



**KURUMSAL SİBER GÜVENLİĞE YÖNELİK TEHDİTLER VE MÜCADELE
YÖNTEMLERİ: EYLEM PLANI ÖRNEĞİ**

Hakan YAŞAR

**YÜKSEK LİSANS TEZİ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ**

MAYIS 2014

Hakan YAŞAR tarafından hazırlanan KURUMSAL SİBER GÜVENLİĞE YÖNELİK TEHDİTLER VE MÜCADELE YÖNTEMLERİ: EYLEM PLANI ÖRNEĞİ adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ / OY ÇOKLUĞU ile Gazi Üniversitesi Yönetim Bilişim Sistemleri Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Danışman: Yrd. Doç. Dr. Hüseyin ÇAKIR

Gazi Eğitim Fakültesi Bil. ve Öğr. Tek. Eğitimi, Gazi Üniversitesi

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.....

Başkan: Doç. Dr. Alptekin SÖKMEN

Gazi İktisadi ve İdari Bilimler Fak. İşletme bölümü, Gazi Üniversitesi

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.....

Üye: Doç. Dr. Sami ŞAHİN

Gazi Eğitim Fakültesi Bil. ve Öğr. Tek. Eğitimi, Gazi Üniversitesi

Bu tezin kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum/onaylamıyorum.....

Tez Savunma Tarihi: 07/05/2014

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

.....
Doç. Dr. Nurettin TOPALOĞLU
Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmada;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Hakan YAŞAR

07/05/2014

KURUMSAL SİBER GÜVENLİĞE YÖNELİK TEHDİTLER VE MÜCADELE YÖNTEMLERİ: EYLEM PLANI ÖRNEĞİ

(Yüksek Lisans Tezi)

Hakan YAŞAR

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Mayıs 2014

ÖZET

Günümüzde bilgi ve iletişim teknolojilerinde çeşitli uygulamaların artarak kişilerin günlük yaşantılarının vazgeçilmez bir parçası haline gelmesiyle birlikte gerek kamu gerekse de özel sektörde birçok kurum hizmet sunumlarını siber ortamda gerçekleştirmektedir. Zaman ve coğrafi sınırlılıkların kalkarak anlık iletişim ve bilgi paylaşımının bulunduğu ve gerekli bilgi ve araçların kolaylıkla temin edilerek karmaşık ve organize saldırı ve tehditlerin gerçekleştirilebildiği bu ortamda etkin bir güvenlik anlayışının sadece ulusal ya da uluslararası alınabilecek güvenlik önlemleri ile sağlanamayacağı açıktır. Bu bağlamda siber ortamda ağırlıklı olarak saldırı ve tehditlere maruz kalan kurum ve şirketlerin kendi siber güvenliklerini sağlama adına gerekli adımları atmaları ihtiyaç olarak hissedilmektedir. Bu çalışmada son zamanların ve önümüzdeki dönemlerde de etkilerini sürdürecekleri tahmin edilen (özellikle kurumların web uygulamalarına yönelik) siber tehditler incelenmiş ve bu tehditlere karşı kurumsal bazda alınabilecek önlemler ile (genel bir çerçeve içinde) atılması gereken adımlar sunularak örnek bir kurumsal siber güvenlik eylem planı hazırlanmıştır. Ülkemizdeki kurumlara siber tehdit ve saldırılara karşı kurumsal siber güvenliklerini korumaları hususunda yardımcı olmanın amaçlandığı çalışma da görüşme ve doküman analizi gibi veri toplama yöntemleri kullanılmıştır. Çalışma sonucunda kurumsal siber güvenliğe yönelik siber tehdit ve saldırıların etki ve zararlarını arttırırken kurumların siber güvenlik konusunda yeteri kadar farkındalık taşımadığının tespit edilmesinin yanı sıra verinin gizliliği, bütünlüğü ve erişebilirliğinin hedeflendiği kurumsal siber güvenliğin kurumsal bazda alınması gereken önlemler ve (bir kurumsal siber güvenlik eylem planı doğrultusunda) atılacak temel adımlar neticesinde etkili ve sağlam kılınarak yaşayan bir süreç olarak ele alınması gerektiği anlaşılmıştır.

Bilim Kodu : 1146.2.094

Anahtar Kelimeler : Kurumsal siber güvenlik, siber güvenlik, siber tehdit

Sayfa Adedi : 149

Danışman : Yrd. Doç. Dr. Hüseyin ÇAKIR

THREATS AGAINST INSTITUTIONAL CYBER SECURITY AND FIGHTING
AGAINST THEM: SAMPLE OF ACTION PLAN

(M. Sc. Thesis)

Hakan YAŞAR

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

May 2014

ABSTRACT

Together with the increase of various applications in information and communication technologies, it has become an indispensable part of people's daily life at present. Moreover both in public and private sectors, many institutions perform their services in the cyber space. As time and geographical limitations are removed, instant communication and information sharing are possible and necessary information and tools are easily provided, sophisticated and organized attacks and threats can be done. Therefore, at such an environment, it is clear that security measures which are now taken only by national or international security precautions cannot ensure an effective understanding of security. Since institutions and companies are mainly exposed to cyber attacks and threats in cyber space, it is important that necessary steps are taken in order to provide the cyber security. In this study (within a general framework) having presented what can be done and measures which will be taken against increased and more sophisticated cyber threats at corporate level, an exemplary institutional cyber security action plan has been prepared. Also, it is aimed to help institutions in our country about threats against institutional cyber security. Interviews and document analysis were used as data collection methods. At the end of the study, two issues were found out: First, the impact and losses of threats against institutional cyber security have been increased and second, institutions do not have enough awareness about cyber security. Moreover, it is understood that effective and robust institutional cyber security which aimed at data confidentiality, integrity and accessibility need to be addressed as a living process at the end of the basic steps which will be taken in accordance with a institutional cyber security action plan and measures which will be taken at corporate level.

Science Code	: 1146.2.094
Key Words	: Institutional cyber security, cyber security, cyber threat
Page Number	: 149
Supervisor	: Assist. Prof. Dr. Hüseyin ÇAKIR

TEŞEKKÜR

Çalışmalarım boyunca her konuda değerli yardım ve katkılarıyla beni yönlendiren kıymetli hocam Yrd. Doç. Dr. Hüseyin ÇAKIR'a, siber güvenlik konusunda değerli tecrübelerini benimle paylaşan Dz. Müh. Yzb. İbrahim ŞİŞANECİ'ye zaman yönetimi ve motivasyon konusunda maddi-manevi desteklerini benden esirgemeyen eşim Nazife YAŞAR'a ve çok kıymetli varlığım kızım SELİN'e teşekkürlerimi bu vesileyle bildirmeyi borç bilirim.

İÇİNDEKİLER

	Sayfa
ÖZET.....	iv
ABSTRACT.....	v
TEŞEKKÜR.....	vi
İÇİNDEKİLER.....	vii
ÇİZELGELERİN LİSTESİ.....	x
ŞEKİLLERİN LİSTESİ.....	xi
KISALTMALAR.....	xiii
1. GİRİŞ.....	1
2. İNTERNET VE SİBER GÜVENLİK	7
2.1. İnternet	7
2.1.1. İnternet servis sağlayıcılar (ISS)	8
2.1.2. İnternet erişim sağlayıcılar (IES)	9
2.1.3. İçerik sağlayıcı (Content provider).....	9
2.1.4. Sunucu (Server).....	9
2.1.5. Host (Barındırıcı).....	9
2.2. Siber Güvenlik.....	10
2.2.1. Siber suçlar.....	12
2.2.2. Siber espionaj (Siber casusluk).....	14
2.2.3. Siber terörizm	15
2.2.4. Siber savaş.....	15
2.2.5. Siber tehdit.....	16
2.3. Kurumsal Siber Güvenlik	35
3. SİBER GÜVENLİĞE YÖNELİK KORUNMA TEDBİRLERİ.....	37
3.1. Fiziksel Korunma Tedbirleri	38
3.2. Kurumsal Korunma Tedbirleri	38

	Sayfa
3.3. İşlemsel ve Teknolojik Korunma Tedbirleri	39
3.3.1. Güvenlik duvarları.....	40
3.3.2. Antivirüs yazılımları.....	46
3.3.3. Saldırı tespit ve önleme sistemi (IDS/IPS).....	47
3.3.4. Sızma (penetrasyon) testleri	50
3.3.5. DoS engelleme sistemi.....	54
3.3.6. Veri Sızma Engelleme (DLP).....	54
3.3.7. Saldırgan tuzağı ağları (Honeynet).....	55
3.3.8. Veritabanı güvenliği.....	56
3.3.9. Bilgi güvenliği yönetim sistemleri (BGYS).....	57
4. SİBER SUÇLARA YÖNELİK HUKUKSAL BOYUT	63
4.1. Dünyada Siber Suçlara İlişkin Yapılan Çalışmalar	64
4.1.1. Avrupa Konseyi tarafından siber suçlara ilişkin yapılan çalışmalar.....	65
4.1.2. Birleşmiş Milletler tarafından siber suçlara ilişkin yapılan çalışmalar.....	67
4.1.3. ABD tarafından siber suçlara ilişkin yapılan çalışmalar.....	68
4.1.4. Fransa tarafından siber suçlara ilişkin yapılan çalışmalar.....	70
4.1.5. İngiltere tarafından siber suçlara ilişkin yapılan çalışmalar.....	71
4.1.6. Japonya tarafından siber suçlara ilişkin yapılan çalışmalar.....	71
4.2. Ülkemizde Siber Suçlara İlişkin Yapılan Çalışmalar	72
4.2.1. İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun (5651).....	73
4.2.2. Fikir ve Sanat Eserleri Kanunu (5846).....	74
4.2.3. Elektronik İmza Kanunu (5070).....	74

	Sayfa
5. SİBER GÜVENLİĞE İLİŞKİN ARAŞTIRMA VERİLERİNİN İNCELENMESİ VE DEĞERLENDİRİLMESİ.....	75
5.1. Siber Tehdit ve Saldırıların İncelenmesi	75
5.1.1. Siber tehdit ve saldırıların kurumsal siber güvenlik yönünden incelenmesi	81
5.1.2. Siber tehdit ve saldırıların etkiledikleri alanlara göre incelenmesi.....	88
5.1.3. Siber tehdit ve saldırılar ile bu tehdit ve saldırıları gerçekleştiren gruplar arasındaki ilişkinin incelenmesi.....	90
5.1.4. Siber tehdit ve saldırılarla mücadele adına yapılanların incelenmesi.....	92
5.2. Siber Suçların İncelenmesi	100
5.3. Siber Tehdit ve Saldırıların Değerlendirilmesi	103
5.3.1. Siber tehdit ve saldırıların kurumsal siber güvenlik yönünden değerlendirilmesi	107
5.3.2. Siber tehdit ve saldırılarla mücadele adına yapılanların değerlendirilmesi.....	113
5.4. Siber Suçların Değerlendirilmesi	115
6. KURUMSAL SİBER GÜVENLİK EYLEM PLANI.....	117
6.1. Kurumsal Siber Güvenliğin Sağlanmasında Dikkat Edilmesi Gereken İlkelerin Belirlenmesi	118
6.2. Siber Güvenlik Vizyon ve Misyonun Belirlenmesi	119
6.3. Kurumsal Siber Güvenlik Politikalarının Oluşturulması	120
6.4. Kurumsal Siber Güvenlik Biriminin Oluşturulması	120
6.5. Eylem Planı	122
7. SONUÇ VE ÖNERİLER.....	123
KAYNAKLAR.....	129
EKLER.....	141
EK-1. Kurumsal Siber Güvenlik Eylem Planı.....	142
EK-2. Görüşme Soruları.....	147
ÖZGEÇMİŞ.....	149

ÇİZELGELERİN LİSTESİ

Çizelge	Sayfa
Çizelge 3.1. Güvenlik testlerinin sınıflandırılması.....	52
Çizelge 3.2. Web Güvenlik Testleri Sınıflandırması.....	53
Çizelge 5.1. 2012-2013 yılları arasında siber tehdit ve siber saldırıların durumu ve sıralaması.....	76
Çizelge 5.2. Siber tehdit ve saldırıların etkiledikleri alanlara göre durumları.....	89
Çizelge 5.3. Siber saldırı ve tehditler ile bu tehdit ve saldırıları gerçekleştiren gruplar arasındaki ilişki.....	90
Çizelge 5.4. Ülkemizde ulusal düzeyde yapılan siber güvenlik yapılanma faaliyetleri.....	95

ŞEKİLLERİN LİSTESİ

Şekil	Sayfa
Şekil 2.1. Dünya çapında 2005 ile 2013 yılları arasında bireysel internet kullanım oranları.....	7
Şekil 2.2. Ülkemizde 2005 ile 2013 yılları arasında (16-74 yaş arası) bilgisayar ve internet kullanım yüzdeleri.....	8
Şekil 2.3. İnternet hizmetinin sağlanmasında kullanılan unsurlar.....	10
Şekil 2.4. Siber güvenlik çalışmalarının temel unsurları.....	12
Şekil 2.5. Siber Suçlar.....	14
Şekil 2.6. Siber tehditlerin sınıflandırılması.....	17
Şekil 2.7. XSS Yönteminin Mantıksal Gösterimi.....	18
Şekil 2.8. Sosyal mühendislik yöntemi.....	34
Şekil 2.9. Siber güvenliğin temel hedefleri.....	36
Şekil 3.1. Güvenlik duvarı temsili gösterimi.....	40
Şekil 3.2. Çift taraflı geçit (Dual-Homed Gateway Host) mimarisi.....	43
Şekil 3.3. Perdelenmiş kullanıcı (Screened Host) tipi mimari.....	44
Şekil 3.4. Perdelenmiş alt ağ (Screened subnet) tipi mimari.....	45
Şekil 3.5. Bir saldırı tespit sistemi modeli.....	47
Şekil 3.6. Saldırı tespit sistemlerinin sınıflandırılması.....	48
Şekil 3.7. BGYS Süreçlerine uygulanan PUKÖ modeli.....	58
Şekil 3.8. BGYS kurulum aşamaları.....	61
Şekil 5.1. Kategorilerine göre internet sitelerinin kötü amaçlı içerik bulaştırma durumları.....	77
Şekil 5.2. Spam hacimleri.....	78
Şekil 5.3. 2013 yılı dünya geneli spam hacmi.....	79
Şekil 5.4. Günümüzde kullanılan APT' lerin hedef seçtiği sektörler.....	80

Şekil	Sayfa
Şekil 5.5. Kullanıcılar tarafından halka açık ve güvensiz ağların kullanılma durumları.....	81
Şekil 5.6. Ziyaret sayılarına göre popüler uygulamalar.....	82
Şekil 5.7. Kurum ve şirket boyutuna göre kötücül yazılım risk durumu.....	83
Şekil 5.8. Kurum ve şirketlerin bilgi teknoloji uzmanlarının APT hakkındaki görüşleri.....	84
Şekil 5.9. Gerçek saldırı ve yazılı senaryoların uygulandığı kurum sayısı.....	85
Şekil 5.10. DDoS saldırısının sonuçları.....	85
Şekil 5.11. Port tarama saldırısının sonuçları.....	85
Şekil 5.12. Kurumlarda tespit edilen web açıklıklarının sayıları.....	86
Şekil 5.13. Meslek gruplarına göre bireylerin (16-74 yaş arası) bilgisayar ve İnternet kullanım oranları.....	88
Şekil 5.14. Siber suçluların hedeflediği 10 ülke.....	94
Şekil 5.15. Ülkemizde işlenen bazı siber suç olaylarındaki yıllık değişim oranları.....	101
Şekil 5.16. 1990 ve 2011 yılları arasında suç türlerine göre toplam dosya sayısı.....	102
Şekil 5.17. TİB tarafından erişimi engellenen internet sitesi sayısı.....	102
Şekil 6.1. Örnek bir kurumsal siber güvenlik birimi yapısı.....	121

KISALTMALAR

Bu çalışmada kullanılmış bazı kısaltmalar açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
ABD	Amerika Birleşik Devletleri
ACLU	American Civil Liberties Union, Amerikan Sivil Özgürlükler Birliği
AET	Avrupa Ekonomik Topluluğu
AK	Avrupa Konseyi
ANSI	American National Standards Institute, Ulusal Amerikan Standartları Enstitüsü
APT	Advanced Persistent Threat, Gelişmiş Kalıcı Tehditler
ARPANET	Advanced Research Projects Agency Network, İleri Araştırma Projeleri Ajansı Bilgisayar Ağı
ASP	Active Server Pages, Etkin Sunucu Sayfaları
ASSK	Avrupa Suç Sorunları Komitesi
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BGYS	Bilgi Güvenliği Yönetim Sistemleri
BM	Birleşmiş Milletler
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CERT	Computer Emergency Response Team, Bilgisayar Acil Durum Ekibi

Kısaltmalar	Açıklama
CD	Compact Disc, Yoğun Disk
CDN	Content Delivery Network, İçerik Dağıtım Ağı
CIA	The Central Intelligence Agency, Merkezi İstihbarat Ajansı
CNCI	Comprehensive National Cybersecurity Initiative, Kapsamlı Ulusal Siber Güvenlik Girişimi”
COBIT	The Control Objectives for Information and related Technology, Bilgi ve ilgili teknolojiler için kontrol hedefleri
COPA	Child Online Prevention Act , Çocukların Çevrimiçi Yayınlardan Korunması Yasası
CSRF	Cross-Site Request Forgery, Siteler arası istek sahteciliği
DDoS	Distributed Denial of Service, Dağıtık yapıyla hizmet aksattırma
DoS	Denial of Service, Hizmet Aksattırma
DHS	Department of Homeland Security, İç Güvenlik Bakanlığı
DLP	Data Loss Prevention, Veri Kaybı Önleme
DOM	Document Object Model, Belge Nesne Modeli
DVD	Digital Versatile Disc, Çok Amaçlı Sayısal Disk
ECPA	Electronic Communications Privacy Act, Elektronik Haberleşmenin Gizliliği Yasası
ENISA	European Network and Information Security Agency, Avrupa Ağ ve Bilgi Güvenliği Ajansı
FBI	Federal Bureau of Investigation, Federal Araştırma Bürosu

Kısaltmalar	Açıklama
FTP	File Transfer Protocol, Dosya Aktarım Protokolü
HIPAA	Health Insurance Portability and Accountability Act, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
HTML	Hypertext Markup Language, Hipermetin İşaret Dili
HTTP	Hypertext Transfer Protocol, Hipermetin Aktarma İletişim Protokolü
HTTPS	Hypertext Transfer Protocol Secure, Güvenli Hipermetin Aktarım İletişim Protokolü
IEC	International Electrotechnical Commission, Uluslararası Elektroteknik Komisyonu
IDS/IPS	Intrusion Detection / Prevention System, Saldırı Tespit ve Önleme Sistemi
IP	Internet Protocol, İnternet Protokolü
IPS	Intrusion Prevention System, Saldırı Önleme Sistemi
ISPA-UK	Internet Service Providers Association of United Kingdom, Birleşik Krallık İnternet Servis Sağlayıcıları Derneği
ISO	International Organization for Standardization, Uluslararası Standardizasyon Örgütü
İES	İnternet Erişim Sağlayıcı
İSS	İnternet Servis Sağlayıcı
KSOM	Kurumsal Olaylara Müdahale Birimi
KSOME	Kurumsal Olaylara Müdahale Ekibi
LDAP	Lightweight Directory Access Protocol, Basit Dizin Erişim Protokolü
MİB	Merkezi İşlem Birimi

Kısaltmalar	Açıklama
NAC	Network Access Control, Ağ Erişim Kontrolü
NSA	National Security Agency, Ulusal Güvenlik Ajansı
NSF	National Science Foundation, Ulusal Bilim Vakfı
OECD	Organisation for Economic Co-operation and Development, Ekonomik Kalkınma ve İşbirliği Örgütü
OWASP	The Open Web Application Security Project, Açık Kaynak Web Uygulama Güvenliği Projesi
PCI DSS	Payment Card Industry Data Security Standard, Ödeme Kartı Endüstrisi Veri Güvenlik Standardı
PHP	Hypertext Preprocessor, Hipermetin Ön İşlemci Betik Dili
PUKÖ	Planla–Uygula–Kontrol Et–Önlem Al
RPC	Remote Procedure Call, Uzak yordam çağrısı
SGE	Siber Güvenlik Enstitüsü
SOAP	Simple Object Access Protocol, Basit Nesne Erişim Protokolü
SNMP	Simple Network Management Protocol, Basit Ağ Yönetimi Protokolü
SQL	Structured Query Language, Yapısal Sorgulama Dili
SSI	Server Side Includes, Sunucu Taraflı Betik
STS	Saldırı Tespit Sistemleri
SNMP	Simple Network Management Protocol, Basit Ağ Yönetimi Protokolü
TCK	Türk Ceza Kanunu
TCP/IP	Transmission Control Protocol/İnternet Protocol, İletim Kontrol Protokolü / İnternet Protokolü

Kısaltmalar	Açıklama
TİB	Telekomünikasyon İletişim Başkanlığı
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
URL	Uniform Resource Locator, Tekdüze Kaynak Konumlayıcı
US-CERT	The United States Computer Emergency Readiness Team, ABD Bilgisayar Acil Durum Hazırlık Ekibi
v.b.	Ve benzeri
WAF	Web Application Firewall, Web Uygulamaları Güvenlik Duvarı
XML	Extensible Markup Language, Genişletilebilir İşaretleme Dili
XPATH	XML Path Language
XSS	Cross Site Scripting Attack, Çapraz Site Betik Saldırısı

1.GİRİŞ

İnsanoğlu var olduğu günden beri en temel ihtiyaçlarından biri güvenlik olmuştur. Yeme-içme, barınma gibi temel ihtiyaçlarından biri olan güvenlik ihtiyacı dönemin ve ortamın şartlarına bağlı olarak değişmiş, artma veya azalma göstermişse de her zaman için hissedilen bir ihtiyaç olarak kalmıştır. İlk çağlarda bu ihtiyaç genellikle fiziki güvenlik anlamında kendini göstermişse de zaman içinde toplulukların meydana getirilmesi, çeşitli yeniliklerin ortaya çıkması ve teknolojik gelişmelerle daha farklı güvenlik ihtiyaçları hissedilmiştir.

Tarım ve sanayi çağlarından sonra evrensel anlamda yeni bir dönüşüm olarak nitelendirebilen (bilişim çağı olarak da adlandırılan) 21. yüzyılda, bilişim sistemlerinin kullanımının hızla yaygınlaşmakta olduğu ve hayatımızın her noktasında önemli roller üstlendiği görülmektedir. Bunun yanında günümüzde teknolojik yeniliklerin had safhaya gelmesi, bilgi ve iletişim teknolojilerinde çeşitli uygulamaların artarak kişilerin günlük yaşantılarının vazgeçilmez bir parçası haline gelmesi ve internet gibi zaman ve coğrafi sınırlılıkların kalkarak anlık iletişim ve bilgi paylaşımının bulunduğu ortamlarla birlikte siber güvenlik gibi farklı bir ihtiyaç türünün oluştuğu gözlenmektedir. Siber güvenlik kavramı, genel manada ulusal ve uluslararası bir ihtiyaç gibi düşünülse de; bir toplumda bütünün güvenliği, kurumların hatta birey bazında kullanıcıların güvenliğinin sağlanmasıyla daha kalıcı ve sağlam olacaktır. Günümüz siber ortamında saldırılara ağırlıklı olarak kurum ve şirketlerin maruz kaldığı bilinmektedir. Kurum ve şirketlere yönelik bu saldırıların giderek artan bir çizgide ilerlemesine ve saldırı riskinin artmasına:

- Siber ortamda saldırı için gerekli yazılım ve bilginin ucuz ve kolay elde edilebilir olması,
- Dünyanın herhangi bir yerinden herhangi bir zamanda kişi veya sistemlerin kasıtlı ya da kasıtsız olarak bu saldırılara katılmalarının mümkün olması,
- Siber uzayın bütüncül ve kesintisiz iletişime açık yapısı nedeniyle kötücül yazılım ve benzeri tehditler ile yapılan saldırılar yoluyla sistemlerin birbirine zarar vermesi,

- Çok geniş kitlelere ulaşan kritik hizmet ve servislerin artarak bilişim sistemleri tarafından veriliyor olması,
- Birçok kurum ve şirketin kritik altyapılarının internete bağlı olması,
- İnternet kullanıcılarının çoğunun siber güvenlik bilincinin yetersiz olması,
- Saldırılara maruz kalma ihtimali olan kurum ve şirketler arasındaki işbirliği eksiklikleri,
- Kurumların genelde itibar ve pazar kaybı gibi nedenlerle kendilerine yapılan saldırıları gizlemesi,
- Kurumlarda bilgi güvenliği yönetiminin yeterli düzeyde olmaması,
- Kurumların üst düzey yöneticilerinin siber güvenlik hususunda yeteri kadar bilinçli olmamaları ve sahiplenmemeleri,
- Kurumların siber güvenlik konusunda yeterince iyi yapılandırılmış olmamaları ve güvenliğin sadece bilgi işlem birimlerinin sorumluluğu olarak görülmesi ve bu birimlerde çalışan personelin de yeterli seviye ve tecrübe de olmaması,
- Siber güvenliği ihlal eden olayların detaylı araştırılmasıyla ve oluşan suçun soruşturulmasıyla ilgili az sayıda yetkin personelin olması,
- Kurumların denetim süreçlerinde siber güvenliğe ilişkin denetimlerin yeterli seviyede olmayışı, donanım ve yazılım noktasında güvenli üretilimin yetersizliği gibi faktörler neden olmaktadır.

Siber korsanların geçmişe nazaran daha organize hale geldikleri günümüzde kurum ve şirketlere yapılan saldırı ve tehditler her geçen gün artarak devam etmekte ve daha kompleks bir yapıya bürünmektedir. Buna karşın maalesef siber güvenlik kavramının (yapılan ulusal tatbikatlarda da ortaya çıktığı üzere) ülkemizdeki kurumlar tarafından yeterince ve doğru anlaşılamadığı görülmektedir. ISC TURKEY 2012 (5th International Conference on Information Security and Cryptology) sonuç bildirgesinde de belirtildiği gibi kurumların %61'inin kendilerini (özellikle web ortamından gelen) siber saldırıların hedefinde gördüğü (siber uzay diye tabir edilen sanal) ortamda siber güvenlik planı oluşturarak temel ve gerekli önlemleri almaları gerekmektedir. Ayrıca, eskiden sistemlere yapılan saldırılar daha çok sistemlerdeki bilgiye sızıp yeteneklerini göstermek isteyenlerin bireysel faaliyetleri iken artık belirli hedeflere daha organize ve karmaşık yapıda saldırılar

düzenlenerek kurum ve şirketlere maddi zarar verme ya da bu kurum ve şirketlerden elde ettikleri bilgilerle kazanç sağlamaya yönelik ekonomik amaçlar hedeflenmektedir. Bu tür saldırılara maruz kalan kurum ve kuruluşların maddi yönden zarara uğramalarına kıyasla müşteri, itibar ve pazar kaybı gibi uğradıkları zararlar çok daha ciddi boyutta olmaktadır. Bu nedenle çeşitli şekillerde siber ortamda hizmet sunan kurumların bu tür saldırılar gerçekleşmeden öncesinde, saldırı esnasında ve de saldırı sonrası oluşabilecek durumlara hazırlıklı olmaları için kendilerine ait bir kurumsal siber güvenlik planı oluşturmaları gerekmektedir. Ayrıca, günümüzde siber ortamın zorunluluk haline gelmesi ile birlikte bilgi sistemlerini ve teknolojilerini bu ortamda kullanan kurum ve şirketlerin, siber tehdit ve saldırıların hedefi haline gelmesi de; kurumsal siber güvenliklerini sağlama adına gerekli ve temel önlemleri yerine getirerek daha etkin mücadele yeteneği kazanmalarını zorunlu kılmaktadır.

Tüm bu hususlara karşın, siber güvenlikle ilgili yapılan çalışmaların genellikle ulusal ve uluslararası boyutta olması nedeniyle kurumsal siber güvenlikle ilgili çalışmalara ihtiyaç hissedilmektedir.

Bu çalışmanın genel amacı, kurumsal siber güvenliğe yönelik tehdit ve saldırılar ile korunma ve mücadele yöntemlerini belirleyerek taslak bir kurumsal siber güvenlik eylem planı hazırlamaktır. Bu genel amaca ulaşabilmek için belirlenen alt amaçlar şunlardır:

1. Kurumsal siber güvenlikte temel amaç ve hedefler nelerdir?
2. Kurumsal siber güvenliğe yönelik siber tehdit ve saldırılar nelerdir?
3. Kurumsal siber güvenliğe yönelik siber tehdit ve saldırılara karşı korunma yöntemleri nelerdir?
4. Kurumsal siber güvenliğe yönelik tehdit ve saldırılarla mücadele adına yapılanlar nelerdir?
5. Siber güvenliğe ilişkin dünyada ve ülkemizdeki hukuki düzenlemeler nelerdir?
6. Kurumsal siber güvenliği sağlama adına kurumsal bazda yapılabilecekler nelerdir?

7. Kurumsal siber güvenliği sağlamak maksadıyla oluşturulacak kurumsal siber güvenlik eylem planına ilişkin olarak:

- a) Kurumsal siber güvenlik eylem planı oluşturma'nın kurumlara sağlayacağı faydalar nelerdir?
- b) Kurumsal siber güvenlik eylem planı oluşturma'nın amacı nedir?
- c) Kurumsal siber güvenliğin sağlanmasında dikkat edilmesi gereken ilkeler nelerdir?
- d) Kurumsal siber güvenlik politikalarının kapsamı (içeriği) ne şekilde oluşturulmalıdır?
- e) Etkin bir kurumsal siber güvenlik sağlama adına oluşturulacak kurumsal siber güvenlik birimine(KSGB) bağlı olarak görev yapacak birimler neler olmalıdır?
- f) Kurumsal siber güvenlik eylem planında bulunması gereken eylem maddeleri nelerdir?
- g) Eylem planında bulunması gereken maddelerdeki her bir eyleme ilişkin sorumlu ve ilgili kurumsal birimler nelerdir?

Bu çalışma ile siber tehdit ve saldırıların etkilerinin artarak devam ettiği günümüzde kurumsal siber güvenlik kavramının net olarak anlaşılması, kurumsal siber güvenliğe yönelik tehdit ve saldırılar hususunda farkındalık bilinci oluşturarak (veya arttırarak) bu tehdit ve saldırılara karşı etkin ve verimli mücadele yeteneği kazandırılması, kurumsal siber güvenliğe ilişkin yapılmış öncü çalışmalardan biri olması nedeniyle (alanyazında örnek bir çalışma niteliğinde) sonraki araştırmalara kaynaklık ederek daha kapsamlı araştırmaların yapılmasına aracılık etmesi hedeflenmektedir.

Bu çalışmada ulaşılmak istenen verilerin elde edilmesinin zorluğu ve uzman görüşlerine olan ihtiyaç nedeniyle görüşme ve doküman analizi gibi veri toplama yöntemleri kullanılarak araştırmacının kendisinin veri toplamada merkezi konumda olduğu nitel araştırma yöntemlerinden yararlanılmıştır[107]. Yerli ve yabancı çalışmaların incelenip siber güvenlik alanında bilirkişi konumunda bulunan 2 bilişim uzmanının görüşlerinin değerlendirilmesi neticesinde görüşme soruları ve alt başlıkların belirlendiği çalışmada yaşları 25 ile 35 arasında değişen ve 2 ile 7 yıl

arasında deęişen görev sürelerine sahip siber güvenlikle ilgili birimlerde çalışan 10 personel ile görüşölmüştür. Görüşme yapılan kişilerin siber güvenlik alanında yeterli bilgi sahibi olmalarının ön koşul kabul edildięi çalışma da kurumsal siber güvenliğe ilişkin temel kavramlar ile bu tehdit ve saldırılara karşı alınacak önlemler ve mücadele yöntemlerini saptayabilmek için (döküman analizi kapsamında) siber güvenlik alanında yetkinliğe sahip ulusal ve uluslar arası kurum ve kuruluşların sunduęu raporlar ile yerli ve yabancı çalışmalar incelenmiş, siber tehdit ve saldırılara karşı (genel bir çerçeve içinde) kurumsal bazda atılması gereken temel adımların ve kurumsal siber güvenlik eylem planına ilişkin verilerin belirlenmesi amacıyla yapılan görüşmede de katılımcılara toplam 10 soru yöneltilmiştir.

Siber güvenliğe yönelik tehdit ve saldırılar ile siber suçların siber güvenliğe ilişkin etkilerini tespit etmek maksadıyla (alt başlıkların hazırlanmasında önerilerinin alındıęı uzmanların görüşlerinin de deęerlendirilmesi neticesinde) siber suçlar ve siber güvenliğe yönelik tehdit ve saldırılar olmak üzere 2 başlık altında incelemeler yapılmıştır. Ayrıca, siber güvenliğe yönelik tehdit ve saldırılarında;

- Siber tehdit ve saldırıların etkiledikleri alanlar,
- Tehdit ve saldırıları gerçekleştirenler arasındaki ilişki,
- Tehdit ve saldırılarla mücadele adına yapılanlar,
- Kurumsal siber güvenlik

bakımından olmak üzere 4 alt başlığa ayrılarak incelenmesinin daha sağlıklı verilerin elde edilmesini sağlayacaęı düşünölmüştür. Bu bağlamda elde edilen verilerin (tez çalışmasının içeriğini ve kapsamını yansıtacak şekilde) siber tehdit ve saldırıların;

- Tehdit ve saldırılarla mücadele adına yapılanlar,
- Kurumsal siber güvenlik

yönünden olmak üzere 2 alt başlıkta ve siber suçlarında ayrı bir başlık altında deęerlendirilmesi uygun görölmüştür.

Alanyazında yeni bir kavram olması, kurumsal siber güvenliğe ilişkin yapılmış öncü çalışmalardan biri olması, siber uzaydaki yenilik ve gelişmelere paralel olarak siber tehdit ve saldırıların her geçen gün çeşitlenerek artması, bu tehdit ve saldırılara karşı gerçekleştirilecek korunma ve mücadele yönteminin her kurumun kritik bilgi ve iletişim altyapısına göre farklılık arz edebilmesi ve belirtilen birçok alt başlığın dahi ayrı bir tez konusu olabilecek kadar geniş bir içeriğe sahip olmasından dolayı her konu hakkında ayrıntılı bilgiler sunulamaması çalışmanın sınırlılıklarını oluşturmaktadır.

Beş farklı bölümden oluşan çalışmanın *birinci bölümünde*; konunun daha iyi anlaşılabilmesi için (literatür taraması sonucu) internet, siber suç, (siber tehdit ve saldırıların da içinde bulunduğu) siber güvenlik, kurumsal siber güvenlik ile ilgili temel kavramlar ele alınarak açıklamalar yapılmıştır.

İkinci bölümde kurumsal siber güvenliği sağlama adına yerine getirilmesi gereken korunma önlemlerinden, *üçüncü bölümde* ise siber güvenliğe ilişkin dünyada ve ülkemizdeki hukuki düzenlemelerden bahsedilmiştir.

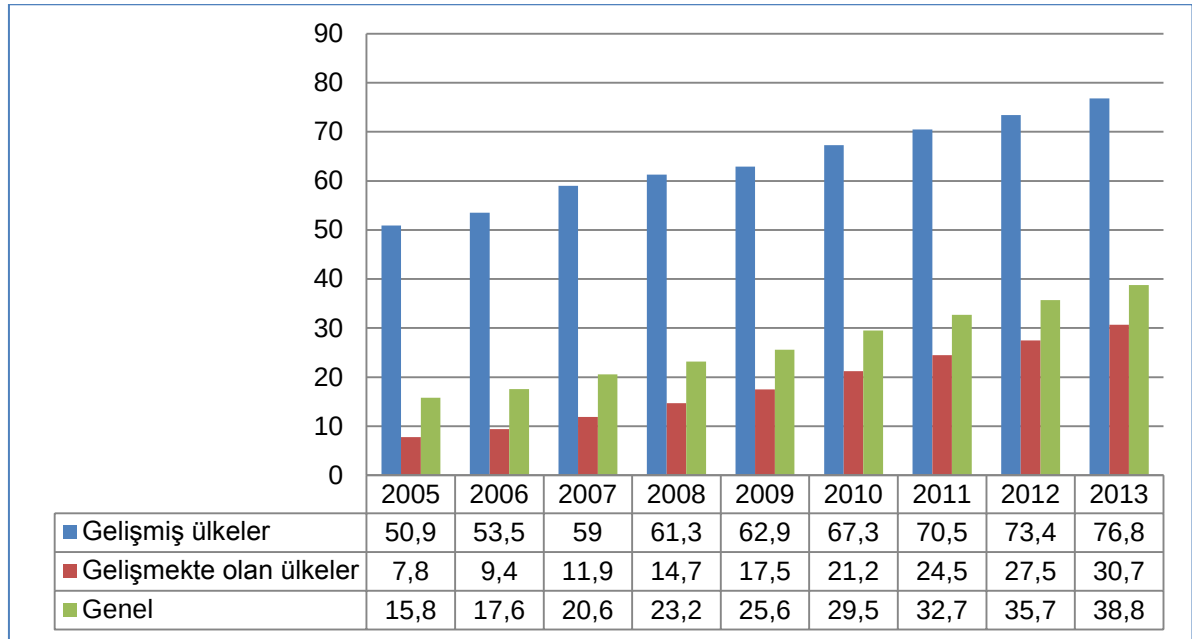
Dördüncü bölümde ise kurumsal siber güvenliğe yönelik tehditler ve bu tehditlerle mücadele adına yapılanlara ilişkin veriler incelenerek elde edilen bulgulara ilişkin analizler yapıp çalışmanın genelini kapsayacak şekilde değerlendirmelerde bulunulmuş ve siber güvenlik hususunda önde gelen bazı kurum ve kuruluşların değerlendirmelerine yer verilmiştir.

Son bölümde ise bilişim uzmanları ile yapılan görüşmeler neticesinde elde edilen verilerin değerlendirilerek kurumsal siber güvenlik eylem planı oluşturulurken yapılması gerekenler belirlenmiş ve taslak bir kurumsal siber güvenlik eylem planı hazırlanmıştır.

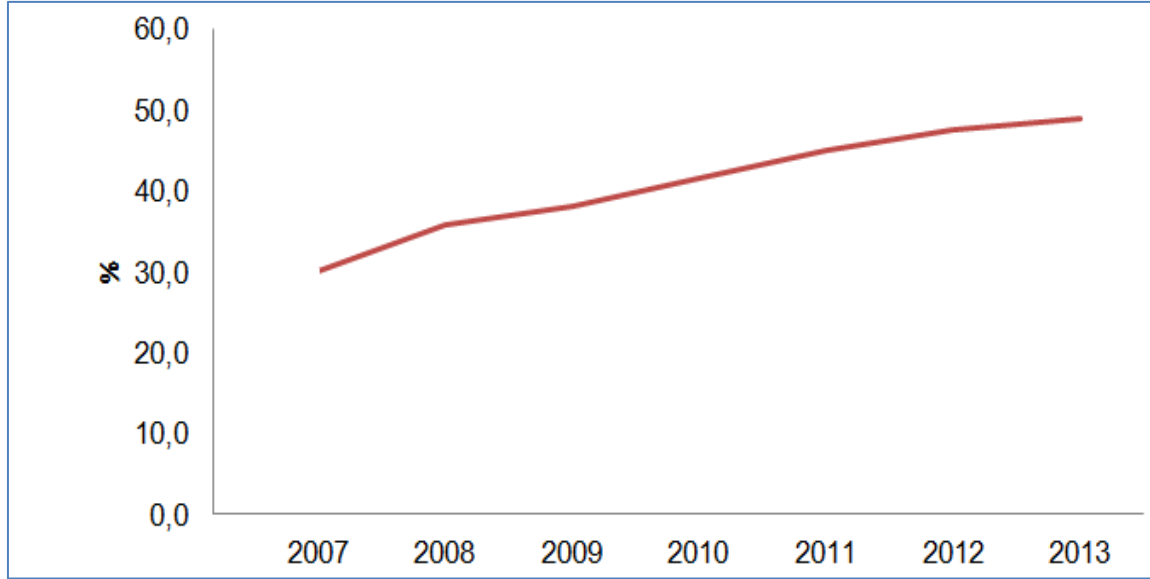
2. İNTERNET VE SİBER GÜVENLİK

2.1. İnternet

Dünya üzerinde milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan küresel bir ağı ifade eden internetin tarihçesi, ABD Savunma Bakanlığı'nın himayesinde İleri Savunma Araştırma Projeleri Kurulu'nun (Advanced Research Project Agency – ARPA) desteğiyle 1971 yılında 23 bilgisayarın birbirine bağlı olduğu ARPANET adlı ağa dayanmaktadır. ARPANET'e bağlı bilgisayarların birbirleriyle aynı özellikte olmamalarından dolayı ortaya çıkan sorunları halledebilmek için İnternet Protokolleri (Transmission Control Protocol/İnternet Protocol- TCP/IP) adı verilen ortak bir dil geliştirilmiştir[97]. ARPANET'e bağlanan bilgisayarların zamanla artması sonucunda önce Ulusal Bilim Vakfı (NSF- National Science Foundation) tarafından kurulan NSFNET adlı ağ sistemi kurulmuş sonrada 1990 yılında artan bağlantı sayısı ile birlikte günümüzdeki şeklini alan internet yapısı ortaya çıkmıştır[80].



Şekil 2.1. Dünya çapında 2005 ile 2013 yılları arasında bireysel internet kullanım oranları[84]



Şekil 2.2. Ülkemizde 2005 ile 2013 yılları arasında (16-74 yaş arası) bilgisayar ve internet kullanım yüzdeleri[95]

Günümüzde tüm dünyada olduğu gibi ülkemizde de internet kullanım oranı giderek artmaktadır(Şekil 2.1 ve Şekil 2.2). Bilgisayarların birbirleri ile internet üzerinden haberleşebilmelerini ve veri paylaşımı yapabilmelerini sağlayan TCP/IP (İnternet Protokolleri) haricinde internette kullanılan (dosya alma ve gönderme protokolü (FTP-File Transfer Protocol), Elektronik Posta İletişim Protokolü (SMTP-Simple Mail Transfer Protocol), Hiper Metin Transfer Protokolü (HTTP-Hyper Text Transfer Protocol) gibi) birçok protokol vardır. Tüm bu protokollerin kullanılmasıyla internet üzerinden dünyanın dört bir tarafındaki tüketicilere ürün sunabilme, 24 saat kesintisiz bankacılık hizmeti sunabilme, çeşitli eğitim-öğretim faaliyetlerini gerçekleştirebilme ve tapu, vergi gibi bir takım işlemleri yapabilme v.b. imkanlarının olması internete eşsiz bir konum sağlamaktadır. Tüm bu anılan hizmetlerden kullanıcılar bazı unsurlar yardımıyla yararlanabilmektedir.

2.1.1. İnternet servis sağlayıcıları (İSS)

Kullanıcıların internete bağlanmalarını, internet üzerinden birbirleriyle iletişim kurmalarını ve internetin sağladığı imkânları kullanabilmelerini sağlayan aracı kurumlardır. İSS' ler başkalarının hazırladığı içerikleri kendi sunucularında saklayabilme ve sakladıkları bu içeriği siber ortama aktarabilme yeteneğindedirler.

Bu özellikleri nedeniyle de internet servis sağlayıcılarının hukuki sorumluluğu bulunmaktadır.

2.1.2. İnternet erişim sağlayıcıları (İES)

Başkalarına ait verilerin saklanmadığı yalnızca başkalarına ait içeriklere ulaşılmasına aracılık eden internet öznesi diyebileceğimiz erişim sağlayıcılar, ISS'ler gibi suç teşkil eden içerikten sorumlu değildir[12].

2.1.3. İçerik sağlayıcı (Content provider)

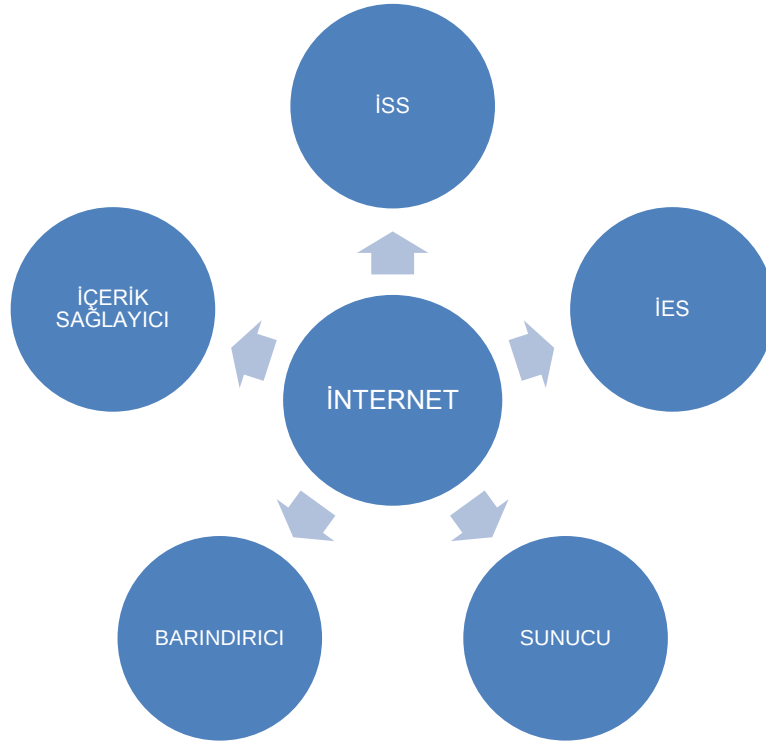
İnternet kullanıcılarının eriştiği (bir web sayfasının içeriği gibi) bir içeriği hazırlayan veya bizzat üretirler.

2.1.4. Sunucu (Server)

Belli bir kapasitesi olan ve diğer bilgisayarlara hizmet sağlayan bir bilgisayar veya yazılım olan sunucular aynı zamanda digital bilgilerin de saklandığı manyetik bir ortam sunmaktadırlar. Bir internet kullanıcısı kendi başına sunucu hizmeti verebileceği gibi başkalarına ait bilgileri saklayarak da aynı hizmeti sunabilmektedir. Ancak başkalarına ait bilgileri saklarken aynı zamanda kendisi de internete bağlantı kurabilme özelliğine sahipse artık İSS statüsüne girmiş sayılır ve ona göre hukuki sorumluluklar taşır[67].

2.1.5. Barındırıcı (Host)

İnternete bağlı bulunan bilgisayara barındırıcı (host), İSS tarafından yayınlanmak istenen sayfaların, resimlerin veya dokümanların internet kullanıcıları tarafından erişebileceği bir bilgisayarda tutulması da barındırmadır(hosting)[103].



Şekil 2.3. İnternet hizmetinin sağlanmasında kullanılan unsurlar

2.2. Siber Güvenlik

Bilgisayar veya bilgisayar ağlarını ilgilendiren veya içeren kavram yahut varlıkları tanımlamak için kullanılan *siber* kelimesi ve birbiriyle bağlantılı donanım, yazılım, sistem ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılan *siber uzay* kelimeleri günümüzde sıkça telaffuz edilmektedir[15]. İnternetin kullanımının artması ve bilgi sistem teknolojilerinin gelişmesiyle birlikte siber uzayda meydana gelen saldırı ve tehditlerin artması ve daha sistematik, kompleks bir yapıya bürünmesi neticesinde siber güvenlik ihtiyacının gerek bireysel bazda olsun gerekse kurumsal ve ulusal bazda olsun en önemli hususlardan biri haline geldiği görülmektedir. Bu bağlamda siber güvenlik (Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda belirtildiği üzere);

Siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sistemlerin yaşanan bir siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade eder.

şeklinde ifade edebildiği gibi, Bilgi Teknolojileri ve İletişim Kurumu(BTK) tarafından yapılan “siber güvenlik, siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür[19].” şeklinde bir ifade ile de yapılmaktadır.

Günümüzde siber tehditlerin (karmaşıklıkları ve gelişmişlikleriyle orantılı olarak) yüksek oranda zarar verici eylemlerde bulunabilmeleri siber güvenlikle ilgili yapılacak çalışmaların önemini arttırmaktadır. Bu bağlamda, siber güvenlikle ilgili yapılacak çalışmalarda bulunması gereken unsurlar:

- Siber güvenlikle ilgili yapılacak tüm çalışmaların belli bir hedef doğrultusunda ilerlemesi şeklinde tarif edilen *ulusal politika ve stratejinin geliştirilmesi*,
- Caydırıcılık unsurunun oluşumunu ve (gelişen teknolojiye paralel olarak ortaya çıkan siber tehdit ve saldırıların cezalandırılarak) ulusal mevzuattaki eksikliklerin giderilmesi anlamına gelen *yasal çerçevenin oluşturulması*,
- Geliştirilecek tüm hukuki düzenlemelerin yanı sıra yazılım, donanım ve iş süreçlerinin kalitesini artırma anlamında *teknik tedbirlerin geliştirilmesi*,
- Siber güvenliğin bütüncül bir yapıda gerçekleştirilebilmesi için belirli bir kurum belirlenerek bu kurumun görev ve sorumluluklarının yanında diğer paydaşlarla çalışma şekillerinin yasal açıdan net olarak saptanması olarak ifade edilen *kurumsal yapılanmanın belirlenmesi*,
- Siber güvenliğin sağlanmasında belirli sorumlulukları olan birimler arasında işbirliği ve koordinasyonu sağlama anlamına gelen *ulusal işbirliği ve koordinasyonun sağlanması*,
- Siber tehdit ve saldırılarla etkin bir mücadele için yazılım, donanım ve uygulama geliştiriciler, hakim, savcı ve siber suçlarla ilgilenen kolluk kuvvetlerinin teknik ve idari yeteneklerinin geliştirilmesini sağlama anlamında *kapasitenin geliştirilmesi*,
- Daha önceden de belirtildiği gibi gelişen siber tehdit ve saldırılar ile bunlara yönelik güvenlik önlemleri konusunda eğitim kuruluşlarının ve (kitle iletişim araçları vasıtasıyla) son kullanıcıların bilgilendirilerek farkındalık düzeylerinin artırılmasını sağlama anlamında *farkındalığın artırılması*,

- Ülkeler arasında yapılacak bir işbirliği ve bunun neticesinde de ülke mevzuatlarının birbirine uyumlu hale getirilmesi ve bilgi paylaşım mekanizmalarının oluşturulmasını sağlama olarak tarif edilen *uluslararası işbirliği ve uyumun sağlanması*[74].



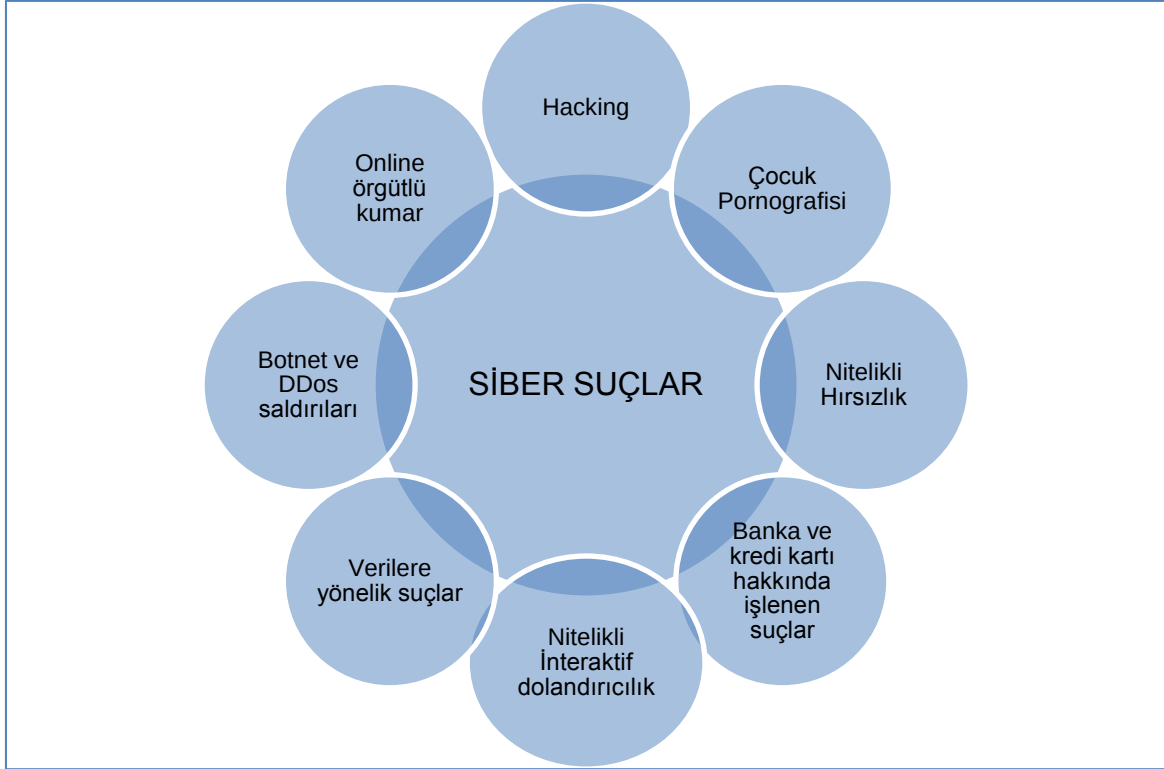
Şekil 2.4. Siber güvenlik çalışmalarının temel unsurları

2.2.1. Siber suçlar

Teknolojinin artmasıyla birlikte hayatımızdaki kolaylıkların artmasına paralel olarak siber suç kavramı da artmış ve kavram olarak değişime uğramıştır. Bir bilişim sistemini ve bu sisteme bağlı verileri ve insanları hedef alarak bu bilişim sisteminin güvenliğini ihlal eden suçlar olarak tanımlanabilen siber suçların en önemli özelliği; bir bilişim sistemi olmadan işlenememesidir. Ancak bilişim sistemlerinin kullanıldığı her eylemin siber suç kategorisine sokulamayacağı açıktır. Çünkü siber suçlar sözleşmesi gereğince bir bilişim sistemine izinsiz ve hukuka aykırı bir şekilde girilmesi ve sonrasında yapılan eylemler kastedilmektedir. Bu bağlamda; bir sisteme girerek zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme,

sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemleri (bu hususa ilişkin olarak) örnek göstermek mümkündür. Siber suçları genel olarak:

- Kişinin bilgisi ve izni olmadan hukuka aykırı bir şekilde bir bilişim sistemine yetkisiz erişim anlamına gelen ‘Hacking’
- Yetkisiz ve hukuka aykırı erişimden sonra verilerin sistemdeki verilere eklenmesi, verilerin silinmesi, değiştirilmesi, şifrelenmesi, çalınması verilere erişimin engellenmesi, yeni veri eklenmesi anlamında ‘Verilere yönelik suçlar’
- Daha önceden zararlı yazılım yüklemek suretiyle ele geçirilen (bot tabir edilen) sistemlere komut göndermek suretiyle herhangi bir internet sitesine çok sayıda istek göndererek farklı kullanıcılar tarafından erişilmesini engelleme anlamında ‘Botnet ve DDoS saldırıları’
- 15 yaşından küçük (büyük olsa da akli yetersizliğe sahip) kişilerin bedenlerinin bir bölümü veya tamamının görüntülenmesi, kaydedilmesi, depolanması ve yayınlanması suçlarını kapsayan ‘Çocuk pornografisi’
- Türk Ceza Kanunu’ na göre kumar oynamaya yer ve imkân sağlamak suçtur. Bu nedenle web ortamında kumar oynamaya yönelik yer ve imkân sağlayan faaliyetler kapsamında siber suç olarak değerlendirilen ‘Çevrimiçi (Online) örgütlü kumar’
- Banka ve kredi kurumlarının aracı olarak kullanılması yoluyla yapılan bu tür dolandırıcılık suçlarında sahte e-posta ve internet siteleriyle kullanıcıların kişisel verileri elde edilip bu verilerin kullanılması suretiyle menfaat temini sağlanan ‘Nitelikli interaktif dolandırıcılık’
- Bir bilişim sisteminde veya bilişim sistemleri arasında aktarılan verilerin (zararlı yazılımlar kullanılarak) yetkisiz ve izinsiz olarak ele geçirilmesi anlamında ‘Nitelikli hırsızlık’
- Sahibinin izni ve bilgisi dışında banka ve kredi kartları üzerinde bulunan manyetik kart bilgilerinin kopyalanması veya bilişim sistemleri üzerinden çalınarak (hukuka aykırı şekilde) kullanılmasıyla oluşan suçlar kapsamında ‘Banka ve kredi kartı hakkında işlenen suçlar’ olmak üzere 8 farklı kategori altında sınıflanmaktadır[28].



Şekil 2.5. Siber Suçlar

Yukarıda sayılan suçlar haricinde ulusal ve uluslar arası alanda görülen farklı siber suçlar da bulunmaktadır.

2.2.2. Siber espionaj (Siber casusluk)

Hedef bilgisayara izinsiz olarak (güvenlik sistemini kırarak) girmeyi ya da izinsiz olarak girilen bilgisayardan bilgilerin kopyalanmasını veya takip edilmesini ifade eden siber casusluğun (siber espionaj) uluslararası kurum ve şirketler tarafından kullanımı giderek artmaktadır. Devletler tarafından yürütülen siber espionaj faaliyetlerine ABD ve Avrupa kaynaklı büyük ölçekte şirketlerin destek verdiği belirtilmektedir. Kurum ve şirketlerin artarak devam etmekte olan bu tür saldırılara karşı kendilerini hedef olarak algılamamalarından dolayı yeterli ve gerekli güvenlik önlemlerini almadıkları belirtilmektedir. Kurumsal siber güvenliğe karşı yapılan siber casusluk faaliyetleri (genel olarak) phishing (sazan avlama) ve sosyal mühendislik yöntemleri kullanılarak hedef kurumda çalışan personelin sistemini ele geçirip kurumsal ağ vasıtasıyla birçok veriye ulaşılmasını kapsamaktadır. Saldırganlar saldırı yapacakları şirket ve kurumlarda çalışan personellerle sosyal ağlar üzerinden iletişime geçerek kurum ve şirketler hakkında bilgi toplama

faaliyetleri de yürütebilmektedirler. Siber casusluk faaliyetleri (başta Çin olmak üzere) birçok devlet tarafından desteklenip yönlendirilmekte hatta bu tür faaliyetlerde bulunmak üzere personel istihdamı bile sağlanmaktadır. Tüm bunlar sonucunda elde edilen veriler, ülkelerin ticari kurum ve şirketlerine servis edilerek haksız kazanç elde edilmesine neden olmaktadır. Echelon ve Promis gibi yazılımların siber casusluk faaliyetlerinde kullanıldığı hesaba katıldığında elde edilebilecek verinin miktarının oldukça fazla olacağı açıktır. Siber espionaj faaliyetlerine örnek olarak; ABD Enerji Bakanlığına bağlı Oak Ridge Ulusal Laboratuvarının (2007 yılı sonunda) 12.000' den fazla çalışanına gönderilen e-postalarla kötücül yazılımlar barındıran sitelere yönlendirilmesi neticesinde kullanıcı bilgisayarlarına zararlı yazılımların yüklenmesiyle birlikte saldırganların veritabanına ulaşmasının yanında sisteme bağlı diğer veritabanlarına da erişim imkânı kazanması gösterilmektedir[1].

2.2.3. Siber terörizm

Siber terörizm, sistemlere ve verilerin depolandığı yerlere, devleti ve ülke içindeki insanları korkutma veya baskı altına alma amacıyla yapılan saldırılar şeklinde tanımlanmaktadır. İnternetin kolay erişim imkânı, devlet tarafından herhangi sansürleme uygulamasından uzak, dünya çapında çok büyük kitlelere ulaşabilme imkânı, sesli ve görüntülü iletişim, hızlı bilgi akışı gerçekleştirebilme, ucuz maliyet gibi faktörleri, organize örgütler kadar terörist gruplar için de propaganda yapma, adam kazanma, eğitim verme ve korku salma gibi eylemler gerçekleştirmesine olanak tanımaktadır. Kritik alt yapılarını internet üzerinden denetleyen ve devam ettiren ülkelerin siber terör faaliyetlerinden daha fazla etkileneceği değerlendirilmektedir. Siber terör faaliyetleri, devlet kurumları ve alt yapılarına yönelik olabileceği gibi özel sektördeki faaliyetlere de odaklanabilmektedir. Örneğin, 2000 yılında bir saldırgan Avustralya' da bir kentin atık yönetim sistemine sızarak milyonlarca litre lağım suyunun parklara ve koylara boşalmasına sebebiyet vererek büyük bir çevre felaketinin yaşanmasına neden olmuştur[85].

2.2.4. Siber savaş

Önümüzdeki dönemlerde askeri harekâtları ayrı bir platforma taşıyacağı düşünülen ve (zarar vermek amacıyla) bir devletin başka bir devletin bilgisayar ve

ağ sistemlerine sızması olarak tanımlanan siber savaş olgusunun kapsamını daha iyi anlamak için Rusya'nın Gürcistan'a karşı 2008 yılında gerçekleştirdiği siber savaş harekâtı bu konuda iyi bir örnektir. Rusya gerçekleştirdiği hizmet aksattırma saldırıları ile dünya bankalarının Gürcistan ile bağlantılarını koparmış ve ülkedeki bankaları işleyemez hale getirerek kredi kartı ve cep telefonu kullanımlarını engellemiştir[104].

Çin ve ABD arasında gelecekte çok büyük etkilerinin olacağına inanılan siber savaş olgusunda ülkelerin enerji, ulaşım ve iletişim gibi kritik alt yapıları birer hedef konumundadırlar. Ülkeler kritik alt yapılarına ait güvenlik açıklıklarını keşfetmeye yönelik araştırmalar yürütmekte ve elde edilen bu bilgilerden de faydalanabilmeyi ummaktadırlar. Ayrıca ABD İç Güvenlik Bakanlığı'na(DHS-Department of Homeland Security) bağlı Ulusal Siber Güvenlik Birimi'nin 2008 yılında gerçekleştirdiği (18 federal birim ve 40 özel şirketin katıldığı) 'Siber Fırtına' adlı eğitim siber savaşın kaçınılmaz olduğu düşüncesini akla getirmiş ve eğitim sonucunda da siber saldırı ve tehditlere karşı kamu ve özel sektörün ortak hareket etmesi gerektiği vurgulanmıştır[1].

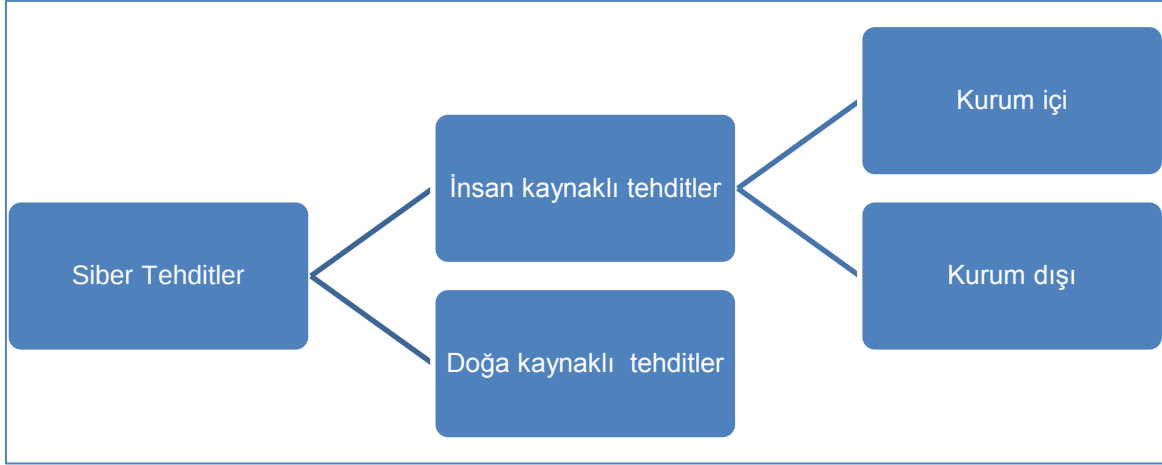
2.2.5. Siber Tehdit

Siber ortamda bulunan verinin gizliliği, bütünlüğü ve erişilebilirliğine yönelik istenmeyen durumlara yol açabilme yeteneği şeklinde tanımlanabilen siber tehditler, siber ortamdaki güvenlik açığını kullanma potansiyeline de sahip olabilmektedirler. Kurumsal siber güvenliğe yönelik tehditleri aşağıdaki gibi gruplamak mümkündür:

a. İnsan kaynaklı tehditler:

- (1) *Kurum içi:* Eğitimsiz ve bilinçsiz kullanıcılar, casuslar ve art niyetli personel davranışları, sistem yöneticisi hataları v.b...
- (2) *Kurum dışı:* İnternet ortamından gelen tehditler ile yetkisiz ve izinsiz erişim, casusluk, hırsızlık v.b. faaliyetler...

b. Doğa kaynaklı tehditler: Sel, yangın, deprem v.b...



Şekil 2.6. Siber tehditlerin sınıflandırılması

Günümüzde kurum ve şirketlerin özellikle internet ortamından gelen siber tehditlere maruz kaldığı bilinmektedir. Bu bağlamda (Avrupa Ağ ve Bilgi Güvenliği Ajansı(ENISA)'nın 250'nin üzerinde raporu inceleyerek elde etmiş olduğu veriler ışığında) son zamanların ve önümüzdeki dönemlerde de etkilerini sürdürecekleri tahmin edilen (özellikle kurumların web uygulamalarına yönelik) siber tehditlerle birlikte kurumsal siber güvenliği sağlama adına dikkat edilmesi gereken bazı güvenlik açıklıkları aşağıda maddeler halinde sayılarak kısaca açıklanmaktadır.

İzinsiz indirmeler (Drive by download)

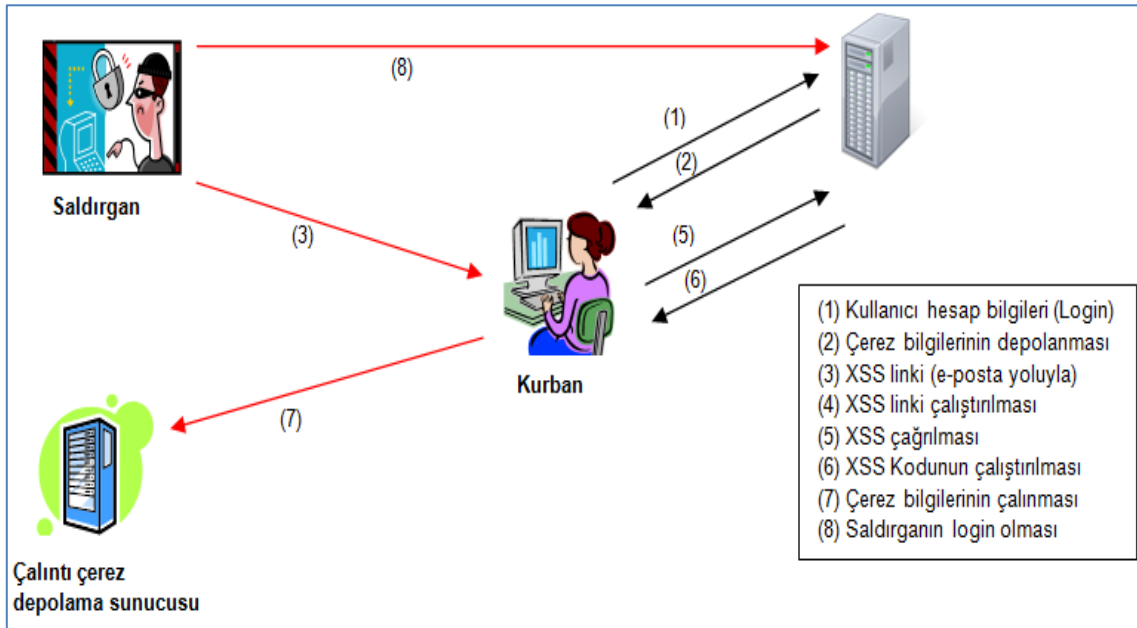
Bu tehdidi, saldırganın bilgisayardan veri okuma, kötücül yazılım çalıştırma gibi isteklerinin web tarayıcı tarafından yerine getirilmesini sağlamak için tarayıcıdaki yazılım hatasından yararlanan kodlar kümesi şeklinde tanımlamak mümkündür. Web tarayıcıların kullanıcının internetle etkileşime geçmesinde en çok tercih edilen araç olması nedeniyle izinsiz indirme yönteminin siber tehditler arasında ilk sırada yer alması normal gözükmemektedir. Saldırganların belirledikleri bir siteye yerleştirdikleri (bunlar genelde ilerleyen sayfalarda tanımlanacak olan exploit kitler denen) zararlı kodların siteyi ziyaret eden kullanıcıların sisteminin otomatik olarak taranıp bulunan güvenlik açıklıklarının kullanılmasıyla sisteme yüklenmesi şeklinde gerçekleşir. Özellikle saldırganlar tarafından mobil cihazların hedeflendiği izinsiz indirme yöntemi ile yapılan saldırılar genelde zararlı linklerin kullanıcılar tarafından tıklanmasıyla yapılmaktadır[65].

Kod çalıştırma (Kod enjeksiyonu)

Otomatik saldırı araçlarının artmasının bu tür tehditlerin görülme sıklığını da arttırdığı gözlenmektedir. Saldırganlar bu tür araçları kullanarak kısa bir süre içinde güvenlik açığı taraması yapabilmekte ve tespit ettikleri bu açığı kullanacak zararlı kodları oluşturarak hedef üzerinde çalıştırılmasını sağlamayı amaçlamaktadırlar. Bu bağlamda saldırganlar tarafından uygulanan kod çalıştırma (kod enjeksiyonu) örneklerini aşağıdaki gibi sıralamak mümkündür.

Çapraz site betik saldırısı (Cross site scripting attack- XSS)

HTML kodları arasına yerleştirilmesi dolayısıyla bazı kaynaklarda HTML enjeksiyonu olarak da geçen XSS kodları kurbanın web tarayıcısına yüklenip (kurbanın giriş yaptığı web sitesinin kurbanın web tarayıcısı için tanımladığı güvenlik ayarları çerçevesinde) çalışmaktadır. Genellikle HTML veya JavaScript dillerinde yazılan XSS kodları (eğer web tarayıcısı üzerinde herhangi bir güvenlik ayarı oluşturulmamışsa) tarayıcının erişebildiği tüm veriyi okuyup değiştirebilir, kurbanın bilgisayarı üzerindeki çerezleri (cookies) çalabilir, tarayıcıyı başka bir adrese yönlendirebilir ve hizmet aksattırma gibi birçok saldırıyı gerçekleştirmek için kurbanın bilgisayarını kullanabilir[43].



Şekil 2.7. XSS Yönteminin Mantıksal Gösterimi[77]

Kullanıcı ile web sitesi arasındaki güvene dayalı uygulanan XSS tehdidinin:

- Kullanıcının önceden hazırlanan ve zararlı kod içeren linki tıklanmasıyla (kodun kullanıcının web tarayıcısında çalışarak) kodun içindeki olayların oluşmasının sağlandığı *Kalıcı olmayan XSS*,
- Saldırgan tarafından hedef web sitesinin veritabanı üzerine yerleştirilen XSS kodlarının siteyi ziyaret eden kullanıcıların web tarayıcısında çalıştırılmasıyla yapılan *Kalıcı XSS yöntemi*,
- Kurbanın web tarayıcısında çalıştırılacak DOM (Document objected) nesnelerini içeren kodların kurbanın web tarayıcısı üzerinde çalıştırılması esasına dayanan *Dom temelli XSS yöntemi* olmak üzere üç çeşidi bulunmaktadır[45].

Siteler arası istek sahteciliği (CSRF - Cross-site request forgery)

En az bilinen web saldırı çeşidi olan CSRF tekniği ile (internet bankacılığını kullanarak) para transferi ve e-posta hesabının ayarlarını değiştirip e-posta gönderme gibi işlemler yapılabilmektedir. XSS saldırısının aksine web sitesinin kullanıcıya olan güveninin istismar edildiği bu teknikte kurban (herhangi bir izni ve bilgisi olmaksızın) saldırgan tarafından belirli bir adrese yönelik olarak bir HTTP isteği yaptırılmaktadır. CSRF ataklarının;

- Kurbanın hedef site üzerinde aktif bir oturuma sahip olması,
- Kurbanın hedef site üzerinde HTTP aracılığıyla yetkilendirilmesi,
- Kurbanın hedef sitenin web sunucusu ile aynı yerel ağ üzerinde olması

gibi etkili olduğu birçok durum vardır. CSRF atağında hedef siteye karşı yapılacak saldırıda öncelikli olarak kurbanın tanınan ayrıcalıklar kullanılır. Hedef site üzerinde bir XSS açığının bulunması (CSRF atakları için bir çeşit platform görevi göreceklerinden) verilecek zararın artmasına neden olacaktır[42].

Örneğin, <http://www.alis-veris.com> adlı (PHP ile hazırlanmış) bir site olsun ve bir kullanıcı kendi hesabını kullanarak bu site üzerinde alışveriş sepetine eklemeler, silmeler yapabilsin. Kullanıcının yaptığı silmeler aşağıdaki gibi bir kod parçası ile yerine getirilsin.

```

<form action="admin.php" method="GET">

<input type="hidden" name="cmd" value="deleteall"/>

<input type="submit" value="delete" />

</form>

```

Bu kod sonucunda GET isteği ile sunucuya gönderilen (sepettekilerin silinmesini isteyen) parametreyle sunucu tarafında oturum kontrolü yapıldıktan sonra ve geçerli bir oturum olduğu anlaşıldıktan sonra işlem yapılmaktadır. Bir saldırgan farklı bir web sitesi oluşturarak (width ve height ayarlarını da yaparak) hazırlamış olduğu web sayfasının içine zafiyetin bulunduğu siteye istek yapmayı sağlayan

```

<html>

...

<img src=www.alis-veris.com/admin?cmd=deleteall width=0 height=0 />

...

<html>

```

gibi bir kod yerleştiriyor. Alışveriş yapmak için girdiği siteyi ziyaret ederken saldırganın hazırlamış olduğu yukarıdaki kodun bulunduğu sayfayı ziyaret eden kullanıcının sepetindekiler silinecektir. Yapılan isteğe kullanıcının oturum bilgisi de eklendiği için yetkilendirme ile ilgili herhangi bir problem çıkmayacaktır[37].

SQL(Structured Query Language) enjeksiyonu

Hem ANSI hem de ISO standardında bir yapısal programlama dili olan SQL ile ilişkisel veritabanı uygulamalarında çalışmalar yapılabilir. Kullanıcı girdilerine göre SQL cümleleri oluşturan web sitelerinde, bu girdilerin kontrol edilmemesi veya yeterli kontrolün sağlanmamasından dolayı kaynaklanan zafiyetleri kullanmaya dayalı SQL enjeksiyonu ile veritabanları üzerinde sorgulama, ekleme, silme v.b. işlemler ve kimlik doğrulama mekanizmalarını atlatma gibi işlemler yapılabilir.

Web uygulamasının girdileri yeteri kadar kontrol etmemesi neticesinde hazırlanan SQL cümleleri sebebiyle oluşan güvenlik ihlalleri sonunda elde edilen kullanıcı hakları kullanılarak (veritabanı dışında) başka sunucu bilgisayarlara da erişim sağlanabilmektedir. Örnek verilecek olursa:

```
SQLCommand = "SELECT Username FROM Users WHERE Username = ""
SQLCommand = SQLComand & strUsername
SQLCommand = SQLComand & "" AND Password = ""
SQLCommand = SQLComand & strPassword
SQLCommand = SQLComand & ""
strAuthCheck = GetQueryResult(SQLQuery)
```

Bir web uygulamasının yukarıdaki gibi SQL cümleleri aracılığıyla kimlik doğrulaması yaptığını göz önüne alalım. Yukarıda yazılı koddaki gibi kullanıcının girdisi (strUserName ve strPassword) alınarak oluşturulan bu yöntemde saldırganın

```
Username : foo
Password : bar' OR '='
```

kodunu kullanarak sisteme giriş yaptığını varsayalım. Yukarıdaki yöntemde saldırganın girmiş olduğu bu değerler

```
SELECT Username FROM Users WHERE Username = 'foo'
AND Password = 'bar' OR '='
```

şeklinde tanımlanacaktır. Bu sorgu sonucunda kullanılan OR deyiminin "=" ifadesiyle yukarıdaki gibi kullanımı neticesinde kullanıcı veritabanından tüm satırlar döndürülecektir. Bu şekilde yeteri kadar kontrol içermeyen kimlik doğrulama kodları sonucunda saldırgan kendini kullanıcı tablosuna ekleyebilmektedir[56].

Arabellek taşması

Web uygulamalarında kullanılmak üzere bellek üzerinde ayrılan alanlara (bu alanların büyüklüklerinden daha fazla) verilerin gönderilmesiyle oluşan bellek

taşması sonucunda komşu bellek bölgelerine verilerin yazılmasına ve uygulamaların çalışmamasına dayanan yazılım kusurudur. Genellikle web sunucular üzerinde etkili web bellek taşıma açıklıkları saldırganlar tarafından özel hazırlanan zararlı kodlarla meydana getirilmektedir[6].

Dizgi Formatı

Programlama dillerindeki kütüphanelerin özellikleri kullanılarak (ara bellek taşıması yönteminde olduğu gibi) bellek üzerinde tahsis edilen bölgenin dışında alanlara ulaşarak rastgele herhangi bir kodun çalıştırılması veya buradaki yığından veri okunması gibi olaylar gerçekleştirilir. Saldırganlar özellikle C, C++ programlama dillerinin fprintf, printf, scanf gibi fonksiyonları için anlamlı ifadeler içeren %x,%s,%n gibi değerler kullanarak istediklerini elde etmeye çalışırlar. Varsayalım kullanıcıdan bir e-posta adresini girdi olarak alıp bunu printf fonksiyonunu kullanarak yazdıran bir web uygulaması olsun. Girilen bu e-posta girdisiyle birlikte gönderilen parametre (biçim karakterlerine sahipse) içinde bulunan karakterler printf fonksiyonunca tanınır ve sonradan verilen parametreleri kullanır. Eğer girdiyle birlikte bu tür parametreler bulunmazsa bellekteki veri yığınının (printf fonksiyonunun beklediği sıraya uygun olarak) alınarak kullanılır. Bu şekilde yapılabilecekler:

- Eğer printf fonksiyonunun çıktı akışı saldırgana geri sunuluyorsa, saldırganın %x gibi karakter göndererek bellekteki veri yığınının değerler okuyabilmesi,
- Eğer printf fonksiyonunun çıktı akışı saldırgana geri sunuluyorsa, saldırganın %s gibi karakter göndererek bellek üzerindeki karakter dizelerini (rastgele bir şekilde) okuyabilmesi,
- %n karakterini kullanarak saldırganın bellek üzerinde herhangi bir konuma sayı değerleri yazabilmesi şeklinde sıralanmaktadır[46].

LDAP enjeksiyonu

Farklı işletim sistemleri üzerinde çalışan dizin servisleri üzerinde sorgulamalar yapma imkânı veren LDAP (Lightweight Directory Access Protocol) açık standartlı bir protokoldür. TCP/IP üzerinde çalışan LDAP protokolü dinamik web sayfaları taleplerini karşılamak için kullanıcı girdilerini kullanarak (SQL'dekine benzer) LDAP

cümleleri oluştururlar. Bu LDAP sorgu cümlecikleri veritabanı veya bir web sunucunun belirlediği izinlere bağlı olarak işlediğinden LDAP sunucu üzerinde (bu izinler çerçevesinde) sorgulamalar ve değiştirmeler yapılabilmektedir. Web tarayıcıya http://example/default.aspx?user=* şeklinde girilecek bir URL adresi ile * karakteri sayesinde sorgulama sonucunda user özelliği bulunan her bir nesne (eğer gerekli kontroller sağlanmamışsa) LDAP aracılığıyla döndürülür[52].

İşletim sistemi enjeksiyonu

İşletim sistemi komut enjeksiyonunda kullanıcı tarafından girilen girdilerin (yeterince denetlenmemesi nedeniyle) saldırgan tarafından (erişimin sağlandığı web sunucu ya da veritabanı sunucusu v.b. tarafından tanımlanan izinler dahilinde) işletim sistemi komutları kullanılarak erişim izni olmayan dosyalara erişim imkanı sağlanır. Örneğin, girdi kontrolü tam yapılmayan bir web uygulamasının gerçek URL adresi: <http://123.com.tr/cgi-bin/bilgigoster.pl?isim=Can°isken=metin1.txt> şeklinde olsun. Web tarayıcıdan [/bin/ls](#) şeklinde komut girilerek <http://123.com.tr/cgi-bin/bilgigoster.pl?isim=Can°isken=/bin/ls> şeklinde oluşturulmasıyla yapılabilmektedir[53].

SSI (Server Side Includes) enjeksiyonu

Sunucu tarafından yerel olarak çalıştırılacak zararlı kodların bir web uygulamasınca gönderilmesine dayanan SSI tekniğinde, kullanıcının gönderdiği verinin sunucu tarafındaki web uygulamasınca yeterince kontrol edilmeden HTML dosyası içine konmasıyla oluşan güvenlik zafiyetleri kullanılmaktadır. Bunun sonucunda da kısıtlı bir dosyanın içeriğinin bir sonraki sayfaya dahil edilebilmesi ve herhangi bir işletim sistemi komutu çalıştırabilme gibi güvenlik ihlalleri oluşabilmektedir[55]. Varsayalım, günlük belirli bazı malların fiyatlarının girildiği bir web sayfası olsun. Bu web sayfasının dosyası aşağıdaki kodun yerleştirilmesiyle bir fiyat girdisi içerebilir.

```
<!--#include virtual="../quote.txt" -->
```

quote.txt dosyasındaki bir değişiklikle bu dosyayı içeren tüm sayfalar en son fiyat girdisini gösterecektir.(Sunucu taraflı girdiler web sitesinin geneli için ortak olan

kodlar bakımından faydalıdır) Bu dosyaya kullanıcı tarafından yapılacak girdilerin kontrolü yeterli olmazsa bu dosyayı kullanan tüm sayfalar (zararlı kodların yaptıklarından) etkilenir[60].

Xpath Enjeksiyonu

SQL enjeksiyon yöntemine benzeyen XPath yönteminde (XPath'in yapısı SQL sorgularına benzediğinden) kullanıcıdan alınan ve yeterince denetlenmeyen girdilerle SQL benzeri ancak daha az güvenlik içeren sorgular oluşturulması sonucunda meydana gelen güvenlik açıklıklarının sömürülmesini içermektedir. XPath kullanılarak XML dokümanlarında SQL benzeri sorgulamalar yapılabilmektedir. Bir örnekle açıklamak gerekirse; kullanıcı isimleri içeren bir XML dokümanı olduğunu varsayalım. Bu dokümanın hesap, isim ve şifre adlı 3 alt ögesi bulunmaktadır. Aşağıdaki XPath ifadesi kullanıcının isminin *ali* şifresinin de *deneme123* olduğunu göstermektedir.

```
string(//user[name/text()='ali' and
password/text()='deneme123']/account/text())
```

Bu şekilde bir gerçek zamanlı XPath sorgu yapısı kullanıldığında saldırgan tarafından sorgu ifadesine güvenilir olmayan girdi gömülmesi sonucunda kullanıcıyı isteği dışında farklı sorgulamalar yaptırılabilir[57].

Botnet

Saldırganlar tarafından internet kullanıcılarının sistemlerine yüklenen zararlı yazılımlar yoluyla (zombi de denen) *bot* adında birçok bilgisayarın oluşturduğu ağ sistemine *botnet* denmektedir. Saldırganlar oluşturdukları botnet sayesinde tek bir merkezden dünyanın farklı noktalarındaki bilgisayarları (istenmeyen e-postalar göndermek, virüs yaymak, sunucu ve sistemlere saldırmak v.b.) kendi amaçları doğrultusunda yönetebilmektedirler.

Kötücül yazılımlar

Mobil cihazlar üzerindeki yayılımı diğer platformlara göre daha etkili olan kötücül yazılımlar sistem üzerindeki açıklıkları bularak hedeflenen veri ya da verileri elde etmek için kullanılmaktadır. Saldırganlar tarafından son zamanlarda oldukça

yoğun olarak kullanılan kötücül yazılımların bazıları hakkında aşağıda bilgi verilmektedir.

Virüs

Başka programların içine kendisini kopyalayarak bulaşan ve kendisi de bir bilgisayar programı olan virüsler en genel tanımıyla; bir bilgisayardan bir diğerine yayılmak ve bilgisayarın çalışmasına müdahale etmek amacıyla tasarlanmış küçük yazılım programlarıdır[23]. Kendi kodunun kopyasını başka programlara ekleyerek verebileceği zararlarını arttırabilen virüsler hem kendilerini kopyalayacak kodları hem de zarar verecek işlem kodlarını içerirler. Kullanıcı tarafından çalıştırılmadan veya programlayan kişi tarafından önceden belirlenmiş bir durum oluşmadan aktif hale geçmezler.

Solucan (Worm)

1975 yılında John Brunner tarafından yazılan “Shockwave Rider” (Şok Dalgası Binicisi) adında bir bilim kurgu romanında, bir bilgisayar ağı üzerinden kendi kendini yayan bir programa verdiği isimden gelen solucanlar başka dosyaları değiştirmese de etkin bir biçimde bellekte durarak kendilerini kopyalayabilir ve (genelde) e-posta, FTP ve HTTP gibi yollarla kendilerini yayabilirler. Solucanlar çoğu kez (bir fotoğraf ya da metin dosyası içerecek şekildeki e-postaların içindeki) bir eklentinin kullanıcı tarafından çalıştırılarak kendini sisteme kopyalaması ve kopyalandıkları sistemdeki kullanıcıların adres defterinde bulunan her bir adrese bulaşmalarıyla yayılırlar. Bunun dışında (W32.Nimda.A@mm ve W32.Aliz.Worm gibi) internet üzerinde yaptığı taramalar sonunda açık kapıları olan veya güvenlik duvarı bulunmayan sistemlere bulaşarak yada yerel ağ üzerinde (ortak paylaşım açılmış bir klasör şeklinde kendini göstermesiyle) kullanıcıların çalıştırması sonucunda da yayılabilmektedirler[30].

Virüslere benzer yapıda olan solucanların yayılmak için kendilerini çalışan bir programa ilitmeye veya bir parçası olmaya ihtiyaçları bulunmamaktadır. Solucanlar ağdaki bandgenişliğini kullansa bile (ulaştıkları sistemdeki dosyaları değiştiren veya tahrip eden virüslere kıyasla) ağ için çok zararlı değildir[59].

Truva atı (Trojan)

Bilgisayarın kontrolünü uzaktan ele geçirerek ekranın görüntüsünün alınması, uzaktan komutlar çalıştırılması ve dosyalar üzerinde izinsiz ve yetkisiz işlemler yapabilme gibi imkânlar veren truva atları (trojan) genelde e-posta ya da internet üzerinden yüklenen ücretsiz ve lisanssız yazılımlar yoluyla yayılmaktadırlar. Solucanlardan farklı olarak:

- Sisteme bulaştığında hangi programla bulaşmışsa o programın açılmasını bekler(açılmadığı sürece aktifleşmez).
- Direkt olarak bilgisayarın işletim sistemine zarar verebilir.
- Bilgisayar üzerinde (monitör izleme, programlar açabilme v.b.) işlemler gerçekleştirerek tüm kontrolü ele alabilir[39].

İstismar kodları (Exploit kit)

Hedef sistem üzerindeki açıklıkları tespit edip bu açıklıkları kullanarak sisteme yönelik saldırılar gerçekleştirebilen exploit kitler, çok sayıda fonksiyon ve yapılandırma seçenekleri sunan kullanıma hazır yazılımlardır. Günümüzde en yaygın web tehdidi olarak görülen Blackhole exploit kiti bulaştığı sistemlerde kullanıcılar hakkında bilgiler toplayan izleme mekanizmaları içermektedir. Bu bilgiler içinde kurbanların ülkesi, işletim sistemleri, kullandıkları web tarayıcı ve kurbanların sistemlerindeki yazılımlardan istismar edilenler bilgisi bulunmaktadır[58].

Sahte antivirüs yazılımları

Bilgisayara zarar vermek amacıyla yazılan ancak (Javascript kodlarını kullanarak bilgisayardaki işletim sistemine göre uygun ara yüze sahip olabilme yetenekleri sayesinde[20]) kendilerini birer virüs koruma programı ya da casus yazılım engelleme aracı şeklinde gösterebilen yazılımlardır. Genelde bilgisayarınızda çok sayıda virüs tespit edildiği ve bunları temizlemek için (verilen linke tıklanarak) bir program indirmeniz gerektiğini belirten mesajlarla bulaşırlar. Başka bir yolda e-posta yoluyla sahte anti virüs programının linki kullanıcıya gönderilerek (30 günlük ücretsiz kullanım hakkı olduğu gibi) ifadelerle kullanıcının bilgisayarına programı

yüklemesi sağlanarak da bulaşabilmektedir. Yapılan araştırmalara göre bu şekilde (7 binden fazla sahte antivirüs programının yer aldığı internette) 30 milyondan fazla kullanıcı etkilenmiş durumdadır. Bunlar arasında en bilinenleri PersonalAntiSpy, VirtualPCGuard, AntiMalware 2009 AntivirusProtection, Security Scanner 2008, VirusResponse Lab 2009, Antivirus Security, Micro Antivirus 2009 AntiSpyware Pro XP, XP Protector 2009, AV Security 2012, Windows Antivirüs 2011, AVG Antivirüs 2011, Protection Center, Vista Security Tool 2010, Antivirüs 8'dir[10]. Bazı sahte antivirüs yazılımların yapabilecekleri şu şekilde sıralanmaktadır:

- Sizi bir dolandırıcılık işlemi için kandırma (örneğin, bir programın aslında bulunmayan ücretli sürümüne yükseltme).
- Kişisel bilgilerinizi çalmak için [sosyal mühendislik](#) kullanma.
- Verilerinizi çalarken saptanmayacak kötü amaçlı yazılımlar yükleme.
- Sahte veya aldatıcı uyarılar içeren pencereler açma.
- Bilgisayarınızı yavaşlatma veya dosyaları bozma.
- Windows veya geçerli virüsten koruma yazılımlarının güncelleştirmelerini devre dışı bırakma.
- Virüsten koruma satıcılarının web sitelerini ziyaret etmenizi önleme[25].

Spam

İnternette kullanıcıların herhangi bir talebi olmaksızın (çok yüksek sayıda kopyaları üretilen) genelde ticari reklam içerikli veya belli bir görüşün propagandası amacı ile oluşturulan e-postalar olarak bilinen spamlar çabuk zengin olma kampanyaları veya güvenilmeyen ürünlerin duyurulması şeklindedir. Spam gönderme için genellikle kullanıcılarının adreslerinin güvenliğine yeterince önem vermeyen sitelere yapılan üyeliklerde, sitelerin forum ve ziyaretçi defterlerinde veya sisteme bulaşan virüsler vasıtasıyla elde edilen e-posta adresleri kullanılmaktadır[21].

Tüm e-posta trafiğinin %75'ini oluşturan spamlar zararlı kod içeren URL linklerin, kötücül yazılımların yayılması ve dolandırıcılıklar için bir kaynak durumundadır. Günümüzde spam üreticilerinin spam filtreleme yazılımlarının performanslarını

düzenli olarak kontrol etmelerinin de etkisiyle spamlara karşı etkin bir korunma sağlanamamaktadır[86].

Kimlik Hırsızlığı ve oturum ihlali

Kimlik hırsızlığı (ve bunun neticesinde işlenen dolandırıcılık) tehditleri en başarılı uygulamaların gerçekleştirildiği tehditler olmanın yanında geniş çaplı zarar verme potansiyeline sahip birçok veriye erişilebilmesini de sağlamaktadır. Trojan gibi kötücül yazılımlar sahip oldukları zararlı kodlar sayesinde kimlik hırsızlığı yapabilmektedirler. Saldırganlar tarafından kullanılarak kimlik hırsızlığı ve oturum ihlaline sebep olan bazı yöntemler ve bu yöntemlerin kullandığı güvenlik açıklıkları şunlardır:

Sazan avlama (Phishing)

Phishing (sazan avlama) yönteminde kullanıcıların şifre, kullanıcı adı, kredi kartı bilgileri v.b. bir takım bilgilerini elde etmek amacıyla (genellikle) e-postalar göndererek kullanıcının (çeşitli kandırmacalarla) e-posta içindeki linke tıklaması sağlanarak, önceden hazırlanmış sahte web sayfalarını ziyaret ettirilmesiyle (bu sayfalardaki ilgili alanları doldurmaları sağlanarak) bilgilerinin elde edilmesidir.

Oturum bilgisi tahmini ve oturum sabitleme

Web uygulamaları tarafından daha önceden tanımlanan kullanıcı ismi ve parola ile sisteme giriş yapan kullanıcılara web siteleri (her işlemde ayrı ayrı bu bilgilerin doğrulanması yerine) bir oturum numarası tahsis ederek kimlik doğrulamasını gerçekleştirirler. Kullanıcı ile site arasındaki etkileşimlerde bu numara eklenerek kimlik doğrulaması sağlanır. Bu oturum numaraları tarayıcılar tarafından çerezler(cookie) içinde (kimi zamanda gizli form alanlarında veya URL içerisinde de) saklanırlar. Bu sayede kullanıcı ilgili siteyi her ziyaret ettiğinde otomatik olarak kimlik doğrulama işlemi gerçekleştirilir. Eğer bu tür bir yetkilendirmede zayıf algoritmalar kullanılır, oturum numarasını elde etmek için yapılacak kaba kuvvet saldırılarına karşı önlem alınmaz ise algoritma üzerinde yapılacak kaba kuvvet saldırısı ile bir sonraki oturum numarası elde edilip mevcut oturum numarası ile değiştirilmesi sonucunda bir sonraki kullanıcının kimliği elde edilebilmektedir. Oturum sabitleme ise saldırganın önceden belirlemiş olduğu oturum bilgisinin

(siteyi ziyaret eden) kullanıcı tarafından kullanılması sağlanarak kullanıcının hesabına erişim hakkı kazanmasıdır. Web siteleri ya oturum numaralarını kullanıcının web tarayıcısında belirleyerek korunmasız bir şekilde tutarlar (ki güvenlik açısından çok risklidir) ya da daha güvenilir bir şekilde sunucu tarafında belirlerler. Öncelikle saldırgan hedef web sitesi üzerinde geçerli bir oturum açarak oturum numarası elde eder(Sunucu tarafında oluşturulan oturum numaralarında oturumun sürekliliği için web sitesiyle belli aralıklarla bağlantı tekrarı yapılması gerekmektedir). Bu elde ettiği oturum numarasını (bir linke tıklatma veya XSS gibi yollarla) kurbanın web tarayıcısına göndererek kurbanın oturum numarasını kendi bildiği değere sabitler. Böylece kurban hedef siteye giriş yaptığında sabitlenen oturum numarasını kullanmaya başlayacağından kurbanın oturum bilgileri ele geçirilmiş olacaktır[77].

Yetersiz yetkilendirme

Bir web sitesi, herhangi bir işlemi gerçekleştirmek veya herhangi bir veriye erişmek isteyen (kullanıcılara yapmak istedikleri işlemler konusunda zorluklar çıkartmadan) kullanıcıyı gerekli kontrollerden geçirmezse bu durum site için bazı güvenlik açıklıklarının meydana gelmesine neden olabilmektedir. 2005 yılında Harvard İş Okulu'na yapılan başvuru sırasında kullanıcıların sitede erişmemeleri gereken kısımlar için yeterli yetkilendirme kontrolleri yapılmadığından kullanıcıların erişim izni olmayan verileri elde etmiş olmaları bu konuda güzel bir örnektir[49]. Ayrıca bu yöntemde saldırganların, web sitesinin kopyasını çıkartarak veya arama motorlarını kullanarak (uygun yetkilendirme işlemleri yapılmazsa) saklı dosya ve klasörlere erişmesi de mümkündür.

Yetersiz oturum sonlandırma

Web siteleri tarafından her bir kullanıcıya özel olarak üretilen oturum bilgilerinin tekrar kullanılmasına imkân veren bir durumdur. Üretilen oturum numaralarının gizliliği aynı hesabın birden çok kişinin erişimine açılmaması için önemlidir. Oturum sonlandırma sürelerinin uzun tutulması açık oturum sayısını arttıracığından oturum numarasının tahmin edilebilmesini kolaylaştırmaktadır. Eğer bir web sitesi kullanıcının oturumunu sonlandırma işlemini gerçekleştirmeden kullanıcı

sistemden çıkmışsa (aynı bilgisayar üzerinden) saldırgan eski sayfaları kullanarak sisteme yetkisiz bir erişim gerçekleştirebilmektedir[51].

Bir örnekle açıklamak gerekirse; bir internet kafeye giden Ali para transferi yapmak için maaş aldığı bankanın internet sitesine girerek işlemlerini yapmıştır. Ancak daha sonra web tarayıcısını *güvenli çıkış* sekmesi yerine başka şekilde kapatmıştır. Ali kalktıktan sonra onun yerine oturan Veli web tarayıcısının adres satırından Ali'nin daha önceden giriş yaptığı linki tıklamasıyla (Eğer banka yeterli sonlandırma ayarlarını yapmamışsa) Ali'nin banka bilgilerine ulaşabilecektir.

Şifre kurtarma denetimi yetersizliği

Web siteleri (uzun zaman aktif olmama gibi nedenlerle unutulmuş ya da kaybolan) şifre veya kullanıcı adları için kullanıcılarına hatırlatma sorusu, ipucu, bilgi doğrulama gibi seçenekler sunarak hesaplarına yeniden erişim imkânı tanırırlar. Eğer bu şifre kurtarma seçenekleri (iyi yapılandırılmazsa), saldırganlar tarafından kaba kuvvet saldırıları, tahmin usulü gibi yöntemlerle atlatılabilmektedir[50].

Örneğin; bir web sitesi, kullanıcılarından hatırlatma sorusu olarak tuttuğu takım ve kimlik doğrulama için posta kodu, telefon numarası gibi bilgiler istiyorsa kurbanı az çok tanıyan bir saldırgan bile zorlanmadan hesabı ele geçirebilecektir.

Kaba kuvvet saldırıları

Kaba kuvvet saldırısı, bir kullanıcı adı veya şifresini bulmak için çok sayıda değer birer birer denenmesine dayanmaktadır. Web uygulamalarının deneme yanılma yoluyla tahmin edilebilecek nitelikte zayıf şifreler oluşturmalarına izin vermesi ve kullanıcıların seçmiş oldukları şifrelerin (hatırla kalabilmesi amacıyla) sözlüklerde yer alan kelimelerden oluşması gibi nedenler, kaba kuvvet saldırılarının başarıya ulaşmasını sağlamaktadır. Saldırganlar oluşturacağı (doğum tarihleri, telefon numaraları gibi bilgiler içeren) şifre ve kullanıcı adı listeleri ile saldırı düzenleyebileceği gibi harf, rakam ve noktalama işaretlerinin rastgele seçilerek denenmesi yoluyla da saldırılabilmektedir. (Bu saldırılar kimi zaman çok uzun süreler devam edebilmekte ve birçok başarısız saldırı girişimden sonra sistemin kilitlenerek erişilememesine neden olabilmektedir). Ayrıca web uygulaması tarafından kullanıcı için belirlenen ve o kullanıcıya has üretilen oturum

numaralarının benzer yöntemlerle ele geçirilerek sisteme erişilmesi de mümkündür[41].

Yetersiz kimlik doğrulama

Web sitelerinin bazı kullanıcılarının erişimini istemediği dizinler vardır.(ve dizinlere site içerisinde herhangi bir yerden bağlantı sağlanmamış da olabilir) Eğer web sitesi herhangi bir bağlantı vermediği ve herhangi bir kullanıcının da bu dizinlere erişmeye çalışacağını göz önünde bulundurmayarak gerekli kimlik doğrulama işlemlerini yapmazsa herhangi bir saldırgan standart bir web tarayıcı ile yetkisiz olduğu bu dizinlere (herhangi bir kısıtlamaya tutulmaksızın) erişebilecektir[48].

Veri ihlalleri ve bilgi sızıntısı

Bu tehditle kasıtlı ya da kasıtsız olarak bilginin açığa çıkmasıyla meydana gelen veri kayıpları kastedilmektedir.(Bilgi yönetim varlıklarındaki hatalarda olduğu gibi) Bu tehdit içsel ve dışsal faktörlerden kaynaklanabilmektedir. Her iki durumda da iyi ya da kötü niyetli sebepler olabilir. Veri ihlalleri hem kötücül eylemlerin etkinliği hem de kurumsal bilgilerin korunma düzeylerinin önemli bir göstergesi olarak değerlendirilmektedir. Veri ihlalleriyle ilgili özellikle kurum içindeki personeller önemli bir rol oynamaktadır. Mevcut güvenlik tedbirlerinin etkinliği hususunda önemli bir gösterge olan (% 70 kadarı basit ve düşük seviyeli saldırılar olan) veri ihlallerini engellemek için basit ve düşük maliyetli güvenlik kontrolleri uygulanması yeterlidir. Bilgi sızıntısı ise, veri ihlalinden farklı olarak kurumların güvenlik sistemlerine ilişkin teknik bilgilerin açığa çıkarılmasına dayanır. Güvensiz dosya transferleri ve mobil cihazlardaki basit şifrelemeler bilgi sızıntısına yol açabilmektedir[65]. Saldırganlar tarafından kullanılarak veri ihlalleri ve bilgi sızıntısına sebep olan bazı yöntemler ve bu yöntemlerin kullandığı güvenlik açıklıkları şunlardır:

Yol Takibi

Web sitesi kök dizininin dışında kalan dosyalara erişimin hedeflendiği yol takibinde (path) web sunucusu üzerinde depolanan (kritik sistem dosyaları da dahil) dosyalara erişmek için mutlak bağlantılar taranır. Bu yöntemde en temel anlamda dosyaların yerini değiştirmek için ".../" karakteri kullanılır. Bir çok web sunucusu bu

karakterle web dosyasının kök dizininden çıkışını engellese de ("..%u2216" veya "..%c0%af" unicode şeklindeki kodlanmasıyla) güvenlik filtreleri aşılabilmektedir. Örneğin, <http://example/scripts/foo.cgi?page=menu.txt> şeklinde bir web sitesi olsun. Saldırgan web tarayıcıya <http://example/scripts/foo.cgi?page=../scripts/foo.cgi> yazarak "../" bir üst dizine çıkmak ve /scripts dizinine girmeye çalışması bu tip durumdur[54].

Dizin listeleme ve Fonksiyonellik suiistimalleri

Başlangıç sayfası olmayan bir web sitesi URL'ye girilen adresteki dizin içerisindeki tüm dosyaları listelemesiyle oluşur. Örneğin web tarayıcıya <http://www.dnm123.com.tr> şeklinde bir adres yazıldığında web sunucusu öncelikle index.html veya default.asp şeklinde bir dosya arar. Eğer bu dosyaya kök dizinde erişilemezse (uygun yapılandırma ayarları da yapılmamışsa) sunucu kök dizindeki tüm dosyaları listeleyecektir. Herhangi bir link verilmezse web sunucu üzerindeki dosyalara erişilemeyeceği gibi yanlış bir düşünce dolayısıyla yapılan bu güvenlik hataları neticesinde çeşitli sistem tarayıcıları site üzerinde (kaba kuvvet, sözlük saldırısı şeklinde) denemeler yaparak sunucudan gelen dönütlere göre dizin yapısı oluşturabilmektedirler. Fonksiyonellik suiistimalleri ise web sitesi içindeki arama uygulamasının web dizini dışındaki erişim izni kısıtlanmış dosyalara erişim için kullanılması, web sitesi içinde kimlik doğrulaması yapan uygulamaya tanımlı kullanıcılar girilip yanlış parolalarla giriş denemeleri yapılarak tanımlı kullanıcıları hesaplarının kilitletmesinin sağlanması gibi web uygulama fonksiyonlarının kötüye kullanılmasını ifade etmektedir[77].

HTTP cevap bölme

Saldırgan bir web uygulamasına bir http isteği girer. Bu girilen http isteğinin başlık kısmında gömülü bulunan zararlı karakterler içeren veri herhangi bir doğrulama işlemine tutulmaksızın kullanıcıya gönderilir[47].

APT (Advanced Persistent Threat)

Hedef odaklı geliştirilen, genellikle devletler veya hacktivist gruplar tarafından gerçekleştirilen geniş çaplı siber saldırılar olarak tanımlanan[73] APT'lerin günümüzde istihbarat amaçlı olarak kullanıldıklarına ilişkin iddialar bulunmaktadır.

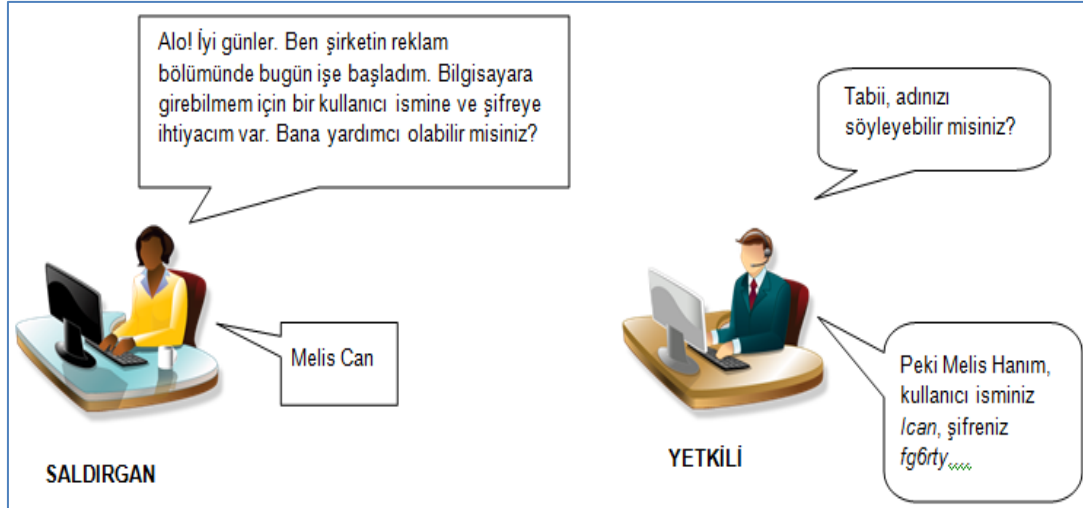
Daha geniş bir ifadeyle; APT' ler, siber savunma sistemlerini kolaylıkla atlatabilen, hedeflere sızmak için gelişmiş teknikler kullanan, bulaştığı sistemlerde yayılarak uzun süre fark edilmeden çalışabilen, belirli sistemleri ve kişileri hedef alabilen, alanında uzman belirgin bir grup veya ülke tarafından geliştirilen yazılımlardır[3].

Genellikle hedef sistemlere sızarak bu sistemlerden veri aktarımı yapmak üzere programlanan APT' lerin en önemli özellikleri olarak enerji, ulaşım gibi belli sistemleri veya belli dillerde çalışan bilgisayarları hedef alarak bu sistemlere sızmaya çalışmaları ve birkaç virüs yazarı tarafından geliştirilemeyecek kadar karmaşık yapılara sahip oluşlarıdır[15]. Örneğin, İran nükleer sistemlerini kontrol eden bilgisayarlara sızan Stuxnet bu türden zararlı yazılımlara örnek olarak verilebilir.

APT kelimesindeki “advanced” ifadesiyle bu tür yazılımların bilinen açıklıkların yanı sıra hedef odaklı güvenlik zafiyeti araştırma yeteneğine sahip olması ve özel bir ekip aracılığıyla bir exploit ve malwareden daha gelişmiş bir yapıda oluşturulmasını, “persistent” kelimesiyle bilinen siber savunma sistemleri tarafından tanınmayacak ve gizli çalışacak şekilde uzun vadeli geliştirilmesini, “threat” kelimesiyle de teknoloji alt yapıları dışında organizasyon ve kişileri de hedef alacak şekilde geliştirilmesi ifade edilmektedir[73].

Popüler adresler üzerinde yapılan saldırılar (Watering hole)

2012 yılında RSA güvenlik firması tarafından tanımlanan bu tip saldırılar, saldırı yapılacak kurum veya şirket tarafından sıklıkla ziyaret edilen web siteleri tespit edilip, bunlardan biri veya daha fazlasına kötücül yazılımların (ya da zararlı kodların) yerleştirilmesiyle o kurum tarafından bu sitelere girilmesi neticesinde bu kötücül yazılımların (veya zararlı kodların) sistemlerine bulaştırılması şeklinde yapılmaktadır[62].



Şekil 2.8. Sosyal mühendislik yöntemi

Sosyal mühendislik

Sosyal mühendislik yönteminde, saldırgan hazırladığı sahte e-postalarla, telefonla ya da sohbet ortamları veya sosyal medyada kullanıcıyı kandırarak istediği bilgilere erişmeye çalışır. Ayrıca (özellikle ortak yazıcının kullanılması neticesinde) kurumda yapılan çalışmalarla ilgili alınan çıktıların değişiklik yapılmasından sonra gerekli şekilde imha edilmemesi sebebiyle kurum ve kurumun çalışmalarıyla ilgili büyük miktarda bilginin elde edilmesi ve kişilerin masalarında bıraktığı (kullanıcı adı, şifre ya da yapılan çalışmalarla ilgili v.b.) notlardan bilgi edinimi faaliyetleri de sosyal mühendislik kapsamındadır. Erkek sesine kıyasla kadın sesinin kullanılarak daha başarılı sonuçların elde edildiği sosyal mühendisliğe Şekil 2.8’ deki gibi kısa bir örnek verilmesi uygun olacaktır[81].

Hizmet aksattırma (DoS- Denial of Service)

Web uygulamalarının gereksiz yere meşgul edilerek normal işleyişinden alıkoyulmasına sebep olan hizmet aksattırma (Denial of Service) saldırıları ile kod enjeksiyonu yöntemiyle veritabanlarının işleyemez hale getirilmesi, web sunucusuna ait sistem kaynaklarının gereksiz meşgul edilmesiyle kullanıcıların erişememesi ve kimliklendirme ve yetkilendirme sistemlerinin kilitlenmesi sağlanabilmektedir. Örneğin, bir hastanede hastalara ait geçmişe yönelik muayene sonuçlarının tutulduğu veritabanı olsun. Bu veritabanından hastaya ait sosyal güvenlik numarasıyla yapılan sorgulama isteklerinin (onbinlerce kayıt taranması

sonucunda) ekrana getirilmesi 2-3 dakika sürecektir olursa (basit bir uygulama ile) böyle bir sorgulamadan eş zamanlı olarak 10 tane yapıldığında sistem kaynaklarını tüketeceğinden diğer kullanıcılar kayıtlara erişemeyecektir[44]. Bu tür saldırılarda genellikle; web uygulamaları üzerinde manüel olarak yapılması gereken (kullanıcı hesabı açma, ziyaretçi defterini doldurma v.b.) işlemlerin (otomatik yapılmasını sağlayan programların kullanılmasıyla) çok fazla sayıda yapılması ve çeşitli programlar aracılığıyla kullanıcı tarafından tutulan bilgileri değiştirmek suretiyle programın akışının değiştirilmesi gibi teknikler kullanılmaktadır.

Fiziksel zarar verme ve hırsızlık(kayıp)

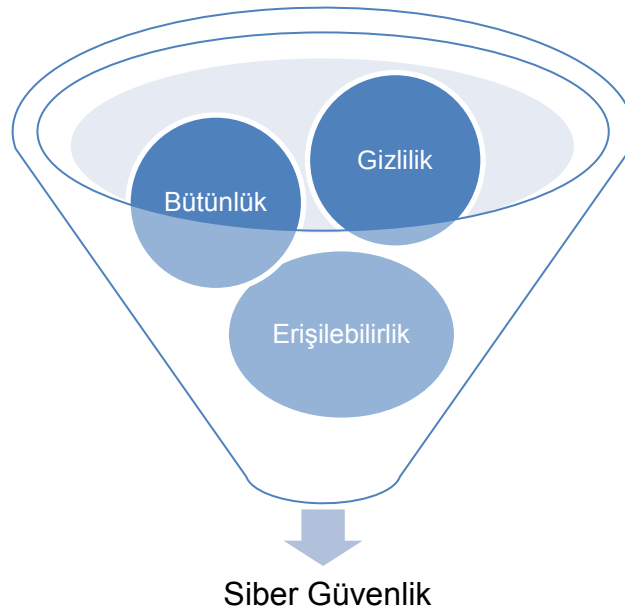
Yangın, sel, deprem v.b. doğa kaynaklı tehditler gibi çevresel ve harici etkiler sonucu oluşabilecek hasarlar ile kurum içi veya kurum dışından kaynaklanabilecek veri ve cihaz hırsızlığı (ya da kayıp) olaylarının kast edildiği bu siber tehdit türüne ilişkin olarak birçok kurum ve kullanıcı diğer siber tehditlerle ilgili endişeler taşıırken bu tehdidin oluşturacağı zararın farkında değildir.

2.3. Kurumsal Siber Güvenlik

Siber güvenlik kavramı genel manada ulusal ve uluslararası bir ihtiyaç gibi düşünülse de bir toplumda bütünün güvenliği, kurumların hatta birey bazında kullanıcıların güvenliğinin sağlanmasıyla daha kalıcı ve sağlam olacaktır. Siber ortamda saldırılara (ağırlıklı olarak) maruz kalan kurum ve şirketlerin siber güvenliklerinin sağlamlılığı ve etkinliği, bir zincirin kuvvetinin en zayıf halkasının kuvvetine denk olduğu prensibi yaklaşımıyla değerlendirilmelidir.

Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımları, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemleri ve siber ortamda iletilen ve/veya saklanan bilgilerinin tümünü kapsayan siber güvenlikte kritik altyapı ve bilgi varlıklarının tespit edilmesi ve bunların saldırılardan korunması maksadıyla öncelikli olarak güvenli risk analizlerinin yapılması gerekmektedir. Sonrasında kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulması ve idame edilmesinin amaçlandığı siber güvenliğin temel hedefleri (Şekil 2.9' da görüldüğü

üzere) erişilebilirlik, bütünlük (aslına uygunluk ve inkâr edilemezliği de kapsar) ve gizlilik[19]. *Gizlilik* ile verinin sadece yetkili kişilerce erişilebilir olması, *bütünlük* ile bilgi ve bilgi işleme yöntemleri ile veri içeriğinin değişmediğinin doğrulanabilmesi ve *erişilebilirlik* ile de erişime yetkisi olan kullanıcıların ihtiyaç duyduklarında bilgi ve ilişkili varlıklara erişebilmesi kastedilmektedir[14]. Kısaca kurumlar için siber güvenliğin amacı; verinin gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanması ve kritik bilgi ve iletişim sistemleri altyapılarında performans ve iş sürekliliğinin sağlanmasıdır.



Şekil 2.9. Siber güvenliğin temel hedefleri

3. SİBER GÜVENLİĞE YÖNELİK KORUNMA TEDBİRLERİ

Ekonomik güvenliğin de ulusal güvenlik unsurlarından sayıldığı günümüzde ulusal güvenliğin sağlanması sınırların korunmasından daha öte anlamlar taşımaktadır. Siber casusluk kurbanı olmak istemeyen iş çevreleri, gerekli ve yeterli siber güvenlik önlemlerini sağlamaları gerekmektedir. Bir kurum veya şirket için güvenlikten tasarruf edilemeyeceği gibi güvenlik endişesiyle sistem verimliliğini sağlayacak alt yapıların kullanımından da vazgeçilemez. Ayrıca, kurumların kendi içlerinde veya aralarında bir ar-ge çalışması yürütmemeleri ve bunun devletçe desteklenmemesi sonucu oluşacak dışa bağımlılık ve ülkemizde devlet veya özel kurumlardaki kullanılan yazılımların birçoğunun aynı olması dolayısıyla bu yazılımlar içine yerleştirilebilecek zararlı bir program aracılığıyla istenmeyen sonuçların gerçekleşebilme durumu ulusal güvenliği tehdit etmektedir.

Aşağıda bahsedilen güvenlik önlemlerinin birbirini destekler nitelikte olmasından dolayı bütüncül bir yaklaşımla ele alınması gerekmektedir. Kurumsal siber güvenlikteki sağlamlık ve etkinlik, (bir zincirin gücünün en zayıf halkasının gücüne eşit olması prensibince) güvenlik mekanizmalarından en zayıf ve düşük olanı kadardır. Bu nedenle aşağıda belirtilen güvenlik basamaklarından birine ya da bir kaçına değil hepsine aynı önemi vererek herhangi bir güvenlik açığına sebebiyet vermeyecek şekilde (kurumun bilgi ve iletişim teknolojileri göz önüne alınarak) her kurumun yapısına uygun önlemlerin yerine getirilmesi gerekmektedir.

Bilinen tüm siber suçların yanı sıra gelişen teknoloji ve değişen suç algısına bağlı olarak gelecekte farklı siber suçların oluşması ya da var olan siber suçların farklı boyutlar kazanması ihtimali her zaman göz önünde bulundurulması gerekmektedir. Maalesef güvenlik kavramı suç kavramına göre şekillenmektedir. Yani öncelikli olarak işlenen zarar verici bir eylem ya da bir suç oluştuğundan sonra o eylem veya suça yönelik güvenlik kriterleri geliştirilmektedir ki bu da siber suçluların hep bir adım önde olduğu anlamına gelmektedir. Bu nedenle siber güvenlikte proaktif olma önemlidir. Yani suç oluşmaması için önceden gerekli önlemlerin alınması oldukça önemlidir.

3.1. Fiziksel Korunma Tedbirleri

Kurumlar için değerli ve kritik verilerin korunmasında en temel yöntemdir. Korunması gereken verinin risk analizi yapılarak fiziki ortamın güvenlik kriterlerinin belirlenmesini kapsamaktadır. Personelin belirli çalışma alanlarına giriş izni yetkileri, oda ve binanın herhangi bir bilgi hırsızlığına maruz kalmayacak şekilde yalıtımı gibi etkenleri içermektedir.

Verilerin çoğaltılması, kopyalanması ya da taşınması gibi durumlarda kullanılan harici bellek, CD-DVD ve disket gibi depolama birimlerinin kilit altına alınarak erişim izinlerinin sınırlandırılması, bu depolama birimlerinin kullanılamaz hale gelmesi veya işlevini yitirmesi durumunda içlerindeki verilere ulaşılamayacak şekilde imha edilmesi, özellikle kritik verilerin barındırıldığı çalışma alanlarında kullanılan yazıcı, tarayıcı gibi donanımların kayıt altına alınarak takibi önemlidir. Bilişim sistemleri ve verilerin bulunduğu yerlere erişim kademelendirilmeli, buralarla ilgili yetkiler paylaştırılıp yazılı hale getirildikten sonra görevli personelin (bu görevli personelin olmadığı durumlarda görevini yapabilecek yedek personelin de) erişebileceği yerde saklanmalıdır. Buralara yetki tanımını dışında üçüncü bir kişinin erişmesi gerektiğinde görevli personel eşliğinde (erişim yerleri sınırlandırılarak) üzerinde herhangi bir kayıt cihazı olmaksızın giriş yapması sağlanmalıdır. Ayrıca bu tip yerlere kartlı giriş/çıkış sistemi ve kamera gözetimi gibi ilave tedbirler uygulanması da gerekmektedir[108].

Fiziksel güvenliği sağlama adına dikkat edilmesi gereken başka bir noktada; bilişim sistemleri ve kritik bilgi varlıklarının bulunduğu yerler seçilirken yangın, su baskını ve doğal felaketler gibi etkenler göz önünde bulundurulması gerektiği ve yangın söndürme sistemleri ve ısı, nem v.b. sensörlerin yerleştirilmesinin yanında buradaki sistemlerle sürekli iletişim durumunda bulunan cihazların farklı noktalarda konuşlandırılması gerektiğidir.

3.2. Kurumsal Korunma Tedbirleri

Teknolojinin gelişmesi ve buna bağlı olarak kurum ve şirketlerin iş yönetimi ve hizmet sunumlarını elektronik ortama taşımaya başlamasıyla birlikte siber güvenliğin sadece teknik ve fiziki önlemlerle sağlanamayacağı aynı zamanda

kurumsal bir yönetim yapısı olarak ele alınıp her iş sürecinde değerlendirilmesi yapılarak personel tarafından da desteklenmesi gerekmektedir. Kurumdaki hassas bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin güvenliğini sağlama, kurumun personellerinin uymasını sağlayacak politikalar üretmesi, ürettiği bu politikalara uyum sağlama adına ilgili kullanıcı ve yöneticilere sistematik eğitimler düzenleyerek siber güvenlik bilinci oluşturmayla mümkün olacaktır. Ayrıca işe alınacak personelin güvenlik tahkikatının iyi yapılması, personelin yanlış kullanımından dolayı oluşacak güvenlik açığına karşı idari tedbirlerin alınması, kullanıcı personelin siber suçları ve ilgili yasal mevzuatı bilerek hareket etmesinin sağlanması ve sistemler üzerindeki dosya paylaşımı ve yetkilendirmenin hiyerarşiye uygun düzenlenmesi alınabilecek kurumsal korunma tedbirleri olarak sayılmaktadır[5].

3.3. İşlemsel ve Teknolojik Korunma Tedbirleri

Bilişim sistemlerinde kullanılacak yazılımların lisanslı ve güvenilir yazılımlar olması, sistemlerin kullanımda olmadığı durumlarda yetkisiz personelin verilere erişimini engellemek amacıyla ekran koruma parolası konarak sadece giriş yetkisi olan personel tarafından bilinmesinin sağlanması, bilgisayarların sistem ayarlarında yapılacak düzenlemelerle harici bellek, CD-DVD ve disket gibi depolama birimlerinin kullanımının kontrol altına alınması, virüs koruma ve güvenlik duvarı yazılımlarının sistem açıldığı andan itibaren aktif olacak biçimde sistemlere kurulumunun ve düzenli olarak güncellenmesinin sağlanması, iç ve dış ağlarda sürücü ve dosya paylaşımıyla ilgili izin ve yetkilerin her personelin bulunduğu pozisyon ve görev yerine uygun şekilde yapılandırılarak ilgisiz kişilerin her veri ve dosyaya erişiminin engellenmesi gibi bir takım güvenlik önlemlerinin uygulanması gibi önlemleri bu tür korunma tedbirlerinden saymak mümkündür.

Ayrıca daha önce ifade edildiği gibi kurum ve şirketlere yapılan saldırıların ağ sistemlerinden web uygulamalarına doğru kayması ve birçok kurum ve şirketin bilgi varlıklarını internet ortamına taşıyıp giderek artan miktarlarda web uygulamaları kullanmasının yanında web sistemleri için gerekli güvenlik önlemlerini alınmadığı bilinmektedir. Yukarıda bahsedilen önlemlerle birlikte aşağıdaki gibi bazı ilave önlemlerin alınması da tehdit ve saldırıların önemli ölçüde azaltılmasını sağlayacaktır.

- İnternette güvenilirliğinden emin olunmaya sitelere girilmemeli ve herhangi dosya yükleme ya da indirmesi yapılmamalıdır.
- Göndereni tanınmayan, bilinmeyen veya şüphe duyulan e-postalar siber tehditlere maruz kalmamak için açılmadan silinmelidir.
- E-posta yoluyla gelen .ini, .exe v.b.. uzantılı dosyalar zararlı yazılımlar olma durumundan dolayı hiçbir şekilde kabul edilmemelidir[71].

Kurumsal siber güvenliğin sağlanmasında yukarıda bahsedilen önlemlerle birlikte uygulanabilecek bazı yazılımsal ve donanımsal önlemlerden bahsetmek yerinde olacaktır.

3.3.1. Güvenlik duvarları



Şekil 3.1. Güvenlik duvarı temsili gösterimi[24]

Özellikle kurumsal ağlarda güvenliği sağlama konusunda güvenlik duvarları en önemli uygulamalardan biridir. Sosyal hayatta nasıl bir market ya da sinema gibi mekânlara giriş ve çıkışlar belirli noktalardan yapılıyorsa (kurumsal ağlardaki) ağ güvenliğini sağlamak için sisteme dışarıdan yapılan erişim istekleri de çeşitli güvenlik önlemlerinden geçirilerek yetkili olup olunmamalarına göre erişim sağlayabilmelerine olanak tanıyan güvenlik duvarları üzerinden yapılması gerekmektedir. En genel anlamda, (kurumsal) ağ sistemine giriş ve çıkışların bir noktadan yapılmasını sağlayarak bu noktada almış olduğu güvenlik önlemleri ile etkin kayıt mekanizmalarının oluşturulmasına imkân veren ağ modeli[9] şeklinde tanımlanan güvenlik duvarlarını, internet ortamından gelen erişim isteklerini ve verileri (yapısında barındırdığı güvenlik ayarlarına göre) denetleyerek bu erişim

istekleri ve verileri engelleyerek veya geiş izni vererek siber saldırı ve tehditlere karşı koruma saėlayan yazılım ya da donanımlar řeklinde tanımlamakta mümkündür[24].

Güvenlik duvarları, virüs koruma yazılımlarıyla aynı deėildir. Ancak etkin bir koruma için her ikisinin de bir arada kullanılması daha uygundur. Güvenlik duvarları (firewall) paket filtreleme ve vekil (proxy) sunucuların (genellikle) birlikte kullanıldığı bir sistemdir.

Paket filtreleme: Güvenlik duvarı üzerinde oluşturulan güvenlik politikalarına göre (kurumsal) aė sistemine gelen paketleri (istekler) engeller ya da ilgili yerlere (yönlendiriciler aracılığıyla) iletilmesini saėlar. Örneėin dışarıdan telnet hizmeti ile herhangi bir istek (paket) erişimi istenmiyorsa güvenlik duvarı üzerinde ilgili porta (23 numaralı porta) gelen isteklerin engellemesini saėlayacak tanımlamalar yapılarak işlem gerçekleştirilir.

Vekil sunucu (Proxy server): İstemci ile sunucunun birbirleriyle iletişim kurmasını saėlayan vekil sunucular, kurumsal aė sistemindeki kullanıcılardan (istemci) gelen erişim isteklerini önceden belirlenmiş güvenlik politikalarına uygunsa internet ortamındaki bilgisayara (sunucu) iletir. Sunucuya ilettiėi tüm işlemlerin kaydını (log) tutarak kullanıcının yaptığı işlemleri izleyen vekil sunucu, belirlenmiş güvenlik politikaları nedeniyle kimi zaman bazı hizmetlerin gerçekleştirilmesini de engeller. Örneėin bir aė sistemindeki kullanıcıların internet ortamına dosya göndermesinin engellenmesi veya belirli sitelerden dosya indirilmesine izin verilmesi FTP vekil sunucu tarafından gerçekleştirilir.

Güvenlik duvarlarının kurumlar tarafından tercih edilmesinin belli başlı sebepleri bulunmaktadır:

- Güvenlik önlemlerinin birçok birim üzerinde dağıtılması yerine tek bir noktada toplanmasını saėlayarak güvenlik kararları hususunda merkezi bir sistem geliştirir.
- İnternet ortamında bulunan zararlı içeriėe sahip pek çok verinin ve hizmetin geişini engelleyerek sadece güvenlik politikalarına uyan hizmet ve verilerin geişine izin verir.

- Ağın kullanımı ve performansı hakkında bilgi toplanması ve gerekli kayıt mekanizmalarının (log faaliyetleri) oluşturulmasında etkilidir.
- Ağın bir bölümünün diğer bölümlerden korunmasını sağlayabilir[9].

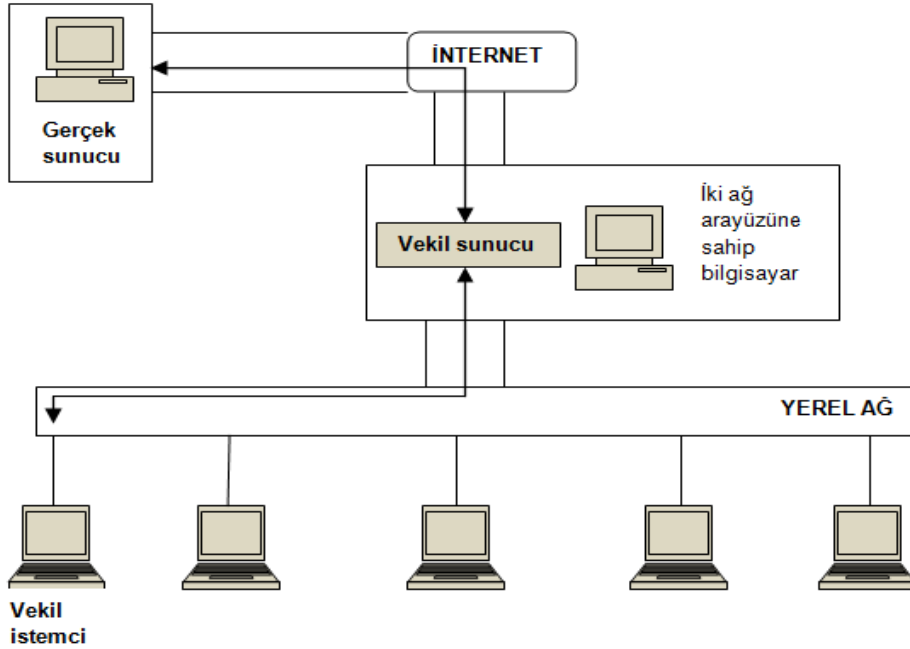
Güvenlik duvarları, internetin temeli olan TCP/IP (Transmission Control Protokol/Internet Protokol) iletişim protokolünün OSI (Open System Interconnection) adlı katman standartları üzerinde aldıkları önlemler ile ağ sistemlerini korudukları bilinmektedir. Bunları üst katmandan alta doğru:

- Uygulama Katmanı (Application Layer)
- Sunum Katmanı (Presentation Layer)
- Oturum Katmanı (Session Layer)
- Nakil Katmanı (Transport Layer)
- Ağ Katmanı (Network Layer)
- Veri Bağlantı Katmanı (Data Link Layer)
- Fiziksel Katmanı (Physical Layer) şeklinde sıralamak mümkündür.

Güvenlik duvarları en üstteki katmana kadar güvenlik sağlayabilmesine karşın günümüzde genelde 4. Katmana kadar güvenlik sağlayanlar kullanılmaktadır. Ancak günümüzdeki siber tehdit ve saldırılardaki karmaşıklık ve gelişmişliğin artması neticesinde çoğu zaman bu geleneksel güvenlik duvarlarının (Microsoft tarafından üretilen IISLock ve URLScan gibi) uygulama tabanlı güvenlik duvarları ile desteklenmesi gerekmektedir. Ayrıca siber saldırı ve tehditlerin özellikle web uygulamalar üzerinde yoğunlaşmasından dolayı HTTP/HTTPS/SOAP/XML-RPC/Web Servisleri üzerinde detaylı paket incelemesi yaparak zararlı istekleri engelleyen (modsecurity Apache gibi) web uygulama güvenlik duvarlarının (WAF - Web Application Firewall) kullanılması da fayda sağlayacaktır[14]. Bu bağlamda (web uygulama güvenlik duvarları hariç) güvenlik duvarı mimarileri:

- Birbirleriyle doğrudan iletişime geçemeyen (yerel ağdaki ve web ortamındaki) bilgisayarlar, iki ağ ara yüzüne sahip olan bilgisayara ya doğrudan bağlanarak ya da bu makine üzerindeki vekil sunucular ile birbirleriyle iletişime geçebildiği ve vekil sunucu kullanılması dolayısıyla (şifre kırma saldırılarına karşı daha etkili olduğu için) daha çok tercih edilmesine karşın IP (Internet Protocol) paketlerindeki yönlendirmelerden

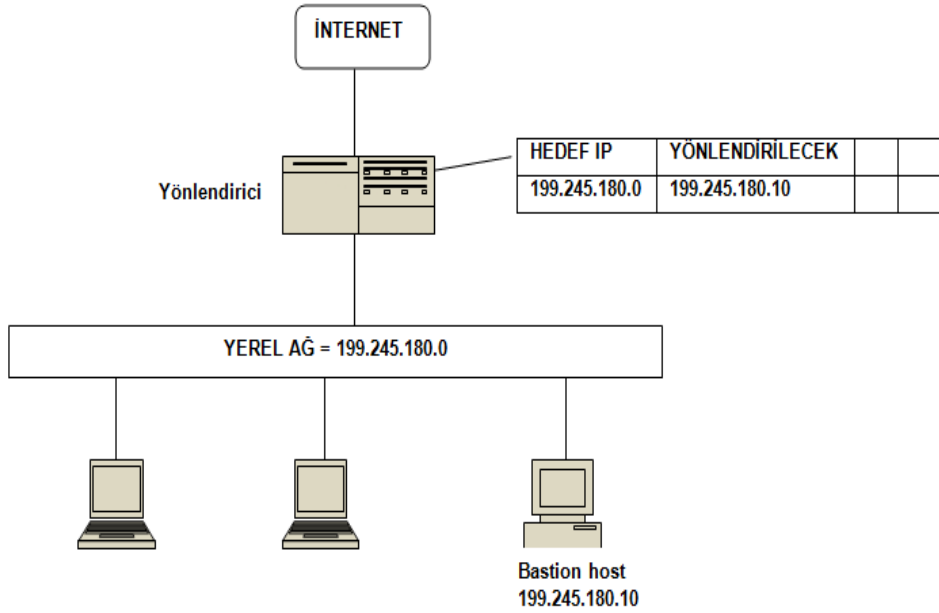
dolayı güvensiz hizmetlerin aktif hale getirilmesiyle saldırganların ağa erişimine olanak tanıyabilme dezavantajına sahip Çift taraflı geçit tipi (Dual-Homed Gateway Host) mimari(Şekil 3.2)



Şekil 3.2. Çift taraflı geçit (Dual-Homed Gateway Host) mimarisi[9]

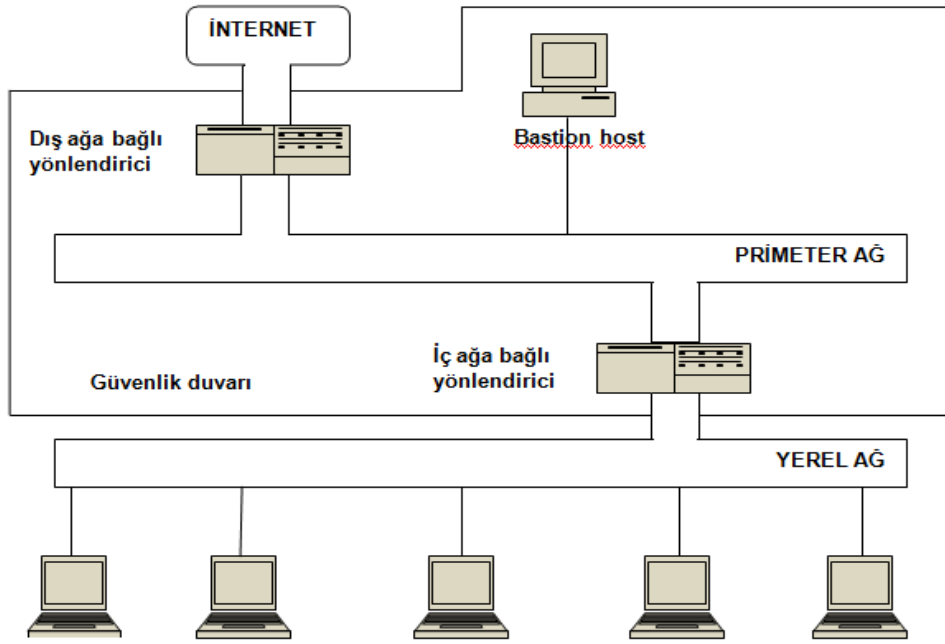
- İnternet ortamından gelen isteklerin öncelikle bir bilgisayarla iletişime geçmesi ve sonrasında (önceden belirlenmiş güvenlik politikalarına uygunsa) gerekli hizmetin ya bu bilgisayar tarafından karşılanması ya da yerel ağdaki hizmeti sağlayan sunucuyla iletişime geçerek karşılanması şeklinde gerçekleşen ve internet ortamından gelen paketlerin (her ne kadar yönlendiricideki (router) paket filtreleme sisteminden geçtikten sonra da olsa) yerel ağa girmesine izin veren bir mimari olduğu için ilk başta çift taraflı geçit tipi mimariye göre daha riskli görülebilse de bir yönlendiricinin güvenliğini sağlamanın daha kolay olması ve (çift taraflı geçit tipi mimarideki gibi) tek bir bilgisayarda yapılabilecek bir yapılandırma hatası nedeniyle bütün bir yerel ağın güvenliğinin tehlikeye düşmesinin söz konusu olmaması gibi durumlardan dolayı bu mimarinin çift taraflı geçit tipi mimariye göre daha güvenilir olmasının yanı sıra ağa bağlı bilgisayara (bastion host) ulaşan bir saldırganın ağdaki tüm bilgisayarlara ulaşmasını engelleyecek bir

güvenlik önleminin olmaması gibi bir eksikliğe sahip olan Perdelenmiş kullanıcı tipi (Screened Host) mimari(Şekil 3.3)



Şekil 3.3. Perdelenmiş kullanıcı (Screened Host) tipi mimari[9]

- (Perdelenmiş kullanıcı tipi mimaridekinden farklı olarak) yerel ağ ile internet ortamı arasına bilgisayarı (bastion host) da içine alan ek bir ağ (perimeter ağ) ilave edilmesiyle yerel ağdan soyutlanmasının sağlandığı ve ilave olunan ağ sayesinde bilgisayara (bastion host) erişebilen saldırganın sadece internet ile yerel ağ arasındaki trafikten ibaret olan ağ (perimeter ağ) trafiğini izleyebildiği, yerel ağdaki trafiğe herhangi bir müdahalede bulunamadığı Perdelenmiş alt ağ (Screened subnet) tipi mimari(Şekil 3.4) olmak üzere 3'e ayrılmaktadır[9].



Şekil 3.4. Perdelenmiş alt ağı (Screened subnet) tipi mimari[9]

Web uygulama güvenlik duvarları

Günümüzdeki güvenlik duvarları genellikle (internet ortamından gelen paketlerin IP adresi, port numarası gibi özelliklerine bakarak) OSI katmanında 4. Seviyeye kadar koruma sağlamaktadırlar. Ancak bu durum artan ve gelişen siber tehdit ve saldırılar için yeterli olmamaktadır. Kurum ve şirketlerin uygulama ve hizmetlerini büyük bir hızla web ortamına kaydırmasıyla (gereksiz servis ve hizmetlerin kullandığı portları kapatarak bir derece güvenlik sağlayabilen) geleneksel güvenlik duvarlarının (80 ve 443 numaralı portları web uygulamaları için açık tutmaları gerektiğinden) web ortamından gelen saldırı ve tehditler konusunda etkisiz kaldığı görülmektedir. Bu noktada detaylı paket incelemesi yaparak zararlı istekleri engelleyebilen web uygulama güvenlik duvarları (WAF) karşımıza çıkmaktadır. Web uygulama güvenlik duvarları için çeşitli yaklaşımlar kullanılmaktadır.

Beyaz liste modeli : İzin verilen belirli işlemler hariç her şeyin engellenmesi yaklaşımı.

Kara liste modeli : Yasaklanmış belirli işlemler hariç her şeye izin verilmesi.

Öğrenme tabanlı model : Gelen ve giden isteklere bakılarak web sayfalarının haritasının çıkarıldığı bu modelde güvenlik duvarı öğrenme sonrasında <http://www.ornek.com/~user/> dizinini zararlı kabul ettiyse ve bu dizinle aynı sunucu

üzerinde izinsiz bir şekilde www.abc.com adlı bir web sitesi çalıştırılırsa güvenlik duvarı bunu fark ederek engeller[17].

3.3.2. Antivirüs yazılımları

Kötücül yazılımlar (virüs, solucan, truva atları v.b.) gibi sisteme ve sistemdeki verilere ciddi zarar verebilecek yazılımları tespit etme, silme işlemlerini yapabilen, sürekli aktif halde çalışarak sistemi koruma özelliğine sahip belirli aralıklarla güncellenmesi gereken yazılımlardır. Belirli aralıklarla güncellenmesinin nedeni; gün geçtikçe gelişen ve daha karmaşık bir yapıya bürünen siber tehditlerin bu koruma yazılımlarını alt edecek şekilde tasarlanmasından dolayı bu tür tehditlere karşı güvenlik etkinliğini kaybetmemek için güncelleme yapılması gerekmektedir. Ayrıca bu yazılımları (özellikle sistem internete bağlı olarak çalıştığı süre içinde) sürekli aktif halde bulundurmak ve web ortamından indirilen dosya ve klasörleri bu yazılımların taramasından geçirilmeden açmamak dikkat edilmesi gereken güvenlik önlemlerindendir[35].

Kurumsal ağlarda sunucuların farklı yerlerde bulunabilmesi nedeniyle antivirüs programlarının bu yapıya uygun şekilde opsiyonlarının alınmasında fayda vardır. Ayrıca kurumsal antivirüs yazılımlarına ilişkin olarak önemli görülen diğer hususlar şu şekilde sıralanmaktadır:

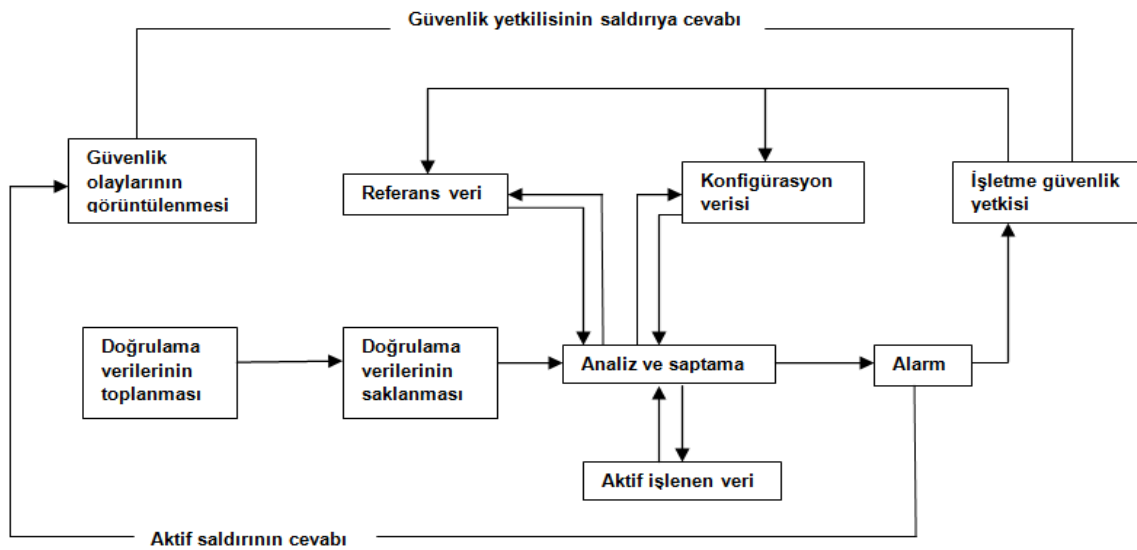
- Özellikle kurulum dosyası uzaktan yapılandırılabilir olmalı ve (Active Directory gibi) izin hizmeti sunan sistemler üzerinden kurulabilmelidir.
- Kurulum dosyasının ağ üzerinde bulunan farklı sunuculara önceden gönderilerek kullanıcılar kurulum dosyalarını bağlı oldukları sunucu üzerinden indirebilmeli ve güncellemeleri de bunlar üzerinden belirli aralıklarla yapabilmelidir.
- Ağdaki kullanıcılar belirli özelliklere göre gruplanıp her gruba özgü farklı güvenlik politikaları atanmalıdır.
- Merkezi konsol aracılığıyla ağ üzerinde anti virüs programının çalışmadığı makinelerin tespit edilerek yazılım kullanıcısıyla etkileşime girmeden kullanıcının sistemine kurulmalıdır.

- Kullanıcıların gerçekleştirdiği (ya da maruz kaldığı tehditler gibi) olaylar merkezdeki konsola gönderilmeli ve bu konsol tarafında bunlar tutularak istenen kriterlere göre raporlanmalıdır[96].

Ayrıca kurumlar ve şirketlerde kullanılan yukarıda belirtilen özelliklere sahip antivirüs programlarının üretici firmalarının Türkiye’de konumlu bir ofisi ve bu ofisinde çalışan Türk temsilcilerinin olması, web sayfasındaki bilgi bankasının gelişmiş ve kolay erişilebilir olması gibi ek özelliklere sahip olması da güvenlik açısından artı değerler katmaktadır.

3.3.3. Saldırı tespit ve önleme sistemi (IDS/IPS)

Güvenlik duvarları internet ortamından gelen saldırı ve tehditlere karşı (belirli oranda) güvenlik sağlasa da özellikle yerel ağlardan gelebilecek tehdit ve saldırılar konusunda yetersiz kalmaktadır. Farklı şekilde yapılandırılabilmelerine rağmen yine de etkin bir koruma sağlayamayan güvenlik duvarlarını desteklemek için geliştirilen saldırı tespit sistemleri, gerek internet ortamında (özellikle kurum ve şirketler tarafından kullanılan web uygulamalarının artmasına paralel olarak) artan siber saldırı ve tehditlere karşı gerekse de kurum veya şirket içindeki yerel ağ üzerinden gerçekleştirilebilecek saldırı ve tehditlere karşı önemli güvenlik mekanizması oluşturmaktadır[2].

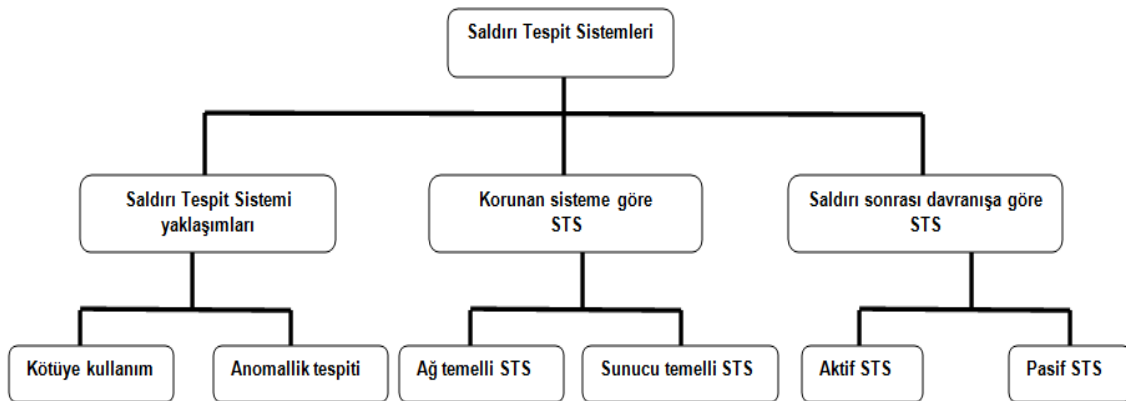


Şekil 3.5. Bir saldırı tespit sistemi modeli[7]

Saldırı tespit sistemlerinin yapısı ve işlevini (Şekil 3.5' te görüleceği üzere) kısaca şu şekilde özetlemek mümkündür[7]:

1. Gerek iç ağda gerekse dış ağda gerçekleşen olayları izleyerek elde edilen (ağ üzerinde çalışan uygulamalar tarafından gerçekleştirilen işlemler, kullanıcılar tarafından yerel ağ veya internet ortamındaki bilgisayarlarla yapılan iletişimler ya da veri aktarımları v.b.) veriler toplanıp (Doğrulama verilerinin toplanması) daha sonra saldırı tanımlamaları veya mevcut saldırı durumlarıyla ilgili raporlar oluşturmak için saklanır.(Doğrulama verilerinin saklanması)
2. Sonrasında şüpheli faaliyetlerin tespit edilmesini sağlayan (Analiz ve saptama) bileşen için doğrulama verilerinin nasıl toplanacağı, saldırılara nasıl cevap verileceği ve hangi nitelikteki verilerin saldırı olarak nitelendirileceğine ilişkin bileşen (Konfigürasyon verisi) ile bilinen saldırılar hakkında saldırı imzalarının (kötüye kullanım tabanlı sistemler için) veya ağdaki normal kabul edilen faaliyetler için referans niteliğindeki bilgilerin (anomali tabanlı sistemler için) yer aldığı bileşen (Referans veri) ve analiz işlemi sonrasında ulaşılan sonuçların değerlendirilmesi (Aktif / işlenen veri) ile elde edilen veriler kullanılır.
3. Son olarak da eğer izinsiz ve yetkisiz bir erişim (sızma) söz konusuysa otomatik bir cevap verilir ya da şüpheli bir durumsa uyarı verilir.

Kısaca yapısından bahsedilen STS' yi (Saldırı Tespit Sistemleri) Şekil 3.6' ya göre sınıflamaya ayırarak bu sistemlerin işlevlerinden bahsetmek yerinde olacaktır.



Şekil 3.6. Saldırı tespit sistemlerinin sınıflandırılması[83]

a. Kötüye kullanım: Virüs tarama yazılımlarıyla benzer mantıkta çalışan bu yöntemde veritabanında (saldırı ve tehditleri tespit etmek amacıyla) daha önceki bilinen saldırıların belirli özelliklerinin dikkate alınmasıyla oluşturulan veriler ve saldırıları tanımlamak için veritabanına girilmiş imzalar, ağ sistemindeki verilerle karşılaştırılır. Bu yöntemde dikkat edilmesi gereken husus, saldırıların tanımlandığı imzaların veritabanında devamlı güncel olmasıdır. Bir takım özel saldırı ve tehdit araçlarına karşı sistemin hızlı bir şekilde uyumlu hale gelebilmesi, büyük oranlarda saldırıların varlığını tespit yüzdesi gibi olumlu yönleri olduğu gibi yalnızca veritabanında bulunan imzaları bulunan saldırıların tespit edilebilmesi ve sadece genel nitelikteki saldırıların çeşitli varyasyonlarının tespit edilebilmesi gibi olumsuz tarafları da bulunmaktadır[82].

b. Anomallik tespiti: Ağdaki hareketlerin uzun süre analiz edilmesiyle belirlenen olaylar sonucunda oluşturulan profillerle ağ sisteminde meydana gelen işlemlerin karşılaştırılmasına dayanmaktadır. Bu yöntemin başarısı, oluşturulan profillerin başarısına bağlıdır. Bu yöntemin daha önceden bilinmeyen saldırıların tespit edilmesi ve elde edilen verilerin (kötüye kullanım tabanlı sistemler için) imza tanımlamalarında kullanılabilmesi gibi olumlu yönleri varken saldırıların varlığı hususunda çoğu kez yanlış saptamalar yapabilmesi ve profilleme yapılabilmesi için kapsamlı sistem denetleme kayıtlarına ihtiyaç duyulması gibi olumsuz yönleri de bulunmaktadır[7].

c. Ağ temelli: Ağ sistemi üzerinde işleyen trafiği algılayarak sistemdeki her bir paketin içeriğinin veritabanındaki bilgilerle karşılaştırmasını yaparak saldırı niteliği taşıyıp taşımadığına karar verebilmektedir. Güvenlik duvarına benzer bir yapısı olsa da işlevleri bakımından farklıdır. Çünkü güvenlik duvarında tanımlanan kurallar çerçevesinde belirli servislere ve sistemlere ulaşabilirsiniz ancak gelen paketin içeriği kontrol edilmemektedir. Bu yapıda ise direk olarak paketin içeriğine bakılarak işlem yapılmaktadır. Ağdaki trafiği izlemeye başarılı olan bu yapının (özellikle anahtarların (switch) kullanıldığı büyük) ağlardaki kör noktaları izleyemeyebilmesi ve şifreli verileri çözememesi gibi eksiklikleri bulunmaktadır[13].

d. Sunucu temelli: Kurum içindeki yerel ağdan kaynaklanabilecek saldırıları tespit edebilen bu yapıda işletim sistemi tarafından tutulan sistem, olay ve güvenlik kayıtlarının izlenmesi sonucunda (bu kayıtlarda herhangi bir değişiklik olduğunda)

kayıt ile veritabanındaki imzaların karşılaştırılması yapılarak saldırı olup olmadığına karar verilir. Bu yapının, ağ temelli yapıya göre daha hızlı olması, dosya erişimi ve dosya yetkilerindeki değişimler gibi alt seviyedeki işlemleri izleyebilmesi, şifreli veriler kullanılarak yapılan saldırıları tespit edebilmesi, ilave donanım gereksinim duymamasından ötürü maliyeti az olması gibi avantajlarıyla birlikte kayıt dosyalarının büyüklüğünden ötürü bu dosyaların analiz edilebilmesi için güçlü bilgisayarlar gerektirmesi ve bu kayıtları inceleyecek personelin çok fazla zamanını alması, (özellikle) büyük ağlarda ağın her tarafına nüfuz edememe gibi dezavantajları bulunmaktadır[83].

e. Aktif ve pasif STS' ler: Ağ sistemine yönelik herhangi bir saldırı olduğunda saldırının kayıtları tutulup sistem yöneticisine veya ilgili personele uyarı mesajları iletiliyorsa *pasif*, tespit edilen saldırıya karşı aynı zamanda duruma göre (güvenlik duvarı ayarlarında değişiklik yapma, bazı servislerin yasaklanması ya da saldırgan kabul edilen kullanıcının oturumunun kapatılması gibi) bazı güvenlik önlemleri alınabiliyorsa *aktif* bir yapının varlığı anlaşılır. Bu tür aktif yapılara saldırı önleme sistemi (IPS(Instrution prevention system)) de denilmektedir.

Saldırı Önleme Sistemleri (IPS), güvenlik duvarından önce konumlandırılarak gelen (zararlı kodlar içeren) paketleri engelleyip kapsamlı bir koruma sağlayabildiği gibi web sunucu üzerinde konumlandırılarak (sunucu tabanlı saldırı önleme sistemleri) http isteklerini işleme tabi tutabilmektedirler.

3.3.4. Sızma (penetrasyon) testleri

Kurumsal anlamda siber güvenliğin sağlanmasında herhangi bir saldırıya maruz kalmadan önce güvenlik zafiyetlerinin tespit edilmesi, bu zafiyetlere yönelik gerekli önlemlerin alınması ve bu sürecin belirli periyotlarla devam ettirilmesi gerekmektedir. Bu noktada karşımıza çıkan güvenlik (sızma) testleri saldırı öncesinde bir saldırgan mantığıyla bilgi sistemlerine kontrollü saldırılar yapılarak güvenlik açıklarının tespit edilmesini sağlar.

Kurumsal siber güvenliğin sağlanmasında bilgi ve iletişim teknolojileri üzerindeki güvenlik açıklıklarının erken tespit edilerek giderilmesi önem taşımaktadır. Bu bağlamda kurumsal bazda etkin bir güvenlik mekanizması sağlamak için kullanılan

sızma testlerinin kurumlar tarafından hangi amaçla ve ne şekilde kullanılması gerektiğinin bilinmesi gerekmektedir. Özellikle günümüzde artarak devam etmekte olan siber tehdit unsurlarının varlığı ve siber saldırıların çoğunun kurumsal bazda olması (özellikle kurumların web uygulamalarına yönelik olması) gibi etkenler penetrasyon (sızma) testlerinin göz ardı edilmemesi gereken bir güvenlik unsuru olduğunu göstermektedir.

Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırıların ciddi ve telafisi zor kayıplara yol açtığı günümüzde sızma testleri; bilgi ve iletişim sistemlerinin saldırgan mantığıyla önceden zafiyetlerinin tespitinin yapılması bu sistemlerin ileride maruz kalabilecekleri saldırıları büyük kayıp ve eksikliklere sebebiyet vermeden atlatmalarını sağlar. Ayrıca teknolojinin gelişimiyle birlikte kurumların ihtiyaçları doğrultusunda bilgi varlıkları üzerinde değişiklikler yapmalarının kaçınılmazlığı dolayısıyla bu yeni sistem ve teknolojilerin entegrasyonu birlikte oluşabilecek bir takım yeni zafiyetlerin tespit edilmesi, bilgi sistemlerinin birçok güvenlik kontrollerinden taviz verilerek tasarlanmasından dolayı meydana gelebilecek yetkisiz erişimlerin engellenmesi, kurumlar için güvenliğin yaşayan bir süreç olarak ele alınmasının zorunlu olduğu günümüzde güvenlik yatırımlarındaki maliyetin azaltılması, yapılan bu yatırımların etkinliğinin değerlendirilmesi ve kurumun bilgi güvenliği politikalarının gözden geçirilmesi için sızma testlerinin işin uzmanlarınca ve belli periyotlarla yapılması gerekmektedir[76].

Sızma (penetrasyon) testlerinin aşamaları

Sızma testleri:

- Uygulanacak sızma testi türlerinin, bilgi ve iletişim teknolojilerine yönelik risklerin, testlerin gerçekleştirilmesinde kullanılacak araçlar, personel, maliyet v.b. konuların belirlendiği *planlama aşaması*,
- Uygulanacak test türüne bağlı olarak (internet gibi) herkesin ulaşabileceği yollarla kurumların bilgi ve iletişim teknolojileri hakkında araştırmaların yapıldığı ve bu araştırmalarda test konumuna (kurum içi, kurum dışı) göre açık kaynaklar (internet, intranet, gazeteler, haber grupları, dergiler,

televizyonlar v.b.) ve sosyal mühendislik testleriyle kurum veya kuruluşlar hakkında detaylı bilgilerin toplandığı *bilgi toplama aşaması*,

- Bilgi kaynakları üzerinde var olan ve istismar edilebilecek güvenlik boşluklarının tespit edilerek tanımlanması ve sınıflandırılmasının yapıldığı *zafiyet analiz aşaması*,
- Bilgi sistemleri üzerinde çalışan uygulama ve yazılımların güvenlik açıklarını kullanmayı sağlayan istismar kodlarının (sızma testi yapılacak sunucu bilgisayar üzerinde daha önceden verilmiş erişim hakkı yok ise “uzak”, erişim hakkı var ise “yerel” istismar kodlarının) kullanıldığı sızma testlerinin en önemli aşamasını oluşturan *zafiyet kullanım aşaması*,
- Sızma testleri sonucunda tüm çalışmayı özetleyen ve karar verme aşamasında üst yönetime tavsiyeler içeren bir kılavuz niteliğinde olan (yönetim özeti, gerçekleştirilen hizmetler ile sonuç ve önerilerin yer aldığı üç ana kısımdan oluşan) raporun hazırlandığı aşama olmak üzere 5 aşamadan oluşmaktadır[77].

Çizelge 3.1. Güvenlik testlerinin sınıflandırılması

KRİTERLER	TEST SEÇENEKLERİ		
Bilgi ve yetki	Yok (kara kutu)	Kısıtlı (Gri kutu)	Detaylı (Beyaz kutu)
Sisteme etkisi	Pasif	Normal	Aktif
Kapsam	Genel	Sınırlı	Özel
Konum	Kurum dışı	Kurum içi	Karma
Yöntem	Teknik olan	Teknik olmayan	Karma

Sızma testleri yöntemler bakımından incelendiğinde ise, *teknik olmayan (sosyal mühendislik) testler* ve *teknik testler* olarak ikiye ayrılmaktadır. Sosyal mühendislik testlerinde; saldırgan hazırladığı sahte e-postalarla, telefonla ya da sohbet ortamları veya sosyal medyada kullanıcıyı kandırarak istediği bilgilere erişmeye çalışır. Ayrıca kurumlarda yapılan çalışmalarla ilgili alınan çıktıların değişiklik yapılmasından sonra gerekli şekilde imha edilmemesi sebebiyle kurum ve kurumun çalışmalarıyla ilgili büyük miktarda bilginin “çöplük karıştırma” diye tabir edilen yolla elde edilmesi ve kişilerin masalarında bıraktığı (kullanıcı adı, şifre veya yapılan çalışmalarla ilgili v.b.) notlardan bilgi edinimi sağlayan “masaüstü testleri”

birer teknik olmayan testtir. Teknik testleri ise bakır ve fiber optik kablolardaki trafiğin dinlenmesi şeklinde ya da kablolu ve kablosuz ağlar üzerindeki paketlerin birer kopyasının alınmasını sağlayan yazılımlarla yapılan *pasif dinlemeler*, kullanıcı adı veya şifrelerin tahmin ya da kaba kuvvet yoluyla elde edilebilirliğinin ölçülmesi, bir veya daha fazla noktadan yapılan saldırılarla sistemi hizmet veremez hale sokmaya veya sistemin kaynaklarını tüketmeye çalışan *hizmet aksattırma testleri* ile yazılım ve donanımlarda bulunan *zafiyetleri tespit etme testleri* şeklinde gruplamak mümkündür[76].

Çizelge 3.2. Web güvenlik testleri sınıflandırması[77]

SIZMA TESTLERİ	YÖNTEMLER
KİMLİK DOĞRULAMA	Kaba kuvvet
	Yetersiz kimlik doğrulama
	Şifre kurtarma denetimi
YETKİLENDİRME	Oturum bilgisini tahmin etme
	Yetersiz yetkilendirme
	Yetersiz oturum sonlandırma
	Oturum sabitleme
KULLANICI TARAFLI	Siteler arası kod yazma
	İçerik sahteciliği
KOMUT ÇALIŞTIRMA	Ara bellek taşması
	Dizgi formatı
	LDAP enjeksiyonu
	İşletim sistemi komut enjeksiyonu
	SQL enjeksiyonu
	SSI enjeksiyonu
	XPath (XML Path Language) enjeksiyonu
BİLGİ AÇIĞA ÇIKARMA	Dizin listeleme
	Bilgi sızıntısı
	Yol takibi
	Tahmin edilebilir kaynak konumu
MANTIKSAL	Fonksiyonellik suiistimalleri
	Hizmet aksattırma
	Otomasyon
	Yetersiz denetim

Kurum hakkında test öncesi bilinen bilgi bakımından; kurumun bilgi ve iletişim varlıkları hakkında herhangi bir bilgi verilmeksizin yapılan testleri *kara-kutu*, kurum içindeki herhangi bir personel kadar bilgi ve yetki verilmesiyle yapılan testleri *gri-kutu*, kurumun bilgi ve iletişim varlıklarının tamamı hakkında bilgi ve yetki verilmesiyle yapılan testler ise *beyaz-kutu* testler şeklinde gruplanmaktadır[105].

Günümüzde (web sayfalarıyla oynanarak web uygulamalarının kaynak kodlarından yararlanılması, uygulamaya ait çerezlerle oynanması sonucunda da bir takım güvenlik açıklığına sebebiyet verebilecek hataların oluşturulması gibi) güvenlik ihlallerinin büyük bir bölümünün web uygulamalarındaki zafiyetlerden kaynaklanması nedeniyle kurumsal siber güvenliğin sağlanmasında özellikle web uygulamalarına yönelik sızma testlerinin (Çizelge 3.2) büyük önem kazandığı anlaşılmaktadır.

3.3.5. DoS engelleme sistemi

Bir bilgisayar veya ağın aşırı veri yoğunluğu ile hizmetinin durdurulması veya servis dışı bırakılması amacıyla yapılan DoS (Denial of service) saldırılarını engelleme de saldırı önleme sistemleri (genellikle) yetersiz kaldıklarından anormal veri trafiğini anlayabilen ve DoS saldırıların varlığını tespit edip gerçek zamanlı olarak bu zararlı trafiği engelleyebilen donanım ve programlardan oluşan sistemdir.

3.3.6. Veri Sızma Engelleme (DLP)

Kurum veya şirketin sahip olduğu kritik öneme sahip hassas verinin veya kişisel verilerin kasıtlı ya da kasıtsız olarak yetkisiz kişilerin eline geçmesi şeklinde tanımlanabilen veri sızmaları, kurumsal ağın dışından yapılacak bir saldırı neticesinde olabileceği gibi kurum içerisinde çalışan bir personelin kasıtlı olarak yapabileceği bir saldırı veya yeterince bilgi güvenliğine önem vermemesinden kaynaklanan hata sonucu olabilmektedir. Kurum ve şirketlerdeki bu veriler mali bilgiler, personellerin kredi kartı bilgileri ve kurum veya şirketin diğer bilgilerini içerebilmektedir.

Özellikle büyük çaptaki kurumlar için bir zorunluluk haline gelen DLP (veri sızma önleme) teknolojileri:

- Kurum personelinin kullandığı bilgisayarlarda saklanan hassas veriler ve kişisel verilerin (personel tarafından oluşturulabilecek güvenlik açığına neden olmaması için) ihlale uğramasına engel olmak için personele farkındalık eğitimi verilmesi, güvenlik politikaları oluşturulması ve (birçok kurumun da kullanmakta olduğu) IDS (Intrusion Detection Systems), güvenlik duvarı ve anti virüs yazılımlarını kapsayan standart güvenlik önlemleri,
- Yapay sinir ağları algoritmaları ve makine öğrenmesi gibi yöntemlerle veriye erişimdeki anormalliklerin tespit edilmesi, e-posta trafiğindeki anormalliklerin tespitini sağlayan uygulamaların kullanımı ve honeypot (bal kasesi) yönteminin uygulanması gibi önlemleri içeren gelişmiş güvenlik önlemleri,
- İç ve dış ağdan kaynaklanabilecek saldırıların neden olabileceği geniş miktarda kişisel verinin ihlaline engel olabilecek ve yetkisiz kullanıcıların erişimini engelleme de kullanılabilecek basit önlemler anlamında erişim kontrolü ve şifreleme,
- Hassas verilere erişim yetkisi bulunan personel tarafından (yetkisi olmayacak şekilde) kasıtlı veya kasıtsız olarak kurum için hassas nitelikteki verileri kopyalama ya da herhangi bir noktaya göndermek için yapılan hareketleri tespit etmek ve engellemek için oluşturulmuş güvenlik çözümleri olarak ifade edilen özel DLP çözümleri olmak üzere 4 farklı kategoriye ayrılmaktadır[66].

3.3.7. Saldırgan tuzağı ağları (Honeynet)

Zararlı yazılım ve saldırıları saptamak için kurulan tuzak sistemlerinden (honeypot) oluşur. Açık kaynak kodlu yazılımlarla kurulabilen bu sistemler; yerel ağın bir alt ağı olacak şekilde oluşturulup güvenlik duvarları tarafından izin verilerek bu ağa gelen bütün trafiği izleyip analiz ederek saldırgan veya zararlı erişimler takip edilmektedir. Ayrıca sistem üzerine konuşlandırılabilen “Honeywall” adlı yazılım sayesinde bu alt ağda oluşturulan tuzak sistemlerinin (bilgisayarların) ele geçirilmesi ve buradan dışarıdaki herhangi bir noktaya saldırı yapılması engellenebilmektedir[63].

3.3.8. Veritabanı güvenliği

Birbirleriyle ilişkili verilerin depolandığı alanlar olarak tanımlanabilen veritabanları[40]; depoladıkları veriyi işlemek ve hizmete sunabilmek için veritabanı yönetim sistemlerine ihtiyaç duymaktadırlar. Her geçen gün artan kurumsal web uygulamalarıyla birlikte internet ortamından veritabanı yönetim sistemlerine olan erişimin artması bu sistemlerin güvenliklerinin önemini ve zorluğunu arttırmıştır. Yapılan araştırmalar göstermiştir ki (eğer gerekli güvenlik önlemleri alınmazsa) basit yöntemlerle internet üzerinden veritabanlarına ulaşılarak kurum ve şirketlerin bilgileri elde edilebilmektedir. Verilerin toplu şekilde bir arada tutulduğu ve ulaşılabilirdiği veritabanlarını, web uygulamaları ile internet ortamına açan kurum ve şirketlerin veritabanı güvenliği hususunda oluşturdukları güvenlik çözümlerini, kurumsal iş süreçlerine entegre etmeleriyle etkin bir güvenlik yönetim sistemi sağlamaları ve veritabanı faaliyetlerini gerçek zamanlı izleyebilme yeteneğine sahip olmaları zorunluluk haline gelmiştir[78].

İnternet ortamına hizmet veren web uygulamaları, genellikle PHP ve ASP web programlama dillerinin kodları ile beraber SQL yapısal sorgulama dilinin komutlarını bir arada kullanarak veritabanına erişim sağlar. Ancak bu durum veri girişi ve sorgusunu hızlandırmasının yanında çeşitli güvenlik sorunlarını da beraberinde getirmektedir. Bu güvenlik açıklıklarından faydalanarak yapılan (özellikle en çok uygulanan SQL enjeksiyonu gibi) saldırılara karşı dikkat edilmesi gereken belli başlı hususları:

- Web uygulaması üzerinden veri girişi veya sorgulama yapılırken web tarayıcısı üzerinden adres çubuğu kaldırılarak bütün işlemlerin tarayıcı üzerinden yapılması sağlanmalı.
- Veri tabanına sızmak isteyen saldırganların hangi konumda olduklarını tespit edememeleri için veritabanına bağlandıktan sonra SQL ifadelerine bağlı herhangi bir hata mesajı web tarayıcısına döndürülmemeli.
- Veri girişi yapılan yer adları ile veritabanındaki değişken isimleri aynı olmamalı.
- Veritabanından veri istendiğinde veya veri gönderildiğinde birkaç veritabanının kullanılarak aralarında doğruluk karşılaştırması yapılmalı.

- Kullanılacak birden fazla veritabanı için her aşamada kullanıcı hakları ayrı ayrı tanımlanmalı. Böylece tek bir veritabanına erişim sağlandığında diğer veritabanlarına sızma gerçekleştirilemeyecektir.
- Veri girişi, okuma ve yazma hakkı tek bir yönetici tarafından verilmeli ve bu haklar kayıt altına alınmalıdır.
- (Veri girişinde kullanılan SQL ifadeleri ayrı bir şekilde olmak üzere) veritabanıyla yapılan her türlü işlem sunucu tarafından güvenilir kayıt mekanizmaları aracılığıyla kayıt altına alınmalıdır.
- Web tarayıcısından gelebilecek SQL komutlarının uzunluğu kontrol edilmeli ki veritabanına sızmak için yapılabilecek SQL komut değişiklikleri tespit edilsin.
- Kullanıcı tarafından veri girişi işlemi yapıldıktan sonra yedekleme işlemi yapılmalı.
- Birçok veritabanı bulunan sistemlerde ana veritabanı üzerinde sadece veritabanı yöneticisi konumundaki personelin yazma ve silme hakkı olmalı. Değiştirme hakkı ise ya yönetici şifresi ya da aynı anda 2-3 veri güvenlik personelinin şifresi ile elde edilebilmeli şeklinde sıralamak mümkündür[13].

3.3.9. Bilgi güvenliği yönetim sistemleri (BGYS)

Kurum içinde üretilen veya kuruma dışarıdan gelen o kurumla ilgili her türlü bilgi anlamındaki kurumsal bilginin güvenliği ile ilgili önlemler alınırken çalışanların benimsemesi, maliyet, kullanıcı tepkileri ve yönetsel zorluklar gibi faktörler de göz önünde bulundurulmalıdır[75]. Eğitim, teknoloji ve insan gibi birçok unsuru içeren kurumsal bilgi güvenliğinin kurumsal kültürün bir parçası haline getirilmesi ve bu bağlamda bazı standartların benimsenerek uygulanması gerekmektedir. Bilgi güvenliği yönetim standartlarına örnek olarak; kurum hedeflerine bilgi teknolojileri alt yapısını kullanarak ulaşmayı sağlayan COBIT, kartlı ödeme sistemlerinde bilgi güvenliği sağlamak için geliştirilen PCI DSS, hastaların sağlık bilgilerinin gizliliği ve güvenliği için çıkarılan HIPAA verilmektedir. Ülkemizde siber güvenliğe yönelik yatırımların yeterli olmamasının da etkisiyle meydana gelen istenmedik durumların kurum ve şirketleri olumsuz etkilemesi; kurumların etkin bir kurumsal siber güvenlik için BGYS (Bilgi güvenliği yönetim sistemleri) oluşturmalarını bir zorunluluk haline getirmektedir.

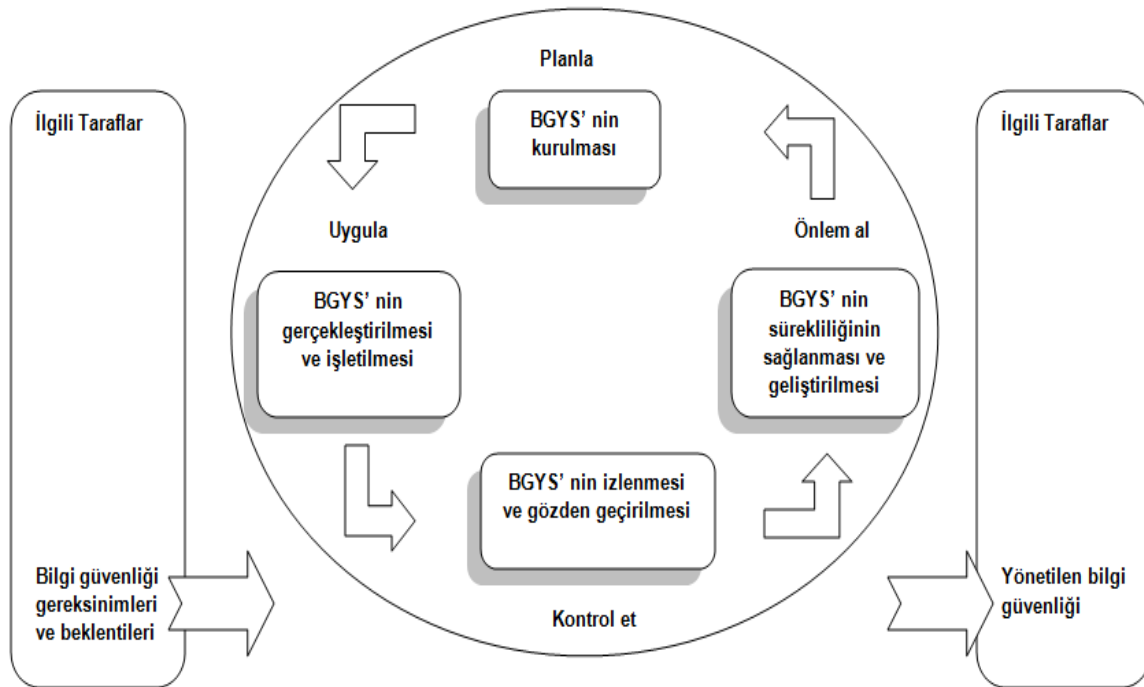
Yukarıda belirtilen standartlar belli bir teknoloji veya ürüne bağlı kalmaksızın direk olarak kurumsal bilgi güvenliği konusunu ele almaktadırlar. Bu standartların kullanımıyla oluşturulan BGYS'lerin kurulumu, işletilmesi, izlenmesi ve sürdürülmesi için PUKÖ (Planla – Uygula – Kontrol et – Önlem al) modeli kullanılmaktadır(Şekil 3.7).

Planla (BGYS'nin kurulması) aşamasında; BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi,

Uygula (BGYS'nin gerçekleştirilmesi ve işletilmesi) aşamasında; BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi,

Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi) aşamasında; BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi,

Önlem al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi) aşamasında; Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi yapılmaktadır.



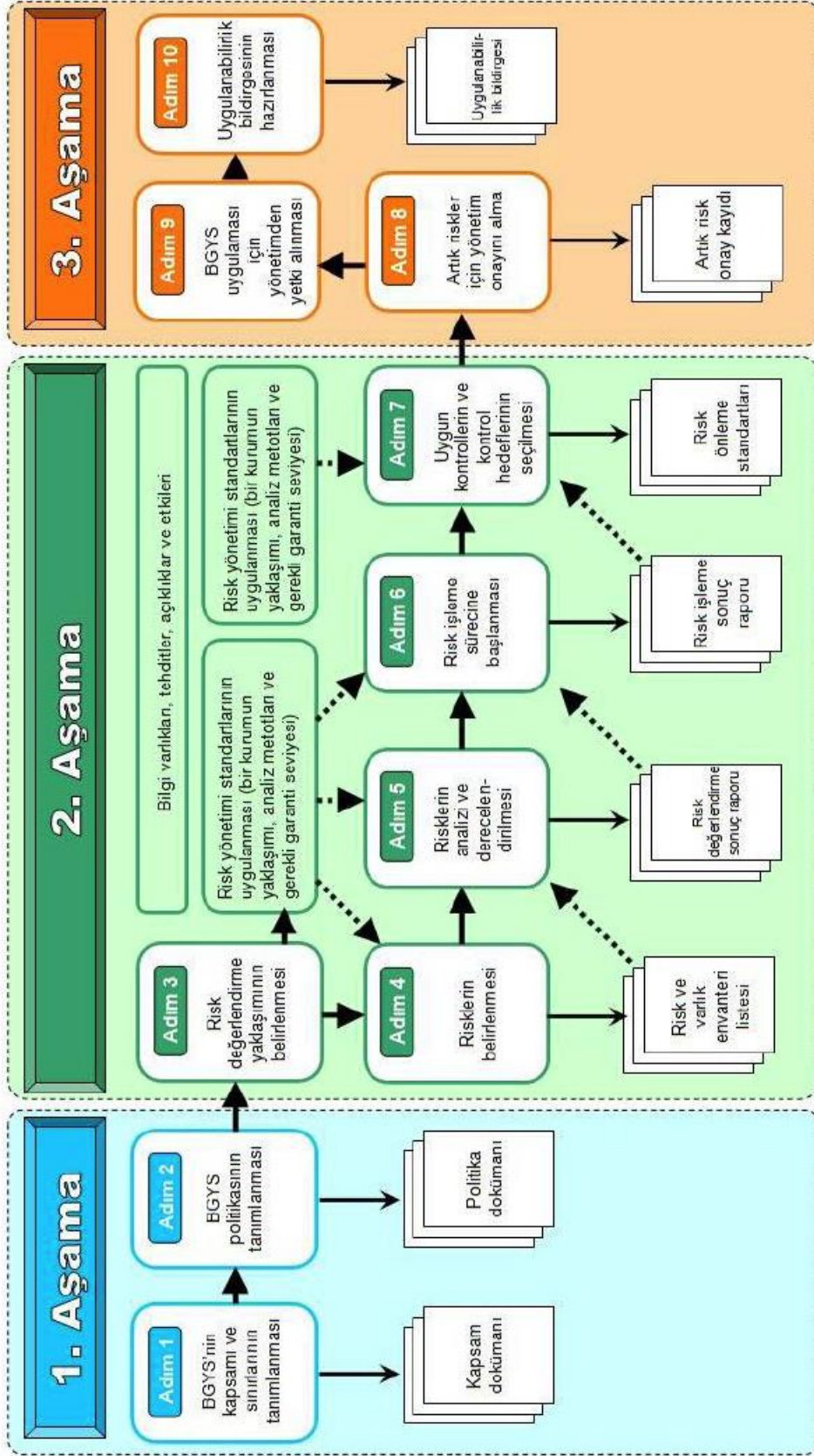
Şekil 3.7. BGYS süreçlerine uygulanan PUKÖ modeli[11]

Bilgi varlıklarının korunmasına yönelik kullanılan Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardı, kurumlar içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve geliştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS ile kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği yine Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı ile belirlenmektedir.

Bilgi güvenliği yönetimi bir defa oluşturulup biten bir proje gibi değerlendirilmeyip yukarıda belirtilen PUKÖ modelinde gösterilen Planla – Uygula – Kontrol et – Önlem al faaliyetleri bir döngü içinde devam ettiren süreç olarak düşünülmelidir. Bir kurumun BT bölümüne ait teknolojik bir çözüm ve teknik bir mesele olarak değil, kurumdaki tüm personelin katılımının ve desteğinin gerektiği, başarılı ve sağlıklı bir işleyişe sahip olması için üst yönetim tarafından desteklenmesi gereken bir süreç olarak değerlendirilmesi gereken BGYS' de; sorunlar ve ihtiyaçların daha iyi belirlenmesi ve yönetim ile teknik kadro arasındaki iletişim kopukluğunu gidermek için kurum içindeki her bölümden bilgi güvenliği konusunda yetkinliğe sahip (ya da bilgi güvenliği hususunda gerekli eğitimi alarak istenen düzeyde yetkinliğe erişimleri sağlanan) personellerin katılımıyla bilgi güvenliği komisyonu oluşturulması, oluşturulacak BGYS için ilk adımını teşkil etmektedir. Tüm bu hususlar ışığında BGYS oluşturulurken:

- (Kapsam dışı bırakılan varlıklar ve diğer kurumlarla olan etkileşimlerinin göz önünde bulundurularak hazırlanacak) BGYS kapsamının kurumun bilgi güvenliği hedefleri ve üst yönetimin niyeti doğrultusunda oluşturulması ve sonrasında kapsam dokümanı halinde yayınlanarak üst yönetim tarafından onaylanması sürecini anlatan kapsam belirleme,
- Yönetime yön veren, hedefleri ortaya koyan ve hangi riskin değerlendirileceğine ilişkin risk yönetim kapsamı çerçevesi içerisinde (üst yönetimin uygulanacağı hususundaki kararlılığını çalışanlarına hissettirdiği) politika oluşturulması anlamında BGYS politikası,

- BGYS kapsamına dahil edilen bilgi varlıkları, türüne ve kullanılabilirlik, gizlilik, bütünlük kriterleri ışığında önem derecesine göre liste şeklinde belgelendirildiği ve korunması gereken bilgi varlıkları için kabul edilebilecek risk seviyelerinin belirlenip bunlar için ölçütlerin geliştirildiği aşama olan Risk değerlendirme yaklaşımı ve risk belirleme,
- Riske neden olan tehdit ve güvenlik açıklıklarından yola çıkılarak bir önceki aşamada belirlenen risklerin yorumlanmasının (risk analizi) yapıldığı, tehdidin gerçekleşme olasılığı ve etki derecesinin hesaplandığı ve risk derecelendirmelerinin yüksek, düşük, orta gibi değerlerle ifade edilerek riski kabul edilebilir olup olmadığına karar verilip risk değerlendirme sonuç raporunun yayınlandığı adım olarak tarif edilen Risk analizi ve derecelendirilmesi,
- Risk değerlendirme sonuç raporu çerçevesinde; uygun kontrollerle riskin ortadan kaldırılması veya kabul edilebilir seviyeye düşürülmesi, riski oluşturan etkenlerin ortadan kaldırılarak riskten kaçınılması veya risk kabul ölçütleri ışığında riskin bilerek kabul edilmesi şeklinde gerçekleştirilebilecek 3 farklı yolun seçilebilmesi anlamında Risk işleme,
- Kurumun kendine özgü geliştirebileceği kontroller veya TS ISO/IEC 17799:2005'te bulunan kontrollerin risk işleme sürecine uygun olarak seçildiği Kontrol seçimi,
- Yukarıda belirtilen süreçler sonunda tamamen ortadan kaldırılamayan veya kabul edilebilen riskler (artık riskler) ile BGYS işletimi ve uygulamasını gerçekleştirmek için yönetimden onay alınmasını gerçekleştirildiği Artık risk ve yönetim onayı,
- (Kontrol seçiminde) 6.aşamada seçilen kontrollerin neler olduğu ve bunların hangi gerekçelerle seçildiğinin ve TS ISO/IEC 27001 EK-A' dan seçilmeyen kontrollerin neler olduğu ile bunların seçilmeme gerekçelerinin anlatıldığı bir belgenin hazırlanmasını belirten Uygulanabilirlik bildirgesi olmak üzere atılması gereken 8 adım bulunmaktadır[11].



Şekil 3.8. BGYS kurulum aşamaları[11]

4. SİBER SUÇLARA YÖNELİK HUKUKSAL BOYUT

Siber suçlar konusunda en geniş kabul gören tarif, AET (Avrupa Ekonomik Topluluğu) Uzmanlar Komisyonu'nun Mayıs 1983 yılında Paris Toplantısında yaptığı; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki ve yetki dışı gerçekleştirilen her türlü davranıştır." şeklindeki tariftir[98]. 1960' lı yıllara dayanan siber suç olgusunun 1970' li yıllarda bugün için basit denebilecek bilgisayar sistemlerinin yasadışı kullanılması ve bilgisayar casusluğu şeklinde görülürken, zaman içerisinde internetin yaygınlaşması ve teknolojinin gelişmesiyle daha karmaşık ve sistematik bir yapıya büründüğü gözlenmektedir.

Ucuz ve kolay bir şekilde işlenebilmelerinden ötürü gelecekte daha da artması beklenen siber suç kavramıyla sadece internet suçları değil (internetle beraber intranet ve diğer ağ sistemlerini kapsayan) siber uzayda işlenen suçlar da kastedilmektedir. Bu bağlamda, literatürde siber suçlar ile klasik suçlar arasındaki ilişkiyle ilgili iki görüş benimsenmektedir. Bunlardan ilki; her iki suçta da temel unsurlar bakımından fark olmadığı, tek farkın siber suçların siber uzay ortamında gerçekleştirilmiş olmaları ve siber uzayda gerçekleştirilen suç teşkil eden eylemlerin yeni bir suç tipi oluşturmadığı ve mevcut ceza normlarının uygulanabileceğini savunurken ikincisi; bazı suçların (LambdaMOO adlı sanal bir ortamda yaşanan "sanal ırza geçme" suçu gibi) sadece siber uzayda işlenebilmesinin mümkün olduğunu, bunların mevcut ceza normları ile çözülemeyeceğini ve ayrı bir hukuki rejimin oluşturulması gerektiğini savunmaktadır[67].

Siber suçların sınıflandırılmasıyla ilgili doktrinde (McConnel International adlı Amerikan global politika ve teknoloji yönetimi danışmanlık firması tarafından yapılan sınıflandırma gibi) bir çok sınıflandırma türü bulunmaktadır. Bu tür sınıflandırmalar bu tezin kapsamı dışında tutularak dünyada ve ülkemizde siber suçlara yönelik geliştirilen hukuki düzenlemeler incelenmektedir.

4.1. Dünyada Siber Suçlara ilişkin Yapılan Çalışmalar

Günümüzde bilişim teknolojilerinin özel ve kamu kurumlarıyla beraber bireysel kullanıcı bazında da artış göstermesiyle birlikte bu tür teknolojilerin güvenliğinin sağlanmasının daha bir önem kazandığı görülmektedir. İnternet kullanımının da yaygınlaşması (özellikle kurum ve şirketlerin internet üzerinden sağladığı hizmet ve uygulamaların artması) güvenlik meselesinin etkin bir çözüme kavuşturulmasını zorunlu kılmaktadır. Güvenlik sağlanırken kişisel özgürlüklerin ve iletişimin engellenmesi istenmeyen bir durum olduğu gibi düşük güvenlik önlemleri nedeniyle mahremiyet ve özgürlüklerin kötü niyetli kişiler tarafından suistimal edilmesi de istenilmemektedir.

Siber tehdit ve saldırıların coğrafi olarak sınırlandırılmaları mümkün olmadığından siber suç işleyen kişi ile siber suçun işlendiği yerler coğrafi olarak ayrılabilir. Bunun sonucunda da suçun faili ile ilgili yapılacak işlemler ve alacağı ceza değişebilmektedir. Bu durum siber suçlar konusunda etkili adımlar atılmasını güçleştirmektedir. Bu nedenle siber suçlara yönelik caydırıcılığın sağlanabilmesi için uluslararası bir işbirliği gerekmektedir. Ancak;

- Siber suçlarla ilgili hangi tipte yapısal düzenlemenin yapılması gerektiği konusunda uzlaşma sağlanamaması,
- Suç oluşturan fiillerin hukuki tanımlamalarının yapılmasında bir bütünlük sağlanamaması,
- Genel anlamda kovuşturma makamlarının bu alandaki tecrübe eksikliği,
- Ulusal düzeydeki usul yasalarındaki kovuşturma hükümlerinin farklılığı sebebiyle siber suçların kovuşturulmasında uyumun sağlanamaması,
- Suçluların iadesi ve karşılıklı yardım anlaşmalarındaki eksiklikler nedeniyle uluslararası işbirliğine izin veren kovuşturma mekanizmalarının uyumlu bir şekilde çalıştırılamaması,
- Devletlerin, egemenlik haklarında uluslararası organizasyonlar lehine tavizde bulunmak istememeleri gibi bazı nedenlerden ötürü siber suçlar konusunda tam bir mutabakat sağlanamamaktadır[70].

Devletler arasında yukarıda belirtilen nedenlerle sağlanamayan işbirliği ve ortak hareketler bazı uluslararası örgütlerin yapmış olduğu düzenlemelerle giderilmeye

çalışılmaktadır. Genel olarak tavsiye niteliği taşıyan bu düzenlemeler ileriki dönemlerde devletler arasında sağlanacak mutabakatlar için sağlam bir zemin teşkil etmektedir. Dünya çapında bu tür örgütler tarafından yapılan düzenlemelere geçmeden önce kısa bir bilgi vermek gerekirse:

- İlk uluslar üstü düzenleme 1970’li yıllarda Avrupa Konseyi (A.K.) tarafından özel hayatın korunması amacıyla elektronik bilgi bankasında işlenen verilere yöneliktir. A.K. tarafından bu konuda alınan iki tavsiye kararı daha sonraları Avrupa ülkeleri tarafından değerlendirilerek kendi hukuk mevzuatlarının içine dahil edilmiştir.
- Kişisel verilerin otomatik işleme tabi tutulmasıyla ilgili olarak bireylerin korunması amacıyla 1981 yılında AK üyesi ülkeler tarafından bir sözleşme imzalanarak yürürlüğe sokulmuştur.
- İlerleyen dönemlerde (değişen siber suç konseptinin etkisiyle) OECD’nin 1986 yılındaki bilişim suçları raporuna dayanarak (ilavelerle) yeni bir düzenleme AK Bakanlar Komitesi tarafından yürürlüğe koyulmuştur. Bu çalışma Avrupa Siber Suç Sözleşmesi için de bir temel teşkil etmektedir.

Tüm bunların ışığında Dünyadaki bazı devletlerin ve uluslararası kuruluşların siber suçlarla ilgili yapmış olduğu düzenlemeler aşağıdaki gibidir.

4.1.1. Avrupa Konseyi tarafından siber suçlara ilişkin yapılan çalışmalar

Yukarıda belirtilen 1986 yılındaki OECD raporuna dayanarak yapılan çalışmalar neticesinde AK tarafından Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesi, Bilişim Sistemleri Aracılığı İle İşlenen Irkçı ve Yabancı Düşmanı Eylemlerinin Suç Haline Getirilmesi için Avrupa Siber Suç Sözleşmesi’ne Ek Protokol ve Avrupa Siber Suç Sözleşmesi adlı siber güvenliği sağlamaya yönelik 3 hukuki düzenleme hayata geçirilmiştir.

Avrupa Siber Suç Sözleşmesi

2004 yılında yürürlüğe giren ve siber suçlarla mücadelede işbirliği adına en önemli sözleşmelerden biri olan Avrupa siber suç sözleşmesi A.K.’nın alt birimlerinden biri olan ASSK (Avrupa Suç Sorunları Komitesi) tarafından hazırlanmıştır. Bir çok

(Arnavutluk, Ermenistan, Bosna Hersek, Bulgaristan, Hırvatistan, Kıbrıs, Danimarka, Estonya, Finlandiya, Fransa, Macaristan, İzlanda, İtalya, Latviya, Litvanya, Hollanda, Norveç, Romanya, Slovakya, Slovenya, Ukrayna, ABD ve Makedonya gibi) devletin onaylayıp iç hukukuna dahil ettiği sözleşme 4 bölümden (birinci bölüm; tanımlamalar, ikinci bölüm; ulusal düzeyde alınacak önlemler, üçüncü bölüm; uluslararası işbirliği ve dördüncü bölüm; diğer hükümlerden) oluşmaktadır. Sözleşmede tanımlanan suç tipleri 4 ana başlık altında toplanmıştır:

- Birinci ana başlık: Bilgisayar veri ve sistemlerinin gizliliği, bütünlüğü ve erişilebilirliğine yönelik suçlar
- İkinci ana başlık: Bilgisayar aracılığı ile işlenen dolandırıcılık ve sahtecilik suçları
- Üçüncü ana başlık: Çocuk pornografisine ilişkin materyale sahip olma ve uluslararası düzeyde dağıtımının sağlanması şeklinde içeriğe ilişkin suçlar
- Dördüncü ana başlık: Fikri mülkiyet haklarının ihlali ve uluslararası düzeyde dağıtımının sağlanması suçlarıdır.

Sözleşme bir ilk olmasının da verdiği nedenlerden ötürü çeşitli eleştirilere maruz kalmıştır:

- Kamu otoritesi bireysel özgürlüklerin üzerinde kalarak temel hak ve özgürlükler sınırlandırılmıştır.
- Siber suçun varlığı için bilgisayarın varlığının aranması ve bazı (ikinci ve onuncu gibi) maddelerinde siber ortam tanımlamalarının eksik yapılması, günümüzde ve ileri dönemlerde gelişecek teknoloji ile ortaya çıkacak bilişim cihazlarına yönelik suçları kapsamaması çok büyük bir eksikliktir.
- Sivil Toplum Kuruluşlarının görüş ve önerilerinden yararlanılmamıştır.
- Servis sağlayıcılara ağır mali yükümlükler getirmektedir[1].

Bilişim Sistemleri Aracılığı İle İşlenen Irkçı ve Yabancı Düşmanı Eylemlerinin Suç Haline Getirilmesi için Avrupa Siber Suç Sözleşmesi'ne Ek Protokol

AB üyesi ülkelerde giderek artan yabancı düşmanlığı ve ırkçılık nedeniyle hazırlanarak 2006 yılında yürürlüğe giren protokol birçok (Arnavutluk, Bosna Hersek, Hırvatistan, Danimarka, Estonya, Finlandiya, Fransa, Kıbrıs, Latviya,

Litvanya, Norveç, Slovenya, Ukrayna ve Makedonya) devlet tarafından onaylanıp iç hukuklarına dahil edilmiştir. İlk bölümünde genel hükümler, ikinci bölümünde ulusal düzeyde alınabilecek tedbirler, üçüncü bölümünde sözleşme ve protokol arasındaki ilişkiler ve son bölümde de son hükümlerin bulunduğu protokolle Avrupa Siber Suç Sözleşmesinin yabancı düşmanlığı ve ırkçılık propagandasını içerecek şekilde genişletilmesinin amaçlanması yanında uluslararası işbirliğinin güçlendirilmesinin de hedeflendiği görülmektedir.

Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesi

2005 yılında imzaya açılarak 2007 yılında yürürlüğe giren Avrupa Konseyi Terörizmin Önlenmesi Sözleşmesi ile birlikte internet üzerinden terör suçlarının işlenmesine tahrik, terör amaçlı eleman toplama ve terörizm amaçlı ideolojik ve askeri eğitimin verilmesi suçları için ülkelerin yapacakları düzenlemelere yönelik bir zemin hazırlanmıştır. Ülkemiz tarafından da imzalanan sözleşme ile yayın ve propaganda suçlarına yönelik yaptırımlar getirilmiştir[99].

4.1.2. Birleşmiş Milletler tarafından siber suçlara ilişkin yapılan çalışmalar

Milletlerarası barış ve güvenliği sağlamak ve insan hak ve hürriyetlerine saygının geliştirilip teşvik edilmesi konusunda milletlerarası işbirliğini sağlamak gibi amaçlar altında kurulan Birleşmiş Milletler; bilgisayar sistemlerine yetkisiz giriş, bilgisayar veya bilgisayar sistemlerinin hukuka uygun olarak kullanılmasına engel olunması, bilgisayar sistemleri içerisindeki verilerin yok edilmesi veya değiştirilmesi, kamu-özel sektör arasında işbirliğinin sağlanması, küresel siber güvenlik kültürünün oluşturulması ve kritik bilgi alt yapılarının korunması gibi siber güvenliğe ilişkin (BM genel kurulu tarafından alınan) kararlar bulunmaktadır[100]. Bu kararlar şunlardır:

- 4 Aralık 2000 tarihli ve 56/63 sayılı karar
- 19 Aralık 2001 tarihli ve 56/121 sayılı karar
- 20 Aralık 2002 tarihli ve 57/239 sayılı karar
- 23 Aralık 2003 tarihli ve 58/199 sayılı karar

4.1.3. ABD tarafından siber suçlara ilişkin yapılan çalışmalar

FBI National Infrastructure Protection Center, Information Technology Association of America, Trap and Trace Center Authority ile Carnegie Mellon's Emergency Response Team gibi pek çok kurum ve kuruluşa ait özel birimlerin bulunduğu ABD'de ayrıca bizzat CIA tarafından bin kişilik personele sahip 24 saat hizmet veren "Information Warfare Center" adlı birim bulunmaktadır. Adalet bakanlığı bünyesinde "Computer Crime and Intellectual Property Section" adlı birim ise siber suçlarla ilgili eğitim vermenin yanında diğer birimlere de destek vermektedir[71].

Hem internetin ilk bulunduğu ve geliştirildiği yer olması hem de bilgisayarın bulunduğu ve bilgisayarla ilgili birçok önemli araştırmanın yapıldığı ülke olması nedeniyle ABD, siber suçlara karşı mücadeleyi başlatan ilk yerlerden biri konumundadır. Bu suçlara karşı her eyaletin kendine has kanunları olduğu gibi tüm ülkeyi kapsayan kanunlarda bulunmaktadır. Bu kanunların bazılarında aşağıda kısaca bahsedilmektedir:

Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Yasası (Computer Fraud and Abuse Act)

Siber eylemleri engellemek amacıyla 1984 yılında kabul edilen yasanın zaman içerisinde yetersiz kalması nedeniyle değişiklikler yapıp kapsamı da genişletilmiştir. Korumalı bir bilgisayara izinsiz ve yetkisiz bir erişimi yasaklayan kanunla:

- ABD hükümetine zarar vermek veya herhangi bir yabancı ülkeye yarar sağlamak maksadıyla, tasnif edilmiş ve gizlilik dereceli savunma ve dış işleri konularına ilişkin enformasyona izinsiz olarak erişmek,
- Finansal bir kurum veya tüketici araştırma ajanslarından herhangi birinin bilgisayarlarındaki finansal kayıtlara izinsiz ve yetkisiz olarak erişmek,
- Kamu kuruluşlarından herhangi birinin kullandığı bir bilgisayara girerek, bu kuruluşların verdiği hizmeti aksatacak şekilde, burada bulunan bilgileri değiştirmek, bozmak veya ifşa etmek,
- Herhangi bir bilgisayara sahtekarlık veya hırsızlık yapmak maksadıyla izinsiz ve yetkisiz olarak girmek,

- Herhangi bir şekilde kasten veya ihmalen, korumalı bir bilgisayara erişmek, bu tip bir bilgisayara data veya program göndermek,
- Bilgisayar şifrelerini veya bilgisayarlara erişmekte kullanılabilecek herhangi bir bilgiyi dağıtmak, başkalarının kullanımına sunmak,
- Para veya para hükmünde olan herhangi bir değeri elde etmek maksadıyla, bir bilgisayar veya bilgisayar sistemine zarar verme yönünde tehditler savurmak şeklinde tarif edilen bazı eylemler suç kapsamına alınmıştır[92].

Anti-Terörizm Yasası (USA Patriot – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)

2001 yılında Dünya Ticaret Merkezi'ne yapılan saldırı sonrası internet servis sağlayıcılara eskiye nazaran daha ağır yükümlülükler getirilerek ulusal güvenliğin söz konusu olduğu durumlarda hakim kararına gerek kalmaksızın denetlenebileceğine hükmedilmiştir.

Bu yasa ile siber suç kavramı genişletilerek herhangi bir noktaya yapılan saldırıyla ilgili veri paketlerinin ABD'de bulunan bir ağ üzerinden geçmesi durumunda ABD'nin ilgili makamları bu siber suçla ilgili gerekli çalışmaları yapabilmektedir. Bu yasa ile "Bilgisayar sahtekârlığı ve bilgisayarların kötüye kullanılması" yasasında;

- Ceza miktarlarının arttırılması
- ABD sınırları dışında gerçekleştirilen saldırılar sonucunda ABD ticaretine zarar verilmesi durumları da kapsama dahil edilmiştir.
- "Bilgisayar sahtekârlığı ve bilgisayarların kötüye kullanılması" yasasında belirtilen suçlara teşebbüs edenlerin yapanlar gibi cezalandırılacaklarının belirtilmesi
- Daha önceden bu tür suçlarla ilgili haklarında (eyalet mahkemelerince verilmiş) mahkûmiyet kararı bulunanların sonradan federal düzeyde işleyecekleri suçlarda cezalarının arttırılacağı şeklinde bir takım değişiklikler olmuştur[70].

İletişim Ahlakı Yasası (Communications Decency Act)

İnternet üzerinden müstehcen içeriğe sahip resim, yazı v.b. materyallerin yayınlanmasının suç olarak düzenlendiği yasa ile yetkili makamlara kullanıcıların e-

posta mesajlarının okunabilmesi ve haber gruplarındaki tartışmaları izleyebilme imkânı verilmiştir. Bu tür anti demokratik uygulama niteliğindeki hükümler (American Civil Liberties Union (ACLU- Amerikan Sivil Özgürlükler Birliği) önderliğinde) sivil toplum örgütleri tarafından tepkiyle karşılanarak açılan davalar sonucunda Amerikan Federal Yüksek Mahkemesi'nin özgür fikir alış verişinin sağlayacağı yararın internette sansürün sağlayabileceği yarardan çok daha önemli olduğu gerekçesiyle iptal edilmiştir[93].

Çocuk Pornografisinin Önlenmesi Yasası (Child Pornography Prevention Act)

İlgili yasa ile çocukların bulunduğu pornografik yayın ve materyallerin elde bulundurulması, internet ortamında yayınlanması ve bilgisayarlar ya da e-posta yoluyla ticaret malzemesi olarak kullanılması yasaklanmış, bu tür suç teşkil eden görüntülerden üç veya daha fazlasını bilgisayarında kasıtlı olarak bulunduranların cezalandırılması sağlanmıştır[94].

Yukarıda belirtilen yasalara ilaveten “Çocukların Online Yayınlardan Korunması Yasası (COPA-Child Online Prevention Act)”, “Elektronik Haberleşmenin Gizliliği Yasası (ECPA-Electronic Communications Privacy Act)” ve “İnternette Kumarın Önlenmesi Yasası (Internet Gambling Prohibition Act)” gibi yasalarla da düzenlemeler yapılarak kullanıcıların korunmasına yönelik tedbirler alındığı görülmektedir.

4.1.4. Fransa tarafından siber suçlara ilişkin yapılan çalışmalar

Önceleri siber suçlarla ilgili düzenlemelerin yapılmadığı ülkede bu tür suçlar için Fransız Ceza Kanunu'ndaki hırsızlık, inancı kötüye kullanma ve dolandırıcılık gibi suçlarla ilgili hükümler kullanılmaktaydı. Teknolojik gelişmelerin de etkisiyle zamanla gizliliğin korunması ve telif hakkının korunmasına ilişkin kanunlar hazırlansa da siber suçlarla ilgili ilk kapsamlı düzenleme 1988 yılında yapılan “relative a la fraude informatique” isimli kanunla yapılmıştır. Kanun genel olarak:

- Hukuk dışı bir bilgisayara girilmesi veya sistemde hukuk dışı kalınması,
- Sistemdeki verilerin tahribi, değiştirilmesi veya yok edilmesi yahut başka veriler yüklenmesi,
- Sistemin işleyişinin engellenmesi veya bozulması,

- Bilgisayar belgelerinde sahtekârlık yapılması,
- Bu tür bir belgenin bilerek kullanımı

olmak üzere beş bilişim suçunu öngörmüştür. Zaman içerisinde siber suçlara ilişkin düzenlemeler yapılarak yeni suç tiplerinin oluşturulduğu ülkede ülkemiz düzenlemesine örnek oluşturan “Bilgileri Otomatik İşleme Tabi Tutan Sistemlere Karşı Saldırıları” başlığı altında bilişim sistemine tamamen veya kısmen izinsiz ve yetkisiz erişim düzenlenerek bu erişim sonucunda meydana gelebilecek verilerin silinmesi, değiştirilmesi şeklindeki işlemler ağırlaştırıcı etkenler olarak öngörülmüştür. İlerleyen dönemlerde ayrıca mevzuatta şifreleme sistemine ilişkin değişikliklerle birlikte elektronik imzanın hukuki değer taşımasına ilişkin bir kanunda düzenlenmiştir[71].

4.1.5. İngiltere tarafından siber suçlara ilişkin yapılan çalışmalar

Anglo hukuk sistemine uygun olacak şekilde düzenlemelerin yapıldığı ülkede siber suçlarla ilgili 1990 yılında yürürlüğe giren “Computer Misuse Act” adlı kanun bulunmaktadır. Bu kanunla:

- Yetkisiz olarak bilişim cihazlarına, veri ve programlarına girilmesi,
- Başka bir suçun işlenmesini sağlamak veya kolaylaştırmak amacıyla yetkisiz olarak bilişim cihazına girilmesi,
- Yetkisiz olarak bir bilgisayarın içerisinde değişikliğe neden olunması şeklinde belirlenen 3 tür suç tipi bulunmaktadır[100].

Ülke de internet hizmeti sunan servisler kurmuş oldukları “Birleşik Krallık İnternet Servis Sağlayıcıları Derneği” (ISPA-UK - Internet Service Providers Association of United Kingdom) adlı bir örgüt çatısı altında bir araya gelerek kendi koymuş oldukları kuralların sağlıklı işleyip işlemediğini yine kendi koydukları kontrol mekanizmaları ile denetlemektedirler.

4.1.6. Japonya tarafından siber suçlara ilişkin yapılan çalışmalar

Gelişmiş teknolojisi nedeniyle siber suçlarla erken tanışan Japonya, siber suçlarla ilgili ilk yasal tedbirler alan ülkelerdendir. Ceza Kanununa 1987 yılında bilişim suçları ile ilgili maddelerin eklendiği ülkede 2000 yılında “İnternete Haksız

Girmenin Yasaklanması Hakkındaki Kanun” yürürlüğe sokulmuştur. Bilgisayar dolandırıcılığı ile ilgili olarak Alman Ceza Kanunu ile benzerlikler taşıyan yasal düzenlemelere sahip ülkede bir bilgisayar sistemine izinsiz giriş yapmak (giriş ile elde edilen bilgiler bir başkasına satılmadıkça yahut zarar verilmedikçe) suç olarak değerlendirilmemektedir[106].

4.2. Ülkemizde Siber Suçlara ilişkin Yapılan Çalışmalar

Ülkemizde siber suçların 1991 yılında 3756 sayılı kanunla “bilgişim alanında suçlar” adı altında 525/a, 525/b, 525/c ve 525/d maddelerinden oluşan bir babın 765 sayılı Türk Ceza Kanunu(TCK)’na eklenmesiyle yasal boyut kazanmaya başladığı görülmektedir. Başlangıçta internet ve bilgişim sistemlerinin yaygın kullanılmamasından dolayı bu maddeler yabancı gelse de zaman içerisinde siber suçların hukuk sistemimizin önemli bir konusu haline geldiği gözlenmektedir.

5237 sayılı TCK’nın 243, 244, 245, 246. maddelerini kapsayan “bilgişim alanında suçlar” ve 135, 136 ve 138. maddelerini kapsayan “özel hayata ve hayatın gizli alanına karşı suçlar” bölümleri içerisinde yer alan siber (bilgişim) suçlarının (aynı zamanda teknolojinin gelişmesiyle birlikte ortaya çıkan yeni suç tipleri nedeniyle) kesin bir ayrımının yapılamaması sonucunda TCK’nın farklı bölümlerinde de yer aldığı görülmektedir. Ayrıca;

- TCK Madde 243’e göre bilgişim sistemine yönelik herhangi bir zarar veya veri ihlali söz konusu olmasa dahi bir bilgişim sistemine izinsiz ve yetkisiz bir şekilde yapılan erişimin (bilgişim sisteminin güvenliğinin ihlal edilmesi ve kullanıcıların menfaatlerinin korunabilmesi sebebiyle) suç teşkil ettiği,
- Bilgişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme ile bilgişim sistemi ile hukuka aykırı yarar sağlama suçunun ele alındığı TCK Madde 244 ile bilgişim sistemlerine ait donanım, yazılımlar ve verilerle birlikte bilgişim sistemi kullanıcılarının da koruma altına alındığı,
- Banka ve kredi kartlarının hukuka aykırı bir şekilde kullanılarak banka ve kredi kartı sahiplerinin zarara uğratılmasını ve bu yolla herhangi bir menfaat elde edilmesini engellemek için TCK Madde 245’in farklı bir suç tipi olarak tanımlandığı,

- Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenen dolandırıcılık suçunun Madde 158/1-f'de (nitelikli dolandırıcılık), bilişim sistemlerinin kullanılması suretiyle işlenen hırsızlık suçunun Madde 142/2-e'de (nitelikli hırsızlık) ve çocukların kullanıldığı müstehcen görüntü, yazı veya sözlere ilişkin suçların da Madde 226/5' te (müstehcenlik) düzenlendiği görülmektedir.

Madde 246 ile 243, 244 ve 245. maddelerde belirtilen suçlarla ilgili tüzel kişilere yönelik güvenlik tedbirleri düzenlenmesi yoluyla tüzel kişilerin menfaat elde etmeleri önlenerek suç işlenmesinde odak noktası olmamaları amaçlanmıştır. Ayrıca TCK madde 135 ile kişinin özel hayatını güvence altına almak için gerçek kişilerle ilgili her türlü verinin kaydedilmesini engelleme ve 136. madde ile de bu kişisel verileri hukuka aykırı bir şekilde (özellikle internet üzerinden) yaymayı ve ele geçirmeyi engelleme amaçlanmaktadır. Sadece kimlik numarası kullanılarak birçok özel işlemin yapılabildiği durumlar göz önüne alındığında bu maddelerin önemi daha iyi anlaşılacaktır. 138. madde de ise özellikle kişisel veri bulunduran kamu ve özel kurumlar ele alınarak bu verileri zamanında yok etmeleri hedeflenmektedir[5].

4.2.1. İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun (5651)

İçerik ve erişim sağlayıcı gibi internet servislerinin sorumluluklarını düzenlemek ve bu servislerin denetlenerek internet üzerinden zararlı içeriklerin yayılmasını engellemek amacıyla düzenlenen bu kanunla birlikte web üzerinden işlenen siber suçların önüne geçilmesi ve bir siber suç olayı sonrasında sorumluların daha kolay tespit edilmesi hedeflenmektedir. Kanuna göre erişimin engellenmesi kararı, hakim (soruşturma evresi), (soruşturma evresinde gecikmesinde sakınca bulunan hallerde) savcı ve (kovuşturma evresinde) mahkeme gibi adli makamların yanısıra içeriği çocukların cinsel istismarı ve müstehcenlik suçları oluşturan yayınlarda TİB tarafından da verilebilmektedir.[27]

4.2.2 Fikir ve Sanat Eserleri Kanunu (5846)

Bu kanunun fikri eser kapsamında değerlendirilen bilgisayar programları üzerindeki maddi ve manevi hakların kasten ihlalini engellemeyi öngördüğü anlaşılmaktadır.

4.2.3 Elektronik İmza Kanunu (5070)

Bir verinin, bütünlüğünün bozulmadan ve tarafların kimliklerinin doğrulanarak iletildiğinin elektronik veya benzeri araçlarla garanti edildiğini gösteren elektronik imzanın hukuki yapısı ile elektronik imzanın kullanımına ilişkin temel hususların bu kanunla düzenlendiği anlaşılmaktadır.

Yukarıda sayılan düzenlemelerin dışında:

- “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik”,
- “İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik”, “İnternet ortamında yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik”
- “Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik “ gibi düzenlemelerle de internet ortamında işlenen suçların engellenmesine yönelik ilave tedbirler alınmıştır[34].

Gelişen teknoloji ve internet kullanımının artmasıyla dinamik bir yapı kazanan siber suçlarla ilgili yapılan düzenlemelerin günün şartlarına bağlı olarak sürekli güncellenmesi ve hukuka aykırı eylem olarak kayıt altına alınması gerektiği anlaşılmaktadır. Bu bağlamda siber suçlarla ilgili tanımlamaların net olarak ortaya konulması, yanlış anlaşılmalara önlenmesi ve internet ortamında işlenen bu suçların takibinin ve cezalandırılması önem kazanmaktadır.

5. SİBER GÜVENLİĞE İLİŞKİN ARAŞTIRMA VERİLERİNİN İNCELENMESİ VE DEĞERLENDİRİLMESİ

5.1. Siber Tehdit ve Saldırıların İncelenmesi

Siber tehdit ve saldırılarla ilgili olarak 2013 yılında yaşanan önemli değişiklikler bulunmaktadır. ENISA, 250' nin üzerinde kaynak ve raporu analiz etmesi neticesinde olumlu ve olumsuz bir takım sonuçlar elde etmiştir. Elde edilen olumsuz gelişmeler:

- Siber tehdit ve saldırılar ile bu tehdit ve saldırılarda kullanılan araçların karmaşıklığının artması
- Siber güvenliği ihlal eden olayların, birkaç devletin meselesi olmaktan çıkarak çok sayıda devletin ve bu devletlerin kamu ve özel kurumlarına yönelik saldırılar haline dönüşmesi
- Siber tehdit ve saldırıların mobil platformlara doğru kayması
- Bu tehdit ve saldırıların *big data* ve *nesnelerin interneti* adlı iki yeni alanda yoğun şekilde yer almasıdır.

Analiz neticesinde ortaya çıkan olumlu gelişmeler:

- Siber tehdit ve saldırılarla ilgili rapor ve verilerin artması neticesinde bu tehdit ve saldırılarla ilgili bilgilerin kalitesinin artarak tehdit analizini kolaylaştırması
- Siber güvenliği sağlamaya yönelik sunulan mevcut ürünlerdeki güncellemeler sayesinde siber tehdit ve güvenlik açıklıklarına karşı verilen tepkinin daha hızlı hale gelmesidir[65].

Bu olumlu ve olumsuz gelişmeler neticesinde dünya çapında yaşanan siber tehdit ve saldırılarla ilgili 2012 ve 2013 yıllarında yaşanan gelişmeler Çizelge 5.1' de gösterilmektedir.

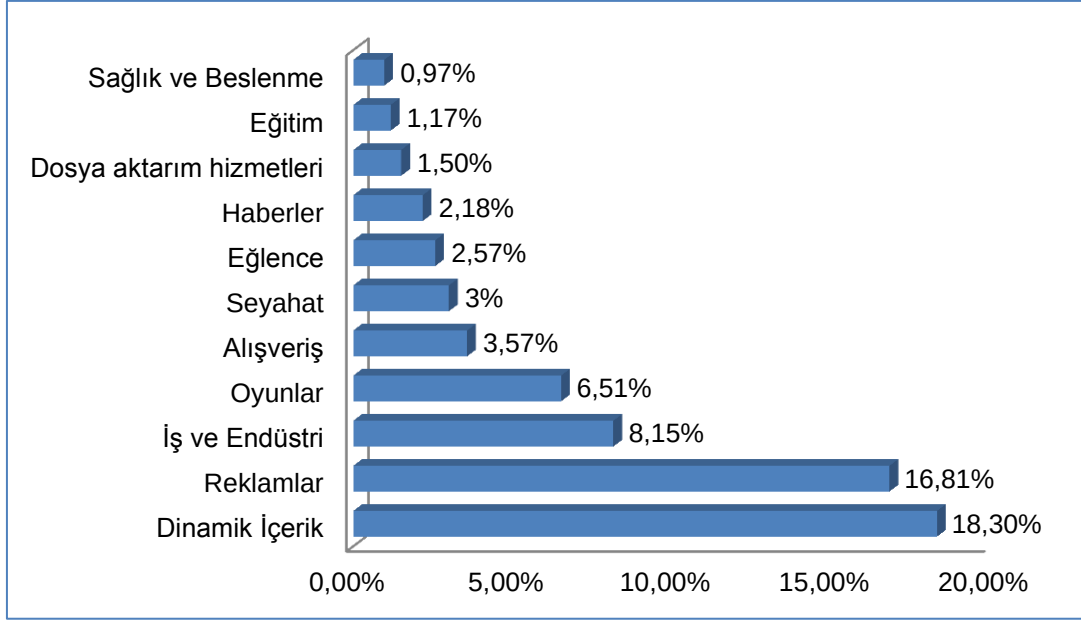
2012 yılında sahte antivirüs yazılımları, phishing (sazan avlama) ve hizmet aksattırma saldırılarında herhangi ciddi bir değişim görülmezken (spam sayısındaki düşüş haricinde) diğer siber tehdit ve saldırılarda artışlar kaydedilmiştir. 2013 yılında ise (spam ve botnet dışında) siber tehdit ve saldırı

sayısında artmalar görülmesine karşın tehdit sıralamasında her iki yılda da zirveyi izinsiz indirmeler ve (özellikle solucan/truva atı gibi) kötücül yazılımlar paylaşmıştır(Çizelge 5.1). Yukarıdaki veriler ışığında siber tehdit ve saldırılarda yaşanan gelişmeler aşağıda maddeler halinde belirtilmektedir.

Çizelge 5.1. 2012-2013 yılları arasında siber tehdit ve saldırıların durumu ve sıralaması[65]

	TEHDİT DURUMU		TEHDİT SIRALAMASI	
	2012	2013	2012	2013
İzinsiz indirmeler	↑	↑	1	1
Kod enjeksiyonu	↑	↑	3	3
Solucan / Trojan	↑	↑	2	2
Exploit kit	↑	↑	4	4
Sahte antivirüs yazılımları	→	↑	9	11
Spam	↓	→	10	10
Botnet	↑	→	5	5
Kimlik hırsızlığı	↑	↑	13	7
Phishing	→	↑	7	9
Fiziksel zarar verme ve hırsızlık (ve Kayıp)	↑	↑	12	6
Veri ihlalleri	↑	↑	8	12
Bilgi sızıntısı	↑	↑	14	13
Hizmet Aksattırma	→	↑	6	8

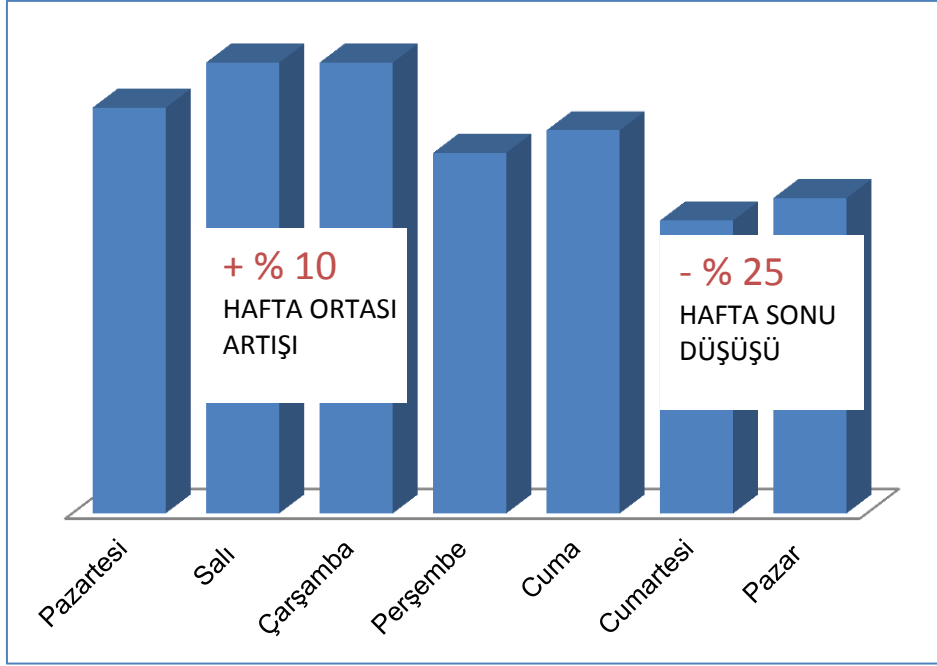
(Artan) ↑ (Durağan) → (Azalan) ↓



Şekil 5.1. Kategorilerine göre internet sitelerinin kötü amaçlı içerik bulaştırma durumları[8]

a) Kötücül yazılımların çoğunlukla sahte web sitelerinden kaynaklandığına inanılsa da aslında bu tür tehditler genellikle kullanıcıların en çok ziyaret ettiği ve güvenli olduğunu düşündüğü sitelerde barınmaktadır. Bu bağlamda Şekil 5.1’de görüldüğü üzere dinamik içeriğe sahip CDN (Content Delivery Network- web sitelerinin statik içeriklerinin normalden daha hızlı tarayıcıya ulaştırılmasını sağlayan yapıdaki) internet siteleri % 18.30 ile ilk sırada yer alırken internet sitelerinden para kazanmanın genel bir yolu olan (dolayısıyla kötücül içeriğe sahip tek bir reklamın neden olacağı büyük bir etkinin söz konusu olduğu) çevrimiçi (online) reklamlar % 16.81 ile ikinci sırada yer almaktadır.

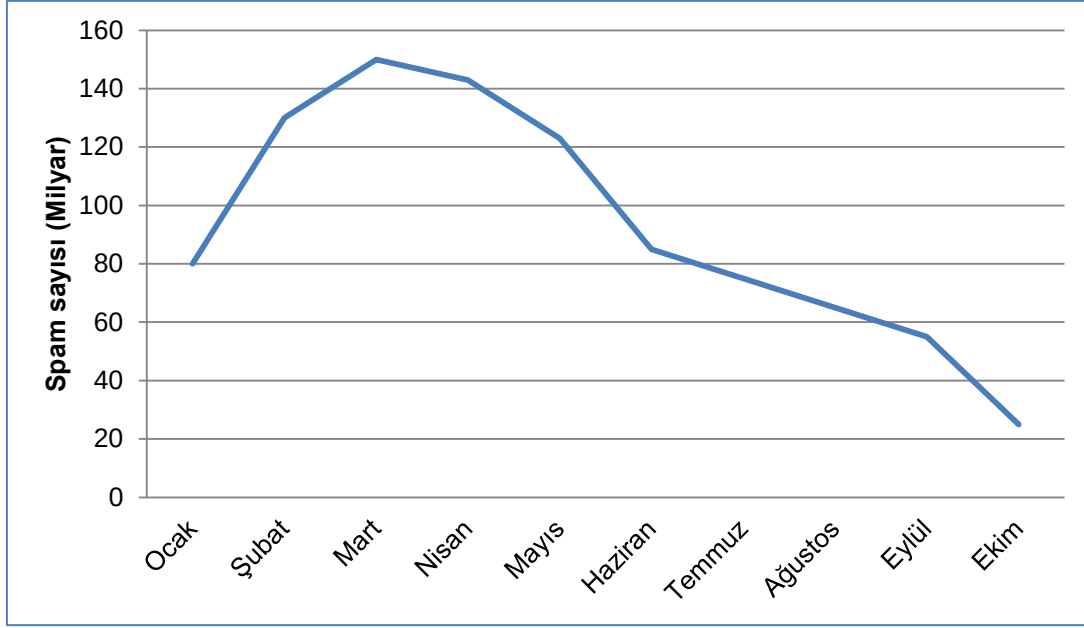
Çevrimiçi alışveriş sitelerinin de kötücül yazılım bulaştıran sahte sitelerden (bu tür tehditleri bulaştırma da) 21 kat daha etkili olabildiği göz önüne alınırsa internet ortamından gelebilecek bu tür tehditlere karşı güvenlik yaklaşımlarının tekrar gözden geçirilerek gerekli önlemlerin alınması gerektiği ortaya çıkmaktadır[8]. Websense 2013 tehdit raporuna göre 2012 yılına oranla zararlı yazılıma sahip sitelerin % 600 oranında artış gösterdiği kaydedilmektedir[79].



Şekil 5.2. Spam hacimleri

b) Şekil 5.2’de görüldüğü üzere hafta içi özellikle kurumsal bazda kullanıcı sayısındaki artışa paralel olarak artan spam sayısı, hafta sonu tatilinde kullanıcı sayısındaki düşüşün de etkisiyle belirli oranda düşmektedir. Bu durum spam üreticilerinin mesai günlerinde daha fazla kullanıcıya erişmek istediklerinin ve kurumsal siber güvenliğe yöneldiklerinin bir göstergesidir. Cisco 2013 güvenlik raporuna göre 2011 yılı ile 2012 yılı arasında dünya spam üretiminde % 18’lik bir düşüş yaşanarak spam üretiminde üst konuma Hindistan (birinci) ve ABD (ikinci) yerleşmiştir[8].2013 yılının ilk aylarında görülen spam artışının ise yılın sonuna doğru giderek azaldığı görülmektedir(Şekil 5.3).

c) Botnetler en eski siber tehditlerden biri olmalarına karşın günümüzde önemli değişikliklere uğramışlardır. Kötücül yazılımların yayılmasında kullanılmasıyla birlikte mevcut olan botnet yapısı 2013 yılı mayıs ayında en yüksek artışa ulaşırken[102] aynı yıl içinde Hindistan’ın ilk sıraya yerleştiği belirtilmektedir[101].



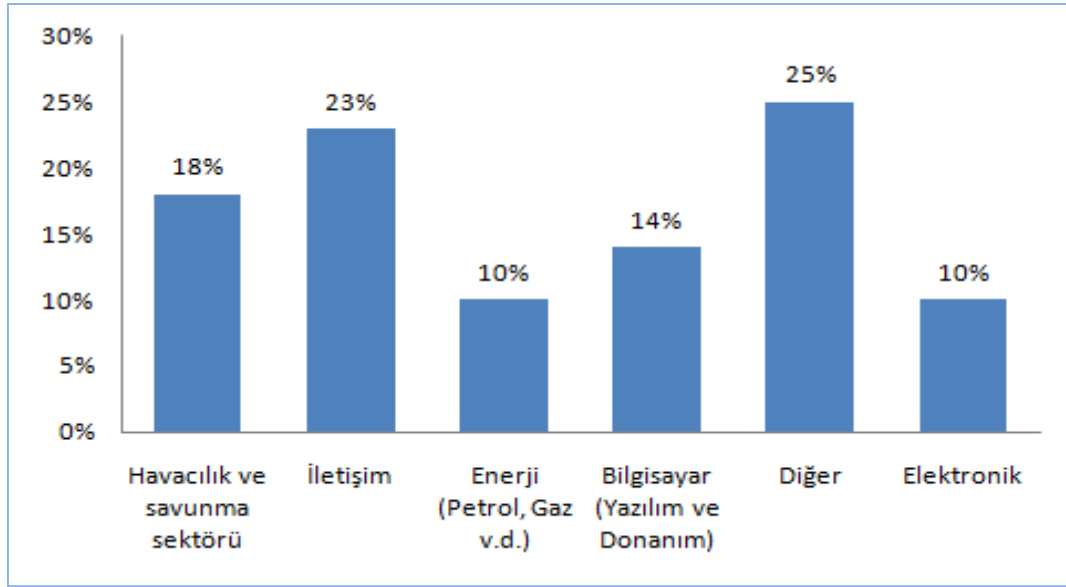
Şekil 5.3. 2013 yılı dünya geneli spam hacmi[89]

d) Son zamanlarda facebook, twitter gibi sosyal ağlar (vasıtasıyla elde edilen kişisel bilgiler kimlik hırsızlığında kullanılabildiği için) sazan avcılarının hedefindedir. Uzmanlar sosyal ağlardaki phishing ataklarının başarı oranının %70'in üzerinde olduğunu ifade etmektedirler[61].

e) Veri ihlalinden kaynaklanan maliyetlerde kötücül yazılımlar ilk sırada yer alırken sistem hataları ve insan faktörü ikinci ve üçüncü sırada yer almaktadır. Ayrıca (70 – 80 milyon kadar cihazın çalındığı, kaybolduğu veya fiziksel olarak zarar uğradığının tespit edildiği 2013 yılında elde edilen verilere göre) veri ihlallerinin % 36'sının cihazların kaybolması ve çalınması neticesinde gerçekleştiği sonucuna varılmıştır[65]. Veri ihlalleriyle ilgili yapılan bir araştırmada (ilginç bir şekilde) veri sızmalarına dışsal etkenlerin neden olduğu görülmektedir. Ancak yine de personel dolayısıyla oluşan sızmaların % 20 civarında olması bunun da % 32'sinin iş ortakları nedeniyle olması dikkate değerdir[66].

f) Siber saldırılar, önceleri teknik düzeyi düşük uygulamalar ve uzmanlık derecesi yüksek siber saldırganlar tarafından gerçekleştirilirken günümüze kadar olan süreç içerisinde saldırı için kullanılan araçların teknik düzeyi artarken (ters orantılı olarak) siber saldırganların uzmanlık düzeyinin düştüğü görülmektedir.

g) Şu ana kadar olan siber savaşlarda genelde DDoS (Distributed Denial of Service) saldırıların yapıldığı ve çok karmaşık silahların kullanılmadığı görülmektedir. Devletler tarafından geliştirilen siber silahlar tespit edildikten sonra etkisini yitirmesi dolayısıyla tek kullanımlık olduğundan birçok ülke zorunlu olmadıkça APT türü silahları kullanmayı tercih etmemektedirler. APT tespiti için her şeyden önce bilinen siber savunma yöntemleri veya ürünlerini kullanmaktan ziyade yeni yaklaşımlar geliştirilmesi gerekmektedir. Bu noktada kullanabilecek yöntemler olarak sızma testleri (APT tespit simülasyonu), ağ güvenliğine ilişkin yöntemler (IDS/IPS, Ağ izleme, NAC...), log yönetimi, adli bilişim ve malware (kötücül yazılım) analizi yöntemleri sayılabilir. Fakat piyasada APT tespitine yönelik Mandiant, FireEye, Damballa, Deep Discovery, Bit9 ve PaloAlto Wildfire gibi ticari ürünler de bulunmaktadır[3].



Şekil 5.4. Günümüzde kullanılan APT' lerin hedef seçtiği sektörler[3]

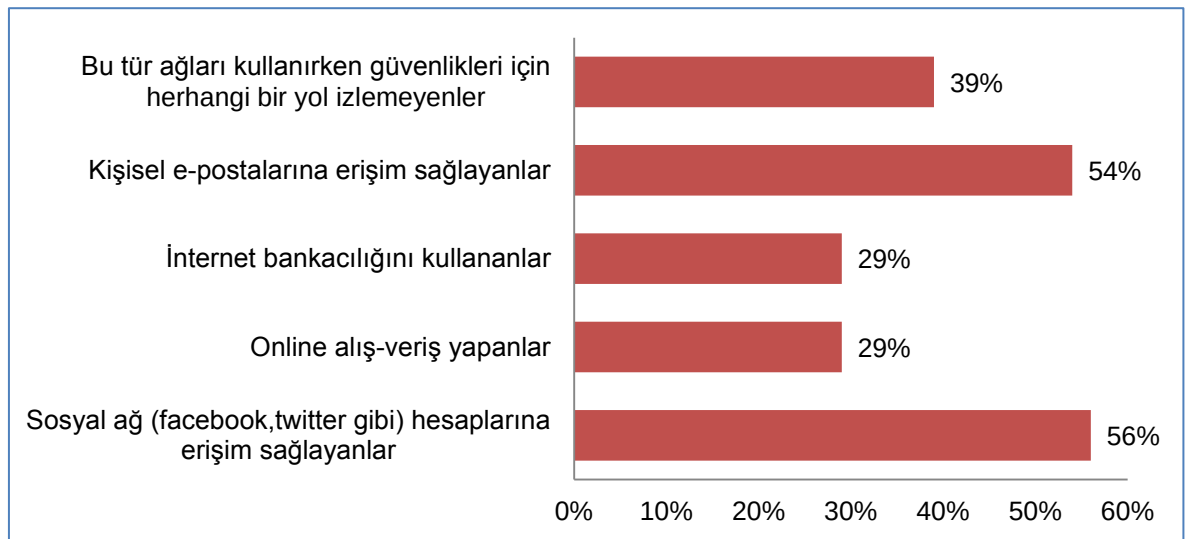
h) Stuxnet ,Duqu ,Flame, Gaussen bilinen siber saldırı (ATP) örnekleridir. Bu APT' lerin bazı ortak özellikleri göze çarpmaktadır[69]:

- ABD açıklık veritabanında bulunan “.lnk” isimli aynı açıklığı kullanmaktalar.
- USB bulaşma, metin kodlama/çözme algoritması gibi pek çok ortak modülü paylaşmaktalar.
- Aynı platformda geliştirilmişlerdir.

- Aynı tesislerde bir ya da birden fazla devlet desteğiyle üretildiği anlaşılmaktadır.

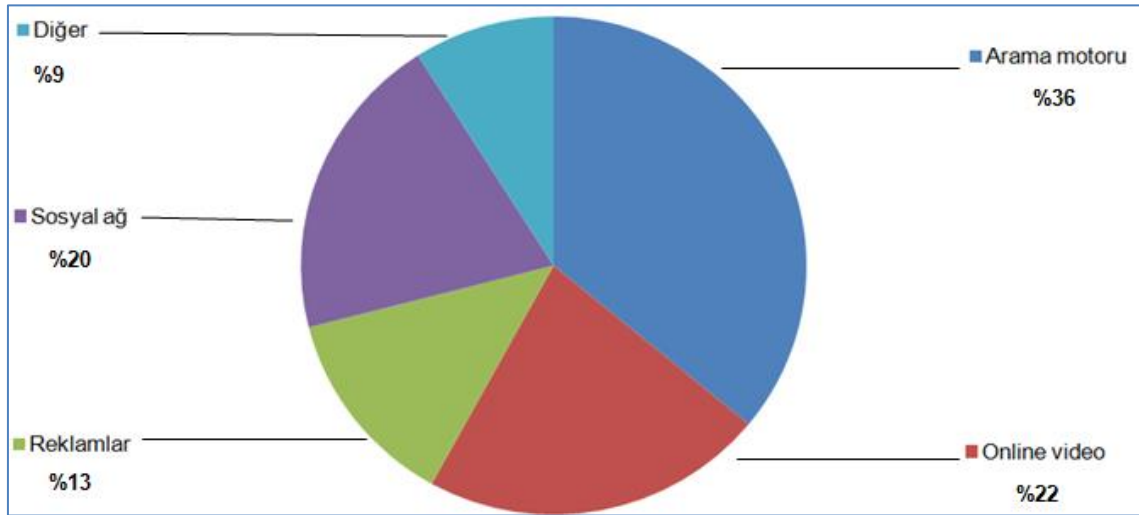
5.1.1. Siber tehdit ve saldırıların kurumsal siber güvenlik yönünden incelenmesi

Norton (2013) tehdit raporunda da belirtildiği üzere kullanıcıların % 34'ünün iş yerinde kullandıkları cihazlarla sosyal ağlara erişim sağladıkları, % 27'sinin bu cihazlarda kişisel verilerini sakladıkları ve % 49'unun da yine bu cihazlar üzerinden kişisel e-postalarını gönderip aldıkları görülmektedir. Tüm bunlarla birlikte kullanıcıların %24'ünün çevrimiçi (online) dosya depolama hesaplarında hem iş hem de kişisel verilerini saklamaları ve % 36'sının da iş için kişisel cihazlarını kullanmaları hususunda çalıştıkları kurumlarının herhangi bir politikasının olmadığını beyan etmeleri gibi veriler de kurumsal siber güvenlik konusunda kurumların yeterince farkındalık taşımadıklarını göstermektedir. Yine aynı raporda görüldüğü üzere kullanıcıların (halka açık ve güvensiz ağları kullanarak) % 56'sının sosyal ağ (facebook, twitter gibi) hesaplarına erişim sağladığı, %29'unun çevrimiçi (online) alışveriş yaptığı, %29'unun internet bankacılığını kullandığı ve % 54'ünün kişisel e-postalarına erişim sağladıkları ve % 39'unun da bu tür ağları kullanırken güvenlikleri için herhangi bir yol izlemedikleri ifade edilmektedir(Şekil 5.5).



Şekil 5.5. Kullanıcılar tarafından halka açık ve güvensiz ağların kullanılma durumları[29]

Sosyal medya kullanıcılarının % 31'inin bildikleri kişilerle irtibata geçerken %25'inin de sosyal ağ hesaplarının şifrelerini başkalarıyla paylaştıklarının belirtilmesi (yukarıda da belirtildiği üzere) kurum çalışanlarının birçoğunun saldırganlara açık davetiye çıkarmaya hazır olduklarını göstermektedir. Ek olarak, mobil cihazların (akıllı telefon, tablet v.b.) eğlence ve iş amaçlı olarak yoğun kullanılmalarına rağmen kullanıcılarının bu cihazların güvenliği konusunda dikkatsiz davranmaları (kullanıcıların % 57'sinin mobil cihazlar için uygulanabilecek güvenlik çözümlerinden haberdar bile olmaması) hatta akıllı telefon ve tablet kullananların yaklaşık %50'sinin şifre kullanmak veya güvenlik yazılımına sahip olmak gibi basit önlemleri almaması ve bunun sonucunda da saldırganlar tarafından açık bir hedef haline gelmeleriyle çalıştıkları kurumlar içinde yeni güvenlik sorunlarına neden olabilmeleri kurumsal siber güvenlikle ilgili alınması gereken önlemlere yol gösterecek niteliktedir[29].



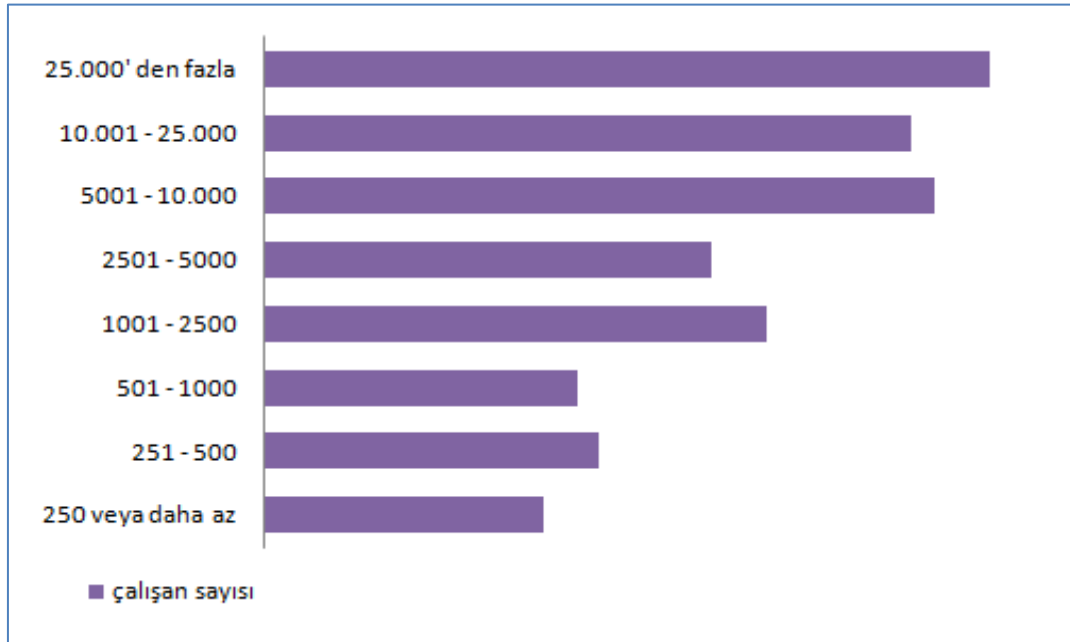
Şekil 5.6. Ziyaret sayılarına göre popüler uygulamalar[8]

Yukarıdaki verilere ilaveten sosyal mühendislik yöntemi, kurumsal siber güvenliğe yönelik etkilerinin beklenenin ötesinde boyutlarda olan APT'ler ve sosyal ağ siteleri ile bulut bilişim altyapılarındaki etkinlikleri nedeniyle kurumlar açısından önemli riskler doğuran kötücül yazılımlar hakkında dikkat çeken noktalar aşağıda belirtilmektedir.

Kurumsal siber güvenlikte en zayıf halkayı oluşturan insan faktörü üzerine odaklanan sosyal mühendislik yöntemi, çabuk sonuca götürmesi, hızlı ve basit olması nedeniyle saldırganlar tarafından sıkça kullanıldığı görülmektedir.

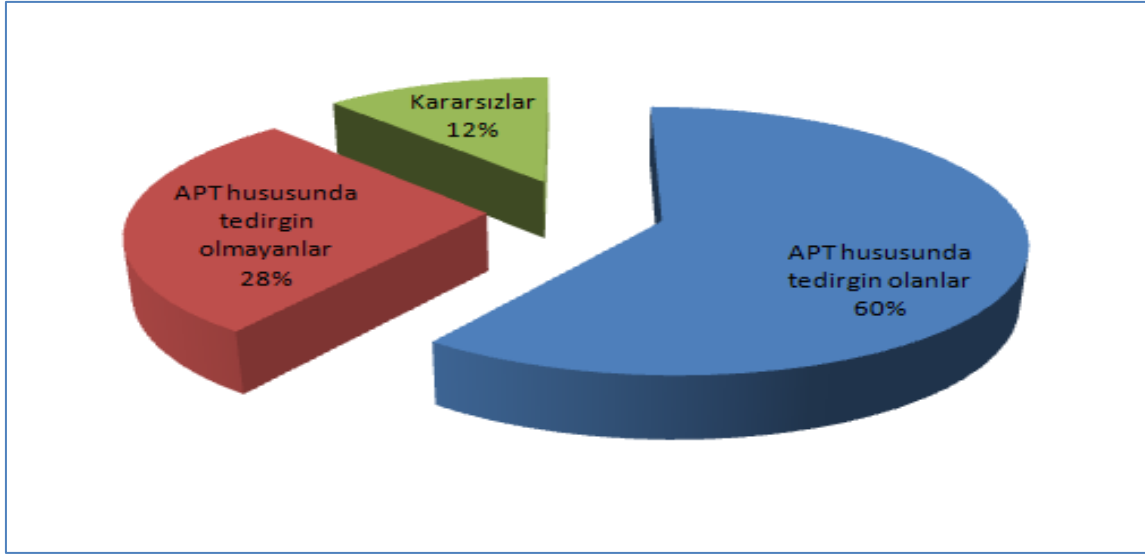
Saldırganların, bu yöntemi kullanmadan önce kurum hakkında bilgi toplamak için e-posta grupları ve forumları inceleyerek acemi ve sorumsuz sistem yöneticilerinin gönderdikleri mesajlardaki (gizli kalması gereken) bilgileri, bu ortamdaki gelişigüzel her sorunun açıkça sorularak yardım istenmesi sonucunda elde ettiği bilgileri ve arama motorlarını kullanarak yaptığı açık kaynak araştırması neticesinde edindiği bilgileri v.b. kullanarak hazırlık yaptığı bilinmektedir.

Kurumsal siber güvenlikte kurum ve şirketlerin karşılaştıkları en büyük tehditlerden bir haline gelen kötücül yazılımlara büyük ölçekli (25.000 ve daha fazla çalışanı olan) kurumların maruz kalma oranı küçük kurumlara oranlara (Şekil 5.7’de görüldüğü üzere) 2,5 kat daha fazla olmaktadır. Ayrıca internette en çok ziyaret edilen siteler hakkındaki veriler, kötücül yazılım bulaştırma riski en yüksek olan sitelerle ilişkilendirildiğinde (Şekil 5.6’da görüleceği üzere) arama motoru ve çevrimiçi video uygulamalarının başı çektiği görülmektedir[8].



Şekil 5.7. Kurum ve şirket boyutuna göre kötücül yazılım risk durumu

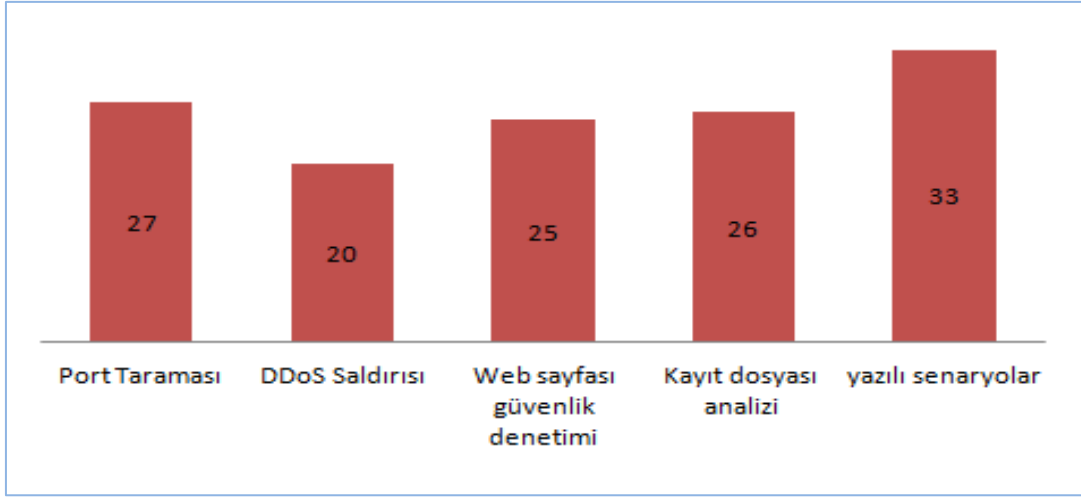
APT'ler ise birkaç virüs yazarı tarafından yapılamayacak şekilde gelişmişlik, karmaşıklık ve gizlilik gibi özelliklere sahip olmaları nedeniyle (Şekil 5.8’de görüleceği üzere) birçok kurum ve şirketin BT yöneticilerini, bilgi sistemlerini bu tür saldırılara karşı etkin bir şekilde koruyabilecekleri hususunda endişelendirmektedir[88].



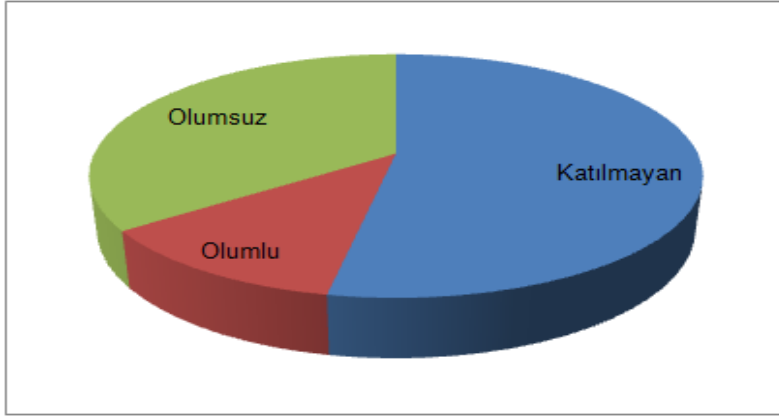
Şekil 5.8. Kurum ve şirketlerin bilgi teknoloji uzmanlarının APT hakkındaki görüşleri

Siber tehdit ve saldırıların ülkemizdeki kurumsal siber güvenlik açısından incelenmesi

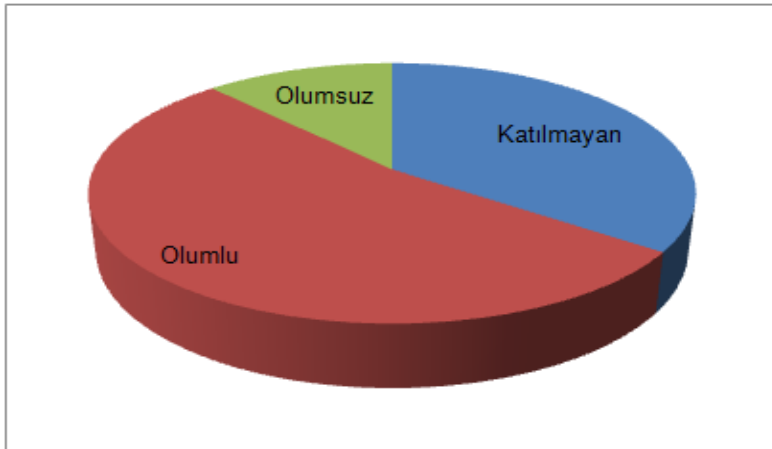
Ülkemizde siber saldırı ve tehditlere karşı hazırlıklı olunması, kurumların bilgi sistemi güvenliği olaylarına müdahale ve kurumlar arası koordinasyon yeteneklerinin tespit edilmesi, ulusal siber güvenlik bilincinin artırılması ve kurumların bilgi ve iletişim sistemlerinin güçlendirilmesi amacıyla Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Bilgi Teknolojileri ve İletişim Kurumu (BTK) işbirliğiyle (belirli aralıklarla) ulusal siber güvenlik tatbikatları düzenlenmektedir. Bu tatbikatlardan çok sayıda kurumun katılım yaptığı, gerçek saldırı ve yazılı senaryoların uygulandığı 2011 yılındaki tatbikata ait katılan kurum sayısı (Şekil 5.9), bu kurumlara yönelik uygulanan DDoS ve port tarama saldırısı sonuçları (Şekil 5.10 ve Şekil 5.11) ile tespit edilen güvenlik açığına (Şekil 5.12) ilişkin veriler aşağıdaki gibidir[31].



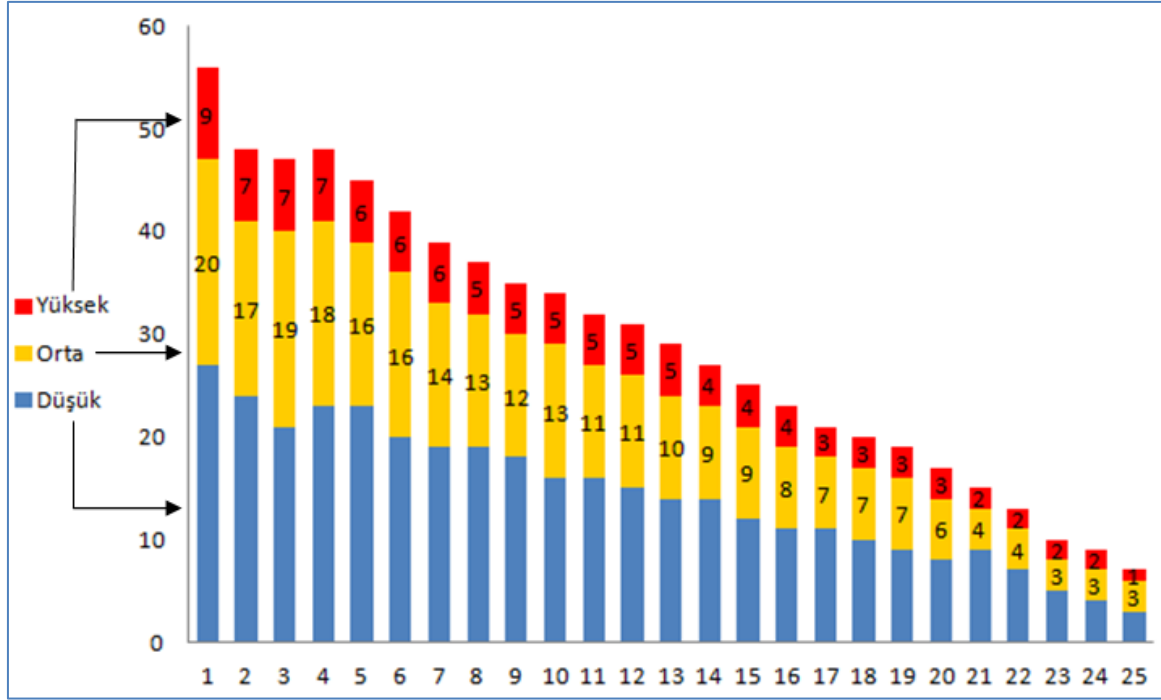
Şekil 5.9. Gerçek saldırı ve yazılı senaryoların uygulandığı kurum sayısı



Şekil 5.10. DDoS saldırısının sonuçları



Şekil 5.11. Port tarama saldırısının sonuçları



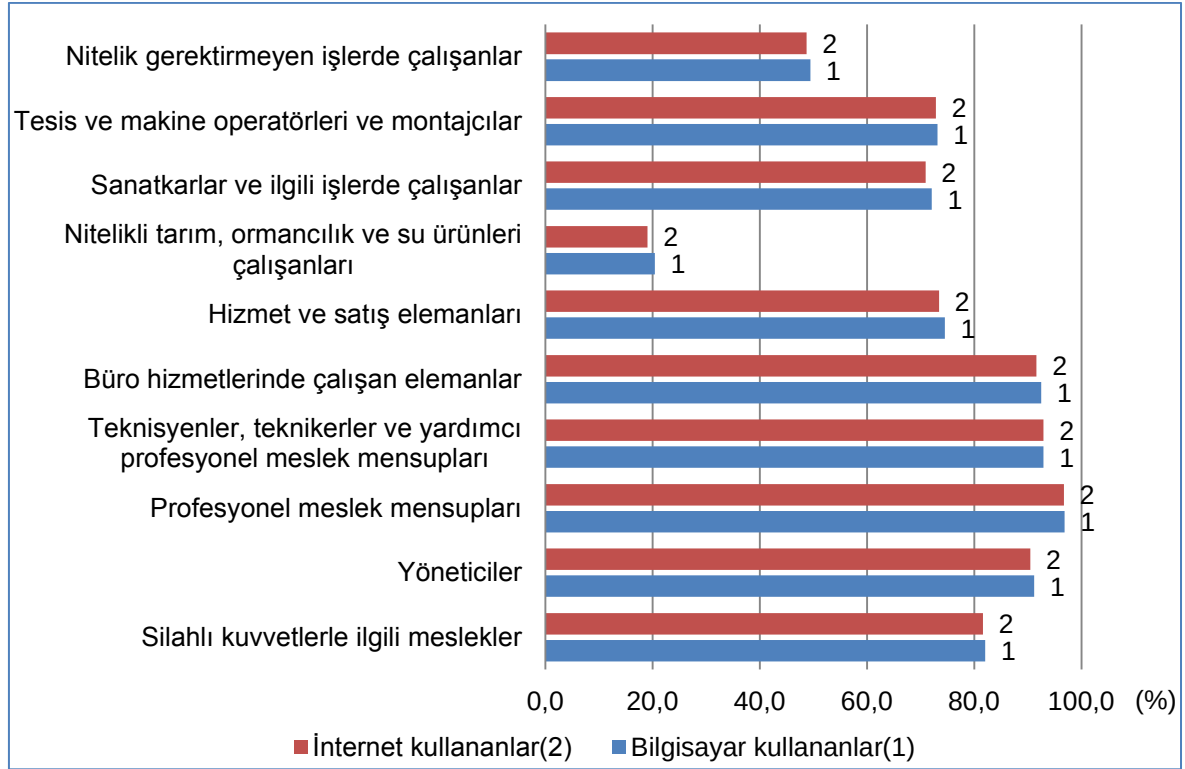
Şekil 5.12. Kurumlarda tespit edilen web açıklıklarının sayıları

Bu tatbikatlar sonucunda (genel olarak):

- Bazı kurumlarda bilgi güvenliği politikalarının olmadığı, saldırı esnasında ve sonrasında ne tür faaliyetler icra edileceğine dair siber güvenlik kültürü oluşturulmadığı,
- Sistem yöneticilerinden birçoğunun yeterli teknik bilgiye sahip olmadığı,
- Bazılarında Saldırı Tespit Sistemleri (STS) olmadığı olanlarda ise saldırıların tespitinde sıkıntılar yaşandığı,
- Bazılarında teknik çözüm arayışına önem verilirken sosyal mühendislik saldırılarına karşı personelde farkındalık eksikliği bulunduğu,
- Antivirüs yazılımlarının düzenli olarak güncellenmediği,
- Bazılarında iletişim hususunda eksiklikler bulunduğu, saldırı anında gerekli adımların atılması konusunda sıkıntılar yaşandığı ve ilgili mercilerle temas kurmada problemler olduğu,
- Bazı personellerin kurumda (erişim izni olmadığı halde) kendisiyle ilgili olmayan hizmetlere erişebildiği,

- Bazılarında sistem tasarım aşamasında güvenliğin temel bir tasarım ilkesi olarak ele alınmamasından dolayı güvenlik olayları yaşandığı ve bu olaylara etkin müdahalenin zorlaştığı,
- Bazılarının (yaşanan sistem kesintisine yol açan güvenlik olayı neticesinde) iş süreçlerinin devamlılığını sağlayacak iş sürekliliği planına sahip olmadıkları,
- DDoS (Distributed Denial of Service) saldırısı sonucunda bazı kurumların hizmetleri kesintiye uğrarken, internet servis sağlayıcı (ISS)'lerden bu tür saldırılara karşı hizmet satın alanların sıkıntı yaşamadığının görülmesi sonucunda kurumlar arası iletişime, işbirliğine ve koordinasyona verilmesi gereken önemin yeterince anlaşılamadığı,
- Birçoğunun web uygulamalarında çeşitli açıklıklar bulunduğu, nispeten daha az güvenlik açığı bulunanların ise web uygulamalarını farklı kurumlara denetlettiği ya da web uygulamalarını geliştirirken güvenliğe dikkat ettikleri,
- Özel bir bilgi güvenliği birimlerine sahip olan kurumların yapılan saldırıları analiz etmede daha başarılı oldukları,
- Bazı kurumların da ulusal mevzuat hususunda yeterli bilgiye sahip olmamalarından dolayı yazılı senaryolarda siber suç olarak tanımlanan fiilleri adli mercilere bildirmediikleri şeklinde bir takım eksiklik ve yanlışlıklar tespit edilmiştir[6].

Saldırganların, çalışanların internet kullanım alışkanlıklarını (bkz. Şekil 5.5 ve Şekil 5.6) göz önünde bulundurarak elde ettikleri veriler neticesinde planlı ve organize saldırılar düzenlemesi nedeniyle çeşitli meslek gruplarına ilişkin elde edilen bilgisayar ve internet kullanma oranları, ülkemizde kurumsal siber güvenliği sağlama adına yol gösterici niteliktedir(Şekil 5.13).



Şekil 5.13. Meslek gruplarına göre bireylerin (16-74 yaş arası) bilgisayar ve İnternet kullanım oranları[87]

5.1.2. Siber tehdit ve saldırıların etkiledikleri alanlara göre incelenmesi

Siber tehdit ve saldırıların ortaya çıktığı alanlara ilişkin güncel durumlar Çizelge 5.2’de görülmektedir. Bu alanlar (yukarıda bahsedilen big data ve nesnelerin interneti (Bkz. 5.1) dışında):

- Bir devletin egemenliği için (iletişim, ulaşım ve enerji gibi hayati öneme haiz ve güvenlikleri öncelikle sağlanması gereken *kritik altyapılar*,
- Yeniliklere açık bir mimariye sahip ve geleneksel bilgi teknolojilerindeki değişimlerle (birlikte bu cihazlara olan rağbet nedeniyle) uygulama sayılarında artışın gözlendiği *mobil platformlar*,
- Gelecek dönemler de etkisinin devam etmesi beklenen internet kullanıcılarının hayatlarının önemli bir bölümüne nüfuz etmiş kavramlardan biri olan ve hedeflenen kurumlardaki personeller hakkında birçok bilgi toplanmasına imkân veren *sosyal ağlar*,
- Mevcut internet mimarisinin ayrılmaz bir parçası olarak değerlendirilen, veri depolama ve (yenilenen bilgi teknolojilerinin) uygulama servislerini barındıran, etkili güvenlik mekanizmalarına sahip bir sistem olan *bulut*

bilişim,

- Sistemler için güçlü kimlik doğrulama mekanizmalarını sunan ve çeşitlik güvenlik mekanizmalarını bir arada bulunduran omurga olarak adlandırılan *güvenilir altyapılardır*(Trust infrastructure)[65].

Çizelge 5.2. Siber tehdit ve saldırıların etkiledikleri alanlara göre durumları[65]

	TEHDİTLER	Kritik alt yapılar	Mobil cihazlar	Sosyal ağ	Bulut bilişim	Güvenli alt yapılar	Big data	Nesnelerin interneti
1	İzinsiz indirmeler	↑	↑	↑		↑	↑	
2	Solucan/ Trojan	↑	↑	↑	↑	↑	↑	↑
3	Kod enjeksiyonu	↑	↑	→	↑	↑	↑	
4	Exploit kit	→	↑	↑	↑	↑	↑	
5	Botnet	↑	↑	↑	↑			
6	Fiz.zarar ve hırsız.(kayıp)	↑	↑	↑	↑	↑	↑	↑
7	Kimlik hırsızlığı		↑	↑	↑	↑	↑	↑
8	Hizmet aksattırma	↑			↑			↑
9	Sazan avlama	↑	↑	↑	↑	↑	↑	↑
10	Spam			↑				↑
11	Veri ihlali		↑		↑	↑	↑	↑
12	Bilgi sızıntısı	↑	↑	↑	↑	↑	↑	↑
13	Hedefli saldırılar(APT)	↑				→	↑	↑

(Artan) ↑ (Durağan) → (Azalan) ↓

Çizelge 5.2’de görüleceği üzere sazan avlama (phishing), kötücül yazılımlar (Solucan/Truva atı) ile veri ihlallerinin en büyük nedenlerinden biri haline gelen kayıp ve hırsızlığın tüm alanlarda etkileri (artarak) görülmesine karşın hizmet aksattırma ve spam tehditlerinin etkiledikleri alanlar bakımından en düşük tehditler olduğu görülmektedir.

5.1.3. Siber tehdit ve saldırılar ile bu tehdit ve saldırıları gerçekleştiren gruplar arasındaki ilişkinin incelenmesi

Çizelge 5.3. Siber saldırı ve tehditler ile bu tehdit ve saldırıları gerçekleştiren gruplar arasındaki ilişki[65]

N O	TEHDİTLER	Kurum ve Şirketler	Devletler	Hackivistler	Siber Teröristler	Siber Suçlular	Siber Savaşçılar	Script kiddie	Çevrimiçi Sosyal Hackerlar	Kurum Çalışanları
1	İzinsiz indirmeler		✓			✓				
2	Solucan/ Trojan		✓		✓	✓	✓		✓	✓
3	Kod enjeksiyonu	✓	✓	✓	✓	✓	✓	✓		
4	Exploit kits			✓	✓	✓	✓	✓		
5	Botnet	✓	✓	✓	✓	✓	✓			
6	Fiz.zarar ve hırsızlık, kayıp	✓	✓	✓	✓	✓	✓	✓	✓	✓
7	Kimlik hırsızlığı	✓	✓	✓	✓	✓	✓	✓	✓	✓
8	Hizmet aksattırma		✓	✓	✓	✓	✓	✓		✓
9	Sazan avlama	✓	✓			✓			✓	
10	Spam	✓				✓			✓	
11	Sahte antivirüs yazılımı					✓				
12	Veri ihlali	✓	✓	✓	✓	✓	✓	✓		✓
13	Bilgi sızıntısı	✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Hedefli saldırılar(APT)	✓	✓	✓	✓	✓	✓		✓	
15	Watering hole	✓	✓			✓	✓			

Siber tehditler arasında sahte antivirüs yazılımlarının yalnız siber suçlular ve izinsiz indirmelerin de siber suçlular ile devletler tarafından kullanılması dikkat çekerken bilgi sızıntısı, kimlik hırsızlığı ile hırsızlık ve kayıp gibi tehditlerin tüm gruplar tarafından kullanıldığı görülmektedir. Başka bir hususta; kurum veya şirketler tarafından sıklıkla ziyaret edilen web sitelerini hedefleyen ve yüksek teknolojiye sahip birçok kuruma başarılı saldırıların gerçekleştirilebildiği popüler adresler üzerinden yapılan saldırıların (watering hole) kısa zaman içinde birçok grup tarafından kullanıldığıdır(Çizelge 5.3).

Siber tehdit ve saldırıları gerçekleştiren (Çizelge 5.3' deki) gruplar:

- Rekabet üstünlüğü elde etmek için siber tehditleri kullanarak rakiplerinin plan ve stratejilerini ele geçirme, gizlilik içeren kurumsal bilgilerine sahip olma gibi faaliyetler de bulunabilen ve hatta bunun için kendi siber yeteneklerini geliştirme çabası içinde olabilen *kurum ve şirketler*,
- Özellikle kendi siber yeteneklerini geliştirerek rakip devletlerin kamu ve özel şirketlerine karşı saldırılar yapan, kritik altyapıları tehdit etme, devlet sırları ve askeri istihbarat bilgileri elde etme amacıyla (başarı oranı oldukça yüksek) saldırılar yapabilen *devletler*,
- Amaçları belirli uygulamaları protesto etmek veya (medyanın ve toplumun dikkatini çekecek şekilde) savundukları fikirlerini açıkça ortaya koymak olan ve medyanın dikkatini çekmekten hoşlanan, ideolojik olarak bir araya gelen grupların oluşturduğu *hacktivistler*,
- Bir ülkenin özellikle kritik altyapılarına yönelik eylemde bulunmak amacıyla saldırı düzenleyen *siber teröristler*,
- Bir kurum ve şirketi yasadışı şekilde mali zarar uğratarak maddi kazanç sağlama eğiliminde olan, ayrıca yeteneklerini geliştirmek için bilgi paylaşımında bulunabilen ya da belli bir hedefe saldırı da bulunmak için kolektif hareket edebilen *siber suçlular*,
- Özellikle hacktivist grupların ve siber suçluların yaptıklarından etkilenerek ne kadar çok kod öğrenirsem o kadar hack eylemi yapabilirim düşüncesi içinde bulunan geç yaştaki saldırgan grupların oluşturduğu *script kiddie*, (Bunlar buldukları hazır kodları ve uygulamaları kullanarak özellikle DoS atakları ve kod enjeksiyonu gibi saldırılarda bulunurlar.)

- Siber saldırılarda sosyal mühendisliğin artmasıyla önemli bir rol oynamaya başlayan, hedef personelle iletişim kurma, güvenini kazanma ve hedefle ilgili psikolojik ve sosyolojik analiz yapabilme yeteneğine sahip olan *çevrimiçi sosyal hackerlar*, (Bu grupların teknik bilgileri düşük olmasına karşın sosyal mühendislik yeteneklerinin yüksek olmasından dolayı (özellikle de sosyal ağların kullanımının artmasından dolayı) bu grupların saldırılarının artması beklenmektedir.)
- Elde ettikleri erişim hakları nedeniyle kurumsal bilgi varlıklarına yüksek oranda zarar verebilen fakat genellikle teknik düzeyi düşük (kötü niyetli ve kasıtlı) saldırılar yapan *kurum çalışanları*, (kasıtsız olarak güvenlik ihlaline sebebiyet veren bilinçsiz kullanıcılar da bu kategoriye dahil edilmektedir.)
- Yüksek milliyetçilik ve kutsal devlet anlayışına sahip ve bu bilinçle bir takım saldırılarda bulunan *siber savaşçılardır*.

5.1.4. Siber tehdit ve saldırılarla mücadele adına yapılanların incelenmesi

Yakın gelecekte yapılacak savaşların siber ortamda yapılacağı ve ortaya çıkan birçok siber tehdit ve saldırılar düşünüldüğünde, ülkelerin siber güvenliğini ulusal güvenliğinin bir parçası haline getirmeleri zorunlu hale gelmektedir. Siber kuvvetler tesis edilmesi için birçok ülke (İngiltere’ de siber güvenlik elemanı yetiştirmek için SANS (SysAdmin, Audit, Networking, and Security) Enstitüsü tarafından eğitimler verilmesi, İran’ın güçlü bir siber ordu peşinde olması, Kuzey Kore’nin siber savaş bölümü personelini 550’ den 3 000’e çıkarması, Çin’in 2050 yılına kadar elektronik egemenliği hedeflemesi v.b.) çeşitli hazırlıklar yapmaktadır[90].

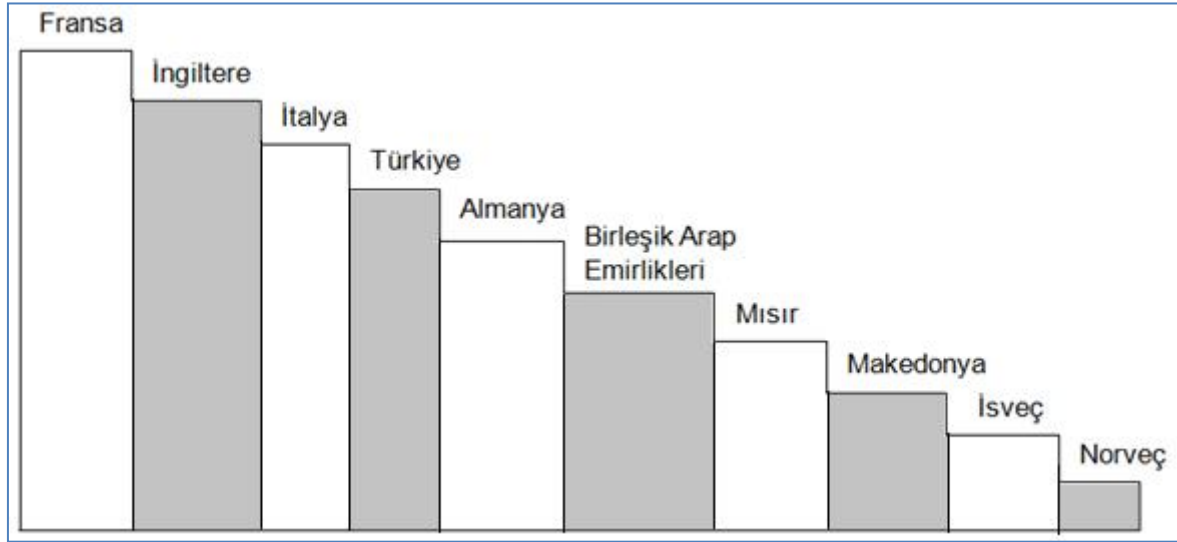
İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü tarafından yayınlanan siber güvenlik raporunda (2012) da belirtildiği gibi siber güvenliğin en üst düzeyde sağlanabilmesi için öncelikle güvenlik politikası oluşturulmalı sonra devlet çatısı altında uygulayıcı kurumlar oluşturup bunların uyum içinde çalışabilmesini sağlayacak mekanizma kurulmalı ve bu yapıların esnek ve hızlı biçimde çalışmasını sağlayacak hukuki alt yapı oluşturulması gerekmektedir. Ayrıca siber güvenlik alanında hem kamu hem de özel sektörde çalışacak nitelikli personel yetiştirme adına üniversitelere düşen roller belirlenmeli ve bu alanda en son gelişmelere ayak uydurabilecek ar-ge merkezleri kurulmalıdır.

Artan ve gelişen siber tehdit ve saldırılara karşı ulusal siber güvenliği sağlamaya ilişkin bazı ülkelerin gerçekleştirdiği uygulamalar ülkemizde siber tehdit ve saldırılarla mücadele adına yapılacaklara yol gösterici niteliktedir[4]:

- Hindistan: Kritik altyapıların ve bilişim sistemlerinin korunmasıyla ilgili çalışan uzmanların listesinin tutulduğu ulusal güvenlik veritabanı (NSD) oluşturularak daha yüksek pozisyonda çalışmak isteyen uzmanların buradaki konumu ve eylemlerine bakılarak karar verilmektedir.
- Amerika: 2008 yılında Amerika’da siber güvenlik politikası yenilenerek “Kapsamlı Ulusal Siber Güvenlik Girişimi” (CNCI-Comprehensive National Cybersecurity Initiative) başlıklı bir direktif hazırlandı. Bu direktifte EINSTEIN adlı (federal web sitelerinden web sitelerine olan internet trafiğini gözlemleyen) programın yetkisi NSA’ya (National Security Agency) aktarılarak ulusal siber güvenlik biriminin (US-CERT) liderliğinde ve amacı ulusal çapta bir siber saldırı olması durumunda 19’dan fazla kurum arasında koordinasyon sağlamak olan Ulusal Siber Tepki Koordinasyon Grubu kurulmuştur.
- Çin: Ülkedeki 3 adet araştırma enstitüsü de siber güvenliğin geliştirilmesi amacıyla ar-ge faaliyetleri yürütmekte ve önde gelen üniversitelerinde desteği alınmaktadır. Ayrıca, Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü süper bilgisayarlarla ilgili yatırımlar yapmakta ve bu bilgisayarlarla şifre kırma gibi çalışmalarla ordu bünyesindeki organizasyonlara destek vermektedir.
- Almanya: IT (Information Technologies) sistemlerinin güvenli kullanımında küçük ve orta ölçekli işletmelerin desteklenmesi için Ekonomi ve Teknoloji Federal Bakanlığı, sanayinin katılımı ile IT güvenliği konusunda bir görev gücünün kurulduğu ülkede devletin, vatandaşlarının çoğunluğunun kullandığı devlet tarafından onaylanmış temel güvenlik işlevleri için özel teşvikler ve fonlar sunması gerektiği siber güvenlik stratejisinde yer almaktadır.
- Avrupa Birliği (AB): Siber güvenlikle ilgili temel adım 2005 yılında Avrupa Ağ ve Bilgi Güvenliği Ajansı’nın (ENISA) faaliyete başlamasıyla atılmıştır. Sonrasında 2007 yılında ‘Webi (ağı) Kontrol Et’ isimli güvenlik portalı olan Avrupa Polis Ofisi (Europol) kurulmuştur. Avrupa’da siber atağa karşı

anında müdahale sistemi kurma çabasında olan Avrupa Komisyonu'nun hedefleri arasında bilgisayarlar için bir acil yanıt takımı (Certs) kurma planı ve ENISA'nın rolünü arttırma bulunmaktadır.

Siber tehdit ve saldırılarla mücadele adına ülkemizde yapılanların incelenmesi



Şekil 5.14. Siber suçluların hedeflediği 10 ülke

Avrupa, Ortadoğu ve Afrika ülkeleri arasında (Şekil 5.14' de görüldüğü üzere) siber saldırganların en çok hedeflediği 4. Ülke konumunda olan[79] ülkemizde siber güvenlikle ilgili çalışmalara 2012 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (UDHB) tarafından başlanıldığı görülmektedir. Bu bağlamda yapılan siber güvenlik yapılanma faaliyetleri Çizelge 5.4' de sunulmaktadır.

Yapılanma faaliyetleri çerçevesinde oluşturulan siber güvenlik kurulu:

- Dışişleri Bakanlığı İçişleri Bakanlığı Milli Savunma Bakanlığı
- Kamu Düzeni ve Güvenliği Müsteşarlığı
- Milli İstihbarat Teşkilatı
- Genelkurmay MEBS Başkanlığı
- Bilgi Teknolojileri ve İletişim Kurumu
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK)
- Mali Suçları Araştırma Kurulu
- Telekomünikasyon İletişim Başkanlığı üyelerinden meydana gelmektedir.

Çizelge 5.4. Ülkemizde ulusal düzeyde yapılan siber güvenlik yapılanma faaliyetleri

Temmuz 2012	Siber Güvenlik Enstitüsü kuruldu.
Ağustos 2012	UDHB ve TÜBİTAK işbirliği ile Siber Güvenlik Projeleri
Eylül 2012	TSK Siber Savunma Merkezi Başkanlığı kuruldu.
Ekim 2012	Siber Güvenlik Kurulu kuruldu.
Aralık 2012	Siber Güvenlik Kurulu ilk toplantısını gerçekleştirdi.
Ocak 2013	UDHB Siber Güvenlik Dairesi kuruldu.
Şubat 2013	Siber güvenlik değerlendirme toplantısı yapıldı.
Mayıs 2013	Siber Güvenlik Kurulu ikinci toplantısı planlandı.

Ülkemizin siber güvenlik ihtiyaçlarının ortaya konarak hedeflerin doğru belirlenebilmesi, belirlenen bu hedeflere yönelik adımların uygun, sistematik, amaca yönelik olabilmesi ve atılmış adımların denetimi ve geliştirilmesi için 2013 yılında ortaya konan siber güvenlik stratejisi ve eylem planı, bilgi güvenliği farkındalığının artırılması, ülkenin siber uzayının güvenliğinin ve savunmasının artırılması, siber saldırılara karşı kritik altyapıların dayanıklılığının ve sürekliliğinin temin edilmesi ve kişisel, kurumsal, ulusal çaptaki verilerin güvenliğinin sağlanması adına çok önemlidir. Bu bağlamda oluşturulan siber güvenlik stratejisi ve eylem planı 30 sorumlu kurum ve kuruluşun kapsandığı 7 ana başlığa (Yasal Düzenlemelerin Yapılması, Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi, Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması, Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi, Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi, Siber Güvenlikte Yerli Teknolojilerin Geliştirilmesi, Ulusal Güvenlik Mekanizmalarının Kapsamının Genişletilmesi) sahip 29 eylem maddesi içermektedir. Ayrıca siber güvenliğin ulusal boyutta odaklandığı (askeri, istihbarat, siber diplomasi, kritik altyapılar, siber suçlar gibi) 5 noktanın da dikkate alınarak hazırlandığı bu gibi planlar birçok gelişmiş ülke tarafından (siber güvenliklerini sağlama adına) yapılmaktadır. Ulusal siber güvenlik adına yapılan çalışmalar kısaca aşağıda belirtilmektedir.

TÜBİTAK tarafından yapılanlar

Ülkemizdeki stratejik kamu kurumlarının ihtiyaç duyduğu bilgi güvenliği ve elektronik sistem projelerini geliştirirken aynı zamanda Türkiye'nin bilgi güvenliği birikimine önemli katkılar sağlayan bir ar-ge kuruluşu olan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UAKEA) TÜBİTAK tarafından oluşturulmuştur. Bilgi güvenliği kapsamında teknolojik dışa bağımlılığı azaltmak amacıyla (tasarımdan tüm devrelerin gerçekleştirilmesine kadar) cihazların kritik öneme sahip tüm bileşenleri UEKAE bünyesinde gerçekleştirilmektedir[33]. Ayrıca belirli bir sorumluluk alanına olay müdahale servisi veya bilgi sistem güvenliği ile ilgili diğer önleyici veya düzeltici servisler veren ve bilgisayar güvenlik olaylarıyla ilgili ulusal danışma noktası olan Bilgisayar Olaylarına Müdahale Ekibi (BOME) ve sorumluluk alanında birden çok kurum veya kuruluş olan ve bu kurum ve kuruluşlar arasında olay müdahale koordinasyonu yapan BOME-KM (Bilgisayar Olaylarına Müdahale Ekibi Koordinasyon Merkezi) de UAKEA Bilişim Sistemleri Güvenliği bölümü bünyesinde faaliyet göstermektedir[36].

Siber güvenlik alanında araştırma ve geliştirme faaliyetleri yürüten askeri kurumlara, kamu kurum/kuruluşlarına ve özel sektöre çözüme yönelik projeler gerçekleştiren ve bugüne kadar başarı ile gerçekleştirdiği pek çok proje ile ülkemizde siber güvenlik bilgi birikimi oluşturulmasına önemli katkı sağlayan SGE (Siber Güvenlik Enstitüsü) faaliyetlerine 1997 yılında "Bilişim Sistemleri Güvenliği (BSG) Birimi" adı ile TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) altında başlayarak 2012 yılından bu yana ise TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak faaliyetlerini sürdürmektedir[32]. Siber Güvenlik Enstitüsü' nün sürdürdüğü faaliyetleri:

- Hem kamu kurum/kuruluşları hem de özel sektör şirketlerine bilişim altyapısındaki tüm bileşenleri kapsayacak şekilde sızma testleri ve güvenlik denetlemeleri yaparak detaylı teknik raporlar ve yönetici özetleri sunmak, (Ayrıca, çalışanların güvenlik bilincini arttırmak için teknik güvenlik testlerinin yanında sosyal mühendislik testleri de yapılmaktadır)

- Gelişen teknolojilere uygun olarak mobil uygulamaların, kritik bilgi sistem altyapılarının, akıllı ağ sistemlerinin ve bulut bilişim altyapılarının güvenliğinin sağlanması ve testlerine yönelik çalışmalar yapmak,
- Bilgi sistemlerinin güvenli tasarımı, kurulumu ve yapılandırması konusunda çalışmalar yapmak,
- Kurumların mevcut bilgi işlem altyapılarının incelenip ihtiyaç duyulan güvenlik önlemlerinin tasarlanması, yeni bilgi işlem altyapılarının kurulumu ve yapılandırılmasıyla ilgili danışmanlık hizmeti vermek,
- Bünyesindeki zararlı yazılım analiz birimi ile güncel zararlı yazılım trendini yakından takip ederek ülkemizin kritik altyapılarına yönelik tehdit oluşturabilecek zararlı yazılımları analiz ederek elde edilen sonuçlarla alınması gereken önlemleri ilgili kurumlara sunmak,
- Önemli kamu kurumları ile kritik altyapı olarak değerlendirilebilecek özel kuruluşlardan talep gelmesi halinde APT tespit ve analizi yapmak,
- Bir siber saldırı olduğunda, saldırının kaynağını, sisteme nasıl sızıldığını ve sistemde neler yapıldığını tespit etmek için yapılacak detaylı incelemeleri yapan Dijital Adli Analiz Laboratuvarı sayesinde adli soruşturma ve davaların aydınlatılabilmesi için güncel adli bilişim tekniklerini ve araçlarını kullanarak gerekli incelemeleri gerçekleştirmek şeklinde sıralanmaktadır[26].

TÜBİTAK tarafından ulusal çapta siber güvenliğin sağlanması adına yapılan diğer faaliyetler:

- Kamu kurumlarına yönelik sistem güvenlik testleri yapılması,
- 2013 yılında 54 farklı kurumdan yaklaşık 150 BT teknik personeline ve üst yöneticilerine verilen (teknik ve yönetsel) 12 farklı siber güvenlik eğitime benzer kamu kurumlarının siber güvenlik yetkinlik artırımını sağlayan kamu bilgi güvenliği programının uygulanması,
- www.bilgimikoruyorum.org.tr ve www.bilgiguvenligi.gov.tr gibi bilgi paylaşım portalları oluşturularak siber güvenlik farkındalığı ve bilgi kaynağı tesis edilmesi,
- Ülkemizde siber güvenlik uzmanı eksikliğinin giderilmesine destek olmak ve kapasite geliştirilmesini sağlamak amacıyla (Siber Güvenlik Enstitüsü ve Bilgi Güvenliği Akademisi ile birlikte) üniversitelerin lisans ve yüksek lisans

öğrencilerinin katıldığı (Akademisyen, kamu ve özel sektör yöneticileri ile temas halinde) teknik eğitim ve yarışmaların yapıldığı siber güvenlik yaz kamplarının düzenlenmesi,

- Ülkemizde siber güvenlik konusunda idari, teknik ve hukuki kapasitenin geliştirilmesine, kurumlar arasında bilgi ve tecrübe paylaşımına ve başta yönetim seviyesinde olmak üzere tüm kademelerde farkındalık oluşumuna önemli katkılar sağlanması ve kurumların bilgisayar olaylarına müdahale yeteneğinin tespit edilmesi amacıyla bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin, adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan kamu kurumları ve (sivil toplum kuruluşuyla birlikte) özel sektör kuruluşlarının da katılımıyla (BTK (Bilgi Teknolojileri ve İletişim Kurumu) ile işbirliği içinde) ulusal siber güvenlik tatbikatlarının gerçekleştirilmesi,
- Kötücül Yazılım Analiz Merkezi kurulması, Siber Tehdit Gözetleme ve Önleme Sistemi geliştirilmesi, Gelişmiş Siber Casusluk (APT) analizlerinin gerçekleştirilmesi ve Veri Kaçağı Önleme (DLP) Sistemi geliştirilmesi gibi ar-ge projelerinin gerçekleştirilmesi şeklinde sıralanmaktadır[72].

EGM (Emniyet Genel Müdürlüğü) tarafından yapılanlar

Bilişim alanındaki hak ihlallerini araştırma ve bu alandaki suç tiplerini belirlemek amacıyla 1999 yılında Bilişim Suçları Çalışma Grubu'nun Emniyet Genel Müdürlüğü bünyesindeki Bilgisayar Suçları ve Bilgi Güvenliği Kurulu'na bağlı olarak oluşturulduğu görülmektedir. Bu gruba farklı alanlarda destek sağlamak amacıyla:

- Bilgi İşlem Daire Başkanlığı,
- Kaçakçılık ve Organize Suçlar Daire Başkanlığı,
- Güvenlik Daire Başkanlığı,
- Kriminal Polis Laboratuvarları Daire Başkanlığı,
- Interpol Daire Başkanlığı,
- Polis Akademisi Başkanlığı,
- Hukuk Müşavirliği üyeleri dahil edilmişlerdir.

Bilişim suçlarıyla ilgili ilk birim 1997 yılında ‘Bilişim Suçları Bürosu’ adıyla kurularak 2001 yılında ‘İnternet ve Bilişim Suçları Şube Müdürlüğü’ olarak adı değiştirilen ve bu birimin dışında diğer daire başkanlıkları altında kendi görev alanlarına giren konularda bilişim suçları ile mücadele etmek üzere Bilgi İşlem Şube Müdürlüklerinin de kurulduğu emniyet teşkilatında siber tehdit ve saldırılarla mücadele adına yapılanları kısaca:

- Merkez teşkilatı içinde ‘Bilgisayar Suçları ve Bilgi Güvenliği Kurulu’ oluşturulması,
- 2001 yılında Kaçakçılık ve Organize Suçlar Daire Başkanlığı ile Birleşmiş Milletler tarafından ortaklaşa kurulan TADOC (Turkish Academy Against Drug and Organised Crime) bünyesinde Bilişim Suçları Araştırma Merkezi oluşturulması,
- EGM bünyesinde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı koordinatörlüğünde Terörle Mücadele Daire Başkanlığı, Asayiş Daire Başkanlığı ve Güvenlik Daire Başkanlığı’nın (bu koordinasyondan farklı olarak İstihbarat Daire Başkanlığı da) bilişim suçları ile mücadele için faaliyet göstermesi,
- Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde yer alan Bilgi İşlem Büro Amirliği, 2003 yılında yapılan değişiklikle Yüksek Teknoloji Suçları ve Bilişim Sistemleri Şube Müdürlüğü adını ve 2006 yılında yapılan bir başka değişiklikle de “Bilişim Suçları ve Sistemleri Şube Müdürlüğü” adını alması,
- 2010 yılında (kötücül e-postalar ve yazılımlar, internet ortamında yapılan saldırılar ve zararlı içeriklere erişimle mücadele amacıyla) Bilgi teknolojileri Daire Başkanlığı’na bağlı Bilişim Güvenliği Şube Müdürlüğü kurulması,
- 2012 yılının mart ayında Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulması ve 2013 yılında yapılan değişiklikle Siber Suçlarla Mücadele Daire Başkanlığı adını alması şeklinde özetlemek mümkündür[5].

Ülkemizde son yıllarda artan internet kullanımıyla birlikte artış gösteren sanal ortamdaki dolandırıcılık suçlarına karşı emniyet teşkilatının, siber suçları önlemeye yönelik doğrudan veya dolaylı katkı sağlayabilecek kişi ve kurumlarla işbirliği

yapılmasına ve dünya standartlarında teknolojilerin kullanılarak faillerin yakalanmasına önem vermesi sayesinde 2012 yılında yapılan 6.718 operasyonda 2.180 şüpheli yakalanmıştır[68].

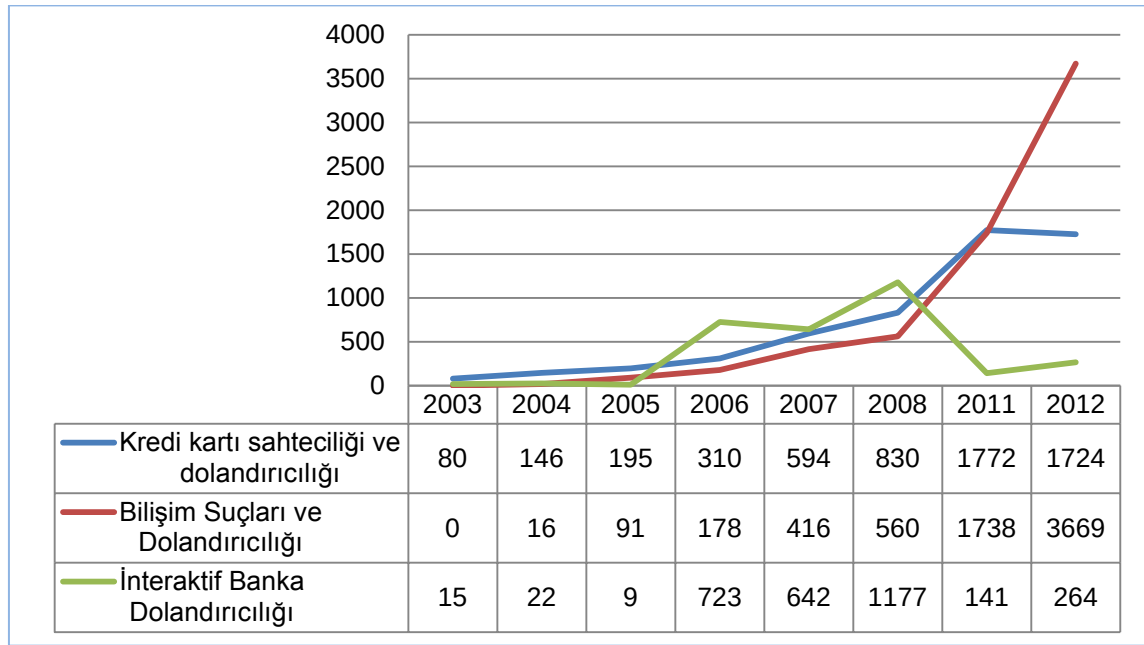
Diğer kurumlar tarafından yapılanlar

- Ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması adına TİB (Telekomünikasyon İletişim Başkanlığı) tarafından USOM (Ulusal Siber Olaylara Müdahale Merkezi) kurulmuştur[38].
- Siber tehditleri tespit amacıyla balküpü sistemi kurulması, siber saldırı raporlama sisteminin kurulması ve geliştirilmesi, siber tehditlerle ilgili veri üretilmesi ve siber tehditlerin önlenmesine ilişkin gerekli mekanizmaların geliştirilmesine yönelik siber tehditleri önleme projesi (STOP) ve siber güvenliğe yönelik tehdit oluşturan ve internet kaynaklarını gereksiz meşgul eden istem dışı e-postaların engellenmesine yönelik Spam e-postalarla mücadele proje çalışmaları BTK tarafından gerçekleştirilmiştir[18].
- Siber tehditleri önleyerek, gelişmiş siber savunma ikaz ve tepki sistemlerine sahip güçlü bir merkezi siber savunma yeteneği kazanmak amacıyla 2012 yılında 'TSK Siber Savunma Merkezi Başkanlığı' kurularak 2013 yılında yapılan yapılandırmalarla TSK Siber Savunma Komutanlığı'na dönüştürülmüştür[22]. (TSK Siber Savunma Harekât Merkezi, 7 gün 24 saat esasına göre siber olayları takip ederek siber olaylarla ilgili USOM, BOME ve uluslararası organizasyonlarla koordineli olarak çalışmalarına devam etmesinin yanında kamu kurum ve kuruluşları ile ortak eğitimler, tatbikatlar icra etmekte ve ar-ge çalışmalarını takip etmektedir.)

5.2. Siber Suçların İncelenmesi

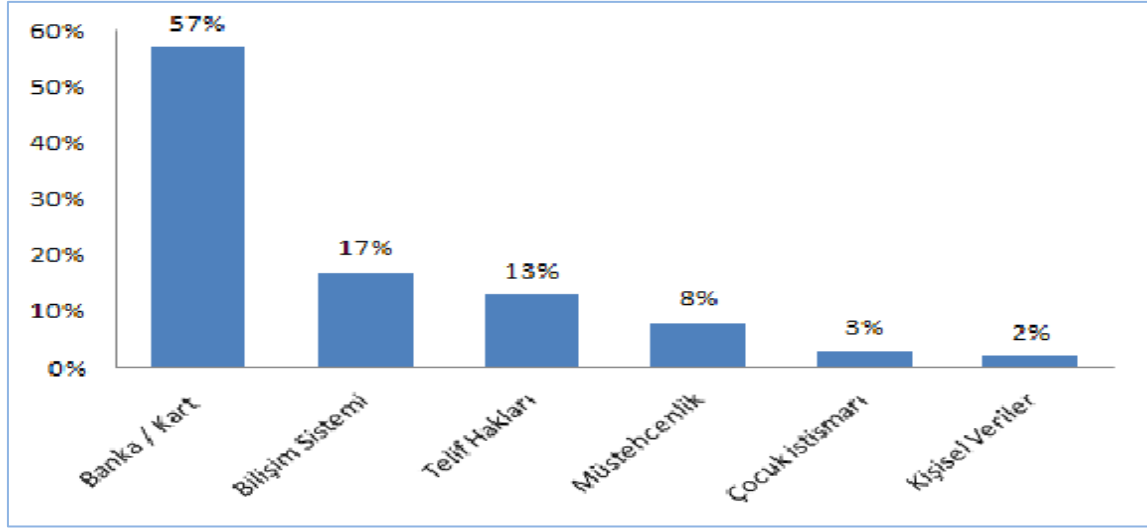
24 ülkeden 13 binin üzerinde kullanıcının verilerine dayanılarak oluşturulan Norton güvenlik raporuna (2013) göre siber suça maruz kalan yetişkinlerin sayısı düşerken siber suça maruz kalanların kişi başına düşen mali kaybı % 50 oranında artmıştır. Aynı rapora göre ülkemizde siber suç mağdurlarının kişi başına düşen mali kaybı 54 dolar iken 2013 yılında (yaklaşık 6 kat artarak) 309 dolar olmuştur. Ortalama her bir saniyede 12 kişinin siber suçtan etkilendiği 2013 yılında (15

Kasım tarihine kadar) toplam 378 milyon kişinin siber suça maruz kaldığı ve bunun sonucunda da 113 milyar dolarlık bir maliyet olduğu görülmektedir. (Bu siber suçların % 38'i dolandırıcılık ve % 21'i de hırsızlık ve kayıp) Bir diğer önemli gelişme de 2013 yılı Kasım ayı itibarıyla son 12 ay için ülkemize siber saldırıların maliyeti 2 milyar dolara ulaşırken bu saldırılardan etkilenen kişi sayısının da 7 milyona ulaştığıdır[29].



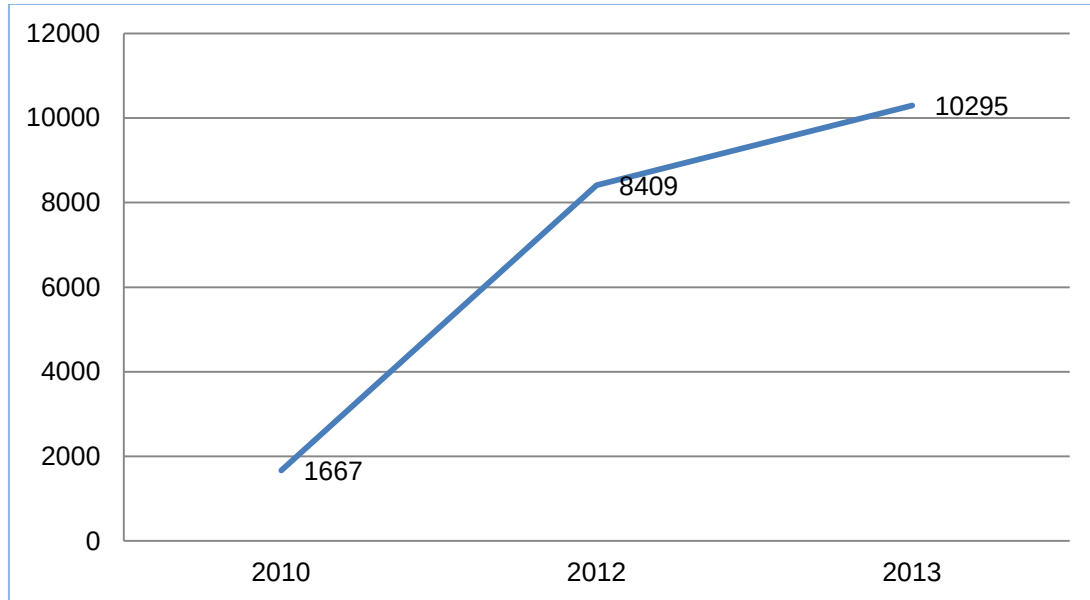
Şekil 5.15 Ülkemizde işlenen bazı siber suç olaylarındaki yıllık değişim oranları[74,68]

Ülkemizde siber suç olaylarının, internet kullanımının yaygınlaşması ve çevrimiçi bankacılık hizmetlerinin artmasına paralel olarak artış gösterdiği gözlenmektedir. Son yıllarda alınan önlemler neticesinde kredi kartı ve interaktif banka işlemlerinde azalma görülse de yeterli olmadığı anlaşılmaktadır(Şekil 5.15). Çünkü yukarıda da belirtildiği gibi sayısal anlamda bir düşüş olmasına karşın verilen zararın boyutlarının arttığı anlaşılmaktadır.



Şekil 5.16. 1990 ve 2011 yılları arasında suç türlerine göre toplam dosya sayıları[16]

Ülke genelinde yapılan bir araştırma neticesinde siber suçlarla ilgili elde edilen veriler göstermektedir ki; banka ve kredi kartı ile ilişkili davalar diğer siber suçlarla ilgili davaların yarısından fazladır. Bilişim sistemlerine yönelik işlenen suçlar ve telif hakları ihlaline ilişkin suçlar ikinci ve üçüncü sırada yer almaktadır(Şekil 5.16).



Şekil 5.17. TİB tarafından erişimi engellenen internet sitesi sayısı[91]

Siber güvenliği sağlamak ve siber suçları azaltma adına her geçen yıl engellenen internet sitesi sayısı artarak devam etmesine rağmen etkili sonuçlar alınamaması,

siber suçların yasakçı bir zihniyet ile engellenemeyeceğinin en büyük göstergesidir(Şekil 5.17).

5.3. Siber Tehdit ve Saldırıların Değerlendirilmesi

Siber tehdit ve saldırıların teknik düzeyinin ve mobil cihazlardaki güvenlik açıklıklarının artmasının yanında devletlerin saldırı kabiliyetlerini geliştirdikleri günümüz siber uzayında uluslararası işbirliği sayesinde siber suç oranında düşmeler olduğu ve bilişim güvenliğinden sorumlu devlet kurumlarının siber yeteneklerinin arttığı gözlenmektedir. Tüm bu gelişmelerle tehdit ve zafiyetlerin tespit edilme hızı artarken

- Bilgi ve iletişim ürünlerindeki artış,
- Mali krizler,
- Yeni güvenlik açıkları ve zafiyetleri,
- Saldırı ve saldırıları gerçekleştirme de kullanılan yazılımların karmaşıklığı,
- Mevcut siber yetenekler ve
- Siber uzaydaki yasadışı kazanımların artması da tehditlerin değişiminde etkili olmuştur[65].

Bu bağlamda mobil cihazlar, big data (büyük veri) ve nesnelerin interneti tabir edilen alanlar üzerinde yoğunlaşan siber tehdit ve saldırılarla ilgili olarak aşağıda (Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı(ENISA) 2013 yılı Aralık ayı raporu ve tez kapsamında elde edilen(Bkz. 5.1) veriler incelendiğinde) bazı değerlendirmelerde bulunulmuştur:

a-) Kurumların ve şirketlerin büyüyen yapısı nedeniyle artan veri büyüklükleri ve çeşitlilikleri için big dataya (farklı büyüklük ve çeşitteki verilerin sayısının artmasıyla ilişkisel veritabanı modelleri ve sistemlerinin yeterli olmaması nedeniyle google, youtube, facebook v.b. büyük ölçekte verisi bulunan işletmelerin sahip olduğu veri işleme ve depolama teknolojisi) olan eğilimlerinin artması ve big data(büyük veri) teknolojisinin ağ üzerinde erişimi mümkün tüm verilere ulaşabilme yeteneği dolayısıyla trojan/solucan gibi kötücül yazılım tehdidine maruz kalabilme ihtimali siber tehditlerin bu alanda yoğunlaşma olasılığını arttırmaktadır.

b-) En yüksek siber tehdit sıralamasında zirveyi paylaşan izinsiz indirmeler ve solucan/trojan gibi kötücül yazılımlar, bireysel kullanıcılarla birlikte sosyal ağ sitelerini ve (birçok kurum ve şirketin hizmet aldığı) bulut bilişim alt yapılarını da tehdit etmektedir. Bir çok kurum ve şirketin kurumsal bilgi varlıklarının bulunduğu bulut yapısında yeterli güvenlik önlemlerinin alınmaması (ile birlikte bulut güvenliği ile ilgili güvenlik önlemlerinin saydam olmaması) sonucunda özellikle kimlik hırsızlığı, kod enjeksiyonu ve botnetlere dahil olma gibi tehditlerle kurumları karşı karşıya bırakmaktadır. Ayrıca solucan ve virüslerin başı çektiği kötücül yazılımların kodları üzerinde yapılan oynamalar sonucunda oluşturulan varyasyonların virüs tarama yazılımlarını atlatmadaki etkililiği, mobil cihazlardaki düşük güvenlik önlemleri ve kullanım artışının da etkisiyle kötücül yazılımların yayılımının diğer platformlardan daha etkili olması ve saldırganların (kötücül yazılımlarla elde ettikleri) kullanıcı bilgilerini satabilecekleri büyüyen bir pazar bulunması gibi durumlar kötücül yazılımların (mobil platformlar üzerinden kullanıcı bilgilerini ele geçirmeye yönelik) kodlanmasını artırması beklenmektedir[65].

c-) Nesnelerin interneti diye bahsedilen kavram günlük hayatta kullanılmakta olan akıllı aletlerin oluşturduğu bir sistem olarak düşünülmelidir. Örnek olarak iş dönüşü eve gelmeden 40 dakika önce ısıtma sisteminin devreye girerek evi ısıtması, sahibinin cep telefonuna kaydettiği sabah uyanma saatine göre sıcak suyu ısıtacak sistemin 20 dakika önceden aktif hale geçip suyu ısıtması gibi işlemleri gerçekleştirebilen aletler gösterilebilir. Bu tür sistemlerdeki verilerin elde edilmesiyle kişiler hakkında profillemeye yapma imkanı da veren bu tür cihazlar genelde düşük güvenlik seviyesinde olmaları ve donanım yapılarının basitliği gibi sebeplerden ötürü çeşitli saldırılara maruz kalabilmektedirler. Örneğin Wi-fi üzerinden veri aktarımı sağlanarak yapılan bahçe sulama sisteminin zayıflığı kullanılarak evdeki kablolu ağa sızma mümkün olabilmektedir. Bu durum sadece evdeki sistemler için değil hastane, fabrika gibi ortamlardaki otomasyon sistemleri için de benzeri bir planlı saldırı öngörülebilmektedir(Ülkemizdeki teknolojik yapıyla şu an bu durum pek mümkün görünmese de ilerleyen teknolojinin sunacağı yeniliklere ayak uydurma her kurum ve şirket için artı bir değer sağlayacaktır).

d-) Çeşitli sosyal mühendislik uygulamaları ve özellikle mobil cihazlara yönelik kötücül uygulama yazılımları ile hedef kullanıcılara yaklaşılan sazan avlama tekniklerinin son kullanıcılar tarafından fark edilmesi oldukça zor olacak şekilde karmaşık bir yapıya bürünmesi, phishing saldırganlarının hedefledikleri kurumların çeşitli birimlerindeki güvenlik sorumlularını kandırabilmek için taktikler geliştirmesi ve sazan avlama saldırılarının coğrafi alanların kültürel, sosyal ve teknolojik gelişimlerine göre planlanmaları bu tehdite karşı (özellikle kurumsal kullanıcılarda) siber farkındalık oluşturulmasının ne kadar önemli olduğunu ortaya koymaktadır. 2013 yılında sazan avlama yöntemiyle (e-postalar, manipüle edilmiş web sayfaları, mobil uygulamaları ve sosyal medya aracılığıyla) kimlik bilgilerinin çalınmasının devam etmesi özellikle web uygulama güvenliğinin sağlanmasında uygulanacak prosedürlerin önemini ortaya koymaktadır[86].

e-) Gelişen teknolojiye uyarlanarak etkinliği daha da artan hizmet aksattırma saldırılarının karmaşıklığının artması sonucunda bu saldırılara karşı yapılan savunmanın zorlaşması, bu tür saldırılarda esneklik, gizli iletişim, şifreleme gibi faktörlerin kullanımının saldırı süresinin artmasına imkân vermesi ve özellikle kurum ve şirketleri hedef alan DoS saldırılarının ABD ve Asya ülkelerinde Avrupa ülkelerine oranla daha çok olması gibi faktörlerin varlığı ülkemiz siber güvenliğinin (bu tür tehditlere karşı korunabilmesi için özellikle teknik boyutta) yeni ve sürdürülebilir siber güvenlik çözümlerine olan ihtiyacını ortaya koymaktadır.

f-) Veri ihlalleri anlık mesajlaşmalar, e-posta trafiği ve dosya transferleri aracılığıyla (kontROLSÜZ ve denetimsiz bir şekilde) yapılan veri iletimleri nedeniyle artmıştır. Dahası kurum dışında çalışan iş ortakları ve müşteriler ile kurum arasında yapılan hassas veri aktarımları da bu ihlalleri arttırmaktadır. Dolandırıcılık için (kötücül yazılımlar tarafından) küçük işletmeler hedeflenirken, büyük işletmeler bilgi toplamak amaçlı hedeflenmektedir. Çünkü büyük işletmeler veri ihlalleri ve bilgi sızıntısına karşı daha sağlam güvenlik önlemlerine sahip olmaktadır. Bir kurumun oluşabilecek tüm veri sızma olayları için oluşturabileceği tek bir çözüm noktası mümkün olabilmektedir. Kurum ve şirketlerin veri sızmaları ile baş edebilmek için sınır güvenlik çözümlerini genişletmeleri, yerel ve ulusal çaptaki organizasyonlar tarafından veri güvenliğine yönelik yapılmış (Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and

Accountability Act (HIPAA) v.b.) güvenlik standartlarıyla güvenlik çözümlerini uyumlu hale getirmeleri de gerekmektedir[66].

g-) Gelişmişlik, gizlilik ve karmaşıklık gibi özellikleri barındıran ve genelde siber espionaj amaçlı geliştirilen belirli hedeflere yönelik saldırıların(ATP) etkilerinin beklenenin çok ötesinde olması ve bu tür siber silahlara karşı tam anlamıyla bir güvenlik olgusundan söz etmenin mümkün olmaması nedeniyle bu tip siber saldırılardan korunmak için öncelikle kurumsal bilgi varlıklarının (kurumdaki personelden teknik altyapıya kadar) bir bütünlük içinde ele alınıp aşağıdaki gibi temel güvenlik önlemlerinin yerine getirilmesi gerekmektedir.

- Saldırıları için hazırlıklı olmalı,
- Sistemlerin sıkılaştırılmalı,
- Güçlü şifre politikaları belirlemeli,
- Personel eğitimine önem verilmeli,
- Kritik sistemlerin internetten izole edilmesi sağlanmalıdır[3].

h-) 2012 yılında tanımlandığı halde hedeflenen birçok yüksek teknolojiye sahip şirketle birlikte devlet kurumlarına başarılı saldırıların yapıldığı watering hole yöntemi, şu an için düşük sayıda olsa da bu tehdidin etkinliği ve diğer saldırı yöntemleri ile birleştirilebilme özelliği dolayısıyla ilerleyen dönemlerde artarak daha kompleks bir hale dönüşmesi ve bunun sonucunda da kurumsal siber güvenliğe vereceği zararın boyutlarının büyümesi beklenmektedir.

i-) Ticari işlemlere erişim sağlamak için saldırganların kullanıcı bilgilerini kazanması ve oturumu ele geçirmesi şeklinde ifade edilen kimlik doğrulama ve oturum yönetimi ihlallerinin başarısı için (farklı kaynaklar üzerinde depolanan verilere erişim için kolaylık sağlayacak) ağ yapısı hakkında toplanabilecek bilgiler önemlidir. Özellikle finans kurumlarına ilişkin verilerin değer kazandığı kimlik hırsızlığında mobil cihazlar için üretilmiş zararlı yazılımlarla yapılan atakların etkili olması ve sosyal medyanın önemli bir kaynak oluşturması, bu tehdidi önümüzdeki dönemlerde arttırarak daha sofistike bir hale dönüştürmesi beklenmektedir[65].

j-) Kod çalıştırma tehditlerine ilişkin önemli bir husus; içerik yönetim sistemlerinin çok fazla kullanımının (kod çalıştırma yöntemiyle yapılabilecek

saldırıları için etkin bir ortam sunmasından dolayı) saldırganların dikkatini bu yöne çekmiş olmasıdır. Bulut servis sağlayıcı ağları içinden geniş çapta (artarak) gerçekleştirilen kod çalıştırma tehditlerinin diğer tehditlerle beraber başarılı bir şekilde uygulanabilme ihtimalini de saldırganların dikkatini bu yöne çeken başka bir husus olarak değerlendirmek mümkündür. Örneğin, watering hole (popüler adresler üzerinden yapılan) saldırılarının SQL enjeksiyonla birlikte gerçekleştirilmesi gibi.

k-) Günümüzde exploit geliştiricilerin ürettikleri exploitlerle ilgili özelleştirilmiş ayarlamalar yapabilmesi ve teknik destek sağlayarak müşterileri ile etkileşim içerisinde olması gibi temel faktörlerin etkisiyle istismar kodlarının (siber tehditler arasında) etkinliğini artırması ve bilgi ve iletişim sistemleri üzerinde yapılan dolandırıcılık faaliyetlerinde de kullanılabilen botnetlerin en önemli siber tehditler arasında yer almaya devam etmesi bu iki tehdide karşı kurumlararası işbirliğinin sağlanarak hızlı ve etkili bir siber tehdit tespiti ve analizi yapılmasını gerektirmektedir.

l-) Günümüzde (teknik düzeyi yüksek) mevcut uygulama ve yazılımları kullanarak düşük düzeyde bilgi birikimi ile siber saldırıların gerçekleştirilebileceği görülmektedir ki; bu durumda saldırı sayısının artması ve buna bağlı olarak hem kurum ve şirketlere hem de bireylere verilebilecek zararların da artması normal karşılanmalıdır.

5.3.1. Siber tehdit ve saldırıların kurumsal siber güvenlik yönünden değerlendirilmesi

Ülkemizde internetin giderek artan altyapısıyla birlikte kurum ve şirketlerin hizmet sunumlarını gerçekleştirdikleri artı bir değer olmaktan ziyade bir zorunluluk haline gelmeye başladığı görülmektedir. İş ya da günlük hayatın bir parçası haline gelen siber ortamdaki uygulamaların artması, elektronik ortamda giderek artan ve ihtiyaç duyulan bilgi ve dosyaların ağ yapıları üzerinden paylaşımı, zaman ve mekândan bağımsız bir şekilde bilgi ve hizmetlere erişilebilirlik imkânları siber ortamların kullanımını daha da cazip hale getirmektedir. Gerek kamu gerekse özel sektörde birçok kurumun hizmet sunumlarını siber ortamda gerçekleştirmesiyle saldırıların arttığı, yapılan bu saldırılar için gerekli bilgi ve araçların kolaylıkla temin

edilebildiği, dünyanın herhangi bir yerindeki sistemlerin bu saldırılara bilerek veya bilmeden iştirak ettiği ve bu gelişmiş ve organize saldırıların kimler tarafından finanse edildiğinin tespit edilmesinin neredeyse imkânsız hale geldiği bu noktada güvenlik faaliyetleri ön plana çıkmaktadır. Ancak buna rağmen siber güvenlik kavramının kurumlar tarafından yeterince ve doğru anlaşılamadığı yapılan birçok bildiri ve araştırmada da vurgulanmaktadır[6]. ISC TURKEY 2012 sonuç bildirgesinde de belirtildiği gibi kurumların %61'inin kendilerini siber saldırıların hedefinde görmesine rağmen yeterli ve etkin bir siber güvenliğe sahip olmadıkları anlaşılmaktadır. Siber tehditlere yönelik çalışmalar çoğunlukla ulusal veya uluslararası boyutta ele alınmakta ve üretilen politika ve standartlarda bu boyutta olmaktadır. Ancak bu seviyede devam eden bütüncül bir yaklaşımdan ziyade bütünü oluşturan (özellikle de kritik alt yapılara sahip kurumların içinde olduğu) parçaların siber güvenliğinin sağlanması, bütünü daha sağlam ve etkin kılacaktır. “Bir zincirin kuvveti zinciri oluşturan en zayıf halkanın kuvveti kadardır” prensibinden yola çıkılacak olunduğunda, (özellikle kritik alt yapılardaki) kurumsal bazda siber güvenliğin ulusal siber güvenlik adına ifade ettiği anlam kendiliğinden ortaya çıkmaktadır.

Boyutuna bakılmaksızın tüm kurum ve şirketlerin siber güvenlikleri için önemli bir risk haline gelen siber tehditlerle ilgili her kurum ve şirketin (başta ağ yapısı ile ilgili olmak üzere) kurumsal güvenliklerine ilişkin gerekli tedbirleri alması gerekmektedir. Ayrıca çeşitli meslek gruplarına göre bilgisayar ve internet kullanma oranlarının farklılaştığı ülkemizde (Bkz. Şekil 5.13) siber suçluların; hedefledikleri kurumlardaki çalışanların internet alışkanlıklarını irdeleyerek elde ettikleri verilere göre çeşitli saldırılar gerçekleştirmeleri, saldırının etkisini ve kurumsal siber güvenliğe verdiği zararı arttırmaktadır. Bilgisayar ve internet kullanma oranı nispeten daha yüksek olan kurum ve şirketlerdeki personelin farkındalığının artırılması ve buralardaki siber güvenlikten sorumlu personellerin daha etkili çözüm önerileri geliştirip uygulamaları gerekmektedir. Ayrıca kötücül yazılım bulaştırarak kurumsal siber güvenliğe zarar vermek isteyen siber suçlular, sosyal ağların ve çevrimiçi video uygulamalarının personellerin işteki zaman geçirme alışkanlıklarını etkilemelerinden faydalanarak yeni güvenlik zafiyetlerinin oluşmasını sağlayabilmektedirler.

Siber ortamda sayıları her geçen gün daha da artan saldırı ve tehditleri bertaraf etmek, kurumsal olarak hizmet sunulan kitlenin memnuniyeti ve kaliteli hizmet anlayışı açısından önem arz etmektedir. Siber ortamda sunulan hizmet ve ürünlerin etkin, kaliteli ve uygun maliyetli olmasının yanında güvenliğin de tesisi önemlidir. Bu bağlamda yapılan görüşme de “Kurumsal siber güvenliği sağlama adına kurumsal bazda yapılabilecekler nelerdir?” sorusuna karşılık bir uzmanın vermiş olduğu:

“...Bir kurum veya şirket için güvenlikten tasarruf edilemeyeceği gibi güvenlik endişesiyle sistem verimliliğini sağlayacak alt yapıların kullanımından da vazgeçilemez.” ifadesi ile yine bir başka uzmanın:

“...Kurumların kendi içlerinde veya aralarında bir ar-ge çalışması yürütmemeleri ve bunun devletçe desteklenmemesi sonucu oluşacak dışa bağımlılık, ulusal güvenlik adına tehditler oluşmasına yol açabilmektedir.”

şeklinde belirttiği görüş; güvenlik ile kullanılabilirlik arasındaki dengeyi ve kurumsal siber güvenliğin ulusal güvenliğe olan etkisini açıklayıcı niteliktedir. Ek olarak, (verilen cevaplar doğrultusunda) atılması gereken adımlar da şu şekilde belirlenmiştir:

- 1- Kurumsal siber güvenliğin sağlanması hususunda hem kurumun departmanlarının görev, yetki ve sorumluluklarını belirleyen hem de ihtiyaç duyulan noktalarda eksiklikleri gidermek amacıyla yönetmelik oluşturulmalıdır. Yönetmelikte geçen kavramların net anlaşılması maksadıyla teknik terimler açıklamalı olarak verilmelidir.
- 2- Saldırıların neticesinde hukuki olarak netice alabilmek için siber saldırıların kaynağının tespit edilmesi hangi boyutta bir etki oluştuğunun bilinmesi gerekmektedir. Bu nedenle zamanın teknolojisine uygun olarak güvenilir ve yeterli kayıt mekanizmaları kullanılmalıdır.
- 3- Siber ortamda oluşan tehditlerin hızla belirlenmesi, yaşanabilecek saldırı etkilerini azaltmaya veya ortadan kaldırmaya yönelik tedbirlerin alınması için siber güvenlik birimi oluşturularak kurumun saldırı ve tehditlere müdahale yeteneği kazanması sağlanmalıdır. Ayrıca kurum veya şirketin

ürün veya hizmet sunduğu sektörel çeşitliliğe bağlı olarak siber güvenlik birimine bağlı alt birimler kurulmalıdır.

- 4- Kritik bilgi ve iletişim sistem altyapıları başta olmak üzere departman bazında siber güvenliğin sağlanması adına çalışmalar yapılmalıdır.
- 5- Asıl mesele kritik bilgi ve iletişim sistem altyapılarına sızma ve keşif, veritabanlarını ele geçirme gibi saldırılar olduğundan, özellikle bu hususlarda kapsamlı bir risk değerlendirilmesi yapılması gerekmektedir.
- 6- Gerek ulusal gerekse uluslararası boyutta siber güvenlikle ilgili eylem planları, bildiriler ve konferanslar yakından takip edilerek edinilen bilgilerin kurumun siber güvenliğine uyarlanmasına çalışılmalıdır.
- 7- Özellikle kurumun kritik bilgi ve iletişim sistem altyapılarına ait bilişim sistemlerinin güvenliğini sağlamak amacıyla oluşturulacak siber güvenlik eylem planının güncel gelişmeler doğrultusunda belirli periyotlarla güncellenmesi sağlanmalıdır.
- 8- Eylem planı ile ilgili olarak şirketin tüm departmanlarında (bilinmesi gereken kadar prensibince) gerekli bilgilendirmeler sağlanmalıdır.
- 9- Kurum olarak bilgi güvenliğine yönelik gerekli politikalar belirlenerek standartlar oluşturmalı ve bu konuda yönetmelik hazırlanarak personele tebliğ edilip farkındalık oluşturulmalıdır. Bu politikaları belirleme de kurum alt birimlerinde de kurullar oluşturularak onların destek ve önerilerinin alınması, belirlenen politikaların benimsenmesinde etkili olacaktır. Ayrıca belirlenen bu politika ve yönetmeliklerin uygulanıp uygulanmadığı kurumun siber güvenlik birimince denetlenmelidir.
- 10-Ulusal ve uluslararası hukuk kuralları çerçevesinde kurumun haklarını korumak için herhangi bir saldırı durumunda saldırının kaynağının tespiti ve etki boyutunu ortaya koyacak saldırı tespit sistemleri ve güvenilir kayıt

mekanizmaları oluşturularak günün teknolojisine uygun olarak güncellemeleri yapılmalıdır.

11-Kurumsal siber güvenlik birimine (KSGB) bağlı olarak görev yapmak üzere 7/24 esasına göre oluşturulacak kurumsal siber olaylara müdahale biriminin(KSOM), gerek diğer kurumların siber güvenlikten sorumlu birimleriyle gerekse ulusal boyutta siber güvenlik hususunda çalışma yapan birimlerle yakın işbirliği içinde olmaları sağlanmalıdır. Siber olaylara müdahale biriminde bulunan kişiler güncel gelişmeler doğrultusunda hizmet içi eğitim veya kurslarla en son gelişmelere adapte olacak şekilde yetiştirmeleri sağlanmalıdır.

12-Kurumun kritik bilgi ve iletişim sistem altyapılarındaki bilişim sistemlerinin, kritiklik seviyeleri, birbirleriyle ilişkileri ve sorumluları belirlenmelidir. Ayrıca bu kritik bilgi ve iletişim sistem altyapılarının güvenliği idari tedbirlerle de desteklenmelidir.

13-Kurumsal siber güvenliği sağlama konusunda departmanların farkındalık ve yetkinlik düzeyini artırıcı teknolojik ve idari boyutta destek verilmelidir.

14-Siber güvenlik sadece teknik bir konu olarak ele alınmamalı, kurumu etkileyecek tüm sosyal ve ekonomik yönleriyle değerlendirilmelidir. Kurum içinde belirli zamanlarda “siber güvenlik farkındalık haftası” gibi etkinlikler doğrultusunda konuyla ilgili çalışmalar yürütülmelidir.

Tüm bu sayılan maddelere ilaveten önceki bölümlerde belirtilen (Bkz. Üçüncü bölüm) gerekli korunma tedbirleri yerine getirilerek, bu önlemlerin etkinliğini ölçmek ve uygun güvenlik çözümleri geliştirmek amacıyla belli periyotlarla uzman kurumlara penetrasyon testleri de yaptırılmalıdır. Ayrıca, Siber güvenlik alanında isim yapmış güvenilir bir kaynak olan ENISA adlı kuruluşun (2013 Aralık raporunda) belirttiği bazı değerlendirmeler de kurumsal siber güvenliği sağlamaya yardımcı olacak niteliktedir:

- Siber tehditlere karşı savunma da son kullanıcılar da aktif olarak dahil edilmeli. Son kullanıcılar tarafından alınabilecek temel ve basit güvenlik

önlemleri sonunda siber olaylar dünya çapında yarıya inebilir.

- Kurumlar işbirliği yaparak ortaya çıkan tehditlerle ilgili bilgi paylaşımında bulunmalı, yardımcı olmalı... Kurumlar arasında ortak bir bilgi toplama, analizi, değerlendirimi ve doğrulamasının yapılması gereklidir. Bu şekilde güvenlik kalitesi ve tehdit değerlendirme hızı artacaktır. Kamu ve özel sektörün bir arada bulunduğu çalışmaların yapılması bu tür tehditlere karşı daha etkili güvenlik mekanizmalarının oluşturulmasını sağlar.
- Tehdidin sebebiyet vereceği etkiyi azaltmak için tehdit değerlendirme hızı arttırılmalı. Ortaya çıkan tehditler hakkında sağlıklı bilgi elde etmek ve bu tehditlere yönelik güvenlik çözümleri geliştirmek maksadıyla yapılacak faaliyetlerle ilgili birimler kurulması ve geliştirilmesi önemlidir. Hayati öneme sahip tehdit değerlendirme hızının artışı için kurum ve şirketlerin oluşturacağı sinerji ve bu sinerjinin eylemlere yansması gereklidir.
- Teknolojinin ilerlemesiyle beraber saldırılardaki karmaşıklığın artmasından dolayı güvenlik mekanizmalarının daha sağlam olması için geliştirilmesi, ek tedbirler alınması gerekirken bilginin gizliliği, erişilebilirliği ve bütünlüğüne ilişkin alınan önlemlerin de kurumsal işleyişin verimliliğini azaltmayacak şekilde esnek olması gerekmektedir.
- Güvenlik kontrol ve politikaları geliştirmek için yapılan araştırmalara yönelik yatırım yapılmalıdır.

Kurumsal siber güvenlik açısından bakıldığında özellikle % 75 gibi yüksek bir orana sahip ticari içerikli web sitelerinin tehditlere açık olduğu görülmektedir. Ayrıca günümüzde kurumların, siber güvenlik anlamında ağ güvenliğini dikkate alırken özellikle web uygulama yazılımları (özellikle ASP ve PHP gibi veritabanı sağlayan uygulama kodlarına sahip web sitelerindeki yazılımların[75]) güvenliği hususunda eksiklikleri bulunmaktadır[13]. Bu bağlamda kurumların internet ortamından gelebilecek tehlikelere karşı (ilave) uygulayabilecekleri maddeleri de:

- Web uygulamalarına yönelik çalışmalarıyla bilinen OWASP' ın Güvenli Kodlama İlkeleri belgesi, Güvenli Web Uygulamaları Geliştirme Kılavuzu belgesi kurum içi eğitimlerde kullanılarak yazılım geliştiricilerin bu esaslara uyup uymadıkları denetlenmelidir.

- İnternet üzerinden gerçekleştirilen etkinlikler (kurumsal ağ üzerinde) sürekli olarak izlenmelidir. Bunun için kullanılan en etkin yöntem, basit ağ yönetim protokolü (SNMP) araçlarının kullanılmasıdır.
- Web sistemleri dönemsel olarak sınaama araçları ile taranmalı ve sınamaya ilişkin rapor teknik sorumlulara ulaştırılmalıdır.
- Kurumsal ağların, web güvenliği altyapıları için kılavuzları ve standartları bulunması gerekmektedir.
- Saldırganların sistemde yapabilecekleri değişikliklerin takibi açısından (Tripwire ve benzeri programlarla) kritik sistem dosyalarında yaşanan değişimler izlenmelidir.
- Sunucu günlükleri (log), sunucu makineleri üzerindeki web sunucu yazılımı ve web uygulama güvenlik duvarı gibi çeşitli sistemlerin günlük içeriklerini içeren sunucu günlükleri (log) tutulmalıdır.

şeklinde sıralamak mümkündür[64].

5.3.2. Siber tehdit ve saldırılarla mücadele adına yapılanların değerlendirilmesi

Siber tehdit ve saldırılarla mücadele için gerçekleştirilmesi gereken etkili ve sağlam bir siber güvenlik adına (dünyada uygulanmış başarılı örnekler çerçevesinde) Türkiye'nin yerine getirebileceği bazı düzenlemeleri:

- Türkiye' de Hindistan' dakine benzer kamu-özel işbirliğini sağlayan ulusal güvenlik veritabanı kurularak siber güvenlik konusunda uzman kişilerin envanterinin çıkartılması sonucunda her bir uzmanın yeteneklerinden yararlanılmalıdır.
- (ABD'deki gibi) EINSTEIN benzeri bir program ulusal siber güvenlik biriminin yetkisine verilerek ulusal çapta bir saldırı olduğu takdirde ilgili tüm kurum ve kuruluşlar arasında koordinasyon sağlanmalıdır.
- Almanya' daki Ekonomi ve Teknoloji Federal Bakanlığı'nın (sanayinin katılımı ile) IT güvenliği konusunda oluşturduğu görev kuvvetine benzer bir yapı oluşturularak vatandaşlar ve KOBİ tarafından kullanılan IT sistemleri için daha güvenli altyapıların oluşturulması sağlanmalıdır.

- Çin’ de olduğu gibi kamu-özel sektör birlikteliğiyle sadece siber güvenlik üzerinde odaklanan ve teknoloji üreten AR-GE merkezleri oluşturularak devlet tarafından gerekli destek sağlanmalıdır.
- USOM(Ulusal Siber Olaylara Müdahale Birimi) ile özellikle kritik alt yapılardaki işletmeler ve ilgili devlet kurumları dirsek temasında olacak şekilde gerçekleştirilebilecek ulusal çapta bir siber saldırı ve tehdide karşı koyması sağlanmalıdır.
- Hukuki düzenlemelerin siber suçları cezalandırıcı ve caydırıcı hale getirmesi için gerekli gözden geçirme ve güncellemelerin yapılması gereklidir. Uluslararası bir işbirliği yapılmalı, siber güvenlik uzmanları yetiştiren programlar açabilmek için lisansüstü programlar geliştirilmeli ve siber güvenlik alanında araştırma yapacak merkezler kurulmalıdır.
- ENISA’ nın yürüttüğü siber güvenlik çalışmalarını takip etmeli ve AB’nin CERT projesiyle süreçleri en azından gözlemci seviyesinde takip edip tecrübe artırımı sağlanmalıdır.
- Milli Güvenlik Kurulu (ordu–ilgili kamu kurumları-hükümet) benzeri bir siber güvenlik organı oluşturulmalı ve düzenli aralıklarla toplanıp Dünya’ da ve ülkedeki siber tehdit durumuna göre alınacak önlemlerin belirlenmesi sağlanmalıdır.

şeklinde sıralamak mümkündür[4]. Tüm bu yukarıda belirtilenlerin dışında, ulusal çapta yapılan düzenleme ve faaliyetlerde eksik görülen hususlar ve bunlara karşı yapılması gerekenler ile ulusal seviyede etkin bir siber güvenliğin oluşturulması adına yapılabilecekler 20-21 Eylül 2013 tarihinde yapılan 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı’nda şu şekilde ifade edilmiştir:

- Türkiye’nin siber güvenlik eylem planı mühendislik ağırlıklı yapıldığından sosyal yanları biraz eksik kalmıştır. Eylem planının, güvenliği sağlarken iş süreçlerini de aksatmaması adına kritik alt yapılar ve internet altyapılarında çalışan uzmanların da katkıları olmalıydı. Özellikle kritik alt yapılarla ilgili uzman tavsiyelerinin alınması bu yapılarda herhangi olumsuz bir durumun oluşması ihtimalini minimuma indirmiş olurdu. Bundan başka STK (Sivil Toplum Kuruluşları) ve özel kuruluşların katılımı da fayda sağlayacaktır.

- Eylem planı kısa vadeli yapılmıştır, orta ve uzun vadeli olmak üzere 2 adet plan daha yapılmalıdır. Ayrıca siber tehditler sürekli olarak değiştiğinden bu planlar da belli periyotlarla güncellenmelidir.
- Zombi bilgisayarların fazla olması ülkemizden yapılan saldırıların fazla olmasına neden olmaktadır. Oluşturulacak (siber güvenlik alanındaki) bir ekosistem sayesinde hem ülkemizden yapılabilecek saldırı oranı düşürülmüş olur hem de daha verimli ve etkin çalışmaların yapılmasına zemin hazırlanarak siber güvenlikte proaktif bir yapı tesis edilmiş olur.(Bu noktada devlet tarafından yerli teknolojilerin gelişiminin ve teşvikinin yapılması önemlidir).
- Siber güvenlikle ilgili hukuki bir altyapı oluşturmalı. Böylece bu konuda vatandaş olarak, kamu ya da özel kuruluş olarak yapılması gerekenler belirlenmelidir.
- Siber güvenliği sağlama da bütüncül bir önlem almak önemlidir. Yani tek bir kurum değil ilgili tüm kurumların siber güvenliği önemlidir.

5.4. Siber Suçların Değerlendirilmesi

Uluslararası alanda yapılan savaşların platform değiştirerek siber ortama doğru kaydığı günümüzde gelişmiş devletlerin siber güvenlikle ilgili gerekli önlemleri almaları bir zorunluluk haline gelmektedir. Birçok devlet siber güvenliğini koruyarak ekonomik kalkınma ve gelişmeyi amaçlamakta ve bu yönde yatırımlar yapmaktadır. Ayrıca bir kurumun medyadaki haber değeri, konumu ve müşteri kitlesi gibi çeşitli faktörleri göz önüne alarak belli bir kurum ve şirketi hedefleyen siber suçlularla mücadelenin sadece ulusal bazda değil kurumsal bazda da yapılması gerektiği anlaşılmaktadır.

Kötü niyetli (çok basit düzeyde bilgisayar kullanma düzeyine sahip olsa bile) birçok kişi siber ortamda bulabileceği ucuz ve kolay erişilebilir uygulamalarla zarar verici saldırılarda bulunabilmekte ve bu tür kimselerin de siber uzayda izlerini sürmek kolay olamamaktadır. Bununla birlikte dünya nüfusunun çoğunun siber ortamdaki uygulamaları kullanıyor olması, hukuksal bütünlüğün ve uluslararası işbirliğinin eksikliği, küresel bağlanabilirlik, teknolojiye bağımlılık, hukuksal açıklıkların bulunması ve ucuz maliyet gibi nedenler de siber suç işleme oranını

arttırmaktadır. Artan bu siber suç olgusuna karşı ulusal, uluslararası ve kurumsal bazda topyekûn mücadele edilmesi daha etkin ve verimli bir güvenlik sunacaktır.

Bilişim sistemlerine yönelik ve müstehcenlik ile ilgili suçlarda alınan önlemler etkisini gösterirken banka ve kredi kartı suçlarına ilişkin önlemlerin daha da artırılarak farkındalık çalışmaları yapılması gerekmektedir. Ayrıca siber suçlarla mücadelede bölge bazında değerlendirmelerle nokta tespitler yapılması daha etkin ve verimli neticeler alınmasını sağlayacaktır. Dikkat edilmesi gereken bir husus; siber suçlarla mücadelede uygulanan erişim engellemelerinin yasakçı bir zihniyet içinde gerçekleştirilmesi, girişimci ve özgür bireylerin yetişmesine engel olarak ülkenin kalkınmasına olumsuz etkide bulunacağı, uygulanacak sınırlamalarında toplum değerleri ve hukuki boyut ele alınarak değerlendirilmesi gerektiğidir.

Siber suçlara yönelik hukuki düzenlemelerle ilgili olarak; ülkelerin siber suçlarla ilgili olarak birbirinden bağımsız ve farklı uygulamalar geliştirmeleri siber suçlarla mücadelede etkinliği azaltmaktadır. Devletlere göre değişen siber suçlarla ilgili algılamalar her ne kadar bilişim dünyasının sınırlandırılması ve düzenlenmesinde farklılıklar gösterse de ortak kararlar alınıp uygulanması adına engel teşkil etmektedir. Bu ortak karar birliği asgari müştereklerde anlaşarak sağlanabilirse başlangıç için küçük ama etkili bir adım olacaktır. Temel hak ve özgürlükler korunarak suçun engellendiği bir yapının sağlanması için uygun politikalar üretilip toplumun bilinçlendirilmesi gerekmektedir. Ayrıca bu tür suçlara yönelik (bilişim mahkemeleri gibi) özel ihtisas mahkemeleri kurulması (en azından gerekli alt yapı çalışmalarının yapılması) ileriki dönemlerde karşılaşılabilecek siber suçlarla ilgili daha etkili sonuçların alınmasını sağlayacaktır.

6. KURUMSAL SİBER GÜVENLİK EYLEM PLANI

Eskiden sistemlere yapılan saldırılar daha çok sistemlerdeki bilgiye sızıp yeteneklerini göstermek isteyenlerin bireysel faaliyetleri iken artık belirli hedeflere daha organize ve karmaşık bir yapıda saldırılar düzenlenerek kurum ve şirketlere maddi zararlar verme ya da bu kurum ve şirketlerden elde ettikleri bilgilerle kazanç sağlamaya yönelik ekonomik amaçlar güdülmektedir. Bu tür saldırılara maruz kalan kurum ve kuruluşların maddi yönden zarara uğramalarına kıyasla müşteri, itibar ve pazar kaybı gibi uğradıkları zararlar çok daha ciddi boyutta olmaktadır. Bu nedenle çeşitli şekillerde siber ortamda hizmet sunan kurumların bu tür saldırılar gerçekleşmeden öncesinde, saldırı esnasında ve de saldırı sonrası oluşabilecek durumlara hazırlıklı olmaları için kendilerine ait bir *kurumsal siber güvenlik eylem planı* oluşturmaları gerekmektedir.

Günümüzde maalesef siber güvenlik kavramı, kurumlar tarafından yeterince ve doğru anlaşılamadığı yapılan birçok bildiri ve araştırmada da vurgulanmaktadır. ISC TURKEY 2012 sonuç bildirgesinde de belirtildiği gibi kurumların %61'inin kendilerini siber saldırıların hedefinde gördüğü bir ortamda *siber güvenlik eylem planı* oluşturma zorunluluğu doğmaktadır.

Yapılan görüşmelerde “Kurumsal siber güvenlik eylem planı oluşturma kurumlara sağlayacağı faydalar nelerdir?” şeklindeki soruya katılımcıların belirtmiş olduğu cevaplar değerlendirildiğinde eylem planının amacıyla ilgili olarak; “*Kurumun siber güvenlik ihtiyaçlarının ortaya konulması, kavramların ve adımların tarif edilmesi, hedeflerin doğru belirlenebilmesi, hedeflere uygun sistematik ve beklenen amaca yönelik adımların atılabilmesi, atılmış adımların denetimi, izlenmesi ve iyileştirilmesi gibi faydaları bulunmaktadır.*” şeklinde bir sonuç ortaya çıkmaktadır. Aynı görüşmelerde “Kurumsal siber güvenlik eylem planı oluşturma amacını belirtiniz” sorusuyla ilgili katılımcı görüşleri ortak bir çizgi etrafında birleştirildiğinde “*kurumun departmanlarınca ağ ve bilgi teknolojileri üzerinden sağlanan her türlü işlem ve verinin sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına, kurumun kritik bilgi ve iletişim sistem altyapılarına ait bilişim sistemlerinin güvenliği, yapılan herhangi bir saldırı neticesinde etkinin en düşük düzeyde kalmasına ve saldırı sonrasında sistemlerin en kısa sürede normale dönmesine yönelik çalışmaların belirlenmesine ve oluşan suçun adli*

makamlarca daha etkin soruşturulmasına yönelik zemin oluşturmaktır.” Şeklinde ortaya çıkan görüş; kurumlar tarafından işletilen kritik bilgi ve iletişim sistem altyapılarına ait bilişim sistemlerini kapsayan eylem planının amacını ortaya koymaktadır.

Tez çalışması esnasında eylem planının hazırlanmasıyla ilgili olarak görüş ve önerilerine başvuru uzmanların değerlendirmeleri çerçevesinde kurumsal siber güvenlik eylem planı oluşturulma sürecinden önce atılması gereken adımlar maddeler halinde sunulmaktadır.

6.1. Kurumsal Siber Güvenliğin Sağlanmasında Dikkat Edilmesi Gereken İlkelerin Belirlenmesi

Kurum çalışanlarının ortak anlayışının temelini oluşturacak ve kurumsal bazda siber güvenlikle ilgili çalışmalara yön verecek ilkeleri belirlemek maksadıyla katılımcılara sorulan “Kurumsal siber güvenliğin sağlanmasında size göre dikkat edilmesi gereken ilkeler nelerdir?” şeklindeki soruya katılımcıların ifade etmiş olduğu cevaplar derlenerek aşağıda maddeler halinde sunulmuştur. Bu soru çerçevesinde bir katılımcının belirtmiş olduğu “... *bu ilkelerin çalışanlar tarafından benimsenmesi ve tatbik edilmesi için belgelendirilme yapılmalıdır.*” şeklindeki ifadesi ilkelerin hayata geçirilmesi adına önemli görülmektedir.

Verilen cevaplar neticesinde belirlenen (kurumsal ihtiyaçlara göre özelleştirilebilecek) ilkeler:

- Siber güvenlik, risk yönetimi esaslı, etkin ve sürekli iyileştirmelere dayalı metotlar aracılığıyla sağlanır.
- Siber güvenlik için teknik boyutun yanında idari, ekonomik ve sosyal boyutlarda güçlü ve zayıf yönlerin, tehditlerin ve fırsatların belirlenmesini içeren bütüncül bir yaklaşım benimsenir.
- Risk yönetiminde teknik zaafaların giderilmesi ve saldırıların önlenmesiyle muhtemel zararın en aza indirgenmesi esas alınır.
- Siber güvenliğin sağlanmasında kurumun departmanları ve çalışanlarınca tüm hukuki ve sosyal sorumlulukların yerine getirilmesi esas alınır.

- Kritik bilgi ve iletişim sistem altyapıları güvenliğinin sağlanmasında kurumun tüm departmanlarının karar mekanizmalarına katılımını içeren bir işbirliği yapılır.
- Kurumsal siber güvenliğin sağlanması ve sürdürülmesinde kurum içi işbirliğinin yanı sıra ulusal ya da uluslararası diğer kurum ve şirketlerle de bilgi paylaşımı esas kabul edilir.
- Diğer kurum ve şirketlerle işbirliği ve bilgi paylaşımı için teknik iletişim kanallarıyla beraber gerektiğinde sosyal, ekonomik ve diğer kanalların da etkin ve sürekli kullanımı esas alınır.
- Kurumsal siber güvenlik için ihtiyaç duyulan yönetmelik geliştirilirken ulusal ve uluslar arası anlaşma ve düzenlemeler de göz önüne alınır.
- Kişilerin özel hayatlarının gizliliği ilkesi temel kabul edilir.
- Siber ortamda şeffaflık, hesap verilebilirlik ve etik değerler desteklenir.
- Güvenlik ile erişilebilirlik arasındaki denge gözetilir.
- Siber güvenlik birimi düzenleyici ve denetleyici birim olarak güvenliğin sağlanmasını gözetir.
- Siber güvenliğin karşılanmasında mümkünse kurumsal ürün ve hizmet kullanımı esas alınır ve bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir şeklindedir.

6.2. Siber Güvenlik Vizyon ve Misyonun Belirlenmesi

Kurumsal siber güvenliğin başlangıç noktası olarak belirlenecek bir vizyonla birlikte kısa, orta ve uzun vade de bu vizyonu gerçekleştirmeye yönelik bir misyonun belirlenmesi hayata geçirilecek eylem planının daha sağlıklı ve verimli yürütülebilmesini sağlayacaktır. Bu bağlamda örnek bir kurumsal siber güvenlik vizyonu :

“Gelişen ve büyüyen teknolojinin artan kullanımına bağlı olarak ihtiyaç haline gelen siber güvenliğe ilişkin hususlarda bilişim sektöründe dünyanın önde gelen kurumlarından biri olmak”

Misyon olarakta:

“Enerji, finans, sađlık v.b.. kritik alt yapılara karřı yapılabilecek siber saldırılara karřı herhangi bir kurumsal bilgi ihlali oluřmadan önleme yeteneđine sahip olmak.” ifade etmek mümkündür.

6.3. Kurumsal Siber Güvenlik Politikalarının Oluřturulması

Belirlenmiř vizyon ve misyona ulařmak için (yukarıda belirtilen) ilkeler ıřığında kurumsal siber güvenlik politikalarının belirlenmesi ve (çalıřanların sorumluluklarını ve siber güvenlik hususunda bilinçlendirilmelerini sađlayacak řekilde) belgelendirilmesi gerekir. Bu belirlenen politikalar, kurum ve řirketleri siber saldırı ve tehditlere karřı hazırlı kılarak herhangi bir saldırı ve tehdit sonrasında sistemi tekrar eski haline getirecek adımların belirlenmesini sađlar. Yapılan görüřmelerde (belirlenecek politika dokümanının içeriđine iliřkin kurumların faaliyet gösterdiđi sektöre bađlı olarak çok farklı sonuçların ortaya çıkaracađı düşünülerek bu politikalarla ilgili ortak bir çerçeve ortaya koymak maksadıyla) katılımcılara “Sizce bir kurumun siber güvenlik politikalarının kapsamı (içeriđi) ne řekilde oluřturulmalıdır?” řeklinde sorulan soru üzerine alınan cevaplar dođrultusunda ařađıdaki bařlıkları içerecek řekilde bir kurumsal siber güvenlik politika dokümanı hazırlanmasının uygun olacađı deđerlendirilmektedir:

- a. Temel ilkeler
- b. Tehditler ve güvenlik zafiyetleri
- c. Güvenlik adımları:
 - 1- Kurumsal yasal mevzuatlar
 - 2- Kurumsal yetenekler
 - 3- Kurumsal Siber Olaylara Müdahale Birimi
 - 4- Kritik bilgi ve iletişim sistem altyapı güvenliđi
 - 5- Eđitim, farkındalık ve bilinçlendirme çalıřmaları
 - 6- Ulusal ve kurumlar arası koordinasyon

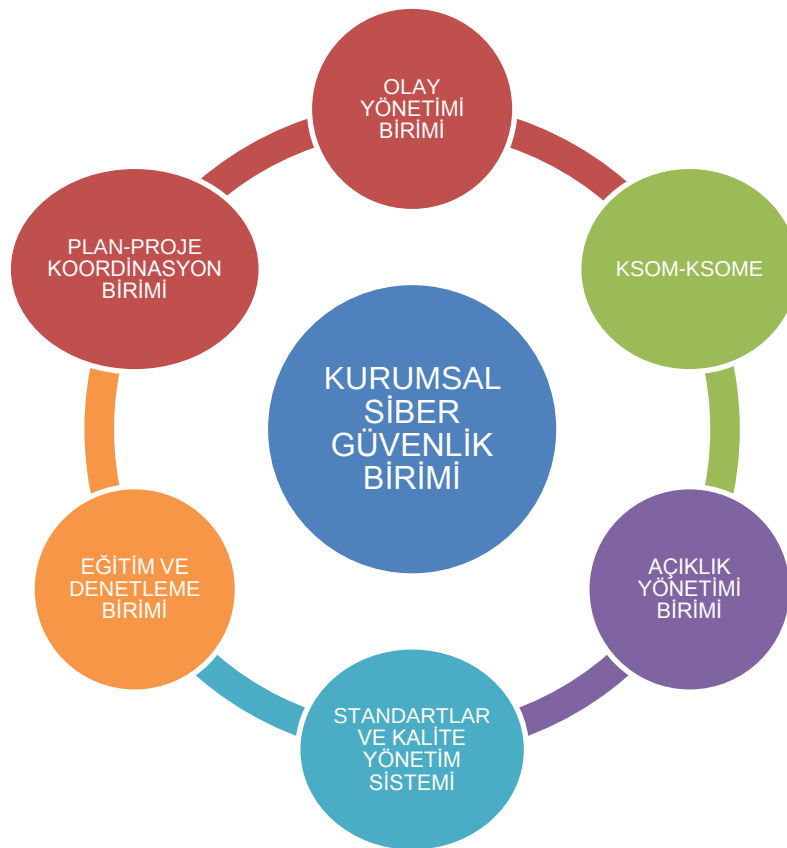
6.4. Kurumsal Siber Güvenlik Biriminin Oluřturulması

Siber tehdit ve saldırıların meydana getireceđi olayları önlemek, müdahale etmek ve siber farkındalık oluřturmak amacıyla kurulacak siber güvenlik birimiyle ilgili olarak görüřmelerde “Etkin bir kurumsal siber güvenlik sađlama adına

oluşturulacak kurumsal siber güvenlik birimine(KSGB) bağlı olarak görev yapacak birimler neler olmalıdır?” şeklindeki soruya ilişkin olarak katılımcılardan bazılarının verdiği artı değer katabilecek nitelikteki cevaplar şu şekildedir:

“...Kurumsal Siber Güvenlik Biriminin(KGSB) kendisine bağlı kurumsal olaylara müdahale birimi (KSOM) ve gerekli olduğu takdirde de bu birime bağlı kurumsal olaylara müdahale ekipleri (KSOME) oluşturulmalıdır.”

“...Oluşturulacak birimin (KSGB), kurumsal siber olaylara müdahale biriminin(KSOM) koordinasyon faaliyetlerini düzenlemesi ve yürütmesinin kurumsal güvenlik için gerekli olduğuna inanıyorum.”



Şekil 6.1. Örnek bir kurumsal siber güvenlik birimi yapısı

Tez çalışmasının kapsamını gereğinden fazla arttıracakı düşünülerek yukarıda belirtilen soruya verilen cevaplar neticesinde Şekil 7.1’ de görüldüğü üzere kurumsal siber güvenlik birimine bağlı olarak çalışacak birimler hakkında bilgi verilmeden sadece oluşturulacak siber güvenlik biriminin yapısı kısaca şematize edilmiştir.

6.5. Eylem Planı

Kurumsal siber güvenlik biriminin oluşturulmasını takiben kurumsal siber güvenliğin sağlanmasında dikkat edilmesi gereken ilkeler ışığında (aynı zamanda belirlenecek politikaların rehberliğinde) kurumsal siber güvenliğin sağlanmasına yönelik eylemlerin belirlenmesi amacıyla “Kurumsal siber güvenlik eylem planında bulunması gereken maddeleri gerçekleştirilme sırasına uygun olacak biçimde belirtiniz?” şeklindeki soru ile “Belirtmiş olduğunuz eylem planında bulunması gereken maddelerdeki her bir eyleme ilişkin sorumlu ve ilgili kurumsal birimler nelerdir?” şeklindeki soruya verilen cevapların çok çeşitlilik arz etmesi ve tüm sayılan maddelerin eylem planında belirtilmesinin planın kapsamını gereğinden çok fazla arttıracığı ve eylem planının amacına hizmet etmeyeceği değerlendirilerek verilen tüm cevaplar (eylemler ve bu eylemlere yönelik gerçekleştirilmesi gereken alt eylemler ile sorumlu ve ilgili birimlerin belirtildiği) ortak bir çerçeveye içinde hazırlanarak katılımcılara sunulmuş ve katılımcılar tarafından %90 gibi yüksek oranda olumlu bulunmuştur. Yukarıdaki iki soruya ilişkin bazı katılımcıların yapmış olduğu (planın uygulanabilirliği açısından önemli görülen) değerlendirmeler şu şekildedir:

“...herhangi bir eylem birden fazla birimi ilgilendirdiği durumlarda sorumlu birimin rehberliğinde (işbirliği halinde) eylemin gerektirdiği çalışmaların yürütülmesi gerekir.”

“...planda yer alan eylem ve alt eylemlerin periyodik olarak yenilenmesi ve sürekli olarak yürütülmesi gibi öngörülen eylemlerin de planda ayrıca belirtilmesi ortaya konacak planın sağlıklı bir şekilde işleyişini sağlayacaktır.”

Tüm bu yukarıda sayılan bilgiler ışığında (kurumsal siber güvenlik ilke, vizyon, misyonun belirlenmesi, politikalar oluşturulması ve kurumsal siber güvenlik biriminin yapılandırılmasını müteakip gerçekleştirilecek eylemler) EK-1’ de bir plan dahilinde sunulmaktadır.

7. SONUÇ VE ÖNERİLER

İnternetin yaygınlaşıp kullanımının artması ve gelişen teknolojiyle birlikte basit düzeyde bilgisayar kullanma becerisine sahip kötü niyetli kişilerin siber ortamda kolayca elde ettiği uygulamalarla (takibi kolay yapılamayacak biçimde) etkili saldırılar yapabildiği görülmektedir. Ayrıca bu saldırı ve tehditlerin daha kompleks bir yapıya bürünerek artmakta olduğu ve eskisi gibi rastgele hedeflere yönelik bireysel bir takım faaliyetlerden belirli hedeflere organize ve karmaşık bir yapıya doğru kayarak kurum ve şirketlere zarar verme ya da elde ettikleri verilerle kazanç sağlamaya dönük ekonomik amaçlar sağlama peşinde olduğu anlaşılmaktadır. Bu bağlamda 2013 yılında, kurum ve şirketlerin sürekli gelişim gösteren yapıları nedeniyle büyük miktarlarda oluşan verinin işlenmesine ve depolanmasına yoğunlaşan *big data teknolojisi*, akıllı aletlerin oluşturduğu bir sistem olan *nesnelerin interneti* ve *mobil platformların* bu tehdit ve saldırıların gözdesi haline geldiği görülmektedir. Ayrıca yine geçtiğimiz yıl, siber saldırılar içinde gelişmişlik, karmaşıklık ve gizlilik gibi özellikleriyle siber espionaj amaçlı kullanılan APT' lerin ulusal ve kurumsal siber güvenliğe yönelik etkilerinin beklenenin ötesinde boyutlarda olması, yüksek teknolojiye sahip birçok kuruma başarılı saldırıların gerçekleştirilebildiği watering hole saldırı yönteminin diğer saldırı yöntemleri ile birleşerek daha etkili sonuçların ortaya çıkabilme durumu güvenlik uzmanlarını ve tehdit analizi yapanları endişelendirmektedir. Ek olarak, siber tehdit sıralamasında zirveyi paylaşan izinsiz indirmeler ve (özellikle solucan/truva atı gibi) kötücül yazılımların sosyal ağ sitelerinde ve bulut bilişim altyapılarındaki etkinlikleri kurumlar açısından önemli riskler doğuracağından kurumsal siber güvenliğin sağlanması gerekliliğini ortaya koymaktadır.

Siber tehdit ve saldırılardaki bu gelişmeye karşın siber güvenlikten sorumlu devlet kurumlarının siber yeteneklerini arttırması ve yapılan bir takım uluslararası işbirlikleri sayesinde siber suç oranında düşmeler olması tehdit ve zafiyetlerin tespit edilme hızını arttırsa da etkin ve verimli bir siber güvenlik olgusunu hayata geçiremediği görülmektedir. Örneğin ülkemizde siber saldırı ve tehditler sayısal anlamda düşüş göstermesine karşın etkinlik anlamında daha zarar verici boyutlara ulaşarak siber suç mağdurlarındaki kişi başına düşen mali kayıp (2013 yılında önceki seneye oranla yaklaşık 6 kat) artmıştır.

Sadece internet suçlarının değil (internetle beraber intranet ve diğer ağ sistemlerini kapsayan) siber uzayda işlenen tüm suçların kast edildiği siber suçların (düşük maliyet, kolay bir şekilde işlenebilme, hukuksal bütünlüğün olmaması, yeterince uluslararası işbirliğinin sağlanamaması, küresel bağlanabilirlik ve teknolojiye bağımlılık gibi nedenlerle) gelecekte daha da artması ve gelişen teknolojiyle birlikte değişen suç algısına bağlı olarak farklı siber suçların ortaya çıkması ya da var olan siber suçların farklı boyutlar kazanması beklenmektedir. Ayrıca güvenlik kavramının suç kavramına göre şekillendiği günümüzde siber suçluların bir adım önde olmasından dolayı siber güvenlikte pro-aktif olunması yani suç oluşmaması için önceden gerekli teknik, idari ve hukuki önlemlerin alınması önem kazanmaktadır.

Tez kapsamında yapılan araştırmalar sonucunda; ülkemizde siber suçlar konusunda hukuki düzenlemelerin yeterli olmadığı değerlendirilerek farklı ülkelerin bu konudaki başarılı uygulamaları doğrultusunda (uygulamada karşılaşılabilecek aksaklıklar göz önüne alınarak) gerekli eksikliklerin giderilmesi maksadıyla çalışmalar yapılması gerektiği anlaşılmaktadır. Ayrıca bu hukuki düzenlemelerin hazırlanması ve uygulanmasında bilişim hukukçularına olan ihtiyacın karşılanması için bu uzmanların sayılarının arttırılarak yetiştirilmesi hususunda üniversitelere önemli görevler düşmektedir. Bu kapsamda hukuk fakültesi ve bilgisayar mühendisliği bölümlerinde siber güvenlik dersinin müfredata yerleştirilmesi son derece önemlidir. Başka önemli bir bulgu da, kurumların kendi içlerinde veya aralarında bir ar-ge çalışması yürütmemeleri ve bunun devletçe desteklenmemesi sonucu oluşacak dışa bağımlılığın ulusal güvenliği zafiyete düşürebileceği, devlet veya özel kurumlardaki kullanılan yazılımların birçoğunun aynı olması dolayısıyla bu yazılımlar içine yerleştirilebilecek zararlı bir yazılım neticesinde istenmeyen sonuçların gerçekleşebileceği öngörülmektedir.

Çoğunlukla ulusal ve uluslararası boyutta ele alınan ve bu düzeyde üretilen politika ve standartlarla sağlanılmaya çalışılan siber güvenliğin daha etkin ve sağlam olması, bu seviyede devam eden bütüncül bir yaklaşımdan ziyade bütünü oluşturan (özellikle de kritik alt yapılara sahip kurumların içinde olduğu) parçaların siber güvenliğinin sağlanması ile olacağı değerlendirilmektedir. Kurum ve şirketlerin türüne ve faaliyet gösterdiği alana göre alanyazında bilgi güvenliği, bilgi

teknolojileri güvenliği v.b. isimlerle ifade edilen ve ülkenin siber uzayının güvenliğinin ve savunmasının artırılması ile kurumsal kritik bilgi ve iletişim sistem altyapılarının iş sürekliliğinin ve verilerin güvenliğinin sağlanmasını temin eden kurumsal siber güvenlik kavramının ülkemizdeki kurumlar tarafından yeterince ve doğru anlaşılmadığı tez çalışması sonucunda tespit edilen en önemli bulgulardan birisidir. Ülkemizde yapılan ulusal çaptaki tatbikatlar neticesinde kurumların siber güvenliklerini sağlamaya yönelik ciddi boyutta eksiklikleri ve hataları olduğu görülmektedir(Bkz. sf:86). Bu nedenle ülkemizde kurumsal siber güvenlikle ilgili daha çok araştırma ve geliştirme çalışması yapılmasına ihtiyaç duyulmaktadır.

Tez kapsamında yapılan araştırmalarda elde edilen önemli bulgulardan bir diğeri de kurumsal siber güvenliği sadece saldırganların yapmış olduğu saldırı ve tehditler değil aynı zamanda personelin neden olduğu durumlarında tehdit ettiği anlaşılmış ama buna rağmen kurumların siber güvenliğin sağlanmasında izlenmesi gereken süreçleri, görev tanımı ve sorumlulukları, kişilerin uyması gereken politika ve standartları uygulamaya koymadığı, çoğu kurumda farkındalık eğitimleri ve bilinçlendirme programlarının da yapılmadığıdır. Bu bağlamda, kurumsal siber güvenliğin istenilen düzeyde sağlanması amacıyla kurumun türüne bağlı olarak mümkün seviyede (tez içinde belirtilen) tüm önlemlerin yerine getirilmesinin yanında teknik olmayan önlemlerinde (personel güvenliği, farkındalık, politikalar, yönetmelikler v.b.) bir bütün olarak değerlendirilip ele alınması gerektiği anlaşılmaktadır. Ayrıca kurumsal siber güvenliğe yönelik tehdit ve saldırıların bilinmesi, bu tür tehdit ve saldırılarla başa çıkabilmek için yapılması gereken mücadele yöntemlerinden haberdar olunabilmesi (ve böylece diğer ülkelerdeki başarılı örneklerin baz alınarak eksiklik ve yanlışlıkların giderilmesi için çalışmalar yapılması), saldırı türlerinin takip edilmesi, saldırganların kullandığı yöntemlerin saptanması, ülkemizde ve dünyada bu konuda yapılan araştırmalar ve raporlar ile tespit edilen güvenlik zafiyetlerinin takip edilerek giderilmesi kurumsal stratejilerin geliştirilmesinde önemli bir role sahip olması dolayısıyla kurumlar tarafından mutlaka yerine getirilmesi gereken faktörler olduğu değerlendirilmektedir.

Artı bir değer olmaktan çıkarak hizmet sunumları gerçekleştirebilmeleri için bir zorunluluk haline gelen siber ortama bilgi ve iletişim teknolojilerini sunan kurum ve

şirketler için uğranılan maddi zarardan çok müşteri, pazar ve itibar kaybı gibi değerler öne çıkmaktadır. Yapılan saldırılarda özellikle kurumların medyadaki haber değeri, konumu ve müşteri kitlesi gibi çeşitli faktörlerinin göz önüne alındığı anlaşılmaktadır. Bu bağlamda, bir kurum veya şirket için güvenlikten tasarruf edilemeyeceği gibi güvenlik endişesiyle sistem verimliliğini sağlayacak alt yapıların kullanımından da vazgeçilemeyeceğinden ve siber ortamda sayıları her geçen gün daha da artan saldırı ve tehditleri bertaraf etmenin, kurumsal olarak hizmet sunulan kitlenin memnuniyeti ve kaliteli hizmet anlayışı açısından önem arz etmesinden dolayı (günümüzde özellikle yapılan saldırı ve tehditlerin web uygulamalarına doğru kayması nedeniyle) internet ortamından gelebilecek tehlikelere karşı kurumların alması gereken zorunlu ve ilave adımlar bulunmaktadır(Bkz. sf: 112). Tüm bu adımların yanı sıra kurumun departmanlarınca ağ ve bilgi teknolojileri üzerinden sağlanan her türlü işlem ve verinin sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına, kurumun kritik bilgi ve iletişim sistem altyapılarına ait bilişim sistemlerinin güvenliği ve yapılan herhangi bir saldırı neticesinde etkinin en düşük düzeyde kalmasına ve saldırı sonrasında sistemlerin en kısa sürede normale dönmesine yönelik çalışmaların belirlenmesine ve oluşan suçun adli makamlarca daha etkin soruşturulmasına yönelik zemin oluşturmak amacıyla etkili bir eylem planı hazırlanması gerekli görülmektedir.

Alanyazında yeni bir kavram olması,(her ne kadar siber güvenlik alanında birçok araştırma yapılsa da) kurumsal bazda bu şekilde yapılmış öncü çalışmalardan biri olması nedeniyle çoğunlukla internet üzerindeki kaynaklardan yararlanılması ve bu kaynaklarda sunulan bilgilerin doğruluğundan emin olunması için uzun araştırmalar yapılması, ilgili kaynağın siber güvenlikte dünyada ve ülkemizde söz sahibi olan ticari firmaların ve sivil toplum örgütlerinin sitelerinden olmasına özen gösterilmesi nedeniyle araştırmaların zorlu süreçler içermesi, tez konusunun tüm boyutlarıyla ele alınması neticesinde neredeyse her bir bölümün tez konusu olabilecek çapta geniş olması, tez konusunda yararlanılan kaynakların birçoğunun ingilizce olması ve türkçe diline çevrilmesi sırasında anlam kayıplarının yaşanmaması için yorucu uğraşların verilmesi, kurumsal siber güvenliğe yönelik tehditler, mücadele yöntemleri ve eylem planı gibi üç yeni ve kapsamlı konunun bir

tek bir çatı altında toplanması tez çalışması sırasında karşılaşılan zorluklardan bazılarıdır.

Kurumsal siber güvenliğin önemli parçası olan kurumsal web güvenliğinin tez çalışması öncesinde birkaç temel önlemlerle sağlanabilecek kadar basit olduğu düşünülürken çalışma sonucunda web güvenliğinin ayrı bir tez konusu olacak kadar kapsamlı olduğu ve kurumsal siber güvenliği en üst seviyede tehdit eden riskler içerdiğinin anlaşılması, tez çalışması sırasında siber güvenlikle ilgili akademik ve ticari alanda uzmanlarla görüşmeler yapılması ve bunun sonucunda da kurumsal siber güvenlik konusu gibi çok değerli olan bir konu üzerinde ciddi bilgi paylaşımlarının elde edilmesi, tez çalışmasının tez yazarının mesleki kariyerini önemli ölçüde etkileyerek işyerinde kurumsal siber güvenliği uygulama adına önemli birikimler elde etmesini sağlaması gibi birçok değerli kazanımlar elde edilmiştir.

Sonuç olarak bu çalışmanın ülkemizdeki tüm kamu ve özel kurumlar için kurumsal siber güvenliğin kapsamlı olarak ele alındığı ilk kaynaklardan biri olması nedeniyle alanyazında örnek bir çalışma olacağı, sonraki araştırmalara kaynaklık ederek daha kapsamlı araştırmaların yapılmasına aracılık edeceği ve kurumsal siber güvenliğin sağlanmasını önemseyen kurumlar için yol gösterici nitelikte bir eser olacağı düşünülmektedir.

KAYNAKLAR

1. Akdağ, P. (2009). *Siber Suçlar ve Türkiye'nin Ulusal Politikası*. Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 84-87, 87-90, 162.
2. Andress, A. (2004). *Surviving Security*. United States of America: A CRC Press Company, 195-196.
3. Bircan, B. (2012, 6 Kasım). *Gelişmiş Siber Silahlar ve Tespit Yöntemleri*. Siber Güvenlik Konferansı 2012 konferansında sunuldu, Ankara.
4. Bilişim ve Teknoloji Hukuku Enstitüsü. (2012). *Siber güvenlik raporu*; İstanbul Bilgi Üniversitesi, *İstanbul*, 5-58, 60-69.
5. Boğa, U. (2011). *Bilişim Suçlarıyla Mücadele Yöntemleri*, Uzmanlık Tezi, Radyo Ve Televizyon Üst Kurulu, Ankara, 60-62, 73-81, 86-88.
6. BTK , TÜBİTAK. (2011). *Ulusal siber güvenlik tatbikatı sonuç raporu*; BTK ve TÜBİTAK, *Ankara*, 10-15.
7. Canlı, C. (2009). *Saldırı tespit sistemlerinin incelenmesi ve bu bağlamda bilgi güvenliği*, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, *İstanbul*, 83, 85-86, 101-105.
8. Cisco Systems. (2013). *Cisco 2013 yıllık güvenlik raporu*; CISCO Inc., *San Jose,CA*, 34-35,44-45, 42-43, 64-65.
9. Çakar, H. (2005). *Bilgisayar ağ güvenliği ve güvenlik duvarları*, Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, *Elazığ*, 13, 16-18, 21.
10. Çakır,S., Kesler, M. (2012, 1-3 Şubat). *Bilgisayar Güvenliğini Tehdit Eden Virüsler ve Antivirüs Yazılımları*. XIV. Akademik Bilişim Konferansında sunuldu, Uşak.
11. Dinçel, Ö., Dinçkan, A. (2008). *Bilgi güvenliği yönetim sistemi kurulumu* (BGYS-0001). Ankara: TÜBİTAK(UEKAE), 7-13.
12. Ergün, İ. (2008). *Siber Suçların Cezalandırılması ve Türkiye' de Durum*. Ankara: Adalet Basım Yayım Dağıtım San. Ve Tic. Ltd. Şti., 52-53, 54-55.
13. Gülmüş, M. (2010). *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, *İstanbul*, 32, 106-108, 100.

14. Gülnaz, M. (2010). *Kamusal web güvenliği*, Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 23, 103-105.
15. Başbüyük, O., Hekim, H. (2013). Siber Suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 4 (2), 136, 144.
16. İlbaş, Ç., Köksal, M. (2011, 17-19 Kasım). *Türkiye bilişim suçları raporu*. 2. Uluslararası Bilişim Hukuku Kurultayında sunuldu, İzmir.
17. İnternet: Bilgi Güvenliği Akademisi. Web Uygulama Güvenlik Duvarı Tercih Rehberi. Bilgi Güvenliği Akademisi. 2014-04-18. URL: <http://www.webcitation.org/query?url=http%3A%2F%2FWeb+Uygulam+a+G%C3%BCvenlik+Duvar%C4%B1+Tercih+Rehberi&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
18. İnternet: Bilgi Teknolojileri ve İletişim Kurumu. Çalışmalar. BTK. 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.btk.gov.tr%2Fbilgi_teknolojileri%2Fsiber_guvenlik%2Fcalismalar.php+&date=2014-04-18. Son Erişim Tarihi: 18.04.2014.
19. İnternet: Bilgi ve İletişim Kurumu. Genel Bilgi. BTK. 2014-04-18. URL: http://www.webcitation.org/query?url=http%3A%2F%2Ftk.gov.tr%2Fbilgi_teknolojileri%2Fsiber_guvenlik%2Findex.php&date=2014-04-18. Son Erişim Tarihi: 18.04.2014.
20. İnternet: Özbudak, Gökay. Sahte antivirüsler çoğalıyor. CHIP Online.tr. 2010-05-05. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.chip.com.tr%2Fhaber%2Fsahte-antivirusler-cogaliyor_19760.html+&date=2014-04-18. Son Erişim Tarihi: 18.04.2014.
21. İnternet: Dokuz Eylül Üniversitesi Bilgi Sistemi. Spam nedir. Dokuz Eylül Üniversitesi. 2014-04-18. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fweb.deu.edu.tr%2Fsss%2Fspam.html&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
22. İnternet: Haberler.com. Genelkurmay Siber Savunma Komutanlığı 7/24 Esasına Göre Çalışıyor. 2013-12-02. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.haberler.com%2Fgenelkurmay-siber-savunma-komutanligi-7-24-esasina-5376224-haberi%2F&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.

- 23.İnternet: Microsoft Güvenlik Merkezi. Bilgisayar Virüsü Nedir?. Microsoft Corp.. 2014-04-18.
URL:<http://www.webcitation.org/query?url=http%3A%2F%2Fwww.microsoft.com%2Ftr-tr%2Fsecurity%2Fpc-security%2Fvirus-what-is.aspx++&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
- 24.İnternet: Microsoft Güvenlik Merkezi. Güvenlik duvarı Nedir?. Microsoft Corp.. 2014. URL:
<http://www.webcitation.org/query?url=http%3A%2F%2Fwww.microsoft.com%2Ftr-tr%2Fsecurity%2Fpc-security%2Ffirewalls-what-is.aspx++&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
- 25.İnternet: Microsoft Güvenlik Merkezi. Sahte virüs uyarılarına karşı dikkatli olun. Microsoft Corp.. 2014-04-18. URL:
<http://www.webcitation.org/query?url=http%3A%2F%2Fwww.microsoft.com%2Ftr-tr%2Fsecurity%2Fpc-security%2Fantivirus-roque.aspx++&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
- 26.İnternet: Siber Güvenlik Enstitüsü . Çözümler. TÜBİTAK. 2014-04-18. URL:
<http://www.webcitation.org/query?url=http%3A%2F%2Fsge.bilgem.tubitak.gov.tr%2Ftr%2Fcozumler%2F&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
- 27.İnternet: Suçlarla Mücadele Şube Müdürlüğü. Bilişim Hukuku. İEM. 2014. URL:
<http://www.webcitation.org/query?url=http%3A%2F%2Fsibersuclar.iem.gov.tr%2FKanun.html&date=2014-04-18>. Son Erişim Tarihi: 18.04.2014.
- 28.İnternet: Siber Suçlarla Mücadele Şube Müdürlüğü. Siber suçlar. İEM. 2014-04-19. URL:
http://www.webcitation.org/query?url=http%3A%2F%2Fsibersuclar.iem.gov.tr%2Fsiber_suclari.html++&date=2014-04-19. Son Erişim Tarihi: 19.04.2014
- 29.Norton by Symantec.(2013). 2013 Norton Report; Symantec Corp., Cupertino, 5-23.
- 30.İnternet: Telekom İnternet Çözümleri. Bilgisayar Solucanları (Worms). Türk Telekom. 2014-04-19. URL:
<http://www.webcitation.org/query?url=http%3A%2F%2Fwww.telekom.com.tr%2Fv2%2Ffaydali-bilgiler%2F182-bilgisayar-solucanlari-worms&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.

31. Tatar, Ü. (Haziran, 2011). *Dünyada ve Türkiye’de Siber Güvenlik Tatbikatları*. 6. Kamu Bilgi Teknolojileri Güvenlik Konferansında sunuldu, Ankara.
32. İnternet: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi(BİLGEM). Siber Güvenlik Enstitüsü. TÜBİTAK. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fsge.bilgem.tubitak.gov.tr%2Ftr%2Fkurumsal%2Fsge-tarihcesi&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
33. İnternet: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(UEKAE). Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü. TÜBİTAK(BİLGEM). 2014. URL:<http://www.webcitation.org/query?url=http%3A%2F%2Fuekae.bilgem.tubitak.gov.tr%2Ftr%2Fkurumsal%2Fuekae+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
34. İnternet: Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğü. Ulusal Mevzuat. Adalet Bakanlığı. 2014-04-19. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.uhdigm.adalet.gov.tr%2Fuhamer%2Fsiber_suc_ulusal_mevzuat.html&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
35. İnternet: Doğu,Koray. İnternet ve bilgisayar güvenliği için temel önlemler. Ulusal Bilgi Güvenliği Kapısı-BİLGEM. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fson-kullanici-kategorisi%2Finternet-ve-bilgisayar-guvenligi-icin-temel-onlemler.html+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
36. İnternet: Ulusal Bilgi Güvenliği Kapısı. TR-BOME/Bilgisayar Olaylarına Müdahale Ekibi. BİLGEM. 2014-04-19. URL: <http://www.webcitation.org/query?url=https%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fcert%2Findex.php&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
37. İnternet: Çeri,Yusuf. Web’teki büyük tehlike:CSRF. Ulusal Bilgi Güvenliği Kapısı. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilgiguvenligi.gov.tr%2Fweb-guvenligi%2Fwebdeki-buyuk-tehlike-csrf.html&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
38. İnternet: Telekomünikasyon İletişim Başkanlığı. Ulusal Siber Olaylara Müdahale Merkezi . BTK. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.usom.gov.tr%2Ftr-menu-2-giris.html+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.

- 39.İnternet: Vikipedi, Özgür ansiklopedi. Solucanı Truva atından farklı kılan farklılıklar. 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Ftr.wikipedia.org%2Fwiki%2FBilgisayar_solucan%25C4%25B1%23Solucan.C4.B1_Truva_at.C4.B1ndan_farkl.C4.B1_k.C4.B1lan_farkl.C4.B1l.C4.B1klar&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
- 40.İnternet: Vikipedi, Özgür ansiklopedi. Veritabanı. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Ftr.wikipedia.org%2Fwiki%2FVeritaban%25C4%25B1&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 41.İnternet: Web Application Security Consortium. Brute Force. WASC. 2014. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246915%2FBrute%2520Force+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 42.İnternet: Web Application Security Consortium. Cross Site Request Forgery. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246919%2FCross%2520Site%2520Request%2520Forgery&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 43.İnternet: Web Application Security Consortium. Cross Site Scripting. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246920%2FCross%2520Site%2520Scripting&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 44.İnternet: Web Application Security Consortium. Denial Of Service. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246921%2FDenial%2520of%2520Service+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 45.İnternet: Klein,Amid. DOM Based Cross Site Scripting or XSS of the Third Kind. Web Application Security Consortium. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.webappsec.org%2Fprojects%2Farticles%2F071105.shtml&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.

- 46.İnternet: Web Application Security Consortium. Format String. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246926%2FFormat%2520String+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 47.İnternet: Web Application Security Consortium. HTTP Response Splitting. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246931%2FHTTP%2520Response%2520Splitting&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 48.İnternet: Web Application Security Consortium. Insufficient Authentication. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246939%2FInsufficient%2520Authentication&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 49.İnternet: Web Application Security Consortium. Insufficient Authorization. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246940%2FInsufficient%2520Authorization&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 50.İnternet: Web Application Security Consortium. Insufficient Password Recovery. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246942%2FInsufficient%2520Password%2520Recovery&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 51.İnternet: Web Application Security Consortium. Insufficient Session Expiration. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246944%2FInsufficient%2520Session%2520Expiration&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
- 52.İnternet: Web Application Security Consortium. LDAP Injection. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246947%2FLDAP%2520Injection+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.

53. İnternet: Web Application Security Consortium. OS Commanding. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246950%2FOS%2520Commanding+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
54. İnternet: Web Application Security Consortium. Path Traversal. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246952%2FPath%2520Traversal+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
55. İnternet: Web Application Security Consortium. SSI Injection. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246964%2FSSI%2520Injection+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
56. İnternet: Web Application Security Consortium. SQL Injection. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13246963%2FSQL%2520Injection&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
57. İnternet: Web Application Security Consortium. XPath Injection. WASC. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fprojects.webappsec.org%2Fw%2Fpage%2F13247005%2FXPath%2520Injection+&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
58. İnternet: Wikipedia, The Free Encyclopedia. Blackhole Exploit kit. 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FBlackhole_exploit_kit&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
59. İnternet: Wikipedia, The Free Encyclopedia. Computer worm. . 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FComputer_worm&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
60. İnternet: Wikipedia, The Free Encyclopedia. Server Side Includes. 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FServer_Side_Includes&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.

61. İnternet: Wikipedia, The Free Encyclopedia. Phishing. . 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FPhishing&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
62. İnternet: Wikipedia, The Free Encyclopedia. Watering Hole. 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fen.wikipedia.org%2Fwiki%2FWatering_Hole&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
63. Karaarslan, E., Akın, G., Fetah, V. (2008). *Kurumsal ağlarda zararlı yazılımlarla mücadele kılavuzu* (ULAKCSIRT-2008-01). Ankara: TÜBİTAK(ULAKBİM), 22-23.
64. Karaarslan, E., Tuğlular, T., Şengonca, H. (2008, 30 Ocak - 1 Şubat). *Kurumsal web güvenliği yapısı*. Akademik Bilişim 2008 konferansında sunuldu, Çanakkale.
65. Marinos, L. (2013). ENISA Threat Landscape 2013 Overview of current and emerging cyber-threats; ENISA, doi:10.2788/14231, Greece, 16, 28-29, 3, 21, 43-45, 22, 61-62.
66. Shabtai, A., Elovici, Y., Rokach, L. (2012). *Data Leakage, A Survey of Data Leakage Detection and Prevention Solutions*. London. Springer, 5-10.
67. Sınar, H. (2001). İnternet ve Ceza Hukuku. İstanbul: Beta Basım Yayım Dağıtım A.Ş., 69-76.
68. Strateji Geliştirme Daire Başkanlığı. (2013). 2012 yılı faaliyet raporu; Emniyet Genel Müdürlüğü, Ankara, 52.
69. Şentürk, H., Çil, Z., Sağıroğlu, Ş. (2013, 20-21 Eylül). *Siber Güvenliğin Taarruzi Boyutu ve Uluslararası Hukuk Kurallarının Uygulanabilirliği*. VI. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansında sunuldu, Ankara.
70. Turhan, O. (2006). *Bilgisayar ağları ile ilgili suçlar(Siber Suçlar)*. Planlama Uzmanlığı Tezi, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara, 74-75, 87.
71. Tulum, İ. (2006). *Bilişim suçları ile mücadele*. Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta, 83, 59-60, 60-62.
72. Türköz, T. (2013, 14 Mayıs). *Ulusal Siber Güvenlik Stratejisi ve Yürütülen Çalışmalar*. Siber Güvenlik Konferansı 2013' te sunuldu, İstanbul.

73. Uçar, O. (2013, 14 Mayıs). *Hedef Odaklı Siber Saldırıları*. Siber Güvenlik Konferansı 2013' te sunuldu, İstanbul.
74. İnternet: Ünver, M., Canbay, C. (Mart, 2010). Ulusal ve uluslararası boyutlarıyla siber güvenlik. *Elektrik Mühendisliği*, sayı 498. 98-101, Web: http://www.emo.org.tr/ekler/a9a502d6e646c25_ek.pdf?dergi=598 adresinden 18.04.2014 tarihinde alınmıştır.
75. Vural, Y., Sağiroğlu, Ş. (2007, 13-14 Aralık). *Kurumsal Bilgi Güvenliği: Güncel Gelişmeler*. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansında sunuldu, Ankara.
76. Vural, Y., Sağiroğlu, Ş. (2011). Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler. *Gazi Üniv. Müh. Mim. Fak. Dergisi*, 26(1), 89-103.
77. Vural, Y. (2007). *Kurumsal Bilgi Güvenliği ve Sızma (penetrasyon) Testleri*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 175-180, 201-206, 137-159.
78. Vural, Y., Sağiroğlu, Ş. (2010). Veritabanı yönetim sistemleri güvenliği: tehditler ve korunma yöntemleri. *Politeknik dergisi*, 13(2), 71-80.
79. Websense Security Labs. (2013). 2013 Threat Report; Websense Inc., San Diego, 3-8, 10-11.
80. Yenidünya, C., Değirmenci, O. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*. İstanbul: Legal Yayıncılık San. Ve Tic. Ltd. Şti., 38-39.
81. Yılmaz, D. (2004). Sosyal Mühendislik. *Bilişim Korsanlığı ve Korunma Yöntemleri*. 2.baskı. İstanbul. Hayat Yayıncılık, s.148-153.
82. Ceylan, G. (2004). *Bilgisayar Ağlarına Yetkisiz Erişimleri Tespit Eden Sistemler*, Yüksek Lisans Tezi, İstanbul Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 13-14.
83. Sancak, S. (2008). *Saldırı tespit sistemleri tekniklerinin karşılaştırılması*, Yüksek Lisans Tezi, Gebze Yüksek teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Gebze, 7, 12-13.

84. İnternet: ITU World Telecommunication/ICT Indicators database. Key ICT indicators for developed and developing countries and the world. ITU. 2014. URL:http://www.webcitation.org/query?url=http%3A%2F%2Fwww.itu.int%2Fen%2FITU-D%2FStatistics%2FDocuments%2Fstatistics%2F2013%2FITU_Key_2005-2013_ICT_data.xls&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
85. Topal, H. (2004). *Siber Terör*, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 20-44.
86. Microsoft. (2013). Microsoft Security Intelligence Report; Microsoft Corp., Volume 15, *Washington*, 83-88.
87. İnternet: Türkiye İstatistik Kurumu. Meslek gruplarına göre bireylerin bilgisayar ve İnternet kullanımı, 2013. TÜİK. 2014-04-19. URL: http://www.webcitation.org/query?url=http%3A%2F%2Ftuik.gov.tr%2FHbGetir.do%3Fid%3D13569%26tb_id%3D15&date=2014-04-19. Son Erişim Tarihi: 19.04.2014.
88. Websense Security Labs. (2011). SECURITY PROS & “CONS”; Websense Inc., *San Diego*, 10.
89. Cisco Systems. (2014). Cisco 2014 Annual Security Report; CISCO Inc., *San Jose, CA*, 26.
90. Atalay, A.H. (2013). Siber güvenlik, siber suçlar ve siber savaşlar. ITGSC’de (ISSA Turkey Grand Security Conference) sunuldu, İstanbul.
91. 10 bin siteye ‘yasak’ geldi. (14 Aralık 2013). *Hürriyet*.
92. Erdoğan, Y. (2010). Bilişim sistemine girme ve kalma suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 12(özel sayı), 1363-1433.
93. İnternet: Çeken, Hüseyin. Amerika Birleşik Devletlerinde siber suçlar. 2014. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Farchiv.jura.uni-saarland.de%2Fturkish%2FHCeken.html+&date=2014-04-18>. Son erişim tarihi: 18.04.2014.
94. Mahmutoglu, F. (2002, 2 Mayıs). *Karşılaştırmalı hukuk bakımından internet suçlarının ceza sorumluluğu*. “İnternet Ortamında Ceza Sorumluluğu” konulu panelde sunulmuştur. İstanbul.

95. İnternet: Türkiye İstatistik Kurumu. Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, 2013. TÜİK. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Ftuik.gov.tr%2FPreHaberBultenleri.do%3Fid%3D13569&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
96. İnternet: Kayar, Beşir. Kurumsal Antivirus Seçerken Dikkat Edilmesi Gerekenler. 2014-04-19. URL: <http://www.webcitation.org/query?url=http%3A%2F%2Fwww.bilginipaylas.com%2Fantivirus-makaleleri%2Fkurumsal-antivirus-secerken-dikkat-edilmesi-gerekenler.html&date=2014-04-19>. Son Erişim Tarihi: 19.04.2014.
97. Leiner, Barry., Cerf, V., Clark, D., Kahn, Robert., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., Wolf, S. (2009). A Brief History of the Internet. *ACM SIGCOMM Computer Communication Review*, 39(5), 22-31.
98. Özbek, V. (2007). Banka veya kredi kartlarının kötüye kullanılması suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 9(özel sayı), 1019.
99. Başbakanlık Kamu Düzeni ve Güvenliği Müsteşarlığı. (2013). *Bütün Boyutlarıyla Terörizmin Önlenmesi Avrupa Sözleşmesi* (2. basım). Ankara: Kamu Düzeni ve Güvenliği Müsteşarlığı Yayınları, 9-11.
100. Turhan, M. (2010). *Siber güvenliğin sağlanması, dünya uygulamaları ve ülkemiz için çözüm önerileri*. Uzmanlık Tezi, Bilgi Teknolojileri ve İletişim Kurumu, Ankara, 52-54, 100.
101. Türkiye Bilişim Derneği. (2013). 2013 Değerlendirme raporu; TBD, Ankara, 15.
102. TREND MICRO Küresel Teknik Destek ve Ar-Ge Merkezi. (2013). TrendLabs 2013 Güvenlik Özeti; Trend Micro Corp., Tokyo, 11.
103. İnternet: Vikipedi, Özgür Ansiklopedi. Barındırma hizmeti. 2014. URL: http://www.webcitation.org/query?url=http%3A%2F%2Ftr.wikipedia.org%2Fwiki%2FBar%25C4%25B1nd%25C4%25B1rma_hizmeti&date=2014-04-21. Son Erişim Tarihi: 21.04.2014
104. Kara, M. (2013). *Siber saldırılar – siber savaşlar ve etkileri*. Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 40-49.
105. Türk Standartları Enstitüsü. (2013). *Sızma testi, eğitim ve danışmanlık hizmeti veren personel ve firmalar için yetkilendirme programı*. Ankara: TSE, 6.

- 106.Nacar, F. (2010). *Avrupa Birliđi ÷lkeleri ve T÷rkiye’de biliřim suçlarının ceza hukukundaki uygulamaları*. Yüksek Lisans Tezi, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 35-36.
107. Böke, Kaan. (2010). Sosyal Bilimlerde Arařtırma. *Sosyal Bilimlerde Arařtırma Yöntemleri*. Ankara: Alfa Yayınları, 16.
- 108.Akbulut, B. (2000). Biliřim Suçları. *Selçuk Üniversitesi Hukuk Fak÷ltesi Dergisi, Milenyum Armađanı*, 8 (1-2), 545-555.

EKLER

NO	EYLEM	ALT EYLEM	SORUMLU(S) VE İLGİLİ(Lİ) BİRİMLER	AÇIKLAMA
1	Siber güvenlik konusunda yönetmelik çalışmalarının yapılması	Siber güvenlikle ilgili ulusal, uluslararası mevzuat ile benzer kurumların yönetmelikleri incelenerek ihtiyaç duyulan düzenlemelerin tespit edilmesi ve yönetmelikte geçecek teknik kavramlarla ilgili açıklamaların hazırlanması	Varsa kurumun hukuki birimi (s) aksi durumda yönetim kurulunca belirlenecek bir birim(s) -Kurumsal Siber Güvenlik Birimi (i) -Kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	Belirli periyotlarla ilgili ve sorumlu birimlerin yapacağı toplantılarla güncellemeler yapılmalıdır.
		Tespit edilen düzenlemeler çerçevesinde kurum veya şirketin sözleşme veya diğer yönetmeliklerinde gerekli güncelleme çalışmaları yapılarak üst yönetime sunulması	Varsa kurumun hukuki birimi (s) aksi durumda KSGB (s) -kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	
2	Kurumsal Siber Olaylara müdahale biriminin (KSOM) oluşturulması ve sektörel çeşitliliğe göre Kurumsal Siber Olaylara Müdahale Ekipleri (KSOME) kurma çalışmalarının gerçekleştirilmesi	7/24 esasına göre çalışacak kurumsal siber olaylara müdahale birimi kurularak çalışma usul ve esaslarının belirlenmesi -Bu birimin gerektiğinde ulusal veya uluslararası kurum veya şirketlerle işbirliğini gerektiren durumlarda çalışma esasları, prosedürler ve süreçlerin belirlenmesi,	Yönetim kurulu(s) -Kurumsal Siber Güvenlik Birimi(i)	
		(Gerekli ise) kurumsal siber olaylara müdahale ekiplerinin oluşturulması, çalışma usul ve esaslarının belirlenerek eğitim planının yapılması ve birimlerde görev alacak personel için yardım sayfalarının hazırlanması	Kurumsal Siber Güvenlik Birimi(s)	Bir defaya mahsus yapılır ve süreç içinde gerekli güncellemeler sağlanır.
3	Kurumsal Siber Olaylara müdahale biriminin (KSOM) ve (ihtiyaç varsa) Kurumsal Siber Olaylara Müdahale Ekipleri (KSOME) faaliyetlerine başlaması	KSOM'un Ulusal Siber Olaylara Müdahale Birimine bağlı olarak çalışmasının sağlanması - KSOM VE KSOME'nin örgütlenmesinin yapılması , gerekli eğitimlerin belirlenerek alınması -KSOME'lerin KSOM koordinasyonunda faaliyetlerini yürütmesi ve desteklenmesi	Kurumsal Siber Güvenlik Birimi(s)	bir defaya mahsus yapılır ve süreç içinde gerekli geliştirmelerle desteklenir.
4	Siber saldırıların delillendirilmesi	Saldırı sonrası incelenmek üzere gerekli delillerin elde edilmesi için tutulacak kayıtların tespiti yapılarak günün teknolojisine uygun kayıt mekanizmalarının devreye alınması	Kurumsal Siber Güvenlik Birimi(s) - kurumun hukuki birimi (i) - kritik bilgi ve iletişim sistem altyapılarında görevlendirilecek etkili ve yetkili birimler(i)	

5	Kritik bilgi ve iletişim sistem altyapılarında bilgi güvenliği yönetimi programı	Siber saldırıların doğrudan hedefi haline gelen ve zarar görmesi durumunda kurum veya şirkete büyük çapta ekonomik ve sosyal zarar verebilecek kritik bilgi ve iletişim sistem alt yapılarının tespit edilmesi -Risk analiz yöntemlerinin belirlenerek risk analizinin yapılması -Acil eylem planlarının oluşturulması -Risk analizi raporlama çalışmalarının tamamlanarak yönetim kuruluna sunulması -İş sürekliliği planlarının gereksinimlerinin belirlenerek uygulanması -Güvenlik önlemlerinin belirlenmesi ve uygulanması	Kurumsal Siber Güvenlik Birimi(s) -kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	
6	Kurumsal bilgi güvenliği programı	Kurum veya şirket personelinin uyması gereken asgari güvenlik kurallarının belirlenmesi -Siber güvenlikle ilgili personele ihtiyaç doğrultusunda eğitimlerinin verilmesi ve yeterliliklerinin tespit edilmesi -Siber güvenliğe mahsus dökümanların hazırlanması, yayınlaması ve gerekli güncellemelerin yapılması	Kurumsal Siber Güvenlik Birimi(s) -kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	bir defaya mahsus yapılır ve süreç içinde gerekli güncellemeler sağlanır.
		Kritik bilgi ve iletişim sistem alt yapılarının bilişim sistemlerinin güvenliğinin yıllık test ve denetimlerinin yapılması	Yönetim kurunca belirlenecek alanında uzman bir kurum(s) ve KSGB(s) -KSOM(i) -(varsa) KSOME(i)	Her yıl bir defa yapılmalıdır
7	Siber güvenlik eğitim alt yapısının güçlendirilmesi	Kurum veya şirketin departmanlarında üst düzey yönetici konumunda bulunanların bilgilendirilmesi - Gerek siber güvenlik teknik personeline gerekte kurum içi güvenlik denetimi yapacak personele ilgili eğitimler verilerek sertifika verilmesi	KSGB(s) -Departmanların üst yöneticileri(i) -KSOM VE KSOME teknik personeli(i) -KSGB iç denetçi personeli(i)	
8	Siber güvenlik tatbikatlarının düzenlenmesi	Kurumsal olarak siber güvenlik tatbikatlarının düzenlenmesi	KSGB(s) -KSOM(i) -(varsa) KSOME(i)	Her yıl bir defa yapılmalıdır
9	Kurum içi güvenli iletişim kurallarının belirlenmesi	Kurum departmanları arasında güvenli veri paylaşımını sağlamak üzere kuralların ve prosedürlerin belirlenmesi	KSGB(s) -Kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	

10	Yazılım güvenliği programının yürütülmesi	Yazılım güvenliği ile ilgili eğitimlerin hazırlanması ve yazılım geliştiricilere verilmeye başlanması -Kritik bilgi ve iletişim sistem alt yapılarında kullanılmak üzere geliştirilen yazılımlar için programlama dili bağımsız güvenli yazılım geliştirmeye yönelik çalışmalar yapılması -Kritik bilgi ve iletişim sistem alt yapılar için geliştirilen yazılımların güvenlik ve kullanılabilirlik değerlendirmeleri kapsamında gerekli fizibilitenin hazırlanması	KSGB(s) -Kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	
11	Siber tehdit ve saldırıları önleme projesinin yürütülmesi	Siber tehditleri tespit amacıyla balküpü sistemi kurulması -Kurumsal siber saldırı raporlama sistemi kurulması ve işletilmesi -Siber tehditlerle ilgili yıllık istatistik üretilmesi -Siber tehdit ve saldırıların tespit edilmesi, izlenmesi ve önlenmesine ilişkin mekanizmaların devreye sokulması	KSGB(s)	
12	Siber güvenlik konusunda ürün ve hizmet sağlayıcıları belgelendirilmesi	Sunulan hizmet ve ürünün niteliğine uygun olarak ilgili kurum ve kuruluşlar aracılığıyla siber güvenliğe ilişkin belgelendirme çalışmalarının yapılması	KSGB(s)	
13	İş sürekliliği ve veri yedekleme sistemleri kurulması	Elektronik ortamda işlem yapan sistemlerin ve verilerin güvenlik risk seviyelerinin belirlenmesi -Kuruma ait hassas verilerin yedeklenme usul ve esaslarının belirlenmesi -İş sürekliliği planları yapılması ve bu planlara yönelik bilişim sistemlerinin kurulması	KSGB(s) -kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	
14	Kurumun internet sayfaları ve uygulamalarının kurum bünyesinde veri merkezlerine taşınması	Kurum veya şirketin internet sayfaları ve uygulamaları farklı veri merkezlerinde ise kurum içinde KSOM kontrolundeki veri merkezlerine taşınması -Bu veri merkezlerinin güvenliğine ilişkin gerekli tasarruf ve planlamaların (KSOM tarafından) yapılması	KSGB(s)	
15	Veri sızması tespitine yönelik test altyapısı geliştirilmesi ve uygulamaya başlanması	Kritik altyapılardan veri sızmasını tespit edebilecek analiz altyapısı geliştirilmesi - KSOM tarafından bu test altyapısının uygulanacağı departmanlarda ilgili testlerin yapılması ve sonuçlarının raporlanması	KSGB(s)	
16	Kurum departmanlarında veriye erişim düzeylerinin belirlenmesi	İSO 27001 gibi standartlarla uyumlu veri erişim kontrol prensiplerinin belirlenmesi -elektronik uygulamaların internet üzerinden yetkisiz erişimi engelleyecek şekilde yeniden ayarlanması	KSGB(s)	

17	Açık kaynak kodlu ürünlerin kullanımının sağlanması	Kurumun asgari siber güvenlik kriterlerini sağlayan açık kaynak kodlu mevcut güvenlik ürünleri hakkında teknik personelin bilgilendirilmesi ve bu tür açık kaynak kodlu siber güvenlik ürünlerinin geliştirilmesi için platformlar oluşturulması -Kritik bilişim sistemlerinin açık kaynak kodlu bilişim sistemlerine taşınması için gerekli planlama yapılarak uygulanması	KSGB(s)	
18	Siber güvenlik konusunda akademik eğitim alınması	Siber güvenlik konusunda kendilerini yetiştirmeleri için ilgili teknik personelin yüksek lisans ve doktora yapmaları konusunda teşvik edilmeliler - Üniversitelerin siber güvenlik hususunda çalışma yapan personellerin tespit edilerek konusunda uzman kişilerin kuruma katkıda bulunmalarına (mümkünse kuruma katılımlarını sağlamaya) dönük çalışmalar yapılmalı	KSGB(s) - İnsan kaynakları ve personel birimi(i)	
19	Siber güvenlik uzmanlığı sağlama ve geliştirmeye yönelik çalışmalar yapılması	KSOM ve (varsa) KSOME'lerde çalışan personelin eğitim alması ve uygulama deneyimi kazanması -Bu personeller arasında siber güvenliğe yönelik etkinlikler düzenleme, yarışmalar düzenlenerek ödüllendirmeler yapılması -İlgili personellerin ulusal veya uluslar arası seminer,panel ve konferans gibi etkinliklere aktif veya pasif katılımını sağlayıcı çalışmalar yapılması	KSGB(s)	Süreç içinde gerekli güncellemeler yapılır.
20	Kurumdaki elektronik uygulama kullanıcılarını siber güvenlik konusunda bilinçlendirme çalışmalarının yapılması	Elektronik uygulama kullanıcılarının siber güvenlik konusunda bilinç düzeyinin artırılması için çalışmalar yapılması(hizmet için eğitim,semineri,broşür v.b...) -İnternetin güvenli kullanımı ve "güvenli internet hizmeti" konusunda bilinç düzeyinin artırılması ve bu hizmetin geliştirilmesi ve yaygınlaştırılması	KSGB(s)	Süreç içinde gerekli güncellemeler yapılır.
21	AR -GE kapsamında siber güvenliğe ilişkin çalışmalar yapılması	Siber güvenliğe ilişkin kurumsal yazılımlar yapılması hususunda teşvikler yapılması -Siber güvenlik konusunda kurulmuş ulusal veya uluslar arası AR-GE laboratuvarlardan kurumsal ihtiyaçlar doğrultusunda azami istifade etmek ve kurumsal güvenliğe yönelik çalışmalarda kullanmak için çalışmalar yapılması -Kurumsal mevcut projeler içinde siber güvenliğin öncelikli konu olarak dahil edilmesini ve gerekli finansmanın temini sağlama	KSGB(s)	

22	Kurum olarak alınması gereken bilgi ve iletişim teknolojilerinde güvenlik sağlamaya dönük çalışmalar yapılması	Kurum departmanlarınca edinilmesi gereken bilgi ve iletişim sistemlerinde yönetimin yerli olarak üretilmiş güvenlik değerlendirilmesi ve sertifikalandırılması yapılmış ürünleri tercih etmelerini sağlama -Yerli ürün bulunmadığı takdirde güvenlik değerlendirilmesi ve sertifikalandırılması yapılmış ürünleri tercih etmelerini sağlama	KSGB(s)	
23	Kurumsal siber güvenliğin genel güvenliğe entegrasyonu	Siber ortamda çeşitli siber güvenlik olayları meydana geldiğinde departmanların sorumluluklarının ve genel koordinasyonun nasıl sağlanacağını belirlenmesi -Kurumu hedef alan olası saldırı senaryolarının ve bunların oluşturabileceği etkilerin belirlenmesi -Siber ortamda meydana gelebilecek çeşitli olaylarda devreye girecek mekanizmaların mevcut durumunun analizi ve iyileştirilmeleri için gerçekleştirilmesi gereken öncelikli eylemlerin belirlenmesi.	KSGB(s) -KSOM(i) -(varsa) KSOME(i) -kurum veya şirketin departmanlarınca görevlendirilecek etkin ve yetkili birimler(i)	

GÖRÜŞME SORULARI

Tarih:

BİRİNCİ BÖLÜM

1. Yaş :
2. Bilişim alanında hizmet verilen görev süresi :

İKİNCİ BÖLÜM

3. Kurumsal siber güvenliği sağlama adına kurumsal bazda yapılabilecekler nelerdir?

.....
.....
.....
.....

4. Kurumsal siber güvenlik eylem planı oluşturmanın kurumlara sağlayacağı faydalar nelerdir?

.....
.....
.....
.....

5. Kurumsal siber güvenlik eylem planı oluşturmanın amacını belirtiniz.

.....
.....
.....
.....

6. Kurumsal siber güvenliğin sağlanmasında size göre dikkat edilmesi gereken ilkeler nelerdir?

.....
.....
.....
.....

7. Sizce bir kurumun siber güvenlik politikalarının kapsamı (içeriği) ne şekilde oluşturulmalıdır?

.....
.....
.....
.....

8. Etkin bir kurumsal siber güvenlik sağlama adına oluşturulacak kurumsal siber güvenlik birimine(KSGB) bağlı olarak görev yapacak birimler neler olmalıdır?

.....
.....
.....
.....

9. Belirtmiş olduğunuz eylem planında bulunması gereken maddelerdeki her bir eyleme ilişkin sorumlu ve ilgili kurumsal birimler nelerdir?

.....
.....
.....
.....

10. Kurumsal siber güvenlik eylem planında bulunması gereken maddeleri gerçekleştirilme sırasına uygun olacak biçimde belirtiniz?

.....
.....
.....
.....

ÖZGEÇMİŞ**Kişisel Bilgiler**

Soyadı, adı : YAŞAR, Hakan
Uyruğu : T.C.
Doğum tarihi ve yeri : 18/12/1980 Almanya
Medeni hali : Evli
Telefon : 0 (312) 480 29 89
E-posta : hakanyasar80@gmail.com

Eğitim Derecesi**Okul/Program****Mezuniyet**

Yüksek Lisans	Gazi Üniversitesi/Bilişim Enstitüsü	devam ediyor
Lisans	YTÜ/BÖTE	2007
Lise	B.Mustafa Kemal Lisesi	1998

İş Deneyimi, Yıl**Çalıştığı yer****Görev**

2008- devam ediyor	Türk Silahlı Kuvvetleri	Subay
--------------------	-------------------------	-------

Yabancı Dili

İngilizce

Hobiler

Yüzme, kitap okuma, sinema.



GAZİ GELECEKTİR..