T.C.
Radyo ve Televizyon Üst Kurulu

SİBER TEHDİTLER VE SALDIRILAR KARŞISINDA KURUMSAL BİLGİ GÜVENLİĞİNİN SAĞLANMASI

ÜST KURUL UZMANLIK TEZİ

Mustafa Kemal BAŞOĞLU

ANKARA

HAZİRAN / 2018

T.C.

Radyo ve Televizyon Üst Kurulu

SİBER TEHDİTLER VE SALDIRILAR KARŞISINDA KURUMSAL BİLGİ GÜVENLİĞİNİN SAĞLANMASI

ÜST KURUL UZMANLIK TEZİ

Mustafa Kemal BAŞOĞLU

DANIŞMAN

ÜST KURUL UZMANI Soner BASLI

ANKARA

HAZİRAN / 2018

RADYO VE TELEVİZYON ÜST KURULU BAŞKANLIĞINA,

Bu çalışma, Tez Değerlendirme Komisyonu tarafından oy birliği/oy çokluğu ile Uzmanlık Tezi olarak kabul edilmiştir.

	Adı Soyadı	İmza
Başkan	: Doç.Dr. Hamit ERSOY	
Üye	: İlker Ilgın	
Üye	: Hikmet İnce	
Üye	: Dr. Yaşar UĞURLU	
Üye	: Soner BAŞLI	

ONAY

..../..../2018

Prof. Dr. İlhan YERLİKAYA

Üst Kurul Başkanı

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI

Radyo ve Televizyon Üst Kurulunda görev yapan Uzman Yardımcısı olarak, Radyo ve Televizyon Üst Kurulu Uzman Yardımcılığı Giriş ve Yeterlik Sınavları ile Uzmanlığa Atanma, Yerleştirme, Görev, Yetki ve Çalışma Usul ve Esasları Hakkında Yönetmelik'in 19 uncu maddesinin 4 üncü fıkrasına istinaden çıkartılan Radyo ve Televizyon Üst Kurulu Tez Hazırlama Yönergesi'ne uygun olarak hazırlamış olduğum uzmanlık tezi ilişikte sunulmuştur.

Bu uzmanlık tezindeki bütün bilgileri akademik kurallara ve etik davranış ilkelerine uygun olarak toplayıp sunduğuma; ayrıca, bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi beyan ederim.

Bilgilerinizi ve gereğini arz ederim.

…./06/2018
Mustafa Kemal BAŞOĞLU
Üst Kurul Uzman Yardımcısı
Uzmanlık Tezinin Adı: Siber Tehditler ve Saldırılar Karşısında
Kurumsal Bilgi Güvenliğinin Sağlanması

EK:
TEZ (2 adet)
2- CD (1 Adet)

Tezi Teslim Alan
Daire Başkanı
…./06/ 2018

TEŞEKKÜR

"Siber Tehditler ve Saldırılar Karşısında Kurumsal Bilgi Güvenliğinin Sağlanması" isimli bu tezin hazırlanması sürecinde öncelikle Üst Kurul Başkanı Sayın Prof. Dr. İlhan YERLİKAYA ve Üst Kurul Üyelerine ve tez komisyon üyelerine teşekkürlerimi sunarım.

Bu tezin hazırlanmasında önerileriyle bana destek veren tez danışmanım Sayın Soner BASLI'ya, çalışmalarım esnasında yardımlarını esirgemeyen arkadaşlarım Sayın Ergün BİLEN'e, Sayın Recep Sinan ARSLAN'a, Sayın Şahin AY'a ve bu tez döneminde bana her konuda destek veren değerli eşim Sayın Esra BAŞOĞLU'ya çok teşekkür ederim.

İÇİNDEKİLER

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI i
TEŞEKKÜR ii
İÇİNDEKİLER iii
KISALTMALAR vii
TABLO VE ŞEKİLLER i
GİRİŞ …… 1
BİRİNCİ BÖLÜM 5
SİBER GÜVENLİKLE İLE İLGİLİ KAVRAMLAR 5
1.1 SİBER ORTAMLA İLGİLİ TEMEL KAVRAMLAR 5
1.1.1 Siber Uzay 5
1.1.2 Siber Risk 6
1.1.3 Siber Suç 7
1.1.4 Siber Tehditler 9
1.1.5 Siber Saldırılar 9
1.2 BİLGİ GÜVENLİĞİ İLE İLGİLİ TEMEL KAVRAMLAR 11
1.2.1 Bilgi Güvenliği 11
1.2.2 Siber Güvenlik 12
1.2.3 Kurumsal Siber Güvenlik 14
1.2.4 Kurumsal Bilgi Güvenliği 15
İKİNCİ BÖLÜM 16
SİBER TEHDİTLER VE SALDIRILAR 16
2.1 SİBER TEHDİT VE SALDIRILARIN SINIFLANDIRILMASI 17
2.1.1 Bilgi Sistemindeki Hasara Göre Siber Saldırı Çeşitleri 18
2.2.2 Bilgi Sistemine Saldırma Yöntemine Göre Siber Saldırı Çeşitleri 19
2.2.3 Bulunduğu Yere Göre Siber Tehdit ve Saldırı Çeşitleri 20
2.2. SALDIRI TÜRLERİ 22
2.2.1 Virüs 22

2.2.2 Solucan 24
2.2.3 Truva Atı 27
2.2.4. Arka Kapılar 29
2.2.5 Kök Kullanıcı Takımları (Rootkits) 31
2.2.6. Casus Yazılım (Spyware) 33
2.2.7 Klavye Dinleme Sistemleri (Keyloggers) 34
2.2.8 Koklayıcı (Sniffer) 35
2.2.9 Aldatma Saldırıları (Spoofing) 37
2.2.10. Hizmet Dışı Bırakma (Denial of Service) 38
2.2.11 Sosyal Mühendislik 41
2.2.12 Sazan Avlama (Phishing) 43
2.2.13 Oturum Çalma (Session Hijacking) 45
2.2.14 SQL Enjeksiyonu 46
2.2.15 Siteler Arası Betik Çalıştırma (XSS) 49
2.2.16. Fidye Yazılım (Ransomware) 51

ÜÇÜNCÜ BÖLÜM 53

KURUMSAL BİLGİ GÜVENLİĞİNİN SAĞLANMASI 53

3.1 GÜVENLİK PRENSİPLERİ 54
3.1.1 Gizlilik (Confidentiality) 55
3.1.2 Bütünlük (Integrity) 55
3.1.3 Kullanılabilirlik (Availability) 56
3.1.4 Kimlik Doğrulama (Authentication) 57
3.1.5 İnkar Edememe (Non-Repudiation) 58
3.1.6 İzlenebilirlik (Accountability) 58
3.1.7 Güvenilirlik (Reliability) 59

3.2 BİLGİ GÜVENLİĞİ İLE İLGİLİ MEVZUAT 59

3.2.1 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu 60
3.2.2 5809 Sayılı Elektronik Haberleşme Kanunu 61
3.2.3 Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği 63
3.2.4 Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik 65
3.2.5 6698 Sayılı Kişisel Verilerin Korunması Kanunu 66
3.2.6 Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar 68
3.2.7 703 Sayılı Kanun Hükmünde Kararname İle Gelen Değişiklikler ... 69
3.2.8 ISO 27001 Standardı ve Bilgi Güvenliği Yönetim Sistemi 70
3.2.8.1 ISO 27000 Ailesi ve Tarihsel Gelişimi 70
3.2.8.2 Bilgi Güvenliği Yönetim Sistemi Kurmanın Faydaları 72
3.2.8.3 Bilgi Güvenliği Yönetim Sistemi Kurulumu 73
3.2.8.4 Bilgi Güvenliği Yönetim Sistemi Kurulum Aşamaları 75
3.2.8.5 Bilgi Güvenliği Yönetim Sistemi Güvenlik Kontrolleri 75

3.3 SIZMA TESTLERİ 76
3.3.1 Tanımlar 77
3.3.2 Sızma Testinin Amaçları 78
3.3.3 Sızma Testlerinin Çeşitleri 78
3.3.4 Sızma Testinin Aşamaları 80
3.3.5 Sızma Testlerinde Kullanılan Araçlar 82
3.3.5.1 Bilgi Toplama ve Tarama Araçları 82
3.5.2 Zafiyet Tarama Araçları 83
3.3.5.3 Saldırı Araçları 84
3.4 KURUMSAL SİBER GÜVENLİK ORGANİZASYONLARI VE GÜVENLİK KONTROLLERİ 85
3.4.1 Kurumsal Siber Güvenlik Organizasyonları 85
3.4.1.1 Ulusal Siber Olaylara Müdahale Merkezi (USOM) 85
3.4.1.2 Siber Olaylara Müdahale Ekipleri (SOME) 86
3.4.1.2.1 Kurumsal SOME Kurulum Aşamaları 87
3.4.1.2.2 Kurumsal SOME'lerin Görev ve Sorumlulukları 88
3.4.1.3 Siber Güvenlik Kurulu 90
3.4.1.4 KamuNet (Kamu Sanal Ağı) 90
3.4.2 Güvenlik Kontrolleri 93
3.4.2.1 İnsan Kaynakları Güvenliği 93
3.4.2.2 Varlık Yönetimi 94
3.4.2.3 Erişim Kontrolü 94
3.4.2.4. Fiziksel ve Çevresel Güvenlik 95
3.4.2.5 Operasyon Güvenliği 96
3.4.2.6 İletişim Güvenliği 96
3.4.2.7 Sistem Edinim, Geliştirme ve Bakım 99
3.4.2.8 Tedarikçi İlişkileri 100
3.4.2.9 Bilgi Güvenliği Olay Yönetimi 101
3.4.2.10 İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönleri 102
3.4.2.11 Uyum 103
SONUÇ VE ÖNERİLER 104
KAYNAKÇA 111
ÖZET … 122
ABSTRACT 124
ÖZGEÇMİŞ 126

KISALTMALAR

a.g.e.	Adı geçen eser
a.g.m.	Adı geçen makale
ABD	Amerika Birleşik Devletleri
ARP	Address Resolution Protocol (Adres Çözümleme Protokolü)
ARPANET	Advanced Research Project Authrotiy Net
APT	Advance Persisent Threat (Gelişmiş Sürekli Tehdit)
ATP	Advanced Threat Protection
BGYS	Bilgi Güvenliği Yönetim Sistemi
BT	Bilgi Teknolojileri
CD	Compact Disc (Yoğun Disk)
DHCP	Dynamic Host Configuration Protocol (Dinamik Makine Yapılandırma Protokolü)
DMZ	Demilitarized Zone
DNS	Domain Name System (Alan Adı Sistemi)
DDoS	Distributed Denial of Service (Dağıtık Servis Dışı Bırakma)
DoS	Denial of Service (Servis Dışı Bırakma)
DVD	Digital Versatile Disc (Çok Amaçlı Sayısal Disk)
e-posta	Elektronik Posta
FTP	File Transfer Protocol (Dosya Aktarım Protokolü)
FW	Firewall
HTML	HyperText Markup Language (Hiper Metin İşaretleme Dili)
HTTP	Hyper Text Transfer Protocol (Hiper Metin Aktarım Protokolü)

HTTPS	HTTP Secure
IDS	Intrusion Detection System (Saldırı Tespit Sistemleri)
IEC	International Electrotechnical Commission (Uluslararası Elektroteknik Komisyonu)
IEEE	The Institute of Electrical and Electronics Engineers (Elektrik ve Elektronik Mühendisleri Enstitüsü)
IMPACT	International Multilateral Partnership Against Cyber Threats (Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık)
IP	Internet Protocol (İnternet Protokolü)
IPS	Intrusion Prevention System (Saldırı Önleme Sistemleri)
ISO	International Organization for Standardization (Uluslarası Standartlar Organizasyonu)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
NAC	Network Access Control (Ağ Erişim Kontrolü)
NetBIOS	Network Basic Input/Output System (Ağ Temel Giriş/Çıkış Sistemi)
PIN	Personel Identification Number (Kisisel Tanımlama Numarası)
RTÜK	Radyo ve Televizyon Üst Kurulu
s.	Sayfa
SIEM	Security Information and Event Management (Güvenlik Bilgi ve Olay Yönetimi)
SQL	Structured Query Language (Yapılandırılmış Sorgu Dili)
SOME	Siber Olaylara Müdahale Ekibi
TCP	Transmission Control Protocol (İletim Kontrol Protokolü)

TRT	Türkiye Radyo Televizyon Kurumu
UBAK	Ulaştırma ve Altyapı Bakanlığı
UDBH	Ulaştırma Denizcilik ve Haberleşme Bakanlığı
UEKAE	Ulusal Elektronik Ve Kriptoloji Araştırma Enstitüsü
USA	United States of America (Amerika Birleşik Devletleri)
USOM	Ulusal Siber Olaylara Müdahale Merkezi
UTM	Unified Threat Management (Birleşik Tehdit Yönetimi)
XSS	Cross-site Scripting (Siteler Arası Betik Çalıştırma)

TABLO VE ŞEKİLLER

Şekil 1 : Siber Suçların Küresel Dağılımında Türkiye Sıralaması 8

Şekil 2: Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi 10

Şekil 3: Kötücül Yazılım Bulaşma Oranı (2016 İlk Çeyrek) 13

Şekil 4: DDoS Saldırılarının Kaynaklandığı Ülkeler (2016 İlk Çeyrek) 14

Şekil 5: Truva Atının Sisteme Bulaşması 28

Şekil 6: Şekil DDoS Saldırılarında Botların ve Botnetin Kullanılması 39

Şekil 7: ISO 27001 Planla, uygula, kontrol et ve önlem al aşamaları döngüsü 74

Şekil 8: Firewalk Aracının Kullanılması 83

Şekil 9: Nessus Aracının Zafiyetleri Sınıflandırması 84

Şekil 10: Usom, Sektörel Some Ve Kurumsal Some İlişkisi 86

Şekil 11: Kurumsal SOME'nin Kurum İçindeki Paydaşları ve Temel Fonksiyonları 88

Şekil 12: Siber Olay Müdahale Akış Diyagramı 89

Şekil 13: Güvenlik Duvarı 97

GİRİŞ

Günümüzde bilişim teknolojilerinin yoğun bir şekilde kullanımı ve özellikle kurumlardaki iş süreçlerinin büyük ölçüde bu sistemlere bağlı olması, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir.

Bilginin kurumlar için en değerli varlıklardan biri olarak sayılması sonucunda bu bilgilerin gizliliğinin korunması yani sadece yetkili kişilerce erişilebilmesi gerekmekte, erişilen bilgilerde herhangi bir bozulma olmaması ve istenildiği anda bu bilgilere ulaşılması gerekmektedir.

Bilgi güvenliğinin sağlanamadığı durumlarda kurumların iş sürekliliği kesintiye uğramaktadır. Buna ilaveten bilginin mahremiyeti zedelenmektedir ve kurumların imajı zarar görmektedir. Ayrıca kurumların hizmet verdiği kişilerde bu durumdan olumsuz etkilenmektedir.

Bilişim teknolojilerindeki gelişme ve iletişim teknolojilerindeki artan kapasiteyle beraber Internet'e ve birbirine bağlı cihazların ve sistemlerin oluşturduğu siber ortam git gide büyümektedir. Bunun neticesinde siber dünyada bulunan ve bilişim sistemlerini tehdit eden siber risklerin etki alanı da artmaktadır.

Tezin Konusu

Siber tehditlerin ve saldırıların yıllar içinde daha karmaşık hale gelmesiyle birlikte bilgi güvenliğinin sağlanması da güçleşmiştir. Bilgi güvenliğini sağlayan teknolojilerdeki gelişmeye ilaveten bu alanı düzenleyen yasal düzenlemeler, standartlar ve yönetim süreçleride karmaşık bir hal almıştır.

Bu kapsamda üç bölümden oluşan "Siber Tehditler Ve Saldırılar Karşısında Kurumsal Bilgi Güvenliğinin Sağlanması" adlı tez çalışmamızın birinci bölümünde

siber ortam ve bilgi güvenliği ile ilgili temel kavramlar anlatılmaktadır. Bu kavramlar anlatılırken dünya ölçeğinde büyük etki yaratmış siber olaylardan örnekler ve istatistiksel bilgiler verilerek konunun boyutları göz önüne serilmiştir.

İkinci bölümde ise siber tehditler ve saldırıların sınıflandırılmasında kullanılan yaklaşım biçimleri incelenmiş ve tez için uygun görülen bir yaklaşıma göre bu tehdit ve saldırılar anlatılmıştır. Siber tehdit ve saldırıların sisteme nasıl bulaştıkları ve nasıl zararlar verdiklerinden sözedilmiştir. Bilişim sistemlerini bu tip tehdit ve saldırılardan korumak için alınacak önlemlerden bahsedilmiştir.

Tezin üçüncü bölümünde kurumsal bilgi güvenliğini sağlamak amacıyla öncelikle güvenlik prensipleri ortaya konmuş ve bu kavramlara açıklık getirilmiştir. Ardından bilgi güvenliği ile ilgili ulusal ve uluslararası yasal düzenlemelerden bahsedilmiştir. Kurumsal bilgi güvenliğini sağlamada uluslarası kabul görmüş ISO 27001 standardının kurumlarda oluşturulmasını elzem gördüğü Bilgi Güvenliği Yönetim Sisteminden (BGYS) bahsedilmiştir. Son olarak BGYS'nin ne seviyede bir güvenlik sağladığını anlamanın en kestirme yolu olan sızma testleri ve ISO 27001'in gerektirdiği güvenlik kontrolleri anlatılmıştır.

Sonuç ve değerlendirme bölümünde ise siber tehdit ve saldırıların bügün geldiği karmaşık düzey ele alınmıştır. Bu tehdit ve saldırılar karşısında kurumsal bilgi güvenliğini sağlamak için kurum içinde alınması gereken teknik ve idari tedbirler ve buna ilaveten kurumlararası organizasyonlar değerlendirilmiştir.

Tezin Amacı

Bu tezin amacı kurumsal bilgi güvenliğini zaafa uğratacak tehditleri ve saldırıları incelemek, bilgi güvenliğini sağlamak için oluşturulmuş mevcut yasal düzenlemeler ve standartlar hakkında bilgi vermek, alınması gereken önlemleri araştırıp sunmaktır.

Tezin Önemi

Siber tehditlerin çoğalmasıyla kurumlar para, itibar kaybı veya iş sürekliliğinin sağlanamaması gibi risklerle karşı karşıya kalmaktadır. Aynı zamanda bu tehditlerin değişmesi ve yenilenmesi bu alanda yapılan çalışmaların güncel olmasını gerektirmektedir. Bu çalışma, bilgi güvenliğinin sağlanmasında en önemli unsurlardan olan farkındalığın arttırılmasına katkıda bulunacaktır. Bilgi güvenliğini tehdit eden olası riskleri ve alınması gereken önlemleri sunmasıyla kurumumuz bilgi varlıklarının korunması, iş sürekliliğinin sağlanması, olası para ve itibar kaybı gibi risklerden korunması kapsamında katkılar sunacağı düşünülmektedir.

Tezin Yöntemi

Bu tez çalışmasında yöntem olarak "Kaynak Tarama Yöntemi" kullanılmıştır. Gerekli bilgi ve belgeler basılı kaynaklar, bilimsel veritabanları (IEEE Explore, ACM Digital Library, Wiley Online Library, Science Direct),yayımlanmış tezler ve kurumsal web siteleri taranarak toplanmıştır. İlgili veriler tezin amacı doğrultusunda bilimsel etik ve kurallara uygun biçimde aktarılmıştır.

Tezin Kapsamı ve Sınırlılıkları

Bu çalışmada, bilgi güvenliği kavramı kurumsal bilgi güvenliğinin sağlanması bağlamında incelenecektir. Bu bağlamda öncelikle bilgi güvenliğini zaafa uğratan siber tehdit ve saldırı türleri incelenmiştir. Bu türlerin sayıca çok olması ve benzer zafiyetleri sömürmeleri sebebiyle bir kısmı bu tezde konu edilmemiştir. Bilgi güvenliği ve siber güvenlik ile ilgili mevzuat (kanunlar, yönetmelikler, bakanlar kurulu kararları, uluslararası sözleşmeler ve standartlar) tez kapsamında incelenmiştir. Dünya genelinde yaygın olarak kullanılan ve tipine, büyüklüğüne ve doğasına bakılmaksızın bütün kurum ve kuruluşlarda uygulanabilecek olan IS0 27001 standartı ayrıntılı bir biçimde incelenmiş, diğer standartlar kapsam dışı bırakılmıştır. Bahsi

geçen standart teknoloji bağımsız ve güvenlik prensipleri üzerine kurulu olduğundan bilgi güvenliği teknolojileri bu tezde yer almayacaktır.

BİRİNCİ BÖLÜM

SİBER GÜVENLİKLE İLE İLGİLİ KAVRAMLAR

1.1 Siber Ortamla İlgili Temel Kavramlar

Bu bölümde bu tezde sıkça kullanılan siber uzay, siber risk, siber tehdit ve saldırı kavramlarının tanımları yapılacaktır. Buna ilavaten istatistiki veriler ve örneklerle bu kavramlara açıklık getirilecektir.

1.1.1 Siber Uzay

Siber uzay kavramı T.C. Ulaştırma ve Altyapı Bakanlığı'nın yayınladığı 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre şöyle tanımlanmıştır: "Siber uzay: Tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden[1] ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı ifade eder." [2]

Siber uzay, bilgisayar ağları üzerinden iletişimi sağlayan konjonktürel çevre ya da İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler ve denetleyicileri içeren bilgi sistemleri altyapılarının birbirine bağlı ağından oluşan bilgi ortamı içindeki küresel bir alan olarak da tanımlanabilir. [3]

[1] Bilişim sistemleri, verileri toplayıp yerleştirdikten sonra bu verileri otomatik işlemlere tabi tutma olanağı veren sistemlerdir.
[2] T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *2016-2019 Ulusal Siber Güvenlik Stratejisi*, UDHB, Ankara, 2016, s.7
[3] İbrahim Şişaneci, Osman Akın, Muharrem Karaman, ve Mehmet Sağlam, "A Novel Concept for Cybersecurity: Institutional Cybersecurity", *6th International Information Security & Cryptology Conference*, ISC Turkey, Ankara, 2013, s. 186

Hekim ve Başıbüyük ise siber uzayı "birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alan" olarak tanımlamaktadır. [4]

Günümüzde siber uzayın ve siber uzaya duyulan güvenin korunması hususuna verilen önem artmıştır. Öyle ki, 19 farklı ulusal siber güvenlik strateji belgesi üzerine yapılan bir inceleme, siber uzayı ticari amaçla kullanma konusunda vatandaşların sahip olduğu güvenin korunmasının, bu gözden geçirme kapsamındaki tüm uluslar tarafından hayati derecede görüldüğünü ortaya koymuştur. [5]

1.1.2 Siber Risk

Siber risk Ulusal Siber Olaylara Müdahale Merkezi tarafından "Siber saldırı neticesinde meydana gelebilecek olası zararlı sonuçlar",[6] 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre ise "tehditlerin bir veya birden çok bilgi varlığındaki açıklığı kullanarak zarar yaratma potansiyeli" [7] olarak tanımlanmaktadır.

Temel olarak tüm BT varlıklarında var olan siber risk, bireylerden kritik BT varlıklarına sahip uluslararası kuruluşlara kadar çeşitlilik gösteren bir risk türüdür. Siber risk, belirli bir risk yerine teknolojide, saldırı vektörlerine, araçlara vb. göre değişen bir grup risk olarak tanımlanır.[8]

Siber risklere örnek olarak enerji, ulaştırma, vb. kritik hizmetlerin kesintiye uğraması; vatandaşa ait kişisel bilgilerin veya kamuya ait gizli bilgilerin saldırganların

[4] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, Cilt:4 Sayı:2, 2013, s.136
[5] Rossouw von Solms, ve Johan van Niekerk, "From information security to cyber security", *Computer & Security*, Sayı: 38, 2013, s. 101.
[6] Ulusal Siber Olaylara Müdahale Merkezi, *Siber Güvenliğe İlişkin Temel Bilgiler*, USOM, Ankara, 2014, s.7.
[7] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 7.
[8] İ. Şişaneci, O. Akın, M. Karaman, M. Sağlam, 2013, s. 186.

eline geçmesi, ifşa olması, değiştirilmesi veya yok edilmesi; çeşitli kurum ve kuruluşların itibarının zarar görmesi verilebilir.[9]

1.1.3 Siber Suç

Siber suçlar, bilgileri otomatik olarak işleyen veya veri aktarımı sağlayan bir sistemde yasa dışı, etik olmayan veya yetkisiz hareketlerdir.[10] Bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçlar olarak da tarif edilebilir.[11]

Siber suçun en yaygın türü "kimlik sahtekarlığı" ya da finansal ve ödeme sistemlerinin dolandırılması için hesap detaylarının kötüye kullanılmasıdır. Bu hesaplara ulaşmak için ya hesapların kullanıldığı bilgisayarlara saldırılır ya da sosyal mühendislik yöntemleri ile kişiler kandırılmaya çalışılır.[12] Siber suçlara verilebilecek bazı örnekler aşağıda maddeler halinde sıralanmaktadır.

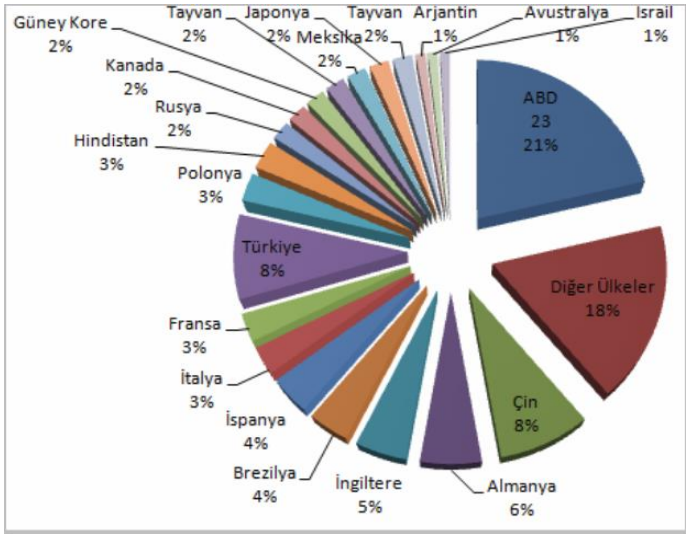
- **Yasadışı ve Zararlı İçerik**: İnternet üzerinde yanıltıcı, yasa dışı ve ahlak dışı, özellikle çocukların istismarına yönelik içeriklerdir.

- **Yazılım korsanlığı ve diğer ürünlerin korsanlığı**: Yazılım ürünlerin kurulumlarını kırmak veya kaynak kodlarını ele geçirmek veya tersine mühendislik gibi yöntemlerle üretmektir. CD, VCD, Ses CD'si ve DVD gibi çoklu ortam ürünlerinin kopyalanmasıdır.

[9] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s. 12-13.
[10] Asaf Varol ve Yeşim Ülgen Sönmez, *The Analysis of the Concepts of Informatics, Cyber Crimes and Computer Forensics*, 10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı, Ankara, 2017, s. 40.
[11] Hakan Hekim ve Oğuzhan Başıbüyük, 2013, s.136.
[12] P.W. Singer, Allan Friedman, *Cybersecurıty And Cyberwar: What Everyone Needs to Know*, Oxford University Press, New York, 2014, s.85

- **Elektronik savaş:** Rakip şirket, düşman ülke gibi hasımlara yönelik yürütülen saldırılardır.[13]

Siber suçların 2021'e kadar dünya genelinde 6 trilyon dolarlık bir zarara yol açacağı öngörülmektedir. Siber suçların küresel dağılımı incelendiğinde, Şekil 1'de görüldüğü gibi ülkemiz % 8 oranıyla 9. Sırada yer almaktadır.



Şekil 1 : Siber Suçların Küresel Dağılımında Türkiye Sıralaması[14]

Uluslararası alanda, siber suçlar hakkında en kapsamlı düzenleme "Avrupa Siber Suç Sözleşmesi" dir. Dört kısım ve kırk sekiz maddeden oluşan bu sözleşme, 23 Kasım 2001'de Budapeşte'de düzenlenen Uluslararası Siber Cemiyetler Konferansı'nda imza için sunulmuştur ve Avrupa Konseyi üyesi 26 devlet, Amerika Birleşik Devletleri, Japonya, Kanada ve Güney Afrika tarafından imzalanmıştır. Türkiye tarafından Strazburg'da 10 Kasım 2010 tarihinde imzalanan Sözleşme, 6533 sayılı Kanun'un (Sanal Ortamda işlenen Suçlarla Mücadele Sözleşmesi'nin Onaylanması Hakkında) 02/05/2014 tarihli resmi gazetede yayımlanmasıyla uygulamaya konulmuştur.[15]

[13] Mesut Gülnaz, *Kamusal Web Güvenliği,* Marmara Üniversitesi, Yüksek Lisans Tezi, İstanbul, 2010, s.48.
[14] Gülcihan Aydaner, Ufuk Çelik ve Senem Nart, "Siber Güvenlikte Kamu ve Özel Sektör İşbirliği", *10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı*, Ankara, 2017, s. 59.
[15] Asaf Varol ve Yeşim Ülgen Sönmez,2017, s.40.

1.1.4 Siber Tehditler

Siber tehdit, Ulusal Siber Olaylara Müdahale Merkezi tarafından "zararlı sonuçlar doğurabilecek olası saldırı ya da açıklık durumları" olarak tanımlanmıştır.[16]

Siber tehdit, bilginin bozulmasını kapsayan, bilgiyi yetkisiz kişilerce değiştiren, bilgiyi ifşa eden veya çalan veya erişilebilirliğini ortadan kaldıran bir potansiyel durum olarak tanımlanabilir. Siber tehdit kaynağı, enfekte olmuş tek bir bilgisayar olabilir veya milyonlarca bilgisayarı içerebilecek bir bot-net[17] olabilir.[18]

Tehditler, özellikle bilgi güvenliği dünyasında belirli ortamlara özgü olma eğilimindedir. Örneğin, bir virüs bir Windows işletim sistemi için bir tehdit oluşturabilse de, aynı virüsün Linux işletim sistemi üzerinde herhangi bir etkisi olmayacaktır.[19]

1.1.5 Siber Saldırılar

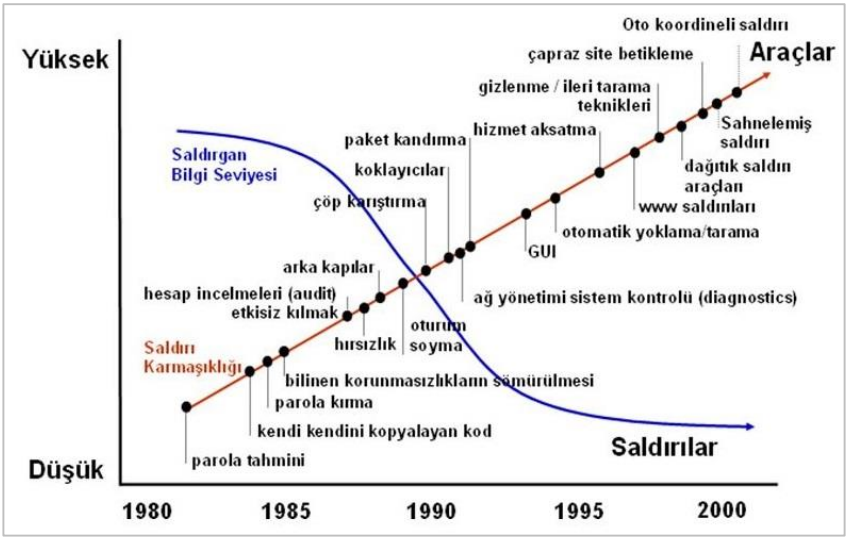
Siber saldırı ise 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre şu şekilde tanımlanır: " Ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemlerdir." [20]

Kısacası, siber saldırılar kukla bilgisayar virüsünden (Morris Worm) Gelişmiş Sürekli Tehdit'e (Advance Persisent Threat) (APT) kadar değişebilir. Siber saldırılar

[16] Ulusal Siber Olaylara Müdahale Merkezi, 2014, s.7
[17] Bot-net başka saldırılarda kullanılmak üzere saldırganlar tarafından ele geçirilmiş bilgisayarlardan oluşturulmuş gruba verilen addır.
[18] İ. Şişaneci, O. Akın, M. Karaman, M. Sağlam, 2013, s.187
[19] Jason Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice Second Edition*, Elsevier, Waltham, USA, 2014, s.11
[20] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s.8

ilk ortaya çıktıkları günden günümüze kadar sürekli ve katlanarak gelişme eğilimindedirler. Bu siber saldırılar, Siber Suç, Hacktivisim, Siber Terörizm, Siber Casusluk ve Siber Savaş gibi sınıflandırılabilir.[21]

Siber saldırıların evrimi incelendiğinde ilginç bir durum ortaya çıkmaktadır. Yıllar geçtikçe saldırı karmaşıklığı arttığı halde saldırganın bilgi seviyesi düşmektedir. Bu durum Şekil 2'de açıkça görülmektedir. Bunun sebebi saldırıların hazır bazı araçlarla kolayca yapılabilmesidir.



Şekil 2: Saldırı Karmaşıklığı ile Saldırgan Teknik Bilgisi [22]

Siber saldırıların ne kadar etkili olabileceğini ortaya koyan bazı olaylar aşağıda sıralanmıştır:

- 2008'de Rusya - Gürcistan savaşında Gürcistan'a yapılan siber saldırılar sonucu finans, haberleşme ve elektrik sistemlerinde ciddi sıkıntılar yaşanması,
- 2010'da İran nükleer zenginleştirme programını hedefleyen ve ciddi sorunlara sebep olan 'Stuxnet' yazılımı saldırısı,

[21] İ. Şişaneci, O. Akın, M. Karaman, M. Sağlam, 2013, s.187
[22] Gürol Canbek ve Şeref Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi,* Cilt:9, Sayı: 3, (2006): s.169

- 2011'de İran Silahlı Kuvvetlerinin ABD'ye ait insansız hava aracının kontrolünü ele geçirerek yere indirmesi,
- 2014'te Sony Şirketinin yoğun siber saldırılar sonucu Kuzey Kore Lideriyle ilgili 44 milyon dolara mal olan filmi gösterimden kaldırması,
- 2016'da ABD'nin doğu yakasına hizmet sunan sistem altyapılarına yönelik olarak başlayan siber saldırıların ülke geneline yayılarak internet bağlantısını engellemesi ve ciddi ekonomik zarara sebep olması.[23]

1.2 Bilgi Güvenliği İle İlgili Temel Kavramlar

Bu bölümde bilgi güvenliği, siber güvenlik, kurumsal bilgi güvenliği ve kurumsal siber güvenlik kavramları açıklanacaktır. Bu kavramların birbirinden farkları ve yakınsadığı noktalar ele alınacaktır.

1.2.1 Bilgi Güvenliği

Bilgi güvenliği ABD yasalarına göre, "bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, ifşa, bozulma, değişiklik veya imhadan korunması" olarak tanımlanmaktadır.[24]

Uluslararası Standart ISO / IEC 27002: 2005'e göre bilgi güvenliğinin sağlanması için bilginin gizlilik, bütünlük ve kullanılabilirlik gibi unsurlarının korunması gerekir. Ayrıca, özgünlük, hesap verebilirlik, reddedilme ve güvenilirlik

[23] Mustafa Şenol, "Türkiye'de Siber Saldırılara Karşı Caydırıcılık", *10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı,* Ankara, 2017, s.69.
[24] Jason Andress, 2014, s.3.

gibi diğer özellikler de bu kapsamda korunması gereken unsurlar olarak zikredilmiştir.[25]

Bilgi güvenliği; gizliliği tehlikeye atan yetkisiz erişim, bütünlüğü tehlikeye atan kötücül yazılımlar veya kullanılabilirliği tehlikeye atan servis dışı bırakma saldırıları gibi tehditleri tespit etmek, belgelemek ve karşı koymak için gerekli önlemleri içerir.[26]

1.2.2 Siber Güvenlik

Siber güvenlik kavramı ile yukarıda bahsedilen bilgi güvenliği kavramı zaman zaman birbiri ile karıştırılmaktadır. Oysaki tanımlardan anlaşılacağı gibi bilgi güvenliğinin sınırları bilginin korunmasıyla sınırlıdır.

Siber güvenlik, İnternet hizmetlerini ve kaynaklarını güvenli bir şekilde kullanma sürecidir. Sadece verileri korumakla kalmaz, aynı zamanda kişisel güvenliği de içerir. Siber güvenliğin amacı, bilgisayarları, kişisel bilgileri ve bireyleri, kurumları, ülkenin kritik altyapılarını siber saldırılardan ve diğer olası tehditlerden korumaktır.[27]

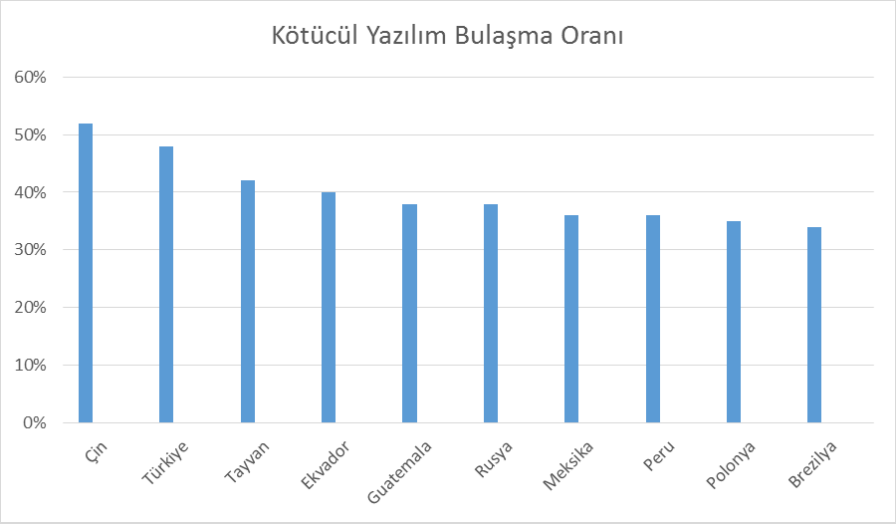
Siber güvenlikle ilgili yapılan tanımlar aşağıda maddeler halinde sıralanmaktadır. [28]

- Siber güvenlik, elektronik verilerin suç niteliğinde veya yetkisiz kullanımından korunmuş olma hali veya bunu elde etmek için için alınan önlemlerdir.

[25] İ. Şişaneci, O. Akın, M. Karaman, M. Sağlam, 2013, s.187.
[26] Karl de Leeuw, ve Jan Bergstra, *History of Information Security: A Comprehensive Handbook*, Elsevier, Amsterdam, 2007, s.2.
[27] John Sammons, ve Michael Cross, *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*, Syngress, Cambridge, USA, 2017, s.1.
[28] İ. Şişaneci, O. Akın, M. Karaman, M. Sağlam, 2013, s.187

- Siber güvenlik, siber riski gidermek için yatırım yapılan çabaların toplamıdır.
- Uluslararası Telekomünikasyon Birliği'nin görüşü: Siber çevreyi ve organizasyonu ve kullanıcının varlıklarını korumak için kullanılabilecek araçların, politikaların, güvenlik kavramlarının, güvenlik önlemlerinin, yönergelerin, risk yönetimi yaklaşımlarının, eylemlerin, eğitimlerin, en iyi uygulamaların, güvence ve teknolojilerin bir araya getirilmesidir. Organizasyon ve kullanıcının varlıkları arasında, bağlı bilgisayar cihazları, personel, altyapı, uygulamalar, hizmetler, telekomünikasyon sistemleri ve siber ortamda iletilen ve / veya depolanan bilgilerin toplamı bulunur.

Yapılan araştırmalar sonucunda ortaya çıkan veriler ülkemizin ciddi bir siber güvenlik sorunuyla karşı karşıya olduğunu göstermiştir. Aşağıda Şekil 3'de gösterilen çizelgede, 2016 yılı ilk çeyreğe ait verilere göre kötücül yazılım bulaşma oranı en yüksek 10 ülke arasında ülkemizin ikinci sırada olduğu gözükmektedir.

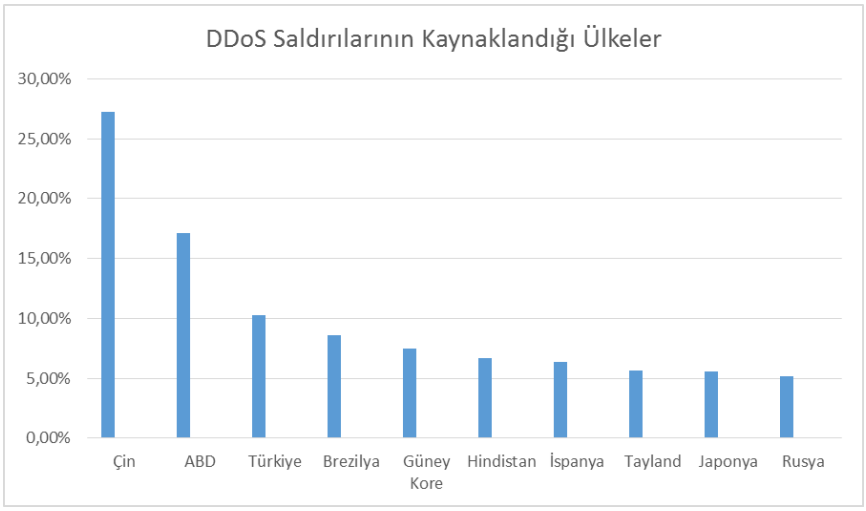


Şekil 3: Kötücül Yazılım Bulaşma Oranı (2016 İlk Çeyrek) [29]

Şekil 4'de ise Dağıtık Servis Dışı Bırakma (DDoS) saldırılarının en çok kaynaklandığı 10 ülke sıralanmaktadır. Bu saldırı tipinde saldırganlar tarafından ele

[29] Havelsan,"Türkiye Siber Güvenliğine Son İstatistikler ile Bakış", *CyberMag*, Sayı: 15, 2017, s. 18-21.

geçirilmiş bilgisayarların kullanıldığı hesaba katılırsa yukardaki şekilde gösterildiği gibi kötücül yazılımlardan ülkece ne kadar etkilendiğimiz ortaya konulmaktadır.



Şekil 4: DDoS Saldırılarının Kaynaklandığı Ülkeler (2016 İlk Çeyrek) [30]

1.2.3 Kurumsal Siber Güvenlik

Kurumsal Siber Güvenlik, bilgi güvenliği bileşenlerini, diğer siber güvenlik ortakları ile işbirliğini ve siber risk perspektifinden siber güvenlik farkındalığını içeren bir yetenektir.[31]

Bu bağlamda, Türkiye uluslararası işbirliği için ITU-IMPACT üyesi olarak siber güvenlik hizmetlerine erişim hakkına sahiptir. Türkiye ayrıca ITU-T ile standart çalışmalarında aktif rol oynamaktadır ve resmi olarak ulusal bir siber olaylara müdahale merkezine sahiptir.(USOM) [32]

[30] a.g.e, 2017, s.19
[31] İ. Şişaneci, O. Akın, M. Karaman, M. Sağlam, 2013, s.187.
[32] CyberMag, "Türkiye'nin Siber Profili", *CyberMag Dergisi*, Sayı: 6, 2016, s. 41-42.

Kurumlar kendi bünyelerinde Siber Olaylara Müdahale Ekipleri (SOME) kurar ve bu ekipler USOM'dan gelen uyarı ve talimatlar ile kurumsal siber güvenliği sağlamaya çalışır.

1.2.4 Kurumsal Bilgi Güvenliği

Kurumsal bilgi güvenliği, kurumların bilgi varlıklarını tespit edip ilgili varlıkların güvenlik açıklıklarının tespit edilmesi ve bu varlıklara yönelik istenmeyen tehdit ve tehlikelerin önlenmesini amaçlamaktadır. Kurumsal bilgi güvenliğinin sadece gerekli donanım ve yazılım ürünleri gibi teknik önlemlerle sağlanması mümkün değildir. Bu ürünlere ilaveten insan, eğitim ve organizasyon gibi birçok etken yer almaktadır. Sonuç olarak bilgi güvenliği sadece bir bilgi teknolojileri (BT) işi değil, kurumun tüm çalışanlarının katkısı ve katılımını gerektiren bir süreçtir.[33]

Kurumsal bilgi güvenliğinin sağlanması konusu bu tezin üçüncü bölümünü oluşturmaktadır. Bu kapsamda kurumların uyması gereken yasal düzenlemeler ve standartlar bu bölümde anlatılmıştır.

[33] Cemile Denerel, "Güvende Olmak İçin Uyumlu Ol", *CyberMag Dergisi*, Sayı: 6, 2016, s.19.

İKİNCİ BÖLÜM

SİBER TEHDİTLER VE SALDIRILAR

Bilgi güvenliğine yönelik tehdit ve saldırılar güçlerini, yeteneklerini ve özelliklerini sistemlerdeki zafiyetlerden (açıklıklardan) alırlar. Bu güvenlik açıklığı bazen açık bırakılmış bir port[34], bazen şifrelemedeki bir zayıflık, bazende güçsüz bir kimlik doğrulama olabilir. Bilgi güvenliğini arttırmak için sistemlerdeki zafiyetler mümkün olduğu ölçüde giderilmelidir. Bu şekilde saldırıya maruz kalma riski azaltılabilir çünkü zafiyet olduğu sürece saldırılara maruz kalma ihtimali vardır.[35]

Bilgi güvenliği için tehdit oluşturan bu saldırılar, temel olarak; keşif, tarama, erişimi sağlama, erişimi devam ettirme ve izleri temizleme olmak üzere beş aşamada incelenmektedir. Aşağıda bu aşamalar maddeler halinde tanıtılmaktadır. [36]

- **Keşif:** Bu aşamada saldırıya hazırlık yapılır. Saldırı yapılacak hedef hakkında toplanabildiği kadar çok bilgi toplanmaktadır. Kurum çalışanlarının e-posta adreslerinin ele geçirilmesi bu aşamaya bir örnektir.

- **Tarama:** Bu aşama, saldırı öncesi son hazırlıkların yapıldığı aşamadır. Keşif aşamasında elde edilen bilgiler ile çeşitli tarama işlemleri gerçekleştirilmektedir. Ağ topolojisinin çıkartılması, port tarama (port scanning), saldırıya açıklığı tarama (vulnerability scanning), sunucu üzerinde

[34] Port, bilgisayarlar üzerinde birtakım soyut bağlantı noktalarına verilen addır. Bu sayede aynı anda, aynı IP Adresinden farklı programlarla veri alışverişi yapılabilmektedir.
[35] Mesut Gülnaz, *Kamusal Web Güvenliği*, Marmara Üniversitesi, Yüksek Lisans Tezi, İstanbul, 2010, s.48.
[36] Özgü Can, M. Fatih Akbaş, "Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması", Tübav Bilim Dergisi, Cilt 7, Sayı:2 2014, s.21.

çalışan işletim sistemi hakkında bilgi edinmek gibi davranışlar bu aşamada yapılabilecek işlemlerdir.

- **Erişimi sağlama:** Bu aşama saldırının gerçekleştiği aşamadır. Saldırgan, tarama evresinde tespit ettiği açığı kullanarak sisteme sızmaktadır. Phyton, Perl gibi programlama dilleri ile yazılabilen ve sömürücü (exploit) adı verilen bu zararlı kod parçacıkları, sistemde veya programda bulunan açıklıkları kullanarak hedef sistemin komut satırını almayı, yetkisiz kullanıcılara yönetici yetkilerini kazandırmayı amaçlamaktadır.

- **Erişimi devam ettirme**: Bu aşamada, saldırgan tarafından ele geçirilmiş olan sistemin açıklığının kullanılmasına devam edilmesi amaçlanmaktadır. Böylelikle, ele geçirilmiş olan sistem aracılığıyla saldırgan ağ üzerindeki diğer sistemlere de erişebilmektedir. Saldırgan, bu amaçla truva atları (trojan horse), kök kullanıcı takımları (rootkit), arka kapılar (backdoor) gibi zararlı yazılımları kullanarak istediği zaman sisteme sızma eylemini gerçekleştirebilmektedir.

- **İzleri temizleme:** Bu aşama, yapılan saldırıya ait izlerin başkaları tarafından tespit edilmeden ortadan kaldırılması sürecidir. Saldırganın amacı yasal olarak işlemiş olduğu suça ait delilleri ortada bırakmamaktır.

2.1. SİBER TEHDİTLER VE SALDIRILARIN SINIFLANDIRILMASI

Siber tehdit ve saldırıların sınıflandırılması tamamen bunlara hangi açıdan yaklaşıldığına göre değişiklik gösterebilir. Örneğin kaynağına göre, saldırı hedefine göre, kazanım amacına göre, elde edilen sonuca göre, bilgi sistemindeki hasara göre siber tehdit ve saldırılar sınıflandırılabilir. Bu sınıflandırma türlerinin kimisinde bireysel, psikolojik motivasyonlar kimisinde ise daha sosyal ve politik faktörler bulunabilir.

Bu tezde ise siber tehdit ve saldırıları sınıflandırırken daha çok teknik bir yol izlenecek, tehdit ve saldırı teknikleri üzerine yoğunlaşılacak, birbirine benzeyenler gruplanıp sırayla anlatılacaktır.

2.1.1 Bilgi Sistemindeki Hasara Göre Siber Saldırı Çeşitleri

Siber tehdit ve saldırıların her türü bilgi güvenliğinin üç temel prensibi olan gizlilik, bütünlük ve erişilebilirlik öğelerinin ihlal edilmesi sonucunu doğurur. Bu yaklaşım biçimine göre sınıflandırma aşağıdaki gibi yapılabilir.

- **Gizlilik öğesine yönelik saldırılar:** Bilginin yetkisiz kişilerin eline geçmesi ve sistemin yetkisiz erişime açık hale getirilmesidir. Klavye dinleme sistemleri, casus yazılımlar ve paket koklayıcılar bunlara örnek olarak verilebilir.

- **Bütünlük öğesine yönelik saldırılar:** Bir bilgi sisteminde yer alan bilginin yetkisiz kişilerce değiştirilmesi ya da kısmen veya tamamen yok edilmesini amaçlayan saldırılardır. Virüsler, Truva atları bu saldırı tipine örnek olarak verilebilir.

- **Erişilebilirlik öğesine yönelik saldırılar:** Erişilebilirliğe yönelik saldırılarda gizlilik ve bütünlük öğelerine hiç dokunmadan sadece bilgiye erişim engellenir. Çevrimiçi hizmet veren internet sitelerine veya hizmetlere ulaşım engellenmektedir. Bunun en kolay yolu Botnet, DoS, DDoS gibi servis dışı bırakmaya yol açan saldırı araçları kullanmaktır.[37]

[37] Murat Güngör, *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma*, T.C Kalkınma Bakanlığı, Uzmanlık Tezi, Ankara, 2015, s.49-51.

2.2.2 Bilgi Sistemine Saldırma Yöntemine Göre Siber Saldırı Çeşitleri

Bilgi sistemleri güvenliğini ihlâl eden saldırganlar, amaçlarını gerçekleştirmek için çeşitli yöntemler kullanmaktadır. Saldırıların karakteristiği dört ana başlıkta toplanmaktadır.

- **Engelleme (Interruption):** Kaynak ve hedef sistemler arasında bilgi akışını engellemek suretiyle bilgiye erişim engellenmiş olmaktadır. Bilgi güvenliğinin erişilebilirlik prensibi ihlal edilmiş olur. DoS, DDoS gibi servis dışı bırakma saldırıları örnek olarak verilebilir.

- **Dinleme (Intercept):** Kaynak ile hedef sistemler veya bilgisayarlar arasındaki iletişimin dinlenmesi yolu ile verinin okunmasıdır. Yetkisiz erişim durumu söz konusudur ve güvenliğin gizlilik prensibi ihlâl edilmektedir. Pasif bir saldırı türüdür. Ağda dolaşan paketlerin görüntülenmesi ve kaydedilmesi yöntemi olan ağ koklama (network sniffing) bu saldırıya örnektir.

- **Değiştirme (Modification):** Kaynak bilgisayardan hedef bilgisayara gönderilen verinin, araya giren saldırgan tarafından değiştirilmesi ve içeriği değiştirilen verinin hedef bilgisayardan geliyormuş gibi gönderilmesidir. Bu saldırı karakteristiğinde, güvenliğin bütünlük prensibi ihlâl edilmektedir. Bunun için virüsler, solucanlar ve truva atları gibi kötü amaçlı yazılımlar kullanılmaktadır.

- **Üretim/Uydurma (Fabrication):** Bu saldırı türünde, saldırgan tarafından üretilen yeni bir veri söz konusudur. Saldırı, hedefe sahte verilerin gönderilmesi yoluyla gerçekleştirilmektedir.[38]

[38] Özgü Can, M. Fatih Akbaş, 2014, s.21

2.2.3 Bulunduğu Yere Göre Siber Tehdit ve Saldırı Çeşitleri

Buradaki yaklaşım daha çok tehdidin veya saldırının bulunduğu katmanla ilgilidir. Örneğin ağ katmanındaki saldırıyla uygulama katmanındaki saldırılar arasında teknik olarak farklar bulunmaktadır. Ağ tehditleri, bilgisayar tehditleri ve uygulama tehditleri olmak üzere üç çeşit bulunmaktadır.

1- AĞ TEHDİTLERİ

- Bilgi Toplama
- Koklama ve Gizlice Dinleme
- Kandırma
- Oturum Çalma ve Ortadaki Adam Saldırısı
- DNS ve ARP Zehirleme
- Parola tabanlı saldırılar
- Servis Dışı Bırakma Saldırıları
- Ele geçirilmiş anahtar saldırıları
- Güvenlik Duvarı ve IDS saldırıları

2- BİLGİSAYAR TEHDİTLERİ

- Kötücül Yazılımlar
- Bilgi Toplama
- Parola Atakları
- Servis Dışı Bırakma

- Rastgele Kod Çalıştırma
- Yetkilendirilmemiş Giriş
- Ayrıcalık Yükseltme
- Arkakapı Atakları
- Fiziksel Güvenlik Tehditleri

3- UYGULAMA TEHDİTLERİ

- Uygun olmayan veri/girdi doğrulama
- Kimlik Doğrulama ve Yetkilendirme Saldırıları
- Yanlış Güvenlik Ayarları
- Bilgiyi İfşa Etme
- Kırık Oturum Yönetimi
- Arabellek Taşması
- Şifreleme Saldırıları
- SQL Enjeksiyonu
- Uygun Olmayan Hata Düzeltme ve Olağandışı Durum Yönetimi[39]

Bu bölümün devamında yukarıdaki sınıflandırma baz alınarak siber saldırı türleri açıklanacaktır.

[39] https://www.slideshare.net/teknetir/cehv9-module-01-introduction-to-ethical-hacking (02.04.2018)

2.2. SALDIRI TÜRLERİ

2.2.1 Virüs

Virüsler, en tehlikeli ve en eski kötücül yazılım olarak kabul edilmektedir. Bilgisayar virüsleri, kendi kopyalarını çalıştırılabilir diğer kodlara veya belgelere yerleştirerek yayılan ve kendi kendine çoğalan programlardır.

Çoğu virüs programının, önemli dosyaları silmek veya konak (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkileri bulunmaktadır. Bu virüsler, bilgisayar solucanının bir parçası olarak ağ üzerinden yayılabilir olmalarına rağmen yayılmak için ağ kaynaklarını kullanmazlar. Bunun yerine disket, CD veya DVD gibi ortamlarla veya e-posta eklentileri ile hedef sistemlere bulaşırlar. Virüsleri diğer kötücül yazılımlardan ayıran en önemli özellik insan etkileşimine ihtiyaç duymasıdır. Virüs dâhilindeki kötücül kod mutlaka bir kullanıcı tarafından yürütülmelidir. Bir dosyanın açılmasıyla, bir e-postanın okunmasıyla, bir sistemi önyüklemesiyle (boot) veya virüs bulaşmış bir programın çalıştırılması ile kullanıcı farkına varmadan virüsü yayar.[40]

Bir virüs başka bir çalıştırılabilir dosyayı enfekte eder ve kendisini yaymak için bu taşıyıcı programı kullanır. Virüs kodu daha önce iyi huylu bir programa enjekte edilir ve program çalıştırıldığında yayılır. Virüs taşıyıcı programlarına örnek olarak makrolar, oyunlar, e-posta ekleri, Visual Basic komut dosyaları ve animasyonlar verilebilir.

[40] Gürol Canbek ve Şeref Sağıroğlu (2007) , "Kötücül ve Casus Yazılımlar-Kapsamlı bir Araştırma", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, Cilt 22, No:1, s. 123-124.

En uzun süredir devam eden virüslerden bir tanesi, 1999 yılında David L. Smith taradından oluşturulmuş, Microsoft Word Makroları aracılığıyla yayılan Melissa virüsüdür. Melissa birçok kullanıcıya virüsü Word dokümanına ekleyerek bulaştırdı ve daha sonra dosya kopyalandığında veya e-postayla gönderildiğinde, virüs dosyayla birlikte yayıldı.[41]

Parazit virüsler bilgisayardaki çalıştırılabilir dosyaları veya programları etkilemektedir. Bu tür bir virüs, genellikle ana bilgisayar dosyasının içeriğini değiştirmeden bırakır, ancak virüs kodunun önce çalıştırılacağı şekilde ana bilgisayara eklenir.

Önyükleme sektörü virüsleri, önyükleme sektörü olarak bilinen sabit diskin ilk bölümünde yaşar (bu da disketi de içerir). Bu virüs, ya diskin içeriği hakkında bilgi depolayan programların veya bilgisayarı başlatan programların yerine geçer. Bu tür virüs en yaygın olarak disketlerin fiziksel değişimi yoluyla yayılır.

Çok parçalı virüsler, parazit virüs ve önyükleme sektörü virüslerinin işlevlerini, dosyaları veya önyükleme sektörlerini bulaştırarak birleştirir.

Companion virüs, mevcut bir programı değiştirmek yerine, varolan meşru bir programla aynı adı taşıyan yeni bir program oluşturur. Daha sonra işletim sistemini bu programı çalıştırmaya ikna eder.

Bağlantı virüsleri, işletim sisteminin bir programı bulma biçimini değiştirerek işlev görür ve ilk önce virüsü çalıştırıp sonra arzu edilen programı kandırır. Tüm dizinlere virüs bulaşabileceğinden bu virüs özellikle tehlikelidir. Dizinde erişilen herhangi bir çalıştırılabilir program virüsü tetikler.

[41] Kimberley Graves, *CEH Certified Ethical Hacker Study Guide,* Wiley Publishing, Indiana, 2010, s. 141-145.

Bir veri dosyası virüsü, veri dosyalarını açabilir, işleyebilir ve kapatabilir. Veri dosyası virüsleri makro dillerinde yazılır ve meşru program açıldığında otomatik olarak yürütülür.[42]

Bir sisteme bulaşan virüsleri tespit etmek için tarama ve bütünlük kontrolü yapılır. Tarama, imza tabanlı tarama ve sezgisel tarama gibi iki biçimde yapılabilir. Bütünlük kontrolünde sistem ve uygulama dosyalarının kontrolü yapılır. Virüsler için alınabilecek önlemler için; antivirüs yazılımları kullanmak ve bunların belirli aralıklarla güncellenmesi, bilinmeyen kaynaklardan indirilen dosyaların çalıştırılmaması, bilinmeyen kaynaklardan gelen maillerdeki eklerin açılmaması, belirli aralıklarla yedek alınması, belirli aralıklarla tarama yapılması, taşınabilir disklerin taranmadan kullanılmaması, güvenlik duvarı kullanımı, farklı uzantılara sahip dosyaların çalıştırılmaması gibi önlemler sayılabilir.[43]

2.2.2 Solucan

Solucan nedir? Bir solucan, dosyaları değiştirmeyen, ancak aktif hafızada bulunan ve kendine bilgisayar ağı vasıtasıyla kopyalar yapan, kendi kendini kopyalayan bir programdır. Solucanlar, işletim sisteminin kullanıcılara otomatik ve görünmezlik kazandırdığı imkânları kullanır. Solucanlar yalnızca kontrol edilemeyen kopyaları sistem kaynaklarını tükettiklerinde fark edilir, bu da diğer görevleri yavaşlatır veya durdurur. Varolan bazı solucanlar kendi kendilerini çoğaltırlar ve zararlı bir payload içerirler.[44]

Solucanların virüslerden ayrıldıkları nokta yayılmaları ve çalışmaları için kullanıcı tarafından herhangi bir programın çalıştırılmasına gerek olmamasıdır.

[42] Michael Cross, *Developer's Guide to Web Application Security*, Syngress, Rockland 2007, s. 12-14.
[43] Vuz Dở Hơi (2015), Cehv8 - Module 07: Viruses and Worms, s. 1016-1100. https://www.slideshare.net/vuzlego/ce-hv8-module-07-viruses-and-wormswwwcert-learningcom (04.03.2018)
[44] Michael Cross, 2007, s.16.

İnternette sayfalar arasında gezinirken istenmeden otomatik olarak açılan reklamların linklerine tıklanması sonucu solucanlar bilgisayarlara yüklenebilmektedir. Özellikle, ağ üzerinden diğer sistemlere veya bilgisayarlara bulaşabilme durumları solucanları, virüslere kıyasla daha tehlikeli yapmaktadır. Solucanlar, ağ üzerindeki kaynakların yüksek miktarda tüketimine de sebep olmaktadırlar. Fakat virüsler gibi silme işlemi gerçekleştiremezler.[45]

Bilgisayar virüslerine benzer bir yapıda olan solucanlar, virüsler gibi bir başka çalıştırılabilir programa kendisini iliştirmez veya bu programın parçası olmazlar. Solucanlar, yayılmak için başka bir programa veya virüslerde olduğu gibi insan etkileşimine ihtiyaç duymayan, kendi kendini çoğaltan bir yapı arz ederler.Bir solucanın yayılmasında kullandığı en yaygın yöntemler arasında, e-posta, FTP ve HTTP gibi İnternet hizmetleri bulunmaktadır. Solucanları yaymak için, hedef sistemdeki korunmasızlıklardan faydalanma veya kullanıcıların solucanları çalıştırabilmeleri için sosyal mühendislik yöntemlerini kullanma gibi yöntemler kullanılmaktadır. Solucanlar, başka dosyaları değiştirmezler fakat etkin bir şekilde bellekte dururlar ve kendilerini kopyalarlar. Solucanlar otomatik olarak gerçekleştirilen ve genellikle kullanıcılara gözükmeyen işletim sistemi yapılarını kullanırlar.[46]

Bir ağ boyunca uygulanan ilk solucan 1971'de kendi kendini kopyalama deneyiydi. Ağ, şimdi İnternet için bir öncül olan ARPANET adlı ağdı. Solucan, Savunma Bakanlığı için bu ağı kuran şirkette çalışan Bob Thomas tarafından yazılmıştı ve enfekte olduktan sonra sistemlerde "Ben sarmaşığım, yapabiliyorsan yakala beni " mesajını veren, ARPANET genelinde bir sistemden diğerine kendini kopyalayan Creeper adlı bir programdı.[47]

İlk önemli solucan, Kasım 1988'de Cornell Üniversitesi öğrencisi Robert T. Morris tarafından salındı. Bu solucan, sistemleri ağ üzerinden bulaştırmak için bilinen

[45] Özgü Can ve M. Fatih Akbaş, , 2014, s. 22
[46] G. Canbek ve Ş. Sağıroğlu, 2007, s. 124
[47] R. Messier, 2016, s. 269-270

birkaç güvenlik açığından yararlandı. Morris, 1986 Bilgisayar Dolandırıcılığı ve Kötüye Kullanım Yasası uyarınca mahkum edilen ilk kişi oldu. Solucanın kasıtlı olarak kötü amaçlı yetenekleri bulunmamakla birlikte, solucan kontrol altına alınana kadar önemli zararlar vermeye devam etti. Sonuç olarak, bu sistemler çok hızlı bir şekide solucanın çok sayıda kopyasıyla boğuldu. Bu solucanlar ağdaki diğer sistemleri tehlikeye atmaya çalışırken kaynakları tüketir. Bu solucandan elde edilen bir avantaj, bugün Birleşik Devletlerde bulunan Bilgisayar Acil Müdahale Ekibinin (CERT) oluşturulmasını sağlamasıydı.[48]

Solucanlar dört grupta incelenebilir. Bunlar e-posta, IM (Internet Messaging), İnternet ve ağ solucanlarıdır. E-posta solucanları, e-postaların içerisinde bulunan ve genellikle bir fotoğraf veya metin dosyası gibi görünen eklentilerin kullanıcılar tarafından çalıştırılmalarıyla konak makineye bulaşır. Solucanlar genellikle bulaştıkları makinede kullanıcının adres defterinden e-posta adreslerini toplar ve kendini bulduğu her bir adrese gönderir. İnternet solucanları, sadece internete bağlı olan makinelere bulaşabilen solucanlardır. Bu tür solucanlar, İnternet üzerinde tarama yapar ve en son güvenlik güncellemelerini kurmamış olan, açık kapıları olan veya güvenlik duvarı olmayan korunmasız bilgisayarları bulmaya çalışırlar. Solucan böyle bir bilgisayar bulununca, kendini bu makineye kopyalar ve kendini kurar. W32/Blaster ve W32/Deloder bu tür solucanlara örnektir. Bir başka ilginç solucan türü olan ağ solucanları, paylaşılan bir klasöre, isimlerini faydalı veya ilginç gözükebilecek bir uygulama veya dosya ismine dönüştürerek kendilerini kopyalarlar. Bu dosyaları çalıştıran kullanıcılar kendi bilgisayarlarına solucanı bulaştırmış olur.[49]

Solucanlara karşı alınabilecek önlemler arasında bir antivirüs programı kullanmak ve bunu güncel tutmak sayılabilir. Ayrıca kullanıcıların internetten program veya dosya indirirken dikkatli olması gerekmektedir. Bilinmeyen göndericilerden gelen e-posta eklentilerini açmaktan kaçınılmalıdır. [50]

[48] a.g.e. , s. 269-270.
[49] G. Canbek ve Ş. Sağıroğlu, 2007, s. 124.
[50] https://www.slideshare.net/vuzlego/ce-hv8-module-07-viruses-and-wormswwwcert-learningcom (04.03.2018)

2.2.3 Truva Atı

Truva atı kendisini kurbanlarına zararsız bir program gibi (örneğin bir oyun ya da yardımcı program) gösteren fakat genellikle kötü amaçlı faaliyette bulunan bir programdır. Görünümü ve ilk çalıştırıldığında yaptığı işler zararsız bir programa benzer fakat çalıştırıldığında verileri silebilir veya değiştirebilir. Truva atları, insanların, meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır.[51] Örneğin antivirüs programı zannedilerek internetten indirilen bir program aslında bir Truva atı olabilir.

Birçok durumda Truva, kullanıcı için arzu edilen bir işlevi yerine getirir gibi görünse de, aslında bir bilgisayar korsanının, kullanıcının bilgisayar sistemine erişmesine izin verir. Truva atları genellikle başka bir program veya yazılım paketi ile birlikte indirilir. Bir kere sisteme yüklendikten sonra, sistem çökmesi veya yavaşlamasına ilaveten veri hırsızlığı veya veri kaybına neden olabilirler. Truva atları, dağıtık hizmet dışı bırakma (DDoS) gibi saldırılar için kullanılabilir.

Birçok Truva atı, kurban bilgisayardaki dosyaları manipüle etmek, süreçleri yönetmek, komutları uzaktan çalıştırmak, tuş vuruşlarını kesmek, ekran görüntülerini izlemek ve virüs bulaşmış bilgisayarları yeniden başlatmak veya kapatmak için kullanılmaktadır. Bir e-posta eki, NetBIOS dosya paylaşımı veya indirilen bir İnternet programı vasıtasıyla bir Truva atı kurban sisteme gönderilebilir. İnternet sitelerindeki ücretsiz programlar, müzik dosyaları veya video dosyaları için yapılan reklamlar Truva programını yüklemek için bir kurbanı kandırır; program hedef sistem üzerinde, yıkıcı ve sinsi olabilecek düzeyde sistem seviyesinde erişime sahiptir.[52]

Farklı saldırılar gerçekleştirmek için Truva atları oluşturulabilir ve kullanılabilir. Örneğin;

[51] Erdoğan, Görkem, ve Şerif Bahtiyar, "Sosyal Ağlarda Güvenlik", *XVI. Akademik Bilişim Konferansı,* Mersin, 2014, s. 267-272.
[52] K. Graves, 2010, s. 126-130.

- Uzaktan Erişimli Truva Atları (RAT'lar), bir sisteme uzaktan erişim elde etmek için kullanılır.
- Veri Gönderen Truva Atları, bir sistemdeki verileri bulmak ve verileri bir bilgisayar korsanına iletmek için kullanılır.
- Zararlı Truva Atları, bir sistemdeki dosyaları silmek veya bozmak için kullanılır.
- Hizmet Reddi Truva Atları, hizmet reddi saldırısı başlatmak için kullanılır.
- Proxy Truva Atları, diğer sistemlerle trafiği kesmek veya saldırı yapmak için kullanılır.
- FTP Truva Atları, dosyaları bir sisteme kopyalama amacıyla bir FTP sunucusu oluşturmak için kullanılır.
- Güvenlik Yazılımı Devre Dışı Bırakma Truva Atları, antivirüs yazılımını durdurmak için kullanılır.[53]



Şekil 5: Truva Atının Sisteme Bulaşması

Şekil 5'de görüldüğü gibi kurban bir oyun indirme niyetindeyken beraberinde bir Truva atını kendi sistemine dahil etmektedir. Truvaların yetenekleri arasında asıl amacını gizleyebilme, kullanıcı ile aynı haklara sahip şekilde çalışabilme ve yetki yükseltme, uzaktan erişim vb. yazılımları kurabilme gibi yetenekler sayılabilir. Ayrıca

[53] a.g.e, s. 130

kredi kartı bilgilerini çalabilirler, ses ve görüntü kaydedebilirler. Sistemde daha sonra faydalanmak üzere arkakapı (backdoor) oluşturabilirler.[54]

Bir sisteme bulaşmış Truva atlarını tespit etmek için şüpheli görülen açık portlar, çalışan işlemler, kayıt defteri girdileri, yüklü aygıt sürücüleri, Windows servisleri, açılış programları, dosya ve klasörler, ağ aktiviteleri ve işletim sistemi dosyalarındaki değişiklikler taranmalıdır. Ayrıca Truvaları tespit etmek için bir Truva tarayıcısı çalıştırılmalıdır. Truva atlarının sisteme bulaşmasını önlemek için alınması gereken önlemler aşağıda sıralanmıştır.

- Kaynağı belli olmayan e-posta eklentileri açılmamalı,
- Kullanılmayan portlardan erişim engellenmeli,
- Anlık mesajlaşma ve sosyal ortamlardan uygulama paylaşılmamalı,
- Kullanılmayan servisler kapatılmalı,
- Şifrelenmiş ve kullanılmayan portlardan trafik kontrol edilmeli,
- Güvenilir olmayan kaynaklardan dosya indirilmemeli,
- İşletim sistemi uygulamaların güncellemesi yapılmalı,
- USB diskler kullanımdan önce taranmalı,
- Dosya bütünlüğü kontrol eden yazılımlar kullanılmalı,
- Son kullanıcı bilgisayarında Antivirus, IDS ve güvenlik duvarı yazılımları kullanılmalıdır.[55]

2.2.4. Arka Kapılar

Bir arka kapı bir bilgisayar korsanının daha sonraki bir zamanda sisteme erişmesi için bir hedef sisteme kurduğu bir program veya bir dizi ilgili programdır. Bir arka kapı kötü niyetli bir Truva atının içine gömülebilir. Bir sisteme bir arka kapı kurmanın amacı, bilgisayar korsanlarının istedikleri anda sisteme girmelerini

[54] https://www.slideshare.net/vuzlego/ce-hv8-module-06-trojans-and-backdoorswwwcert-learningcom (18.03.2018)
[55] https://www.slideshare.net/vuzlego/ce-hv8-module-06-trojans-and-backdoorswwwcert-learningcom (18.03.2018)

sağlamaktır. Windows işletim sisteminde arka kapıyı gizlemek için en yaygın teknik, yeni bir servis eklemektir. Bir arka kapı yüklenmeden önce, çalışan servisleri bulmak için sistem bilgisayar korsanı tarafından araştırılmalıdır. Bilgi toplama tekniklerinin kullanılması, hedef sistem üzerinde hangi servislerin veya programların çalıştığını bilme anlamında kritik önem taşır. Çoğu durumda, bilgisayar korsanı arka kapıyı kurar, bunu da yeni bir servis ekleyerek ve bu servise göze çarpmayan bir ad vererek yapar. Bu yöntemden daha iyisi, hiç kullanılmayan ve manuel etkinleştirilen veya tamamen devre dışı bırakılan bir servis seçmektir.[56]

Arka kapılar en çok programcılar tarafından, hataları düzeltmek ve hata durumunda sisteme erişmek için bilerek bırakılırlar. Ancak arka kapılar, saldırganlar tarafından keşfedildirse sisteme yetkisiz erişim yapılmasına olanak tanırlar. Arka kapılara işletim sisteminin müdahale etmesi zordur. Bunların tehdit haline gelmemeleri için uygulama geliştirilirken ve güncellenirken güvenlik prosedürlerine uyulmalı, uygulama kullanıma açılmadan önce arka kapılardan arındırılmalıdır.[57]

Arka kapılar için bazı önlemler alınabilir. Örneğin bir çok ticari antivirüs ürünü herhangi bir zarardan önce otomatik bir şekilde arka kapıları tarayıp tespit edebilir. Kullanıcılar da güvenilmeyen internet siteleri ve e-posta eklentilerindeki uygulamaları yüklememeleri konusunda bilinçlendirilmelidir.[58]Açık portlar atak düzenlemek için birincil kaynaklardır. Bu yüzden, ağı güvenli hale getirmek için bu açık portlar bulunmalı ve bunlar korunmalıdır.[59]

[56] K. Graves, 2010, s. 127
[57] Mustafa Gülmüş, *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği*, Yayımlanmış Yüksek Lisans Tezi, İstanbul, 2010, s. 95.
[58] https://www.slideshare.net/teknetir/cehv9-module-06-malware-threats (20.03.2018)
[59] https://www.slideshare.net/vuzlego/ce-hv8-module-06-trojans-and-backdoorswwwcert learningcom (18.03.2018)

2.2.5 Kök Kullanıcı Takımları (Rootkits)

Virüsler veya solucanlar gibi kendini kopyalama amacı gütmeyen kök kullanıcı takımları kendilerini işletim sisteminin derinliklerine saklarlar ve tespit edilebilmeleri çok zordur. Kök kullanıcı takımları, genellikle sistemde bulunan çekirdek (kernel) açıkları kullanılarak, kök (root) yetkisinin kazanılması sonucu bulaşmaktadırlar. Anti-virüs yazılımları kök kullanıcı takımlarını tespit etmekte ve temizlemekte zorlanmaktadır. Bundan dolayı anti-virüs yazılımlarına ek olarak bir takım güvenlik yazılımları kullanılması gerekmektedir. Bu doğrultuda, sadece kök kullanıcı takımlarına karşı geliştirmiş bazı anti-virüs programları mevcuttur.[60]

Bir kök kullanıcı takımı hem kendisinin hem de eşlik eden bir virüsün varlığını gizlemek için sistem yazılımını değiştirebilir. Her şeyden önce bir virüs genellikle bir sistemin enfeksiyonunu korumak isteyecektir. Bunu yapmak için, gizli olması gerekir. Bu bir kök kullanıcı takımı tarafından halledilebilir. Windows sisteminde, bir kök kullanıcı takımı, dizin listelerinin kötü amaçlı yazılım ile ilişkili dosyaları göstermesini engelleyebilir. Çalışan virüsün Görev Yöneticisi'nde görünmesini de engelleyebilir.

Bir kök kullanıcı takımı uygulamak için bir başka neden, bir sistem üzerinde kök düzeyinde erişim elde etmek ve korumaktır. Unix benzeri bir sistemde, yönetim kullanıcısına kök adı verilir. Bu, bir Windows sistemindeki yönetici (administrator) kullanıcısına benzer. Kök kullanıcısı, Linux içeren bir Unix benzeri sistem üzerinde en üst düzeyde ayrıcalıklara sahiptir. Kök kullanıcı hesabı bazen süper kullanıcı olarak adlandırılır. Bir saldırgan kök ayrıcalıkları edinebilir, kullanıcı ekleyebilir, sistem programlarını değiştirebilir, ayrıcalıklı ağ dinleyicilerini başlatabilir, parolaları değiştirebilir ve sistemdeki herhangi bir dosyayı görüntüleyebilir veya silebilir.[61]

Kök kullanıcı takımlarının bulundukları seviyeye göre değişik türleri vardır. Bunlardan Çekirdek-seviyesi kök kullanıcı takımları, bir bilgisayar sisteminde bir arka kapıyı gizlemeye yardımcı olmak için kod ekler ve / veya çekirdek kodunun bir

[60] Ö. Can ve M.F. Akbaş, 2014, s.23.
[61] R. Messier, 2016, s. 270-271.

bölümünü değiştirilmiş kodla değiştirir. Bu, genellikle, Linux'ta yüklenebilir çekirdek modülleri veya Windows'daki aygıt sürücüleri gibi bir aygıt sürücüsü veya yüklenebilir modül aracılığıyla çekirdeğe yeni kod ekleyerek gerçekleştirilir. Çekirdek düzeyindeki kök kullanıcı takımları özellikle tehlikelidir, çünkü uygun yazılımlar olmadan tespit edilmesi zor olabilir.[62]

Kütüphane-Seviyesi kök kullanıcı takımları saldırganla ilgili olan bilgiyi gizlemek için orijinal sistem çağrılarıyla sahte olanı yer değiştirir. Uygulama-seviyesi kök kullanıcı takımlarında ise Truva atıyla ikili uygulama (application binaries) yer değiştirir veya kötücül kod enjekte edilerek var olan uygulamaların davranışları değiştirilir.[63]

Kök kullanıcı takımlarına karşı korunmak için alınması gereken önlemler aşağıda sıralanmıştır[64].

- Kritik verileri yedekledikten sonra uygulamalar/işletim sistemi güvenilir bir kaynaktan yeniden yüklenmelidir.
- Personel güvenilmeyen kaynaklardan herhangi bir dosya/program indirmemeleri konusunda eğitilmelidir.
- İyi dökümante edilmiş otomatik kurulum prosedürleri tutulmalıdır.
- Ağ ve host bazlı güvenlik duvarı yüklenmelidir.
- Kök kulllanıcı takımlarının varlığını tespit etmek için çekirdek bellek dökümü analizi yapılmalıdır.
- Güvenilir restorasyon ortamlarının kullanılabilirliği sağlanmalıdır.
- Bilgisayarlar ve sunucular ataklara karşı sıkılaştırılmalıdır.
- İşletim sistemleri ve uygulamalar güncellenmelidir.

[62] K. Graves, 2010, s. 112.
[63] http://ismailsen.com.tr/sistem-ele-gecirme-system-hacking/ (24.03.2018)
[64] https://www.slideshare.net/teknetir/cehv9-module-05-system-hacking (24.03.2018)

2.2.6. Casus Yazılım (Spyware)

Casus yazılım, kullanıcıların önemli bilgilerini ve yaptığı işlemleri, kullanıcının bilgisi olmadan toplar ve bu bilgileri kötü niyetli kişilere gönderir. Casus yazılımlar, özellikle İnternet kullanıcıları tarafından sistemlere farkında olmadan bulaştırılmaktadır. Virüs ve solucanlardan farklı olarak hedef sisteme bir kez bulaştıktan sonra kendi kopyasını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar. Casus yazılımlarla elde edilmeye çalışılan bilgi kimi zaman bir kredi kartı numarası gibi önemli bir bilgi olabileceği gibi başkalarına satılmak üzere herhangi bir kişisel veride olabilir. Bunun dışında, ticari firmalar İnternet üzerindeki kullanıcı alışkanlıklarını saptamak amacıyla casus yazılımları İnternet üzerinde yayabilmektedir.[65]

İnternet'te, bir saldırganın kullanıcı onayı ve bilgisi olmadan bilgisayardaki kullanıcı etkinliği hakkında bilgi çalmak için kullanabileceği on ana casus yazılım türü vardır. Bunlar masaüstü, e-posta ve internet, çocuk izleme, video, baskı, ekran görüntüsü yakalama, usb, ses, gps, mobil telefon ve telefon casus yazılımlarıdır. Bu casus yazılımlarla kullanıcı ile ilgili log bilgileri, gönderilen mailler, ziyaret edilen web sayfaları, klavye girişleri, dosya işlemleri ve benzeri bilgileri belli aralıklarla dışarı aktarabilirler. Casus yazılımlar sistemi izlemenin yanında sistemde değişiklik de yapabilir.[66]

Casus yazılımlar üç temel kaynaktan gelir. Bunlar internetten indirilen ücretsiz yazılımlar, e-posta eklentileri ve web siteleridir. Casus yazılımlardan korunmak için alınacak tedbirlere örnek olarak karşı casus yazılım (anti-spyware) ürünlerinin bilgisayarlara kurulması, bilinmeyen göndericilerden gelen şüpheli e-postaların ve dosya eklentilerinin açılmaması verilebilir. Ayrıca İnternet güvenlik ayarları çok

[65] G. Canbek, Ş. Sağıroğlu, 2007, s.125-126
[66] https://www.slideshare.net/vuzlego/ce-hv8-module-05-system-hacking-wwwcert-learningcom (22.05.2018)

düşük olarak seçilmemeli ve görev yöneticisi raporları düzenli bir şekilde kontrol edilmelidir.[67]

2.2.7 Klavye Dinleme Sistemleri (Keyloggers)

Kullanıcının klavye girişlerini kaydeden yazılımlar veya donanım cihazlarıdır. Ekran görüntüsünü kaydedebilme ve çalışan uygulamaların listesini alabilmek gibi yetenekleri de vardır. Klavye donanımı ile işletim sistemi arsına yerleşirler. Bazı yasal uygulama alanları da vardır. Çalışanların aktivelerinin izlenmesi veya anne babanın kendi çocuklarını bu yazılımlar vasıtasıyla izlemesi gibi uygulamalar buna örnek olarak verilebilir. Bunların dışındaki uygulamalarda kullanıcılara ait önemli bilgiler saldırganlar tarafından ele geçirilebilir.[68]

Klavye dinleme sistemlerinin donanımsal ve yazılımsal olmak üzere iki temel türü vardır. Donanımsal keylogger klavye ve usb girişi arasına takılır. Klavye girişlerini kendi üzerindeki depolama alanına kaydeder ve mutlaka fiziksel erişime ihtiyaç duyarlar. Yazılımsal keylogger uygulama seviyesindedir ve Kernel keylogger, Rootkit Keylogger, Device Driver Keylogger gibi türleri vardır. [69] Yazılımsal klavye dinleme sistemleri, bir sistemde Truva Atları veya virüsler tarafından yayılır.[70]

Klavye dinleme sistemlerinden korunmak için bir antivirüs programı kullanılabilir. Çünkü çoğu antivirüs şirketi zaten bilinen keyloggerları veritabanlarına ekleyerek keyloggerlara karşı koruma sağlamış ve diğer türden kötü amaçlı programlara karşı koruma sağlamıştır. Burda önemli olan bu veritabanını güncel tutmaktır. Bununla birlikte, virüsten koruma ürününüzün varsayılan ayarlarla bu tür kötü amaçlı yazılımları algılayacağından emin olunmalıdır. Değilse, en yaygın

[67] a.g.e
[68] a.g.e.
[69] a.g.e.
[70] Michael Cross, 2007, s. 109

keylogger'lara karşı koruma sağlamak için ürün uygun bir şekilde yapılandırılmalıdır. Keyloggerların temel amacı, gizli verileri (banka kartı numaraları, parolalar, vb.) almak olduğundan, bilinmeyen keyloggerlara karşı korunmak için bir kerelik parola veya iki adımlı kimlik doğrulama kullanmak, keylogging yazılımını algılamak için tasarlanmış proaktif koruma içeren bir sistem kullanmak ve sanal klavye kullanmak gibi önlemler alınmalıdır.[71]

2.2.8 Koklayıcı (Sniffer)

Bir ağ üzerindeki IP paketlerini dinlemek ve kaydetmek, bir diğer ifadeyle "koklamak" için kullanılan donanım ve yazılımlar, koklayıcı olarak adlandırılmaktadır. Bu tip bir yazılım veya donanım, bütün paketleri dinleyen ayrımsız kipe (promiscuous mod) geçerek bütün ağ trafiğini dinler ve kaydeder. Bu paketler içinde yer alan şifre bilgileri gibi önemli bilgiler, paket içeriği taranarak elde edilebilir.[72]

Koklama (sniffing) aktif ve pasif olmak üzere iki türlü olur. Aktif koklamada saldırgan trafiği dinleyebilmek için paket gönderir. Switch kullanılan ağ altyapılarında tercih edilir. Trafiğin dinlenebilmesi için farklı atak tiplerinin kullanılması gereklidir. Ayrıca ağ cihazında SPAN/Monitor port ayarlanarak trafik dinlenebilir. Pasif koklamada ise saldırgan herhangi bir paket göndermez, sadece gelen trafiği dinler. Hub kullanılan ağlarda diğer kullanıcıların trafiği dinlenebilir.[73]

Koklama ataklarına örnek olarak MAC Adres [74] Taşması (MAC Flooding), ARP Zehirlenmesi (ARP Poisoning) ve DHCP [75] atakları verilebilir.

[71] https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/ (24.03.2018)
[72] G. Canbek ve Ş. Sağıroğlu, 2007, s. 124
[73] https://www.slideshare.net/polichen/ce-hv8-module-08-sniffing (24.03.2018)
[74] MAC adresleri bilgisayarların fiziksel adreslerine verilen addır. IP adresleri ise mantıksal adreslerdir.
[75] DHCP servisi, bilgisayarlara dinamik bir şekilde ip adresi dağıtan servisin adıdır.

Mac Flooding saldırısında, saldırgan Mac tablolarını doldurarak trafiğin bütün ağa gönderilmesini sağlar. Çünkü switchler (anahtarlar) her portunda bağlı olan sistemlerin MAC adreslerini MAC adres tablolarında tutmaktadır ve MAC tabloları belirli sayılarda girdileri tutabilmektedir. Bu saldırıları yapabilmek için Macof ve Yersina gibi araçlar kullanılabilir. Saldırılardan korunmak için kenar anahtarlarda MAC adres sayısı sınırlanmalıdır.[76]

ARP Poisoning saldırısında ARP protokolünün çalışma prensiplerinden faydalanılır. ARP protokolü, bilgisayarların aynı ağda bulunan ve IP adreslerine sahip bilgisayarların MAC adreslerini öğrenmek için kullanılmaktadır. ARP istekleri bütün ağa bağlanan sistemlerin duyacağı şekilde yani broadcast olarak gönderilmektedir. ARP protokolü istekte bulunup bulunmadığına bakmaksızın gelen ARP cevaplarını kaydetmektedir. ARP cevapları ARP tablosuna kaydedilmektedir. Sahte ARP istekleri ve cevaplarıyla anahtarlar aşırı yüklenebilir. Ortaya çıkan bu taşkın neticesinde anahtar yönlendirme moduna geçer ve saldırgan ağı dinlemeye başlar. Son adım olarak kurban bilgisayara sahte arp cevapları göndererek trafiğin kendi üzerinden geçmesini sağlar. Arpspoof, Ettercap, Driftnet, Networkminer gibi saldırı araçları vardır. [77]

ARP Poisoning saldırıları, network firmaları tarafından satılan ürünlerde ARP security veya Dynamic ARP Inspection özellikleri aktif hale getirilerek önlenebilir. Ayrıca ağı küçük Vlan'lere bölmek ve yetkili kullanıcıları dış ortamdan soyutlamak arp poisoning saldırısının yüzeyini azaltmaktadır.[78]

Yukarıda zikredilen saldırılar ve bunların dışındaki tüm koklama saldırılarına karşı alınabilecek en iyi önlem şifrelemedir. Çünkü şifreleme, koklama işlemini engellememesine rağmen korsanların bilgileri yorumlayamaması nedeniyle koklama

[76] a.g.e.
[77] a.g.e
[78] http://blog.btrisk.com/2016/01/arp-poisoning-nedir-nasil-yapilir.html (24.03.2018)

saldırısı sırasında yakalanan verileri işe yaramaz hale getirir. AES ve RC4 veya RC5 gibi şifreleme genellikle bir ağdaki koklama işlemini önlemek için kullanılır.[79]

2.2.9 Aldatma Saldırıları (Spoofing)

Aldatma saldırılarında hedef bilgisayara bağlanırken kaynak bilgisayarın iletişim bilgileri; örneğin IP adresi, MAC adresi veya port numarası farklı gösterilerek karşı taraf aldatılır.[80]

En sık kullanılan aldatma saldırılarından olan IP spoofing işlemi; hizmet dışı bırakma(DoS)gibi saldırılarda takipten kurtulmak için saldırıda bulunan kişinin IP adresini gizlemesi, ip adres tabanlı kimlik doğrulamayı atlamak için güvenilir bir kullanıcı gibi görünme, ağ trafiğini dinlemek gibi amaçlar için kullanılabilir.[81]

MAC Spoofing saldırısında, ağ anahtarına gönderilen çerçevelerin içerisindeki kaynak MAC adresi kısmına, dinlenmek istenen bilgisayarın MAC adresi yazılır. Hedef bilgisayar ağa paket gönderene kadar hedef bilgisayara gönderilen çerçeveler de böylece saldırganın bilgisayarına gönderilmiş olmaktadır.[82]

DNS Spoofing saldırılarında, alan isimlerinin tutulduğu tablolarda değişiklik yapılması suretiyle kullanıcıların DNS isteklerine sahte cevaplar vererek saldırganın belirlediği IP adresine sahip sunuculara yönlendirme işlemi yapılır.[83]

---

[79] K. Graves, 2010, s. 158

[80] İsmail Karadoğan, *Ağ İletişiminde Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları*, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2016, Elazığ, s.21.

[81] M. Zekeriya Gündüz, *Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti*. Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, ,2013, Elazığ, s.47.

[82] http://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/ikinci-katman-atakları (27.03.2018)

[83] Komal Gandhi, "Network security problems and security attacks", *2016 International Conference on Computing for Sustainable Global Development,* New Delhi, 2016, s. 3856.

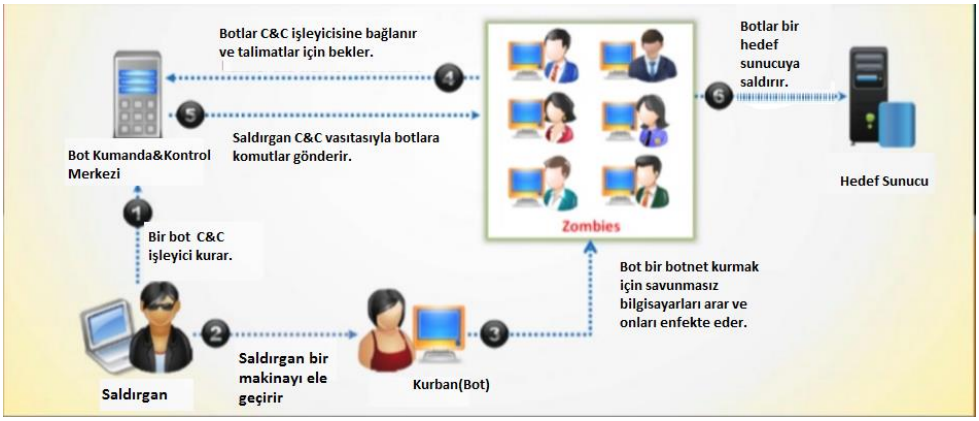
Spoofing olaylarından korunmak için; hedef IP ve MAC kontrolünün yapılması, yönlendiricilerde kaynak yönlendirme fonksiyonunun pasif hale alınması, anahtarda port-security kullanılması, paket filtreleme, şifreleme yöntemleri gibi önlemler alınmalıdır..[84]

2.2.10. Hizmet Dışı Bırakma (Denial of Service)

Hizmet dışı bırakma saldırıları, bir sistemin veya ağın kullanılamaz hale getirilmesi için kullanılır ve kullanıcı verilerinin kullanılabilirliğine yönelik saldırılar olarak değerlendirilir. Bir hizmet dışı bırakma (DoS) saldırısı sırasında, bir bilgisayar korsanı sisteme aşırı yüklenerek veya meşru kullanıcıların sisteme erişmesini engelleyerek sistemi bir daha kullanamaz hale getirir veya sistemi önemli derecede yavaşlatır. Tek bir sistem tarafından tek bir hedefe gönderilen saldırılar basit DoS olarak adlandırılırken, birçok sistem tarafından tek bir hedefe gönderilen saldırılar dağıtılmış hizmet reddi veya DDoS olarak adlandırılır.[85]

DDoS saldırılarında bot adı verilen saldırganlar tarafından ele geçirilmiş bilgisayarlar kullanılır. Bu botlarla oluşturan botnetler Command&Control (C&C) Server denen merkezi sunucu tarafından uzaktan yönetililirler. Bu senaryo aşağıda Şekil 6'da gösterilmiştir.

[84] M. Zekeriya Gündüz, 2013, s. 47-48.
[85] K. Graves, 2010, s. 174.



Şekil 6 Şekil DDoS Saldırılarında Botların ve Botnetin Kullanılması [86]

Hizmet Dışı Bırakma (DoS) saldırıları çeşitli şekillerde olabilir:

Arabellek Aşımı Saldırıları, DoS saldırılarının en yaygın çeşitidir. Arabellek hafızada ard arda dizili türdeş veri depolayan hafıza bloğudur. Arabellek aşımı saldırıları; bir internet sitesine, sitenin programcısının gelmesinin beklediği ve bu amaçla veri akışı için planladığı arabellek değerinin karşılayamayacağı kadar çok trafik yollanması sonucu oluşur. Saldırı, hedef sistemdeki bilinen zayıf bir noktanın üzerine, başarıya ulaşacağı bilinerek yapılabileceği gibi zayıf bir nokta bilinmeden başarı ihtimaliyle de yapılabilir.[87]

Syn Atağı esnasında, bir ağdaki TCP istemcisi ve sunucu arasında bir oturum başlatılmak istendiğinde aralarında " üçlü el sıkışma" tekniğiyle birbirlerine paketler gönderilir. Bu paket değişimini işlemek için küçük bir ara bellek alanı bulunur. Bir SYN saldırısında, bilgisayar korsanı çok sayıda bağlantı isteğini çok hızlı bir şekilde gönderir ve karşıdan gelen isteğe yanıt vermez. Hedef makinenin cevaplar için ayırdığı alan sınırlı olduğundan ve sahte istekle uğraştığından meşru bağlantılara cevap veremez duruma gelir. Böylece oturum yavaşlar veya çöker. Bu tür bir saldırı ile

[86] https://www.slideshare.net/teknetir/cehv9-module-09-denial-of-service (04.06.2018)
[87] https://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/denial-of-service-(dos)-saldırıları-ve-korunma-yöntemleri (27.03.2018)

mücadele etmek için işletim sisteminizin doğru ayarları sağlaması veya sistem yöneticisinin arabellek boyutunu ve zaman aşımı süresini ayarlaması gerekmektedir.[88]

Bu atak tiplerinin dışında Smurf atağı, Teardrop atağı ve virüsler yoluyla hizmet dışı bırakma saldırıları yapılabilir. Hizmet dışı bırakma saldırılarından saptamak, durdurmak veya önlemek için yapılması gerekenler aşağıda maddeler halinde sıralanmıştır.

- **Ağ Giriş Filtreleme**: Tüm ağ erişim sağlayıcıları, veri indiren ağların, sahte veya sahte adresler içeren paketleri İnternet'e enjekte etmesini durdurmak için ağ giriş filtrelemeyi uygulamalıdır. Bu, meydana gelen bir saldırıyı durdurmasa da, saldırının kaynağını izlemeyi çok daha kolay hale getirir ve saldırıyı hızlı bir şekilde sonlandırır. Çoğu IDS, güvenlik duvarları ve yönlendirici, ağ giriş filtreleme özellikleri sağlar. [89]

- **Hızı Sınırlandıran Ağ Trafiği**: Bugün piyasada bulunan bir dizi yönlendirici, bazı trafik türlerinin tüketebileceği bant genişliği miktarının sınırlanmasına izin veren özelliklere sahiptir. Buna bazen trafik şekillendirmesi denir.[90]

- **Saldırı Tespit Sistemleri**: Köle, efendi veya ajan makinelerle iletişim kuran saldırganları tespit etmek için bir saldırı tespit sistemi (IDS) kullanılmalıdır. Bunu yapmak, ağdaki bir makinenin bilinen bir saldırıyı başlatmak için kullanılıp kullanılmadığının bilinmesini sağlar, ancak muhtemelen bu saldırıların veya bunları uygulayan araçların yeni varyasyonlarını algılamaz. Çoğu IDS satıcısının, Trinoo, TFN veya Stacheldraht ağ trafiğini algılamak için imzaları vardır.[91]

[88] Bradley A. Wayland, *Security for Business Professionals: How to Plan, Implement, and Manage Your Company's Security Program*, Butterworth- Heinemann, Newton, MA, USA, 2014, s.156-157
[89] K. Graves, 2010, s. 182
[90] K. Graves, 2010, s. 50
[91] a.g.e, s.50

- **Otomatik Ağ İzleme Araçları**: Sahte adresleri olan paket akışlarını ağ vasıtasıyla izlemek, trafiği taşıyan tüm ağların işbirliğini gerektiren ve çok zaman harcatıcı bir görevdir. Bu, saldırı devam ederken tamamlanmalıdır.[92]

- **Ana Bilgisayar Denetimi ve Ağ-Denetim Araçları**: Bir sistemde bilinen DDoS aracı istemci ve sunucu ikililerinin varlığını saptamaya çalışan dosya tarama araçları mevcuttur. Ağ tarama araçları, ağdaki ana makinelerde çalışan DDoS ajanının varlığını saptamaya çalışır.[93]

2.2.11 Sosyal Mühendislik

Sosyal mühendislik, bir sisteme veya ağa girmek için kullanılan ve teknik olmayan bir yöntemdir. Sosyal mühendisler, insan doğasından kaynaklanan zaafiyetleri kullanarak elde edilen bigilerle sisteme girmeye çalışır. Sistemdeki kullanıcıların güvenlik açısısından zayıf halka olduğu konusunda genel bir kanı vardır. Sosyal mühendisliği mümkün kılan bu ilkedir. Sonuç olarak kimlik doğrulama işlemleri, güvenlik duvarları, sanal özel ağlar ve ağ izleme yazılımına sahip şirketler bile bu saldırılara maruz kalabilir; çünkü sosyal mühendislik doğrudan güvenlik önlemlerine saldırmaz.[94]

İnsanların inanç, güven, vicdan, korku ve yardım etme duyguları kullanılarak yapılan ve bu şekilde elde edilen bilgilerle yapılan saldırılar sosyal mühendislik kapsamına girer. Saldırganın kendini kurum içi bir çalışanmış gibi göstermesi ve kurum çalışanları vasıtasıyla bir takım bilgilere ulaşmaya çalışması, aceleci bir dil kullanarak o an önemli bir olay (yangın vb.) olduğunu söyleyerek yardım talebinde bulunması gibi senaryolar sosyal mühendislik saldırısı örnekleridir.[95]

---

[92] a.g.e, s.50
[93] a.g.e, s.50
[94] K. Graves, 2010, s. 50
[95] Ö. Can ve M. Fatih Akbaş, 2014, s. 24

Sosyal mühendislik kullanılan yönteme göre insan tabanlı ve bilgisayar tabanlı olmak üzere ikiye ayrılır. İnsan tabanlı sosyal mühendislikte insanlarla doğrudan bire bir etkileşim vardır. Burada amaç istenen bilginin doğrudan elde edilmesidir. Kullanılan teknikler arasında kimliğe bürünme, önemli bir kullanıcı gibi davranmak, üçüncü taraf olmak, yardım masası, omuz sörfü, çöp dalışı ve vishing gibi teknikler sayılabilir. Bilgisayar tabanlı sosyal mühendislikte istenen bilgilerin elde edilebilmesi için bilgisayar yazılımları kullanılır. Bu yöntemlerden en bilindikleri sazan avlama ve çevrimiçi dolandırıcılıktır.[96]

Sosyal mühendislerin kullanmış olduğu yöntem ve tekniklerine karşı hem bireysel hemde kurum bazında alınabilecek önlemlerinden bazıları aşağıda maddeler halinde sıralanmaktadır.

- Çöpe atılan belge ve dökümanlar, kırpıcılardan geçirilmeli veya okunmayacak şekilde yırtılmalıdır.
- Şifre korumalı ekran koruyucular kullanılmalıdır.
- Kişisel şifreler kesinlikle bir başkasına söylenmemelidir.
- Bir kurum için işten ayrılan çalışanların uyması gereken prosedürler hazırlanmalıdır.
- Bir kurum için işten ayrılan personellerin kullandıkları sistem parolaları hemen pasif hale getirilmelidir.
- Kişiye özel bilgiler (şifre, kredi kartı numarası gibi) kimseyle paylaşılmamalıdır.
- Bilgi güvenliği için birden fazla e-posta kullanmanın bazı durumlarda daha etkili olabileceği bilinmelidir.
- Hassas kişisel bilgiler (T.C kimlik numarası, telefon numarası, doğum yeri, doğum tarihi vb.) her yerde, özellikle sosyal medyada (facebook, twitter vb.) paylaşılmamalıdır.

[96] M.Z. Gündüz ve R. Daş, "Sosyal Mühendislik ve Korunma Yolları", *CyberMag Dergisi*, 2017, Sayı: 18, s. 19.

- Klavye türü giriş birimlerinden şifre girilirken, giriş yapan kişinin fark etmeyeceği şekilde gözetlenmesi anlamına gelen omuz sörfü yapanlara karşı dikkatli olunmalıdır.[97]

Sosyal mühendislik için en önemli önlem, çalışanların eğitimidir. Tüm çalışanlar, gizli verileri nasıl güvenli tutacakları konusunda eğitilmelidir. Yönetim ekipleri, güvenlik politikasının oluşturulması ve uygulanması sürecinde yer alırlar; böylece, güvenlik politikasını tam olarak anlamaları ve tüm organizasyonda desteklemesi sağlanır. Kurum güvenlik bilinci politikası, tüm yeni çalışanların bir güvenlik yönergesi izlemelerini gerektirir.[98]

2.2.12 Sazan Avlama (Phishing)

Phishing sözcüğü İngilizcedeki password ve fishing sözcüklerinin birleştirilmesiyle oluşturulmuştur.[99] Türkçede yemleme, oltalama ve sazan avlama gibi karşılıkları vardır. Başkasına ait kişisel verileri elde etmek için kullanılan metotların başında sazan avlama (phishing) olarak adlandırılan yöntem gelmektedir.

Sosyal mühendislikte olduğu gibi sazan avlama yöntemleri saldırganın yaratıcılığı ve hayal gücüyle orantılı olarak çeşitlilik gösterebilir. Oltalama yapan kişiler kurbanlarına gönderdikleri e-postalar ile bu insanları kendi hazırladıkları ve Facebook gibi popüler sitelere, alışveriş sitelerine veya finansal kurumlara ait internet sitelerine tıpatıp benzeyen sitelere yönlendirirler. Saldırgan tarafından hazırlanmış sahte sitelere giren kurbanlar burada kullanıcı adı, şifre, kredi kartı bilgileri gibi kişisel verilerini girerler ve böylelikle bu bilgileri kötü niyetli kişilerin eline geçmiş olur.[100]

[97] M.Z. Gündüz ve R. Daş, 2017, s.21.
[98] K. Graves, 2010, s. 54
[99] https://tr.wikipedia.org/wiki/Yemleme (05.05.2018)
[100] Hakan Hekim, Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı:2, 2013, s. 139-140.

Yukarıda belirtildiği gibi oltalama senaryoları çok çeşitli olabilir. Örneğin, kurbana bir bankadan, kredi kartı şirketinden veya başka bir finansal kuruluştan geliyormuş gibi görünen bir e-posta gönderilir. E-posta, alıcının bankacılık bilgilerini doğrulamasını veya şifreleri veya PIN'leri sıfırlamasını ister. Kullanıcı, e-postadaki bağlantıyı tıklar ve sahte bir web sitesine yönlendirilir. Hacker daha sonra bu bilgileri yakalayabilir ve maddi kazanç elde etmek veya diğer saldırıları yapmak için kullanabilir. Gönderenin çok miktarda paraya sahip olduğunu ve bu parayı ülke dışına çıkarmak için yardımınıza ihtiyacı olduğunu söyleyen e-postalar kimlik avı saldırılarına örnek olarak verilebilir. Bu saldırılar, banka hesap erişim kodlarını veya diğer gizli bilgilerin bilgisayar korsanının eline geçmesini amaçlamaktadır.[101]

Oltalama suçlarının tespit ve takibi bir kısım zorlukları beraberinde getirmektedir. Öncelikle kurbanlar kimlik hırsızlığının farkına varmakta çok geç kalmaktadırlar. Saldırganlar ise takipten kurtulmak için hazırladıkları sahte web sitelerini belli bir süre sonra iptal etmekte veya başka bir sunucu üzerine taşımaktadırlar. Ayrıca bu sahte web siteleri genellikle başka ülkelerde bulunan sunucular üzerinde bulunmakta ve hatta çoğu zaman sunucunun sahibi de böyle bir sitenin varlığından habersiz olabilmektedir.[102]

Sazan avlama saldırısı yapmak için gönderilen bu tür e-postalara karşı kullanıcılar bilinçli ve uyanık olmalıdır. Sazan avlamak isteyen kişilerin attıkları oltaya yem olunmamalı ve hiç bir şekilde kişisel bilgileri bu yolla isteyen mesajların söyledikleri yapılmamalıdır. Sazan avlamaya yönelik e-postalar, ilgili bankalara gönderilerek bankaların gerekli tedbirleri alması ve diğer müşterilerini bilinçlendirmesi sağlanmalıdır.[103]

[101] K. Graves, 2010, s. 52
[102] Hakan Hekim, Oğuzhan Başıbüyük, 2013, s. 139-140
[103] G. Canbek ve Ş. Sağıroğlu, 2007, s. 130-131.

Teknik bir önlem olarak, bu tip saldırılardan korunmak için, e-posta sunucusunun önüne konumlandırılmış olan ve kötü niyetli gönderileri tespit edebilecek e-posta güvenlik cihazı (e-mail security gateway) kullanılmalıdır.[104]

2.2.13 Oturum Çalma (Session Hijacking)

Oturum çalma, kullanıcı bir sunucuyla başarılı kimlik doğrulamasını yaptıktan sonra bir bilgisayar korsanının bu kullanıcı oturumunun kontrolünü ele geçirmesiyle ortaya çıkar. Oturum çalma, bir istemci / sunucu iletişiminin geçerli oturum kimliklerini tanımlayan sıra numarasını tahmin eden araçlar tarafından gerçekleştirilebilir. Bu tip saldırılar, saldırıyı gerçekleştirmek için aktif olarak başka bir kullanıcıyı çevrimdışı duruma getirmeyi içerir.[105]

Oturum çalma, saldırıyı devam ettirmek için aşağıdaki üç adımı içerir:

- **Oturumun İzlenmesi**: Bilgisayar korsanı açık bir oturumu tanımlar ve bir sonraki paketin sıra numarasını öngörür.
- **Bağlantının Eş Zamanlılığının Bozulması**: Bilgisayar korsanı, geçerli kullanıcının sistemine oturumunu kapatmasına neden olacak şekilde bir TCP sıfırlama (RST) veya bitiş (FIN) paketi gönderir.
- **Saldırganın Paketini Enjekte Etmek**: Bilgisayar korsanı, sunucuya tahmini sıra numarası olan bir TCP paketi gönderir ve sunucu bunu geçerli kullanıcının bir sonraki paketiymiş gibi kabul eder.[106]

Oturum çalmak için saldırganlar çeşitli teknikler kullanmaktadır. Aşağıda bu teknikler maddeler halinde sıralanmıştır.

[104] Özgü Can, M. Fatih Akbaş, 2014, s.25
[105] K. Graves, 2017, s.183
[106] a.g.e, s. 183.

- **Çalma:** HTTP yönlendirici başlığı kullanarak, ağ trafiğini dinleyerek, siteler arası betik çalıştırma saldırılarını kullanarak, istemci makinalara Truva atı göndererek bu teknik gerçekleştirilir.
- **Tahmin Etme**: Saldırgan oturum kimliklerinin değişik kısımlarını gözlemleyerek oturum kimliğini tahmin etmeye çalışır.
- **Kaba Kuvvet Saldırıları:** Saldırgan oturumu çalana kadar değişik kimlikleri dener.[107]

Oturum çalma olayını önlemek için uygulanacak önlemlerin listesi aşağıda maddeler halinde sıralanmaktadır. [108]

- Şifreleme kullanılmalıdır.
- Güvenli bir protokol kullanılmalıdır.
- Gelen bağlantılar sınırlanmalıdır.
- Uzaktan erişim en düşük düzeye indirilmelidir.
- Güçlü bir kimlik doğrulama yapılmalıdır.
- Çalışanları eğitilmelidir.
- Farklı hesaplar için farklı kullanıcı adları kullanılmalı ve şifreler korunmalıdır.
- Oturum çalma saldırılarını önlemek için hub yerine Ethernet anahtarları kullanılmalıdır.

2.2.14 SQL Enjeksiyonu

SQL ifadeleri bir veri tabanı üzerinde veri oluşturma, okuma, değiştirme ve bulma gibi temel işlemlerin belirli sorgu komutlarıyla istemciler tarafından yapılmasını sağlar. Günümüzde SQL dilinin pek çok çeşidi olmasına rağmen temel komutlar (Select, Update, Delete, Insert, Drop, Union, vb.) hepsinde aynıdır. SQL enjeksiyonu yöntemi, kullanıcı girdilerine göre SQL cümleleri oluşturan web

[107] https://www.slideshare.net/teknetir/cehv9-module-10-session-hijacking (31.03.2018)
[108] K. Graves, 2017, s.187

sitelerinde, kullanıcı kaynaklı girdilerin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin manipüle edilmesini sağlayan saldırı yöntemleridir. SQL enjeksiyonu, bir saldırganın veritabanı içeriğine erişmesini sağlayabilir veya bilgisayar korsanının uzaktan sistem komutlarını çalıştırmasına izin verebilir.[109]

SQL enjeksiyonu yöntemiyle veritabanları üzerinde yapılabilecek saldırılardan bazıları aşağıda maddeler halinde sıralanmıştır.

- Veritabanları üzerinde istenmeyen işlemler (sorgulama, ekleme, silme, değiştirme, vb.) yapılabilir.
- Kimlik doğrulama mekanizmaları atlatılabilir.
- İşletim sistemi seviyesinde komutlar çalıştırılabilir.
- Yeni kullanıcılar veya gruplar oluşturulabilir.[110]

SQL enjeksiyonu ataklarının etkileri çok büyük çaplarda olabilmektedir. Aşağıda dünyadan bazı olaylar rakamlarla birlikte maddeler halinde sıralanmıştır.

- 2014 yılında kamuya açıklanan yazılım paketlerinde tespit edilen SQL enjeksiyonundaki zayıf noktaların belirgin bir şekilde arttığına tanık olundu.
- 1 milyon Wordpress web sitesi SQL enjeksiyonuna karşı savunmasız durumda.
- Çevrimiçi alışveriş mağazası Mapp bilgisayar korsanlarının bazı müşteri bilgilerini çaldığını müşterilerine bildirdi. Bu kapsamda 157.000 e-posta adresi ve şifrelenmiş parolalar SQL enjeksiyonu saldırısıyla çalınmış oldu.[111]

SQL enjeksiyonu, hata tabanlı sql enjeksiyonu ve kör sql enjeksiyonu olmak üzere iki türe ayrılır.

---

[109] Yılmaz Vural, Şeref Sağıroğlu, "Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri", *Politeknik Dergisi*, Cilt 13, Sayı: 2, 2010, s.76.
[110] a.g.e, s.76.
[111] https://www.slideshare.net/teknetir/cehv9-module-13-sql- injection (31.03.2018)

Hata tabanlı sql enjeksiyonunda, uygulama hataya zorlanır ve hata mesajı yakalandığı takdirde SQL enjeksiyonu açıklığının varlığı belirlenmiş olur. Union ve Double olmak üzere iki alt çeşidi vardır. [112]

Kör SQL Enjeksiyonu adında anlaşılacağı üzere kör atış sql saldırılarıdır. Veritabanından direkt olarak bir tablo ya da kolana ait bilgilere veya veritabanına ait teknik bilgilere ulaşılamaz ancak istenilen bilgiler harf harf denendiği takdirde doğru sonuçlara ulaşılacaktır. Bu sebepten ötürü el ile yapılması uğraştırıcı olup bu açıklık tespit edildiği takdirde otomatize programlar ile açıklık suistimal edilmektedir. Kör SQL Enjeksiyonu, Boolean ve ZamanTabanlı olarak ikiye ayrılmaktadır.[113]

SQL enjeksiyonu saldırılarından korunmak için alınması gereken önlemler aşağıda maddeler halinde sıralanmıştır.

- Uygulama tarafından alınan verilerin boyutu, türü veya içeriği hakkında hiçbir varsayım yapılmamalıdır.
- Girdi boyutu ve veri türü test edilmelidir ve arabellek taşmalarını önlemek için uygun sınırlar uygulanmalıdır.
- String değişkenlerinin içeriği test edilmelidir ve yalnızca istisnai değerleri kabul edilmelidir.
- İkili veri, kaçış dizileri ve yorum karakterleri içeren girdiler reddedilmelidir.
- Kullanıcı girdisinden doğrudan Transact-SQL deyimleri oluşturulmamalıdır ve kullanıcı girdisini doğrulamak için saklı yordamlar(stored procedure)[114] kullanılmalıdır.
- Birden çok doğrulama katmanı uygulanmalıdır ve doğrulanmamış kullanıcı girdisi hiçbir zaman birleştirilmemelidir.[115]

[112] http://www.lifeoverpentest.com/2016/04/sql-injection-turleri-ve-login-bypass.html (04.06.2018)
[113] a.g.e
[114] Stored Procedure: Herhangi bir fonksiyonu yerine getirmek için kullanılan kodların bir paket haline getirilmesidir. Özelliği ise birçok defa yaptığımız işlemler neticesinde o işlemleri bir defa yazarak birçok defa tekrardan kullanabilmemizi sağlayan bir fonksiyondur. Bu fonksiyonun çalışma şekli ise oluşturdugumuz kodların bir paket haline getirdikten sonra kullanılan program ile birlikte bir komut vasıtası ile ulaşabilmemizi sağlar.
[115] https://www.slideshare.net/teknetir/cehv9-module-13-sql- injection, s.88

2.2.15 Siteler Arası Betik Çalıştırma (XSS)

Siteler arası betik çalıştırma (XSS), günümüzde web uygulamalarında daha yaygın olan bir güvenlik açığıdır, ancak çoğu zaman basit bir JavaScript pop-up penceresinden daha fazla önem verilmez. Bir web sitesi ziyaret edildiğinde, web tarayıcısı bu web sitesiyle bir güven ilişkisi geliştirir. Tarayıcı, web sitesi istendiği için uygulamanın yanıtına güvenmesi gerektiğini varsayar. Bu güven ilişkisi, tam özellikli bir web tarama deneyimi sağlamak için uygulama tarafından gelen resimlerin, belgelerin, komut dosyalarının ve diğer kaynakların, tarayıcı tarafından kabul edilmesine izin verir. Bu ilişki, % 99,9 oranda olumsuz sonuçlara yol açmadan çalışır, ancak uygulama XSS'e karşı savunmasız olduğunda işler kötüye gider.[116]

Bir uygulama XSS'ye karşı savunmasız ise, bir bilgisayar korsanı genellikle kötü amaçlı komut dosyası içeren ve bu URL'yi meşru bir kullanıcıya aktaran bir URL isteği oluşturabilir. Örneğin, kurbanın tarayıcısı http://www.auctionsite.com(bir açık arttırma sitesi) adresine güvenir çünkü kullanıcı bu URL'ye bir istekte bulunur, ancak http://www.l33thacker.net adresine güvenmez, çünkü hiçbir kullanıcı bu siteyi isteyerek ziyaret etmez. Saldırgan, açık artırma sitesinin web uygulamasında bir yerde bir XSS güvenlik açığı bulmalı, böylece kullanıcı tarafından bağlantı tıklandığında, betik açık artırma sitesine gönderilecek ve yanıtta geri gönderilecektir (böylece kullanıcının tarayıcısı buna güvenecektir) ve çalıştırılacaktır. Bu, hacker'ın kullanıcıya gönderilen uygulamanın yanıtına kötü amaçlı komut dosyası eklemesine izin verir. Bu şekilde kurbanın oturum bilgilerini tanımlayan çerez bilgileri ele geçirilir, kullanıcı başka adreslere yönlendirilebilir.[117]

Siteler arası betik çalıştırma (XSS) saldırıları iki farklı türde gerçekleştirilir. Yansıtılmış (Reflected) XSS atağında, saldırgan kurbana kötü amaçla oluşturulmuş link yollar. Kurban kötü amaçlı linke tıklar. Sunucu enjekte olmuş HTML yollar.

[116] Josh Pauli, *The Basics of Web Hacking: Tools and Techniques to Attack the Web*, Elsevier, Waltham, USA, 2013, s.106

[117] Gökhan Muharremoğlu, *Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı Ve Savunma Öğelerinin İncelenmesi,* İstanbul Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2013, s.85-86

Depolanmış (Stored) XSS atağında, kötü amaçla oluşturulmuş istek gönderilir ve sunucuda tutulur. Kurban sunucuya normal istek mesajı gönderir. Sunucudan enjekte olmuş HTML sayfası gelir.[118]

XSS saldırılarından korunmak için uygulanması gereken önlemler aşağıda maddeler halinde sıralanmaktadır. [119]

- Tüm başlıklar, çerezler, sorgu dizeleri, form alanları (diğer bir deyişle, tüm parametreler) titiz bir spesifikasyona göre doğrulanmalıdır.
- Kötü niyetli komut dosyalarının yürütülmesini engellemek için bir web uygulama güvenlik duvarı kullanılmalıdır.
- Girdi ve çıktı şifrelenmelidir, girişteki tanımlayıcı karakterler filtrelenmelidir.
- Komut dosyası çıktısını filtrelemek, XSS güvenlik açıklarını kullanıcılara bulaşmasını engelleyerek de ortadan kaldırabilir.
- Kullanıma başlamadan önce uygulamadaki XSS açıklarını gidermek için tasarım aşamasında kapsamlı olarak test araçları kullanılmalıdır.
- Kullanıcı girdisini arama motorlarında ve forumlarda görüntülemeden önce, alfa-sayısal olmayan karakterler HTML karakteri varlıklarına dönüştürülmelidir.
- XSS söz konusu olduğunda HTTPS kullanan web sitelerine her zaman güvenilmemelidir.
- Girilen betiğin gerçekten kimliği doğrulandığını kontrol etmek için özel ve genel anahtarlarla birlikte bazı standart veya imzalama betikleri geliştirilmelidir.

[118] https://www.slideshare.net/ahmedfawzyvip2/hacking-web-applications-cehv8-module-13 (01.04.2018)
[119] https://www.slideshare.net/teknetir/cehv9-module-12-hacking-web-applications (01.04.2018)

2.2.16. Fidye Yazılım (Ransomware)

Son yılların popüler tehditlerinden biri haline gelen fidye yazılım, bilgisayar sisteminin dosya ve klasörlerine erişimi kısıtlayan ve kısıtlamayı kaldırmak için bu kötücül yazılımın yaratıcı(lar)sına çevrimiçi bir fidye ödenmesini talep eden bir kötücül yazılım türüdür.[120]

Fidye yazılımların yayılma yöntemleri aşağıdaki gibidir: [121]

- Çeşitli firmalara ait sahte e-postalara içerisine eklenmiş faturalara ait eklerin veya linklerin tıklanması yoluyla,
- Bilinmeyen kaynaklardan indirilen oyun, film, müzik dosyaları ile,
- Çevrimiçi film, dizi izleme platformlarında çalıştırılan flash/java eklentileriyle,
- Web tarayıcı eklentileriyle,
- Çeşitli blog ve haber portalları yoluyla.

En bilinen fidye yazılımlarından olan CryptoLocker Türkiye'de son dönemlerde genellikle e-fatura içeren sahte e-postalar yoluyla yayılmaktadır. Kullanıcı, "*.zip" uzantılı dosyayı açıp içindeki e-fatura olarak görünen dosyaya tıkladığında bu zararlı yazılım tüm dokümanları virüs tarafından güçlü şifreleme algoritmaları (AES-256 vb.) ile şifrelenmektedir.[122]

2017 yılına damgasını vuran ve dünya genelinde çeşitli ülkelerde sistemlere zarar veren WannaCry ve Petya gibi fidye yazılımları, oltalama e-postalarını kullanmalarına ek olarak işletim sistemindeki güvenlik açıklarından faydalandılar.[123]

---

[120] https://www.slideshare.net/teknetir/cehv9-module-06-malware-threats (17.03.2018)
[121] İrfan Kotman, "Son Yılların En Etkili Tehditleri Fidye Yazılımları (Ransomware)", *Beyaz Şapka Dergisi*, Sayı: 2, 2016, s. 8-9.
[122] http://www.udhb.gov.tr/images/duyurular/74bc0128f065b41.pdf (03.05.2018)
[123] CyberMag, "BTK-USOM'dan Petya Zararlı Yazılımı Açıklması", *CyberMag Dergisi*, Sayı:19, 2017, s. 32.

Fidye yazılımlarından korunmak için yapılması gerekenler aşağıda maddeler halinde sıralanmıştır. [124]

- Kritik veriler düzenli olarak yedeklenmelidir
- Güvenlik yamaları düzenli bir şekilde uygulanmalıdır.
- Güncel bir anti-virüs uygulaması kullanılmalıdır.
- Kullanıcıların fidye yazılımlarının bulaşma yöntemleri hakkında bilgilendirilmelidir.

[124] İrfan Kotman, 2016, s.9

ÜÇÜNCÜ BÖLÜM

KURUMSAL BİLGİ GÜVENLİĞİNİN SAĞLANMASI

Bu tezin ikinci bölümünde anlatılan siber tehdit ve saldırılar karşısında kurumsal bilgi güvenliğinin sağlanmasının önemli gerekçeleri aşağıda maddeler halinde sıralanmıştır. [125]

- Güvenlikle ilgili tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması ve kurumsal itibarın korunması,
- İş sürekliliğinin sağlanması,
- Bilgi kaynaklarına erişimin denetlenmesi,
- Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi,
- Bilgi varlıklarının gizliliğinin, bütünlüğünün ve doğruluğunun sağlanması,
- Kurumsal bilgi varlıklarının kötü amaçlı olarak kullanılmasının ve/veya suistimal edilmesinin engellenmesi,
- Bilgilerin güvenli bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanması,
- Bilgi sistemlerini kullanan kişilerin umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suistimal etme gibi nedenlerden dolayı oluşabilecek donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızalara karşı korunmasıdır.

Kurumsal bilgi güvenliğinin sağlanmasında alınması gereken teknik önlemlerin (örneğin güvenlik donanım ve yazılım ürünleri) yanında yasal mevzuatın

[125] Yılmaz Vural ve Şeref Sağıroğlu, "Kurumsal Bilgi Güvenliği: Güncel Gelişmeler", *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı*, Ankara, 2007, s.192.

ve standartların kurum bünyesinde uygulanması gerekmektedir. Bu kapsamda güvenliğin temel prensipleri iyi anlaşılmalı ve güvenliğin sağlanmasının bir süreç meselesi olduğu kavranmalıdır.

3.1 GÜVENLİK PRENSİPLERİ

Bilginin güvenliğinin sağlanması için üç temel unsur olan gizliliğin, bütünlüğün ve erişebilirliğin korunması gerekmektedir. Bunlara ek olarak kimlik doğrulama, inkâr edememe, izlenebilirlik ve güvenilirlik prensiplerinden bahsedilebilir.

Kurumların ihtiyaçları doğrultusunda yukarıda bahsedilen prensiplerin bazıları diğerlerine nispeten ön plana alınabilir. Örneğin askeri kurumlarda gizlilik ve bütünlük prensiplerine daha fazla önem verilmektedir. Bunun nedeni düşmanların kriritik bilgilere ulaşmasını (gizlilik) ve değiştirmesini (bütünlük) engellemektir. Kâr amacı gütmeyen kurumlarda genellikle erişilebilirlik ve bütünlük unsurları ön planda gelmektedir. Üniversite sınav sonuçlarının açıklandığı yükseköğretim kurumunda öğrenciler sınav açıklandıktan sonra istediği zaman diliminde (erişilebilirlik) doğru bir şekilde (bütünlük) sınav sonuçlarına bakabilmelidir. Kar amacı güden çevrimiçi alışveriş mağazaları için en önemli unsurun erişebilirlik olduğu açıktır çünkü siteye ulaşılamadığı her an gelir kaybıyla eşdeğerdir.[126]

Güvenlik prensipleri arasındaki ilişki birbirini olumsuz yönde etkileyebilir. Bilginin gizliliğini veya bütünlüğünü geliştirmeye yönelik alınacak tedbirler erişilebilirliği ters yönde etkilemekte, erişilebilirliğin geliştirilmesiyse gizlilik ve bütünlüğü tehlikeye atabilmektedir.[127]

[126] Muhammet Baykara, Resul Daş, ve İsmail Karadoğan, "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", *1st International Symposium on Digital Forensics and Security*, Elazığ, 2013, s.238

[127] Hakan Hekim, Oğuzhan Başıbüyük, 2013, s.137

3.1.1 Gizlilik (Confidentiality)

Gizlilik, 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre "bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliği" olarak tanımlanır. [128]

Ulusal Siber Olaylara Müdahale Merkezi ise gizliliği "bilişim sistem ve verilerine sadece yetkili kişi veya sistemlerce erişilebilmesini; bilişim sistemlerine ait veya sistemdeki gizli verinin yetkisiz kişi veya sistemlerce ifşa edilmemesi" olarak tanımlar.[129]

Gizliliği sağlamak için kurumlarda yapılması gereken ilk şey hassas ve gizli bilgilerin asla teminatsız ve gözetimsiz bırakılmaması için gerekli prosedürleri oluşturmaktır. Bunu başarmak için, her organizasyonun yapması gereken ilk şeylerden biri, bu bilgilerle temas eden her çalışanın gizliliğini korumak için sahip olduğu ilave sorumluluğu anladığından emin olmaktır. Veriler iletilirken ele geçirilmesine karşı alınabilecek en temel önlem güçlü şifreleme teknikleridir. Bu şekilde veriler ele geçirilse bile okunamadığından ötürü gizlilik korunmuş olur.[130]

3.1.2 Bütünlük (Integrity)

Bütünlük, tüm yaşam döngüsü boyunca verilerin tutarlılığını, doğruluğunu ve güvenilirliğini korumayı içerir.[131] Verinin yetkilendirilmemiş bir şekilde değişiminin veya verinin bir şekilde bozulması, değiştirilmesi ya da silinmesi gibi durumların engellenmesi amaçlanmaktadır.[132]

---

[128] Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2016, s.7
[129] Ulusal Siber Olaylara Müdahale Merkezi, 2014, s.6
[130] Bradley A. Wayland, 2014, s.148
[131] Guillaume Collard, Stéphane Ducroquet, Eric Disson, ve Guilaine Talens, "A definition of Information Security Classification in cybersecurity context", *11th International Conference on Research Challenges in Information Science*, Brighton, 2017, s.80
[132] Özgü Can, M. Fatih Akbaş, 2014, s.17

TS 13268-1'e göre bütünlük "Saklanan, işleme tabi tutulan ya da aktarılan bilginin doğru ve eksiksiz olmasının; doğru bir biçimde işleme tabi tutulduğunun ve yetkisiz kişilerce herhangi bir şekilde değiştirilmediğinin teyit edilmesidir. Ayrıca kuruluş, olmasını tasarladığı ağ şebekelerinin ve bilgi sistemlerinin bütünlüğünü tesis etmeyi de isteyebilir".[133]

Bütünlük, bilgilerin iletim sırasında, diğer verilerle bütünleşme sırasında veya verilerin gönderildiği diğer durumlarda değişmeden kalması gerektiği anlamına gelir. Veri bütünlüğü kavramı, önemi ile birlikte, aşağıdaki varsayımsal örnekle gösterilebilir. Bir hasta tedavi altındadır ve doktoru tarafından günlük 10 mg ilaç verilmektedir. Bu hastane, bilgisayar sistemi üzerindeki bu bilgiyi korursa doktor hastanın elektronik tıbbi kaydına doğru dozu ve ilacı gösterir. Hastanenin bilgi sisteminin bütünlüğü zayıf ise ve programda elektronik kaydı ileten bir aksaklık, dozaj miktarına bir 0 ekler, böylece hastanın dozu artık 100 mg olur. İlaç dozajının kritik niteliği ile, hastanenin bilgi sistemi içindeki bütünlük eksikliği, bu durum için ölümcül sonuçlara yol açabilir. Bu olayın kendi bilgi sisteminizde meydana gelmesini engellemek ve verilerin iletim ve depolama sırasında doğru şekilde korunmasını sağlamak için, veri bütünlüğü, herhangi bir bilgi güvenliği programının kritik bir bileşeni olmalıdır.[134]

3.1.3 Kullanılabilirlik (Availability)

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne göre "Kullanılabilirlik, bilginin her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun ya da problem çıkması durumunda bile bilginin erişilebilir olması kullanılabilirlik özelliğinin bir gereğidir. Bu erişim kullanıcının hakları çerçevesinde

[133] Türk Standartları Enstitüsü, *TS 13268-1:TS ISO/IEC 27001'E Göre Bilgi Güvenliği Yönetim Sistemi (BGYS) Belgelendirmesi İçin Gereksinimler Ve Hazırlık Kılavuzu*, TSE, Ankara, 2007, s.3
[134] Bradley A. Wayland, 2014, s.149

olmalıdır. Kullanılabilirlik ilkesince her kullanıcı erişim hakkının bulunduğu bilgi kaynağına, yetkili olduğu zaman diliminde mutlaka erişebilmelidir".[135]

Kullanılabilirlik, bilgi sistemlerinin çalışır durumda olduğu süreye ve sistemde yer alan verilerin kullanım için uygunluğuna ilişkindir. Diğer bir deyişle, kullanılabilirlik, kurumun bilgi sisteminin doğru politikalar sınırları içinde doğru kişilere doğru verileri ve bilgileri sunma yeteneğini açıklar.[136]

Kurumdaki verilerin kullanılabilir olmasını sağlamak ve genel bilgi sistemini çalışır durumda tutmak için bazı güvenlik önlemleri alınmalıdır. Veri bütünlüğünde olduğu gibi, uygun donanımı sağlamak ve bu donanımın düzgün bir şekilde bakımını sağlamak, bilgilerinizin mevcut olduğundan emin olmanıza yardımcı olacaktır. Acil bir durumda, kurumdaki kritik bileşenler için yedekli sistemler sağlanmalıdır. Ayrıca, kurumdaki bilgi sistemlerini çalıştırmak için gerekli olan bant genişliği değerlendirilmeli ve bunun her zaman için yeterli bir şekilde sağlandığından emin olunmalıdır. Son olarak, bilgi sistemini bilgisayar korsanları veya diğer potansiyel failler tarafından olası saldırılara karşı koruyacak donanım ve yazılım çözümleri sağlanmalıdır. [137]

3.1.4 Kimlik Doğrulama (Authentication)

Canbek ve Sağıroğlu kimlik doğrulamayı "geçerli kullanıcı ve işlemlerin tanınması ve doğrulanması ile bir kullanıcının veya işlemin hangi sistem kaynaklarına erişme hakkının olduğunun belirlenmesi süreci" olarak tanımlar.[138]

[135] Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, *Bilgi Güvenliği Yönetim Sistemi Kurulumu,* TÜBİTAK – UEKAE, Ankara, 2007, s. 6-7.
[136] Bradley A. Wayland, 2014, s. 153.
[137] a.g.e, s. 158.
[138] Gürol Canbek, Şeref Sağıroğlu, 2006, s.170

Kimlik doğrulama; bilgi sisteminin herhangi bir yerine erişmek isteyen kişinin gerçekten iddia ettiği kişi olduğunu anlama mekanizmalarını içerir. Kullanıcıların kurum bilgisayarlarına girerken kullandıkları kullanıcı adı ve şifre bir kimlik doğrulama mekanizmasıdır.[139] Günümüzde bu şekildeki tek faktörlü kimlik doğrulama yerine şifre girildiğinde cep telefonuna gelen tek kullanımlık ikinci bir şifrenin girilmesi suretiyle gerçekleştirilen iki faktörlü kimlik doğrulama yöntemi yaygınlaşmaktadır.

3.1.5 İnkar Edememe (Non-Repudiation)

UEKAE, inkâr edememe özelliğinden şu şekilde bahseder: "Bilgiyi gönderenin gönderdiğini, alanın da aldığını inkâr edememesi sistemin izlenebilirliği açısından önemlidir".[140]

Dijital imzalar inkâr edememe özelliğine iyi bir örnek olabilir. Bu imzalarla mesajın içeriğindeki değişikliklerin algılanması ve mesajın beklenen taraftan meşru bir şekilde gönderilmesi sağlanır. En önemlisi gönderenin gönderdiği mesajın kendisi tarafından gönderildiğini inkâr etmesinin önüne geçilmiş olur.[141]

3.1.6 İzlenebilirlik (Accountability)

İzlenebilirlik, bir bilgi sistemindeki faaliyetlerin takibi ve ihtiyaç duyulduğunda daha sonra da izlenebilmesi için kaydedilmesidir. Bu faaliyetler bir web sayfasına girmek veya bir sunucuya erişmek gibi faaliyetler olabilir.

---

[139] Özgü Can, M. Fatih Akbaş, 2014, s.17-18
[140] Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, *BGYS - Risk Yönetim Süreci Klavuzu*, UEKAE, Ankara, 2007, s.18
[141] Jason Andress, 2014, s.80

İzlenebilirlik; kimlik belirleme, kimlik doğrulama ve erişim denetiminin varlığına bağlıdır. Böylece, belirli bir işlemin kiminle ilişkilendirildiği ve bunların yürütülmeleri için hangi izinlerin kullanıldığı öğrenilebilir. Doğru izleme ve kayıt tutma (logging) yapıldığında çok kısa bir sürede söz konusu durumun ayrıntıları belirlenebilir.[142]

3.1.7 Güvenilirlik (Reliability)

Canbek ve Sağıroğlu güvenilirliği şu şekilde tanımlar: "Güvenilirlik bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilme yeteneğidir".[143]

3.2 BİLGİ GÜVENLİĞİ İLE İLGİLİ MEVZUAT

İnternet ortamı bilgiye erişim kolaylığı sağlamakla birlikte aynı zamanda günlük hayattaki işlerin pratik bir şekilde yapılmasına olanak sağlamıştır. Ancak internetin getirdiği kolaylıkların yanı sıra birçok güvenlik problemine yol açtığı görülmektedir. Bu noktadan yola çıkarak internet ortamının bazı güvenlik kurallarına tabi olması kaçınılmaz hale gelmiştir. Bu güvenlik önlemleri ve bu önlemlerin alınmaması durumunda ortaya çıkacak cezai yaptırımlar devlet tarafından düzenlenmiştir. Bu bölümde bilgi güvenliği ile ilgili mevzuata değinilmiştir.

[142] a.g.e, s.59.
[143] Gürol Canbek, Şeref Sağıroğlu, 2006, s.170.

3.2.1 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Kanunu

23.05.2007 tarihinde yürürlüğe giren bu kanunun amacı internet ortamında işlenen belirli suçlarla mücadeleye ilişkin esas ve usulleri düzenlemektir. Bu kanun aşağıda tarifi yapılan içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcıların yükümlülükleri ve sorumluluklarını kapsamaktadır.

MADDE 2 'de

> "e) Erişim sağlayıcı: Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri,
>
> f) İçerik sağlayıcı: İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri
>
> i) Toplu kullanım sağlayıcı: Kişilere belli bir yerde ve belli bir süre internet ortamı kulla-nım olanağı sağlayanı,
>
> m) Yer sağlayıcı: Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri,"
> j) Trafik bilgisi: Taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini,[144] tarif eder.

Bu kanunun 5. Maddesinin 3. Fıkrasına göre "yer sağlayıcı, yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla" yükümlüdür.[145]

Bu kanunun 6. Maddesinin 1. Fıkrasının (b) bendine göre "erişim sağlayıcı, sağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve

[144] İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, RG: 23.05.2007, 26530, s.1.
[145] a.g.e, s.3.

iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla" yükümlüdür.[146]

İnternet ortamında yapılan yayınlarla ilgili erişimin engellenmesi Madde 8'de düzenlenmiştir. Buna göre yayınlar intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş, kumar oynanması için yer ve imkân sağlama gibi suçları oluşturuyorsa bu yayınlarla ilgili olarak erişimin engellenmesine karar verilir.[147]

Bu kanunun 10. Maddesinin 6. Fıkrasında belirtildiği üzere, Bilgi Teknolojileri ve İletişim Kurumu, "ulusal siber güvenlik faaliyetleri kapsamında, siber saldırıların tespiti ve önlenmesi konusunda, içerik, yer, erişim sağlayıcılar ve ilgili diğer kurum ve kuruluşlarla koordinasyon sağlar, gerekli tedbirlerin aldırılması konusunda faaliyet yürütür ve ihtiyaç duyulan çalışmaları yapar."[148]

3.2.2 5809 Sayılı Elektronik Haberleşme Kanunu

Bu kanunun 5. maddesinin birinci fıkrasının (h) bendinde Ulaştırma ve Altyapı Bakanlığının siber güvenlikle ilgili görev ve yetkilerinden bahsedilmiştir.

> "h) (Ek: 6/2/2014-6518/102 md.) Ulusal siber güvenliğin sağlanması amacıyla politika, strateji ve hedefleri belirlemek, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilere yönelik siber güvenliğin sağlanmasına ilişkin usul ve esasları belirlemek, eylem planlarını hazırlamak, ilgili faaliyetlerin koordinasyonunu sağlamak, kritik altyapılar ile ait oldukları kurumları ve konumları belirlemek, gerekli müdahale merkezlerini kurmak, kurdurmak ve denetlemek, her türlü

[146] İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, RG: 23.05.2007, 26530, s.4.
[147] a.g.e, s.5.
[148] a.g.e, s.12.

siber müdahale aracının ve millî çözümlerin üretilmesi ve geliştirilmesi amacı ile çalışmalar yapmak, yaptırmak ve bunları teşvik etmek ve siber güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek, siber güvenlik alanında faaliyet gösteren gerçek ve tüzel kişilerin uyması gereken usul ve esasları hazırlamak."[149]

Bakanlığın ulusal kamu entegre veri merkezleriyle ilgili ve görev ve yetkileri ise 5. maddenin birinci fıkrasının (ı) bendinde sıralanmıştır.

"ı) (Ek: 27/3/2015-6639/31 md.) Ulusal kamu entegre veri merkezlerine yönelik politika, strateji ve hedefleri belirlemek, eylem planlarını hazırlamak, eylem planlarını izlemek, e-Devlet hizmetlerinde kullanılan verilerin ve sistemlerin barındırıldığı veri merkezlerini kamu entegre veri merkezlerinde toplamak amacıyla verilerin transferi de dahil gerekli altyapıları kurmak, kurdurmak, işletmek, işlettirmek ve tüm bu faaliyetlere yönelik uygulama usul ve esaslarını belirlemek, kurulum, uygulama ve işletim süreçlerini planlamak, yürütmek ve koordine etmek."[150]

Bu kanun kapsamında Bilgi Teknolojileri ve İletişim Kurumuna bilgi güvenliği ve siber güvenlikle ilgili bazı görev ve yetkiler verilmiştir. Kurum, bu kanunun 6. maddesinin birinci fıkrasının (c) bendine göre, "Abone, kullanıcı, tüketici ve son kullanıcıların hakları ile kişisel bilgilerin işlenmesi ve gizliliğinin korunmasına ilişkin gerekli düzenlemeleri ve denetlemeleri yapmak"[151] ile görevli ve yetkilidir. Kurum, 60. Maddenin onbirinci fıkrasına göre, "kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır."[152]

[149] Elektronik Haberleşme Kanunu, RG:10.11.2008, 27050, s.7.
[150] a.g.e, s.7.
[151] a.g.e, s.8.
[152] a.g.e, s.33.

Kişisel verilerin işlenmesi ve gizliliğin korunması ile ilgili konuların düzenlendiği 51. maddenin birinci fıkrası Anayasa Mahkemesi'nin 9/4/2014 tarihli ve E.: 2013/22 K.:2014/74 sayılı kararı ile iptal edilmiştir.[153] Bahsi geçen fıkrada "Kurum, elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirlemeye yetkilidir" ifadesiyle Bilgi Teknolojileri ve İletişim Kurumu yetkilendirilmişti. Anayasa Mahkemesi iptal gerekçelerini şu şekilde ifade etmiştir:

> "Yasama yetkisinin devredilemezliği ilkesi gereğince, Anayasa'nın açıkça kanunla düzenlenmesini öngördüğü konularda yürütme organına doğrudan ve ilk elden düzenleyici işlem yapma yetkisi verilemez. Elektronik haberleşme sektörüyle ilgili kişisel verilerin işlenmesi ve gizliliğinin korunmasına yönelik usul ve esasları belirleme yetkisini Bilgi Teknolojileri ve İletişim Kurumuna veren itiraz konusu kural, Anayasa'nın 20. maddesinde öngörülen kişisel verilerin korunmasına ilişkin usul ve esasların ancak kanunla düzenlenebileceğine ilişkin güvenceye aykırıdır."[154]

Elektronik Haberleşme Kanununa dayanılarak hazırlanan yönetmeliklerden aşağıda bölüm 3.2.3 ve 3.2.4 'te bahsedilmiştir.

3.2.3 Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği

Resmi Gazete'de 13.07.2014 tarihinde yayınlanan Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği, 5809 sayılı Elektronik Haberleşme Kanununun 4 üncü maddesinin birinci fıkrasının (l) bendi, 6. maddesinin birinci fıkrasının (n), (ş) ve (v) bentlerine, 12 nci maddesinin ikinci fıkrasının (i) ve (j) bentlerine ve 60 ıncı maddesinin birinci fıkrasına dayanılarak hazırlanmıştır. Bu

[153] Elektronik Haberleşme Kanunu, RG:10.11.2008, 27050, s.28.
[154] http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/94117278-50ca-4203-88f3-72a5537258a5?excludeGerekce=True&wordsOnly=False

yönetmelik bilgi güvenliğinin sağlanması için kurumların uyması gereken kuralları kapsamaktadır.

Bu yönetmeliğin 3. maddesi olan tanımlar kısmında uluslararası güvenlik standartları, bu standartların oluşturduğu BGYS, bu sistemin ortaya koyduğu temel prensipler tanımlanmıştır. Buna ilaveten ilişkili kurumlar ve kurullar, koordineli çalışılması gereken USOM, kurum bünyesinde kurulacak olan SOME tanımlanmıştır.

Üçüncü bölümde ise bilgi güvenliğinin sağlanmasına ilişkin temel yükümlülükler anlatılmıştır. Bu kapsamda BGYS'nin kurulması, politikası, bilgi güvenliği grubu ve faaliyetleri, varlık yönetimi sınıflandırması, risk değerlendirme ve işleme, iş sürekliliği gibi konularda açıklamalar yapılmıştır. Ayrıca bilgi güvenliği ihlal olaylarının ve güvenlik açıklarının yönetimi, İç denetim, personel ve istihdam, eğitim, fiziksel erişim, zararlı kodlara karşı korunma, sistem kayıt dosyalarının tutulması, erişim yönetimi, erişim yönetimi gibi konularda da açıklamalar yapılmıştır.

Dördüncü bölümde siber saldırılara yönelik tedbirler, belgelendirme yükümlülüğü, rapor hazırlama yükümlülüğü, ihlallerin bildirilmesi yükümlülüğü, felaket kurtarma merkezi konuları açıklanmıştır.[155]

Bu yönetmelik bahsettiği konularla kurumsal bilgi güvenliğinin sağlanması için alınması gereken idari ve teknik önlemlerin çerçevesini çizmiş olup gerek kurum içi gerekse kurumlar arası yapılanmayı tarif etmiş olmaktadır.

[155] Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği, RG:13.07.2014, 29059

3.2.4 Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik

Bu Yönetmelik 5809 sayılı Elektronik Haberleşme Kanununun 4, 6, 12 ve 51 inci maddelerine dayanılarak hazırlanmıştır. Yönetmeliğin amacı kişisel verilerin işlenmesi, saklanması ve gizliliğinin korunması ile ilgili usul ve esasları düzenlemektir.

Yönetmeliğin birinci bölümünde, MADDE 3'te kişisel verilerle ilgili şu tanımlar yapılmıştır:

"MADDE 3

h) Kişisel veri: Belirli veya kimliği belirlenebilir gerçek ve tüzel kişilere ilişkin bütün bilgiler

ı) Kişisel veri ihlali: İstem dışı, yetki dışı ya da yasa dışı olarak; kişisel verilerin tahrip edilmesine, kaybolmasına, iletilmesine, değiştirilmesine, depolanmasına veya başka birortama kaydedilmesine, işlenmesine, ifşa edilmesine ve söz konusu verilere erişilmesine neden olan güvenlik ihlalini,

i) Kişisel verilerin işlenmesi: Kişisel verilerin otomatik olan veya olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, değiştirilmesi, silinmesi veya yok edilmesi, yeniden düzenlenmesi, açıklanması veya başka bir şekilde elde edilebilir hale getirilmesi, üçüncü kişilere aktarılması, kullanılmasının sınırlanması amacıyla işaretlenmesi, tasniflenmesi veya kullanılmasının engellenmesi gibi bu veriler üzerinde gerçekleştirilen işlem ya da işlemler bütününü,

ö) Rıza: İlgili kişinin kendisine ait kişisel verisinin işlenmesine yönelik, verinin işlenme amaç ve kapsamı dâhilinde, verinin işlenmesi öncesinde özgür iradesiyle verdiği ispatlanabilir kabul beyanını,"[156] ifade eder.

[156] Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik, RG: 24.07.2012, 28363

İkinci bölümde kişisel verilerin işlenmesine ilişkin ilkeler, kişisel verilerin güvenliğinin sağlanması ile ilgili yükümlükler, riskin ve kişisel veri ihlalinin bildirilmesi gibi konulardan bahsedilmiştir.[157]

Üçüncü bölümde hangi verilerin nasıl işleneceği ve ne kadar saklanacağı ayrıca saklanan bu verilerin güvenliği ile ilgili düzenlemeler getirmektedir.[158]

3.2.5 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Ülkemizde özellikle son zamanlarda kişisel verilerin çok fazla yerde ve kontrolsüz bir şekilde tutulması verilerin ait olduğu kişiler için hak kaybı oluşturmakta ve bu veriler bazı ticari faaliyetlerde kişilerin rızası dışında kullanılmaktadır. Bu kanunla kişisel verilerin korunması amaçlanmaktadır.

Bu kanunda da Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik'te olan kişisel veri, rıza gibi kavramların dışında veri sorumlusu gibi önemli bir tanım yapılmıştır. Bu tanım aşağıdaki gibidir:

"Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder."[159]

Veri sorumlusu olarak tanımlanan rolün görevleri Madde 12' de aşağıdaki gibi sıralanmaktadır:

"MADDE 12- (1) Veri sorumlusu;

[157] a.g.e
[158] a.g.e
[159] 6698 Sayılı Kişisel Verilerin Korunması Kanunu, RG:07.04.2016, 29677, s.2

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak,

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."[160]

Bu kanunda belirtilen hususları yerine getirmek amacıyla idari ve mali özerkliğe sahip Kişisel Verileri Koruma Kurumu kurulmuştur. Bu kurumun görevi uygulamaları ve mevzuattaki gelişmeleri takip etmek, değerlendirme ve önerilerde bulunmak, araştırma ve incelemeler yapmak ve yaptırmaktır. Özerk bir kurum olan KVKK içerisinde yürütme faaliyetlerini gerçekleştirmek üzere Kişisel Verileri Koruma Kurulu oluşturulmuştur.

[160] a.g.e, s.5

3.2.6 Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı bu karara göre siber güvenlikle ilgili alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla Siber Güvenlik Kurulu kurulmuştur.[161] Kurulun görevlerinden bu tezin 3.4.1.3. bölümünde bahsedilmiştir.

Bu karar kapsamında Ulaştırma ve Altyapı Bakanlığı'nın görevleri belirlenmiştir. Bu görevler 5809 Sayılı Elektronik Haberleşme Kanununa eklenmiştir ve bu tezin 3.2.2. bölümünde anlatılmaktadır. Bakanlık bu görevleri BTK ve diğer kamu kurum ve kuruluşları aracılığıyla yerine getirebilir. Kamu düzeninin korunması gibi zorunlu hallerde, ilgili makamların ve Siber Güvenlik Kurulu'nun talebi doğrultusunda bakanlık ulusal siber güvenlikle ilgili tedbirleri alır.[162]

Bakanlık, 26/9/2011 tarihli ve 655 sayılı Ulaştırma ve Altyapı Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 29 uncu maddesinin yedinci fıkrası ve 30 uncu maddesine göre Ulusal Siber Güvenlik ile ilgili çalışma grupları ve kurullar oluşturabilir.[163]

[161] Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, RG:20.10.2012, 28447, s.2.
[162] a.g.e, s.2.
[163] a.g.e, s.2.

3.2.7 703 Sayılı Kanun Hükmünde Kararname İle Gelen Değişiklikler

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın[164] 6. Maddesinde belirtildiği gibi Bakanlık, 26/9/2011 tarihli ve 655 sayılı Ulaştırma ve Altyapı Bakanlığı'nın Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin[165] 29 uncu maddesinin yedinci fıkrası ve 30 uncu maddesine göre Ulusal Siber Güvenlik ile ilgili çalışma grupları ve kurullar oluşturabilmekteydi. 9 Temmuz 2018 tarihli Resmi Gazetede yayımlanan 703 sayılı KHK[166] 'nın 31. Maddesi ile bu maddeler yürürlükten kaldırılmıştır.

703 sayılı KHK'nın 205. maddesi[167] ile Elektronik Haberleşme Kanununda[168] Siber Güvenlik Kurulu ile ilgili Ek Madde 1 kısmındaki birinci ve üçüncü fıkralar yürürlükten kaldırılmıştır. Ek Madde 2 ile "Mevzuatta Siber Güvenlik Kuruluna yapılmış olan atıflar, Cumhurbaşkanınca belirlenen kurul veya mercie yapılmış sayılır." ifadesi kanuna eklenmiştir. Böylece Ulaştırma Bakanı başkanlığında kurulan bu kurul kaldırılmıştır ve 02.08.2018 tarihinde yayımlanan 2018/3 sayılı Cumhurbaşkanlığı genelgesi[169] ile mevzuatta verilen görev ve yetkileri Cumhurbaşkanlığı makamına devredilmiştir.

---

[164] Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, RG:20.10.2012, 28447, s.2.

[165] Ulaştırma, Denizcilik Ve Haberleşme Bakanlığının Teşkilat Ve Görevleri Hakkında Kanun Hükmünde Kararname, RG:01.11.2011, 28102
http://www.resmigazete.gov.tr/eskiler/2011/11/20111101M1-1.htm

[166] Anayasada Yapılan Değişikliklere Uyum Sağlanması Amacıyla Bazı Kanun Ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılması Hakkında Kanun Hükmünde Kararname, RG:09.07.2018, 30473, s.16-17.
http://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3.pdf

[167] a.g.e, s.112-113.

[168] Elektronik Haberleşme Kanunu, RG:10.11.2008, 27050, s.36.

[169] 2018/3 sayılı Cumhurbaşkanlığı genelgesi, RG:02.08.2018, 30497, s.5.
http://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20180802-3.pdf

3.2.8 ISO 27001 Standardı ve Bilgi Güvenliği Yönetim Sistemi

3.2.8.1 ISO 27000 Ailesi ve Tarihsel Gelişimi

ISO/IEC 27000 ailesi, bir bilgi güvenliği yönetim sisteminin uygulanması için oluşturulmuş ve uluslararası kabul görmüş bir standartlar topluluğudur. ISO/IEC 27000 serisi aslında 16 farklı standart ve dokümandır. Bu standartların arasında örneğin ISO/IEC 27799 bir sağlık kuruluşunda bir bilgi güvenliği yönetim sisteminin uygulanması için, ISO/IEC 27011 ise telekomünikasyon kuruluşları içindir.[170]

Bu tezde ise tipine, büyüklüğüne ve doğasına bakılmaksızın bütün kurum ve kuruluşlarda uygulanabilecek olan ve BGYS için gerekliliklerden bahseden ISO/IEC 27001 standardı anlatılacaktır.

Dünyada ve ülkemizde ISO/IEC 27001 bilgi güvenliği standardının tarihsel gelişimi aşağıdaki gibidir: [171]

- Endüstri çalışma grubunun kurulması - 1993
- Kural rehberi olarak yayınlanması (BS 7799 - 1) - 1993
- İngiliz standardı olarak kabul görmesi - 1995
- BS 7799 - 2'nin oluşturulması - 1998
- BS 7799 - 1 ve BS 7799 - 2 bölümlerinin uyumluluğunun gözden geçirilmesi- Mayıs1999
- BS ISO/IEC 17999 (BS7799 - 1:2000) - Geçici versiyon / Ocak - Ağustos 2000
- ISO tarafından yayınlanması - Aralık 2000

[170] Henry Dalziel, *Infosec Management Fundamentals*, Elsevier, Waltham, 2015, s. 4.
[171] Kerem Gencer, *ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım*, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Afyon, 2015, s.5-6.

- İngiltere'de BS ISO/IEC 17799:2000 / BS 7799 - 1: 2000 olarak adlandırılması -2000
- BS 7799 - 2:2002'nin yayınlanması - 5 Eylül 2002
- TS ISO/ IEC 17799' un TSE (Türk Standartları Enstitüsü) tarafından kabulü 11 Kasım 2002
- TS 17799 - 2'nin TSE tarafından kabulü - 17 Şubat 2005
- TS 17799 - 2'nin iptali - 2 Mart 2006 (TS 17999 - 2'nin yerini TS ISO/IEC 27001 aldı.)
- TS ISO/IEC 27001:2005' in TSE tarafından kabulü - 2 Mart 2006
- TS ISO/IEC 27001:2013 olarak TSE tarafından revizyon- 25 Eylül 2013

ISO/IEC 27001:2013, kuruluşun kapsamı dahilinde bilgi güvenliği yönetim sisteminin kurulumunu, yerine getirilmesi ve sürekli geliştirilmesi için gereklilikleri tanımlar. Ayrıca, kuruluşun ihtiyaçlarıyla bağlantılı olan bilgi güvenliği risklerinin değerlendirilmesi ve iyileştirilmesi için gereklilikleri de içermektedir.

ISO/IEC 27001; kurumların risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Kurum tüm bu faaliyetlerinde içinde yer aldığı bir bilgi güvenliği politikası yayımlamalı ve personelini bilgi güvenliği ve tehditler hakkında biliçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımcılığıyla başarılabilir.[172]

[172] Cemile Denerel, 2016, s.20.

3.2.8.2 Bilgi Güvenliği Yönetim Sistemi Kurmanın Faydaları

Bilgi Güvenliği Yönetim Sistemi (BGYS), "Bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası" [173] olarak tanımlanmaktadır.

Bir kurumda Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmanın faydaları aşağıda maddeler halinde sıralanmıştır.

- Kurumun bilgi güvenliğini yönetmesi ve bunun için tehdit ve riskleri belirleyerek etkin bir risk yönetimi sağlaması,
- Bilgi varlıklarının farkına varılması ve bunları ihtiyaca en uygun şekilde koruma altına alarak iş sürekliliğinin ve kurumsal itibarın sağlaması,
- Bilgi varlıklarının gizliliğinin, bütünlüğünün ve doğruluğunun sağlanması,
- Kuruma rekabet avantajı sağlaması ve kurum imajina olumlu etki etmesi, [174]
- Uluslararası temsillerde kurumsal bilgi güvenliğine verdiği önemi ortaya koyması,
- Bilgi kaynaklarına erişimin denetlenerek bilgi sistemleri kaynaklarının kötü amaçlı olarak kullanılmasının ve/veya kaynakların suistimal edilmesinin engellenmesi,
- Personelin, yüklenicilerin ve alt yüklenicilerden kaynaklanan risklerin azaltılması ve bu kişilein güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi,
- Otomatik ve elle yönetilen sistemlerde, duyarlı bilgilerin uygun bir şekilde kullanıldığının garanti altına alınması amacıyla gerçekçi bir kontrol sistemi kurulması,

---

[173] Türk Standartları Enstitüsü, *TS ISO/IEC 27001 Bilgi Teknolojisi- Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler*, TSE, Ankara, 2006, s. 4

[174] Hasan Yılmaz, "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi" Denetişim Dergisi, Sayı 15, No:11, 2014, s. 55.
http://dergipark.gov.tr/download/article-file/208742 (11.06.2018)

- Bilgi sistemlerini kullanan kişilerin, umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suistimal etme gibi nedenlerden dolayı oluşabilecek donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızaların bir daha tekrar etmemesi için iyileştirme sürecinin olması olarak sıralanabilir.[175]

3.2.8.3 Bilgi Güvenliği Yönetim Sistemi Kurulumu

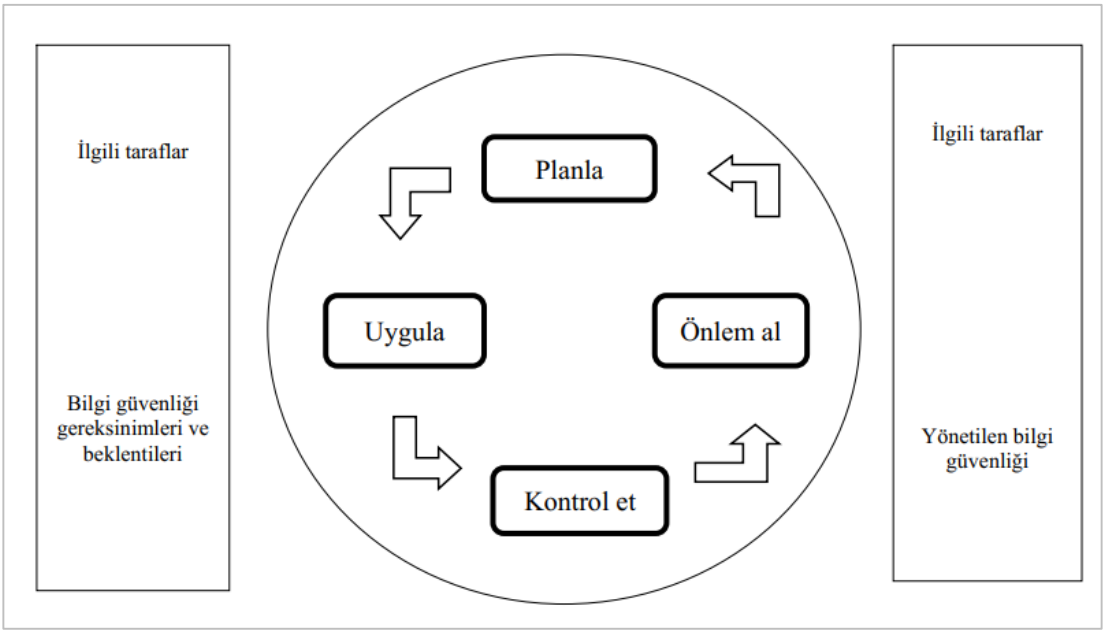
Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumun hassas bilgilerini yönetebilmek amacıyla oluşturulmuş ve çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsayan sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır.[176]

Bir kuruluşta BGYS'nin kurulması için öncelikle bu sistemin sadece bir BT işi olmadığı anlaşılmalı ve bununla birlikte üst yönetim desteği ve alt çalışan desteği sağlanmalıdır. Sistem kurulumu aşamasında dayanak olarak yasal gerekçeler, sızma testleri ile gerçek açıklıkların ortaya koyduğu tehdit ve riskler kuruluma olan hevesi artıracaktır. [177]

Kurum tehditleri ve riskleri belirledikten sonra bunları azaltmak ve yönetmek için sürekli devam eden bir faaliyet modeli uygulamalıdır. Bu model Şekil 7'de gösterildiği gibi PUKÖ (planla- uygula - kontrol et - önlem al) döngüsü olarak adlandırılmaktadır.[178]

---

[175] Mustafa Gülmüş, 2010, s. 60-61.
[176] Mehtap Çetinkaya, *Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi*, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2008, s.7.
[177] Kerem Gencer, 2015, s. 11.
[178] Hasan Yılmaz, 2014, s. 53.



Şekil 7: ISO 27001 Planla, uygula, kontrol et ve önlem al aşamaları döngüsü [179]

Planla aşaması BGYS'nin kurulmasıdır. Risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin kurulduğu aşamadır.[180]

Uygula aşaması BGYS'nin gerçekleştirilmesi ve işletilmesidir. Bir önceki aşamada kurulan BGYS politikası, kontroller, süreçler ve prosedürler gerçekleştirilip işletilmeye başlanır.[181]

Kontrol et aşaması bir önceki aşamada yapılan işlerin doğru şekilde uygulanıp uygulanmadığının doğrulanmasıdır. [182]

Önlem al bu döngünün son aşamasasıdır. Bu aşamada yeni denetimlerin belirlendiğini ve bu denetimleri uygulamak için önerilerin geliştirildiği aşamadır.

[179] Kerem Gencer, 2015, s. 11.
[180] Türk Standartları Enstitüsü, 2006, s.2.
[181] a.g.e, s.2.
[182] Henry Dalziel, 2015, s. 10.

Döngünün doğası gereği Planla, uygula, kontrol et ve önlem al (PUKÖ) başa dönebilir.[183]

3.2.8.4 Bilgi Güvenliği Yönetim Sistemi Kurulum Aşamaları

Bir kurumda Bilgi Güvenliği Yönetim Sistemini kurulurken uygulanan aşamalar aşağıdaki gibidir:

- Varlıkların sınıflandırılması
- Gizlilik, bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi
- Risk analizi
- Risk analizi çıktılarına göre uygulanacak kontrolleri belirleme
- Dokümantasyon oluşturma
- Kontrolleri uygulama
- İç tetkik
- Kayıtları tutma
- Yönetimin gözden geçirmesi
- Belgelendirme

3.2.8.5 Bilgi Güvenliği Yönetim Sistemi Güvenlik Kontrolleri

ISO 27001 Standardı etkin bir Bilgi Güvenliği Yönetim Sistemi kurarken öngörgüğü bazı kontrol maddeleri vardır. Bu maddeler ayrıntılı değildir ve kurumlar

[183] a.g.e, s.10.

ek kontrol amaçlarının ve kontrollerin gerekli olduğunu düşünebilir.[184] Bu kontrol maddeleri aşağıda sıralanmaktadır. [185]

- Bilgi Güvenliği Politikaları
- Bilgi Güvenliği Organizasyonu
- İnsan Kaynakları Güvenliği
- Varlık Yönetimi
- Erişim Kontrolü
- Kriptografi
- Fiziksel ve Çevresel Güvenlik
- Operasyon Güvenliği
- İletişim Güvenliği
- Sistem Edinim, Geliştirme ve Bakım
- Tedarikçi İlişkileri
- Bilgi Güvenliği Olay Yönetimi
- İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönleri
- Uyum

Bu kontrol maddeleriyle ilgili detaylı bilgiler bu tezin 3.4.5. bölümünde yer almaktadır.

3.3 SIZMA TESTLERİ

Bir önceki bölümde bahsedilen bilgi güvenliğini yönetim sisteminin ne seviyede bir güvenlik sağladığı ve eksiklerinin hangi noktalarda olduğunun anlaşılması için en iyi yol sızma testi yaptırmaktır. Sızma testleriyle saldırı senaryoları oluşturup sistemin zayıf noktaları bulunur. Kurumlar bu şekilde bilgi sistemlerinin nasıl riskleri

[184] Türk Standartları Enstitüsü, 2006, s.14.
[185] Cemile Denerel, 2016, s.20.

taşıdığının farkına varabilir ve zafiyetleri giderip daha güçlü bir güvenlik seviyesi sağlayabilir.

3.3.1 Tanımlar

Sızma testi ile ilgili olarak, geniş bir tanım aralığı vardır. Bu tanımlar aşağıda maddeler halinde sıralanmaktadır. [186]

- Sızma testi, güvenlik zayıflıklarını tanımlamak ve bunlardan faydalanmak için üstlenilen bir dizi faaliyettir.
- Bir sistemin güvenlik özelliklerini atlatmaya çalışan güvenlik testidir.
- Test edilen sistem, uygulama, ana bilgisayar ve ağlardan oluşan bir bilgisayar sistemi değildir. Aynı zamanda güvenli bir bina, ya da büyük olasılıkla, kullanıcıların, bir ofisin ve bir bilgisayar sisteminin bir birleşimi olabilir.
- Ayrıca, sızma testi "korumanın zayıflıklarını göstermek için bir sisteme girme çabası" olarak tanımlanabilir.
- Sızma testi; ağ geçitlerinin, güvenlik duvarlarının ve sistemlerin, yetkisiz erişime veya hizmetleri aksatmaya yönelik girişimlere karşı korunmak için uygun şekilde tasarlandığından ve yapılandırıldığından emin olmak için bir testtir.
- Sızma testi, BT ortamının bir analizi ve istismar edilebilir güvenlik açıklarını araştırmaktır. Test, sisteme ne kadar derin girilebileceğini vurgular.

Sonuç olarak hedeflenen bilgi sistemlerine mümkün olabilecek her yolun denenerek sızılmasıdır. Sızma testinde amaç sadece güvenlik açığını bulmak değil bundan öte bulunan açıklığı değerlendirip sistemde nereye kadar erişildiğini keşfetmektir. [187]

---

[186] Chiem Trieu Phong, *A Study of Penetration Testing Tools and Approaches*, Auckland University of Technology Yüksek Lisans Tezi, Auckland, 2014, s.5
[187] Mustafa Gülmüş, 2010, s.114.

3.3.2 Sızma Testinin Amaçları

Ne şimdi ne de gelecekte % 100 güvenli hiçbir sistem olmadığından, sızma testinin temel amaçlarından biri, bir sistemin ne kadar güvenli olduğunu veya başka bir deyişle ne kadar güvensiz olduğunu incelemektir. Daha detaylı söz etmek gerekirse; güvenlik boşluklarını tanımlamak, istismar araçlarını kullanarak hedef ağa girmek ve daha sonra hassas verilere erişmek için sızma testi kullanılır.[188]

Sızma testleri kurumlar tarafından ne amaçlarla yapıldığı aşağıda maddeler halinde sıralanmıştır. [189]

- Önceden bilinmeyen zafiyetlerin bulunması,
- Tasarımdan kaynaklanan zayıflıkların belirlenmesi,
- Kurumun güvenilir olduğu imajının korunması,
- Bilgi güvenlik politikalarının gözden geçirilmesi,
- Bilgi güvenliği belgelendirme aşamalarında uyumda sürekliliğin sağlanması,
- Güvenlik yatırımı yapılırken daha doğru karar verilmesi,
- Teknik personelin sorumluluğunun gözden geçirilmesi,
- Kurumsal bilgi sistemlerine yapılabilecek olan muhtemel saldırı veya saldırılara karşı güvenliğin sürekli olarak yüksek seviyede sağlanması.

3.3.3 Sızma Testlerinin Çeşitleri

Sızma testleri testi yapacak kişilerin kurum hakkındaki bilgi seviyesine göre Kara Kutu (Black Box), Beyaz Kutu (White Box) ve Gri Kutu (Gray Box) olarak üçe ayrılır.

---

[188] Chiem Trieu Phong, 2014, s.7.

[189] Yılmaz Vural, *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri,* Gazi Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi, Ankara, 2007, s. 121-122

Kara Kutu: Bu test yaklaşımında test edilecek sistem hakkında testi yapacak kişilere herhangi bir bilgi verilmez. Sistemi test edenler kendi yöntemleriyle bilgileri toplar ve bunları anlamlandırarak sisteme sızmaya çalışır.[190] Kara kutu testi bilinmeyen bir saldırganın neyi başardığını anlamak için pratik olarak yararlıdır.[191]

Beyaz Kutu: Bu yöntemde kurum içinde önemli bilgiler (ağ topolojisi, sunucular vb.) testi yapanlara sağlanarak kurumun iç yapısı da incelenir, kaynak kod incelemesi yapılır.[192] Beyaz kutu testi, hedefli testlerde güvenlik açıklarını ve saldırı vektörlerini olabildiğince açığa çıkarmak için daha kullanışlı bir yöntemdir.[193]

Gri Kutu: Bu test türünde, testi yapanlar ve test edilen kurumun çalışanları aynı bilgi ve haklara (kurumun geçmişi, kurumsal kültür, fiziki mekânlara erişim, kullanıcı adı ve şifresi, vb.) sahiptir.[194] Gri kutu testi, bir sistemin yetkili bir kullanıcısının edinebileceği erişim derecesini anlamaya çalışır.

Bir kurum yukarıda bahsedilen test türleri arasında yapacağı seçim kendi gereksinimlerine bağlıdır. Amaç, kötü niyetli bir bilgisayar korsanının sistemlere neler yapabileceğini keşfetmekse, kara kutu testi en iyi karardır. Bunun yerine, şirketin güvenlik altyapısını bir bütün olarak iyileştirmek istendiğinde, beyaz kutu testi daha anlamlı olacaktır.[195]

[190] Gökhan Muharremoğlu, 2013, s.20-21.
[191] Chiem Trieu Phong, , 2014, s.11.
[192] Kerem Gencer, 2015, s. 11
[193] Chiem Trieu Phong, , 2014, s.11.
[194] Yılmaz Vural, 2007, s. 126
[195] Chiem Trieu Phong, , 2014, s.11.

3.3.4 Sızma Testinin Aşamaları

Sızma testlerinin aşamaları aşağıda maddeler halinde sıralanmaktadır. [196]

- Kapsam Belirleme (Scope) (Planlama)
- Bilgi Toplama (Reconnaissance, Discovery)
- Keşif ve Tarama (Enumeration)
- Zafiyet Taraması ve Analizi (Vulnerability Scanning)
- İstismar Etme (Exploitation)
- İstismar Sonrası (Post Exploitation)
- İzleri Temizleme (Clearing Tracks)
- Raporlama (Reporting)

Kapsam Belirleme (Scope) (Planlama) : Bu aşama; bu testi yaptırma amacı, kapsamı, gizlilik ve etik anlaşmalar gibi konularda kurumla anlaşmaya varıldığı bir sözleşme-öncesi aşamadır. Taraflar kapsam, raporlama formatı ve diğer konular hakkında hemfikir olduğunda, gerçek test başlar.[197]

Bilgi Toplama (Reconnaissance, Discovery): Zaman zaman keşif adımı olarak adlandırılan bu aşama, bir sızma testinde kullanılan mevcut bilgilerin aranmasıdır. Sızma testinin kapsamına bağlı olarak, keşif aktiviteleri, bir ağdaki IP adreslerini keşfetmek için ping taraması yapmak, çalışanlardan yararlı bilgiler almak, telekomünikasyon hizmetlerinin makbuzlarını bulmak için şirketin çöplüklerini karıştırmak; hırsızlık, insanlara yalan söyleme, telefonları ve ağları dinlemek gibi farklı şekillerde olabilir.[198]

[196] https://www.crypttech.com/tr/images/pdf/SIZMATESTI_2017.pdf, s. 6. (28.04.2018)
[197] Georgia Weidman, *Penetration Testing: A hands-on Introduction to Hacking*, No Starch Press, San Francisco, 2014, s. 2.
[198] Chiem Trieu Phong, , 2014, s. 20.

Keşif ve Tarama (Enumeration): Bu aşamada aktif olarak tüm çalışan servislerin ve uygulamaların kullanıcı isimleri, ağ paylaşım bilgisi ve uygulama sürümü bilgisi elde edilir.[199]

Zafiyet Taraması ve Analizi (Vulnerability Scanning): Keşfedilen sistemlerdeki mevcut servislerin ve işletim sisteminin bilinen açıklıkları ücretli ve açık-kaynak kodlu zafiyet tarama araçları ile taranır. Buna ek olarak manuel bir şekilde de servisler üzerinde zafiyet analizi yapılır. Sistemler üzerinde bulunan öntanımlı kullanıcıların analizi, zayıf parola denemeleri yapılır.[200]

İstismar Etme (Exploitation): Son olarak, önceki aşamadan elde edilen bilgilerle, sömürü aşamasında, tanımlanmış güvenlik açıkları veya açık bulunan diğer kanallar aracılığıyla sistemi ele geçirmek için özel bir şekilde yürütülen farklı otomatik araçlar, teknikler ve ince ayarlı manuel adımlar kullanılır. Bu sürecin nihai hedefi, sisteme yetkili erişim elde etmektir.[201]

İstismar Sonrası (Post Exploitation) : Bu aşama, bir sistemin veya cihazın ele geçirilmesinden sonra gerçekleştirilen eylemleri ifade eder. Bu, genellikle, sistemlere ya da ağ kaynaklarına ek erişim sağlamak için, test ekibinin sistemdeki yeni noktadan yeni bir saldırı kaynağı oluşturmasını sağlayan ayrıcalık yükseltme ya da döndürme tekniklerini kullanma yöntemini açıklar.[202]. Bu yapılanlarla esas hedeflenen erişim sağladıktan sonra bu erişimin kalıcı hale getirilmesi ve sürdürülmesidir.[203]

İzleri Temizleme (Clearing Tracks): Sızma testi esnasında oluşturulmuş hesaplar ve istismar için yüklenmiş zararlı yazılımların ortadan kaldırılmasıdır.[204]

---

[199] Penetration Test Guidance Special Interest Group, *Information Supplement: Penetration Testing Guidance*, 2015, s.25
https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
[200] https://www.crypttech.com/tr/images/pdf/SIZMATESTI_2017.pdf, s.7 (28.04.2018)
[201] Chiem Trieu Phong, 2014, s.21
[202] Penetration Test Guidance Special Interest Group, 2015, s.16
[203] http://blog.btrisk.com/2016/07/pentest-post-exploitation.html (05.06.2018)
[204] Penetration Test Guidance Special Interest Group, 2015, s.17

Raporlama (Reporting): Bu aşama sızma testinin son aşamasıdır. Yapılan test sonucunda elde edilen bulgular, hem yönetici özetini hem de teknik detayları içeren bir raporla kurumla paylaşılır.[205]

3.3.5 Sızma Testlerinde Kullanılan Araçlar

Sızma testlerinde kullanılan otomatik araçlar sızma testi yapan ekibin daha karmaşık işler (örneğin yeni saldırı imzasını modelleme, yeni saldırı vektörünü tanımlama vb.) yapması için zaman kazanmasına olanak tanır.[206] Bu araçlar kabaca aşağıdaki gibi sınıflandırılabilir:

- Bilgi Toplama ve Tarama Araçları
- Zafiyet Tarama Araçları
- Saldırı Araçları

Aşağıda bu araçlarla ilgili detaylı bilgi verilmiştir.

3.3.5.1 Bilgi Toplama ve Tarama Araçları

Bilgi toplama araçlarına örnek olarak google.com, dnsstuff.com, archive.org, whois.com gibi web siteleri; traceroute, hping2, nslookup, tracert, ping, firewalk, nmap gibi işletim sistemleriyle birlikte gelen birçok yardımcı komut ve araç örnek verilebilir.[207]

[205] Georgia Weidman, 2014, s. 2.
[206] Chiem Trieu Phong, 2014, s. 28.
[207] Gökhan Muharremoğlu, 2013, s. 43-44.

Şekil 8'de firewalk aracıyla port taramasının nasıl yapıldığı gösterilmiştir. Tarama sonucu açık ve kapalı portlar listelenmiştir.

```
root@kali:~# firewalk -S8079-8081  -i eth0 -n -pTCP 192.168.1.1 192.168.0.1
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through 192.168.1.1 using 192.168.0.1 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.1.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port 8079: *no response*
port 8080: A! open (port not listen) [192.168.0.1]
port 8081: *no response*

Scan completed successfully.

Total packets sent:                4
Total packet errors:               0
Total packets caught               2
Total packets caught of interest   2
Total ports scanned                3
Total ports open:                  1
Total ports unknown:               0
```

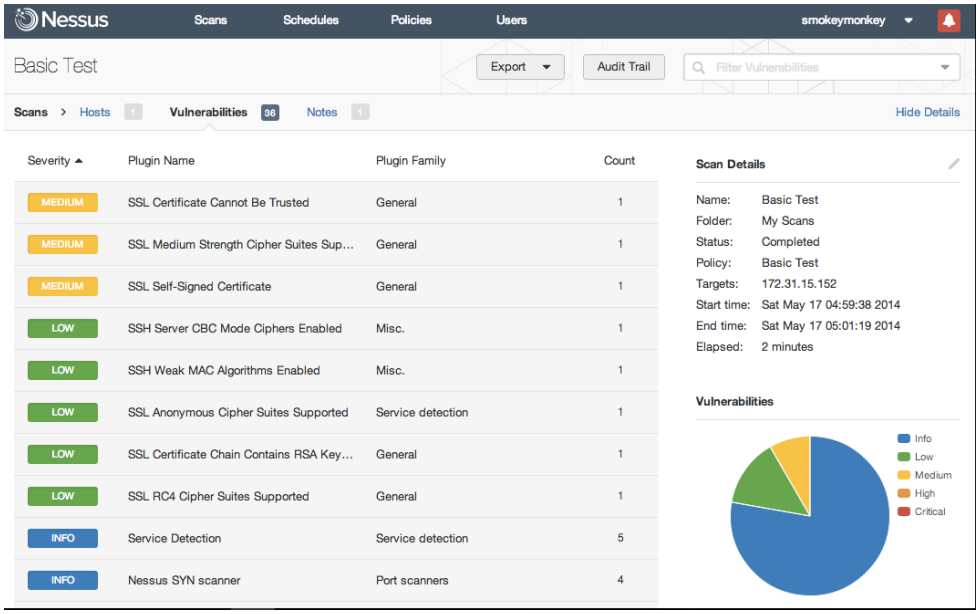
Şekil 8: Firewalk Aracının Kullanılması[208]

3.3.5.2 Zafiyet Tarama Araçları

Bu araçlara örnek olarak Nessus, Core Impact, SAINT gibi ağ zafiyetlerini tarayan araçlar; Nikto, W3AF, Acunetix, WebScarab, Burpsuite gibi web zafiyet tarama araçları verilebilir.

Şekil 9'da Nessus aracının bulduğu zafiyetleri nasıl sınıflandırdığı gösterilmektedir. Görüldüğü gibi zafiyetler listelenmiş ve zaafiyetin ciddiyetine göre bir sınıflandırma yapılmıştır.

[208] https://tools.kali.org/information-gathering/firewalk (01.05.2018)



Şekil 9: Nessus Aracının Zafiyetleri Sınıflandırması [209]

3.3.5.3 Saldırı Araçları

Saldırı araçlarına örnek olarak metasploit framework, armitage, hydra, john the ripper, sslsplit, sqlmap, burp suite, aircrack –ng gibi araçlar sayılabilir.

Bu saldırı araçlarından en önemlilerinden biri olan Metasploit Framework, hedeflenecek istismarın seçilmesi ve yapılandırılması, seçili sistemin istismara açık olup olmadığının doğrulanması, kullanılacak bir payload[210] seçilmesi ve yapılandırılması, güvenlik cihazlarının atlatılması için kodlama şemasının seçilmesi ve yapılandırılması dahil olmak üzere birkaç temel adımı izler.[211]

[209] https://www.sorenasecurity.ir/wp-content/uploads/2015/08/Nessus.png (01.05.2018)
[210] Payload: İstismar (exploit) sonrasında hedef sisteme sızmayı sağlayan ve istenilen işlemleri gerçekleştirmek için kullanılan bileşenlerdir. Örnek ile açıklayacak olursak bir servisin açığını kullanmak exploitin, o açıktan faydalanarak sistemde kullanıcı oluşturmak ise payload'un görevidir.
[211] Georgia Weidman, 2014, s.29.

3.4 KURUMSAL SİBER GÜVENLİK ORGANİZASYONLARI VE GÜVENLİK KONTROLLERİ

3.4.1 Kurumsal Siber Güvenlik Organizasyonları

Kurumsal bilgi güvenliğini sağlamak, sadece kurumların kendi bünyelerinde kuracakları organizasyonlarla ve yapacakları çalışmalarla değil buna ilaveten kurumlar arası işbirliği ve koordinasyonu gerektiren bir durumdur. Böylelikle ulusal siber güvenlikle kurumsal bilgi güvenliği birbirinden ayrılmayan kavramlara dönüşmüştür. Bu bölümde, bu kapsamda oluşturulan organizasyonlar ve bunların arasındaki ilişki incelenecektir.

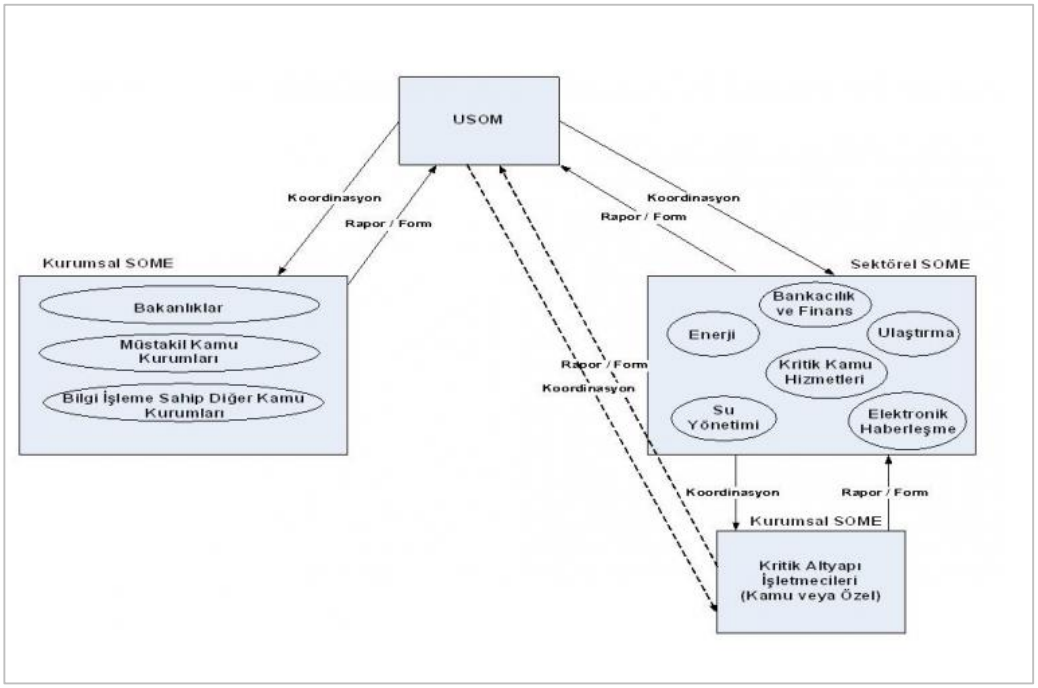
3.4.1.1 Ulusal Siber Olaylara Müdahale Merkezi (USOM)

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4. eylem maddesi uyarınca, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde USOM kurulmuştur.[212]

USOM; siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi, yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesi ve paylaşılması için 7/24 müdahale esasına göre çalışır ve kurum ve kuruluşların siber güvenlik olaylarına müdahale yeteneği kazanmasını amaçlar.[213]

[212] https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi (02.05.2018)
[213] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı*, UDBH, Ankara, 2013, s. 18-19.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nına göre USOM koordinasyonunda çalışacak sektörel "Siber Olaylara Müdahale Ekipleri" (SOME), kurumların bünyesinde ise sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır.[214] Bu kurumlar arasındaki ilişki Şekil 10'da gösterilmektedir.



Şekil 10: Usom, Sektörel Some Ve Kurumsal Some İlişkisi[215]

3.4.1.2 Siber Olaylara Müdahale Ekipleri (SOME)

Ulusal siber güvenliğin ve kurumsal bilgi güvenliğinin sağlanmasında en önemi unsurlarından biri olan SOME ve bu ekiplerin ulusal anlamda işbirliği ve eşgüdüm içinde çalışmasıdır. Bu amaçla 11.11.2013 tarihinde "Siber Olaylara

[214] a.g.e, s.19.
[215] https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi (01.05.2018)

Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ", UBAK tarafından resmi gazetede yayınlanmıştır.[216]

Bu tebliğin 7. Maddesine göre kurumsal SOME'lerin bazı görev ve sorumlulukları aşağıda maddeler halinde sıralanmaktadır. [217]

- Siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmalarını yapmak veya yaptırmak,
- Siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışmak, yapamadağı takdirde sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunmak,
- Birlikte çalıştığı sektörel SOME ile faaliyetlerini eşgüdüm içinde yürütmek, yaşanan siber olayı USOM'a bildirmek, eğer suç içeren bir durum varsa kanunen yetkili birimlere haber vermek,
- USOM ve birlikte çalışılan sektörel SOME'den gelen uyarılar neticesinde tedbirler almak.

3.4.1.2.1 Kurumsal SOME Kurulum Aşamaları

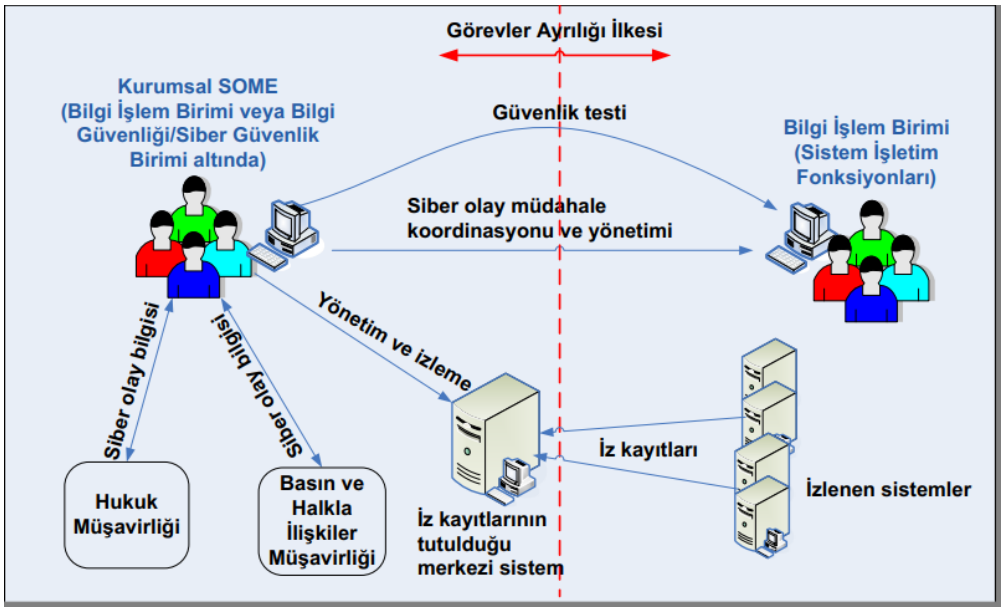
UBAK, Temmuz 2014 tarihinde yayınladığı "Kurumsal SOME Kurulum ve Yönetim Rehberi" ile kurumsal SOME'lerin kurulum aşamalarını detaylı bir şekilde anlatmıştır. Bu aşamalar aşağıda maddeler halinde sıralanmaktadır.

- Kurum İçerisindeki Yeri ve Kapasite Planlaması
- Kurum İçi Paydaşlarla İletişim Esasları

[216] Mustafa Ünver, "Türkiye'de Siber Güvenlik", *CyberMag Dergisi*, Sayı: 1, 2016, s. 20.
[217] Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ, Resmi Gazete: 11.11.2013, 28818.

- Kurum Dışı Paydaşlarla İletişim Esasları
- Eğitimlerin Alınması
- Kurumsal SOME'lerin Kuruluş Süreleri
- Kurumsal SOME'ler için Kuruluş Esasları

"Kurum İçi Paydaşlarla İletişim Esasları" kısmı kurum içindeki görev ayrılığına vurgu yapması bağlamında önem taşımaktadır. Bu amaçla bilgi işlem biriminin sistem işletimi yapan kişilerle Kurumsal SOME fonksiyonlarının farklı personel tarafından yapılması önem arzetmektedir. Bu durum Şekil 11'de gösterilmektedir.



Şekil 11: Kurumsal SOME'nin Kurum İçindeki Paydaşları ve Temel Fonksiyonları[218]

3.4.1.2.2 Kurumsal SOME'lerin Görev ve Sorumlulukları

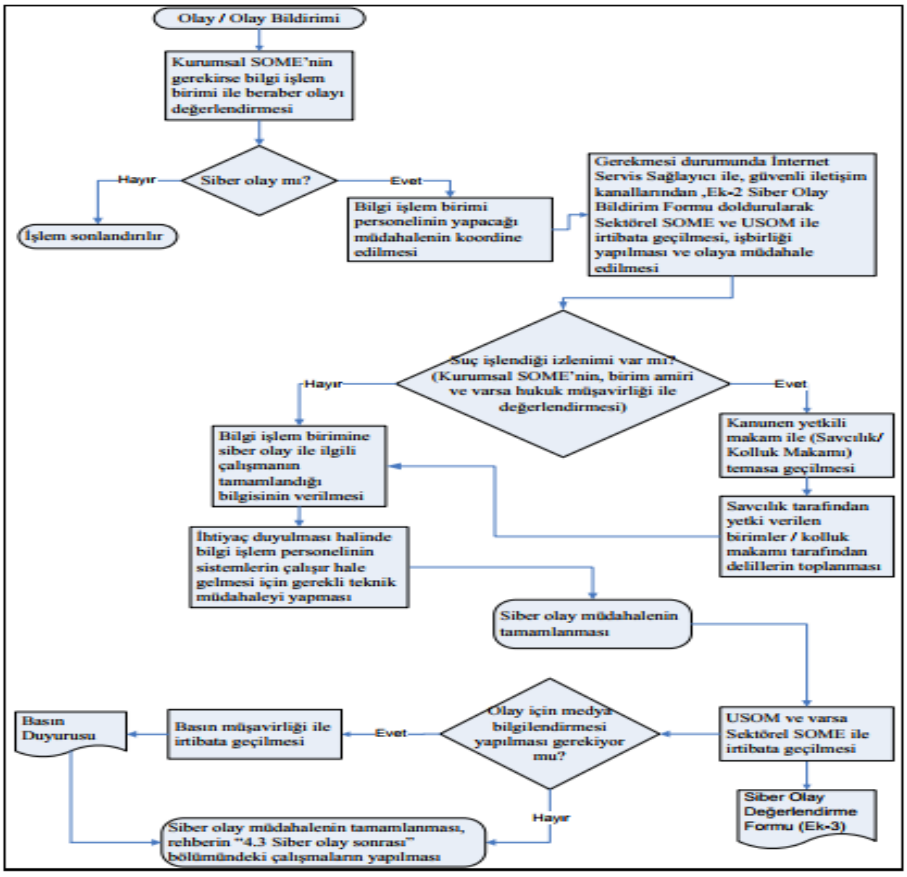
UBAK, Temmuz 2014 tarihinde yayınladığı "Kurumsal SOME Kurulum ve Yönetim Rehberi" ile kurumsal SOME'lerin görev ve sorumluluklarını üç aşamada ele almıştır:

[218] T.C. Ulaştırma ve Altyapı Bakanlığı, *Kurumsal SOME Kurulum ve Yönetim Rehberi*, UBAK, Ankara, 2014, s.13-14

- Siber olay öncesi
- Siber olay esnası
- Siber olay sonrası

Siber olay öncesinde; "kurumsal SOME'ler, kurum içi farkındalık çalışmalarının gerçekleştirilmesi, kurumsal bilişim sistemleri sızma testlerinin yapılması / yaptırılması ve kayıtların düzenli olarak incelenmesi çalışmalarını yaparlar".[219]

Siber olay esnasında yapılacak işler Şekil 12'de gösterildiği gibi adım adım yapılması gerekmektedir.



Şekil 12: Siber Olay Müdahale Akış Diyagramı[220]

[219] T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı,2014, s.17.
[220] a.g.e, s.23

Siber olay sonrasında olaya neden olan açıklık belirlenir, olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler kurum yönetimine arz edilir. Yaşanan siber olayla ilgili yapılan işlere dair bir rapor hazırlanır, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilir.[221]

3.4.1.3 Siber Güvenlik Kurulu

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar gereğince; Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma ve Altyapı Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.

Kurulun görevleri şunlardır: [222]

- Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak
- Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak
- Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek

3.4.1.4 KamuNet (Kamu Sanal Ağı)

KamuNet'in oluşturulması çalışmaları UBAK tarafından yürütülmekte olup, 5809 sayılı Elektronik Haberleşme Kanunu'nun 5. Maddesinin birinci fıkrasının (h)

[221] a.g.e, s.24.
[222] https://www.btk.gov.tr/siber-guvenlik-kurulu (01.05.2018)

bendine, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile Siber Güvenlik Kurulu Kararlarına dayanmaktadır.[223]

KamuNet, "kamu kurum ve kuruluşları tarafından özel ağ ile internet ortamından yalıtılmış şekilde hizmet, işlem ve veri trafiğinin aktarılacağı, fiziksel ve siber saldırılara karşı daha güvenli kapalı devre, kamu sanal ağı altyapısı"[224] şeklinde tanımlanır.

KamuNet projesinin amaçları ve hedefleri aşağıda maddeler halinde sıralanmaktadır:

- Kamu kurum ve kuruluşları arasındaki veri iletişiminin, kurumlar arası ve internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi
- Mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması
- Ortak uygulamalar için uygun alt yapının tesis edilmesi ve oluşturulması
- Planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi

Kamu kurum ve kuruluşlarının KamuNet'e dahil olabilmeleri için bazı koşulları yerine getirmesi gerekmektedir. Bunlardan bir kısmı aşağıda maddeler halinde sıralanmaktadır. [225]

- BGYS kurulmalı ve ISO 27001[226] ile uyumlu hale getirilmelidir.
- Kuruma ait kritik sistemler üzerinde sızma testleri[227] yapılıp tespit edilen açıklıkların giderilmesi için çalışmalar yapılmalıdır.
- Kurum içerisinde maksimum güvenlikli ideal çözümün sağlanabilmesi için sunucu ve istemci (client) ağları ayrılmalıdır.

[223] http://www.hgm.gov.tr/tr/sayfa/45 (03.05.2018)
[224] Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ, RG:21.06.2017, 30103, s.1.
[225] http://www.udhb.gov.tr/doc/siberg/KamuNetweb.pdf (03.05.2018)
[226] BGYS ve ISO 27001, Bölüm 3.2.5'de detaylı bir şekilde anlatılmıştır.
[227] Sızma Testleri Bölüm 3.3'te detaylı bir şekilde anlatılmıştır.

- İstemci (Client) ağı içerisinde Dizin Hizmeti kullanılmalı ve her bir kullanıcı bilgisayar Dizin Hizmeti'ne dahil edilmelidir.
- Sunucu ve istemci (client) ağlarının birbirine erişiminde mutlaka FW[228], IPS[229], içerik filtreleme ve antivirüs gibi fonksiyonların bir arada olduğu UTM vb. ya da bu fonksiyonların ayrı ayrı olduğu cihazlar kullanılarak bir güvenlik katmanı oluşturulmalıdır.
- Kamu kurumlarının hizmet olarak verdiği, internete açık servislerinin (web vb.) bulunması halinde bu servislerden gelen saldırıların KamuNet ağını olumsuz etkilememesi için DDoS[230] ataklarını önleyen hizmetlerden faydalanılmalıdır.[231]
- KamuNet ağını olumsuz etkilememesi için NAC (Network Access Controller)[232] çözümleri ile kullanıcıların yapılandırmasının güvenli olup olmadığı kontrol edilerek kendi ağlarına alınmaları sağlanmalıdır.
- Sunucular üzerindeki gereksiz uygulamalar ve servisler mutlaka kapatılmalı, işletim sistemleri ve uygulama yazılımları güncel tutulmalıdır.
- KamuNet ağına dahil olacak her bir cihazda (bilgisayar, sunucu vb.) virüsler, solucanlar, truva atları ve casus yazılımlar vb. gibi zarar verebilecek yazılımları saptama, silme işlevlerini yapabilecek, sürekli aktif halde çalışan ve güncellenmesi gereken son kullanıcı güvenlik yazılımlarını kurulu bulundurmalıdır.

[228] FW(Firewall):Güvenlik Duvarı: Yerel ağlar üzerindeki cihazları diğer ağlar (internet vb.) üzerinden gelecek saldırılara karşı koruyan bir donanım ürünü

[229] IPS(Intrusion Prevention System) :Saldırı Tespit Sistemleri: Üzerinden geçen tüm trafiğe ait paketleri derinlemesine inceleyerek özellikle uygulamalara yönelik paketlerin hangisinin saldırı niteliği taşıdığını hangisinin ise zararsız olduğunu tespit edebilen sistemlerdir.

[230] DDoS saldırıları Bölüm 2.2.9'da detaylı bir şekilde anlatılmıştır.

[231] Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ, Resmi Gazete: 21.06.2017, 30103, s. 1-2.

[232] Bu cihaz sayesinde sadece güvenlik ilkelerine uyan ve erişim izni alan cihazlar ağa bağlanabilir.

3.4.2 Güvenlik Kontrolleri

Bu bölümde ISO 27001 Standardında öngörülen güvenlik kontrollerinden bahsedilecektir.

3.4.2.1 İnsan Kaynakları Güvenliği

İnsan Kaynakları Güvenliği maddesi işe alım, çalışma ve işe son verilmesi aşamalarında yapmamız gerekenleri tarif etmektedir. Bu kapsamda yapılması gerekenler aşağıda maddeler halinde sıralanmıştır.

- İşe alınacak personele yüklenecek rol ve sorumluluklar açıkça tanımlanmış ve işe alınmadan önce personel tarafından iyice anlaşılması sağlanmış olmalıdır.[233]
- Kurumlar işe aldıkları kişilerin geçmiş doğrulama kontrollerini kişilerin erişecekleri bilgilerin kritikliği ölçüsünce yapmalıdır.[234]
- Gizli bilgilere erişim izni olan tüm çalışanlar ve yükleniciler ile bilginin olduğu yere erişim yetkisi vermeden önce birer gizlilik ve açığa çıkarmama sözleşmesi imzalatılmalıdır.[235]
- Çalışan personelin bilgi güvenliği ile ilgili farkındalığının arttırılması ve eğitilmesi gerekmektedir.
- Görevden ayrılan personel, zimmetinde bulunan malzemeleri, elindeki bilgi ve belgeleri teslim etmelidir.[236]
- Çalışanın işten ayrılmasıyla veye bölüm değiştirmesiyle beraber ilgili erişim haklarıda kaldırılmalıdır.[237]

---

[233] Hasan Yılmaz, 2014, s.53
[234] Türk Standartları Enstitüsü, 2006, s.17.
[235] https://www.burakeksi.com/iso-27001-bilgi-guvenligi-yonetim-sistemi-insan-kaynaklari-guvenligi-1-istihdam-oncesi/ (05.05.2018)
[236] https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPolitikalar%C4%B1K%C4%B1lavuzu.pdf (05.05.2018)
[237] https://lostar.com.tr/2009/03/bilgi-guvenligi-yonetim-sistemi-bgys-ve-insan-kaynaklari-yonetimi.html (05.05.2018)

3.4.2.2 Varlık Yönetimi

Kurum için değer taşıyan herşey bir varlıktır. Bu varlıklara örnek olarak bilgi, altyapı, yazılım&donanım ve personel verilebilir. Varlıklar, risk değerlendirmesi ve sorumluluk atanması yapılabilmesi için bilgi güvenliği yönetiminde önemli bir yer teşkil etmektedir.[238]

Bu varlıkların yönetimi için yapılması gerekenler aşağıda maddeler halinde sıralanmaktadır. [239]

- Bilgi ve bilgi işlem tesisleriyle ilişkili varlıklar belirlenmeli ve bu varlıkların envanteri düzenlenerek korunmalıdır.
- Envanterde bulunan varlıklar sahiplenilmelidir.
- Bilgi işleme olanakları ile ilişkili bilgi ve varlıkların kabul edilebilir kullanım kuralları tanımlanmalı, dokümante edilmeli ve gerçekleştirilmelidir.
- Bilgi; yasal gereksinimleri, değeri, kritikliği ve yetkilendirilmemiş ifşaya ve değiştirmeye karşı hassasiyetine göre sınıflandırılmalıdır.
- Bilgi etiketleme için kuruluş tarafından benimsenen sınıflandırma düzenine uygun olarak bir dizi uygun prosedür geliştirilmeli ve gerçekleştirilmelidir.

3.4.2.3 Erişim Kontrolü

- Erişimle ilgili iş ve güvenlik ihtyaçları göz önünde bulundurularak bir Erişim Kontrol Politikası oluşturulmalı ve hangi kullanıcıların hangi ağlara ve hizmetlere erişebileceği tanımlanmalıdır.
- Kullanıcıların sisteminize kayıt olmalarını nasıl isteneceği, kullanıcılara nasıl erişim sağlanacağı, kimlik doğrulama verilerini yönetimi gibi konularla ilgili prosedüler olmalıdır.

[238] https://www.slideshare.net/AnkitaLachhwani/iso-27001-a8-asset-management (05.05.2018)
[239] a.g.e

- Normal kuralların dışında olan erişime izin verilmesi gerekiyorsa (ayrıcalıklı erişim), bu tür kullanıcı erişim kurallarını kimin onaylayabileceği tam olarak tanımlanmalıdır.
- Kullanıcılar şirketten ayrılırken veya kurumdaki pozisyonlarını değiştiğinde tüm erişim haklarının uygun bir şekilde kaldırılması veya değiştirilmesi ile ilgili işlemler yapılmalıdır için bir süreç olmalıdır.

3.4.2.4. Fiziksel ve Çevresel Güvenlik

Fiziksel ve çevresel güvenlik, bilgi güvenliği açısından değerlendirildiğinde pratikte kuruma yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunması olarak algılanabilir. Fiziksel ve çevresel güvenliğin sağlanması için yapılması gerekenler aşağıda sıralanmıştır.

- Bilgi işleme servisini korumak amacıyla herhangi bir fiziksel sınır güvenliği (kart kontrollü giriş, duvarlar, insanlı nizamiye vb.) tesis edilmelidir.
- Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre oluşturulmalıdır.
- Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları oluşturulmalı ve ziyaretçilerin giriş-çıkış zamanları ve ziyaret sebepleri kaydedilmelidir.
- Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karşı fiziksel koruma tedbirleri alınmış olmalı ve uygulanmalıdır.[240]

[240] Hasan Yılmaz, 2014, s.54

3.4.2.5 Operasyon Güvenliği

- Kullanıcı faaliyetlerini, ayrıcalıkları, hataları ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak gözden geçirilmelidir.
- Günlüğe kaydetme olanakları ve kayıt bilgileri, kurcalamaya ve yetkisiz erişime karşı korunmalıdır.
- Sistem yöneticisi ve sistem operatörü etkinlikleri günlüğe kaydedilmeli, günlükler korunmalı ve düzenli olarak gözden geçirilmelidir.
- Bir organizasyon veya güvenlik alanı içerisindeki tüm ilgili bilgi işlem sistemlerinin saatleri, tek bir referans zaman kaynağına senkronize edilmelidir.
- Yazılımların işletim sistemi üzerindeki kurulumunu kontrol etmek için prosedürler uygulanmalıdır.
- Kullanılan bilgi sisteminin teknik açıkları ile ilgili bilgiler zamanında alınmalıdır.
- Yazılımın kullanıcılar tarafından kurulmasını yöneten kurallar oluşturulmalı ve uygulanmalıdır.[241]

3.4.2.6 İletişim Güvenliği

İletişim güvenliği ISO 27001 ‘de Ağ Güvenliği ve Yönetimi ve Bilgi Transferi olmak üzere iki başlık altında verilmektedir.

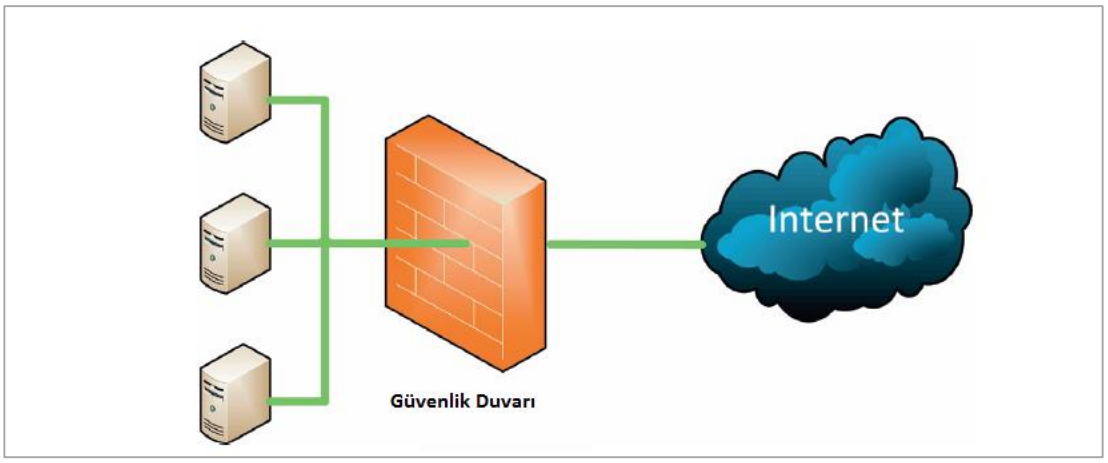
Ağ güvenliğinin sağlanması için; ekipman yönetimi için sorumlulukların ve prosedürlerin tanımlanması, ağlar ve bilgisayar etkinlikleri arasındaki görevlerin ayrıştırılması, birbirine bağlı sistemlerde iletilen verilerin korunması için kriptografik çözümlerin (örn., VPN) kullanılması, gerçekleştirilen ağ faaliyetlerinin izlenmesi ve günlüğe kaydedilmesi (örn., bir Saldırı Tespit sistemleri kullanılarak - IDS), kimlik

[241] https://www.slideshare.net/Hitz_I4/iso-27001-2013-a12-operations-security-part-2 (08.05.2018)

doğrulama ve ağ kaynaklarının erişimini ve kullanımını kısıtlamak için diğer araçlar(güvenlik Duvarı) gibi bir dizi genel kontrol uygulanmalıdır.[242] Aşağıda ağ güvenliğini sağlamak için geliştirilmiş bazı çözümlerden bahsedilecektir.

Güvenlik Duvarları (Firewalls)

Bir güvenlik duvarı, ağlarımıza giren ve çıkan trafiğin kontrolünü sağlamak için bir mekanizmadır. Güvenlik duvarı genellikle güvenli olarak gördüğümüz kısım (örneğin iç ağımız) ile güvensiz olanın (İnternet) arasına Şekil 13'de görüldüğü gibi yerleştirilir.



Şekil 13: Güvenlik Duvarı

Bugün kullanılan güvenlik duvarlarının çoğu, ağ üzerinden gelen paketlerin incelenmesi kavramına dayanmaktadır. Bu inceleme, neye izin verilip verilmeyeceğini belirler. Trafiğe izin verilip verilmemesi, çeşitli faktörlere dayanabilir ve büyük ölçüde güvenlik duvarının karmaşıklığına bağlıdır. Örneğin, kullanılan protokole dayanarak trafiğe izin verebilir veya izin vermeyebiliriz, Web ve e-posta trafiğinin geçmesine izin verebiliriz, ancak diğer her şeyi engelleyebiliriz.[243]

[242] https://advisera.com/27001academy/blog/2016/06/27/how-to-manage-network-security-according-to-iso-27001-a-13-1/ (08.05.2018)
[243] Jason Andress, 2014, s. 153-154

Kavramsal olarak, üç çeşit güvenlik duvarı vardır:

- **Packet Filters Firewall (Paket Filtreleme Güvenlik Duvarı)**:Önceden belirlenmiş politikalara göre Protokol, IP adresi ve port numaraları bazında yönlendiricideki arayüz üzerinden ağa girecek veya çıkacak paketlere izin verir.
- **Uygulama Katmanı Güvenlik Duvarı (Application Level (Gateway) Firewall)**: Kaynak ve hedef düğümler arasında bir ara sunucu görevi gören bir vekil sunucu gibi hareket eder.
- **Durum Denetim Güvenlik Duvarları (Stateful Inspection Firewal):** Paketi, içeriğine göre doğrular. Burada güvenlik duvarı, paketlere girmeden veya ağdan ayrılmadan önce paketlerin içeriğini inceleyecektir. Paketlerin içeriği, paket ile bildirilen protokol ile uyumlu olmalıdır. Örneğin, bildirilen protokol HTTP ise, paketin içeriği HTTP paket tanımıyla tutarlı olmalıdır.[244]

Saldırı Tespit Sistemleri (Intrusion Detection System)

Ağa izinsiz girişe karşı, saldırı tespit teknolojisi esastır. Güvenlik duvarı sadece işgalcilere direnmeye çalışır, izinsiz giriş teşebbüsleri ve başarılı işgali bulmak için saldırı tespit teknolojisi kullanmak gerekir. Ağ saldırı tespit teknolojisi, saldırgan davranışları önlemek için kullanıcıları zamanında uyarmak üzere, istila davranışı ve saldırı girişimini algılayabilir. Saldırı tespit sistemi tipi, kaynağa göre ana bilgisayara bağlı saldırı tespit sistemi, ağ tabanlı saldırı tespit sistemi ve dağıtılmış saldırı tespit sistemi olmak üzere üçe ayrılabilir.[245]

[244] John R. Vacca, *Computer and Information Security Handbook: Second Edition*, Elsevier, Waltham, 2013, s.276-277

[245] Yanqing Sun, "The Study on Network Information Security", *2016 International Conference on Network and Information Systems for Computers (ICNISC*), Wuhan, 2016, s. 87.

Ağ Erişim Kontrolü (Network Access Control) (NAC)

Bir NAC sistemi, güvenlik politikalarına uyumlu olmayan cihazların ağ erişimini reddedebilir, karantinaya alınmış bir alana yerleştirebilir veya bilgisayar kaynaklarına yalnızca kısıtlı erişime izin verir, böylece ağı güvenli olmayan kısımlardan korumuş olur.[246]

Sanal Özel Ağ (Virtual Private Network) (VPN)

Sanal özel ağ, verilerin şifreli bir şekilde gönderildiği ve internet ağı üzerinde belirlenen iki uç arasına tahsis edilmiş özel bir ağdır. Sağladıkları bu güvenlik sayesinde kullanıcıların veri sızıntısı endişesi olmaksızın kurumun iç ağına uzaktan bağlanmalarına olanak tanırlar. [247]

3.4.2.7 Sistem Edinim, Geliştirme ve Bakım

Bilgi sistemlerinde bu tip kontrollerin yapılmasıyla amaçlananlar aşağıda maddeler halinde sıralanmıştır. [248]

- Güvenliğin bilgi sistemlerinin dahili bir parçası olmasını sağlamak,
- Uygulamalardaki bilginin hatalarını, kaybını, yetkisiz değiştirilmesini ve kötüye kullanımını önlemek,
- Bilginin gizliliğini, aslına uygunluğunu ya da bütünlüğünü kriptografik yöntemlerle korumak,
- Sistem dosyalarının güvenliğini sağlamak,
- Uygulama sistem yazılımı ve bilgisinin güvenliğini sağlamak.
- Yayınlanmış teknik açıklıkların istismarından kaynaklanan riskleri azaltmak.

[246] https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html (04.06.2018)
[247] Yanqing Sun, 2016, s.87
[248] Türk Standartları Enstitüsü, 2006, s.25-26.

Yukarıda sıralanan amaçlara ulaşmak için yapılması gereken kontroller aşağıda sıralanmıştır. [249]

- Yeni sistemlerin geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmalıdır.
- Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmalı; doğru girilmiş bilginin işlem sırasında sırasında hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmelidir.
- Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmalıdır.
- Bilginin korunması için kriptografik kontrollerin kullanılmasını düzenleyen politika geliştirilmiş ve uygulamaya alınmış olmalıdır.

3.4.2.8 Tedarikçi İlişkileri

Kuruma ait verilerin giderek daha fazla oranda kurum dışındaki kişilerce işlendiğinden ve depolandığından, bu bilgilerin korunması, bilgi güvenliği uzmanları için giderek daha önemli bir konu haline gelmektedir.[250] Bu kapsamda yapılması gereken kontroller aşağıda maddeler halinde sıralanmıştır. [251]

- Tedarikçinin kuruluş varlıklarına erişiminden doğan risklerin düşürülmesi için gerekli bilgi güvenliği gereksinimleri tedarikçi ile karşılıklı olarak anlaşılmalı ve dokümante edilmelidir.
- Kuruluşun bilgi teknolojileri altyapı bileşenlerine erişen, işleyen, depolayan veya bileşenleri sağlayan tedarikçiler ile tüm bilgi güvenliği ihtiyaçları karşılıklı olarak anlaşılmalı ve dokümante edilmelidir.

[249] Hasan Yılmaz, 2014, s.54
[250] https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/ (10.05.2018)
[251] Eray Çek, *Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2017, s. 46-47.

- Bilgi ve iletişim teknoloji servisleri ve ürün tedarik zinciri ile ilgili bilgi güvenliği risklerini ortadan kaldıracak şekilde gizlilik anlaşmaları yapılmalıdır.
- Kuruluş, tedarikçi hizmetlerini düzenli aralıklarla izlemeli, gözden geçirmeli ve denetlemelidir.
- Tedarikçiler tarafından sağlanan servislerdeki değişiklikler iş bilgisinin, sistemlerin ve süreçlerin kritikliği dikkate alınarak yönetilmelidir. Değişiklikler, mevcut bilgi güvenliği politikaları, prosedürleri ve kontrollerinin iyileştirilmesi ve sürdürülmesini de içermelidir.

3.4.2.9 Bilgi Güvenliği Olay Yönetimi

Bir kurumda bir bilgi güvenliği olayı meydana geldiğinde aşağıda anlatıldığı gibi beş adımlık bir yöntem izlenebilir. [252]

- **Olay bildirimi:** Kurumun işleyişine zarar verebilecek bir olayı tespit eden personel kurumun iletişim prosedürlerine (genellikle bir e-posta, telefon araması, yazılım aracı vb.) göre olayı bildirmesi gerekir.
- **Olayın sınıflandırılması:** Bildirimi yapılan olay çeşitli parametrelere bağlı olarak sınıflandırılır. Olayı tespit eden kişi de bir sınıflandırma yapabilir, ancak bunu uygun şekilde sınıflandıran teknik bir uzmandır.
- **Olaya Müdahale**: Olay sınıflandırıldıktan ve ciddiyeti anlaşıldıktan sonra bu sorunu çözmek için gerekli önlemler kararlaştırmalıdır.
- **Olayı Kapatma:** Olay çözüldükten sonra, müdahale sırasında üretilen tüm bilgiler kaydedilir ve son olarak, olayla ilgili bildirimi ilk gönderen kişi olayın kapandığını bildirir.

[252] https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/ (11.05.2018)

- **Bilgi güvenliği ihlal olaylarından öğrenme**: Olaya müdahale sırasında ortaya çıkan tüm bilgiler bilgiler kaydedilir,bu bilgiler gelecekte olası benzer olaylar için kullanılabilir.

3.4.2.10 İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönleri

İş sürekliliği yönetimi, bir işletmenin devam eden faaliyetlerini etkileyebilecek riskleri, tehditleri ve zafiyetleri tanımlayan bir yönetim sürecidir ve organizasyonel esneklik ve etkili bir karşılık verme yeteneği için bir çerçeve sunar.[253]

Bu kapsamda yapılması gereken kontroller aşağıda maddeler halinde sıralanmaktadır. [254]

- Kurum kriz veya felaket durumları için bilgi güvenliği ve bilgi güvenliği yönetimi süreklilik ihtiyaçlarını belirlemelidir.
- Kurum kötü durumlar esnasında gereken bilgi güvenliği sürekliliğini sağlamak için işlemler, prosedürler ve kontroller oluşturmalı, dokümante etmeli, uygulamalı ve sürdürmelidir.
- Kurum, oluşturduğu ve uyguladığı bilgi güvenliği süreklilik kontrollerini olası kötü durumlarda geçerli ve etkin olduğunu belirlemek üzere düzenli aralıklarla doğrulamalıdır.
- Bilgi işleme tesisleri, erişilebilirlik ihtiyaçlarını karşılamak üzere yeterli yedeklik yapısına sahip olmalıdır.

[253] https://www.slideshare.net/iFourpooja/iso-27001-clause-17-is-aspects-of-business-continuity-management (11.05.2018)
[254] Eray Çek, 2017, s.49-50.

3.4.2.11 Uyum

Son kontrol maddesi olan uyum kontrollerinde amaçlananlar aşağıda maddeler halinde sıralanmıştır. [255]

- Her türlü hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek,
- Sistemlerin kurumsal güvenlik politikaları ve standartlarıyla uyumunu sağlamak,
- Bilgi sistemleri denetim işlemlerinin etkinliğini artırmak ve müdahaleleri azaltmak.

Bu amaçlara ulaşmak için yapılması gerekenler aşağıda maddeler halinde sıralanmaktadır.

- Her bir bilgi sistemi için ilgili bütün yasal, düzenleyici ve sözleşmeye bağlı gereksinimler ve gereksinimleri sağlamak için kullanılacak kurumsal yaklaşım açık şekilde tanımlanmış ve belgelenmiş olmalı ve bu gereksinimleri karşılamak amacıyla kontroller ve bireysel sorumluluklar tanımlanmalı ve belgelenmelidir.
- Kullanılmakta olan yazılım ve diğer her türlü materyal ile ilgili olarak yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasını güvence altına alan prosedürler yürürlüğe sokulmalıdır.[256]
- Yasalar, düzenlemeler ve sözleşmelerle uyum için şifreleme kontrolleri kullanılmalıdır.[257]

[255] Türk Standartları Enstitüsü, 2006, s. 29-30.
[256] Hasan Yılmaz, 2014, s.53
[257] Eray Çek, 2017, s.51.

SONUÇ VE ÖNERİLER

Kurumsal bilgi güvenliğinin sağlanabilmesi için bilgi güvenliğini tehdit eden siber saldırıların başlangıçtan bu güne nasıl evrildiği çok iyi bilinmelidir. Araştırmalar göstermiştir ki yıllar geçtikçe daha karmaşık saldırılar yapılmakta, üstelik bu saldırıları yapmak için gereken bilgi seviyesi düşmektedir. Bunun sebebi saldırıların otomatik araçlarla yapılabilmesidir. Böylece siber saldırılar yaygınlaşmış, eskiden hobi, kişisel tatmin vb. gibi bireysel motivasyonlarla yapılan saldırılar artık daha organize hale gelmiştir. Günümüzde artık devletler arasında yapılan siber savaşlardan sözedilmektedir.

Ülkemizin siber tehdit ve saldırılardan etkilenme oranına bakılacak olursa bilgi güvenliği konusunda aşama katetmemiz gerektiği görülecektir. 2016 verilerine göre kötücül yazılım bulaşma oranı en yüksek ikinci ülke, Dağıtık Servis Dışı Bırakma (DDoS) saldırılarının en çok kaynaklandığı üçüncü ülke olmamız güvenlik politikalarımızı ve uygulamalarımızı yeniden gözden geçirmemiz gerektiğini bize söylemektedir. DDoS saldırıların ülkemizden çok yapılması bilgisayarların kötücül yazılımlarla ele geçirilip bu tip saldırılarda kullanıldığını göstermektedir.

Siber tehdit ve saldırıların sınıflandırılması çeşitli şekillerde yapılabilir. Örneğin bilgi sistemindeki hasara göre sınıflandırma, bilgi güvenliğinin üç temel prensibi olan gizlilik, bütünlük ve erişilebilirlik öğelerinden hangisinin ihlal edildiği esas alınarak yapılır. Bilgi sistemine saldırma yöntemine göre sınıflandırma yapılırken veri akışına olan etki esas alınır. Bu yaklaşıma göre DDoS saldırılarında olduğu gibi veri akışı engellenebilir; ağ koklama gibi yöntemlerle veriler dinlebilir; virüs, solucan ve truva atı gibi kötücül yazılımlarla veriler değiştirilebilir veya veriler yeniden

üretilebilir. Bulunduğu yere göre siber tehdit ve saldırılar sınıflandırılırken verinin bulunduğu katman esas alınır. Saldırı teknikleri ve alınacak tedbirler sınıflar içinde benzeştiği için bu tezde saldırı türlerinin anlatılmasında bu yaklaşım esas alınmıştır.

Son yıllardaki siber saldırı trendleri incelendiğinde, 2017 yılı güvenlik raporlarına göre siber saldırganların kazançlarını artırabilmek için fidye yazılım, kripto para madenciliği ve BEC (Şirket E-Postaları Dolandırıcılığı) saldırılarına yöneldiği görülmüştür. Bu teknikler uygulanırken sosyal mühendislik, oltalama ve işletim sistemlerindeki güvenlik zafiyetlerinden faydalanma gibi yöntemler birleştirilmektedir. Bu tip saldırılardan korunmak için son kullanıcıların e-postalardaki linkler ve eklentileri açarken dikkatli olmaları gerekmektedir. Bu konulardaki farkındalığın arttırılması için son kullanıcıların bu konularda bilgilendirilmelidir. Ayrıca işletim sistemi zafiyetleri güvenlik yamalarıyla giderilmelidir ve bu güncellemeler zamanında yapılmalıdır. Kritik veriler yedeklenmeli ve güncel bir anti-virüs uygulaması kullanılmalıdır.

Siber saldırganlar, zeki ve kendilerini gizlemekte süratli olduklarından siber tehditler her an değişmekte ve gelişmektedir. Bu sebeple, bir saldırganın daha önceki aktivitelerinden çıkarım yaparak öğrenen yapay zeka ve makine öğrenmesi yöntemlerinin; sabit kural tabanlı ölçümlerle karar veren yöntemlerden daha faydalı olacağı değerlendirilmektedir. Bu sayede yalnızca mevcut tehlikelerin değil, tehlikeyi önceden sezen, hatta sonraki nesil siber saldırıların neler olabileceğini daha başından tespit edebilen yapay zeka destekli siber güvenlik çözümlerinin yakında daha fazla gündeme geleceği öngörülmektedir.

Siber saldırıların dünya genelindeki tahmini maliyeti yıllık yaklaşık 400 milyar dolar ve 2019 yılında bu rakamın 2.1 trilyon dolar olması bekleniyor. Bu saldırılardan korunmak için alınması gereken bazı önlemler aşağıda sıralanmıştır.

Öneriler

Bireysel Önlemler:

- Tanınmayan kişilerden gelen, spam olduğundan şüphelenilen mailler açılmamalıdır. Bazen bu tarz mailleri sadece açmak bile bilgisayarı virüsün bulaşması için yeterli olabilir.
- Tanınan kişilerden gelen maillerde şüphe uyandırıcı bir şeyler varsa (.exe uzantılı bir eklenti veya tuhaf bir link) bu maili açmadan önce; diğer iletişim kanallarıyla bu kişileler iletişime geçerek bu mailin gerçekten o kişi tarafından atılıp atılmadığı kontrol edilmelidir.
- Bilgisayarda mutlaka bir antivirüs programı kurulmalı ve belirli aralıklarla güncelleyin.
- Kullanılan yazılımların mutlaka en güncel sürümü kullanılmalıdır.
- Bilinmeyen, şüpheli ve güvensiz görünen sitelerden dosya indirilmemelidir.
- Kullanılan şifreler kolaylıkla tahmin edilemeyecek şekilde seçilmelidir.

Kurumsal Önlemler:

- Kurumun ağının analiz edilip gözlemlenmesi gerekmektedir. Mevcut sistemin normal zamanda ne kadar trafik altında olduğunu bilmek önem taşımaktadır. Bunu ölçümlemek adına SIEM ürünlerinin raporlamaları kullanılabilir.

- Tüm ağ güvenlik cihazlarının (güvenlik duvarı, yönlendirici, anahtar, saldırı tespit Sistemi, yük dengeliyici vb.) güncel tutulması gerekmektedir. Burdaki bir güvenlik açığı DDOS atağına açık kapı bırakabilir.

- Uygulamalar çalıştırılırken yapılandırma limitleri dikkatli bir şekilde belirlenmelidir. Gerek duymadıkça kullanılmayan protokollerin ve portların kapatılması sistem sağlığı için önemli olacaktır.

- Uygulamalar DMZ ortamında ise saldırı sadece dıştan değil içten de olabilir bu durumda her iki trafiğinde iyi düzenlenmiş olmalıdır.

- Son kullanıcı makinelerinde mutlaka uç nokta güvenlik çözümü olmalıdır ve güncelliği kontrol edilmelidir.

- Oltalama amaçlı ve mesaj sağanağı (Spam) şeklinde gelen maillerden korunmak adına mutlaka bir SPAM koruma çözümü kullanılması gerekmektedir.

- Özellikle Gelişmiş İnatçı Tehditlere karşı koruma altında olmak adına mutlaka bir ATP cihazı ve Proxy kullanılması önerilmektedir.

- Genellikte gözden kaçan ve gereksiz gibi görülen ama en önemli ürün olan yama ürünlerinin ve zafiyet kontrol ürünleri mutlaka kullanılmalıdır.

Bilgi güvenliğinin sağlanması için üç temel unsur olan gizlilik, bütünlük ve erişebilirlik prensiplerinin sağlanması gerekmektedir. Bunlara ek olarak kimlik doğrulama, inkâr edememe, izlenebilirlik ve güvenilirlik prensiplerinden bahsedilebilir. Kurumlar kendi yapıları ve ihtiyaçları doğrultusunda bu sayılan güvenlik unsurlarından bazılarını ön plana alabilirler. Kurumsal bilgi güvenliğinin yeterli seviyede olması için uluslarası düzeyde kabul görmüş bilgi güvenliği standartlarının bilinmesi ve uygulanması gerekmektedir.

Kurumlar; bilgi varlıklarının tespit edilip bunların korunması, karşılaşılabilecek siber risklerin en aza indirgenmesi, iş sürekliliğinin sağlanması ve bilgi güvenliği kontrollerinin sürekliliğini bilgi güvenliği esaslarına göre sağlamak için yönetim süreçlerini kabul etmeli ve uygulamalıdır. Bu kapsamda, ISO tarafından yayınlanan ve uluslararası kabul görmüş ISO 27001 standardıyla uyumlu bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulmalıdır.

Bir kuruluşta BGYS'nin kurulması için öncelikle bu sistemin sadece bir BT işi olmadığı anlaşılmalı ve bununla birlikte üst yönetim desteği ve alt çalışan desteği sağlanmalıdır. Oluşturulan güvenlik politikaları ve güvenlik prosedürleri açık ve tutarlı olmalıdır. Ayrıca, güvenlik tehditleri zamanla değiştiğinden, güvenlik politikaları da devamlı kontrol edilip güncellenmelidir. Kurumsal bilgi güvenliğinin yönetilmesinin zorunlu bir süreç olduğu bilinciyle uygulamalar sürekli izlenmeli, denetlenmeli ve gerektiğinde iyileştirilmelidir.

Bilgi güvenliğini yönetim sisteminin ne seviyede bir güvenlik sağladığı ve eksiklerinin hangi noktalarda olduğunun anlaşılması için en iyi yol sızma testi yaptırmaktır. Sızma testleriyle saldırı senaryoları oluşturup sistemin zayıf noktaları bulunur. Kurumlar bu şekilde bilgi sistemlerinin nasıl riskleri taşıdığının farkına varabilir ve zafiyetleri giderip daha güçlü bir güvenlik seviyesi sağlayabilir. Bu önemi dolayısıyla sızma testleri belirli peryotlarda (yılda 1-2 kez) yapılmalıdır.

Kurumsal bilgi güvenliğini sağlamak, sadece kurumların kendi bünyelerinde kuracakları organizasyonlarla ve yapacakları çalışmalarla değil buna ilaveten kurumlar arası işbirliği ve koordinasyonu gerektiren bir durumdur. Böylelikle ulusal siber güvenlikle kurumsal bilgi güvenliği birbirinden ayrılmayan kavramlara dönüşmüştür. Bu kapsamda kurumlar, siber olayın öncesinde, olduğu anda ve sonrasında yapılacak işleri yerine getirmek için Siber Olaylara Müdahale Ekipleri (SOME) kurmalıdır. Bu ekipler yaşanan siber olayları USOM ile paylaşmalı ve USOM'dan gelen gelen uyarılar neticesinde tedbirler almalıdır. Ayrıca bu ekipler son çıkan tüm zafiyetleri, tüm istismar yöntemlerini, meydana gelen önemli siber olayları takip etmeli ve ekip içerisinde düzenli olarak eğitim toplantıları düzenlemelidir.

Kamu kurum ve kuruluşları, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ olan KamuNet'e (Kamu Sanal Ağı) dahil olmalıdır. Kurumlar, KamuNet Ağı'na dahil olmak için asgari güvenlik gereksinimlerini yerine getirmelidir. Bu şekilde içerik güvenliği sağlanan veri iletişiminin güvenli bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı

devre çözümlere standart sağlanması, ortak uygulamalar için uygun alt yapının tesis edilmesi ve oluşturulması, planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi mümkün hale gelecektir.

Kamu kurumları ile kritik altyapıların siber saldırılara karşı dirençlerinin arttırılması, siber saldırı sonrası ise sistemlerin en kısa sürede hizmete alınabilmesi, ulusal kapasitenin arttırılması için siber güvenlik tatbikatları yapılmalıdır. Tatbikatlar sektör odaklı olmalı ve katılım zorunlu hale getirilmelidir. Tatbikat sonuçları kamuya açık olmalı ve bu sonuçlar analiz edilerek her kurum için ev ödevi çıkarılmalıdır.

Kurumların siber saldırılara karşı yapması gerekenler aşağıda sıralanmıştır.

- Tüm kurumlardaki Siber Olaylara Müdahale Ekiplerinin (SOME) daha efektif hale getirilmelidir ve desteklenmelidir.
- 7x24 izleme ve olaylara müdahale kapasiteleri güçlendirilmelidir.
- Kurumlar arasındaki bilgi paylaşımı ve koordinasyon arttırılmalıdır.
- Risk odaklı güvenlik yaklaşımına geçilmeli ve yatırımlara bu yönde yer verilmedir.
- Siber istihbarattan daha etkili yararlanılmalıdır.
- Kurumsal güvenlik farkındalığının arttırılması gerekmektedir.

Siber güvenlik uzmanı eksikliği kurumsal bilgi güvenliğini yakından ilgilendirmektedir. Gelecek 5 yıl içinde dünyada yaklaşık 1.5 milyon, ülkemizde ise 30 bin siber güvenlik uzmanı ihtiyacı olacağı öngörülmektedir. Bundan dolayı siber güvenlik açığının oluşmaması için yeterli düzeyde siber güvenlik uzmanı yetiştirilmelidir. Üniversitelerde siber güvenlik enstitüleri kurulması ve yaygınlaştırılması desteklenmelidir.

Siber güvenlikte milli çözümler olmadan tamamen güvende olamayız. Dolayısıyla milli işletim sistemimiz olan PARDUS'un geliştirilmesi ve

yaygınlaştırılması için TÜBİTAK ve ULAKBİM desteklenmeli ve yeterli düzeyde AR-GE yatırımı yapılmalıdır.

Siber güvenlik alanında yerli ve milli sistemler ile güvenlik katmanlarının oluşturulması, tüm bilgisayar kullanıcılarının siber güvenlik farkındalıklarının yükselterek aldatılmalarının engellenmesi, yine yerli siber güvenlik ekipleri ile kurumların siber güvenliklerinin desteklenmesi, siber uzayda önde olmak için bir şart olarak karşımızdadır.

KAYNAKÇA

Andress, Jason (2014), *The Basics of Information Security : Understanding the Fundamentals of InfoSec in Theory and Practice Second Edition,* Elsevier, Waltham,USA.

Aydaner, Gülcihan, Çelik, Ufuk ve Nart, Senem (2017), "Siber Güvenlikte Kamu ve Özel Sektör İşbirliği", *10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı,* s. 57-67.

Baykara, Muhammet, Daş, Resul ve Karadoğan, İsmail (2013), " Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi ", 1*st International Symposium on Digital Forensics and Security*, Elazığ, s. 231-239.

Can, Özgü ve Akbaş, M. Fatih (2014), " Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması, *Tübav Bilim Dergisi* 7, No:2, s. 16,31

Canbek, Gürol (2005), *Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme,* Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara.

Canbek, Gürol ve Sağıroğlu, Şeref (2007), "Kötücül ve Casus Yazılımlar-Kapsamlı Bir Araştırma", *Gazi Üniv. Müh. Mim. Fak. Dergisi* 22, No:1, s. 121-136.

Canbek, Gürol ve Sağıroğlu, Şeref (2006), *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri,* Grafiker Yayınları, Ankara.

Canbek, Gürol ve Sağıroğlu, Şeref (2006), "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi,* Cilt: 9, No: 3, s. 165-174.

Collard, Guillaume, Ducroquet, Stéphane, Disson, Eric, ve Talens, Guilaine (2017),"A definition of Information Security Classification in cybersecurity context", *11th International Conference on Research Challenges in Information Science,* Brighton, s. 77 -82.

Cross, Michael (2007), Developer's Guide to Web Application Security, Syngress, Rockland.

Crypttech (2017), "Sızma Testi", s. 6-8
https://www.crypttech.com/tr/images/pdf/SIZMATESTI_2017.pdf (28.04.2018)

CyberMag (2017), "BTK-USOM'dan Petya Zararlı Yazılımı Açıklaması", *CyberMagDergisi*, No: 19, s. 32.

CyberMag (2016), "Türkiye'nin Siber Profili", *CyberMag Dergisi*, Sayı: 6, s. 41-42.

Çek, Eray (2017), *Kurumsal Bilgi Güvenliği Yönetişimi Ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi,* İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Çetinkaya, Mehtap (2008), *Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi*, İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Dalziel, Henry (2015), *Infosec Management Fundamentals,* Elsevier, Waltham.

De Leeuw, Karl ve Ergstra, Jan (2007), *History of Information Security: A Comprehensive Handbook.* Elsevier, Amsterdam.

Denerel, Cemile (2016), "Güvende Olmak İçin Uyumlu Ol", *CyberMag Dergisi*, Sayı: 6, s. 19.

Ekşi, Burak, *ISO 27001 Bilgi Güvenliği-İnsan Kaynakları Güvenliği-1- İstihdam Öncesi.*
https://www.burakeksi.com/iso-27001-bilgi-guvenligi-yonetim-sistemi-insan-kaynaklari-guvenligi-1-istihdam-oncesi/ (05.05.2018)

Elektronik Haberleşme Kanunu, RG:10.11.2008, 27050

Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi Ve Gizliliğinin Korunması Hakkında Yönetmelik, RG: 24.07.2012, 28363

Elektronik Haberleşme Sektöründe Şebeke Ve Bilgi Güvenliği Yönetmeliği, RG: 13.07.2014, 29059

Erdoğan, Görkem ve Bahtiyar, Şerif (2014), "Sosyal Ağlarda Güvenlik", *XVI. Akademik Bilişim Konferansı,* Mersin, s. 267-272.

Gandhi, Komal (2016), "Network security problems and security attacks", *International Conference on Computing for Sustainable Global Development*, New Delhi, s. 3855 - 3857.

Gencer, Kerem (2015), *ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım,* Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Afyon.

Graves, Kimberley (2010), *CEH Certified Ethical Hacker Study Guide*, Wiley Publishing, Indiana.

Grebennikov, Nikolay (2007), *Keyloggers: How they work and how to detect them (Part1)*
https://securelist.com/keyloggers-how-they-work-and-how-to-detect-them-part-1/36138/ (24.03.2018)

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

Gülnaz, Mesut (2010), *Kamusal Web Güvenliği,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2010.

Gündüz, M. Zekeriya (2013), *Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti,* Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Elazığ.

Gündüz, M. Zekeriya ve Daş, Resul (2017), "Sosyal Mühendislik ve Korunma Yolları", *CyberMag Dergisi*, Sayı: 18, s. 14-23.

Güngör, Murat (2015), *Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma,* Uzmanlık Tezi, T.C Kalkınma Bakanlığı, Ankara.

Havelsan (2017), "Türkiye Siber Güvenliğine Son İstatistikler ile Bakış", *CyberMag Dergisi*, Sayı: 15, s. 18-21.

Hekim , Hakan ve Başıbüyük, Oğuzhan (2013), "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", *Uluslararası Güvenlik ve Terörizm Dergisi*, Cilt: 4, Sayı: 2, s. 139-140.

iFour Consultancy (2016), *ISO 27001 2013 A12 Operations Security Part 2 - by Software development company in india.* https://www.slideshare.net/Hitz_I4/iso-27001-2013-a12-operations-security-part-2 (08.05.2018)

İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, RG: 23.05.2007, 26530.

Kamunet Ağına Bağlanma Ve Kamunet Ağının Denetimine İlişkin Usul Ve Esaslar Hakkında Tebliğ, RG:21.06.2017, 30103

Karadoğan, İsmail (2016), *Ağ İletişiminde Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları,* Fırat Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Elazığ.

Kişisel Verilerin Korunması Kanunu, RG: 07.04.2016, 29677.

Kosutic, Dejan (2014), *6-step process for handling supplier security according to ISO 27001.* https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/ (10.05.2018)

Kotman, İrfan (2016), "Son Yılların En Etkili Tehditleri Fidye Yazılımları (Ransomware)", *Beyaz Şapka Dergisi*, Sayı: 2, s. 8-9.

Lachhwani, Ankita (2016), *ISO 27001 A8 Asset Management.* https://www.slideshare.net/AnkitaLachhwani/iso-27001-a8-asset-management (05.05.2018)

Leal, Rhand (2016), *How to manage network security according to ISO 27001 A.13.1.* https://advisera.com/27001academy/blog/2016/06/27/how-to-manage-network-security-according-to-iso-27001-a-13-1/ (08.05.2018)

Lostar, Murat (2009), *Bilgi Güvenliği Yönetim Sistemi (BGYS) ve İnsan Kaynakları Yönetimi.* https://lostar.com.tr/2009/03/bilgi-guvenligi-yonetim-sistemi-bgys-ve-insan-kaynaklari-yonetimi.html (05.05.2018)

Messier, Ric (2016), *Operating System Forensics.* Syngress,Waltham.

Muharremoğlu, Gökhan (2013), *Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı Ve Savunma Öğelerinin İncelenmesi,* İstanbul Üniversitesi Fen bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Önok, Murat (2013), "Avrupa Konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Cilt:19, Sayı: 2, s. 1229-1270.

Pauli, Josh (2013), *The Basics of Web Hacking: Tools and Techniques to Attack the Web*, Elsevier, Waltham,USA.

Person, Wise (2016), *Hacking web applications CEHv8 module 13* https://www.slideshare.net/ahmedfawzyvip2/hacking-web-applications-cehv8-module-13 (01.04.2018)

Penetration Test Guidance Special Interest Group PCI Security Standards Council (2015), Information Supplement:Penetration Testing Guidance. https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf (09.06.2018)

Phong, Chiem Trieu (2014), *A Study of Penetration Testing Tools and Approaches,* Auckland University of Technology, Yüksek Lisans Tezi, Auckland.

Polichen (2014), *Cehv8 module 08 sniffing* https://www.slideshare.net/polichen/ce-hv8-module-08-sniffing (24.03.2018)

Sammons , John ve Cross, Michael (2017), *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy,* Syngress, Cambridge, USA.

Schiffman, Mike D. ve Goldsmith, David (2014), *Kalı Tools.* https://tools.kali.org/information-gathering/firewalk (01.05.2018)

Segovia, Antonio Jose (2015), *How to handle incidents according to ISO 27001 A.16.* https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/ (11.05.2018).

Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliğ, RG:11.11.2013, 28818

Singer, P.W. ve Friedman, Allan (2014), *Cybersecurıty And Cyberwar: What Everyone Needs to Know,* Oxford University Press, New York.

Sooni, Pooja (2016), *ISO 27001 Clause 17 - IS Aspects of Business Continuity Management.* https://www.slideshare.net/iFourpooja/iso-27001-clause-17-is-aspects-of-business-continuity-management (11.05.2018)

Sun, Yanqing (2016), "The Study on Network Information Security", *2016 International Conference on Network and Information Systems for Computers,* Wuhan, s. 85-88.

Şen, İsmail (2018), *Sistem Ele Geçirme (System Hacking)* http://ismailsen.com.tr/sistem-ele-gecirme-system-hacking/ (24.03.2018)

Şenol, Mustafa (2017), "Türkiye'de Siber Saldırılara Karşı Caydırıcılık", *10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı,* Ankara, s. 68-75.

Şişaneci, İbrahim, Akın, Osman , Karaman, Muharrem, ve Mehmet Sağlam (2013), "A Novel Concept for Cybersecurity: Institutional Cybersecurity", *6th International Information Security & Cryptology Conference*, Ankara, s. 186-191.

T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016), *2016-2019 Ulusal Siber Güvenlik Stratejisi*, UDBH, Ankara.

T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü (2014), *Bilgi Güvenliği Politikaları Kılavuzu.* https://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPolitikalar%C4%B1K%C4%B1lavuzu.pdf (05.05.2018).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2014), *Kurumsal SOME Kurulum ve Yönetim Rehberi,* UDBH, Ankara.

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2013), *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı,* UDBH, Ankara.

Teknetir (2017), *CEHv9 : module 12 - hacking web applications* https://www.slideshare.net/teknetir/cehv9-module-12-hacking-web-applications (01.04. 2018).

Teknetir (2017), *CEHv9 : module 13 - SQL injection* https://www.slideshare.net/teknetir/cehv9-module-13-sql-injection (31.03.2018)

Teknetir (2017), *CEHv9 : module 06 -malwarethreats* https://www.slideshare.net/teknetir/cehv9-module-06-malware-threats (17.01.2018)

Teknetir (2017), *CEHv9 : module 05 - system hacking.* https://www.slideshare.net/teknetir/cehv9-module-05-system-hacking (24.03.2018)

Türk Standartları Enstitüsü (2006), *TS ISO/IEC 27001 Bilgi Teknolojisi- Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler,* TSE, Ankara.

Türk Standartları Enstitüsü (2007), *TS ISO/IEC 27001'E Göre Bilgi Güvenliği Yönetim Sistemi (Bgys) Belgelendirmesi İçin Gereksinimler Ve Hazırlık Kılavuzu-TS 13268-1*, TSE, Ankara.

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (2007), *BGYS - Risk Yönetim Süreci Klavuzu,* UEKAE, Ankara.

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (2007), *Bilgi Güvenliği Yönetim Sistemi,* TÜBİTAK – UEKAE, Ankara.

Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, RG:20.10.2012, 28447

Ulusal Siber Olaylara Müdahale Merkezi (2014), *Siber Güvenliğe İlişkin Temel Bilgiler,* USOM, Ankara

Ünver, Mustafa (2016), "Türkiye'de Siber Güvenlik", *CyberMag Dergisi*, Sayı: 1, s. 18-21.

Vacca, John R. (2013), *Computer and Information Security Handbook: Second Edition,* Elsevier, Waltham.

Varol, Asaf ve Ülgen Sönmez ,Yeşim (2017), "The Analysis of the Concepts of Informatics, Cyber Crimes and Computer Forensics", *10. Uluslararası Bilgi Güvenliği Ve Kriptoloji Konferansı,* Ankara, s. 38-43.

Von Solms, Rossouw ve van Niekerk, Johan (2013), "From information security to cyber security", *Computer & Security*, Sayı: 38, s. 97-102.

Vural, Yılmaz (2007), *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri,* Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara.

Vural, Yılmaz, ve Şeref Sağıroğlu (2010), "Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri", *Politeknik Dergisi,* Cilt: 13, Sayı: 2, s. 71-81.

Vural, Yılmaz, ve Şeref Sağıroğlu (2007), "Kurumsal Bilgi Güvenliği: Güncel Gelişmeler", *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı.* Ankara, s. 191-199.

Vuz Dở Hơi (2015), *Cehv8 - Module 05: System Hacking* https://www.slideshare.net/vuzlego/ce-hv8-module-05-system-hacking-wwwcert-learningcom (22.03.2018)

Vuz Dở Hơi (2015), *Cehv8 - Module 06: Trojans and Backdoors* https://www.slideshare.net/vuzlego/ce-hv8-module-06-trojans-and-backdoorswwwcert-learningcom (18.03.2018)

Vuz Dở Hơi (2015), Cehv8 - Module 07: Viruses and Worms https://www.slideshare.net/vuzlego/ce-hv8-module-07-viruses-and-wormswwwcert-learningcom (04.05.2018)

Wayland, Bradley A. (2014), *Security for Business Professionals: How to Plan, Implement, and Manage Your Company's Security Program,* Butterworth-Heinemann , Newton, MA, USA.

Weidman, Georgia (2014), *Penetration Testing: A hands-on Introduction to Hacking,* No Starch Press, San Francisco.

Yılmaz, Hasan (2014), "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi", *Denetişim Dergisi*, Sayı: 15, s. 45-59. http://dergipark.gov.tr/download/article-file/208742 (11.06.2018)

ELEKTRONİK KAYNAKLAR

https://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/denial-of-service-(dos)-saldırıları-ve-korunma-yöntemleri (27.03.2018)

http://blog.btrisk.com/2016/07/pentest-post-exploitation.html (05.06.2018)

http://blog.btrisk.com/2016/01/arp-poisoning-nedir-nasil-yapilir.html (24.03.2018)

https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi (02.05.2018)

https://www.btk.gov.tr/siber-guvenlik-kurulu (02.05.2018)

https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html (04.06.2018)

http://www.hgm.gov.tr/tr/sayfa/45 (03.05.2018)

http://www.lifeoverpentest.com/2016/04/sql-injection-turleri-ve-login-bypass.html (04.06.2018)

https://www.sorenasecurity.ir/wp-content/uploads/2015/08/Nessus.png (01.05.2018)

https://tr.wikipedia.org/wiki/Yemleme (05.05.2018)

http://www.udhb.gov.tr/doc/siberg/KamuNetweb.pdf (03.05.2018)

http://www.udhb.gov.tr/images/duyurular/74bc0128f065b41.pdf (03.05.2018)

http://www.kararlaryeni.anayasa.gov.tr/Karar/Content/94117278-50ca-4203-88f3-72a5537258a5?excludeGerekce=True&wordsOnly=False

http://www.resmigazete.gov.tr/eskiler/2011/11/20111101M1-1.htm

http://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3.pdf

http://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20180802-3.pdf

ÖZET

Bilgi ve iletişim teknolojilerindeki gelişmelerle birlikte internete bağlı cihazların ve sistemlerin artmasıyla siber uzay giderek büyümektedir. Bu büyüme aynı zamanda beraberinde çeşitli siber riskleri ve tehditleri getirmektedir. Siber tehdit ve saldırıların yıllar içindeki gelişimi incelendiğinde karmaşıklıklarının ve etki alanlarının arttığı, icra edilmeleri için gereken bilgi seviyesinin de düştüğü görülmüştür. Bu durum siber saldırıları daha da yaygın ve etkili hale getirmektedir.

Kurumlardaki iş süreçlerinin büyük ölçüde bilgi ve iletişim teknolojilerine bağlı olduğu göz önüne alındığında, siber tehdit ve saldırılar karşısında etkin bir kurumsal bilgi güvenliği sağlamak gerekmektedir. Aksi takdirde iş sürekliliğinin sağlanamaması, kurumsal itibar kaybı ve kurumlar için çok değerli hale gelen bilginin korunamaması gibi durumlarla karşılaşılmaktadır.

Bu çalışmada kurumsal bilgi güvenliğini tehdit eden siber saldırılar sınıflandırılmış, bilgi sistemlerine bulaşmak için izledikleri yol ve yöntemler anlatılmış ve verdikleri zararlardan bahsedilmiştir. Bu tehdit ve saldırılar karşısında alınması gereken teknik önlemler araştırılıp sunulmuştur.

Kurumsal bilgi güvenliğinin sağlanması için sadece teknolojik önlemlerin alınması yeterli değildir. İnsan, teknoloji ve eğitim gibi unsurları içeren bir bilgi güvenliği yönetim yaklaşımına gereksinim duyulduğu anlaşılmıştır. Bu kapsamda siber güvenlikle ilgili ulusal ve uluslararası yasal düzenlemeler incelenmiş, kurumlarda oluşturulması gereken bilgi güvenliği yönetim sistemlerinin uyumlu olması gerektiği standartlar hakkında bilgi verilmiştir.

Ülkemizde siber güvenlik alanındaki faaliyetler incelenmiş ve bu alanda kurumsal siber güvenlik organizasyonun işleyiş biçimi gösterilmiştir. Kurumsal bilgi

güvenliğinin sağlanması için gereken güvenlik kontrolleri değerlendirilerek kurum için öneriler getirilmiştir.

ARŞİV Kayıt Bilgileri

Tezin Adı	Siber Tehditler Ve Saldırılar Karşısında Kurumsal Bilgi Güvenliğinin Sağlanması
Tezin Yazarı	Mustafa Kemal BAŞOĞLU
Tezin Danışmanı	Soner BASLI
Tezin Konumu	Uzmanlık Tezi
Tezin Tarihi	Haziran 2018
Tezin Alanı	Bilgi Güvenliği
Tezin Yeri	RTÜK – ANKARA
Anahtar Kelimeler	Siber Tehdit, Siber Saldırı, Bilgi Güvenliği, Kurumsal Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi

ABSTRACT

Together with the advances in information and communication technologies, cyber space is growing with the increase of internete connected devices and systems. This growth also brings with it various cyber risks and threats. When examining the development of cyber threats and attacks over the years, it has been seen that their complexity and impact areas have increased and the level of knowledge required for their execution has dropped. This makes the cyber attacks even more common and effective.

Given that the business processes at the institution are largely tied to information and communication technologies, it is necessary to provide effective institutional information security against cyber threats and attacks. Otherwise, business continuity can not be ensured, institutional reputation is lost, and information that is invaluable for institutions can not be protected.

In this study, we describe the ways and methods of categorizing the cyber attacks that threaten the institutional information security, the ways they are infecting information systems, and the damages they have been mentioned. Technical measures to be taken against these threats and attacks have been investigated and presented.

It is not enough to take technological precautions to secure institutional information security. It has been understood that there is a need for an information security management approach involving people, technology and education. In this context, national and international legal regulations related to cyber security have been examined and information has been given on the standards that the information security management systems that should be established in the institutions should be compatible.

Activities in the field of cyber security have been examined in our country and the mode of operation of the institutional cyber security organization has been shown

in this area. Recommendations have been made for the institution by evaluating the security controls required to secure institutional information security.

Key words: Cyber Threat, Cyber Attack, Information Security, Institutional Information Security, Information Security Management System

ÖZGEÇMİŞ

Mustafa Kemal BAŞOĞLU 1981 yılında Rize'de doğdu. Ulucami İlkokulu, Mehmet Akif Ersoy Ortaokulu ve Fener Lisesi'nden mezun oldu. 2007 yılında Karadeniz Teknik Üniversitesi Mühendislik-Mimarlık Fakültesi Elektrik-Elektronik Mühendisliği bölümünde lisans eğitimini tamamladı. 2008-2015 yıllarında özel sektörde elektrik-elektronik mühendisi olarak çalıştı. 2015 yılı mayıs ayında Radyo ve Televizyon Üst Kurulu'nda uzman yardımcısı olarak göreve başladı. İyi derecede İngilizce bilen Mustafa Kemal BAŞOĞLU, evli ve bir çocuk babasıdır.