bütünsel bir yaklaşımın temel unsurlarıdır. Belirli koşullar için sağlanabilecek fazlasıyla ek adım bulunmakta, ancak iyi bir başlangıç noktası için belirtilen yöntemler uygulanabilir (Şahinaslan,2013).

2.9. Test ve Otomasyon

Siber riskleri azaltma stratejilerinin diğer önemli yönü olan testler, bütün kullanıcılara, sistem bileşenlerine ve verilere erişim için benzersiz bir kimlik atandığını onaylamak adına yapılan manüel testleri kapsamaktadır. İlaveten otomatik ağ testi, bağlı cihazların tamamının periyodik keşfini barındıran bir dizi faktör için kullanılmaktadır. Bu tür testlerden elde edilen raporlar, kullanıcı kimliği, tarih ve saat, olay türü ve daha fazlası da dâhil olmak üzere bütün sistem bileşenleri için denetim yollarını içermektedir (Irmak ve Erkek, 2018).

Güvenlik ve fiziksel gözetim fonksiyonlarını otomatik hale getirmek, siber riskleri azaltmak adına ek bir yöntem olarak kullanılabilmektedir. Örneğin, işletmeler ile birlikte, havalimanları, hastaneler, belediyeler ve toplu taşıma sistemleri siber bir ihlal sonucu olarak video gözetim kesintileri yaşayabilmektedir. İşletmeler, kameraların otomatik olarak güncellenmesini sağlayan otomatik bir kamera ürün yazılımı güncelleme yöneticisi kullanmalıdır. Bu sistem, her bir kameranın manüel olarak güncellenmesi için harcanacak zamandan önemli miktarda tasarruf edilmesini sağlamakta ve aynı zamanda en son güncellemeler sayesinde her bir sistemin güncel kalması sağlanmaktadır (Erol, Ceyhan ve Sağıroğlu)

Siber riskleri ortadan kaldırmak adına otomasyon kullanmak, verimli bir alan oluşturmak için iş akışlarını basit hale getirmek gibi pek çok fayda sağlamaktadır. Organizasyon yalnızca güvenlik bakımından güçlenmez, aynı zamanda daha uygun maliyetli bir hal alır. Diğer bir fayda ise, makinelerin insanlara oranla çok daha az hata yapma oranına sahip olmalarıdır. Otomasyon, hata eğilimi insan faktörünü sürecin bir kısmından kaldırmaktadır (Güneş, 2019).

Otomasyon, güvenlik problemlerinin otomatik olarak belirlendiği ve düzelttiği video analiz uygulamalarının kullanımını da içerisine alabilir. Aynı zamanda oluşabilecek güvenlik problemlerini çözmek adına daha gelişmiş bir analizle veri toplanmasını da sağlamaktadır. Son olarak otomatik bir sistem ile sistem, güvenlik protokollerini ihlal edecek problemleri izlemek üzere programlandığı için, çeşitli yönetmeliklere uyum konusunda herhangi bir şüpheyi de ortadan kaldırmaktadır (https://www.guvenlikonline.com/)

ÜÇÜNCÜ BÖLÜM

KONAKLAMA İŞLETMELERİNİN SİBER GÜVENLİK YÖNETİM YAKLAŞIMLARININ DEĞERLENDİRİLMESİ

Bu bölümde, İzmir İlinde faaliyet gösteren dört ve beş yıldızlı konaklama işletmelerinin siber saldırılara karşı aldıkları önlemler değerlendirilmiş ve ölçüm aracı ile elde edilen veriler analiz edilip araştırma bulgularına yer verilmiştir.

3.1. Araştırmanın Amacı ve Önemi

Teknolojide yaşanan gelişmeler sonucunda turizm sektörü yenilikçi bir iş alanı olan dijitalleşme ile bir dönüşüm geçirmiştir. Dijitalleşme turizm sektörüne çok farklı bir dinamizm katarken bir yandan da siber güvenlik açısından savunmasız bir hale getirmiştir (Fragniere ve Yağcı, 2021). Bu nedenle birçok turizm işletmesi hem operasyonları hem de itibarlarını zedeleyecek siber saldırılarla mücadele etmektedir. Turizm sektörü, Covid-19pandemisinden en fazla etkilenen sektörlerden biri olmasına rağmen, beklenenden daha hızlı bir şekilde toparlanmaya başlamıştır. 2020'de pandeminin zirvesindeyken bile, turizm endüstrisinin Gayri Safi Yurt İçi Hâsılat' a katkısı 121,9 milyar dolar olmuştur. Sektörde yaşanan büyüme siber suçluların dikkatini çekmekte ve her geçe gün yapılan siber saldırılar artmaktadır (Bhardwaj, 2022).

Phocus Wire tarafından 2022 yılında yayınlanan bir rapora göre, Birleşik Krallık, Amerika Birleşik Devletleri ve Avrupa'daki tüm sektördeki Küçük ve Orta Ölçekli (KOBİ) İşletmelerin %72'sinin en az bir kez siber saldırıya maruz kaldıkları görülmektedir. Turizm sektöründeki KOBİ'lerin %80'inin siber saldırılara karşı savunmasız olduğu ve bu saldırılara karşı riski azaltmaları gerektiği belirtiliyor. Ancak sadece KOBİ'ler siber saldırılara maruz kalmıyor. Carnival Corporation, Carnival CruiseLine, Princess Cruises, Holland America Line, Seabourn ve Cunard olmak üzere 10 marka altında sefer yapan ve dünyanın en büyük kurvaziyer hattı operatörü 2020 yılında siber saldırıya uğramıştır (Fox, 2022). Turizm işletmelerin en fazla maruz kaldığı siber saldırı türleri e-dolandırıcılık, kötü amaçlı yazılım ve fidye yazılımı olmaktadır (Hussain, 2021).

Yukarıda sıralanan gerekçeler doğrultusunda bu çalışmanın amacı otel işletmelerinin siber saldırılara karşı algılarını ölçmek ve mevcut durumlarını ortaya koymaktır. Bu

çalışmanın araştırma sorusu şöyledir; “Profesyonel olarak yönetilen 4 ve 5 yıldızlı otel işletmelerinde siber güvenlik konusunda işletmelerin aldıkları önlemler nelerdir? Bu araştırma sorusundan hareketle aşağıdaki hipotezler geliştirilmiştir:

H_1: İşletmenin türüne göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_2: İşletmenin siber saldırıyla karşılaşma durumuna göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_3: Ticari faaliyetlerde internete bağılı olma derecesine göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_4: Ticari faaliyetlerde internete bağılı olma derecesine göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_5: Bilişim sistemlerinde 24 saatlik bir aksama yaşanması durumunda 24 saat süresince ticari faaliyet olan satışların etkilenme derecesine göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_6: İşletmenin olası bir siber saldırıya karşı önlem alınmasına göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_7: İşletme tarafından bilgisayar ağlarını korumak için kullanılan ağ güvenliği araçları ve tekniklerine göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_8: İşletmenin olası bir siber saldırıya karşı önlem alınmasına göre siber güvenlik yaklaşımı farklılık göstermektedir.

H_9:İşletmedeki bilgisayar ağı güvenliğine yönelik mevcut tehditlere göre siber güvenlik yaklaşımı farklılık göstermektedir.

3.2. Araştırmanın Evren ve Örneklemi

Araştırma evrenini Ocak 2021 yılında İzmir İl Kültür ve Turizm müdürlüğünden alınan bilgiler doğrultusunda İzmir ilinde hizmet gösteren 77 adet 4 ve 5 yıldızlı konaklama işletmelerinin bilgi işlem bölümünden sorumlu yöneticileri oluşturmaktadır. Araştırmada örnekleme yöntemlerine başvurulmadan tamsayım yöntemi ile evrenin tamamına ulaşmak hedeflenmiştir. Evrende bulunan 77 adet işletme yöneticileriyle iletişime geçilmiş ve araştırmaya dâhil olmaları istenmiştir. Araştırma verileri 2021 Ocak-Şubat aylarında toplanmıştır. Evrende yer alan tüm işletmelere ulaşmak için farklı yöntemler kullanılmıştır. Öncelikle hepsi telefon ile aranmış ve randevu vermeyi kabul eden işletmelerle doğrudan anket formu

uygulanmıştır. Telefonla ulaşılamayan işletmelere anket formları mail olarak gönderilmiştir. Ancak çalışmanın yapıldığı dönemde bazı otel işletmeleri Covid-19 pandemisi nedeniyle faaliyetleri durdurdukları için onlara ulaşılamamıştır. Bu nedenle 77 işletmeden 47 işletmeden veri elde edilmiştir. Anketlerin cevaplanma oranı %67'dir.

3.3. Veri Toplama Araçları

Araştırma verilerini toplamak için oluşturulan anket formu iki kısımdan oluşmaktadır. İlk kısımda siber güvenlik yaklaşımına ilişkin sorular yer almaktadır. İkinci kısımda ise demografik sorular yer almaktadır. Çalışmada konaklama işletmesi yöneticilerin siber güvenliğe verdikleri önemi ve aldıkları önlemleri ölçmek amacıyla, Japonya Ticaret ve İnovasyon Bakanlığı'na Japonya Bilgi Teknolojileri Özendirme Ajansı'nın (IPA) Bilgi Güvenliği Yöntemi Kıyaslama Sistem'inden (ISM – Benchmark) uyarlanılarak hazırlanan ölçek kullanılmıştır. Siber Güvenlik Yaklaşımı Ölçeği, 29 sorudan oluşmaktadır ve 5'li Likert tipi ölçekle ölçülmüştür. Ölçek soruları 1='Hiç katılmıyorum/Hiç uygulanmıyor', 2='Kısmen katılıyorum/Kısmen uygulanıyor', 3='Çoğunlukla katılıyorum/Çoğunlukla uygulanıyor', 4='Katılıyorum/Uygulanıyor' ve '5=Tamamen Katılıyorum/ Tamamen Uygulanıyor' şeklinde ifade edilmiştir.

3.4 Verilerin Analizi

Araştırmadan elde edilen veriler uygun istatistik programıyla değerlendirilmiştir. Ankete katılan kişilerin verdikleri cevaplara ilişkin sonuçları belirlemek amacıyla frekans ve yüzde analizleri belirlenmiştir. Çalışmada ele alınan ölçeklere güvenirlik düzeylerini tespit etmek için Cronbach's Alpha analizi yapılmıştır. Öncelikle ele alınan verilerin normallik ve homojenlik sınamasıyla çarpıklık basıklık kontrolleri gerçekleştirilmiştir. Örneklem büyüklüğünün yeterli olmaması nedeniyle elde edilen veriler non-parametik testler ile analiz edilmiştir. Bu kapsamda verilerin işletme özelliklere göre farklılık gösterip göstermediğini sınamak amacıyla Mann-Whitney U ve Kruskal Wallis testi uygulanmıştır. Kruskal Wallis analizi neticesinde anlamlı farklılığın hangi gruplardan kaynaklandığının tespit edilmesi için Post-Hoc testlerine başvurulmuştur.

3.5. Bulgular

Araştırma kapsamında yapılan test sonuçları Tablo 1'de verilmiştir.

Tablo 1. Araştırma kapsamında yapılan test sonuçları

	N	Frekans	**Yüzde (%)**
İşletme Türüne Göre Dağılımı	**47**		
4 Yıldızlı		**10**	**21.3**
5 Yıldızlı		**37**	**78.7**
İşletmenin ve Misafirlerin Gizli Tutulan Bilgilerine Ulaşım Sağlama İzni Olan Çalışan Sayılarına Göre Dağılımı	**47**		
1-4 arası		**6**	**12.8**
5-8 arası		**39**	**83.0**
9-13 arası		**1**	**2.1**
14 ve üzeri		**1**	**2.1**
İşletmelerin Ticari Faaliyetlerde İnternete Bağımlı Olma Derecesine Göre Dağılımı	**47**		
%50-%75 arası		**4**	**8.5**
%75 ve daha fazla		**43**	**91.5**
Sistemlerinizde 24 Saatlik Bir Aksama Yaşanması Durumunda 24 Saat Süresince Ticari Faaliyet Olan Satışların Etkilenme Derecesine Göre Dağılımı	**47**		
Satışlarda aksama meydana gelir		**12**	**25.5**
Eski yöntemler kullanılarak çalışmalara devam edilir		**10**	**21.3**
Çevrimiçi sistemler kullanılarak yapılan satışlar durur ve mevcut hesaplara erişim problemleri yaşanır		**10**	**21.3**
İş takibi zorlaşır		**2**	**4.4**
Yedekleme programları kullanmaktayız.		**6**	**12.8**
Misafir kayıpları ve şikayetleri meydana gelir.		**3**	**6.4**
Teknik aksaklıklardan oluşacak mali kayıplar meydana gelir		**4**	**8.5**
İşletmenin Olası Bir Siber Saldırıya Karşı Aldığı Önlemlere Göre Dağılımı	**47**		
Anti virüs programları		**10**	**21.3**
Veri koruma programları		**15**	**31.9**
Siber güvenlik şirketleri		**9**	**19.1**
Saldırı tespit sistemleri ve güçlü tanılama sistemleri		**2**	**4.3**
Şifreleme programları		**6**	**12.8**
Ağ koruma sistemleri		**3**	**6.4**
Merkezi bilgi işlem bölümleri		**2**	**4.3**
İşletmedeki Bilgisayar Ağı Güvenliğine Yönelik Mevcut Tehditlere Göre Dağılımı	**47**		
Siber saldırılar		**21**	**44.7**
Misafirlerin gizli bilgilerine erişilmek istenmesi		**26**	**55.3**

İşletmeye Yapılacak Olası Bir Siber Saldırı ile Misafirlere Ait Kişisel Bilgilerin Sızdırılmasının İşletmeye Etkisine Göre Dağılımı	**47**		
Maddi ve manevi zararlar		**8**	**17.0**
Güven eksikliği		**21**	**44.7**
Olumsuz bir imaj		**8**	**17.0**
Hukuki açıdan sorunlar		**7**	**14.9**
Tercih edilebilirlik oranının azalması		**3**	**6.4**
İşletmelerin İlk Defa Siber Saldırıyla Karşılaşma Durumlarına Göre Dağılımı	**7**		
2012		**1**	**2.1**
2013		**1**	**2.1**
2017		**1**	**2.1**
2018		**1**	**2.1**
2019		**3**	**6.4**
İşletmelerin Daha Önce Bir Siber Saldırı ile Karşılaşma Durumlarına Göre Dağılımı	**47**		
Evet		**7**	**14.9**
Hayır		**40**	**85.1**
İşletmelerin Karşılaştığı Siber Saldırı Türüne Göre Dağılımı	**7**		
Virüs saldırısı		**1**	**2.1**
Veri ağları sabotajı		**3**	**6.4**
İşletmeye ait bilgilerin ele geçirilmesi		**3**	**6.4**
İşletmelerin Siber Saldırı Sonucunda Ortaya Çıkan Mali Kaybına Göre Dağılımı	**7**		
Belirsiz		**1**	**2.1**
100000$		**1**	**2.1**
Yok		**5**	**10.6**
İşletmelerin Siber Saldırıdan Etkilenme Derecesine Göre Dağılımı	**7**		
Sistemsel aksaklıklar		**1**	**2.1**
Kısa sureli erişim problem		**3**	**6.4**
Olumsuz imaj		**1**	**2.1**
Veri kayıpları		**2**	**4.3**
Siber Saldırı Sonrasında Saldırılara Karşı Alınan Ek Önlemlere Göre Dağılımı	**7**		
Bilinmiyor		**1**	**2.1**
Program seviyesini arttırma		**4**	**8.5**
İlave koruma programları kullanma		**1**	**2.1**
Şifreleme programları		**1**	**2.1**
Siber Saldırı Sonrasında Bildirim Yapılan Kuruluşa Göre Dağılımı	**5**		
Savcılık		**1**	**2.1**
Cumhurbaşkanlığı İletişim Merkezi		**1**	**2.1**

Emniyet birimleri		**1**	**2.1**
Adli birimler		**1**	**2.1**
Bilişim Teknolojileri Kurumu		**1**	**2.1**

Tablo 1. incelendiğinde işletmelerinin %21.3' ünün 4 yıldızlı, %78.7' sinin ise beş yıldızlı olduğu görülmektedir. İşletmenin ve misafirlerin gizli tutulan bilgilerine ulaşım sağlama izni olan çalışan sayılarına göre dağılım incelendiğinde %12.8' sinin 1-4 arası, %83'ünün 5-8 arası, %2.1'inin 9-13 arası, %2.1'inin 19 ve üzeri çalışanı olduğu görülmektedir. Ticari faaliyetlerde internete bağımlı olma derecesine göre dağılım incelendiğinde %8.5' inin %50 - %75 arasında ve %91.5'inin %75 veya daha fazla internete bağımlı olduğu görülmektedir. Bilişim sistemlerinde 24 saatlik bir aksama yaşanması durumunda 24 saat süresince ticari faaliyet olan satışların etkilenme derecesine göre dağılım incelendiğinde %25.5' i satışlarda aksama meydana geleceğini, %21.3'ü eski yöntemlerle çalışmaların sürdürüleceğini, %21.3'ü çevrimiçi satışların yapılamayacağını ve mevcut hesaplara erişim sıkıntısı yaşanacağını, %12.8' i yedekleme programı kullandıklarını, %8.5' i teknik aksaklıklardan oluşacak mali kayıplar meydana geleceğini, %6.4'ü misafir kayıpları ve şikayetleri meydana geleceğini ve %4.3' ü iş takibinin zorlaşacağını belirtmektedir. İşletmenin olası bir siber saldırıya karşı aldığı önlemlere göre dağılım incelendiğinde katılımcıların %21.3' ünün anti virüs programları, %31.9' unun veri koruma programları kullandığı, %2.1' inin dış kaynaklardan faydalandığı, %4,3' ünün saldırı tespit sistemleri ve güçlü tanılama sistemleri, %12,8'inin şifreleme programları, %6.4' ünün ağ koruma sistemleri kullandığı, %17' sinin siber güvenlik şirketleriyle çalıştığı, %4.3' ünün merkez bilgi işlem bölümüyle çalıştığı görülmektedir. İşletmedeki bilgisayar ağı güvenliğine yönelik mevcut tehditlere göre dağılım incelendiğinde %47.7' sini siber saldırılar ve %55.3' ünün misafirlerin gizli bilgilerine erişilmek istenmesiyle tehdit edilmektedir.

İşletmeye yapılacak olası bir siber saldırı ile misafirlere ait kişisel bilgilerin sızdırılmasının işletmeye etkisine göre dağılım incelendiğinde %17' sinin maddi-manevi zarara uğrayacağı, %44.7' sinde işletmeye karşı güven eksikliği oluşacağı, %17' sinde işletmeye karşı olumsuz bir imaj oluşacağı, %14.9' unun hukuki açıdan sorunlar yaşayacağı, %6.4' ünün tercih edilebilirlik oranının azalacağı görülmektedir. İşletmelerin daha önce bir siber saldırı ile karşılaşma durumlarına göre dağılım

incelendiğinde işletmelerin %14.9’ unun daha önce bir siber saldırıya uğradığı, %85.1’ inin ise daha önce bir siber saldırıya uğramadığı görülmektedir. İşletmelerin ilk defa siber saldırıyla karşılaşma durumlarına göre dağılım incelendiğinde işletmelerin %2.1’ inin 2012, %2.1’ inin 2013, %2.1’ inin 2017, %2.1’ inin 2018 ve %6.4’ ünün 2019 yılında ilk defa siber saldırıya uğradığı görülmektedir. İşletmelerin karşılaştığı siber saldırı türüne göre dağılım incelendiğinde işletmelerin %2.1’ inin veri saldırısına, %6.4’ ünün veri ağları sabotajına, %6.4’ ünde ise işletmeye ait bilgilerin ele geçirilmesi. İşletmelerin siber saldırı sonucunda ortaya çıkan mali kaybına göre dağılım incelendiğinde işletmelerin %2.1’ inde mali kaybın belli olmadığı, %2.1’ inde 10000$ olduğu ve %10.6’ sında ise mali kaybın olmadığı görülmektedir. İşletmelerin siber saldırıdan etkilenme derecesine göre dağılım incelendiğinde %2.1’ inde sistemsel aksaklıklar, %6.4’ ünde kısa süreli erişim sorunu, %2.1’ inde olumsuz imaj, %4.3’ ünde veri kaybı meydana geldiği görülmektedir.

Siber saldırı sonrasında saldırılara karşı alınan ek önlemlere göre dağılım incelendiğinde %2.1’ inin bilgisi olmadığı, %8.5’ inin program seviyesini arttırdığı, %2.1’ inin ilave koruma programları kullandığı, %2.1’ inin şifreleme programları kullandığı görülmektedir. Siber saldırı sonrasında bildirim yapılan kuruluşa göre dağılım incelendiğinde %2.1’ inin savcılığa, %2.1’ inin Cumhurbaşkanlığı İletişim Merkezi’ ne, %2.1’ inin emniyet birimlerine, %2.1’ inin adli birimlere ve %2.1’ inin ise Bilişim Teknolojileri Kurumu’na bildirim yaptığı görülmektedir.

3.5. Parametrik Varsayımların İncelenmesi

Verilerin analizi yapılırken parametrik testlerin mi yoksa non-parametrik testlerin uygulanmasına karar verme aşamasında yapılan analizler sonucunda parametrik test değerlerinin iyi çıktığı gözlenmiştir. Fakat her grupta bulunan denek sayısının 30’dan az olmasından dolayı çalışmada non-parametrik testler kullanılmıştır.

3.6. Güvenilirlik Analizi

Çalışma kapsamında kullanılan Siber Güvenlik Yaklaşım Ölçeği’ne ait güvenilirlik analiz sonuçları aşağıdaki gibidir;

Tablo 2. Güvenilirlik Analizi Sonuçları

Ölçekler	Cronbach's Alpha	İfade sayısı (N)
Siber Güvenlik Yaklaşımı	0.954	47
Bilgi Güvenliğinin Kurumsal Yaklaşımları	0.911	8
Çevresel ve Fiziksel Güvenlik Önlemleri	0.894	4
Bilgi Sistemleri Ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	0.921	7
Yazılım Geliştirme Ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	0.956	5
Siber Güvenlik İhlalleri Ve İş Sürekliliği Yönetimi	0.950	3

Siber Güvenlik Yaklaşım Ölçeği'nin güvenilirliğini hesaplamak için Cronbach-Alpha testi ele alınmıştır. Cronbach Alpha değerleri, 0.5 altında olduğunda ölçeğin güvenilir olmadığı söylenebilir, değer 0.7 ile 0.9 aralığın da ise ölçeğin iyi olduğu, 0.9'dan fazla olduğunda ise mükemmel derecede güvenilirdir.

Tablo 2.' de görüldüğü üzere siber Güvenlik Yaklaşım Ölçeği'ne ait Cronbach Alpha sonucu 0.954 olarak hesaplanmıştır. Buna göre ölçeğin mükemmel derecede güvenilir olduğunu söylemek mümkündür. Ölçek boyunlarının ayrı ayrı güvenilirliğine bakıldığı zaman bilgi güvenliğinin kurumsal yaklaşımları boyutunun Cronbach Alpha değeri 0.911 olarak, çevresel ve fiziksel güvenlik önlemleri boyutunun Cronbach Alpha değeri 0.894, bilgi sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri boyutunun Cronbach Alpha değeri 0.921, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü tedbirleri boyutunun Cronbach Alpha değeri 0.956 ve son olarak siber güvenlik ihlalleri ve iş sürekliliği yöntemi boyutunun Cronbach Alpha değeri 0.956 olarak hesaplanmıştır.

3.7. Siber Güvenlik Yaklaşımına İlişkin Tanımlayıcı İstatistikler

Araştırma kapsamında katılımcılara sorulan siber güvenlik yaklaşımlarına ilişkin boyutların genel ortalama ve standart sapma değerleri aşağıdaki gibidir;

Tablo 3. Siber güvenlik yaklaşımlarına ilişkin boyutların genel ortalama ve standart sapma değerleri

Boyutlar	**Ortalama**	**Standart Sapma**
Bilgi Güvenliğinin Kurumsal Yaklaşımları	**4.00**	**0.691**
Çevresel ve Fiziksel Güvenlik Önlemleri	**5.00**	**0.741**
Bilgi Sistemleri Ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri	**3.833**	**0.738**
Yazılım Geliştirme Ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü Tedbirleri	**4.046**	**0.844**
Siber Güvenlik İhlalleri Ve İş Sürekliliği Yönetimi	**3.978**	**0.899**

Ölçek: 1='Hiç katılmıyorum/Hiç uygulanmıyor', 2='Kısmen katılıyorum/Kısmen uygulanıyor', 3='Çoğunlukla katılıyorum/Çoğunlukla uygulanıyor', 4='Katılıyorum/Uygulanıyor' ve '5=Tamamen Katılıyorum/ Tamamen Uygulanıyor'

Tablo 3. İncelendiğinde katılımcıların siber güvenlik yaklaşımlarına yönelik sonuçlar incelendiği zaman en yüksek değerle (5.00) çevresel ve fiziksel güvenlik önlemleri boyutu, ikinci olarak 4.046 ile yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü tedbirleri boyutu, üçüncü olarak 4.00 ile bilgi güvenliğinin kurumsal yaklaşımları boyutları, dördüncü olarak 3.978 ile siber güvenlik ihlalleri ve iş sürekliliği yönetimi yaklaşımı ve son olarak da 3.833 değeri ile bilgi sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri boyutu olduğu anlaşılmaktadır.

3.8. Faktör Analizleri

Siber güvenlik yaklaşım ölçeğine uygulanan faktör analizi aşağıdaki gibidir;

Tablo4: Siber güvenlik yaklaşımı ölçeği faktör analizi sonuçları

FAKTÖRLER	Faktör Yükü	Özdeğer	Varyans (%)
Siber Güvenlik Yaklaşım Ölçeği		**2.771**	**81.375**
Bilgi Güvenliğinin Kurumsal Yaklaşımları (8 İfade)			
Otelimizin bilgi güvenliğine ilişkin yazılı kural ve politikaları vardır.	0.830		
Otelimiz bilgi güvenliğine ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek, tehlike ve güvenlik açıklarını dikkate almıştır.	0.881		
Otelimizin bilgi güvenliğine ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.	0.615		
Otelimiz kritik bilişim teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetir.	0.608		
Otelimiz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önlemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)	0.648		
Otelimiz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil eder.	,453		
Otelimiz tüm çalışanlara bilgi güvenliğine ilişkin yükümlülükleri açıkça bildirilmektedir.	0.900		
Otelimiz tüm çalışanlara düzenli olarak bilgi güvenliği eğitimleri vermektedir.	0.769		
Çevresel Ve Fiziksel Güvenlik Önlemleri (4 İfade)			
Otelimize ait tesislerin güvenliğini iyileştirmek için gerekli güvenlik önlemleri uygulanmaktadır.	0.595		
Otelimize ait tesislere giriş-çıkışı düzenleyen yazılı kurallar vardır.	0.662		
Otelimiz, bilgi teknolojilerine yönelik her türlü tehlikeye (doğal felaketler veya insan kaynaklı zararlar) karşı koruyu önlemler alınmıştır.	0.665		
Otelimizde, taşınabilir bilgisayar veya harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır.	0.663		
Bilgi Sistemleri Ve İletişim Ağlarının İşletim Ve Bakım Kontrolleri (7 İfade)			
Otelimiz, bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korur.	0.826		
Otelimizde bilgi teknolojileri kurulum ve kullanım süreçleri bilgi güvenliği hususları dikkate alınarak icra edilir.	0.761		
Otelimiz, verilerini uygun bir şekilde yedekler.	0.729		
Otelimiz, kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler alır.	0.595		
Otelimiz, bilişim sistemlerinin güvenlik açıklarını azaltmak için önlemler alır.	0.707		
Otelimiz, bilişim sistemlerine bağlantıları güvenli bir şekilde tesis eder. (VPN, sertifika vb.)	0.750		
Otelimiz, tüm cihaz ve aygıtların çalınma riskine karşı önlemler alır.	0.849		
Yazılım Geliştirme Ve Destek Aşamalarında Bilgi Sistemleri Erişim Kontrolü (5 İfade)			
Otelimiz, bilişim sistemlerine bağlantı için gerekli kimlik denetimlerini yapar.	0.875		

Otelimizde bilişim teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlemiştir.	0.852		
Otelimiz, yerel ağlar üzerinde yetki denetimi uygular.	0.876		
Otelimiz, yazılım geliştirme projelerinin güvenlik gereksinimlerini projelere dâhil eder.	0.847		
Otelimiz, yazılım ürünlerinin seçimi, satın alınması ve / veya bakım işlerinde güvenlik kontrolleri gerçekleştirir.	0.864		
Siber Güvenlik İhlalleri Ve İş Sürekliliği Yönetimi (3 İfade)			
Otelimiz, bilişim arızalarının kurum faaliyetlerini aksatmaması için önlemler alır.	0.700		
Otelimizde, olası bilişim kaynaklı problemler için acil eylemleri belirten yazılı prosedürler bulunur.	0.872		
Otelimizin, tüm bileşenleri kapsar nitelikte arızalara karşı mücadeleyi ele alan bir İSY (İş Sürekliliği Yönetimi) bulunmaktadır.	0.828		

Kaiser-Meyer-Olkin örneklem yeterliliği: 0.815
Bartlett küresellik testi: 1525.485

Ölçek: 1=‘Hiç katılmıyorum/Hiç uygulanmıyor’, 2=‘Kısmen katılıyorum/Kısmen uygulanıyor’, 3=‘Çoğunlukla katılıyorum/Çoğunlukla uygulanıyor’, 4=‘Katılıyorum/Uygulanıyor’ ve ‘5=Tamamen Katılıyorum/ Tamamen Uygulanıyor’

Tablo 4.’ de siber güvenlik yaklaşımı ölçeğinde bulunan sorulara ilişkin faktör analizlerinde faktör yükleri görülmektedir. Analiz sonucunda KMO ve Barlett değerleri 0.815 olarak elde edilmiştir. Tablo 4. İncelendiği zaman ölçeği beş boyuttan oluştuğu görülmektedir. Bu boyutlarda bilgi güvenliğinin kurumsal yaklaşımları boyutunda 8 adet ifade, çevresel ve fiziksel güvenlik önlemleri boyutunda 4 adet ifade, bilgi sistemleri ve iletişim ağlarının işletim ve bakım kontrolleri boyutunda7 adet ifade, yazılım geliştirme ve destek aşamalarında bilgi sistemleri erişim kontrolü boyutunda 5 adet ifade ve son olarak siber güvenlik ihlalleri ve iş sürekliliği yönetimi boyutunda 3 adet ifade bulunmaktadır.

3.9. Farklılık Testleri

Araştırmanın demografik değişkenleri ile işletme yöneticilerinin siber güvenlik yaklaşımına yönelik verdikleri sorulara farklılık testi uygulanmıştır. İşletmenin türü, daha önce siber saldırıya maruz kalma durumları gibi toplam iki değişken olduğu durumlarda bağımsız iki örneklem testinin non-parametrik karşılığı olan Mann-WhitneyU testi ve iki değişkenden fazla olduğu durumda ise Kruskal Wallis testi uygulanmıştır.

3.9.1. Mann-Whitney U Test Bulguları

İşletmenin türüne göre siber güvenlik yaklaşımı arasında farklılık olup olmadığına ait yapılan Mann-Whitney U testi sonuçları aşağıdaki gibidir;

Tablo 5. İşletmenin Türüne Göre Siber Güvenlik Yaklaşımı Arasındaki Mann-Whitney U Testi Sonuçları

	Değer
Mann-WhitneyU	92.000
Wilcoxon W	158.000
Z	-2.665
Anlamlılık değeri Asymp. Sig (2 yönlü)	0.008

Gruplama değişkeni:1.Konaklama işletmenizin türü nedir?

Tablo 6. İşletmenin Türüne Göre Siber Güvenlik Yaklaşımına İlişkin Sıra Ortalaması Sonuçları

1.Konaklama işletmenizin türü nedir?	N	Sıra ortalaması	Sıra değerlerinin toplamı
4 Yıldızlı	11	14,36	158,00
5 Yıldızlı	36	26,94	970,00
Toplam	47		

Siber güvenlik yaklaşımlarının işletmenin türüne göre anlamlı farklılık gösterip göstermediğine yönelik yapılan Mann-Whitney U testi sonuçları Tablo 5.‘ de verilmiştir. Analizler sonucunda elde edilen bulgular işletme türlerine göre siber güvenlik yaklaşımlarında anlamlı bir farklılık olduğu ($U=92.000$, $p<0.05$) görülmektedir. Sıra ortalamaları incelendiğinde dört yıldızlı konaklama işletmelerine ait sıra ortalaması (14.36), 5 yıldızlı konaklama işletmelerine alt sıra ortalaması (26.94)’dür. Bu nedenle 5 yıldızlı otel işletmelerinin siber saldırılara daha önem verdiğini söylemek mümkündür. 5 yıldızlı otel işletmelerinde bilgi işlem birimi olmakta veya bu hizmeti dışarıdan almaktadırlar. Bu nedenle 4 yıldızlı işletmelere kıyasla bu konuya daha ciddiyetle yaklaştıkları ve önlem aldıkları söylenebilir.

İşletmenin siber saldırıyla karşılaşma durumuna göre siber güvenlik yaklaşımı arasında farklılık olup olmadığına ait yapılan Mann-Whitney U testi sonuçları aşağıdaki gibidir;

Tablo 7.İşletmenin Siber Saldırıyla Karşılaşma Durumuna Göre Siber Güvenlik Yaklaşımı Arasındaki Mann-Whitney U Testi Sonuçları

	Değer
Mann-WhitneyU	84,500
Wilcoxon W	904,500
Z	-1,660
Anlamlılık değeri Asymp. Sig (2 yönlü)	,098

Gruplama değişkeni: 10.Daha önce siber saldırı ile karşılaştınız mı?

Siber güvenlik yaklaşımlarının işletmenin siber saldırıyla karşılaşma durumuna göre anlamlı farklılık gösterip göstermediğine yönelik yapılan Mann-Whitney U testi sonuçları Tablo 7. 'de verilmiştir. Analizler sonucunda elde edilen bulgular işletmelerin daha önce siber saldırı ile karşılaşma durumlarına göre siber güvenlik yaklaşımlarında anlamlı bir farklılık olmadığını ($U=84.500$, $p>0.05$) görülmektedir.

İşletmenin ticari faaliyetlerinde internete bağlı olma derecelerine göre siber güvenlik yaklaşımı arasında farklılık olup olmadığına ait yapılan Mann-Whitney U testi sonuçları aşağıdaki gibidir;

Tablo 8. Ticari Faaliyetlerde İnternete Bağılı Olma Derecesine Göre Siber Güvenlik Yaklaşımı Arasındaki Mann-Withney U Sonuçları

	Değer
Mann-WhitneyU	13,50
Wilcoxon W	23,500
Z	,006
Anlamlılık değeri Asymp. Sig (2 yönlü)	,005

Gruplama değişkeni: 3. Ticari faaliyetlerde ne derecede internete bağımlısınız

Tablo 9. Ticari Faaliyetlerde İnternete Bağılı Olma Derecesine Göre Siber Güvenlik Yaklaşımına İlişkin Sıra Ortalaması Sonuçları

3. Ticari faaliyetlerde ne derecede internete bağımlısınız?	N	Sıra ortalaması	Sıra değerlerinin toplamı
%50-%75 arası	4	5,88	23,50
%75 veya daha fazla	43	25,63	110,50
Total	47		

Siber güvenlik yaklaşımlarının işletmenin türüne göre anlamlı farklılık gösterip göstermediğine yönelik yapılan Mann-Whitney U testi sonuçları Tablo 8.'de verilmiştir. Analizler sonucunda elde edilen bulgular işletme türlerine göre siber güvenlik yaklaşımlarında anlamlı bir farklılık olduğu ($U=13.50$, $p<0.05$) görülmektedir. Sıra ortalamaları incelendiğinde ticari faaliyetlerinde internete %50-%75 oranında bağlı olan işletmelerin işletmelere ait sıra ortalaması (5.88), %75 ve daha fazla oranda bağlı olan işletmelerin sıra ortalaması (25.63)' tür. Bu sonuçlardan anlaşılacağı üzere ticari faaliyetlerinde internete %75 ve daha fazla bağlı olan konaklama işletmeler siberin siber saldırılara uğrama riskleri daha fazladır. Bu nedenle ticari faaliyetlerinde internete %50-%75 oranları arasında bağlı olan işletmelere kıyasla siber güvenlik konusuna daha fazla önem vermektedirler.

3.10. Kruskal Wallis Testleri

İşletmelerin siber güvenlik yaklaşımları ile değişkenler arasında yapılan Kruskal Wallis test sonuçları aşağıdaki gibidir;

Tablo 10. İşletmelerin siber güvenlik yaklaşımları ile aşağıdaki değişkenlerin Kruskal Wallis test sonuçları

Değişkenler	Ki kare	Anlamlılık (Asymo. Sig)
Bilişim Sistemlerinde 24 Saatlik Bir Aksama Yaşanması Durumunda 24 Saat Süresince Ticari Faaliyet Olan Satışların Etkilenme Derecesine Göre Siber Güvenlik Yaklaşımı	2.67	0.846
İşletmenin Olası Bir Siber Saldırıya Karşı Önlem Alınmasına Göre Siber Güvenlik Yaklaşımı	5.339	0.376
İşletme Tarafından Bilgisayar Ağlarını Korumak İçin Kullanılan Ağ Güvenliği Araçları ve Tekniklerine Göre Siber Güvenlik Yaklaşımı	12.209	0.024
İşletmedeki Bilgisayar Ağı Güvenliğine Yönelik Mevcut Tehditlere Göre Siber Güvenlik Yaklaşımı	0.588	0.443

Değişkenlere yönelik yapılan Kruskal Wallis testleri sonucunda Tablo 10.' da Ki Kare (Chi-square) ve Anlamlılık (Asymo. Sig) değerleri görülmektedir. Bu değerler sonucundan değişkenlerden sadece işletmeler tarafından bilgisayar ağlarını korumak için kullanılan ağ güvenliği araçları ve tekniklerine göre siber güvenlik yaklaşımı

değişkeninde siber güvenlik yaklaşımının farklılaştığı ($p<0.05$) görülmektedir. Bu farklılıkların hangi unsurlar arasında meydana geldiğini görmek üzere Post Hoc testi yapılmıştır. Yapılan bu test sonucunda (bkz Ek 2.) siber güvenlik şirketlerinden hizmet alma ile şifreli giriş sistemleri ve veri koruma programları arasında olduğu görülmektedir.

SONUÇ VE ÖNERİLER

Siber casuslar işletmelerin veya örgütlerin veri kayıtlarının ele geçirilmesine karşı büyük bir risk oluşturmaktadır. Bu bilgiler siber casuslar tarafından ele geçirmesi halinde işletmeler veya örgütler hem maddi olarak (müşteriler tarafından açılabilecek tazminat davaları) hem de manevi olarak (imaj zedelenmesi, müşteriler üzerinde güven eksiklikleri, vb.) kayıplar vererek büyük zararlara uğrayabilirler. İşletme veya organizasyonların bünyelerinde bulundurdukları bu bilgileri korumaları adına sürekli denetim sağlamaları gerekmektedir. Siber saldırıların başarılı bir şekilde sonuçlanmasının nedenleri sistem açıkları, yazılım sahtekârlıkları, kontrolsüz depolama olabileceği gibi nedenlerden biri de personel açıklarından meydana gelmektedir. Bu nedenden dolayı çalışan personellerin bu konu üzerinde ne derece bilgi sahibi olduğu ve işletmelerin personellerini bu konu hakkında ne derecede bilgilendirdiği işletme adına büyük bir önem taşımaktadır.

Konaklama işletmelerinde misafirlerin konaklama işletmelerinde yapmış olduğu ilk işlem olan rezervasyon ve son işlem olan çıkış işlemleri arasında bilişim sistemleri yoğun bir şekilde kullanılmaktadır. Bu bilişim sistemleri içerisinde işletmelerin ve misafirlerin kişisel bilgileri bunmaktadır. Bu doğrultuda yapılan bu çalışmada konaklama işletmelerindeki bilgi işlem bölümü yöneticilerinin bilgi güvenliği konularında bilgi sahibi olmalıdırlar.

Siber güvenlik olgusu temel olarak internet bağlantılı ya da bazı durumlarda bağlantısız sistemlerin, donanım, yazılım ayırt etmeksizin siber ataklardan korunması adına kullanılan ve sürekli gelişen bir sistem olarak ifade edilebilmektedir. Bilgisayar ve internet kullanımının dünya çapında giderek daha da yaygınlaşması kullanıcılarına belli kolaylıklar sağlarken kendisiyle birlikte belli tehditler de getirmektedir. İçeriğinde sürekli artan bilgiyi bulunduran ve büyüyen bu boyut hırsızlığın, dolandırıcılığın, casusluğun, şiddetin, istismarın da hedef alanı olmuş ve siber saldırı olarak alan yazınına girmiştir.

Bilgi teknolojilerinin yoğun olarak kullanıldığı alanlar, konaklama işletmelerinde bilgi güvenliği bakımından risk oluşturan unsurları meydana getirmektedir. Rezervasyon sırasında misafirlerin kimlik ve banka bilgileriyle ilgili bilgileri

sistemlerine kaydetmesi siber casusların gözde hedefi olmaktadır. Turistik bölgelerde faaliyetlerini sürdüren konaklama işletmeleri çoğunlukla belirli sezonlarda hizmet vermektedirler. Bu sebeple personel devir hızı yüksek düzeydedir. Sezon sonunda işletmeye karşı art niyet taşıyan personel konaklama işletmesinin gizli tutulması gereken bilgilerini rakip işletmelerle paylaşma riski oluşturmaktadır.

Çalışma, amaçlandığı gibi konaklama işletmesindeki bilgi işlem bölümü yöneticilerinin siber saldırılara karşı ne derecede bilgi sahibi oldukları ve ne derecede önlem aldıkları konusunda bilgiler aktarılmaya çalışılmıştır. Yöneticilerin siber saldırılara karşı önlem aldıkları ve bu bilgilere ulaşabilen kişi sayısı arttıkça oluşabilecek saldırı riski de yükselmektedir. Bilişim sistemlerinin sürekli gelişmesi sadece faydalı alanlarda değil siber casusların saldırılarını daha etkili bir şekilde gerçekleştirebilmeleri için de kullanılmaktadır.

Bu şekilde sürekli gelişen bir sistem karşısında konaklama işletmeleri hem siber güvenlik konusunu ciddiye alıp işletme sürekliliğinin devamı ve imaj zedelenmelerini önlemek adına hem de personellerini bu gelişen sistemlerle uyumlu bir şekilde çalışabilmeleri adına sürekli olarak bilinçlendirme ve eğitme konularında devamlılık sağlamalıdır. Bu çalışma İzmir ilindeki 4 ve 5 yıldızlı konaklama işletmeleri bilgi işlem bölümleri yöneticilerine yönelik yapılmıştır. Daha sonraki çalışmalarda farklı niteliklere sahip konaklama işletmelerine veya farklı sektörlerde hizmet veren işletmelere yönelik çalışmalar yapılabilir. Yapılacak olası bir çalışmada sonuçlar farklılık gösterebilir.

KAYNAKÇA

Akıncı Z (2016) *Otel İşletmeciliği Ve Yönetimi* (Detay Yayınları, Ankara).

Altıner M, Çakır F (2017) Siber uzay ve uluslar arası ilişkiler/teorisi. *Cyberpolitik Journal*, *2*(4): 183-190.

Amoroso E (2006) *Cyber Security* (Silicon Press, New Jersey).

Barutçugil İ (2002) *Bilgi Yönetimi* (Karıyer Yayıncılık, İstanbul).

Baykara M, Daş R, Karadoğan İ (2013) Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. *1st International Symposium On Digital Forensics And Security (ISDFS'2013)* 13: 231-239.

Bayraktar BB (2006) *Bilgi Yönetimi Akademik Yaklaşımlar* (Beta Basım A.Ş, İstanbul).

Uit Beijerse RP (2000) Knowledge management in small and medium-sized companies: knowledge management for entrepreneurs. *Journal Of Knowledge Management* 4 (2): 162-174.

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

Cavelty MD (2010) Cyber-security. T*he Routledge Handbook Of New Security Studies* : 166-174.

Celep C, Çetin B (2003*) Bilgi Yönetimi* (Anı yayıncılık, Ankara)

Chen HS, Fiscus J (2018) The inhospitable vulnerability: a need for cybersecurity risk assessment in the hospitality industry. *Journal Of Hospitality And Tourism Technology*.

Çakmakçı E (2012) Bilgi teknolojisi kullanımının otel performansı ve verimliliğine etkisi. *Verimlilik Dergisi* (4): 47-66.

Çetin H, Gundak İ, Çetin HH (2015) E-işletme güvenliği ve siber saldırılar üzerine bir araştırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 6*(2): 223-240.

Davenport T, Prusak L (2000) *İş Dünyasında Bilgi Yönetimi*, çev. Günay Günhan. (Rota Yayınları, İstanbul)

Değirmenci O (2002) Bilişim Suçları. Yüksek Lisans Tezi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı, İstranbul.

Eldem T (2021) Birleşmiş milletler sistemi ve küresel siber alan güvenliği regülasyonu. *Marmara Üniversitesi Siyasal Bilimler Dergisi* 9(1): 17-45.

Erol SE, Ceyhan EB, Sağıroğlu Ş (2015) Kişisel, kurumsal ve ulusal bilgi güvenliği farkındalığı üzerine bir inceleme. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı*. Ankara, Türkiye, 30-31 Ekim.

Fırat SÜ, Fırat OZ (2017) Sanayi 4.0 devrimi üzerine karşılaştırmalı bir inceleme: kavramlar, küresel gelişmeler ve Türkiye. *Toprak İşveren Dergisi* 114: 10-23.

Göçoğlu V (2018) Türkiye'nin siber güvenlik politikalarının kamu politikası analizi çerçevesinde değerlendirilmesi. Doktora Tezi, Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Ankara

Gülmüş M (2011) Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik Mühendisliği Anabilim Dalı, İstanbul.

Güneş B (2019) Siber fiziksel sistemler üzerinde bütünleşik siber güvenlik risk değerlendirmesi: bir konteynır limanı uygulaması. Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Deniz Ulaştırma Mühendisliği Anabilim Dalı, İstanbul.

Gürkaynak M, İren AA (2011) Reel dünyada sanal açmaz: siber alanda uluslararası ilişkiler. *Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi Sayı: 2*. 16(16): 263-279.

Hathaway OA, Crootof R, Levitz P, Nix H (2012), The law of cyber-attack, *California Law Review* 100: 817-885.

Ilgar T, Erdoğdu G (2018) Kurumsal risk yönetimi türk kamu yönetimine nasıl entegre edilebilir ?. *Denetişim* (18): 63-76.

Johnson ME, Goetz E (2007) Embedding ınformation security into the organization. *Managing Organizational Security.* May/June 2007: 16–24.

Kalkan VD (2006) Örgütsel öğrenme ve bilgi yönetimi. *Elektronik Sosyal Bilimler Dergisi* 5(16): 22-36.

Karabıyık BK, Armağan E (2017) Tüketicinin çevrimiçi davranışsal reklamlara tıklama kararını etkileyen faktörler. *Journal Of Yaşar University* 12(47): 202-215.

Kurgun OA (2006) Bilgi yönetim sistemlerinin yapılandırılması. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 8: 274-291.

Kurnaz S, Önen SM (2019) Avrupa birliğine uyum sürecinde türkiye'nin siber güvenlik stratejileri. *International Journal Of Politics And Security 1*(2): 82-103.

Libicki MC (2009) *Cyberdeterrence And Cyberwar* (Rand Corporation, Santa Monica, Ca).

McCumber J (2005) *Assessing And Managing Security Risk In It Systems* (Auerbach Publications, New York).

Offsey S (1997) Knowledge management: linking people to knowledge for bottom line results. *Journal Of Knowledge Management* 1(2): 113-122.

Pelit E (2009) Turizm İşletmelerinde Bilgi Teknolojilerinin Kullanımı Ve Yaygınlaştırılmasına Yönelik Uygulamalar, *Avrupa Birliği Eğitim Ve Gençlik Programları Merkezi Başkanlığı Leonardo Da Vinci Hareketlilik Projesi* (2008-1): 14-16.

Pfleeger CP (1997) The fundamentals of information security. *IEEE Software* 14:1-14.

Singer PW, Friedman A (2014) *Cybersecurity: What Everyone Needs To Know* (Oxford University Press, USA).

Siponen MT (2000) A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*. 8(1): 31–41.

Şahinaslan Ö (2013) Siber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma. Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Edirne.

Şencan E (2013) *Bilgi Yönetimi Ve Sanal Halkla İlişkiler* (Eğitim Yayınevi, Konya).

Tdk (2010) *Büyük Türkçe Sözlük* (Türk Dil Kurumu Yayınları, Ankara).

Thomson KL, Solms RV, Louw L (2006) Cultivating an organizational information security culture *Computer Fraud & Security* 2006 (10) : 7–11.

Tutar H (2010) *Yönetim Bilgi Sistemi* (Seçkin Yayıncılık, Ankara).

Ünver M (2012) Uulusal siber güvenliğin sağlanmasında farkındalık çalışmaları. *Bilgi Güvenliği Derneği*

Whitman ME, Mattord HJ (2021) *Principles Of Information Security* (Cengage Learning, USA).

Yeniçeri Ö, İnce M (2005) *Bilgi Yönetim Stratejileri Ve Girişimcilik* (IQ Kültür Sanat Yayıncılık, İstanbul).

Yeşilyurt H (2015) Finansal hizmet sektöründe siber güvenlik riskleri ve çözüm yolları: ödeme sistemleri ve tedarik zinciri bütünlüğü. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi* 13(02): 97-120.

Zaim H (2005) *Bilginin Artan Önemi Ve Bilgi Yönetimi* (İşaret Yayınları, İstanbul).

EKLER

EK 1: İzmir İlinde Faaliyet Gösteren 4 Ve 5 Yıldızlı Konaklama İşletmelerinin Bilişim Teknolojileri Bölümü Sorumlularına Ya Da Çalışanlarına Uygulanan Anket Formu

Değerli Katılımcı, bu çalışmanın amacı 4 ve 5 yıldızlı konaklama işletmelerinin siber güvenlik yönetim yaklaşımlarının incelenmesidir. Bu anketten elde edilecek veriler yalnızca akademik çalışmalar için kullanılacaktır. Ankette yer alan sorulara vereceğiniz yanıtlar gizli tutulacak ve toplu olarak değerlendirilecektir. Göstereceğiniz ilgi ve ayıracağınız zaman için teşekkür ederiz Çalışma ile ilgili sorularınız ve önerileriniz için .....mail adresi üzerinden iletişim kurabilirsiniz.

Aşağıdaki sorulara size en uygun cevabı verecek şekilde yanıtlayınız. ***1- Hiç katılmıyorum/Hiç uygulanmıyor*** ***2- Kısmen katılıyorum/Kısmen uygulanıyor*** ***3- Çoğunlukla katılıyorum/Çoğunlukla uygulanıyor*** ***4- Katılıyorum/Uygulanıyor*** ***5- Tamamen Katılıyorum/ Tamamen Uygulanıyor***	**1**	**2**	**3**	**4**	5
1. Otelimizin bilgi güvenliğine ilişkin yazılı kural ve politikaları vardır.					
2. Otelimiz bilgi güvenliğine ilişkin yazılı kural ve politikaları oluştururken hayati öneme sahip alanlarda oluşabilecek, tehlike ve güvenlik açıklarını dikkate almıştır.					
3.Otelimizin bilgi güvenliğine ilişkin kural ve politikaları, ülkemizdeki ilgili kanun ve yönetmeliklere uygundur.					
4.Otelimiz kritik bilişim teknolojilerini önem derecesine göre sınıflandırıp, bu sistemleri oluşturulan sınıflandırmaya göre yönetir.					
5.Otelimiz bilgi yaşam döngüsünün tüm aşamalarında gerekli güvenlik önlemlerini almaktadır. (Bilgi yaşam döngüsü: bilginin oluşturulması, kullanılması, depolanması, iletilmesi, işlenmesi ve imha edilmesi)					
6.Otelimiz bilgi teknolojilerine yönelik hizmet alımlarında, gerekli güvenlik önlemlerini sözleşme maddelerine dahil eder.					
7. Bu soruyu kesimlikle katılıyorum olarak işaretleyiniz.					
8.Otelimiz tüm çalışanlara bilgi güvenliğine ilişkin yükümlülükleri açıkça bildirilmektedir.					
9.Otelimiz tüm çalışanlara düzenli olarak bilgi güvenliği eğitimleri vermektedir.					

10. Otelimize ait tesislerin güvenliğini iyileştirmek için gerekli güvenlik önlemleri uygulanmaktadır.					
11. Otelimize ait tesislere giriş-çıkışı düzenleyen yazılı kurallar vardır.					
12. Otelimiz, bilgi teknolojilerine yönelik her türlü tehlikeye (doğal felaketler veya insan kaynaklı zararlar) karşı koruyu önlemler alınmıştır.					
13. Otelimizde, taşınabilir bilgisayar veya harici depolama aygıtlarının kullanımına ilişkin güvenlik önlemleri alınmıştır.					
14. Otelimiz, bilgi teknolojileri verilerini (sistem konfigürasyon ve yedekleri) uygun bir şekilde korur.					
15. Otelimizde bilgi teknolojileri kurulum ve kullanım süreçleri bilgi güvenliği hususları dikkate alınarak icra edilir.					
16. Otelimiz, verilerini uygun bir şekilde yedekler.					
17. Bu soruyu kesinlikle katılmıyorum olarak işaretleyiniz.					
18. Otelimiz, kötü amaçlı yazılımlara (virüs, trojan, vb.) karşı önlemler alır.					
19. Otelimiz, bilişim sistemlerinin güvenlik açıklarını azaltmak için önlemler alır.					
20. Otelimiz, bilişim sistemlerine bağlantıları güvenli bir şekilde tesis eder. (VPN, sertifika vb.)					
21. Otelimiz, tüm cihaz ve aygıtların çalınma riskine karşı önlemler alır.					
22. Otelimiz, bilişim sistemlerine bağlantı için gerekli kimlik denetimlerini yapar.					
23. Otelimizde bilişim teknolojilerine kimlerin hangi şartlarda erişebileceği düzenlemiştir.					
24. Otelimiz, yerel ağlar üzerinde yetki denetimi uygular.					
25. Otelimiz, yazılım geliştirme projelerinin güvenlik gereksinimlerini projelere dâhil eder.					
26. Otelimiz, yazılım ürünlerinin seçimi, satın alınması ve / veya bakım işlerinde güvenlik kontrolleri gerçekleştirir.					
27. Otelimiz, bilişim arızalarının kurum faaliyetlerini aksatmaması için önlemler alır.					
28. Otelimizde, olası bilişim kaynaklı problemler için acil eylemleri belirten yazılı prosedürler bulunur.					
29. Otelimizin, tüm bileşenleri kapsar nitelikte arızalara karşı mücadeleyi ele alan bir İSY (İş Sürekliliği Yönetimi) bulunmaktadır.					

1. Konaklama işletmenizin türü nedir?
   ( ) 4 Yıldızlı ( ) 5 Yıldızlı
2. İşletmenizin ve misafirlerinizin gizli tutulan bilgilerine ulaşım sağlama izni olan çalışan sayınız?
3. Ticari faaliyetlerde ne derecede internete bağımlısınız?
   ( ) %25 veya daha az ( ) %25 - %50 arası
   ( ) %50 - %75 arası ( ) %75 veya daha fazla
4. Bilişim sistemlerinizde 24 saatlik bir aksama yaşanması durumunda 24 saat süresince ticari faaliyetleriniz olan satışlarınız ne derecede ve ne şekilde etkilenir?
5. Konaklama işletmeniz siber saldırılara karşı önlem almakta mıdır?
   ( ) Evet ( ) Hayır
6. İşletmeniz olası bir siber saldırıya karşı ne gibi önlemler almaktadır?
7. Oteliniz tarafından bilgisayar ağlarını korumak için kullandığınız ağ güvenliği araçları ve teknikleri nelerdir?
8. Otellinizdeki bilgisayar ağı güvenliğine yönelik mevcut tehditler nelerdir?
9. İşletmenize yapılacak olası bir siber saldırı ile müşterilerinize ait kişisel bilgilerin (kimlik, banka vb.) sızdırılması işletmenizi nasıl etkiler?
10. Daha önce siber saldırı ile karşılaştınız mı? Bu soruya yanıtınız “EVET” ise 11, 12, 13, 14, 15 ve 16. 17. Ve 18. soruları yanıtlayınız.

( ) Evet ( ) Hayır

11. Siber saldırıya ilk defa ne zaman ve kaç kere maruz kaldınız?
12. Karşılaştığınız bu siber saldırının türü neydi?

( ) Virüs saldırısı

( ) Veri ağları sabotajı

( ) İşletmeye ait bilgilerin ele geçirilmesi

( ) Diğer

13. Siber saldırı sonrası ortaya çıkan mali kaybınız ne kadar oldu? (Mali kaybınız yok ise "YOK" şeklinde belirtiniz?

14. Bu siber saldırı işletmenizi ne derecede ve ne şekilde etkiledi?
15. Siber saldırı sonrasında saldırılara karşı aldığınız ek önlemler oldu mu? Ne gibi önlemler aldınız?
16. Siber saldırı sonrası herhangi bir kuruluşa bildirim yapıldı mı? (Bu soruya yanıtınız EVET ise 17. Soruyu yanıtlayınız. Bu soruya yanıtınız Hayır ise 18. Soruyu yanıtlayınız.)

( ) Evet ( ) Hayır

17. Siber saldırı sonrası hangi kuruluşa bildirim yaptınız?
18. Siber saldırı sonrası herhangi bir kuruluşa bildirim yapmadıysanız bunun sebepleri nelerdir?

EK 2: İşletmedeki Bilgisayar Ağı Güvenliğine Yönelik Mevcut Tehditlere Göre Siber Güvenlik Yaklaşımı Arasındaki Farklılıkların Hangi Gruplar Arasındaki Farklılıktan Meydana Geldiğini Gösteren Post Hoc Testi Sonuçları

		Güven aralığı (I-J)	Standart hata	Sig.	%95 güven aralığı	
					Alt sınır	Üst sınır
Güvenlik duvarı	Siber güvenlik şirketlerinden hizmet alma	,83348	,40999	,810	-1,4948	3,1617
	Anti virüs programları	1,14655	,51817	,831	-3,1306	5,4237
	Şifreli giriş sistemleri	,16379	,37272	1,000	-2,9186	3,2462
	Merkez bilişim sistemleri bölümü	,35837	,37907	1,000	-2,5304	3,2471
	Veri koruma programları	,21552	3,37428	1,000	-2,8193	3,2503
Siber güvenlik şirketlerinden hizmet alma	Güvenlik duvarı	-,83348	,40999	,810	-3,1617	1,4948
	Anti virüs programları	,31307	,40221	1,000	-13,8374	14,4635
	Şifreli giriş sistemleri	,66969*	,17941	,020	-1,2668	-0,726
	Merkez bilişim sistemleri bölümü	-,47511	,19225	,270	-1,0978	,1476
	Veri koruma programları	,61797*	,18264	,047	-1,2299	-,0060
Anti virüs programları	Güvenlik duvarı	1,14655	,51817	,831	-5,4237	3,1306
	Siber güvenlik şirketlerinden hizmet alma	-,31307	,40221	1,000	-14,4635	13,8374
	Şifreli giriş sistemleri	-,98276	,36414	,977	-61,6085	59,6430
	Merkez bilişim sistemleri bölümü	-,78818	,37064	,989	-45,0294	43,4530
	Veri koruma programları	-,93103	,36574	,980	-56,9501	55,0880
Şifreli giriş sistemleri	Güvenlik duvarı	-,16379	,37272	1,000	-3,2462	2,9186
	Siber güvenlik şirketlerinden hizmet alma	,66969*	,17941	,020	,0726	1,2668
	Anti virüs programları	,98276	,36414	,977	-59,6430	61,6085
	Merkez bilişim sistemleri bölümü	,19458	,08824	,468	-,1043	,4935
	Veri koruma programları	,05172	,06466	1,000	-,7828	,8863
Merkez bilişim sistemleri bölümü	Güvenlik duvarı	-,35837	,37907	1,000	-3,2471	2,5304
	Siber güvenlik şirketlerinden hizmet alma	,47511	,19225	,270	-,1476	1,0978
	Anti virüs programları	,78818	,37064	,898	-43,4530	45,0294
	Şifreli giriş sistemleri	-,19458	,08824	,468	-,4935	,1043
	Veri koruma programları	-1,4286	,09463	,939	-,5338	,2481
Veri koruma programları	Güvenlik duvarı	-,21552	,37428	1,000	-3,2503	2,8193
	Siber güvenlik şirketlerinden hizmet alma	,61797*	,18264	,047	,0060	1,2299
	Anti virüs programları	,93103	,36574	,980	-55,0880	56,9501
	Şifreli giriş sistemleri	-,05172	0,6466	1,000	-,8863	,7828
	Merkez bilişim sistemleri bölümü	,14286	,09463	,939	-,2481	,5338