OKU Fen Bilimleri Enstitüsü Dergisi
6(Ek Sayı): 402-414, 2023

OKU Journal of The Institute of Science and Technology,
6(Suppl): 402-414, 2023

Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi

Osmaniye Korkut Ata University Journal of The Institute of Science and Technology

Siber Güvenlik Konusunda Bilgi İşlem Yönetici ve Çalışanlarının Farkındalıkları**

Fatih Çağatay BAZ[1*], Kadir ULUDAĞ[2]

[1]Osmaniye Korkut Ata Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, 80010, Osmaniye
[2]Osmaniye Korkut Ata Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, 80010, Osmaniye

[1]https://orcid.org/0000-0002-6398-9851,
[2]https://orcid.org/0000-0002-7359-1396
*Sorumlu yazar: fatihcagataybaz@osmaniye.edu.tr

Araştırma Makalesi

Makale Tarihçesi:
Geliş tarihi: 13.01.2023
Kabul tarihi:18.04.2023
Online Yayınlanma: 20.12.2023

Anahtar Kelimeler:
Siber güvenlik
Siber saldırı
Siber güvenlik farkındalığı

ÖZ

Bilgi teknolojisinde yaşanan gelişmeler verilerin güvenliğinin sağlanmasını zorunlu kılmaktadır. Özellikle bankacılık, savunma ve benzer alanların hassasiyeti sebebiyle bilgi işlem dairelerinin siber güvenlik konusunda hassasiyetleri ortadadır. Bu anlamda milyonlarca öğrencinin ve personelin bulunduğu üniversiteler de siber güvenlik konusunda önemli kurumlardır. Bu çalışmanın amacı, Türkiye'de siber güvenlik konusunda üniversite bilgi işlem daire başkanlıklarının farkındalıklarının ilgili daire başkanları ve personelleri ile görüşmeler yapılarak, bu alanla ilgili mevcut durum ve yapılması gerekenlere yönelik gereklilikleri ortaya koymaya çalışmaktır. Bu çalışmada, nitel araştırma yöntemlerine dayalı olarak yarı yapılandırılmış görüşme tekniğiyle veriler toplanmıştır. Katılımcıların bilgileri, nitel araştırma yöntemlerinde kullanılabilen Nvivo 12 paket programı ile analiz edilmiş ve elde edilen bulgulara yer verilmiştir. Araştırmada elde edilen bulgulara göre, siber güvenlik konusunda üniversitelerde en önemli konunun bu alanda farkındalığın oluşturulması olduğu tespit edilmiş ve farkındalığın artırılmasına yönelik önermelerde bulunulmuştur. Bu açıdan çalışmanın alana ilgi duyan araştırmacılara katkı sağlayabileceği düşünülmektedir.

Awareness of IT Managers and Employees on Cyber Security

Research Article

Article History:
Received: 13.01.2023
Accepted: 18.04.2023
Published online: 20.12.2023

Keywords:
Cyber security
Cyber attack
Cyber security awareness

ABSTRACT

Developments in information technology necessitate the security of data. Especially due to the sensitivity of banking, defense and similar areas, the sensitivity of the IT departments about cyber security is obvious. In this sense, universities with millions of students and staff are also important institutions in cyber security. The aim of this study is to try to reveal the current situation in this field and the requirements for what needs to be done by interviewing the relevant department heads and personnel of the awareness of university IT departments on cyber security in Turkey. In this study, data were collected by semi-structured interview technique based on qualitative research methods. The information of the participants was analyzed with the Nvivo 12 package program, which can be used in qualitative research methods, and the findings were included. According to the research findings, it has been determined that the most important issue in universities about cyber security is raising awareness in this area and suggestions have been made to increase awareness. In this respect, it is thought that the study can contribute to researchers who are interested in the field.

** Bu çalışma, ikinci yazarın birinci yazar danışmanlığında hazırladığı yüksek lisans tezinden üretilmiştir

To Cite: Baz FÇ., Uludağ K. Awareness of IT Managers and Employees on Cyber Security. Osmaniye Korkut Ata Üniversitesi Fen Bilimleri Enstitüsü Dergisi 2023; 6(Ek Sayı): 402-414.

Giriş

Günümüzde siber güvenlik kavramı en dar kapsamda kişileri daha geniş kapsamda ise ülkeleri ve ülke içerisindeki resmi ya da özel kurum ve kuruluşları yakından ilgilendiren bir konu haline gelmiştir. Kamu kurumları ya da özel teşebbüsler uğradıkları siber saldırılar sonucunda ciddi anlamda maddi ve manevi kayıplara uğramaktadır. Bu açıdan bakılınca kurumlar bünyesinde teşkil edilmiş olan bilgi işlem birimlerinin bu konudaki farkındalık düzeyleri ve birikimleri hem kurum açısından hem de ulusal siber güvenliğin sağlanması açısından tartışılmaz bir öneme sahiptir.

Dünya hızla büyümektedir ve büyürken de bir o kadar küreselleşen dünyanın evrensel gelişim aracı bilişim teknolojileri olmaktadır. Türkiye'nin bilim ve teknolojide önemli bir konumda yer alabilmesinde bilişimin önemi tartışılmazdır. Bilgi teknolojileri, bilgiye erişimin sağlanması, toplanması, düzeltilmesi, saklanması, dağıtımının yapılması ve uygulanması işleviyle birbirleriyle ilgili parçalar grubundan meydana gelen teknolojileri tanımlamaktadır. Genellikle bilişim, özel yazılım sektörlerinde nitelikli işgücü darlığı yaşanılan, Türkiye ve birçok ülkede bilgi ekonomisine yönelik ekonomilerde yapısal dönüşümü gerçekleştirilme sürecinin ana sorunlarından birini oluşturmaktadır (Ekinci, 2006; Şener, 2006; Çalışır ve ark., 2011; Aydın, 2012).

Birçok kurum bilgilere erişimin sağlanma sırasında yetkilendirme açısından problem yaşamaktadır. Böylelikle sisteme erişim sağlayan kişiler önlerine çıkan tehditleri fark etmemektedir (İleri, 2017). Günümüzde birçok kurumda bilgi kaynaklarında erişimde ve yetkilendirme konusundaki bilgi eksikliği oldukça fazladır. Yapılan araştırmalar sonucunda (Eminağaoğlu ve Gökşen, 2009; Baykara ve ark., 2013; Doğan ve Abacı, 2021) bilgi kaynaklarına dair tehditlerde sorumlu kişilerin tespit edilmesinde zorluk yaşanmaktadır. Bunun sebebi ise bilgi kaynaklarında güvenlik konusunun yeterince izlenememesi ve sistemlere erişimlerin standartlar kapsamında kayıt altına alınmamış olmasıdır.

Bilgiye dair güvenliğin oluşturulması, organizasyonların sahip olduğu bütün bilgilerin her açıdan tehlikelere karşı önlemler alınarak bilgi güvenliğinin sağlanmasını amaçlamaktadır. Ayrıca işletmelerin izlediği normal iş akışları açısından da bilgilerin korunması durumu hassas bir mevzudur. Bilginin güvenliği konusu sadece bilişim sistemlerinin güvenliği anlamında olmamakta aynı zamanda bilgisayarın güvenliği ve şifrelerimizin güvenliği üstünde düşünülen bir kavram olmaktadır (Vural ve Sağıroğlu, 2008; Eminağaoğlu ve Gökşen, 2009; Baykara ve ark., 2013; Öztemiz ve Yılmaz, 2013; Laybats ve Tredinnick, 2016; Naicker ve Mafaiti, 2019). Bütün kuruluşlar sahip oldukları bilgilerin güvenliğinin sağlanması amacıyla kullanacağı sistemleri kendi bünyelerine özel olarak kullanmalıdır (Win, 2005).

Bilgi güvenliğinin temin edilmesinde e-imza, anti-virüs sistemleri, güvenlik duvarlarının oluşturulması ve erişim denetimi gibi uygulamalar yer almaktadır. Kullanıcıların hatalarından kaynaklı bazı güvenlik

sorunları anlaşılamamakta ve giderilememektedir. Bilgi güvenliğine yönelik oluşan tehditler, kurum veya kuruluşların maddi ve manevi açıdan zarar görmesine sebep olan tüm tehditleri içermektedir. Organizasyonların iç ve dış tehditlere karşı kendilerini koruyabilmeleri amacıyla bilgi güvenliği standartlarını etkili ve verimli şekilde kullanmaları gerekmekte, ayrıca kullanıcıların eğitilmesi gerekmektedir (Fung, ve ark., 2003; Yıldız, 2009; Baykara ve ark., 2013; Öztemiz ve Yılmaz, 2013).

Bu çalışmada konu hakkında tüm diğer kurum ve kuruluşlara lokomotif görevi yapmakta olan üniversitelerin bilgi işlem birimlerinde çalışan yönetici ve personelin farkındalık düzeylerinin tespit edilerek durum analizleri yoluyla aydınlatıcı tarzda bir belge ortaya konulması amaçlanmıştır.

Yapılan çalışmada, yükseköğretim kurumları bilgi işlem yöneticileri ve personelinin siber güvenlik konusundaki farkındalıkları araştırılmıştır. Yapılan araştırmanın temel amacı, yükseköğretim kurumlarındaki bilgi işlem yönetici ve çalışanlarının siber güvenlik ile ilgili farkındalık düzeylerinin incelenmesidir. Yükseköğretim kurumları bünyesinde çalışan personelin meslek hayatlarında ve kişisel gelişimlerinde bilgi teknolojilerinin yeri oldukça büyüktür. Bilgi teknolojilerindeki hızlı gelişim ve değişim üniversitelerdeki dijital yetenekleri de geliştirmiştir. Teknolojik gelişmelerin birçok olumlu sonucunun yanında olumsuzlukları da bulunmaktadır. Bu gelişmelere paralel olarak siber alana yönelik saldırılarda da artış meydana gelmektedir. Bu durum üniversiteler açısından farklı bir boyut oluşturmakla birlikte siber saldırılara karşı farkındalığın yaratılarak olası saldırılara karşı güvenlik önlemlerinin alınması son derece önem arz etmektedir. Bu konuda üniversitelerin bilgi işlem yöneticileri ve çalışanlarının sorumlulukları bulunmaktadır. Bu çalışma, üniversitelerin bilgi işlem yöneticileri ve çalışanlarının siber güvenliğe dair farkındalıklarının ölçülmesi ve değerlendirmesi açısından son derece önem arz etmektedir. Ayrıca çalışma konuyla ilgili literatüre katkı sağlaması ve yapılacak araştırmalar için örnek oluşturması açısından da önemlidir.

Materyal ve Metot

Türkiye'de aktif olarak faaliyetini sürdürmekte olan üniversite bilgi işlem yönetici ve çalışanlarının siber güvenlik konusundaki farkındalıklarının tespit edilmesine yönelik olarak yapılan bu çalışma, olgubilim deseni baz alınarak kurgulanmıştır. Çalışmada kullanılan veriler bir nitel araştırma tekniği olan görüşme yöntemi kullanılarak elde edilmiştir. Olgubilim diğer bir adıyla fenomenolojik model, deneyim ve duygularımızı inceleyerek bunların nasıl oluştuğu, başka kişilerle konuşurken bu duygu ve düşüncelerimizin nasıl aktarıldığı, kişide bilince dönüşürken yöntemsel olarak tasvir edilmesini sağlayan derin bir analize dayanmaktadır (Patton, 2002). Dolayısıyla olgubilim modelinde araştırmacı ölçmek istediği olguları görüşme, gözlem ve belge gibi veri toplama araçlarını kullanarak ayrıntılı olarak inceledikten sonra elde ettiği sonuçlar üzerinden temaları oluşturur. Katılımcıların dikkatinin deneyime odaklanmasını sağlamaya yönelik derinlemesine görüşme ve açık uçlu sorular kullanarak araştırmacılar araştırma konusu ile ilgili nitel verileri toplarlar (Christensen, Johnson ve Turner, 2011). Kullanışlı bir örneklem seçiminde kolaylıkla ve hızlı bir biçimde ulaşılabilir olma nitel araştırmalarda her ne kadar çok tercih edilen bir strateji olsa da araştırmanın sonuçlarını etkilemesi açısından

kullanımı çok istenmeyen bir durumdur (Patton, 2005). Araştırmacıların birçoğu örneklem kullanımının evrenin tamamı hakkında genelleme fırsatı veremeyeceğini düşündüğü halde ulaşılması kolay ve elde edilmesi daha az maliyetli olan durumları tercih etmektedirler (Ghosh ve Vogt, 2012). Dolayısıyla ulaşımdaki kolaylık ve düşük maliyetler önemli olsa da değerlendirme aşamasında en fazla bilginin elde edilebileceği bir strateji ile örneklemin seçilmesi son derece önemlidir. Çalışmanın katılımcılarını çeşitli üniversitelerde görev yapmakta olan 36 bilgi işlem yönetici ve çalışanı oluşturmaktadır.

Veri toplama aracı olarak görüşme formu kullanılmıştır. Çalışmada kullanılan görüşme formu iki kısımdan ibarettir. Birinci kısımda katılımcılara ait demografik bilgileri içeren sorular bulunmaktadır. İkinci kısımda ise katılımcıların siber güvenlik konusundaki farkındalıklarının incelenmesi amacıyla oluşturulan 15 sorudan oluşan görüşme formu bulunmaktadır. Bu çalışmada araştırmacının sormayı planladığı sorular görüşme öncesinde hazırlanmış ve dil uzmanları tarafından anlatım, şekil ve imla kuralları kontrol edilmiştir. Sorular açık uçlu hazırlanmış olup; katılımcının cevaplarını açmasına ve ayrıntı vermesine imkân sağlayabilecek şekilde kurgulanmıştır.

Elde edilen veriler görüşme formundaki sorularda aranan problemler ışığında çözümlenmiş sorular ve sorulara verilen yanıtlar karşılaştırmalı olarak incelenmiş ve sonuçları literatür taramalarıyla ilişkili olarak açıklamalı bir şekilde sunulmuştur.

Veriler kodlanırken nitel araştırmalarda sıklıkla kullanılan içerik analizi yöntemi kullanılmıştır. Bu yöntemin asıl amacı, "toplanan verileri açıklayabilmek için verileri derinlemesine analiz ederek fark edilemeyen kavramlara, ilişki ve temalara ulaşmaktır." (Yıldırım ve Şimşek, 2013).

Araştırmanın ilk aşaması olan bu adımda görüşme formu soruları ve görüşme formlarından elde edilen veriler teorik bilgiler ışığında ilişkisel olarak kodlanmıştır. Bundan sonraki adımda ise kodlanan sözcükler arasında anlam ilişkisi bağı kurulmak suretiyle ortak yönler tespit edilmiş ve buradan da hareketle araştırmanın alt problemlerine ilişkin sınıflandırma yapılmıştır. Bu sınıflandırma sonrasında oluşan ana ve alt sınıflar araştırmacının kendi fikir ve yorumlamalarına mahal vermeden objektif ve okuyucuların anlayabileceği şekilde izah edilmiştir. Üçüncü adımda, elde edilen verilerin daha anlamlı hale getirilmesi açısından bulgular ve veriler arasında sebep-sonuç ilişkisi sağlanmaya çalışılmış ve nihai aşamada bulguların yorumlanması neticesinde elde edilen sonuçlara yer verilmiştir.

Bulgular

Katılımcılarla yapılan görüşmeler neticesinde elde edilen veriler üzerinde içerik çözümlemesiyle kodlar elde edilmiştir. Elde edilen kodlar benzerliklerine göre bir araya getirilerek kategorize edilmiştir. Sunulan kategoriler temalarla ilişkilendirilmiştir.

Katılımcılara Ait Demografik Bilgiler

Araştırmaya katılanlara ait demografik bilgiler Tablo 1'de sunulmuştur.

Tablo 1. Katılımcıların demografik bilgilerinin dağılımı

		Frekans (n)	Yüzde (%)
Cinsiyet	Kadın	1	2,8
	Erkek	35	97,2
	Toplam	36	100,0
Eğitim Durumu	Ön Lisans	3	8,3
	Lisans/Üniversite	21	58,4
	Lisans Üstü/Yüksek Lisans	8	22,2
	Doktora	4	11,1
	Toplam	36	100,0
Yaş	18-30	1	2,8
	31-40	13	36,1
	41-50	13	36,1
	51-60	9	25,0
	Toplam	36	100,0
Kurumdaki Çalışma Süresi	1-5 Yıl	8	22,2
	6-10 Yıl	8	22,2
	10 Yıl Üzeri	20	55,6
	Toplam	36	100,0
Unvan	Memur	6	16,7
	Bilgi İşlem Daire Başkanı	23	63,9
	Mühendis	5	13,9
	Teknisyen	2	5,5
	Toplam	36	100,0

Tablo 1'de görüleceği üzere araştırmaya katılan katılımcıların 1'i kadın 35'i erkektir.3'ü ön lisans mezunu, 21'i lisans mezunu, 8'i yüksek lisans mezunu ve 4'ü doktora mezunudur. 1'i 18-30 yaş aralığında, 13'ü 31-40 yaş aralığında, 13'ü 41-50 yaş aralığında ve 9'u 51-60 yaş aralığındadır. Kurumda çalışma süreleri ise 8'inin 1-5 yıl, 8'inin 6-10 yıl ve 20'sinin 10 yıl üzeridir. 6'sı memur, 23'ü bilgi işlem daire başkanı, 5'i mühendis ve 2'si teknisyendir.

Araştırmanın Tema, Kategori ve Kodlarına İlişkin Bulgular

Araştırmada yapılan görüşmeler sonucu elde edilen veriler üzerinden yapılan ön incelemede, sorular ile ilintili olacak biçimde sekiz temel tema ortaya çıkarılmıştır. Elde edilen bulgulardan hareketle Şekil 1 oluşturulmuştur.

Şekil 1. Araştırma tema ve kategorileri

Araştırmada yapılan görüşmeler sonucunda elde edilen sekiz tema ile ilgili katılımcıların verdiği cevaplar aşağıda listelenmiştir.

Saldırı Türleri kategorisine verilen cevaplar:

K1: Her türlü bilgi hırsızlığı.

K:2 Bilgi barındıran her alan siber terörizmin kapsamındadır. Genelde bankacılık, eğitim, iletişim, sanayi, güvenlik sahaları daha yaygın hedef olmaktadır.

K3: Sosyal ve politik amaçlı özel ve kamu kurumları ağına yapılan her türlü yasa dışı saldırılar

K4: Sosyal mühendislik, sosyal medya zorbalığından ddos'a kadar tüm taciz ve saldırılar.

K5: En basit olarak web sayfalarının hacklenerek propaganda malzemesi olarak kullanılması.

Güvenlik Politikaları kategorisine verilen cevaplar:

K1: Devlet memurluğuna giriş aşamasında siber güvenlik eğitim ve uygulamaları yer almalı, asgari düzeyde siber güvenlik sertifikası istenebilir.

K2: Ülkemizin bu konuda yeterli çalışma yaptığını düşünüyorum, USOM, İSO27001, Cumhurbaşkanlığı Bilgi Güvenliği Rehberi, KVKK süreçlerinin tamamı zorunlu olmasından dolayı kurumlara ciddi farkındalık oluşturmuştur.

K3: Ülkemiz uygulanan politikalar konusunda çağı yakalamış durumdadır.

K4: Tecrübeli personeli ve iyi eğitim almış kadrolar gerekli.

K5: Yerli ürünler geliştirilmeli.

Teknolojik Yeterlilik kategorisine verilen cevaplar:

K1: Firewall cihazları ve güvenlik yazılımları.

K2: Ağ güvenlik sistemini yeni versiyon cihazlarla yeniledik. Personele siber güvenlik alanında bilgilendirici toplu e-postalar, kurum haberleri ve broşürler yayınladık.

K3: Güncel yazılımlar ve eğitimler sağlanıyor.

K4: Güvenli altyapı oluşturulmuştur.

K5: SIEM SOAR Sistemleri doğru kullanılarak riskler azaltılmalı.

K6: Açık kaynak kullanmak önemli. Ciddi bir ufuk sağlar. Kendi işletim sistemini yazmak, kendi güvenlik altyapısını kurup yönetmek müthiş bir duygu. Ayrıca ciddi ekonomik tasarruf sağlar. Önemli olan böyle faaliyetleri yapanların arkasında olmak ve onların önünü açmak. Bu süreçte aksamalar olsa dahi motivasyonu düşürmeyen teşvik eden yöneticiler lazım. Dezavantajı ise tam sisteme hâkim olmadan projeler üretmek ve kurumları sıkıntıya sokmak. Ayağını yorganına göre uzatmak lazım. Adım adım gelişmek çok önemli. Yöneticilerin engeli de cabası.

Eğitim Faaliyetleri kategorisine verilen cevaplar:

K1: Gerekli eğitim ve yazılımlar yenileniyor.

K2: ISO27001, KVKK süreçleri, alt yapı iyileştirmeleri ve personel eğitimleri ile önlemler alınmaktadır.

K3: Hizmet içi eğitimler düzenlenmekte.

K4: Online eğitimler verilmektedir. Bültenler yayınlanmaktadır.

K5: Siber güvenlik eğitimi alan personelin diğer personele eğitim vermesi veya uzman kişilerce eğitim verilmesi.

K6: İlk yapılan eğitimler daha çarpıcı ve verimli olurken devam eden eğitimler daha az farkındalık oluşturuyor.

K7: Verdiğimiz farkındalık eğitimlerinin personel üzerinde istediğimiz düzeyde etkisi olmadı. Personelde özellikle kurumsal aidiyet olmayınca eğitimlerin bir anlamı olmuyor. Mesela e-posta

sistemimizin ana sayfasında her açılışta şifrenizi hiçbir şekilde paylaşmayınız diyoruz. Ama gel gör ki her hafta birkaç personelimiz bilgilerini paylaşıyor. Uyarıda bulunsanız dahi dikkate almıyor.
K8: Güncel tehditlere karşı eğitim verilmeli.

Kurumsal Önlemler kategorisine verilen cevaplar:
K1: Siber saldırılara karşı bilinçlendirilmesi gerekir.
K2: Test senaryoları uygulanacak şekilde testler yapılmalıdır. Test hizmetleri alınmalıdır.
K3: Cumhurbaşkanlığı Bilgi ve İletişim Rehberi çok kapsamlı bir çalışma. Uygulanabilirse riskleri azaltacaktır.
K4: Özellikle Cumhurbaşkanlığı Dijital Dönüşüm Ofisi siber güvenlik rehberi ile oldukça üst bir seviyeye çıkmıştır. ISO27001 alınması gerekliliği yine kurumlara olumlu katkılar sağlamıştır.
K5: Üst yönetimin yaklaşımı diğer personellerde etkili olmaktadır. Ancak tamamen etkisi bulunmamaktadır.
K6: Kurum içi geliştirilen yazılımlara zafiyet önlemede daha hızlı çözümler üretilebilmektedir. Satın alınan yazılımlar da bu konu çok uzun sürede yapılmakta veya hiç yapılmamaktadır.
K7: Siber güvenlik konusunda firma yazılımları tercih edilmeli daha geniş bir ekiple daha güncel koruma sağlanabilir.

Bireysel Önlemler kategorisine verilen cevaplar:
K1: Güvenlik duvarı, anti virüs yazılımları, bilgi güvenliği eğitimleri.
K2: Eğitim alınıyor.
K3: Karşılaştığımız sorunları direkt bildirip gerekli önlemlerin alınmasını sağlamak.
K4: Bilinçli kullanıcı daha az etkileniyor.

Etkin Kullanım kategorisine verilen cevaplar:
K1: Son kullanıcıya düzenli eğitimler verilmeli kullanıcılar bilgilendirilmelidir.
K2: Bilgi işlem birimlerine gerçekten değer verilmeli. Bilişim personeli alımında KPSS ile değil, deneyimli personel alımı için kurumlara yetki verilmeli. Bu personele de maddi ve manevi destek verilip, başka yerlerde iş araması engellenmeli. Bilişim teknolojileri etkin kullanmak için personel olmazsa olmaz şart. Personel olmuyorsa o zaman YÖK ve Ulakbim Bilişim teknolojilerini üniversitelere kullandırması gerekmektedir. Üniversite değilde, kurum olarak bakacak olursak merkezi bir bilişim teknoloji altyapısı olması gerekmektedir. Bilişim Teknolojilerinde ayrıca yerli ve milli ürünler olması gerekiyor.
K3: Wireless doğrulama sisteminde 802.1x doğrulama sistemine geçtik.
K4: Görsel materyaller hazırlanmış ve bina girişlerine asılmış durumda. Belli aralıklarla duyuru epostaları atılmakta. Ve en az senede 1 kez eğitim planlanmaktadır.

K5: Tüm ağ trafiği firewall üzerinden geçmekte, kullanıcıların bilgisayarlarında ve bilgisayar laboratuvarlarındaki bilgisayarlarda antivirüs kurulması. Personel ve öğrencilerimize siber saldırılar konusunda farkındalık eğitimi verilmektedir.
K6: Bütünleşik yedekli güvenlik duvarı alt yapısı üzerinde çalışan port bazlı engelleme, uygulama bazlı engelleme, url tabanlı engelleme, dns koruması, thread, virüs kontrolleri, bulut tabanlı malware analizi, web application firewall, antispam gateway, siem sistemi.

Farkındalık Çalışmaları kategorisine verilen cevaplar:
K1: farkındalık yaratacak Videolar hazırlayarak, topluca veya yüz yüze bilgilendirmelerle.
K2: Düzenli penetrasyon testleri ile farkındalık yaratılmaya çalışılıyor.
K3: Katılım oranına göre, özellikle günümüzde siber saldırıların artmasından da dolayı, farkındalık oluşmaktadır.
K4: Büyük bir çoğunluğunda farkındalık oluşmasına rağmen, yeterli seviyede olmamaktadır. Siber güvenlik sadece birkaç eğitimle olacak bir şey değildir. Siz eğittikçe karşı saldırganlardan da kendilerini düzenli olarak eğitmekte ve firmaların yayınladıkları teknolojik açıkları kullanmaktadırlar, her zaman saldırılara karşı bilinçli ve uyanık olmak zorundayız.
K5: Sertifikalı olacak şekilde farkındalık eğitimleri çeşitlendirilmeli. Eğitimler etik hack eğitimi olmamalıdır. Siber güvenlik bilincinin artırılmasına yönelik giriş seviyesinde olmalıdır.
K6: Tüm bilgi teknolojileri kullanıcıları farkındalık düzeyinde eğitilmeli, buna ilave olarak bilgi işlem çalışanları ağ güvenliği ve bilgi güvenliği konusunda detaylı eğitimlere tabi tutulmalıdır. Eğitimlerde zafiyetlerden mustarip olmuş kurumlarla ilgili örnek vakalara yer verilmeli ve bunlar kendi kurumumuzdaki durum ile karşılıklı analiz edilmelidir. Örnek vakalar çalışanların daha iyi bilinç kazanmasına yol açıyor.
K7: Teorik ve pratik uygulama örnekleri üzerinden farkındalık oluşturulmalı.
K8: Üst yönetimin herhangi bir konudaki farkındalık düzeyi o konu için kesinlikle önemlidir.

Bu çalışma kapsamında üniversite bilgi işlem yönetici ve çalışanlarının siber güvenlik konusundaki farkındalıklarını incelemek amacıyla 36 katılımcıyla görüşme yapılmıştır. Çalışmaya katılan katılımcıların 1'i kadın 35'i erkektir.3'ü ön lisans mezunu, 21'i lisans mezunu, 8'i yüksek lisans mezunu ve 4'ü doktora mezunudur. 1'i 18-30 yaş aralığında, 13'ü 31-40 yaş aralığında, 13'ü 41-50 yaş aralığında ve 9'u 51-60 yaş aralığındadır. Kurumda çalışma süreleri ise 8'inin 1-5 yıl, 8'inin 6-10 yıl ve 20'sinin 10 yıl üzeridir. 6'sı memur, 23'ü bilgi işlem daire başkanı, 5'i mühendis ve 2'si teknisyendir.

Sonuç

Araştırmaya katılanlara yöneltilen birinci araştırma sorusu katılımcıların siber terörizmi nasıl tanımladıkları ile ilgilidir. Soruya katılımcıların çoğunluğu dijital ortamda kişi veya kurumlara yapılan saldırılar yanıtını vermiştir. Araştırmanın ikinci araştırma sorusu katılımcıların siber terörizm kapsamına hangi saldırıları dahil ettikleri ile ilgilidir. Katılımcıların çoğunluğu devlet ve şirketlerin bilgilerine yapılan saldırılar yanıtını vermiştir.

Katılımcıların kurumlarında siber güvenlik konusunda ne gibi önlemler aldıkları ile ilgili olarak üçüncü soru yöneltilmiştir. Katılımcıların çoğunluğu güvenlik kapsamında birçok farklı önlem yanıtını vermiştir. Araştırmanın dördüncü araştırma sorusu katılımcıların kurumlarında yönetici ve çalışanların siber güvenlik konusundaki farkındalıklarını geliştirmeye yönelik ne tür çalışmalar yaptıkları ile ilgilidir. Katılımcıların çoğunluğu eğitimler verilmekte yanıtını vermiştir.

Katılımcılara kurum çalışanlarına verilen siber güvenlik farkındalık eğitimlerinin kurum çalışanlarının farkındalık kazanmaları üzerindeki etkileri hakkındaki düşünceleri ile ilgili beşinci soru yöneltilmiştir. Katılımcıların çoğunluğu çoğunlukla etkili oluyor cevabını vermiştir. Araştırmanın altıncı araştırma sorusu katılımcıların kurumda düzenlenen siber güvenlik farkındalık eğitimlerinin bilgi işlem çalışanlarının iş yükü üzerindeki etkileri hakkındaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu etkisi yok cevabını vermiştir.

Araştırmanın yedinci araştırma sorusu katılımcıların kurumlar ve bireyler açısından kaçınılmaz olan bilişim teknolojileri kullanımının siber saldırılar üzerindeki etkileri hakkındaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu siber saldırı ve ihlaller artacaktır cevabını vermiştir. Araştırmanın sekizinci araştırma sorusu katılımcıların kurumlarının siber güvenlik konusunda yerli ürün geliştirilmesine ve kullanımına yönelik faaliyetler ile ilgilidir. Katılımcıların çoğunluğu maalesef herhangi bir faaliyet yok yanıtını vermiştir.

Katılımcıların kurumlarında siber saldırılara karşı kurumsal direncin artırılması için çalışanların nasıl bilinçlendirilmesi ve çalışanlara hangi eğitimlerin verilmesi gerektiği ile ilgili araştırmanın dokuzuncu sorusu yöneltilmiştir. Katılımcıların çoğunluğu güncel tehditlere karşı eğitimler verilmeli yanıtını vermiştir. Araştırmanın onuncu araştırma sorusu katılımcıların kurumlarının ciddi siber saldırılar karşısındaki teknolojik altyapısı ve deneyimi hakkındaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu gerekli güvenlik önlemleri alındı cevabını vermiştir.

Araştırmanın on birinci araştırma sorusu katılımcıların siber saldırılara karşı koymada bilişim teknolojilerinin etkin kullanımı için nasıl çalışmalar yapılması gerektiğini düşündükleri ile ilgilidir. Katılımcıların çoğunluğu teorik ve pratik uygulama örnekleri üzerinden farkındalık oluşturulmalı yanıtını vermiştir. Araştırmanın on ikinci araştırma sorusu katılımcıların ülkemizdeki siber güvenlik politikalarının etkinliği ve yeterliliği konusundaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu yeterli daha da artırılabilir yanıtını vermiştir.

Araştırmanın on üçüncü araştırma sorusu katılımcıların siber güvenlik zafiyetlerini önlemede açık kaynak kod yazılım ve işletim sistemlerinin kullanımının ne tür avantajlar veya dezavantajlar

sağlayacağı hakkındaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu maliyet avantajı sağlar cevabını vermiştir. Araştırmanın on dördüncü araştırma sorusu katılımcıların üst yönetimin siber güvenlik farkındalık düzeyinin kurumdaki siber güvenlik faaliyetlerine etkisi konusundaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu güvenliğin artırılmasında ve çözüm üretiminde etkili yanıtını vermiştir.

Araştırmanın on beşinci araştırma sorusu katılımcıların kurum içi geliştirilen uygulamalar ile firmalardan alınan yazılımların siber güvenlik zafiyetlerini önlemedeki etkililiği konusundaki düşünceleri ile ilgilidir. Katılımcıların çoğunluğu yetkin bir ekip çalışması gerekli yanıtını vermiştir.

Tartışma ve Öneriler

Son yıllarda bireylerin, kamu kuruluşlarının ve devlete ait bilgilerin muhafaza edilmesi ve korunması büyük önem taşımaktadır. Aynı zamanda bu bilgilerin korunması zorunlu hale gelmiştir. Bununla birlikte ülke için oldukça önemli olan kritik altyapıya dair sektörlerin de güvenliği sağlaması gerekmektedir. Siber güvenlik konusu bireysel ve kurumsal açıdan önemli bir konudur. Siber saldırılara maruz kalınmasına yönelik kurumlara, bu konu hakkında bilgilendirmelerin yapılması ve saldırılara dair korunma yöntemlerine uyulması gerekmektedir. Bu sayede saldırıların zararları en aza indirilebilecektir.

İnternet alanının gelişmesi ve teknolojinin hızla yenilenmesi sonucunda siber suçlarda artış gözlemlenmiş bununla paralel şekilde siber saldırıların oranlarında da artış meydana gelmiştir. Bu durumla mücadele edilmesine yönelik birçok çalışma yürütülmektedir. Siber suçlara ve saldırılara yönelik önlemlerin yanında yerli ve milli teknolojiler de üretilmeye başlanmıştır. Bütün bunlara ek olarak siber suçlara karşı daha etkili ve verimli bir şekilde mücadelenin gerçekleşmesi için kendi silahlarımızın kullanılması daha avantajlı bir durum sağlamaktadır. Önlemlerin alınmasında teknolojilerin kullanılmasının yanında bu konu hakkında gerekli politikaların ve stratejilerin de ortaya koyulması ve uygulanması gerekmektedir.

Siber suçlarla ve siber alanda güvenlik konusunda bilinçli olmak önemli bir etkendir. Siber suç ve siber alanda güvenlik konusunda bireyler, kurum ve kuruluşların bilinçlendirilmesi ve çeşitli eğitimlerin düzenlenmesi gerekmektedir. Böylelikle oluşabilecek herhangi bir saldırı sırasında meydana gelen zararın etkisi azaltılmış olacaktır. Çeşitli araştırmalar yapılarak toplumun siber güvenliğe dair bilgi düzeyinin tespit edilmesi ve toplumun bilinçlendirilmesine yönelik adımların atılması gerekmektedir.

Üniversiteler bir ülkenin en üst düzey akademik kurumları olması nedeniyle siber güvenlik alanında gerek eğitim gerek yeni ürün geliştirme gerek inovasyon gerekse sektörel bazda ihtiyaç duyulan iş gücünü yetiştirmesi açısından son derece önemli kurumlardır. Dolayısıyla bu kurumların siber güvenlik faaliyetlerinde lokomotif rolü üslenmesi beklenmektedir. Bu vizyonu gerçekleştirmek için üniversitelerdeki tüm çalışanların, üst yönetimin ve bilgi işlem çalışanlarının aktif şekilde rol alması gerekir. Özellikle siber güvenlik açıklarının giderilmesi amacıyla yeni ürün geliştirme, açık kaynak

kod sistemlerin kullanımı, yerli ve milli ürünlerin geliştirilmesi hususunda üniversite üst yönetimlerinin bilgi işlem yönetici ve çalışanlarından kopuk olmaması, iş süreçleri ve faaliyetleri hakkında yeterli bilgiye sahip olması ve bu anlamda vereceği destek çok önemlidir.

Çıkar Çatışması Beyanı

Makale yazarları aralarında herhangi bir çıkar çatışması olmadığını beyan ederler.

Araştırmacıların Katkı Oranı Beyan Özeti

Yazarlar makaleye eşit oranda katkı sağlamış olduklarını beyan ederler.

Kaynakça

Aydın İ. Bilişim sektörü ve Türkiye'nin sektördeki potansiyeli. International Journal of New Trends in Arts, Sports & Science Education 2012; 1(1): 180-200.

Baykara M., Daş R., Karadoğan İ. Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. First International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, 231-239 Elâzığ, Turkey.

Christensen LB., Johnson B., Turner LA. Research methods, design, and analysis; 2011.

Çalışır F., Çiğdem A. Gümüşsoy İİ. Factors affecting intention to quit among it professionals in Turkey 2011; Personnel Review, 40(4): 514-533.

Doğan A., Abacı F. Türkiye'de siber terörizme karşı bilişim teknolojilerinin kullanımı, Uluslararası Toplum Araştırmaları Dergisi 2021; 18(42): 5970-5998.

Ekinci H. Bilgi teknolojilerinin rekabet açısından önemi ve değişim yönetimindeki etkilerine ilişkin yöneticilerin algılarını ölçmeye yönelik bir araştırma, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 2006; 11(1): 54-70.

Eminağaoğlu M., Gökşen Y. Bilgi güvenliği nedir, ne değildir, Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi 2009; 11(4): 10-15.

Fung ARW., Farn KJ., Lin AC. A study on the certificiation of the information security management systems. Computer Standarts & Interfaces 2003; 25(5): 447-461.

Ghosh D., Vogt A. Outliers: an evaluation of methodologies. ın joint statistical meetings; 2012.

İleri YY. Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama, Anadolu Üniversitesi Sosyal Bilimler Dergisi 2017; 17(4): 55-72.

Laybats C., Tredinnick, L. Information security. Business Information Review 2016; 33(2):76-80.

Naicker V., Mafaiti M. The establishment of collaboration in managing information security through multisourcing. Computers & Security 2019; 80: 224-237.

Öztemiz S., Yılmaz B. Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. Bilgi Dünyası 2013; 14(1): 87-100.

Patton MQ. Two decades of developments in qualitative inquiry: a personal, experiential perspective. Qualitative Social Work 2002; 1(3): 261-283.

Şener S. Karar destek ve üst yönetim bilişim sistemleri ve Türkiye'de bilişim sektöründe bir analiz. Yüksek lisans tezi. Beykent Üniversitesi, İstanbul, Türkiye, 2006.

Vural Y., Sağıroğlu Ş. Ülke bilgi güvenliği. 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 25-26-27 Aralık 2008, 3-8, Ankara, Türkiye.

Win KT. A Review of security of electronic health records. Health Information Management 2005; 34(1): 13-18.

Yıldırım A., Şimşek H. Sosyal bilimlerde nitel araştırma yöntemleri. 9. genişletilmiş baskı. Ankara: Seçkin Yayınevi; 2013.

Yıldız Ç. Telekomünikasyon sektöründe firma içindeki bilgi güvenliğini etkileyen faktörler ve bu faktörlerin çalışanlar üzerine etkileri. Yüksek lisans tezi, Gebze Yüksek Teknoloji Enstitüsü, Gebze, Türkiye, 2009.