Konaklama İşletmesi Yöneticilerinde Bilgi Güvenliği Farkındalığı: Kuşadası'ndaki Beş Yıldızlı Oteller Örneği[1]

Arş. Gör. Turan OKUL
Aydın Adnan Menderes Üniversitesi, Turizm Fakültesi
Seyahat İşletmeciliği Bölümü
turanokul@hotmail.com

Dr. Öğr. Üyesi Güntekin ŞİMŞEK
Aydın Adnan Menderes Üniversitesi, Turizm Fakültesi
Seyahat İşletmeciliği Bölümü
gsimsek@adu.edu.tr

Büşra HAFÇI
Aydın Adnan Menderes Üniversitesi
Turizm İşletmeciliği ABD
busrahafci@gmail.com

Zafer BARIŞ
Aydın Adnan Menderes Üniversitesi
Turizm İşletmeciliği ABD
zafer1984baris@hotmail.com

Özet

Bu çalışmada, Kuşadası'ndaki 5 yıldızlı konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıklarını belirlemek amaçlanmıştır. Bu amaç doğrultusunda veri toplama aracı olarak anket tekniği kullanılmıştır. Çalışma iki bölümden oluşmaktadır. Birinci bölümde bilgi güvenliği ve bilgi güvenliği farkındalığının teorik çerçevesi verilmiştir. İkinci bölümde ise konaklama işletmesi yöneticileri üzerinde yapılan uygulamaya ait veriler sunulmuştur. Çalışmada yöneticilerin verdiği yanıtların aritmetik ortalamaları çıkarılmış ve karşılaştırmalı analizler için independent sample t testi ve one way anova testleri uygulanmıştır. Elde edilen bulgulara göre, Kuşadası'ndaki konaklama işletmesi yöneticilerinin bilgi güvenliği konusunda farkındalıklarının yüksek olduğu tespit edilmiştir. Ancak, konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıklarının yüksek olmasına rağmen, bilgi güvenliği ile ilgili bazı önemli hususlarda yeterli bilgiye sahip olmadıkları göze çarpmaktadır. Buna yönelik olarak, konaklama işletmelerinde bilgi güvenliği farkındalık eğitimleri verilmesi önerisi getirilmiştir.

Anahtar Kelimeler: Turizm, Otel Yöneticileri, Bilgi Güvenliği, Bilgi Güvenliği Farkındalığı.

[1] Bu makale 20-22 Nisan 2017 tarihlerinde Kırgızistan Bişkek'te düzenlenen "3.Türk Dünyası Turizm Sempozyumu"nda sunulan ve bildiriler kitabında yer alan bildirinin geliştirilmiş halidir.

Information Security Awareness on Managers of Hotels: The Case of Five-Star Hotels in Kuşadası

Abstract

In this study, it was aimed to reveal the information security awareness of 5 star hotel managers in Kuşadası. For this purpose, survey technique was used for data collection. The study consists of two parts. In the first part, the theoretical framework of information security awareness is presented. In the second part, the information about the survey is presented. In the study, In the study, arithmetic averages of the responses were taken and independent sample t test and one way anova tests were applied for comparative analysis. According to the findings, managers have high awareness of information security. However, in some important cases, it is revealed that managers do not have sufficient knowledge about information security. Accordingly, the proposal of information security awareness training in hotels has been introduced.

Keywords: Tourism, Hotel Managers, Information Security, Information Security Awareness.

Giriş

Devasa boyutlardaki ilk bilgisayarın (ENIAC) üretilmesinden, akıllı telefonların insanın günlük hayatına girmesine kadar geçen süreçte bilgi teknolojilerinde meydana gelen gelişmeler oldukça büyük bir ivme göstermiştir. Teknolojinin bu hızlı gelişimi ile birlikte kişisel veya kurumsal bilgileri depolamak, işlemek ve transfer etmek daha az maliyetli, daha az zaman alıcı ve daha basit hale gelmiştir. Günümüzde bir kibrit kutusundan daha küçük ölçülere tekabül eden boyutlardaki harici belleklerde bir kütüphanenin içeriğini muhafaza etmek mümkün olmaktadır. Kamu kurumları, ticari kuruluşlar ve bireyler bilgilerini elektronik ortama taşımaktadır. Elektronik ortamın bugün sunduğu en büyük imkânlardan birisi internet hizmetleridir. İnternet hizmetlerinin kullanımı askeri alanda, kamusal hizmetlerde, eğitimde, bilimsel araştırmalarda, sağlık hizmetlerinde, ekonomide, haberleşmede ve ticarette vazgeçilmez bir hal almıştır. Sağladığı tüm kolaylıklara karşın bilgi teknolojilerinde meydana gelen bu gelişmeler bazı zafiyetleri ve riskleri de beraberinde getirmiştir. Küresel bir alanı içine alan internet ortamında varlık gösteren tüm makinelerde (kişisel bilgisayar, tablet, akıllı telefon ve internet bağlantısı olan diğer cihazlar) yer alan bilgiler, çeşitli yollarla saldırılara açık bir konuma gelmiş ve sanal ortamda güvenlik açıkları ortaya çıkmaya başlamıştır. Söz konusu güvenlik açıkları; bilgileri elde etme, yok etme, bütünlüğünü bozma veya farklı bir amaç doğrultusunda kullanma amacı taşıyan kişiler, kuruluşlar ve hatta devletler bazında bir silaha dönüşmüştür. Bu durumdan hareketle; siber saldırı, siber savaş ve siber güvenlik gibi kavramlar ortaya çıkmıştır. Bilgi güvenliğinin sağlanması gerekliliği de bu gelişmelere paralel olarak anlaşılmaya başlamıştır.

Bilgi yoğun bir endüstri haline dönüşen turizmde faaliyet gösteren işletmeler için bilgi; işletmenin varlığını, prestijini ve karlılığını devam ettirebilmesi için en önemli unsurlardan birisidir. Turizm ürünlerinin ve hizmetlerinin üretimi ve pazarlamasında küresel dağıtım sistemleri (GDS/Global Distrubition System) ve bilgisayarlı rezervasyon sistemleri (CRS/Computer Reservation System) yoğun olarak kullanılmaktadır. Hizmet endüstrilerinde müşterilerin memnuniyeti için onlarla ilgili bilgilerin muhafaza edildiği bir veri tabanına sahip olmak işletmeler için önemlidir. Bu bilgiler daha sonra bireylere yönelik pazarlama çabalarında da kullanılabilmektedir. Bu nedenle işletmelerin sahip olduğu bilgiler, gerek işletmenin özel bilgileri gerekse müşterilere ait bilgiler, kendilerine ait mahrem bir alanı oluşturmaktadır. İşletme dışındaki bireyler tarafından elde edilen bilgiler, işletme aleyhine kullanılabilir veya rakip işletmelerin eline geçen bilgiler işletmenin pazardaki rekabet

gücünü yitirmesine neden olabilir. Bu gibi sebeplerden ötürü turizm işletmelerinde bilgi güvenliğine dair önlemler alınması zorunluluk haline gelmiştir.

Turizm hareketlerine katılan insanların konaklama ihtiyacı temel ihtiyaçlardan birisidir. Bu sebeple konaklama işletmeleri turizm endüstrisinde değişmez bir yere sahiptir. Konaklama işletmelerinde de bilgi teknolojileri yoğun olarak kullanılmaktadır. Ön büroda kullanılan emniyet birimleri ile entegre otomasyonlar, rezervasyonda ve muhasebede kullanılan yazılımlar, elektronik ödeme sistemleri, odalarda sunulan teknolojik araçlar bunların başlıca örnekleridir. Konaklama işletmelerinin bu iş süreçlerindeki herhangi bir güvenlik açığı işletme için büyük bir tehdit oluşturmaktadır. Bununla beraber müşterilerin özel bilgilerinin de konaklama işletmelerinde mevcut olması yine işletme için bilgi güvenliğinin önemini ortaya koymaktadır. Bu nedenle konaklama işletmelerinde bilgi güvenliğine dair önlemler alınması gerekliliği söz konusu olmaktadır. Bu önlemlerin alınabilmesi içinse işletme sahiplerinin ve yöneticilerinin bilgi güvenliği konusunda malumat sahibi olması ve bir farkındalıklarının oluşması büyük önem arz etmektedir. Buradan yola çıkarak çalışmada Kuşadası'ndaki 5 yıldızlı konaklama işletmesi sahiplerinin ve yöneticilerinin bilgi güvenliği farkındalıklarını ölçmek amaçlanmıştır.

Çalışma iki bölümden oluşmaktadır. Çalışmanın teorik çerçevesini oluşturan birinci bölümde; bilgi güvenliğinin tanımı, kapsamı, unsurları ve konaklama işletmelerinde bilgi güvenliğinin kapsamı ve bilgi güvenliği riskleri ikincil verilerden yararlanarak hazırlanmıştır. İşletme sahipleri ve yöneticilerin bilgi güvenliği farkındalığı ele alınan araştırma kısmını oluşturan ikinci bölümde ise anket tekniği ile elde edilen birincil nicel veriler analiz edilmiş ve sonuçları paylaşılmıştır.

Bilgi Güvenliği

Bilgi güvenliği, en genel tanımı ile bilgi sistemlerinin içerdiği bilginin yetki sahibi olmayanlar tarafından erişimine, incelenmesine, kullanılmasına, ortaya çıkarılmasına, değişiklik yapılmasına, zarar verilmesine veya yok edilmesine karşı korunması ve bununla ilgili alınan önlemlerin tümü şeklinde tanımlanabilir (FISMA, 2002).

Bilgi güvenliğinin tarihi gelişimi bilgisayar güvenliği ile başlamaktadır. Bilgi güvenliği, depolama, işleme ve iletme dahil olmak üzere bilgi varlıklarının gizliliğinin, bütünlüğünün ve kullanılabilirliğinin korunmasını amaçlar. Bunu başarmanın yolu da güvenlik politikaları, güvenlik eğitimi, güvenlik farkındalığı ve güvenlik teknolojilerinin uygulanmasından geçmektedir (Whitman ve Mattord, 2012:1). Bilgi güvenliği genel olarak bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya odaklanmaktadır. Bilgi güvenliği farkındalığı ise, güvenlikle ilgili olumlu davranışları etkin bir bilgi güvenliği ortamında kritik bir unsur olarak yaratmak ve korumak için güvenlik farkındalığını geliştirme programlarını kullanmakla ilgilidir (Kruger ve Kearney, 2006: 289).

Bilgi güvenliğinin üç temel unsuru gizlilik, bütünlük ve kullanılabilirliktir. Bunların haricinde hesap verebilirlik, güvenilirlik, erişim denetimi ve emniyet de bilgi güvenliğini destekleyen unsurlardır. Doğruluk ve inkâr edilemezlik ise elektronik ticaretin yaygınlaşması ile ortaya çıkan unsurlar olarak değerlendirilmektedir. Doğruluk, bilginin gerçekten yer aldığı bilgi sistemi üzerinden işlem yapılmasını; inkar edilemezlik ise kullanıcıların elektronik ortamda gerçekleştirdikleri işlemleri inkar edemeyeceği şekilde önlemlerin alınmasını ifade eder (Güngör, 2015: 8-9). Gizlilik ilkesi; bilgiye erişme yetkisi olmayanların erişememesini, yalnızca yetki sahibi olanların bilgiye erişebilmesini ifade eder. Bütünlük ilkesi; bilginin bozulmadan, tahribata uğramadan orijinal yapısının korunmasıdır. Kullanılabilirlik ilkesi ise; bilgiye ulaşılmak istendiği anda ulaşılabilmesini

ve kullanılabilmesini ele alır (Al, 2002; Şahinaslan vd., 2009; Gülmüş, 2010). Bilgi güvenliğini destekleyen unsurlar olan hesap verebilirlik, bilgiyi kullanan ve erişim sahibi olanların kurumsal anlamda bilgiyle ilgili güvenlik konularında hesap verebilir olmasını; güvenilirlik, yine bilgiye erişim sahibi olan ve onu kullananların güvenilir olmasını; erişim denetimi ve emniyet ise, bilgiye yalnızca yetki sahibi olanların erişebilmesini ve bunun denetimini ifade etmektedir.

Bilgi Güvenliği Forumu (ISF, 2003), bilgi güvenliği farkındalığının, her personelin bilgi güvenliğinin önemini, organizasyona uygun bilgi güvenliği düzeylerini, bireysel güvenlik sorumluluklarını ve bu doğrultuda hareket ettiğini anladığı derecede tanımlandığını belirtmektedir. Bilgi güvenliğinin etkin yönetimi, bilgi riskini yönetmek için teknik ve usul kontrollerinin bir kombinasyonunu gerektirir. Kontrollerin değeri genellikle onları uygulayan ve kullanan kişilere bağlıdır. Güvenlik politikalarını ve prosedürlerini ihmal eden çalışanlar tarafından kontrollerden kaçılabilir veya istismar edilebilir. Etkili güvenlik kontrollerinin uygulanması, herkesin anladığı ve onlardan beklenen davranışlara girdiği bir güvenlik ortamının yaratılmasına bağlıdır.

Bilgi Güvenliği Forumu (ISF, 2002)'na göre, güvenlik farkındalığı, her üyenin bilgi güvenliğinin önemini, örgüt için uygun bilgi güvenliği seviyelerini, bireysel güvenlik sorumluluklarını ne derecede anladığını ve ne derece buna göre hareket ettiğini ifade eder. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD, 2002), güvenlik bilincinin amacını şöyle tanımlamaktadır: "Katılımcılar, bilgi sistemlerinin ve ağlarının güvenlik gereksiniminin farkında olmalı ve güvenliği artırmak için neler yapabileceklerini bilmelidir. Bir örgütün üyeleri, bilgi güvenliğinin önemini anlamalı ve güvenlik politikası tarafından sağlanan yönergelere uymalıdır" (Kim, 2013).

Bilgi sistemleri güvenliğini oluşturmak ve sürdürmek için sadece teknik güvenlik kontrollerinin uygulanması değil aynı zamanda idari, teknik ve prosedürle ilgili kontrollerin uygulanması da gereklidir (Tsohou vd., 2008; 207). Geçmiş çalışmalar ve deneyimler göstermektedir ki bilgi güvenliği konusunda en zayıf halkayı son kullanıcılar, yani insanlar oluşturmaktadır. Bilgi güvenliğinin önemini anlamadıkları takdirde kullanıcıların bilgi güvenliği tekniklerini veya prosedürlerini doğru bir şekilde kullanamayacağı açıktır. Kullanıcıların bilgi güvenliği için ne yapmaları gerektiğini anlamalarına yardımcı olmak için güçlü bir bilinçlendirme ve eğitim programı çok önemlidir.

Konaklama İşletmelerinde Bilgi Güvenliği

Konaklama işletmelerinde bilgi güvenliğinin kapsamı işletmenin bilgi varlıklarını ve onların bulundukları yerleri içine almaktadır. Bununla beraber, bilgi teknolojilerinin konaklama işletmeleri içerisindeki kullanım alanlarının artması ile bilgi güvenliğinin kapsamı bu işletmelerde daha da genişlemiştir. Bu nedenle öncelikle konaklama işletmelerinde bilgi teknolojilerinin kullanım alanlarından bahsetmek yerinde olacaktır.

Bilgi teknolojilerinin konaklama endüstrisinde kullanımı ilk olarak ön büro departmanında başlamıştır. Müşterilerin check-in işlemleri, rezervasyon kayıt, müşteri sicil kayıtlarının saklanması, odalar ile ilgili işlemler, kasa işlemleri, raporlama ve istatistik çıkarma, santral hizmetleri gibi ön büro tarafından gerçekleştirilen işlemler, bilgisayarlar yardımıyla çok daha hızlı, pratik ve doğru bir şekilde yapılabilmektedir (Çakmakçı, 2012: 52). Müşterilere ihtiyaç duydukları anda geçerli ve doğru bilgileri sağlamaya yarayan elektronik danışma hizmeti de bu konuda verilebilecek bir diğer örnektir. Bilgiler televizyon ekranında gösterilebilmekte ve yerel hava koşullarını kontrol etme, restoranları bulma, ziyaret yerlerini seçme ve hatta bir tur haritasını çıkarmak için menüden seçim yapabilme şansına sahip olmaktadır. Bilgi teknolohjileri, akıllı otel odasının yaratılması ve

tasarımında da yoğun biçimde kullanılmaktadır. Bu sistemle müşteriler, sıcaklığı, hava temizliğini, ışıkları ve sesleri bireysel olarak kontrol edebilmektedir (Pelit, 2009: 22-23).

Muhasebe uygulamaları, enerji tasarruf sistemleri, kartlı kapı sistemleri, mini bar kontrol sistemleri, otomatik santral uyandırma ve sesli mesaj sistemi, kablolu-kablosuz internet bağlantısının kurulması, oda içi eğlence-multivizyon sistemleri gibi hizmetler de konaklama işletmelerinde bilgi teknolojilerinin yoğun olarak kullanıldığı alanları oluşturmaktadır (Çakmakçı, 2012: 52-54).

Konaklama işletmelerinde bilgi güvenliği açısından risk oluşturan alanlar, bilgi teknolojilerinin yoğun biçimde kullanıldığı alanlar olarak görülmektedir. İşletmenin bilgi güvenliğini tehdit edecek unsurları iç kaynaklı tehdit unsurları ve dış kaynaklı tehdit unsurları şeklinde iki kategoriye ayırmak mümkündür.

İç kaynaklı tehdit unsurları, işletme personelinin bilgi güvenliği konusunda bilinçsiz olması, işletmede kullanılan yazılımların ve otomasyonların yeterli güvenlik yapısına sahip olmaması, donanımsal olarak eksikliklerin bulunması, işletmede lisanssız programların kullanılması gibi unsurlar sıralanabilir. Dış kaynaklı tehdit unsurları ise siber saldırılar, işletmenin müşterilerinden kaynaklanan güvenlik açıkları, işletmenin kendi içerisinde halledemediği bir takım işleri dış kaynak kullanarak başka işletmelere devrederek çözmeye çalışması gibi unsurlar şeklinde ifade edilebilir.

Turizm bölgelerinde faaliyet gösteren konaklama işletmeleri genellikle belli bir sezon içerisinde hizmet vermektedir. Bu nedenle, personel devir hızı oldukça yüksektir. Personel devir hızının yüksek olması işletme için bir riski de beraberinde getirmektedir. Sezon içerisinde çalışmış ve işletme ile problem yaşamış bir personel, ayrılırken müşterilere ait özel bilgileri veya işletmenin özel yazışmalarını, anlaşmalarını ifşa edebilir ve işletmenin zarar görmesine neden olabilir. Konaklama işletmesinde çalışan personellerin bilgi teknolojileri konusunda da eğitimli olmasında fayda görülmektedir. Çünkü işletmeler artık iş süreçlerini büyük oranda elektronik ortamda yürütmektedir. Bu alanda çalışan personelin bu konuda eğitiminin olması ve bilinç sahibi olması işletme için daha yararlı olacaktır.

Konaklama işletmelerinin internet hizmetlerini rezervasyon ve satış amaçlı kullanmaya başlaması ile beraber elektronik alanlarda bazı güvenlik riskleri de söz konusu olmaya başlamıştır. Elektronik ticaret yapan işletmeler, faaliyetlerini elektronik ortamda gerçekleştirebilmek için bir web sitesine ihtiyaç duymaktadır. Web sitesinin elektronik ortamda, bir mağaza, bir iletişim platformu veya bir pazarlama ve tanıtım aracı olarak kullanılması gibi pek çok fonksiyonu bulunmaktadır. Bu nedenle web sitesi konaklama işletmeleri için büyük önem taşımaktadır. Web sitesi kurmak ve tasarlamak ayrı bir uzmanlık gerektirdiği için işletmeler genellikle bunu kendi bünyesinde halledememektedir ve dış kaynak kullanımına gitmektedir. Burada işletme özel bilgilerini dışarıdan herhangi bir işletmeyle veya bir bireyle paylaşmak zorunda kaldığı için bu noktada bir güvenlik riski söz konusu olmaktadır. Benzer şekilde, eğer işletme içerisinde teknik bir birim yok ise arızalanan bilgisayarlar ve diğer elektronik cihazlar için de dış kaynak kullanımına gidilmektedir. Böylece işletmenin cihazları başkalarının eline geçmekte ve kötü niyetli kişiler veya işletmeler tarafından içindeki bilgilerin çalınmasına, bütünlüğünün bozulmasına neden olabilmektedir. Aynı zamanda, bilgisayar içine gömülecek herhangi bir kötü niyetli yazılım ile ilerisi için daha kötü sonuçlar doğuracak durumların meydana gelmesine de zemin hazırlanmaktadır.

Ödeme sistemleri işletme için en önemli güvenlik konularından bir tanesidir. Point Of Sale (POS, satış noktası) sistemleri, müşterilerin otelin değişik departmanlarında yaptığı harcamaların işlenmesi, bunların ön büro müşteri hesaplarında anında görüntülenmesi ve işletme içinde para

alışverişinin ortadan kaldırılarak satış denetiminin etkin bir biçimde gerçekleştirilmesini mümkün kılmıştır. Sanal POS yöntemi ise internet üzerinden talimat verilerek bir mal veya hizmetin, alıcı ve satıcının bir araya gelmesinin zor olduğu durumlarda, satın alınmasını mümkün hale getiren bir yazılımı ifade etmektedir. Tüketicilerin kredi kartı veya nakit kartı bilgilerini girerek çevrimiçi olarak elektronik ortamda ödeme yapılabilmesini sağlar. Burada fiziki bir POS'a gerek duyulmaz (Sanal POS Nedir?, 2016). Müşterilerin kart bilgilerinin çalınmaması veya kopyalanmaması için işletmenin hem fiziki ortamda hem de elektronik ortamda ödeme sistemlerini güvenli bir hale getirmesi gerekmektedir. Elektronik ortamda bunun için 3D güvenli ödeme sistemi kullanılabilir.

Konaklama işletmelerinde internet ağları, lobide ve odalarda sunulmaktadır ve yoğun bir şekilde bu ağlar kullanılmaktadır. Burada ortak bir ağ kullanımı söz konusu olduğu için müşterilerin bilinçsiz veya kötü niyetli internet hizmeti kullanımları işletme için bazı riskleri beraberinde getirmektedir. Ortak ağdan yapılacak bilinçsiz işlemler ağı saldırıya açık hale getirebilir ve işletmenin bilgi sistemlerinin zarar görmesine sebebiyet verebilir. Birçok konaklama işletmesinde müşterilere verilen kablosuz ağ şifresi ortak bir şifre olmaktadır. Böylece otelden çıkan müşterilerin şifreyi dışarıda paylaşması söz konusu olabilmekte ve burada da bir güvenlik açığı ortaya çıkabilmektedir. Bunu önlemek için işletmeler tüm odaların farklı bir şifre ile ağa bağlanması için bir sistem kurma yoluna gidebilir.

Konaklama işletmelerinde bilgi güvenliği açığı oluşturabilecek başlıca alanlar; personelden kaynaklanan açıklar, müşteriden kaynaklanan açıklar, yazılım ve donanım sorunlarından kaynaklanan açıklar, dış kaynaklardan gelen açıklardır. Bilgi güvenliğinde en önemli unsur, en zayıf halka olmaları nedeniyle şüphesiz ki kullanıcılar yani insanlardır. Ancak bakıldığı zaman güvenlik açıklarını belirlemeye ve bunlara yönelik önlemler almaya yetkili olan kişiler yöneticilerdir. Yöneticiler aynı zamanda personeli bu konuda bilgilendirecek ve yönlendirecek olan kişilerdir. Bu nedenle yöneticilerin bilgi güvenliği farkındalığına sahip olması konaklama işletmeleri için büyük önem taşımaktadır.

Yöntem

Araştırmanın amacı; Kuşadası'ndaki 5 yıldızlı konaklama işletmeleri ölçeğinde işletme sahiplerinin ve yöneticilerinin bilgi güvenliği farkındalığını ortaya koymaktır. Bu amaç doğrultusunda araştırmada nicel araştırma yöntemi kullanılmış ve veri toplamak için anket tekniğinden yararlanılmıştır. Araştırmanın sorun cümlesi ise şu şekilde ifade edilmiştir; Kuşadası'ndaki 5 yıldızlı konaklama işletmesi sahiplerinin ve yöneticilerinin bilgi güvenliği farkındalıkları ne düzeydedir?

Araştırmada yöneticilerin bilgi güvenliği farkındalıklarının, cinsiyet, yaş, çalışma pozisyonu, mesleki deneyim, öğrenim durumu, günlük bilgisayar ve internet kullanım süreleri, bilgisayar, akıllı telefon ve tablete sahip olmaları gibi değişkenlere göre farklılık gösterip göstermediğini tespit etmek amacı ile bazı testler uygulanmıştır. Buna göre araştırmanın hipotezleri aşağıdaki şekildedir:

H1a: Cinsiyete göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1b: Yaşa göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1c: Çalışma pozisyonuna göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1d: Mesleki deneyime göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1e: Öğrenim durumuna göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1f: Günlük bilgisayar kullanım süresine göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1g: Günlük internet kullanım süresine göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1h: Kişisel bilgisayara, akıllı telefona veya tablet sahibi olmaya göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1i: Akıllı telefon sahibi olmaya göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

H1j: Tablet sahibi olmaya göre konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anlamlı bir farklılık göstermektedir.

Anakütle ve Örneklem

Araştırmanın anakütlesini Türkiye'deki tüm konaklama işletmelerinin yöneticileri oluşturmaktadır. Ancak zaman ve maddi kısıtlılıklardan dolayı Kuşadası'ndaki konaklama işletmeleri çalışma alanı olarak seçilmiştir. Kuşadası'nın Türkiye'nin en eski turizm merkezlerinden biri olması ve çok sayıda konaklama işletmesine sahip olması nedeniyle temsil gücünün yüksek olduğu düşünülmüştür. Araştırmanın örneklemi Kuşadası'ndaki yaklaşık 30 tane olan 5 yıldızlı konaklama işletmesi yöneticilerinin tamamı olduğu için tam sayım yapmak hedeflenmiştir. Araştırmanın yapıldığı dönemde (Kasım-Aralık, 2016) turizm sezonunun hareketli olmaması ve ülkede meydana gelen terör saldırılarından ötürü rezervasyonların iptal edilmesi ile işletmelerin kapalı durumda olması gibi nedenlerden ötürü 52 adet yöneticiye ulaşılabilmiştir.

Anket Formunun Hazırlanması

Bilgi güvenliği farkındalığı konusunda literatürde farklı ölçekler bulunmaktadır. Kjorvik, (2010), yüksek lisans tez çalışmasında bir bilgi güvenliği farkındalığı ölçeği geliştirilmiş ve uygulanmıştır. Veseli (2011), yüksek lisans tezi için bilgi güvenliği farkındalığı ölçeği geliştirmiştir. Yılmaz, (2015)'in doktora tezi için geliştirdiği öğretmenlerin dijital veri güvenliği farkındalığı ölçeği bunlardan bir tanesidir. Güldüren, Çetinkaya ve Keser (2016)'ın ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarını belirlemek için geliştirdikleri bir ölçek bulunmaktadır. Bunların içerisinden Veseli (2011)'in kullandığı ölçeğin bu çalışma için ifadeler ve uzunluk bakımından daha uygun olduğu uzman görüşünden yararlanarak (3 akademisyen) düşünülmüştür ve bu ölçek kullanılmıştır. Ölçekte, 5'li Likert Tipi'nde hazırlanmış (1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: Kararsızım, 4: Katılıyorum, 5: Kesinlikle katılıyorum) 20 ifade yer almaktadır. Ayrıca, 1 adet üç seçenekten oluşan kapalı uçlu soru ve 1 adet açık uçlu soru anket formunda yer almaktadır. Üç seçenekli kapalı uçlu soruda, yöneticilere şifrelerinin 8 karakterden uzun mu, kısa mı veya tam olarak 8 karakter mi olduğu, açık uçlu soruda ise yöneticilere güvenli bir şifrenin nasıl olması gerektiğine dair şahsi düşüncelerinin ne olduğu sorulmuştur. Bunlara ek olarak, yine uzman görüşünden yararlanarak hazırlanan demografik soruların bulunduğu ikinci bölüm de anket formunda yer almaktadır.

Güvenilirlik ve Geçerlilik

Ölçeğin güvenilirlik düzeyini belirlemek amacı ile güvenilirlik analizi uygulanmıştır. Uygulanan güvenilirlik analizi neticesinde ilk olarak 0,592 Cronbach Alpha değeri tespit edilmiştir. Daha sonra çıkarıldığında güvenilirlik düzeyinin artacağı 4 madde sıralı olarak ölçekten çıkarılmış ve 0,664 Cronbach Alpha güvenilirlik düzeyine ulaşılmıştır. Geri kalan maddeler içerisinden çıkarılsa da ölçeğin iç tutarlılık düzeyinde yükselme olmayacağı görülmüş ve ölçeğin güvenilirliği % 66,4 gibi yüksek bir düzeyde kabul edilmiştir (Cronbach, 1990).

Ölçeğin daha önce kullanıldığı çalışmada faktör analizi yapılmadığı için yapı geçerliliğini test etmek amacıyla güvenilirlik analizi neticesinde kalan 16 maddeye açımlayıcı faktör analizi uygulanmıştır. Varimax döndürme tekniği ile uygulanan açımlayıcı faktör analizi sonucunda dağılımı bozan 3 madde ölçekten çıkarılmıştır. Kalan 13 madde ile % 66,3'lük toplam varyansı açıklama oranıyla 5 boyuttan oluşan yapı geçerliliği sağlanmış bir ölçek yapısı elde edilmiştir. Birinci boyutta, yöneticilerin şifreler ve önemli belgelerle ilgili hassasiyetlerini belirten ifadeler bulunmaktadır. İkinci boyutta, yöneticilerin bilgi güvenliği sorumlulukları ile ilgili farkındalıklarını belirten ifadeler yer almaktadır. Üçüncü boyutta, yöneticilerin bilgi güvenliği konusundaki duyarlılıkları ile ilgili ifadeler bulunmaktadır. Dördüncü boyutta, yöneticilerin şifreleme bilinci ile ilgili ifadeler yer almaktadır. Beşinci boyutta ise, yöneticilerin gizlilikle ile ilgili bilinç düzeylerini ölçen ifadeler bulunmaktadır.

Veri analizi

Toplanan veriler SPSS for Windows 21.0 istatistik paket programı ile analiz edilmiştir. Veri setinin Kolmogorov-Smirnov Testine göre anlamlılık değeri 0.200 olarak bulunmuş ve normal dağılım varsayımını karşıladığı kabul edilmiştir (bkz. Tablo 1). Bu sebeple karşılaştırmalı analizler için parametrik testler uygulanmıştır. Uygulanan testler, cinsiyet için independent sample t testi ve ikiden fazla değişkeni olan sorular için one way anova testleridir.

Tablo 1. Normallik Testi

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Ortalama	,062	52	,200*	,987	52	,854

Bulgular

Demografik Veriler

Araştırma kapsamında ulaşılan 52 katılımcının 34 tanesini (% 65.4) erkekler, 18 tanesini (% 34.6) kadınlar oluşturmaktadır. Katılımcıların yaş gruplarını bakıldığında, 3 kişinin 18-30 yaş aralığında, 19 kişinin (% 36.5) 31-40 yaş aralığında, 19 kişinin (% 36.5) 41-50 yaş aralığında, 9 kişinin ise 51 ve üzeri yaş aralığında olduğu, 2 kişinin ise yaş aralığını belirtmediği görülmektedir. Katılımcıların 11 tanesini genel müdür (% 21.2), 27 tanesini (% 51.9) departman müdürü, 8 tanesini kısım şefleri (% 15.4) oluşturmaktadır. 2 kişinin ise çalışma pozisyonunu belirtmediği görülmektedir. Mesleki deneyimlerine göre ise % 83.7'lik bir oranda 11 yıl ve üzerinde deneyime sahip katılımcıların olduğu göze çarpmaktadır. Bu katılımcıların 36 tanesi (% 69.2) lisans ve yüksek lisans mezunlarından oluşmaktadır.

Katılımcılara, bilgi güvenliği farkındalıkları üzerinde etkili olabileceği düşünülen günlük bilgisayar kullanım süresi, günlük internet kullanım süresi, kişisel bilgisayara sahip olup olmadıkları, tablet bilgisayara sahip olup olmadıkları ve akıllı telefona sahip olup olmadıkları sorulmuştur. Verilen yanıtlara göre katılımcıların 22 tanesi (% 42.3) 4-6 saat, 22 tanesi (% 42.3) 7 saat ve üzeri günlük bilgisayar kullandıklarını belirtmiştir. Toplamda 44 kişi (% 84.7) günlük 4 saat ve üzerinde bilgisayar kullanmaktadır.

Günlük internet kullanım süresi, günlük bilgisayar kullanımına oranla biraz düşüş göstermektedir. 15 kişi (% 28.8) günlük 1-3 saat aralığında, 16 kişi (% 30.8) 4-6 saat aralığında, 14 kişi (% 26.9) 7 saat ve üzeri internet kullandıklarını belirtmişlerdir. 5 kişi ise günlük internet kullanım süresini 1 saatten az olarak belirtmiştir. 2 kişi ise günlük internet kullanım süresini yanıtsız bırakmıştır.

Katılımcıların 40 tanesi (% 76.9) kendine ait bilgisayarı olduğunu, 16 tanesi (% 30.8) kendisine ait tablet bilgisayarının olduğunu, 41 tanesi ise (% 78.8) akıllı telefonlarının olduğunu belirtmiştir.

Betimsel İstatistikler

Ölçekte yer alan 13 ifadeye verilen yanıtlar 1.15 ile 4.46 arasında dağılım göstermektedir ve aralığı 3.31'dir. Ölçeğin ortalaması 2.61, standart sapması 0,599 olarak tespit edilmiştir. Basıklık ve çarpıklık değerleri ise 1.0 ve 0.442 biçimindedir. Ölçekte yer alan ifadeler, verilen yanıtların ortalamaları ve standart sapmaları Tablo 2.'de verilmiştir. Burada yer almayan bir açık uçlu soru ve bir de üç seçenekli kapalı uçlu soru bulunmaktadır. Kapalı uçlu soruda katılımcılara şifrelerinin 8 karakterden daha kısa mı, daha uzun mu yoksa 8 karakter mi olduğu sorulmuştur. Verilen 48 yanıtın 24'ü daha uzun, 12'si tam olarak 8 karakter, 12'si ise daha kısa şeklinde olmuştur. Açık uçlu soruyu yanıtlayan 20 kişi ise güvenli bir şifrenin harf + sayı şeklinde olması gerektiğini belirtmiştir.

Tablo 2'de verilen yanıtların aritmetik ortalamaları incelendiğinde ifadelerin pek çoğunda katılımcıların farkındalık seviyelerinin yüksek olduğu ortaya çıkmaktadır. Ancak bazı ifadelerde yanıtlarda ikiye ayrılma söz konusudur. Örneğin, katılımcıların, "farklı hesaplar için iki aynı şifreyi kullanırım" ifadesine ait genel ortalama 2.76 seviyesindedir ve ortalamanın biraz üzerindedir. Benzer şekilde, "birisi iş amaçlı birisi özel kullanım amaçlı olmak üzere en az iki şifre kullanırım" ifadesinin genel ortalaması 3.29 seviyesindedir ve değer ortalamanın üzerinde olmasına rağmen çok yüksek değildir. Şifreleme ile ilgili diğer ifadelere bakıldığı zaman ise "bir şarkının sözlerinden bir bölümünü alıp her kelimenin baş harfini kullanarak oluşturulan şifre iyi bir şifre örneğidir" ifadesinin genel ortalaması 2.37'dir ve oldukça düşük olduğu görülmektedir. Açık uçlu "güvenli bir şifre nasıl olmalıdır" sorusuna verilen harf + sayı cevabının ağırlık kazandığı da dikkate alınırsa katılımcıların güvenli şifre konusunda yeterli düzeyde bilgi sahibi olmadığı yorumu yapılabilir. Çünkü güvenli bir şifrede sadece harfler ve sayıların değil noktalama işaretleri ve tahmin edilemeyecek karmaşık ifadelerin de olması gerekmektedir.

Katılımcıların, bilgilerin gizliliği ile ilgili ifadelere ("şifrelerimi bilgisayarın yanı başındaki bir kağıt parçasına yazarım" ve "işimle ilgili hassas bilgileri tüm iş arkadaşlarımla paylaşırım") verdikleri yanıtların ortalamasına bakıldığında 1.58 ve 1.72 şeklinde olduğu ve oldukça yüksek olduğu göze çarpmaktadır. Bu noktadan hareketle, bilgilerin gizliliği konusunda yöneticilerin farkındalıklarının yüksek olduğu söylenebilir. "Bilgi güvenliği konusunda önlemler almaktan sadece bilgi işlem departmanı sorumludur." ifadesine ait ortalamanın 2.27 şeklinde olması yöneticilerin bilgi güvenliği konusunda sorumlulukların tüm çalışanlara ait olduğunun farkında olduklarını göstermektedir şeklinde yorumlanabilir. "Çalışma saatleri içerisinde uzakta olsam bile ofisimin kapısını kilitlemem." ifadesine ait genel ortalamanın 2.97 olduğu görülmektedir. Bilginin güvenliğinin

sağlanabilmesinin ilk koşullarından birinin bilginin bulunduğu yerin güvenliğinin sağlanması gerektiği göz önüne alınırsa yöneticilerin bu konuda farkındalıklarının yüksek olmadığı söylenebilir.

Tablo 2. Ölçek Maddeleri ve Ortalamaları

İfadeler	N	Ortalama	St. Sapma
Şifrelerimi bilgisayarımın yanı başındaki bir kağıt parçasına yazarım.	51	1.58	1.18
İşimle ilgili hassas bilgileri tüm iş arkadaşlarımla paylaşırım (projeler hakkındaki bilgiler, çalışanlar hakkındaki kişisel bilgiler).	51	1.72	1.09
İş arkadaşlarımdan birinin bilgi güvenliği konusundaki kurallara veya düzenlemelere uymadığını gördüğümde onu görmezlikten gelirim.	51	2.05	1.12
Bilgi güvenliği konusunda önlemler almaktan sadece bilgi işlem departmanı sorumludur.	51	2.27	1.32
Bir şarkının sözlerinden bir bölümünü alıp her kelimenin baş harfini kullanarak oluşturulan şifre iyi bir şifre örneğidir.	51	2.37	1.32
Şifrelerimi cep telefonuma veya hafıza kartına kaydederim.	51	2.39	1.57
Hassas bilgiler içeren belgeleri atmak için parçalayıcı/dilimleyici kullanmam.	50	2.56	1.37
İş yerindeki bilgisayarımda şifre korumalı ekran koruyucu kullanmam.	51	2.66	1.57
Farklı hesaplar için aynı şifreyi kullanırım.	52	2.76	1.55
Çalışma saatleri içerisinde uzakta olsam bile ofisimin kapısını kilitlemem.	48	2.97	1.61
Birisi iş amaçlı birisi özel kullanım amaçlı olmak üzere en az iki şifre kullanırım.	51	3.29	1.47
Hassas bilgilerimi bir hafıza kartına veya bir harici harddiske kaydederim.	51	3.52	1.40
Masamın üzerinde çoğu zaman hassas belgeleri bulundurmam.	52	3.69	1.47

Demografik sorularla verilen yanıtlar arasında anlamlı bir farklılık olup olmadığını bulabilmek için uygulanan testler sonucunda (bkz. Tablo 3);

Cinsiyet ile farkındalık ölçeği ortalaması arasında uygulanan independent sample t testinin anlamlılık değeri 0.512'dir ve anlamlı bir farklılaşma bulunamamıştır.

Yaş ile farkındalık ölçeği ortalaması arasında uygulanan one way anova testinin anlamlılık değeri 0.812'dir ve anlamlı bir farklılaşma bulunamamıştır.

Çalışma pozisyonu ile farkındalık ölçeği ortalaması arasında uygulanan one way anova testinin anlamlılık değeri 0.702'dir ve anlamlı bir farklılaşma bulunamamıştır.

Mesleki deneyim ile farkındalık ölçeği ortalaması arasında uygulanan one way anova testinin anlamlılık değeri 0.240'tır ve anlamlı bir farklılaşma bulunamamıştır.

Öğrenim durumu ile farkındalık ölçeği ortalaması arasında uygulanan one way anova testinin anlamlılık değeri 0.169'dur ve anlamlı bir farklılaşma bulunamamıştır.

Günlük bilgisayar kullanım süresi ile farkındalık ölçeği ortalaması arasında uygulanan one way anova testinin anlamlılık değeri 0.969'dur ve anlamlı bir farklılaşma bulunamamıştır.

Günlük internet kullanım süresi ile farkındalık ölçeği ortalaması arasında uygulanan one way anova testinin anlamlılık değeri 0.969'dur ve anlamlı bir farklılaşma bulunamamıştır.

Kendime ait bilgisayarım var ifadesi ile farkındalık ölçeği ortalaması arasında uygulanan independent sample t testinin anlamlılık değeri 0.542'dir ve anlamlı bir farklılaşma bulunamamıştır.

Akıllı telefonum var ifadesi ile farkındalık ölçeği ortalaması arasında uygulanan independent sample t testinin anlamlılık değeri 0.383'tür ve anlamlı bir farklılaşma bulunamamıştır.

Tablet bilgisayarım var ifadesi ile farkındalık ölçeği ortalaması arasında uygulanan independent sample t testinin anlamlılık değeri 0.158'dir ve anlamlı bir farklılaşma söz konusu değildir.

Tablo 3. Hipotez Testleri

Bağımsız değişken	Bağımlı değişken	Test	Anlamlılık değeri (Sig.)	Sonuç
Cinsiyet	Bilgi güvenliği farkındalığı	Independent Sample T Testi	0.512	H1a hipotezi desteklenmemiştir.
Yaş	Bilgi güvenliği farkındalığı	One Way Anova	0.812	H1b hipotezi desteklenmemiştir.
Çalışma pozisyonu	Bilgi güvenliği farkındalığı	One Way Anova	0.702	H1c hipotezi desteklenmemiştir.
Mesleki deneyim	Bilgi güvenliği farkındalığı	One Way Anova	0.240	H1d hipotezi desteklenmemiştir.
Öğrenim durumu	Bilgi güvenliği farkındalığı	One Way Anova	0.169	H1e hipotezi desteklenmemiştir.
Günlük bilgisayar kullanım süresi	Bilgi güvenliği farkındalığı	One Way Anova	0.969	H1f hipotezi desteklenmemiştir.
Günlük internet kullanım süresi	Bilgi güvenliği farkındalığı	One Way Anova	0.969	H1g hipotezi desteklenmemiştir.
Kişisel bilgisayara sahip olma	Bilgi güvenliği farkındalığı	Independent Sample T Testi	0.542	H1h hipotezi desteklenmemiştir.
Akıllı telefona sahip olma	Bilgi güvenliği farkındalığı	Independent Sample T Testi	0.383	H1i hipotezi desteklenmemiştir.
Tablet bilgisayara sahip olma	Bilgi güvenliği farkındalığı	Independent Sample T Testi	0.158	H1j hipotezi desteklenmemiştir.

Sonuç ve Öneriler

Bu araştırmada Kuşadası'ndaki 5 yıldızlı konaklama işletmesi yöneticilerinin bilgi güvenliği farkındalıkları anket tekniği kullanılarak ölçülmüştür. Genel olarak yöneticilerin bilgi güvenliği farkındalık seviyelerinin yüksek olduğu sonucuna varılmıştır. Ancak sonuç ölçüm tekniğine göre farklılık gösterebilir, çünkü buradaki yanıtlar kişilerin kendilerini değerlendirmelerine ve kendi bildirimlerine dayanmaktadır.

Konaklama işletmesi yöneticilerinin güvenli şifre konusunda harf + sayı kullanmanın önemi bildiği görülmüştür. Ancak ölçekte yer alan güvenli şifre ile ilgili ifadelere verilen yanıtlar dikkate alındığında bir ikiye ayrılma söz konusudur. Yılmaz, Şahin ve Akbulut (2016)'nın öğretmenler

üzerinde yaptıkları araştırmanın sonucuna göre öğretmenlerin güvenli şifrenin nasıl olması gerektiği konusunda bilgi sahibi oldukları görülmektedir. Bu noktada araştırma sonuçları kısmen benzerlik göstermektedir.

Araştırma sonucunda, demografik değişkenlere göre ölçek maddeleri arasında uygulanan analizler sonucunda cinsiyete göre, yaşa göre, mesleki deneyime göre, öğrenim durumuna göre, günlük bilgisayar ve internet kullanım sürelerine göre anlamlı bir farklılık bulunamamıştır. Bu noktada araştırma sonuçları diğer araştırma sonuçlarıyla benzerlik göstermemektedir. Tekerek ve Tekerek (2013) ilköğretim ve lise öğrencileri üzerinde yaptıkları çalışmada yanıtların cinsiyete göre farklılık gösterdiği sonucuna ulaşmıştır. Yılmaz, Şahin ve Akbulut (2016) da cinsiyete göre verilen yanıtların farklılaştığını belirtmektedir. Ancak mesleki deneyime göre ve öğrenim durumuna göre öğretmenlerin yanıtlarında farklılık olmadığı ifade edilmiştir, bu noktada sonuçlar bu çalışmanın sonuçları ile paralellik göstermektedir. Bir diğer nokta ise öğretmenlerin günlük bilgisayar kullanım sürelerine göre yanıtlarında farklılık olduğudur. Konaklama işletmesi yöneticilerinin günlük bilgisayar kullanım süresine göre yanıtlarında farklılaşma tespit edilmemiştir.

Bu araştırmada örneklem olarak Kuşadası'ndaki 5 yıldızlı konaklama işletmesi yöneticileri seçilmiştir. Bu nedenle denek sayısı çok fazla değildir. Bundan sonra yapılacak çalışmalarda konaklama işletmelerinde personeller ve kullanılan teknolojik cihazlar ele alınarak bilgi güvenliği ölçümü yapılabilir. Ayrıca turizm endüstrisinde faaliyet gösteren seyahat işletmeleri, yiyecek içecek işletmeleri de bilgi güvenliği kapsamında ele alınabilir. Araştırmada anket tekniği kullanılmıştır, sonraki araştırmalarda farklı ölçüm teknikleri kullanılarak elde edilen sonuçlar kıyaslama yapılabilir.

Sonuç olarak, bilgi güvenliği konusunda en önemli unsurun insan olduğu göz önüne alınırsa farkındalık büyük önem taşımaktadır. Sadece işletmeler ve kurumlar bazında değil devletler bazında bilgi güvenliği çok önemli hale gelmiştir. Siber saldırılar her dakika dünyanın her yerinden her kesiminden gelebilmektedir. Bu nedenle teknolojiyle iç içe olan herkesin ve her işletmenin bilgi güvenliği konusunda önlemler alması zorunluluk haline gelmiştir. Buna yönelik olarak işletmelerin ve kurumların bilgi güvenliği konusunda eğitimler veya etkinlikler düzenlemesi önemli görülmektedir.

Kaynakça

Al, U. (2002). İnternette Veri Güvenliği. Oluşum Dergisi. 38, s. 37-50.

Çakmakçı, E. (2012), Bilgi Teknolojisi kullanımının otel performansı ve verimliliğine etkisi. Verimlilik Dergisi, 2012(4), 47-66.

Cronbach, L. J. (1990). Essentials of Psychological Testing. (Fifth Edition). New York: HarperCoIIins.

Federal Information Security Management Act, (2002), http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması. İlköğretim Online, 15(2).

Gülmüş, M. (2010), Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Güngör, M. (2015), Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, Bilgi Toplumu Dairesi Başkanlığı, Uzmanlık Tezi.

Information Security Forum. (2002). Effective security awareness workshop report. London, England.

Information Security Forum. (2003). The standard of good practice for information security. Version 4.0. Information Security Forum; 2003.

Kim, E. B. (2013). Information security awareness status of business college: Undergraduate students. Information Security Journal: A Global Perspective, 22(4), 171-179.

Kjørvik, H. (2010). Implementing and improving awareness in information security (Doctoral dissertation, University of Agder).

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. computers & security, 25(4), 289-296.

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, Ankara.

Sanal POS nedir?, https://www.vakifbankpos.com.tr/SanalPosNedir, Erişim Tarihi: 01.06.2016

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi Ve Oluşturma Yöntemleri. Akademik Bilişim, 9, 11-13.

Tekerek, M. ve Tekerek, A. (2013). A research on students' information security awareness. Turkish Journal of Education, 2(3), 61-70.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. Information Security Journal: A Global Perspective, 17(5-6), 207-227.

Veseli, I. (2011). Measuring the Effectiveness of Information Security Awareness Program. Master's Thesis Master of Science in Information Security, Department of Computer Science and Media Technology Gjøvik University College.

Whitman, M. E. ve Mattord, H. J. (2012), Introduction to information security. Principles of Information Security, 1-35.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. NIST Special publication, 800, 50.

Yılmaz, E., Şahin, Y. L., ve Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. Sakarya University Journal of Education, 6(2), 26-45.