T.C.
KTO Karatay Üniversitesi
Fen Bilimleri Enstitüsü

ADLİ BİLİŞİM MÜHENDİSLİĞİ ANABİLİM DALI TEZLİ YÜKSEK LİSANS PROGRAMI

KÜÇÜK VE ORTA BÜYÜKLÜKTEKİ İŞLETMELER İÇİN VERİ GÜVENLİĞİ VE STANDARTLARI

Berna ILGAZ

KONYA

TEMMUZ 2018

KÜÇÜK VE ORTA BÜYÜKLÜKTEKİ İŞLETMELER İÇİN VERİ GÜVENLİĞİ VE STANDARTLARI

Berna ILGAZ

KTO Karatay Üniversitesi Fen Bilimleri Enstitüsü
Adli Bilişim Ana Bilim Dalı Yüksek Lisans Programı

Yüksek Lisans Tezi

KONYA
Temmuz, 2018

Fen Bilimleri Enstitü Onayı

Prof. Dr. Hüseyin Bekir
YILDIZ
Fen Bilimleri Enstitüsü Müdürü

Bu tezli yüksek lisans tezinin yapılması gereken bütün gerekliliklerinin yerine getirdiğini onaylıyorum.

Prof. Dr. Novruz ALLAHVERDİ
Anabilim Dalı Başkanı

Berna ILGAZ tarafından hazırlanan KÜÇÜK VE ORTA BÜYÜKLÜKTEKİ İŞLETMELER İÇİN VERİ GÜVENLİĞİ VE STANDARTLARI başlıklı bu çalışma 04.07.2018 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jüri tarafından tezli yüksek lisans tezi olarak kabul edilmiştir.

Dr. Öğr. Üyesi Ali ÖZTÜRK
Tez Danışmanı

Jüri Üyeleri

Başkan: Prof. Dr. Harun UĞUZ

Üye: Dr. Öğr. Üyesi Ali Öztürk

Üye: Dr. Öğr. Üyesi Semih Yumuşak

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir aksi bir durumda aleyhime doğabilecek tüm hak ve kayıplarını kabullendiğimi beyan ederim.

16.07.2018

Berna ILGAZ

ÖZET

KÜÇÜK VE ORTA BÜYÜKLÜKTEKİ İŞLETMELER (KOBİ) İÇİN VERİ GÜVENLİĞİ VE STANDARTLARI

ILGAZ, Berna

Yüksek Lisans- Adli Bilişim Mühendisliği Anabilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Ali ÖZTÜRK

Temmuz 2018

Günümüzde az sayıda çalışanları bulunan işletmelerden binlerce çalışanı bulunan işletmelere kadar her biri farklı kapasitede ve büyüklükteki işletmeler bilgi teknolojilerini kullanmakta ve bilgi teknolojilerinin avantajlarından yararlanmaktadır. Bilgi teknolojileri bu işletmelere sağladığı pek çok yarar karşısında birçok riski de barındırır. KOBİ'ler için bu riskleri önlemek büyük işletmelere oranla daha zordur ve siber tehditlerden daha çok zarar görmektedirler. Bu tez çalışmasında, KOBİ'lerde bilgi teknolojileri güvenliği ve KOBİ'lerin karşılaşabilecekleri bilgi teknolojileri güvenliği tehditleri ile bilgi ve veri güvenliğini sağlamaya yönelik güvenlik doğrulama araç setleri incelenmiş, siber tehditlere karşı alınabilecek önlemler ele alınmış, uluslararası bilgi güvenliği standartları incelenmiştir.

Anahtar Kelimeler: Bilgi teknolojileri, BGYS, BS 7799, güvenlik doğrulama, KOBİ, PUKÖ, veri güvenliği

ABSTRACT

DATA SECURITY AND STANDARDS FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

ILGAZ, Berna

M.Sc. Forensic Science Engineering

Ass.Prof. Dr. Ali ÖZTÜRK
July 2018

From businesses that employ thousands of employees to businesses with fewer employees, different capacities and sizes of businesses benefit from the advantages of information technology. Besides its many benefits, the information technology can be risky to these businesses. For SMEs, these risks are more than the large enterprises and they suffer more from cyber threats. In this study, the safety verification toolkit for information security and data security related to SMEs' security and SME issues is examined and measures against cyber threats are discussed and international information security standards are examined.

Keywords: Information technology, BS 7799, Data security, ISMS, Security authentication, SMEs, PDCA

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren hocam Dr. Öğr. Üyesi Ali ÖZTÜRK'e ve kıymetli tecrübelerinden faydalandığım KTO Karatay Üniversitesi Adli Bilişim Mühendisliği Bölümü öğretim üyelerine teşekkürü bir borç bilirim.

Çalışmalarım sırasında yardımını ve desteğini esirgemeyen değerli eşim Muhammet ILGAZ'a, vermiş oldukları tüm maddi ve manevi destekleri için babam Sabit BOZGÖZ ve Şeref ILGAZ'a, annem Hayriye BOZGÖZ ve Ayşe ILGAZ'a teşekkürlerimi sunuyorum.

Berna ILGAZ
Temmuz-2018

İÇİNDEKİLER

ÇİZELGELERİN LİSTESİ

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

KISALTMALAR

Kısaltmalar	Açıklama
KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
NIPS	Network Intrusion Prevention System
NIDS	Network Intrusion Detection System
IPS	Intrusion Prevention Systems
TCP	Transmission Control Protocol
AJAX	Asynchronous JavaScript and XML
JSON	JavaScript Object Notation
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
SBL	Spider Bot Language
FTP	File Transfer Protocol
GPL	General Public License
LAN	Local Area Network
WLAN	Wireless Local Area Network
RAM	Random-Access Memory
OWASP	Open Web Application Security Project
SQL	Structured Query Language
OS	Operating System
LDAP	Lightweight Directory Access Protocol
API	Application Programming Interface
XML	Extensible Markup Language
XXE	XML External Entities
XSS	Cross-Site Scripting
VPN	Virtual Private Network
ISO	International Organization for Standardization
IEC	International Electrotechnical Organization
JTC	Joint Technical Committee
JTC/SC	Joint Technical Committee/ Subcommittee
JTC/SC/WG	Joint Technical Committee/ Subcommittee/Working Group
TSE	Türk Standartları Enstitüsü
BSI	British Standards Institue
BGYS	Bilgi Güvenliği Yönetim Sistemi
PUKÖ	Planla - Uygula - Kontrol et - Önlem al

1. GİRİŞ

Bilişim teknolojilerinin günümüzde kullanımı küresel anlamda yaygınlaşmış, hem bireysel hem de kurumsal kullanım için bu teknolojilerden yararlanmak kaçınılmaz hale gelmiştir. Hızla gelişmekte olan bu teknolojiler sağladığı birçok olanak ile kurumlara çeşitli avantajlar sağlamaktadır. Bilgi ve veri alışverişinin kolay olması, bankacılık hizmetlerinden internet sayesinde yer ve zaman kavramı olmaksızın yararlanılabilmesi, ticari ve kurumsal verilerin kayıt altına alınabilmesi gibi kolaylıklar sayesinde kurumların bilişim teknolojilerine bağımlılıkları gün geçtikçe artmaktadır. Bu kolaylıklar ile birlikte gelen birçok risk de bulunmaktadır.

Büyük işletmeler de küçük ve orta büyüklükteki işletmelerde de bilişim teknolojilerini kullandıkları sürece her türlü tehditle karşı karşıya kalma riskine sahiptirler. Bu noktada değinilmesi gereken asıl mevzu gerekli güvenlik önlemlerini yazılım ve donanım için sağlayabilmek, çalışanları güvenlik eğitimleri ile bilgilendirmek, gün geçtikçe artan ve çeşitli hale gelen güvenlik tehditleri ile ilgili gelişmeleri takip edebilmek, en kötü durum senaryosu hazırlayarak acil bir durumla karşılaşıldığında nasıl hareket edilmesi gerektiğini planlayabilmektir.

Günümüzde bilgilere ulaşabilmek kolaylaşmış, dolayısıyla ulaşılan bu bilgilerin kopyalanması, saklanması, değiştirilmesi gibi riskler de artmış bulunmaktadır. Bilgi güvenliğinin sağlanması için tüm dünyaca kabul görmüş bilgi güvenliği standartları bulunmaktadır. Bu standartlar incelendiğinde bir kurumun ihtiyacı olabilecek bilgi güvenliği yönetim sisteminin gerekliliği daima vurgulanmaktadır. Bilgi güvenliği yönetim sistemi bir kurumun bilgi varlıklarının gizlilik, doğruluk ve erişilebilirliğini güvence altına almak için uygulanması gereken güvenlik denetimlerini düzenler.

İnternet kullanımın giderek artması ve sağladığı avantajlar insan hayatını kolaylaştırmaktadır. Ancak bunun yanında bir takım riskleri de beraberinde barındırmaktadır. Küçük ve orta büyüklükteki işletmelerde veri güvenliğine ve bütünlüğüne yönelik tehditler de bu risklerden biridir. Teorik olarak güvenlik kontrollerini sağlamak kolay gibi görünse de, bilgi eksikliği, dikkatsizlik, tedbirsizlik, teknik destek ve uzman eksikliği, finansal kaynakların yetersizliği gibi sebeplerle pratikte bu iş zorlaşmaktadır.

Bu çalışmanın 1. kısmında bilgi ve veri güvenliğinin gerekliliğine giriş yapılmış, 2. kısımda küçük ve orta büyüklükteki işletmelerde veri güvenliğine dair literatür taraması yapılmıştır. 3. kısımda küçük ve orta büyüklükteki işletmelerin tanımına yer verilmiş, küçük ve orta büyüklükteki işletmeler ekonomik ve çalışan yönünden ele alınmıştır. 4. kısımda ise küçük ve orta büyüklükteki işletmelerde veri güvenliğinin nasıl sağlanacağı, güvenlik tehditlerinin neler olabileceği, bu güvenlik tehditlerine karşı alınabilecek önlemler, güvenlik tehditleri daha oluşmadan kullanılabilecek güvenlik araç setlerinin ne oldukları, son kullanıcı işletmelerin güvenlik konusundaki zafiyetleri ve küçük ve orta büyüklükteki işletmelerde veri güvenliğine yönelik çalışmaların ve farkındalığın artırılması için önerilere yer verilmiştir. Siber güvenlik tehditleri ve bu tehditlere karşı alınabilecek önlemlerden bahsedilmiştir. 5. Kısımda uluslararası bilgi güvenliği standartları incelenmiş, bu kapsamda bir kurumun ihtiyacı olan Bilgi Güvenliği Yönetim Sistemi gerekliliği vurgulanmış, Bilgi Güvenliği Yönetim Sistemi kurulması ve yönetilmesi için gerekli aşamalar anlatılmıştır.

2. LİTERATÜR TARAMASI

Son yıllarda veri güvenliğini sağlamaya yönelik birçok çalışma ve akademik araştırma yapılmaktadır. Ortaya çıkabilecek yeni güvenlik tehditlerine karşı alınabilecek önlemler ve var olan ve geliştirilen uluslararası veri güvenliği standartları sayesinde bu çalışmalarla birlikte veri güvenliğini sağlama tekniklerinin güncel tutulmasına yardımcı olmaktadır.

Ali ACILAR tarafından yapılan çalışmada büyük işletmelerin küçük işletmelere göre veri güvenliğini sağlama konusunda daha donanımlı oldukları belirtilmektedir. Büyük işletmeler veri güvenliğini sağlamak adına gerekli olan teknik destekleri temin etme konusunda herhangi bir zorluk çekmezken küçük ve orta büyüklükteki işletmeler diye adlandırdığımız KOBİ'ler bu konuda yeterli maddi olanağa sahip değildirler. KOBİ'ler, gerekli güvenlik ihtiyaçlarını belirleme ve bu güvenlik ihtiyaçlarına bütçe ayırma konusunda en fazla zorlanan kesimdir [1].

Yılmaz VURAL ve Şeref SAĞIROĞLU tarafından yapılan çalışmada kurumların veri güvenliğinin sağlanması için sistemlerin güncel tutulması, gerekli eğitimlerin alınması, mevcut güvenlik açıklarının tespit edilip belirli aralıklarla bu işlemin tekrar edilmesi gerektiği belirtilmektedir. Ayrıca veri güvenliğini sağlamak için sadece teknik yeterlilikler ön plana çıkarılmamalı, aynı zamanda teknik olmayan nitelik olarak değerlendirilebilecek olan çalışanların eğitimi, kurum etiği, fiziksel güvenlik önlemleri de dikkate alınmalıdır [2].

Yılmaz VURAL ve Şeref SAĞIROĞLU tarafından yapılan bir başka çalışmada kurumsal bilgi güvenliğini sağlamaya yönelik çalışmaların ve eğitimlerin artırılması gerektiği, kurumsal bilgi güvenliğine gerekli önemin verilmesi ve iç ve dış tehditlere karşı gerekli önlemlerin alınması gerektiği belirtilmektedir. Kurumsal bilgi güvenliğini sağlamaya yardımcı olması açısından uluslararası standartların önemi vurgulanmaktadır [3].

Gürol CANBEK ve Şeref SAĞIROĞLU tarafından yapılan çalışmada internet yoluyla kullanıcıların bilgisayarlarına bulaşabilecek zararlı yazılımlardan ve bu yazılımların doğuracağı kötü sonuçlara karşı alınabilecek önlemlerin üzerinde durularak detaylı bir araştırma gerçekleştirilmiştir. Kullanıcıların kötücül yazılımlar karşısında nasıl hareket etmesi gerektiğine dair öneriler sunulmaktadır [4].

Mehtap ÇETİNKAYA KILIÇ ve Orhan GÖKÇÖL tarafından yapılan çalışmada kurumlarda Bilgi Güvenliği Yönetim Sistemi (BGYS) altyapısı oluşturmanın ve ISO 27001 standardına uygun olarak bu altyapıyı geliştirmenin gerekliliğinden bahsedilmektedir. Bilgi Güvenliği Yönetim Sistemi kurulurken geçen süreçte hangi adımların takip edileceği detaylı olarak incelenmektedir [5].

Atila BOSTAN ve İbrahim AKMAN tarafından yapılan çalışmada veri güvenliği farkındalığı ve uygulamaları konusunda 466 katılımcı ile bir anket çalışması gerçekleştirmişlerdir. Kullanıcıların bilgisayar ve web güvenliği konusundaki duyarlılıkları ve farkındalıkları ile yaş, cinsiyet, eğitim seviyesi ve bilgisayar ve diğer iletişim teknolojileri kullanım deneyimi arasındaki ilişkisini tespit etmeye yönelik bir araştırma gerçekleştirmişlerdir. Bu anket çalışmasının sonucunda ise;

- Artan yaş oranı ile bilgisayar güvenliği konusundaki duyarlılığın azaldığı,
- Kadınların erkeklere oranla bilgisayar güvenliği konusunda daha dikkatli olduğu,
- Eğitim seviyesi arttıkça bilgisayar güvenliği hususunda daha dikkatli davranıldığı, bilgisayar ve diğer iletişim teknolojileri kullanım tecrübesinin artması ile bilgisayar güvenliği konusunda duyarlılık, dikkat ve farkındalığın da arttığı,
- Yaş oranının ve eğitim seviyesinin artması ile web güvenlik uygulamaları farkındalığının da arttığı tespit edilmiştir [6].

Mete EMİNAĞAOĞLU ve Yılmaz GÖKŞEN tarafından yapılan çalışmada ülkemizde ve dünyada bilgi güvenliği konusunda yapılan ortak hatalar istatiksel olarak ortaya konulmuş ve bu hataların çözümlerine yönelik önerilere yer verilmiştir [7].

Ali ACILAR ve Ayşe BASTUĞ tarafından yapılan çalışmada işletmelerde veri güvenliği tehditlerinden biri olan sosyal mühendislik üzerine araştırma yapılmıştır. Sosyal mühendisliğin ne olduğu, içeriğinde barındırdığı saldırı çeşitleri, sosyal mühendislik saldırılarına karşı alınabilecek önlemlerin neler olduğu üzerine bir çalışma sunulmuştur [8].

Yves Barlette ve Vladislav V. Fomin tarafından yapılan çalışmada, bilişim sistemleri güvenlik standartlarının küçük ve orta büyüklükteki işletmelerin ihtiyaçlarına uygunluğunu incelemişlerdir. Ayrıca, yakın zamanda yayınlanmış olan ISO 27001 IS güvenlik standardını, ISO 9001 standardıyla karşılaştırmalı olarak, yeni uygulamaya konulan ISO 27001 standardının nasıl benimseneceğine dair beklentileri geliştirmek için karşılaştırma yapmışlardır. Küçük ve orta büyüklükteki işletmelere yönelik bir sertifikasyon çerçevesi oluşturmak amacıyla, basitleştirilmiş güvenlik yöntemlerinin veya standartlarının akademik ve yönetimsel düzeyde oluşturulmasına ve benimsenmesine yönelik daha fazla araştırma yapılmasının gerekliliğini vurgulamışlardır [9].

Craig Allan ve arkadaşları tarafından yapılan çalışmada, Avustralya'daki küçük ve orta büyüklükteki işletmeler arasında bilişim ve iletişim teknolojileri ile güvenlik teknolojisinin benimsenme oranlarını ve bunların benimsenmesini etkilemede rol oynayan faktörleri özetlemişlerdir. Bilişim ve iletişim teknolojilerinin benimsenmesi, güvenlik teknolojilarinin benimsenmesi ve güvenliğin evrimsel sürecini gösteren bir çerçeve geliştirmişlerdir. Bu çerçeve, her bir evrimde kurulması gereken güvenlik teknolojilerini ve güvenlik seviyelerini tanımlar. Yaptıkları çalışma ile, Bilişim ve iletişim teknolojilerinin benimsenmesi, güvenlik teknolojileri ve Avustralya küçük ve orta büyüklükteki işletmelerinin güvenliğine yönelik daha fazla araştırma için bir çerçeve oluşturmayı hedeflemişlerdir [10].

Ji-Yeu Park ve arkadaşları tarafından yapılan çalışmada, güvenlik kavramının dört seviyede ele alınması gerektiğinin üzerinde durmuşlardır. Bu seviyeler örgütsel seviye, iş akışı seviyesi, bilgi seviyesi ve teknik seviye olarak sıralanabilir. Belirlenen bu seviyeler ile iş süreçlerinin modellenmesi ve güvenliğin/güvenilirliğin dikkate

alınması, iş akışı seviyesinin güvenilirliğini ve sağlamlığını artırabileceğini önermektedirler [11].

Yukarıdaki çalışmalarda kurumlarda bilgi ve iletişim teknolojilerinin güvenliğini sağlamak için farklı yöntemler mevcuttur. Bu çalışmanın amacı ise küçük ve orta büyüklükteki işletmelerde veri güvenliği hakkında farkındalık oluşturmak, küçük ve orta büyüklükteki işletmeledeki kullanıcıların ve/veya personellerin veri güvenliği konusunda bilinçlendirilmesini sağlamaktır. Günümüzde küçük ve orta büyüklükteki işletmelerin en büyük problemlerinden birisi olan veri güvenliğinin sağlanmasında küçük ve orta büyüklükteki işletmelere çözümlerin üretilmesinde yardımcı olmaktır.

3. KOBİ TANIMI

KOBİ kelimesi "Küçük ve Orta Büyüklükteki İşletmeler"in kısaltması olarak kullanılmaktadır. KOBİ'ler, yıllık 250 kişiye kadar çalışan istihdam eden ve cirosu 40 milyon Türk Lirasını aşmayan işletmelerdir [12]. Küçük ve Orta Büyüklükteki İşletmelerin (KOBİ) Tanımını ve Niteliklerini Belirleyen Yönetmelik, 24 Haziran 2018 tarihli resmi gazetede yayımlanarak yürürlüğe girmiştir [13]. KOBİ'ler kendi içinde 3 ayrı sınıfa ayrılmaktadır [14]:

a) ***Mikro İşletmeler:*** Yıllık çalışan sayısı 10 kişiden az olan ve yıllık satış hasılatı veya mali bilançosundan herhangi biri 3 milyon Türk Lirasını aşmayan işletmeler, mikro işletme olarak adlandırılmaktadır.

b) ***Küçük İşletmeler:*** Yıllık çalışan sayısı 50 kişiden az olan ve yıllık satış hasılatı veya mali bilançosundan herhangi biri 25 milyon Türk Lirasını aşmayan işletmeler, küçük işletme olarak adlandırılmaktadır.

c) ***Orta Büyüklükteki İşletmeler:*** Yıllık çalışan sayısı 250 kişiden az olan ve yıllık satış hasılatı veya mali bilançosundan herhangi biri 125 milyon Türk Lirasını aşmayan işletmeler, orta büyüklükte işletme olarak adlandırılmaktadır.

Türkiye'deki Küçük ve Orta Büyüklükteki İşletmeler şu şekilde sınıflandırılmaktadır:

	Mikro Ölçekli KOBİ	Küçük Ölçekli KOBİ	Orta Ölçekli KOBİ
Çalışan Personel Sayısı	< 10	< 50	< 250
Yıllık Net Satış Hâsılatı	≤ 3 Milyon TL	≤ 25 Milyon TL	≤ 125 Milyon TL
Yıllık Mali Bilanço Toplamı	≤ 3 Milyon TL	≤ 25 Milyon TL	≤ 125 Milyon TL

Çizelge 3.1: Türkiye'deki Küçük ve Orta Büyüklükteki İşletmelerin Sınıflandırılması [15]

2003/361/EC sayılı tüzük çerçevesinde Avrupa Birliği'nde 1 Ocak 2005'te KOBİ tanımı yürürlüğe girmiştir [16]. Avrupa Birliği'ndeki Küçük ve Orta Büyüklükteki İşletmelerin Sınıflandırılması Çizelge 3.2'de gösterilmektedir.

Bir işletmenin bir KOBİ olup olmadığını belirleyen temel faktörler şunlardır [17]:

- Personel sayısı
- Ciro veya bilanço toplamı

	Mikro Ölçekli KOBİ	Küçük Ölçekli KOBİ	Orta Ölçekli KOBİ
Çalışan Personel Sayısı	< 10	< 50	< 250
Yıllık Net Satış Hâsılatı	≤ 2 Milyon Euro	≤ 10 Milyon Euro	≤ 50 Milyon Euro
Yıllık Mali Bilanço Toplamı	≤ 2 Milyon Euro	≤ 5 Milyon Euro	≤ 43 Milyon Euro

Çizelge 3.2: Avrupa Birliği'ndeki Küçük ve Orta Büyüklükteki İşletmelerin Sınıflandırılması [16]

4. KOBİ'LERDE VERİ GÜVENLİĞİ

Bilgi ve veri güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme, yok edilme ve hasar verilmesini önlemek olarak tanımlanır ve "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik unsurundan herhangi biri zarar görürse güvenlik zafiyeti oluşur. Bu unsurlar şu şekilde tanımlanır:

- **Gizlilik:** Bilginin yetkisiz kişilerin eline geçmesinin önlenmesi ve yetkisiz erişime karşı korunmasıdır.
- **Bütünlük:** Bilginin yetkisiz kişiler tarafından değiştirilmesinin önlenmesidir.
- **Erişilebilirlik:** Bilginin yetkili kişilerce ihtiyaç duyulduğunda ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bilgi ve veri güvenliği her işletmenin devamlılığı, saygınlığı, güvenilirliği vb. gibi manevi değerlerini oluşturan birikimleri güvence altına almayı garantiler. Büyük şirketlerin yanı sıra KOBİ'ler, devlet kurumları, kar amacı gütmeyen organizasyonlar gibi farklı oluşumlar da sürekli veri güvenliği sorunları yaşamaktadırlar [7].

KOBİ'ler için veri güvenliğini sağlamak büyük kurumlara oranla daha azdır. Bunun sebebi ise finansal kaynaklarının kısıtlı olması, yeterli teknik bilgiye ve deneyime sahip olmamalarıdır. Bu yüzden karşılaşabilecekleri her türlü siber saldırılar ve bu saldırılardan doğan zararlar karşısında dayanıksızdırlar [1].

Hem büyük şirketler hem de KOBİ'ler için, iş başarısı giderek daha fazla bilgi teknolojileri altyapısına dayanmaktadır. Ancak birçok KOBİ yöneticisi, işletmelerinde bilgi teknolojileri güvenliğinin temelde güvenlik duvarına sahip olmakla ve virüsten koruma yazılımını düzenli olarak güncellemekle eşdeğer olduğuna inanmaktadır. Stratejik politikalar, bilgi hırsızlığı, iş sürekliliği, erişim kontrolleri ve diğer pek çok husus sadece güvenlik olayları durumunda ele alınmaktadır [11].

4.1. Kobi’lerin Veri Güvenliği Konusundaki Eksiklikleri

Küçük işletmelerin çoğunluğu, bilişim teknolojileri uzmanı istihdam edemediği gibi yöneticilerinin de bilgi güvenliği tehditlerinden ve bunların işletme faaliyetlerinde neden olacağı sonuçlardan çok az bilgisi vardır [10].

Birçok durumda KOBİ'lerin yönetimi, işletmelerini kötü amaçlı saldırılar için olası bir hedef olarak görmemektedir. Bu nedenle, bilgi teknolojileri güvenliğini düşük öncelikli olarak kabul etmektedirler. Bu, modern bilgi teknolojileri altyapısına yönelik gelişen tehditler için çok yanlış bir tutumdur. Bununla birlikte, KOBİ'ler genellikle daha az para harcadıklarından, bilgi teknolojileri yönetimi ve bilgi güvenliği konusunda; dışarıdan veya içeriden olası saldırılara daha az hazırlıklıdırlar [11].

Bazı KOBİ yöneticileri [1];

- Kendilerinin çok küçük olduğu için internet ortamında erişilemeyeceklerini,
- İşletmelerinin saldırganların dikkatini çekmeyecek kadar küçük olduğunu,
- Hiçbir saldırganın ilgisini çekecek ölçüde bir veriye sahip olmadıklarını,
- Yakınlarında saldırıya uğramış hiç kimse tanımamakta veya bu konudaki haberlerin çok abartılı olduğunu,
- İnternetten alışveriş yapmadıklarından endişelenilmemesi gerektiğini
- İnternette çok kısa zaman kaldıkları için saldırıya maruz kalmayacaklarını,
- Anti-virüs yazılımlarını ve güvenlik duvarını yeterli olduklarını düşünmektedirler.

KOBİ yöneticileri, genellikle kendilerini saldırganların dikkatini çekemeyecek kadar küçük olduklarını düşündüklerinden dolayı internet ortamında kendileri için bir tehlike öngörmeseler bile günümüz internet ve bilgi paylaşım ortamında her türlü veri saldırganların dikkatini çekebilmektedir [1].

4.2. Güvenliği Doğrulama Araçları

Bilgi teknolojilerinin bütünlük, gizlilik, güvenlik ve her zaman çalışabilir vaziyette olmasını engelleyebilecek veya sisteme zarar verebilecek her türlü şahıs, olay veya durum bir tehdit olarak değerlendirilmektedir. Bilgi teknolojilerinin hızla gelişmesi ve

büyümesi, verilerin depolanmasını ve paylaşılmasını kolaylaştırmakla beraber verilerin her türlü çalınabilme, değiştirilme, yok edilme gibi riskleri de yanında barındırır [2]. Bu bölümde tanıtılan araçlar, işletmelerin uygulamalarını, ağ altyapısını ve güvenlik varlıklarını korumak için koyduğu güvenlik önlemlerini izlemeye, test etmeye ve doğrulamaya yardımcı olacaktır [18].

4.2.1. Güvenlik Açığı Değerlendirmesi ve Tehdit Analizi

Güvenlik açısından kapsamlı bir sistem anketi gerçekleştirmek, Güvenlik Açığı Değerlendirmesi ve Tehdit Analizi olarak adlandırılmaktadır [18]. Sistemi ayrı tutmak, parçaları birer birer analiz etmek, parçaları tekrar bir araya getirmek ve güvenliklerini bir bütün olarak değerlendirmek gerekir. Güvenlik açığı değerlendirmesi ve tehdit analizi gerçekleştirilmesi süreci bir sistemden diğerine farklılık gösterir, çünkü her sistemin güvenlik özellikleri farklıdır.

4.2.1.1. Snort Kullanarak Saldırı Tespiti ve Önleme

Snort, kural tabanlı olup, Ağ Geçidi Önleme Sistemi (Network Intrusion Prevention System - NIPS) ve algılayıcı kullanarak çalışan Ağ Saldırı Tespit Sistemi (Network Intrusion Detection System - NIDS) 'dir [18].

Snort üç modda çalışır [19]:

- Paket İzleyici modu (packet sniffer): Ağdan paketleri okuyup sürekli olarak ekrana aktarır. Komut satırında *"./snort –v"* şeklinde çalıştırılabilir; bu şekilde sadece TCP paket başlık bilgilerini ekrana basar.
- Paket Günlükleme modu (packet logger): Paketleri diske yazar. Komut satırında *"./snort -dev -l ./log"* komutu ile çalıştırılabilir. Burada TCP paket başlıkları ile birlikte paket bilgilerini de kaydeder ve /log dizinine günlükler.
- Ağ Sızma Tespit/Engelleme Sistemi modu (NIDS/NIPS): Snort'un en karmaşık ve yapılandırılabilir modudur. Snort bu modda temel olarak trafiği analiz edip kullanıcı tarafından tanımlanabilen bir kural seti ile gördüklerine karşı çeşitli eylemler gerçekleştirebilir.

Snort, ağın algılama ve önleme gereksinimlerine bağlı olarak çeşitli alt modlarda da çalışır. Snort bir IP ağı üzerinde paket günlüğü ve trafik analizi yapar. Yani, ağa bağlanır ve transit olan veri paketlerini değerlendirir. Snort kural tabanlıdır, bu da değerlendirmenin nasıl yapıldığına bağlı olarak bir dizi koşul tanımlanabileceği anlamına gelir. Web'de en yaygın olarak kullanılan IPS (Intrusion Prevention Systems - İzinsiz Giriş Önleme Sistemleri) sistemlerinden biridir. Çeşitli işletim sistemlerinde bulunur, çok esnektir ve yapılandırılabilir.

Snort başlangıçta Martin Roesch tarafından yazılmıştır. Hem açık kaynak hem de Sourcefire tarafından sunulan ticari bir sürümü de mevcuttur. Snort çok iyi belgelenmiştir ve kolayca indirilebilecek iyi bir kural arşivine sahiptir. Snort'un, kullanıcıların sorularına cevap alabilecekleri çok aktif bir forumu da vardır.

4.2.1.2. Nmap Kullanarak Ağ Tarama

Hacker topluluklarında Fyodor Vascovich takma adıyla da tanınan Gordon Lyon tarafından yazılmıştır. Nmap, mevcut en güçlü, esnek ve yapılandırılabilir ağ tarayıcı araçlarından biridir. Bir ağın tamamını ondan fazla farklı derinlik seviyesiyle profilleyebilir.

Nmap, ana makineye, hizmetlere, portlara, topolojiye, zamanlamaya ve diğer çeşitli profillere dayalı olarak şebekeyi eşleyebilir. Örneğin, hedef ana bilgisayara bir ağ paketi göndererek, yanıt başlığını inceleyerek ve veritabanındaki bilinen kalıplarla karşılaştırarak bir ana makinenin çalıştığı işletim sistemini tahmin edebilir.

Nmap çeşitli öğeleri keşfeder ve ağ haritasını çıkarır. Nmap'ın en güçlü özelliklerinden biri, pasif hizmetleri keşfetme yeteneğidir. Yani, Nmap, bir servisin mevcut olup olmadığını keşfedeceği için, bir servis bulma protokolü gibi kendisini tanıtmak için servise bağımlı değildir. Nmap'ın temel gizli ağ tekniklerine derinlemesine nüfuz etmesini sağladığı için bu, Nmap'ın önemli bir özelliğidir. Çoğu durumda, Nmap ayrıca uygulama adını ve sürüm numarasını da belirleyebilir [18].

4.2.2. Web Uygulaması Araştırması

Kullanıcıların bir sistemle etkileşimde bulunduğu yerlerde, web siteleri, sistemle kullanıcı arasındaki başlangıç aşamasıdır. Ayrıca, genellikle bilgisayar korsanlarının kendisiyle etkileşimde bulunduğu yerdir. Bu katmanın mantığını ve akışını son derece dikkatle değerlendirmek gerekir. Bunu yapmanın en iyi yolu, bütünlüğünü kontrol etmek ve tüm sayfaların tasarımcı tarafından tasarlandığı gibi çalışmasını sağlamak için tüm bağlantıları manuel olarak kontrol etmektir. Bununla birlikte, karmaşık bir site için, bu her zaman pratik değildir. Bu nedenle, bu görevi daha verimli yapmak için aşağıdaki araç koleksiyonu seti tanıtılmıştır [18].

4.2.2.1. Lynx

Lynx, World Wide Web için bir metin tarayıcısıdır. JavaScript'in ve AJAX ve JSON gibi ilgili teknolojilerin (örneğin, hedef web sitesinde) geniş kullanımı, dinamik içerik oluşturma ve anında işlevsellik uygulamaktan büyük ölçüde arınmış oldukları için Lynx'i işe yaramaz hale getirebilir; bu da, güvenilir Lynx çıktı analizini gerçekleştirmeyi zorlaştırır. Lynx etkileşimli bir araçtır. Lynx arayüzü kullanıcının hedef bölgeyi dinamik olarak dolaşmasına ve içeriğini değerlendirmesine olanak tanır. Bir web sitesi içeriğinin otomatik olarak taranması için, tarama ve çaprazlama gibi yararlı seçenekler vardır; bunlar, daha sonraki işlemler için biçimlendirilmiş HTML içeriğini bir dosyaya dökecektir.

4.2.2.2. Wget

Wget, HTTP, HTTPS ve FTP protokollerini kullanarak dosyaları almak için GNU tarafından sağlanan ücretsiz bir yazılım paketidir. GNU, 1984 yılından beri aktif olarak gelişmekte olan ücretsiz bir Unix benzeri işletim sistemidir. Wget, etkileşimli olmayan, neredeyse yüz seçeneği bulunan bir komut satırı aracıdır. Bir komut dosyası ve Wget‘i kullanarak statik analiz için otomatik olarak bir web sitesinin tamamı indirilebilir. Yalnız Wget, gelişmiş bir Web uygulaması araştırma aracı sayılmaz, ancak diğer otomatik araçlar tarafından çağrıldığında, bir web sitesinde olası tasarım kusurlarını ortaya çıkarabilir.

4.2.2.3. Teleport Pro

Teleport Pro, Tennyson Maxwell Information Systems, Inc. tarafından çevrimdışı tarama için geliştirilmiş bir yazılımdır. Çerez desteği, JavaScript ayrıştırma yeteneği, eş zamanlı erişim parçaları, Java Applet alımı ve alma filtreleri sağlaması Lynx ve Wget'in üstünlüğünü taşır. Teleport Pro çeşitli içerikler (dinamik ve statik) elde etmek için kullanışlı bir araçtır; boyutuna, türüne ve arama anahtarlığına göre filtrelenebilir ve aynı dosyalar için birden fazla sitede arama yapılabilir.

4.2.2.4. BlackWidow

Teleport Pro'ya benzer şekilde, BlackWidow, bir siteyi taramak, yapısının ve iç ve dış bağlantıların eksiksiz bir profilini oluşturmak ve hatta bağlantı hatalarını bulmak için SoftByte Labs, Inc. tarafından geliştirilmiştir. BlackWidow, daha fazla çevrimdışı analiz için ve tüm dosyanın içeriğini indirmek için güçlü bir filtreleme kabiliyetine sahiptir. Hedef site ekranının anlık görüntüsünü oluşturabilir ve depolayabilir. BlackWidow'un çekici özelliklerinden biri, yerel sisteme indirmeden bir siteyi uzaktan tarama yeteneğidir. Bu özellik, aktif ve devam etmekte olan keşif işlemleri için zamandan ve depolama kapasitesinden tasarruf edebilmeyi sağlar.

4.2.2.5. BrownRecluse Pro

BrownRecluse Pro, web tarama için SoftByte Labs, Inc.'in kullandığı başka bir ücretli programdır. BlackWidow'un gelişmiş, programlanabilir bir sürümüdür; örümcek komutlarıyla beslenebilir; bunlar, aracın nasıl çalıştığını ve neyin nasıl yakalandığını otomatikleştiren talimatlardır. Senaryolar SoftByte Labs, Inc tarafından hazırlanan SBL (Spider Bot Language - Örümcek Bot Dili) adlı bir dilde yazılmıştır; hazır betiklerin geniş bir arşivi kullanıcılara da sunulmaktadır.

4.2.3. Güvenlik Açığı Taraması

Güvenlik açığı taraması, bilinen kusurların varlığı hakkında zaten bilgiye sahip olunduğundan, bunların nasıl tespit edileceği bilindiğinden ve hedef ürünlerde bulunmaya çalışıldığından, uygulama anketi ve ağ taramasından farklıdır. Bu tekniği kullanarak, hedef sisteme gönderilen paketleri titizlikle hazırlar ve alınan tepkileri çok dikkatli bir şekilde inceleme imkanı verir. Güvenlik açığı taraması yıkıcı bir moda

monte edilebilir; bu da hedef sistemin çökmüş olmasına ya da hedef sistemin faydasız hale getirilmesine ya da yıkıcı olmamasına neden olarak hedef sistemin çalışmasına devam etmesine izin verir. Bu bölümde açıklanan araçlar güvenlik açıkları taramasında en iyi araç setlerinden bazılarıdır [18].

4.2.3.1. Nessus

Güvenlik uzmanlarının kullanabileceği en kapsamlı güvenlik açığı tarayıcılarından biri Nessus'tur. Tenable Network Security, Inc. tarafından geliştirilmiş ve sürdürülmüştür. Nessus, iki katmanlı bir mimariye sahiptir. Bir istemci ve bir sunucu bileşeninden meydana gelir. Sunucu parçasına Nessus güvenlik açığı tarayıcı adı verilir. Nessus sürüm 4.2 itibariyle, istemci bileşeni web tabanlı bir arabirimdir ve bu herhangi bir tarayıcı ile kullanılabilir. Bilinen güvenlik açığı modelleri hakkında kapsamlı bir veritabanına sahiptir ve güvenlik açığı taraması yapmakla ilgili yapılandırma seçenekleri olan önceden tanımlanmış ilkelere dayanarak çalışır.

4.2.3.2. Nikto

Nikto, web sunucusu taraması için açık kaynak kodlu bir yazılım paketidir. Chris Sullo tarafından geliştirilmiştir. Nikto, GPL (www.gnu.org/licenses/licenses.html#GPL) kapsamında lisanslıdır ve özellikle web sunucularını test etmeye yönelik kullanışlı bir araçtır. Web sunucuları, dağıtımlarının çokluğundan ötürü meta yazılımı olarak düşünülseler de, güvenli olmayan şekilde yapılandırılmaları kolaydır veya en son güvenlik yamaları ile senkronize edilmezler. Nikto, hedef web sunucularında kapsamlı testler yapar, her bir web sunucusu sürümü için bilinen güvenlik açıkları bulunan bir veritabanına sahiptir ve bulgularını standart günlük dosyalarında raporlar. Nikto'nun kullanışlı özelliklerinden biri de öğeleri doğrulamak veya taramak için kullanılan seçenekler modülerdir ve ayrı ayrı güncellenebilir. Nikto, toplu iş ve komut dosyası oluşturma ortamları gibi otomatikleştirilmiş araçlara entegre olabilen çok yetenekli bir komut satırı arabirimine sahiptir.

4.2.3.3. Wireshark

Wireshark çok güçlü bir ağ protokol analizörüdür. Wireshark tüm popüler ve gelişmiş işletim sistemlerinde çalışır. GNU GPL v2 kapsamında lisanslanan ücretsiz ve açık kaynaklı bir yazılımdır. Wireshark takılabilir ve genişletilebilir bir ağ paket analizörüdür. Diğer ağ analiz cihazlarını kullanarak bir ağdan paket veri yakalayabilir ve Wireshark'ın bu dosyaları okuması ve analiz etmesi için araçlarını kullanması ihtimali çok yüksektir. Bu araç tarafından desteklenen dosya biçimleri listesi, dosya biçiminin ne olduğunu belirtir.

4.2.4. Penetrasyon Testi (Penetration Testing)

Penetrasyon testi olası güvenlik açıkları için sistem korumasını değerlendirmek için düşman varlıkların - makine, insan veya her ikisinin bir kombinasyonu - tarafından yapılan bir saldırıyı simüle etmek için kullanılan yöntemlerin bir kombinasyonudur. Kısaca, bir saldırgan bir kurumun sistemini kırmadan önce sistemi kurumun kendisinin kırmaya çalışmasıdır [20]. Bu bağlamda güvenlik açığı, bir hedef sistemin güvenlik mekanizmasındaki potansiyel bir zayıflıktır; bir istismar, güvenlik açığına yol açtığı bilinen bir yoldur ve bir saldırı, bir istismarı gerçekleştirmek için aktif girişimdir.

İki tür test vardır: zararlı ve zararsız testler [18]. Zararlı testler, testin hedefini, normal çalışmasını etkileyecek şekilde çalışır. Zararsız testler, test hedefini etkilenmeden bırakır. Penetrasyon testi çoğunlukla zararlı olabilmektedir. Penetrasyon testi, yanlışlıkla olsa bile, hedef sistemde bir miktar zarara neden olma potansiyeline sahiptir. Test ekibi, testleri gerçekleştirme iznine sahip olduğundan emin olmalı ve olası sonuçları, hedef sistemlerin sahiplerine veya yöneticilerine açıkça bildirmelidir.

4.2.4.1. Metasploit

Güvenlik uzmanları tarafından kullanılan en gelişmiş penetrasyon test araçlarından biridir. Metasploit tam teşekküllü bir platformdur. Yani, bir çalışma ortamı (Metasploit Framework veya MSF), bir kabuk (Meterpreter saldırı platformu), önceden tanımlanmış istismarlar (Payloads) ve iyi tanımlanmış bir işlevi (Exploits) vardır.

Meta kaynağı modülerdir. Diğer bir deyişle, farklı yüklenen veriler oluşturabilir ve uygunsa, aynı Framework ve Meterpreter bileşenlerini kullanarak bunları bir hedef

üzerinde çalıştırabilir. Hedef bir bilgi işlem ortamındaki bir istismarın, işletim sistemi gibi farklı özelliklere sahip başka bir hedef sistem için de geçerli olup olmadığı test etmeye çalışıldığında, Metasploit'in modülerliğinin gücü belirginleşir.

Metasploit, Yumuşak Mimari olarak adlandırılan araçları uygular. Diğer bir deyişle, Nmap, Nessus, Wireshark, kod düzenleyiciler ve IDA Pro veya SoftIce gibi çeşitli hata ayıklayıcılar ve ayrıştırıcılar gibi tamamlayıcı araçlar ile kolayca bütünleşir. Metasploit, çok çeşitli popüler ve gelişmiş işletim sistemlerinde çalışır.

Metasploit'in gücü göz ardı edilemez; güvenilir ellerde çalıştırıldığında, iyi hazırlanmış yükler enjekte ederek sıklıkla güçlendirilmiş sistemleri uzaktan rahatça atlatabilir.

4.2.4.2. Aircrack-ng

Aircrack-ng, 802.11 WEP ve WPA-PSK kablosuz protokolleri için kilit bir programdır. Hedef kablosuz erişim noktasından yeterli miktarda veri paketi yakalayarak anahtarları kırar. Ayrıca kablosuz LAN'lar için denetim aracı olarak da kullanılabilir. Aircrack-ng, çoğu Microsoft Windows kablosuz ağ sürücüsünün tescilli yapısı nedeniyle Linux işletim sisteminde en iyi şekilde kullanılır. Aircrack-ng, bu sürücülerde açıkça bulunandan daha fazla kablosuz ağ sürücüsü dahili bilgi seviyesi gerektirir. Ancak, bu kısıtlama, bilgisayar korsanlığı topluluğu ve genel olarak güvenlik uzmanları için büyük bir problem oluşturmaktadır.

4.2.5. Kablosuz Ağları Tespit Etme

Bu bölümde, hangi trafik türlerinin mevcut olduğunu belirlemeye yardımcı olacak araçlar incelenecektir [18].

4.2.5.1. NetStumbler

Kablosuz Yerel Ağları (WLAN'lar) veya kablosuz hotspot'ları tespit etmek için kullanılan basit bir araçtır. Yalnızca Microsoft Windows işletim sistemi için kullanılabilir ve kullanımı çok kolaydır. Dizüstü bilgisayarın kablosuz ağ arabirimleriyle birlikte verilen yönetim aracı yerine NetStumbler'ı kullanmanın bir avantajı, NetStumbler'ın komut dosyalarını desteklemesidir. Bu, NetStumbler'ı bir

haritalama uygulamasıyla arabirim yapmayı ve daha ileri işlemler için verileri bir özel veritabanına göndermeyi de içeren çeşitli şekillerde genişletme olanağı sağlar: NetStumbler, bu tür uzantılar için entegre bir GPS desteği ile birlikte gelir.

4.2.5.2. Kismet

NetStumbler'ın üzerinde bir adımdır, zengin özelliklere sahip bir kablosuz ağ dedektörü ve İzinsiz Giriş Algılama Sistemi'dir. Kismet, 802.11 protokolünün (802.11b, 802.11a, 802.11g ve 802.11n standartları) tüm varyantlarının içeriğini yoklayabilir veya engelleyebilir. Kismet, 802.11 dışındaki protokolleri de algılar, yoklamak ve çözmek için kullanılan eklenti bir mimariyi destekler. Yani, kişiler kendi eklentilerini farklı bir protokol (örneğin Bluetooth) için indirebilir veya kodlayabilir ve Kismet'in tüm işlevlerini kullanabilir.

Kismet Linux, FreeBSD, NetBSD, OpenBSD ve Mac işletim sistemlerinde çalışır. Windows için bir istemci bileşeni de vardır; bununla birlikte, bu işletim sistemi için desteklenen kablosuz ağ kartlarının sayısı sınırlıdır. Herhangi bir ücretsiz ve açık kaynaklı yazılım gibi, Kismet özel ihtiyaçlara uyacak şekilde inşa edilebilir veya var olan araçlarla bütünleştirilebilir.

Neredeyse tüm çalışma modlarında Kismet, kök (root) veya yönetici (administrator) ayrıcalıkları gerektirir. Kismet'in sağladığı avantajlardan biri, sınırlı bir RAM bulunan ve kaynakları kısıtlı, gömülü sistemler üzerine kurulabilmesidir. Kismet paketleri yakalamak için ağ katmanında bulunduğu için ağ arabiriminin modunu değiştirir. Bu nedenle, üst düzey araçlar için varlığını saptamak zor olacaktır. Kismet bir komut satırı kullanıcı arabirimine sahiptir ve otomatik keşif araçlarına entegre edilebilir.

4.2.5.3. AirMagnet Wi-Fi Analyzer

802.11 protokol standartları için ticari bir izleme aracıdır. Bu ürünün avantajlarından biri kapsamlı izleme, yönetim ve denetim araçlarıyla ilgilidir. Ayrıca oldukça sezgisel bir grafik kullanıcı arayüzü vardır. Bu araç kablosuz keşif için tasarlanmamış olmasına rağmen, gerçek zamanlı arıza giderme, Wi-Fi çerçeve çözme ve saldırı algılama motoru (AirWISE'ye dayanan, AirMagnet ürünlerinin arkasındaki çekirdek algılama motoru) gibi bazı yetenekleri de aktif keşif için çekici bir araç haline getirmektedir.

4.2.6. Güvenliği Doğrulama Araçlarının KOBİ'lere Faydaları

Bu bölümde tanıtılan güvenliği doğrulama araçlarının en çok da bilişim sektöründe yer alan KOBİ'ler için faydası bulunmaktadır. Bilişim sektöründe yer alan KOBİ'ler, bu çalışmada anlatılan test araçlarının yanı sıra internet üzerinden de kolayca bulunabilecek diğer test araçlarından da faydalanarak işletmelerinin internet ortamında güvenlik açıklarını kolayca test edebilirler. Tanıtılan güvenlik açığı test araçlarının birçoğunun ücretsiz sürümleri mevcuttur. İşletme yöneticileri ve bilgi teknolojileri uzmanları bu test araçlarına herhangi bir bütçe ayırmadan ücretsiz bir şekilde kullanabilirler. Böylece işletmenin mevcut güvenlik açıkları tespit edilecek ve gerekli güvenlik önlemleri alınarak tehlikelere açık olan unsurlar ortadan kaldırılacaktır.

4.3. **Siber Güvenlik Tehditleri**

Birçok kurum sahip olduğu verileri siber tehditlere karşı korumaya çalışırken önemli problemlerle karşılaşmaktadır. Bu problemler, kurum içinden veya dışından insan kaynaklı olabileceği gibi kötü niyetli kullanıcıların geliştirmiş oldukları zarar verici yazılımlardan da kaynaklanabilir.

Genellikle internet üzerinden bulaşan truva atları, virüsler, solucanlar, anahtar kaydediciler (klavye dinleyiciler), casus yazılımlar, kimlik avı yöntemleri ile kurumlara veya kurumların çalışanlarına ait veriler ele geçirilip kurumlar veya şahıslar zarara uğratılmaktadır. Ele geçirilen bu veriler kötü amaçlı olarak kullanılabilir, fidye amacıyla çalınmış olabilir, ilgili kurumu veya şahsı maddi veya manevi yönden zarara uğratmak amacıyla değiştirilmiş veya yok edilmiş olabilmektedir [1].

OWASP (The Open Web Application Security Project - Açık Web Uygulama Güvenliği Projesi) tarafından 2017 yılı için en çok rastlanan 10 uygulama güvenliği riskleri belirlenmiştir. OWASP, kurumların güvenilir olabilecek uygulamaları ve API'leri geliştirmelerine, satın almaları ve muhafaza etmelerine olanak tanıyan açık bir topluluktur [21].

OWASP'ta ücretsiz olarak bulunan hizmetler [21]:

- Uygulama güvenlik araçları ve standartları.
- Uygulama güvenliği testi, güvenli kod geliştirme ve güvenli kod incelemesi ile ilgili eksiksiz kitaplar.
- Sunumlar ve videolar.
- Birçok yaygın konuda hile sayfaları.
- Standart güvenlik kontrolleri ve kütüphaneler.
- Dünya çapında yerel bölümler.
- Son teknoloji araştırması.
- Dünya çapında kapsamlı konferanslar.
- Eposta listeleri.

OWASP'ta 2017 yılı içinde en çok rastlanan 10 güvenlik açığı şu şekilde listelenmiştir [22]:

1) **Enjeksiyon Açıkları (Injection):** SQL, NoSQL, OS ve LDAP enjeksiyonu gibi enjeksiyon kusurları, güvenilmeyen veriler bir komutun veya sorgunun bir parçası olarak bir yorumlayıcıya gönderildiğinde ortaya çıkar. Saldırganın düşmanca verileri, yorumlayıcıyı istenmeyen komutları yürütme veya uygun yetkilendirme olmadan verilere erişme konusunda kandırır.
2) **Bozuk Kimlik Doğrulama (Broken Authentication):** Kimlik doğrulama ve oturum yönetimi ile ilgili uygulama işlevleri genellikle saldırganların şifreleri, anahtarları veya oturum jetonlarını riske atmasına veya diğer kullanıcıların kimliklerini geçici veya kalıcı olarak kabul etmek için diğer uygulama kusurlarından yararlanmasına izin vermeyerek yanlış uygulanmaktadır.
3) **Hassas Veri Maruziyeti (Sensitive Data Exposure):** Birçok web uygulaması ve API, finansal, sağlık hizmeti ve kişisel bilgiler gibi hassas verileri doğru şekilde korumaz. Saldırganlar, kredi kartı sahtekarlığı, kimlik hırsızlığı veya diğer suçları işlemek için zayıf korumalı verileri çalabilir veya değiştirebilir. Hassas veriler, istirahatte veya transitte şifreleme gibi ekstra koruma olmaksızın tehlikeye girebilir ve tarayıcı ile değiştirilirken özel önlemler gerektirir.

4) **XML Dış Öğeleri (XML External Entities - XXE):** Birçok eski veya zayıf yapılandırılmış XML işlemcisi, XML belgeleri içinde harici varlık referanslarını değerlendirir. Dış varlıklar, dosya URI işleyicisi, iç dosya paylaşımları, iç bağlantı noktası taraması, uzaktan kod yürütme ve hizmet reddi saldırılarını kullanarak dahili dosyaları açıklamak için kullanılabilir.
5) **Bozuk Erişim Kontrolü (Broken Access Control):** Kimliği doğrulanmış kullanıcıların yapmasına izin verilen kısıtlamalar genellikle uygun şekilde uygulanmaz. Saldırganlar, diğer kullanıcıların hesaplarına erişmek, hassas dosyaları görüntülemek, diğer kullanıcıların verilerini değiştirmek, erişim haklarını değiştirmek vb. gibi yetkisiz işlevlere ve / veya verilere erişmek için bu kusurları kullanabilir.
6) **Yanlış Güvenlik Yapılandırması (Security Misconfiguration):** Yanlış güvenlik yapılandırması en sık görülen sorundur. Bu genellikle güvensiz varsayılan yapılandırmaların, tamamlanmamış veya geçici yapılandırmaların, açık bulut depolamanın, yanlış yapılandırılmış HTTP başlıklarının ve hassas bilgiler içeren ayrıntılı hata iletilerinin bir sonucudur. Tüm işletim sistemleri, çerçeveler, kütüphaneler ve uygulamalar güvenli bir şekilde yapılandırılmalı, aynı zamanda düzeltilmeli ve güncellenmelidir.
7) **Siteler Arası Komut Dosyası (Cross-Site Scripting):** XSS kusurları, bir uygulama uygun doğrulama veya çıkış olmadan yeni bir web sayfasında güvenilmeyen verileri içerdiğinde veya HTML veya JavaScript oluşturabilen bir tarayıcı API'sı kullanarak mevcut bir web sayfasını kullanıcı tarafından sağlanan verilerle güncellediğinde ortaya çıkar. XSS, saldırganların kurbanın tarayıcısında kullanıcı oturumlarını ele geçirebilecek, web sitelerini yok edebilecek veya kullanıcıyı kötü amaçlı sitelere yönlendirebilecek komut dosyaları çalıştırmasına izin verir.
8) **Güvensiz Serileştirme (Insecure Deserialization):** Güvensiz serileştirme genellikle uzaktan kod yürütülmesine yol açar. Seri hale getirme kusurları uzaktan kod yürütme ile sonuçlanmasa bile, yeniden oynatma saldırıları, enjeksiyon saldırıları ve ayrıcalık yükseltme saldırıları dahil olmak üzere saldırılar gerçekleştirmek için kullanılabilir.

9) **Bilinen Güvenlik Açıkları Olan Bileşenler (Components with Known Vulnerabilities):** Kitaplıklar, çerçeveler ve diğer yazılım modülleri gibi bileşenler, uygulama ile aynı ayrıcalıklarla çalışır. Savunmasız bir bileşen kullanıldıysa, bu tür bir saldırı ciddi veri kaybını veya sunucu devralmasını kolaylaştırabilir. Bilinen güvenlik açıklarına sahip bileşenleri kullanan uygulamalar ve API'ler, uygulama savunmalarını zayıflatabilir ve çeşitli etkileri ve saldırıları etkinleştirebilir.
10) **Yetersiz Kayıt ve İzleme (Insufficient Logging & Monitoring):** Yetersiz kayıt ve izleme, gelen yanıtla eksik veya etkisiz entegrasyonla birleştiğinde, saldırganlara daha fazla saldırı sistemine izin verir, kalıcılığını sürdürür, daha fazla sisteme dönebilir ve verileri kurcalayabilir, ayıklayabilir veya yok edebilir. Çoğu ihlal çalışması, ihlali tespit etme süresinin 200 günü aştığını, genellikle iç süreçler veya izleme yerine harici taraflarca tespit edildiğini gösterir.

OWASP tarafından sunulan bu hizmetlerden faydalanarak işletmelerin genel güvenlik önlemleri alınabilir. Böylece güncel tehditler takip edilerek olası tehditler önceden öngörülebilir, buna dayanarak risk senaryoları oluşturulabilir ve güvenlik önlemleri bu doğrultuda oluşturulabilir.

4.4. **Siber Güvenlik Tehditlerine Karşı Alınabilecek Önlemler**

KOBİ'lerde veri güvenliğini sağlamak ve oluşabilecek siber tehditlerden korunmak için öncelikli olarak kurumun çalışanlarına bilgi teknolojilerinin güvenliğinin sağlanmasına yönelik eğitimler aracılığı ile farkındalık oluşturulması gerekmektedir. Çünkü bir güvenlik zincirinin en zayıf halkası insandır. Kurumlarda güvenlik tehditlerine yönelik önlemler almaya çalışırken hangi verilerin veya bilgilerin, hangi tehdit ve tehlikelerden, ne derece korunması gerektiği, güvenliğin nasıl sağlanacağı ve alınacak önlemin finansal maliyetinin planlanması gerekmektedir. Bu planlamaların dışında alınabilecek diğer önlemler şunlardır [2]:

- **Ağ Güvenliği:** Ağ güvenliği tam olarak aşağıdaki güvenlik kavramlarını bir bütün olarak ele alınmasıyla sağlanabilir [23].
- **İnternet bağlantı güvenliği:** Kurumun her zaman açık olan bir bant bağlantısı varsa saldırıya uğrayabilir. Saldırıları önlemek için güvenlik duvarları (firewall) kullanılmalıdır.
- **Şifreleme:** Kurum içinde kullanılan ağ için güçlü parola ve şifreler kullanılmalıdır.
- **Log analizi:** Ağ üzerinde oluşan trafiğin kayıtları tutulmalıdır ve acil durumlarda hangi noktalarda problem olduğu tespit edilirken bu kayıt defterlerinden faydalanılmalıdır.
- **VPN Güvenliği:** Kurumun sistemine kurum dışından erişim varsa bu bağlantının güvenliği özel sanal ağ (virtual private network - VPN) gibi ağlarla sağlanmalıdır.

Ayrıca ağ güvenliğini sağlamak için kullanılmayan ve gereksiz ağ bağlantı noktaları mutlaka kapatılmalıdır. Kablosuz ağlarda, güvenlik ve gizlilik seçenekleri mutlaka arttırılmalıdır.

Kurum içinde alınması gereken önlemler sadece ağ güvenliğine yönelik değildir. Alınabilecek diğer önlemler şu şekilde sıralanabilir:

Kurum İçi Kullanılan Programların Güvenliği: Kurum içinde kullanılan muhasebe, finans ve diğer özel programların güçlü şifreleme, yetkisiz erişimi kısıtlama, güvenlik duvarını kullanma gibi güvenlik önlemlerini almakla birlikte düzenli olarak güncelleştirme ve yedeklemelerinin de yapılması gerekir.

Kötü Amaçlı Yazılımlara Karşı Koruma: Truva atları, virüsler, solucanlar vb. gibi sisteme zarar verebilecek kötü amaçlı yazılımlardan korunmak için antivirüs programları kullanılmalı ve bu programlar düzenli olarak güncelleştirilmelidir.

Şifre Yönetimi: Kullanıcı hesaplarını ve verilerini korumak için alınabilecek en büyük önlemlerden birisi de kuşkusuz belirlenecek şifreler olacaktır. Şifrelerde mutlaka büyük-küçük harfler, özel karakterler ve rakamların hepsi bir arada bulunmalı, kişisel

bilgiler (doğum tarihi, isim-soyisim, cep telefonu numarası vb.) ve sözlükte bulunabilen kelimeler kesinlikle kullanılmamalıdır. Ayrıca, aynı şifreyi farklı hesaplar için kullanmak güvenlik zafiyetine sebep olabilir. Çalışanlara mutlaka güvenli şifre oluşturma konusunda bilgi verilmelidir.

Disk Şifreleme Politikası: Kurum açısından hayati önem taşıyan dosyalar ve programlar şifrelenmeli, bu tür dosyalara ve programlara sadece yetkili kişiler erişebilmelidir. Windows işletim sistemlerinde veri güvenliği ve tüm dosyaların saklanması için sunulan Bitlocker veya benzeri tüm disk şifreleme ile güvenlik düzeyi bir seviye daha arttırılabilir. Ayrı ayrı dosyaları şifrelenmesini sağlayan sistemden farklı olarak sürücünün tamamını şifreler. Tüm disk şifrelemenin en büyük özelliği, saldırganlar şifre öğrenmek için sistem dosyalarına girdiğinde ya da sürücü bilgisayardan çıkarılıp başka bir bilgisayara takıldığında sürücüye erişim engellenmiş duruma gelir. Ayrıca yeni dosyalar eklediğinde, bu tür yazılımlar bu dosyaları da otomatik olarak şifreler ve saklar.

Çoklu Adımlı Doğrulama: Kurumsal yapılarda mutlaka alınması gereken bir diğer güvenlik önlemi ise iki adımlı doğrulama sistemidir. Son yıllardaki veri sızıntısı vakalarının çoğunda, ele geçirilen kullanıcı bilgileri büyük rol oynamıştır. Kullanıcı hesabına giriş yaparken şifresini girdikten sonra, telefonuna gelecek olan ikinci bir şifreyi girerek hesabına erişim sağlayabilmelidir. Bu yöntem ile kullanıcının hesabı daha güvenli bir hal alacaktır.

Kurum İçi Erişim Yetki Düzeyini Sağlama: Yetki ile bazı dosyalara, programlara hatta sunucuya erişim kısıtlanmalıdır. Çalışanlar arasında uygun görev dağılımı yapılıp, herkes kendi görevi gereğince yetkili olduğu kaynaklara erişebilmelidir.

Fiziksel Erişim Güvenliği: Kurum içi güvenlik sadece donanım ve yazılımdan ibaret olmamakla birlikte, güvenlik kontrolleri yapılarak (kimlik kartı, parmak izi veya yüz tanıma sistemleri ile giriş yapma) kurumun fiziksel olarak var olduğu bina veya ofis içerisine giriş yapılmalıdır. Bu sistemler aracılığıyla yapılan giriş-çıkışların kayıtları da kayıt defterlerinde (log) tutulmalıdır.

Güvenlik Eğitimleri: Kurumların düzenli olarak güncel güvenlik tehditlerini ve açıklarını takip etmesi gerekmektedir. Bu doğrultuda çalışanlara internette güvenli bir şekilde gezinmeleri ve riskli sitelere bilgi aktarımında bulunmamaları yönünde gerekli eğitimler verilmelidir.

Alınabilecek bu önlemlerin dışında kurumdaki çalışanların günlük faaliyetlerini gerçekleştirdikleri durumlar da birçok güvenlik açığına sebep olabilmektedir. Bunlar genellikle internet üzerinde yapılan işlemlerden kaynaklanır. Bunların en yaygın olanı ise kimlik avı (phishing) saldırıları ile kişinin özel bilgilerini ele geçirme yöntemidir. Bu ele geçirilen bilgiler sadece çalışana has olmayabilir, çalıştığı kurum ve diğer çalışanların bilgilerini de içerebilir [21]. İşte bu sebeple çalışan kaynaklı bir mağduriyetin söz konusu olmaması için de şunlara dikkat edilmelidir:

1) Bir web sitesinde gezinirken güvenilir bir site olduğundan emin olmadıkça, kişisel bilgiler açılır pencerelere (pop-up) kaydedilmemelidir. Açılır pencereler genellikle bir web sitesini meşru bileşenleriymiş gibi hareket eder. Bununla birlikte, çoğu zaman, dolandırıcılık denemeleridir. Birçok popüler tarayıcı, açılır pencereleri engellemeyi sağlar; duruma göre bunlara izin verilmelidir. Eğer ki açılır pençeler herhangi bir şekilde önünüze gelirse, kesinlikle "iptal et" düğmesine tıklanmamalıdır; bu tür düğmeler genellikle kimlik avı sitelerine bağlantı içerir. Bunun yerine, pencerenin üst köşesindeki küçük "x" işaretine tıklanması önerilir.

2) E-postalardaki bağlantıları da tıklamaktan kaçınılmalıdır. Rastgele e-postalarda ve anlık iletilerde görünen bağlantıları tıklamak o kadar akıllıca değildir. Bağlantıların üzerine tıklamadan önce emin olunmayan bağlantıların üzerine fare ile gelinmeli, gerçekten e-posta içeriğinde yazan bağlantı ile aynı olup olmadığı kontrol edilmelidir. Bir kimlik avı e-postası resmi bir kurumdan gelebilir ve web sitesine olan bağlantı açıldığında, tam olarak gerçek web sitesine benzeyebilir.

3) Kullanılan tarayıcılar güncel tutulmalıdır. Her zaman popüler tarayıcılar için güvenlik yamaları yayımlanır. Çoğu tarayıcının en son sürümü, kimlik avı önleme filtreleri ile birlikte gelir. Bir güncelleme olduğunda bu atlanmamalı, güncelleme işlemi başlatılmalıdır.

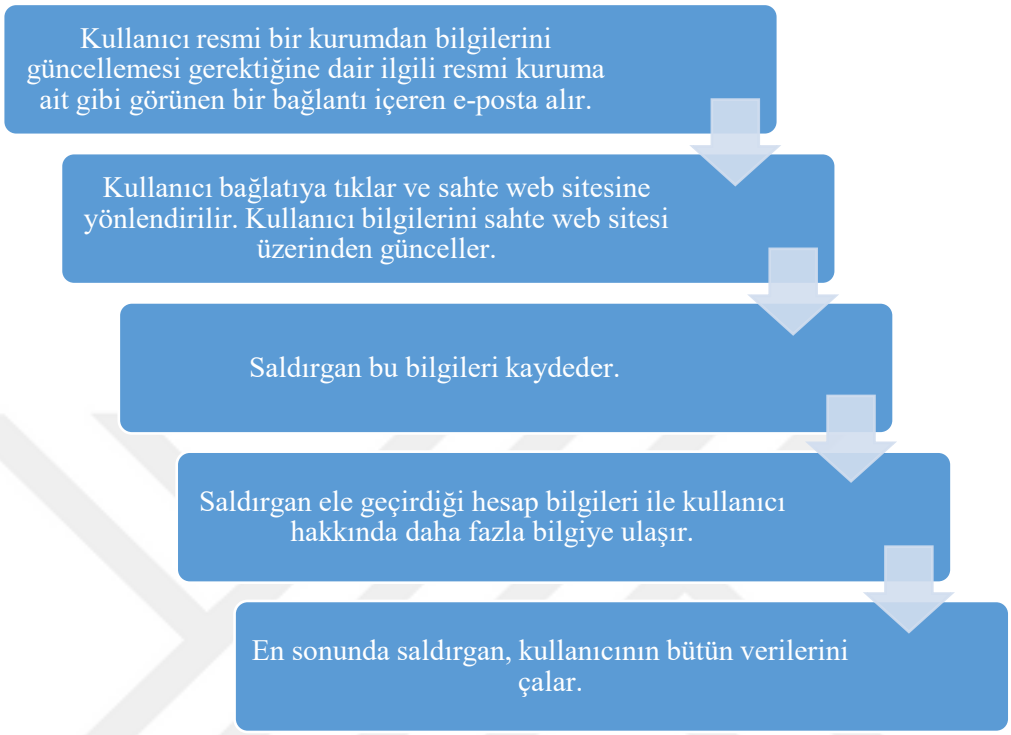
4) Yalnızca güvenilir sertifikalar kabul edilmeli, tarayıcı uyarıları yok sayılmamalıdır. Herhangi bir bilgi göndermeden önce, sitenin URL'sinin "https" ile başladığından ve adres çubuğunun yanında kapalı bir kilit simgesi bulunduğundan emin olunmalıdır. Sitenin güvenlik sertifikasını da kontrol edilmelidir. Belirli bir web sitesinin kötü amaçlı dosyalar içerdiğini belirten bir mesaj alınırsa, web sitesi açılmamalıdır. Şüpheli e-postalardan veya web sitelerinden dosyalar asla indirilmemelidir. Hatta arama motorları, kullanıcıları düşük maliyetli ürünler sunan bir kimlik avı web sayfasına yönlendiren bazı bağlantıları gösterebilir. Kişi böyle bir web sitesinde alışveriş yaparsa, kredi kartı ayrıntılarına siber suçlu tarafından erişilir.

5) İnternet tarayıcılarına bir kimlik avı tespit etme araç çubuğu kurulmalıdır. En popüler İnternet tarayıcıları, kimlik avı önleme araç çubuklarıyla özelleştirilebilir. Bu tür araç çubukları, ziyaret edilen sitelerde hızlı kontroller yapar ve bunları bilinen kimlik avı sitelerinin listeleriyle karşılaştırır. Kötü amaçlı bir siteye rastlandığında, araç çubuğu kullanıcıyı uyarır.

6) Güvenlik duvarları kullanılmalıdır. Yüksek kaliteli güvenlik duvarları kullanıcının bilgisayarı ve dışarıdaki davetsiz misafirler arasındaki arabellek gibi davranır. İki farklı tür kullanılmalıdır: bir masaüstü güvenlik duvarı ve bir ağ güvenlik duvarı. Birinci seçenek bir yazılım türü ve ikinci seçenek ise bir tür donanımdır. Birlikte kullanıldıklarında, bilgisayar korsanlarının ve kimlik avı hırsızlarının bilgisayara veya ağa sızma ihtimalini önemli ölçüde azaltırlar.

7) Antivirüs yazılımı kullanılmalıdır. Antivirüs yazılımını kullanmak için pek çok neden vardır. Virüsten koruma yazılımıyla birlikte gelen özel imzalar, bilinen teknoloji çözümlerine ve boşluklarına karşı koruma sağlar. Kimlik avı saldırılarını önlemek için casus yazılım önleme ve güvenlik duvarı ayarları kullanılmalı ve kullanıcılar programları düzenli olarak güncellemelidir. Güvenlik duvarı koruması, saldırıları engelleyerek kötü niyetli dosyalara erişimi engeller. Virüsten koruma yazılımı, internetten gelen her dosyayı kullanıcının bilgisayarında tarar.

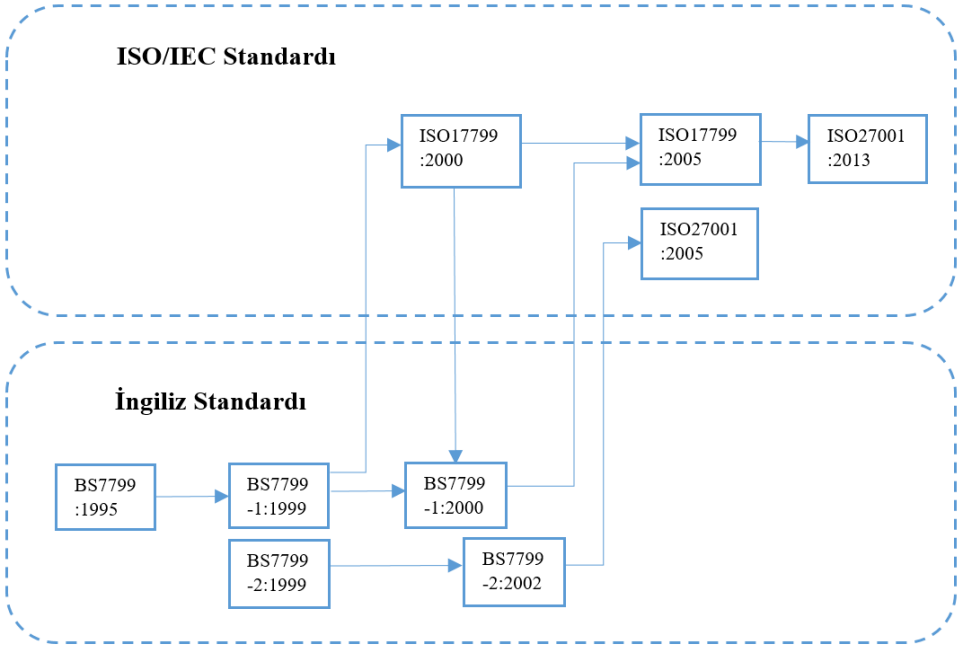
Kimlik avı saldırılarının gerçekleşme aşamaları Çizelge 4.1'de gösterilmiştir.



Çizelge 4.1: Bir kimlik avı saldırısının gerçekleşme aşamaları

5. ULUSLARARASI BİLGİ GÜVENLİĞİ STANDARTLARI

İngiliz Standartlar Enstitüsü (British Standards Institute - BSI) tarafından 1995 yılında BS-7799 standardının ilk kısmı olan BS7799-1, 1999 yılında ise aynı standardın ikinci kısmı olan BS7799-2 yayınlanmıştır. BS7799-1 2000 yılında güncellenerek ISO tarafından ISO/IEC-17799 ismiyle dünya genelinde kabul edilen bir standart haline gelmiştir. 2002 yılında ise BSI tarafından BS-7799 standardının ikinci kısmı olan BS-7799-2 standardı üzerinde güncellemeler yapılarak ikinci defa yayınlanmıştır. 2005 yılında ise ISO tarafından ISO/IEC-17799 standardı üzerinde eklemeler ve düzeltmeler yapılmış ISO/IEC-17799:2005 adıyla yeniden yayınlanmıştır. ISO, 2005 yılında İngiliz standardı olan BS7799-2 üzerinde güncelleler yaparak ISO/IEC-27001:2005 standardını yayınlamıştır [3]. 2013 yılında ISO/IEC-27001 standardının son versiyonu olan ISO/IEC-27001:2013 standardını yayınlamıştır [24]. ISO/IEC-27001 standardının tarihsel gelişimi Şekil 5.1'de gösterilmiştir.



Şekil 5.1: Uluslararası Bilgi Güvenliği Standartları Tarihçesi

5.1. **ISO/IEC Standartları**

IEC (The International Electrotechnical Organization - Uluslararası Elektroteknik Komisyonu) 1906 yılında kurulmuştur [25]. ISO (International Organization for Standardization - Uluslararası Standartlar Organizasyonu) 1947 yılında uluslararası alanda geçerli standardizasyonun sağlanması için, İsviçre'nin Cenova şehrinde kurulmuştur [26]. ISO ve IEC teknik çalışma gruplarıyla (Joint Technical Committee - JTC) standartlar oluşturmaktadırlar [3]. Ayrıca ISO tarafından Bilgi Teknolojileri Güvenlik Standartları ile ilgili çalışmalar JTC 1/SC 27 (Joint Technical Committee 1/Subcommittee 27 - Ortak Teknik Komite 1/Alt Komite 27) tarafından ele alınmaktadır. Bilgi güvenliği konusunda çalışan bu alt komisyonun yöntemlerinden bazıları şunlardır [27]:

- Güvenlik gereksinimleri yakalama metodolojisi,
- Bilgi yönetimi güvenliği; özellikle bilgi güvenliği yönetim sistemleri, güvenlik süreçleri ve güvenlik kontrolleri ve hizmetleri,
- Kriptografik ve diğer güvenlik mekanizmaları, bunlarla sınırlı olmamak kaydıyla, bilginin hesap verebilirliğini, kullanılabilirliğini, bütünlüğünü ve gizliliğini korumaya yönelik mekanizmalar,
- Güvenlik bileşenlerinin kaydı için prosedürlerin yanı sıra terminoloji, kılavuzlar dahil olmak üzere güvenlik yönetimi destek belgeleri,
- Kimlik yönetimi, biyometri ve mahremiyetin güvenlik yönleri,
- Bilgi güvenliği yönetim sistemleri alanında uygunluk değerlendirmesi, akreditasyon ve denetim gereksinimleri,
- Güvenlik değerlendirme kriterleri ve metodolojisi.

Bu yöntemlerin gerçekleştirilmesi için SC 27 alt komitesi de kendi içerisinde 5 ayrı çalışma grubuna (WG – Working Group) ayrılmaktadır [25]:

1) Çalışma Grubu-1 (JTC 1/SC 27/WG 1): Bilgi güvenliği yönetim sistemleri
2) Çalışma Grubu-2 (JTC 1/SC 27/WG 2): Kriptografi ve güvenlik mekanizmaları
3) Çalışma Grubu-3 (JTC 1/SC 27/WG 3): Güvenlik değerlendirmesi, test ve şartname
4) Çalışma Grubu-4 (JTC 1/SC 27/WG 4): Güvenlik kontrolleri ve hizmetleri
5) Çalışma Grubu-5 (JTC 1/SC 27/WG 5): Kimlik yönetimi ve gizlilik teknolojileri

Ayrıca SC 27 komitesi, ilgili alanlarda SC 27 standartlarının ve teknik raporların doğru şekilde geliştirilmesi ve uygulanmasını sağlamak için uygun kurumlarla aktif irtibat ve işbirliği yapmaktadır.

ISO/IEC 27001, bilgi risklerinin yönetimi ile ilgili bir standart olan Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) resmi olarak belirler (standartta "bilgi güvenliği riskleri" olarak adlandırılır). BGYS, kuruluşun bilgi risklerini tanımladığı, analiz ettiği ve ele aldığı kapsamlı bir yönetim çerçevesidir. BGYS, güvenlik düzenlemelerinin, güvenlik tehditleri, güvenlik açıkları ve iş etkileriyle ilgili değişimlere ayak uydurmak için ince ayar yapılmasını sağlar [24].

Standart, her türlü kuruluşu (örneğin ticari işletmeler, devlet kurumları, kar amacı gütmeyen kuruluşlar), her büyüklükteki kuruluşu (mikro işletmelerden çokuluslu şirketlere) ve tüm sektörleri veya pazarları (örn. perakende, bankacılık, savunma, sağlık, eğitim ve devlet) kapsamaktadır [24].

ISO/IEC 27001, gerekli olan kontroller, standardı benimseyen kuruluşların geniş bir yelpazesinde belirgin bir şekilde farklılık gösterdiğinden, spesifik bilgi güvenliği kontrollerini resmi olarak zorunlu kılmaz. ISO / IEC 27002'den gelen bilgi güvenliği kontrolleri, bir menü gibi değil, ISO / IEC 27001 ekinde belirtilmiştir. ISO / IEC 27001'i benimseyen kuruluşlar, belirli bilgi güvenliği kontrollerinin kendi bilgi riskleri için geçerli olduğunu, menüde listelenenlere göre çizim yapabileceklerini ve potansiyel olarak diğer seçeneklerle (bazen genişletilmiş kontrol setleri olarak da bilinir) eklerini seçme konusunda özgürdürler. ISO / IEC 27002'de olduğu gibi,

uygulanabilir kontrolleri seçmenin anahtarı, kuruluşun bilgi risklerinin kapsamlı bir değerlendirmesini yapmaktır. Bu, BGYS'nin hayati bir parçasıdır [24]. ISO / IEC 27001: 2013 aşağıdaki bölümlere sahiptir [24]:

1) **Giriş** - standart, bilgi risklerini sistematik olarak yönetmek için bir süreci açıklar.
2) **Kapsam** - herhangi bir tür, boyut veya nitelikteki organizasyonlar için uygun genel BGYS gerekliliklerini belirtir.
3) **Normatif referanslar** - sadece ISO / IEC 27000 ailesinde 27001 kullanıcıları için kesinlikle temel olarak kabul edilir: kalan ISO27000 ailesinde yer alan standartlar isteğe bağlıdır.
4) **Terimler ve tanımlar**
5) **Örgütün içeriği** - örgütsel bağlamı, "ilgili tarafların" ihtiyaçlarını ve beklentilerini anlamak ve BGYS'nin kapsamını tanımlamak. Kısım 4.4, "Örgüt, BGYS'yi kuracak, uygulayacak, sürdürecek ve sürekli geliştirecektir" ifadesini açıkça belirtmektedir.
6) **Liderlik** - üst yönetim, BGYS'ye liderlik ve bağlılık göstermeli, görev politikasını sağlamalı ve bilgi güvenliği görevlerini, sorumluluklarını ve yetkilerini atamalıdır.
7) **Planlama** - bilgi risklerini tanımlamak, analiz etmek ve planlamak için süreçleri özetlemekte ve bilgi güvenliğinin hedeflerini açıklığa kavuşturmaktadır.
8) **Destek** - yeterli, yetkin kaynaklar atanmalı, farkındalık yaratılmalı, dokümantasyon hazırlanmalı ve kontrol edilmelidir.
9) **Operasyon** - bilgi risklerinin değerlendirilmesi ve işlenmesi, değişikliklerin yönetilmesi ve belgelerin belgelendirilmesi (kısmen sertifikasyon denetçileri tarafından denetlenebilsin diye) hakkında biraz daha fazla ayrıntı.
10) **Performans değerlendirmesi** - Bilgi güvenliği kontrolleri, süreçleri ve yönetim sistemini izlemek, ölçmek, analiz etmek ve değerlendirmek / denetlemek / incelemek, gerektiğinde sistematik olarak iyileştirmek.
11) **İyileştirme** - denetimlerin ve incelemelerin bulgularını ele alır (ör. uygunsuzluklar ve düzeltici eylemler), BGYS'ye sürekli iyileştirmeler yapar.

5.2. **Türk Standartları**

Türkiye'de standartlarla ilgili çalışmalar ve belgelendirmeler, Türk Standartları Enstitüsü (TSE) tarafından yapılmaktadır. TSE teknik komitesinin ISO/IEC 17799:2000 standardının tercümesini yaparak TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri Türk standardı olarak kabul edilmiştir. TS ISO/IEC 17799 standardı; kurumlar üzerinde bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan, bilgi güvenliği yönetimi ile ilgili tavsiyeleri içermektedir.

BGYS belgelendirilmesine yönelik TSE teknik kurulu tarafından yapılan çalışmalar sonucunda ilk olarak BS 7799-2:2002 standardının tercümesi yapılarak "Bilgi Güvenliği Yönetim Sistemleri-Özellikler ve Kullanım Kılavuzu" ismiyle TS 17799-2 standardı olarak kabul edilmiştir. Daha sonra TS ISO/IEC 27001:2006 "Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler", Türk standardı olarak kabul edildiğinden TS 17799-2 standardı TSE tarafından iptal edilmiştir [3].

TS ISO/IEC 270001 standardının hazırlanış amacı; Bilgi Güvenliği Yönetim Sistemini (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model oluşturmaktır [28].

5.3. **İngiliz Standartları**

BS-7799 kuruma ait bilgi varlıklarının tümünün gizlilik doğruluk ve erişilebilirlik ilkeleri doğrultusunda güvence altına almayı garanti eden 2 aşamalı bir standarttır. 1999 yılında yayınlanan ilk sürümünün birinci bölümünde bilişim güvenliği için çalışma kuralları anlatılmaktatır. İkinci bölümünde ise bilgi güvenliği yönetim sistemi planlamak, kurmak ve devam ettirmek gerekli süreçler adım adım anlatılmaktadır.

BSI (British Standards Institution) tarafından geliştirilmiş olan bu standardın tarihsel gelişimi aşağıdaki gibi özetlenebilir [29]:

- 1993 – Uygulanabilirlik Şartnamesi (Code of Practice)
- 1995 – İngiliz Standardı (British Standard)

- 1998 – BS 7799 Bölüm 2 (BGYS için gereklilikler)
- 1999 – BS 7799 Bölüm 1 ve güncellenmiş Bölüm 2 (Tutarlı çift)
- 2000 – BS ISO/IEC 17799: 2000 (BS 7799-1: 2000)
- 2002 – BS 7799-2: 2002

5.3.1. Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi, kuruluşların hassas bilgilerini yöneten ve güvenli kalmasını sağlayan sistematik bir yaklaşımdır. Bu sistem risk yönetim süreci uygulayarak çalışanları iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini içerir. Herhangi bir sektördeki küçük, orta ve büyük ölçekli işletmelerin bilgi varlıklarını güvende tutmasına yardımcı olabilir [30]. BGYS'nin temel amacı hassas bilginin korunmasıdır [31].

Tüm dünyada kabul edilen standart yaklaşımla bilgi güvenliğinin sağlanabilmesi için üç temel unsurun yerine getirilmesi gerekmektedir. Bu unsurlar; gizlilik (Confidentiality), bütünlük (Integrity), erişilebilirlik (Availability) olarak sıralanabilir [28].

- **Gizlilik (Confidentiality):** Önemli ve hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmesi önlenmelidir ve sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğu garanti altına alınmalıdır.
- **Bütünlük (Integrity):** Bilginin bir kısmının veya tümünün yetkili olmayan kişilerce değiştirilmesinin, silinmesinin ve bozulmasının önlenmesi gerekmektedir.
- **Erişilebilirlik (Availability):** Bilgi veya bilgi sistemleri sürekli kullanıma hazır ve erişilebilir olmalıdır.

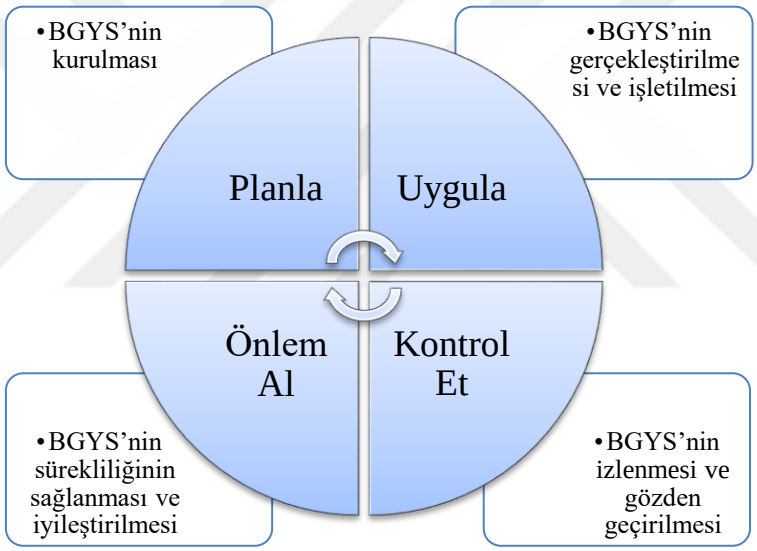
BGYS standartları kapsamında PUKÖ (Planla - Uygula - Kontrol et - Önlem al) modeli kullanılmaktadır [31]. Çizelge 5.1'de PUKÖ döngüsü modelinin aşamaları gösterilmiştir.

a) **Planla (BGYS'nin kurulması):** BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesidir.

b) **Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi):** BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesidir.

c) **Kontrol et (BGYS'nin izlenmesi ve gözden geçirilmesi):** BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesidir.

d) **Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi):** Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesidir.



Çizelge 5.1: PUKÖ döngüsü modeli

5.3.2. Bilgi Güvenliği Yönetim Sisteminin Kurulumu Aşamaları

BGYS kapsamında, güvenlik ile ilgili kontroller 11 aşama halinde toplanmıştır. Şekil 5.2'de BGYS kurulumu aşamaları gösterilmiştir. Bu aşamalar ve kısa tanımları asağıdaki gibidir [28] [31]:

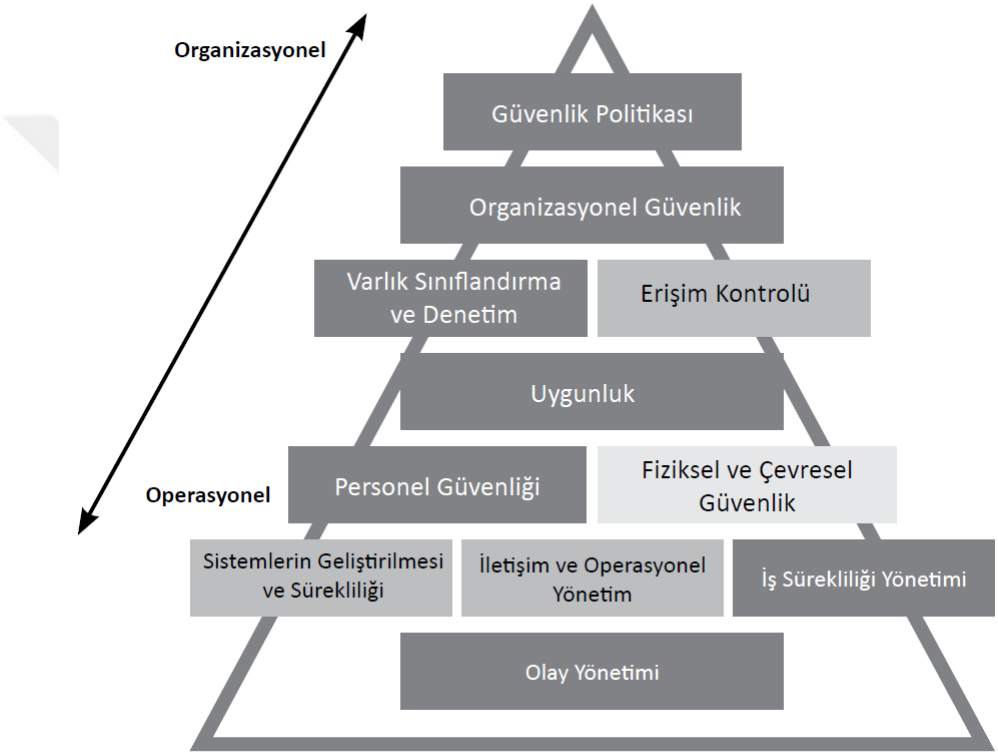
1) **Güvenlik Politikası:** Bilgi güvenliğini artırmaya yönelik hazırlanmış kurallar ve yönetim tavsiyelerini içerir. Yönetim tarafından onaylanmış bir bilgi güvenliği politikası oluşturulmalıdır.

2) **Bilgi Güvenliği Organizasyonu:** Kurum içindeki bilgi güvenliği erişimleri organize edilmelidir.
3) **Varlıkların Sınıflandırılması ve Denetim:** Kuruma ait varlıkların envanteri çıkartılmalıdır. Envanterler hazırlanırken;
   - Bilgi: Kuruma ait sözleşmeler, veritabanı bilgileri gibi
   - Yazılım varlıkları
   - Fiziksel varlıklar: Bilgisayarlar ve iletişim araçları.
   - Hizmete dönük varlıklar: Bilgisayar ve iletişim hizmetleri, ısıtma, aydınlatma, güç vb.
   - Personel
   - Soyut varlıklar: Kurumun itibarı ve imaj

   gibi varlık türleri de göz önünde bulundurulmalıdır.

4) **İnsan Kaynakları Güvenliği:** Kurum içinde çalışan personellerin güvenlik ilke ilgili görev ve sorumlulukları belgelenmeli, çalışanların gizlilik ve açığa çıkarmama anlaşmaları işe alınma şartının bir parçası olarak sözleşme metninde yer almalıdır.
5) **Fiziksel ve Çevresel Güvenlik:** Kurum içerisinde belirli yerlere sadece yetkili olan personelin girişine izin verecek şekilde kontrol mekanizmaları oluşturulmalıdır. Fiziksel saldırıları, kalite kaybını ya da endüstriyel araçların ve verinin bozulmasını engellenmesi sağlanmış olur.
6) **İletisim ve Operasyonel Yönetim:** Bilgi işleme donanımlarının yeterli ve güvenilir olduğunun kontrolü devamlı yapılmalıdır.
7) **Erişim Kontrolü:** Bilgiye erişimin kontrolü sağlanmalı, çalışanların hangi bilgiye hangi yetkiyle erişebileceğinin kuralları açıkca belirtilmelidir.
8) **Sistemlerin Gelistirilmesi ve Sürekliliği:** Güvenliğin bilgi sistemlerinin içine dâhil edilmesini sağlar.
9) **Olay Yönetimi:** Güvenlik ihlallerinin ne sekilde ele alınacağına yönelik tavsiyeler verilmelidir.

10) **İş Sürekliliği Yönetimi:** Kurum içerisinde bilgi güvenliği ihtiyaçlarına yer veren iş sürekliliği için geliştirilmiş bir süreç oluşturulmalıdır. İş kesintilerini ve etkilerini azaltmak ve kurumun temel işlemlerini arıza ve büyük felaketlerden korunmasına yardımcı olur.
11) **Uygunluk:** Herhangi bir yasal ihlal ve güvenlik kosulları ile ilgili ihlallerden kaçınmasına yardımcı olur.



Şekil 5.2: BGYS Kontrolleri Şeması [28]

BGYS kurmak daha çok büyük kurumlara has gibi görünse bile ISO/IEC 27001 standardının KOBİ'ler için revize edilebilir sürümü de mevcuttur. KOBİ'ler karşılaştıkları bilgi güvenliği risklerini yönetmek için daha kısıtlı bir bütçeye ve daha az zamana sahip olduklarından ve bu riskleri güvence altına almak istediklerinden dolayı bu sürümde sadece ihtiyacını duyduğu hizmetleri içerecek hizmet paketleri hazırlatabilir, böylelikle ISO/IEC 27001 almanın gereksiz masraf ve karmaşasını ortadan kaldırabilirler [32].

6. SONUÇ

Günümüzde hızla gelişen bilgi ve iletişim teknolojileri getirdiği kolaylıklar sayesinde kişilere ve kurumlara büyük kolaylıklar sağlamaktadır. Aynı zamanda çeşitli veri güvenliği tehditlerini de yanında barındırmaktadır. Özellikle KOBİ'ler büyük işletmeler gibi veri güvenliğini sağlayacak ölçüde teknik altyapıya ve mali güce sahip olmadıklarından saldırganlar için daha kolay hedef haline gelebilmektedirler.

İster büyük kurumlar olsun isterse de KOBİ'ler olsun bilişim teknolojilerini kullandıklarından dolayı veri güvenliğine büyük önem vermeleri gerekmektedir. Küçük işletmelerin düştüğü en büyük hata ise kendilerinin internet ortamında saldırganların önemsemeyeceği kadar küçük olduklarını ve dikkat çekilecek derecede önemli veri/verilere sahip olmadıklarını düşünüp, gerekli güvenlik önlemlerini almamalarıdır. Bilişim sektörü dışında çalışan KOBİ'ler için özellikle işletmelerin güvenlik konusundaki fikirleri ve eksiklikleri yüzünden birçok güvenlik açığı meydana gelmektedir. Bu noktada aşağıdaki hususlara dikkat edilmesi gerekmektedir:

1) KOBİ yöneticileri üzerine büyük sorumluluk düşmektedir. Yöneticilerin teknik altyapı eksikliğini gidermek adına işletme çalışanlarının eğitimi ve işletme içerisinde veri güvenliğini sağlamak için gerekli araştırmaları yapmaları gerekmektedir.

2) Güvenlik sadece teknik bir terim değildir, işletme içinde bulunan her kademedeki çalışanın bu konuda bir sorumluluğu bulunmaktadır. Bunun için KOBİ'lerde veri güvenliğinin sağlanması amacıyla öncelikle yönetici ve çalışanların bilişim teknolojileri güvenliği bilincinin oluşturulması gerekmektedir.

3) Her işletme çalışanlarını siber güvenlik tehditlerine karşı eğitmelidir. Bunun için KOSGEB gibi yetkili kuruluşların bu konuda KOBİ'lere ve KOBİ çalışanlarına veri güvenliği eğitimleri konusunda destek vermesi gerekmektedir.

5) İşletme içerisinde bulunan her bir birey, üzerine düşen sorumluluğun farkına varmalı ve zafiyetlere yol açmayacak şekilde hareket etmelidir.

6) İşletmenin ihtiyacı olan güvenlik kontrolleri için işletme, kendi güvenlik uzmanını istihdam edemese bile bilgi güvenliği danışmanlarından faydalanmalı ve daima işbirliği içinde olmalıdır.

KOBİ'ler için veri güvenliğini sağlama noktasında izleyecekleri politika diğer herhangi büyüklükteki işletmeden çok da farklı değildir. Büyük işletmeler için oluşturulan genel güvenlik kaidelerinin yanı sıra kendi bilgi ve becerileri doğrultusunda web güvenliğini sağlamaya yönelik kullanılan araç setlerinden kendileri faydalanabileceği gibi danışman bir firma aracılığı ile de bu araç setlerinden faydalanabilirler. Şunun altını çizmek gerekir ki bu araç setlerinden özellikle bilişim sektöründe yer alan KOBİ'ler kolaylıkla faydalanabilirler. Ücretsiz olarak sunulan bu test araçlarının ticari sürümleri de bulunmakta olup, kurumlarının güvenlik açıklarını tespit etmek için istedikleri sürümü ücretsiz olarak veya satın alarak kullanabilirler. Bu araç setlerini özetleyecek olursak; web uygulamalarının güvenliğini, kurum içinde kullanılan ağ güvenliğini, kullanılan yazılım ve donanımların güvenliğini kontrol eden test araçlarıdır.

Bilgi ve iletişim teknolojileri her daim yenilenen ve gelişen bir yapıda olduklarından bilgi güvenliğini sadece bir defalığına sağlayıp daha sonra çıkan gelişmeleri takip etmemek, uygulamamak yeterli olmamaktadır. Siber tehditlerin gün geçtikçe yenilendikleri ve alınan her önleme karşı daha güçlü hala geldikleri unutulmamalıdır. KOBİ'lerin siber tehditler karşısında alabileceği önlemler ile yöneticiler ve çalışanların dikkat etmesi gereken durumlar şu şekilde özetlenebilir:

1) Her tespit edilen güvenlik tehdidinin karşılığında alınan önlemle beraber, var olan tehditler daha yıkıcı hale getirilmekte ve yeni tehditler de ortaya çıkmaktadır.

2) Örneğin; OWASP tarafından 2017 yılı içinde en çok rastlanan güvenlik açıkları belirtilmiştir. Bu güvenlik açıkları; enjeksiyon açıkları, bozuk kimlik, hassas

veri maruziyeti, xml dış öğeleri, bozuk erişim kontrolü, yanlış güvenlik yapılandırması, siteler arası komut dosyası, güvensiz serileştirme, bilinen güvenlik açıkları olan bileşenler yetersiz kayıt ve izleme şeklinde sıralanabilir.

3) Bu ve bunun gibi açık kaynak olarak internet üzerinden takip edilebilecek, veri güvenliğini sağlamak için önerilerde ve çözümlerde bulunabilecek topluluklara ait kaynaklardan faydalanmak ve güncel tehditlerin takibinde olmak gerekmektedir.

4) Kurumsal bilgi güvenliğine etki eden faktörler içinde en zayıf halka insan faktörüdür. Dolayısıyla insan faktörünün sebep olabileceği en tehlikeli güvenlik açığı olarak kabul edilen güvenlik bilinci zayıflığının belirlenmesinde sosyal mühendislik yöntemiyle yapılan güvenlik testleri önemli bir role sahiptir.

5) Her geçen gün teknolojik önlemlerin artması sebebiyle saldırganlar, insan zafiyetlerinden faydalanarak saldırılarını gerçekleştirmektedirler. Bu tür saldırıların kurumsal bilgi güvenliğini en az oranda tehdit etmesi amacıyla sosyal mühendislik teknikleri ve önemi her kademede yer alan personel ve yönetim tarafından bilinmesi gerekmektedir.

6) Ayrıca veri güvenliği sağlanmaya çalışırken, hangi zafiyetin hangi tehdit ve tehlikelerden nasıl korunması gerektiği, güvenliğin nasıl sağlanacağı ve güvenlik önlemleri için harcanacak giderlerin değerlendirilmesi yapılması gerekmektedir. Bu değerlendirmeler sonucunda güvenlik önlemlerini uygulamaya geçmek gerekmektedir.

İşletmeler, büyüklüklerine ve mali durumlarına göre tüm dünyada geçerli olan uluslararası güvenlik standartlarının gerekliliklerini yerine getirebilir, standartların ortak olarak vurguladıkları bilgi güvenliği yönetim sistemini kurumlarında uygulayabilirler. Kurumların BGYS kurmaları, uygulamaları ve belgelendirilmeleri gerekmektedir. KOBİ'ler için BGYS kurmanın gereklilikleri ve BGYS kurmanın mali yönleri şu şekilde açıklanabilir:

1) BGYS çerçevesinde oluşturulacak güvenlik politikalarına, yönetimde bulunan yetkililerin ve tüm personelin destek vermesi ve eksiksiz bir şekilde uygulaması, işbirliğinde bulunulan tüm kişi ve kuruluşlarında bu politikalara uyma zorunluluğu, kurumsal bilgi güvenliğinin sağlanmasında en önemli etmendir.

2) Mali yeterlilikleri iyi olan KOBİ'ler için bu standarttan faydalanmaları ve verilen eğitimlere katılımları önerilmektedir.

3) BGYS kurmak isteyen KOBİ'ler için BSI ISO/IEC 27001 standardının basitleştirilmiş hali de mevcuttur.

4) Ayrıca ISO/IEC 27001 standardının KOBİ'ler için revize edilebilir sürümü de mevcuttur. KOBİ'ler bu sürümde sadece ihtiyacını duyduğu hizmetleri içerecek hizmet paketleri hazırlatabilir, böylelikle ISO/IEC 27001 almanın gereksiz masraflarını ve karmaşıklığını ortadan kaldırabilirler.

Sonuç olarak bu tez çalışmasında KOBİ'lerin veri güvenliği konusundaki eksiklikleri tespit edilmiş, KOBİ'lerde veri güvenliğini sağlamak için alınması gerekli önlemler üzerinde durularak, web platformunda veri güvenliğini sağlamak için kullanılan araçların neler olduğu, bu araçların kullanılmasının veri güvenliği açısından nasıl bir fayda sağlayacağı incelenmiş, siber güvenlik tehditleri incelenerek, ne tür önlemler alınması gerektiği üzerine önerilerde bulunulmuş, uluslararası standartların yapısı incelenip KOBİ'lerin ne kadarından faydalanabileceği detaylı olarak anlatılmıştır.

KAYNAKLAR

[1] Acılar, A., 2009, KOBİ'lerde Bilişim Teknolojileri Güvenliği Sorunu: Tehditler ve Önlemler, Afyon Kocatepe Üniversitesi, İ.İ.B.F. Dergisi, 11(1): 1-16.

[2] Vural, Y., Sağıroğlu, Ş., 2010, Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler, Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 26(1): 89-103.

[3] Vural Y., Sağıroğlu Ş., 2008, Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme, Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, 23(2): 507-522.

[4] Canbek, G., Sağıroğlu, Ş., 2008, Casus Yazılımlar: Bulaşma Yöntemleri ve Önlemler, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(1): 165-180.

[5] Çetinkaya Kılıç, M., Gökçöl, O., (2010). Türkiye'deki İşletmelerin Bilgi Güvenliği Yönetim Sistemi Alt Yapısının Değerlendirilmesi. 3. Ağ ve Bilgi Güvenliği Sempozyumu 2010, Ankara.

[6] Bostan, A., Akman, İ., Bilişim Güvenliği: Kullanıcı Açısından Bir Durum Tespiti, 2011, Tmmob Emo Ankara Şubesi Haber Bülteni 2011/6.

[7] Eminağaoğlu, M. & Gökşen, Y., 2009, Bilgi Güvenliği Nedir, Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(4): 01-15.

[8] Acılar, A., Bastuğ, A., 2016, İşletmelerde Bir Bilgi Güvenliği Tehdidi Olarak Sosyal Mühendislik, Global Business Research Congress (GBRC), May 26-27, 2016, Istanbul.

[9] Barlette Y., Fomin V., 2008, "Exploring the suitability of IS Security Management Standards for SMEs," In: R. H. Sprague, Ed., Proceeding of 41st Hawaii International Conference on System Sciences (HICSS), Los Alamitos, 308-317.

[10] Allan C., Annear J., Beck E., Beveren J., 2003, "A Framework for the Adoption of ICT and Security Technologies by SMEs", 16th Annual Conference of Small Enterprise Association of Australia and New Zealand, Ballarat, Australia.

[11] J. Park, R. Robles, C. Hong, S. Yeo, and T. Kim, 2008, "IT Security Strategies

for SME's," International Journal of Software Engineering and Its Applications, 2(3): 91-98.

[12] "Türkiye'deki KOBİ Tanımı" erişim adresi: http://www.kobi.org.tr/index.php/tanimi/layout, erişim tarihi: 22 Mart 2018.

[13] "KOBİ Tanımı Değişti" erişim adresi: http://www.kobi.org.tr/index.php?option=com_content&view=article&id=239:kob-tanm-deiti&catid=3:kobi-haberler, erişim tarihi: 22 Mart 2018.

[14] "KOBİ Nedir? Kimler KOBİ Sayılır? KOBİ miyim?" erişim adresi: https://kanalfinans.com/egitim/kobi-bilgileri/kobi-nedir-kimler-kobi-sayilir-1, erişim tarihi: 22 Mart 2018.

[15] "Türkiye'de KOBİ Tanımı" erişim adresi: https://www.tobb.org.tr/KobiArastirma/Sayfalar/KOBITanimi.php, erişim tarihi: 22 Mart 2018.

[16] "AB'deki KOBİ Tanımı" erişim adresi: http://www.kobi.org.tr/index.php/tanimi/abde, erişim tarihi: 22 Mart 2018.

[17] "What is an SME?" erişim adresi: http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en, erişim tarihi: 22 Mart 2018.

[18] Nahari, H., Krutz, R. 2011, Web Commerce Security Design and Development, Indianapolis, Indiana, 245-266.

[19] "Bir Ağ Güvenlik Aracı Olarak SNORT" erişim adresi: http://cisn.odtu.edu.tr/snort.php, erişim tarihi: 30 Mart 2018.

[20] Vural, Y., 2007, Kurumsal Bilgi Güvenliği Ve Sızma (Penetrasyon) Testleri, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

[21] "About The Open Web Application Security Project" erisişim adresi: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project, erişim tarihi: 1 Nisan 2018.

[22] "OWASP Top 10 - 2017" erişim adresi: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf, erişim tarihi: 1 Nisan 2018.

[23] Jøsang, A. AlFayyadh, B. Grandison, T. AlZomai, M., McNamara, J. (2007) S Security Usability Principles for Vulnerability Analysis and Risk Assessment. In:

23rd Annual Computer Security Application Conference, Miami Beach, Florida, U.S.A., Aralık 2007.

[24] "ISO/IEC 27001:2013 Information security management systems requirements" erişim adresi: http://www.iso27001security.com/html/27001.html, erişim tarihi: 25 Mart 2018.

[25] "About the IEC" erişim adresi: http://www.iec.ch/about/, erişim tarihi: 25 Mart 2018.

[26] "The ISO story" erişim adresi: https://www.iso.org/the-iso-story.html#0, erişim tarihi: 25 Mart 2018.

[27] "ISO/IEC JTC 1/SC 27 IT Security techniques" erişim adresi: https://www.iso.org/committee/45306.html, erişim tarihi: 25 Mart 2018.

[28] Yılmaz, H., 2014, TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi, Denetişim, 45-59.

[29] "BS 7799-2 Nedir?" erişim adresi: http://www.belgelendirme.com.tr/belgelendirme-standartlari/iso-27001-standart/181-bs-7799-2-nedir, erişim tarihi: 25 Mart 2018.

[30] "What is an ISMS?" erişim adresi: https://www.iso.org/isoiec-27001-information-security.html, erişim tarihi: 25 Mart 2018.

[31] Marttin, V., Pehlivan, İ., 2010, ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme, Mühendislik Bilimleri ve Tasarım Dergisi, 1(1): 49-56.

[32] "KOBİ'ler için ISO 27001 Bilgi Güvenliği Yönetimi" erişim adresi: https://www.bsigroup.com/tr-TR/ISO-27001-Bilgi-Guvenligi-Yonetimi/KOBIler-icin-ISO-27001/ , erişim tarihi: 25 Mart 2018.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: ILGAZ, Berna
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 01.05.1992 - Eskil
Medeni hali	: Evli
Telefon	: -
Faks	: -
E-mail	: berna@entegreyazilim.com.tr

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Lisans	Mevlana Üniversitesi / Bilgisayar Mühendisliği	2014

İş Deneyimi

Yıl	Yer	Görev
2014 -	ON2 Elektronik	Bilgisayar Mühendisi

Yabancı Dil

İngilizce