İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 19(38), Güz 2020, 208-223.

İSTANBUL TİCARET ÜNİVERSİTESİ
FEN BİLİMLERİ DERGİSİ

Istanbul Commerce University Journal of Science

http://dergipark.gov.tr/ticaretfbd

Araştırma Makalesi / Research Article

KVKK VE GDPR KAPSAMINDA FİRMALARIN MEVCUT DURUM ANALİZİ ÜZERİNE BİR İNCELEME*

RESEARCH ON FIRMS' CURRENT SITUATION ANALYSIS WITHIN THE SCOPE OF THE KVKK AND GDPR

Reyhan Nur SAVAŞ[1] **Abdül Halim ZAİM[2]** **Muhammed Ali AYDIN[3]**

Sorumlu Yazar / Corresponding Author
reyhan.nur.hut@gmail.com

Geliş Tarihi / Received
12.05.2020

Kabul Tarihi / Accepted
04.06.2020

Öz

Bu çalışmada, bilgi teknolojisi departmanına sahip olan kurumlara anket çalışması yapılarak; KVKK ve GDPR kapsamında kurumların uyum sürecinde, mevcutta bilgi varlıklarına yönelik aldıkları önlemleri saptamak, KVKK ve GDPR ile ilgili temel kavramları bilme düzeylerini ölçerek uyum sürecinin ne derece anlaşıldığı saptanmak istenmiştir. Bahsedilen anket çalışması, İstanbul'da bilişim, teknoloji, eğitim ve endüstri sektöründen birbirinden farklı 38 firma ile temelde 3 ana sorun belirlenerek gerçekleştirilmiştir. Birinci olarak, firmalardaki yetkili kişilerin bilgi güvenliği farkındalıklarını tespit etmeye yönelik sorular sorulmuştur. İkinci olarak, bu yetkili kişilere KVKK ve GDPR kapsamında temel terimler sorularak uyum sürecini doğru anlayıp anlamadıkları tespit edilmeye çalışılmış ve son olarak firmaların karşılaştıkları ataklar ve bu ataklara karşı alınan tedbirler hakkında teorik bilgi edinilmiştir.

Anahtar kelimeler: BGYS, bilgi güvenliği, GDPR, ISO 27001, KVKK, sızma testleri.

Abstract

In this study, a questionnaire study conducted to organizations that have Information Technologies Department; in their adaptation process within the scope of the KVKK and GDPR, it is aimed to determine the precautions that they take for their information assets, and to determine the extent to which the orientation period is understood by evaluating their level of knowledge of basic concepts about the KVKK and GDPR. The mentioned survey study, conducted with 38 different companies in the sectors of informatics, technology, education, and industry in Istanbul; essentially 3 major issues are specified. First, questions enquired to authorized persons at the firm to ascertain their information security awareness. Secondly, within the KVKK and GDPR, fundamental terms are asked to that authorized personnel in order to determine whether they understood the adaptation process right or not. Lastly, theoretical information obtained about the attacks that companies faced, and the measures taken against those attacks.

Keywords: GDPR, information security, ISMS, ISO 27001, KVKK, penetration tests.

**Bu çalışma, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü'nde yapılan "KVKK VE GDPR KAPSAMINDA FİRMALARIN MEVCUT DURUM ANALİZİ ÜZERİNE BİR İNCELEME" başlıklı yüksek lisans tezinden hazırlanmıştır.*

[1]İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Küçükyalı, İstanbul, Türkiye.
reyhan.nur.hut@gmail.com, Orcid.org/0000-0003-1138-1024.

[2]İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Küçükyalı, İstanbul, Türkiye.
azaim@ticaret.edu.tr, Orcid.org/0000-0002-0233-064X.

[3]İstanbul Üniversitesi- Cerrahpaşa, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Avcılar, İstanbul, Türkiye
aydinali@istanbul.edu.tr, Orcid.org/0000-0002-1846-6090.

1. GİRİŞ

Genel Veri Koruma Yönetmenliği (General Data Protection and Regulation) Avrupa ülkelerinde görülürken, bu düzenlemenin ülkemiz için oluşturulmuş olan Kişisel Verileri Koruma Kanunu (KVKK), ülkemizde 7 Nisan 2016 tarihi itibariyle firmalarda uyum sürecinin başladığını ve o tarihten 2018 yılına kadar uyum sürecinin tamamlanmış olduğunu ve böylece kanunun artık yürürlükte olduğu kabul edilmiştir. Fakat gerek alınan yetersiz önlemler gerek bu sürecin yeteri kadar anlaşılamaması sonucu bugün birçok firmada varlık kaybı, yetersiz teknolojik önlemlerden kaynaklı siber saldırılar, vb. gibi sorunların devam ettiği görülerek aslında kurumlarda bilgi güvenliği meselesinin dikkat edilmesi gereken bir nokta olduğu fikri oluşmaya başlamıştır.

Kurumsal bilgi güvenliğinin sağlanması için kurumun bilgi varlıklarını iyi tanıması, olası riskleri belirlemesi ve gerekli önlemleri alması için yönetimsel bir sürecinin olması gerekmektedir. Bu aşamaları gerçekleştiren firmaların varlık kaybının, bilgi güvenliğini sağlamak için gerekli aşamaları gerçekleştirmeyen firmalara oranla daha az olduğu tespit edilmiştir.

Bu çalışmada, kurumsal bilgi güvenliği için tehditleri ve alınması gereken önlemler, yönetimsel bir süreç olan Bilgi Güvenliği Yönetim Sistemi (BGYS) ana hatları ile açıklanacak, KVKK ve GDPR kapsamında veri işleme ve veri işleme prensiplerinden bahsedilecek ve bilgi varlıkların güvenliği için yapılan sızma testleri aşamaları ve bu zafiyet keşif araçlarından bahsedilecektir. Son olarak anket çalışmasında elde edilen veriler verilerek; analiz edilecektir.

2. KURUMSAL BİLGİ GÜVENLİĞİ

Bilgi güvenliği kavramını ele alındıktan sonra kurumsal bilgi güvenliğini anlamak daha anlamlı olacaktır. Bilgi güvenliği, varlık olarak ele alınan, yanlış kişiler tarafından ele geçilmesi istenilmeyen bilginin, olası tahribatlardan gerekli teknolojik önlemler ve amaçlar doğrultusunda dijital veya fiziksel ortamda korunması olarak tanımlanabilir (Canbek ve Sağıroğlu, 2006).

Kurumsal bilgi güvenliği, kurumların varlık olarak korunmasını istedikleri bilginin ne olduğunun tespit etmesi, olası tehlikelere karşı güvence altına alınmak istenerek güvenlik açıklarının belirlenmesi ve alınan bu tedbirler vasıtasıyla bilgi varlıkların güvenliğine yönelik analizlerin yapılmasıdır (Vural ve Sağıroğlu, 2008).

2.1. Kurumsal Bilgi Güvenliğine Yönelik Tehditler

Yapılan tanımlar doğrultusunda, kurumlarda bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğini olumsuz olarak etkileyen faktörlere kurumsal bilgi güvenliğine yönelik tehditler olarak bakılabilir. Kurumsal bilgi güvenliğine yönelik tehditler; insan kaynaklı tehditler ve doğa kaynaklı tehditler olarak ele alınır (Yaşar ve Çakır, 2015).

İnsan kaynaklı tehditler; bilgi güvenliğini olumsuz etki edecek sonuçlar meydana getiren kasıtlı veya kaza ile bireylerin oluşturduğu tehlike çeşididir. İnsan kaynaklı tehditler, kurum içindeki kişilerden veya kurum dışındakilerden gerçekleşmesi mümkündür (Irmak ve Baz, 2019).

Kurumların karşılaşabilecekleri en yaygın tehditler aşağıda belirtildiği gibidir(Irmak ve Baz, 2019):

Tablo 1. Kurumsal Bilgi Güvenliğinde En Yaygın Tehditler

Veri İhlalleri ve Bilgi Sızıntısı
Sosyal Mühendislik
İzinsiz İndirmeler
Kötücül Yazılımlar
Spam
Kod Enjeksiyonu
Hizmet Aksattırma
Dağıtık Hizmet Aksattırma
Kimlik Hırsızlığı
Gelişmiş Sürekli Tehdit
Botnet
Fiziksel Zarar Verme ve Hırsızlık

1. Veri İhlalleri ve Bilgi Sızıntısı: bilginin kasıtlı veyahut kasıtsız olarak açığa çıkması veri ihlali olarak adlandırılırken; firmalardaki teknik sistem bilgisinin ortaya çıkmasına bilgi sızıntısı denir.

2. Sosyal Mühendislik: saldırganın e-posta, telefon görüşmeleri, vb. gibi yollarla kurbanları kandırarak kişisel bilgileri elde etmesi ile sonuçlanan tehdit çeşididir.

3. İzinsiz İndirmeler: zararlı kod bulunan bir siteye saldırıya uğrayacak olan kişinin girmesi ile bu kodun kurbanın sistemlerine yerleşmesi ve bu sistemlerde bulunan zafiyetlerin keşfedilip; kullanılmasıyla gerçekleşecek olan tehdit çeşididir.

4. Kötücül Yazılımlar: İstenilen verilerin elde edilmesi amacıyla sistemlere yönelik zafiyetleri bulan tehdit çeşididir. Örneğin; istismar kodları, Truva atları, vb., gibi.

5. Spam: kötücül yazılımların yayılmasını sağlayan ve genelde e-posta üzerinden yayılan tehdit çeşididir.

6. Kod Enjeksiyonu: saldırıya uğrayan kişinin sistemlerinde bulunan güvenlik açığı göz önüne alınarak, saldırganın bu sistemleri ilgili açıklarla sömürmesi sonucu oluşan tehdit çeşididir. Örneğin; SQL Enjeksiyonu, SSL Enjeksiyonu, vb., gibi.

7. Hizmet Aksattırma (DoS): Saldırıya uğrayan sistemlerin veri tabanlarının gereksiz sorgularla meşgul edilmesi ile gerçekleşen tehdit şeklidir.

8. Dağıtık Hizmet Aksattırma (DDoS): Hizmet aksattırma tehdidinden farklı olarak; saldırıya uğrayan firmaların sistemlerindeki veri tabanlarına birden fazla saldırgan tarafından aynı anda yüklenmesi gerçekleşen tehdit şeklidir.

9. Kimlik Hırsızlığı: saldırıya uğrayan kişinin kredi kartı, kimlik bilgileri, vb., gibi kişisel bilgilerinin dolandırıcılık amacıyla kullanılması sonucu oluşan tehdit biçimidir.

10. Gelişmiş Sürekli Tehdit (APT): devletler ve gruplar arasında gerçekleşen ve siber alanda ulaşılmak istenilen bir nokta belirlenerek gerçekleşen tehdit çeşididir.

11. Botnet: saldırıya uğrayan kişilerin sistemlerine güvensiz olan ortamlardan yapılan indirmeler sonucunda yüklenen ve bot adı verilen bilgisayarların bir araya gelerek bir ağ oluşturması (botnet) sonucu oluşan tehdit çeşididir.
12. Fiziksel Zarar Verme ve Hırsızlık: doğal afetler sonucu karşılaşılması mümkün olan ve kurum içindeki cihazların çalınması gibi durumlar sonucu oluşabilecek olan tehditlerdir.

Doğa kaynaklı tehditler; doğal afetler (deprem, sel, vb., gibi) sonucu oluşabilecek olan tehditlerdir (Yaşar ve Çakır, 2015).

2.2.Kurumsal Bilgi Güvenliğine Yönelik Önlemler

Belirtilen tehditler sonucu firmaların bilgi varlıklarına yönelik almaları gereken önlemler ise; eğitim ve çalışanların farkındalıkları, çalışanların yetkilendirme denetimi, yönetsel ve teknolojik önlemler ve son olarak yedekleme ve felaket kurtarma merkezi olarak sıralanabilir (Irmak ve Baz, 2019).

Tablo 2. Kurumsal Bilgi Güvenliğine Yönelik Önlemler

Eğitim ve Çalışanların Farkındalıkları
Çalışanların Yetkilendirme Denetimi
Teknolojik ve Yönetsel Önlemler
Yedekleme ve Felaket Kurtarma Merkezi

2.2.1. Eğitim ve çalışanların farkındalıkları

Kurumun, çalışanlarına olası saldırılara karşı bilgilendirilmelerine yönelik eğitim gibi faaliyet düzenleyerek saldırıları önleyebilecekleri yöntemdir (Irmak ve Baz, 2019).

2.2.2. Çalışanların yetkilendirme denetimi

Kurum çalışanlarının çalıştıkları alanlarla ilgili kısımlara erişebiliyor olması yani sunucu odasına sistem ile ilgilenen kişilerin girip işlem yapması ya da çalışanların görev tanımı dışındaki alana erişememesi olarak da tanımlanabilir (Irmak ve Baz, 2019).

2.2.3. Teknolojik ve yönetsel önlemler

Teknolojik önlemleri yazılım ve donanım tabanlı olarak ele alınır (Tan ve Aktaş, 2011). Bunlar: güvenlik duvarı, ağ erişim kontrolü, veri kaçaklarını önleme sistemi, zafiyet tarama sistemleri, saldırı tespit sistemleri, vb. gibi.

Yönetsel önlemler ise, kurumların bilgi varlıklarını korumanın kompleks yapıda olduğu ve disiplin odaklı denetimsel bir çalışma gerektirdiğinden dolayı Bilgi Güvenliği Yönetim Sistemi (BGYS) gibi bir yönetim sistemi ile alınabilir (Vural ve Sağıroğlu, 2008).

2.2.4. Yedekleme ve felaket kurtarma merkezi

Kurumların iş sürekliliklerinin sağlaması, bilgi varlıkları olan verinin yedeklenmesi ve sistemlerde sürekli olarak gerçekleşen veri akının kesintisiz devam etmesi için bir yedekleme ve felaket kurtarma merkezi alınabilecek en iyi önlemlerden biridir (Can ve Akbaş, 2014).

3. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ (BGYS)

Kurumsal bilgi güvenliği teknolojik altyapı, çalışanlar, sistemsel süreçler ve bilgi sistemlerini kapsayan, bu kavramları bir yapı altında toplayan bir yandan da denetimsel ve yönetimsel bir merkezi noktaya ihtiyaç duyulmuştur. Kurumlarda bu ihtiyacı karşılayan ve her bir olgunun risk analizini hesaplayıp riskleri minimize eden bir BGYS oluşturulmalıdır. ISO 27001 standartları kapsamında olan BGYS kurumlardaki yönetimsel sistemin bir parçasıdır (Şen ve Yerlikaya, 2013).

ISO 27001, BGYS'nin kabul edilebilir olması için gerekli aşama ve adımları belirten ve kurumların bilgi güvenliklerini nasıl sağlayabileceğinin belirten ve bu işlem için model sunan bir dokümandır. BGYS'nin süreklilik gerektirdiği göz önüne alındığında, kurumun politikaları doğrultusunda riskleri kontrol etmek ve BGYS'nin başarımını takip etmek, ihtiyaçlar doğrultusunda revize etmek gerekir. Buradan yla çıkarak BGYS'de Planla- Uygula- Kontrol Et-Önlem (PUKÖ) döngüsü temel alınmıştır (Gülmüş, 2010).

3.1. BGYS Oluştururken Yapılacak Adımlar

Bilgi Güvenliği Yönetim Sistemini oluşturmak isteyen kurumların, bilgi varlıkları doğrultusunda güvenlik politikaları oluşturmalı, varlıkları belirlenmeli, olası veri sızıntıları gibi durumların senaryolarını önceden belirleyerek ilgili durumlar ile riskler ve alınması gereken önlemler tespit edilmeli yani bilgi güvenliklerinin organizasyonunu sağlamaları gerekir. Kurumun fiziksel güvenliğinin sağlanması ve çalışanların erişim sağlayacakları alanlar belirlenerek; erişim denetim politikası belirlenmeli ve yapılan bu adımların sürekli kontrol edilmesi ve revize edilmesi ile gerçekleşen süreçtir (Yılmaz, 2014).

4. KİŞİSEL VERİLERİN KORUNMASI KANUNU (KVKK) ve GENEL VERİ KORUMA YÖNETMENLİĞİ (GENERAL DATA PROTECTION AND REGULATION- GDPR)

Bu bölümde Kişisel Verilerin Korunması Kanunu (KVKK) ve Genel Veri Koruma Yönetmenliği (GDPR) tanımları verilerek genel olarak veri işleme ilkelerinden bahsedilecektir.

4.1. Kişisel Verilerin Korunması Kanunu (KVKK)

7 Nisan 2016 tarihinde yürürlülüğe giren, kişisel verinin işlenmesinde verinin işlendiği kişinin temel hak ve özgürlüklerinin korunması temel alınarak, bu verileri işleyenlerin uymaları gereken usulleri kapsayan bir düzenlemedir (Kişisel Verileri Koruma Kurumu [KVKK], 2018).

Veri işleme kurallarını aşağıdaki gibi sıralamak mümkündür:

1. Ülkemizde bulunan hukuk sistemine uygun ve dürüstlük kurallarıyla örtüşmeli,
2. Veriye ihtiyaç duyulduğunda, verinin doğrulanabilir ve güncel olmalı,
3. Verinin işlendiği amaçla ilgili, sınırlı ve ilişkili, gerekli zaman boyunca muhafaza edilmelidir.

4.2. Genel Veri Koruma Yöntemleri (GDPR)

25 Mayıs 2018 tarihinde yürürlüğe giren ve Avrupa Birliği ülkelerinde bulunan tüm vatandaşlar için verilerinin gizliliği ve korunması amacıyla oluşturulan bir düzenlemedir (IAB, bt).

Veri işleme kurallarını aşağıdaki gibi sıralamak mümkündür:

1. Veri işlemede şeffaf ve hukuka uygun olmalı
2. Verilerin ilişkili olduğu amaçla sınırlanmalı
3. Veri kalitesi, doğruluğu ve hesap verilebilirliği olmalı
4. İlgili verinin tutulmasındaki zaman kısıtlanmalı
5. Verinin gizliliği ve bütünlüğü korunmalıdır (Kişisel Verilerin Korunması Platformu [KVKP], 2019).

Bu iki kanun birbiri ile kıyaslandığında iki düzenlemenin de kişisel verilerin ilişkili olduğu kişinin korunmasının amaç olarak alındığı, şeffaflığın ve hukuka uygunluğun önemli olduğu sonucuna varılmıştır.

5. SIZMA TESTLERİ

Kurumların ağ altyapılarını, yazılım ve donanımları ile uygulamalarını kısacası bilişim sistemlerine saldırganın saldırabilme ihtimali düşünülerek; sistemlere siber saldırı yapılmasıyla zafiyetlerin keşfedilmesine, bu senaryoların simüle edilmesi ve gerçekleşen bu adımların raporlanmasıdır (Secops, bt). Üç farklı şekilde gerçekleştirilebilir:

1. Black box: Testi yapacak olan kişi/kişinin kurumun bilgisi dahilinde olmaksızın sadece hedef sistem gösterilere yapılan sızma testi çeşididir (Secops, bt).

2. White box: Testi yapacak olan kişi/kişilerin kurumun bilgisi dahilinde ilgili sistem bilgileri verilerek yapılan sızma testi çeşididir (Secops, bt).

3. Gray box: Black box ve White box testlerini kapsayan ve seviyesi düşük yetkilerle kurumun sistemlerine sızma denetimi gerçekleştiren sızma testi çeşididir (Secops, bt).

Sızma testleri yapılırken gerçekleştirilen adımlar;

- Gerçekleşecek olan saldırı önce planlanır,
- Kurumun bilgi varlıkları hakkında bilgi toplanır,
- İlgili sistemlere saldırı gerçekleştirilerek zafiyetler bulunur,
- Bulunan zafiyetler olası sömürü senaryoları dahilinde kullanılır,
- Son olarak bu senaryolar, alınan aksiyonlar raporlanarak kurumda yetkili kişiye ilgili rapor teslim edilir (Vural ve Sağıroğlu, 2010).

5.1. Sızma Testlerinde Kullanılan Araçlar

Bu bölümde, sızma testleri gerçekleştirilirken kullanılan araçlar ele alınacaktır.

5.1.1.Bilgi toplama araçları

Bilgi toplama aşamasında, en etkili aşama kurumun sosyal medya hesapları, resmi web siteleri incelenebilir. Ayrıca Bilgi toplama aşaması aktif ve pasif tarama araçları olarak iki kısımda incelenebilir (Beyaznet, 2019).

Pasif Bilgi Toplama; ilgili hedefle bilgi toplamanın yapıldığı fakat bu ilgilinin haberi olmayan bilgi toplama çeşididir. Örneğin; Whois, nslookup, vb. gibi.

- Whois; hedef alınan kurumun alan adının sorgulanması ile tutulan kayıtları keşfeden servistir.

- Nslookup; nSlookup dns sorgusunun yapılması ile kullanıcı alan adını ve ip adreslerini bulan bir araçtır (Beyaznet, 2019).

Aktif Bilgi Toplama; ilgili hedefle bilgi toplamanın yapıldığı ve pasif bilgi toplamanın aksine ilgili kişinin haberinin olduğu bilgi toplama çeşididir. Örneğin; Sandmap, BruteX, vb. gibi.

- Sandmap; ilgili hedefin sistem ve ağlarını keşfeden ve yaygın bir araç olan nmap'i kullanan bir bilgi toplama aracıdır.

- BruteX; ilgili hedefin SSH gibi protokollerinin kullanılmasına olanak sağlayan ve kaba kuvvet saldırısı uygulanmasını sağlayan bilgi toplama aracı çeşididir (Beyaznet, 2019).

5.1.2. Zafiyet tarama araçları

Zafiyet tarama araçları, kurumun sahip olduğu servisleri, ağ mimarisi bilgisayarları, portları, vb., gibi sistemlerin taranarak var olan güvenlik zafiyetlerini keşfeden araçlardır. Örneğin; Nessus, Nmap, vb. gibi.

- Nmap; kurumun işletim sistemlerinin ve servislerinin tespit edilmesi ve ağ haritasının çıkarılmasını sağlayan zafiyet tarama aracıdır.

- Nessus; kurumun sistemlerinde var olduğu bilinen güvenlik açığını denetleyerek; varsa bu güvenlik açığını oluşturduğu raporun içerisine dahil eder (Sparta Bilişim, bt).

Ayrıca web üzerindeki güvenlik açıklarını tespit eden ve kurumlarca tespit edilen web güvenlik zafiyetlerini keşfeden araçlarda vardır. Örneğin; Netsparker, Burpsuite, vb. gibi (Vural ve Sağıroğlu, 2007).

Bilgi toplama ve zafiyet tarama araçları kullanılarak; kurumlardaki zafiyetler tespit edilir ve böylece elde edilenler rapor edilerek sızma testleri tamamlanır.

6. BULGULAR

Yapılan anket çalışmasında KVKK ve GDPR kapsamında kurumların uyum sürecinde uygulamaya başladıkları kanunsal tedbirlerin boyutu ve idrak seviyesi analiz edilmek istenmiştir. Bu minvalde ankette elde edilmek istenen 4 boyut belirlenmiştir.

1.Sektörlerin KVKK ve GDPR kapsamındaki uyum sürecinde aldıkları önlemleri, idrakleri sektör bazlı karşılaştırarak; sektörlerin ne şekilde uyum sağladığını analiz etmek;

2.Kurumlarda BGYS olduğunu belirten firmaların aldıkları önlemleri, BGYS gereği alınması ve yapılması gerekenleri yapıp yapmadıklarını saptamak;

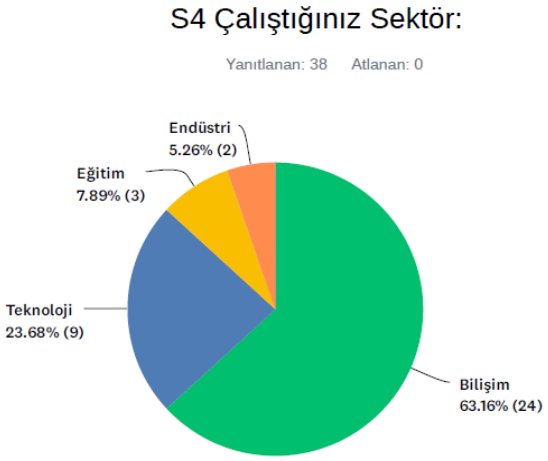
3.KVKK ve GDPR kapsamında firmaların Kişisel Verileri Korumadaki mantığı kavramsal boyutta idrak seviyesini ölçmek;

4.KVKK ve GDPR kapsamındaki uyum sürecinde, bu sürecin desteklenmesi gereken BGYS 'nin gereklerinden biri olan sızma testi uygulayan firmaların, aldıkları önlem ve tedbirlerin seviyesini analiz etmektir.

Belirlenen bu 4 kapsamda, 38 firmadan bilgi teknoloji direktörlüğü ve alt birimlerinden bilgi güvenliğinden sorumlu yetkililerle görüşülmüş ve anket soruları yanıtlanmıştır. Anket 4 bölümden oluşur. İlk bölümde katılımcıları ve kurumları tanımaya yönelik sorular sorulmuştur. İkinci bölümde ise; kurumların bilgi güvenliği farkındalığını ölçmeye yönelik, üçüncü bölümdeyse; firmalara kavramsal olarak KVKK ve GDPR uyum sürecinde bilmeleri gereken kavramları sorulmuş ve son bölümdeyse; firmaların uğradıkları saldırılar ve bu saldırı çeşitlerine karşı alınan tedbirlerin yeterliliği saptanmak istenmiştir.

Anketin temel problem konuları ile alakalı belirli sorular verilerek yapılan çalışma hakkında bilgilendirme yapılacaktır.

Şekil 1' de katılımcılara çalıştıkları sektörler sorulmuş ve 38 kişiden 24 kişinin bilişim, 9 kişinin teknoloji, 3 kişinin eğitim ve 2 kişinin endüstri sektöründe çalıştığı tespit edilmiştir.

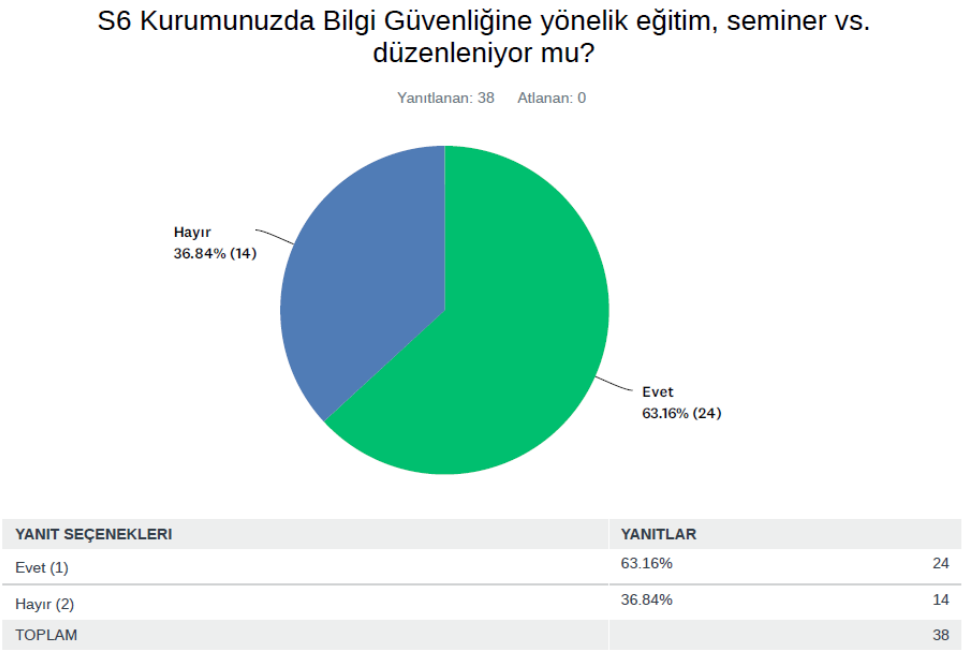


YANIT SEÇENEKLERI	YANITLAR	
Bilişim (1)	63.16%	24
Teknoloji (2)	23.68%	9
Eğitim (3)	7.89%	3
Sağlık (4)	0.00%	0
Endüstri (5)	5.26%	2
Hukuk (6)	0.00%	0
Diğer: (7)	0.00%	0
Diğer (lütfen belirtin) (8)	0.00%	0
TOPLAM		38

Şekil 1. Uygulanan Ankette Katılımcıların Sektör Tespiti

Şekil 2'de katılımcılara firmalarında bilgi güvenliğine yönelik eğitim, seminer gibi etkinliklerin düzenlenip düzenlenmediği sorulduğunda, 38 firmadan 24'ü evet cevabını verirken; 14 kişinin hayır dediği gözlenmiştir.

Verilen cevaplar doğrultusunda; 24 firmada bilgi güvenliğine yönelik eğitimlerin düzenlenmesi, KVKK ve GDPR uyum sürecinde firmaların aldığı tedbirlerin arasında, çalışanların farkındalıklarını arttırmaya yönelik faaliyet düzenlediği; hayır diyen 14 yetkili kişinin firmalarında çalışanların farkındalığına yönelik bir aksiyon almadıkları söylenebilir.

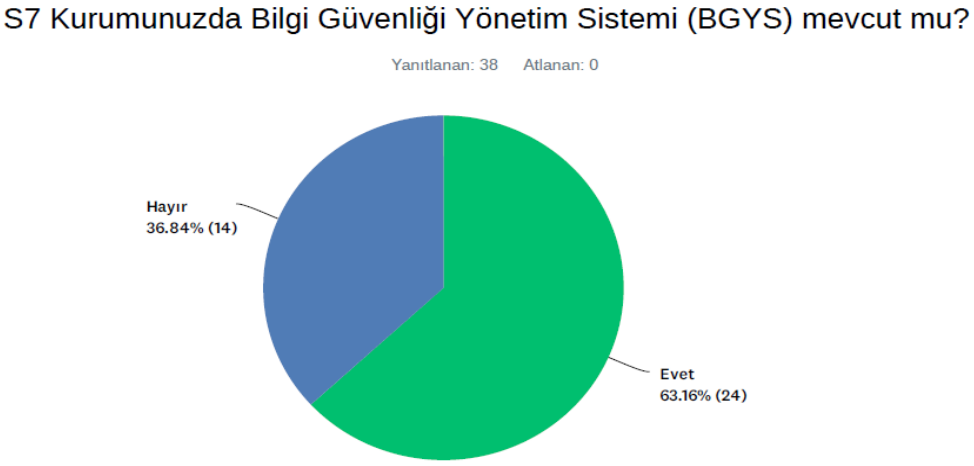


YANIT SEÇENEKLERI	YANITLAR	
Evet (1)	63.16%	24
Hayır (2)	36.84%	14
TOPLAM		38

Şekil 2. Uygulanan Ankette Firmaların Eğitim Verme Oranı

Şekil 3'de katılımcılara firmalarında Bilgi Güvenliği Yönetim Sistemi mevcut mu diye sorulduğunda, 24 kişi evet derken; 14 kişinin hayır cevabını verdiği gözlenmiştir.

Verilen cevaplar doğrultusunda; BGYS bulunan firma sayısının azlığı KVKK ve GDPR uyum sürecinde firmaların etkin bir şekilde bu süreci disipline edemedikleri görülür. Çünkü bilgi varlıklarının güvenliğinin takibi, kompleks ve karmaşık bir yönetimsel sürece ihtiyaç duyar. Bu nedenle, BGYS 24 firmanın uyum sürecinin kolaylaştırırken, 14 firma bu kolaylıktan faydalanmadığı ifade edilebilir.

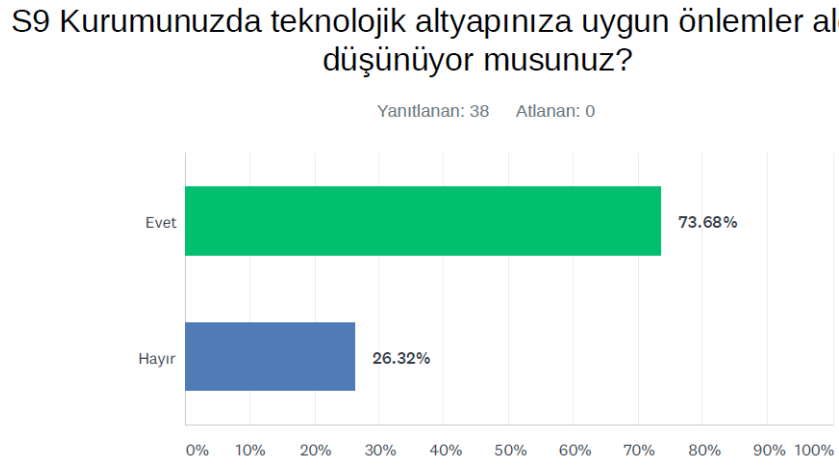


YANIT SEÇENEKLERI	YANITLAR	
Evet (1)	63.16%	24
Hayır (2)	36.84%	14
TOPLAM		38

Şekil 3. Uygulanan Ankette Firmaların BGYS Bulundurma Oranı

Şekil 4'de katılımcılara firmalarında teknolojik altyapılarına uygun önlemler aldığınızı düşünüyor musunuz sorusu sorulduğunda, 38 firmadan yetkili kişilerin 28 evet, 10 hayır cevabı verildiği görülmüştür.

Verilen cevaplara istinaden, teknolojik altyapılarına uygun önlem almadığını düşünen 10 firmanın BGYS bulundurmayan firmalar olduğu düşünülebilir. Çünkü BGYS yönetimsel süreci disipline eden politikalar bütünüdür, bu sebeple yeterli önlem almadığını düşünen firmaların denetimsel bir sürece ihtiyaç duyduğu saptanmıştır.

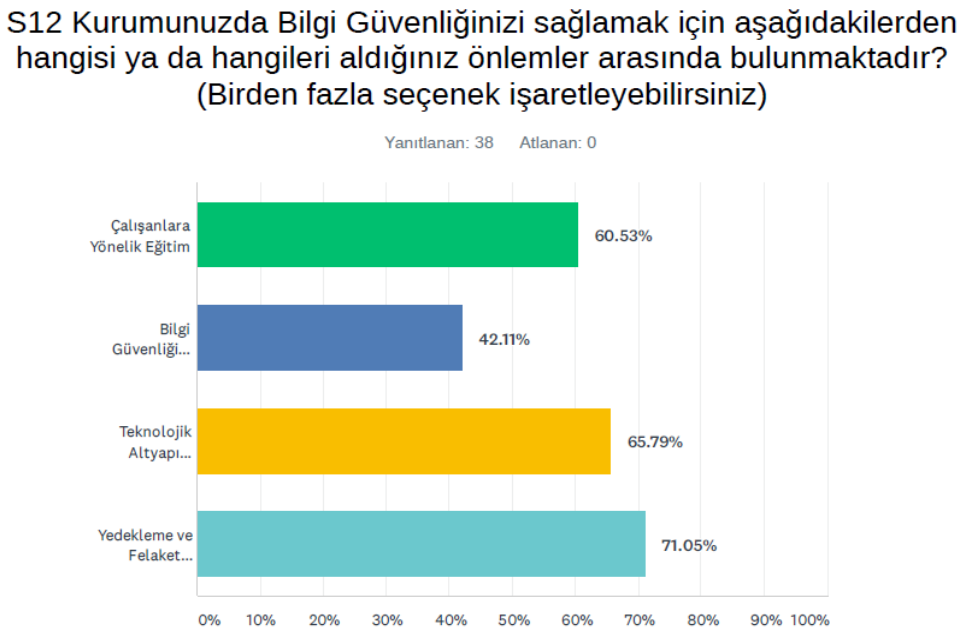


YANIT SEÇENEKLERI	YANITLAR	
Evet (1)	73.68%	28
Hayır (2)	26.32%	10
TOPLAM		38

Şekil 4. Uygulanan Ankette Firmaların Teknolojik Altyapı Oranı

Şekil 5'de katılımcılara, firmalarında bilgi güvenliğini sağlamak için aldıkları önlemler sorulmuş ve 38 firmadan 23 yetkili kişinin çalışanlara yönelik eğitim cevabını verdiği, 16 yetkili kişinin bilgi güvenliği yönetim sistemi kullandığı, 25 kişinin teknolojik altyapı güçlendirme çalışmaları yaptığı ve 27 kişinin de yedekleme ve felaket kurtarma merkezi bulundurduğu tespit edilmiştir.

Verilen cevaplara istinaden, alınan önlemlere bakıldığında BGYS'yi önemli bir tedbir olarak görenlerin sayısının 16 olması, firmasında BGYS bulunduğunu ifade eden 24 firma olduğu düşünüldüğünde 8 firmanın aslında bu süreci yeteri derecede anlamadığı ifade edilebilir. Ayrıca teknolojik altyapı güçlendirme ve firmaların yedekleme ve felaket kurtarma merkezi bulundurması ise bilgi varlığı kaybı oranını azaltırken; firmaların somut önlemlere daha çok önem verdiği saptanmıştır.

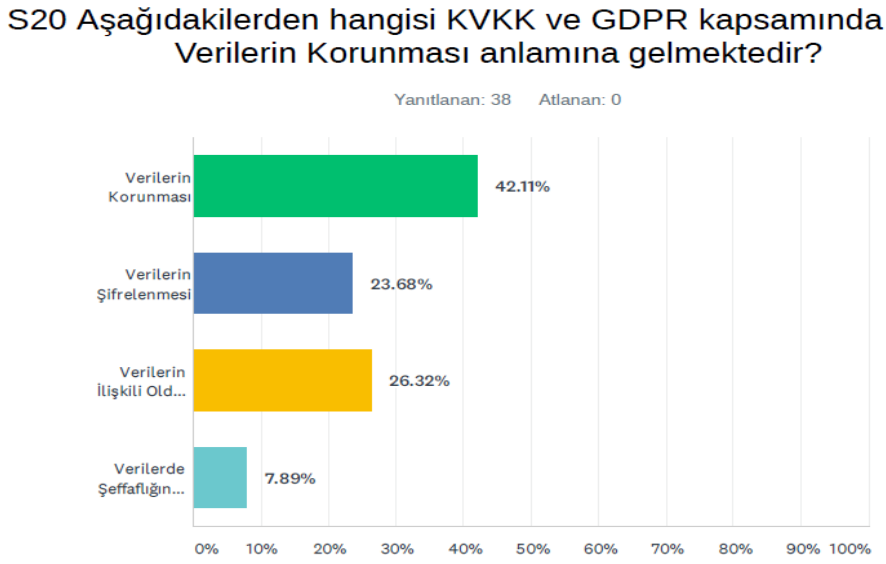


YANIT SEÇENEKLERI	YANITLAR	
Çalışanlara Yönelik Eğitim (1)	60.53%	23
Bilgi Güvenliği Yönetim Sistemi (2)	42.11%	16
Teknolojik Altyapı Güçlendirme (3)	65.79%	25
Yedekleme ve Felaket Kurtarma Merkezi (4)	71.05%	27
Toplam Yanıtlayan: 38		

Şekil 5. Uygulanan Ankette Firmaların Aldıkları Güvenlik Önlemleri

Şekil 6'da firmaların kavramsal olarak KVKK ve GDPR kapsamında kişisel verilerin korunması ne anlama gelir sorusu sorulduğunda, 38 firmadan 16 kişinin kişisel verilerin korunması, 9 kişinin verilerin şifrelenmesi, 10 kişinin verilerin ilişkili olduğu kişilerin korunması diyerek doğru cevap verdiği görülürken; 3 kişinin de verilerde şeffaflığın korunması cevabını verdiği saptanmıştır.

Verilen cevaplara istinaden, doğru cevap verenlerin sayısının 10 olması KVKK ve GDPR uyum sürecinde firmalarda kavramsal noktaları idrakte noksanlıklar olduğu, kişisel verilerin korunması kavramının anlamanın ilgili düzenlemeleri anlama ve uygulama da önemli bir adım olduğu söylenebilir.

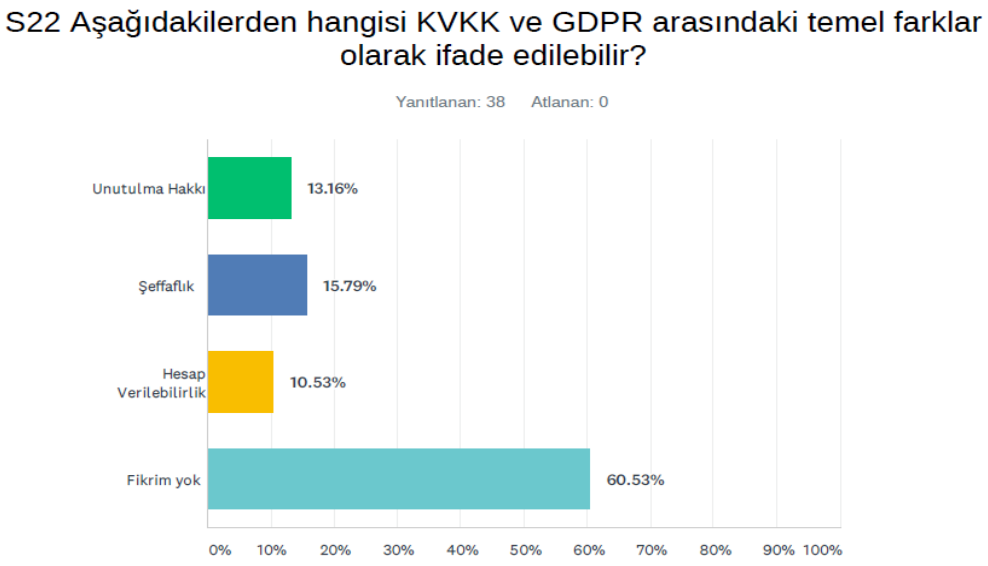


YANIT SEÇENEKLERI	YANITLAR	
Verilerin Korunması (1)	42.11%	16
Verilerin Şifrelenmesi (2)	23.68%	9
Verilerin İlişkili Olduğu Kişinin Korunması (3)	26.32%	10
Verilerde Şeffaflığın Korunması (4)	7.89%	3
TOPLAM		38

Şekil 6. Uygulanan Ankette Firmaların Kavramsal Bilgi Oranı

Şekil 7'de firmalara KVKK ve GDPR arasındaki temel farklar sorulmuş ve 38 firmadan 5 yetkili kişinin unutulma hakkı diyerek doğru cevap verdiği, 6 kişinin şeffaflık, 4 kişinin hesap verilebilirlik ve 23 kişinin fikrim yok cevabını verdiği görülmüştür.

Verilen cevaplara istinaden, KVKK ve GDPR sürecinde firmaların daha çok kavramsal noktada eksiklikleri olduğu; fikrim yok diyen 23 firmanın olması KVKK ve GDPR arasındaki temel kavramın bilinmediğini ve mantık yürütülemediği ifade edilmiştir. KVKK ve GDPR uyum sürecinde firmaların kavramsal noktalarda yetersiz olduğu düşünülürken, aynı zamanda aradaki temel farklardan birinin de bilinmediği söylenebilir.



YANIT SEÇENEKLERI	YANITLAR	
Unutulma Hakkı (1)	13.16%	5
Şeffaflık (2)	15.79%	6
Hesap Verilebilirlik (3)	10.53%	4
Fikrim yok (4)	60.53%	23
TOPLAM		38

Şekil 7. Uygulanan Ankette Firmaların Kavramsal Bilgi Grafiği

Şekil 8'de katılımcılara firmalarında bilgi varlıklarını koruma amacıyla sızma testleri yapılır mı diye sorulduğunda, 38 firmadan 23 kişinin evet, 1 kişinin hayır dediği görülmüştür.

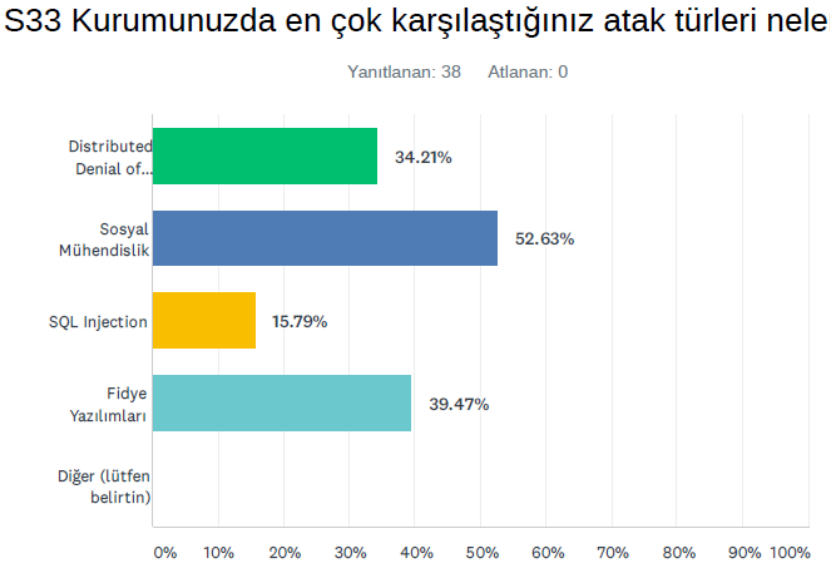
Verilen cevaplara istinaden, kurumlarında BGYS olduğunu ifade eden 24 firmanın 23'ünde sızma testleri yapıldığı, kurumun ihtiyacı olan önlemi sağlamada önemli bir adım olan sızma testi, bu 23 firmanın da bilgi varlıklarını korumaya yönelik gerekli ve yeterli tedbirleri alabileceği söylenebilir.

YANIT SEÇENEKLERI	YANITLAR	
Evet (1)	60.53%	23
Hayır (2)	39.47%	15
TOPLAM		38

Şekil 8. Uygulanan Ankette Firmaların Sızma Testi Yaptırma Oranı

Şekil 9'da yetkili kişilere kurumlarında en çok karşılaştıkları atak türleri sorulduğunda 38 firmadan 13 yetkili kişinin DDoS saldırısı ile karşılaştığı, 20 kişinin sosyal mühendislik saldırısına uğradığı, 6 kişinin Sql Injection ve 15 firmanın fidye yazılımları ile karşılaştığı tespit edilmiştir.

Verilen cevaplara istinaden, en çok yapılan saldırının sosyal mühendislik saldırısı olması, kurum çalışanlarının aslında saldırıya uğramada en zayıf halka olduğu yapılan bu çalışmada tespit edilirken; kurumların çalışanlarına bilgi güvenliği farkındalığına dair eğitim gibi etkinliklerini vermesi bu saldırıya karşı alabilecekleri en önemli tedbir olduğu söylenebilir.



YANIT SEÇENEKLERI	YANITLAR	
Distributed Denial of Service (DDOS) (1)	34.21%	13
Sosyal Mühendislik (2)	52.63%	20
SQL Injection (3)	15.79%	6
Fidye Yazılımları (4)	39.47%	15
Diğer (lütfen belirtin) (5)	0.00%	0
Toplam Yanıtlayan: 38		

Şekil 9. Uygulanan Ankette Firmaların En Çok Karşılaştıkları Atak Türleri

7. SONUÇ VE DEĞERLENDİRME

Yapılan anket çalışmasında elde edilen veriler sonucu;

- 38 firmadan sadece 24 firmada bilgi güvenliğine yönelik farkındalık eğitimleri verilirken 14 firmada verilmediği ve firmalara yapılan saldırıların belli bir çoğunluğunun zayıf halka olan insana yapıldığı göz önünde bulundurulduğunda bu oranın yetersiz olduğu,

- 38 firmadan 24 firmada Bilgi Güvenliği Sistemi bulunduğu ve 14 firmanın KVKK ve GDPR uyum süreci kapsamında yönetimsel bir süreç olan BGYS'yi kullanma oranının yetersiz olduğu,

- 38 firmadan 28 firmanın teknolojik altyapılarına güvendiği ve 10 firmanın firmanın yetersiz gördüğü tespit edilmiştir. Bu 10 firmada BGYS olmadığı varsayılırsa, yeterli önlem alınmama nedeninin bu sonuca bağlı olduğu,

- 38 firmaya aldıkları teknolojik önlemler sorulduğunda 16 firmanın BGYS'ye dikkat ettiği ve bunun yanında teknolojik önlemler, yedekleme ve felaket kurtarma merkezi ve çalışanlarına farkındalık eğitimleri vermeye de dikkat ettiği ve istenilen tablonun 16 firmada görüldüğü,

- 38 firmaya KVKK ve GDPR kapsamında kişisel verinin korunması nedir diye sorulduğunda, sadece 10 kişinin doğru cevap vermesi ve KVKK ve GDPR arasındaki temel farkın unutulma hakkı olduğu cevabını ise; sadece 5 kişinin doğru olarak cevap vermesi uyum sürecinde firmaların mevcut durumlarının zayıf olduğu,

- 38 firmadan sızma testi yaptıran 23 firma olması, BGYS olduğu cevabını veren 24 kişi olduğu düşünüldüğünde 1 firmanın BGYS gereklerini yerine getirmediği,

- 38 firmaya en çok karşılaştıkları atak türü sorulmuş ve 20 firmadan sosyal mühendislik cevabı alındığı görülmüştür böylece bilgi güvenliğine yönelik firmalarında farkındalık eğitimleri veren 24 firmanın yapılan bu saldırıya binaen kurumlarda eğitim veriliyor oluşu çalışanların farkındalıklarını arttırdığı tespit edilmiştir.

Sonuç olarak; KVKK ve GDPR kapsamında firmaların mevcut durum analizi incelendiğinde, belirlenen 4 yaklaşımda bilişim sektörünün bu konuya daha çok önem verdiği, bilgi güvenliği yönetim sistemi bulunduran firmaların sayısının yetersiz fakat uyum sürecinde uyguladıkları sistemle daha disiplinli bir şekilde süreci ilerlettiği, kişisel veri korunması kavramının anlaşılma oranının düşük olduğu ve saldırılara karşı alınan önlemlerin daha işe yarar olmasını sağlayan sızma testleri yaptıran firmaların sayılarının yetersiz olduğu ve bu yüzden firmaların sistemlerinin ihtiyaç duydukları tedbirleri almada sayıca az oldukları tespit edilmiştir.

Elde edilen bu sonuçlara bakılarak Kişisel Verileri Koruma Kurumu ve diğer ilgili kurumlar tarafından firmalara, kavramlar ve düzenlemeler hakkında eğitim vermeleri gerektiği, KVKK ve GDPR uyum sürecinde firmaların doğru bildikleri yanlışları görmeleri için uyguladıkları BGYS'nin yetkili kurumlar tarafından belirli periyotlarla denetlenmesi gerektiği ve bu denetlemenin ne şekilde gerçekleşmesi gerektiği gelecekteki çalışmaların arasında düşünebilir.

Ülkemizde KVKK ve GDPR uyum sürecinde firmaların mevcut durum analizi üzerine yeterli çalışma olmadığı ve yapılan bu araştırmanın ileride yapılacak olan akademik çalışmalara katkı sağlayacağı düşünülmektedir.

KAYNAKÇA

Beyaznet, (2019), Sızma Testlerinde Bilgi Toplama Araçları, 10.05.2020, https://www.beyaz.net/tr/guvenlik/makaleler/sizma_testitlerinde_bilgi_toplama_araclari.html.

Can, Ö., Akbaş, M., (2014), "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", TUBAV Bilim Dergisi, 7, 16-31.

Canbek, G., Sağıroğlu, Ş., (2006), "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9, 165-174.

Gülmüş, G., (2010), Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 155, İstanbul.

IAB, (2020), 08.05.2020, https://www.iabturkiye.org/UploadFiles/Reports/iab_GDPR452018173051.pdf.

Irmak, H., Baz, F., (2019), Kurumsal Bilgi Güvenliği Tehditler ve Alınması Gereken Önlemler Üzerine Bir İnceleme, 2. Uluslararası Mardin Artuklu Bilimsel Araştırmalar Kongresi, Sosyal ve Beşerî Bilimler Kitabı, 333-341.

KVKK, (2020), 05.01.2020, https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf.

KVKP, (2020), 10.05.2020, https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri/.

Secops, (2020), 08.05.2020, https://seccops.com/hizmetler/sizma-testleri-penetrasyon-testi/.

Şen, Ş., Yerlikaya, T., (2013), ISO 27001 Kurumsal Bilgi Güvenliği Standardı, XV. Akademik Bilişim Konferansı Bildirileri, 719-723.

Vural, Y., Sağıroğlu, Ş., (2008), "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 23, 507-522.

Yaşar, H., Çakır, H., (2015), "Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri", Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3, 488-507.

Yılmaz, H., (2014), "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi", Dergipark, 45-59.

Yılmaz, V., (2007), Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 297, İstanbul.