KURUMSAL BİLGİ GÜVENLİĞİ VE SIZMA (PENETRASYON) TESTLERİ

Yılmaz VURAL

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2007
ANKARA

Yılmaz VURAL tarafından hazırlanan KURUMSAL BİLGİ GÜVENLİĞİ VE SIZMA (PENETRASYON) TESTLERİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Şeref SAĞIROĞLU
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. Taner ALTINOK

Üye : Prof. Dr. Nazife BAYKAL

Üye : Doç. Dr. Şeref SAĞIROĞLU

Tarih : 9/05/2007

Bu tez, Gazi Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Yılmaz VURAL

KURUMSAL BİLGİ GÜVENLİĞİ VE
SIZMA (PENETRASYON) TESTLERİ
(Yüksek Lisans Tezi)

Yılmaz VURAL

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Mayıs 2007

ÖZET

Bu tez çalışmasında bilgi güvenliği genel olarak incelenmiş, kurumsal bilgi güvenliği ve standartları değerlendirilmiş, bilgi güvenliğini zaafa uğratan tehditler gözden geçirilmiş, ülkemiz bilişim hukuku incelenmiş ve yüksek tehdit altında olan web uygulamaları üzerine odaklanılmıştır. Yapılan incelemelerde web ortamlarında büyük tehdit oluşturan SQL enjeksiyonu ve sızma testleri genel olarak gözden geçirilmiş ve bu konularda uygulamalar yapılarak, konu detaylı olarak değerlendirilmiş ve alınması gereken önlemler sunulmuştur.

Yüksek seviyede bir bilgi güvenliğinin sağlanmasında önemli olan insan faktörü-teknoloji-eğitim kavramları tekrar gözden geçirilmiş ve sızma testlerinin bu faktörler üzerindeki etkisi araştırılmış, tespit edilen tehditlerin giderilmesine ve mevcut durumun iyileştirilmesine yönelik çözüm önerileri sunulmuştur.

Bu tez çalışmasının ülkemizde kurumsal bilgi güvenliği alanında yapılan kapsamlı ilk çalışma olması, ülkemizde bilgi güvenliğine gereken önemin verilmesine katkı sağlaması, kurum ve kuruluşlar için rehber bir kaynak olması, bilgi güvenliği bilincinin daha yüksek oranda oluşturulması ve yapılacak yeni çalışmalara ışık tutması beklenmektedir.

Bilim Kodu : **902.1.063**
Anahtar Kelimeler :**Kurumsal Bilgi Güvenliği, Sızma Testleri, Penetrasyon Testleri, Bilgi Güvenliği Yönetim Sistemleri, Bilgi Güvenliği, Web Uygulama Güvenliği, Sosyal Mühendislik**
Sayfa Adedi :**269**
Tez Yöneticisi : **Doç. Dr. Şeref SAĞIROĞLU**

ENTERPRISE INFORMATION SECURITY AND PENETRATION TESTING

(M.Sc. Thesis)

Yılmaz VURAL

GAZİ UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

May 2007

ABSTRACT

In this study, Information Security has been investigated, Information Security and standards have been assessed, threats which causes Information Security weaknesses overviewed, our country's Information Technology law has been examined and web applications that are facing the highest threat have been focused. During the studies, SQL injection and penetration tests that constitute high threat have been thoroughly examined. Applications in this subject have been investigated in detail, and precautions that should be taken are presented.

Concept of human factor-technology-education which is important for providing a high level of Information Security has been overviewed and effects of penetration testing on these factors have been investigated. Solution suggestions are offered to cease threats and make existing condition better and to obtain high level Enterprise Information Security.

Because of being the first comprehensive study on the field of Enterprise Information Security in Turkey, this study aims to contribute the necessary importance, being a guide source for institutions and organizations raise an awareness of Information Security and direct future studies in this field.

Science Code : **902.1.063**
Key Words : **Enterprise Information Security, Penetration Testing, Information Security Management Systems, Information Security, Web Application Security, Social Engineering**
Page Number : **269**
Adviser : **Assoc. Prof. Dr. Şeref SAĞIROĞLU**

TEŞEKKÜR

Çalışmalarım boyunca her konuda değerli yardım ve katkılarıyla beni yönlendiren, laboratuar çalışmaları için kaynaklar sunan kıymetli hocam Doç. Dr. Şeref SAĞIROĞLU'na, tez çalışması boyunca yardımlarını esirgemeyen değerli arkadaşım Yrd. Doç. Dr. Mehmet TEKEREK'e, bilgi güvenliği konusunda değerli tecrübelerini benimle paylaşan Bilgisayar Mühendisi eşim Şebnem VURAL'a zaman yönetimi ve motivasyon konusunda maddi manevi desteklerini benden esirgemeyen annem Nurten ve babam Ahmet, kardeşlerim Erdal ve Sibel VURAL'a ve çok kıymetli varlığım kızım BERİL'e teşekkürlerimi bu vesileyle bildirmeyi borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ABD	Amerika Birleşik Devletleri
ACK	Acknowledge, Onaylama paketi
ACT	Association for Competitive Technology, Rekabetçi Teknoloji Birliği
ADSL	Asymmetric Digital Subscriber Line, Asimetrik Sayısal Abone Hattı
AFRINIC	African Region Internet Registry, Afrika Bölgesi İnternet Kayıt Kurumu
ANSI	American National Standards Institute, Ulusal Amerikan Standartları Enstitüsü
API	Application Programming Interface, Uygulama Programlama Arabirimi
APNIC	Asia-Pacific Network Information Centre, Asya/Pasifik Bölgesi Kayıt Kurumu
ARIN	American Registry for Internet Numbers, Amerika Bölgesi Kayıt Kurumu
ARP	Address Resolution Protocol, Adres Çözümleme Protokolü
ARPANET	Advanced Research Projects Agency Network, İleri Araştırma Projeleri Ajansı Bilgisayar Ağı
ASP	Active Server Pages, Etkin Sunucu Sayfaları
AT&T	American Telephone & Telegraph Company, ABD Telefon ve Telgraf Şirketi
BBS	Bulletin Board System, Mesaj Pano Sistemleri
BGYS	Bilgi Güvenliği Yönetim Sistemi

Kısaltmalar	Açıklamalar
BSDI	Berkeley Software Design, Berkeley Yazılım Tasarım Şirketi
BSI	British Standards Institute, İngiliz Standartlar Enstitüsü
BT	Bilgi Teknolojileri
CERT	Computer Emergency Response Team, Bilgisayar Acil Durum Ekibi
CGI	Common Gateway Interface, Ortak Geçiş Arayüzü
CPU	Central Processing Unit, Merkezi İşlem Birimi
CSI	The Computer Security Institute, Bilgisayar Güvenlik Enstitüsü
CVE	Common Vulnerabilities and Exposures, Bilinen Güvenlik Zafiyetleri
DACL	Discretionary Access Control List, İsteğe Bağlı Erişim Denetim Listeleri
DARPA	Defense Advanced Research Projects Agency, ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı
DEC	Digital Equipment Corporation, Bilgisayar Firması
DHCP	Dynamic Host Configuration Protocol, Dinamik İstemci Ayarlama Protokolü
DNS	Domain Name Server, Bölge Ad Sunucusu
DOM	Document Object Model, Belge Nesne Modeli
DoS	Denial of Service, Servis Aksattırma
EAP	Extensible Authentication Protocol, Genişletilebilir Kimlik Doğrulama Protokolü
EMEA	Europe, the Middle East and Africa, Avrupa, Ortadoğu ve Afrika
FBE	Fen Bilimleri Enstitiüsü

Kısaltmalar	Açıklamalar
FBI	Federal Bureau of Investigation, Federal Araştırma Bürosu
FIN	Finish Packet, Bitiş kontrol biti bir olan herhangi bir paket
FISMA	Federal Information Security Management Act, Federal Bilgi Güvenliği Yönetimi Yasası
FTP	File Transfer Protocol, Dosya Aktarım Protokolü
GÜ	Gazi Üniversitesi
GD	Güvenlik Duvarı
GHDB	Google Hacking Database, Google Saldırı Veritabanı
GLBA	Gramm-Leach-Bliley Act, Gramm-Leach-Bliley Yasası
GNU	General Public License, Genel Kamu Lisansı
HIPAA	Health Insurance Portability and Accountability Act, Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası
HP/UX	Hewlett Packard ve Unix
HTML	Hypertext Markup Language, Hipermetin İşaret Dili
HTTP	Hypertext Transfer Protocol, Hipermetin Aktarma İletişim Protokolü
IANA	Internet Assigned Numbers Authority, İnternet Atanmış Numaralar Yetkilisi
ICMP	Internet Control Message Protocol, Internet Denetim Mesaj Protokolü
IDS	Intrusion Detection System, Saldırı Tespit Sistemi
IEC	The International Electrotechnical Organization, Uluslararası Elektroteknik Komisyonunu
IEEE	Institute of Electrical and Electronics Engineers, Elektrik Elektronik Mühendisleri Enstitüsü
IGI	Investigative Group International, Uluslararası Araştırma Grubu Firması

Kısaltmalar	Açıklamalar
IM	Instant Messaging, Anlık Mesajlaşma
IMAP	Internet Message Access Protocol, İnternet Mesaj Erişim Protokolü
IP	Internet Protocol, İnternet Protokolü
IPC	Inter-Process Communication, Prosesler Arası Haberleşme
IPS	Intrusion Prevention System, Saldırı Önleme Sistemi
IRIX	Unix Tabanlı İşletim Sistemi
ISACA	Information Systems Audit and Control Association, Bilgi Sistemleri Denetimi ve Kontrolü Birliği
ISECOM	The Institute for Security and Open Methodologies, Güvenlik ve Açık Kaynaklar Enstitüsü
ISF	The Information Security Forum, Bilgi Güvenliği Forumu
ISF	Information Security Forum, Bilgi Güvenliği Forumu
ISN	Initial Sequence Number, Başlangıç Sıra Numarası
ISO	International Organization for Standardization, Uluslararası Standardizasyon Kurumu
ISP	Internet Service Providers, İnternet Servis Sağlayıcıları
ISS	Internet Security Systems, İnternet Güvenlik Sistemleri Firması
JSP	Java Server Pages, Java Sunucu Sayfaları
JTC	Joint Technical Committee, Birleşik Teknik Kurul
KBG	Kurumsal Bilgi Güvenliği
KGB	Komit Gosudarstvennoy Bezopasnosi, Sovyet Gizli Servisi
LACNIC	Latin American and Caribbean Internet Addresses Registry, Latin Amerika ve Karayip Adaları Bölgesi İnternet Kayıt Kurumu

Kısaltmalar	Açıklamalar
LAN	Local Area Network, Yerel Alan Ağı
LDAP	Lightweight Directory Access Protocol, Kolay Dizin Erişim Protokolü
MAC	Media Access Control, Ortam Erişim Denetimi
MIT	Massachusetts Institute of Technology, Massachusetts Teknoloji Enstitüsü
MSN	Microsoft Network, Microsoft Ağı
MVS	Multiple Virtual Storage, Çoklu Sanal Depolama
NASD	National Association of Securities Dealers, Hisse Senedi Alım-Satımcıları Ulusal Derneği
NAT	Network Address Translation, Ağ Adres Çevirimi
NISER	National ICT Security & Emergency Response Center, Malezya Bilgi ve İletişim Teknolojileri Ulusal Güvenlik ve Acil Durum Merkezi
NIST	National Institute of Standards and Technology, ABD Teknoloji ve Standartlar Enstitüsü
NOP	No Operation, Makine dilinde işlem yok komutu
NTFS	New Technology File System, Yeni Teknoloji Dosya Sistemi
OSSTMM	The Open Source Security Testing Methodology Manual, Açık Kaynak Güvenlik Testleri Yöntemler Kılavuzu
OWASP	The Open Web Application Security Project, Açık Kaynak Web Uygulama Güvenliği Projesi
PDF	Portable Document Format, Taşınabilir Belge Biçemi
PDP–1	Programmed Data Processor, DEC tarafından geliştirilen klavye ve fareye sahip ilk bilgisayar
PHP	Hypertext Preprocessor, Hipermetin Ön İşlemci Betik Dili
PIN	Personal Identification Number, Kişisel Kimlik Numarası

Kısaltmalar	Açıklamalar
PING	Packet Internet Groper, İnternet Yoklayıcı Paketi
POP3	Post Office Protocol Version 3, E-posta iletişim protokolü
PUKÖ	Planla–Uygula–Kontrol Et–Önlem Al
RFC	Request For Comments, Yorumlar İçin Rica
RIP	Routing Information Protocol, Yönlendirme Bilgisi Protokolü
RIPE NCC	Reseaux IP Europens Network Coordination Center, Avrupa, Ortadoğu ve Asya'nın bir kısmı için yetkili olan IP dağıtım merkezi
RSH	Remote Shell, Uzaktan komut çalıştırma
RST	Reset, Sıfırlama
RTÜK	Radyo ve Televizyon Üst Kurulu
SAN	Storage Area Network, Veri Depolama Ağı
SATAN	Security Administrator Tool for Analyzing Networks, Ağların Çözümlenmesi İçin Güvenlik Yöneticisi Aracı
SC	SubCommittee, Alt Komisyon
SEAL	Securing External Access Link, Harici Güvenlik Erişim Hattı
SEC	Securities and Exchange Commission, Menkul Kıymetler ve Borsalar Komisyonu
SMTP	Simple Mail Transfer Protokolü, Basit Posta Gönderme Protokolü
SNMP	Simple Network Management Protocol, Basit Ağ Yönetimi Protokolü
SOA	Statement of Applicability, Uygulanabilirlik Beyannamesi
SOX	Sarbanes-Oxley Yasası
SQL	Structured Query Language, Yapısal Sorgulama Dili

Kısaltmalar	Açıklamalar
SSI	Server Side Includes, Sunucu Taraflı Betik
SYN	Synchronize, Senkronize
TBB	Türkiye Bankalar Birliği
TCB	Trusted Computing Base, Güvenli Hesaplama Esasları
TCK	Türk Ceza Kanunu
TCP	Transmission Control Protocol, İletim Kontrol Protokolü
TCSEC	Trusted Computer System Evaluation Criteria, ve Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri
TEMPEST	Transient Electro Magnetic Pulse Emanation Standard, Elektromanyetik Salınım ve Yayılım Standardı
TFTP	Trivial File Transfer Protocol, Önemsiz Dosya Aktarım Protokolü
TKIP	Temporal Key Integrity Protocol, Geçici Anahtar Bütünlük Protokolü
TOS	Type of Service, Hizmet Türü
TSE	Türk Standartları Enstitüsü
TTL	Time To Live, Artan Yaşam Süresi
TÜBİTAK	Türkiye Bilimsel ve Teknik Araştırma Kurumu
UDP	User Datagram Protocol, Kullanıcı Veri Protokolü
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UKAS	United Kingdom Accreditaion Service, İngiltere Akreditasyon Kurumu
URG	Urgent Flag, Acil Bayrağı
URL	Uniform Resource Locator, Tekdüze Kaynak Konumlayıcı
US-CERT	The United States Computer Emergency Readiness Team, ABD Bilgisayar Acil Durum Hazırlık Ekibi

Kısaltmalar	Açıklamalar
VPN	Vitual Private Network, Sanal Özel Ağ
WASC	The Web Application Security Consortium, Web Uygulamaları Güvenlik Konsorsiyumu
WEP	Wired Equivalent Privacy, Kabloya Eşdeğer Mahremiyet Güvenlik Protokolü
WG	Working Group, Çalışma Grubu
WPA	Wireless Fidelity (Wi-Fi) Protected Access, Kablosuz Bağlantı Korumalı Erişim
XSS	Cross Site Script, Çapraz Site Kod Çalıştırma

1. GİRİŞ

Bilgi; tarih boyunca insanoğlunun düşüncesini, yaşayışını, davranışını, gelişimini belirleyen faktörlerin başında gelen büyük bir güç olarak yerini korumuştur. Bilişim teknolojilerinin hızla yaygınlaşmasıyla; bilginin yönetilmesi, iş verimliliğin ve akışlarının hızlandırılması, çalışanlar ve diğer kurumlarla daha hızlı iletişim kurulabilmesi sağlanmış, hayatımız kolaylaşmış, üretilen ve tüketilen bilgilerde de artışlar olmuştur. Bunun sonucu olarak, elektronik ortamlarda bilginin işlenmesi, taşınması ve saklanması kolaylaşmış, bilgiye mekândan bağımsız olarak istenilen ortamlardan erişilmesi sağlanmıştır. Günlük yaşantımızda yapmış olduğumuz birçok iş ve işlem ise kolaylıkla ve hızlıca yapılabilir hale gelmiştir. Bankacılık işlemlerini bankaya gitmeden ev, iş yerindeki bilgisayarlardan veya cep telefonundan yapmak, vergi dairesine gitmeden vergi ve ceza ödemeleri yapmak, fatura ödemek, pasaport başvurusunda bulunmak, otel rezervasyonları yapmak, uçak bileti satın almak, çalıntı cep telefonlarını sorgulamak, sınav sonuçlarını öğrenmek, öğrenci kayıtlarını yaptırmak, hastane tetkik sonuçlarını almak ve uzaktan eğitim, bilgi ve iletişimde gelinen noktaya verilebilecek örneklerdir.

Elektronik ortamlarda kişiler ve kurumların sahip olduğu bilgilerin mahremiyetlerinin korunması, bu ortamların yaygınlaşmasının önünün açılması ve bu ortamlarda herhangi bir kaybın oluşmaması için bu ortamlarda bulunan bilgilerin güvenliğinin sağlanması gereklidir. Bilgi güvenliğini sağlamak toplumda sadece güvenlikle uğraşan kişi ve kuruluşların görevi değil bilgi çağı olarak adlandırılan günümüzde bilgi sistemlerinin küreselleşmesi sonucunda bu sistemlerle herhangi bir şekilde doğrudan veya dolaylı yönden ilişkisi olan ve bu sistemleri kullanan tüm birey, kurum ve kuruluşların katkıda bulunması ve görev alması gereken önemli bir konu halini almıştır.

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda elektronik ortamlarda bulunan bilgilerin her iki ayda neredeyse iki katına çıkmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel veya kurumsal olarak en üst seviyelere çıkmıştır. Bunun önemli sebepleri iş veya günlük yaşamın bir parçası haline gelen

elektronik uygulamaların artması, ihtiyaç duyulan bilgilerin ağ sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir.

Hayatımızı kolaylaştırması iş ve işlemlerin hızlandırılmasına katkılar sağlayan bilgi teknolojileri insan hayatında günden güne daha da önem kazanmakta ve her geçen gün güvenliği üst düzeyde sağlanan güvenilir bilgi sistemlerine duyulan ihtiyaç artmaktadır [1]. Herhangi bir bilgisayar ağında meydana gelen güvenlik ihlali bir anda o ağın bağlı olduğu diğer tüm ağları etkileyebilmektedir. Bu kurumsal ağlar üzerinden haberleşen, sayıları hızla artarak yaygınlaşan ve geniş kitlelerce kullanılan uygulamalar üzerinde tutulan bilgilerin değeri düşünüldüğünde kurumsal anlamda bilgi güvenliğinin sağlanmasının önemi daha iyi anlaşılacaktır.

Elektronik ortamlarda verilen hizmetlerin (e-ticaret, e-kurum, e-devlet, e-ödeme, e-öğrenme, vb.) sayısı her geçen gün artmakta ve bu ortamların kullanımı ise yaygınlaşmaktadır. Elektronik ortamlarda kurumlar tarafından verilen hizmetler yaygınlaştıkça, saldırganlar için bu hizmetlerin verildiği sistemler cazibe merkezi haline gelmektedir. İçerisinde önemli bilgiler (kurumsal ve kişisel) barındıran bilgi sistemlerinin güvenliğinin sağlanması ve yönetimi önem kazanmıştır. Bilgi teknolojileriyle birilikte geliştirilen yeni uygulamalar bir yandan hayatımızı kolaylaştırırken diğer yandan yeni güvenlik tehditlerini beraberinde getirmektedir. Kişilerin ve kurumların sahip oldukları önemli bilgiler, çeşitli sahtekârlıklar, bilgi hırsızlığı, korsan saldırıları, bilgi sızdırma ve kötü niyetli kurum çalışanlarınca oluşturulabilecek iç saldırılar gibi çok geniş bir yelpazeye sahip kaynaklardan gelen tehdit ve tehlikelerle karşı karşıyadır. Bilgi güvenliğini tehdit eden unsurlar sadece elektronik ortamda yapılan saldırılarla sınırlı değildir. İnsan hataları, yangın, sel, deprem, terör saldırıları, sabotaj gibi istenmeyen olaylar veya doğal felaketler sonucunda da bilgiler ve bilgi sistemleri tamamen ya da kısmen zarar görmektedir.

Günümüzde elektronik ortamda yapılan güvenlik ihlâllerinden hemen hemen her gün bahsedilmektedir. Bu durumdan elektronik ortamda hizmet veren kuruluşlar da hizmet alan kullanıcılar da etkilenmektedir. Örneğin internet bankacılığı yapan

kullanıcılar dolandırıldığı zaman; parasını kaybederken, o hizmeti sağlayan banka ise müşterilerinin gözünde güven kaybına uğrayarak ticari itibarını kaybetme tehlikesiyle karşı karşıya kalmaktadır. Bu ve buna benzer tehditlerden etkilenmeyi en aza indirmek için kurumlara, kuruluşlara ve kullanıcılara düşen önemli görevler vardır. Kullanıcıların bilgi güvenliği konusunda bilinçli olmaları gerekirken, kurumların bilgi güvenliği konusunda kurumsal önlemler almaları ise mutlaka yapılması gereken görevler arasındadır. Kullanıcılar bilgi güvenliği hakkında alacakları bilinçlendirme ve bilgilendirme eğitimleri sayesinde kendi üzerine düşen görevleri bilerek ve uygulayarak gerekli korumayı sağlamış olacaklardır. Kurumlar ise kurumsal bilgi güvenliği kavramının temel gereği olan bilgi güvenliği standartlarına uyumluluk kapsamında altyapılarını uzman kuruluşlardan yardım alarak gözden geçirmeli ve gözden geçirme sonucunda ortaya çıkan ihtiyaçlara bağlı olarak alınması gereken önlemleri ve yatırımları zamanında yapmalıdır. Bireyler ve kurumların dışında devletimize de düşen önemli görevler vardır. Bu görevlerin en başında bilgi güvenliğinin sağlanmasıyla ilgili yasaların çıkartılarak hukuksal boşlukların doldurulması ve yeni düzenlemelerin hızlıca yapılması gerekmektedir. Diğer önemli bir konu ise bilgi güvenliği eğitiminin verilebilmesi ve ülke genelinde bilgi güvenliği bilincinin yaygınlaştırılabilmesi amacıyla gerekli olan çalışmaların ve düzenlemelerin yapılmasıdır.

Kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını doğrudan veya dolaylı olarak kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Kurumsal bilgi varlıklarının güvenliği sağlanmadıkça, kişisel güvenlikte sağlanamaz.

Ülkemizde son yıllarda sayıları yetersiz de olsa sunulan güvenlik raporlarında kurumsal bilgi güvenliği konusunda kurumlarımızın yeterince duyarlı olmadığı ve gerekli olan önlemleri genellikle bilgisizlik, maddi gerekçeler, personel gibi sebeplerden dolayı alamadıkları tespit edilmiştir. Kurumlar yeni teknolojileri veya

kendi uzmanlıkları dışında uzmanlık gerektiren alanları takip etmeyi ve kurumsal altyapılarını buna uyarlama çalışmalarını mevcut kısıtlı kaynaklar nedeniyle başaramamaktadırlar. Kurumların bilgi güvenliği konusunda alanında uzman olan güvenlik profesyonellerine ihtiyaçları vardır. Ancak ülkemizde kurumların kendi bünyesinde bilgi güvenliği alanında yetişmiş eleman sayısı yok denecek kadar azdır. Kurumların bilgi güvenliği alandaki uzmanlık açığını kapatmaları için dış kaynak (Outsource) kullanmaları zorunlu hale gelmiştir. Doğru seçilen dış kaynak kullanımında alınan hizmetin servis kalitesi yüksek olacağından bilgi güvenliği ihlallerinin birçoğu önceden tespit edilecek ve kurumların zararı minimuma inebilecektir.

Alınan birçok önleme geliştirilen birçok yeni donanım ve yazılıma rağmen bilgi teknolojilerine yönelik güvenlik saldırıları her geçen gün hızla artmaktadır. Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırılar ciddi ve giderilemeyecek kayıplara yol açmaktadır. Bu kayıpları tamamen yok etmek mümkün değildir. Ancak önceden veya zamanında alınacak güvenlik tedbirleriyle kayıpları en aza indirmek mümkündür. Kurumlar tarafından güvenlik tedbirleri alınırken göz önüne alınması gereken önemli noktalar vardır. Öncelikli olarak alınan tedbirlerin çalışanlar tarafından benimsenmesi ve sahiplenilmesi gerekmektedir. İkinci önemli nokta ise korunması gereken bilgi varlıklarının koruma maliyetinin göz önünde tutulmasıdır. Koruma maliyetinin, hasar olasılığı * hasarın değeri * hasarın etkisi çarpımlarının toplam değerinden küçük olması dikkate alınmalıdır. Son olarak kullanıcıların tepkileri (performans kaybı, erişim engellemesi, prosedürsel yaptırımlar, vb.) ve yönetimsel zorluklar dikkate alınarak gerekli planlamalar yapılarak arzu edilen güvenlik düzeyinde koruma veya korunma sağlanmalıdır.

Bilgi sistemlerine saldırıların yapılabilmesi için gerekli olan bilgi ve beceri seviyeleri hızla azalırken otomatik araçlar aracılığıyla yeni saldırı yöntemleri geliştirilmekte, bilgi sistemlerine zarar verecek olan saldırgan sayısı her geçen gün artmakta ve koruma teknolojileri saldırı tekniklerinin hep bir adım arkasında kalmaktadır.

Literatürde son yıllarda meydana gelen bilgi güvenliği olayları incelenerek aşağıda paragraflar halinde kısaca özetlenmiştir.

Güvenli olarak bilinen PDF (Portable Document Format) biçimindeki dokümanlar çok yaygın şekilde internet üzerinde kullanılmaktadır. Hemen hemen her kullanıcı internette gezinirken PDF dokümanlarına genelde hiç tereddüt etmeden tıklayarak tarayıcıları içerisinde açmaktadırlar. Alman saldırı grubu olan Chaos Computer Club, yıllık konferansında Adobe Reader'da bir güvenlik açığı bulunduğunu 3 Ocak 2007 tarihinde rapor etmiştir [2]. Bu açıkta Adobe Reader programının, PDF'lerin tarayıcı penceresinden okunmasını sağlayan eklentisi (plug-in), bir güvenlik açığını da beraberinde getirmektedir. Bu açığa göre kullanıcı, herhangi bir web sayfasında bir PDF bağlantısına tıkladığında, JavaScript koduyla yazılmış bir dizi komut da arka planda çalıştırılabilmektedir. Kullanıcı hiçbir şeyden habersiz dokümanı incelerken, bu komutlar sayesinde kullanıcı bilgisayarı içerisinde dosyaları açmak, silmek ve hatta casus programları çalıştırmak bile mümkün olmaktadır.

2005 yılında yaygın olarak kullanılan ve 2006 yılının son aylarına damgasını vuran sazan avlama (phishing) saldırganlar tarafından kullanılan etkili bir saldırı yöntemidir. Geçmiş yıllarda bilgi sistemlerine en büyük zararları veren virüsler 2006 yılı itibariyle yerlerini casus programların sazan avlama yöntemiyle kullanıldığı saldırılara bırakmıştır. Dünyada olduğu gibi ülkemizde de sıkça karşılaşılan bu yöntemde genellikle bilgi güvenliği bilinci olmayan kullanıcılar kurban olarak seçilmekte ve internet bankacılığı odaklı soygunlar yapılmaktadır. Sazan avlama çalışma grubu (Anti-Phishing Working Group) tarafından Temmuz 2006 tarihinde yayınlanan aylık rapora göre 14,191 web sitesi üzerinde kimlik hırsızlığı, soygun ve diğer kötücül amaçlar için kullanılan 23,670 tekil sazan avlama vakası tespit edilmiştir [3]. Yine bu konuda dünyaca ünlü güvenlik firması Netcraft tarafından verilen rakamlar tehlikenin hangi hızla ilerlediğinin gösterilmesi açısından önemlidir. Netcraft firması tarafından geliştirilen ve web tarayıcılarıyla bütünleşik olarak çalışan güvenlik yazılımı sayesinde sazan avlama saldırıları konusunda yapılan incelemelerde 2005 yılında 41.000 olan saldırı sayısının 2006 yılı sonunda 609.000'e çıktığı gözlemlenmiştir [4]. Sazan avlama konusunda Messagelabs firması tarafından yapılan bir başka araştırmada Netcraft firmasının sonuçlarını desteklemektedir. Ocak 2006 tarihi itibariyle %10,6 olan sazan posta oranı Aralık 2006 sonu itibariyle %68,6 gibi yüksek bir rakama çıkmıştır. Bu artışın 2005 yılı genelinde %13,1 olduğu göz

önüne alındığında 2006 yılındaki rakamın ne kadar büyük olduğu görülmektedir [5]. Ülkemizde sazan avlama ve benzeri saldırı teknikleriyle ilgili araştırmalar yapılmadığından, bu konuda istatistikler verilememiştir. Ancak bu tür araştırmaların bilgi güvenliğine önem veren gelişmiş ülkelerde yapıldığını (A.B.D. İngiltere, Avustralya, vb.) göz önüne alırsak ülkemizde durumun daha da kötü olduğu ortaya çıkacaktır. Buradan da anlaşılacağı gibi önümüzdeki yıllarda çok yüksek teknik bilgiler üzerine kurulu saldırılardan ziyade bilgi güvenliği bilincine haiz olmayan kişilerin kandırılması sonucunda ortaya çıkan güvenlik açıklarının saldırganlar tarafından ustaca kullanılacağı tahmin edilmektedir. Bu tipteki saldırılarla kullanıcıların kandırılmasını önlemenin yegâne yolunun eğitim ve bilinçlendirme olduğu unutulmamalıdır.

Bilgi güvenliği alanında yaşanan güvenlik ihlallerinin giderek artan bir bölümü ağ ve sistemlerden yazılımlara (uygulamalara) doğru kaymaktadır. Kurum bazında veya birey bazında güvenli ortamlarda iş yapma ihtiyaç ve istekleri her geçen gün hızla artmakta, kullanılan yazılımların güvenliği bilgi güvenliğinin sağlanmasında anahtar rol oynamaktadır [6]. Yıllar içerisinde ağ ve sistemlerin güvenliğinin sağlanmasına ilişkin geliştirilen yöntemler kurumlar tarafından başarıyla uygulanmış ve Sınır Ağ Güvenliği (Perimeter Network Security) kavramının önemi çoğu kuruluş tarafından anlaşılmış ve gerekleri yerine getirilmiştir. Ancak benzer durumu yazılım güvenliği için belirtmek zordur. Bilgi güvenliğinin sağlanmasında yazılım güvenliği merkezi ve kritik bir öneme sahiptir [7]. Günümüzde ağ ortamlarında çalışan kişiler ve diğer uygulamalar tarafından erişilebilen uygulama yazılımlarındaki güvenlik zafiyetleri bilgi güvenliği tehditlerinin başında gelmektedir. Özellikle internet ortamında çalışan yazılımlara güvenlik göz ardı edilerek esneklik ve kullanım kolaylığı altında bir sürü eklentiler yapılması ise yangın halinde olan bir binaya benzin dökmekle eş anlamlıdır. Başlıca yazılım güvenliği tehditleri incelendiğinde çevresel değişkenler, bellek taşmaları, enjeksiyonlar, güvensiz ağ ve haberleşme ortamları, varsayılan sistem ayarları, programcı arka kapıları bilinmesi ve önlem alınması gereken önemli zafiyetlerdir [8]. Yazılımlardaki zafiyetlerin artarak güvenlik problemlerinin her geçen gün arttığı US-CERT (The United States Computer Emergency Readiness Team) koordinasyon merkezi tarafından yıllık olarak yayınlanan rapor ve istatistikî

veriler incelendiğinde açıkça görülmektedir. US-CERT tarafından açıklanan güvenlik zafiyetleri 2004 yılında 3,780 iken, 2005 yılında 5,990'a ulaşmış 2006 yılında ise 8,064 olarak rapor edilmiştir [9].

Gartner ve Deloitte gibi bağımsız araştırma kuruluşlarının raporları incelendiğinde kurum ve kuruluşların güvenlik teknolojilerine yeterli ölçüde yatırım yapmadıkları görülmektedir. Deloitte firmasının 30 ülkede 2006 yılında gerçekleştirdiği araştırmada kurumların %73'nün güvenlik yatırımı yaptığı, yatırım yapan firmaların bilgi işlem müdürlerinin %54'nün ise bu yatırımları yetersiz buldukları belirtilmiştir [10]. Türkiye'de yapılan araştırmalarda ise 2005 yılı bilişim genel yatırımları 19 milyar dolar iken güvenlik yatırımları 30 milyon dolar, 2006 yılında bilişim yatırımları 23 milyar dolar iken güvenlik yatırımları 40 milyon dolara ulaşmakta ve 2007 yılında ise 47 milyon dolar olması beklenmektedir [10]. Bilgi güvenliğinin sağlanmasına yönelik kurumlar tarafından maddi yatırımlar yapılmadığında meydana gelen zararların ekonomik boyutu her geçen gün katlanarak artmaktadır. Bilgi güvenliği ihlallerinin meydana getirdiği zararlar yapılması gereken güvenlik yatırımlarıyla kıyaslandığında farkın çok büyük olduğu güvenlik firmalarının yapmış olduğu araştırmalar tarafından açıkça görülmektedir. Dünyada ve ülkemizde bilgi güvenliği alanında yapılan araştırmalara tez çalışmasının 2. bölümünde geniş olarak yer verilmiştir.

Kurumsal bilgi güvenliği insan, eğitim, teknoloji gibi birçok faktörün etki ettiği yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır. Bu süreçlerin yönetilmesi, güvenlik sistemlerinin uluslararası standartlarda yapılandırılması ve yüksek seviyede bilgi güvenliği sağlanması amacıyla tüm dünyada kurumsal bilgi güvenliğinin yönetimi konusunda standartlaşma çalışmaları hızla sürmektedir. Standartlaşma konusuna önderlik eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799 sonrasında ise ISO–27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir [11]. Ülkemizde Avrupa Birliği Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar yetersiz olup bu standardı uygulayan kurum ve kuruluşların sayısı yok denecek kadar azdır. ISO–27001:2005 standardı

ülkemizde Türk Standartları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 “Bilgi Güvenliği Yönetim Sistemi” standardı adı altında yayınlanmış ve belgeleme çalışmaları başlatılmıştır. Bu standart kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde sağlanabilmesi amacıyla; gizlilik, bütünlük ve erişilebilirlik gibi güvenlik unsurlarının kurumlar tarafından sağlanması gerekmektedir.

Bilgi güvenliği bilginin üretildiği, işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bilginin korunmasına çalışıldığı ilk günden itibaren güvenlik zincirinin en zayıf halkasını her zaman insanlar oluşturmuşlardır [12]. Birçok teknik veya teknik olmayan güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan faktörü kullanılarak çeşitli yöntemlerle aşılabilmektedir. Genel bir söylem olan “gücünüz en zayıf halkanız kadardır” ilkesi bilgi güvenliği içinde geçerlidir [13]. Bilgi güvenliğini en üst düzeyde tehdit eden ve güvenlik kontrollerinin aşılmasını sağlayan önemli risklerin başında insan faktörü gelmektedir. Bilgiye erişen, onu yönlendiren ve kullanan insanların karşılaşabileceği riskleri görmezden gelmek kurumsal bilgi güvenliği açısından kurumların yapabileceği en ciddi hatalardan bir tanesidir.

Günümüzde saldırganlar teknolojik olmayan ve engellenmesi daha zor olan sosyal teknikleri daha fazla tercih etmektedirler. İnsan faktörünü kullanarak bilgi güvenliği ihlalleri oluşmasını sağlayan aldatmaca sanatı teknik yöntemlere göre daha tehlikeli sonuçların oluşmasını sağlayan önemli bir saldırı aracıdır [14]. Sosyal mühendis olarak adlandırılan aldatma sanatçılarının amaçları bilgiye erişim yetkisi olan kullanıcılar aracılığıyla güvenlik teknolojilerinin atlatılmasını (by-pass) sağlamaktır. Teknolojik önlemler sosyal mühendislik saldırılarından kurumları koruyamaz çünkü saldırganların hedefinde ne güvenlik duvarı, ne veri tabanı ne de bir web sunucusu vardır. Onlar için hedef sadece insanlardır [15]. Eğer hedef bir yazılım olsaydı yazılımın zafiyetini gidermek için yamalar yazılarak veya yeniden kodlanarak güvenli hale getirilebilirdi. Ancak söz konusu insan olduğundan güvenlik zafiyeti çalışanların bilgi güvenliği konusunda yeterli bilince ve bilgiye sahip olmasıyla

giderilebilmektedir. Sosyal mühendislik tekniklerinin önümüzdeki yıllarda dünyada ve ülkemizde daha etkili olması beklenmektedir.

Güvenlik sadece teknoloji problemi olarak değil aynı zamanda insan ve yönetim problemi olarak değerlendirilmelidir [16]. Kurumlarda insan ve yönetim hatalarından kaynaklanan güvenlik ihlallerinin sebeplerine bakıldığında son kullanıcılardan üst yönetime kadar farklı kademelerde çalışan insanların ortak eksikliklerinin eğitim ve bilinçlendirme olduğu görülür. Kurumun stratejik hedeflerini belirleyen en üst seviyedeki yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek çok önemlidir. Bilgi güvenliğinin sağlanması için gerekli olan idari ve mali kararların verilebilmesi amacıyla yönetim tarafından bilgi güvenliği birimi kurulmalıdır. Bu birim tarafından güvenlikle ilgili stratejik kararlar zamanında ve doğru bir şekilde alınmalıdır. Yönetim tarafından bilgi güvenlik biriminin kurulması ve etkin bir yapıda çalışması yönetimin kurumsal bilgi güvenliğini sahiplendiğinin ve desteklediğinin önemli bir göstergesidir.

Web üzerinden yapılan ve hayatımızı kolaylaştıran uygulamaların başında gelen saldırganların bir numaralı hedefi olan internet bankacılığı, üzerinde önemle durulması gerekmektedir. Dünyada ve ülkemizde yayınlanan güvenlik raporlarına göre internet bankacılığı alanında yaşanılan dolandırıcılık olayları hızla artmakta ve sazan avlama, casus yazılımlar ve sosyal mühendislik kullanılan yöntemlerinin başında gelmektedir. Türkiye Bankalar Birliği'nin (TBB) Eylül 2006 verilerine göre15 milyon 510 bin bireysel müşteriden 2 milyon 605 bininin, 812 bin kurumsal müşteriden de 380 bininin internet bankacılığını kullandığı, 2005 yılı sonu itibariyle internet bankacılığını aktif olarak kullanan bireysel müşteri oranının yüzde 22 iken 2006 yılı sonunda güvenlik sorunları nedeniyle bu oranın yüzde 17'ye gerilediği, Eylül 2006 itibariyle internet bankacılığı yoluyla yapılan finansal işlem sayısının 37 milyon 722 bine, işlem tutarının ise 109,7 milyar YTL' ye ulaştığı belirtilmiştir [17]. TBB tarafından açıklanan veriler kurumsal bilgi güvenliğinin sağlanamadığı durumlarda bilgi sistemlerinin kullanılmamasının ispatı ve internet bankacılığının saldırıların odağı olmasındaki mali boyutunun öğrenilmesi açısından önem taşımaktadır. Bilgi güvenliği konusunun kurumsal bilgi sistemlerinin kullanılmasında

ve yaygınlaştırılmasında önemli bir rol oynadığı göz önüne alındığında, ülkemizin bilişim teknolojileri açısından ilerlemesine doğrudan katkısı olan kurumsal bilgi güvenliği konusunda yapılan çalışmaların kurumsal bilgi güvenliğine büyük katkılar sağlayacağı ortadır.

Literatürde bahsedilen ve yukarıda paragraflar halinde kısaca özetlenen güvenlik ihlallerinin oluşmasına sebep olan birçok zafiyet vardır. Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında bu zafiyetlerin giderilmesi, güvenlik bileşenlerinin güvenli biçimde kurulumu ve işletimi kontrollerin etkin biçimde uygulanıp uygulanmadığını anlamanın tek yolu bilgi sistemlerini sızma testleriyle (Penetration Testing) test etmekten geçmektedir. Sızma testleri felaket başa gelmeden önce, onu önleyecek ve ona karşı savunulacak ihtiyaçların ve tedbirlerin alınmasında kullanılan önemli bir erken uyarı sistemidir. Sızma testlerinin başarılı olabilmesi için kurumların güvenliğine etki eden faktörlerinin ağırlıkları dikkate alınarak kurumlara özgü farklı senaryolar geliştirilmesi gereklidir. Sızma testleri için geliştirilen senaryolar kurumlarda kullanılan teknolojilere, çalışanların bilgi düzeylerine, kurumsal bilgi güvenliği seviyesine, bilgi güvenliği bileşenlerinin dozuna göre farklılık gösterebilir.

Yapılan araştırmalar sonucunda ülkemizde sızma testlerinin henüz yaygınlaşmadığı ve kurumlar tarafından kurumsal bilgi güvenliğinin sağlanmasında bir bileşen olarak kullanılmadığı tespit edilmiştir. Bu durum sızma testlerinin ülkemizde pek bilinmediğinin ve yeterince önem verilmediğinin göstergesidir. Ülkemizde çok az sayıda olan güvenlik firmalarıyla sızma testleri konusunda görüşmeler yapılmış ve izlediği metodolojiler hakkında bilgiler edinilmeye çalışılmıştır. Çoğunluğunun sızma testlerini piyasadaki hazır araçlar (zafiyet tarama, port tarama, şifre kırma, vb.) kullanarak yaptıkları tespit edilmiştir. Ancak sadece otomatik araçlarla yapılan teknik içerikli sızma testlerinin sonuçları kurumsal bilgi güvenliğinin ölçümünde gerçek durumu yansıtamayacağından bu çalışmada açıklanan manüel araçlarında kullanılması gerekmektedir.

Tez kapsamında yapılan sızma testleri sonucunda kurumlarda görülen en büyük güvenlik açığının literatür ve güvenlik firmaların yaptığı araştırmalarda vurgulandığı

gibi web uygulamalarından kaynaklandığı tespit edilmiştir. Günümüzde web uygulamaları, güncel ve doğru bilgiyi insanlara ulaştırmak için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır. Web sunucuları ve sundukları site içeriği, kurumların vitrini ve itibarı haline gelmiştir. Web üzerinden verilen hizmetler çoğaldıkça web'e yönelik saldırılar da her geçen gün artmaktadır. Bunun nedeni, web uygulamaları güvenliğinin ilgisizlikten ve bilgisizlikten kaynaklanan sebeplerden ötürü yeterince ciddiye alınmaması ve güvenli yazılım geliştirme tekniklerinin kullanılmaması olarak açıklanabilir. Web uygulamaları genellikle güvenlik göz önünde bulundurulmadan tasarlanıp güvenlik sızma testlerine tâbi tutulmadan hizmete sunulmaktadır. Özellikle kullanıcıdan girdi alınarak dinamik içerik sağlamak amacıyla veritabanı desteği sağlayan uygulama kodları (asp, jsp, php, cgi, vb.) web sitelerinin en zayıf halkalarını oluşturmaktadır. Verinin doğruluğunun kontrol edilmemesi sonucunda meydana gelen enjeksiyon yöntemiyle yapılan saldırılarda "sadece web uygulamaları (siteleri) etkilenir" mantığı doğru olarak bilinen yanlışların başında gelmektedir. Enjeksiyon yöntemiyle yapılan saldırılarla web uygulama açığı bulunan kurumun ağ üzerinde yer alan tüm kurumsal bilgi varlıklarına ulaşılması mümkündür.

Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında insan faktörü önemli bir yere sahiptir. İnsan faktörü sayesinde birçok güvenlik denetimi devre dışı bırakılabilmektedir. Yeterli düzeyde eğitim almamış kurum çalışanları (yönetici, teknik sorumlu, son kullanıcı) veya kurumsal bilgi sistemleri üzerinde yetkileri olan ve yerel saldırgan (internal hacker) olarak adlandırılan iyi niyetli olmayan üst derecede bilgiye sahip olan çalışanlar kurumsal bilgi güvenliğini üst düzeyde tehdit eden insan faktörleridir. Kurumsal bilgi güvenliğinin sağlanmasıyla ilgili olarak bu tez çalışmasında güvenliğin bir ürün veya hizmet olmadığı, insan faktörü, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve yönetilmesi zorunlu bir süreç olduğu esas alınmış, bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı ortaya konmuştur.

Bilgi güvenliğinin sağlanmasında eğitimin önemi büyüktür. Ülkemizde bilgi güvenliği eğitiminin verilmesiyle ilgili olarak üniversitelerimize ve Milli Eğitim

Bakanlığımıza önemli görevler düşmektedir. Ülkemizdeki bilgi güvenliğiyle ilgili verilen eğitim ve öğretim müfredatları tez kapsamında incelenmiş olup, bilgi ve bilgisayar güvenliği konusuyla ilgili derslere ilköğretim ve liselerde hatta üniversitelerin lisans programlarında rastlanılmaması bu alanda yetişmiş akademisyen sayısının çok az olduğunu göstermektedir. Bu durum ülkemiz açısından önemli bir kayıp olarak değerlendirilmektedir. Bilgi ve bilgisayar güvenliği bilgisayar kullanma çağına gelen her birey için verilmesi gereken temel bir eğitim olarak görülmeli ve ilköğretim müfredatından başlayarak yüksek öğretime kadar değişik içeriklerde öğrencilere verilmelidir. Aksi takdirde bilgisayar kullanan çocuklarımıza hiçbir eğitim vermeden başıboş olarak internet dünyasında gezinmesi beraberinde bir sürü istenmeyen olayların meydana gelmesine neden olacaktır. Bu kapsamlı çalışmanın ortaya çıkmasında Gazi Üniversitesi Bilgisayar Mühendisliği Bölümünde alınan Bilgi ve Bilgisayar Güvenliği isimli dersin önemli bir rolü olması eğitimin bilgi güvenliği alanında ne kadar önemli olduğuna verilebilecek güzel örneklerdendir. Bu ve benzeri derslerin artması sonucunda doğal olarak bu tür çalışmalar artarak ülkemizin ihtiyacı olan bilgi güvenliği konusunda akademisyenlerin yetişmesi sağlanacak ve ülkemiz açısından önemli kazanımlar elde edilecektir. Bilgi güvenliği konusunda bilinçli bir nesil yetiştirilmesi için çalışmalar yapılması ülkemizin bilgi güvenliğinin sağlanmasında yapılabilecek en önemli vazifelerden birisidir.

Şu ana kadar özetlendiği üzere, kurumsal bilgi güvenliği konusu bir zincirin halkaları misali birbirleriyle alakalı eğitim, insan, teknoloji, süreçler, standartlar gibi birçok unsuru içinde barındırmaktadır. Bundan dolayı ülkemizde elektronik ortamları kullananları ilgilendiren önemli bir konudur. Bu tez çalışması kapsamında bilgi, bilgi güvenliği, kurumsal bilgi, kurumsal bilgi güvenliği, bilgi güvenliği yönetim sistemleri, sızma testleri, web uygulamalarına özel sızma testleri, bilgi güvenliğinin sağlanmasına etki eden faktörler gibi konu başlıkları altında kapsamlı araştırmalar sunulmuş ve uygulamalar yapılmıştır.

Bu tez kapsamında; kurumsal bilgi güvenliğinin anlaşılabilmesi için öncelikle geniş bir anlama sahip olan bilgi ve bilgi sistemleri kavramının açıklanması gerekmektedir.

Bilgi sistemlerinin tarihçesi ve geçmişten günümüze kadar bilginin güvende tutulması için geliştirilen yöntemlerin anlaşılabilmesi için bilgi güvenliğinin gelişimi hakkında bilgi sahibi olunması gereklidir. Günümüzde kurumsal bilgi güvenliğinin sağlanabilmesi için bilgi sistemleri için risk oluşturan tehdit sınıflarının açıklanması alınması gereken önlemlerin planlanması açısından önem taşımaktadır. Dünyada ve ülkemizde bilgi güvenliğinin gidişatını görerek önleyici tedbirleri alabilmek amacıyla güvenlik firmalarının yayınlandığı raporların bilinmesinde fayda vardır. Bilgi güvenliği ihlallerinin önlenmesinde caydırıcı güç olarak veya meydana gelen güvenlik ihlallerinin cezalandırılmasında kullanılmak üzere bilgi güvenliğiyle ilgili mevzuata hâkim olunmalıdır. Yukarıda sıralanan gereklerin kapsamlı olarak açıklanması amacıyla bilinmesi gerekenler "*Bilgi ve Bilişim Sistemleri Güvenliği*" konu başlığı altında Bölüm 2'de anlatılmıştır.

Bilgi teknolojileri sürekli gelişen ve değişen bir yapıda olduğundan, bilgi güvenliğinin bir defaya mahsus sağlanması veya yapılandırılması kurumsal bilgi sistemleri açısından yeterli değildir. Kurumsal bilgi güvenliğinin sağlanabilmesi amacıyla bilgi güvenliği yaşayan bir süreç olarak ele alınmalı, sistemler güncellenmeli, eğitimler alınmalı, oluşabilecek yeni riskler karşısında yatırımların zamanında ve doğru bir şekilde yapılması gerekmektedir. Karmaşık süreçlerden oluşan kurumsal bilgi güvenliğinin sağlanması ve bilgi güvenliği çarkının döndürülebilmesi amacıyla bilgi güvenliği yönetim sistemleri kavramının bilinmesi ve kurumlara uygulanması gerekmektedir. Bilgi güvenliği yönetim sistemleri oluşturulurken dünya genelinde kabul görmüş standartların uygulanması ve kurumlara uyarlanması amacıyla kurumsal bilgi güvenliği politikalarının, standartların ve prosedürlerin yazılması gerekmektedir. Bu durum gösteriyor ki bilgi güvenliğinin sağlanmasında bilgi güvenliği sürecinin devamlılığı ve yönetimi daha fazla önem kazanmaktadır. Bu tez çalışmasında bu konunun önemi gözetilerek kurumsal bilgi güvenliğinin sağlanmasında önemli bir yeri olan bilgi güvenlik yönetimi sistemleri ve standartları *"Kurumsal Bilgi Güvenliği Yönetim Sistemi"* konu başlığı altında Bölüm 3'de kapsamlı olarak anlatılmıştır.

Kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında zayıflıkların ve eksikliklerin erken teşhisinin önemi büyüktür. Saldırı gelmeden önce güvenlik eksiklikleri ve zayıflıklarının tespit edilerek giderilmesini sağlayan sızma testleri kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Ülkemizde pek fazla bilinmediği için çok fazla kullanılmayan sızma testlerinin tanımı ve hangi amaçla kullanıldığının kurumlar tarafından bilinmesi kurumsal bilgi güvenliğinin sağlanması ve sızma testlerinin yaygınlaşması açısından gereklidir. Testlerin sınıflandırılarak kurumların ihtiyaçları doğrultusunda, belirli bir yöntem ve disiplin çerçevesinde etik kurallara saygılı güvenlik uzmanları tarafından yapılması sızma testlerinin başarılı olması için önemlidir. Bu testlerin amacı kurumsal bilgi sistemlerine düzenlenebilecek saldırıları, saldırgan gözüyle kontrollü olarak saldırı gelmeden önce kontrollü saldırılar düzenleyerek gerekli tedbirlerin önceden alınmasında kurumlara yardımcı olmaktır. Kurumsal bilgi güvenliğinin sağlanmasında önemli bir role sahip olan, ülkemizde bu alanda kullanımı çok yaygın olmayan sızma testleri konusu hakkında *"Sızma Testleri"* konu başlığı altında Bölüm 4'de kapsamlı bir araştırma yapılmış elde edilen bulgulara bağlı metodoloji geliştirilerek uygulama çalışmaları yapılmıştır.

Web uygulamalarının sayısının artmasıyla internet üzerinden bilgilere erişim kolaylaşmış gerek kişisel gerek kurumsal işlemler mekândan ve zamandan bağımsız hale gelmiştir. Bilgiye erişimin internet gibi tamamen güvensiz ortamlardan yapılması üst düzeyde bilgi güvenliğinin sağlanmasını zorunlu kılmaktadır. Tez çalışması kapsamında yapılan sızma testleri sonucunda literatürde de belirtildiği gibi ülkemiz ve dünya genelinde bilgi güvenliği zafiyetlerinin web uygulamalarında yoğunlaştığı tespit edilmiştir. Kurumlar tarafından web uygulama güvenliği denildiğinde çok yanlış bir kanı olan web sayfalarının zarar görmesi olarak algılanması ve böyle düşününler içinde teknik insanlarında (yazılımcı, sistemci, vb.) olması düşündürücüdür. Tüm bu gelişmelere paralel olarak ülkemizde ve dünyada kurumsal uygulamaların hızla web üzerine taşınması, web uygulamalarının güvenliği konusunun kurumsal bilgi güvenliğini doğrudan etkileyen bir unsur halini aldığını göstermektedir. Web uygulamaları farklı kişi veya kurumlar tarafından birbirinden farklı yazılım teknikleri kullanılarak güvenlik göz önünde bulundurulmadan

geliştirilen standart olmayan yazılımlar olduğundan, güvenliğinin sağlanmasında kullanılacak en etkili yöntemin web uygulamalarına özel olarak geliştirilmiş sızma testleri olduğu değerlendirilmektedir. Bu gereksinimler çerçevesinde web uygulamalarının güvenliğinin sağlanmasına yönelik sızma testlerinin nasıl yapılacağına dair geniş kapsamlı bir çalışma yapılarak *"Web Uygulamaları Sızma Testleri"* konu başlığı altında Bölüm 5'de anlatılmıştır.

Kurumsal bilgi güvenliğinin sağlanmasına etki eden en önemli üç faktörün insan eğitim ve teknoloji olduğu düşünülmektedir. Bu faktörlerin doğru analiz edilmesi ve bilgi güvenliğinin sağlanmasındaki rollerinin iyi belirlenmesi gerekmektedir. Kurumsal bilgi güvenliğine etki eden faktörler üzerindeki zafiyetlerin belirlenmesinde sızma testlerinin önemli bir rolü vardır. Kurumsal bilgi güvenliğinin sağlanmasına etki eden faktörler ve sızma testlerinin bu faktörler üzerindeki önemi *"Kurumsal Bilgi Güvenliğine Genel Bir Bakış"* konu başlığı altında Bölüm 6'da ayrıntılı olarak açıklanmıştır.

Tez çalışmasının bir bütün olarak değerlendirilmesi, elde edilen bulgular, ülkemiz açısından sağlanan katkılar, çalışmalar sırasında karşılaşılan güçlükler, kazanımlar ve sunulan öneriler *"Sonuçlar ve Öneriler"* konu başlığı altında Bölüm 7'de verilmiştir.

Kurumların günümüzde saldırganların teknolojik hızına yetişebilmesi ve kurumsal bilgi varlıklarını saldırılardan koruyabilmesi için bu tez çalışmasında da açıklanan kurumsal bilgi güvenliği kavramını kavrayabilmeleri ve o kavramın tüm gereklerini yerine getirmeleri gerekmektedir. Bu tez çalışmasının gereksinimlerinden biri olan en önemli korunma yönteminin insanlarda bilgi güvenliği bilincinin oluşturulması olduğu konusunda ülkemize önemli katkılar sağlayacağı, bu konudaki bilgi yetersizliğinin giderilmesi ve kurumlara rehber olması amacıyla ülkemizde bilgi güvenliği konusunda büyük bir eksikliği gidereceği umut edilmektedir.

Sonuç olarak; bu tez çalışması bilgi güvenliğine geniş bir açıdan bakılması ve gerek kişisel gerekse kurumsal ve ulusal bilgi güvenliğinin sağlanmasında önemli birçok unsurun bir araya getirilmesi, ülkemizde alanında hazırlanan ilk tez olması, ülkemizde yapılan çalışmalara ve alınan koruma tedbirlerine rağmen gözden

kaçırılan küçük fakat bilgi güvenliği açısından büyük açıkların tespiti ve bunların kapatılmasına yönelik olarak yapılması veya alınması gerekli tedbirlerin ortaya konulması açısından önem arz eden bu çalışmanın ülkemizdeki bilgi güvenliği çalışmalarına büyük katkılar sağlayacağı değerlendirilmektedir.

2. BİLGİ VE BİLİŞİM SİSTEMLERİ GÜVENLİĞİ

Dünyada olduğu gibi bilgi ve bilişim sistemleri güvenliği ülkemizde de güncel konulardan birisidir. Birinci bölümde önemi vurgulandığı gibi gelişen toplumların temel hammaddesi olan bilgiler elektronik ortamlarda işlendikçe taşındıkça ve depolandıkça bu ortamlarda alınması gereken tedbirler, emek, metodoloji, güvenlik seviyeleri, değer, maliyet ve boyut açısından da farklılıklar göstermektedir. Bunun yüksek oranda sağlanması için bilgi varlıklarının değerinin iyi tespit edilmesi, yüksek seviyede bir bilgi güvenliği bilincinin yerleşmesi, kullanılan yazılım veya donanım açıklarının iyi takip edilmesi, meydana gelen açıkların her an izlenmesi ve giderilmesi, meydana gelebilecek açıkların önceden tespit edilerek zamanında giderilebilmesi, bunun sağlanması için personelin eğitimli olması ve kendini yetiştirmesi, sistemleri ve bilgileri belirli politikalar çerçevesinde korumak ve bu bilinçle güvenliğin dinamik bir süreçte ele alınması gerektiği artık bilinen veya bilinmesi gereken konulardır.

Tez çalışmasının bu bölümünde konunun öneminin daha iyi anlatılması ve iyi bir farkındalık oluşturulmasının sağlanması için bu bölümde veri, bilgi, özbilgi, kavramları incelenmiş, bilişim korsanlığı tarihçesi gözden geçirilmiş, bilgi güvenliğinin gelişimi açıklanmış, güvenlik boyutunun anlaşılması için fiziksel, haberleşme, yayılım, bilgisayar, ağ ve bilgi güvenliği konuları gözden geçirilmiş, bilgi güvenliğini tehdit eden unsurlar incelenmiş, bu konudaki yasal mevzuatlar değerlendirilmiş, güvenliğin öneminin anlaşılması için ülkemiz ve dünya istatistikleri incelenmiş ve sunulmuştur.

2.1. Bilgi

Bilgi (information) kelimesinin menşei, Latince'deki herhangi bir şeye şekil vermek anlamına gelen "informare" kelimesinden gelmektedir [18]. Sözlük anlamıyla bilgi;

- Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü,
- İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat,

- İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf,
- Genel olarak ve ilk sezi durumunda zihnin kavradığı temel düşünceler ve
- Kurallardan yararlanarak kişinin veriye yönelttiği anlam

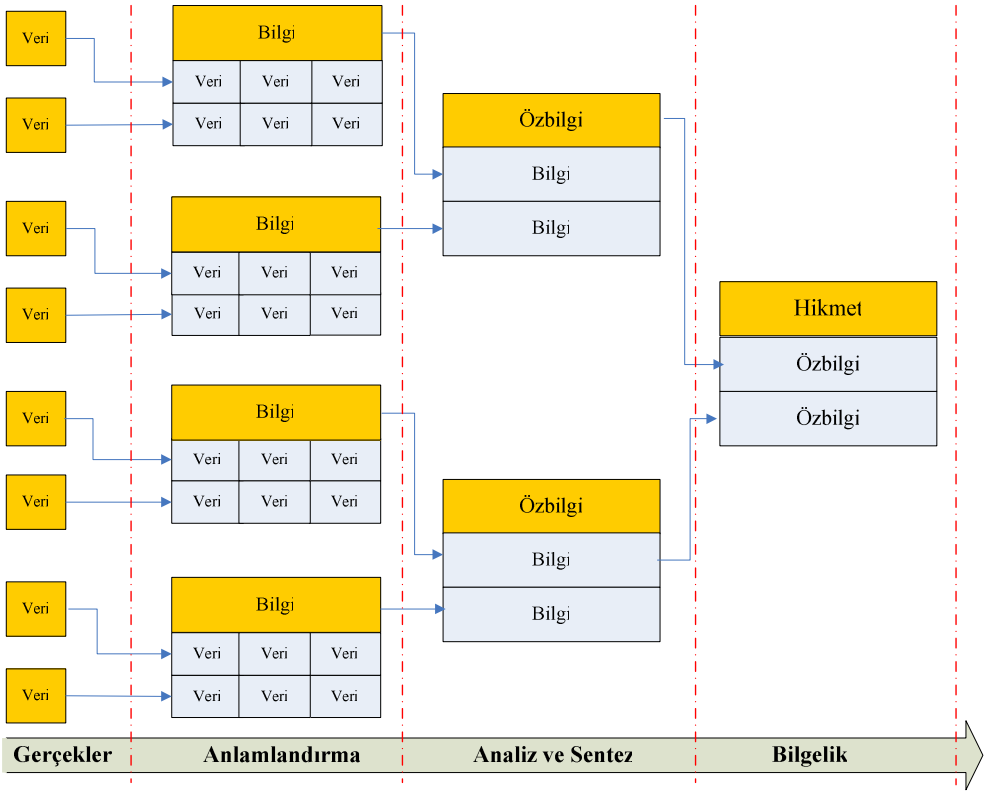
olarak tanımlanmaktadır [19].

Bilgi literatürde çok farklı şekillerde tanımlanmaktadır.

- Bilgi, doğruluğu ispatlanmış inançlardır [20].
- Bilgi, sosyal olaylarda karşımıza çıkan eylem ve olayları anlamamıza yardım eden işaret ve kodlamalardır [21].
- Bilgi, insanın varlığı tanıma ve anlama isteği sonucu ortaya çıkan, düşünen özne ile nesne arasındaki ilişkidir. Özne; bilgiye yönelen, bilen insandır. Nesne; bilgiye konu olan, bilinen somut veya somut tüm varlıklardır. İnsan başka bir varlığı düşündüğünde özne, başkası tarafından düşünüldüğünde nesnedir. Ayrıca insan kendisini de nesne edinebilir, kendisi hakkında ortaya bilgi koyabilir [22].
- Claude Shannon bilgiyi, bir konu hakkında belirsizliği azaltan kaynak olarak tanımlamıştır [23].
- Gregory Bateson bilgiyi, farklılık meydana getiren her türlü farklılık şeklinde tanımlamıştır [18].
- Kişi/kurum/kuruluşlar için önemli ve değerli olan bir kaynaktır ve korunması gerekir [24].

Bilginin önemi, eğitimde, sanatta, sağlıkta ve iş yaşamı gibi hayatın çeşitli alanlarında ve ilk çağlardan beri bilinmekte ve gelecek nesillere farklı ortamlarda ve şekillerde aktarılmaktadır. Bilginin aktarılmasında ilk çağlardan başlayarak hikâyeler, masallar ve destanlar aracı olmuş 12. yüzyıldan sonra da bilginin yaygınlaştırılmasında ve öğretilmesinde medreseler, üniversiteler ve kitaplar önemli roller üstlenmişlerdir. Ancak, son dönemde iletişim ve işbirliğini son derece kolaylaştıran bilgi teknolojilerinin gelişmesiyle bilgi çağı adı verilen bir döneme girilmiştir. Yaşadığımız çağa adını veren bilginin günümüzde olduğu gibi gelecekte de insanoğlunun yaşantısına yön verecek varlıkların başında yerini koruyacaktır. Bilgiyi daha iyi tanımlamak için benzer bazı kavramların anlamı ile bilginin anlamı

arasındaki farklılıkların ortaya konması gereklidir. Çok geniş bir kavram olan bilginin tanımının yapılabilmesi için kategorilere ayrılması, yüklendiği değerler yönüyle çeşitli gruplar altında değerlendirilmesi gerekmektedir. Bu grupları ifade etmekte kullanılan kavramlar veri (data), bilgi (information), özbilgi (knowledge), hikmet (wisdom) olarak sıralanabilir ve bu kavramlar arasında Şekil 2.1'de gösterildiği gibi veriler bilginin, bilgiler özbilginin, özbilgiler ise hikmet'in inşasında kullanılan yapıtaşlarıdır.



Şekil 2.1. Veriden hikmete bilgilerin sınıflandırılması [25]

İşlenmemiş ham bilgi olarak adlandırılan veri, data kelimesinin karşılığı olarak kullanılan Latince datum sözcüğünün çoğulu olup sayısal, alfa nümerik karakterler, semboller, kelimeler veya grafik gösterimler şeklinde ifade edilebilmektedir [26]. Veriler çeşitli işlemlere tabi tutulduktan sonra hem anlam hem de değer kazanarak bilgiye dönüşürler. Bilgi genellikle, bireyler veya kurumlar tarafından bir sorunun çözümü, herhangi bir çalışmanın başlatılması ya da bitirilmesi gibi faaliyetler sonucunda ortaya çıkarılan verilerin bütününü ifade etmektedir. Özbilgi ise herhangi

bir konuda insanların kendi alanlarında edindikleri bilgiyi (tecrübeyi) yorumlayarak elde ettiği kararlar ve yeteneklerdir. Bütün bu kavramların da üstünde olan hikmet, veriden bilgiye, bilgiden özbilgiye ve özbilgiden de yeteneğe dönüşen sürecin en uç noktasını oluşturmaktadır [27].

Veri, bilgi, özbilgi ve hikmet arasındaki hiyerarşinin daha iyi anlaşılabilmesi için örnek vermekte fayda vardır. Kurumsal bilgi güvenliği konusunda bir tez yapıldığını bilmek veridir. Bu tezin kim tarafından, ne zaman, hangi üniversitenin hangi bölümünde yapıldığını, içeriğinin ne olduğunu ve danışman hocasının kim olduğunu bilmek ise bir bilgidir. Bu tezi okuyup içindeki bilgileri anlamak, bunları değerlendirerek farklı çıkarım ve sonuçlar elde etmek ise öz bilgidir. Bu tezi okuyup anlayan bir kişinin sahip olduğu bilgi birikimlerinden ve tecrübelerinden konular üstü çıkarımlar elde etmesi ise hikmettir.

Bilgi, içeriğine göre bireysel ve kurumsal olmak üzere ikiye ayrılmaktadır. Bireysel bilgi, kurumsal bilgi tabanının gelişmesi için gerekli olan beceri ve yeteneklerden oluşmaktadır. Kurumsal bilgi, kurum içinde üretilen veya kuruma dışarıdan gelen, o kurumla ilgili kayıtlı ya da kayıtsız her türlü bilgiyi ifade etmektedir. Kurumsal bilgi, bireysel bilgilerin toplamının yanı sıra, diğer kurumlar tarafından kolayca taklit edilemeyecek şekilde insan, teknoloji ve yönetim ilkeleri arasında üretilen bilgi kaynaklarını ifade etmektedir [28]. Kurumsal bilgilerin diğer kurumlar tarafından taklit edilmesi, söz konusu unsurlar arasında oluşturulan etkileşim, kurumun kendine özgü kültürü ve kurumun tarihçesini de içine aldığından zor ve zaman alıcıdır.

Bu tanımların iyi bilinmesi bilgi varlıklarının farkında olunması ve değerlerinin doğru bir şekilde belirlenmesi yüksek seviyede bir bilgi güvenliğinin sağlanması için önemlidir. Günümüzde kurumlar açısından kurumsal bilginin önemini göstermesi açısından 1980'li yılların ortalarında kurulan Microsoft firması buna örnek olarak verilebilir. Günümüzde neredeyse yüzyıllık bir şirket olan ve uzun yıllar dünyanın en büyük kuruluşu olarak kabul edilen General Motors firmasıyla Microsoft firmasının piyasa değerleri kıyaslandığında Microsoft firmasının piyasa değerinin General Motors firmasından iki buçuk kat daha büyük olduğu görülür [29]. Bilginin günümüz rekabetçi pazarlarında son derece büyük bir role ve öneme sahip olduğunu ve

gelecekte daha da öneminin artacağını kanıtlayan buna benzer örnekler her geçen gün daha fazla ortaya çıkmaktadır.

Kurumsal bilginin rekabeti körükleyici, itici, üretken gücünü doğru ve yerinde kullanan işletmeler, dünyanın her bölgesinde rekabet edecek duruma gelebilmektedirler. Kurumsal bilgi yönetiminin bu derece önemli olduğu günümüzde kurumsal bilgilerin güvende olması ve güvenli şekillerde gönderilmesi ve alınması çok önemlidir. Kurumsal bilgi güvenliğinin sağlanması her kurum için olmazsa olmazların başında gelmektedir. Bu tez çalışması bunun gerekçelerini açıkça ortaya koymak ve alınması gereken güncel önlemleri sunmak ülkemizde çokta önem verilmeyen kurumsal bilgi güvenliği ve bu güvenliği sağlamada çok önemli bir yöntem olan sızma testlerini bilimsel açıdan ele alıp kurumların bilgi güvenliği ihlallerinden doğan kayıplarının azaltılmasında dikkat edilmesi gereken hususları detaylı olarak sunmaktadır. Bilgi güvenliğinin sigortası olan sızma testleri günümüzde bilgi sistemlerinin yüksek seviyede güvenliğinin devamını sağlamak için yapılması gerekmektedir.

2.2. Bilişim Korsanlığı Tarihçesi

Bilişim, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi olarak tanımlanmaktadır [30]. Bilişim güvenliği denildiğinde insan faktörü ve teknoloji bir arada değerlendirilmelidir. Bilgi güvenliğinin öneminin anlaşılabilmesi, bilgi güvenliği tehditleri ve önlemleri konusunda geçmişte yaşanan hatalar sonucu meydana gelen güvenlik ihlallerinden ders alarak gelecekte benzer hatalara düşmemek ve korsanların gelecekte bilişim sistemlerinin güvenliği konusunda neler yapabileceğine dair doğru tahminler yapılması açısından önemlidir.

Bilişim sistemleri sızma testleriyle sınanırken dikkat edilmesi gereken kritik nokta testlerin gerçekçi olmasının sağlanmasıdır. Sızma testleri yapılırken gerçek bir saldırgan gibi düşünerek saldırganların kullandığı araç ve yöntemlerle kurumsal bilgi varlıkları test edilmelidir. Bunun için geçmişten günümüze kadar bilişim

sistemlerinin güvenliğini tehdit eden saldırıların ve alınan önlemlerin neler olduğu, günümüze kadar geçirdiği değişim ve gelişim süreçlerinin bilinmesinde fayda vardır.

1960'lı yıllar

Korsan (hacker) teriminin doğduğu yıllar olarak literatüre geçmiştir. Bugün bildiğimiz şekli ile korsan kültürünün başlangıcı, M.I.T.'nin (Massachusetts Institute of Technology) ilk PDP–1 (Programmed Data Processor) makinesini satın aldığı 1961 tarihi olarak kabul edilebilir. PDP–1 DEC (Digital Equipment Corporation) firması tarafından 1960'lı yıllarda ilk defa geliştirildiğinde çok pahalı bir cihaz olduğundan belirli zaman dilimlerinde kiralama yöntemiyle eğitim kurumları ve ticari amaçlı firmalara kiralanıyordu. Kiralama yöntemiyle aynı bilgisayar üzerinde birden fazla kurum, kuruluş ve bireyin bilgilerinin ve programlarının korunmasız vaziyette yer alması kapıların ilk defa korsanlar için açılması anlamını taşıyor kötüler için "korsan" iyiler için "bilişim güvenliği" kavramının doğuşunu simgeliyordu [31]. Özellikle M.I.T.'deki yapay zekâ laboratuarı korsanların maharetlerini geliştirebileceği bir platform olmuştur. Günümüzde olumsuz bir anlama sahip olan korsan sıfatı (Hacker), 1960'lı yıllarda olumlu bir anlama sahip olup, programları planlanandan daha farklı işler yapmaya zorlayan bilgisayar dâhisi anlamında kullanılmıştır.

1970'li yıllar

Bu yıllarda telefon korsanları (phreaking) ücretsiz görüşme yapabilmek için uluslararası telefon şebekelerine sızmaya başlamıştır. Bunların en ünlüsü olan John Draper, Cap'n Crunch marka gevrekten çıkan bir oyuncağın çıkardığı ses ile defalarca ücretsiz görüşme yapmayı başarmıştır. Daha sonra Captain Crunch lakabıyla anılan Draper, bu oyuncağın 2600 Hertz'lik bir sinyal (AT&T'nin uzak mesafe görüşme sistemine erişim için kullanılan tonun aynısı) çıkardığını tespit etmiş ve mavi kutu (Blue Box) adı verilen cihazı geliştirmiştir. Bu cihaz sayesinde çok sayıda insana para ödemeden telefonla milletlerarası görüşme yaptırmıştır. Draper gerçekleştirdiği bu olayla, bilişim sistemlerinin bir parçası olan telefon sistemlerinin güvenlik önlemini delen ilk başarılı saldırı denemesini yapıp adını tarihe ilk telefon

korsanı (phone phreaker) olarak yazdırmıştır [32]. Bu olay kayda geçen ilk bilişim güvenliği ihlali olması açısından önemlidir. Tutuklanmasının sonrasında bilgisayar güvenliğiyle ilgili yazılım geliştirmeye başlamıştır. O dönemde mavi kutuları üretenler arasında Steve Wozniak ve Steve Jobs adlı iki kolejli yıllar sonra bilgisayar dünyasında devrim yaratan Apple'ı kurmuştur.

1980'li yıllar

Telefon korsanları yavaş yavaş bilgisayar alanına kaymaya başlamıştır. Ayrıca ilk elektronik mesaj pano sistemleri (BBS) ortaya çıkmıştır. Bu yıllarda ilk bilgisayar korsan grupları kurulmuştur. ABD'deki Legion of Doom ve Almanya'daki Chaos Computer Club gibi korsan gruplar öncüler arasındadır. 1982 yılında Xerox Palo Alto araştırma merkezinde ağ ortamlarında yapılan işlemlerin performansının ölçülmesi amacıyla ilk defa solucanlar (worm) kullanılmıştır. 1983 yılında ise "Bilgisayar Virüsü" terimi DEC-VAX sistemleri üzerinde akademik deneylerini yapan Fred Cohen tarafından resmen tanımlanmıştır [33].

1983 yılında Savaş Oyunları (War Games) isimli sinema filmi saldırı ve korsan efsanesini geniş kitlelere tanıtmıştır. Filmde, Matthew Bredorick'in oynadığı ana karakter, oyun oynamak için bir üretici firmanın bilgisayar sistemine girmeye çalışmış ancak yanlışlıkla ordunun nükleer savaş simülasyon sistemine girmiş ve ordu yüksek düzeyde alarm (Def Con 1) vermiştir. Aynı yıl, 414 olarak bilinen bir çeteye mensup altı genci, dokuz gün içinde aralarında nükleer silahların geliştirildiği ABD'deki Ulusal Laboratuar'dakilerin de bulunduğu 60 bilgisayara sızması üzerine yetkililer tutuklamışlardır [33].

1984 yılında Steven Levy "Hackers: Heroes of the Computer Revolution" isimli, bilgisayar dünyasının son elli yıllık tarihine korsan bazlı olarak değinmiş gerçek, donanım ve oyun korsanları adı altında korsanları ve yaptıklarını detaylı olarak incelemiştir. Özellikle ilk bölümde (gerçek korsanlar) yer alan ve kitabın can alıcı noktalarının başında gelen kısım "Korsan Etiği"i olarak adlandırılan korsan manifestosu, kitapta şu şekilde özetlenmiştir [34].

- Herkesin bilgisayara serbestçe erişim hakkı olmalı ve tüm bilgi özgür bir biçimde paylaşıma açık olmalı.
- Otoritelere güvenmemeli, merkezileşmeye karşı çıkan yapılanmalar desteklenmeli.
- Korsanlar yaptıkları işlerle değerlendirilmeli (diplomaları, kaç yaşında oldukları, cinsiyetleri ya da konumlarıyla değil).

1984 yılında Eric Corley (takma adıyla Emmanuel Goldstein) editörlüğünde "2600:The Hackers Quarterly" isimli ünlü korsan dergisi düzenli olarak basılmaya başlanmış bir yıl sonra Phrack isimli çevrimiçi korsan dergisi şimdiki adresiyle www.phrack.org adresinde yayına başlamıştır. Her iki dergide de korsanlar için yararlı bilgilerin yanı sıra yorumlarında yer aldığı güvenlik ve saldırı içerikli haberler yer almıştır [33].

1986 yılında korsan grupları bilgilerini para karşılığında satmaya başlamıştır. Bu alanda bilinen ilk olay olan 1986 yılında Almanya Hannover şehrindeki Chaos Computer Club üyesi olan birkaç korsan ABD'deki kamu (Enerji Bakanlığı, Savunma Bakanlığı, NASA) ve özel sektör (savunma firmaları) sistemlerine sızmışlardır. Elde ettikleri bilgileri Sovyet'lerin gizli servisi KGB'ye satmışlardır. 1988 yılında ilk defa fark edilen korsanlar 18 ay boyunca Alman ve Amerikan polislerinin ortak takipleri sonucunda yakalanarak casusluk suçundan tutuklanmıştır. Bu olay, açığa çıkan ilk siber casusluk vakası olarak tarihe geçmiştir [35].

1988 yılında Cornell Üniversitesi öğrencisi Robert T. Morris, ARPAnet üzerinde kendi kendine çoğalan bir kötücül kod (solucan) yazmıştır. Morris, bu kodun UNIX sistemlerini etkileyip etkilemeyeceğini görmek istemiştir. Morris denemesini yapmak üzere 99 satırdan oluşan solucan yazılımını internet ortamında çalıştırdığında solucan kontrolünden çıkmış ve ağa bağlı 6 bin bilgisayarı etkilemiştir. Bu denemesinin sonucunda üniversiteden kovulan Morris, 10 bin dolar para ve 3 yıl gözaltı cezasına çarptırılmıştır [33]. Bu olayla birlikte internet güvenliği kavramı tartışılmaya başlanmış ve güvenliğin sağlanması üzerine akademik ve ticari çalışmalar başlamıştır. 1988 Kasım ayında Morris isimli solucanın hızla yayılması üzerine

DARPA (Defense Advanced Research Projects Agency) gelecekte ihlallerin engellenmesi ve acil durumlarda koordinasyonu sağlamak ve krizleri yönetmek amacıyla Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsüyle işbirliğine gitmiş ve CERT (Computer Emergency Responce Team) isimli acil müdahele ekibi kurulmuştur [36].

1989 yılında DEC firmasında çalışan Jeffrey Mogul tarafından güvenlik duvarı ile ilgili ilk makale yayınlanmıştır. Mogul makale içeriğinde erişim kontrolü için ağ trafiğinin nasıl filtreleneceğini anlatmış ve Unix işletim sistemi üzerinde çalışan bir ağ geçidinin (router) paketleri nasıl filtreleyeceğini açıklamıştır. Mogul'un açıklamaları doğrultusunda DEC firmasında çalışmalara devam edilmiş, Marcus Ranum tarafından Güvenli Harici Erişim Bağlantısı (Securing External Access Link-SEAL) kavramı açıklanmış ve ilk ticari güvenlik duvarı olan DEC SEAL piyasaya sürülmüştür [37].

1990'lı yıllar

Uzun bir araştırma döneminin ardından ABD'deki gizli servis ajanları 14 şehirde (Austin, Cincinnati, Detroit, Los Angeles, Miami, New York, Newark, Phoenix, Pittsburgh, Richmond, Tucson, San Diego, San Jose ve San Francisco) baskınlar düzenleyerek BBS'lerden takip ettikleri bazı korsanları tutuklamışlardır. 1990 yılında organize suçlar ve dolandırıcılık bürosu tarafından düzenlenen operasyon ile kredi kartı hırsızlığı ve telefon sahtekârlığının önüne geçilmesi için yapılmış operasyon, korsanların af karşılığında birbirlerini ihbar etmeleri yüzünden korsan camiasında bir bölünmeye yol açmıştır [38].

1993 yılında dünyanın dört bir yanındaki korsanların ve korsan olmaya hevesli bilgisayar meraklıları DefCon adı altında ilk defa toplanmıştır. Aynı yıl içerisinde Kevin Poulsen ve iki arkadaşı, Los Angeles'ta, o andan itibaren kendilerini arayan 102. kişiye Porsche marka bir araba vermeyi vaad eden bir yerel radyo (KISS FM) istasyonun telefon hatlarını kontrolü altına almıştır. Üç korsan radyonun telefon sistemiyle oynayarak kendilerinin dışındaki aramaları engellemişler ve büyük ikramiyeyi kazanmışlardır. Poulsen daha önce de bir telefon sistemine sızdığı için 5

yıl hapis cezasına çarptırılmıştır. 1996 yılında dışarı çıktıktan sonra bilgisayar suçları üzerine serbest gazetecilik yapmaya başlamıştır [39].

1993 yılında İngilterede BSI (British Standards Institute) tarafından kurumların güvenliğinin sağlanması için yapılması gerekli olan tavsiyelerin yer aldığı Uygulanabilirlik Şartnamesi (Code of Practice) adı altında bir kılavuz yayınlanmıştır. Bu kılavuz kurumsal bilgi güvenliğinin sağlanmasında kurumlara yol gösteren ilk belge olması açısından önemlidir [40].

1994 yılında Netscape firması tarafından kendi adıyla geliştirilmiş olan internet tarayıcısının çıkmasıyla bilgiler internet ortamına taşınmaya başlamıştır. İnternet yeni tarayıcısı Netscape'e kavuştuğu zaman korsanlarda BBS'lerdeki bilgilere daha kolay erişilebilmesi amacıyla web sayfalarına taşınmaya başlamıştır. Saldırı programları ve ipuçlarına erişim kolaylaştığı için korsanlar istedikleri bilgiye internet üzerinden kolayca erişmeye başlamıştır. Netscape tarayıcısının açıklarını kullanan korsanlar bilgilerini herhangi bir güvenlik önlemi almadan internet üzerine taşımaya başlayan kurum ve kuruluşlara saldırmışlardır. Böylece korsanlıkta yeni ve günümüze kadar uzanan bir dönem başlamıştır [41]. Aynı yıl içerisinde, Al Huger Avalon Güvenlik Araştırma takma adı altında Bugtraq listesinde bellek taşması zafiyetinin nasıl kullanılacağını gösteren bir mesaj yayınlaması korsanların paylaşımının önemli bir göstergesi olmuştur.

1995 yılı Şubat ayında ünlü korsan Kevin David Mitnick, 20 binin üzerinde kredi kartı numarası çalmak suçundan uzun zamandan beri takipte olan FBI tarafından yakalanarak tutuklanmıştır. Mahkemeye bile çıkarılmadan dört yıl hapiste tutulan Mitnick, korsan dünyasında büyük bir isim haline gelmiştir. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi büyük bilişim şirketlerinin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. 21 Ocak 2000'de başlayan bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te bitmiştir. Kevin Mitnick sosyal mühendislik saldırı tekniklerini ustalıkla kullanmış ve insan faktörünün güvenliğin sağlanmasındaki rolünü ortaya koymuştur. Kevin Mitnick günümüzde yazarlık ve bilgi güvenliği konusunda kurumlara danışmanlık vermektedir. Günümüzde, beyaz şapkalı bir bilgisayar korsanı olarak güvenlik danışmanlığı yapmakta ve dünya

çapında bilgi güvenliğiyle ilgili kongrelere katılmaktadır [42]. Aynı yıl içerisinde ilk zafiyet tarama programı olan SATAN (Security Administrator Tool for Analyzing Networks) yazılmış programcılar güvenlik zafiyetlerini tanımlayabilecek hale gelmiştir [43]. Yine aynı yıl içerisinde kurumsal bilgi güvenliğinin sağlanmasında kullanılacak olan BS–7799 İngiliz standardı olarak kabul edilmiştir.

1997 yılında korsanlar tarafından geliştirilen "AOHell" adlı küçük bir yazılım piyasaya sürülmüştür. Bu yazılım sayesinde sınırlı bilgisi olan acemi korsanlar bile AOL sistemine kolayca girmiş ve kullanıcıların e-postaları, mesaj grupları günlerce e-posta sağanağına tutulmuştur. Geliştirilen bu yazılımla birlikte bilişim güvenliği için yeni bir dönem başlamıştır. Bu dönemden günümüze kadar bu tür yazılımların hızla artması sonucunda korsanların bilgi ve becerisine duyulan ihtiyaç her geçen gün azalmıştır. Kurumlar için sadece usta korsanlar değil onların yazmış olduğu yazılımları ustalıkla kullanan acemi korsanlarda artık önemli bir tehdit unsuru haline gelmiştir [44].

1998 yılında Pentagon'un bilgisayarlarına saldırılmış ve çok sayıda programın kodları çalınmıştır. Hükümet yetkilileri eylemin Amerikan askeri sistemlerine yapılan en organize ve sistematik saldırı olduğunu açıklamıştır. Olayla ilgili Ehud Tenebaum adlı 19 yaşında bir İsrailli genç tutuklanmıştır. Tenebaum bugün bir teknoloji danışmanlığı şirketinde güvenlik konusunda çalışmaktadır.1990'lı yıllarda, CIA, NASA, Hava Kuvvetleri, Pentagon ve Adalet Bakanlığı gibi ABD'nin önde gelen kurumlarının bilgisayar sistemleri ya da web siteleri defalarca korsanlar tarafından ele geçirilmiştir. İsrailli korsanlarında içinde bulunduğu ünlü korsan grubu The Cult of Death Cow "Truva atı" olarak tanımlanan Back Orifice programını tanıtmıştır. Bu program Windows 95 ya da Windows 98 işletim sistemi kurulu bilgisayarlarda aktif hale geldiğinde, makineye uzaktan izinsiz erişimi yapılmasını sağlamıştır. En etkili saldırı araçlarından biri olarak bilinen Back Orifice girdiği bilgisayarın kontrolünü kötü niyetli kişilerin erişimine açmaktadır [45]. Aynı yıl içerisinde BS–7799 standardının ikinci kısmı yayınlanmıştır. BS 7799–2 Bilgi Güvenliği Yönetim Sisteminin kurulması, uygulanması ve dokümante edilmesi için gereklilikleri tanımlayarak, kurumların hangi güvenlik kontrollerine ihtiyacı

olduğunun belirlemesini sağlayarak kurumlara kurumsal anlamda bilgilerinin güvende olduğuna dair belgelendirme imkânı verilmesini sağlar.

1999 yılında Microsoft Windows 98 işletim sistemini çıkarmasıyla birlikte, 1999 saldırıların çok olduğu ve bilgi güvenliğinin gerekliliğinin fazlaca hissedildiği bir yıl olmuştur. Windows işletim sisteminde yer alan açıklar için yüzlerce uyarı ve yama yayınlanmıştır. Kurumsal bilgi güvenliği ve Bilgi Güvenliği Yönetim Sistemi kavramları duyulmaya ve yaygınlaşmaya başlamıştır. İngilterede İngiliz Standartları tarafından ilk kez BS–7799 standardının ikinci bölümünün gerekleri yerine getirilmiş ve belgelendirme işlemi gerçekleştirilmiştir. Belge alan ilk kuruluş İngiltere'de bulunan The Co-Operative Bank isimli e-bankacılık yapan bir işletme olmuştur [46].

2000'li yıllar

Kurumsal açıdan güvenlik kaygılarının en üst seviyeye çıktığı, saldırıların ve korsanların çok tehlikeli olduğu yeni bir döneme girilmiştir. Bu yeni dönemde kötücül kodlar internet aracılığıyla hızla yayılmış milyonlarca bilgisayara bulaşmış ve milyonlarca dolarlık maddi hasara yol açmıştır. Saldırılar ve etkileri hızla artarken Marty Roesch ve Ron Gula tarafından Snort ve Dragon isimli saldırı tespit sistemleri hakkında ilk defa bilgi vermişlerdir [47].

2000 yılında BS–7799 Bölüm–1 Uluslararası Standardizasyon Kurumu (ISO) tarafından tanınmış ve BS ISO/IEC 17799:2000 olarak yayınlanmıştır. BS 7799–2 standardı 2002'de gerçekleştirilen güncelleme ile diğer yönetim sistemi standartları ile daha uyumlu hale getirilmiştir. 2005 yılında Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların bilgi güvenliği yönetim sistemini kurmaları, uygulamaları, sürdürmeleri ve iyileştirmeleri için hazırlanmış olan ISO/IEC 17799:2005 kılavuzunu yayınlamıştır. Aynı yıl içerisinde BS 7799–2:2002 standardını Uluslararası Standardizasyon Kurumu ISO/IEC 27001:2005 adıyla yayınlamıştır. Kurumsal bilgi güvenliğinin sağlanmasında olmazsa olmaz bir unsur olan standartlar konusu Bölüm 3'de kapsamlı olarak anlatılmıştır.

2000 yılından günümüze kadar birçok saldırı olmuş ve kurumlar yüksek oranda bu saldırılardan etkilenerek maddi manevi zararlar görmüştür. 2000 yılından sonraki yıllarda otomatik saldırı araçlarının hızla yayılması sonucunda yapılan saldırılara burada yer verilmemiştir. Bunun başlıca sebebi saldırıların büyük bir kısmının otomatik araçlarla yapılmasından dolayı saldırıların etkisi, kapsamı, saldırganların bilgi seviyesi gibi sızma testlerinin başarılı bir şekilde sonuçlanmasında dikkat edilmesi gereken bilgilerin analizinin doğru yapılamamasından kaynaklanmıştır.

Sonuç olarak son 50 yılda saldırganların geldiği nokta kurumsal bilgi güvenliğini üst düzeyde tehdit etmekte ve kurumların ve bireylerin bilgi güvenliğini sağlamaları konusunda üzerine düşen görevlerini eksiksiz yerine getirmeleri gerekmektedir.

2.3. Bilgi Güvenliğinin Gelişimi

Bilgi güvenliğinin sağlanması için tarih boyunca çeşitli yöntemler kullanılmıştır. Yaşadığımız çağa adını veren bilginin güvenliğinin sağlanmasının günümüze kadar olan değişimi ve gelişimi bilgi güvenliğinin sağlanmasında izlenilen yöntemlerin anlaşılabilmesi açısından önemlidir. Geçmişten günümüze bilgi güvenliğinin sağlanması için sırasıyla fiziksel güvenlik, haberleşme güvenliği, yayılım (emissions) güvenliği, bilgisayar güvenliği, ağ güvenliği konularında çalışmalar yapılmıştır [48]. Günümüzde bilgi güvenliğinin sağlanabilmesi için yukarıda bahsedilen güvenlik önlemlerinin hepsinin bir arada düşünülmesi gerektiğinden bu önlemler takip eden alt başlıklarda sırasıyla açıklanmıştır.

2.3.1. Fiziksel güvenlik

Geçmiş zamanlarda insanlar için önemli bilgiler, taşlara kazılarak saklanmış daha sonraları kâğıtlara yazılarak fiziksel güvenliği sağlanan ortamlarda saklanmıştır. Fiziksel güvenliğin sağlanabilmesi amacıyla, duvarlar örülmüş, kale hendekleri çekilmiş, giriş çıkışı kontrol eden nöbetçiler görev yapmıştır. Bilginin güvenliğini sağlamaya yönelik fiziksel önlemler alınmasına rağmen genellikle bu korumalar yeterli olmamış, bilgilerin çalınması veya istenmeyen kişilerin eline geçmesi engellenememiştir [48]. Geçmişten günümüze fiziksel güvenlik önemini korumakta

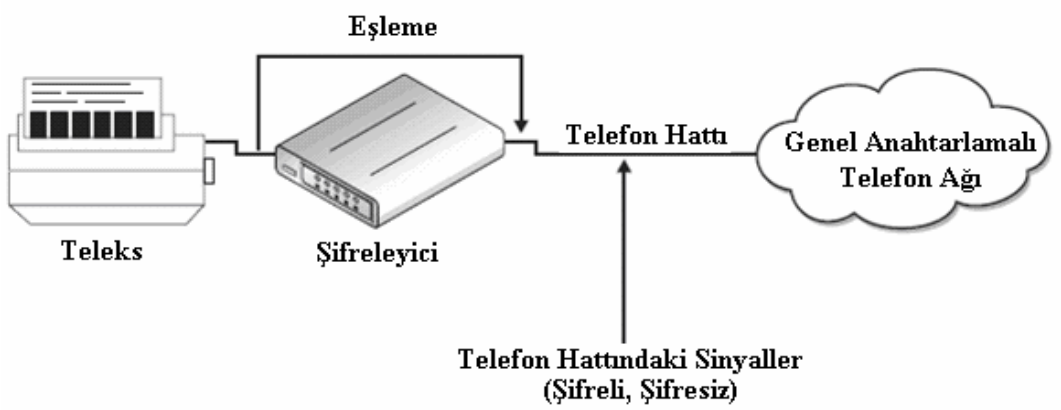
ve bu konuyla ilgili gerekli çalışmalar, gelişen teknolojinin yardımıyla günümüzde de yapılmaktadır. Binaların etrafına çitlerin çekilmesi, bina içi ve dışının kameralarla izlenmesi, koruma duvarlarının yapılması, bina girişinde özel güvenlik görevlilerinin bulundurulması, önemli bilgilerin tutulduğu odaların kilitlenmesi, önemli odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler günümüzde kullanılan fiziksel güvenlik önlemlerine örnek olarak verilebilir.

2.3.2. Haberleşme güvenliği

Karşılıklı bilgi alışverişinde güvenli bir haberleşme ortamını oluşturmak üzere yapılan faaliyetlerin ortak adı haberleşme olarak adlandırılır [49]. Haberleşme anında fiziksel olarak bilgilerin güvenliğinin sağlanması, güvenlik açısından yeterli değildir. İletişim sırasında bilginin hedefe ulaşmadan önce başka kişiler tarafından ele geçirilmesi ve içeriğin öğrenilmesi riski her zaman vardır. Haberleşme güvenliğinin sağlanmasında kullanılan yöntemler tarih boyunca değişmemiş fakat bu güvenliği sağlamak için kullanılan teknikler ve yöntemler sürekli olarak gelişmiştir. Haberleşme güvenliğinin sağlanmasında kriptografi ve steganografi yöntemleri kullanılmaktadır [50–55].

2.3.3. Yayılım güvenliği

Yayılım güvenliği, elektronik sistemlerin meydana getirdiği yayılımların yetkisiz kişilerce ele geçirilip analizinin önlenmesidir [56]. İyi bir şifreleme sistemini kırmak için zamana ve iyi donanımlara ihtiyaç vardır. Ancak zaman ve donanım çoğunlukla sağlansa bile şifreleme sistemlerini kırmak zordur. O zaman saldırganların aklına şu soru gelmektedir “Acaba gizli bilginin şifrelenmeden önceki haline ulaşabilirmiyiz?” bu sorunun cevabı evet’tir. Gizli bilgilerin şifrelenmeden önceki hallerinin yakalanabilmesi olasılığı bilgi güvenliğini tehdit eden en büyük risklerden birisidir. 1950’li yıllarda teleks cihazıyla yazılan bir mesajın şifreli şekilde telefon hattına iletilmesine rağmen, telefon hattı üzerinde şifreli ve şifresiz (orijinal) metinlerin yer aldığı görülmüştür [48].



Şekil 2.2. Şifrelemenin atlanması (by-pass)

Şekil 2.2'de gösterilebileceği gibi şifreleme cihazı mesajı şifreleyerek telefon hattına iletmektedir. Teleks cihazından istem dışı yayılan elektrik sinyalleri sebebiyle mesajın orijinal hali (şifresiz) telefon hattı üzerinde bulunmaktadır. Bu durumdan yararlanılarak ve bu işe özgü geliştirilmiş donanımlarla hat üzerindeki şifrelenmemiş bilgiye erişmek mümkündür.

Tüm elektronik cihazlar çevreye elektromanyetik sinyal yayarlar. Elektromanyetik sinyaller havadan radyoelektrik dalgalar olarak, elektrik dağıtım veya telefon şebekesine elektriksel gürültü olarak, çeşitli kabloların yüzeylerinden iletilen elektromanyetik dalgalar olarak yayılırlar [57]. Elektronik cihazlardan yayılan istenmeyen elektromanyetik yayılımlardan faydalanılarak bilgiye ulaşmak mümkündür. Özel anten veya başka uygun cihazlarla elde edilen işaretler uygun bir işleme devresinden geçirilerek (filtreleme, şiddetlendirme, eksik kısımları yeniden oluşturma, vb.) anlamlı bir hale getirilebilir.

ABD tarafından, her türlü istem dışı yayılımın kaydedilerek bilgi/veri analizi yapılması şeklindeki bilgi elde etme şekli Tempest (Transient Electro Magnetic Pulse Emanation Standard) adı altında standartlaştırılmıştır [58]. Tempest standartlarının tamamı güvenlik gerekçesiyle gizli tutulmaktadır. Tempest yöntemiyle bilginin elde edilmesine en yaygın örnek bir bilgisayar ekranından yayılan istem dışı elektromanyetik dalgaların yüzlerce metre öteden kaydedilerek analizinin yapılıp bilgisayarın ekran görüntülerine ulaşılmasıdır. Diğer bir örnek ise bilgisayar

kullanıcısının bastığı her tuş bina dışında, karşı apartmanda bulunan bir Tempest alıcısının ekranında görüntülenebilmesidir. Tempest dinlemelerini engellemek için Tempest sertifikalı cihazlar satılmaktadır. Ülkemizde Tübitak UEKAE tarafından geliştirilen bu cihazlar diğer ürünlere göre çok daha pahalıdır. Daha ucuz bir çözüm ise elektromanyetik dalgalara gürültü adı verilen anlamsız dalgalar katarak dinlenmelerin engellenmesi yöntemidir. Daha yüksek seviyede bilgi güvenliği arzu edilen yerlerde binalar inşa edilirken Tempest kurallarına göre binaların dış yüzeyleri özel zırhlarla giydirilmeli (faraday kafesi), dışa bakan pencere sayıları sınırlı olmalı, kabloların geçtiği kanallar yine özel zıhlarla kaplanarak korunmalıdır.

2.3.4. Bilgisayar güvenliği

Bilgisayarların ortaya çıkması ve kullanımının yaygınlaşmasıyla birçok veri ve bilgi, bilgisayar ortamlarında tutulmaya başlanmıştır. Fiziksel güvenlik, yayılım güvenliği ve haberleşme güvenliğinden sonra bilgisayar güvenliği, bilgi güvenliğinin sağlanması açısından önem kazanmıştır. İlk elektronik bilgisayar geliştirildiğinde, eğitimli kişilerin çok az olması ve bu kişilerin iyi niyetli olması nedeniyle, fiziksel tehditler dışında pek fazla güvenlik problemi ortaya çıkmamıştır. Bilgisayarlar iş dünyasında kullanılmaya başladığında, bilgisayarların güvenliğini korsan saldırıları ve bilgisayarlardan sorumlu olan kişilerin kötü niyetli davranışları tehdit etmeye başlamıştır. 1970'li yılların başında David Bell ve Leonard La Padula bilgisayar güvenliğine ilişkin bir model geliştirmişlerdir [59]. Bu model 1983 yılında ABD Savunma Departmanı 5200.28 nolu bu standardı kabul etmiş ve Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri (TCSEC-Trusted Computer System Evaluation Criteria) adlı kitabın (Turuncu Kitap-Orange Book) oluşmasını sağlamıştır [60]. Bu kitapta, bilgisayar sistemlerinin güvenliğini test etmek için oluşturulan güvenlik seviyeleri aşağıdaki gibi özetlenebilir [61–62].

En Düşük Koruma (D Seviyesi): Daha üst seviyedeki koşulları sağlayamayan sistemler bu kategoride yer alarak güvensiz ürünler sınıfında yer alırlar.

İsteğe Bağlı (discretionary) Koruma (C1 Seviyesi): Bu seviyedeki bir sistem, kullanıcıları ve veriyi ayırarak isteğe bağlı güvenlik seviyesini sağlamaktadır.

Bunlara ek olarak kişisel seviyede erişim sınırlamaları da sağlamaktadır. Kullanıcıların özel bilgilerini korumaları ve diğer kişilerin kazayla okumalarını engellemeleri için uygun bir sistemdir. Bir sistemin bu seviyede yer alabilmesi için güvenlik politikalarının, izlenebilirlik (kimlik denetimi, yetkilendirme) sistemlerinin, güvence ve dokümantasyon işlemlerinin sağlanması gerekmektedir.

Kontrollü Erişim (C2 Seviyesi): Bu seviye C1'e göre daha fazla ve daha alt düzeyde erişim kontrolü sağlamaktadır. Bu seviye oturum açma işlemleri, güvenlik olaylarının izlenmesi ve kaynak tahsisiyle kullanıcıların her birinin kontrol edilebilmesini gerektirmektedir.

Etiketlenmiş Güvenlik (B1 Seviyesi): B1 seviyesi kontrollü erişim seviyesinin tüm özelliklerini içermektedir. Bunlara ek olarak resmi olmayan güvenlik politikası modelini, veri etiketleme, isimlendirilmiş nesneler üzerinde zorunlu erişim kontrolünü de sağlaması gerekmektedir.

Yapısal Güvenlik (B2 Seviyesi): B2 seviyesinde Güvenli Hesaplama Esaslarının (TCB-Trusted Computing Base) açık olarak belirtilmesi ve döküm edilmiş biçimsel güvenlik politikası modeline dayanması gerekmektedir. Etiketlenmiş güvenlik seviyesindeki tüm özellikleri içermesi ve zorunlu erişim kontrolünün veri işleme sistemindeki tüm olay ve nesnelere kadar genişletilmesi gerekmektedir.

Güvenlik Alanları (B3 Seviyesi): B3 sınıfı TCB referans monitör gereksinimlerini sağlaması gerekmektedir. Bu seviye güvenlik yöneticisi tarafından desteklenmeli ve denetleme mekanizması tüm güvenlikle ilgili olayları kontrol etmesi için genişletilmeli ve sisteme düzeltme işlemleri eklenmelidir.

Onaylanmış Tasarım (A1 Seviyesi): A1 sınıfı fonksiyonellik açısından güvenlik alanları seviyesiyle aynıdır. Aradaki farklılık TCB'nin tasarım ve gerçekleme tekniklerinde yatmaktadır. Kullanılan teknikler sonucunda TCB daha doğru ve güvenilir bir şekilde gerçekleşir.

Bilgisayar güvenliği denildiğinde günümüzde akla bilişim sistemlerinin gizlilik, bütünlük, erişilebilirlik tehditlerine karşı korunması gelmektedir. Bilişim sistemleri

bilgisayarlar, bilgisayar ağları ve bilginin tutulduğu diğer tüm elektronik cihazlardan oluşmaktadır. Bilgisayar güvenliğini doğal olaylar (deprem, sel, vb.), kazalar (yangın, vb.), hizmet kesintileri (güç kaynağının arızalanması, vb.) ve insan faktörü gibi değişik kaynaklardan oluşan tehditler olumsuz yönde etkilemektedir. Bu tehditler ilerleyen bölümlerde kapsamlı olarak ele alınmıştır.

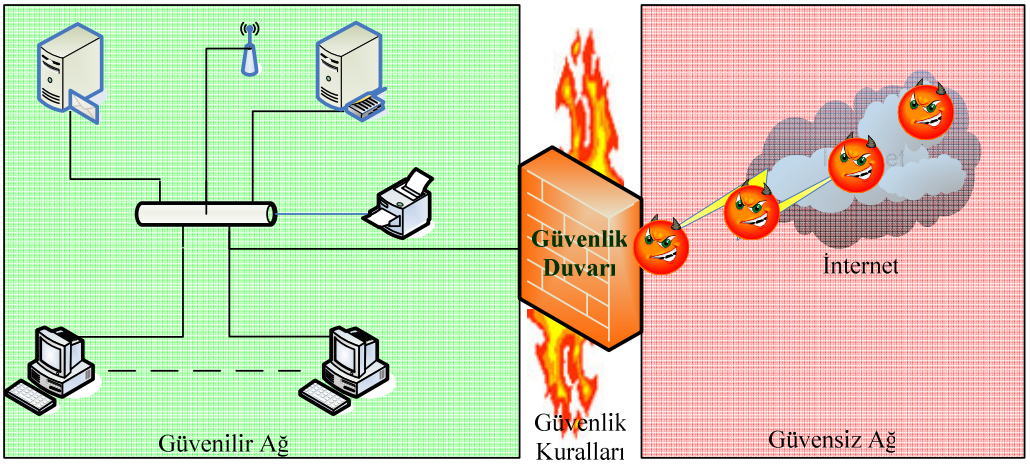
2.3.5. Ağ güvenliği

Ağ (network), paylaşım amacıyla iki ya da daha fazla bilgisayarın belirli bir ortam (media) aracılığıyla (bakır, fiber, vb.) haberleşme, bilgiye erişim, kaynak paylaşımı (veri, yazıcı, uygulamalar ve internet), yedekleme, gibi amaçlar için oluşturduğu yapıdır [63]. Ağ ortamlarının temelinde yatan paylaşım ve uzaktan erişim imkânlarının kullanılması sonucunda yeni güvenlik açıkları meydana gelmiştir. Bu açıklar, kötü niyetli veya meraklı kişiler tarafından kullanıldığında; bilgilere yetkisiz erişim, sistemler ve servislerin kullanılamaz olması, bilgilerin değiştirilmesi veya ifşa edilmesi vb. güvenlik ihlâlleri oluşmaktadır. Bilgisayar ağlarının yaygınlaşmasıyla güvenlik ihlâlleri artmış, bilgi güvenliği için alınması gereken önlemler fazlalaşmıştır.

Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri (TCSEC-DoD Trusted Computer System Evaluation Criteria) ağ sistemlerinin güvenliği için geliştirilmediğinden 1987 yılında TCSEC'in güvenilir ağ yorumlaması (Trusted Network Interpretation) adını verdiği Kırmızı Kitap (Red Book) yayımlanmıştır [64]. Kırmızı Kitap, Turuncu Kitaba ek olarak bilgisayar ağları ve bileşenlerinin güvenliğiyle ilgili konuları da içermektedir. Ancak işlevsellik açısından pek kullanışlı olmadığından çok fazla kullanım alanı olmamıştır.

Bilgisayarlar, ağlar aracılığıyla kablolu veya kablosuz olarak birbirleriyle iletişim kurmaktadır. Kablolu ve kablosuz ağ ortamlarının güvenliğinin sağlanmasıyla ilgili farklı çözümler geliştirilmiştir. Bu bölümde öncelikle genel olarak ağ güvenliğinin sağlanmasında kullanılan temel çözümler olan güvenlik duvarları (firewall), saldırı tespit sistemleri (IDS) açıklanacak, sonrasında ise kablosuz ağlara özel olarak geliştirilen güvenlik çözümlerinden bahsedilecektir.

Güvenlik Duvarı: Güvenilir ağların (kurumsal ağlar) sınır kısmında denetleme noktaları oluşturarak, bu denetleme noktalarından güvensiz ağlara (internet) doğru giden veya güvensiz ağlardan gelen ağ trafiğini, kurumsal güvenlik politikalarında belirlenen kurallar veya filtrelere göre denetleyerek hangi isteklerin kabul veya red edileceğine karar veren yazılım veya donanım çözümleridir [65]. Güvenlik duvarları, tek noktadan erişim denetimi ile ağ üzerindeki bilgisayarlara dış dünyadan erişen kullanıcıların kullanımına kurallar koyarak olası saldırıların en aza indirilmesinde kullanılmaktadır. Bilgisayar güvenliğinin sağlanmasında gizlilik, erişilebilirlik, bütünlük ve kimlik denetimi gibi temel bilgi güvenliği unsurlarını tehdit eden saldırılara karşı bazı önlemler güvenlik duvarları tarafından alınmakta ancak bu önlemler bilgisayar güvenliğinin sağlanmasında tek başına yeterli değildir. Kurumsal bilgisayar ağlarında ağ güvenliğinin sağlanmasında kullanılan güvenlik duvarına bir örnek, Şekil 2.3'te verilmiştir.



Şekil 2.3. Güvenlik duvarı yapılandırmasına bir örnek

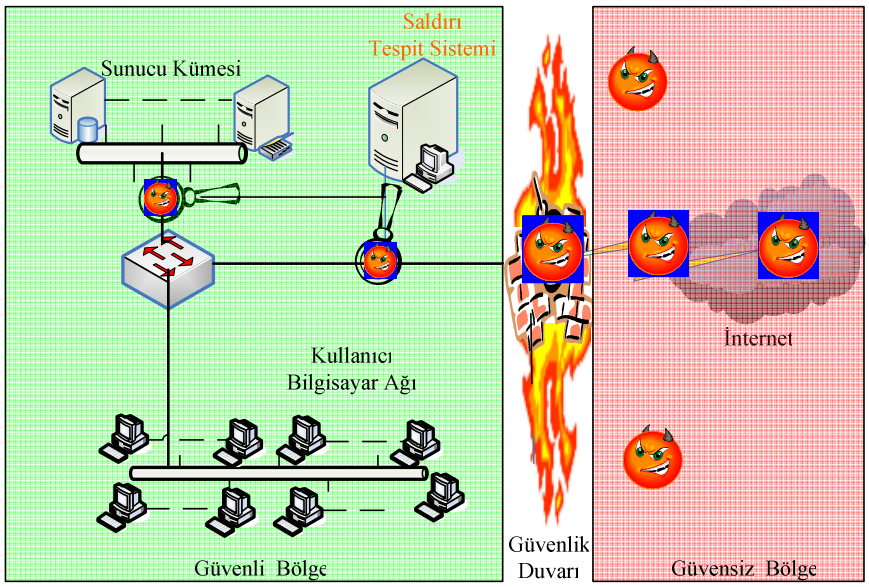
Güvenlik duvarları, dış ağlardan (güvensiz ağ) gelecek tehditlere karşı kendi üzerinden geçen ağ trafiğini koruma altına alırken ağ içerisinden gelecek tehditlere, izin verilen servislerden gelen saldırılara, arka kapılara ve virüslere, sazan avlamalara ve casus yazılımlara karşı koruma sağlayamazlar. Farklı yapılandırma şekilleri olsa da güvenlik duvarları saldırıları engellemede ve güvenliği sağlamada daha önceki paragrafta vurgulandığı gibi tek başına yeterli değildir ancak ağ güvenliğinin sağlanmasında önemli bileşenlerden birisidir.

Saldırı Tespit Sistemi (Intrusion Detection System-IDS) bilgilerin; gizlilik, bütünlük ve erişilebilirliğini tehdit eden, yetkisiz olarak bilgiye erişebilmek için bilgisayar ağlarına veya bilgisayarlara karşı yapılan saldırıların tespit edilmesinde kullanılan uyarı veya alarm sistemleri olup güvenlik duvarının yetersiz kaldığı durumlarda ek koruma sağlamaktadır [66]. Saldırıyı önceden tespit ederek engellemek, saldırı sonucu çalışmayan bir sistemi yeniden çalışır hale getirmekten daha ekonomik bir çözümdür.

Saldırı tespit sistemleri, içerik olarak iki farklı mimaride çalışmaktadırlar. İlk yapıda çeşitli imzalar (veri tabanına kayıtlı saldırılar) ile paketleri incelemek ve saldırıları tespit etmek amaçlanmaktadır. İkinci yapıda ise bilgisayarların ve ağın normal işleyişi belirlenerek, olabilecek herhangi bir normal dışı hareketin saldırı olarak algılanması sağlanmaktadır. İmza tabanlı saldırı tespit sistemleri günümüzde yaygın olarak kullanılmaktadır. Antivirüs sistemleri gibi ağ üzerinde yakalanan paketleri inceleme şeklinde çalıştıkları için saldırının imza tanımının önceden tanımlanmış olması gereklidir. Bu yöntemin can alıcı noktası, saldırı imza listelerinin güncellenmesinin sağlanmasıdır aksi takdirde güncel saldırılara karşı koruma sağlanamayacaktır.

İkinci yapıdaki saldırı tespit sistemlerinde ise, ağda veya çeşitli sunucularda düzenli olarak yapılmakta olan işlemler takip edilerek sistemin normal işleyişinin zeki yaklaşımlarla (yapay sinir ağları, bulanık mantık, uzman sistemler, vb.) öğrenilmesi esasına dayanır. Bu yapıda çalışan saldırı tespit sistemleri, anormal hareketler gördüklerinde bu hareketleri saldırı olarak rapor ederler. Örnek vermek gerekirse, isim çözme sunucusuna (DNS) normal işleyişinde TCP/UDP 53 nolu porttan istek gelmesi gerekirken, TCP/23 (telnet) portundan istek gelmesi saldırı olarak algılanabilir. Öğrenme temelli saldırı tespit sistemlerinin gerçek hayattaki çalışması örnekte anlatıldığı kadar da başarılı değildir. Çünkü bu tür sistemlerin normal olarak nitelendirilebilecek davranışları öğrenmeleri oldukça fazla zaman almaktadır. Ayrıca bu davranışların zaman içerisinde değişebilirliği, kurulduğu sistemlerin yeniden yapılandırılması veya yeni sistemlerle birlikte yeni davranışların eklenmesi öğrenme işini zorlaştırmaktadır.

Kurumsal bilgisayar ağlarında yer alan saldırı tespit sistemine bir örnek Şekil 2.4'te verilmiştir.



Şekil 2.4. Saldırı tespit sistemine bir örnek

Saldırı tespit sistemlerinin kullanımında en fazla karşılaşılan problemlerden birisi saldırı tespit sistemlerinin sistemdeki normal bir davranışı saldırı olarak tespit etmesidir (False Positive). Bu hatadan dolayı saldırı tespit sistemlerinden beklenen başarı elde edilememiştir.

Kablosuz ağlar, son zamanlarda oldukça ilgi gören ve kullanımı gittikçe yaygınlaşan bir ağ türüdür. Kullanıcılara sunduğu hareketlilik (mobility) imkânı, kablolama maliyetinin olmayışı, kullanım kolaylığı ve buna benzer üstünlüklerinden dolayı günümüzde giderek daha fazla tercih edilmeye başlanmıştır. Kablosuz ağların, iletim ortamı olarak havayı kullanmasından kaynaklanan güvenlik problemlerinden dolayı, kablolu ortamlara göre güvenliğinin sağlanması daha zordur.

WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) ve EAP (Extensible Authentication Protocol) kablosuz ağlar için geliştirilen güvenlik protokolleridir [67]. Kimlik doğrulama mekanizması olmayan WEP algoritması, kablosuz ağ güvenliğini sağlamada (bütünlük, gizlilik) sonradan yapılan

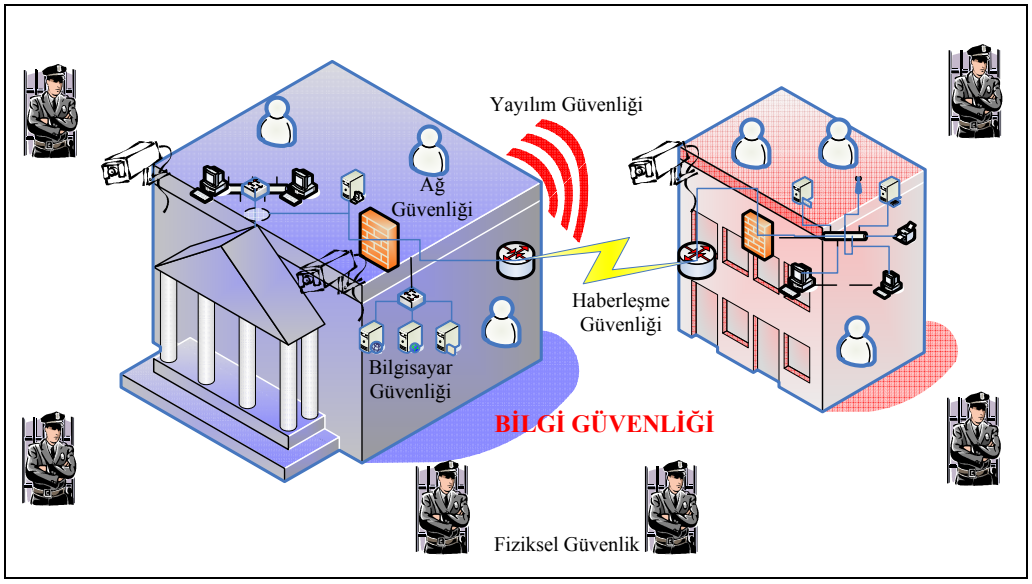
iyileştirmelere rağmen başarısız olmuştur. WPA, WEP protokolünün eksikliklerini gidermesi için Wi-Fi Alliance ve IEEE tarafından geçici olarak oluşturulmuş bir protokoldür. WPA, WEP'e göre daha güçlü bir şifreleme yöntemi olan TKIP (Temporal Key Integrity Protocol)'i desteklemektedir. EAP protokolü ise uçtan uca iletişim için kimlik doğrulaması sağlar [68]. Kablosuz ağların güvenliğinin sağlanması için IEEE tarafından kablosuz ağlardaki güvenlik problemlerine detaylı çözümler üretmesi amacı ile 802.11x standardı geliştirilmiştir. Bu standartla güvenilir bir şifreleme, kimlik doğrulama ve veri bütünlüğünün sağlanması amaçlanmaktadır [69].

2.3.6. Bilgi güvenliği

Bilgi güvenliğinin sağlanabilmesi için daha önceki bölümlerde anlatılan güvenlik önlemlerinin tamamının birlikte değerlendirilmesi gerekmektedir. Bir kurum veya kuruluşun kâr etmek, değer yaratmak, rekabet avantajını ve sürdürülebilir büyümeyi yakalamak için sahip olduğu veya sahip olması gereken, pazar, ürün, teknoloji ve organizasyona ait bilgilerin tamamı bilgi varlıkları olarak tanımlanabilir. Bilgi varlıklarının fiziksel olarak korunması için fiziksel güvenliğin, iletim halindeki bilgilerin güvenliğinin sağlanması için haberleşme güvenliğinin, elektronik sistemlerden istem dışı yayılan sinyallerin kullanılarak önemli bilgilerimize ulaşılmaması için yayılım güvenliğinin, bilgisayarlarımıza erişimin kontrol altına alınması için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir.

Bilginin güvenliğinin yüksek seviyede sağlanabilmesi için yukarıda açıklanan güvenlik türlerinin tamamının Şekil 2.5'de gösterildiği gibi uygulanması gerekmektedir. Bilgi güvenliği ile ilgili literatürde çeşitli tanımlamalar yapılmıştır. Bu tanımlardan bazıları şu şekildedir.

- Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır [70].
- Bilgi güvenliği, yetkisiz erişim ve kullanım, ifşa etme, yok etme, değiştirme, bozma gibi saldırı tehditlerinden verilerin korunması sürecidir [71].



Şekil 2.5. Bilgi güvenliğini sağlama unsurları

- Bilgi güvenliği; bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etme (gizlilik), bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etme (bütünlük) ve yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etme (erişilebilirlik) olarak tanımlanmaktadır. [72].
- Bilgi güvenliği kurumsal BT (Bilgi Teknolojileri) kaynaklarının erişilebilirlik, bütünlük ve gizliliği üzerindeki risk etkilerinin azaltılarak disiplinize edilmesidir [73].
- BS 7799 bilgiyi, diğer bütün önemli iş varlıkları gibi, bir kurum açısından değeri olan ve dolayısıyla korunması gereken bir varlık olarak tanımlamaktadır. Bilgi güvenliği; iş devamlılığını sağlamak, iş hasar ve zararlarını asgari düzeyde tutmak ve yatırım geri dönüşü ve getirilerini ve iş fırsatlarını azami düzeye çıkartmak amacıyla, bilgiyi çok çeşitli tehditlere karşı korur [74].
- Programlar ve medyalar (sabit diskler, bilgisayar ağları, cdrom, vb.) üzerinde depolanan verilerin korunması, kaybolmaması ve gizliliğinin sağlanmasını içerir [75].
- Elektronik bilgi güvenliği, haberleşme ve bilgisayar güvenliğini kapsar. Temel olarak bilgilerin ifşa edilmesini, yok edilmesini, değiştirilmesini engeller [76].

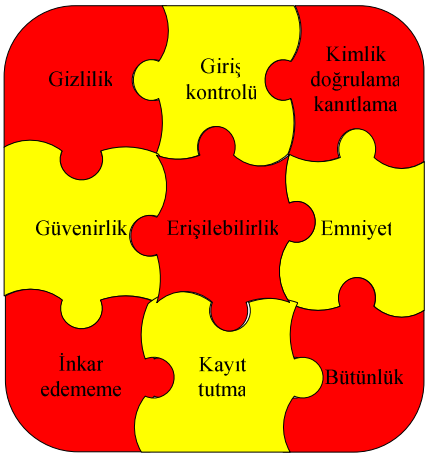
- Gizlilik, inkâr edilemezlik, veri bütünlüğü, erişim kontrolü ve kimlik denetimi ilkelerini gözeterek bilginize kim tarafından erişilebildiğinin kontrol edilmesidir [77].
- Bilgi güvenliği yalnızca yetkili tarafların veriyi görmesini ve işlem yapmasını (gizlilik), yasal yollardan kodları ve veriyi değiştirmesini (bütünlük), ihtiyacı olduğunda verilere veya programlara erişmesinin (erişilebilirlik) sağlanmasıdır [78].
- Bilgi güvenliği bilgi ve onu destekleyen (taşıma, depolama, işleme, vb.) altyapının kazara veya kasıtlı olarak doğal veya yapay tehditler aracılığıyla gelebilecek zararlardan korunması anlamına gelmektedir [79].

Bilgi güvenliği ile ilgili literatürdeki tanımlarda dikkate alındığında uzmanların sahip oldukları bilgi birikimi ve özel uzmanlık alanlarına göre bilgi güvenliğine farklı açılardan bakıldığı görülebilir. Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci *bilgi güvenliği* olarak tanımlanabilir.

Bilgi güvenliğinin sağlanılmasında uyulması ve uygulanması gereken birçok güvenlik bileşeni vardır. Öncelikle üç ana ilke olan gizlilik, bütünlük ve erişilebilirlik ilkelerine uyulması sonrasında da bu ilkelere ek olarak değerlendirilebilecek giriş kontrolü, emniyet, inkâr edememe, güvenirlik, kayıt tutma, kimlik tespiti gibi Şekil 2.6'da gösterilen ilkelere uyulması bilgi güvenliğinin üst düzeyde sağlanabilmesi için gereklidir [80]. Şekil 2.6'da kırmızıyla gösterilen unsurlar ana unsurları göstermektedir. Sarı ile gösterilen diğer unsurlar ise destekleyici unsurlardır. Bu unsurlar aşağıda kısaca tanıtılmıştır.

Gizlilik: Elektronik ortamlarda taşınan bilginin; yetkisi ve izni olmayan kişiler veya süreçler tarafından elde edilse bile anlamlı olarak ele geçmesinin engellenmesi olarak tanımlanabilir. Gizlilik, statik ortamlar (disk, teyp, cd, dvd, vb.) veya ağ üzerinde bir göndericiden bir alıcıya gönderilen dinamik ortamdaki veriler için sağlanmak zorundadır. Saldırganlar, yetkileri olmayan gizli bilgilere birçok yolla erişebilirler. Burada amaç saldırganlar tarafından bu bilgiler elde edilse bile anlaşılmasını veya

çözülmesini zorlaştıracak yaklaşımlar kullanılarak taşınan bilgi çözülemeyecek başka bir formata dönüştürülür. Gizlilik ilkesinin sağlanmasında şifreleme algoritmaları ve steganografi yöntemleri kullanılmaktadır [50–55].



Şekil 2.6. Bilgi güvenliği unsurları

Bütünlük: Bilginin göndericiden çıktığı haliyle bozulmadan bir bütün olarak alıcısına ulaştırılmasını garanti eden bir güvenlik unsurudur. Bilgi haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaştırılarak bütünlüğü sağlanır. Bilginin bütünlüğünün sağlanılması için özetleme (hashing) algoritmaları kullanılmaktadır.

Erişilebilirlik: Talep edilen bilgiye kullanıcıların yetkisi dâhilinde zamanında erişim yapabilmesi için gerekli olan önlemlerin alınması olarak tanımlanabilir. Erişilebilirlik bilişim sistemlerini kullanan kişiler veya süreçler tarafından büyük bir önem taşımaktadır. Bilişim sistemlerinden kendilerinden beklenen işleri belirlenen bir zaman diliminde yapmaları beklenir. Erişilebilirlik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek erişilebilirliği düşürücü tehditlere (Denial of Service Attack-DoS) karşı korumayı hedefler. Bu bileşen sayesinde, kullanıcılar, erişim yetkileri dâhilinde olan bilgilere, güncel, zamanında, hızlı ve güvenli bir şekilde ulaşabilirler. Bilgisayar yazılımlarındaki güvensiz kodlar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması veya konfigüre edilmesi,

doğal felaketler sistem erişilebilirliğini olumsuz yönde etkileyen önemli faktörlerdir. Bilgi sistemlerine erişilebilirliğin sürekli sağlanması için fiziksel önlemler alınmalı, güvenlik duvarları, casus savar yazılımlar, atak tespit sistemleri, virüs savar yazılımlar kurulmalı ve güncellenmelidir.

Kayıt (Log) tutma: Elektronik ortamda gerçekleşen olayların (bilgisayar ağı üzerinde meydana gelen herhangi bir faaliyet) daha sonra analiz edilmek üzere kayıt altına alınması olarak tanımlanabilir. Kullanıcının parolasını yazarak sisteme girmesi, web sayfasına bağlanması ve e-posta iletişimi gibi örnekler kayıt altına alınması gereken olaylara örnek olarak verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin izlerine rastlanırsa ve saldırı olasılığı yüksek bir aktivite tespit edilirse, atak tespit sistemleri tarafından alarm mesajları üretilerek sistem yöneticileri uyarılır. Kayıt tutma bileşeni saldırıların ve saldırganların belirlenmesi içinde ayrıca bir önem arz etmektedir. Saldırı olduktan sonra oluşan kayıtlar saldırı tipi ve saldırganın kimliğinin tespit edilmesine yardımcı olur. Kayıt tutulmayan bir sisteminm güvenliğinden bahsedilemeyeceği her zaman hatırda tutulmalıdır.

Kimlik tespiti (kanıtlama ve doğrulama): Bilgi sistemlerinden hizmet alan alıcının, iddia ettiği kişi olduğundan emin olunması olarak tanımlanabilir. Örneğin, giriş izniniz olan herhangi bir elektronik ortama eriştiğinizde size sorulan şifreler, bilgisayarınızı açarken şifre girilmesi kullanıcının kimliğinin tespit edilmesinde kullanılan yöntemlerdir. Günümüzde kimlik tespiti, bilgisayar ağları ve diğer sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı kartlar, tek kullanımlık parolalar (one time password), jetonlar, elektronik imza kartları, biyometrik teknolojiler kimlik tespitinde kullanılan teknolojilerden bazılarıdır.

Güvenirlik: Bilgisayar sistemlerinin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumu olarak tanımlanabilir. Diğer bir ifadeyle güvenirlik, herhangi bir bilgi sisteminden ne yapmasını bekliyorsak, sistemin kendisinden beklenileni yaparak her çalıştırıldığında da aynı sonuçları vermesi olarak tanımlanabilir. Örneğin ağ içerisinde yer alan merkezi dağıtıcı anahtarın (switch) 24

saat boyunca kesintisiz çalışması beklenmektedir. Güvenirlik, cihazın çalıştığı zaman dilimi ile çalışması gereken zaman dilimi kıyaslanarak hesaplanmaktadır.

İnkâr edememe: Elektronik ortamlarda gönderici ve alıcı arasındaki haberleşmenin inkâr edilmemesi için gerekli olan önlemlerinin alınmasını sağlayan güvenlik unsurudur. Alınan güvenlik önlemleri sayesinde gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların, oluşabilecek zararların en aza indirilmesi sağlanır. Bu güvenlik unsuru, özellikle gerçek zamanlı işlem gerektiren bankacılık ve finans bilgi sistemlerinde yoğunlukla kullanılmaktadır. İnkâr edememe unsuru elektronik imza ve açık anahtar altyapısı kullanılarak sağlanmaktadır.

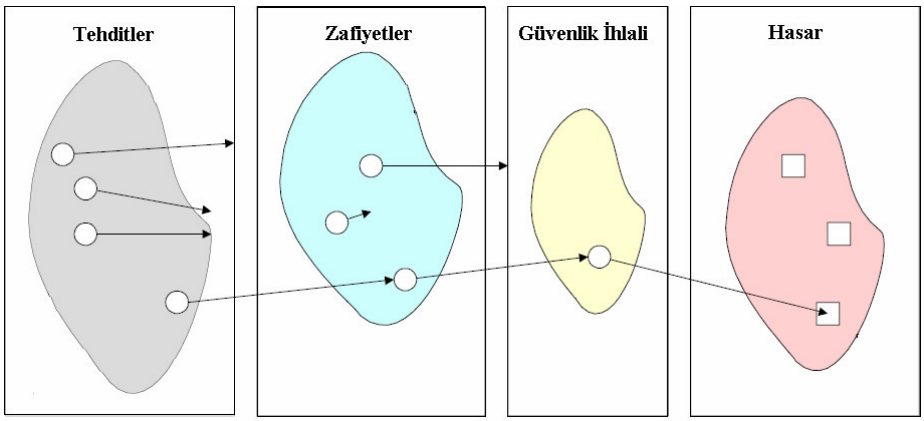
Giriş kontrolü (Erişim listeleri): Bilgi sistemlerine erişmek için kimlik tespiti yapılmış olan kullanıcı veya uygulamalara belirlenen yetkilerin atanması, bir kaynağa erişmek için belirli izinlerin verilmesi veya alınması olarak tanımlanabilir.

Emniyet: Bilgi sistemlerini tehlikelerden koruyacak olan fiziksel veya teknik çözümlerdir. Bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda kendisi veya gömülü olduğu ortam için istenmeyen potansiyel veya bilfiil tehlike oluşturacak etkinlik veya olayları engelleme girişimidir.

2.4. Bilgi Güvenliği Tehditleri

Tehdit, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini olumsuz yönde etkileme olasılığı olan tanımlı risklerdir [81]. Tehditlerin bilgi sistemlerinde etkili olabilmesi için bilgi sistemleri üzerindeki var olan zafiyetleri kullanmaları gereklidir. Tehditlerin bilgi varlıklarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki açık ve varlığın değeri ile doğru orantılıdır. Tehditler uygun ortam şartlarının oluşmasıyla bilgi sistemlerine zarar verecek kusurları içeren zafiyetlere, zafiyetler saldırganlar tarafından kullanıldığında güvenlik ihlallerine yol açarak bilgi sitemlerine zarar vermektedir.

Tehditlerin bilgi sistemleri üzerinde hasar oluşmasına kadar izlediği süreç Şekil 2.7'de şematik olarak gösterilmiştir.



Şekil 2.7. Tehditlerin bilgi sistemlerine etkisi

Tehditler, tehdit kaynağı açısından bakıldığında;

- Doğal afetler veya teknik arızalarla ilgili tehditler
- Prosedürel eksiklerle ilgili tehditler
- İnsan faktöründen kaynaklanan tehditler ve
- Kötücül yazılımlarla ilgili tehditler, olarak

sıralanabilir.

Bu tehditler aşağıda alt başlıklar halinde anlatılmıştır.

2.4.1. Doğal afetler ve teknik arızalarla ilgili tehditler

Doğal afetler ve teknik arızalar çoğunlukla önceden tespit edilemedikleri için engellenmeleri çok zordur. Bu tehditlere karşı tüm tedbirler önceden planlanmalı ve uygulanmalıdır. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, kasırgalar, fırtınalar ve çığ düşmesi gibi afetler meydana gelebilecek tehditlere örnek olarak verilebilir. Doğal afet ve teknik arızalarla ilgili tehditlere verilebilecek diğer örnekler aşağıda maddeler halinde verilmiştir. Bunlar;

- Güç kaynağının arızalanması,
- Yangın söndürme sistemindeki arızalar,
- Telefon santral arızası,

- Aktif cihaz (yönlendirici, anahtar, vb.) arızaları,
- Sunucu bilgisayarlarda oluşabilecek yazılım veya donanım arızaları,
- Kripto sistemlerdeki hatalar (algoritma zayıflığı, anahtarların yetersizliği, vb.),
- Havalandırma sistemi arızaları,
- Kamera sistemlerinin arızaları,
- Kapı giriş çıkış sisteminde meydana gelen arızalar,
- Terör saldırıları (bombalama, kundaklama, vb.),
- Ayaklanmalar, gösteriler, eylemler, protestolar ve
- Veri depolama ağı ve yedekleme sistemlerinde meydana gelen arızalar

olarak sıralanabilir.

Doğal afetler ve teknik arızlarla ilgili tehditlerden herhangi birinin meydana gelmesi genellikle tüm bilgi sistemlerinin zarar görmesine veya çalışmamasına sebebiyet vermektedir. Bu tür tehditleri en az indirmek için kurumsal yapıya uygun felaket senaryoları üretilmeli ve felaketten en kısa zamanda nasıl geriye dönülebileceğiyle ilgili (disaster recovery) iş devamlılığı konusundaki çalışmalar önceden yapılmalıdır.

Çizelge 2.1. Prosedürel tehditler

İdari Prosedür Eksiklikleri	Teknik Prosedür Eksiklikleri
Personel işe alma ve işe son vermede güvenlik prosedürlerinin olmaması	Bilgi yedekleme prosedürlerinin olmaması
Güvenlikle ilgili görev ve sorumlulukların verilmesinde eksiklikler	Yardım masası (bilgisayar, kurulum ve bakım) prosedürleri eksikliği
Çalışanların güvenlik kural ve prosedürlerinden habersiz olması veya bu konuda eksik bilgilerinin olması	Bilgi envanterinin tutulmaması ve güncelliğini sağlayacak mekanizmanın olmaması
Görevlerin ayrıştırılması ve görev rotasyonu prosedürlerinin olmaması	Bilgi sistemleri izleme prosedürlerinin olmaması
Acil durumlarda veya felaket anlarında devreye alınacak Bilgi Süreklilik Planlarının olmaması	Ağ hizmetleri (e-posta, internet, dosya paylaşımı, vb.) kullanım prosedürlerinin olmaması
Güvenlik Politikası ve prosedürlerinin olmaması	Etki alanı hizmet (Şifre değiştirme, hesap açma, vb) prosedürlerinin eksikliği
Güvenlik bilinçlendirme eğitimlerinin planlanması ve uygulanmasına ait eksiklikler	Sunucu hizmetleri (dns, dhcp, etki alanı, vb.) Planlama ve Yönetim prosedür eksikliği
Tüm iş süreçlerinin belgelendirilmesine yönelik eksiklikler	İletişim hatlarının (ses, veri, vb.) denetimi ve yönetimine ait prosedür eksikliği

2.4.2. Prosedürel eksiklere dayalı tehditler

Bu tehdit türü kurumsallaşma süreçlerini tamamlayamayan kurum ve kuruluşlarda görülür. Prosedürel eksiklikler kendi arasında teknik ve idari olmak üzere iki gruba ayrılmaktadır. Prosedürel eksiklerle ilgili tehditlere örnekler Çizelge 2.1'de verilmiştir.

2.4.3. İnsan faktöründen kaynaklanan tehditler

İnsan faktöründen kaynaklanan tehditleri istem dışı veya bilinçli olarak yapılan kullanıcı davranışları olarak iki grupta incelemekte fayda vardır. Herhangi bir sistem üzerinde yetkiye sahip olan bir kullanıcının, bilgi sistemlerini bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerinin birinin veya birkaçının ihlal edilmesine sebep olan bilmeyerek veya ihmalkârlık sonucu yapılan kullanıcı davranışlarını insan faktöründen kaynaklanan istem dışı tehditler olarak tanımlayabiliriz. Son kullanıcılar, yazılım geliştiriciler, sistem yöneticileri gibi değişik düzeyde bilgi sahibi olan insanlar tarafından istem dışı veya ihmalkârlık sonucu yapılan davranışlardan kaynaklanan bazı tehditler maddeler halinde aşağıda sıralanmıştır. Bunlar:

- Güvenlik politikalarına uymama veya ihlal etme
- Güvenlik önlem ve kontrolleri almadan yazılım geliştirme
- Temizlik görevlisinin sunucunun fişini çekmesi
- Eğitilmemiş çalışanın yapılandırma ayarlarını kurcalaması
- Bilişim sistemlerinin yanlış kullanımı veya yönetimi
- Eksik veya hatalı yapılandırma
- Erişim haklarının ayarlanamaması
- Sistem kayıtlarının (log) analiz edilmeden silinmesi veya hiç tutulmaması
- Bilgisayar başında olunmayan zamanlarda parola korumalı ekran koruyucuyu devreye almama
- Hatalı yedekleme veya yedek almama
- Gereksiz servislerin hizmete açılması

- Antivirüs programını bilgisayarı yavaşlatıyor gerekçesi ile devre dışı bırakma
- Tanımadığı kişilerden gelen e-postaların eklerini açma veya e-postalar aracılığıyla istenilen gizli bilgileri verme
- Şifresini unutan kullanıcıların şifrelerini telefon yoluyla değiştirme
- Sistemlerin başlangıç (default) ayarlarında bulunması ve
- Şifrelerin masa üzerinde küçük yazılı kâğıtlarda tutulması olarak verilebilir.

İnsan faktöründen kaynaklanan ikinci tehdit türü iş yerine kızgın veya küskün olan ve hiçbir beklentisi olmayan sorunlu personelin görevini ve yetkisini kötüye kullanarak bilinçli olarak yaptığı kötücül davranışlardır. Bu kişiler günümüzde yerel saldırgan (internal hacker) olarak adlandırılmaktadır. Yerel saldırganların yapmış olduğu saldırılar sonrasında kurumlar yüksek oranda zarara uğramaktadır. Bilinçli olarak yapılan kötücül davranışlardan kaynaklanan bazı tehditler maddeler halinde aşağıda sıralanmıştır

- Yetkisi ve görevi dâhilinde olmayan bilgisayar sistemlerine girmek ve içerisindeki gizli bilgilere erişmek
- Görevi gereği bildiği üst düzey yetkiye sahip şifreleri kurum dışına menfaat sağlama amacıyla sızdırmak
- Veritabanındaki bazı kayıtları silmek, değiştirmek veya tamamen yok etmek
- Güvenlik sunucularını (güvenlik duvarı, saldırı tespit sistemi, antivirüs, vb.) bilerek yanlış yapılandırma veya devre dışı bırakma
- Yapılan kötücül davranışların iz bırakmaması amacıyla güvenlik kayıtlarından silinmesi ve
- Bilinçli olarak kötücül programların bilgisayarlara bulaştırılması gibi ve benzeri örnekleri daha da çoğaltmak mümkündür. Bilinçli olarak yapılan birçok davranış suç teşkil etmektedir.

Verilen örneklerden anlaşılacağı gibi bilgisizlik, bilinçsizlik, isteksizlik ve ihmalkârlık ve görevini kötüye kullanma gibi insan hatalarından kaynaklanan tehditler bilgi güvenliği tehditleri arasında önemli bir yer tutmaktadır. Bilgi

güvenliğinin sağlanmasında insan faktörü Bölüm 6.1'de kapsamlı olarak incelenmiştir.

2.4.4. Kötücül yazılımlara dayalı tehditler

Saldırganların, donanım veya yazılım açıklıklarını kendi çıkarları için kullanarak istedikleri bilgiye erişebilmelerini sağlayan tehditlerdir. Saldırılar çıkar amaçlı olarak yapılabildiği gibi kendi ünlerini duyurmak isteyen bireysel saldırganlar veya önceden planlanmış belirlenen hedefler doğrultusunda organize olmuş çeteler veya çıkar amaçlı örgütler tarafından yapılmaktadır. Günümüzde saldırıların büyük bir çoğunluğu kötücül yazılımlar (Malicious Programs) olarak adlandırılan programlar aracılığıyla yapılmaktadır. Kötücül yazılımlara dayalı olarak yapılan saldırılarda kullanılan yaygın tehditler başlıklar halinde takip eden paragraflarda verilmiştir.

Virüsler: Virüsler üzerinde ilk ciddi çalışmaları yapmış olan matematikçi Dr. Frederick Cohen virüsü "başka programların içine kendisini kopyalayarak bulaşan bir bilgisayar programı" olarak tanımlamıştır [82]. Virüsleri bilgisayar sistemlerine, ortamlarına ve bilgilere zarar vermek üzere geliştirilmiş program kodları olarak da tanımlayabiliriz. Bu programlar bilgisayarlara doğrudan zarar vereceği gibi, kendi kodunun kopyasını başka program kodlarına ekleyerek çoğalırlar ve verilen zararları artırırlar. Virüsler hem kendilerini kopyalayacak kodları, hem de zarar verici işlem yapacak kodları birlikte içerirler. Virüsleri diğer programlardan ayıran özellik, girdiği sistemlere kendilerini, kullanıcının farkında olmadan isteği dışında kopyalayarak sistemlere zarar vermesidir. Kullanıcı tarafından çalıştırılmadan veya kendisini programlayan kişi tarafından önceden belirlenmiş durum oluşmadan aktif hale gelemezler. Bazı virüsler ise aktif hale geldikleri halde, belli bir süre etkilerini göstermezler.

Bulaşma aşamasında virüsler, kendilerini başka dosyalara kopyalayarak hızla çoğalırlar, yürütme (execution) aşamasında ise programlandıkları zararlı faaliyeti gerçekleştirirler. Virüsler, disketler, ağ paylaşımı, internet (e-posta, dosya indirme, vb.) yollarıyla yayılırlar. Aktif olduklarında dosyaları silebilirler, verileri değiştirebilirler, bilgisayarı yavaşlatabilirler, müzik çalabilir, ekrana çeşitli mesajlar

çıkartabilirler. Bazı virüsler zarar verici işlemler yapmasa da hata içerirler ve sistem kaynaklarını gereksiz yere kullanırlar. Genelde işletim sistemine veya donanıma bağımlı olarak çalışırlar. Her geçen gün sayıları ve verdikleri zararları artmakta olan virüslerin boot sektörü, yürütülebilir, TSR, gizli, şifreli, polimorfik ve makro virüsleri olmak üzere çok sayıda çeşidi bulunmaktadır.

Solucanlar (worms): Herhangi bir yardım almaksızın ağ üzerindeki bilgisayarların korunmasızlıklarından faydalanarak kendiliğinden diğer bilgisayarlara bulaşan ve bilgisayar ağları üzerinde yayılan saldırı yapma amaçlı kullanılan kötücül programlardır. Virüslerden farkı tanımda belirtildiği gibi kendiliğinden yayılır ve kendisinin değişik kopyalarını otomatik olarak ağ aracılığıyla başka sistemlere dağıtırlar. Solucanlar ilk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirdikten sonra kendi başına ilerleyebilir. Solucanların en büyük tehlikesi, kısa zamanda kendilerini büyük sayılarda internet üzerinden çok kullanılan protokoller (HTTP, SMTP, vb.) aracılığıyla çoğaltma becerileridir. Örneğin bir solucan, e-posta adres defterinizdeki herkese kopyalarını gönderebilir ve sonra yaptığı işlemlerin aynısı gönderilen bilgisayarlarda da yapabilir. Yeni solucanlar ilk ortaya çıktıklarında çok hızlı yayılırlar. Solucanlar; işlemci, bellek veya ağ bant genişliği gibi kaynakları tüketerek, kaynağını kullandığı sistemlerin yavaşlamasına veya çökmesine yol açabilirler. Solucanların e-posta aracılığıyla tek veya toplu olarak yayılabilen, birden fazla bilgisayar üzerindeki program kümeleri şeklinde çalışabilen (ahtapot), ağ üzerindeki bilgisayarlar üzerinde tekil kopyalarını en yakınındaki bilgisayara kopyalayarak tavşan misali yayılan (rabbit) birçok türü vardır [83].

Truva atı (Trojan): Truva atları mitolojide bir armağan gibi görünüp, aslında Troya kentini ele geçirecek Yunanlı askerleri taşıyan bir araçsa; bugünün Truva atları görünüşte yararlı olup istenmeyen, zarar verici işlemler yapacak kodları içinde barındıran programlardır. Yaygın truva atlarına Back Orifice, Netbus, Schoolbus gibi programlar örnek olarak verilebilir. Truva atları bir bilgisayarın kontrolünü uzaktan ele geçirerek ekranın izlenmesini, dosyalar üzerinde işlemlerin yapılmasını, uzaktan komut çalıştırılmasını, klavye tuşlarının kontrol edilmesini sağlarlar. Truva atları

daha çok kullanıcılar tarafından rağbet gören oyunlar ve yazılım güncellemelerinde yer alırlar.

Truva atları; insanların meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya ikna edilmesi yoluyla genellikle e-postalar aracılığıyla yayılır. Truva atlarına, ücretsiz (shareware, freeware) veya lisanssız (kaçak) olarak yüklenilen yazılımlarda daha fazla rastlandığından güvenilmeyen kaynaklardan indirilen yazılımlar bilgisayara yüklenmemelidir. Truva atlarının bazıları da bulaştıkları sistemlerde tıpkı solucanlar gibi arka kapılar açarak sistemlere uzaktan erişim yapılmasını sağlarlar.

Casus yazılım (Spyware): Tanıtım, kişisel bilgi toplama veya kullanıcı onayının alınmadan bilgisayar yapılandırmasını değiştirme, kullanıcı bilgisayarının her türlü aktivitesini takip etme gibi çok farklı işlemleri kullanıcının bilgisi olmadan gerçekleştiren yazılımlar için kullanılmaktadır [84]. İstenmeyen zamanlarda açılan reklâm pencereleri, tarayıcıların ilk açtığı sayfa (giriş sayfanız) veya arama ayarları istem dışı değişmişse, bilgisayarın kısa zamanda tamamlaması gereken görevleri normalden daha uzun sürede tamamlıyorsa, aniden kilitlenmeler gibi olaylar casus yazılım veya başka bir "istenmeyen" veya "casus yazılım" olduğunun habercisi olabilir. Casus yazılımın veya diğer istenmeyen yazılımların bilgisayarlara girebilmesinin çeşitli yolları vardır. Müzik veya video dosyası paylaşım programı gibi istediğiniz başka bir yazılımı yüklerken, bu yüklenen yazılımın gerisinde gizlenmiş ve bu işlemle sisteme gizlice yüklenme, çok karşılaşılan yöntemlerden birisidir.

Arka kapılar (Back Door): Bilgisayar programlarına veya bilgi sistemlerine gizli giriş amacıyla kullanılan gizli bağlantı noktalarıdır. Arka kapılar önceden belirlenen yöntemlerle güvenlik kontrollerinin aşılarak bilgi sistemlerine erişilmesine izin verirler. Sisteme arka kapılar aracılığıyla erişim yapıldığında sistem kayıtlarında o erişimle ilgili kayıtlar yer almamaktadır. Belli bir kullanıcı tarafından çalıştırılınca veya belli giriş değerleri verilince tetiklenen kodlardır. En çok programcılar tarafından test işlemlerini kolaylaştırmak, hataları düzeltmek ve hata durumunda erişime izin vermek için kullanılır. Örneğin programa girişte doldurulması gereken

belli alanlar veya uzun bir kurulum aşaması varsa test işlemlerinde her seferinde aynı işlemleri yapmamak için, hata oluştuğunda programa müdahale izni verilmesi için kullanılabilirler. Ancak arka kapılar, uygulamalarda bırakılınca saldırganlar tarafından keşfedildiğinde tehdit haline gelerek yetkisiz erişim yapılmasına izin verirler. Arka kapılara işletim sisteminin müdahale etmesi zordur. Bunların tehdit haline gelmemeleri için uygulama geliştirilirken ve güncellenirken güvenlik prosedürlerine uyulmalı, uygulama kullanıma açılmadan önce arka kapılardan arındırılmalıdır.

Mantıksal bombalar (Logic Bombs): Daha önceden programlanan koşullar oluştuğunda zarar verecek işlemler yapan zararlı programlardır. Koşullar bir tarih (Şubat ayının 13. günü), günün belli bir saati (21:00), belli bir kullanıcının sisteme girişi, işten çıkarılan bir çalışanın personel listesinden silinmesi gibi durumlar olabilir. Mantıksal bombalar sistem kaynaklarına (bellek, sabit disk, CPU, vb.) büyük zararlar verebilen tespit edilmesi zor programlardır. Bu nedenle fark edildiklerinde genelde sistem hasara uğramıştır ve müdahale için artık çok geçtir. Mantıksal bombanın geri döndürülemez zararlar vermesine örnek 1996 yılında yaşanmıştır. Timothy Allen Lloyd, yüksek teknoloji ürünü, ölçme ve kontrol cihazları üreten Omega Mühendislik şirketinde bilgisayar ağı program tasarımcısı olarak 11 yıl çalıştıktan sonra 10 Haziran 1996'da şirket ile ilişkisi kesilmiştir. Bunun üzerine Lloyd hazırladığı "zaman bombası" yardımı ile Omega şirketinin tüm karmaşık üretim yazılımlarını geri döndürülemez bir şekilde silmiştir. Bu sabotaj sonucunda şirket, satışları ve ileri tarihli anlaşmaları da göz önünde bulundurulduğunda 10 Milyon dolarlık bir kayba uğramıştır. Bu olayın, benzer olaylar arasında yol açtığı zarar en yüksek olan sabotajlardan biri olarak FBI tarafından kayda geçirildiğini belirtmekte fayda vardır. Olay ortaya çıkarıldığında, Lloyd 41 ay hapis ile cezalandırılmıştır [85].

Sazan Avlama (Phishing): İngilizce *Password Harvesting Fishing* sözcüklerinden türetilen Phishing kelimesi Türkçemize sazan avlama olarak çevirilmiştir. Bu yöntemde kredi kartı bilgileri ya da parolalar gibi özel ve gizli kalması gereken mahremiyet gerektiren bilgileri, elde etmek için e-postalar veya sahte web siteleri

hazırlayarak kandırma ve kullanıcıların gizli bilgilerini elde etme için yapılan kandırmaca girişimlerinin tümüne verilen addır [86]. Sazan avlama sosyal boyutları olan elektronik kimlik hırsızlığı (identity theft) olarak da tanımlanmaktadır [87-88]. Sazan avcıları (Phisher), genelde e-posta, web sayfaları ve anlık mesajlaşma (chat) programları gibi çok kullanılan sanal ortam araçları ile eğitimsiz, bilinçsiz ve dikkatsiz (sazan) kullanıcılara ulaşarak onların gizli kimlik bilgilerini (kredi kartı, kullanıcı adı, şifre, vb.) elde etmekte ve bu kullanıcıların banka hesapları boşaltılmaya kişileri yanlış yönlendirmeye kandırmaya veya psikolojisini bozmaya çalışmaktadır.

Genellikle e-postalar yoluyla iletilen bağlantılara tıklanarak web sitelerinde açılan pencereler yoluyla kullanıcılara sunulan sahte web arayüzü ile hem kişisel hem de kurumsal anlamda bilgi hırsızlığı yöntemi olan sazan avlama, elektronik ticaret veya bankacılık uygulamaları için sahte giriş ekranları oluşturularak kişilerin gizli şifre ve mâli bilgilerinin elde edilmesinde kullanılan sazan avlamanın sembolik olarak gösterimi Şekil 2.8'de verilmiştir.

Şekil 2.8. Sazan avlama sembolik gösterimi

1999 yılında Kanada'da yaşanan olay ise, sazan avlama konusunda verilebilecek en iyi örneklerdendir. Kanadalı Alyn Richard Waage ve Kaliforniyalı James Michael Webb isimli sazan avcıları tarafından, Tri-Net Investment Club adıyla tanıtılan www.triwestinvest.com adlı siteden yayın yapan, daha önceden sadece çok zengin

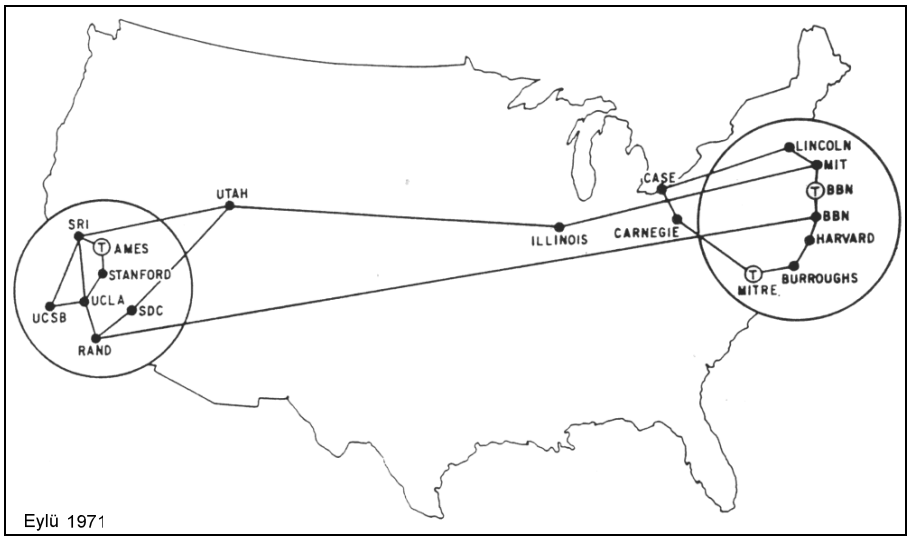
yatırımcılara sunulan, yıllık %120'lik bir kâr payı olan ve para kaybı riski olmayan bir yatırımı anlatan sazan postaları yayarak yatırımcılardan, 1000 dolarlık paketler halinde paralarını yatırmalarını istemişlerdir. Bu siteye paralarını ilk yatıranlara, kâr payı ödemesi altında bir takım ödemeler de yapılmış siteyle daha fazla müşterinin ilgilenmesi sağlanmıştır. 1999–2001 yılları arasında bu site aracılığı ile yatırım yapan 15000 kurbanın paraları ile Mexico ve Kosta Rika'da milyon dolarlık gayrimenkuller, yatlar ve helikopterler satın almışlardır. Dolandırıcılar bunun yanında, dolandırdığı paraların bir kısmını gizlemek için de Kosta Rika'da paravan şirketler kurmuş ve paraların bir kısmını da bu şirketlerden kazanmış gibi göstermişlerdir. Waage, internet üzerinden dolandırıcılık yapmak ve bu yolla yatırımcıları kandırarak 50 Milyon $ toplamaktan suçlu bulunmuş ve toplanan paranın çoğu sahiplerine iade edilmiştir [89].

2.5. Dünyada ve Türkiye'de Bilgi Güvenliği

Dünyada olduğu gibi bilgi güvenliği ülkemizde de gündemde olan bir konudur. Bunun için konuyla ilgili olarak geniş çaplı araştırmalar ve anketler dünyanın ileri gelen güvenlik kuruluşları tarafından düzenli olarak yapılmakta ve yüksek seviyede güvenlik sağlanması için gerekli olan çözümler araştırılmakta ve öneriler sunulmaktadır. Dünyada ve ülkemizde güvenlik tehditlerinin neler olduğu, yol açtığı zararların miktarı, kimleri tehdit ettiği ve buna benzer soruların cevaplarının yer aldığı önemli raporlar dünyada ve Türkiyede bilgi güvenliğinin hangi düzeyde olduğunun gösterilmesi amacıyla bu bölümde incelenmiştir. Dünyadaki bilgi güvenliği durumunun özetlenebilmesi amacıyla Symantec ve FBI Bilgisayar Güvenlik Enstitüsü tarafından, yapılan güvenlikle ilgili güncel araştırma ve anketlerden bu bölümde bahsedilmiştir. Ayrıca tez kapsamında yapılan araştırmalar sonucunda ülke bilgi güvenliğinin hangi düzeyde olduğunun gösterilmesi amacıyla Türkiye genelinde yapılan iki çalışmaya rastlanmıştır. Bu çalışmalardan birincisi 2003, 2004 ve 2005 yıllarında Koç-Net tarafından yapılmış ikinci çalışma ise 2006 yılında kamu kuruluşları için TÜBİTAK tarafından yapılmıştır.

Günümüzde bilgi güvenliği ihlâllerinin büyük bölümünün internet üzerinden yapılan saldırılardan kaynaklanmasından dolayı internet ve bilgi güvenliği arasındaki

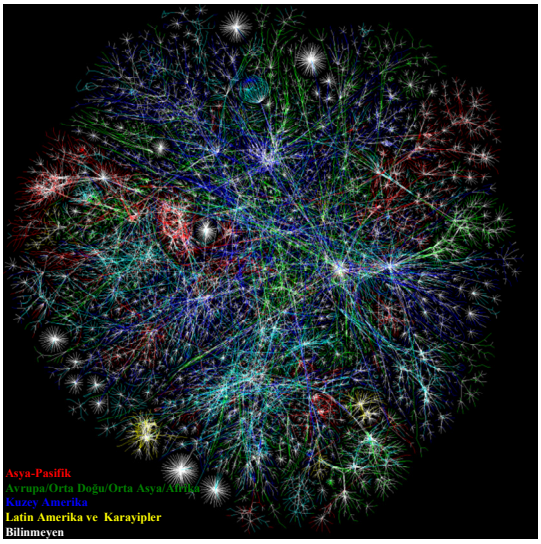
ilişkinin bilinmesinde fayda vardır. Kurulduğu yıllardan günümüze kadar sürekli büyüyerek gelişmekte olan internetin dününün ve bugününün karşılaştırılması büyümenin boyutunun görülmesi açısından önemlidir. Büyümeye paralel olarak güvenlik riskleri ve ihlâlleri artmakta ve doğası gereği güvensiz bir ortam olan internet kendisine bağlı olan kurum kuruluş ve bireyleri üst derecede tehdit etmektedir. İnternetin ilk günkü bağlantıları Şekil 2.9'daki harita üzerinde gösterilmiştir.



Şekil 2.9. 1971 yılı internet (Arpanet) bağlantıları [90]

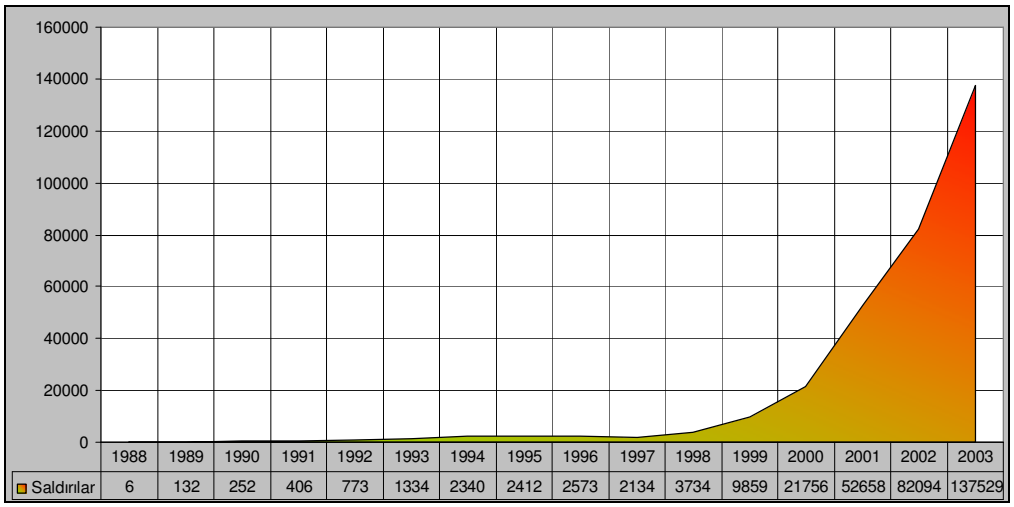
1971 yılında Şekil 2.9'da gösterildiği gibi sadece 18 kurumu bünyesinde barındıran internet her geçen gün hızla büyümekte ve yaygınlaşarak işlevi artmaktadır.İnternetin yaygınlaşmasına ve büyümesine paralel olarak günlük yaşantımızda yaptığımız iş ve işlemlerin bu ortamlara kayması sonucunda güvenlik ihlâllerinin etkileri daha fazla hissedilmektedir. İnternetin bugünkü büyüklüğünü Şekil 2.10'da verilen harita görsel bir şekilde özetlemektedir.

Şekil 2.9 ve Şekil 2.10 kıyaslandığında, internetin baş döndürücü bir hızla büyüdüğü açıkça görülmektedir. İnternetin bu hızda büyümesi ve kullanımının yaygınlaşması, saldırganların iştahını kabartmaktadır. İnternet gelişirken elbette interneti tehdit eden saldırılarda aynı oranda gelişmektedir. İnternet üzerindeki güvenlik olaylarıyla ilgili olarak araştırma yapan önemli kuruluşlar vardır.



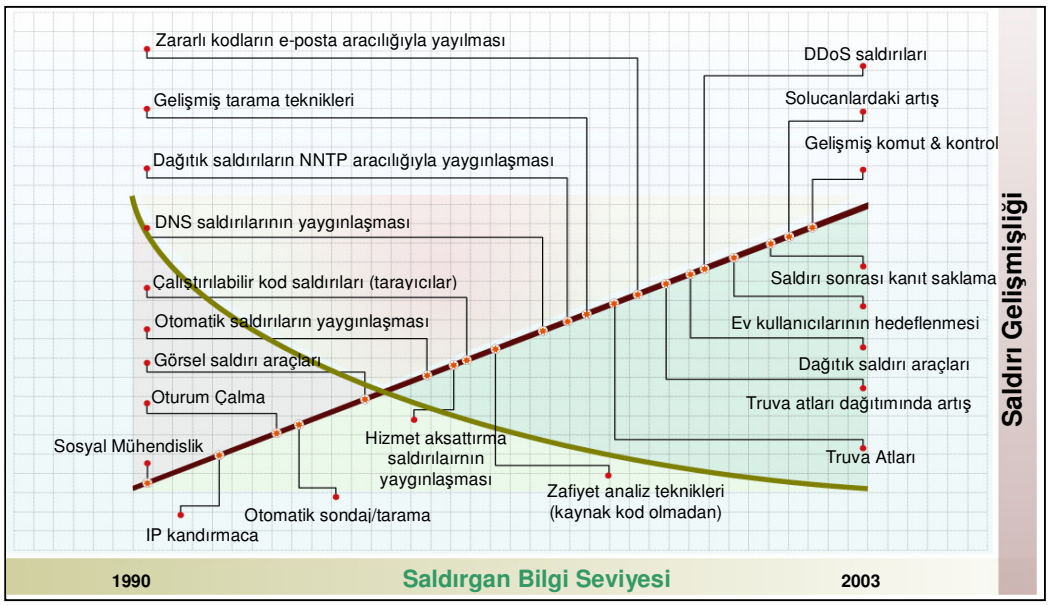
Şekil 2.10. Günümüz internet haritası [91].

Bu kuruluşların başında internet güvenliği konusunda uzman kişilerin çalıştığı Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü bünyesinde yer alan CERT (Carnegie Mellon University's Computer Emergency Response Team) gelmektedir. CERT, internet güvenlik zafiyetleri, ağ sistemlerindeki uzun dönemli değişimlerin incelenmesi, güvenlik konusunda eğitim ve danışmanlık hizmeti veren resmi bir kuruluştur. İnternet üzerinde 1988 yılından 2003 yılına kadar CERT tarafından kaydedilen güvenlik ihlâllerine ait grafik Şekil 2.11'de gösterilmiştir [92].



Şekil 2.11. İnternet güvenlik olaylarının yıllara göre artışı

Şekil 2.11'de gösterildiği gibi saldırıların sayısıda hızla artmaktadır. CERT'in web sitesinde 2003 yılına kadar güvenlik ihlâllerinin izlendiğini ancak otomatik saldırı araçlarının hızla yayılması sonucunda saldırı sayılarının yayınlanmasından vazgeçildiği vurgulanmıştır. CERT saldırı istatistiklerinin yayınlanmamasının başlıca sebebi olarak saldırıların büyük bir kısmının otomatik araçlarla yapılmasından dolayı saldırıların etkisi, kapsamı, saldırganların bilgi seviyesi gibi bilgilerin analizinin doğru yapılamamasını göstermiştir. CERT tarafından vurgulanan otomatik araçların kullanılmasıyla saldırganların saldırı yapabilmek için gerekli olan bilgi seviyesi ihtiyacıda Şekil 2.13'de gösterildiği gibi hızla azalmaktadır. Saldırıların analizi CERT tarafından 2003 yılına kadar yapıldığı için grafik 1990–2003 yılları arasını kapsamaktadır

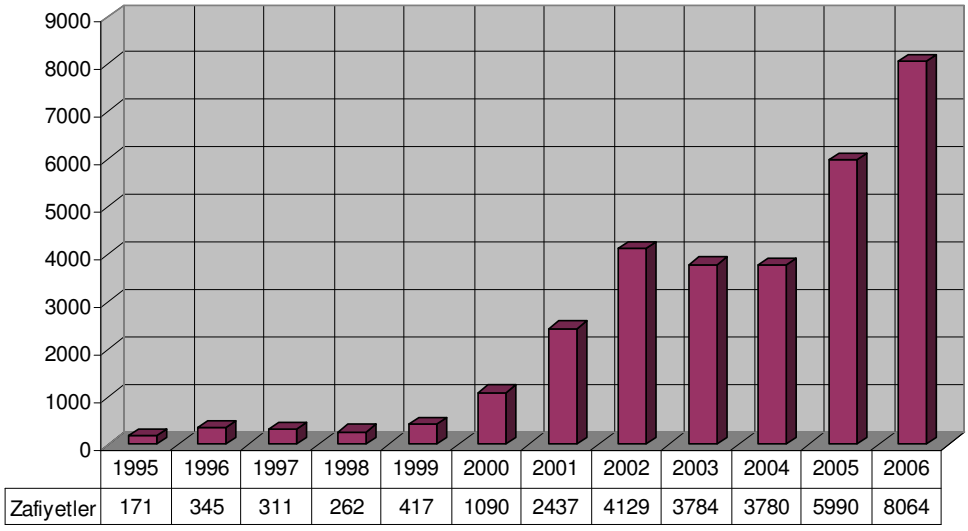


Şekil 2.12. Saldırılar ve saldırganların bilgi seviyesi [93]

Şekil 2.12'de gösterilen durum üzerinden 4 yıl geçmesi ve günümüzde otomatik saldırı araçlarının 4 yıl öncesine oranla çok daha fazla olması tehlikenin 2003 yılından daha fazla olduğunu açıkça ortaya koyması bilgi güvenliği açısından çok düşündürücüdür. Bilgisayar ve internet kullanmasını bilen her kötü niyetli insan bilgi güvenliğini tehdit eden potansiyel bir saldırgan olarak karşımıza çıkabilir. Aslında saldırganlara karşı teknik olarak alınabilecek önlemler zamanla bilgi güvenliğinin

sağlanması için yeterli olmayacaktır. İşte bu noktada devreye caydırıcı ve cezai yaptırımları olan bilgi güvenliği ile ilgili kanunlar girecektir. Bilgi güvenliğiyle ilgili hukuki boyutlar kapsamlı olarak Bölüm 2.6 ve Bölüm 2.7'de anlatılmıştır.

Bilgi güvenliğini ilgilendiren ve saldırılar kadar önemli olan diğer unsur zafiyetlerdir. Zafiyetlerin gidişatına ait istatistikler 1995 ve 2006 yıllarını kapsayacak şekilde CERT'in resmi web sitesinde yayınlanmıştır. Şekil 2.13'de CERT tarafından yayınlanan zafiyet artışlarına ilişkin istatistikler gösterilmektedir.



	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006
Zafiyetler	171	345	311	262	417	1090	2437	4129	3784	3780	5990	8064

Şekil 2.13. Zafiyet sayılarının yıllara göre dağılımı

Bilgi güvenliği tehditlerinin artmasında doğrudan etkili olan internet kullanımıyla ilgili yapılan ve 11 Ocak 2007 tarihli kullanıcı sayısına göre sıralı istatistikler Çizelge 2.2'de gösterilmiştir. Çizelge 2.2'de belirtildiği gibi Türkiye internet kullanımı konusunda dünya ortalamasının üzerinde bulunması ülkemiz açısından önemli bir gelişme olup tek başına yeterli değildir. İnternet kullanımının standartların üzerinde olduğu ülkemizde internet kullanan kurum, kuruluş ve bireylerin güvenliğinin sağlanması gerekmektedir.

Önümüzdeki yıllarda internet kullanımın daha da artacağı düşünülürse bilgi güvenliği ihlâlleri de internet kullanımıyla doğru orantılı artacağından alınması gereken önlemlerin daha da önem kazanacağı değerlendirilmektedir.

Çizelge 2.2. İnternet kullanım oranları [94]

	Ülkeler	Kullanıcı Sayısı	Nüfus	Kullanım (%)
1	A.B.D.	210 080 067	301 967 681	69,6
2	Çin	132 000 000	1 317 431 495	10,0
3	Japonya	86 300 000	128 646 345	67,1
4	Almanya	50 616 207	82 509 367	61,3
5	Hindistan	40 000 000	1 129 667 528	3,5
6	İngiltere	37 600 000	60 363 602	62,3
7	Güney Kore	33 900 000	51 300 989	66,1
8	Fransa	30 837 592	61 350 009	50,3
9	İtalya	30 763 848	59 546 696	51,7
10	Brezilya	25 900 000	186 771 161	13,9
11	Rusya	23 700 000	143 406 042	16,5
12	Kanada	21 900 000	32 440 970	67,5
13	Meksika	20 200 000	106 457 446	19,0
14	İspanya	19 204 771	45 003 663	42,7
15	Endonezya	18 000 000	224 481 720	8,0
16	Türkiye	16 000 000	75 863 600	21,1
17	Avustralya	14 729 209	20 984 595	70,2
18	Vietnam	14 509 075	85 031 436	17,1
19	Tayvan	13 800 000	23 001 442	60,0
20	Arjantin	13 000 000	38 237 770	34,0
	Toplam	1 022 863 307	6 499 697 060	16,6

Symantec firması bilgi güvenliğinin sağlanması konusunda dünyanın önde gelen güvenlik firmalarından biridir. Symantec firması tarafından 2002 yılından itibaren hazırlanan ve altı aylık periyotlarla yayınlanan internet güvenlik tehdit raporu dünyada meydana gelen güvenlik olaylarının değerlendirilerek analizinin yapıldığı, internet üzerinden yapılan saldırılar, zafiyetler, kötücül kodlar, mesaj sağanağı, güvenlik riskleri ve gelecekte öngörülen tahminlerin yer aldığı güvenlik dünyasında itibar gören bir çalışmadır. Bilgi güvenliğinin dünyadaki genel durumunu göstermek amacıyla, Symantec tarafından 2007 yılı Mart ayında yayınlanan 11. Internet Güvenliği Tehdit Raporu'na göre, günümüzün internet tehdit ortamında, finansal kazanç elde etme amacına yönelik olarak gizli bilgileri elde etme amaçlı zararlı kodların hazırlanması, veri sızdırma ve veri hırsızlığı gibi alanlarda büyük artış yaşanmıştır. Sanal ortamda bir yanda küresel ve işbirlikçi ağlar oluşturmuş suç teşkil eden aktiviteler hızla artırmaya devam ederken, diğer yanda siber suçlular "fark edilmemek" için saldırı metotlarını her geçen gün daha da geliştirmişlerdir.

11. Symantec internet güvenliği raporunun temel bulguları aşağıda maddeler halinde açıklanmıştır [95].

- Dünya genelinde bot-enfekte bilgisayar sayısı bir önceki döneme göre %29 luk bir artışla 6 milyonun üzerine yükselmiştir.
- Truva atları, bir önceki döneme göre %23 lük bir artışla en tehlikeli ilk 50 kötücül kodun %45 ini oluşturmuştur.
- Kurum, kuruluş ve bireylerin bilinmeyen tehditlere ilişkin savunmasızlığını arttığını gösteren sıfır gün açıkları, bir önceki döneme göre %23 lük artışla 12 'ye yükselmiştir.
- Yeraltı ekonomisine ait sunucular, suçlular ve suç örgütleri tarafından, e-posta adres listeleri, kullanıcı hesapları, kişisel şifreler (PIN), banka ve kredi kartları ve resmi kimlik numaraları da dâhil olmak üzere çalınan bilgileri satmak amacıyla organize bir şekilde kullanılmaktadır.
- Kimlik hırsızlıklarına ilişkin veri kayıplarının %54'ünü taşınabilir bellek ünitelerinin kaybedilmesi veya çalınması oluşturmuştur.
- İlk defa, ülkelerin kendi ağlarından kaynaklanan kötü niyetli aktivitelerin hacmine göre sıralama yapılmıştır. Bu sıralamada; Amerika zararlı aktivitelerin yoğunluğu açısından %31 ile en yüksek orana sahip bulunan ülke olarak ilk sırayı, onu % 10 ile Çin ve %7 ile Almanya izlemiştir.
- Siber suçluların verdiği zararlar artmış, saldırı yöntemleri gelişmeye devam etmiş ve fark edilmelerini önleyecek daha ileri ve karmaşık yöntemlere başvurmuşlardır.
- Kişisel gizli bilgilere yönelik tehditler artmıştır. Kişilere ait kimlik bilgileri 14-16 gibi rakamlara satılmaktadır. Çalınan bilgiler yoğunlukla yeraltı ekonomisine ait sunucular üzerinde satılmıştır. Söz konusu sunucular, yoğunlukla saldırganlar ve suç şebekeleri tarafından çalınan bilgilerin satılması işlemlerinde kullanılmıştır. Satılan bilgiler arasında sosyal güvenlik numaraları, kredi kartları, kişisel kimlik bilgileri, e-posta adresleri yer almıştır. 2006 yılının son altı aylık döneminde dünyada bilinen yeraltı ekonomisine ait sunucuların %51'i Amerika Birleşik Devletlerinde bulunmaktadır.
- Symantec son raporlama döneminde, artan Truva atı ve bot ağlarının daha çok kişisel gizliliğe sahip bilgilerin çalınmasında kullanıldığını tespit etmiştir.

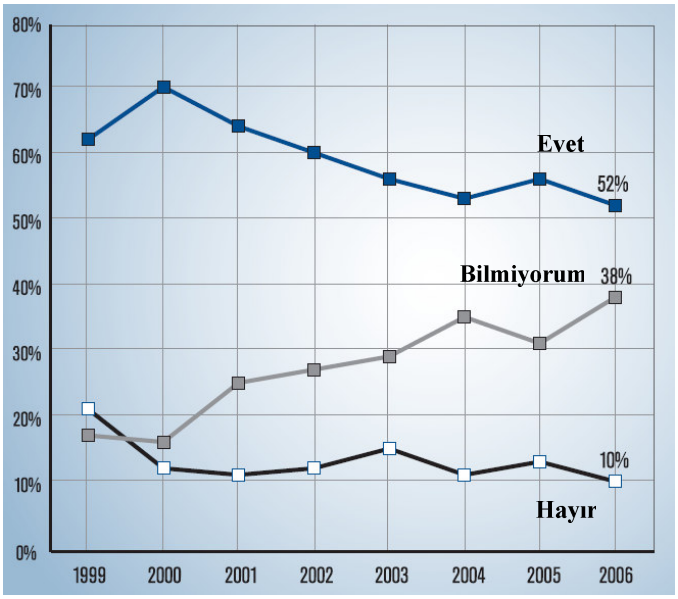
Symantec'e rapor edilen en tehlikeli 50 kötü niyetli kodun %66 sı bu tür gizli bilgilerin ele geçirilmesine yönelik olarak hazırlanmıştır. Bu oran bir önceki döneme göre %48 oranında bir artış göstermiştir. 2006 yılının 2.yarısında ad, soyadı, şifre gibi kullanıcı verilerini bilgisayarlardan çalmaya yönelik tehditler gizli bilgilerin çalınmasına yönelik tehditlerin %62'sini oluşturmuş, yılın ilk yarısına göre %38 lik bir artış göstermiştir

- 2006 yılının 2.yarısında saldırgan aktivitesi, donanım çalınması ya da kaybolması, güvenlik politikalarının ihlali gibi nedenlerle yaşanan veri erişim ihlalleri ve bunun sonucunda elde edilen gizli bilgilerin kimlik hırsızlığında kullanılma potansiyeli %25 lik oranla en fazla kamu sektörünü etkilemiştir.
- Saldırganlar spam e-postaları, kötü niyetli kodları ve sazan avlama hilelerini bir araya getirerek koordine eden çok sayıda atak düzenlemiştir. Spam e-postalar izlenen e-posta trafiğinin %59'luk bölümünü temsil ederken, finans endüstrisine yönelik spam e-postalar ise toplam spam e-postaların %30'luk bölümünü oluşturmuştur.
- 2006 yılının son altı aylık döneminde bir önceki döneme göre %6'lık bir artışla 166248 adet tekil sazan avlama postası saptanmıştır. Bu rapor döneminde ilk kez haftanın günleri, mevsimsel hareketler açısından sazan avlama atakları incelenmiş hafta içi günlerde ortalama 961 sazan avlayan postayla karşılaşılırken, hafta sonlarında bu oran yaklaşık %27'lik bir azalma göstermesi saldırganların kurumsal e-posta gönderimini taklit etme girişimlerini ortaya koymuştur.
- Raporda Türkiye'ye ilişkin ek bilgilerde yer almıştır. Türkiye, en fazla saldırıda bulunan ülkelere ilişkin dünya sıralamasında 17. sırada yer almış sadece Orta Doğu ve Afrika bölgeleri açısından bakıldığında ise 1. sırada yer aldığı tespit edilmiştir.
- Tehlikeli aktiviteler açısından gözlemlendiğinde ise Türkiye, EMEA (Avrupa, Orta Doğu,Afrika) bölgesinde 8. sırada bulunurken, spam zombileri açısından ise dünya sıralamasında 10., EMEA bölgesinde ise 6. sırada yer almıştır.
- Spam yoğunluğu açısından şehirlere göre yapılan sıralandırmada ise Ankara EMEA Bölgesinde 4. sırada yer almıştır.
- Sazan avlama yoğunluğu açısından en yoğun ülkeler sıralamasında Türkiye, dünya genelinde 29. sırada yer alırken, tüm e-postalara göre spam yüzdesi Türkiye için %79,03 olarak belirtilmiştir.

- Bot-enfekte olmuş bilgisayarlar açısından bakıldığında ise Türkiye, dünya sıralamasında 15. sırada, EMEA bölgesini kapsayan sıralamada 8. sırayı almıştır.
- Bot-enfekte olmuş bilgisayarlar açısından yapılan şehir sıralamasında Ankara 4. sırada yer almıştır.
- Internet kullanıcısı başına en çok tehlikeli aktivite gözlenen ülkeler sıralamasında Türkiye, dünya genelinde 20., DoS ataklarınca en çok hedeflenen ülkeler sıralamasında ise dünya genelinde 34. sırada yer almıştır.
- Türkiye, Spam açısından en yoğun ülkeler sıralamasında ise İsrail'den sonra 20. sırada yer almıştır

Dünya genelinde güvenlik dünyasında itibar gören diğer bir çalışma 11 yıldır periyodik olarak FBI (Federal Bureau of Investigation) Bilgisayar Güvenlik Enstitüsü (The Computer Security Institute -CSI) tarafından yapılmaktadır. Bu çalışmanın içeriğinde bilgisayar suçları ve güvenlik konuları hakkında yapılan anketler yer almaktadır. 2006 yılında yapılan araştırmaya üniversiteler, sağlık sektörü, finansal kurumlar, devlet kuruluşlarından çok sayıda kurum katılmıştır. Tez çalışmasını ilgilendiren bilgisayar sistemlerinin yetkisiz kullanımı, güvenlik ihlâlleri, tespit edilen saldırıların tipleri, saldırılar karşısında alınan önlemler gibi konularda yapılan araştırma sonuçlarından bu bölümde bahsedilmiştir [96].

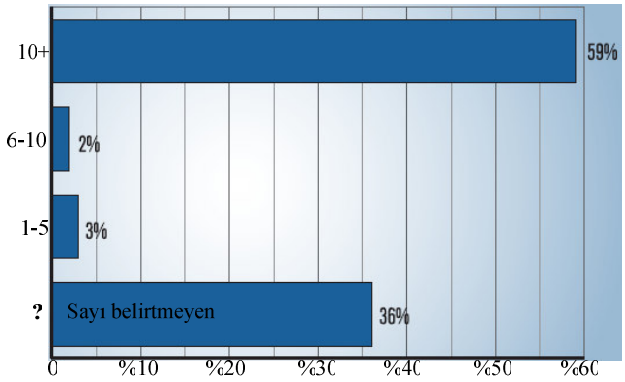
Yapılan araştırmaya göre 2000 yılından süre gelen başarılı yetkisiz kullanımların azalması yönündeki gidişat 2005 yılında yükselmiş ancak 2006 yılında saldırılar yeniden azalmaya başlamıştır. 2004 yılında bilgisayarların yetkisiz kullanım oranı %53 olurken, 2005 yılında ise bu oran %56'ya yükselmiş, 2006 yılında bu oran %52'ye gerilemiştir. Yetkisiz erişim konusunda bilgisi olmayan kurum sayısının oranı 2004 yılında %35 olurken 2005 yılında bu oran %31'e gerilemiş, 2006 yılında tekrar yükselişe geçerek bu oran %38 olmuştur. Yetkisiz kullanımın olmadığını belirten kurum sayısının oranı 2004 yılında %11'iken 2005 yılında oran %13'e yükselmiş, 2006 yılında düşüşe geçerek %10 oranına gerilemiştir. Yetkisiz kullanımlarla ilgili araştırmaya ait grafiksel gösterim Şekil 2.14'te gösterilmiştir.



Şekil 2.14. 2006 yılında bilgisayar sistemlerinin yetkisiz kullanımı [96]

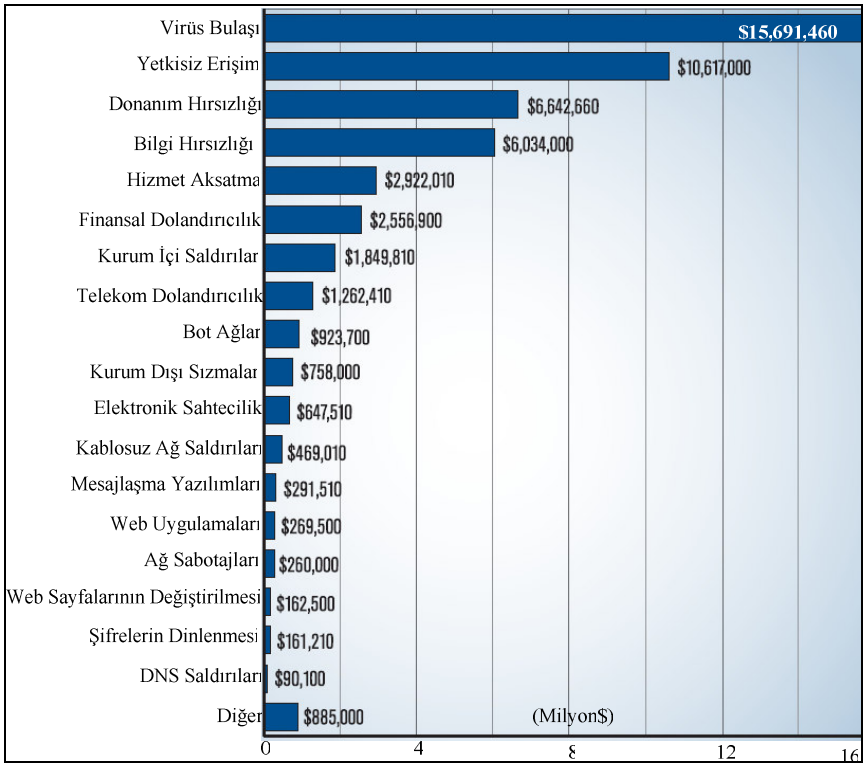
2006 yılının en göze çarpan sonuçlarından biri web uygulamalarında meydana gelen güvenlik ihlâllerindeki artışlardır. 2004 yılında yapılan araştırmalara göre kurumların %89'u 1 ile 5 arasında güvenlik ihlâlleriyle karşılaşırken yalnızca %5'lik kısmı 10'dan fazla web uygulamalarında güvenlik ihlâliyle karşılaştığını belirtmiştir. 2005 yılında rakamlar tersine dönmüş kurumlarının %95'i 10'dan fazla güvenlik ihlâli yaşarken %3'ü 6 ile 10 arasında, %2'si ise 1 ile 5 arasında güvenlik ihlâlleri yaşadığını beyan etmiştir. 2006 yılında saldırılarda azalma görülmüş 10'dan fazla ihlâl yaşayan kurumların sayısı %59, 6–10 arasında ihlâl yaşayan kurum sayısı %2, 1–5 arasında ihlâl yaşayan %3 olurken sayı belirtemeyen kurum sayısı ise %36 gibi yüksek bir oran olmuştur. Web uygulamalarında güvenlik ihlâli yaşayan kurumlara ait grafiksel gösterim Şekil 2.15'te gösterilmiştir.

Güvenlik ihlâllerinin mali boyutunun ortaya çıkartılması için yapılan araştırmadaki değerler oldukça yüksek çıkmıştır. 2006 yılında güvenlik ihlallerinden kaynaklanan kayıplarla ilgili ankete 313 kuruluş katılmıştır. 2006 yılında güvenlik ihlâllerinden kaynaklanan toplam kayıp 52 494 290 milyon dolar olmuştur. Geçen yıllarda olduğu gibi en yüksek kayıplara virüsler ve yetkisiz erişimlerden kaynaklanan güvenlik ihlâlleri sebep olmuştur.



Şekil 2.15. Web uygulamalarında meydana gelen güvenlik ihlalleri [96]

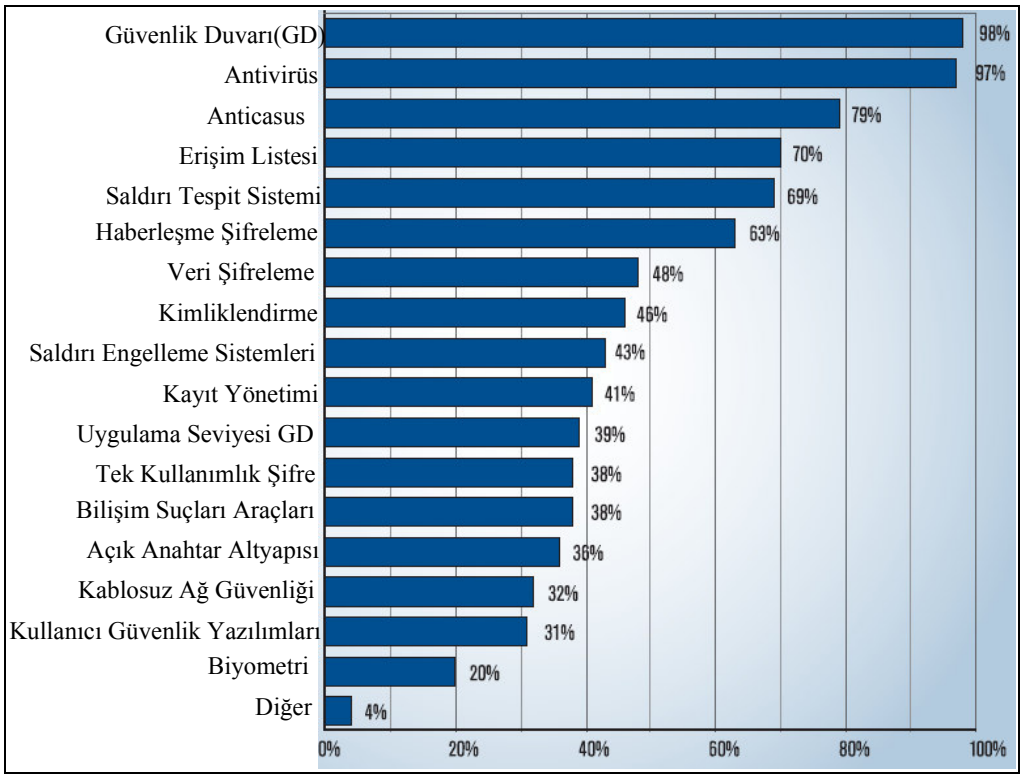
2005 yılında aynı ankete 639 kuruluş katılmış meydana gelen kayıpları yaklaşık 130 milyon dolar olmuş ve 2004 yılına göre kuruluş başına düşen maddi kayıp ortalama olarak %61 oranında azalmıştır.



Şekil 2.16. Güvenlik ihlallerinden kaynaklanan kayıplar [96]

Ankete katılan kurumların bilgi güvenliğinin sağlanmasında kullandıkları çözümler araştırılmıştır. 2006 yılında ortaya çıkan sonuçlar 2005 yılında yapılan anket

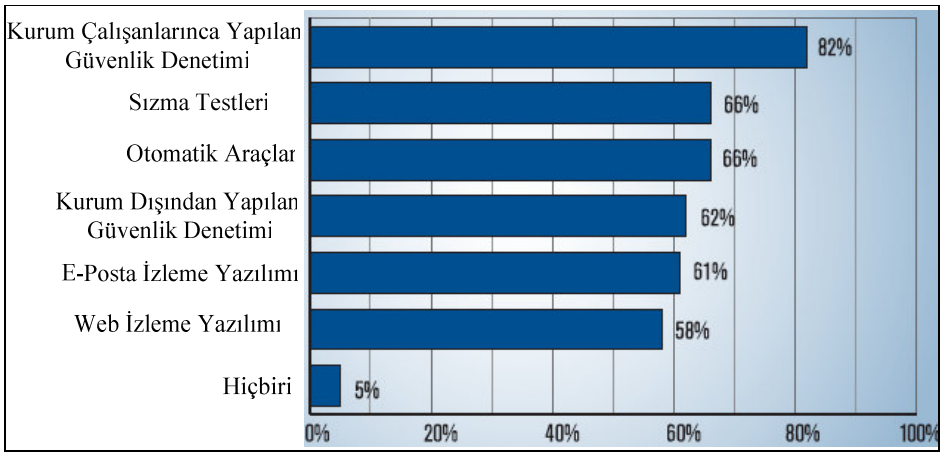
sonuçlarıyla benzerlikler göstermektedir. 2006 yılında güvenlik duvarı kullanımı %98, antivirüs kullanımı %97, saldırı tespit sistemlerinin kullanımı %69 olurken 2005 yılının sonuçlarına göre güvenlik duvarı kullanımı %97, antivirüs kullanımı %96, saldırı tespit sistemlerinin kullanımı %72, erişim kontrol listelerinin kullanımı %70 olarak tespit edilmiştir. 2006 yılında araştırmaya katılan 616 kurumun kullandığı güvenlik yazılımlarına ait grafik Şekil 2.17'de gösterilmiştir.



Şekil 2.17. Kullanılan güvenlik çözümleri [96]

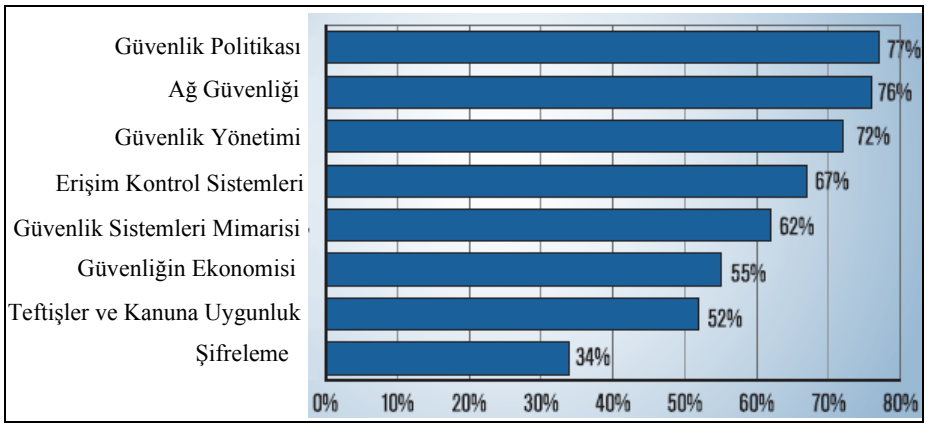
Bilgi güvenliğinin sınanması ve etkinliğinin değerlendirilmesi için kendi imkânlarıyla güvenlik denetimi yapan kurumların oranı 2005 yılında %87 iken 2006 yılında bu oran %82'ye düşmüştür. Bu tez çalışmasının konusu olan sızma testleri %66 oranıyla ikinci, otomatik araçların kullanımı %66, dışarıdan bilgi güvenliği uzmanlarınca yapılan denetimler %62, e-postaların izlenmesi %61, web aktivitelerinin izlenmesi %58 olarak tespit edilmiştir. Bu soruyu cevaplayan 597 kurumun %5'ise hiçbir yöntem kullanmadığını belirtmiştir. Bilgi güvenliğinin

etkinliğinin değerlendirilmesine yönelik kuruluşların vermiş olduğu cevaplara ait grafik Şekil 2.18'de gösterilmiştir.



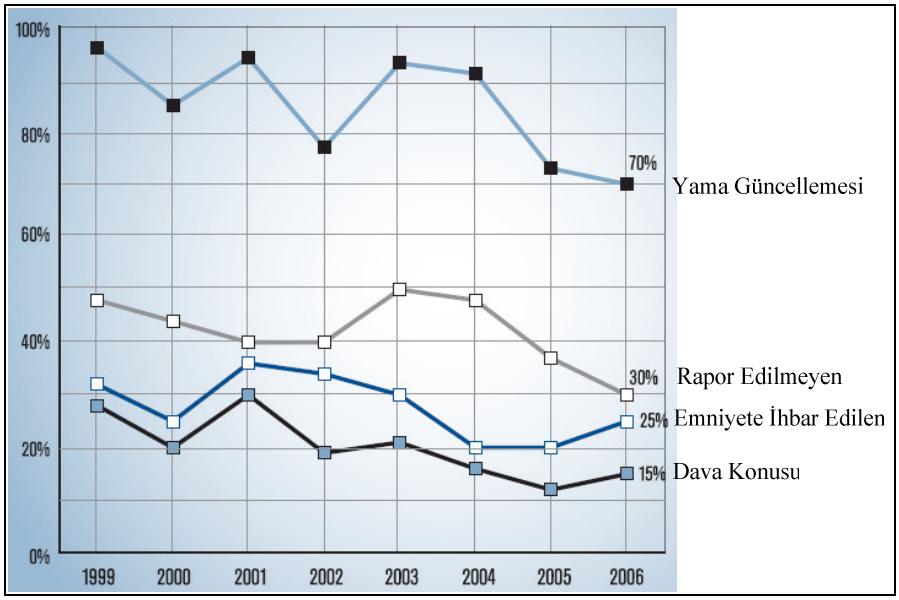
Şekil 2.18. Bilgi güvenliği etkinliğinin değerlendirilmesi [96]

Güvenlik, farkındalık eğitimlerinin önemli olduğu güvenlik alanlarının neler olduğuna dair yönetilen soruyu 599 kurum cevaplamıştır. Kurumlara seçmesi için sekiz farklı alan listelenmiş ve kurumların bu alanları önem sırasına göre listelemeleri istenmiştir. Güvenlik eğitimlerinin önemli olduğu ilk üç alan %77 ile güvenlik politikası, %76 ile ağ güvenliği, %72 ile güvenlik yönetimi olarak sıralanmıştır. Güvenlik eğitimlerinin önem sırasına göre listelendiği grafik Şekil 2.19'da gösterilmiştir.



Şekil 2.19. Güvenlik eğitimlerinin sıralanması [96]

Araştırmaya katılan kurumlara saldırı sonrasında neler yaptıkları sorulmuş ve soruya cevap veren 385 katılımcının %70'i saldırıyı takiben güvenlik yamalarını geçtiklerini belirtmişlerdir. Yamalara bağlı güvenlik ihlâllerinin 2003 yılından beri düşüşte olmasının sebebi yamaların otomatik olarak geçilebilmesi için geliştirilen yazılımlardır. En büyük düşüş ise 2004 yılından 2005 yılında geçerken olmuş ve oran %91'den %73'e gerilemiştir. Katılımcıların %30'u güvenlik ihlâlleriyle ilgili bilgileri paylaşmadıklarını belirtirken, saldırı sonrasında saldırıyı emniyete ihbar edenlerin oranı %25, avukatlar aracılığıyla dava açanların oranı ise %15 olarak tespit edilmiştir. Güvenlik ihlâlleri sonrasında katılımcıların yapmış olduğu hareketlere ait grafik Şekil 2.20'de gösterilmiştir.

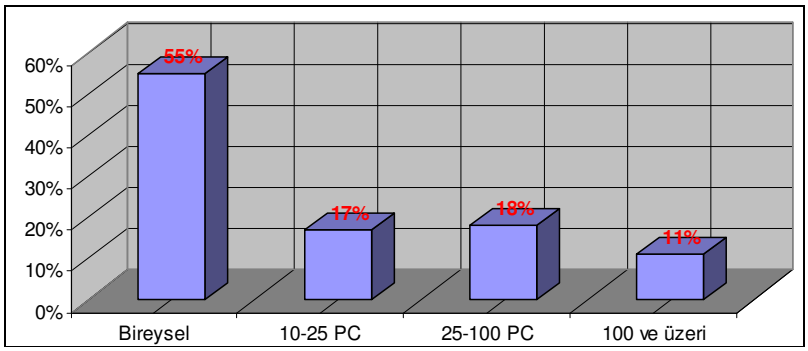


Şekil 2.20. Güvenlik ihlâli sonrası yapılan hareketler [96]

Ülkemizde güvenlikle ilgili özel sektör veya kamu kurumları tarafından yapılan araştırmalar yetersiz kalmaktadır. Son yıllarda yapılan araştırmaların sayısı yetersiz olsa da yapılmaya başlanmıştır. Türkiye'de güvenlik bilincinin oluşturulması ve bu konuya dikkat çekilmesi amacıyla bu tür çalışmaların artarak geniş katılımlarla yapılması gerekmektedir. Koç.net firması tarafından 2003, 2004 ve 2005 yılında yapılan ülkemizde güvenlik alanındaki ilk geniş kapsamlı çalışma özelliği taşıyan Türkiye internet güvenliği raporundan ülkemizdeki bilgi güvenliğinin

değerlendirilmesi amacıyla bahsedilecektir [97]. Bu çalışmalarda, özel sektörden kamuya, üniversitelerden belediyelere kadar her kuruluşun güvenli bir ortamda iş yapmaları amacıyla yaşanan güvenlik tehditlerini, eksiklerini ve sistemlerine yapılan saldırı türlerinin belirlenmesi amaçlanmıştır.

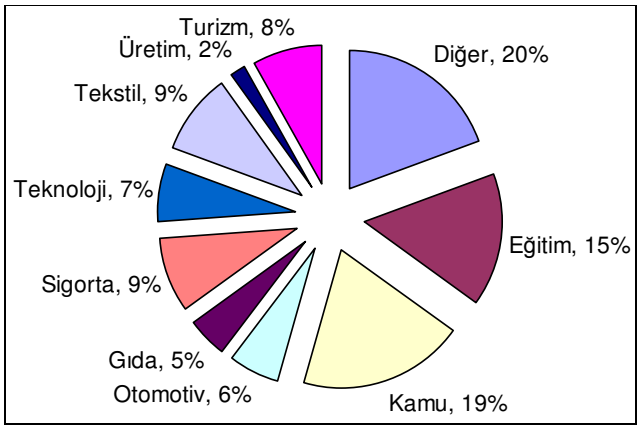
Koç.net, firması tarafından web üzerinden çevrimiçi güvenlik denetimi sistemi olan Rizikometre ile 2004 yılında yapılan denetlemeye 800 civarında ADSL abonesi ve 500'ün üzerinde şirket, 2005 yılında yapılan denetlemeye ise 1025 ADSL abonesi ve 850 şirket katılmıştır. 2005 yılındaki denetlenen katılımcı profili %55'i bireysel ADSL kullanıcıları, şirket kullanıcıları %17'si 10–25, %18'i 25–100, %11'i 100+ kişisel bilgisayara sahip olan kuruluşlardır. Katılımcı kitlesinin dağılımı Şekil 2.21'de gösterilmiştir.



Şekil 2.21. Katılımcı profili

Güvenlik açıklarının sektörel bazlı dağılımına göre en yüksek güvenlik açıkları %19 oranı ile kamu, %15 oranı ile eğitim %9 oranı ile tekstil ve sigorta sektörlerinde tespit edilmiştir. Eğitim sektörünün büyük oranda devlet okulları olduğu göz önüne alınırsa güvenlik açıklarına sahip olan en yüksek sektörün kamu kurumları olduğu görülür. Kamu kurumlarında açık oranlarının yüksek çıkması güvenlik yamalarının takip edilmemesi, yeterli yatırım ve yetişmiş personelin olmaması, güvenlik programlarının hatalı yapılandırmasından kaynaklanmaktadır. Kamuda elektronik dönüşümün her gün konuşulduğu ve bu kapsamda çok sayıda projelerin yapıldığı kamu sektöründe bilgi güvenliği konusuna yeteri kadar önem verilmediği

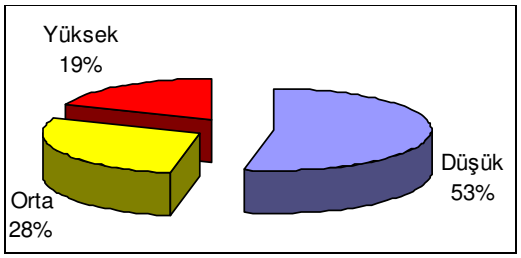
görülmektedir. 2005 yılında yapılan güvenlik açıklarının sektörel bazlı dağılımı (ADSL hariç) Şekil 2.22'de gösterilmektedir.



Şekil 2.22. 2005 yılı güvenlik açıklarının sektörel dağılımları

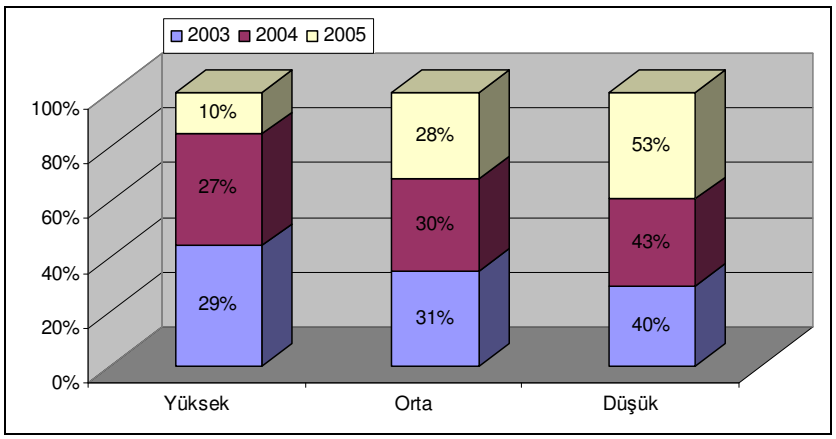
Güvenlik açıklarının giderilmesinde güvenlik yamalarının güncellenmesi, bilgi sistemlerinin güvenli bir şekilde tasarlanması, sistem güvenlik yapılandırmalarının hatasız yapılması, risk analizi yönetimini gerçekleştirilmesi, güvenlik bilinçlendirme eğitimlerinin verilmesi çözüm olarak sunulmuştur. Sistemlerdeki güvenlik açıklarına dair oranları Şekil 2.23'de gösterilmiştir. Açıklıklar kendi arasında düşük, orta ve yüksek olmak üzere üç sınıfa ayrılmıştır. Yüksek ve orta seviyedeki açıklar gizli bilgilerin çalınması, değiştirilmesi, sunucuların hizmet veremez hale gelmesi, web sitelerinin değiştirilmesi, şifrelerin ele geçirilmesine neden olmaktadır.

Yüksek seviyedeki açıkların oranı 2003 yılında %29, 2004 yılında % 27 olarak tespit edilmiştir. 2005 yılı açıklarıyla 2004 ve 2003 yılına ait açıklar karşılaştırıldığında yüksek seviyeli açıkların düşmeye devam ettiği görülmüştür.



Şekil 2.23. 2005 yılı güvenlik açıklarının dağılımları

Yüksek seviyeli güvenlik açıklarının çoğunluğu ADSL bağlantılarında görülmüştür. ADSL bağlantılarındaki güvenlik açıkları solucanların çok daha hızlı yayılma özelliği göstermesine neden olmaktadır. Tüm sistemler için ciddi risk yaratan solucanlar, virüsler ve saldırganlar, ADSL kullanıcılarının korumasız bağlantıları üzerinden daha geniş kitlelerin sistemlerini tehdit etmektedir. ADSL'nin hız ve fiyat avantajından dolayı kullanıcıların güvenlik önlemlerini yeterince araştırmadan internete bağlanması, internet bağlantısındaki yüksek riskin önemli nedenlerdendir. Türkiye'de bu araştırmanın yapıldığı 2004 yılsonu itibariyle 450 bin olan ADSL kullanıcı sayısının hızlı bir ivme ile artarak 2005 yılı sonunda 1,5 milyona, 5 Haziran 2006 yılında 2 milyona ulaştığı ADSL kullanıcı sayısı 2006 yılsonunda 3 milyona ulaşmıştır. Açıkların senelere göre dağılımı Şekil 2.24'te gösterilmiştir.



Şekil 2.24. Güvenlik açıklarının yıllara göre dağılımları

Yüksek seviyeli açıkların dağılımına bakıldığında iyileşme görülmektedir. Ancak orta seviyedeki açıkların aynı kalması, düşük seviyedeki açıkların artış göstermesi hala kuruluşların ciddi riskler taşıdığı anlamına gelmektedir.

Yapılan inceleme ile kritik web sunucu açıklarında son üç sene içinde ciddi bir iyileşme olmadığı görülmektedir. DNS sunucu açıklarıyla ilgili ise 2003–2004 arasında ciddi bir iyileşme gözlenmiş olsada 2005 denetiminde iyileşme ivmesinin azaldığı ortaya çıkmaktadır. Uzaktan yönetim uygulamaları, ftp ve e-posta sunucularında da benzer şekilde var olan açık yüzdeleri iyi yönde düzelme göstermemiştir. Sadece dosya sunucu açıkları %85'ten %45'e inerek olumlu bir

gelişme kaydetmiştir. Araştırmaya katılan kurumların %43'ünün güvenlik açığı olan sürümler kullandığı tespit edilmiştir. Bu açıklar sayesinde web sunucu bilgilerinin kolaylıkla çalınabileceği, ana sayfalarının değiştirilebileceği veya bir başka adrese yönlendirilebileceği tespit edilmiştir.

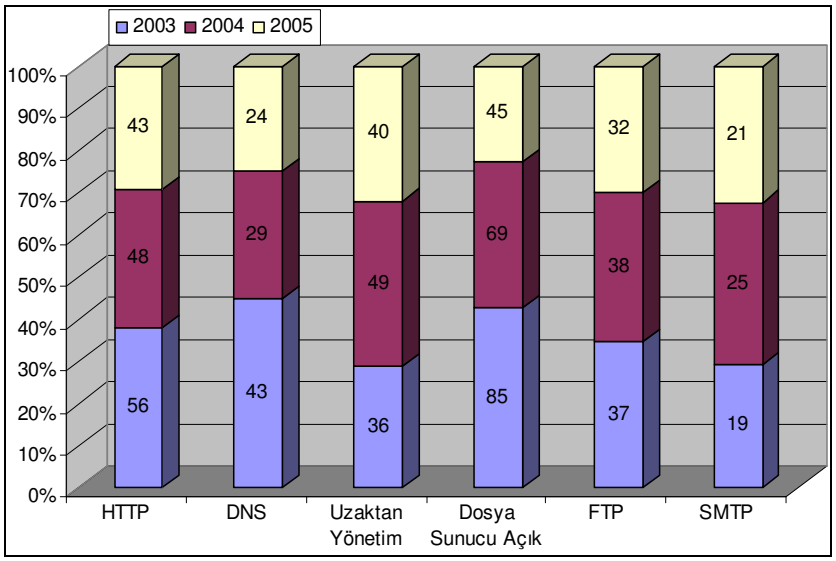
Alan adı sunucusu açıkları 2003 yılında %43, 2004 yılında %29, 2005 yılında ise %24 olarak tespit edilmiştir. 2003 yılından 2005 yılına doğru açıklarda azalma olsa bile alan adı sunucusu olarak hizmet veren bilgisayarların dörtte birinde güvenlik açığı olması yüksek bir orandır. Alan adı çözmek için kullanılan DNS (Domain Name System) sunucularındaki açıkları, şirket e-postalarının ele geçirilmesi, çalışanların internet üzerinden eriştiği bankacılık işlemlerinde kullandıkları şifrelerin çalınması, web sayfalarının başka adreslere yönlendirilmesi gibi güvenlik ihlâllerinin yaşanmasına sebep olabilir.

Sistemlerin yönetiminde esneklik sağlaması açısından internet üzerinden erişilmek üzere açık bırakılan bazı servisler büyük riskler yaratmaktadır. Bu servisleri kullanmak için gerekli olan kullanıcı adı ve şifreler ele geçirildiğinde, sistemlere yönetici hakkıyla erişim yapılabilmektedir. Sistem yönetimi için açık bırakılan servislerden kaynaklanan güvenlik açıkları, 2003 yılında %36, 2004 yılında %49, 2005 yılında %40 olmuştur.

Dosya transferi yapılmasını sağlayan FTP (File Transfer Protocol) sunucularının kimliklendirme ve yetkilendirme mekanizmaları olmadan internete açılmamalıdır. FTP sunucularının 2005 yılında %32'sinde güvenlik açıkları tespit edilmiştir. E-posta (SMTP) atılmasını sağlayan sunucu bilgisayarlar üzerinde 2005 yılında %21 oranında ciddi açıklar bulunmuştur. Bu açıklar sayesinde kurum e-postalarının yetkisiz insanlar tarafından okunabilmesi, çöp postaların atılması gibi güvenlik ihlâlleri yaşanabilir. Özellikle spammer adı verilen kişiler tarafından bu açıkların kullanılarak spam postaların atılması sonucu e-posta sunucuları spam atan bilgisayar olarak kara listeye girebilir. Şekil 2.25'de servislere göre açıklıklar gösterilmiştir.

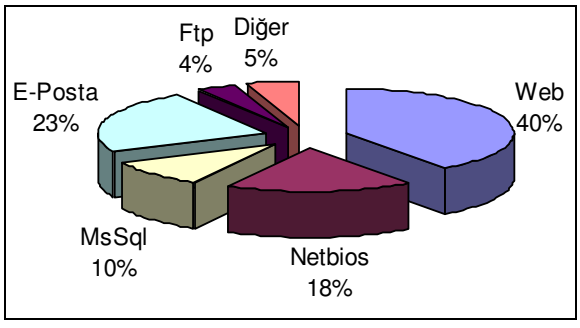
Koç.net firması tarafından yönetilen atak tespit sistemlerinin 2004 yılına ait aylık istatistikleri incelendiğinde, en çok atağın yüzde 45 oranıyla Microsoft TCP 445

portuna yapıldığı tespit edilmiştir. İkinci sırada ise yüzde 37 oranıyla web servislerine yapılmaktadır. 2005 yılında en çok saldırıya uğrayan servisin %40 oranıyla web olduğu tespit edilmiştir.



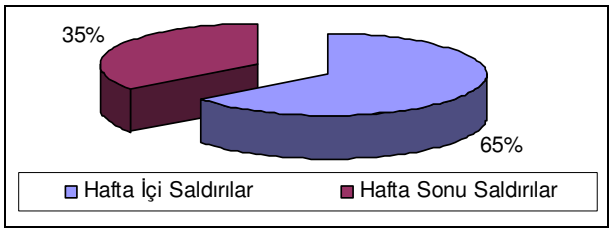
Şekil 2.25. Servislere göre açıklıklar

İkinci sırada %23 oranıyla e-posta tabanlı saldırıların aldığı görülmektedir. Bu durum elektronik sahtecilik ve spam postaların artmasına yorumlanabilir. Solucan bulaşlarının sebep olduğu Netbios %18 olarak dördüncü sırada yer almaktadır. En çok saldırıya uğrayan servisler Şekil 2.26'da gösterilmiştir.



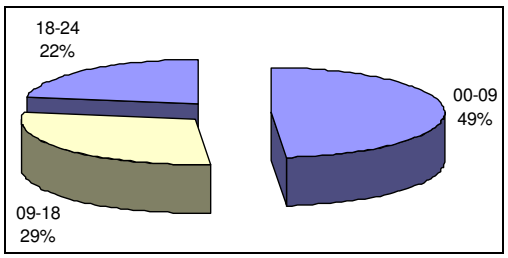
Şekil 2.26. En çok saldırıya uğrayan servisler

Şekil 2.27'de gösterildiği gibi, saldırıların yüzde 35'i çalışanların olmadığı hafta sonlarında yapılırken hafta içinde yapılan saldırıların oranı ise yüzde 65 olarak tespit edilmiştir.



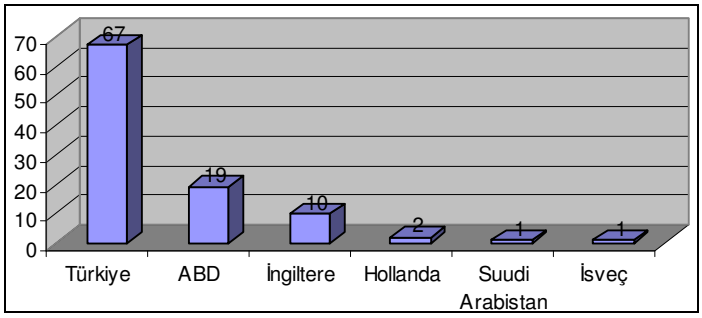
Şekil 2.27. Haftalık saldırı dağılımı

Hafta içinde yapılan atakların çoğunluğu Şekil 2.28'de gösterildiği gibi yüzde 71 gibi büyük bir oranla mesai saatleri dışında olduğu gözlemlenmiştir. Saldırıların mesai saatleri dışında yoğunlaşmasının sebebi güvenlik ihlâllerinin fark edilmesini önlemek veya geciktirmek olarak yorumlanabilir.



Şekil 2.28. Günlük saldırı dağılımı

Türk firmaları yüzde 67 oranı ile en çok saldırıyı Türkiye'den yüzde 19 oranı ile ABD ve yüzde 10 oranıyla İngiltere izliyor. ABD ve İngiltere kaynaklı saldırıların daha çok e-ticaret sistemlerine yapılması Türkiye'nin sanal ortamda cazibe merkezi haline geldiğini göstermektedir. Meydana gelen güvenlik ihlallerinin ülkelere göre dağılımı Şekil 2.29'da gösterilmiştir



Şekil 2.29. Meydana gelen saldırıların ülkelere göre dağılımı

Ülkemizde kamu sektöründeki kurumların bilgi güvenliğinin değerlendirilmesiyle ilgili iki farklı çalışma da TÜBİTAK tarafından yapılmıştır [98–100].

Yapılan çalışmalar değerlendirildiğinde dünyada ve ülkemizde bilgi güvenliği ihlalleri alınan tüm tedbirlere rağmen yaşanmakta ve sayıları her geçen gün artmaktadır. Güvenlik ihlallerinin en aza indirilmesi için zafiyetlerin saldırganlardan önce tespit edilmesi ve gerekli önlemlerin zamanında alınması gerekmektedir. Sızma testleri sayesinde birçok zafiyetin saldırıya dönüşmeden giderilmesi ve kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında etken bir rol oynamasından dolayı Bölüm 4'de sızma testleri ayrıntılı olarak açıklanmıştır. Dünyada ve ülkemizde yapılan güvenlik raporlarına bakıldığında saldırılar web uygulamaları üzerinde yoğunlaşmaktadır. Web uygulamalarının her geçen gün yaygınlaşması ve kurumsal bilgi sistemlerinin web üzerine hızla taşındığı düşünüldüğünde web uygulama güvenliğinin kurumsal bilgi güvenliğinin sağlanmasında en önemli unsur olacağı değerlendirildiğinden web uygulamalarının güvenliğinin sağlanmasıyla ilgili geniş kapsamlı çalışma Bölüm 5'de verilmiştir.

Saldırıların artmasının yanında otomatik saldırı araçlarının artması bir diğer önemli tehdit unsurudur. Otomatik araçların en çok tehdit ettiği sistemler güvenlik açığı bulunan ve bu açığın kapatılması için yayınlanan yamaları zamanında yüklemeyen bilgi sistemleridir. Bu tür tehditleri en aza indirmek için teknik sorumlulara önemli görevler düşmektedir. Teknik sorumlular ve diğer çalışanların kurumsal bilgi güvenliğinin sağlanmasındaki rolü Bölüm 6'da kapsamlı olarak anlatılmıştır.

Kötücül yazılımlar kurumsal bilgi güvenliğini tehdit eden diğer önemli risk unsurlarıdır. Bu bölümde incelenen raporlardan da görüldüğü gibi günümüzde zararlı kodlar ve insan faktöründen kaynaklanan hatalar birleştiğinde ortaya çok büyük tehditler çıkmaktadır. Sazan postaların casus yazılımlarla birlikte kullanılması günümüzde bilgi güvenliği tehditlerinin başında gelmektedir. Bu tür tehditlerin engellenmesi için öncelikle insan faktörünün an aza indirgenmesi gerekmektedir. İnsan faktörünün en aza indirgenmesi için kullanıcılarda bilgi güvenliği farkındalığı oluşturulması ve bilgi güvenliği eğitimlerinin verilmesi gerekmektedir. Ayrıca kurumsal bilgi güvenliğinin sağlanmasındaki ihtiyaç duyulan uzman ve bilgi eksikliğinin giderilmesi amacıyla kurum ve kuruluşların güvenlik konusunda bilgi güvenliği hizmeti veren firmalarda danışmanlık hizmeti almaları gerekmektedir.

Ülkemizde abone sayısı hızla artan ve kurum, kuruluş ve bireyler tarafından oldukça yaygın olarak kullanılan, en çok güvenlik açıklarına sahip olan ADSL kullanıcılarının güvenliği unutulmamalıdır. ADSL kullanıcılarının güvenliğinin sağlanmasına yönelik merkezi tedbirlerin alınması, gerekli yatırımların yapılması ve kullanıcı eğitimlerinin devlet destekli merkezler tarafından verilmesi gerekmektedir.

2.6. Bilgi Güvenliğiyle İlgili Uluslararası Mevzuatlar

Uluslararası standartlar, yasalar ve yönetmelikler tüm dünyada olduğu gibi ülkemizde de birçok işletmeyi ve kamu kuruluşunu etkilemektedir. Kuruluşların bilgi güvenliğinin sağlanması konusundaki yaklaşımlarına yönelik standartlar getirmesi açısından bilgi güvenliğiyle ilgili mevzuatın bilinmesi önemlidir. Bilgi güvenliğini direkt veya dolaylı olarak ilgilendiren önemli yasa ve yönetmelikler aşağıda kısaca açıklanmıştır [101].

Sarbanes-Oxley Yasası (SOX): Finansal raporlama bilgilerinin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanmasının yanı sıra finansal bildirim için de denetimler ve standartları zorunlu kılar. Yöneticiler tarafından kişisel sertifika verilmesi, uyuma yönelik baskıyı artırır ve üst yönetimin konuyla somut olarak ilgilenmesini mecburi kılar.

Gramm-Leach-Bliley Yasası (GLBA): Finansal Hizmetler Modernizasyon Yasası olarak da bilinen GLBA, bankalara, menkul kıymet şirketlerine ve diğer finans kuruluşlarına uygulanır. Bu yasa, müşteri kayıtlarının gizliliğini zorunlu kılar ve korunmalarıyla ilgili güvenceleri şart koşar.

Yeni Basel Sermaye Uzlaşısı (Basel II): Uluslararası Ödemeler Bankası tarafından yayımlanan Basel II, uluslararası para transferleri yapan bankalarda risk ölçümüne yönelik yeni standartlar getirmektedir. Buna göre, minimum sermaye yedekleri düzeylerini belirlemek için kredi ve pazar riskine ilk kez olarak operasyonel riskin hesaplanması gereği de eklenmiştir.

AB Veri Koruma Yönergesi: AB ülkelerinde oturanların kişisel bilgilerinin korunmasına yöneliktir. AB üyesi olan ülkeler ile AB üyesi olmayan ülkeler arasında kişisel bilgilerin aktarılmasını kısıtlar. Yönerge, kişisel bilgilerin elde edilmesi, kullanılması, açıklanması, silinmesi, kaydedilmesi ve saklanmasına yönelik kısıtlamaları da içerecek şekilde veri işlenmesine yöneliktir. Yönerge, birçoğu kendi yasalarını da Yönerge ile uyumlu hale getirmiş bazı üye devletler tarafından uygulanmaktadır. İngiltere'nin 1998 tarihli Veri Koruma Yasası buna örnek olarak gösterilebilir.

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA): Sağlık sigortasının taşınabilirliğini sağlamanın yanı sıra hasta bilgilerinin güvenliği ve gizliliği için de bir dizi şart getirmektedir.

Menkul Kıymetler ve Borsalar Komisyonu (SEC) Kuralları: Belirli borsa üyesi kuruluşları, komisyoncular ve hisse senedi satıcıları tarafından, ilk iki yılı kolay erişilebilir durumda bulunmak kaydıyla en az altı yıl boyunca tutulması gereken iletişim türlerini belirler.

Hisse Senedi Alım-Satımcıları Ulusal Derneği (NASD) Kuralları: Komisyoncuların ve hisse senedi alım-satımcılarının, kamuya duyurular da dâhil olmak üzere tüm aktivitelerinin kontrolü için bir sistem kurmak zorundadır. Bu şart, tüm elektronik iletişimin düzenli olarak araştırılması ve incelenmesine yönelik bir süreç gerektirir.

Ayrıca, üye firmaların, tüm müşteri kayıtları ve işlem verilerine ait kayıtların denetlenebilir biçimde ve kolay erişilebilen bir ortamda tutulmasına yönelik kayıt tutma stratejisi uygulaması gerekmektedir.

Federal Bilgi Güvenliği Yönetimi Yasası (FISMA): Bu yeni yasa, her federal kuruluşun bilgi sistemleri ve varlıklarının güvenliğini sağlayacak bir program uygulaması ve belgelendirmesini gerektirir.

Bilgi Güvenliği Forumu (ISF) Bilgi Güvenliği En İyi Uygulamalar Standardı: BT araştırma ve risk yönetimi organizasyonu alanında dünya lideri olan ISF üyeleri tarafından yayımlanan, işletmelere odaklanmış en iyi uygulamalar bildirgesidir.

2.7. Türkiye'de Bilişim Suçları Hukuku

Sızma testleri yapılırken yasalar karşısında suç işlememek ve bilgi güvenliğinin sağlanmasında caydırıcı rol oynaması açısından bilişim suçları hukukunun bilinmesi gereklidir. Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi elektronik ortamlarda teknolojinin kullanılması ile işlenilen suçlar bilişim suçları olarak tanımlanmaktadır. Bilişim vasıtasıyla işlenen suçlara, internet ve diğer bilişim sistemleri üzerinden de gerçekleştirilebilen küfür, hakaret, dolandırıcılık gibi klasik suçların yanında bilişime özgü suçlar olan verilerin tahrip edilmesi veya değiştirilmesi, sistemlere yetkisiz girişler, sistemin işleyişini değiştirmek örnek olarak verilebilir. Türkiye'de bilişim suçlarıyla 2002 yılında Emniyet Genel Müdürlüğü bünyesinde kurulan İnternet ve Bilişim Suçları Şube Müdürlüğü ilgilenmektedir. Türkiye'de en çok karşılaşılan bilişim suçları aşağıda maddeler halinde verilmiştir [102].

- Başkalarının adına e-posta göndererek özellikle ticari ve özel ilişkilerin zedelenmesi.
- Başkalarının adına web sayfası hazırlamak ve tanıtım amacıyla başkalarına e-posta ve mesaj göndermek
- Kişisel bilgisayarlar ya da kurumsal bilgisayarlara yetkisiz erişim ile bilgilerin çalınması ve karşılığında tehdit ederek maddi menfaat sağlanması.

- Şirketlere ait web sayfalarının alan adının izinsiz alınarak tescil edilen alan adlarının karşılığında yüklü miktarlarda para talep edilmesi
- Yasal olmayan (korsan) programların kopyalanması ve satılması
- Finans kurumlarına ait web sayfalarının taklit edilerek kullanıcıya ait kullanıcı adı ve parola gibi bilgilerin elde edilmesi

Türkiye'de bilgi güvenliğiyle dolaylı ya da direkt olarak ilgili olan kanunlar maddeler halinde aşağıda verilmiştir [103]. Bu kanunlar arasında yer alan ve bilgi güvenliğini direkt ilgilendiren 5237 nolu kanunun ilgili kısımları aşağıda kaçıklanmıştır.

- 1991 tarihinde 3756 sayılı kanunla yapılan düzenlemeler.
- Fikri hakları koruyan 5846 sayılı kanunun ilgili maddeleri.
- 5237 sayılı Yeni Türk Ceza Kanunu'nda yapılan düzenlemeler.
- 5070 sayılı Elektronik İmza Kanunu'nda yapılan düzenlemeler.
- 6762 sayılı Türk Ceza Kanunu'nun ilgili maddeleri.
- 2499 sayılı Sermaye Piyasası Kanunu'nun ilgili maddeleri.

1 Nisan 2005 tarihinde yürürlüğe giren yeni TCK'nin kapsamında, bilişim sistemlerine karşı işlenen suçlar gerekçeleriyle birlikte yer almaktadır. Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme, tüzel kişiler hakkında güvenlik tedbiri uygulanması, banka ve kredi kartlarının kötüye kullanılması kapsamındaki suçları tanımlayan kanun maddeleri aşağıda açıklanan TCK'nin 5237 nolu kanunun onuncu bölümündeki 243 ve 246 nolu maddelerinde yer almaktadır [104].

Bilişim sistemine girme

Madde 243

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye iki yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, iki yıldan dört yıla kadar hapis cezasına hükmolunur.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 244

(1) Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

(2) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

(3) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve 5000 güne kadar adli para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması

Madde 245

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adli para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır

cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

Madde 246

(1) Bu Bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Ayrıca Adalet Bakanlığı tarafından bilişim suçlarına ilişkin "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" hazırlanmıştır [105]. Tasarıya göre, bilgisayar korsanlarına 2 yıldan 5 yıla kadar hapis ve adli para cezası da öngörülmektedir. Tasarı kanunlaşırsa bir bilişim ağı aracılığıyla; bilişim sisteminde bulunan verileri veya programları hukuka aykırı olarak bozan, silen, değiştiren, yok eden, erişilmez kılan veya sisteme veri veya program yerleştiren, ekleyen, veri veya programlara zarar veren kişiye, 2 yıldan 5 yıla kadar hapis ve adli para cezası verilecektir. Tasarıda, bir bilişim ağı aracılığıyla; bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı giren veya her hangi bir şekilde sistemde kalmaya devam eden kimseye 6 aydan 2 yıla kadar hapis cezası veya 2 yüz günden 8 yüz güne kadar adli para cezası verilmesi öngörülüyor. Bilişim ağına bağlanmak suretiyle, ağdaki verileri hukuka aykırı olarak herhangi bir şekilde izleyen kimseye 1 yıldan 3 yıla kadar hapis ve adli para cezası, bilişim ağına bağlanmaksızın herhangi bir yöntemle bilişim sistemindeki verileri hukuka aykırı izleyen kimseye üç yıldan beş yıla kadar hapis cezası verilecek.

Tasarıya göre, bir çocuğa veya çocuk gibi görünen veya çocuk olduğu izlenimi veren bir kişiye ait gerçek ya da temsili görüntü, yazı veya sesleri içeren pornografik ürünleri bilişim ortamında dağıtmak amacıyla üreten kişiye 8 yıldan 12 yıla kadar hapis ve 5 bin güne kadar adli para cezası verilebilecektir. Bilişim ortamında; Türk Ceza Kanunu'nda belirlenen devletin güvenliğine karşı işlenecek suçlar ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan ve bilişim sistemi veya bilişim ağı kullanılarak işlenen suçlara ilişkin içeriği üreten, tanıtan veya

sunanlar hakkında hükmedilecek cezalar yarı oranında arttırılacaktır gibi hükümlerde bulunmaktadır.

Bilişim hukuku alanında 2006 yılı önemli ve hareketli bir yıl olarak geçmiştir. Her geçen gün kullanımı gittikçe yaygınlaşan internet ve mobil teknolojilerin kullanımı hukukun sınırlarını zorlamaya devam etmektedir. Ülkemizde bilişim hukuku alanında teknolojinin gerisinde kalınmaması için üniversiteler, kamu kurumları, sivil toplum kuruluşları, bilgi güvenliği uzmanları ve hukukçular tarafından çalışmaların sürdürülmesi ülkemizde bilgi güvenliğinin sağlanması açısından önem taşımaktadır

Bilişim teknolojilerindeki baş döndürücü hız insanların eğlence, iletişim, haber alma ve buna benzer günlük yaşamında ihtiyaç duyduğu alışkanlıklarında büyük değişikliklere yol açmaktadır. Özellikle internet üzerinden geniş banttan yayın yapan radyo ve TV yayıncılığının hızlı bir gelişim içinde olması, mobil telefonlar için televizyon, video, fotoğraf makinesi gibi uygulamalarının yaygınlaştırılması, film–müzik–resim–e-posta vb. birçok özelliği bir arada barındıran cep bilgisayarlarının hızla yaygınlaşması günlük yaşantımızın ne kadar değiştiğini göstermektedir. Teknolojinin yakınsaması diyebileceğimiz bu durum elbette hukuk alanında da birçok karmaşaya sebep olacaktır. Örneğin internet üzerinden yayın yapan bir televizyon veya radyo yayınlarının denetimi, yayıncılık yapmak için alınması gereken izinler vb. gibi konularda hangi kurumun yetkili olacağı konusunda belirsizlikler vardır. Ülkemizde bu belirsizlikler sonucundan RTÜK ile Telekomünikasyon Kurumu arasında çatışmalar yaşanabileceği söylenebilir.

Sonuç olarak bilişim alanına özgü hukuksal düzenlemeler ve yaptırımlar elbette dünyada olduğu gibi ülkemizde de gerekmektedir. Yasal boşluklardan faydalanılarak meydana gelen ihlal sayısı her geçen gün artmakta ve bunların önüne geçilmesi gerekmektedir. Ancak burada dikkat edilmesi gereken en önemli hususun, çıkarılacak olan yasaların internet kullanımını engelleyici veya caydırıcı yaptırımlar içermemesine dikkat edilmesi gerekmektedir.

3. KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Sızma testlerinden bahsetmeden önce dünyada ve Türkiye'de yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasında önemli bir rol oynayan güvenlik yönetim sistemleri ve bilgi güvenliği standartları bu bölümde detaylı olarak açıklanmıştır. Bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak tanımlanmaktadır [106].

Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları, anticasus yazılımlar, şifreleme, vb.) bilgi güvenliğinin sağlanması mümkün değildir. BGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, BGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

BGYS'nin kurumlara sağlayacağı faydalar ana hatlarıyla aşağıda belirtilmektedir [101]. Bunlar;

- Tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması
- Kurumsal saygınlığın korunması ve artışı
- İş sürekliliğinin sağlanması
- Bilgi kaynaklarına erişimin denetlenmesi
- Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi

- Otomatik ve elle yönetilen sistemlerde, duyarlı bilgilerin uygun bir şekilde kullanıldığının garanti altına alınması amacıyla gerçekçi bir kontrol sistemi kurulması
- Bilgi varlıklarının gizliliğinin, bütünlüğünün ve doğruluğunun sağlanması
- Personelin, müşterilerin ve yüklenicilerin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanma ve/veya kaynakları suistimal etmelerinin engellenmesi
- Personelin, başkaları tarafından yapılabilecek olan suistimal ve tacizlere karşı zan altında kalmasının engellenmesi
- Duyarlı bilgilerin uygun bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanması ve
- Bilgi sistemlerini kullanan kişilerin, umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suistimal etme gibi nedenlerden dolayı oluşabilecek donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızalara karşı korunması,

olarak sıralanabilir.

Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, risk yönetimi, denetim kontrollerinin seçilmesi, uygulanabilirlik beyannameleri BGYS kurulabilmesi için, yapılması gereken adımlardır [107]. Bilgi güvenliğinin yönetiminin kurulmasında izlenmesi gereken adımlar bu bölümde sırasıyla takip eden başlıklarda açıklanmıştır.

3.1. Kurumsal Bilgi Güvenliği Politikaları

Güvenlik politikaları kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür [108]. Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması için tüm bilgi güvenlik faaliyetlerini kapsayan ve yönlendiren talimatlar olup kurumsal bilgi kaynaklarına erişim yetkisi olan çalışanların uymaları gereken kuralları içeren resmi bir belge niteliğindedir.

Güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından benimsenmelidir. Güvenlik politikası kullanıcılar tarafından uygulanabilir ve anlaşılabilir, güvenlik yöneticileri tarafından yönetilebilir olmalıdır. Bilgi güvenliği politikaları her kuruluş için farklılık gösterse de, genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadelerdir. Yönetimin, kurumsal bilgi güvenliği hakkında aldığı ayrıntılı kararları da içerir.

Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikadan sorumlu olan çalışanların ve gruplarının belirlendiği, uygulanması ve yapılması gereken kuralların, ihlal edildiğinde uygulanacak cezai yaptırımların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı 7 bölümden oluşmalıdır [108]. Kurumsal Güvenlik Politikası içerisinde bulunması gereken bölümler Çizelge 3.1'de gösterilmiştir.

Çizelge 3.1. Güvenlik politikası kısımları

Bölüm Adı	İçeriği
Genel Açıklama	Politikayla ilgili gerekçeler ve buna bağlı risklerin tanımlandığı kısım
Amaç	Politikanın yazılmasındaki amaç ve neden böyle bir politikaya ihtiyaç duyulduğu
Kapsam	Politikaya uyması gereken çalışan grupları (ilgili bir grup veya kurumun tamamı) ve hangi bilgi varlıklarını kapsandığını belirleyen kısımdır.
Politika	Uygulanması ve uyulması gereken kuralların yani politikanın yazıldığı kısımdır.
Cezai Yaptırımlar	Politika ihlallerinde uygulanacak cezai yaptırımların açıklandığı kısımdır
Tanımlar	Teknik terimlerin veya muğlâk ifadeler listelenerek açıklandığı kısımdır.
Düzeltme Tarihçesi	Politika içerisinde yapılan değişiklikler, tarihleri ve sebeplerinin yer aldığı kısımdır.

Belli konularda çalışanların daha fazla bilgilendirilmesi, dikkat etmesi gereken hususlar, ilgili konunun detaylı bir şekilde ifade edilmesi istendiğinde alt politikalar geliştirilmelidir. Örneğin kullanıcı hesaplarının oluşturulması ve yönetilmesi, şifre

unutma, şifre değiştirme, yeni şifre tanımlama gibi durumlarda uyulacak kurallar alt politikalar aracılığıyla açıklanmalıdır. Bir diğer örnek ise, e-posta gönderme ve alma konusunda, üst yönetimin kararlarını, haklarını, kullanıcının uyması gereken kuralları alt politika içerisinde ifade etmek daha uygun olacaktır. Bu alt politikayla üst yönetimin, gerekli gördüğünde çalışanlarının e-postalarını okuyabileceği, e-postalar yoluyla gizlilik dereceli bilgilerin gönderilip alınamayacağı gibi hususlar, e-posta alt politikası içerisinde ifade edilebilir. Alt politikalar içerisinde, izin verilen yazılımlar, veritabanlarının nasıl korunacağı, bilgisayarlara uygulanacak erişim denetim ölçütleri, güvenlikle ilgili kullanılan yazılım ve donanımların nasıl kullanılacağı gibi konular da açıklanabilir.

Kurumsal bilgi güvenlik politikaları kuruluşların ihtiyaçları doğrultusunda temel güvenlik ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) bazıları üzerinde yoğunlaşabilir. Örneğin askeri kurumlarda, bilgi güvenlik politikalarında genellikle gizlilik ve bütünlük ihlâlinin engellenmesi amaçlanmaktadır. Erişilebilirlik de önemlidir ancak birinci planda gizlilik ve bütünlük gelmektedir. Askeri bir savaş uçağının kalkış zaman bilgilerinin onaylanıp yürürlüğe girmesi için düşmanlar tarafından görülmemesi (gizlilik) ve değiştirilmemesi (bütünlük) gereklidir. Bir diğer örnek ise kâr amacı gütmeyen işletmelerde uygulanan bilgi güvenlik politikalarında genellikle erişilebilirlik ve bütünlük ihlâlinin engellenmesi amaçlanmaktadır. Gizlilik unsuru da önemlidir ancak birinci planda erişilebilirlik ve bütünlük gelmektedir. Üniversite sınav sonuçlarının açıklandığı yükseköğretim kuruluşunda uygulanan güvenlik politikasında öğrenciler sınav açıklandıktan sonra istediği zaman diliminde (erişilebilirlik) doğru bir şekilde (bütünlük) sınav sonuçlarına bakabilmelidir.

İyi bir güvenlik politikası, kullanıcıların işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve sistem yöneticilerinin eldeki imkânlarla uyabilecekleri ve uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Alınan güvenlik önlemleri ve politikayı uygulayan yetkililer veya birimler yaptırımları uygulayabilecek idari ve teknik yetkilerle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri tanımlanarak kullanıcılar, sistem

yöneticileri ve diğer kişilerin sisteme ilişkin sorumlulukları, yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıkça tanımlanmalıdır. Politikalar içerisinde uygulanacak olan yasal ve ahlaki mahremiyet koşulları ile elektronik mesajların ve dosyaların içeriğine ulaşım, kullanıcı hareketlerinim kayıt edilmesi gibi denetim ve izlemeye yönelik işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır. Gerekli durumlarda istisnalar ve alternatif uygulamalar açıklanmalıdır.

Saldırıların ve diğer sorunların tespitinde kullanıcıların, yöneticilerin ve teknik personelin sorumluluk ve görevleri ile tespit edilen sorun ve saldırıların hangi kanallarla kimlere ne kadar zamanda rapor edileceği güvenlik politikalarında açıkça belirtilmelidir. Sistemlerin gün içi çalışma takvimleri, veri kaybı durumunda verinin geri getirilmesi koşulları gibi kullanıcının sisteme erişmesini sınırlayan durumlara politikalar içerisinde yer verilmelidir. Bu durumlarda kullanıcıya, izlemesi gereken yolu anlatacak ve yardımcı olacak kılavuzlara da yer verilmelidir.

3.2. Bilgi Güvenliği Yönetim Sistemlerinin Kapsamı

Bilgi Güvenliği Yönetim Sistemleri (BGYS) kapsamına dâhil edilecek bilgi varlıkları kurumların belirlediği ihtiyaçlar doğrultusunda tespit edilir. Kapsamlar aşağıda gösterilen kategorilerde sınıflandırılabilir [107].

- Kurumun sahip olduğu bilgi sistemlerinin tamamı
- Bilgi sistemlerinin bir kısmı (Bilişim sistemleri, kâğıt ortamdaki bilgiler, elektronik bilgi varlıkları, vb.)
- Belli bir yerleşim birimindeki bilgi sistemleri (Merkez binalar, Genel Müdürlükler, vb.)
- Odaklanılmış bir bilgi sistemi (bilgisayarlar, ağ sistemi, sunucu bilgisayarlar, web sunucusu, vb.) olabilir.

Bir kuruluşta elektronik ortamlarda üretilen, dağıtılan ve saklanan bilgi BGYS kapsamına örnek olarak verilebilir.

3.3. Risk Yönetimi

Fransızca “risque” kelimesinden dilimize geçmiş olan risk, sözlük anlamı olarak zarara uğrama tehlikesi ve öngörülebilir tehlikeleri ifade eder [109]. Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığı olarak da tanımlanabilir. Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliği, ticari kuruluşlar içinse öncelikle kârlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir. Sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesi amaçlanmaktadır.

Başarılı bir risk yönetimi için, kuruluşların bilgi varlıklarına ve hedeflerine yönelik risklerin belirlenerek, analiz edilmesi, tanımlanan risklerin denetim altında tutularak izlenmesi gereklidir. Riski yönetmenin en doğru yolu, gerçekleşme olasılığı ve gerçekleştiğinde vereceği zarar en yüksek olan riskleri azaltacak bilgi teknolojisi risk yönetim sürecinin oluşturulmasıdır. Risk yönetim süreci oluşturulduktan sonra yapılması gereken diğer bir iş risk yönetimi sorumlusunun atanmasıdır. Sorumlunun kim olacağı veya işi nasıl yürüteceği, kurumun büyüklüğüne ve ihtiyaçlarına göre değişecektir. Büyük ölçekli kurum ve kuruluşlarda, risklerle ilgili önemli bilgileri toplayarak uygulanması gereken kararları verecek, risk yönetimi politikalarını ve kılavuzlarını oluşturacak özel amaçlı risk yönetim sistemlerinin devreye alınmasını sağlayacak ayrı bir birimin kurulması gereklidir. Risk yönetiminde tek bir birimin veya tek bir kişinin çalışmasının yanında kurum içi ortak bir çalışmaya da ihtiyaç duyulmaktadır.

Risk yönetiminde kurum içi haberleşme kanallarının doğru yapılarak üst yönetimle iyi bir iletişim kurulması gereklidir. Risk yönetimi çalışmalarının başarısı, üst yönetimin desteğine ve kurumun iş hedefleriyle uyumlu olmasına bağlıdır. Risk yönetimi ile ilgili üst yönetim ve kurum çalışanlarının desteği sağlandıktan sonra işleyiş yöntemlerinin oluşturulması gereklidir. Öncelikle kuruluşun uzun dönemdeki

hedefleri üzerinde çalışılmalı ve gelecekteki hedefleri tehlikeye atacak risklerin tanımlanarak denetimlerin oluşturulması gereklidir. Risk yönetim planları daima güncel tutulmalıdır.

Bilgi güvenliği risk yönetiminde, bilgi güvenliğini tehdit eden daha önceki bölümlerde açıklanan unsurların meydana gelmesinin engellenmesi hedeflenmektedir. Ancak riskler tamamen ortadan kaldırılamayacağından tedbirlere rağmen riskler oluştuğunda bilgi güvenliğinin bu risklerden en az etkilenmesi risk yönetimiyle sağlanacaktır. Risklerin oluşmasını en aza indirgemek için, önceden alınması gereken tedbirler ve denetimler tarif edilerek kurum çalışanları ve yöneticileri tarafından gerekli önlemler alınmalıdır. Risk oluştuğunda probleme müdahale, iş sürekliliğinin sağlanması ve olağanüstü durumdan kurtulma yöntemlerini içeren felaket yönetimiyle ilgili politikalar oluşturulmalı ve sorun oluştuğunda gecikmeksizin uygulanmalıdır. Burada önemle üzerinde durulması gereken, risklerin ortadan kaldırılması veya azaltılması için oluşturulacak denetimlerin dengesidir. Gereksiz veya iyi bir risk planlaması yapılmadan oluşturulan denetimler sonucunda iş yapılamaz duruma gelinmesi de kurumlar için önemli bir risk faktörüdür. Risk tanımlaması yapıldıktan sonra, riskler karşısında alınacak kararlar şunlar olabilir [110].

- *Riskin Yönetilmesi (Azaltılması):* Tanımlı risklerin kabul edilebilir seviyeye çekilmesi için yapılması gerekenler ve ek güvenlik denetimleri (yazılım, donanım, prosedür, vb.) devreye alınarak riskin istenilen seviyeye düşürülmesidir. Kabul edilebilir seviyedeki riskler ise artık (Residual) risk olarak kabul edilir ve herhangi bir işlem yapılmaz.
- *Riskin Kabullenilmesi*: Herhangi bir ek güvenlik denetimine ihtiyaç duyulmadan; riskin tespit edilen seviyede sürdürülmesi kararıdır. Güvenlik riski mevcut olan ancak saldırı riski olmayan bilgi varlıkları için risk maliyetine girmek yerine, riskin göz ardı edilmesi tercih edilir.
- *Riskin Transferi*: Riskin etkilediği bilgi varlıklarının zararlarını başka kuruluş veya sigorta kurumlarına devir edilmesi kararıdır. Bu sayede riskin önlenmesi için gerekli maliyet düşürülür ve sorumluluk başkasına verilir.

Risklerin tanımlanması, hesaplanması ve değerlendirilmesi süreçleri risk analizi olarak tanımlanmaktadır. İki farklı risk analizi yöntemi mevcuttur. Bunlar, nicel (Quantitative) ve nitel (Qualitative) yöntemlerdir [111].

Nitel Hesaplama Yöntemi: Bilgi sahipleri ve uzman kişiler tarafından bilginin önemine ve kritikliğine değer atanması ve bu değerlerin bir ekip tarafından karşılıklı müzakereler ile son kabul gören güvenlik değerine atanmasıyla yapılan risk hesaplama yöntemidir. Sayısal değerler yerine yüksek, çok yüksek gibi tanımlayıcı değerler kullanılır.

Nicel Hesaplama Yöntemi: Bilgi varlıklarına, önemine ve korunmasına göre mali değerler atanması ile yapılan risk hesaplama yöntemidir. Nicel risk analizinde, bilginin değeri, zafiyeti, tehditin olma ihtimali, tehditin etkisi gibi değerlere sayısal değerler verilir ve bu değerler matematiksel ve mantıksal yöntemlerle hesaplanıp risk değeri bulunur.

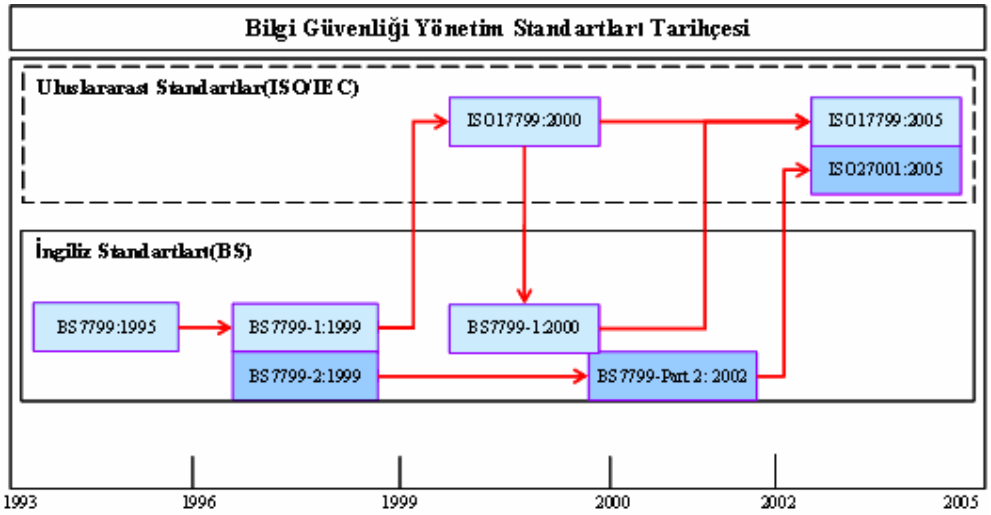
Tüm kuruluşlara uyan standart risk analizi yöntemleri mevcut değildir. Her kuruluşun kendine özel bir varlık envanteri, bu varlıkların güvenliğini tehdit eden farklı tehlikeler vardır. Bunlara ek olarak, kurumdan kuruma güvenlik anlayışı ve güvenlik ihtiyaçları değişim göstermektedir. Kurumların risk yönetiminde izlemesi gereken süreçler maddeler halinde aşağıda açıklanmıştır [112]. Bunlar;

- Varlıkların tespit edilerek sınıflandırılması,
- Tehlike (tehdit) analizleri ve tanımlamaları yapılması,
- Mevcut güvenlik açıklarının tespit edilmesi,
- Risk hesaplama yöntemlerinin seçilerek risklerin hesaplanması,
- Mevcut güvenlik denetimlerinin belirlenmesi,
- Risklerle ilgili kararların alınması,
- Riskleri azaltmak için ek güvenlik denetimlerinin belirlenmesi,
- Yönetim tarafından ek güvenlik denetimlerinin seçiminin yapılması ve
- Seçilen ek güvenlik denetimlerinin uygulanmak üzere planlanması

olarak sıralanabilir.

3.4. Bilgi Güvenliği Standartları

Tehditlerin sürekli olarak yenilenmesi, kullanılan yazılım veya donanımlarda meydana gelen güvenlik açıklarının takibi, insan faktörünün kontrolü gibi süreçlerin takip edilebilmesi ve üst seviyede bilgi güvenliğinin sağlanması için bilgi güvenliği sürecinin yönetilmesi gerekmektedir. BGYS oluşturma yönünde yapılan çalışmalar sonucunda İngiliz Standartlar Enstitüsü (British Standards Institute-BSI) tarafından 1995 yılında BS–7799 standardının ilk kısmı olan BS7799–1, 1999 yılında ise aynı standardın ikinci kısmı olan BS7799–2 İngiliz standardı olarak yayınlanmıştır. BS7799–1 2000 yılında küçük düzeltme ve adaptasyonlardan geçerek ISO tarafından ISO/IEC–17799 adıyla kabul edilmiş ve dünya genelinde kabul edilen bir standart halini almıştır. 2002 yılında ise BSI tarafından BS–7799 standardının ikinci kısmı olan BS–7799–2 standardı üzerinde eklemeler ve düzeltmeler yapılarak ikinci defa İngiliz standardı olarak yayınlanmıştır. 2005 yılında ise ISO tarafından ISO/IEC–17799 standardı üzerinde eklemeler ve düzeltmeler yapılmış ISO/IEC–17799:2005 adıyla yeniden yayınlanmıştır. Son olarak 2005 yılında ISO İngiliz standardı olan BS7799–2 üzerinde eklemeler ve düzeltmeler yaparak ISO/IEC:27001 standardını yayınlamıştır [113]. Bilgi güvenliği yönetim sistemlerinin temelini teşkil eden standartların yayınlanma süreleri Şekil 3.1'de tarihsel akışa göre verilmiştir.



Şekil 3.1. BGYS'de önemli olan standartların yayımlanma süreleri

Şekil 3.1'de gösterilen ve kurumsal bilgi güvenliğinin üst düzeyde sağlanması için gerekli olan bilgi güvenliği yönetiminde kullanılan uluslararası standartlar takip eden alt bölümde sırasıyla açıklanmıştır.

3.4.1. İngiliz standardı (BS–7799)

BS–7799, bilgi varlıklarının gizlilik, doğruluk ve erişilebilirliğini güvence altına almak için uygulanması gereken güvenlik denetimlerini düzenleyen ve belgelendiren iki aşamalı İngiliz standartıdır. 1999 yılında yayınlanan ilk sürümün birinci bölümünde bilişim güvenliği için çalışma kuralları anlatılmakta olup (Information Technology–Code of Practice for Information Security Management) 10 bölüm içerisinde 36 kontrol 127 alt kontrol maddesi bulundurmaktadır. İkinci bölümde (Information Security Management Systems–Specification with Guidance for Use) bilgi güvenliği yönetim sistemini planlamak, kurmak ve devam ettirmek için gerekli olan süreçler adım adım tanımlamakta ve bilgi güvenliği yönetim sistemine ait belgelendirme (sertifikasyon) bu kısımda yapılmaktadır.

BS–7799 kurumların sadece kendi bilgi güvenlik prosedürlerini değil birlikte çalıştıkları iş ortaklarıyla ilgili sözleşmelerinde bilgi güvenliği yönünden analiz edilmesine yardımcı olmaktadır. BS–7799 standardı endüstri, devlet ve ticari kuruluşlardan ortak bir güvenlik modeli oluşturulmasına gelen talepler sonucu BSI kuruluşu ve BOC, BT, Marks and Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever ve diğer bazı şirketlerin katılımıyla hazırlanmış bir standarttır. Standardın tarihsel oluşumuna bakıldığında 1993 yılında Kural rehberi, 1995 yılında İngiliz standardı, 1998 yılında Sertifikasyon tarifi yapılmış 1999 yılında büyük bir düzeltmeden geçerek birinci kısmı, 2002 yılında ise ikinci kısmı yayınlanmıştır [114].

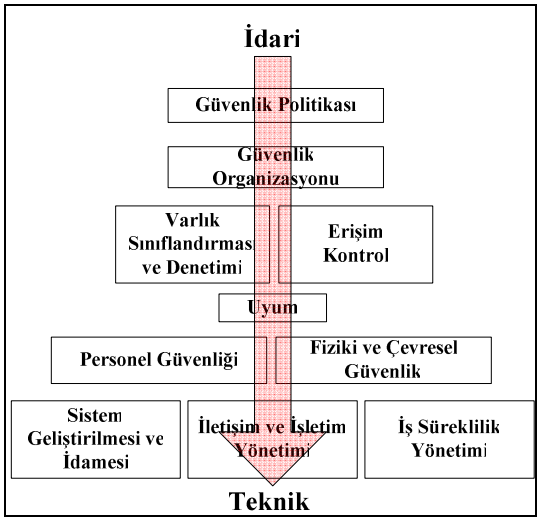
BS–7799 standardı teknik ve idari bölümlerden oluşmaktadır. Standardın birinci kısmının ilk sürümünde yer alan on bölümünün idari ve teknik kısımlara göre sınıflandırılması Şekil 3.2'de gösterilmiştir. Kısa açıklamaları ise aşağıda maddeler halinde belirtilmiştir [115].

Güvenlik politikası

- Bilgi güvenliği için yönetimin yönlendirilmesi ve desteğinin sağlanması

Güvenlik organizasyonu

- İşletme içindeki bilgi güvenliğinin yönetilmesi
- Üçüncü taraflarca erişilen işletmeye ait bilgi işleme araçlarının ve bilgi varlıklarının güvenliğinin korunması
- Bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından dışarıdan sağlandığında bilgi güvenliğinin sürdürülmesi



Şekil 3.2. BS–7799 (Versiyon–1) bölümleri

Varlık sınıflandırması ve denetimi

- İşletmeye ait varlıklar için uygun korunmanın sağlanması
- Bilgi kaynaklarının uygun koruma seviyesine sahip olduklarının garanti edilmesi

Erişim kontrol

- Bilgiye erişimin denetlemesi
- Bilgi sistemlerine yetkisiz erişimin engellenmesi

- Yetkisiz kullanıcı erişiminin engellenmesi
- Ağ oluşturulmuş hizmetlerin korunması
- Yetkisiz bilgisayar erişiminin engellenmesi
- Bilgi sistemleri içinde tutulan bilgiye yetkisiz erişimi engellemek
- Yetkisiz işlemlerin tespit edilmesi
- Mobil bilgi işlem ve uzaktan çalışma araçları kullanıldığında bilgi güvenliğinin temin edilmesi

Uyum

- Herhangi bir suçtan kaçınılması
- Organizasyonun güvenlik politikalarının ve standartlarının sisteme uyumunun sağlanması
- Sistem izleme işlemlerinin etkisini artırılması ve engellerinin azaltılması

Personel güvenliği

- İnsan hatalarını, hırsızlığı, sahtekârlığı ve araçların yanlış kullanılması risklerinin azaltılması
- Kullanıcıların bilgi güvenliği tehditlerinden ve sorunlarından haberdar olduklarının ve normal çalışma seyirleri içinde organizasyonla ilgili güvenlik politikasını desteklemek üzere donatıldıklarının garanti edilmesi
- Güvenlik arızalarından ve bozulmalarından meydana gelen hasarın en aza indirilmesi ve bu gibi olayların gözlenmesi ve bunlardan öğrenilmesi

Fiziki ve çevresel güvenlik

- İş alanına ve bilgilerine yetkisiz erişim, hasar ve müdahalenin engellenmesi
- Varlıkların kayıplarını, hasar veya tehlikelerini ve ticari faaliyetlerdeki kesilmenin önlenmesi
- Bilgi ve bilgi işleme araçlarının hırsızlığa veya tehlikeye atılmasının önlenmesi

Sistem geliştirilmesi ve idamesi

- Bilgi işlem sistemleri içerisinde güvenliğin kurulmasının temin edilmesi
- Uygulama sistemlerindeki kullanıcı verilerinin kaybedilmesini, değişmesini ya da hatalı kullanımının önlenmesi
- Bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması
- IT projelerinin ve destek etkinliklerinin güvenli bir şekilde yürütülmesini temin etmek
- Uygulama sistemi yazılımının ve bilgilerin güvenliğini korumak

İletişim ve işletim yönetimi

- Bilgi işlem tesislerinin doğru ve güvenle işletildiğinden emin olunması
- Sistem arızalarını en az seviyeye indirilmesi
- Bilgi ve yazılım bütünlüğünün korunması
- Bilgi işlem ve iletişim hizmetlerinin kullanılabilirliliği ve bütünlüğünün sürdürülmesi
- Ağlarda yer alan bilgilerin emniyetinin ve destekleyen altyapı sisteminin korunmasının sağlanması
- İş faaliyetlerinin kesintiye uğratılması ve varlıklara zarar verilmesinin önlenmesi
- Organizasyonlar arasında değişilen bilginin yanlış maksatlarla kullanılması, değiştirilmesi ve kaybedilmesinin önlenmesi

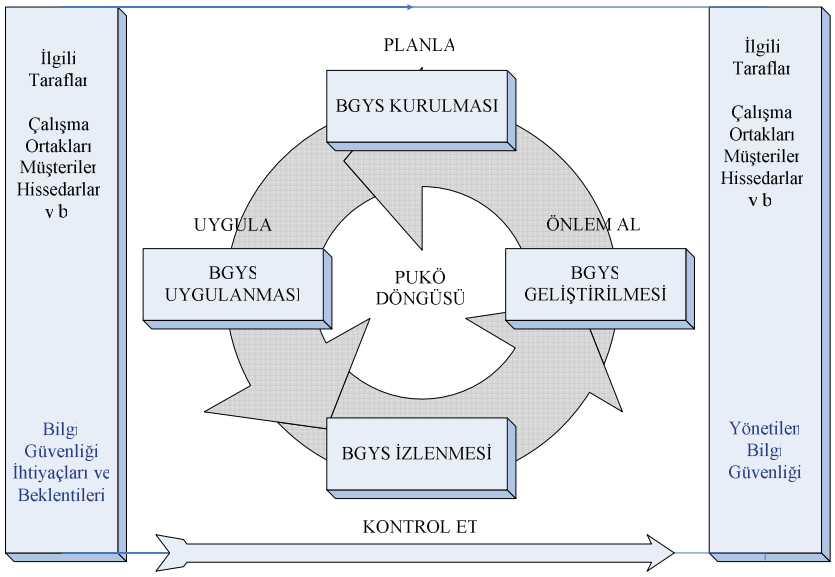
İş süreklilik yönetimi

- Ticari aktivitelerin karşılaştığı engellere karşı etkileri oluşturmak ve kritik ticari işlemleri büyük başarısızlıklar ve felaketlerden korunması

Kurumlar bilgi varlıklarını tespit edip sınıflandırdıktan sonra, bilgi varlıklarına yönelik tehditleri ve zafiyetleri değerlendirerek yukarıda anlatılan kontrollerden hangilerini uygulayıp, hangilerini uygulamayacaklarına karar vererek standardın kapsamını kendi kurumlarına özgü bir şekilde belirleyebilmektedirler.

BS–7799 ikinci kısmında kurumsal güvenlik ihtiyaçlarının belirlenmesi için gerekli olan bilgi güvenliği yönetiminin çatısı tanımlanarak BS–7799 birinci kısmında

tanımlanan kontroller uygulanmaktadır. Bu standart, yöneticilere ve personele etkin bir BGYS kurmaları ve yönetmeleri açısından bir model sağlamak üzere hazırlanmıştır. Bu model aşağıdaki tabloda açıklanan "Planla– Uygula–Kontrol Et– Önlem Al" (PUKÖ) modeli olarak bilinmektedir.



Şekil 3.3. BGYS PUKÖ döngüsü [116]

Şekil 3.3'te gösterilen modelin basamakları maddeler halinde kısaca aşağıda açıklanmıştır [116].

Planlama (BGYS'nin Kurulması)

- BGYS kapsamının tanımlanması
- BGYS politikasının belirlenmesi
- Risklerin belirlenmesi
- Risklerin değerlendirilmesi
- Risklerin giderilmesi için gerekli kontrollerin belirlenmesi
- Uygulanabilirlik bildirisinin hazırlanması

Uygulama (BGYS'nin işletilmesi)

- Risk iyileştirme planının hazırlanması

- Risk iyileştirme planının uygulamaya alınması
- Seçilmiş kontrollerin uygulanması
- Eğitim ve bilinçlendirme programlarının uygulanması
- Operasyonların yönetimi
- Kaynakların yönetimi
- Güvenlik olaylarını tespit ederek cevaplayabilen prosedür ve kontrollerin uygulanması

Kontrol (BGYS'nin gözden geçirilmesi)

- İzleme prosedürlerinin uygulamaya alınması
- BGYS'nin etkinliğinin düzenli olarak gözden geçirilmesi
- Arta kalan ve kabul edilebilir risklerin değerlendirilmesi
- Planlamış aralıklarda BGYS iç denetimlerinin gerçekleştirilmesi
- Olay ve hareketlerin kayıt edilmesi

Önlem Alma (BGYS'nin iyileştirilmesi)

- Tanımlanmış iyileştirme yöntemlerinin uygulanması
- İlgili düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi
- Faaliyetlerin sonuçlarının ilgili birimlerle paylaşılması
- İyileştirmelerin amaçlanan hedeflere ulaşmasının garanti altına alınması

Bilgi güvenliği yönetim sistemleriyle ilgili diğer bir İngiliz standardı Aralık 2005'te BS7799–3:2005 Bilgi Güvenliği Yönetim Sistemleri Risk Yönetiminin Kuralları ismiyle hazırlanmıştır. Standart 2006 yılında tekrar gözden geçirilmiş ve BS7799–3:2006 ismiyle yayınlanmıştır. BS7799–3 standardı BS7799–2 standardının uygulanması için destek sağlayarak ölçeklenebilir (küçük, orta veya büyük kurumlar) yapıda standardın yaygınlaşmasına yardımcı olması için geliştirilmiştir. Standard içerisinde risk değerlendirmesi, belirlenen risklere kontrollerin uygulanması, tanımlanmış risklerin izlenmesi, kontrol yönetim sistemlerinin bakımı gibi risk yönetimi ile ilgili konular üzerine odaklanılmıştır. Kapsamın belirlenmesi, kural oluşturan referanslar, terimlerin tanımı, kurum bağlamında risk, risk

değerlendirmesi, risk kararının verilmesi, risk yönetimi BS7799–3 standardının bölümlerini oluşturmaktadır [117].

3.4.2. ISO/IEC standartları

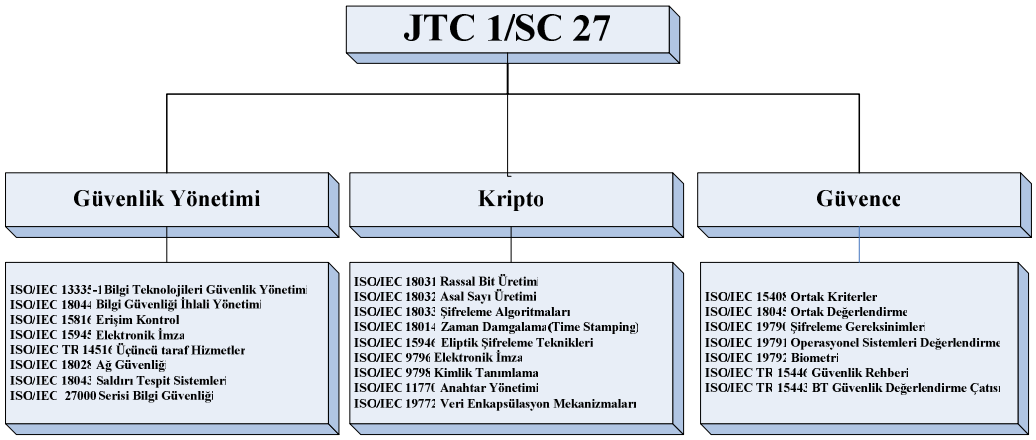
Uluslararası Elektroteknik Komisyonunu (The International Electrotechnical Organization-IEC) 1906 yılında Uluslararası Standartlar Organizasyonu (International Organization for Standardization-ISO) 1947 yılında uluslararası alanda ticari (ISO) ve elektroteknik (IEC) standardizasyonun sağlanması için, İsviçrenin Cenova şehrinde kurulmuştur [117]. ISO ve IEC birlikte teknik çalışma grupları oluşturarak (Joint Technical Committee-JTC) tüm dünyada geçerli olacak standartlar oluşturmaktadırlar. Bununla birlikte ISO tarafından IT Güvenlik Standartları ile ilgili çalışmalar JTC–1 Bilişim Teknolojileri Komitesine bağlı SC 27: BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bilgi güvenliği konusunda çalışan bu komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir [119].

- Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması
- Güvenlik teknikleri ve mekanizmalarının geliştirilmesi
- Güvenlik kılavuzlarının geliştirilmesi
- Yönetim destek dokümanları ve standartların geliştirilmesi

Yukarıda açıklanan görevleri yerine getirmek üzere bu komisyon içinde 5 ayrı çalışma grubu (Working Group) bulunmaktadır. Bu gruplar aşağıda belirtilmiştir.

- Çalışma Grubu–1 (JTC 1/SC 27/WG 1): Bilgi güvenliği yönetim sistemleri
- Çalışma Grubu–2 (JTC 1/SC 27/WG 2): Şifreleme ve güvenlik mekanizmaları
- Çalışma Grubu–3 (JTC 1/SC 27/WG 3): Güvenlik değerlendirme kriterleri
- Çalışma Grubu–4 (JTC 1/SC 27/WG 4): Güvenlik denetimleri ve hizmetleri
- Çalışma Grubu–5 (JTC 1/SC 27/WG 5): Kimlik yönetimi ve mahremiyet

1, 2 ve 3 nolu çalışma grupları ve sorumlu oldukları konular Şekil 3.4'de gösterilmiştir.



Şekil 3.4. ISO/IEC güvenlik çalışma grupları

SC27'ye bağlı çalışma gruplarından Çalışma Grubu–1 (WG1), Şekil 3.4.'de gösterilen bilgi güvenliği yönetim sistemleri standartları (ISO/IEC 17799, ISO/IEC 27000 Serisi) ile ilgili çalışmaları yürütmektedir. Bu standartlar aşağıda kısaca açıklanmıştır.

ISO/IEC 17799 standardı: BS–7799 standardının ikinci sürümü Mayıs 1999'da çıktığında ISO BSI'nın yayınladığı çalışmayla ilgilenmeye başlamıştır. Aralık 2000'de, ISO BS–7799 standardının ilk bölümünü alarak ISO/IEC 17779 olarak yeniden adlandırmış ve yeni bir standart olarak yayınlamıştır. ISO/IEC 17779 standardı daha önceki bölümde açıklanan BS–7799 standardının ilk bölümüne eşdeğerdir. Çizelge 3.2 standartların kullanımı ile ilgili seçenekleri göstermektedir [120].

Çizelge 3.2. Standartların kullanım amaçları

Şirket Tipi	Çalışan	Amaç
Küçük	<200	Bilgi güvenliği hakkında bilinçlendirme
Büyük	>200	Güvenlik sertifikası almak

ISO/IEC 17799 standardının uygulanmasıyla kurumsal bilgilerin tamamen güvende olduğunu söylemek doğru değildir. Bu standart bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan kurumların kullanımı için, bilgi güvenlik

yönetimi ile ilgili tavsiyeleri kapsar. ISO/IEC 17799 güvenlik standartlarını uyguluyor olmak kurumlara aşağıda açıklanan üstünlükleri sağlar.

Organizasyon Seviyesinde, sorumlulukları belirleyerek, kurumsal bilgi güvenliğinin her seviyede uygulanmasının yararlarını garanti eder.

Kanuni Seviyede, kurumun ilgili tüm kural ve yönetmeliklere uyduğunu yetkili makamlara göstererek diğer standart ve mevzuatları tamamlar.

İşletme Seviyesinde, Bilgi sistemleri, zafiyetleri ve nasıl korunacakları konusunda işletmenin yönlendirilmesini sağlayarak kurumsal bilgi sistemlerine daha güvenli erişim sağlanır.

Ticari Seviyede, iş ortakları, hissedarlar ve müşteriler; kurumun bilgi koruması konusuna verdiği önem sayesinde kuruma olan güvenleri artırır ve ticari rakipleri arasında piyasada farklı bir yere gelmesini sağlar.

Finansal Seviyede, güvenlik açıklarının belirlenerek önlem alınması sonucunda maliyetler azalacaktır.

Çalışan Seviyesinde, çalışanın güvenlik konuları ve organizasyon içinde kendisine düşen sorumluluk hakkındaki bilgisini arttırarak bireysel olarak bilinçlendirilmesini sağlar.

ISO/IEC 17799 standardı 2005 yılında revize edilerek ISO/IEC 17799:2005 ismiyle son halini almıştır. ISO/IEC 17799:2005 Bilgi Güvenliği Yönetimi için uygulama kodu, kuruluşların bilgi güvenliği yönetim sistemini kurmaları, uygulamaları, sürdürmeleri ve iyileştirmeleri için hazırlanmış bir kılavuz olup önceki sürümünden farklı olarak aşağıda kısaca açıklanan Bilgi Güvenliği İhlallerinin yönetimi ile ilgili bilgi güvenliği denetimlerini ve ilgili uygulamaları da içermektedir [121].

- *Bilgi güvenliği ihlallerinin yönetimi:* Yaşanan problemlerden, arızalardan, kazalardan ders çıkarılması ve tekrar yaşanmaması için gerekli önlemlerin alınması için gerekli olan yönetim mekanizmasının kurulmasını sağlar.

ISO 2005 yılında bir düzenlemeye giderek aşağıdaki tabloda gösterilen 27000 serisini bilgi güvenliğiyle ilgili standartlara ayırmıştır [122]. ISO/IEC 27000-27059 arasındaki standartlar ISO tarafından SC27 grubuna dâhil çalışma grupları için bilgi güvenliğiyle ilgili planlanan standartlara ayrılmıştır.

Çizelge 3.3. ISO 27000 serisi standartları

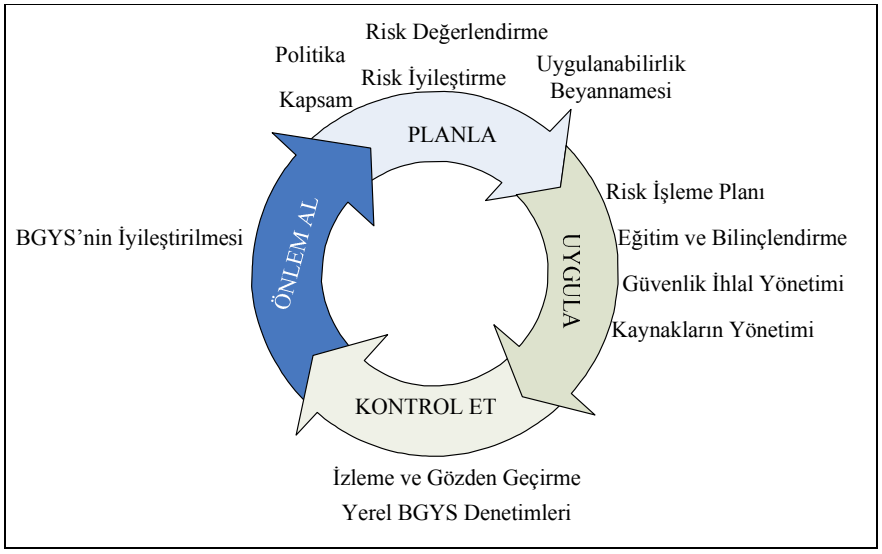
Standart Adı	Açıklaması
ISO/IEC 27000–27059	Bilgi güvenliğiyle ilgili standartlar için ayrılmış aralık
ISO/IEC 27000	BGYS standartları için genel bir sözlük (hazırlanıyor)
ISO/IEC 27001	BGYS ihtiyaçları (BS7799 Bölüm–2) (2005 yılında yayınlanmıştır)
ISO/IEC 27002	BGYS uygulama ilkeleri (ISO/IEC 17799:2005)
ISO/IEC 27003	BGYS uygulama rehberi (hazırlanıyor)
ISO/IEC 27004	BGYS metrikleri ve ölçüm (hazırlanıyor)
ISO/IEC 27005	BGYS risk yönetimi (hazırlanıyor)
ISO/IEC 27006	BGYS belge kaydı ve belgelendirme süreçleri kılavuzu (hazırlanıyor)
ISO/IEC 27007	BGYS izleme (Audit) için kılavuz (hazırlanıyor)
ISO/IEC 27031	ISO/IEC 17799/27002 standardının Telekom sektörü için uyarlanması (hazırlanıyor)

Çizelge 3.4'de gösterilen standartların hepsi yayınlanarak kullanıma açılmamıştır. Yayınlanan standarta ek olarak geliştirme ve düşünce aşamasında olan standartlara ait açıklamalar aşağıda verilmiştir.

ISO/IEC 27000, serisinde yer alan standartlar içerisinde geçen teknik terimler ve açıklamalarının yer aldığı genel bir sözlük formatında geliştirilmektedir.

ISO/IEC 27001, BGYS için gereklilikleri ortaya koyan bir standarttır. Bilgilerin düzenli olarak maruz kaldığı tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olur. BGYS kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için ISO/IEC 17799:2005 standartındaki kontrollerin uygulandığı süreçleri tanımlar. BS–7799 standartının ikinci bölümü üzerinde bazı iyileştirmeler ve değişiklikler yapılarak ISO/IEC Çalışma Grubu–1 tarafından 15 Ekim 2005 tarihinde standart olarak yayınlanmıştır. Bu standardın yayınlanmasından sonra İngiliz BS7799–2 standartı iptal edilmiş ve yerini ISO/IEC

27001 standartıyla içeriği aynı olan BS-ISO/IEC 27001 standardı almıştır. Bu standart kurumların büyüklüğüne bakılmaksızın BGYS kurulması bakım ve idamesi ile ilgili kurumlara yardım etme ve belgelendirme amacıyla oluşturulmuştur. ISO/IEC 27001 standardı yönetim standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirildiğinden yönetim standartlarının gereklerinide yerine getirmektedir. Standart, BS7799:2 standardının "Planla-Uygula-Kontrol Et-Önlem al" (PUKÖ) modelini esas alır. ISO/IEC 27001 standardının PUKÖ döngüsü Şekil 3.5'de gösterilmiştir.

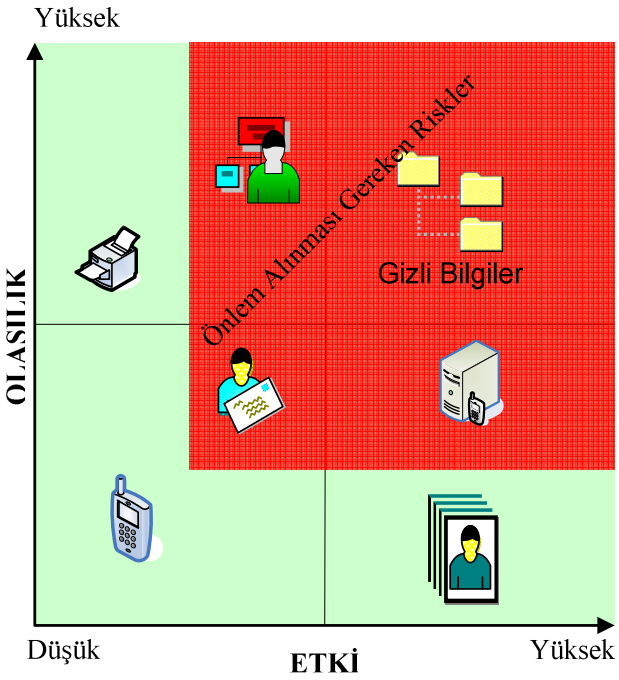


Şekil 3.5. ISO/IEC 27001 PUKÖ döngüsü [123]

PUKÖ döngüsünde yer alan kısımlar kısaca aşağıda açıklanmıştır [123]. Bunlar;

- *Kapsam*, daha önceki bölümlerde açıklandığı gibi kurumun tamamı veya belirli bir kısmını veya belirli bir hizmetini (internet bankacılığı, web uygulamaları, vb.) içerebilir.
- *BGYS Politikası,* bilgi güvenliği neden önemlidir? tehditler nelerdir? risk yönetimi nasıl yapılmalıdır? uyulması gereken kısıtlar (kanunlar yönetmelikler, vb.) nelerdir? Bu ve benzeri soruların cevabını içeren üst yönetici tarafından onaylanan bilgi güvenliği politikasının bir üst kümesi olarak kabul edilen kısa dokümanlardır.

- *Risk Değerlendirmesi,* kapsamında hangi bilgi varlıklarının korunacağı belirlendikten sonra kuruluşa uygun risk değerlendirme yönteminin seçilerek risklerin tanımlanması yapılır. Seçilen risk değerlendirme yöntemine göre bilgi varlıkları Şekil 3.6'da örneği gösterilen risk haritasında konumlandırılır.



Şekil 3.6. Risk değerlendirme haritası

- Riskler değerlendirildikten sonra risk değerlendirme haritasında, etkisi ve olasılığı yüksek olan tehditler için risklerin iyileştirilerek kontrol altına alınmasına ihtiyaç duyulmaktadır. Risk haritasında bilgi varlıklarının yeri değişebileceğinden risk değerlendirme haritası düzenli olarak güncellenmeli ve gerekli önlemler alınmalıdır.
- Risk iyileştirme, risklerin değerlendirilmesi tamamlandıktan sonra ISO/IEC 27001 standardı risklerin nasıl iyileştirileceğinin açıklanmasını ister. İyileştirme çalışmaları kapsamında risk kabul edilebilir, transfer edilebilir (sigorta, vb.), azaltma çalışmaları yapılabilir. Riskler karşısında alınması gereken önlemlerin bulunduğu dokümanlar risk iyileştirme planlarını oluşturmaktadır.

- Uygulanabilirlik beyannamesi (Statement of Applicability-SOA), ISO/IEC 27001:2005 standardındaki kontrollerden hangilerinin kullanıp kullanılmadığını nedenleriyle açıklayan belgelerdir. Kullanılan kontrollerin seçilme nedenleri, kullanılmayan kontrollerin dışarıda bırakılmasının açıklamasını içerir. Kullanılmayan kontrollerin yanlışlıkla çıkarılmadığının çapraz denetimini sağlar. Uygulanabilirlik beyannamesi risk yönetimini ilgilendiren kararların özetini sağlar.
- Risk işleme planı, güvenlik risklerini yönetmek için uygun yönetim eylemini, kaynakları, sorumlulukları ve öncelikleri tanımlar. Seçilen kontrollerin yapılabilmesi için gerekli olan alt kontroller gerçekleştirilerek kontrollerin etkinliği ölçülür. Yöneticiler ve personele alt kontrollerin planlanan kontrollerin ne kadar iyi düzeyde başardığına karar verme olanağı verir.
- Eğitim ve bilinçlendirme, programlarıyla kurumdaki tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin farkında olarak BGYS'nin amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olması sağlanmalıdır. Ayrıca BGYS'yi teknik olarak etkileyecek işlerde çalışmak üzere uzman personel istihdam edilmesi veya ilgili personelin eğitimleri bu kapsamda yapılır.
- Güvenlik ihlal yönetimi, güvenlik olaylarının anında tespit edilerek güvenlik ihlâllerine zamanında cevaplar verilmesini sağlar. Daha önce denenen ve başarılı olan güvenlik kırılmaları, güvenlik yöneticisinin güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığının belirlenebilmesi, güvenlik önlemlerinin alınarak güvenlik ihlallerinin önlenmesi, bir güvenlik kırılmasını önlemek için alınan önlemlerin etkili olup olmadığına karar verilir.
- Kaynakların yönetimi, kapsamında BGYS'yi kurma, gerçekleştirme, işletme, izleme, gözden geçirme, sürekliliğini sağlama ve iyileştirme için gereken kaynaklar kurum tarafından sağlanarak yönetimi yapılmalıdır.
- İzleme ve gözden geçirme, BGYS'nin etkinliğinin düzenli olarak gözden geçirilmesi ve oluşabilecek değişiklikleri (teknoloji, iş amaçları ve süreçleri, tehditler, vb.) dikkate alarak, bilgi varlıklarının risk değerlendirmesinin belirli aralıklarla yeniden yapılmasını sağlar.
- Yerel BGYS denetimleri, ilk taraf denetimleri olarak adlandırılan yönetim tarafından kapsamın uygun kalması ve süreçlerin iyileştirilmesini sağlamak için

düzenli olarak kuruluş tarafından veya kuruluş adına danışman firmalar tarafından gerçekleştirilir.

BGYS'nin iyileştirilmesi için kurum tarafından önleyici ve düzeltici tedbirler alınması gereklidir. Olumsuzlukların edilmemesi için, risk değerlendirme sonuçlarına bağlı olarak değişen riskler bazında önleyici tedbirler alınmalıdır. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. BGYS gereksinimleriyle olumsuzlukları gidermek üzere düzeltici önlemler alınmalıdır. Önleyici tedbirler için gerçekleştirilen faaliyetler çoğunlukla düzenleyici tedbirler için gerçekleştirilen faaliyetlerden daha az maliyetlidir.

ISO/IEC 27002, halen hazırlanma aşamasındadır. Bu standardın daha önceki bölümde açıklanan ISO/IEC 17799:2005 standardına eşdeğer olması beklenmektedir. Bilgi güvenliği ile ilgili standartların 27000 serisi altında yer almasından dolayı ISO/IEC tarafından öyle bir düzenlemeye gidilmiştir. Tahmini olarak 2007 yılı ortalarında yayınlanması beklenmektedir [124].

ISO/IEC 27003, 27001 standardının nasıl kullanılacağına dair açıklamalar ve örnekler içeren uygulama rehberi olarak geliştirilmekte olup tahmini olarak 2008 yılının ekim ayında standart olarak yayınlanması beklenmektedir. Geliştirilen standart içerisinde

- Giriş,
- Kapsam,
- Deyimler ve tanımlar,
- Kritik başarı faktörleri,
- Süreç yaklaşımı üzerine rehber,
- PUKÖ modeli rehberi,
- Planlama süreç rehberi,
- Uygulama süreç rehberi,
- Kontrol süreç rehberi,
- Önlem alma süreç rehberi ve

- Diğer kurumlarla birlikte çalışma

isimli konu başlıklarının yer alması beklenmektedir [125].

ISO/IEC 27004, halen geliştirilme aşamasında olan bu standart bilgi güvenliği yönetim metrikleri ve ölçümüne tahsis edilmiştir. Bilgi güvenliği yönetim sistemlerinin etkinliğinin ölçülmesi ve raporlanmasında kurumlara yardımcı olması beklenen bu standardın tahmini olarak 2007 yılsonu veya 2008 başlarında yayınlanması beklenmektedir [126].

ISO/IEC 27005, halen geliştirilme aşamasında olan bu standart BS 7799 Kısım–3 "BS 7799–3:2006 – Bilgi Güvenliği Yönetim Sistemleri – Bilgi Güvenliği Risk Yönetimi Kılavuzları" isimli İngiliz standardının ISO tarafından uyarlanması çalışmasını içermektedir. 2008 veya 2009 yılı içerisinde yayınlanması tahmin edilmektedir. BS 7799–3:2006 standardı 16 Mart 2006 tarihinde İngiliz standardı olarak kabul edilmiş, risklerin değerlendirilmesi, kontrollerin uygulanması, risklerin düzenli olarak izlenmesi ve gözden geçirilmesi gibi konu başlıklarını içermektedir [127].

ISO/IEC 27006, halen geliştirilme aşamasında olan bu standart "Bilgi Teknolojileri Felaket Önleme Hizmetleri Kılavuzu" ismiyle duyurulmuş ve tahmini olarak Kasım 2007 yılında yayınlanması planlanmaktadır [128].

ISO/IEC 27007, ISO 27001 standartına göre BGYS denetlemesinde kullanılacak kılavuz niteliğinde geliştirilmesi düşünülen bu standart 2009 yılında tamamlanması beklenmektedir [129].

ISO/IEC 27031, standardı ISO 17799/27002 standartı esas alınarak Telekom sektörü için geliştirilmektedir. 2007 yılı ortalarında ITU-T X.1051 ve ISO/IEC 27031 ismiyle yayınlanması beklenmektedir [130].

3.5. Türkiye'deki Bilgi Güvenliği Standartları

Türkiye'de bilgi güvenliği standartlarıyla ilgili çalışmalar ve belgelendirmeler, Türk Standartları Enstitüsü (TSE) tarafından yapılmaktadır. TSE teknik kurulunun ISO/IEC 17799:2000 standardını tercüme ederek 11 Kasım 2002 tarihinde aldığı karar ile TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri Türk standardı olarak kabul edilmiştir. TS ISO/IEC 17799 standardı, kuruluşlar bünyesinde bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlamak için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri içeren belgelerdir.

BGYS belgelendirilmesine yönelik TSE teknik kurulu tarafından yapılan çalışmalar sonucunda BS 7799–2:2002 standardının tercümesi yapılarak "Bilgi güvenliği yönetim sistemleri–Özellikler ve kullanım kılavuzu" ismiyle TS 17799–2 standardı olarak 17 Şubat 2005 tarihinde kabul edilmiş ve yürürlüğe girmiştir. Ancak TS ISO/IEC 27001:2006 "Bilgi teknolojisi–Güvenlik teknikleri-Bilgi güvenliği yönetim sistemleri–Gereksinimler", 2.3.2006 tarihinde Türk standartı olarak kabul edildiğinden TS 17799–2 standartı TSE tarafından iptal edilmiştir [101].

TS ISO/IEC 27001:2006 standardı, tüm kuruluş türlerini (örneğin, ticari kuruluşlar, kamu kurumları, kâr amaçlı olmayan kuruluşlar) kapsar. Bu standart, bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. Bu standart ISO/IEC 27001:2005 standardından yararlanarak hazırlanmıştır. ISO/IEC 27001:2005 standardın tercümesidir. Dünyada ve ülkemizde belgelendirme konusunda yapılan çalışmalar bir sonraki bölümde anlatılmıştır.

3.6. BGYS'de Belgelendirme

BGYS'de belgelendirme, kurumsal bilgi güvenliğinin standartlara uyumlu bir şekilde yönetildiğine dair otoriteler tarafından verilen sertifikasyonlar aracılığıyla

yapılmaktadır. Dünyada ve ülkemizde kurumsal bilgi güvenliği yönetim sistemlerinin sertifikalandırılmasında uyumluluğa esas teşkil eden standart 2005 yılına kadar BS7799–2 standardı olurken bu yıldan sonra ISO/IEC 27001 standardı olarak değiştirilmiştir. 15 Ekim ile 15 Nisan 2006 tarihine kadar olan hazırlık dönemi sırasında, denetimler ve belgelendirme ISO/IEC 27001:2005 veya BS 7799–2:2002 standartlarına göre gerçekleştirilmiştir. Ancak, bu süre içerisinde yayınlanmış olan yeni bir BS 7799–2:2002 sertifikasının, 15 Nisan 2007 tarihine kadar ISO/IEC 27001:2005'e geçişi tamamlanacaktır. 15 Nisan 2006 tarihinden sonra bütün denetimler ve belgelendirmeler ISO/IEC 27001:2005 standardına göre gerçekleştirilmiştir. BS 7799'a göre belgelendirilmiş olan kuruluşların, 15 Nisan 2007 tarihine kadar yeni standarda geçişlerini tamamlamaları gerekmektedir. 23 Temmuz 2007 tarihi itibariyle BS7799–2 sertifikasyonu geçersiz olacaktır. ISO/IEC 27001:2005 belgelendirmesi için geçilmesi gereken altı aşama aşağıda kısaca açıklanmıştır [131].

Aşama 1: ISO/IEC 27001:2005 standartının tüm gereklerinin yerine getirilmesi ve standartta belirtilen yönetim iskelet yapısının oluşturulması.

Aşama 2: Uyumluluk denetimleri için yetkilendirilmiş sertifikalandırma kuruma ön başvuru yapılır. Bu başvuruya istinaden denetimi yapacak firma belgelendirme için maliyet ve zaman çizelgesi sunar.

Aşama 3: Maliyet ve zaman çizelgesinin kurum tarafından onaylanarak denetimi gerçekleştirecek firmaya resmi başvuru yapılır.

Aşama 4: Denetimi gerçekleştirecek olan kurum güvenlik politikasını, risk değerlendirmesi dokümanlarını, risk eylem planını, uygunluk beyanını (SOA) ve güvenlik prosedürlerini içeren dokümantasyonu gözden geçirir. Bu işlem sonucunda, bilgi güvenliği yönetim sistemindeki sorunlu olan ve çözüme kavuşturulması gereken herhangi bir zayıflığın veya göz ardı edilen hususun ortaya çıkarılmasını sağlayacaktır.

Aşama 5: Masa üstü kontrol başarılı şekilde sonuçlandıktan sonra, denetim firmasının belirlediği denetçiler tarafından yerinde (on-site) denetim gerçekleştirilir. Kuruluşun büyüklüğüne ve iş tipine uygun kontrollerin olup olmadığı gözden geçirilir ve elde edilen sonuçlara göre kurumlara önerilerde bulunulur.

Aşama 6: Değerlendirmenin başarı ile tamamlanmasının ardından, Bilgi Güvenliği Yönetim Sisteminin kapsamını açık bir şekilde tanımlayan bir sertifika verilecektir. Bu sertifika 3 yıl boyunca geçerliliğini korur ve rutin değerlendirme ziyaretleri ile desteklenir.

ISO/IEC 27001 standardına göre kurulmuş olan bir bilgi güvenliği yönetim sisteminin varlığı, kurumların bilgi güvenliği yönetiminde, kapsamlı prosedürler aracılığıyla güvenlik kontrollerini sürekli ve düzenli olarak işletmeyi ve sistemin sürekli iyileştirilmesini gerektirmektedir. Güven ve güvenilirliğin hayati önem taşıdığı alanlarda hizmet veren kuruluşların, uluslararası geçerlilikte bilgi güvenliği yönetim sistemleri standardına uygunluk belgesine sahip olması, hem mevzuat hem de kuruluşun güvenli işleyişi açısından bir zorunluluk olarak değerlendirilmektedir.

Kurumların ISO/IEC 27001 sertifikası almasının avantajları aşağıda maddeler halinde listelenmiştir [132].

- *Kredilendirilebilirlik, güven ve itimat:* Belgelendirme, kurum veya kuruluşun bilgi güvenliğini dikkate aldığını, bilgi güvenliğinin sağlanması için gerekli olan adımları uyguladığını ve kontrol ettiğini ispatlamaktadır. Bu sayede kurumlar veya kuruluşlar birlikte iş yaptıkları veya hizmet verdikleri kurum veya bireylerin tüm bilgilerinin BGYS sayesinde güvende tutulacağı konusunda verdikleri taahhütten dolayı iş yaptıkları kurum, kuruluş veya bireylerin kendilerini güvende hissetmelerini sağlayacaklardır. Belgelendirme sonucunda özellikle özel sektör firmalarında rekabet anlamında sertifika almamış rakiplerinin bir adım önüne geçerek avantaj sağlayacaklardır. Ayrıca günümüzde uluslararası işlerin çoğunluğunda ISO/IEC 27001:2005 şartı koşulmaktadır.
- *Tasarruf:* Oluşabilecek güvenlik ihlallerine karşı kontrollerin uygulanması ile maliyetler düşmektedir. Sadece bir bilgi güvenlik ihlalinin çıkaracağı masraf bile

çoğu zaman çok büyük maddi zararlara yol açabilir. Belgelendirme işlemi kurumların maruz kalacağı bu tür ihlalleri azaltarak bilgi güvenliği ihlallerinden doğan zararları en aza indirecektir.

- *Yasal Uygunluk*: Belgelendirme işlemi, kanun ve tüzüklere uygunluğun yetkili ve ilgili makamlara yasal anlamda uygunluğun sağlandığına dair kanıt teşkil edilmesine yardımcı olur.
- *Taahhüt:* Belgelendirme işlemi, organizasyonun tüm aşamalarında taahhüt/bağlılığın sağlanması ve kanıtlanmasında yardımcı olur.
- *Operasyonel Seviye Risk Yönetimi:* Kuruluş genelinde, bilgi sistemleri ve zayıflıklarının nasıl korunacağı konusundaki farkındalık artar. Ayrıca donanım ve veriye daha güvenli bir şekilde erişim sağlanır.
- *Çalışanlar:* Çalışanların kuruluş içerisindeki sorumlulukları ve bilgi güvenliği konularındaki bilinçlerinin artmasını sağlar.
- *Sürekli İyileşme:* Düzenli olarak gerçekleştirilen güvenlik tetkiklerine bağlı olarak bilgi sistemlerinin etkinliği izlenecek ve izleme sonucunda tespit edilen problemler giderilerek bilgi sistemlerinde genel anlamda bir iyileşme hissedilecektir.
- *Onay:* Organizasyon için tüm seviyelerde bilgi güvenliğinin varlığının bağımsız kuruluşlar tarafından onaylandığını göstermektedir.

Kurumların bilgi güvenliği sertifikası verebilmesi için akreditasyon kurumları tarafından yetkilendirilmesi gerekmektedir. BS7799–2 standardı için yetkili olan akreditasyon kurumu, İngilteredeki UKAS (United Kingdom Accreditaion Service), ISO/IEC 27001 standardı için ise ISO kurumudur. BGYS sertifikaları bilgi güvenliği yönetim standartlarına göre kurumları denetleyen ve değerlendiren akredite edilmiş belgelendirme kurumları tarafından verilmektedir.

Belgelendirme Kurumu gerektiğinde değerlendirme sürecini denetler, değerlendirmenin ilgili standarta uygunluğunu garanti ederek değerlendirmeleri başarılı olan kurumlara sertifikalarını verir. Dünya genelinde akredite edilmiş sertifikasyon kurumlarına örnekler Çizelge 3.4'de gösterilmiştir [133]. Çizelge 3.4'de Türkiye'de BGYS sertifikası veren TSE'nin adının geçmediği görülmektedir. Bu durumda TSE tarafından verilen belgelerin sadece ulusal olarak geçerli olduğu

görülmektedir. Belgelendirilen BGYS sistemi her geçen gün hızlı bir şekilde artmaktadır. Ülkelere göre belge sayısı incelendiğinde dünya genelinde toplam 182 adet ISO/IEC 27001 sertifikası olduğu bunların 73 adedinin BS 7799–2 güncellenmesiyle alınan sertifikalar geriye kalan 109 tanesi ise yeni alınan sertifikalar olduğu görülmektedir [134]. Önümüzdeki yıllarda çoğu sektörde kurumlara bilgi güvenliğini sağladıklarına dair belgelendirme şartının getirileceği düşünüldüğünde bu sayının çok daha fazla olacağı aşikârdır.

Çizelge 3.4. BGYS belgelendirme kurumları

Akredite Edilmiş Sertifikasyon Kurumları	
(1). AJA	(29). KPMG RJ
(2). BM TRADA	(30). KPMG SA
(3). BSI	(31). LRQA
(4). BSI-J	(32). LTSI SAS
(5). BVQI	(33). Moody
(6). BVQI Japan	(34). MSA
(7). Bureau Veritas.	(35). National Quality Assurance
(8). Center Teknologisk	(36). Nemko
(9). Certification Europe	(37). PJR (Perry Johnson Registrars)
(10). CIS	(38). PJR-J
(11). CQS	(39). PSB Certification
(12). BSK	(40). RINA S.p.A.
(13). DNV	(41). TUV NORD CERT GmbH
(14). DQS GmbH	(42). SAI Global Limited
(15). DS Certification	(43). SEMKO-DEKRA Certification
(16). Intertek Systems	(44). SFS-Inspecta Certification)
(17). ISOQAR	(45). SGS ICS Limited
(18). JACO	(46). SGS Philippines Inc.
(19). JATE	(47). SIRIM QAS International
(20). JICQA	(48). SQS (Swiss Quality System)
(21). JMAQA	(49). STQC IT Certification Services
(22). JQA	(50). TECO
(23). JSA	(51). TÜV Rheinland Group
(24). JUSE-ISO	(52). TÜV RJ
(25). J-VAC	(53). TÜV SÜD Gruppe
(26). KEMA Quality BV	(54). UIMCert
(27). KPMG Audit plc	(55). United Registrar of Systems Ltd
(28). KPMG Certification	

Özellikle iş süreçlerini elektronik ortamlara taşıyan kurumlarda bu ihtiyacın daha da fazla olacağı tahmin edilmektedir. Türkiyedeki sertifika sayısı dünya geneline

bakıldığında ortalamaların üzerinde görülmesine rağmen yetersizdir. Türkiyedeki kurumlar ve sahip oldukları sertifikalar ise Çizelge 3.5'de gösterilmiştir [134].

Çizelge 3.5 Ülkemizde BGYS sertifika durumu

Kurum Adı	Denetçi	Standart Adı
Beko Elektronik A.Ş.	SGS	BS 7799-2:2002
Corbuss Kurumsal Telekom Servis Hizmetleri A.Ş.	BSI	ISO/IEC 27001:2005
E-Kart Elektronik Kart Sistemleri San. ve Tic. A.Ş.	BVQI	ISO/IEC 27001:2005
Global Bilgi Pazarlama, Danışma	BSI	ISO/IEC 27001:2005
İstanbul Gaz Dağıtım Sanayi ve Ticaret A.Ş.	BVQI	BS 7799–2:2002
Siemens Business Services	SGS	BS 7799–2:2002
TUBİTAK UEKAE Kamu Sertifikasyon Merkezi	SGS	BS 7799–2:2002
Türk Traktör ve Ziraat Makineleri A Ş.	BSI	ISO/IEC 27001:2005
TÜRKTRUST Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.	SGS	BS 7799–2:2002
Tusas Aerospace Industries	BVQI	ISO/IEC 27001:2005
E-Güven	TSE	TS 17799–2 BGYS
EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.	TSE	TS ISO/IEC 27001 BGYS
Sermaye Piyasası Kurulu	TSE	TS ISO/IEC 27001 BGYS

Ülkemizde "E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları" kılavuzu içerisinde yer alan 4.1.1 Bilgi Güvenliği Yönetim Sistemi (BGYS) maddesine göre kurumlara Bilgi Güvenliği Yönetim Sistemi kurması tavsiye edilmekte ve ihtiyaç sahibi kurumların kendi bünyelerinde BGYS'ye sahip olmaları ve BGYS'yi tamamlayan kurumlara, sertifika belgelendirme çalışmaları yapmaları önerilmektedir [135]. Buradan da anlaşılacağı gibi önümüzdeki yıllarda ülkemizde BGYS sistemlerinin fazlalaşması ve bunun sonucunda BGYS sertifikası sayısında da artış olacağı değerlendirilmektedir.

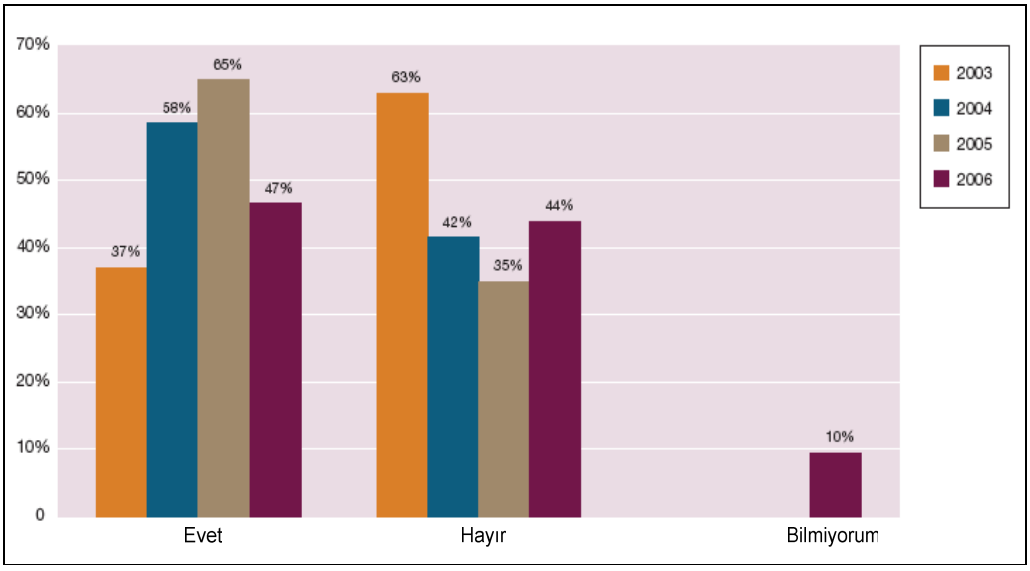
3.7. Dünyada ve Türkiye'de BGYS

Bu bölümde BGYS ile ilgili dünyada ve Türkiyede yapılan araştırmalara yer verilmiştir. BGYS konusunda literatür tarandığında yapılan araştırmaların azlığı

dikkat çekmektedir. Bunun sebebi yeni bir konu olan BGYS konusunda kuruluşların farkındalığının henüz istenilen seviyede olmamasıdır. Bu bölümde Avustralya, Malezya ve Türkiyede BGYS konusunda yapılan araştırmalardan bahsedilmiştir. Diğer ülkelerle ilgili BGYS konusunda yapılan araştırmalara rastlanılmadığından bu bölümde sadece bu ülkelerle ilgili açıklamalara yer verilmiştir.

Avustralya'da 2006 yılında polis teşkilatları tarafından oluşturulan AusCERT isimli çalışma grubu tarafından yapılan anket çalışmasının bir bölümünde katılımcılardan BT standartları ile ilgili verilen soruları cevaplandırmaları istenilmiştir. Anket çalışmasının BGYS'yi ilgilendiren kısımları aşağıda maddeler halinde açıklanmıştır [136].

- Katılımcılara kurumlarında kullanılan veya referans alınan bilgi güvenliği standartları sorulmuştur. Katılımcıların verdikleri cevaplar Şekil 3.7'de gösterilmiştir.

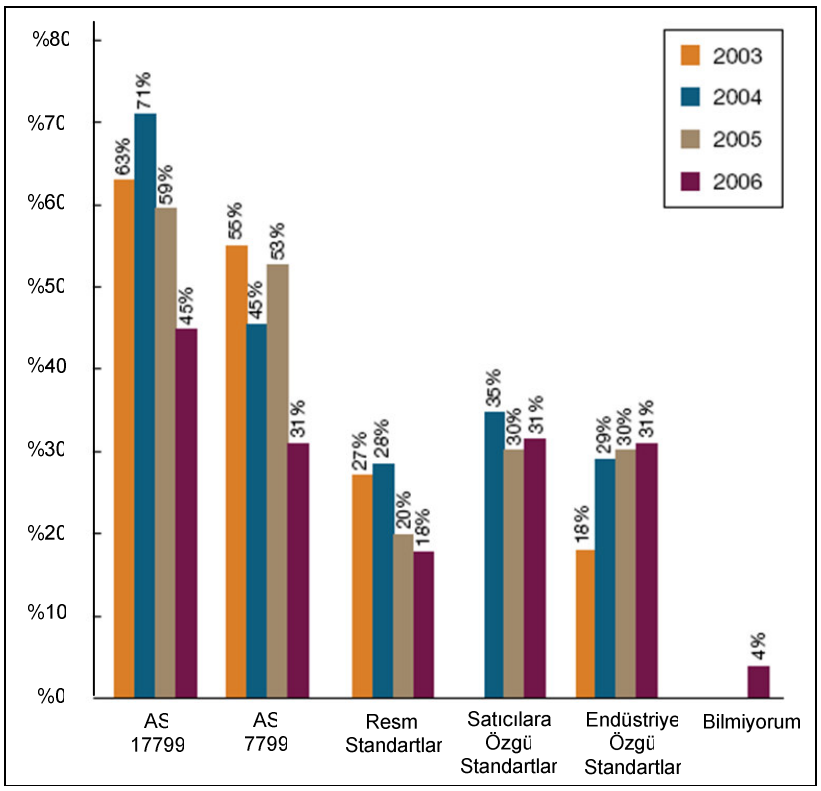


Şekil 3.7. Bilgi güvenliği standart kullanımının yıllara göre dağılımı [136]

2005 yılındaki standart kullanım oranı %65'ten 2006 yılında %47'ye düşmüştür. Bu düşüş standartların kurumların beklentilerine cevap vermemesi olarak yorumlanabilir.

Standart kullandığını belirten katılımcılara kurumlarında hangi standartları kullandığına dair soruya verilen cevaplar Şekil 3.8'de gösterilmiştir.

Kurumlar tarafından 2003 yılından beri en çok kullanılan standardın ISO 17799 standardına denk gelen AS17799 standardı olduğu Şekil 3.8'de görülmektedir. 2006 yılında kurumlar tarafından endüstriye özgü standartlara kaymalar olduğu gözlenmektedir. Tüm kurumlara özgü ve genel içerikli olan AS17799 standardından kurumların iş alanlarına özgü standartlara kaydığı görülmektedir.

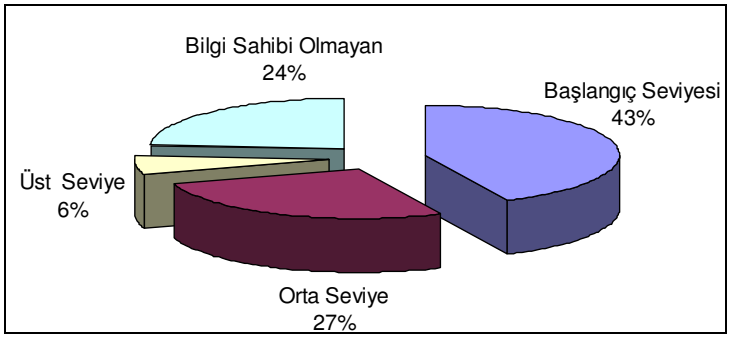


Şekil 3.8. Yıllara göre kullanım dağılımları [136]

BGYS konusunda diğer bir anket çalışması Malezya'da 2003 yılında yapılmıştır. Çalışmanın tarihi eski olmasına rağmen içerik bakımından sadece BGYS konusunda yapılmış bir çalışma olması bu çalışmanın önemini artırmaktadır. Malezyada NISER (National ICT Security & Emergency Response Centre) tarafından e-posta daveti aracılığıyla çevrimiçi anket olarak yapılan bu çalışmaya devlet, finans, perakende,

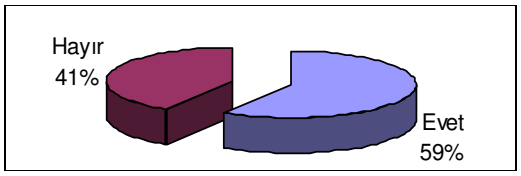
üretim ve telekomünikasyon sektöründen yüz kurum katılmıştır. Çalışmanın sonuçları aşağıda maddeler halinde özetlenmiştir [137].

- Katılımcıların BGYS farkındalık seviyesinin ölçülmesi amacıyla sorulan soruda çoğunluk %43 gibi bir oranla BGYS hakkında başlangıç seviyesinde bilgiye sahipken BGYS hakkında hiçbir fikre sahip olmayanların sayısı Şekil 3.9'da gösterildiği gibi %24 olarak belirlenmiştir.



Şekil 3.9. BGYS farkındalık seviyeleri

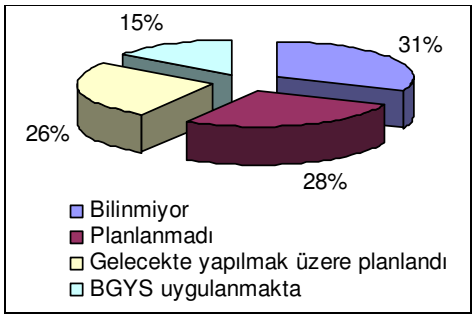
- Şekil 3.10'dan görüleceği gibi katılımcıların %59'ı bilgi güvenliğini yönetmenin en iyi yolunun kurumlarında BGYS uygulaması olduğunu belirtmişlerdir. Bu soruya evet cevabı veren katılımcıların %86'sı BGYS uygulanması sonucunda daha güvenli bir çalışma ortamı kurulacağını, %78'i ise iç ve dış güvenlik ihlâllerinin azalacağı yönünde görüş belirtmişlerdir.



Şekil 3.10. Bilgi güvenliği yönetiminde BGYS uygulaması

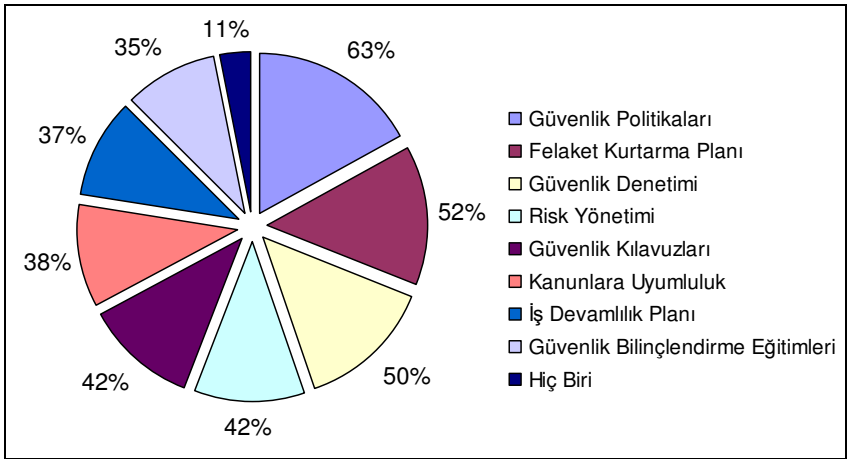
- Katılımcıların %31 gibi büyük bir oranı kurumlarında BGYS uygulamaları konusunda kararsızken %28'i ise BGYS'yi ne zaman uygulayacağı konusunda herhangi bir plana sahip değildirler. Herhangi bir plana sahip olmayan kurumların %57 gibi yüksek bir oranı, BGYS sistemlerinin kurumlarında uygulanabilirliği için

çalışmalara ihtiyaç olduğunu, %32'si ise kaynak yetersizliğini sebep göstermiştir. Kurumların BGYS planlamasına ait grafik Şekil 3.11'de gösterilmiştir.



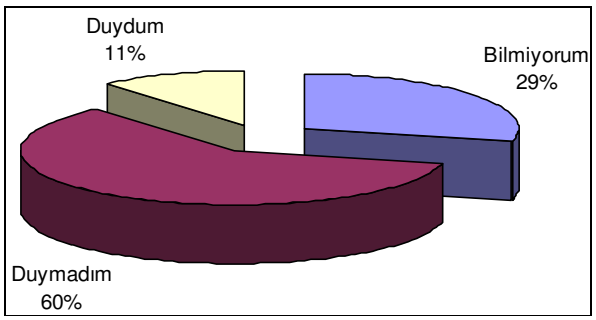
Şekil 3.11. BGYS planlaması

- Kurumların güvenlik ihlâllerinin önlenmesi için kullandıkları çözümlerin başında %63 oranıyla güvenlik politikaları, ikinci olarak %52 oranıyla felaket kurtarma planı üçüncü sırada ise %50 oranıyla güvenlik denetimleri gelmektedir. Ayrıca katılımcıların %62'si BGYS sistemlerinin uygulanması sonucunda güvenlik ihlâllerinin önlenebileceğini belirtmişlerdir. Güvenlik ihlâllerinin önlenmesine yönelik kurumlar tarafından kullanılan çözümler Şekil 3.12'de gösterilmiştir.



Şekil 3.12. Güvenlik ihlâllerinin önlenmesinde kullanılan çözümler

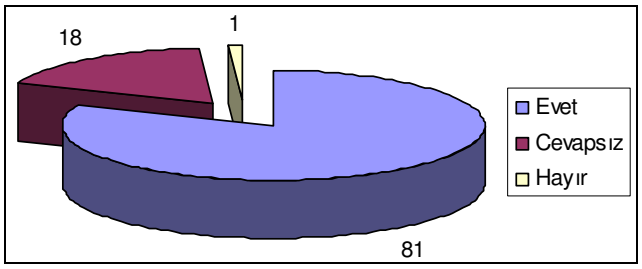
- Katılımcılara Malezyada çalışan BGYS uygulamasından haberdar olup olmadıkları yönünde yönetilen soruya Şekil 3.13'de gösterildiği gibi %60 gibi büyük bir kesim çalışanın BGYS uygulamasından haberdar olmadığını söylemiştir.



Şekil 3.13. Çalışan BGYS uygulamalarından haberdarlık

Dünyada olduğu gibi ülkemizdede bu alanda yapılan araştırmalar yok denecek kadar azdır. Türkiyede BGYS konusunda TÜBİTAK tarafından 2006 yılında kamu kurumları için yapmış olduğu çalışmanın sonuçları aşağıda kısaca özetlenmiştir [100].

- Katılımcılara ISO 17799 standardının kurumlarına faydalı olup olmayacağı yönündeki soruya Şekil 3.14'de gösterildiği gibi %81 gibi büyük bir oranda standardın kurumlarına faydalı olacağı konusunda görüş bildirmişlerdir.



Şekil 3.14. ISO 17799 standardından fayda beklentileri

- Katılımcıların %43'ü, kurumlarında ISO 17799 ile ilgili bir planları olmadığını %92'si yıl içerisinde, %11'i ise iki yıl içerisinde almayı planladıklarını belirtmiştir.

Yapılan araştırmalar değerlendirildiğinde dünyada ve ülkemizde BGYS konusunda kurumlar tarafından istenen düzeyde olmasa da farkındalık oluştuğu ancak uygulama konusunda yeterli olmadığı yapılan anket çalışmalarından anlaşılmaktadır.

3.8. Genel Değerlendirme

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için, teknik önlemlerin yanında teknik olmayan (insan faktörü, prosedürel faktörler, vb.) önlemlerin ve denetimlerin alınması, tüm bu süreçlerin devamlılığının sağlanılması ve bilgi güvenliği standartlarına uygun olarak yönetilebilmesi amacıyla yönetim tarafından desteklenen insanları, iş süreçlerini ve bilişim teknolojilerini kapsayan bilgi güvenliği standartlarına uygun olarak BGYS kurmaları gerekmektedir. Bilgi güvenliği standartları kurumların kendi iş süreçlerini bilgi güvenliğine yönelik risklerden korumaları ve önleyici tedbirleri sistematik biçimde işletebilmeleri ve standartların gereğini yerine getiren kurum veya kuruluşların belgelendirilmesi amacıyla geliştirilmiştir.

Ülkemizde genellikle güvenlik politikaları standartlara uygun olmadan yazılı veya sözlü, onaylı veya onaysız bir biçimde kuruluşlar tarafından uygulanmakta ve çoğu kurum tarafından da bilgi güvenliği yönetimi için yeterli görülmektedir. Bu yanlış anlamanın giderilmesi için dünya genelinde kabul görmüş ve uygulanabilirliği test edilmiş bilgi güvenliği standartları esas alınarak kuruluşların bilgi güvenliği yönetimi konusunda eksikliklerini gidererek BGYS kurmaları ve belgelendirilmeleri gerekmektedir. BGYS çerçevesinde oluşturulacak güvenlik politikalarına üst yönetim ve tüm çalışanların destek vermesi ve tavizsiz bir şekilde uygulanması, işbirliğinde bulunulan tüm kişi ve kuruluşlarında bu politikalara uyma zorunluluğu, kurumsal bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir faktördür.

BGYS standartlarının kurumlara uyarlanması, anlatılması, kullanıcı, teknik çalışanların ve yöneticilerin eğitilmesi konusunda kuruluşların danışmanlık hizmetleri almaları gerekmektedir. BGYS uygulamaları kurumlar tarafından başarılı bir şekilde uygulandıktan sonra kuruluşların bilgi güvenliğini yönettiklerine dair uluslararası alanda geçerli olan belgeler alması bilgi güvenliğinin kritik olduğu kurumlar açısından önemli bir göstergedir.

Bilgi güvenliğinin yönetilmesi bilgi güvenliğinin sağlandığı anlamına gelmemektedir. BGYS'nin kurumsal bilgi güvenliğini taahhüt ettiği seviyede

sağlayıp sağlamadığı, sağlamıyorsa eksikliklerinin neler olduğu, güvenlik denetimlerinin güvenli biçimde kurulup kurulmadığı, güvenlik denetimlerinin etkin ve politikalara uygun olarak uygulanıp uygulanmadığı, iyi bir belgelendirme yapılıp yapılmadığı gibi bilgi güvenliğinin sağlanması açısından çok kritik olan soruları cevaplamanın tek yolu BGYS kapsamında belirlenen bilgi varlıklarının (insan faktörü, bilişim teknolojileri, vb.) güvenliğini sızma testleriyle test etmekten geçmektedir.

Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında sızma testlerinin katkısı çok yüksektir. Sızma testleri felaket başa gelmeden önce, onu önleyecek ve ona karşı savunulacak ihtiyaçların ve tedbirlerin alınmasında kullanılan önemli bir erken uyarı sistemidir. Bu önemden dolayı, sızma testleri takip eden bölümde detaylı bir şekilde incelenmiş ve kurumsal bilgi güvenliğinin sağlanmasındaki rolü kapsamlı bir şekilde sunulmuştur.

4. SIZMA TESTLERİ

Bu tezin ilk üç bölümünde detaylı olarak açıklandığı gibi, bilgi ve bilgi güvenliğinin kişisel ve özellikle kurumsal tarafta istenilen seviyede yapılıp yapılmadığını bilmek, varsa mevcut zafiyetleri açığa çıkarmak, açık kapıları bulmak, uygulanan politikalarda yeni açıklar olup olmadığını anlamak amacıyla belirli zaman dilimlerinde sistemlerin gözden geçirilmesi amacıyla yapılan veya yapılması gereken etik testler sızma (penetration) testleridir.

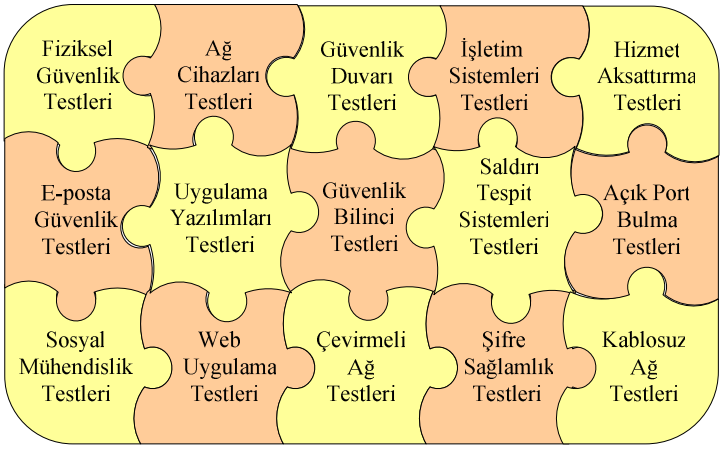
Yapılan incelemelerde ülkemizde sızma testleriyle ilgili herhangi bir tez çalışmasıyla karşılaşılmamış olması sebebiyle, öncelikle literatürdeki mevcut tanımlar gözden geçirilmiştir. Daha sonraki bölümlerde sızma testlerinin amaçları, sınıflandırılması, kapsamı ve sınırları, kullanılan yaklaşımlar, test teknikleri, test aşamaları ve test aşamalarında kullanılan araçlar sırasıyla açıklanmıştır.

Tez çalışmasının esasını teşkil eden sızma testleri, bu bölümde ayrıntılı bir şekilde incelenmiştir. Sızma testleri bilgisayar sistemlerinin güvenliğini değerlendirmede kullanılan en eski yöntemlerden birisidir. 1970'lerin başında A.B.D Savunma Bakanlığı, daha güvenli sistemler oluşturmak için yazılımların geliştirilmesindeki ve bilgisayar sistemlerindeki güvenlik zayıflıklarının gösterilmesinde bu yöntemi kullanmıştır. “Bilişim sistemlerinde sızma testi” kavramı 1995 yılında geliştirilen ve ilk Unix tabanlı ilk zafiyet tarama sistemi olan “SATAN” programıyla birlikte kullanılmıştır [138].

Daha önceki bölümlerde de açıklandığı gibi kurumsal bilgi sistemlerinin güvenliği sadece teknik önlemlerin alınmasıyla sağlanamaz. Teknolojik sebeplerden kaynaklanmayan konularda bilgi sistemlerinin güvenliğini tehdit etmektedir. Sızma testleriyle sınanan bilgi sistemleri teknik (bilişim sistemleri, doküman yönetim sistemleri, süreç analizleri, vb.) ve teknik olmayan (çalışanların bilinci, kurum kültürü, yönetimsel prosedürler, fiziksel güvenlik vb.) etkenler dikkate alınarak bir bütün olarak değerlendirilmelidir. Sızma testleri değişen risklere paralel olarak periyodik zaman aralıklarında tekrarlanmalıdır. Tekrarlama zaman dilimi kurumların bilgi dinamikleri dikkate alınarak belirlenmelidir. Genel kanaat yılda iki kere

yapılması yönündedir. Bu süre zarfında işe yeni başlayan veya işinden yeni ayrılan personel, kurumsal bilgi envanterine yeni katılan veya envanterden çıkarılan bilgi varlıkları, yeni yapılan binalar ve buna benzer nedenlerle meydana gelebilecek olan yeni zafiyet ve açıklıkların ortaya çıkarılması sızma testlerinin periyodik olarak yapılmasının yanında yeniden yapılmasınıda zorunlu kılmaktadır.

Genel bir fikir vermesi amacıyla sızma testlerinde kullanılacak güvenlik testleri Şekil 4.1'de verilmiştir. Bu şekilde sızma testlerinin gösterimi bir yapboz şeklinde tarafımızdan ifade edilmiştir. Sızma testlerine bir bütün olarak bakılması içlerinden herhangi birinin yapılmaması ve üstün körü yapılması kurumsal bilgi güvenliğini zafiyete uğrtacağından bu testlerin tamamlayıcı olduğu dikkate alınmalıdır. Bu yüzden şekilsel olarakta dikkat çekici olması için bu gösterim tercih edilmiştir.



Şekil 4.1.Sızma testlerinde kullanılan güvenlik testlerinin yap-boz gösterimi

Sızma testleri kapsamında uygulanması gereken testlerin ne olduğu, nasıl ve hangi metotlarla yapılması gerektiği takip eden alt başlıklar içerisinde ayrıntılı olarak açıklanmıştır.

4.1. Tanımlar

Literatürde sızma testleriyle ilgili yapılan tanımlardan önemlileri aşağıda özetlenmiştir.

- Bilgisayar ağı ve ağ kaynaklarındaki zafiyetlerin tespit edilerek bilgi sistemlerinin güvenlik seviyesini değerlendirmek üzere hazırlanan testlerdir. Çoğu zaman etik amaçlı saldırılar (Ethical Hacking) olarak da adlandırılır [139].
- Açık kapı bulma sanatıdır [140].
- Bilgisayar ağlarının güvenliğini artırmak, yeni zafiyet ve sömürüleri ortaya çıkarmak, bilgi sistemlerinin ne derece güvende olduğunu anlamak üzere yapılan testlerdir [141].
- Kurum veya kuruluşların güvenliğini sağlamak amacıyla gerçek dünyadaki saldırı ve saldırgan mantığıyla bilgi sistemlerinin ne derece güvende olduğunu anlamak üzere bilgisayar ağlarına yetkisiz erişim sağlamak için yapılan testlerdir [142].
- Yetkili kişiler tarafından bilinen zafiyetlerin sistematik ve planlı olarak kullanılmasıyla bilgi kaynaklarına (uygulamalar, bilgisayarlar, bilgisayar ağları ve bileşenleri) yapılan kontrollü saldırılardır [143].
- Bilgi güvenliği ölçümlerinin yapılmasını sağlayan bir yöntemdir [144].
- Saldırganların yapabileceğine benzeyen kötücül saldırılar yapılarak bilgisayar sistemlerinin ve ağlarının güvenliğinin değerlendirilmesi yöntemidir [145].
- Güvenlik danışmanları (Ethical Hacker) tarafından sistem veya ağ üzerinde saldırganların hangi tür açıkları tespit edebileceği ve açıklara dayalı bilgilerle neler yapabileceklerinin görülmesi amacıyla yapılan güvenlik testleridir [146].
- Bilgisayar ağları üzerinde saldırganların beceri ve teknikleri kullanılarak, var olan zafiyetlerin uzak konumlardan bulunması amacıyla ağların taranması, tarama sonuçlarının incelenmesi, var olan zafiyetlerin kötüye kullanılması ve son olarak zafiyetin giderilmesi amacıyla yapılan güvenlik testleridir [147].
- Bilgi varlıklarının (uygulamalar, bilgisayar ağları, bilgisayar sistemleri) güvenlik durumunu değerlendirmek için zafiyet, yapılandırma hataları, zayıflıklar yönünden saldırgan teknikleri ile analiz edilmesi sürecidir [148].
- Kurumlar tarafından saldırılar ve yetkisiz erişimlerden bilgisayar sistemlerinin nasıl korunacağıyla ilgili zafiyetlerin değerlendirilmesinde kullanılan ortak bir yoldur [149].

- Koruma sistemlerinin sahip olduğu zayıflıkların gösterilmesi amacıyla yapılan sızmalardır [150].
- Teknik donanımlı ehil kişiler tarafından yapılan sistematik testlerdir [151].
- Sızma testlerinin amacı güvenliğin test edilmesi olup, kurumsal bilgi sistemlerinin kırılması olarak algılanmamalıdır [152].
- Güvenli Hesaplama Esaslarının (TCB) güvenlik seviyesinin değerlendirmede kullanılan yöntemlerden bir tanesidir [153].

Yukarıda yapılan tanımlar dikkate alındığında, bizde kişisel tanımımızı şu şekilde yapabiliriz. Kurumsal bilgi varlıklarının (bilişim sistemleri, insan faktörü, iş süreçleri) zayıflık ve zafiyetlerinin saldırgan gözüyle ortaya çıkarılarak giderilmesi amacıyla belirli zamanlarda, yazılımlar, donanımlar ve insanlar üzerinde işinin ehli bir ekip tarafından yapılan etik testlerdir. Sızma testlerinde kullanılacak güvenlik testleri Şekil 4.1'de gösterilmiştir.

4.2. Sızma Testlerinin Amaçları

1974 yılında Paul A. Karger ve Roger R. Schell tarafından yazılan "zafiyet analizi", 1975 yılında Richard R. Linde tarafından uluslararası bir konferansta sunulan "işletim sistemleri ve sızma testleri" isimli bildiriler literatürdeki bu konuyla yapılmış ilk çalışmalardır [154]. O günden bu güne, kurumsal bilgi güvenliğinde sızma testlerinin kullanımı ve önemi gün geçtikçe artmaktadır. Yapılan bu testlerin ortak amacı, kurumsal bilgi varlıklarına ait güvenlik tehditlerinin (zayıflıklar, zafiyetler, yapılandırma hataları, vb.) kötü niyetli saldırganlardan önce belirlenerek gerekli güvenlik önlemlerinin kurumlar tarafından alınmasına yardımcı olmaktır. Sızma testlerinin amacı kötü niyetli kişilerin yetkisiz erişimlerini engellemek amacıyla zafiyetlerin tanımlanarak giderilmesidir [155]. Sızma testleri kurumlar tarafından çok çeşitli amaçlar için pek çok alanda kullanılmaktadır. Bu testler;

- Yeni zafiyetlerin bulunması,
- Tasarım zayıflıklarının belirlenmesi,
- Güvenilir kurum imajının korunulması,
- Bilgi güvenlik politikalarının gözden geçirilmesi,

- Bilgi güvenliği sertifikasyonlarına uyumda sürekliliğin sağlanması,
- Etkili ve bilinçli güvenlik yatırımının yapılması,
- Güvenlik yatırımlarının geri dönüşümünün mümkün olduğunca yüksek olması,
- Teknik personelin sorumluluğunun gözden geçirilmesi,
- Kurumsal bilgi sistemlerine yapılabilecek olan muhtemel saldırı veya saldırılara karşı güvenliğimizi sürekli olarak yüksek seviyede sağlamak

için yapılmaktadır. Yukarıda maddeler halinde açıklanan sızma testlerinin amaçları aşağıda sırasıyla açıklanmıştır.

Yeni zafiyetlerin bulunması, güvenlik satın alınacak bir ürün değil devamlılık gerektiren bir süreçtir [156]. Gelişen teknolojilerin, geliştirilen teknik ve yaklaşımların kullanılması beraberinde sistem güvenliği üzerinde yeni kullanım, zafiyetler oluşabilmektedir. Bu yaşayan süreçte meydana gelebilecek yeni zafiyetler (kurtçuklar, işletim sistemi açıkları, virüsler, protokol açıklıkları, personel, vb.) belirli periyotlarda yapılan sızma testleriyle tespit edilerek gerekli önlemler alınır.

Tasarım zayıflıklarının belirlenmesi, bilgi sistemlerinin mantıksal veya fiziksel tasarımları yapılırken tasarımcılar çoğunlukla güvenlik önlemlerini atlamakta veya gereken önemi vermemektedirler. Örneğin yazılımların kodlanması aşamasında yazılımcı kod yazarken programa dış dünyadan yapılacak veri girişlerinin doğrulanması işini çok dikkate almamaktadır. Bu dikkate alınmadığı için ise büyük güvenlik ihlalleri (SQL enjeksiyonu, siteler arası kod çalıştırma, vb.) yaşanabilmektedir. Tasarım zayıflıkları konusunda çok rastlanan bir başka örnek ise ağ tasarımları yapılırken ağ bileşenlerinin (router, switch, hub, kablo, panel, fiber optik kablo sonlandırıcıları) fiziksel güvenliğin düşünülmemesi (kilitsiz dolaplar, kilitsiz odalar, vb.) sonucu yetkisiz kişilerin aktif cihazlar üzerinden bilgilere erişerek bilgi güvenliğinin ihlal edilmesi verilebilir. Fiziksel güvenlik ihmal edildiği takdirde, yönlendiricinin saldırıya uğraması (hack edilmesi), verilerin dinlenmesi, hizmetin durması gibi ciddi güvenlik ihlalleri meydana gelebilecektir. Mantıksal ve fiziksel tasarımlardan kaynaklanan açıklıkların güvenlik ihlallerine dönüşmeden önce sızma

testleriyle tespit edilerek önlemlerin alınması üst düzeyde kurumsal bilgi güvenliğinin sağlanması açısından önemlidir.

Güvenilir kurum imajı, elektronik ortamlarda iş yapan kurum ve kuruluşların en büyük sermayelerinden birisidir. Müşteri sayısının artması ve mevcut müşterilerin korunması ancak ve ancak "güven" veya "güvenirlik" duygusunun sürekliliğidir. Elektronik ortamlarda kurumların bu imajını sağlamlaştırmaları için saldırıya uğramadan veya zafiyetlerle karşılaşılmadan önce önlemler alarak, maddi ve manevi kayıpları engelleyebilirler. Bunun için ise sızma testleri önemli bir yer tutmaktadır.

Bilgi güvenlik politikalarının oluşturulmasında, kurumsal bilgi sistemlerinin güvenliğini tehlikeye atan tehditler sızma testleriyle tespit edildikten sonra risk değerlendirmeleri ve risk analizleri yapılır. Risk analiz sonuçları kurumsal bilgi güvenliği politikaları içerisinde yer alan prosedürler ve standartların oluşturulması için yapılan çalışmalara teknik bir dayanak oluşturur.

Kurumsal bilgi güvenliği sertifikasyonları, daha önceki bölümlerde anlatılan kurumsal bilgi güvenliği yönetim sistemlerinin oluşturulması ve işletilmesi adımlarda kurumsal bilgi varlıklarına ait güvenlik risklerinin tespiti ve analizi çalışmalarına yardımcı olur. Meydana gelebilecek başka açıklarının ve risklerinin güvenlik uzmanları tarafından önceden belirlenmesine katkılar sağlar.

Güvenlik yatırımının yapılması, ile çoğu kuruluş çoğu kuruluşta kurumsal bilgi güvenliğinin en üst seviyede sağlanacağını düşünmektedir. Mesela bir güvenlik duvarı ve antivirüs yazılımlarının satın alınmasıyla güvenliğin tamamen sağlanacağı düşünülmektedir. Ancak kurumsal bilgi güvenliğinin sağlanabilmesi için sadece antivirüs ve GD yazılımının yanında ağ ve host tabanlı IDS/IPS (Intrusion Detection / Prevention Systems), kişisel bilgilerin gizliliğinin sağlanması için gerekli olan koruma sistemleri, e-posta temelli antivirüs yazılımları, içerik filtreleme, spam posta filtreleme, casus yazılım engelleme ve eğitim gibi yatırımların da yapılması gerekmektedir. Bu yatırımların tamamının yapılmaması, yapılsa bile doğru yapılandırılması veya yapılmamasından kaynaklanan zayıflıklar sızma testleriyle

ortaya çıkartılarak gerekli yatırımların doğru etkili ve bilinçli bir şekilde yapılması konusunda yönetime yol gösterir.

Güvenlik yatırımlarının geri dönüşümünde, sızma testleri önemli rol oynamaktadır [157]. Sızma testleri sayesinde doğru güvenlik yatırımları yapılması kurumların maddi ve manevi anlamda kâr etmelerini, saygınlığının, itibarının ve güvenilirliğinin artmasını sağlayacaktır. Günümüzde kurumların çoğu, kurum dışındaki çalışanlarıyla (satış mühendisleri, şubeler, vb.) veya iş ortaklarıyla internet üzerinden güvensiz bir şekilde haberleşmektedirler. Bu haberleşmenin güvensiz ortamlar üzerinden yapılması, kurumların gizli bilgilerinin saldırganlar tarafından çalınması riskini beraberinde getirmektedir. Örneğin, satış personelinin çok önemli bir ihale için yaptığı fiyatlandırmalar ticari sır niteliği taşıyan bir bilgidir. Satış personelinin ihaleye ait dokümanları hazırlayıp kurumdaki ilgili kişilere internet ortamından güvensiz bir şekilde yollaması sırasında fiyatların rakip firma tarafından ele geçirilmesi hiçbir kurumun istemeyeceği bir olaydır. Bu olayın farkına varılması çok zordur. Ancak bu ve bunun gibi güvensiz ortamlardaki bilgi kaçakları sızma testleriyle belirlenebilir. Sızma testleri sonucunda oluşturulan raporlarla dayanarak yapılan doğru güvenlik yatırımları sayesinde daha sonra meydana gelebilecek kayıpların önüne geçilmesi sağlanabilir.

Güvenlik zafiyetlerinin erken tespitinde sızma testleri önemli rol oynamaktadır. Günlük hayatımızdan bir örnek verecek olursak, çoğu ölümcül hastalıkların tedavisinde erken teşhisin çok önemli bir yeri vardır. Erken safhalarda bu tip hastalıkların tespiti için ayrıntılı tetkiklerin (check-up) düzenli aralıklarla yapılmasına ihtiyaç duyulur. Örneğin kadınlar arasında en sık görülen bir kanserin erken teşhisinde ve tedavisinde yılda bir kere yapılan tetkikin (pab smear) bu kanserin yayılmasında ve önlenmesinde etkili olduğu kanıtlanmıştır [158]. Sızma testleri bilgi sistemlerinin güvenliğinin sağlanması konusunda önceden tetkikler yapılmasını sağlayarak gelecekte meydana gelebilecek onarılamaz felaketlerin önlenmesinde veya en aza indirgenmesinde önemli bir rol oynar.

Teknik personelin verimliliğinin ölçümü, üst düzeyde güvenliğin sağlanması için önemlidir. Çalışanlar bilgi eksiklikleri ve çalışma motivasyonlarının düşük

olmasından kaynaklanan, bilerek veya bilmeden önemli hatalar yapmaktadırlar. Çalışanların hatalarına örnek olarak düzenli olarak yedek alınmaması veya alınan yedeklerin test ortamlarında sınanmamış olması, bilgi sistemlerinin üretim esnasında verilen varsayılan (default) şifre ve yapılandırmalarla kullanıma alınması, yayınlandığı halde yazılımlara ait güncelleme ve yamaların yapılmaması, güvenlik yazılımlarındaki kural hataları, gereksiz servislerin kapatılmaması, imza tabanlı güvenlik yazılımlarının veritabanlarının güncel tutulmaması gibi kusurlar gösterilebilir [159]. Sızma testleriyle bu tip hatalar tespit edilerek alınması gereken önlemlerin ne olduğu kurumlara bildirilir. Kurum tarafından sızma testleri sonucuna bakılarak teknik çalışanların becerisi ve motivasyonu değerlendirilerek eksik olunan noktalar tespit edilerek çalışanlardaki bilgi eksiklikleri giderilir.

4.3. Sızma Testlerinin Sınıflandırılması

Sızma testlerinin sınıflandırılabilmesi için dikkate alınan kriterler bu bölümde ayrıntılı bir şekilde açıklanmıştır. Bu kriterler Çizelge 4.1.'de gösterilen, test başlangıç bilgisi, bilgi sistemleri üzerinde oluşturduğu etkiler, teste yaklaşım yöntemleri, testte kullanılan yöntemler (teknik, teknik olmayan) ve testin yapılacağı yer olarak sıralanabilir.

Çizelge 4.1. Sızma testlerinin sınıflandırılması

Kriterler	Sızma Testinin Türü		
Başlangıç Bilgisi ve Yetkisi	Yok	Kısıtlı	Detaylı
Sisteme Etkisi	Pasif	Normal	Aktif
Kapsam	Genel	Sınırlı	Özel
Yaklaşım	Gizli	Açık	Karma
Başlangıç noktası	Kurum dışı	Kurum içi	Karma
Test Teknikleri	Teknolojik	Teknolojik olmayan	Karma

Kurumların istek ve ihtiyaçları doğrultusunda Çizelge 4.1'de yer alan bilgilere dayanarak hangi türde sızma testlerinin yapılacağına güvenlik uzmanları tarafından karar verilir. Örneğin bir kurumda sadece dışarıdan gelecek saldırılar önemliyse testi yapacak kişi veya kişilerin başlangıçta kurum hakkında ekstra bir bilgiye sahip olmaları gerekmemektedir. Çizelge 4.1'de yer alan kriterler sırasıyla aşağıda altbaşlıklar halinde açıklanmıştır.

4.3.1. Başlangıç bilgisi ve yetkisi

Sızma testleri uzman kişilerden oluşan test takımları tarafından yapılmaktadır. Test takımının sızma testi uygulanacak kurum hakkında başlangıç bilgisi üç farklı düzeyde olabilir. Eğer test başlangıcında kurumsal bilgi sistemleri hakkında test takımına hiç bir bilgi ve yetki verilmemişse kara-kutu, bir çalışanın sahip olduğu ölçüde sınırlı bir bilgi ve yetki verilmişse gri-kutu, kurumsal bilgi sistemlerinin tamamı hakkında bilgi ve yetki verilmişse beyaz-kutu testi olarak adlandırılır [160]. *Kara-kutu testlerde*, test takımı kurumla ilgili bilgileri kamuya açık alanlardan (internet, dergi, kitap, gazete, vb.) çeşitli bilgiler (kurumun web sayfasının adı, kullandığı IP adres aralıkları, vb.) toplar. Sonrasında bu bilgileri anlamlandırarak test için gerekli aşamalarda kullanır. *Gri-kutu testlerde*, test takımı bir kurum çalışanı ile aynı bilgi ve haklara (kurumun geçmişi, kurumsal kültür, fiziki mekânlara erişim, kullanıcı adı ve şifresi, vb.) sahiptir. *Beyaz-kutu testlerde*, test takımı bilgi sistemleri hakkında üst derece bilgilere (iş-akışı, doküman yönetim sistemi, işletim sistemlerinin listesi, veritabanı yazılımı platformları, bilgisayar ağı haritası, aktif cihazlar, güvenlik duvarı bilgileri vb.) sahiptir. Kara-kutu testler kurum dışından gelebilecek, gri ve beyaz kutu testler ise kurum içinden gelecek veya kurum içine sızmış saldırganlardan kaynaklanabilecek tehditlerin boyutunu ortaya çıkartması açısından önemlidir.

4.3.2. Sızma testlerinin sistemler üzerinde etkisi

Sızma testleri yapılırken sistemler üzerinde etkilerinin önceden planlanması gereklidir. Testlerin sistemlere olan etkisini pasif, normal ve aktif olmak üzere 3 seviyede sınıflandırabiliriz. Bu testlerde;

Pasif testlerde, port ve zafiyet tarayıcıları gibi yazılımlarla elde edilen zayıflıklar ve zafiyetler sadece raporlanır.

Normal testlerde, tespit edilen zafiyetlerin tanımlanması ve kullanılması, zayıf parolaların tespiti ve kırılması, bellek taşması gibi yöntemler kullanıldığından sistemlerde bazı anlarda kısa süreli aksamalar veya yavaşlamalar meydana gelebilir.

Aktif testler, elektronik ortamda verilen hizmetlerin aksamasını veya durmasını sağlayan hizmet aksattırma testleri (denial of service), kötü amaçlı yazılımların çalıştırılması (trojan, worm, virüs, vb.), web sayfalarının değiştirilmesi, veritabanı içindeki bilgilerin değiştirilmesi veya silinmesi, yönlendiricilerin çökertilmesi gibi tamamen bir saldırganın yapabileceği tüm saldırıları içerir. Aktif testler uygulanmadan önce tam yedekler alınmalı ve sistemlerin sanal bir kopyası çıkarılmalıdır. Kurumlar açısından çok kritik olan bilişim sistemlerine ait sızma testleri çalışan sistemlerin bire bir aynısı olan sanal kopyaları üzerinde uygulanması gerekmektedir.

4.3.3. Test kapsamı ve sınırları

Sızma testlerinde kapsamlar belirlenirken sistemlerin en az zarar görmesi, iş sürekliğinin sağlanması gibi nedenlerden dolayı testlere sınırlamalar getirilmelidir. Sızma testlerine getirilecek olan sınırlamalar, planlama aşamasında aşağıda örnekleri verilen sorulara kurumlar tarafından verilen cevaplara göre yapılmalıdır. Bunlardan bazıları;

- Testler mesai saatlerinde mi veya mesai saatleri dışında mı yapılacak?
- Hizmet aksattırma saldırıları düzenlenecek mi?
- Sistemler üzerinde arka kapılar (truva) yüklenmesine izin verilecek mi?
- Kayıt dosyaları silinecek mi?
- Testlerden çalışanlar haberdar olacak mı?
- Sosyal mühendislik testleri yapılacak mı eğer yapılacaksa hangi teknikler kullanılacak?

olarak verilebilir.

Kurumsal bilgi varlıklarının hangilerinin test edileceği, testin amacına uygun olarak belirlenen kapsamlar çerçevesinde belirlenir. Sızma testleri ilk defa yapılıyorsa kurumsal bilgi varlıklarının tamamının kapsam içine alınması, kurumsal bilgi güvenliğinin genel bir değerlendirilmesinin yapılması açısından önemlidir. Test

kapsamları genel olarak genel, sınırlı ve odaklı olmak üzere üç farklı grupta incelenebilir. Bunlar aşağıda kısaca açıklanmıştır.

Genel kapsam içerisinde kurumların tüm bilgi varlıklarına ek olarak, bilgi alışverişinde bulunulan kurumlar, iş ortakları, danışmanlık alınan firmalar test kapsamı içerisine dâhil edilir. Bu kapsamı seçen kurumların amacı kurumsal bilgi trafiklerinin tamamının denetlenerek kurumun genel bir güvenlik resminin çıkartılması ve güvenlik seviyelerinin ne düzeyde olduğunun belirlenmesidir. Bu ilk kez yapılacak güvenlik testleri için uygun bir yaklaşımdır.

Sınırlı kapsam içerisinde kurum tarafından belirlenen alan veya alanlar dikkate alınarak testler yapılır. Merkez binaların test edilmesi, bilişim ortamlarının test edilmesi gibi genele göre daha sınırlı alanların test edilmesi sınırlı kapsama örnek olarak gösterilebilir. Sınırlı kapsamda amaç çok geniş ölçekli kuruluşlarda kurumsal bilgi varlıklarının parçalara ayrılarak sırasıyla test edilmesi esasına dayanır.

Odaklanmış kapsam kurumlar açısından kritik olan ve iş süreçlerini birinci derecede etkileyen bilgi varlıklarının derinlemesine ve dikkatlice test edilmesini içerir. İnternet erişim firmaları için erişilebilirliği, bankalar için bütünlüğü, askeri kurumlar için bütünlük ve gizliliği etkileyen faktörlerin gözönüne alınarak kapsamın belirlenmesi odaklanmış kapsama örnek olarak verilebilir.

4.3.4. Yaklaşımlar

Sızma testlerinin gerçekçi sonuçları vermesi için testlerin bazı aşamalarında gizlilik bazı aşamalarında şeffaflık önemlidir. Sızma testlerinin uygulanmasında testlerin gizliliği, test sonuçlarının doğruluk oranını önemli derecede etkiler. Çalışanların güvenlik bilincinin gerçek anlamda ölçülebilmesi için kendinden bilgi almak isteyen test ekip üyesinin farkında olmamalıdır. Önemli sunucuların performansını düşürecek, beklenmedik hatalar oluşturacak ve geri dönüşü olmayacak şekilde kayıplara sebebiyet verebilecek testlerin uygulanmasında ise şeffaflık testlerin sonucunda meydana gelebilecek istenmeyen sonuçların en az indirgenmesi veya kısa zamanda telafi edilebilmesi için önemlidir. Örneğin sunucular ve üzerinde çalışan

servisler test edilirken, sistem yöneticisinin bu testlerden haberinin olması ortaya çıkabilecek olumsuz durumlarda olaylara acil bir şekilde müdahaleye hazır olması gereklidir.

4.3.5. Test konumu

Kurum içinden veya kurum dışından yapılan sızma testleri testlerin konumunu belirler. Kurum içinden yapılan testler iyi niyetli olmayan kullanıcılar veya kurum içerisinde sızmış yerel saldırganlar (internal hacker) tarafından kullanılabilecek olası zayıflıkların ortaya çıkarılmasını sağlar. Kurum dışından yapılan testlerde ise dış dünyadan gelebilecek tehditler ve zayıflıkların belirlenmesi hedeflenmektedir. Kurum dışından yapılan testlerde test ekibinin başlangıçtaki bilgisi dış dünyadaki bir saldırgana eşdeğerken, kurum içinden yapılan testlerde ise test ekibi başlangıçta bilgi sistemleri hakkında detaylı bir bilgiye sahiptir. Kurum içinden yapılan testlere örnekler aşağıda verilmiştir [161]. Bunlara;

- Yetkisiz olarak bilgi kaynaklarına erişme ve bu kaynakları kullanma,
- Yerel alan ağ mimarisinin belirlenerek ağ topolojisinin oluşturulması,
- Ağ cihazlarının yapılandırılmasının değiştirilmesi,
- Web sayfasının değiştirilmesi,
- Güvenlik duvarı kurallarının atlanması (by-pass),
- Yetki seviyesinin değiştirilmesi,
- Yerel alan ağındaki bilgilerin dinlenmesi ve değiştirilmesi,
- Çalışanlar adına e-posta atılması,
- Antivirüs yazılımlarının sistemden kaldırılması,
- Parola kırma testlerinin yapılması,
- Sunucu dayanıklılık (stres) testleri,
- Fiziksel olarak yapılan erişim ihlâllerinin test edilmesi ve
- Kurum içi bilgi güvenliği farkındalık testleri (sosyal mühendislik)

gibi örnekler vermek mümkündür.

Günümüzde yapılan araştırmalardan ve yayınlanan raporlardan [95–100, 136–137] saldırıların büyük bir kısmının yerel saldırganlar tarafından kurum içerisinden yapıldığı belirtilmektedir. Kurum içindeki bir saldırganın verebileceği zararları tespit etmek (kurum içi sızma testleriyle) kurumsal bilgi güvenliğinin üst seviyede sağlanması açısından büyük önem taşımaktadır.

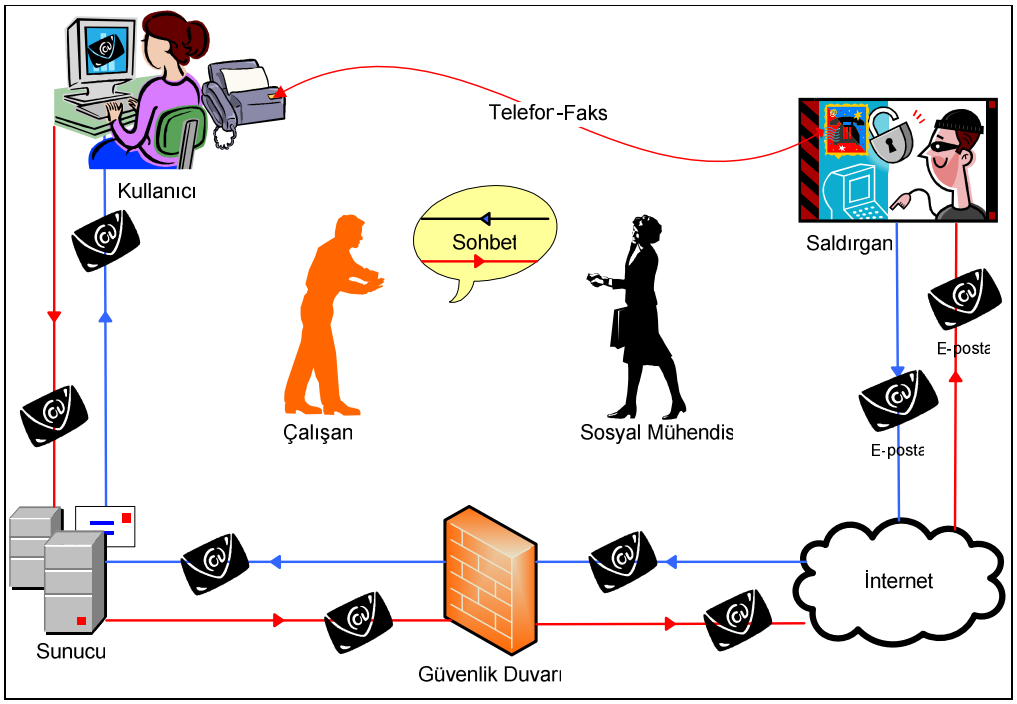
Kurum dışından yapılan sızma testlerinde ise genellikle; güvenlik güncellemeleri yapılmamış, güvenlik programları yanlış yapılandırılmış, güvenlik dikkate alınmadan geliştirilmiş web uygulamaları, kullanıcıların bilmedikleri ama cazip başlıklı e-postalar (spam, phishing, hoax, vb.), bilgi ve bilinç eksikliğinden kaynaklanan insan hatalarının araştırıldığı sosyal mühendislik testleri karşısında çalışanların davranışlarının ortaya çıkartılması, gibi kurumsal bilgi güvenliğini doğrudan etkileyecek unsurlar üzerinde yoğunlaşılmaktadır.

4.3.6. Test yöntemleri

Kurumsal bilgi güvenliğinin üst seviyede sağlanabilmesi amacıyla kullanılan sızma testlerinin uygulanmasında kullanılan yöntemler teknik ve teknik olmayan testler olarak iki grupta incelenir. Bu yöntemler aşağıda kısaca açıklanmıştır.

Teknik olmayan testler, teknolojik ürünler yerine insanların zafiyetlerinden faydalanılarak kurumsal bilgi varlıkları hakkında bilgi ve belge toplamak için yapılan testlerdir. Teknik olmayan testlerin başında sosyal mühendislik (social engineering) testleri gelmektedir. Sosyal mühendislik (toplum mühendisliği), yalan söyleme ve ikna etme üzerine kurulan inandırma ve bilgi toplama sanatıdır [162]. Sosyal mühendislik testlerinden sonuç alabilmek için farklı yöntemler kullanılmaktadır. Bu yöntemlerden en çok kullanılanı telefon yoluyla taklit ve ikna yöntemidir. Sosyal mühendisliğin başarılı olabilmesi için testi yapan kişilerin, ikna ve taklit yeteneği yüksek, her türlü cevaba ve soruya kendini hazırlayan, hazır cevap, ses tonuyla kişiler üzerinde olumlu etkiler bırakan, kendini iyi pazarlayan, ikna edici senaryo yazan, kişilerin zafiyetlerinin farkında olan, iyi derecede iletişim kabiliyetine sahip insanlar olmalıdır. İnsan-makine, makine-makine, insan-yazılım, yazılım-yazılım,

korsan-karma (makine, yazılım, insan) arayüz ortamları sosyal mühendislik vakaların yaşanabileceği muhtemel ortamlardır.



Şekil 4.2. Bir resim içerisinde sosyal mühendisliğin temsili gösterimi

Şekil 4.2'de sosyal mühendislik tek bir resim içerisinde temsili olarak gösterilmektedir. İlk yöntem olarak, saldırgan bilgisayar başından hazırladığı sazan postalarla kullanıcıyı kandırmakta ve istediği bilgilere ulaşabilmektedir. İkinci bir yöntem ise saldırgan farklı bir iletişim ortamı olan telefon veya faks cihazları üzerinden yapılan kandırmacalarla istediği bilgilere ulaşabilmektedir. Sosyal mühendislik testlerinin en etkili yöntemlerinden birisi olan üçüncü yöntemde ise sohbet ortamlarında, sosyal mühendis sohbet ortamlarında hissettirmeden istediği bilgilere karşısındaki insanı yönlendirici konuşmalar yaparak ulaşmaktadır. Sosyal mühendisler genellikle bakımlı, iyi giyimli, şık, konuşması düzgün karşısındaki insanı etkileyeci bir görünüme sahiptirler.

Sosyal mühendislik testlerinde kullanılan diğer bir yöntem ise *çöplük karıştırma* (dumpster diving) diye tabir edilen testlerdir. Kurumların kırtasiye çöplerinde bulunabilecek ve tam anlamıyla imha edilmemiş dokümanlar üzerinde geçerliliğini

yitirmemiş bilgiler sayesinde kurumlar hakkında önemli bilgilere ulaşılabilir. Kırtasiye atıklarıyla ilgili olarak kurumlar tarafından yapılan hatalara örnek olarak, ortak kullanıma açık olan yazıcılarda çıktıların karışmaması için kullanıcının ismi, dokümanların adının yazılı olduğu ve genellikle çıktı sahibi tarafından direkt olarak çöpe atılan kâğıtlar vardır. Bu kâğıtlar sayesinde kurumun kullanıcı profili ve üzerinde çalıştığı konu başlıkları hakkında fikir sahibi olunabilir. İkinci örnek olarak, aynı dokümanın çalışma sonuçlanıncaya kadar çok defa çıktısı alınır ve her defasında üzerinde değişiklik yapılarak bir önceki kopya çöpe atılır. Ancak, çöpe atılan dokümanlar hala geçerliliğini korumakta ve yapılan çalışmalar hakkında detaylı bilgiler içermektedir. Üçüncü örnek olarak, küçük notların yazıldığı ve üzerinde genellikle önemli hatırlatıcı bilgilerin yer aldığı küçük kâğıtlar üzerine yazılı bilgi notları vardır. Bu bilgi notları telefon numaraları, adresler, toplantı notları, kullanıcı adı ve şifreleri içerebilir.

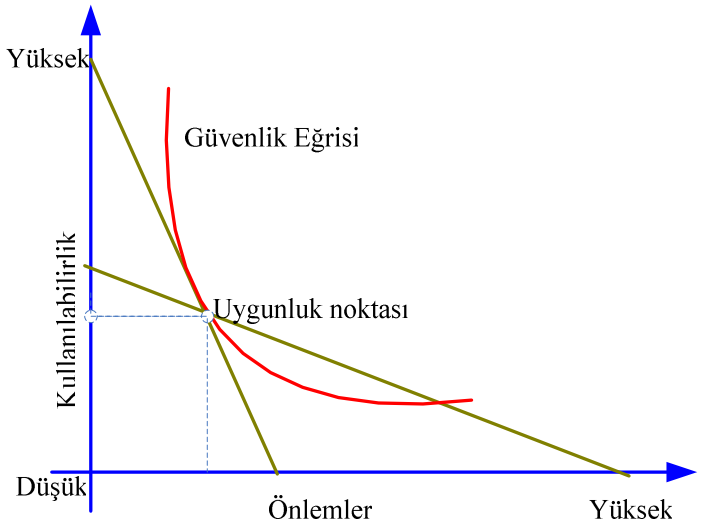
Yaşanmış bir örnek olarak, Oracle bilgisayar yazılım şirketi, özel bir dedektiflik bürosundan (Investigative Group International-IGI) kendileri için bir soruşturma yapmasını talep etmiş ve danışman şirket bu kapsamda Microsoft'a yakın olduğu belirtilen bir kuruluş olan Association for Competitive Technology (ACT) için çalışan temizlik işçilerinde şirketin çöpleri karşılığında rüşvet teklifinde bulunmuştur [163]. Danışman şirket sosyal mühendislik yöntemi olan çöp karıştırma sayesinde Microsoft hakkında ticari ve teknik konuların yer aldığı birçok bilgiye bu yöntemle ulaşmak istemiştir.

Sosyal mühendislik testlerinde kullanılan diğer bir yöntem ise *masaüstü testleridir*. Kişilerin masalarında bıraktığı ve herkes tarafından kolaylıkla okunabilecek bilgi notları, açık bırakılan bilgisayar ekranları, evrakların kilitli olmayan ortamlarda muhafaza edilmesi sonucunda kurum ve kişiler açısından çok değerli bilgiler rahatlıkla elde edilebilir. Masaüstü testleri, çalışanlar masasında otururken ve masasından ayrıldıktan sonra yapılabilir. Çalışanlar masadayken göz ucuyla civarda veya masa üzerinde bulunan bilgi notlarına bakmak, şifresini bilgisayara girerken gözetlemek (omuz sörfü), çalışanların masadan uzaklaşmasıyla parola korumalı

ekran koruması olmayan bilgisayara girmek, kilitli olmayan dolapları açmak şeklinde yapılabilir.

Örnek olarak, şifrelerin saldırganlar tarafından kırılmasını zorlaştırmak amacıyla karmaşık şifre politikası (şifrelerin büyük harf, küçük harf, rakam, noktalama işaretlerini içermesi) uygulanmakta olan bir kurumda bazı kullanıcılar şifrelerini unutmamak için kâğıtlara yazarak bilgisayar ekranının üstünde veya her an görebileceği bir yerde muhafaza etmek isteyeceklerdir. Teknik olarak kırılması zor olan şifrelerin sosyal mühendislik testleriyle çok daha kolay bir şekilde elde edilmesi sosyal mühendisliğin ne kadar ciddi bir tehdit olduğunu göstermektedir. Sosyal mühendislikle ilgili birçok yaşanmış olay Mitnick ve Simonun Aldatma Sanatı isimli kitabından [162] elde edilebilir.

Vurgulanması gereken çok hassas bir nokta ise, kullanıcılar tarafından uygulanabilirliği çok düşük, aşırı güvenlik kontrollerinin güvenlik açıklarına yol açmasıdır. Güvenlik denetimleri ve uygulanabilirlikleri arasındaki hassas dengeler gözetilerek Şekil 4.3'de gösterildiği gibi güvenlik önlemlerinin alınması gerekmektedir. Güvenlik ile kullanılabilirlik arasındaki hassas dengenin, kurumların güvenlik ihtiyaçları doğrultusunda kurulmalıdır.



Şekil 4.3. Güvenlik ve kullanılabilirlik arasındaki ilişki

Şekil 4.3'de verildiği gibi güvenliğin sağlanması için alınan önlemler ile kullanılabilirlik arasında ters bir orantı vardır.

Çizelge 4.2. Sosyal mühendislik testleri ve alınması gerekli önlemler

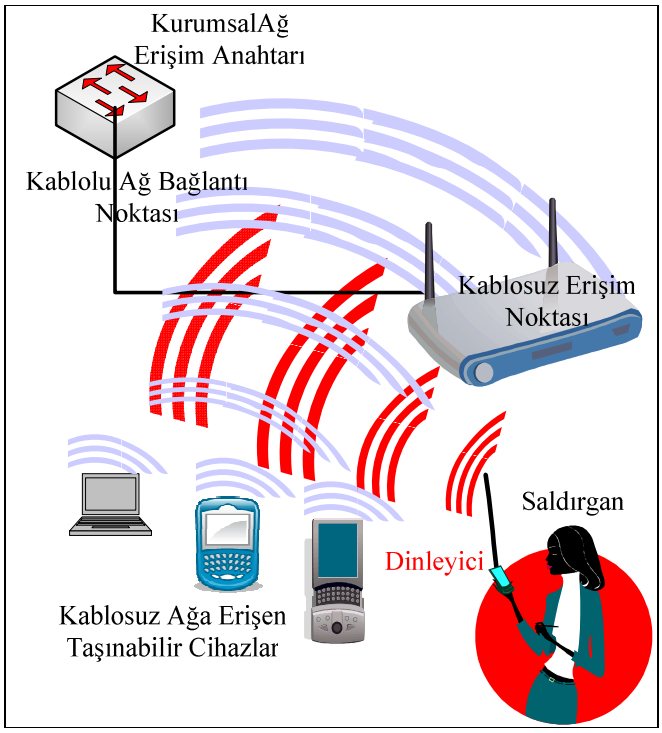
Test türü	Kullanılan test tekniği	Alınabilecek önlemler
Telefon (Yardım Masası)	Taklit ve inandırma	Çalışanların ve yardım masasının telefonla hiç bir şekilde şifre veya diğer gizli bilgilerin verilmemesi için eğitilmesi
Binaya giriş	Yetkisiz fiziksel erişim	Sıkı kimlik kartı güvenliği, çalışanların eğitilmesi ve güvenlik görevlilerin çalıştırılması
Ofis ziyaret	Omuz sörfü	Sizden başka birinin olduğu durumlarda şifrenizi girmeyin. Girmeniz gerekiyorsa çabuk şekilde tuşlayın.
Telefon (Yardım Masası)	Yardım masası aramalarında taklit	Bütün çalışanlara yardım masası desteği alabilmesi için tekil bir PIN numarası ata.
Ofis	Açık odalar bulabilmek için koridorlarda dolaşma	Bütün misafirlere işyerinden bir refakatçi sağla.
Posta odası	Taklit notların sokulması	Posta odasını kilitle ve izlemeye tabi tut.
Makine odası – Santral	Erişmeye teşebbüs, cihazların kaldırılması ve gizli bilgileri elde edebilmek için bir protokol analizcisi eklenmesi	Santral, sunucu odaları v.s. her zaman kilitli tut ve cihazların güncel envanterini tut.
Telefon ve PBX	Telefon görüşme ücreti erişimi çalma	Şehirlerarası, milletlerarası ve cep telefonu aramalarını kontrol et, konuşmaları izle, aktarmaları reddet.
İş yeri atık deposu (dumpster)	Çöplük karıştırma	Bütün atık kovalarını güvenli ve izlenen alanlarda tut. Önemli belgeleri kesme makinesiyle yok et, manyetik ortamdaki verileri sil.
İntranet - İnternet	Şifre çalmak için İntranet veya İnternet üzerinde sahte yazılımların oluşturulması ve konulması	Sistem ve ağ değişikliklerinden sürekli haberdar olma, şifre kullanımı eğitimi ver/al.
Ofis hırsızlık	Hassas belgelerin çalınması	Belgelere gizlilik derecesi ver ve bu belgeleri kilitli yerlerde sakla.
Genel - Psikolojik	Taklit ve ikna	Bütün çalışanları sürekli uyanık tutarak ve eğitim programlarına tabi tutarak bilinçlendir.

Sosyal mühendislikte kullanılan test yöntemleri, saldırganın uyguladığı taktikler ve kurumların alması gereken önlemler Çizelge 4.2'de gösterilmiştir [164].

Teknik sızma testleri, sistemlere sızmak için özel olarak geliştirilmiş yazılımlar ve donanımlar kullanılarak yapılan testlerdir. Teknik testlerin önemlileri sırasıyla aşağıda açıklanmıştır. Teknik testlerin birincisi, güvenli bölgelerden güvensiz bölgelere yetki olmaksızın fark edilemeyecek şekilde bilginin sızdırılabilirlik testleridir. Bilgi kaçakları, bilgi güvenliği uzmanlarının en çok başını ağrıtan ve engellenmesi zor olan güvenlik ihlallerinin başında gelmektedir. Bilgi kaçaklarının önlenebilmesi için güvenli bölgelerin devamlı izlenmesi, kullanıcı bilgisayarlarında veri saklanması ve taşınmasını engelleyecek önlemlerin alınması (disk, disket, veri çubukları, kompakt disk bileşenlerine erişimlerinin kısıtlanması, kurum dışına yazıcı çıktılarının çıkartılmaması, çalışanların tecrübe ve bilgilerini menfaatleri doğrultusunda dışarı sızdırmaları, vb.) çok zordur. Sistematik olarak verilerin güvenli alanlardan güvensiz alanlara sızdırılmasını sağlayan yöntemlerden biriside steganografidir. Steganografik yazılımlar kullanılarak yapılan bu testlerde; nesne (müzik, resim, görüntü dosyaları, vb.) içerisine nesne (müzik, resim, görüntü dosyaları, vb.) gizlenerek bilgiler dış dünyaya sızdırılabilmektedir. Örneğin bir resim dosyası içerisine çok gizli bilgiler içerebilen bir metin belgesi, bir ses dosyası içerisine yine gizli bilgiler içeren bir ses kaydı, görüntü dosyası içerisine yine önemli bilgiler içeren bir metin belgesinin gizlenmesiyle bilgiler dış dünyaya e-postalar ve taşınabilir depolama ürünleri vasıtasıyla sızdırılabilir. Bu tür sızdırmalar teknik testlerle önlenmektedir.

Teknik testlerden ikincisi ise pasif dinlemelerdir (intercepting). Dinlemeler yoluyla kullanıcı sistemleri (terminal, iş istasyonları, telefonlar, veri hatları, vb.) ile merkezi sistemler (sunucular, internet servis sağlayıcıları, vb.) arasında akan iletişim trafiği yetkisiz olarak izlenebilmektedir. Dinleme, farklı iletişim ortamlarında gerçekleştirilebilir. Bunlardan birincisi bakır teller üzerindeki iletişim trafiğinin dinlenmesidir. Asenkron, senkron veya kiralık bakır hatlar üzerinde akan trafiğin herhangi bir noktadan paralel olarak hatta girilmesiyle dinlenebilme imkânı vardır. İkinci dinleme ortamı ise yerel alan ağları üzerindeki paketlerin dinleyici yazılımlarla bir kopyasının alınmasıdır. Sunucu bilgisayara bağlanmak üzere sisteme giriş yapan bir kullanıcının, kullanıcı adı ve şifresi bu teknikle ele geçirilebilir. Üçüncü dinleme ortamı, güvenli olarak bilinen fiber optik kablolarda yapılır. Fiber kabloların

dışındaki koruyucu tabaka soyulup U biçiminde kıvrılarak kıvrılan yerden gerekli ışık çoğaltılarak fiber kablo üzerinden geçen trafik dinlenebilir. Dördüncü dinleme ortamı Şekil 4.4'de gösterilen kablosuz ortamlardır. Kablosuz ortamlarda çalışan, bilgisayarlar kablosuz ağ ortamları için geliştirilmiş olan dinleyici yazılımlar yardımıyla dinlenebilir.

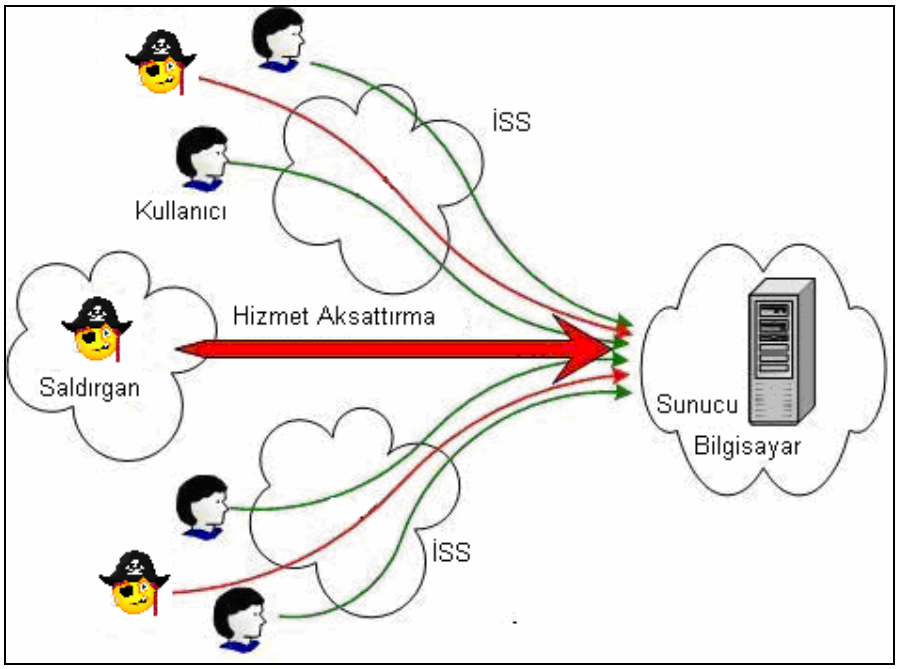


Şekil 4.4. Kablosuz ortamlarda dinleme

Teknik testlerden üçüncüsü, erişim kontrollerinin ihlal edilebilirliğinin ölçümlenmesidir. Bu testler vasıtasıyla kullanıcı adları ve şifreler kaba kuvvet teknikleri (brute force) veya akıllı tahminlerle elde edilebilirliği ölçümlenmektedir. Kaba kuvvet testleri güçlü bilgisayarlar kullanılarak bütün olasılıkların değerlendirilmesi esasına dayanır [165]. Akıllı tahmin adı verilen testlerde çok kullanılan şifre ve kullanıcı adlarını barındıran veri tabanlarından faydalanılır.

Teknik testlerden dördüncüsü, Şekil 4.5'de gösterilen hizmet aksattırma testleridir [166]. Bu testlerle bir sisteme düzenli olarak yapılan saldırılar sonucunda hedef sistemin hizmet veremez hale gelmesi veya o sisteme ait tüm kaynakların tüketimi

amaçlanmaktadır. Hizmet aksattırma testleriyle bir veya daha fazla noktadan bilgi sistemleri üzerine gereğinden fazla yükler bindirilerek, sistemler üzerindeki asli hizmetlerin aksaması ve bu aksama anında zayıflayan sistemlere sızılabilirlik ölçümlenmektedir. Disk alanlarının doldurulması, işlemci tüketimi, yerel alan ağlarındaki merkezi anahtarlara trafik yüklemek, internet yönlendiricilerine gereksiz trafik yükleyerek yetkisiz erişim elde etmek, hizmet aksatma testlerinden bazılarıdır.



Şekil 4.5. Hizmet aksattırma saldırıları

Teknik testlerden beşincisi, yazılım ve donanımlarda var olabilecek zafiyetlerin ortaya çıkarılmasıdır. Bu zafiyetlere örnek olarak bellek taşmaları, işletim sistemi açıklıkları, uygulama yazılımı açıklıkları, kodlama zayıflıkları ve konfigürasyon zayıflıkları örnek olarak gösterilebilir.

4.4. Sızma Testleri Aşamaları

Sızma testleri planlama, bilgi toplama, zafiyetlerin bulunması, zafiyetlerin kullanılması, raporlama olmak üzere beş aşamada gerçekleştirilirler [167]. Bu aşamalar sırasıyla aşağıda maddeler halinde verilmiştir.

(1) Testi yapan uzman kuruluş ile testi yaptıracak olan kurum arasında kapsam, gizlilik ve etik anlaşmaları, test türleri, kullanılacak araçların ne olduğu gibi konularda anlaşmaya varıldığı başlangıç aşaması "*Planlama*" aşaması olarak ifade edilir.

(2) Kurumların sahip olduğu bilgi varlıklarına ait envanterin (teknik, teknik olmayan), belirlenen test türüne göre araçlar kullanılarak veya kullanılmadan elde edilmesi için gerekli olan çalışmaların yapıldığı aşama ise "*Bilgi toplama*" olarak isimlendirilir. Kullanılan ağ cihazlarının tespit edilmesi, ağ üzerinden erişilebilen bilgisayarların tespit edilerek üzerinde çalışan servislerin ve işletim sistemlerinin belirlenmesi gibi çalışmalar bu aşamada yapılır.

(3) *"Zafiyetlerin bulunması*", bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini tehdit eden zafiyetlerin bulunmasına yardımcı olan taramalar bu aşamada yapılır.

(4) "*Zafiyetlerin kullanılması*", bilgi sistemlerine sızma amaçlı olarak bir önceki aşamada bulunan zafiyetlerin kullanıldığı aşamadır. Başarılı olan sızmalar aracılığıyla, ağ üzerinde başka zafiyetlerin ortaya çıkmasının sağlanması açısından bu aşamadaki testlerin yapılması önemlidir.

(5) Önceki aşamalarda yapılan testler sonucunda elde edilen bilgilerin yorumlanarak yazıldığı, test sonuçlarının (risk seviyeleri, sistemlere etkileri, önem sıraları, vb.) analiz edildiği, çözümler ve önerilerin yer aldığı dokümanlar ise "*Raporlama*" aşamasında oluşturulur.

Sızma testlerinin daha iyi anlaşılabilmesi ve gerçekçi olarak değerlendirilmesi için bu aşamalar takip eden alt başlıklarda detaylı olarak açıklanmıştır.

4.4.1. Planlama

Planlama aşamasında, kapsam tespiti, test türleri, zaman dilimleri, riskler, araçlar, personel, işin süresi, maliyet, etik, bilgi değişimi ve gizlilik anlaşmaları konularını içeren başlangıç aşamasıdır. Bu konuları kısaca açıklayalım. *Kapsam*, sızma testlerinin yapılmasına karar verildikten sonra ihtiyaçlar doğrultusunda Bölüm

4.3.3'te bahsedilen kapsamlardan birisine karar verilir. *Test türleri*, Bölüm 4.3.6'da anlatılan testlerden hangileri yapılacağına dair kararlar verilir. *Riskler*, uygulanacak olan testlerin hangi riskleri taşıdığına dair bilgiler test ekibi tarafından belirlenerek testi yaptıracak kuruma bildirilir. Bazı testler ve bu testlerin uygulanması sonucunda ortaya çıkabilecek olan risk seviyeleriyle ilgili bilgiler Çizelge 4.3'de gösterilmiştir.

Çizelge 4.3. Testler ve risk seviyeleri

Testler	Risk Seviyesi
Sosyal Mühendislik	Orta
Hostların Keşfedilmesi	Düşük
Kullanılan Portların Keşfedilmesi	Düşük
Kullanılan Servislerin Tespiti	Düşük
Otomatik Zafiyet Tarama	Orta
Çevirmeli Ağ Tarama (Wardialing)	Düşük
Kablosuz ağlarda Tarama (Wardriving)	Düşük
Parola Kırma	Orta
Zafiyetlerin İstismarı	Yüksek
Hizmet Aksattırma Testleri	Orta

Araçlar, yazılımlar (bilgi toplama yazılımları, zafiyet tarama yazılımları, programlama dilleri, vb.) veya donanımlar (telefon, faks, ağ dinleme cihazları, bilgisayar, vb.) olabilir. Teknik testlerde kullanılan komutlara örnekler Çizelge 4.4'de gösterilmiştir.

Çizelge 4.4. Sızma testlerinde kullanılan komutlardan bazıları [168]

Whois	Test Yapılacak Kuruma ait domain isimlerinin ve IP adres aralıklarının tespit edilmesi
Traceroute	TCP/IP yoluyla bağlanmış iki host arasındaki iletişim yolunun belirlenmesi
Nslookup	İsim sunucuları üzerinde sorgulama yapılması
Ping	ICMP ECHO paketinin gönderilmesi
Nmap	Güvenlik tarama yazılımı
Strobe	Port tarama yazılımı
Nessus	Zafiyet tarama yazılımı
Telnet	Telnet portunun kontrol edilmesi

Sızma testlerinin başarılı bir şekilde yapılabilmesi için ekip çalışmasına ihtiyaç vardır. Bu ekip içerisinde teknik yönden ileri düzeyde bilgi sahibi olması gereken

kişilerin yanında ve sosyal yönü gelişmiş, insanlarla iyi iletişim kurabilen ikna kabiliyeti yüksek kişilere de ihtiyaç vardır. Ayrıca ekip içerisinde koordinasyonu sağlayan, planlamayı yapan, test sonuçlarını yorumlayan ve raporların yazılmasını sağlayan bir koordinatöre ihtiyaç vardır. Bahsedilen ve sızma testlerini yapan test ekipleri için terminolojide kullanılan ekip (tim) isimleri aşağıda maddeler halinde kısaca açıklanmıştır [169].

- Kaplan timi (Tiger team): Sızma test takımlarının koordinasyonundan ve fiziksel testlerden sorumludurlar.
- Kırmızı tim (Red team): Bilgi bakımından kıdemli çalışanların bulunduğu aktif sızma testlerini yapan ekibe verilen isimdir.
- Mavi tim (Blue team): Mevcut durumun (politika, prosedür, süreç, planlar, vb.) tespit edilmesi ve testler sırasında yapılan saldırıların izlenmesinden sorumludurlar.
- Beyaz tim (White team): Hakem görevi yapan bu ekip güvenlik politikaları prosedürler, planlar, sızma süreçlerin eksiksiz olarak yapılmasını ve uygulanmasını izler.

Süre, sızma testlerinde belirlenen kapsama bağlı olarak değişir. Kapsam genişledikçe test edilecek bilgi varlıklarının sayısının artmasına bağlı olarak süre ve maliyet artışı olur.

Planlama aşaması yapıldıktan kurumsal bilgi varlıklarının tespit edildiği, tespit edilen bilgi varlıklarının sınıflandırıldığı ve sızma testinin çatısının oluşturulduğu bilgi toplama aşamasına geçilir.

4.4.2. Bilgi toplama

Bilgi toplama aşamasında test tipine bağlı olarak, kamuya açık ortamlarda yapılan aramalar yoluyla kurumların bilgi sistemleri üzerinde araştırmalar yapılır. Bu araştırmalarda test konumuna (kurum içi, kurum dışı) göre açık kaynaklar (internet, intranet, gazeteler, haber grupları, dergiler, televizyonlar, vb.) ve sosyal mühendislik testleriyle kurum veya kuruluşlar hakkında detaylı bilgiler toplanır. Sızma testleri

sonucunda kurum içinden ve kurum dışından toplanabilecek bilgilere ait örnekler Çizelge 4.5'de verilmiştir.

Kurumlar hakkında bilgi toplanabilmesi için internet büyük bir fırsat sunmaktadır. İnternet üzerinden yapılan alan adı sorgulamaları kurumlar hakkında birçok bilginin elde edilmesini sağlamaktadır.

Çizelge 4.5. Sızma testleriyle elde edilecek bilgiler

Konum/ Yöntem	Toplanabilecek Bilgiler
İnternet (Kurum Dışı)	İletişim Bilgileri (Web, Posta Adresi, Telefon, Faks, E-posta)
	Alan İsimleri
	Dış Dünyaya Açık IP Bloğu
	IP'lerin Sunucularla (Güvenlik Duvarı, Web, DNS, E-posta, vb.) Eşleştirilmesi
	Yazılımların ve İşletim Sistemlerinin Tespiti
	Ağ Geçidinin Belirlenmesi (Yönlendirici)
	Güvenlik Yazılımlarının Tespiti (Güvenlik Duvarı, Atak Tespit Sistemi, vb.)
	Uzaktan Erişim Protokollerinin Keşfedilmesi (VPN, Remote Desktop)
İntranet (Kurum İçi)	Kullanılan Ağ Protokolleri (IP, DHCP, DNS, NAT, vb.)
	Dâhili Alan İsimleri Yapılandırması
	Dâhili Ağ IP Bloklarının Belirlenmesi
	Ağ Topolojisinin Belirlenmesi
	Erişim Kontrol Listeleri Mekanizmalarının Tespiti
	Dâhili Atak Tespit Sisteminin Keşfedilmesi
	Uygulama Platformlarının Belirlenmesi (.Net, Java)
	Veri Tabanlarının Belirlenmesi (Oracle, SQL)
	Sunucu Bilgisayarların Belirlenmesi ve Görevlerinin Tespiti
	Güvenlik Yazılımlarının Tespiti (Güvenlik Duvarı, Atak Tespit Sistemi, vb.)
Sosyal Mühendislik (Kurum İçi-Kurum Dışı)	Telefon Yoluyla Taklit ve İkna
	E-posta Yoluyla Kandırmaca
	Çöplük Karıştırma
	Masaüstü Testleri
	Fiziksel Erişim

Alan adı sorgulamasının yapılmasını sağlayan önemli sitelere http://www.whois.net/, http://ws.arin.net/whois, http://www.ripe.net/, https://www.nic.tr,

http://www.apnic.net/apnic-bin/whois.pl/, adreslerinden ulaşılabilmektedir. Alan adı sorgulamasından elde edilebilecek bilgiler aşağıda maddeler halinde gösterilmiştir.

- Alan adı
- Alan adını kayıt eden kişi veya kuruluşun adı
- Alan adını kayıt eden kişi veya kuruluşun e-posta adresi
- Alan adını kayıt eden kişi veya kuruluşun iletişim bilgileri (telefon, faks, posta adresi)
- Sistem yöneticisinin adı
- Sistem yöneticisinin e-posta adresi
- Sistem yöneticisinin iletişim bilgileri (telefon, faks, posta adresi)
- İsim çözme sunucularının adları
- Alan adının oluşturulma tarihi
- Alan adının son bulma tarihi

Bilgi toplamada en çok başvurulan ikinci yöntem arama motorlarıdır. Arama motorları içerisinde bilgiye ulaşımda Google arama motoru ön plana çıkmaktadır. Google arama motoru kullanarak gizli bilgilere ve zafiyetlere ulaşılabilmesine "Google Hack", arama motorunda kullanılacak olan ifadeleri içeren veritabanıda "Google Hack Veri Tabanı (GHDB)" olarak adlandırılmaktadır [170]. Sızma testlerinde arama motorları hem kamuya açık bilgilere, hemde web yöneticilerinin yapılandırma hatalarından kaynaklanan güvenlik açıkları sayesinde gizli bilgilere ulaşmakta kullanılmaktadır. Arama motorlarıyla ulaşılabilecek bilgiler aşağıda maddeler halinde verilmiştir. Bunlar;

- Genel bilgiler (Çalışan sayısı ve kabiliyetleri, iş yaptığı alanlar, finansal bilgiler, iletişim bilgileri, teşkilat şemaları, vb.),
- Telefon numaraları ve
- E-posta adresleri

olarak sıralanabilir.

Bilgi toplamada kullanılacak üçüncü yöntem, etki alanı isim çözümleme sunucularının (DNS) sorgulanmasından elde edilen teknik bilgilerdir. Sorgulama sonucu aşağıdaki bilgilere erişilebilmektedir. Bu bilgiler;

- Etki alanı isim çözümleme sunucu bilgisayarının adı ve IP numarası,
- Sorumlu kişinin e-posta adresi,
- İsim çözümleme sistemi hakkında bilgiler (DNS Sunucu Adı, Sorumlu kişi, Seri numarası, Yenileme aralığı, Yeniden deneme aralığı, Kullanım süresi aralığı),
- Dış dünyaya hizmet veren (e-posta, web, vb.) sunucu bilgisayarların adı ve IP numarası ve
- Dış dünyaya hizmet veren sunucu bilgisayarların detaylarını

içermektedir.

DNS sorgulama hizmeti veren http://www.dnsstuff.com/ adresinden yukarıda verilen bilgilerin tamamına erişilebilmektedir.

Bilgi toplamada kullanılacak sonuncu yöntem sosyal mühendislik veya toplum mühendisliği yöntemleridir. Sosyal mühendislik yöntemleriyle ikna kabiliyetine bağlı olarak önceki paragraflarda bahsedilen birçok bilgiye ulaşmak mümkün olabilmektedir.

4.4.3. Zafiyet analizi

Zafiyet, saldırganların sömürebileceği hatalardır [171]. Bilgi kaynakları (insan, haberleşme, bilgisayar ağları, bilgisayar, vb.) üzerinde var olan ve istismar edilebilecek güvenlik boşluklarının tespit edilmesi, tanımlanması ve sınıflandırılması süreci zafiyet analizi olarak adlandırılmaktadır [172]. Bilgisayarlar ve ağlar üzerindeki zayıflıklara ek olarak bu sistemlerin işletilmesiyle ilgili politika ve prosedürlerden kaynaklanan zafiyetlerde bu kısımda tanımlanır. Bu tez çalışmasında zafiyet, bilgi sistemlerinde gizlilik, bütünlük ve erişilebilirlik faktörlerinden en az birinin ihlâl edilmesini sağlayan kusurlar olarak tanımlanmıştır. Sosyal mühendislik, politika, prosedür eksikliklerinden kaynaklanan zafiyetler insanları etkilerken, mantıksal yazılım hataları veya tasarım zayıflıklarından kaynaklanan zafiyetler ise

sistemleri etkilemektedir [173]. Sosyal mühendislik Bölüm 4.3.6, politika, prosedür eksiklikleri ilgili tehditler Bölüm 2.4.2'de açıklandığından bu bölümde bilgisayar ağları üzerinde var olan güvenlik zafiyetlerinin bulunmasıyla ilgili açıklamalar yapılmıştır. Zafiyet analizi yapılırken izlenen basamaklar:

- Ağ veya sistem kaynaklarının tanımlanması ve sınıflandırılması,
- Kaynakların önem seviyelerine göre önceliklendirilmesi,
- Her bir kaynak için potansiyel tehditlerin belirlenmesi,
- Önemli görülen potansiyel problemlerle ilgili güvenlik stratejilerinin geliştirilerek gerekli önlemlerin alınması ve
- Eğer saldırı başarılı olursa meydana gelebilecek kötü sonuçların en aza indirgenebilmesi için yapılması gerekenlerin tanımlanması

olarak sıralanabilir.

Sızma testlerinin uygulanacağı kurumsal bilgisayar ağlarında, zafiyet analizlerinin yapılabilmesi için ağa bağlı cihazlar (bilgisayar, yönlendirici, anahtar, vb.) üzerindeki açık portların belirlenmesi, işletim sistemleri ve çalışan uygulamaların (sürüm numarası, yama seviyesi, servis paketleri, vb.) tespit edilmesi gerekmektedir. Günümüzde zafiyet analizlerinin yapılmasını sağlayan zafiyet tarayıcıları olarak da adlandırılan otomatik yazılımlar vardır. Bu yazılımlar içerisinde bulunan veri tabanlarında daha önceden duyurusu yapılmış mevcut zafiyet tanımları yer almaktadır. Veri tabanına kayıt edilmemiş ve yeni bir zafiyetin keşfedilmesi açısından otomatik yazılımlarla yapılan zafiyet analizlerine ek olarak manüel yöntemlerle yapılan zafiyet analizlerinin yapılmasıda gerekmektedir. Zafiyet analizleri sonucunda daha önce duyurulmamış yüksek seviyeli tehditler içeren güvenlik boşlukları bulunduğunda, yazılım ve donanım üreticilerine güvenlik boşluğuyla ilgili bilgi verilmesi ilgili yamaların çıkartılması açısından önemlidir.

İşletim sistemlerinin belirlenmesi: Bilgisayarların ağ yığınlarından sızan bilgiler vasıtasıyla, uzaktaki bir bilgisayarın işletim sistemi tespit edilebilmektedir. İşletim sistemlerinin belirlenmesinde aktif ve pasif olmak üzere iki yöntem kullanılmaktadır [174]. Aktif yöntemde uzaktaki işletim sistemine özel paketler gönderilmekte ve

işletim sisteminin gönderilen paketlere verdiği cevaplar dikkatlice incelenerek işletim sisteminin tespit edilmesi sağlanmaktadır. Pasif yöntemde ise uzaktaki işletim sistemiyle sıradışı hiçbir etkileşime girmeden izin verilen bağlantılar (web, ftp, smtp, vb.) sonucunda elde edilen bilgilerin dikkatlice göz geçirilmesi sonucunda işletim sistemleri tespit edilmektedir. Güvenlik açıklarının işletim sistemleriyle doğrudan ilişkili olması zafiyetlerin tespit edilmesinde bu aşamanın önemini ortaya koymaktadır.

Aktif belirleme yönteminde, hedefteki işletim sistemine modifiye edilmiş (bayrak bitlerinin işaretlenmesi, parçalanma işaretlerinin değiştirilmesi, ACK değeri veya servis tipi, vb.) IP paketleri gönderilerek alınan cevapların incelenmesi esasına dayanır. Modifiye edilerek gönderilmiş IP paketi uzaktaki sistem tarafından cevaplandıktan sonra paket içerisindeki bayraklar, pencere boyutları, gönderilen alınan sıra numaralarının incelenmesiyle hedefteki işletim sistemi tespit edilebilir [175]. *Pasif belirleme yönteminde*, uzaktaki sistemde izin verilen servislerin (http, smtp, ftp, telnet, pop3, nntp, dns, vb.) kullanımı esnasında oluşan TCP/IP bağlantısı sırasında TCP/IP paketi içerisindeki alanların TOS, TTL ve paket bölünme şekli değerlerinin dikkatlice gözden geçirilmesiyle işletim sisteminin tespit edilmesine çalışılır [176]. Çoğu işletim sisteminin TCP/IP yığınının farklı olması bu tekniğin geliştirilmesine yardımcı olmuştur. Bu yöntemi uygulamak için geliştirilmiş otomatik araçlar vardır. Ancak sistem yöneticileri tarafından işletim sistemleri üzerinde yukarıda bahsedilen parametrelerin değiştirilme imkânı olması pasif belirleme yönteminin aktif yönteme göre daha zayıf bir yöntem olduğunu göstermektedir.

Bu tez çalışmasında Türkiye'de kurum ve kuruluşlarda en fazla kullanılan Microsoft Windows işletim sistemi temel alınmıştır. Bu işletim sistemi üzerindeki zafiyetlerin bulunmasına dair sorgulamaların nasıl yapıldığına ilişkin bilgiler verilmiştir. Windows İşletim Sistemi, içerisinde yer alan ağ ve TCP/IP komutları hakkında önemli bilgilerin edinilmesinde önemli rol oynar. Bu komutların çoğunluğu NetBIOS (ağ basit giriş/çıkış sistemi) vasıtasıyla bilgisayar üzerindeki bilgilerin toplanmasına ve zafiyetlerin kullanılmasına yardımcı olur [177]. Zafiyetlerin tespit edilmesinde kullanılacak Windows komutları Çizelge 4.6'da gösterilmiştir [178].

Çizelge 4.6. Sızma testlerinde kullanılabilecek Windows komutları

Komut	Açıklama
Net Use	Parametreleriyle kullanıldığında bilgisayarı paylaştırılmış kaynağa bağlar, bağlantısını keser veya bilgisayar bağlantıları ile ilgili bilgileri ekranda görüntüler. Bu komut vasıtasıyla kalıcı ağ bağlantıları denetlenebilir. Ayrıca, parametresiz kullanıldığında, ağ bağlantılarının bir listesini alır.
Net View	Parametreleriyle kullanıldığında belirtilen bilgisayar tarafından paylaştırılan etki alanlarının, bilgisayarların veya kaynakların listesini görüntüler. Parametresiz kullanıldığında, Net View komutu geçerli etki alanınızdaki bilgisayarların bir listesini görüntüler.
Net Accounts	Kullanıcı hesapları ve veritabanını güncelleştirerek tüm kullanıcı hesapları için parola ve oturum açma gereksinimlerini değiştirir.
Net Config	Çalışmakta olan yapılandırılabilir hizmetleri görüntüler, bir sunucu hizmeti veya iş istasyonu hizmeti ayarlarını görüntüler veya değiştirir. Parametresiz kullanıldığında, yapılandırılabilir hizmetlerin bir listesini görüntüler.
Net Group	Etki alanlarındaki genel grupları ekler, görüntüler veya değiştirir.
Net Share	Paylaştırılmış kaynakları yönetir. Parametresiz kullanıldığında Net Share, yerel bilgisayarda paylaşılan tüm kaynaklar hakkındaki bilgileri görüntüler.
Net Localgroup	Bilgisayarlara yerel grupları ekler, görüntüler veya değiştirir. Parametresiz kullanıldığında, sunucunun adını ve bilgisayar üzerindeki yerel grup adlarını görüntüler.
Net User	Kullanıcı hesapları ekler, değiştirir veya kullanıcı hesabı bilgilerini görüntüler.
Nslookup	Etki Alanı Ad Sistemi (DNS) altyapısını sorgulamak için kullanılabilecek olan bilgileri görüntüler.
Nltest	Etki alanındaki birincil ve ikincil etki alanı sunucuları ile etki alanındaki bilgisayarlar ve o anda oturum açmış kullanıcıların listesini verir.
Arp	IP adresleri ve IP adreslerinin çözümlenmiş Ethernet veya Token Ring fiziksel adreslerini saklamak için kullanılan bir veya birden fazla tablo içeren Adres Çözümleme İletişim Kuralı (ARP) önbelleğindeki girdileri görüntüler ve değiştirir.
AT	Belirtilen saat ve tarihte bilgisayarda çalıştırılacak komut ve programların zamanlamasını yapar. Parametresiz kullanıldığında, AT komutu zamanlanmış komutları listeler.
Cacls	Paylaşım verilen dosyalardaki isteğe bağlı erişim denetimi listelerini (DACL) görüntüler veya değiştirir.
Cipher	NTFS birimlerinde klasör ve dosya şifrelemesini görüntüler veya değiştirir. Parametresiz kullanıldığında, cipher geçerli klasörün ve içerdiği dosyaların şifreleme durumunu görüntüler.
DsQuery	Belirtilen kritere göre Aktif Dizini sorgular.
Finger	Kullanıcı veya kullanıcılar hakkında bilgiler görüntüler.
GetMac	Yerel olarak veya bir ağ içinde, her bilgisayardaki tüm ağ kartları için ortam erişim denetimi (MAC) adresini ve her adresle ilişkili ağ iletişim kurallarının listesini verir.
IpConfig	Bilgisayar üzerinde geçerli olan tüm TCP/IP ağ yapılandırması ayarlarını görüntüler. Dinamik Ana Bilgisayar Yapılandırma İletişim Kuralı (DHCP) ve Etki Alanı Ad Sistemi (DNS) ayarlarını yeniler. Parametresiz kullanıldığında tüm bağdaştırıcılar için IPv6 adresleri veya IPv4 adresi, alt ağ maskesi ve varsayılan ağ geçidi görüntülenir.
NetStat	Aktif TCP bağlantılarını, bilgisayarın bağlı olduğu bağlantı noktalarını, Ethernet istatistiklerini, IP yönlendirme tablosunu, IP, ICMP, TCP ve UDP iletişim kuralları için IPv4 istatistikleri ile IPv6, ICMPv6, IPv6 üzerinden TCP ve IPv6 iletişim kuralları üzerinden UDP için IPv6 istatistiklerini görüntüler. Parametre olmadan kullanıldığında aktif TCP bağlantılarını görüntüler.
PathPing	Kaynak ve hedef arasındaki ara atlamalarda ağ gecikmesi ve ağ kaybı konularına ilişkin vererek ağ haritası çıkartılmasını sağlar.
Ping	Internet Denetim İletisi İletişim Kuralı (ICMP) Yankı İsteği iletileri göndererek, başka bir TCP/IP bilgisayara IP düzeyinde erişilebilirliği doğrular. Karşılık olarak gelen Yankı İsteği iletileri, iletim süreleriyle birlikte görüntülenir.
Rexec	Rexec hizmetini (arka plan programı) sağlayan ve bu hizmeti çalıştıran Windows dışı bilgisayarlara bağlanmak için Rexec aracını kullanabilirler. Rexec komutu, uzak bilgisayarda belirtilen komutu çalıştırmadan önce kullanıcı adını doğrular.
Route	Yerel IP yönlendirme tablosundaki girdileri görüntüler ve değiştirir.
RSH	RSH hizmeti veya arka plan programı çalıştıran uzak bilgisayarlarda komut çalıştırır.
TaskList	Yerel veya uzak makinede çalışan geçerli işlemlerin listesini görüntüler.
Telnet	Telnet protokolünü kullanan uzak bilgisayarla iletişim kurulmasını sağlar.
Tftp	Önemsiz Dosya Aktarım İletişim Kuralı (TFTP) hizmeti veya arka planını çalıştıran ve genellikle UNIX ile çalışan bir bilgisayardan dosya alır ve gönderir.
TraceRt	Hedefe, Artan Yaşam Süresi (TTL) alanı değerleriyle, Internet Denetim İletisi Protokolü (ICMP) Yankı İstek veya ICMPv6 iletileri gönderildiğinde izlenen yolu belirleyerek ağ haritalarının çıkartılmasını sağlar.

Port tarama: Zafiyet analizinin ikinci aşamasında uzaktaki sistem üzerinde kullanımda olduğu tespit edilen ağ adresleri için port taraması yapılır. Portlar bilgisayarlar üzerinde çalışan uygulamaların birbirleriyle iletişim kurduğu fiziksel ve mantıksal bağlantı noktalarıdır. Bu tez çalışmasında port kavramıyla mantıksal bağlantı noktaları kastedilmektedir. TCP/IP protokolü içerisinde port numarası için 2 Byte'lik bir alan tahsis edildiğinde 65536 tane portun kullanılabilme imkânı vardır. Port numaraları IANA (Internet Assigned Numbers Authority) tarafından atanmakta ve standart, kayıtlı ve özel olmak üzere üç gruba ayrılmaktadır [179].

Standart portlar, protokoller tarafından kullanılan sistemlerin üzerinde uzlaşmaya vardığı 0–1023 arasındaki numaraların atandığı portlardır. Kayıtlı portlar, sıradan (ordinary) uygulamalar tarafından kullanılan 1024–49151 arasındaki portlardır. Özel portlar ise, 48152–65535 arasında özel amaçlı kullanımlar için ayrılmıştır.

Port tarama ile kullanımda olan hostlar üzerinde açık olan portların tespit edilmesi için çalışılır. IP takımındaki portlar TCP (Transmission Control Protocol) ve UDP (User Datagram Protocol) olmak üzere iki farklı protokol kümesi üzerinde çalışırlar. TCP komutu [180] :

- IP veri birimlerinin teslim edileceğini garanti altına alır.
- Programların gönderdiği büyük veri bloklarını parçalar ve yeniden birleştirir.
- Bölünen blokların doğru sırada ve düzenli teslimini sağlar.
- Sağlama toplamı hesapları yaparak iletilen verilerin bütünlüğünü denetler.
- Verilerin başarıyla alınıp alınmadığına bağlı olarak onaylama iletileri gönderir.
- Seçici bildirimler yoluyla alınmayan verilerin alınmadı bildirimini de yapar.
- İstemci/sunucu veritabanı ve e-posta programları gibi güvenilir oturuma dayalı veri iletimleri kullanmak zorunda olan programlar için tercih edilen bir taşıma yöntemi sağlar.

Standart TCP tabanlı programların kullandığı bazı iyi bilinen TCP sunucu bağlantı noktaları Çizelge 4.7'de gösterilmiştir.

Çizelge 4.7. Bazı TCP portları ve görevleri

TCP Port Numarası	Açıklama
20	FTP sunucusu (veri kanalı)
21	FTP sunucusu (denetim kanalı)
23	Telnet sunucusu
53	Etki Alanı Adı Sistemi bölge aktarımları
80	Web sunucusu (HTTP)
139	NetBIOS oturum hizmeti

Performans gerektiren, az yükle ve düşük güvenilirlikli veri taşıma işlemleri için programlar tarafından TCP yerine UDP kullanılmaktadır. UDP bağlanma gerektirmeyen ve herhangi bir veri biriminin teslimini veya sıralı oluşunu garanti etmeyen yüksek performansta paketlerin teslim edilmesini sağlar. Çizelge 4.8'de standart UDP tabanlı programlarda çok kullanılan UDP sunucu bağlantı noktaları gösterilmiştir [181].

Çizelge 4.8. Bazı UDP portları

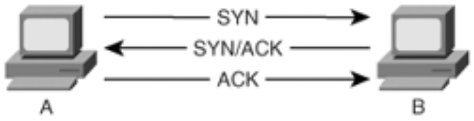
UDP Port Numarası	Açıklama
53	DNS ad sorguları
69	Yalancı Dosya Aktarım Protokolü (TFTP)
137	NetBIOS ad hizmeti
138	NetBIOS veri birimi hizmeti
161	Basit Ağ Yönetimi Protokolü (SNMP)
520	Yönlendirme Bilgisi Protokolü (RIP)

TCP hedefin erişilebilir ve iletişime hazır olduğunu doğrulayarak bir telefon çağrısı gibi çalışırken UDP ise posta kartı gibi işler; iletiler küçüktür ve teslimat büyük olasılıkla gerçekleşir fakat bu asla garanti edilemez. UDP genelde bir seferde küçük miktarlarda veri ileten veya gerçek zamanlı işlemlere gereksinim duyan programlar tarafından kullanılır. Bu durumlarda UDP'nin düşük üstbilgi yükü ve çok noktaya yayın yetenekleri (örneğin bir veri birimi için birden çok alıcı) TCP'den daha elverişlidir. Çizelge 4.9'da verilerin taşınmasında UDP veya TCP kullanılmasına bağlı olarak TCP/IP iletişiminin nasıl çalıştığı gösterilmektedir.

Çizelge 4.9. UDP ve TCP karşılaştırılması

UDP	TCP
Bağlanma olmadan verilen hizmet; ana bilgisayarlar arasında oturum açılmaz.	Bağlanarak verilen hizmet; ana bilgisayarlar arasında oturum açılır.
UDP verilerin sırasını veya teslimini garanti etmez veya doğrulamaz.	TCP, doğrulamayla verinin hedefe ulaşmasını ve verilerin sıralı teslimini garanti altına alır.
UDP kullanan programlar verilerin taşınması için gerekli güvenilirliği kendileri sağlamak zorundadır.	TCP kullanan programlara güvenli veri taşıma garantisi sağlanır.
UDP hızlıdır, ek yükü azdır, noktadan noktaya ve noktan birden çok noktaya iletişimi destekleyebilir.	TCP daha yavaştır, ek yükü fazladır ve yalnızca noktadan noktaya iletişimi destekler.

TCP verilerin güvenilirliği, kullanım kolaylığı ve programcılara sağladığı geliştirme ortamları, gibi özelliklerinden dolayı uygulamalar arasında en fazla kullanılan TCP/IP protokolüdür. Port tarama tekniklerinin daha iyi anlaşılabilmesi için iki host arasındaki TCP bağlantısının nasıl kurulduğunun bilinmesi önemlidir. İki host arasındaki TCP bağlantısı aşağıdaki şekilde gösterildiği üzere üç aşamada sağlanır [182].

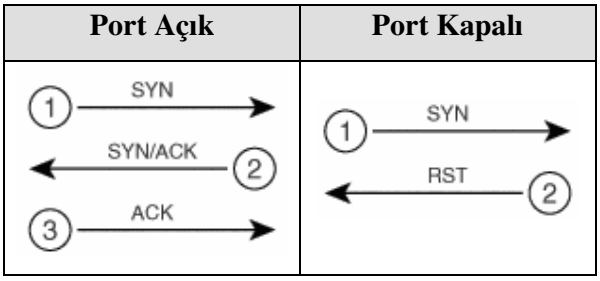


Şekil 4.6. TCP bağlantısı

A bilgisayarı B bilgisayarı ile bağlantı kurmak istediğinde, B bilgisayarına SYN paketi ve başlangıç sıra numarası (ISN) gönderir. Başlangıç sıra numarası 0 ile 4 294 967 295 arasında bir sayıdır. B bilgisayarı kabul paketi (ACK) ile sıra numarasını bir artırarak (ISN+1) A bilgisayarına gönderir. Daha sonra A bilgisayarı B bilgisayarına kabul (ACK) paketi göndererek TCP bağlantısının iki bilgisayar arasında kurulmasını sağlar. ACK paketinin sıra numarası B bilgisayarının sıra numarasıdır (ISN+1). TCP bağlantısında sıra numaralarında tutarsızlık yaşandığında reset (RST) paketi gönderilerek bağlantı kesilir.

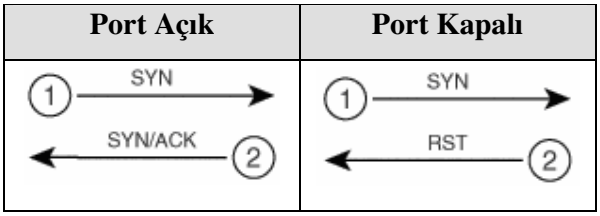
Port tarama teknikleri, TCP_Connect, TCP Syn, TCP Null, TCP Fin, TCP_Ack, Xmas-Tree, Dumb, UDP Tarama olmak üzere sekiz gruba ayrılarak aşağıda detaylı şekilde aşağıda açıklanmıştır [183].

TCP_Connect tekniğinde, hedef porta bağlanmak için SYN paketi gönderilir, bu pakete karşılık SYN/ACK paketi gelirse ACK paketi göndererek porta bağlanarak portun açık olduğu onaylanır. Eğer SYN paketine RST cevabı gelirse portun kapalı olduğu varsayılır. Bu tarama türünün dezavantajı açılan tüm oturumların hedefteki güvenlik sistemleri (STS, GD, vb.) tarafından tespit edilerek kayıtlarının tutulmasıdır.



Şekil 4.7. TCP_Connect tarama

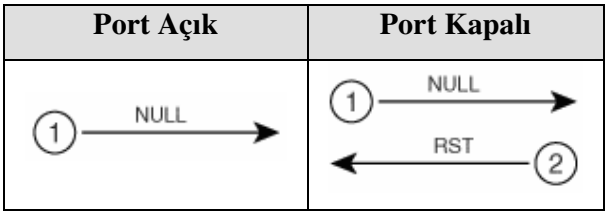
SYN Port Taraması, yarı açık olarakta tanınan SYN tarama TCP oturumu tamamen açmaz, SYN paketinin karşılığında SYN/ACK paketi geldiğinde portun açık olduğunu rapor eder ve RST paketi göndererek oturumu kapatır, port kapalı ise hedef RST cevabı gönderir. Bu tür taramada güvenlik duvarları tarafından farkedilme ihtimali düşük, atak tespit sistemleri (IDS) tarafından farkedilme olasılığı yüksektir.



Şekil 4.8. SYN tarama

NULL Tarama, normal TCP haberleşmesinden farklı olarak hiç bir bayrak biti işaretlenmez. RFC 793'e göre eğer gelen TCP segmentinde işaretli bir bayrak biti

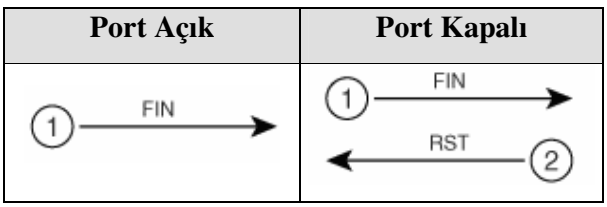
yoksa alıcı TCP segmentinin haberleşmesini keserek gönderene RST paketi yollar. Aşağıdaki şekilde görüleceği gibi bayrak biti işaretlenmeyen bir paket gönderildiğinde, eğer hedefteki port açıksa paketi yok sayarak cevap vermez, ancak port kapalı ise gönderene RST paketi yollayarak cevap verir.



Şekil 4.9. NULL tarama

Bu tarama tekniğinin kullanılacağı ortamlar RFC 793 ile uyumlu olmalıdır. Örneğin, Windows işletim sisteminin çalıştığı ortamlar bu RFC ile uyumlu değildir. Bu sebepten Windows yüklü bilgisayarlarda bu arama yöntemi kullanılamamaktadır. Windows işletim sistemi yüklü olan bilgisayarlar bayrak seti işaretlenmemiş bir TCP paketi aldığında, RFC 793 ile uyumlu olmadığı için göndericiye RST paketi yollayarak cevap verir. UNIX tabanlı sistemler RFC 793 ile uyumlu olduğundan port taramalarında bu yöntem kullanılabilir. Bu yöntemde gelen TCP paketine hiç bir cevap verilmemesiyle portların açık olduğu belirlendiğinden ters tarama sonuçlu port tarama sistemi olarak sınıflandırılır. Güvenlik duvarları ve atak tespit sistemleri tarafından bu tarama yönteminin algılanması zordur.

FIN Tarama, bir diğer ters tarama sonuçlu port tarama yöntemidir. NULL taramaya benzer, fakat bu yöntemde FIN biti işaretlenmiş TCP paketi hedefe gönderilir. FIN biti TCP oturumunun bittiğini belirten bir alandır. RFC 793 ile uyumlu olan ortamlarda geçerlidir.



Şekil 4.10. FIN tarama

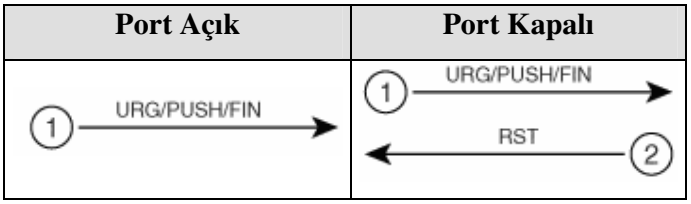
ACK Tarama, yöntemi güvenlik duvarlarının erişim kontrol listelerini geçerek tarama hedefteki hostların portları üzerinde tarama yapılmasını sağlar. Stateful veya basit paket filtreleme güvenlik duvarları, dışarıdan gelen SYN paketlerini bloke edebilir ancak ACK paketinin geçişine izin verirler. Bu tarama yönteminde ACK paketine rastgele üretilmiş sıra numaraları verilir. Hedeften cevap gelmez veya ICMP port ulaşılamaz mesajı gelirse port filtrelenen bir porttur. Eğer port güvenlik duvarları tarafından filtrelenmemişse RST paketi üretilerek kaynağa gönderilir. RST paketlerine bakılarak portların güvenlik duvarları tarafından filtrelenip filtrelenemediği öğrenilebilir.

Xmas-Tree Tarama, Noel ağacı anlamına gelen ters amaçlı tarama tipinde aşağıda belirtilen bayrakların işaretlendiği paket gönderilir. İşaretlenen bayraklar aşağıda gösterilmiştir.

URG Verinin acil olduğunu ve derhal işleme alınması gerektiğini belirtir.

PUSH Tampona veri gönderilmesini belirtir

FIN TCP oturumu bittiğini belirtir



Şekil 4.11. Xmas-Tree tarama

Bu tarama yönteminde yukarıda gösterilen bayrakların işaretlendiği paket hedef hosta gönderildiğinde RFC793'e göre hedeften hiç bir cevap gelmezse port açık, RST paketi döndürülürse portun kapalı olduğu anlaşılır.

Dumb Tarama, Salvatore Sanfilippo tarafından geliştirilmiş bir tarama tekniğidir [184]. Hedefteki hostlara ait portlar zombie diye tabir edilen üçüncü bir bilgisayardan taranır. Zombie bilgisayar önemli işlerde kullanılmayan boş bir bilgisayar olarak tanımlanabilir. Hassas bilgiler içermeyen, erişimi genellikle

izlenmeyen ve güvenlik zafiyetleri olan bilgisayarlardır. Çevirmeli olarak (dial-up) bilgilerini transfer eden kuruluşların veya kişilerin bilgisayarları bu amaçla kullanılabilir. Bu bilgisayarlar modem arama yazılımları (war dialer) adı verilen yazılımlarla kolayca tespit edilebilir. SYN tarama yöntemindeki gibi hedefteki hosta SYN paketi gönderilir. Eğer port açıksa hedefteki host SYN/ACK paketi döndürür, port kapalı ise hedefteki host RST paketi göndererek oturumu kapatır. Dumb taramada yukarıda anlatılan tüm işlemler zombie hostlar üzerinde yapılır.

UDP tarama, yönteminde hedefteki host'a UDP tipinde bir paket gönderilir. Eğer port kapalı ise hedefteki bilgisayardan ICMP port ulaşılamaz mesajı döndürülür herhangi bir mesaj döndürülmediğinde ise uzak sistemdeki host üzerindeki portun açık olduğu anlaşılır.

Uygulama ve zafiyet eşleştirilmesi: Port tarama işlemi sonucunda sızma testi yapılacak ağ üzerinde çalışan hostlara ait açık portların bir listesi çıkartılır. Uygulamaların tespit edilmesinde en çok kullanılan yöntem reklâm bandı korsanlığı (banner grabbing) adı verilen yöntemdir. Uzaktaki uygulamalara bağlanarak programların çıktıların gözlemlenmesi, reklâm bandı korsanlığı olarak adlandırılır [185].

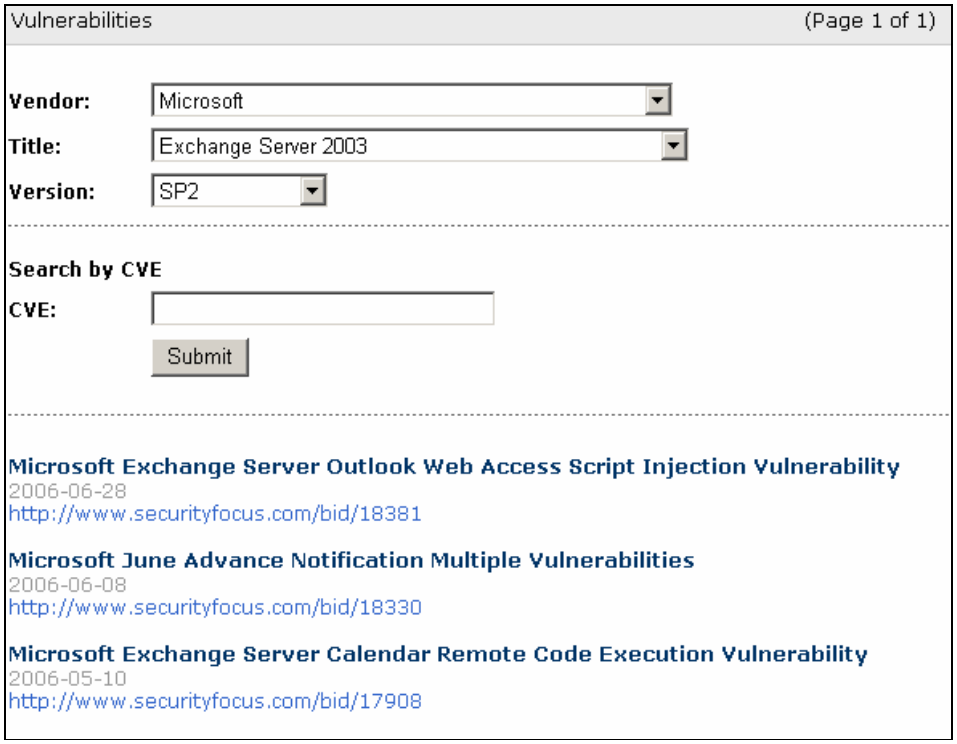
Bu yöntem hedef sistemler üzerinde izin verilen servisler (Telnet, FTP, HTTP, SNMP, vb.) kullanılırken giriş veya hoşgeldin mesajlarının analiz edilmesine dayanmaktadır. Reklâm bantları sayesinde uzaktaki sunucular üzerinde çalışan yazılımların tanımlanması ve sürümü, gibi bilgiler elde edilerek uygulamalar ve uygulamalara ait zafiyetlerin eşleştirilmektedir. Bu yöntem birçok zafiyet tarama yazılımı tarafından kullanılmaktadır. Reklâm bantları çalışan uygulamaların tespit edilmesinde Şekil 4.12'de gösterildiği gibi uzakta çalışan uygulamalar hakkında çok yararlı bilgiler vermektedir.

220 abc.mail.com.tr **Microsoft** ESMTP MAIL Service, **Version: 5.0.2195.6713** ready at Sat, 26 Aug 2006 22:33:49 +0300

Şekil 4.12. Reklâm bandı

Açık portların hangi uygulamalar tarafından kullanıldığının tespit edilmesinden sonra ilgili uygulamalara ait o ana kadar duyurulan zayıflıkların ne olduğuna dair araştırmalar yapılır.

Keşfedilen zafiyetlerin güncel olarak yayınlandığı MITRE CVE (www.cve.mitre.org), Security Focus (www.securityfocus.com) ve Secunia (www.secunia.com) sitelerinde yazılım veya işletim sistemlerine göre sorgulama yapılabilmektedir. Örneğin Şekil 4.13'de Microsoft Exchange Server 2003 SP2 yazılımına ait zafiyetlerin sorgulanması gösterilmektedir. Sorgulama sonrasında zafiyetleri listeler halinde sunulmaktadır.

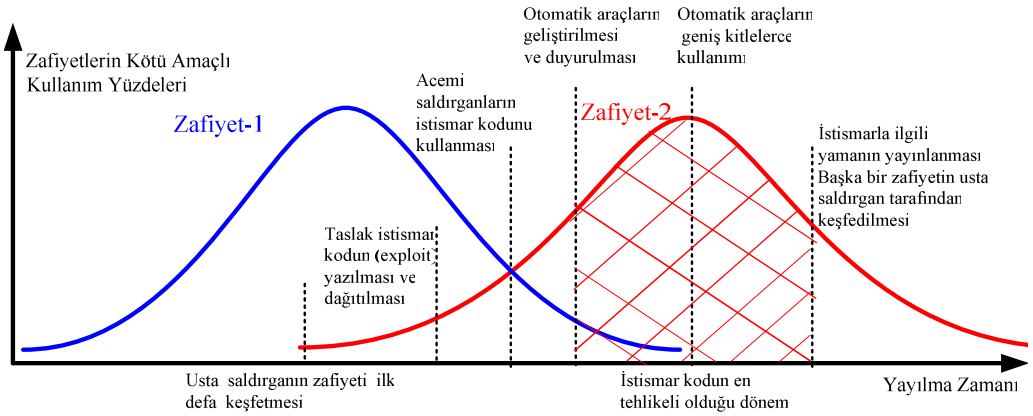


Şekil 4.13. Uygulamalara göre zafiyetlerin sorgulanması

4.4.4. Zafiyetlerin kullanımı

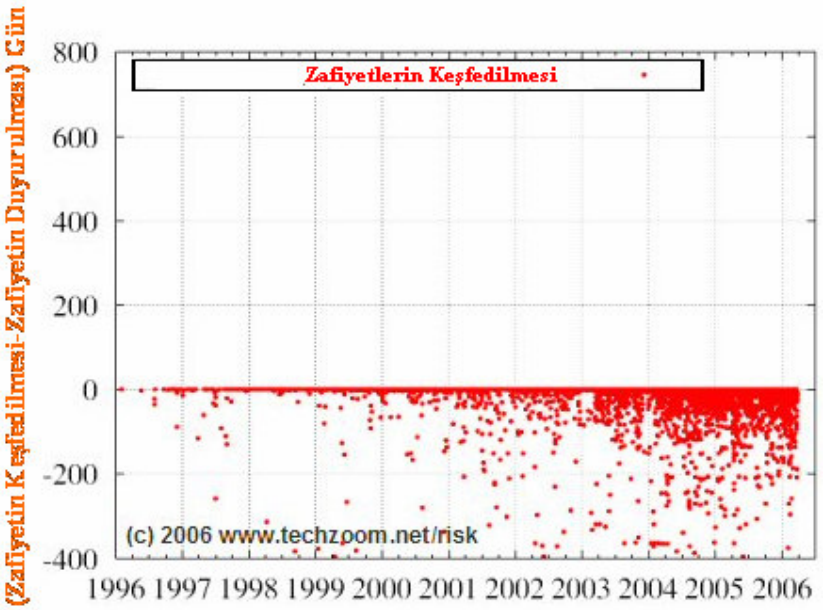
Zafiyetlerin kullanımı sızma testlerinin en önemli aşamasıdır. Bilgi sistemleri üzerinde bulunan yazılımlara ait güvenlik açıklarının kullanılmasını sağlayan küçük programlar istismar kodları (exploit) olarak adlandırılmaktadır [186]. İstismar kodları

zafiyetlerin genel veya özel kullanımı için farklı programlama dillerinde (C, C++, Perl, Lisp, Python, vb.) uzman yazılımcılar veya usta saldırganlar tarafından geliştirilmektedir. İstismar kodları bilgi sistemlerine olan erişim haklarına göre uzak (remote) ve yerel (local) olmak üzere iki sınıfa ayrılırlar. Sızma testi yapılacak sunucu bilgisayar üzerinde daha önceden verilmiş erişim hakkı yok ise "uzak", erişim hakkı var ise "yerel" istismar kodları olarak adlandırılmaktadır. "Kara-kutu" testlerde (erişim hakkı olmayan) sistemlere erişim sağlanabilmesi amacıyla uzak istismar kodları kullanılırken, "Beyaz-kutu" testlerde (erişim hakkı olan) sınırlı yetkilere sahip kullanıcı hesabına ait erişim hakkının yükseltilebilmesi için yerel istismar kodları kullanılmaktadır. Zafiyet ve istismar kodları arasındaki ilişki grafik olarak Şekil 4.15'de gösterilmiştir.



Şekil 4.14. Zafiyet yaşam döngüsü

Güvenlik açığının keşfedilmesini takiben geliştirilen istismar kodları sıfır gün istismar kodları olarak adlandırılmaktadır [187]. Güvenlik yamaları yayınlanana kadar sıfır gün istismar kodları tüm bilgi sistemlerini tehdit etmektedir. Sıfır gün istismar kodları Şekil 4.15'de gösterildiği gibi hızlı bir şekilde artmaktadır. Saldırganlar tarafından oluşturulan sıfır gün istismar kodlarının hızlı bir şekilde artması sızma aşamalarında kullanılan mevcut istismar kodlarına ek olarak yeni istismar kodlarının geliştirilmesi ihtiyacını doğurmuştur.



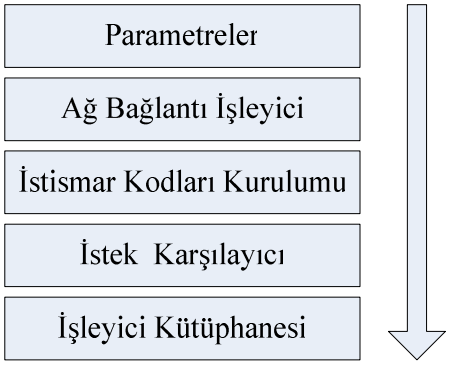
Şekil 4.15. Sıfır gün istismar kodları [188]

İstismar kodlarının geliştirme aşamalarına geçmeden önce konunun daha iyi anlaşılabilmesi için bilinmesi gereken kavramlar Çizelge 4.10'da gösterilmiştir [189].

Çizelge 4.10. İstismar kodu kavramları

Adı	Açıklaması
Payload	İstismar için çalıştırılacak ve normal dışı işlemi yapacak içerik
Shellcode	İstismar kodlarının çalıştırılacağı platforma özel ikili kodlar
NOP	"Not Operation", işlevi olmayan veya bellek yerinin öğrenilmesi amaçlı bellek dolduran bitler
Encoder	Çalıştırılacak Shellcode'u değiştiren ve IDS'ler tarafından yakalanmasını önleyen yazılımlar

İstismar kodlarının geliştirilme aşamaları Şekil 4.16'da gösterilmiş ve kısaca açıklanmıştır. Parametreler, son kullanıcı seviyesinde işlem gören seçeneklerin (uzak hedefin seçilmesi, ofset seçimi, derinlemesine çalıştırma, hata giderme, vb.) belirlenmesini sağlar. Ağ bağlantı işleyici, isim çözümlemesi, soket bağlantılarının kurulması, hataların işlenmesi gibi çeşitli ağ yordamlarını içermektedir. İstek karşılayıcı, istismar kodlarını tetikleyen betiklerdir (script). İşleyici yordamı istismar kodunun büyük bir kısmını kapsayan shellcode operasyonlarının yapıldığı aşamadır.



Şekil 4.16. İstismar kodlarının geliştirilme aşamaları

İstismar kodlarının yazılabilmesi, test edilebilmesi amacıyla ticari ve açık kaynak kodlu çerçeve yazılımlar geliştirilmiştir. 2006 yılında insecure.org sitesi tarafından en çok kullanılan yüz güvenlik aracının belirlenmesi için yapılan ankete 3,243 kişi katılmıştır. Zafiyet kullanım araçları isimli kategoride açık kaynak ve ticari programlar değerlendirilmiş ilk üçü Metasploit Framework, Core Impact ve Canvas isimli yazılımlar almıştır. Bunlar aşağıda kısaca tanıtılmıştır [190]. Çizelge 4.11'de kısaca tanıtılan bu yazılımlar 17 farklı özellik dikkate alınarak karşılaştırılmıştır [189].

Metasploit Framework, istismar kodlarının kullanılması, test edilmesi ve yazılması için komple çözüm sağlayan sızma testlerinde kullanılan ücretsiz (açık kaynak) zafiyet kullanım aracıdır. Bunlar Perl ve Ruby dilinde geliştirilmiştir. *Core Impact*, ticari amaçlar için geliştirilmiş geniş bir istismar kodu veri tabanına sahip güçlü ve oldukça pahalı bir çerçeve yazılımıdır. Python ve C++ programlama dilinde geliştirilmiştir. *Canvas*, ImmunitySec firması tarafından ticari amaçlar için geliştirilmiş zafiyet kullanım yazılımıdır.

Sızma aşamasında çerçeve yazılımların yanında elle (manüel) yapılan istismarlar da çok önemlidir. Özellikle web uygulamalarında sıkça rastlanan ve kodlama esnasında güvenliğin ihmal edilmesinden kaynaklanan SQL enjeksiyonu, siteler arası kod çalıştırma, parametre manipüle edilmesi, uzak dosya yükleme gibi zafiyetlerin tespit edilmesinde elle yapılan yöntemlerin kullanılması gerekmektedir.

Elle yapılan yöntemde bilinçli olarak, uygulamalar üzerinde hataların meydana getirilerek, meydana gelen hatalardan sistem hakkında bilgiler alınması ve alınan bilgilerin yardımıyla sistemlere yetkisiz erişim yapılması hedeflenmektedir. Web uygulamaları üzerinde mevcut sayfalarla oynanarak, uygulamanın kaynak kodlarından yararlanılması, uygulamaya ait formlarla, başlık bilgileriyle, çerezlerle oynanması sonucunda istenilen hatalar oluşturulabilir. Web sızma testlerine yönelik açıklamalar Bölüm 5'de detaylı olarak verilmiştir.

Çizelge 4.11. İstismar kodlarının çerçeve yazılımlarının karşılaştırılması

Özellikler	Core Impact	Canvas	Metasploit
(1). İşletim Sistemi	Windows	Windows / Unix	Windows / Unix
(2). Grafik Kullanıcı Arabirimi	Var	Var	Var
(3).Betik Dili	Python	Python	V 2.x Perl / V 3.x Ruby
(4). Ağ Haritalama	Var	Var	V 2.x Yok / V 3.x Planlanıyor
(5).Uzak İstismar Kodları	Var	Var	Var
(6). Yerel İstismar Kodları	Var	Var	Yok
(7). Web İstismar Kodları	Var	Yok	Yok
(8). Encoder Kullanımı	Yok	Yok	Var
(9). Ajan Üzerinden Saldırı	Var	Yok	Meterpreter / SocketNinja
(10).Payload Kullanımı	Agent / InlineEgg	Agent	Meterpreter / Shellcode
(11). İstismar Sonrası Bağlantı	Bind/Reverse/ Re-use	Bild/Reverse/ Re-use	Bild/Reverse/FindSock
(12). Otomatik İstismar İşlemi	Var	Var	Yok
(13). Raporlama	Var	Yok	Yok
(14). Diğer Araçlarla Entegrasyon	Var	Var	V 2.x Yok / V 3.x Planlanıyor
(15).Harici Geliştirme Araçları	Yok	Yok	Var
(16). Anti-Forensic Özellikleri	Yok	Yok	Var
(17). Fiyat	25.000$	2.000$ (10 Kullanıcı)	Ücretsiz

4.4.5. Raporlama

Sızma testleri sonucunda verilecek rapor tüm çalışmayı özetleyerek güvenliğin sağlanması için gerekli olan önlemler ve tavsiyeleri içeren, karar verme aşamasında üst yönetime tavsiyeler içeren bir kılavuz niteliğinde olmalıdır [191]. Raporun içeriği yönetim özeti, gerçekleştirilen hizmetler ile sonuç ve önerilerin yer aldığı üç ana kısımdan oluşmalıdır. Bunlar kısaca aşağıda açıklanmıştır.

Yönetim özeti, sızma testleri sonucunda bulunan olumlu veya olumsuz önemli noktaların yer aldığı, genellikle bir sayfaya sığdırılması istenilen üst yönetim tarafından okunması gereken raporun özet kısmıdır. Üst yönetimin kurumsal bilgi güvenliğinin mevcut durumunu doğru değerlendirmesi açısından bu kısımda güvenliği olumsuz etkileyen noktaların yanında, olumlu noktalarında belirtilmesi zorunludur.

Gerçekleştirilen hizmetler, kısmında testlerle ilgili olarak kapsam, yöntem, kısıtlamalar ve yapılan testlerin detaylarının yer aldığı bu kısım raporun en önemli bölümünü oluşturmaktadır. Testler sonucunda elde edilen ham teknik bilgiler raporun ekinde verilmelidir.

Sonuç ve öneriler kısmında, test sonuçlarının yorumlanarak önerilerin önem derecesine göre sıralanarak kısa, orta ve uzun vadede alınması gereken önlemler ve tavsiyeler yer almalıdır. Ayrıca testler sırasında karşılaşılan güçlükler ve sebepleri bu kısımda gerekçeleriyle birlikte anlatılmalıdır.

4.5. Sızma Testlerinde Kullanılan Araçlar

Sızma testlerinde, açık kaynak veya ticari olarak satılan birçok araç kullanılmaktadır. Bu bölümde sızma testlerinde kullanıldıkları aşamalara göre bu araçlar sınıflandırılarak açıklanacaktır.

4.5.1. Bilgi toplama araçları

Bilgi toplama aşamasında kuruluşlar hakkında en fazla bilgi içeren ortamlar kuruluşların resmi web siteleridir. Web sitelerinin ayrıntılı bir şekilde incelenebilmesi amacıyla kopyalarının çıkartılmasını sağlayan çevrimdışı göz atıcı araçlar (offline browser) Çizelge 4.12'de gösterilmiştir.

Çizelge 4.12. Web kopyalama yazılımları

Aracın Adı	Platform	Lisans	Web Adresi
GNU wget	Linux, Windows	Ücretsiz	www.gnu.org/software/wget
HTTrack	Linux, Windows	Ücretsiz	www.httrack.com
Teleport	Windows	Ücretli	tenmax.com/teleport
WebZIP	Windows	Ücretsiz	www.brothersoft.com
BlackWidow	Windows	Ücretsiz	www.softaward.com/1775.html
WebCopier	Windows, Mac	Ücretli	www.maximumsoft.com

Kuruluşların alan adının sorgulanması bilgi toplama aşamasında başvurulacak ikinci kaynaklardır. Bölgelere göre alan adı sorgulaması yapan web sayfalarının adresi Çizelge 4.13'de gösterilmiştir.

Çizelge 4.13. Bölgelere göre alan adı sorgulaması yapan siteler

Bölge	Web Adresi
Amerika (ARIN)	www.arin.net/whois/index.html
Asya Pasifik (APNIC)	www.apnic.org/search/index.html
Avrupa (RIPE NCC)	www.ripe.net/perl/whois
Afrika (AFRINIC)	www.afrinic.net/cgi-bin/Whois
Latin Amerika & Karayipler (LACNIC)	lacnic.net/cgi-bin/lacnic/whois

Bilgi toplama aşamasında Çizelge 4.13'e ek olarak işletim sistemleriyle birlikte gelen birçok yardımcı komut (nslookup, tracert, ping, telnet, vb.) ve internet üzerindeki bilgiye erişimi sağlayan arama motorları (Google, Yahoo, Altavista, vb.) vardır.

Windows işletim sistemi içerisinde gelen ve sızma testlerinin tüm aşamalarında kullanılabilecek komutlara ait liste Bölüm 4.4.3'de sunulmuştur. Bu araçların dışında

internet üzerinden indirilebilecek birçok yazılım vardır. Ancak bu tür yazılımların güvenlik tehditlerine karşı (virüs, trojan, arka kapı, vb.) mutlaka güvenilir sitelerden indirilmesi gerektiğini hatırlatmakta fayda vardır.

4.5.2. Tarama araçları

Sızma testlerinde kullanılan kritik araçların başında tarama yapmak üzere geliştirilen yazılımlar gelmektedir. Tarama yazılımları vasıtasıyla çalışan bilgisayarlar ve bu bilgisayarlar üzerinde kullanılan portların tespit edilmesi sağlanır. En fazla kullanılan tarama yazılımlarına ait liste Çizelge 4.14'de gösterilmiştir.

Çizelge 4.14. Sızma testlerinde kullanılan tarama araçları

Aracın Adı	Platform	Lisans	Web Adresi
SuperScan	Windows	Ücretsiz	www.foundstone.com/resources/proddesc/superscan.htm
AngryIP Scanner	Windows	Ücretsiz	www.angryziber.com/ipscan
Unicornscan	Unix, Linux	Ücretsiz	www.unicornscan.org
Hping	Unix, Linux	Ücretsiz	www.hping.org
Nmap	Linux, Windows, Unix, Mac	Ücretsiz	insecure.org/nmap
Strobe	Unix, Linux	Ücretsiz	www.deter.com
Xprobe2	Windows, Unix, Linux	Ücretsiz	xprobe.sourceforge.net
Amap	Windows, Linux	Ücretsiz	www.thc.segfault.net
Nbtscan	Windows, Linux, Unix	Ücretsiz	www.unixwiz.net/tools/nbtscan.html
Firewalk	Linux	Ücretsiz	www.packetfactory.net/Projects/firewalk
Scanrand	Linux	Ücretsiz	www.doxpara.com
P0f	Windows, Linux, Unix	Ücretsiz	camtuf.coredump.cx/p0f.shtml

Güvenlik problemlerinin daha fazla yaşandığı kablosuz ortamların tespit edilmesini sağlayan araçlar ise Çizelge 4.15' de verilmiştir.

Çizelge 4.15. Kablosuz ortamların tespit edilmesini sağlayan araçlar

Aracın Adı	Platform	Lisans	Web Adresi
Kismet	Windows, Linux, Unix	Ücretsiz	www.kismetwireless.net
NetStumbler	Windows	Ücretsiz	www.stumbler.net
KisMAC	Mac	Ücretsiz	kismac.de

4.5.3. Zafiyet tarama araçları

Zafiyet tarama araçları, tarama aşamasında çalıştığı tespit edilen bilgisayarlar ve bu bilgisayarlar üzerindeki servislerin kullandığı portların oluşturduğu güvenlik açıklarının tespit edilmesi için geliştirilen yazılımlardır. Güvenlik uzmanları tarafından en fazla tercih edilen zafiyet tarama araçları Çizelge 4.16'de verilmiştir [192].

Çizelge 4.16. Sızma testlerinde kullanılan zafiyet tarama programları

Aracın Adı	Platform	Lisans	Web Adresi
Nessus	Windows, Linux, Unix	Ücretsiz,	www.nessus.org
GFI LANguard	Windows	Ücretli	www.gfi.com/lannetscan
Retina	Windows	Ücretli	www.eeye.com/html/Products/Retina/index.html
Core Impact	Windows	Ücretli	www.coresecurity.com/products/coreimpact
ISS Internet Scanner	Windows	Ücretli	www.iss.net
X-scan	Windows	Ücretsiz	www.xfocus.org
Sara	Windows, Linux, Unix, Mac	Ücretsiz	www-arc.com/sara
Qualys Guard	Windows, Linux, Unix	Ücretli	www.qualys.com
SAINT	Linux, Unix	Ücretli	www.saintcorporation.com/saint

Günümüzde güvenlik ihlâllerinin büyük bir bölümü Web uygulamalarındaki zafiyetlerden kaynaklanmaktadır. Web uygulamalarının derinlemesine incelenmesi ihtiyacı yüzünden sadece Web uygulamaları üzerindeki açıklıkların tespit edilmesini sağlayan, Web zafiyet tarama yazılımları geliştirilmiştir.

Güvenlik uzmanları tarafından en fazla tercih edilen Web zafiyet tarama yazılımları Çizelge 4.17'de gösterilmiştir.

Çizelge 4.17 Sızma testlerinde kullanılan web zafiyet tarama yazılımları

Aracın Adı	Platform	Lisans	Web Adresi
Nikto	Windows, Linux, Unix	Ücretsiz	www.cirt.net/code/nikto.shtml
Parosproxy	Windows, Linux, Unix	Ücretsiz	www.parosproxy.org
WebScarab	Windows, Linux, Unix	Ücretsiz	www.owasp.org/index.php/Category:OWASP_WebScarab_Project
WebInspect	Windows	Ücretli	www.spidynamics.com
Whisker	Windows, Linux, Unix	Ücretsiz	www.wiretrip.net/rfp
Burpsuite	Windows, Linux	Ücretsiz	portswigger.net/suite
Wikto	Windows	Ücretsiz	www.sensepost.com/research/wikto
Acunetix	Windows	Ücretli	www.acunetix.com
Watchfire AppScan	Windows	Ücretli	www.watchfire.com/products/appscan/default.aspx
NStealth	Windows	Ücretli	www.nstalker.com/nstealth

Kullanıcı ve sistemler seviyesinde uygulanan şifreleme politikalarındaki zafiyetlerin ortaya çıkartılması için gerekli olan araçlar Çizelge 4.18'de sıralanmıştır.

Çizelge 4.18. Şifreleme sistemlerinin sağlamlığını denetleyen araçlar

Aracın Adı	Platform	Lisans	Web Adresi
Cain and Abel	Windows	Ücretsiz	www.oxid.it/cain.html
John the Ripper	Windows, Linux, Unix, Mac	Ücretsiz	www.openwall.com/john/
L0phtcrack	Windows	Ücretli	www.insecure.org/stf/lc5-setup.exe
SolarWinds	Windows	Ücretli	www.solarwinds.net/
Pwdump	Windows	Ücretsiz	www.foofus.net/fizzgig/pwdump
Rainbow crack	Windows, Linux, Unix, Mac	Ücretsiz	www.antsight.com/zsl/rainbowcrack/
Brutus	Windows	Ücretsiz	www.hoobie.net/brutus/
Aircrack	Windows, Linux, Unix, Mac	Ücretsiz	www.aircrack-ng.org/
Airsnort	Windows, Linux, Unix, Mac	Ücretsiz	airsnort.shmoo.com/

4.5.4. Zafiyet kullanma araçları

Zafiyetlerin oluşturduğu güvenlik açıklarının kullanılmasını sağlayan araçlar otomatik ve açığa özgü olmak üzere iki farklı sınıfta incelenebilir. Genel olarak zafiyetlerin kullanılmasını sağlayan otomatik araçlar Bölüm 4.3.4'te ayrıntılı bir

şekilde açıklanmıştır. Detaylı bilgi için ilgili bölüme gidiniz. Açığa özgü olarak geliştirilen yazılımlar sızma testleri için önemli araçlardan birisidir. Bu yazılımlar güvenlik açısından gizlilik gerektirmektedir. Açığa özgü geliştirilen yazılımlar açığın giderildiği anlaşıldıktan sonra yapılan anlaşmalara göre sızma testleri sonucunda yok edilmektedir.

4.6. Sızma Testlerinde Kullanılan Standartlar ve Kılavuzlar

Bilgi güvenliğiyle ilgili genel standartlar ve kılavuzlar Bölüm 3'de ayrıntılı olarak açıklanmıştır. Sızma testlerinin yapılmasında kullanılan açık kaynaklı projeler olarak geliştirilen dünyada yaygın olarak bilinen önemli standart ve kılavuzlar takip eden alt başlıklarda kısaca açıklanmıştır.

4.6.1. OSSTMM

Sızma testlerinde kullanılan en yaygın rehberlerden bir tanesi olan ve açık kaynak olarak geliştirilen OSSTMM (The Open Source Security Testing Methodology Manual) güvenlik testlerinin ve ölçümlerinin yapılması için oluşturulan çerçeve bir yapıdır [193]. Bu çerçeve yapı ISECOM (The Institute for Security and Open Methodologies) isimli kar amacı güdmeyen Amerika ve İspanya'da faaliyet gösteren bir enstitü bünyesinde geliştirilmektedir. Bu projenin amacı sızma testlerinin yapılmasında bir model geliştirmek ve bu modele uygun yapılan sızma testlerinin enstitü tarafından onaylanmasını sağlamaktır.

OSSTMM modeline göre sızma testleri bilgi güvenliği, süreç güvenliği, internet teknolojileri güvenliği, iletişim güvenliği, kablosuz ağ güvenliği ve fiziksel güvenlik, olmak üzere altı ana bölümde yapılmaktadır. Her ana test bölümünün kendi içerisinde yapılacak testlerin bulunduğu modüller bulunmaktadır. Bu modüllerin içerisinde ilgili testin nasıl yapılması gerektiğine dair adımlar testlerde kullanılacak taslak dokümanlar, testlerin sonucunda elde edilmesi gereken bilgilerin yer aldığı açıklamalar yer almaktadır. OSSTMM modeline göre ana test alanları ve modülleri aşağıda kısaca açıklanmıştır [194].

Bilgi güvenliği testleri: Bu bölümde sızma testi yapılacak olan kurum hakkında ayrıntılı gözden geçirme ve incelemeler yapılmaktadır. Mevcut durumun değerlendirilmesi, bilgi bütünlüğünün, insan kaynaklarının ve mahremiyet denetimlerinin gözden geçirilmesi bu bölümde yapılan çalışmalardan bazılarıdır.

Süreç güvenliği testleri: Bu bölümde kurumun işleyişine etki eden süreçlerin güvenliği test edilmektedir.

İnternet güvenlik testleri: Test alanları içerisinde en fazla modüle sahip olan bu bölümde 19 adet test uygulanmaktadır. Bu testler aracılığıyla ağ ve internet ortamları üzerinde bilgi güvenliğinin test edilmesi amaçlanmaktadır. Ağ haritasının çıkarılması, saldırı tespit sistemlerinin gözden geçirilmesi, sistem servislerinin tanımlanması, internet üzerinden hizmet veren uygulamaların test edilmesi, yönlendirme testleri, erişim kontrolü, şifre kırma, hizmet aksattırma ile güvenlik politikalarının gözden geçirilmesi gibi testlerdir.

İletişim güvenlik testleri: Haberleşme ortamlarının güvenliğinin sağlanmasıyla ilgili testler bu bölümde yapılmaktadır. Genel bir değerlendirmenin arkasından, telefon, faks, modem, sesli posta ve uzaktan erişim gibi iletişim ortamlarına ait testlerdir.

Kablosuz ortam testleri: Kablosuz ortamlar aracılığıyla haberleşen cihazların güvenliği bu bölümde test edilmektedir. Genel bir değerlendirme sonrasında, 802.11x kablosuz ağlarının test edilmesi, bluetooth ağlarının test edilmesi, kablosuz diğer cihazların ve elektromanyetik yayılım testlerini kapsar.

Fiziksel güvenlik testleri: Fiziksel güvenliğin sınanması için kapı giriş ve çıkış sistemlerinin edilmesi, alarm ve izleme sistemlerinin test edilmesi, erişim kontrollerinin test edilmesi bu bölümde yapılan çalışmalardan bazılarıdır.

OSSTMM modeline göre yukarıda açıklanan test alanlarının bir kısmı veya tamamı kurumlara uygulanabilir.

4.6.2. NIST

İkinci sızma testi modeli, Ulusal Standart ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) tarafından geliştirilmiş ve "Ağ Güvenliği Test Rehberi" ismiyle Amerika'da standart haline getirilmiştir. Bu rehber kurumların BT altyapılarını kendi kendilerine test edebilmeleri ve ağ güvenliklerini sağlayabilmeleri için gerekli olan çalışmaların bir yaşam döngüsünde nasıl yapılacağına dair açıklamaları içermektedir. Bu standart kurumların ağ güvenliğinin test edilmesi için sahip olduğu bilgi teknolojisi altyapısının sistematik bir şekilde incelenip araştırılması konusunda bir metodoloji tanımlamaktadır [195].

4.6.3. OWASP

Açık kaynak Web Uygulama Güvenliği Projesi (The Open Web Application Security Project-OWASP) güvenli web servisleri ve web uygulamaları geliştirilmesi amacıyla yazılım araçları geliştirilmesini ve kılavuzlar yazılmasını sağlayan açık kaynaklı bir çalışmadır [196]. OWASP aynı zamanda web servisleri ve web uygulamalarının güvenlik testinin yapılması için geniş katılımın sağlandığı topluluklar tarafından yürütülen çalışmalar yapmaktadır. Web uygulama güvenliği, saldırganların web servisleri ve web uygulamalarını hedef haline getirmesiyle daha fazla önem kazanmıştır. Kurumsal bilgi güvenliğini en üst düzeyde tehdit eden web servisleri ve web uygulamalarının güvenliğinin sağlanması için yapılması gereken sızma testleri Bölüm 5'de ayrıntılı bir şekilde açıklanmıştır.

4.6.4. ISACA

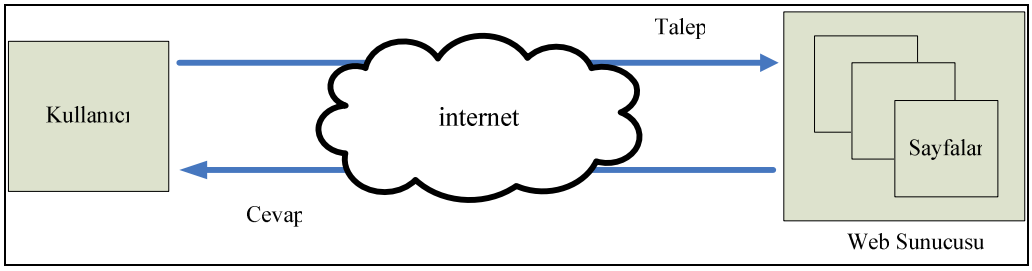
İsviçre Bilgi Güvenliği Derneği'nin bilgi güvenliğiyle ilgilenen özel bir grubu ile ISACA (Information Systems Audit and Control Association) tarafından ortaklaşa yapılan bir çalışma sonucunda "Kaplan Timiyle BT Sistem Güvenliği Testi" adında bir kitapçık yayınlanmıştır. Kaplan takımı kavramı sızma testlerini yapan takıma karşılık gelmektedir. Bu kitapçık sızma testlerini tespit etme önerme ve kontrat, risk analizi, testler ile rapor ve sunum olmak üzere 4 kısımda incelemektedir. Testler

bölümü sızma testlerinin nasıl yapılacağına dair açıklamaların tanımlandığı bölümdür [139].

5. WEB UYGULAMALARI SIZMA TESTLERİ

Daha önceki bölümlerde de açıklandığı gibi günümüzde kurum ve kuruluşlar bilgilerini elektronik ortamlara açtıkça, elektronik ortamlarda yapılan iş ve işlemler artmakta karşılaşılan tehdit ve tehlikelerde de doğal olarak artışlar gözlenmektedir. Web uygulamaları, güncel bilgiye kurum, kuruluş veya bireylerin kolayca erişebilmesi için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır. Web uygulamaları denilince akla ilk gelen kurumsal web sitelerinin içeriği, kurumların vitrini ve itibarı haline gelmiştir. Web üzerinden verilen hizmetler çoğaldıkça web'e yönelik saldırılar da her geçen gün artmaktadır. Bunun nedeni, web uygulamaları güvenliğinin ilgisizlikten ve bilgisizlikten kaynaklanan sebeplerden ötürü yeterince ciddiye alınmaması ve güvenli yazılım geliştirme tekniklerinin kullanılmaması olarak açıklanabilir.

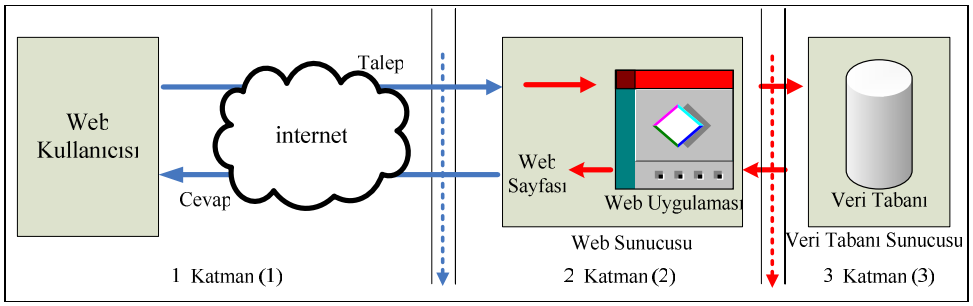
Bu bölümde zafiyet ve zayıflık açısından değerlendirildiğinde korunmasızlık seviyesinin yüksek olması nedeniyle sızma testlerinin en fazla uygulandığı alan olan web uygulamaları ele alınmıştır. Sızma testlerinin daha iyi anlaşılabilmesi için web uygulamalarının çalışma prensipleri ile web uygulamalarının geliştirildiği statik ve dinamik çalışma ortamları aşağıda açıklanmıştır. Web siteleri dinamik veya statik yapıda çalışan HTML içerikleri sunmaktadırlar. Şekil 5.1'de şematik olarak gösterilen ve statik yapıda çalışan web siteleri, kullanıcıdan gelen talepler üzerine ilgili web sayfalarının gösterilmesini sağlayan HTML kodlarını içermektedirler.



Şekil 5.1. Statik web sitesi çalışma yapısı şematik gösterimi

Statik web siteleri günümüzde yerlerini artık dinamik içerikli web sitelerine veya portallarına bırakmaktadır. Dinamik web siteleri, kullanıcı istekleri doğrultusunda

çalışan web uygulamaları içermektedir. Dinamik web siteleri Şekil 5.2'de şematik olarak gösterildiği gibi üç katmanlı bir yapı içerisinde çalışmaktadır [197].



Şekil 5.2. Dinamik web sitesi çalışma yapısı şematik gösterimi

Şekil 5.2'de gösterilen katmanlar aşağıda maddeler halinde kısaca açıklanmıştır.

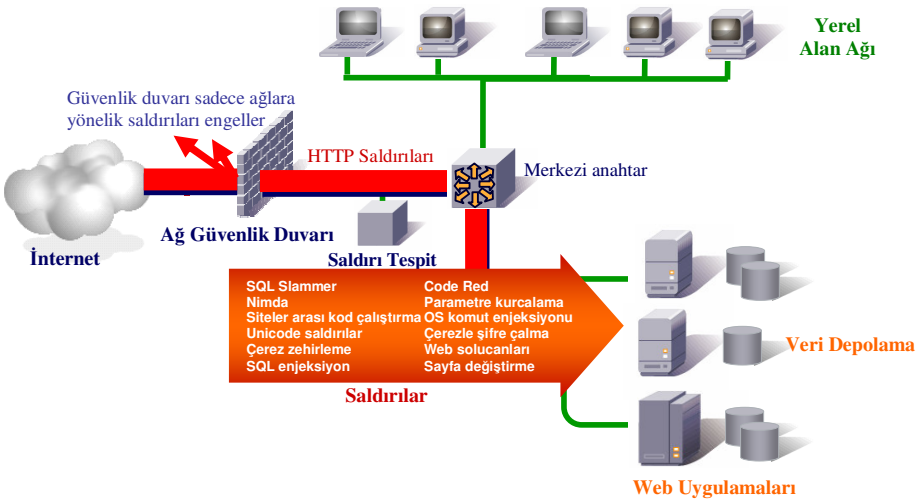
(1) Web siteleri için taleplerin başladığı Web tarayıcılarıdır (Internet Explorer, Mozilla, Firefox, Netscape, vb.). Web tarayıcıları üzerinden kullanıcılar, web sunucusuna içerikle ilgili taleplerini iletirler.

(2) Dinamik sayfaların üretildiği uygulama katmanıdır (Hypertext Processor-PHP, Active Server Pages-ASP, Java Server Pages-JSP, WebSphere, ColdFusion, SunONE, vb.).

(3) Web uygulamaları tarafından kullanılan verilerin depolandığı veri tabanlarıdır (MS SQL, My SQL, Informix, Oracle, vb.).

Dinamik içerikli web sitelerinde, web tarayıcıları taleplerini web uygulamalarına ilettikten sonra bu istekler doğrultusunda veritabanı sorgulaması yapılır ve talep edilen isteklere ait sonuçların yer aldığı sayfalar üretilerek, tarayıcılar üzerinde gösterilir. Dinamik içerikli web sayfaların bu esnek çalışma yapısı birçok güvenlik tehdidini ve ihlâllerini beraberinde getirmektedir. Gartner Grup tarafından yapılan bir araştırmada bu durum açıkça ortaya konmaktadır. Günümüzde yapılan saldırıların %70'i uygulama seviyesindeki ataklardan kaynaklanmakta ve ticari içerikli web sitelerin %75'i ise korunmasız durumdadır [198]. Web uygulamalarında oluşabilecek bir zafiyet, güvenlik önlemlerini (güvenlik duvarı, saldırı tespit ve önleme sistemleri,

vb.) Şekil 5.3'de gösterildiği gibi devre dışı bırakarak güvenilir bölgede yer alan sistemleri üst düzeyde tehdit etmektedir.



Şekil 5.3. Güvenlik önlemlerinin web saldırılarıyla aşılması

Ağ güvenlik duvarları kendilerine gelen tüm HTTP isteklerini kabul ederek yarı güvenilir bölgede bulunan web uygulama sunucularına bu paketleri iletirler.Paketler içerisinde yer alan saldırı kodları web uygulamalarının bulunduğu sunucu bilgisayarlar üzerinde çalışarak güvenlik ihlalerinin meydana gelmesine neden olurlar.

Web uygulamalarının güvenliğiyle ilgili birçok çalışma yapılmaktadır. Bu çalışmalardan birisi olan, Mark Curphey tarafından 2001 yılında kurulan, kâr amacı güdmeyen ve herkese açık bir ortam olan OWASP (The Open Web Application Security Project) web uygulama güvenliğinin artırılmasına yönelik ücretsiz araçlar, standartlar, web uygulamaları güvenliğiyle ilgili forumların yapılması, makalelerin yazılması konusunda çalışmaktadır [199]. Diğer bir çalışma ise 2004 yılında Jeremiah Grossman ve Robert Auger tarafından kurulan ve web uygulamaları güvenliğiyle ilgili açık standartların geliştirilmesi, yaygınlaştırılması ve kullanımı gibi konularda çalışan Web Uygulamaları Güvenlik Konsorsiyumudur (The Web Application Security Consortium-WASC) [200]. Web uygulama güvenliği

konusunda dünyada kabul görmüş OWASP ve WASC tarafından belirlenen, web uygulamalarında en fazla rastlanan saldırılar bu bölümde anlatılacak olan sızma testlerine esas teşkil etmiştir.

5.1. Kimlik Doğrulama Sızma Testleri

Burada web sitesinin kimlik doğrulama mekanizmasını atlatmak veya istismar etmek için kullanılabilecek zafiyetler ele alınmaktatır. Kimlik doğrulamasında "sahip olunan bir nesne", "bilinen bir bilgi" veya "sahip olunan bir özellik" kullanılmaktadır [201]. Kimlik doğrulama sızma testleri, web uygulamalarının kullanıcı, servis veya uygulama kimliğini onaylayan kısımları üzerinde yapılmaktadır. Kimlik doğrulama saldırıları, web sitesinin kullanıcı, servis veya uygulama kimliğini doğrulayan sistemleri hedef alan tehditleri kapsar. Web sitelerinin, kimlik doğrulama mekanizmasını atlatmak veya istismar etmede kullanılan zafiyetlerin ortaya çıkartılmasını amaçlayan sızma testleri, kaba kuvvet, yetersiz kimlik doğrulamaları ve şifre kurtarma denetimlerinin zayıflığı olmak üzere üç gruba ayrılır [202]. Bu hususlar takip eden alt başlıklarda açıklanmıştır.

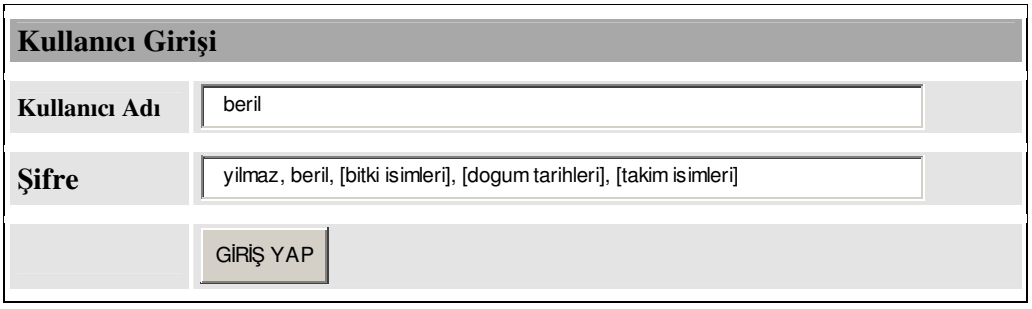
5.1.1. Kaba kuvvet yöntemi

Kaba kuvvet saldırısı, bir kullanıcı isminin, parolasının, kredi kart numaralarının veya gizli anahtarlarının birer birer denenerek (A'dan Z'ye, 0'dan 9'a, vb.) tahmin edilmesine dayalı işlemdir [203].

Kimlik doğrulama sistemlerinin kaba kuvvet teknikleriyle aşılmasını sağlayan iki zafiyet vardır. Birinci zafiyet web uygulamalarının, deneme yanılma yoluyla tahmin edilebilecek olasılıkta kombinasyon içeren zayıf şifre ve kriptografik anahtar kullanılmasına izin vermesidir. İkinci zafiyet kullanıcıların kimlik doğrulamasında seçmiş oldukları parolaların sözlüklerde yer alma ihtimali olan kolay hatırlanabilir şifreler seçmesidir. Kaba kuvvet sızma testiyle, insanlar tarafından şifre seçiminde kullanılabilecek ifadeleri içeren sözlükler ve sistem üzerinde parola olarak kabul edilebilecek karakterler içerisinden oluşturulacak olan, milyonlarca tahmin yardımıyla geçerli bir şifre bulunması amaçlanmaktadır. Tahmin edilen şifre, sisteme

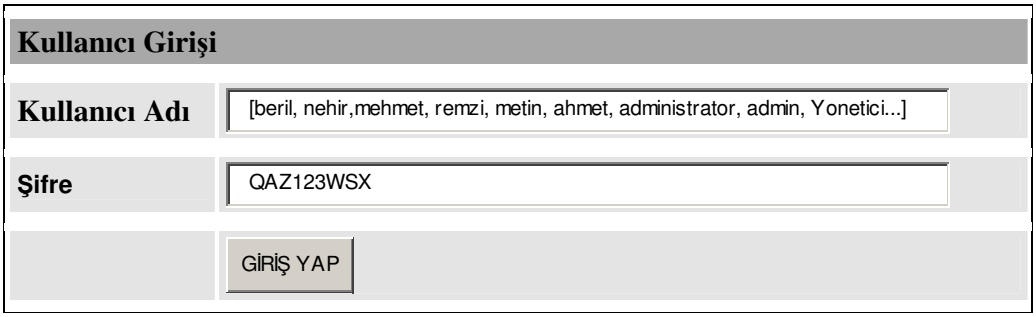
erişime izin verdiğinde, kaba kuvvet sızma testi başarılı olmuştur. Aynı deneme ve yanılma tekniği, şifreleme anahtarlarının tahmini için de uygulanabilmektedir. Web sitesi zayıf ve kısa bir anahtar kullandığında, sızma testiyle bütün olası anahtarlar denenerek doğru anahtarın tahmin edilmesi mümkündür.

Kaba kuvvet sızma testlerinde, normal ve ters olmak üzere iki farklı yöntem uygulanmaktadır [204]. Normal yöntemde, tek kullanıcı ismine ait şifrenin bulunması için Şekil 5.4'de gösterildiği gibi birçok parola, deneme yanılma yöntemiyle tahmin edilmeye çalışılmaktadır. Burada bazı kelimeler üzerine odaklanıldığı görülebilir.



Şekil 5.4. Kaba kuvvet sızma testlerinde normal yöntemin temsili gösterimi

Ters yöntemde Şekil 5.5'de gösterildiği gibi tek parolaya ait birçok kullanıcı ismi deneme yanılma yöntemine tabi tutularak tahmin edilmeye çalışılmaktadır. Milyonlarca kullanıcı hesabına sahip sistemlerde, birden çok kullanıcının aynı parolaya sahip olma olasılığı yüksek olduğundan ters kaba kuvvet sızma testlerinin başarı olasılığı daha yüksektir.



Şekil 5.5. Kaba kuvvet sızma testlerinde ters yöntemin temsili gösterimi

Çoğunlukla başarılı olan kaba kuvvet sızma teknikleri ile şifre tahmini kullanılan donanıma bağlı olarak saatler, haftalar veya yıllarca sürebilir.

5.1.2. Yetersiz kimlik doğrulama yöntemi

Yetersiz kimlik doğrulama yönteminde, web uygulamasının uygun bir kimlik doğrulama gerçekleştirmeden hassas içeriğe veya yönetim fonksiyonlarına erişim izni vermesi sınanmaktadır. Kritik web uygulamalarına kullanıcıların tam olarak kimlikleri onaylanmadan direk olarak erişilmemesi gerekmektedir.

Kritik bilgilerin yer aldığı ve erişilmesi istenmeyen kaynakların adres bilgilerinin gizlenmesi, söz konusu adres bilgilerinin web sitesi üzerinde diğer genel adresler ile herhangi bir bağlantısının olmaması (kaynağın web sitesi üzerinde gizlenmesi), web sitelerinde yetkisiz kimlik doğrulama açıklarına yol açmaktadır. Günümüzde arama motorları ve birçok otomatik araç ile web sitesinde gizlenen alanlara rahatlıkla ulaşılabilmektedir. Sızma testleriyle tespit edilen bu kaynaklar uygun yöntemlerle korunmalıdır.

Çoğu web uygulaması, görünen dizinler dışında görünmeyen (yönetim, sistem, kullanıcılar, vb.) başka dizinler ve yönetici fonksiyonları içermektedir. Gizli olan dizinlere web sitesinin herhangi bir yerinden link verilmemekte ancak söz konusu dizine standart bir web tarayıcısı ile erişebilmek mümkündür. Uygulamayı geliştiren yazılımcılar, web sayfasına herhangi bir link oluşturulmadığı ve herhangi bir kullanıcının da bu web sitesini görmesini beklemediği için söz konusu sayfaya kimlik doğrulama fonksiyonu eklemeyi çoğu zaman ihmal etmektedirler. Herhangi bir saldırgan basit bir şekilde bu web sayfasını ziyaret edecek olursa, web sitesine tüm yönetici yetkileri ile erişme yetkisi kazanacaktır.

5.1.3. Şifre kurtarma denetimi

Şifre kurtarma denetimlerinin zayıflığının belirlenmesi için yapılan sızma testlerinde, web sitelerinin kullanım şifresini unutan kullanıcıların şifrelerini tekrar kullanabilmeleri için otomatik olarak verdiği hizmeti kullanarak, şifrelerin ele geçirilmesi, değiştirilmesi veya hatırlanmasını sağlayan zafiyetler araştırılmaktadır.

Birçok farklı web uygulaması kullanımına bağlı olarak kullanıcılar zamanla şifrelerini unutmaktadır. Şifre hatırlatma servisleri unutulan şifrelerin kullanıma otomatik olarak açılabilmesi açısından web üzerinden servis veren uygulamaların önemli bir parçası haline gelmiştir.

Otomatik olarak unutulan şifrenin geri elde etme işlemleri, kullanıcının kayıt olma sürecinde belirlediği gizli soruya cevap vermeyi gerektirmektedir. Gizli sorular daha önceden uygulama tarafından belirlenen soru listesinden veya kullanıcı tarafından belirlenir. Kullanılan diğer yöntemler ise kullanıcının şifreyi hatırlaması için kayıt olma işlemi sırasında belirlenen bir yardım bilgisi, kullanıcının kimliğini doğrulamak için anne kızlık soyadı, vatandaşlık numarası, ev adresi, posta kodu gibi kişisel bilgilerin girilmesini gerektirmektedir. Kullanıcının sisteme kendisinin iddia ettiği kişi olduğunu kanıtlamasından sonra sistem yeni şifreyi kullanıcıya gösterir veya e-posta yolu ile gönderir.

Sızma testleriyle şifre kurtarma mekanizmalarının sağlamlığının kontrolü yapılmaktadır. Şifre kurtarma işlemi sırasında kullanıcının kimliğini onaylamak için gereken bilgi tahmin edilebiliyorsa veya bu bilgi isteme işlemi atlatılabiliyorsa ilgili web sitesinin zayıf bir parola kurtarma mekanizmasına sahip olduğu anlaşılır. Şifre geri kurtarma sistemleri, kaba kuvvet saldırıları, sistem açıklıkları ve kolay tahmin edilebilir gizli sorular kullanılarak saldırganlar tarafından istismar edilir. Sızma testleriyle zayıf şifre geri elde etme için bilgi onaylama, şifre imaları ve gizli soru ve cevap gibi mekanizmalar kullanılmaktadır [205]. Bu mekanizmalar aşağıda açıklanmıştır.

- *Bilgi Onaylama:* Birçok web sitesi, şifre geri elde etmede kullanıcılardan e-posta adresi, ev adresi ve telefon numarası, baba adı gibi kişisel bilgilerini istemektedirler. Sızma testleriyle bu bilgilerin elde edilmesi hedeflenmektedir. Bu bilgilerin çoğunluğu gizli olmadığı için kamuya açık ortamlardan, XSS ve sazan avlama yöntemleriyle rahatlıkla elde edilebilir.
- *Şifre imaları:* Kullanıcıya şifre hatırlatmak için kullanılır ve bazı ipuçlarını içerirler. Kullanılan şifre imaları web sitelerinde kaba kuvvet kullanılarak şifrelerin

bulunması açısından zafiyet oluşturmaktadır. Örneğin kullanıcı, sağlam bir şifre olan "Ye1L$a1!", şifre hatırlama ipucu olarak ise "mez.old.okul+tut.takım" ifadelerini kullanabilir. Bu durumda şifre hatırlatma ipucundan kullanıcının şifresinin mezun olduğu okul ve tuttuğu takım olduğu rahatlıkla çıkarılabilir. Elde edilen bu bilgi, sayesinde kaba kuvvet teknikleriyle okullar ve takımlar üzerine yoğunlaşılarak şifrenin tahmin edilme olasılığı çok yükselir.

- *Gizli soru ve cevap:* Bu yöntemde kullanıcı tarafından daha önce belirlenen sorunun cevabının doğru olarak verilmesi beklenir. Örneğin, kullanıcının şifresi "£iR@0" gizli sorusu "Oturduğunuz Şehir" olabilir. Şifre çok sağlam olmasına rağmen gizli soru bir o kadar kolaydır. Gizli sorudan elde edilen bu bilgi, sayesinde şifrenin tahmin edilme olasılığı çok yükselir.

Şifrenin sağlam bir şifre olması, şifre güvenliği için önemli bir şart olmasına rağmen şifre güvenliğini sağlamamaktadır. Şifrelerin geri elde edilmesinde kullanılan yöntemler, şifrelerin güvenliğinin sağlanması açısından çok büyük önem taşımaktadır.

5.2. Yetkilendirme Sızma Testleri

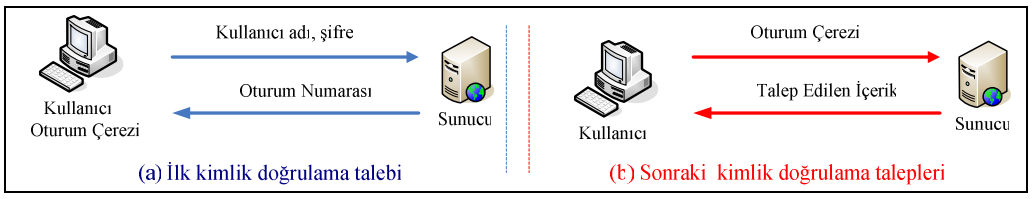
Yetkilendirme sızma testleri, bir web sitesinin kullanıcı, servis veya uygulamanın istenen bir işlemi gerçekleştirmesi için gereken izinleri belirlemek için kullanılan yöntemlerin sınanmasını hedef alan testleri kapsamaktadır. Yetkilendirme sızma testlerini, oturum bilgisi tahmin etme, yetersiz yetkilendirme, yetersiz oturum sonlandırma, oturum sabitleme olmak üzere kendi arasında dört grupta sınıflandırmak mümkündür. Bu gruplar takip eden alt başlıklarda detaylı olarak açıklanmıştır.

5.2.1. Oturum bilgisi tahmini

Yetki veya oturum bilgisi tahmin etme, web sitesi kullanıcısının rolüne girme veya söz konusu kullanıcının oturumunun ele geçirilmesi yöntemidir. Oturumun ele geçirilmesi olarak da bilinen bu yöntemin kullanılmasıyla istismar edilen kullanıcının hakları ile web sitesine istek gönderilir. Web sitelerinde çalışan uygulamalar,

iletişimin kurulmasından sonra kullanıcının kimliğinin doğrulanmasını sağlamak ve takibini yapacak mimaride tasarlanmıştır. Bu mimariye uygun olarak kullanıcılar kimliklerini web uygulamaları üzerinde daha önceden tanımlı olan kullanıcı ismi ve parola bilgilerini girerek onaylatırlar. Bu gizli yetki bilgilerinin her işlemde web sitesine gidip gelmesi yerine, web siteleri tek bir oturum numarası üreterek kullanıcı oturumunun kimliğinin doğrulandığını takip eder. Web sitesi ile kullanıcı arasındaki yapılacak haberleşmelerde, üretilen bu oturum numarası eklenerek oturumun kimliğinin doğrulandığına dair kanıt oluşturulur. Eğer sızma testleri sırasında web sitesi üzerindeki başka bir kullanıcının oturum numarası tahmin edilirse yetkilendirme mekanizması aşılmış olur.

Oturum numaraları genellikle tarayıcılar tarafından, çerezler içerisinde kalıcı ve geçici olmak üzere iki farklı yöntemle saklanmaktadır. Geçici depolamada, oturum numarasını içeren çerezleri, tarayıcı kapandığında süresi dolduğundan silinirler. Kullanıcı web siteleri yetkilendirme ekranlarında yer alan "Beni Hatırla" seçeneğini aktif hale getirirse, oturum numaraları kullanıcı bilgisayarları üzerinde kalıcı olarak depolanmaktadır. Kalıcı çerezler işletim sistemi ve tarayıcıların tipine bağlı olarak kullanıcı bilgisayarlarında farklı yerlerde (Netscape tarayıcısı, C:\program files\netscape\users\username\cookies.txt, Internet Explorer C:\Documents and Setting\username\Cookies) saklanırlar [206]. Oturum çerezleri sayesinde web sitelerine bir sonraki bağlantılar kullanıcı adı ve şifre istenmeden Şekil 5.6'da gösterildiği gibi otomatik olarak yapılır.



Şekil 5.6. Oturum çerezleri

Oturum numarası kullanarak yetkilendirme yönteminde, zayıf algoritmaların kullanılması, kaba kuvvet saldırılarını engelleyecek önlemlerin alınmaması (hesap kilitleme, doğrulama resimleri, vb.), sunucu bilgisayarlarca oturum numaralarının

şifresiz gönderilmesi, oturum numaralarını içeren çerezlerin çalınması gibi birçok tehdit vardır. Oturum numaraları çerezler dışında, gizli form alanı veya URL içerisinde depolanmaktadır. Oturum numarası tahmin edilmesi yöntemiyle kullanıcıların kimliğinin ele geçirilmesi için sızma testlerinde, aşağıdaki işlemler sırasıyla yapılmalıdır.

(1) Web uygulamasına bağlanarak geçerli bir oturum numarası elde edilir.
(2) Oturum numarası incelenerek, oturum numarası üretme algoritması ortaya çıkartılır. Oturum numarası üretme algoritması üzerinde kaba kuvvet saldırıları uygulanarak bir sonraki oturum numarası elde edilir.
(3) Elde edilen bir sonraki oturum numarası mevcut oturum numarası ile değiştirilerek bir sonraki kullanıcının kimliği ele geçirilir.

5.2.2. Yetersiz yetkilendirme

Web siteleri içerisinde kullanıcılar dışında sitenin yönetimini sağlayan ve sadece yetkili yöneticiler tarafından kullanılması gereken hassas bölümlerde yer almaktadır. Sızma testlerinde kullanılan yetersiz yetkilendirme, web uygulamalarının daha geniş erişim kontrol kısıtlamaları gereken hassas bilgiye, yapılandırma hatalarından kaynaklanan zayıflıklardan faydalanılarak erişilmesidir.

Web sitelerinin kopyalarının çıkartılabilmesi, arama motorlarıyla web siteleri üzerinde yer alan görünmeyen dosya veya klasörlere ulaşılması gibi, bu ve buna benzer nedenler yüzünden web siteleri üzerinde yer alan gizli bilgilerin bulunduğu kısımlar yetkili yöneticiler dışında herkese kısıtlanmalıdır. Kimlik doğrulama sonucunda yetkilendirme mekanizmalarıyla, bir kullanıcının, servisin veya uygulamanın yapmasına izin verilen işlemlerin ne olduğuna karar verilir. Yetersiz yetkilendirme yöntemiyle yapılan sızma testlerinde, arama motorlarından veya kaba kuvvet yöntemlerinden yararlanılarak web sitesi üzerinde yer alan hassas bilgilere yetkilendirme olmaksızın ulaşabilme amaçlanmakta ve bu açıklar tespit edilmeye çalışılmaktadır.

5.2.3. Yetersiz oturum sonlandırma

Yetersiz oturum sonlandırma, web sitelerinin yetkilendirme için kullanılan eski oturum kimlik bilgisini tekrar kullanma imkânı vermesinden kaynaklanmaktadır. HTTP durum bilgisi tutmayan bir protokol olduğundan, web siteleri çoğunlukla kullanıcıların isteklerini birbirinden ayırt edebilmek için oturum bilgileri kullanmaktadırlar. Bu nedenle birden çok kullanıcının aynı kullanıcı hesabına erişmesini engellemek için, oturum numaralarının gizliliğinin sağlanması gerekmektedir. Yetersiz oturum sonlandırma yöntemiyle yapılan sızma testlerinde sonlanmamış oturumlar elde edilerek başka bir kullanıcının kimliğine bürünerek onlar adına işlem yapabilme amaçlanmaktadır. Oturum bilgisi, muhtemel bir ağ dinleyicisi veya siteler arası kod çalıştırma (XSS) saldırısı ile elde edebilir. Yetersiz oturum sonlandırma, web tarayıcısının geri düğmesine basılarak daha önceki kullanıcı tarafından girilmiş web sitelerine yetkilendirme olmaksızın erişilmesine neden olur. Oturum sonlandırma zamanlarının uzun tutulması, geçerli bir oturum numarasını başarı ile tahmin edebilme olasılığını artırmaktadır. Uzun süreli sonlandırma zamanları, aynı anda bulunan açık oturum sayısının artmasına sebep olduğundan sızma testleriyle oturum numaralarının tahmin edilebilmesi kolaylaşmaktadır.

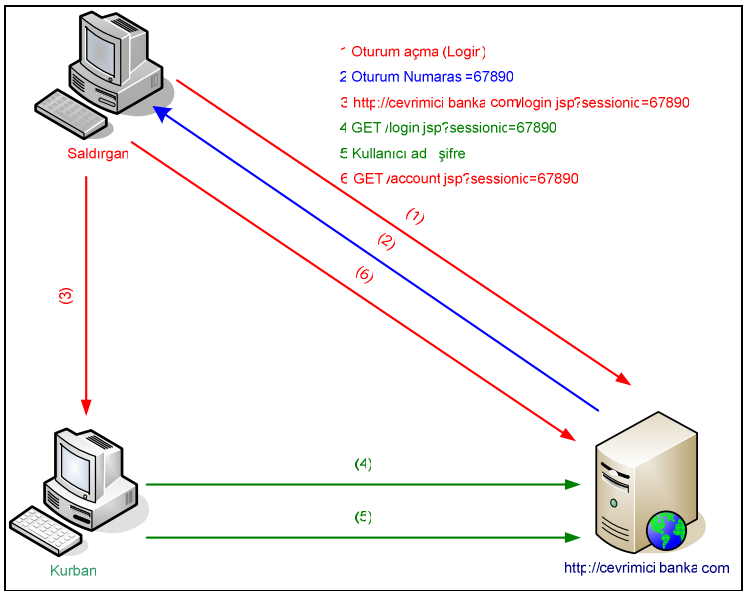
Bilgisayar ortamlarındaki paylaşım (birden fazla kişinin bir bilgisayara sınırsız olarak fiziksel erişim sağlayabildiği durum), yetersiz oturum sonlandırma bir başkasının web aktivitelerini gözlemleme amacıyla istismar edilebilir. Eğer bir sitenin oturum kapama fonksiyonu, oturumu sonlandırmadan sitenin ana sayfasına kullanıcıyı gönderiyorsa, başka bir kullanıcı web tarayıcısının eski sayfalarına ulaşır ve bir önceki kullanıcı tarafından erişilen sayfaları görebilir. Kurbanın oturum bilgisi sonlandırılmadığından, saldırgan, kurbanın oturumunu sisteme herhangi bir kimlik doğrulama bilgisi sunmadan kullanabilir [207].

5.2.4. Oturum sabitleme

Oturum sabitleme yönteminin kullanıldığı sızma testlerinde, daha önceden belirlenen oturum numarasının zorlama yöntemlerle kurbanlar tarafından benimsenmesi

amaçlanmaktadır. Hedef web sitesinin sağladığı fonksiyonlara göre değişen birçok saldırı tekniği (XSS, önceki http erişimleri, vb.) oturum bilgisini belirli bir değere sabitlemek amacıyla kullanılabilir. Kullanıcının oturum bilgisi belirlenip, kullanıcı web sitesine giriş yaptıktan sonra saldırgan, kurbanın sistem tarafından oluşturulan kimliğini ele geçirmek için önceden belirlenmiş oturum bilgisini kullanır.

Genel olarak, oturum bilgileriyle ilgili iki çeşit oturum yönetim sistemi mevcuttur. Birincisinde, kullanıcının web tarayıcısında (client side), oturum numaralarının belirlendiği ve korunmasız olarak tutulduğu güvenlik açısından tercih edilmemesi gereken sistemlerdir. İkincisinde ise sadece sunucu tarafında (server side), oturum numarasının belirlendiği güvenilir sistemlerdir. Kullanıcı tarafında oturum bilgisinin tutulduğu ve üretildiği sistemlerde rastgele üretilen oturum bilgisi web sitesiyle temas kurulmadan belirlenmektedir. Sunucu temelli oluşturulan oturum numaralarında, saldırganın web sitesi ile belirli aralıklarda iletişime geçerek ve aktivitesiz geçen süre sonunda oturumun kapanmaması için sunucu bilgisayarla senkronize olarak oturumun sonlandırılmamasını önlemelidir [208].



Şekil 5.7. Oturum sabitleme adımları

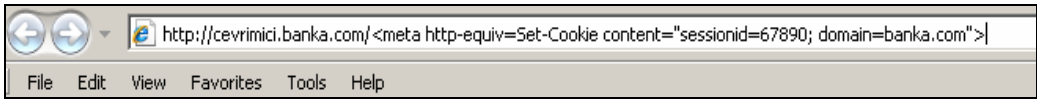
Oturum sabitleme yönteminin kullanıldığı sızma testleri, Şekil 5.7'de gösterildiği gibi Adım (1)'den, (2)...(6)'ya kadar olan altı adımda yapılmaktadır. Adım (1)'de,

sızma testi yapılacak bilgisayar üzerinden hedef web sitesine geçerli bir oturum açılır. Sunucu temelli oluşturulan oturum numaralarında, oturum bilgisinin web sunucusu tarafında geçerliliğini koruması için, web sitesiyle tekrarlanan bir bağlantının kurulması gerekmektedir. Adım (2)'de, hedef web sitesinden geçerli bir oturum numarası tahsis edilir. Adım (3)'de, tahsis edilen oturum numarası kurbanın web tarayıcısına hileli yöntemlerle gönderilerek kullanıcının oturum numarasını kendi bildiği bir değere sabitlemiş olur. Adım (4)'de, kullanıcının hedef web sitesine girmesi beklenir. Beşinci adımda, kullanıcı web sitesine girdiğinde sabitlenen oturum numarasını kullanmaya başlamıştır. Altıncı ve son adımda ise oturum test bilgisayarı üzerine alınarak kurbanın kimliği elde edilir ve hedef web sitesi üzerinde kurbanın kimliğiyle işlem yapılabilir.

Kullanıcı bilgisayarlarında oturum sabitlenmesi için kullanılan yöntemler aşağıda açıklanmıştır. Yeni oturum bilgisinin kullanıcı bazlı kodlar kullanılarak dağıtılması yoluyla hedef web sitesinde mevcut bulunan siteler arası kod çalıştırma açığı kullanılarak, çerez değerinin sabitlenmesi işlemi yapılabilir. Çerez değerinin sabitlenmesiyle ilgili örnek Şekil 5.8'de gösterilmiştir.

Şekil 5.8. Çerez değerinin sabitlenmesi

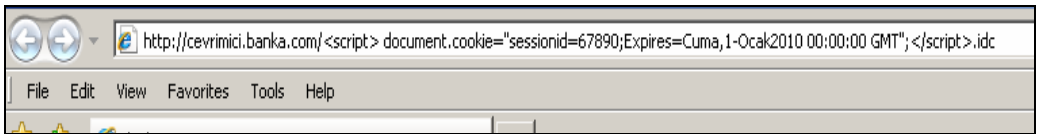
HTML kodu üzerinde yapılan değişiklikler aracılığıyla oturum çerezlerinin kullanıcı web tarayıcısına Şekil 5.9'da gösterildiği gibi gönderilmesi sağlanır.



Şekil 5.9. Oturum çerezlerinin kullanıcı web tarayıcısına gönderilmesi

HTTP cevap başlığı ile çerez dağıtma yöntemiyle aynı etki alanındaki hedef web sitesinin veya başka bir sitesinin çerez dağıtması zorlanır. Çerez dağıtmanın, hedef sunucu dışındaki sunucularla yapılabilmesi birçok yöntemle gerçekleştirilebilir. Bu

yöntemler; aynı alandaki farklı bir web sunucunun kırılması, kullanıcının DNS sunucusunun zehirlenerek saldırganın sahibi olduğu web sitesinin etki alanına dâhil edilmesi, etki alanında kötü niyetli başka bir web sunucusu kurma, HTTP araya girme saldırısının kullanılması olarak sıralanabilir. Kullanıcı bilgisayarlarında kalıcı oturum çerezleri kullanılarak, oturumun bilgisayar tekrar açıldığında bile sabit kalmasıyla ilgili örnek Şekil 5.10'da gösterilmiştir.



Şekil 5.10. HTTP cevap başlığı ile çerez dağıtma

5.3. Kullanıcı Taraflı Sızma Testleri

Kullanıcı taraflı sızma testleri, web sitesi ve kullanıcı arasında kurulan güvenin istismar edilmesi üzerine odaklanır. Yasal olan web siteleriyle, kullanıcıları arasında teknolojik ve psikolojik bir güven kurulmaktadır. Kullanıcı, web sitesinin geçerli içerik sunmasını beklerken web sitesinden bir saldırı gelmesini beklemez. Kullanıcı taraflı sızma testleri, içerik sahteciliği ve siteler arası kod çalıştırma olmak üzere iki sınıfta takip eden alt başlıklarda incelenmiştir.

5.3.1. İçerik sahteciliği

İçerik sahteciliği (Content Spoofing), kullanıcının ziyaret ettiği dinamik içerikli web sitesinde harici olarak çalışan web uygulamasının ziyaret edilen web sitesinin resmi içeriği olduğuna inandırılmasını sağlayan sızma testi yöntemidir. Bu yöntem kullanıcı ile web sitesi arasındaki güveni istismar ederek giriş formları, tahrif edilmiş içerik ve yanlış yayın sürüm bilgileri içeren sahte web siteleri oluşturmak için kullanılmaktadır. Bu yöntemde sazan avlama teknikleri sıklıkla kullanımaktadır.

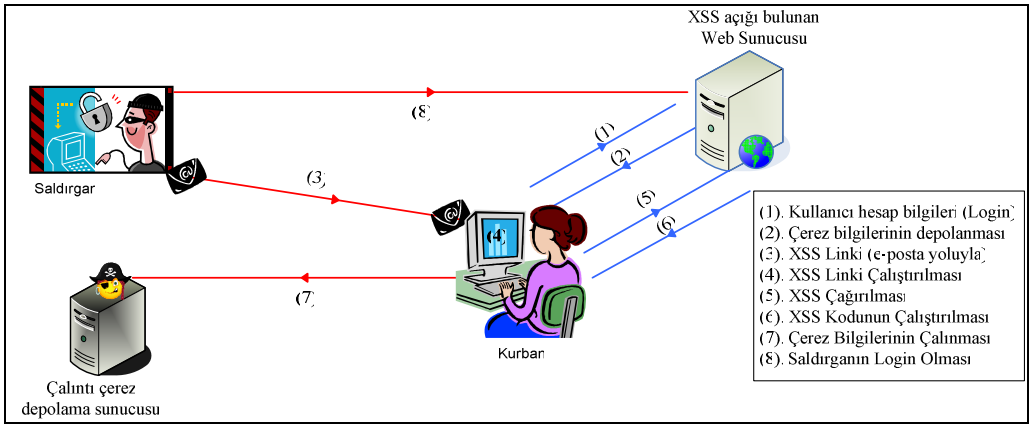
Örneğin, web sitesi içerisinde yer alan herhangi bir çerçeve kaynağının yeri "<frame src=http://deneme.com.tr/havadurumu.html>, ise içerik sahteciliği yöntemiyle "frame_src" parametresinin değeri "frame_src=http://saldiri.com.tr/sahte.html"

değeri ile değiştirildikten sonra e-posta, anında mesajlar, duyuru panoları mesajları veya diğer yollardan kullanıcıya gönderilir. Kötü içerikli URL adresini kullanıcının ziyaret etmesi sağlanırsa, kullanıcı doğru içeriğe ulaşmadığı halde ulaştığına inanır ve içerik sahteciliği yöntemi başarıyla uygulanmış olur. Kullanıcılar, sahte içeriğe güvenirler çünkü tarayıcının adres kısmında ziyaret edilen sitenin adresi yazılıdır. Web sayfası hizmeti esnasında, web tarayıcısının adres kısmında kullanıcının beklediği alana ait adres bulunmasına rağmen yabancı içerik bu yöntem sayesinde normal içerikle örtülmüştür.

5.3.2. Siteler arası kod (XSS) yazma

Siteler arası kod yazma yöntemiyle yapılan sızma testleri, kullanıcı ile web sitesi arasındaki güven ilişkisi istismar edilerek, web sitesinin sızma ekibi tarafından belirlenen çalıştırılabilir kodu kullanıcıya göndermesi ve bu kodun kullanıcı web tarayıcısında yüklenerek çalışmasıyla gerçekleşmektedir. XSS yöntemiyle yazılan küçük kodlar, HTML kodları arasına enjekte edildiğinden bazı kaynaklarda bu yöntemin adı HTML kod enjeksiyonu olarak adlandırılmaktadır. XSS kodları genellikle HTML/JavaScript dilinde yazılmaktadır, ancak VBScript, ActiveX, Java, Flash veya web tarayıcılar tarafından desteklenen diğer dillerdede kodlama yapılabilmektedir [209].

XSS yöntemiyle zararlı kodun kullanıcı web tarayıcısında çalıştığında, zararlı kod sunucu web sitesinin tarayıcı için tanımlı olduğu güvenlik ayarları kapsamında çalışacaktır. Eğer web tarayıcısı üzerinde herhangi bir kısıtlamaya gidilmemişse zararlı kod vasıtasıyla tarayıcı tarafından erişilen her türlü hassas veri okunabilir, değiştirilebilir ve e-posta aracılığıyla farklı yerlere iletilebilir. XSS yöntemiyle kullanıcı bilgisayarı üzerindeki oturum çerezleri çalınabilir, kullanıcının web tarayıcısı başka bir adrese yönlendirilebilir, web siteleri üzerinde bilgi toplama amaçlı kodlar çalıştırılabilir, sazan avlama yöntemine davetiye çıkartılır, web sayfalarının değiştirilmesi veya hizmet aksattırma saldırılarının yapılmasını sağlamaktadır. XSS saldırı yöntemi şematik gösterimi Şekil 5.11'de verilmiştir.

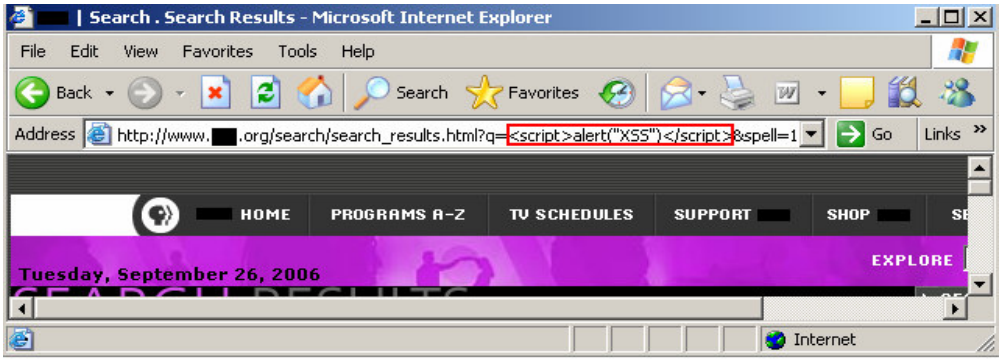


Şekil 5.11.XSS yönteminin mantıksal gösterimi

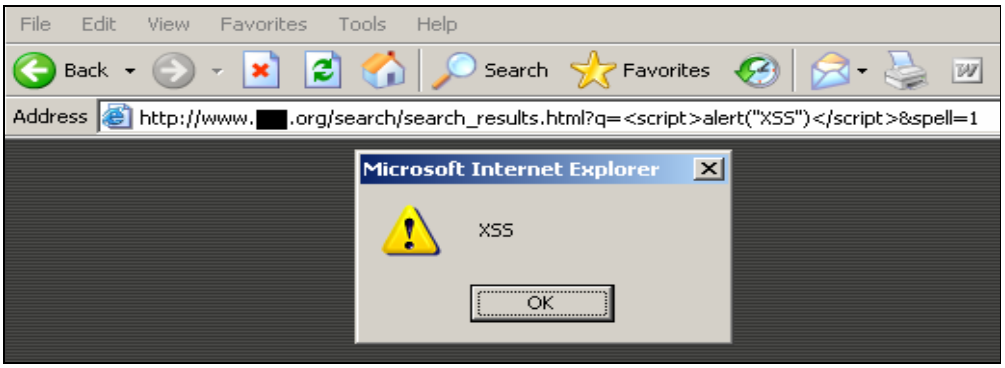
Şekil 5.11'de görüldüğü gibi XSS yönteminde Adım(1)'de kullanıcının şifre ve parolasını kullanarak web uygulamasına giriş yapması sonucunda (1), kullanıcıya ait hesap bilgileri çerez formatında kullanıcı bilgisayarında saklanmak üzere XSS açığı bulunan uygulama sunucu bilgisayarından kullanıcı bilgisayarına gönderilmektedir (2). Saldırgan XSS zafiyetini kullanan URL (Uniform Resource Locator)'yi sazan e-posta aracılığıyla kurbana göndererek (3), XSS açığı bulunan web sunucusuna gitmesini sağlayacak bağlantıya tıklamasını sağlar (4). XSS açığının bulunduğu sayfanın çağırılmasıyla (5), XSS saldırısı yapılmasını sağlayacak kod çalıştırılır (6). XSS kodunun çalıştırılmasıyla kullanıcı bilgisayarında daha önceden depolanan çerez bilgileri çalınarak saldırganın denetiminde olan sunucu bilgisayarına depolanır (7). Çalıntı çerez depolama sunucusundaki kullanıcı erişim bilgilerinin yer aldığı çerez saldırgan tarafından kullanılarak web uygulamasına kurbanın kullanıcı haklarıyla erişir (8).

XSS yöntemleri kalıcı, geçici ve DOM (Document Object Model) temelli olmak üzere üç farklı kategoride sınıflandırılmaktadır [210].

Kalıcı olmayan XSS yöntemi, kullanıcının zararlı kod içeren özel olarak değiştirilmiş linkleri ziyaret etmesini gerektirir. Link ziyaret edildiğinde, URL içine gömülü zararlı kod, istemci tarafına gönderilir ve kod kullanıcının web tarayıcısında çalışır. Kalıcı olmayan XSS yöntemiyle ilgili örnek Şekil 5.12'de gösterilmiştir.



(a)



(b)

Şekil 5.12. Kalıcı olmayan XSS kodu işlemleri a) Kodlama b)İcra ettirme

Şekil 5.12 (a)'da XSS açığı bulunan bir web sitesinde arama yapılmasını sağlayan HTML kodları arasına yerleştirilen XSS kodu web tarayıcısının adres kısmında kırmızı dikdörtgen içerisinde gösterilmektedir. Bu şekilde hazırlanan linkin kullanıcılar tarafından ziyaret edilmesi sağlandığında XSS yöntemiyle sızma testi Şekil 5.12 (b)'de gösterildiği gibi başarıyla gerçekleştirilmiş olacaktır.

Kalıcı XSS yöntemi, mesaj panoları, ziyaretçi defterleri, tartışma forumları, web posta mesajları gibi kullanıcı tarafından web sitelerine girdi yapılabilecek hedefler seçilerek zararlı kodların sunucu tarafında XML dosyaları veya veri tabanlarında depolanmasıyla sağlanır. Bu sızma yönteminde kullanıcının herhangi bir linke tıklamasına gerek yoktur, sadece zararlı kodu içeren web sayfasının tarayıcıda çalışması yeterlidir. Kalıcı XSS yöntemiyle zararlı kod hedef web sitesine

sızdırıldıktan sonra; hedef web sitesini ziyaret eden geniş bir kullanıcı kitlesi bu durumdan etkilenmektedir.

DOM temelli XSS yönteminde, dinamik web sayfaları üzerinde çalışan diğer XSS yöntemlerinden farklı olarak sunucu tarafına zararlı kod gönderilmesine ihtiyaç duyulmayan, kullanıcı tarafında çalıştırılan kod parçalarını içerir [211]. Bu yöntemle yapılan sızma testlerinde kullanıcının web tarayıcısında etkili olacak DOM nesneleri (document.location, document.URL, document.referrer, vb.) kullanılmaktadır.

5.4. Komut Çalıştırma

Komut çalıştırma yöntemi, web uygulamalarında uzaktan çalıştırılan komutlar yardımıyla yapılan sızma testleridir. Web uygulamaları HTTP üzerinden gelen istekler (kullanıcı girdileri) doğrultusunda nasıl davranacağına karar vermektedir. Çoğu zaman bu kullanıcı girdileri dinamik web sitesi içeriğinin hazırlanılmasında kullanılan komutların çalıştırılmasını sağlarlar. Eğer dinamik web sitelerinin içeriğinin hazırlanmasında kullanılan bu komutların kodlanmasında güvenlik ölçütleri göz önüne alınmaz ve girdi doğruluğu sınanmazsa, çalıştırılan komutların saldırganlar tarafından manipüle edilmesi sonucu web siteleri üzerinde güvenlik ihlalleri oluşur. Komut çalıştırmada karşılaşılabilecek güvenlik ihlalleri takip eden alt başlıklarda açıklanmıştır.

5.4.1. Ara bellek taşması

Ara bellek taşması (buffer overflow) yöntemi, uygulamalarda kullanılmak üzere hafızada ayrılan alanlara tahsis edilen büyüklüklerin üzerinde veri gönderilmesiyle uygulama akışının değiştirilmesinde kullanılır. Ara bellek taşması, uygulamalar içerisinde hata ile sonuçlanan genel bir yazılım kusurudur [212]. Bellek taştığında, komşu hafıza bölgelerinin üzerine yazılarak hatalara veya uygulamaların çalışmamasına neden olur. Bellek taşması yazılımcılar tarafından kontrol edilmediği takdirde saldırganlar tarafından özel olarak hazırlanan girdilerle istismar edilerek birçok güvenlik ihlâlinin oluşmasına neden olur.

Uygulamalar veya sunucu bilgisayarlar üzerinde bellek taşması yöntemiyle yapılan sızma testleri sonucunda, web uygulamalarının çalışması aksayacağından testlerin uygulamaların kopyaları üzerinde yapılması gerekmektedir. Bellek taşması hizmet aksattırma dışında, yığın işaretçilerinin (stack pointer) üzerine yazmak suretiyle programı yeniden yönlendirmek, zararlı kodlar çalıştırmak ve program parametrelerinin değiştirmek için de kullanılmaktadır. Bellek taşması açıklıkları, genel olarak web sunucular üzerinde etkili olmaktadır. Bellek taşması açıklıkları genellikle C ve C++ gibi programlama dillerinde meydana gelmektedir. Bu açıklıkların meydana geldiği programları kullanan web sayfasında bellek taşmalarında daha dikkatli olunmalıdır.

5.4.2. Dizgi formatı

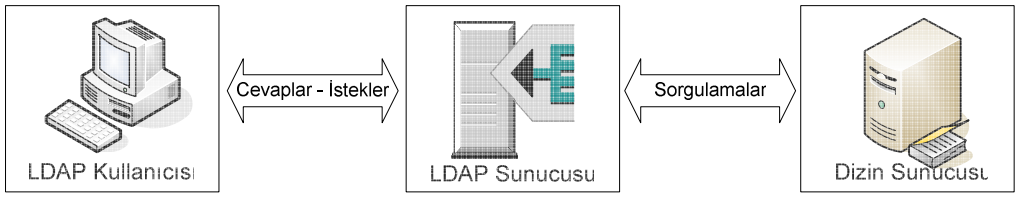
Dizgi formatı (Format String) yöntemi, programlama dilleri kütüphanesinde yer alan özellikler sayesinde hafızanın diğer bölümlerine ulaşarak web uygulamasının akışının değiştirilmesini sağlar. Dizgi formatı açıklıkları, genellikle kullanıcı taraflı verilerin programlama dilleri (C, C++) fonksiyonlarının (fprintf, printf, scanf, fscanf, syslog, vb.) doğrudan kullanılması sonucunda oluşmaktadır. Sızma testleriyle, fonksiyonlar için anlam içeren bilgiler (%s, %x, vb.) kullanılarak bellekten bilgiler okunmaya çalışılır.

Web uygulamasına fonksiyonlara ait parametrelerden (%s, %x, vb.) oluşan bir dizgi formatı verilirse, web sunucudaki rasgele herhangi bir kodun çalıştırılmasına, yığından değer okunup atılmasına, kesme (interrupt) hataları sonucu web uygulamalarının çalışmamasına sebep olur. Örneğin, bir web uygulaması, kullanıcı tarafından belirlenen bir e-posta değişkenin değerini printf fonksiyonunu kullanarak, printf (E-posta Adres) şeklinde yazdırıyorsa ve e-posta adresi ile gönderilen parametre, biçim karakterlerini içeriyorsa, printf bu karakterleri tanır ve sonradan verilen parametreleri kullanır. Eğer böyle parametreler bulunmazsa, veri yığından, printf fonksiyonunun beklediği sırada uygun olarak alınır ve kullanılır. Dizgi formatı yöntemiyle sızma yöntemlerinin olası kullanımları aşağıda özetlenmiştir [213]:

- *Yığından veri okumak*: Eğer printf fonksiyonunun çıktı akışı geri sunuluyorsa, "%x" değiştirme karakterini (bir veya daha fazla kez) yollayarak yığındaki değerleri okuyabilir.
- *Hafızada işleme ayrılan bölümden karakter dizileri okumak*: Eğer printf fonksiyonunun çıktı akışı geri sunuluyorsa, saldırgan, "%s" değiştirme karakterini kullanarak rasgele hafıza bölgelerindeki karakter dizilerini okuyabilir.
- *Hafızada işleme ayrılan bölümdeki yerlere tamsayı yaz*mak: "%n" değiştirme karakterini kullanarak, hafızadaki herhangi bir bölgeye bir sayı değeri yazabilir. Programın erişim ayrıcalıklarını kontrol eden değerlerin veya fonksiyonların dönüş adreslerinin üzerine yazmak buna örnel olarak verileiblir.

5.4.3. LDAP enjeksiyonu

LDAP (Lightweight Directory Access Protocol) X.500 dizin servislerini kullanıcı sunucu mimarisinde düzenlemeye ve sorgulamaya yarayan açık standartlı bir protokoldür [214]. LDAP enjeksiyonu yöntemi, kullanıcı girdilerinden LDAP cümleleri oluşturan dinamik web sitelerinin zafiyetlerinin kullanılmasını sağlayan bir sızma test tekniğidir. LDAP sunucusu aracılığıyla kullanıcılar (web tarayıcı, e-posta kullanıcısı, e-posta sunucusu, vb.), farklı işletim sistemleri üzerinde çalışan dizin servisleri üzerinde sorgulamalar (yetkilendirme, kimliklendirme, vb.) yapmaktadırlar. LDAP çalışma mimarisi Şekil 5.13'de gösterilmiştir.



Şekil 5.13. LDAP çalışma mimarisi

LDAP protokolü TCP/IP protokol kümesi üzerinde çalışmaktadır. Web uygulamaları, dinamik web taleplerini karşılamak için, kullanıcı girdileri ile oluşturulan LDAP sorguları kurar ve kullanırlar. Eğer kullanılan bu kullanıcı girdileri düzgün bir şekilde denetlenmezse, LDAP sorgusunun oluşumu kötü niyetli insanlar tarafından değiştirilebilir. LDAP sorguları, sorgulama isteğinde bulunan bilgisayarın

(Veritabanı sunucusu, Web uygulaması sunucusu, Web sunucusu) haklarıyla çalışır. Bu hakların kullanılmasıyla LDAP ağacındaki herşeyin sorgulanmasını, değiştirilmesini veya silinmesini sağladığından, yüksek seviyeli güvenlik ihlâllerine sebep olmaktadır. Benzer gelişmiş sömürü teknikleri bu bölümde ayrıntılı bir biçimde açıklanacak olan LDAP enjeksiyonuna benzer bir şekilde uygulanabilen SQL enjeksiyonu için de geçerlidir.

Örneğin http://ybv.com.tr/ldapsearch.asp?kullaniciID=* şeklindeki URL adresinde kullaniciID parametresi olarak "*" karakteri web tarayıcıdan istendiğinde, sorgulama sonucunda kullaniciID özelliği bulunan her nesnenin LDAP aracılığıyla döndürülmesi sağlanacaktır. Bu ve buna benzer örnekler sızma testlerinin amacı doğrultusunda çoğaltılabilir.

5.4.4. İşletim sistemi komut enjeksiyonu

İşletim sistemi komut enjeksiyonu (OS Commanding Enjection) tekniği, bazı kaynaklarda dizin takibi (Directory Traversal) olarak da adlandırılmaktadır. Bu sızma yöntemiyle, web tarayıcılar üzerinden yapılan kullanıcı girdilerinin manipüle edilmesiyle işletim sistemi seviyesinde komutların çalıştırılarak web sitelerinin güvenlik açığının istismar edilmesi hedeflenmektedir.

Web uygulaması, kullanıcı girdilerini uygulama kodunda kullanmadan uygun yöntemlerle denetlemelidir. Kullanıcı girdileri düzgün bir biçimde denetlenmediği takdirde, uygulamaları işletim sisteminin komutlarını çalıştıracak biçimde kandırmak mümkündür. Kullanıcı girdileriyle çalıştırılan işletim sistemi seviyesindeki komutlar o anki uygulamayı çalıştıran sunucunun (Veritabanı sunucusu, Web uygulaması sunucusu, Web sunucusu) haklarıyla çalışır.

Örneğin, girdi kontrolü düzgün olarak yapılmayan bir web uygulamasının orijinal URL adresi:

http://ybv.com.tr/cgi-bin/bilgigoster.pl?isim=Ali&degisken=ber1.txt ise;

Web uygulamasına /bin/ls komutu enjekte edilmesi

http://ybv.com.tr/cgi-bin/bilgigoster.pl?isim=Ali&degisken=/bin/ls|

şeklinde olur.

Birçok betik (script) dili, değişik çalıştırılabilir (exec) fonksiyonları kullanarak, programcıya yürütme esnasında işletim sistemi komutları çalıştırma izni verir. Eğer bir web uygulaması kullanıcı kaynaklı girdinin denetlenmeden böyle bir fonksiyon çağrısının içerisinde kullanılmasına izin verirse, uzaktan işletim sistemi komutları çalıştırması mümkün hale gelir.

5.4.5. SQL (Structured Query Language) enjeksiyonu

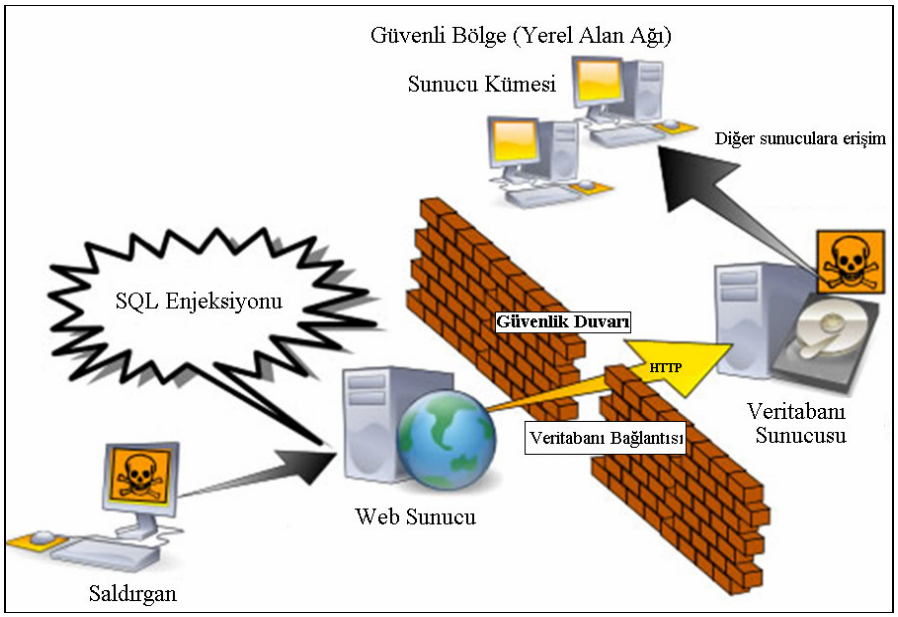
SQL veritabanları, sorgu yapmak üzerine özelleşmiş hem ANSI hem de ISO standardı olan yapısal bir programlama dilidir. Değişen büyüklükteki ilişkisel veritabanı uygulamalarına SQL sorguları aracılığıyla ulaşılabilir. SQL'i destekleyen birçok veritabanı ürünü (Oracle, MS SQL Server, MS Access, Ingres, DB2, Sybase, Informix, vb) standart dile özel eklentiler getirir [215]. Web uygulamaları kullanıcı kaynaklı girdileri, dinamik web sayfası talepleri için, değişik SQL cümleleri oluşturmada kullanabilir.

SQL enjeksiyonu yöntemi, kullanıcı girdilerine göre SQL cümleleri oluşturan web sitelerinde, kullanıcı kaynaklı girdilerin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin manipüle edilmesini sağlayan sızma testleridir [216]. SQL enjeksiyonu sızma yöntemiyle yapılabilecek işlemler aşağıda sıralanmıştır.

- Veri tabanları üzerinde istenmeyen işlemler (sorgulama, ekleme, silme, değiştirme, vb.) yapılabilir.
- Kimlik doğrulama mekanizmaları atlatılabilir.
- İşletim sistemi seviyesinde komutlar çalıştırılabilir.
- Etki alanında yeni kullanıcılar veya gruplar oluşturulabilir.

Eğer bir web uygulaması, kullanıcı kaynaklı girdiyi etkin bir biçimde denetlemezse, SQL enjeksiyon yöntemiyle arka taraftaki SQL cümlesi oluşumu değiştirilerek

güvenlik ihlalleri oluşturulabilir. SQL enjeksiyon yöntemiyle SQL cümlesi değiştirilerek bilgisayar sistemlerine sızılması durumunda, SQL servisini çalıştıran kullanıcı haklarına sahip olunacaktır. Veritabanı üzerinde bu haklara sahip olan kişi ileri derece sızma teknikleri kullanarak veritabanı dışındaki diğer sunucu bilgisayarları üzerinde de erişim hakkı kazanabilir.



Şekil 5.14. SQL enjeksiyonu yöntemiyle sızma

Şekil 5.14'de şematik olarak gösterildiği gibi saldırgan hedef web sitesi üzerinde SQL enjeksiyonu yapabileceği dinamik içerikli web sayfalarını tespit ettikten sonra, SQL enjeksiyonu aracılığıyla veritabanı sunucu bilgisayarına veritabanını çalıştıran servisin (muhtemelen üst seviyede erişim hakları bulunan yönetici hesapları) kullanıcı hesabıyla ulaşabilir. Veritabanı sunucu bilgisayarı üzerinde, SQL enjeksiyonu yardımıyla işletim sistemi seviyesinde komutlar çalıştıran saldırganın bir sonraki hedefi diğer bilgisayarlar ve özellikle sunucular olacaktır. Saldırgan, diğer sunucu bilgisayarlarına veritabanı kullanıcı hesabıyla bağlantı yaptıktan sonra tüm sunucu bilgisayarlara daha sonra doğrudan bağlanabilmesi (remote desktop, telnet, http, ftp, vb.) için gerekli olan servisleri kendi kullanımına açabilecek ve saldırıdan beklediği sonuçları elde edebilecektir.

SQL enjeksiyonu yapılırken SQL'e özel anlam içeren karakterlerin kullanılması gereklidir. Bu karakterler ve kısa açıklamaları Çizelge 5.1'de gösterilmiştir.

Çizelge 5.1. SQL enjeksiyonu karakterleri

Karakter	Açıklama
' veya "	String ayracı
-- veya #	Tek satırlık açıklama
/*…*/	Çok satırlı açıklama
+	Ekleme, birleştirme (URL adresi içerisinde boşluk)
||	Birleştirmek
%	Genel (wildcard) özellik ayracı
?Param1=foo&Param2=bar	URL Parametresi
PRINT	Cevap gerektirmeyen komutlar
@variable	Yerel değişken
@@variable	Bölgesel değişken
wait for delay '0:0:10'	Zaman geciktirme

SQL enjeksiyonun anlaşılabilmesi için birçok web sitesinde kullanılan web tabanlı kimlik doğrulama formları üzerinde bu yöntem basit olarak açıklanacaktır. Güvenlik kriteri gözönüne alınmadan geliştirilen birçok web uygulamasında kimlik doğrulama için Şekil 5.16'dakine benzer bir yapıda SQL cümlesi kullanılmaktadır.

Şekil 5.15. Bir SQL cümlesi

Şekil 5.15'de gösterilen SQL cümlesinde, uygulama geliştirici, kullanıcı girdisini hiçbir denetime sokmadan formdan alıp doğrudan SQL sorgusunun içine yansıtmaktadır. Bu durum SQL enjeksiyonu yönteminin başarılı olabilmesi için gerekli olan ortamın saldırganlara sağlanması anlamına gelmektedir. Web formu üzerinde yer alan "kullanıcı adi" ve "şifre bilgileri" Şekil 5.16'da gösterildiği gibi girilirse SQL enjeksiyonu yöntemi başarıyla uygulanmış olur.

Şekil 5.16. SQL enjeksiyonu kullanıcı girdisi

Arka planda kimlik doğrulaması için çalışacak olan SQL sorgusunun son hali Şekil 5.17'de gösterilmiştir.

Şekil 5.17. Kimlik doğrulamanın atlatılması (by-pass)

Şekil 5.17'de gösterilen SQL cümlesi ile 1=1 değeri kullanıcı adı için doğru bir sonuç döndürecek "--" ise kendisinden sonraki gelen söz diziminin SQL tarafından açıklama kabul edilerek çalıştırılmamasını sağladığından parola girme zorunluluğunu ortadan kaldıracaktır. Şekil 5.15'de gösterilen SQL cümlesinin çalıştırılması sonucunda kullanıcılar listesindeki ilk kullanıcı olarak sisteme girilecek ve kimlik doğrulama mekanizması devre dışı bırakılacaktır.

SQL enjeksiyon yöntemiyle veritabanlarından bilgilerin okunabilmesi için

- Sorgu kurcalama (yeniden yapılandırma veya yönlendirme),
- Hata mesajlarının kullanılması ve
- Kör (Blind) enjeksiyon

olmak üzere 3 yaklaşım kullanılmaktadır. Bu yaklaşımlar aşağıda alt başlıklar halinde açıklanmıştır.

Sorgu kurcalama

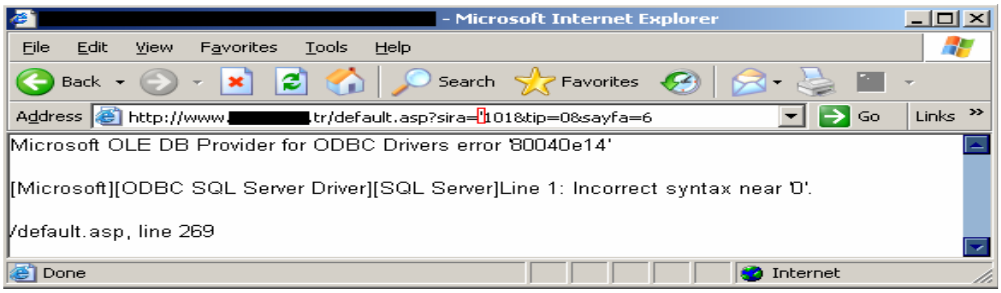
Sorgulamaların yeniden yapılandırılması veya yönlendirilmesi yöntemiyle, sızma testlerinin yapılabilmesi için izlenmesi gereken standart bir yol yoktur. Bu yöntemle veritabanlarından bilgi okunabilmesi için web uygulamalarının kodlamasındaki zafiyetlerin durumuna bağlı olarak değişir.

Hata mesajlarının kullanılması

Hata mesajlarının kullanılması yöntemiyle yapılan sızma testleri, bilinçli olarak veritabanı sunucusuna hata mesajı verdirilmesi esasına dayanır. Veritabanı

sunucusuna verdirilecek hatalarla veritabanının çözümlenmesi ve sonrasında bilgilerin okunması için izlenmesi gereken yol aşağıda maddeler halinde yazılmıştır. Ayrıca bu tez çalışması kapsamında yapılan web uygulamaları, sızma testlerinden bu kısımda örnekler verilecektir. Yapılan araştırmalar sonucunda web uygulamaları tarafından en fazla kullanıldığı tespit edilen MS SQL veritabanı üzerinde yapılan testlere odaklanılmıştır. Bu testler aşağıda açıklanmıştır.

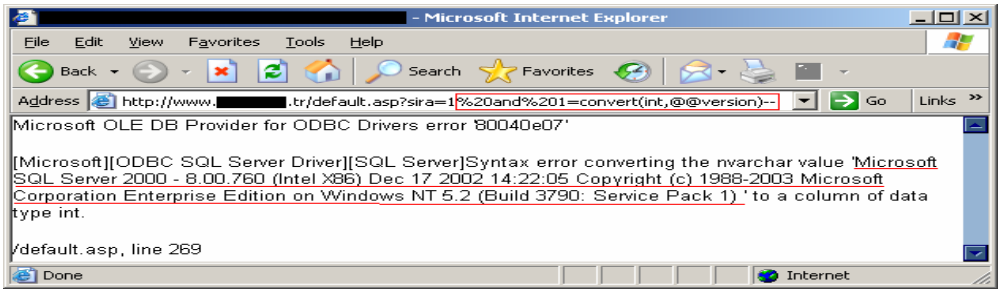
Açığın tespit edilmesi: SQL enjeksiyonunun yapılabilmesi için dinamik içerikli web sayfaları (ASP, JSP, PHP, CGI, vb.) içerisinde yer alan web form alanları, URL'nin parçası olarak gönderilen sorgu cümleleri, web uygulamalarına gönderilen çerez değerleri, gizli alanlar gibi parametreler içerisinde zafiyet taramaları elle (manüel) ve otomatik araçlar vasıtasıyla yapılır. SQL enjeksiyon sızma yönteminde, Çizelge 5.1'de verilen SQL enjeksiyon karakterleri, web vekâlet yazılımları (web proxy), karıştırıcı (fuzzer) yazılımları kullanılarak veritabanları hata mesajı verdirmeye zorlanır. SQL enjeksiyonun tespit edilmesine dair örnek Şekil 5.18'de gösterilmiştir. Bu örnekte ASP uzantılı dinamik web sayfası içerisinde "sira" parametresinden tek tırnak işaretçisi gönderildiğinde SQL hatası alınmakta ve enjeksiyon noktası belirlenmektedir.



Şekil 5.18. SQL enjeksiyon açığı tespit ekranı

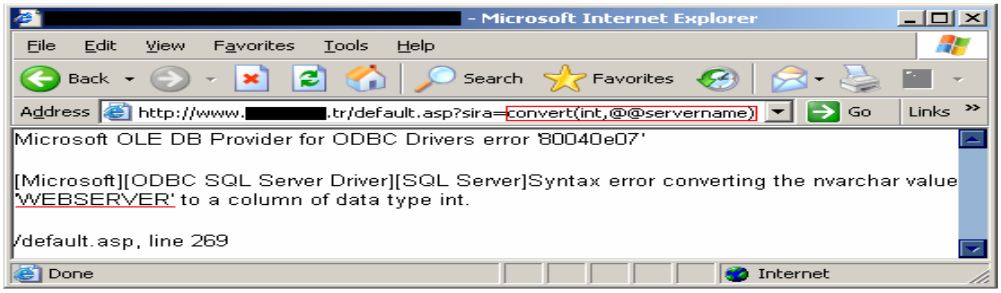
MS SQL versiyonun belirlenmesi: MS SQL veritabanının hangi versiyonun kullanıldığı, veritabanının yamalarının güncel olup olmadığı, SQL veritabanı sunucusunun enjeksiyon açığı dışında başka açıklarının tespit edilmesi açısından önemlidir. MS SQL versiyonunun belirlenmesinde "VERSION" komutu kullanılmaktadır [218]. Bu komutla, Şekil 5.19'da gösterildiği gibi versiyon bilgisine

ek olarak işlemci mimarisi, versiyon yayınlanma tarihi ve işletim sistemi hakkında bilgilerde elde edilmektedir.



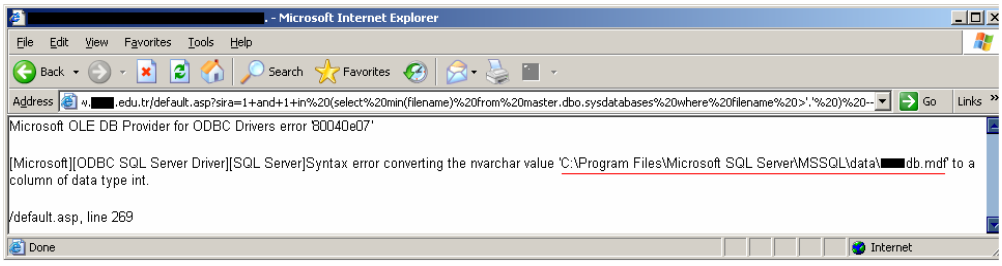
Şekil 5.19.MS SQL versiyonu belirleme ekranı

Sunucu isminin belirlenmesi: MS SQL veritabanı sunucusunun yerel isminin belirlenmesi için "SERVERNAME" komutu kullanılır [219]. Sunucu isminin "SERVERNAME" komutu ile bulunması Şekil 5.20'de gösterilmiştir.



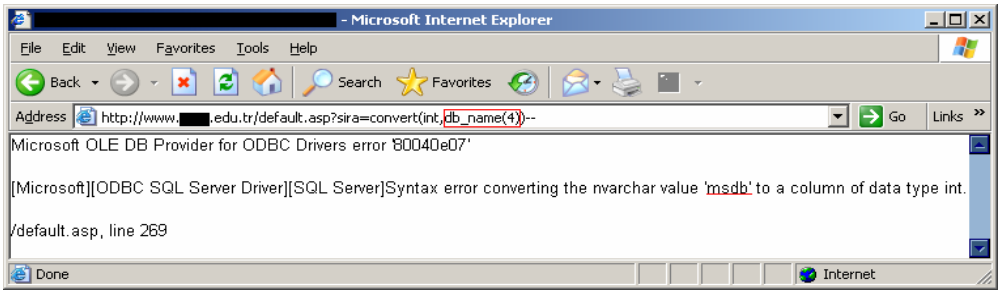
Şekil 5.20. MS SQL sunucu makinesinin adını belirleme ekranı

Veritabanının disk içerisinde yerinin tespit edilmesi: Veritabanının disk içerisindeki yerinin bulunmasında Şekil 5.21'de gösterildiği gibi "FILE_NAME" komutu kullanılmaktadır [220].



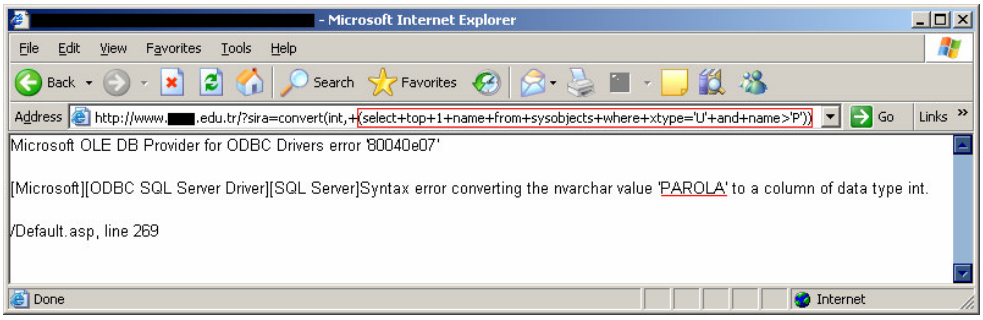
Şekil 5.21. Veritabanı dosyasının disk üzerindeki yeri gösterim ekranı

Veritabanı isimlerinin belirlenmesi: Veritabanı isimlerinin belirlenmesinde "DB_NAME(X)" komutu kullanılmaktadır [221]. Bu komut sayesinde veritabanlarının ismi X değişkenine değerler verilerek Şekil 5.22'de gösterildiği gibi elde edilmektedir. X değişkenine herhangi bir değer atanmazsa o anda kullanılan veritabanı ismi döndürülür.



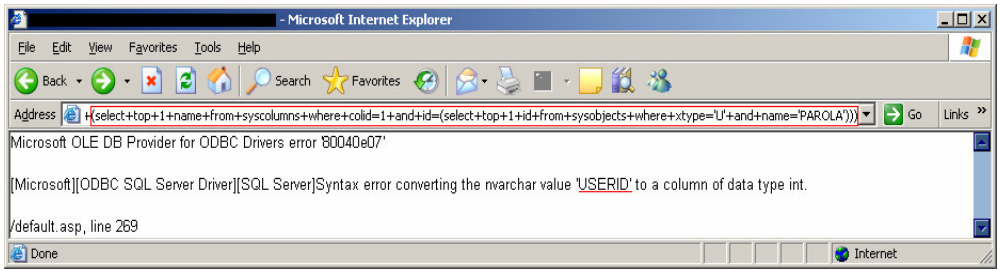
Şekil 5.22. Veritabanları isimleri gösterim ekranı

Tabloların belirlenmesi: Veritabanı içerisinde yer alan kullanıcı tablolarının belirlenmesi için "SYSOBJECT" isimli sistem tablosundan faydalanılır. Bu tablo içerisinde yer alan XTYPE isimli kolonun "U" parametresi (User table) ile kullanıcı tablolarının isimleri alınır [222]. Veritabanı içerisinde yer alan tablo isimlerinin alınması için Şekil 5.23'de verilen SQL cümlesinin kullanılması gerekmektedir.



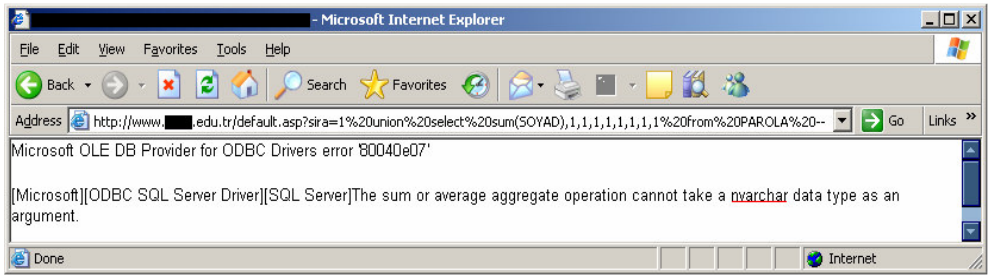
Şekil 5.23. Tablo isimlerini bulma ekranı

Atanan değer kolon sayısından büyük olduğunda veritabanı farklı bir hata mesajı verir ve o tablo içerisinde yer alan kolon isimlerinin tamamı bulunmuş olur [223]. Belirlenen bir tablo içerisinde yer alan kolon isimlerinin bulunması için Şekil 5.24'de verilen SQL cümlesinin kullanılması gerekmektedir.



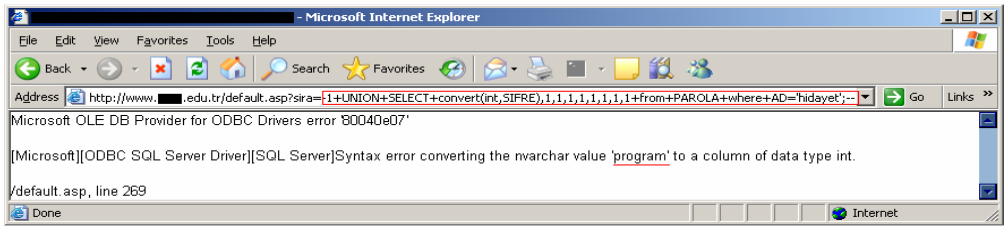
Şekil 5.24. Kolon isimlerini bulma ekranı

Değişken tiplerinin belirlenmesi: Kolonlar içerisindeki alan isimleri belirlendikten sonra bu alanlara ait değişken tiplerinin bulunması için Şekil 5.25'de verilen SQL cümlesinin kullanılması gerekmektedir.



Şekil 5.25. Alan adları değişken tiplerin belirleme ekranı

Bilgi okunması: Veritabanı içerisinden bilgi okunabilmesi için birden fazla SELECT cümlesinin tek bir ifade altında toplanmasını sağlayan "UNION SELECT" komutundan yararlanılmaktadır [224]. "UNION SELECT" komutu ile veritabanından bilgi okunmasıyla ilgili örnek Şekil 5.26'da gösterilmektedir. Bu örnekte gösterildiği gibi veri tabanından istenilen bir alana ait değer okuma işlemi diğer alanlar için de tekrarlanarak istenilen bilgilere bu yöntemle ulaşılması mümkündür.



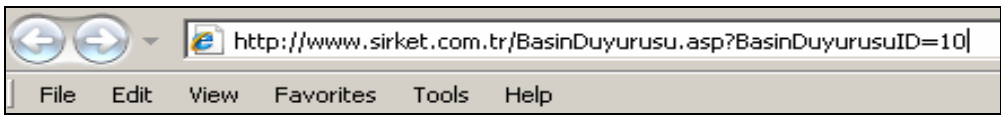
Şekil 5.26. Alan içerik okuma ekranı

Kör (Blind) enjeksiyon yöntemi

Veritabanı hatalarının geliştiriciler tarafından son kullanıcıya gösterilmediği durumlarda kullanılmaktadır. Bu yöntemle SQL enjeksiyon sızma testi yapılması diğer yöntemlere oranla en zor olanıdır. Veritabanı hatalarının gizlenmesi enjeksiyon açığını kapatmamakta sadece açığın tespit edilmesini zorlaştırmaktadır. Kör SQL enjeksiyon yöntemiyle açıkların keşfedilmesinde parametre değerine doğru veya yanlış cümleler girilmesi ortak kullanılan bir yoldur.

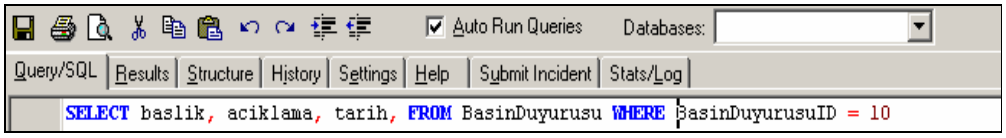
Web uygulamaları genellikle SQL sorgularında kullanıcı girdileri doğrultusunda veritabanından bilgi çekmek için WHERE yan cümlesini kullanmaktadır. WHERE yan cümlesine ek koşullar ekleyerek oluşan yeni SQL cümlesi doğrultusunda, web uygulamasının davranışları değerlendirilir. Değerlendirme sonucunda uygulamada SQL enjeksiyon açığının olup olmadığı tespit edilebilir. Bu durumu bir örnekle açıklamak kör enjeksiyon yönteminin daha iyi anlaşılabilmesi açısından önemlidir.

Kör enjeksiyon yönteminin açıklanması için şirketlerin internet üzerinden yaptığı basın duyuruları ele alınmıştır. Çoğu kurum basın duyurularını web sayfaları üzerinden yapmaktadır. Şirketin 10. basın duyurusuna erişebilmek için URL adresi Şekil 5.27'de gösterildiği gibi olur.



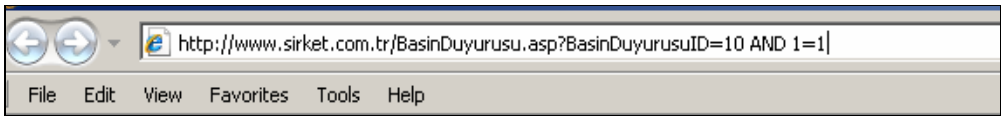
Şekil 5.27. URL adresi

Web uygulaması kullanıcı girdisi vasıtasıyla 10 numaralı basın duyurusunun istendiğini tespit ettikten sonra SQL cümlesi Şekil 5.28'de gösterildiği gibi olur.



Şekil 5.28. Bir SQL cümlesi

Veritabanı sunucusu bu SQL cümlesi doğrultusunda 10. basın duyurusunu web uygulaması aracılığıyla HTML formatında kullanıcıya gönderir. Bu web uygulamasında SQL enjeksiyonu açığının olup olmadığını anlamak için WHERE yan cümlesi içerisine yeni koşullar eklenir. SQL cümlesine yeni bir koşul eklendiğinde URL adresi Şekil 5.29'da gösterilen hali alır.



Şekil 5.29. SQL enjeksiyonun tespit edilmesi

URL adresinden yeni bir koşul eklendiğinde SQL cümlesinin son hali Şekil 5.30'da gösterildiği gibi olur.

Şekil 5.30. SQL cümlesinin son hali

Veritabanı sunucusu için bu cümlenin bir önceki cümleden farkı yoktur. Eğer yazılım geliştirici, veritabanı hatalarının kullanıcıya gösterilmesini engellemesine rağmen kullanıcı girdilerini kontrol etmiyorsa yeni SQL cümlesi yine 10. basın duyurusunu gönderecektir. Bu sonuç aslında web uygulamasında kör enjeksiyon yöntemiyle açığın tespit edilmesine dair bir kanıttır. Eğer web uygulamasında kullanıcı girdileri kontrol ediliyorsa kullanıcı tarafından girilen "10 AND 1=1" değeri için hata mesajı kullanıcıya iletilir ve ilgili basın duyurusu kullanıcıya gösterilmez.

5.4.6. SSI (Server Side Includes) enjeksiyonu

SSI genellikle SHTML uzantılı dosyalar içerisinde CGI programları çalıştırmak, dosya yerleştirmek, zaman ve tarih bilgisi eklemek vb. gibi işlerin sunucu tarafında yapılmasını sağlayan betik yazma dilidir [225]. Adından da anlaşılabileceği gibi web sunucular aracılığıyla bir dosyanın başka bir dosyanın içeriğine dâhil edilmesini sağlar. SSI Enjeksiyonu bir web uygulamasına, daha sonradan web sunucusu

tarafından yerel olarak çalıştırılması için, kod göndermesine izin veren sızma tekniğidir. SSI enjeksiyonu sızma yöntemi, web uygulamasının kullanıcı kaynaklı veriyi, sunucu tarafında hazırlanan HTML dosyasına denetim yapmadan koymasından meydana gelen zafiyetin kullanılmasını sağlar ve oluşan hatalar ve zafiyetlerden faydalanılmasına destek verir.

Bir web sunucusu HTML web sayfasını sunmadan önce, sunucu tarafında çalışan betikler bulup çalıştırabilir. Bazı durumlarda (mesaj tahtaları, misafir defterleri veya içerik yönetim sistemleri), web uygulaması kullanıcı kaynaklı verileri web sayfasının kaynak kodunun içine koymaktadır. SSI enjeksiyonu yöntemiyle yapılan sızma testleriyle, sunucu taraflı betikler yollanırsa, işletim sistemi komutları çalıştırabilme, kısıtlı bir dosyanın içeriğini sayfanın bir sonraki servisine dâhil ettirebilme gibi güvenlik ihlalleri ortaya çıkartılır [226].

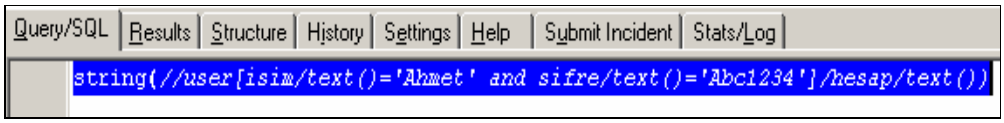
5.4.7. XPath (XML Path Language) enjeksiyonu

XPath, XML dokümanları içinde yer alan elemanlara erişmek için kullanılan sorgulama dilidir [227]. XPath ile doğrudan uygulama tarafından bir XML dokümanını sorgulamada kullanılabildiği gibi, XSTL dokümanının XML dokümanına dönüşümü veya XML dokümanına Xquery uygulanması gibi daha büyük bir işlemin parçası olarakta kullanılabilir. XPath enjeksiyonu yöntemiyle, kullanıcı kaynaklı girdilerden Xpath sorguları oluşturan ve kullanıcı girdilerini denetlemeyen web sitelerinin zafiyetlerinin sömürülmesi hedeflenmektedir.

Xpath'in sözdizimi SQL sorgusuna benzediğinden, XML dokümanında SQL benzeri sorgular oluşturmak mümkündür. XPath, SQL sorgulama diliyle benzerlikler göstermesine rağmen güvenlik açısından daha korunmasızdır. XPath sorgulamasıyla erişim kontrol kısıtlamaları olmaksızın XML dokümanlarına erişim sağlanabilmektedir [228].

XPath cümlesinin yapısının anlaşılabilmesi için örnek verilirse; kullanıcı isimli bir elemanı olan XML dokümanı olsun, kullanıcı elemanın "isim", "şifre" ve "hesap"

isimli 3 tane alt elemanı olsun. “Ahmet” isimli ve “Abc1234” şifreli kullanıcının hesap numarasını veren Xpath cümlesi Şekil 5.31’de gösterildiği gibi olur.

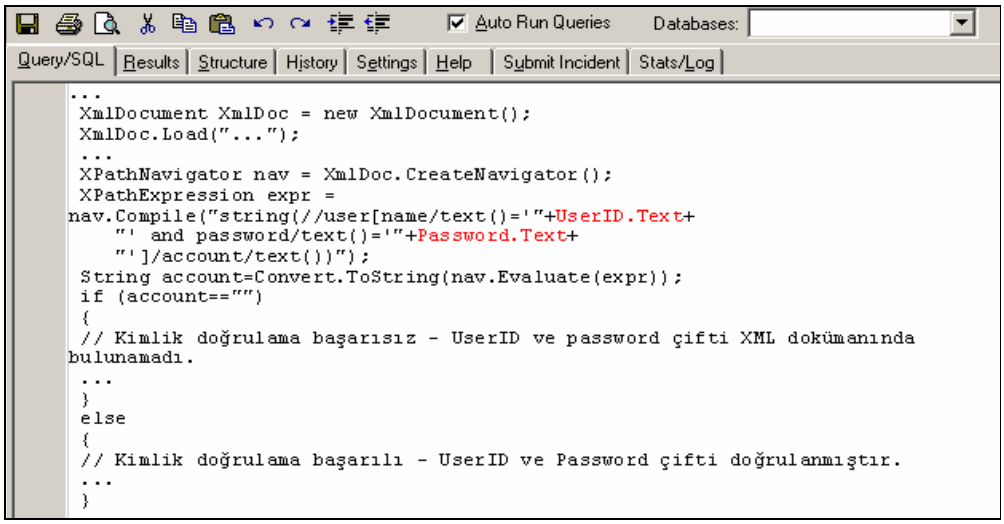


Şekil 5.31. Örnek Xpath cümlesi

Eğer böyle bir kullanıcı yoksa geriye sorgulama sonucunda geriye hiçbir değer dönmeyecektir.

Eğer bir web uygulamasında, Xpath sorgusu dinamik olarak kullanıcı girdilerine göre oluşturuluyor ve yeterli denetim yapılmıyorsa, XPath enjeksiyonu yöntemiyle XPath sorgu cümlesine güvenli olmayan kullanıcı girdileri enjekte edilebilir. Enjekte edilen girdilere bağlı olarak XML dokümanı üzerinde yer alan bilgilere yetkisiz erişim yapılabilir.

Şekil 5.32’de verilen örnek web uygulamasında, kimlik doğrulama işlemi için XML dokümanı içerisinde Xpath sorgusu kullanmaktadır. Kullanıcı girdileri hiç denetlenmeden Xpath sorgusuna dâhil edildiğinden, web uygulamasında güvenlik açığı meydana gelmektedir.



Şekil 5.32. Xpath zafiyet örneği

Şekil 5.32'de gösterilen kod içerisinde Xpath sorgusunda yer alan UserID alanına SQL enjeksiyonu yönteminde de kullanılan girdiler (' or 1=1 or =') enjekte edildiğinde doğru kullanıcı adı ve parolası girilmemesine rağmen XML dokümanındaki ilk kullanıcı olarak kimlik doğrulaması yapılır.

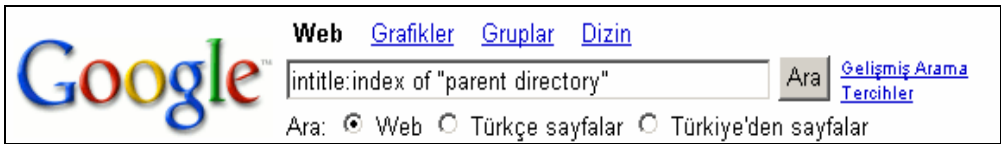
5.5. Bilgi Açığa Çıkarma

Bilgi açığa çıkarma yöntemiyle yapılan sızma testleri, web sitelerinin çalışmasıyla ilgili sisteme özel (versiyon, çalıştığı platform, yama seviyesi, yedek veya geçici dosyaların yeri, vb.) bilgilerin elde edilmesi için yapılacak işlemleri kapsamaktadır. Çoğu durumda, web siteleri kendileri hakkında bir kısım bilgiyi gösterecektir. Ancak burada önemli olan mümkün olduğunca, web siteleri hakkında gösterilen bilgilerin boyutu en aza indirgenmektedir. Web sitesi hakkında ne kadar çok bilgi toplanırsa, web sitesinin zafiyetlerinin belirlenmesi ve kullanılmasıda o kadar kolay olur. Bu bölümde web sitelerinde yer alan önemli bilgilerin nasıl açığa çıkarılacağıyla ilgili dizin listeleme, bilgi sızıntısı, yol takibi, tahmin edilebilir kaynak konumu ve mantıksal sızma testleri bu çerçevede takip eden alt başlıklarda açıklanmıştır.

5.5.1. Dizin listeleme

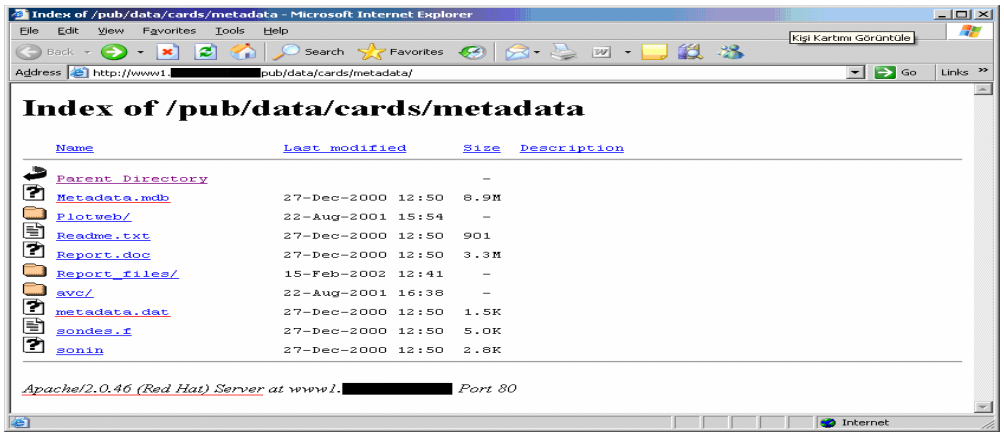
Dizin listeleme (directory indexing), başlangıç sayfası (homepage) olmayan bir web sitesinin, talep edilen dizin içerisinde yer alan dosyalarının tamamının listelenerek HTML formatında kullanıcıya aktarılmasıdır [228]. Kullanıcı ziyaret etmek istediği web sitesinin etki alanı ismini kullanarak, herhangi bir özel dosya ismi belirtmeyerek URL (http://www.şirket.com.tr) isteğinde bulunur. Web sunucusu; yapılandırma ayarlarına bağlı olarak ziyaretçiden gelen istek doğrultusunda dokümanın bulunduğu kök dizininde varsayılan dosyayı (default.asp, default.jsp, index.asp, index.html, vb.) arar ve bu dosyayı HTML formatında kullanıcıya gönderir. Eğer varsayılan başlangıç dosyası bulunamazsa, web sunucusu web kök dizini içerisinde yer alan dosya ve klasörlerin ("ls" veya "dir" komutunun web kök dizininde çalıştırılmasına eşdeğerdir) listelemesini içeren sonuçları kullanıcıya gönderir. Web sunucusundaki hatalı yapılandırmalar ve zafiyetler dizin listelenmesini sağlayan nedenlerin başında gelmektedir.

Dizin listelemeleri yöntemiyle yapılan sızma testlerinde Google Hacking tekniği oldukça sık olarak kullanılmaktadır. Bu teknik aracılığıyla web sunucusu, dizin içeriğinin gösterilmesini sağlayan arama cümlelerine örnek Şekil 5.33'de gösterilmiştir.



Şekil 5.33 Google Hacking tekniğiyle dizin listeleme

Genellikle web yöneticileri "gizlilik üzerinden güvenlik" ilkesini uygulayarak, dokümanlara ulaşan bağlar yoksa o dokümanların bulunamayacağını ve kimsenin bu dokümanları okuyamayacağı gibi yanlış varsayımlar üzerine kurulu web dizin yapısı oluşturmaktadır. Ancak günümüzde kullanılan zafiyet tarayıcıları, yaptıkları incelemelerinin sonuçlarına, deneme yanılma (kaba kuvvet, sözlük) yöntemiyle dizin veya dosya isimleri ekleyerek web sunucunun cevaplarına göre dizin yapısını oluşturmaktadır. Bunun yanında web sitelerinde listelenmesi istenmeyen içeriklerin yer aldığı "robots.txt" dosyası dikkatlice incelenerek açıklık tarayıcı web sunucusunu bu yeni verilerle tekrar sorgulayabilir. Dizin listeleme Şekil 5.34'de gösterilen veri kaçaklarına (gizli dizin veya dosyalar, web sunucu yazılımı sürüm bilgileri, yedekler, yapılandırma dosyaları, vb.) neden olarak web sızma testleri için gerekli olacak olan bilgilerin sağlanmasına sebep olabilir.



Şekil 5.34. Web dizin listelemeye örnek bir ekran çıktısı

5.5.2. Bilgi sızıntısı

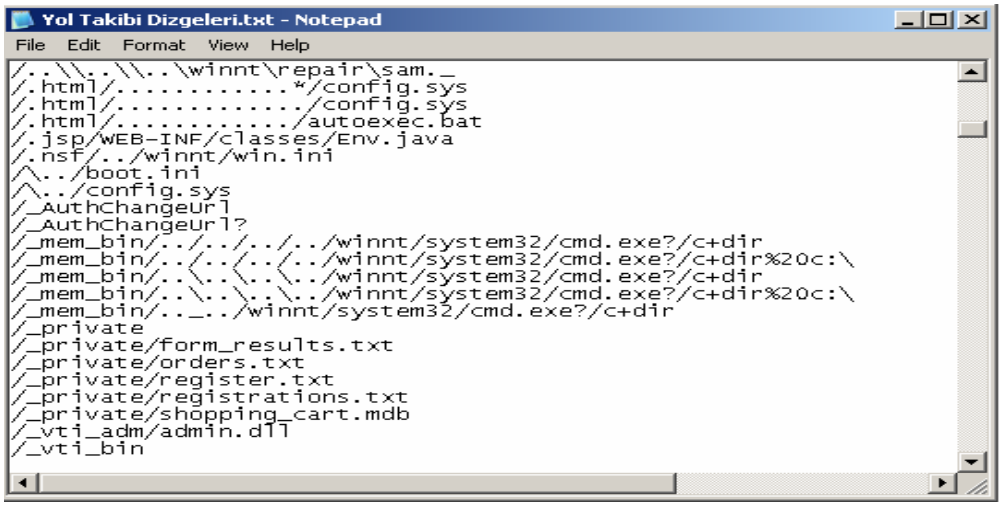
Bilgi sızıntısı (Information Leakage), web sitesi geliştirilirken yazılımcılar tarafından HTML kaynak kodları içerisinde unutulan geliştiriciye ait notlar, web sitesi hata mesajları veya site içerisinde açık bir düzyazı şeklinde unutulan hassas verilerden faydalanılarak sisteme sızma için gerekli olan bilgilerin toplanmasına yardımcı olan sızma test tekniğidir [230]. Bilgi sızıntısı sızma testleri yapılırken, hassas bilgilere ulaşabilmek için iki aşamalı bir yol izlenir. İlk aşamada web sitesi kodları satır satır incelenerek rehber bilgiler araştırılır. İkinci aşamada web sitesi üzerinde yer alan uygulamaların çalışma mantığının çözümlenmesi için çalışmalar yapılır. Web uygulaması çözümlendikten sonra, uygulama içerisinde geliştirici tarafından varsayılmayan durumların tespit edilmesiyle uygulama hakkında önemli bilgiler içeren hata mesajlarının oluşturulması sağlanır. Bu türlü sızıntılar, her zaman doğrudan sızma yapılmasını sağlayacak güvenlik açığı içermeyebilir ancak sızma testlerini yönlendirecek yararlı bilgiler elde edilmesini sağlayabilirler.

5.5.3. Yol takibi

Yol takibi (path traversal), sızma tekniğiyle, web sitesi kök dizininin dışında kalan dosyalara, dizinlere veya komutlara erişim sağlanması hedeflenir. Birçok web sitesi, dosya sisteminin sadece bir kısmına, genellikle "web dokümanı kök dizini" veya "CGI kök dizini" kısmını kullanıcı erişimine açar. Bu dizinler, kullanıcı erişimine açık dosyaları ve web uygulamasını çalıştırabilmek için gereken yürütülebilir dosyaları içerir. Dosya sistemindeki herhangi bir dosyaya ulaşabilmek veya komutu çalıştırabilmek için kullanılan yol takibi sızma testleri Şekil 5.35'de gösterilen özel karakter dizilerinden meydana gelen cümleleri kullanır.

En genel "Yol Takibi", URL'de istenen kaynağın yerini değiştirmek için "../" özel karakterlerini kullanır. Birçok popüler web sunucusu web dokümanı kök dizininden çıkışı engellese de, "../" karakterlerinin değişik kodlanması, güvenlik filtrelerini aşabilir. Bu karakterlere ek olarak, eğik çizgi karakterinin unicode olarak kodlanması ("..%u2216" veya "..%c0%af"), Windows tabanlı sistemlerdeki ters eğik çizgi karakterinin kullanılması ("..\"), URL kodlanmış karakterler ("%2e%2e%2f"), ve

ters eğik çizgi karakterinin iki kez URL kodlanması (“..%255c”) örnek olarak verilebilir.



Şekil 5.35. Yol takibi cümleleri

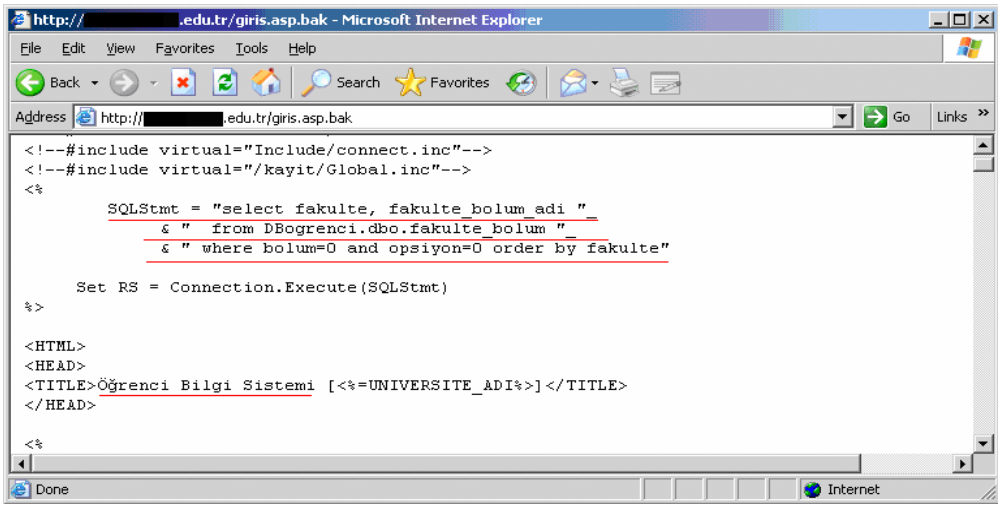
Günümüzde web sunucuları, URL üzerinden, “Yol Takibi”’ni genellikle engellediğinden yol takibi sızma testleri web uygulamasının kullanıcı girdileri üzerine odaklanmaktadır [231].

5.5.4. Tahmin edilebilir kaynak konumu

Tahmin edilebilir kaynak konumu (predictable resource location), web sitesinin gizli içeriğini veya fonksiyonunu açığa çıkarmak için kullanılan sızma tekniğidir. Sızma testiyle mantıklı tahminler yapılarak, web sitesi içerisinde izlenime kapalı olan içeriğin deneme yanılma yöntemiyle bulunmasına çalışılır. Geçici dosyalar (test.asp, test.jsp, vb.), yedek dosyalar (yedek.bak, yedek.zip, vb.) ve yapılandırma dosyaları potansiyel olarak hassas bilgiler içeren ve tahmin yoluyla bulunmaya çalışılan dosyalara örnek olarak verilebilir. Bu dosyalar web uygulamasının içeriği, veritabanı bilgisi, şifreler, bilgisayar isimleri, diğer hassas bölgelere olan dosya yolları hakkında güvenlik açığı oluşturabilecek gizli bilgiler içermektedir [232].

Tahmin edilebilir dosya isimleriyle ilgili örnek Şekil 5.36’da gösterilmektedir. Hâlihazırda çalışan bir üniversite öğrenci işleri sisteminin kimliklendirme ekranının

kodlarını içermesi açısından çarpıcı bir örnektir. Şekil 5.36'da gösterilen uygulama kodu incelendiğinde, SQL cümlesi görülmekte ve bu cümleden tablolar ve kolon isimleriyle ilgili veritabanı hakkında önemli bilgiler elde edilmektedir.



Şekil 5.36. Tahmin edilebilir kaynak konumu örneği ekranı

Tez çalışması sırasında bu tür örneklere oldukça fazla rastlanmış, tespit edilen bu açıklar ilgili birimlere bildirilmiş ve bu konuda gerekli uyarılar yapılmıştır. Bu tür açıkların ortadan kaldırılması için öncelikle web sitesi üzerinde bu tür bilgiler içeren dosyalara kesinlikle yer verilmemelidir. Eğer bu tür hassas dosyalara yer verilmek zorunda kalınıyorsa tahmin edilme olasılığı düşük konumlarda ve isimlerde yer verilmelidir.

5.6. Mantıksal Sızma Testleri

Mantıksal sızma testleri, web uygulama geliştiricileri tarafından ortaya konulan varsayımların aksi yönünde hareket ederek uygulama mantık akışının kötüye kullanımına veya uygulamaların sömürülmesine odaklanır. Uygulama yazılım mantığı, belli bir eylemi (kimlik denetleme, hesap açma, ürün satın alma, vb.) gerçekleştirmek için kullanılan ve yazılımcı tarafından öngörülen prosedürsel akıştır.

Web uygulamaları, belli bir eylemin tamamlanması için kullanıcının uyması gereken mantıksal adımları gerçekleştirmesini zorunlu kılarlar. Yanlış olmasına rağmen, web

uygulama geliştiricileri kullanıcı davranışının nasıl olacağı yönünde varsayımlarda bulunmaktadır. Mantıksal sızma testleriyle uygulama geliştiricisi tarafından öngörülen varsayımların dışındaki davranışların tespit edilmesi için gerekli olan çalışmalar yapılmaktadır.

5.6.1. Fonksiyonellik suistimalleri

Web uygulamaları fonksiyonelliğin kötüye kullanılmasıyla yapılan sızma testleri, web uygulamalarındaki mantık hatalarından faydalanılarak web uygulama fonksiyonlarının suistimal edilmesi üzerine odaklanır. Web uygulamalarının fonksiyonelliğin kötüye kullanılmasıyla ilgili örneklerden bazıları aşağıda bahsedilmiştir [233].

- Bir web sitesindeki arama fonksiyonunun web dizini dışındaki kısıtlanmış hassas dosyalara ulaşılmasında kullanılması.
- Dosya yükleme bileşenleriyle kritik yapılandırma dosyalarının değiştirilmesi.
- Web uygulamaları içerisinde yer alan kimliklendirme sayfasının tanımlı kullanıcı isimleri ve tanımsız parolalar ile bombardıman edilerek tanımlı kullanıcıların hesaplarının kilitlenmesinin sağlanması.

5.6.2. Hizmet aksattırma (DoS)

Hizmet aksattırma yöntemiyle yapılan sızma testlerinde, web uygulamalarının gereksiz yere meşgul edilerek normal işleyişinden alıkoyulması amaçlanmaktadır. Günümüzde web uygulamaları, web sunucusu, veritabanı sunucusu, kimliklendirme ve yetkilendirme sunucusu içerdiğinden, DoS sızma testleriyle bu bileşenlerden herhangi biri veya hepsi hedef alınabilir. DoS sızma testlerinin uygulanmasıyla ilgili örnekler aşağıda açıklanmıştır [234].

Kimliklendirme ve yetkilendirme sistemleri: Bilinen bir kullanıcı adı ve bilinçli olarak üretilmiş yanlış bir şifreyle kullanıcı hesabının kilitlenmesi sonucu kullanıcının hizmet alamaması sağlanabilir.

Veritabanını sistemleri: Enjeksiyon sızma teknikleriyle veritabanı üzerinde tahrifatlar (silme, değiştirme, ekleme, vb.) yapılarak veritabanı sistemlerini kullanılmaz hale getirilebilir.

Web sunucusu: Özel yazılmış programlarla web sunucusuna ait sistem kaynaklarının (CPU, hafıza, disk yeri, vb.) gereksiz yere meşgul edilerek, normal kullanıcılar tarafından erişilemez hale getirilebilir.

5.6.3. Otomasyon

Otomasyon yöntemiyle yapılan sızma testleriyle, web uygulamaları üzerinde elle (manüel olarak) yapılması gereken işlerin (kullanıcı hesabının açılması, ziyaretçi defterlerinin yazılması, vb.) otomatik olarak çok yüksek sayılarda yapılmasıyla web uygulamasının çalışamaz hale getirilmesi amaçlanmaktadır [235]. Otomatik bir robot (programlar), web uygulamaları üzerinde bir dakika içinde binlerce istek çalıştırıp potansiyel iş ve hizmet kaybına neden olmaktadır.

Örneğin, bir kaç dakika içinde otomatik bir robot aracılığıyla ücretsiz e-posta hizmeti veren web uygulaması üzerinde onbinlerce yeni hesap açılabilir, yine benzer bir yöntemle forum içerisinde yer alan mesaj alanlarına onbinlerce e-posta gönderilebilir.

5.6.4. Yetersiz denetim

Web uygulamalarında yetersiz denetim yapılması sonucunda uygulamanın akışı değişebilmektedir. Eğer kullanıcı durumu iş süresince denetlenmiyor ve uygulanmıyorsa, web uygulaması sömürülmeye veya dolandırıcılığa açık olabilir. Web uygulamaları kullanıcı durumlarını izlemek için çerezler veya gizli HTML alanlarını kullanırlar. Denetleme bilgisinin bütünlük içerisinde izlenebilmesi için sunucu tarafında tutulması gereklidir ancak izleme bilgileri istemci tarafın tarayıcıda tutulursa denetimin tam olarak yapılamamasından kaynaklanan güvenlik ihlalleri ortaya çıkabilecektir [236].

Yetersiz denetim yöntemiyle yapılan sızma testlerinde, kullanıcı tarafında tutulan bilgiler üzerinde yerel vekil (local proxy) programları aracılığıyla kullanıcı tarafında tutulan tüm bilgiler üzerinde değişiklik yapılarak programın akışı değiştirilebilmektedir.

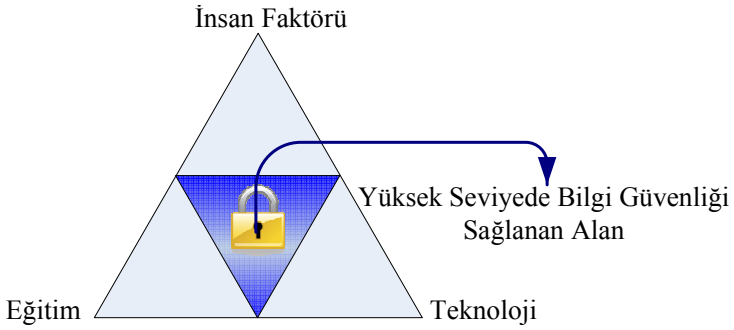
6. KURUMSAL BİLGİ GÜVENLİĞİNE GENEL BİR BAKIŞ

Bu bölümde, bilgi güvenliği konusunda daha önceden alınmış olunan dersler ve eğitimler, bilgi güvenliğiyle ilgili uluslararası alanda sahip olunan sertifikalar, bilgi güvenliği konusunda katılım sağlanan uluslararası seminerler, bilgisayar ağları konusunda üniversitelerde verilen dersler, 11 yıllık sektörel çalışmalardan elde edilen tecrübeler, tez çalışması esnasında incelenen çalışmalar ile elde edilen bilgi birikimi ve deneyimler ile yapılan pratik uygulamalara dayanılarak kurumsal bilgi güvenliğinin sağlanmasında yapılması gerekenler, alınması gereken önlemler, atılması gereken adımlar, elde edilen deneyim ve birikimler sonucu oluşan öneriler ile sızma testleri üzerinde durulacaktır.

Bölüm 2'de açıklandığı gibi bilgi güvenliği alanında yaşanan güvenlik ihlalleri, ağ ve sistemlerden web uygulamalarına doğru hızlı bir şekilde kaymaktadır. Tez çalışması kapsamında kamu ve özel sektörde hizmet veren kurumların (eğitim, sağlık, finans, gıda, basın, vb.) bilgi güvenliği seviyelerini test etmek için sızma testleri yapılmıştır. Dünyada olduğu ve literatürde de vurgulandığı gibi en fazla güvenlik açığına web uygulamalarında rastlanmıştır. Kurumların genelde sınır ağ güvenliğinin (Perimeter Network Security) sağlanmasıyla ilgili çözümleri (güvenlik duvarı, saldırı tespit sistemleri, antivirüs programları, vb.) ve farkındalıkları olduğu saptanmıştır. Ancak web uygulama güvenliği kavramının dünyada olduğu gibi ülkemizde de, uygulamayı geliştiren yazılımcılarında dâhil olduğu büyük bir çoğunluk tarafından anlaşılamadığı, bilinmediği veya bilinse dahi uygulanamadığı görülmektedir.

Kurumsal bilgi güvenliğinin sağlanmasında sızma testleri, bilgi güvenliği sürecini etkileyen temeldeki üç unsur olan insan faktörü, eğitimsizlik, teknolojik eksikliklerden kaynaklanan zafiyetlerin meydana çıkartılmasında önemli bir rol oynamaktadır. Kurumsal bilgi güvenliğinin sağlanmasıyla ilgili olarak bu tez çalışmasında güvenliğin bir ürün veya hizmet olmadığı, Şekil 6.1'de gösterilen insan faktörü, teknoloji ve eğitim üçgeninde yaşayan canlı bir süreç olduğu esas alınmış, bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı saptanmıştır. Yüksek seviyede

kurumsal bilgi güvenliğin sağlanması için yapılması gerekenler, alınması gerekli önlemler ve tedbirler bu çerçeve dâhilinde açıklanmıştır.



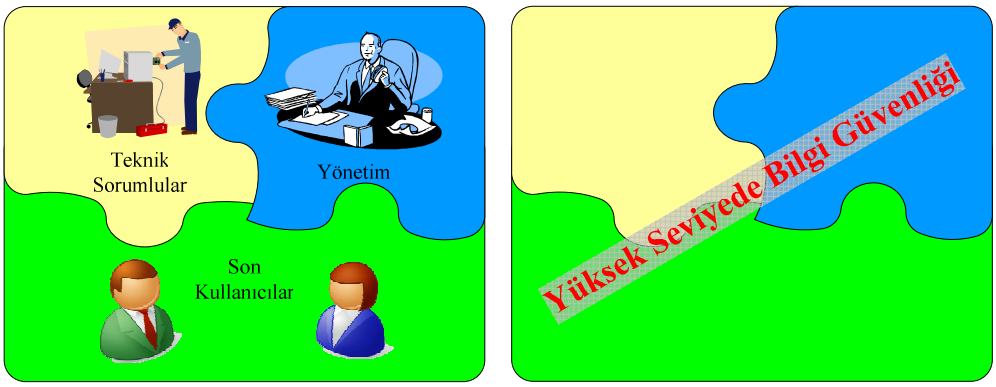
Şekil 6.1. Güvenlik sürecini etkileyen faktörler

Şekil 6.1'den görüleceği gibi bilgi güvenliği insan faktörü, eğitim ve teknoloji üçgeninde yer almaktadır. Şekildeki maviye boyanmış taralı alanın maksimum güvenliğin sağlanabileceği bir alan olduğu söylenebilir. Yüksek seviyede kurumsal bilgi güvenliğinin sağlanması için gerekli unsurları oluşturan faktörler takip eden alt başlıklarda ayrıntılı olarak açıklanmıştır.

6.1. İnsan Faktörü

Tez kapsamında yapılan sızma testleri, bilgi güvenliğiyle ilgili yapılan çalışmalarda (raporlar, anketler, kitaplar, makaleler, vb.) vurgulandığı gibi kurumsal bilgi güvenliğinin sağlanmasındaki en zayıf halkanın insan faktörü olduğunu göstermiştir. Örnek vermek gerekirse bilgi güvenliği için büyük tehdit oluşturan web uygulamalarındaki zafiyetler incelendiğinde kodlama hataları, sistem yapılandırma hataları, telefon görüşmeleriyle istenilen bilgiye ulaşılması, yüksek seviyede bilgi güvenliğinin sağlanması için gereken teknoloji ve eğitim yatırımlarının yapılmaması gibi insan faktöründen kaynaklanan zafiyetlere oldukça sık rastlanmıştır. Bu zafiyetlerin saldırganlar tarafından kullanılması durumunda bilgi güvenliği ihlalleri yaşanacak ve kurumlar zarar göreceklerdir. Kurumsal bilgi güvenliğinin sağlanmasından teknik sorumlular kadar yöneticiler ve son kullanıcılar olmak üzere tüm kurum çalışanları sorumludur. Yüksek seviyede bir bilgi güvenliğinin sağlanması tüm tarafların sorumluluklarını yerine getirmesiyle sağlanabilecektir.

Bilgi güvenliği konsepti bir yap-boz'a benzetilecek olursa, yüksek seviyede bir güvenlik sağlanabilmesi için (resmi tam olarak görebilmek), Şekil 6.2(a)'de gösterildiği gibi bu unsurların bulunması ve birbirlerini destekleyerek tamamlamaları gerekir.



(a) (b)

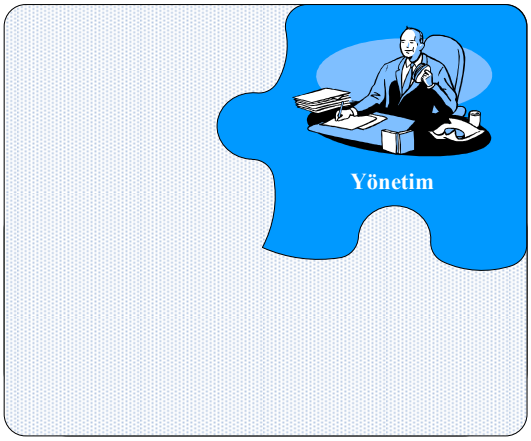
Şekil 6.2. Kurumlarda insan faktörü a) Unsurlar b) Bilgi güvenliği resmi

Yüksek seviyede bir kurumsal bilgi güvenliğinin sağlanması için teknik sorumlular, yönetim ve son kullanıcı sorumluluklarının yerine getirilmesi gereklidir. Yönetim güvenlik sürecini etkileyen idari ve mali kararların alınmasından, teknik sorumlular güvenlik çözümlerinin uygulanmasından, son kullanıcılar ise idari ve teknik kararlara uyulmasından sorumludur. Şekil 6.2(b)'de gösterildiği gibi bu üç grubun herhangi birisi görevini aksattığında resmin bütünlüğü bozularak insan faktörü bilgi güvenliğini olumsuz olarak etkilemeye başlayacak ve bilgi güvenliği ihlalleri meydana gelerek yüksek seviyeli bir koruma sağlanamayacaktır. Bu unsurların kurumsal bilgi güvenliği sağlanmasında yerine getirmesi gereken sorumlulukları ve yapması gerekenler takip eden alt başlıklarda ayrıntılı olarak açıklanmıştır.

6.1.1. Yönetim

Kurumun stratejik hedeflerini belirleyen üst yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek yüksek seviyede bilgi güvenliğinin sağlanabilmesi açısından çok önemlidir. Bilgi güvenliğinin sağlanmasıyla ilgili

olarak insan faktörleri içerisinde yer alan yönetim birimi Şekil 6.3'de temsili olarak gösterilmektedir.



Şekil 6.3 Yönetimin insan faktörü içerisindeki yeri

Bilgi güvenliğinin sağlanması için gerekli olan idari ve mali kararlar, yönetim tarafından zamanında ve doğru bir şekilde alınmalıdır. Kurumsal bilgi güvenliğinin etkin bir şekilde yönetilmesi amacıyla, içerisinde yöneticilerinde bulunduğu Bilgi Güvenlik Biriminin kurulması gereklidir. Bilgi güvenlik biriminin kurulması ve etkin bir yapıda çalışması, yönetimin kurumsal bilgi güvenliğini sahiplendiğinin ve desteklediğinin önemli bir göstergesidir. Bilgi Güvenlik Biriminin başlıca görevleri aşağıda maddeler halinde belirtilmiştir. Bunlar;

- Kurumsal bilgi güvenliğinin (KBG) sağlanması için kurum içi ve kurum dışı tehdidin tespit edilmesini sağlamak, gerekli tedbirleri almak ve alınmasını sağlamak,
- KBG yönetim sistemini oluşturmak için kapsam, politika, ilke, standart ve usulleri tespit etmek, geliştirmek, değiştirmek ve sonrasında onaylamak,
- KBG'nin sağlanmasına esas olan kurumsal bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerine uygun olmasını sağlayacak tedbirleri belirlemek, uygulamak, uygulanmasını sağlamak ve kontrol etmek,
- KBG risk yönetimi ve değerlendirmesini yapmak ve yapılmasını sağlamak,
- Kurumsal bilgi güvenliğin sağlanması amacıyla gerekli görülecek kurumsal bilgi güvenliği sistemi esaslarını tespit ederek kurmak ve geliştirmek,

- KBG sisteminin mimarisinin oluşturulmasında caydırma, koruma, ikaz, tespit, onarım ve tedbir unsurlarını belirlemek,
- KBG ile ilgili mevzuat ve teknolojideki gelişmeleri takip etmek,
- Güvenlik hassasiyeti gösteren personel, yazılım, donanım, şifreleme, iletişim ortamları ve iletişim ağlarını her türlü tehdit kaynağına karşı maliyet-etkin tedbirlerle koruma altına alınmasını sağlamak, bu tedbirleri uygulamaya sokmak ve kontrol etmek,
- KBG'ye ilişkin güvenlik kategorilerini ve sistemin minimum güvenlik ihtiyaçlarını belirlemek ve uygulanmasını sağlamak,
- KBG'yi ilgilendiren kurumsal bilgiyle işlem yapacak donanım ve yazılım ihtiyaçlarına ait güvenlik değerlendirmesini yapmak ve değerlendirilmiş ürün listelerini hazırlamak ve yayımlamak,
- Bilişim güvenliği sistemlerinin zafiyet analizi ve hassasiyet değerlendirmelerini ve sızma testlerini periyodik olarak yaptırmak,
- Gizlilik dereceli bilgiyi korumak üzere şifreleme esaslarını belirlemek,
- Şifreleme sistemlerinde kullanılacak materyal ve anahtarları üretecek teçhizatı onaylamak, özel anahtarların dağıtılmasına ilişkin usul ve esaslarını belirlemek ve denetlemek,
- KBG için, ihtiyaçlar, gizlilik ve kullanım arasında uygun bir denge kurmak
- KBG ile ilgili değişikliklere ilişkin teklifleri üst yönetime sunmak,
- Bilgi çağının gerektirdiği güncel güvenlik çözümlerini belirlemek,
- KBG konusunda kurum içerisinde verilecek eğitim standartlarını belirlemek, planlamak ve eğitimin verilmesini ve alınmasını sağlamak,
- KBG konusunda oluşan ihlallere ait gerekli yaptırımları belirlemek ve yapılacak yatırımları onaylamak,
- KBG yönetim sistemlerine ait sertifikasyon çalışmalarının yapılması ve idame ettirilmesini sağlamak,
- Güvenli bilgi sistemlerinin kullanıcı tarafında yaygın bir şekilde kullanımını özendirmek ve teşvik etmek,

- KBG ihlallerine karşı alınacak tedbirleri belirlemek, ihlallere karşı gerekli tedbirleri almak ve ilgili birimlerle koordineli olarak çalışılmasını sağlayarak ihtiyaç duyulan durumlarda bilgi güvenlik kriz masası kurularak yönetimini sağlamak,

olarak sıralanabilir.

Bilgi güvenliği birimine yönetim kademesinde çalışan bir kişinin başkanlık etmesi birimin almış olduğu kararların uygulanması ve yaptırımı açısından önem taşımaktadır. Ayrıca birim üyelerinin kurum içerisindeki diğer tüm birimlerden birer temsilci içerecek şekilde kurulması ve düzenli aralıklarla toplanarak bilgi güvenliğinin sağlanması için gerekli olan kararları alması gerekmektedir.

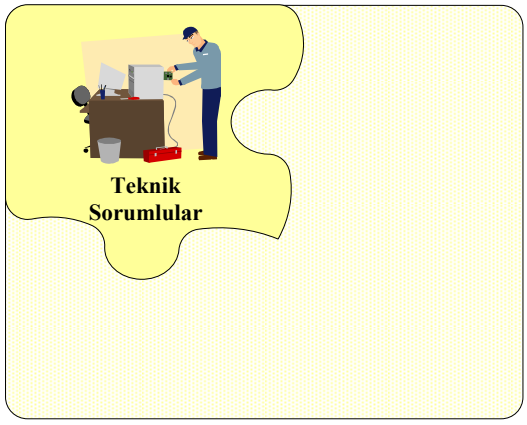
KBG'nin sağlanması konusunda yönetim tarafından dikkat edilmesi gereken istihdam ve yatırım hususları ile ilgili tavsiyeler aşağıda özetlenmiştir.

İstihdam: Bilgi güvenliği bölümlerine yeterli derecede eğitim ve deneyime sahip olmayan insanların işe alınması sonucunda, deneyimsizlikten kaynaklanan bilgi güvenliği ihlalleri meydana gelebilir. Özellikle bilgi güvenliği açısından kritik olan konumlardaki işe alımlarda, adaylardan bilgi ve tecrübelerini kanıtlayacak sertifikasyonlar istenmesi, bilgi güvenliği konusunda uzman kişilerden yardım alınması istihdam konusundaki sıkıntıları en aza indirgeyecektir.

Yatırım: Bilgi güvenliğinin sağlanmasına yönelik, yeterli veya doğru yatırımların yapılmaması, bilgi güvenliği konusunun yönetim tarafından anlaşılamadığının veya önemsenmediğinin bir göstergesidir. Bilgi varlıklarının yüksek seviyede güvenliğinin sağlanması gerekmektedir aksi takdirde bilgi güvenliği ihlalleri meydana gelecektir. Kurumsal bilgi güvenliğinin yüksek seviyede sağlanabilmesi için doğru ve yeterli yatırımların zamanında yönetim tarafından yapılabilmesi için konunun önemi uzman ve tarafsız kişilerce eğitim ve bilinçlendirme toplantıları aracılığıyla yöneticilere aktarılmalıdır.

6.1.2. Teknik sorumlular

Teknik sorumlular bilişim sistemleri üzerinde yüksek seviyeli erişim haklarına ve bilgiye sahip olan kişilerdir. Teknik sorumlular genellikle sistem ve kullanıcı yönetimi, donanım bakımı, uygulama geliştirme, programların uyarlanması ve teknik destek hizmetlerini yerine getirmektedir. Bilgi güvenliğinin teknolojik boyutundan sorumlu olan teknik sorumlu; oluşabilecek saldırılara karşı bilgi sistemlerini koruyacak önlemleri almalı; bilgi sistemlerine karşı yapılan saldırıları zamanında tespit ederek önleyebilmeli, meydana gelen güvenlik ihlallerinin verdiği zararları en kısa zamanda giderebilmeli, geliştirmiş olduğu yazılımlarda güvenlik esaslarına uymalıdır. Bilgi güvenliğinin sağlanmasında lokomotif görevi üstlenen teknik personelin bilgi güvenliği konusunda eğitimli ve uzman kişiler olması gerekmektedir. Kurumsal bilgi güvenliğinin sağlanmasında insan faktörü unsurları içerisinde yer alan teknik sorumlular Şekil 6.4'de temsili olarak gösterilmektedir.



Şekil 6.4. Teknik sorumluların insan faktörü içerisindeki yeri

KBG'nin sağlanmasında teknik sorumlular tarafından yapılması gereken hususlar ve tavsiyeler aşağıda başlıklar halinde sunulmuştur.

Güvenli kodlama: Günümüzde kurumsal bilgi güvenliğinin sağlanmasında teknik kullanıcılar içerisinde en önemli görevlerden bir tanesi yazılımcılara düşmektedir. Yazılımlardan kaynaklanan güvenlik açıklarının en aza indirgenebilmesi için yazılımcıların güvenli kodlama esaslarına uyması gerekmektedir. Güvenli kodlamada

dikkat edilmesi gereken dört önemli husus vardır. Dikkat edilmesi gerekli birinci husus, veri girişlerinin doğruluğunun kontrol edilmesidir. Veri girişlerinin kontrol edilmesi için girdi veya çıktı alanlarına özgü kabul edilebilecek karakterlerin bir listesi oluşturulmalı ve bu karakterler dışında kalanlar engellenmelidir. Daha önce vurgulandığı gibi sızma testleri sonuçlarına göre, kurumsal bilgi güvenliğini en fazla tehdit eden uygulamalar web uygulamaları olarak belirlenmiştir. Web uygulamalarında görülen en yaygın güvenlik açığı ise veri girişlerinin tam olarak doğrulanmaması olarak tespit edilmiştir. Güvenli kodlamada uygulanması gereken ikinci önemli husus kod testlerinin iyi yapılmasıdır. Kodlar test aşamasında yeniden gözden geçirilmeli ve güvenliği sınanmalıdır. Güvenli kodlamada uygulanması gereken üçüncü önemli husus yetki mekanizmalarının tasarımında yetkilerin ayrıştırılarak güvenliğin sağlanmasındaki önemli ilkelerden biri olan "en az yetki" ilkesine uyulmasıdır. Güvenli kodlamada uygulanması gereken dördüncü önemli husus uygulamalar hakkında önemli bilgiler içeren hataların kontrol edilmesidir. Hata kontrol yönetimi yapılarak oluşan hatalar, uygulamalar tarafından güvenli formatta dış dünyaya iletilmelidir.

Yama yönetimi: Güvenlik sürecinin sürekliliğini sağlayabilmek için, yeni çıkan güvenlik açıklarından haberdar olmak, saldırılara karşı bilgi sistemlerini koruyacak önlemlerin alınmasını sağlayacaktır. Riskleri önceden kestirmek ve gerekli önlemi felaket gerçekleşmeden alabilmek amacıyla yayınlanan güvenlik bültenleri ve güncel yamaların teknik personel tarafından takip edilmesi gereklidir. Güvenlik açıklarının giderilmesi amacıyla yüklenmesi gereken yamalar öncelikle test ortamlarında yüklenip denenmelidir. Test edilen yamalar daha sonra gerçek sistemler üzerine yüklenmelidir. Yama yönetiminin bilgi güvenliği açısından öneminin açıklanması amacıyla web sunucuları örnek olarak verilecektir. Tez kapsamında yapılan sızma testlerinde çoğu kurumun ağlarında bulunan web sunucu yazılımlarını düzenli olarak güncellemedikleri tespit edilmiştir. Web sunucu yazılımların eski sürümlerinin birçok güvenlik açığı barındırdığı güvenlik açıklarının, web sunucularının servis dışı kalmasına veya tüm sunucunun ele geçirilmesine neden olacağı düşünülürse yama yönetiminin önemi daha iyi anlaşılacaktır. Web sunucularının düzenli güncellenememesinin sebeplerinden en önemlisi, bu yazılımların parçası olduğu

ticari ürünlerin kullanılıyor olmasıdır. Önceden belirlenmiş yapılandırma ile kurulan web sunucuları, gerekli olmayan birçok bileşeni bünyelerinde barındırmakta ve gelecekte bu bileşenlere ait ortaya çıkabilecek güvenlik açıklarından etkilenebilmektedir. Web sunucu yazılımların düzenli olarak güncellenmeleri, ayrıca gerekli olmayan tüm bileşenlerin kapatılarak devre dışı bırakılması gereklidir.

Kayıt yönetimi: Bilgi sistemlerine karşı yapılacak saldırıların tespit edilmesinde iç ve dış güvenlik tehditlerine karşı güvenlik kayıtlarının tutulması önemlidir. Güvenlik kayıtlarının günlük olarak tutulup düzenli olarak izlenmesi ve teknik personel tarafından değerlendirilmesi gerekmektedir. Güvenlik ihlalleri meydana geldiğinde sistemin kontrolünü ele geçiren saldırganlar izlerini kaybettirmek amacıyla kayıtları yok etmek isteyeceklerdir. Bu durumda kayıtların güvenliğinin sağlanması için sistemle ilgili tüm kayıtların merkezi olarak güvenilir bir ortamda depolanması ve güvenliğinin yüksek seviyede sağlanması gerekmektedir.

Yedekleme ve geri yükleme: Bilgi güvenliği ihlali sonrasında kaybolan veya bozulan bilgilerin geri döndürülmesi amacıyla kurumlar açısından teknik (sistemler) ve stratejik (kurumsal bilgiler) açıdan önem arz eden bilgilerin düzenli olarak yedeklenmesi, bilgi güvenliği açısından önemlidir. Bilgiler yedeklendikten sonra test ortamlarında geri yüklemeleri yapılarak yedeklemenin düzgün bir şekilde yapıldığından emin olunması gereklidir.

Hatasız yapılandırma: Bilgi sistemlerinin doğru yapılandırılmaması veya varsayılan ayarlarla bırakılması sonucunda ciddi güvenlik açıkları meydana gelmektedir. Yapılandırma hatalarına bağlı olarak bilgi güvenliği ihlallerinin meydana gelmemesi için teknik personelin eğitimli ve konularında uzman kişiler olması gerekmektedir. Günümüzde en fazla yapılandırma hatalarının rastlandığı kablosuz ağlar bu konuda örnek olarak gösterilebilir. Kablosuz ağ cihazları üzerinde görünen yapılandırma hatalarına, kimlik doğrulamasının yapılmaması, kriptolu erişim kullanılmaması, kablosuz ağların güvenlik duvarı aracılığıyla erişim denetimine tabi tutulmaması ve sinyal kalitesinde kısıtlama olmaması örnek olarak gösterilebilir. Kurum yerel alan ağındaki kablosuz ağlarda meydana gelebilecek güvenlik ihlallerinin kablolu ağları etkilememesi için kablosuz ağ tasarımı yapılırken, kablosuz ağın güvensiz bir ağ

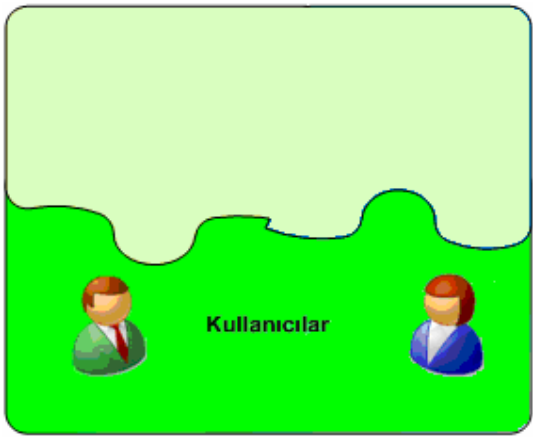
olduğu varsayılmalı ve güvenlik duvarı yapılandırmasında yarı güvenilir bölge içerisine dâhil edilmelidir. Kablosuz ağlarda güvenliğinin sağlanması amacıyla, kablosuz ağ iletişiminin kriptolu yapılması, kablosuz ağa dâhil edilecek kullanıcıların kimliklendirme mekanizmalarına tabii tutulması, kablosuz yayın yapılacak alanların belirlenerek sinyal mesafesinin (menzil) ayarlanması gerekmektedir.

Kullanılmayan hizmetlerin kapatılması: İşletim sistemleri ve uygulamalar ilk defa kurulduğunda, üretici firma tarafından belirlenen varsayılan (default) ayarları temel alınmaktadır. Varsayılan ayarlar incelendiğinde, çoğu kurum tarafından kullanılmayacak birçok destek ve hizmeti içermekte olduğu tespit edilmiştir. Bu destek ve hizmetlerin çoğunlukla üreticinin ürün kullanımının kolaylaştırılması amacıyla açıldığı bilinmektedir. İşletim sistemi ve uygulamaların ön tanımlı kurulumlarında kolay tahmin edilebilir şifreler, güvenlik açığı içermekte olan bileşenler ve örnek uygulamalar, kolay kurulum sebebiyle tercih edilmektedir. Bu şekilde kurulan işletim sistemi ve uygulamalar genel özelliklere sahip olmakta, yayınlanmış ve kullanılmayan bileşenleride içermekte olduğu güvenlik açıklarından etkilenmektedir. Yazılımlarda bulunan yayınlanmış güvenlik açıkları, kullanımlarının güvenlik tehdidi içerebileceği öngörülmemiş uygulamalar ve gerekli olmayan servisler sonucu, sistemin tamamen ele geçirilmesi veya servis dışı bırakılması mümkün olmaktadır. İşletim sistemi ve uygulama kurulumlarında, kurulum seçenekleri özelleştirilmeli, yönetim şifreleri zor tahmin edilebilir olmalı, gerekli olmayan servisler durdurulmalı ve örnek uygulamalar sistemden çıkarılmalıdır. Kurulumlarda, bilgi güvenliğinde temel prensiplerden biri olan “en az yetki” yaklaşımı benimsenmeli ve gerekli olmayan tüm erişim yetkileri kısıtlanmalıdır.

6.1.3. Son kullanıcılar

Son kullanıcılar kurumun bilgi kaynaklarını kullanmaya yetkili olan tüm kullanıcılardır. İnsan faktörü unsurları içerisinde bilgi güvenliğini en fazla tehdit eden unsur, kurumsal bilgileri oluşturan, değiştiren ve üzerinde işlem yapan son kullanıcılardır. Son kullanıcıların bilgi güvenliği konusundaki bilinçsizliği, eğitim eksiklikleri, dikkatsizlikleri ve sahip olduğu bilginin kıymetini bilmemeleri,

sistemlerde veya bilgisayarlarda bilgi güvenliği ihlalleri yaşanmasını kolaylaştıracaktır. Son kullanıcılardan kaynaklanan güvenlik ihlallerinin en aza indirgenmesi, farkındalık ve güvenlik eğitimleri ile kurumsal bilgi güvenliği politikalarının uygulanmasıyla sağlanır. Özellikle Bölüm 4'de açıkladığımız sosyal mühendislik yöntemlerine karşı, son kullanıcıların bilinçli olması azami ölçüde bilgi güvenliği politikalarına uyması kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Kurumsal bilgi güvenliğinin sağlanmasında insan faktörü unsurları içerisinde son kullanıcılar Şekil 6.5'de temsili olarak gösterilmektedir.



Şekil 6.5. Son kullanıcıların insan faktörü unsurları içerisindeki yeri

Kurumsal bilgi güvenliğini tehdit eden, son kullanıcıların sıkça yaptığı hatalar ve alınması gereken önlemler aşağıda başlıklar halinde özetlenmiştir.

Güvenlik politikaları ihlali: Kurumsal bilgilere erişim hakkı olan her çalışanın üst yönetim tarafından onaylanan KBG politikalarına uyması gerekmektedir. Güvenlik politikaları son kullanıcılar tarafından çoğu zaman bilerek veya bilmeyerek ihlal edilmektedir. Tez çalışması kapsamında yapılan araştırmalarda güvenlik politikalarının ihlal edilme sebeplerinin başlıcaları, kullanıcı alışkanlıkları, uygulanamayacak yaptırımlar, bilinçsizlik olarak tespit edilmiştir. Politika ihlallerinin önüne geçebilmek için kullanıcıların genel bilgi güvenliği konusunda eğitilmesi ve güvenlik politikalarının kurum kültürüyle ters düşmeyecek uygulanabilir ifadeler içermesi gerekmektedir.

Bilgi aktarımı: Genellikle kurum çalışanları tanımadıkları insanlarla sohbet esnasında birçok önemli bilgiyi farkında olmaksızın karşı tarafa iletmektedir. Hiçbir kurum çalışanı ortam farketmeksizin (e-posta, telefon, faks, yüzyüze, vb.) kimliğinden emin olmadığı kimselere hiçbir konuda bilgi vermemelidir. Bölüm 4'te ayrıntılı bir şekilde anlatılan ve 162 nolu kaynak içerisinde birçok örneği verilen sosyal mühendislik teknikleri, insanların tanımadığı kişilere vereceği, kendince önemsiz bilgiler sayesinde nelerin yapılabileceğine dair birçok örnekler içermektedir. Hiçbir teknoloji kullanılmadan kurum çalışanlarından alınacak bilgilerle tüm güvenlik kontrollerinin aşılabileceği hiçbir zaman unutulmamalıdır. Başlangıçta önemsiz gibi görünen küçük bilgiler bir araya geldiğinde, içinde gizli bir bilgiyi barındıran ciddi bir güvenlik açığına dönüşebileceğine dair örnekler her geçen gün artmaktadır. Bilinmeyen kişilere bilgi aktarılmaması için kullanıcıların özellikle sosyal mühendislik konusunda eğitilmesi gerekmektedir.

Şifrelerin kâğıtlara yazılması: Şifreleme politikaları, kırılması güç olan şifrelerin kullanıcılar tarafından kullanılmasını ve düzenli aralıklarla bu şifreleri değiştirilmesini zorunlu kılmaktadır. Şifrelerin güçlü olması, içerdiği karakterlerin karmaşıklığıyla doğru orantılıdır. Güçlü şifrelerin kullanılmasıyla birlikte kullanıcıların bu şifreleri hatırlama problemleri ortaya çıkmaktadır. Kullanıcılar, bu durumda şifrelerini hatırlayabilmek amacıyla görebilecekleri bir yere şifrelerinin yazılı olduğu kâğıdı asmaktadır. Bu durum ilgili kullanıcı şifresinin kötü niyetli başka bir kişi tarafından okunarak kullanılmasıyla güvenlik ihlalinin oluşmasına sebep olacaktır. Bu durumların meydana gelmemesi için kullanıcılara şifre seçimi ve hatırlanmasıyla ilgili eğitimler verilmelidir.

Güvenilir olmayan yazılımların kullanımı: Güvensiz yazılımlar illegal olarak kopyalanmış veya internetteki güvenilir olmayan sitelerden indirilmiş, lisanssız yazılımlar olup içlerinde bilgisayara zarar verebilecek virüs, truva atı, tuş kaydedici ve her türlü kötü amaçlı yazılımları barındırabilen programlardır. Güvenilir olmayan yazılımlar, ziyaret edilen web sitelerinin kayıtlarını tutarak başkalarına gönderen, istenmeyen reklâm pencerelerinin gelmesini sağlayan, bilgisayar içerisinde yer alan kişisel dosyaları başkalarına gönderebilen, bilgisayarın performansını düşüren ve

internet erişimini gereksiz yere meşgul eden istenmeyen yazılımlardır. Güvenilir olmayan yazılımların kullanımı sonucunda, birçok güvenlik ihlali meydana gelmektedir. Bu tür ihlallerin önüne geçebilmek için kullanıcılara güvenilir olmayan yazılımların ne olduğu ve bu yazılımlardan nasıl korutulacağı konusunda eğitimler verilmelidir. Güvenilir olmayan yazılımların kötücül etkilerinden korunmak için korsan yazılım kullanmaktan kaçınarak lisanslı yazılım kullanılması gerekmektedir. Lisanslı yazılımların kullanılmasıyla birlikte, birçok güvenlik zafiyeti ortadan kalkacaktır. Lisanslı yazılım kullanmaya ek olarak güvenilir olmayan web sitelerinden yazılım indirmeme, bedava olduğu için ne olduğu bilinmeyen yazılımların bilgisayarlara yüklenmemesi alınabilecek diğer önlemlerdir.

Bilgisayarların fiziksel güvenliğinin sağlanmaması: Genellikle kullanıcılar koruma önlemi almaksızın bilgisayarlarının başından ayrıldığında kötü niyetli insanlar bu durumu değerlendirerek bilgisayarı kötücül amaçlar için kullanmakta ve güvenlik ihlalleri meydana gelmektedir. Fiziksel güvenlik zafiyetinden faydalanarak bilgisayarı kullanan kötü niyetli kişi gizli bilgiler içeren dosyaları dışarıya e-posta aracılığıyla gönderebilir, bilgisayar üzerindeki bilgileri silebilir, değiştirebilir ve o anki kullanıcının yetkisi ölçüsünde birçok işlemi kötücül amaçlar için yapabilir. Bilgisayarların fiziksel güvenliğinin sağlanmasıyla ilgili olarak; kullanıcılar bu konuda bilinçlendirilmeli bilgisayarların başından ayrılan kullanıcıların en azından parola korumalı ekran koruyucusu kullanmaları bilgisayarlara fiziksel olarak yapılabilecek saldırıların en aza indirgenebilmesi açısından önem arz etmektedir.

Bilgisayarların yönetici hakkıyla açılması: Kullanıcılar kurum içerisinde kendilerine tahsis edilmiş olan kişisel bilgisayarlarını, herhangi bir kısıtlama olmaksızın kullanmak amacıyla genellikle yönetici haklarına sahip olan hesaplarla kullanmaktadırlar. Bu durum, bilgi güvenliğinin sağlanmasında önemli ilkelerden biri olan “en az yetki” prensibinin (principle of least privilege) ihlali anlamına gelmektedir. Yönetici haklarına sahip bir hesapla bir kullanıcının bilgisayarında oturum açılması, güvenlik ihlali meydana geldiğinde bilgisayar üzerinde yönetici işlemlerini (bilgisayar üzerinde kullanıcı hesabı grubu açma, değiştirme ve silme, gruplara yeni kullanıcı ekleme ve gruplardan kullanıcı silme, gruplara özel hak ve

yetkiler tanıyabilme, işletim sistemi üzerinde değişiklikler yapabilme, yeni uygulama yazılımları ve donanımlar kurup, eskilerini güncelleyebilme, sistem dâhilindeki herhangi bir diski biçimleyebilme, vb.) yapma yetkisine sahip olacağından güvenlik ihlalinin etkisi çok daha büyük olacaktır. Bu tür ihlallerin etkisini azaltmak için kullanıcıların ihtiyaçlarını karşılayacak kısıtlı haklara sahip olan hesaplar tanımlanmalı ve bu hesaplarla kullanıcıların oturum açmaları zorunlu hale getirilmelidir. Bu önleme ek olarak kullanıcılara yönetici haklarına sahip hesaplarla oturum açmalarının gereksizliği ve zararları anlatılarak, kısıtlı haklara sahip olan hesapları kullanmaları yönünde özendirici ve bilgilendirici eğitimler verilmelidir.

Bilinçsiz e-posta kullanımı: Kurum çalışanları tarafından kullanılan iletişim araçlarının başında e-posta gelmektedir. Günümüzde kötücül yazılımlar çoğunlukla e-postalar aracılığıyla yayıldığından, e-posta kullanımının önemi artmıştır. Bilinçsiz e-posta kullanımı sonucunda bilgi güvenliği ihlalleri meydana gelmektedir. Kullanıcıların tanımadığı kişilerden gelen şüpheli e-postaları açmaması, e-posta eklerini virüs taramasından mutlaka geçirmesi, e-posta aracılığıyla kişisel gizli bilgilerini (internet bankacılığı hesap bilgilerini, kimlik bilgileri, kullanıcı hesap bilgileri) kimseye vermemesi gibi e-posta kullanımında dikkat edilmesi gereken hususlar konusunda kullanıcılar bilinçlendirilmeli ve eğitilmelidir. Bu eğitimler sonucunda e-posta kullanımından kaynaklanacak zafiyetler en aza indirgenecektir.

Kurumsal bilgi güvenliğinin sağlanmasında en zayıf halka olan insan faktöründen meydana gelen zafiyetlerin giderilmesinde eğitim önemli bir rol oynamaktadır. İnsan faktörü unsurlarının KBG'nin sağlanması açısından ortak ihtiyaçları olan eğitim faktörü ayrıntılı olarak bir sonraki bölümde incelenmiştir.

6.2. Eğitim

KBG'nin sağlanması açısından önemli olan bilgi güvenliği eğitimleri ve bilinçlendirme farklı yöntemlerle çalışanlara periyodik olarak verilmelidir. Bu yöntemler bilinçlendirme toplantıları, kurum içi web üzerinden eğitimler, e-posta yoluyla kullanıcılara bildirimler, yazılar ve duyurular, seminerler, kurum içi bültenler

ve güvenlik posterleri şeklinde olabilir. Bilgi güvenliğinin insan faktörü unsurlarının ortak ihtiyacı olan eğitim unsuru Şekil 6.6'da görsel olarak verilmiştir.

İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bilgi güvenliği eğitimleri riskin kabul edilebilir bir seviyeye indirilmesine yardımcı olacaktır. Çalışma gruplarının bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması bilgi güvenliğinin sağlanması açısından kritik bir öneme sahiptir.

Şekil 6.6. Eğitim unsuru

Bilgi güvenliği eğitimlerinin temel hedefi çalışanları kurumsal bilgilerin ve bilgi kaynaklarının gizlilik, bütünlük ve erişilebilirlik konusundaki yapması gereken görev ve sorumlulukları konusunda eğitmektir. Bilgi güvenliği eğitimleriyle insanlar sadece bilginin korunması konusunda nasıl katkı sağlayabileceklerini değil aynı zamanda bilginin neden korunması gerektiğini de öğrenmelidir. Çalışanlar hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etkiyi eğitimler aracılığıyla açıkça anlamalıdır. Kullanıcı bilinçlendirme çalışmaları, güvenlik ihlallerinin maliyetini azaltmaya ve kontrollerin kurumun tüm bilgi kaynakları üzerinde dengeli uygulanmasına yardımcı olacaktır.

Güvenlik farkındalık eğitimlerinin amacı, güvenlik ve güvenlik kontrollerinin önemi hakkında kurum çalışanlarında kollektif bir bilinç oluşturmasıdır. Bilinçlendirme

mesajları basit ve açık olmalı, bilinçlendirme eğitimleri çalışma gruplarının anlayabileceği basit bir formatta verilmelidir.

Çoğu kurumda güvenliğin sağlanması için yapılması gereken kısıtlamaların kullanıcıların alışkanlıklarıyla ters düşmesinden dolayı güvenlikle ilgili yaptırımların uygulanmasında geç kalınmaktadır. Kurumsal güvenlik uygulamaları başından itibaren uygulanmadığından zamanla her kullanıcının, güvenliğe dikkat etmeksizin farklı kullanım alışkanlıkları edindiği görülmüştür. Bu durum bilgi güvenliği bilinçlendirme eğitiminin uygulanmasını zorlaştırarak, kullanıcılarda güvenlik uygulamalarına karşı direnç oluşmasını sağlamaktadır. Çünkü sadece kullanıcıları eğitmek değil aynı zamanda eski alışkanlıklarından kurtarmak gerekmektedir. Kullanıcılara göre kurum güvenlik önlemleri olmaksızın bugüne kadar gayet iyi çalışmıştır ve hiçbir sorunla karşılaşmamıştır. Yeni güvenlik önlemleri hayatı zorlaştırıcı gereksiz değişiklikler olarak görülür. Bilinçlendirme eğitimleri güvenlikle ilgili bilgi vermenin yanında kullanıcı alışkanlıklarından nasıl kurtarılacağı göz önüne alınarak hazırlanmalı akıcı ve eğlenceli bir içerikle kullanıcılara sunulmalıdır.

Tez kapsamında yapılan araştırmalarda çoğu kurumda güvenlik bilinçlendirme programının olmadığı görülmüş, olan kurumlarda ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi başaramadığı tespit edilmiştir. Eğitimin başarılı olabilmesi için kullanıcıların kafasındaki neden sorusunun cevabı kullanıcıyı ikna edecek şekilde verilmelidir. Örneğin, güçlü şifrelerin kullanılmasını sağlayan kurallara sahip bir şifre politikasını kullanıcılara güçlü şifreler kullanarak bilgi güvenliği ihlallerini önleyebilirsiniz açıklaması yerine, basit şifrelerin nasıl ve ne kadar kısa sürede kırıldığını, saldırganlar tarafından nasıl kötü niyetli kullanılabildiğini, şifrelerin çalınması durumunda meydana gelebilecek güvenlik ihlallerinin sonuçlarını kendilerini nasıl etkileyeceği konusunda örnekler ve yaşanmış gerçek hikâyelerle desteklemesi eğitimin amacına ulaşmasını sağlayacaktır. Başarılı bir eğitim sonrasında kullanıcıların şifreleme politikasına sahip çıkarak yeni politikanın uygulanmasında gayretli olacakları görülecektir.

Etkili bir bilgi güvenliği için uygun eğitim programının geliştirilebilmesinde dikkat edilmesi gereken hususlar aşağıda maddeler halinde verilmiştir.

Kurumsal bilgi güvenliği politikalarının oluşturulması: İyi yazılmış bilgi güvenliği politikası başarılı bir eğitim ve bilinçlendirme çalışmasının temelini oluşturur. Bilinçlendirme çalışmasına başlamadan önce tüm üst seviye hedeflerin ve güvenlik programının gereklerinin dokümante edilmiş olması kritik önem taşımaktadır. Bölüm 3'de ayrıntılı bir şekilde açıklanan güvenlik politikaları kurumun bilgi güvenliği konusundaki önceliklerini yansıtmalıdır. Politikalar oluşturulduktan sonra kullanıcılar politikanın varlık ve içeriğinden haberdar olmalıdır. Kullanıcılar aynı zamanda politikaya uymamanın doğuracağı cezai sonuçlar ve yaptırımlar hakkında da bilgi sahibi olmalıdır.

Eğitim ihtiyaçlarının tespiti: Başarılı bir bilinçlendirme ve eğitim programının geliştirilmesindeki ikinci adım kurum personelinin bilgi seviyeleri gözetilerek mevcut eğitim ihtiyaçlarının belirlenmesidir. Yapılan araştırmalarda bu adımın genellikle göz ardı edilmekte veya geçiştirilmekte olduğu görülmüştür. Çoğu kurumda programların içeriği kullanıcıların ihtiyaçlarına göre değil de varsayımlara dayanılarak geliştirilmektedir. Kullanıcıların güvenlik konusundaki mevcut bilgi düzeyinin ölçülmesi için gerekli görüldüğünde kullanıcılarla kısa sohbetler yapılması eğitim ihtiyaç ve önceliklerinin doğru tespitine yardımcı olacaktır. Kullanıcıların öğrenme becerisi ve tercihleri, özel ilgi alanları, bilinçlendirme programına karşı duyulan direnç ya da sempati, daha önceki başarılı veya başarısız eğitim girişimleri, daha önceden mevcut bulunan eğitim, kaynak ve materyalleri, programın başarısı için destek alınabilecek kişi veya grupların tespitinin yapılması eğitim ihtiyaç ve önceliklerinin doğru tespitine yardımcı olacaktır. Farklı kıdem, unvan ve iş tanımlarına sahip kullanıcılar ile görüşme, genel kullanıcılara temel güvenlik bilgileri hakkında anket veya kısa soru listesi gönderme, kurumda son zamanlarda karşılaşılmış güvenlik problemlerinin tespiti, sızma testlerinden elde edilen sonuçların değerlendirilmesi, yüz yüze toplantılar gerçekleştirilmesi, bina ve kullanım alanlarının ziyaret edilerek fiziksel güvenlik seviyesinin gözlenmesi (kilitlenmemiş ofis odaları, dolaplar ve güvenliği bulunmayan kişisel bilgisayar) eğitim ihtiyaçlarının tespitinde izlenmesi gereken yöntemlerdir.

Gerekli desteğin sağlanması: Eğitim ihtiyaçlarının tespitinden sonraki aşama, yönetimin ve kurum genelinde kullanıcıların desteğinin alınması için yapılması gereken çalışmalardır. Bilinçlendirme ve eğitim programı ihtiyacının kurum genelinde kabul ettirilmesi zor bir iştir. Tez kapsamında yapılan çalışmalarda güvenlik eğitimi ve bilincinin genellikle güvenlik araçlarından sonra düşünülen ikincil bir öneme sahip olduğu gözlemlenmiştir. Aslında güvenlik bilinci güvenlik araçlarından daha önemli bir seviyede değerlendirilmesi gereken önemli bir unsurdur. Yönetim desteğinin sağlanmasındaki birinci hedef kaynak teminidir. Kurumun büyüklüğüne göre gerekli bütçe ve istihdam sağlanmalıdır. Bir diğer önemli hedef ise yönetim kademesindeki personelin davranışları ile tüm kurum çalışanlarına örnek olacak şekilde bilinçlendirme programına değer vermeleri ve programa katılmaları, kurum genelinde kullanıcıların desteğinin alınması için çok önemlidir. Yöneticiler, eğitimin önemini ortaya koyup desteklerse eğitime katılma ve yarar sağlama konusundaki kullanıcı istekliliği daha da artacaktır. Yönetim desteğinin sağlanması için yönetim bilinçlendirme çalışması kurumsal bilgi güvenliği açısından hayati önem taşımaktadır.

Eğitim gruplarının belirlenmesi: Bir sonraki önemli adım eğitim alacak grupların seviyelerine göre sınıflandırılmasıdır. Kullanıcılar işlerini yaparken aynı derece veya tipte güvenlik bilincine ihtiyaç duymaz. Kullanıcı grupları arasında gerekli ayrımı yapan ve her gruba sadece ilgili bilgiyi sunan bir bilinçlendirme ve eğitim programı en iyi sonucu elde edecektir. Yaşadığımız bilgi çağında neredeyse her gün bilgi bombardımanına maruz kalınmaktadır. Bilgi güvenliği bilinçlendirilmesi amacıyla iletilmek istenen mesajların kulak ardı edilmemesi için sadece gerekli bilgilerin ilgili gruplara iletilmesi gerekmektedir. Tez kapmasında yapılan araştırmalarda genellikle tek tip programların tüm gruplara uygulandığı ve bilinçlendirme programının istenen başarıya ulaşamadığı tespit edilmiştir. Eğitim grupları kurum ihtiyaçlarına göre güvenlik bilinci seviyesi, teknik bilgi seviyesi, ünvan/yetki, iş fonksiyonu, kullanılan teknolojiler gibi yöntemler izlenerek belirlenebilir.

Eğitim araçlarının belirlenmesi: Bilinçlendirme programındaki bir sonraki adım eğitim için kullanılacak iletişim araçlarının belirlenmesidir. Her kurum kendine özgü

farklı iletişim araçlarına sahiptir. Eğitimde kullanılabilecek kaynakların tespiti yapıldıktan sonra, ilgili kaynakların kullanımına yönelik prosedürler oluşturulmalıdır. Eğitimlerde kullanılabilecek kurumsal iletişim araçlarına e-posta, sesli veya görüntülü çoklu ortam dosyaları, genelgeler, intranet, yazılı yayın (posterler, dergiler, kitaplar, broşürler, kurum yayınları), yüz yüze görüşmeler (toplantılar, sunumlar, eğitim ve güvenlik seminerleri) örnek olarak verilebilir. İletişim aracının seçiminde farklı kitlelerin farklı biçimlerde öğrenmeye açık oldukları düşünülmelidir. Eğitimin etkili ve istenilen düzeyde başarılı olması için ihtiyaçlar ölçüsünde farklı iletişim araçları kullanılabilir.

Eğitim stratejisinin geliştirilmesi: Başarılı bir bilinçlendirme çalışmasının uygulanabilmesi için gerekli olan, bir diğer adım tutarlı ve etkili bir eğitim stratejisinin geliştirilmesidir. Strateji geliştirilmeden verilen eğitimler kullanıcılar tarafından düzensiz ve geçici bir çalışma olarak algılanacaktır. Bilinçlendirme stratejisinin parçası olarak işe alım sırasında yapılacak bilgilendirme, aylık şirket bülteni, şirket eğitimleri, yemek listesi veya menüsü, yıllık güvenlik seminerleri, bilgi güvenliği konusundaki başarılar için teşvik ödülleri, oyunlar, yarışmalar düzenli olarak periyodik şekilde yapılmalıdır. Eğitimler, temel son kullanıcı eğitimi, teknik eğitim, gelişmiş bilgi güvenliği eğitimi (bilgi güvenliği uzmanları ve denetçileri), dönemsel eğitim paketi (her dönem farklı bilgi güvenliği konusuna odaklanılır) içeriğiyle hazırlanmalı ve ilgili çalışma gruplarına periyodik olarak verilmelidir.

Ölçme: Eğitim programının son adımıdır. Verilen eğitimler sonrasında çalışma gruplarının eğitimlerden hangi oranda faydalandığının ölçümlenerek değerlendirmelerin yapılması katılımcılardaki ilerleme ve gerilemelerin ölçümlenmesi açısından önemlidir. Verilen eğitimler sonrasında yapılacak olan sızma testleriyle kullanıcıların seviyeleri ölçümlenebilir.

Artan güvenlik ihlallerinin kaynaklarına dikkat edildiğinde kullanıcıların bilinç ve eğitim seviyelerinde yetersizliklerin ön planda olduğu ortaya çıkmaktadır. Pek çok kullanıcı, bilgi ve bilgi kaynaklarının korunmasının önemi konusunda yeterli bilgiye sahip değildir. İyi tasarlanmış ve sonuçlandırılmış bilinçlendirme ve eğitim çalışması

güvenlik zincirinin en kırılgan halkası olan insan faktörünün güçlendirilmesine büyük katkı sağlayacaktır

Bilinçlendirme programlarında son kullanıcıların bilgilendirileceği alanlar ve içerik örnekleri Çizelge 6.1'de verilmiştir.

Çizelge 6.1. Bilinçlendirme programı örnekleri

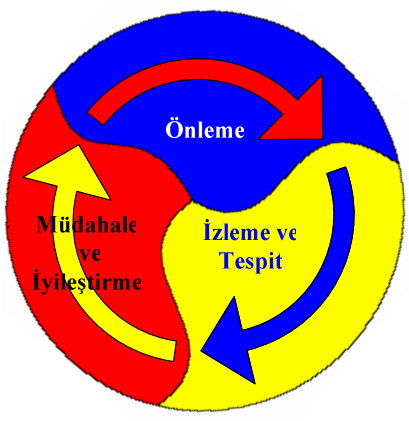
Bilinçlendirme Konusu	İçerik Örnekleri
Sosyal Mühendislik	Telefon yoluyla kandırmaca, e-posta aracılığıyla bilgi alma, sohbet, vb.
Şifre kullanımı ve yönetimi	Şifrelerin oluşturulması, değiştirme sıklığı, şifrelerin korunması, şifrelerin uzunluğu, tek kullanımlık şifreler, vb.
Kötücül yazılımlardan korunma	Tipleri, bulaşma belirtileri, tarama, temizleme, imzaların güncelleştirilmesi, vb.
Güvenlik politikaları	Sorumluluklar, cezai yaptırımlar, vb.
E-posta kullanımı	Şüpheli e-postaların ve eklerinin silinmesi, sazan e-postaların tespiti, vb.
Web kullanımı	Güvensiz ve yasaklı sitelere girilmemesi, dosya indirme, vb.
Yedekleme ve geri alma	Güvenli yedekleme, periyot, yedekten geriye dönme, vb.
Güvenlik ihlali	Kime başvurulmalı, ilk ne yapılmalı, vb.
Mobil cihazların güvenliği	Hırsızlık önlemleri, şifreleme, vb.
Erişim	En az yetki ilkesi
Masaüstü güvenliği	Şifre korumalı ekran koruyucuları, temiz masa temiz ekran, vb.
Fiziksel güvenlik	Bariyerler, kilitli dolaplar, kameralar, vb.
Lisanslama	Lisanssız programların zararları, hukuki boyutları, vb.

6.3. Teknoloji

Bilgi güvenliğinin sağlanmasında kullanılan teknolojiler zafiyetleri bulmak ve gidermek için geliştirilmiş yazılım veya donanım çözümleridir. Günümüzde bilgi güvenliğinin sağlanmasında kullanılan teknolojilerin seçiminde karma yapılar gittikçe artmaktadır. Karma yapılarla kurulan katmanlı güvenlik mimarileri bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir rol oynamaktadır. Ancak burada dikkat edilmesi gereken en önemli husus karma yapıdaki katmanlı mimarilerin

kurulum, bakım ve işletilmesinde üst düzeyde teknik bilgiye gereksinim duyulmasıdır. Eğer bu teknik işçilik kurumun kendi bünyesinde mevcut değilse dış kaynak kullanımına gidilmelidir. Aksi takdirde teknoloji seçiminin doğru yapılmasına rağmen insan faktörü ve eğitimlere gerekli hassasiyetin gösterilmemesi teknolojik yatırımları boşa çıkartacağı gibi daha çok güvenlik ihlallerinin meydana gelmesine neden olacak ve yatırımların boşa gitmesine ve kaynakların israf edilmesi sonucunu doğuracaktır.

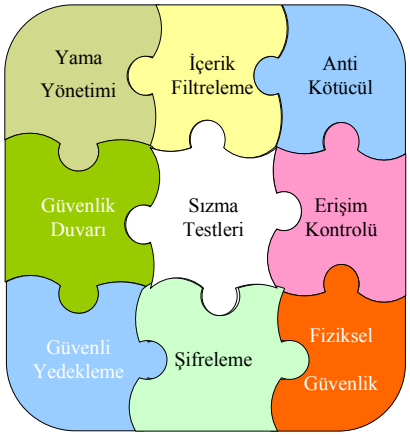
Bilgi güvenliğinin sağlanması konusunda kullanılan, teknolojik çözümleri işlevlerine göre önleme (prevention), izleme ve tespit etme (detection), tepki verme (reaction) şeklinde üç grupta sınıflandırılmaktadır [237]. Şekil 6.7'de bu sınıflandırma ve aralarında olması gereken akış verilmiştir. Şekilden de görülebileceği gibi sınıfların birbirinden farklı olduğu gibi bir anlam çıkartılmamalı bir bütünün parçaları gibi değerlendirilmelidir. Aralarındaki bu ilişkide oklarla gösterilmiştir. İşlevlerine göre bu sınıflandırma aşağıda detaylı olarak açıklanmıştır.



Şekil 6.7. İşlevlerine göre teknoloji sınıfları

Önleme: Bilgi sistemlerinin güvenlik ihlallerine maruz kalmaması için koruma ve sağlamlaştırma amaçlı önleyici teknolojiler kullanılmaktadır. Sızma testleri, sistemlerin güncellenmesi, kötücül yazılımlardan korunma (virüs, solucan, casus yazılımlar, vb.) servis (URL, SMTP, vb.) içeriklerinin filtrelenmesi, atakların güvenlik duvarı aracılığıyla engellenmesi, gizli bilgilerin şifrelenmesi veya özetlenmesi, bilgiye erişimlerin kontrollü yapılması, bilgilerin yedeklenmesi önleyici

teknolojilerin görevleri arasında yer almaktadır. Başlıca önleyici teknolojiler Şekil 6.8'de gösterilmiştir.



Şekil 6.8. Bilişim sistemleri güvenliği için önleyici yaklaşımlar

Sızma testleri, güvenlik kontrollerinin sınanması ve ölçümlenmesi açısından ayrı bir önem taşımaktadır. Bölüm 4'de ayrıntılı bir şekilde açıklanan sızma testleri, bilgi güvenliği ihlallerinin önlenmesinde önemli bir görev üstlenmektedir. Sızma testleri sayesinde bilgi güvenliği ihlalleri meydana gelmeden zafiyetler belirlenebilir. Tespit edilen zafiyetlerin giderilmesi amacıyla, gerekli olan güvenlik kontrolleri sağlanarak bilgi güvenliği ihlallerinin oluşmaması veya önlenmesi için gerekli önlemler alınabilir.

Güvenlik duvarı, önleyici teknolojiler denildiğinde ilk akla gelen çözümlerdendir. Bölüm 2'de anlatılan güvenlik duvarları kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında kullanılan teknolojilerin başında gelmektedir. Ağları koruyan güvenlik duvarlarına ek olarak, günümüzde uygulamaları koruyan güvenlik duvarları hızla yaygınlaşmaktadır. Bu mimaride geliştirilen güvenlik duvarları uygulama (application) katmanında (FTP, HTTP, SMTP, POP3, IMAP, TELNET, FINGER, DNS) meydana gelen saldırıların önlenmesinde kullanılmaktadır.

Erişim kontrolü, kaynakların yetkisiz kullanımının önlenmesi amacıyla bilgiye, kim tarafından, hangi yetkiyle, hangi zaman dilimlerinde erişileceğinin tanımlandığı önleyici teknolojilerin kullanıldığı yazılım veya donanım çözümleridir. Erişim

kontrolleri daha önceden tanımlanan IP adresleri, MAC adresleri, kullanıcı adları gibi ayırt edici özelliklerin bir veya bir kaçının yer aldığı erişim listeleri kullanılarak yapılmaktadır.

Güvenli yedekleme, bilgi güvenliği ihlalleri sonucunda en kısa zamanda felaket öncesindeki duruma geri dönülebilmesi amacıyla alınması gereken önlemlerden en önemlisidir. Ancak yapılacak yedeklemenin güvenliğinin sağlanması ve erişilebilirliğinin doğrulanması gerekmektedir. Güvenli yedekleme teknolojileri sayesinde yedeklenen bilgilerin doğruluğu denetlenerek güvenli bir ortamda depolanması sağlanır.

Şifreleme, bilgilerin gizliliğine ve bütünlüğüne karşı yapılacak saldırıların önlenmesi amacıyla kullanılan yazılım veya donanım çözümleridir. Şifreleme Bölüm 2'de anlatılan haberleşme güvenliğine ek olarak önemli bilgilerin (parolalar, ticari bilgiler, vb.) şifreli olarak depolanması, inkâr edememe, özetleme algoritmaları, özel sanal alan ağları gibi bilginin gizlilik veya bütünlüğünü sağlayan amaçlar içinde kullanılmaktadır.

Fiziksel güvenlik, bilgilerin yer aldığı fiziksel mekânlara erişilmesini engelleyen veya belirlenen yetkiler dâhilinde erişilmesini sağlayan teknolojilerin kullanıldığı çözümlerdir. Bölüm 2'de açıklanan fiziksel güvenliğin sağlanması amacıyla binaların çevrelerine çitler çekilebilir, kapıların önlerine nöbetçiler veya bariyerler konulabilir, kapı giriş çıkış sistemleriyle kimliklendirme ve yetkilendirme yapılabilir, kameralarla tüm olaylar kayıt altına alınabilir.

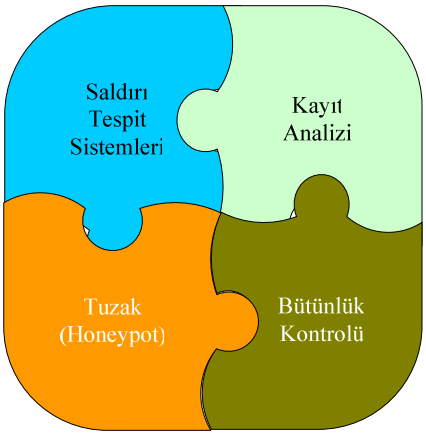
Yama yönetimi, kurumsal bilgi güvenliğinin sağlanması amacıyla önleyici teknolojiler arasında en fazla ihtiyaç duyulan ve teknik sorumlular tarafından genellikle ihmal edilen çözümlerden bir tanesidir. Tez kapsamında yapılan çalışmalar çerçevesinde güvenlik ihlalleri incelenmiş ve ihlal sebeplerinin çoğunlukla güvenli yaması yüklenmemiş bilişim sistemlerindeki açıklıklar olduğu görülmüştür. Yamaların düzenli olarak geçilmemesi sonucunda üretici firma tarafından tüm dünyaya duyurulan açıkların bilgi seviyesi düşük olan saldırganlar veya basit

solucanlar tarafından bile rahatlıkla kullanılarak bilgi güvenliği ihlalleri oluşturduğu bilinmektedir.

İçerik filtreleme, uygulama katmanında çalışan bazı protokoller (HTTP, SMTP, FTP) içerisindeki zararlı içeriklerin (virüsler, solucanlar, truva atları, vb.) temizlenmesi amacıyla kullanılan yazılım veya donanım çözümleridir. İçerik filtreleme yazılımları son kullanıcıların kötücül içerikli e-posta almalarını veya zararlı web sitelerini ziyaret etmelerini engelleyerek güvenlik risklerini minimuma indirgemektedir.

Karşı (anti) kötücül yazılım veya donanım çözümleri sayesinde bilgi sistemleri kötücül yazılımlardan korunmaktadır. Bilgi güvenliği ihlallerinin oluşmasına birinci dereceden neden olan kötücül yazılımlar her geçen gün değişik yöntemlerle bilgi sistemlerine saldırmakta ve zarar vermektedir. Bu saldırıların üstesinden gelmek için kötücül yazılımların sürekli güncel tutulması gerekmektedir.

İzleme ve tespit: Önleyici tedbirlere rağmen şüpheli bir durumun araştırılması veya meydana gelen güvenlik ihlallerinin aydınlatılmasını sağlayan teknolojilerdir. Saldırı tespit sistemleri, kayıt analizi yapan yazılımlar, bütünlük kontrolü yapan yazlımlar, tuzak sistemler (honeypot), fiziksel güvenlik bileşenleri (kamera kayıtları, ses kayıtları, vb.) başlıca izleme ve tespit teknolojileri olarak sıralanabilir. İzleme ve tespit teknolojilerinin iyi bir altyapı oluşturması için Şekil 6.9'da gösterildiği gibi dört unsuruda içermesi gerekmektedir.



Şekil 6.9. İzleme ve tespit teknolojileri

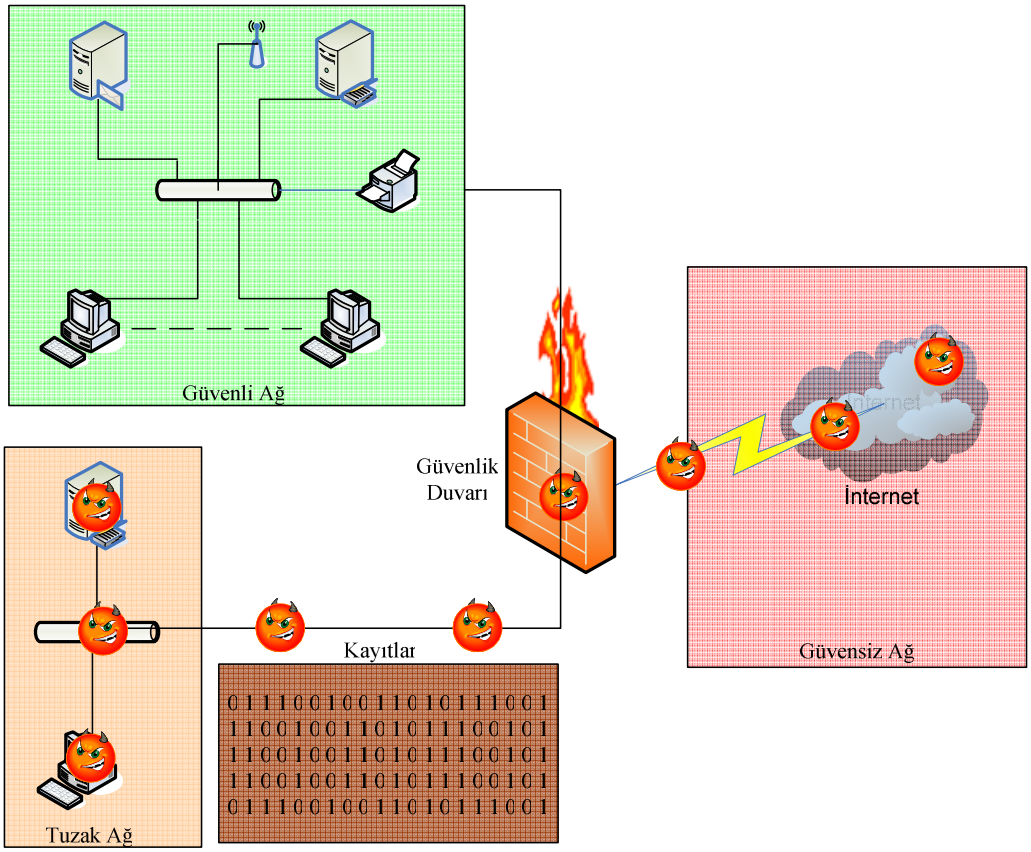
Bölüm 2'de anlatılan saldırı tespit sistemlerinin kurulması, ağ veya sunucular üzerinden gerçekleşen saldırıların anında tespit edilmesi ve tüm ilgili trafiğin kayıt altına alınmasını sağlayan izleme ve tespit teknolojisidir. Uygulanacak güvenlik mimarisine göre, ağ'ın uygun noktalarına ve önemli sunuculara yerleştirilecek saldırı tespit sistemleri üzerinde tanımlanacak kurallar ile beklenmeyen durumların tespit edilebilmesi mümkün olacaktır. Bu yöntemle, örneğin, veri tabanı sunucusuna gelen ve aslında beklenen bir istek olmayan http bağlantı isteklerinin tespit edilmesi sağlanabilir. Sunucu temelli saldırı tespit sistemleri ile ağ üzerinden gerçekleşmeyen ya da ağ üzerinden şifrelenmiş bir bağlantı (VPN, IPSEC, SSH, vb.) aracılığı ile gerçekleşen saldırıları tespit etmek ve saldırıya ilişkin tüm adımları kayıt altına alarak izlemek mümkün olabilecektir

Günümüzde bilgi istemleri üzerinde üretilen kayıtların sayısı insanlar tarafından takip edilemeyecek büyüklük ve karışıklıktadır. Güvenlik ihlallerinin karmaşıklığı ve sayısı her geçen gün artmakta ve tespit edilmesi zorlaşmaktadır. Şüpheli bir durumun olup olmadığının tespit edilebilmesi için ağ sistemleri, işletim sistemleri ve güvenlik yazılımlarının ürettiği kayıtları merkezi olarak depolayan ve yorumlayan kayıt analizi yazılımlarına ihtiyaç duyulmaktadır. Kayıt analizi izleme ve tespit teknolojileri içerisinde güvenlik ihlallerinin tespit edilmesindeki tek yöntem olduğundan önemli bir yere sahiptir.

Güvenlik ihlallerinin doğru tespit edilebilmesi için kayıtların hatasız ve herhangi bir değişime uğramadığından emin olunması gerekmektedir. Başarılı bir saldırı sonrasında saldırganlar iz bırakmamak veya hedef şaşırtmak amacıyla tutulan kayıtları yok etmek veya değiştirmek amacıyla kayıt tutan yazılımlara da saldırmak isteyeceklerdir. Verilerin veya uygulamaların hiç bir değişime veya bozulmaya uğramadığından emin olunması için özetleme algoritmalarının kullanıldığı bütünlük kontrolü yapan yazılımlardan faydalanılmaktadır. Kayıt tutan yazılımların belirli aralıklar ile bütünlük kontrolü yapan yazılımlar aracılığıyla denetlenmeleri bu yazılımlara yönelik saldırıların gerçekleşip gerçekleşmediğini gösterebilir.

Kurumsal ağ içerisinde özel olarak hazırlanmış, ağın diğer kısımlarıyla izole edilmiş bir konumda yerleştirilen aldatıcı veya gerçek güvenlik açıkları barındıran,

saldırganlar için çekici bir hedef olarak görünen tuzak sistemlerdir. Tuzak sistemlerine bir örnek Şekil 6.10'da verilmiştir.



Şekil 6.10. Tuzak sistemlerin örnek gösterimi

Gelişmiş bir tespit sistemi olan tuzak veya hedef şaşırtma teknolojisi, bilgisayar korsanlarının veya saldırganların tespit edilmesi ve onların hangi amaçla saldırılarını düzenlediğinin anlaşılması açısından önem taşımaktadır. Normal şartlar altında hiçbir kullanıcı tarafından erişilemeyecek ve kullanılamayacak bir bilgisayar sistemi olan tuzağa her erişim potansiyel bir saldırı olarak değerlendirilebilir. Tuzak kayıtlarının incelenmesi ile saldırganlar, davranışları ve hedefleri ile ilgili bilgiler toplanabilir. Tuzak sistemlerin gerçek sistemlerden tam anlamıyla izole edilebilmesi için çok iyi yapılandırılması gerekmektedir. Aksi takdirde saldırganlar tuzak sistemlerdeki açıklardan faydalanarak, gerçek bilgiler içeren güvenilir ağlara sızarak bilgi

güvenliği ihlalinin oluşmasına neden olabilir. Tuzak sistemlerini bir tür erken uyarı sistemi olarak düşünmek mümkündür.

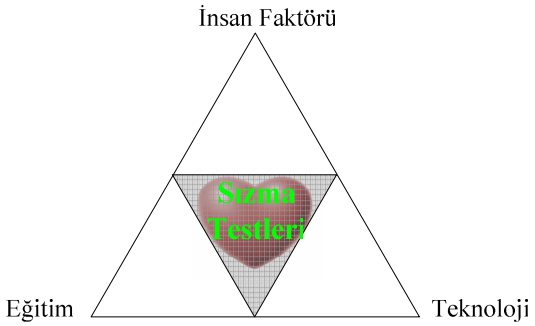
Müdahale ve iyileştirme: Kurumsal bilgi sistemlerinde meydana gelen bilgi güvenliği ihlallerinin oluştuktan sonra durdurulmasını sağlayan, en kısa zamanda bilgi sistemlerinin çalışır hale getirilmesine yardımcı olan teknolojilerin kullanıldığı yazılım veya donanım çözümleridir. Müdahale aşamasında, saldırı sonrasında meydana gelen zararların tespiti ve meydana gelen ihlallerin ne olduğunun detaylı olarak araştırılması amacıyla analizler gerçekleştirilir. Saldırının hukuki ve teknik boyutunun çözümlenebilmesi amacıyla adli (forensic) araçlar kullanılır. Delillerin toplanması, hasarın büyümesinin önlenmesi, en kısa sürede güvenlik ihlali öncesine dönülmesi ve saldırı izlerinin temizlenmesi bu teknolojiler sayesinde gerçekleştirilen hizmetlerdir.

Sızma testleri müdahale ve iyileştirme aşamasında iki farklı amaç için kullanılmaktadır. Sızma testleri aracılığıyla saldırıya uğrayan sistemlerdeki açıkların tespit edilerek saldırının nasıl gerçekleştirilmiş olacağına dair senaryoların ortaya çıkartılması sızma testlerinin bu aşamadaki kullanım amaçlarından birisidir. Sızma testlerinin bir diğer kullanım amacı ise bilgi sistemlerinde iyileştirmeler yapıldıktan sonra iyileştirmelerin güvenlik açığını kapattığının sınanması açısından yapılan çalışmalardır. Sızma testleriyle saldırganın ihlali nasıl gerçekleştirdiğinin belirlenemediği durumlarda sistemlerin kısa sürede yeniden hizmete alınması mümkün olmayabilir. İhlale neden olan zayıflık tespit edilmeksizin saldırı öncesi duruma dönülmesi halinde saldırının aynı biçimde tekrar gerçekleşmesi riski söz konusu olacaktır. İyileştirme kapsamında, diğer adımlarda edinilen bilgi ve deneyimlerin ışığında bilgi sistemlerinin güvenliğinin arttırılmasına yönelik, tespit teknolojilerinin iyileştirilmesine ve müdahale süreçlerinin etkinliğinin arttırılmasına çalışılır.

6.4. Sızma Testlerinin Önemi

KBG'nin sağlanmasında baş aktörler olan insan, eğitim ve teknoloji faktörleri bu bölüm içerisinde alt başlıklar halinde sırasıyla incelenmiştir. Bilgi güvenliğine etki

eden faktörlerin bir bütün olarak saldırgan gözüyle sınanması, zafiyetlerin tespit edilerek giderilmesi için yapılacak düzeltmelerin ve sıkılaştırmaların belirlenmesi, sızma testlerinin bilgi güvenliğinin sağlanmasındaki önemini özetlemektedir. Bilgi güvenliğine etki eden faktörlerin sızma testleriyle olan ilişkisi Şekil 6.11'de gösterilmiştir. Yüksek seviyede bilgi güvenliğinin sağlanmasında sızma testleri yaşayan bilgi güvenliği üçgeninin merkezinde yer almakta ve bir kalp gibi davranarak bilgi güvenliğinin devamlılığının sağlanmasında önemli rol oynamaktadır.



Şekil 6.11. Sızma testlerinin bilgi güvenliğindeki yeri

Sızma testleri, çalışan bilgisayar sistemlerinin başına olumsuz bir durum gelmeden önce, sistem açıklarını önleyecek ve alınabilecek karşı tedbirlerin karşı savunulacak ve ihtiyaçların düşünülmesinde kullanılan önemli bir erken uyarı sistemidir. Sızma testlerinin başarılı olabilmesi için kurumların güvenliğine etki eden faktörlerinin ağırlıkları dikkate alınarak kuruma özgü farklı senaryolar geliştirilmesi gereklidir. Sızma testleri için geliştirilen senaryolar kurumlarda kullanılan teknolojilere, çalışanların bilgi düzeylerine, kurumsal bilgi güvenliği seviyesine, bilgi güvenliği bileşenlerinin dozuna göre farklılık gösterebilir.

Sızma testleri, bilgi güvenliği ihlallerinin kontrollü bir şekilde tespit edildiği, kurumsal bilgi güvenliğinin sağlanması için düzenli olarak yapılan askeri tatbikatlara benzetilebilir. Tatbikatlar bir ülkenin güvenliğini sağlayan ordular için ne kadar önemliyse, sızma testleride kurumlar için bilgi güvenliğinin sağlanması açısından aynı derecede öneme sahiptir. Tatbikatın başarısı gerçek savaş ortamlarının tam anlamıyla simülasyonuna bağlıyken, sızma testlerinin başarısı da gerçek dünyada

bilgi güvenliği için tehditler oluşturan saldırganların teknik ve taktiklerinin tam olarak simülasyonuna bağlıdır. Saldırganlar her geçen gün yeni teknik ve taktikler geliştirerek veya geliştirilmiş araçları kullanarak kurumlara saldırmaktadır. Kurumsal bilgi güvenliğinin sağlanabilmesi için saldırganlarla meydana gelebilecek olası sanal savaşların kazanılması gerekmektedir. Düzenli olarak yapılan sızma testleri, eksiklikler, aksaklıklar, zayıflıklar ve ihtiyaçların meydana çıkartılarak sanal savaşların saldırganlara karşı kazanılmasında önemli rol oynayacaktır.

Bu tez çalışmasında bir kez daha açıkça görüldüğü gibi günümüzde birçok bilgisayar sisteminin büyük ölçekli bilgi sistemi güvenlik gereksinimleri gözönünde bulunmaksızın tasarlanıldığı ve doğru yaklaşımlar kullanılmadığı için donanımsal ve yazılımsal çözümlere yönelmeden dolayı maliyetlerde artışlar olmaktadır. Bu sistemleri yeniden kurmak çoğunlukla maliyet ve zaman açısından imkânsızdır. Bu sistemler üzerinde yapılacak sızma testleri sonucunda zafiyetlerin tespit edilerek güvenlik açıklarının giderilmesi zaman ve maliyet açısından uygun ve istenen bir çözümdür. Bu durum kurumsal bilgi güvenliğinde sızma testlerinin maliyet ve zaman boyutları açısından önemini göstermektedir.

Tez kapsamında yapılan araştırmalar sonucunda ülkemizde sızma testlerinin henüz yaygınlaşmadığı ve kurumlar tarafından kurumsal bilgi güvenliğinin sağlanmasında önemli bir bileşen olduğunun bilinmediği tespit edilmiştir. Bu durum sızma testlerinin kurumlara katkılarının, sağlayacağı farkındalığın ve güvenlik seviyesinin artırılmasına katkısının ülkemizde pek bilinmediğinin ve yeterince önem verilmediğinin göstergesidir. Ülkemizde çok az sayıda olan güvenlik firmalarıyla sızma testleri konusunda görüşmeler yapılmış ve izlediği metodolojiler hakkında bilgiler edinilmeye çalışılmıştır. Çoğunluğunun sızma testlerini piyasadaki hazır araçlar (zafiyet tarama, port tarama, şifre kırma, vb.) kullanarak yaptıkları tespit edilmiştir. Bölüm 4'de açıklandığı gibi sadece hazır araçlar kullanılarak iyi bir sızma testi yapılamaz. Doğal olarak, otomatik araçlarla yapılan teknik içerikli sızma testlerinin sonuçları gerçek durumu yansıtmayacaktır. Yüksek seviyede bir bilgi güvenliğinin sağlanabilmesi amacıyla birçok elle yapılan teknik olmayan testlerinde mutlaka yapılması gerekmektedir.

7. SONUÇ VE ÖNERİLER

Ülkemizin üzerinde bulunduğu bölgenin jeopolitik açıdan çok önemli olması, bölgede süper güç olma yolunda ilerleyebilme, tarih boyunca olduğu gibi gelecekte de varlığımızı istemeyen birçok düşmanımızın olması ve burada bahsedilmeyen birçok sebeplerden dolayı ulusal bilgilerimizin güvenliğinin sağlanması ülkemizin geleceği açısından çok önemlidir. Ulusal bilgilerin güvenliği, ülkemizde silahlı kuvvetler, sağlık, eğitim, hukuk, teknoloji ve diğer birçok alanda hizmet veren kurum ve kuruluşların bilgilerinin güvenliğinin sağlanmasına bağlıdır. Bu kapsamda kurumsal bilgi güvenliği sadece kurumların kendisi için değil ulusal güvenliğimizin sağlanması konusunda da ülkemiz için çok önem taşımaktadır.

7.1. Sonuçlar ve Değerlendirmeler

Her geçen gün e-toplum olma yolunda hızla ilerleyen ve e-devletleşme çalışmalarını sürdüren ülkemizde, maalesef bilgi güvenliğinin öneminin kamu veya özel sektör tarafından kavranmadığı veya yüksek seviyede bir farkındalığın oluşmadığı tez çalışması sonucunda tespit edilen en önemli bulgulardan birisidir. Ülkemizde bilgi güvenliği konusunda yapılan araştırmalar incelendiğinde bilgi güvenliğinin sağlanmasında dünya standartlarının altında kaldığımız görülmektedir. Bunun için ülkemizde bilgi güvenliği konusunda daha çok araştırma ve geliştirme çalışmalarına ihtiyaç duyulmaktadır.

İnternet ülkemizde her geçen gün hızla yaygınlaşmakta, ticari ve günlük yaşantımızdaki varlığını hissedilir oranda arttırmaktadır. İnternetin doğasında var olan güvensizlik unsuru, internet üzerindeki uygulamaları tehdit eden en büyük unsurdur. 2006 yılı, bilgi güvenliğine yönelik tehditlerin nitelik ve boyut değişimine uğradığı bir yıl olmuştur. Geçmiş yıllarda saldırılar, yaygın ve hedef gözetmeksizin yapılmaktayken artık nokta hedefi gözeten ve bölgesel olarak düzenlenen saldırılar yapılmaktadır. E-posta ve anlık mesajlaşma yoluyla gelen tehditlerin yanı sıra, web'in kendisi de bir tehdit unsuru haline gelmiştir. Günümüzde e-posta ve web tehditlerinin birleşmesiyle çok zararlı ve bulaşıcı virüsler doğmaktadır. Son yıllarda bilgi ve bilgisayar güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, kurumlar

üzerinde maddi manevi büyük zararlara yol açan, kişi, kurum ve kuruluşları tehdit ederek zararlara uğramasına yol açan bilgi güvenliği tehditlerinin engellenmesi için kurumsal bilgi güvenliği sağlanmalıdır.

Kurumsal bilgi güvenliğini tehdit eden saldırıların bilinmesi, bilgi güvenliğinin sağlanmasına yönelik kurumsal stratejilerin geliştirilmesinde önemli bir role sahiptir. Bilgi sistemlerine yönelik olarak yapılan saldırılar incelendiğinde; saldırıların çok geniş bir yelpazede yapıldığı, otomatik teknikler kullanılarak saldırıların kolayca yapılmasının sağlanmasında önemli artışların görüldüğü tespit edilmiştir. Otomatik saldırı araçları sayesinde kurumsal bilgi güvenliğini tehdit eden usta saldırganların yanında bilinçsiz ve bilgi eksiği olan birçok acemi saldırgan türemiştir. Virüs yazarları, eskiye göre çok daha gelişmiş araçlarla çalışmaktadır. Bu araçları kullanan virüs yazarları, yazılım robotları ve rootkitler, sosyal mühendislik, casusluk ve reklâm amaçlı yazılımlardan yararlanarak karmaşık virüslerle bilgi sistemlerini üst düzeyde tehdit etmektedirler.

Kurumsal bilgi güvenliğinin sağlanması amacıyla, saldırı türlerinin takip edilmesi, saldırganların kullandığı yöntemlerin saptanması, ülkemizde ve dünyada bu konuda yapılan araştırmaların, raporların ve çalışmalar ile tespit edilen açıkların takip edilmesi ve giderilmesi bilgi güvenliği ihlalinin yaşanmaması için gerekli önlemlerin zamanında alınması, güvenlik ihlallerine anında müdahale edilerek saldırıların zararlarından en az şekilde etkilenme, felaket anında uygulanabilecek felaket ve iş sürekliliği planlarının uygulanması gibi stratejiler, kurumlar tarafından uygulanmalıdır.

Bilişim sektöründeki gelişmelere bağlı olarak ülkemizde ve dünyada hukuksal sorunlarda gün geçtikçe artmaktadır. Tez kapsamında yapılan çalışmalar 2006 yılında saldırganların saldırıları düzenleme amaçları geçmişte olduğu gibi şan, şöhret, hava, kişisel tatmin iken günümüzde ekonomik amaçlı saldırılar daha ön plana çıkmaktadır. Saldırganlar tarafından yazılan kötücül yazılımlar, artık maddi çıkar sağlamak için kullanılmaktadır. Geçmiş kötücül yazılımlar incelendiğinde; dosyaların silinmesi, işletim sistemlerinin çökertilmesi, bilgisayar performansının düşürülmesi, kullanıcı isteği dışında e-posta gönderilmesi vb. gibi bireysel eylemler

gerçekleştirilirken, günümüzde ise kullanıcı bilgisayarlarına yerleştirilen casus programlar aracılığıyla, internet bankacılığı şifreleri, kredi kartı bilgileri vb. gibi hassas bilgilerin ele geçirilmesi için organize eylemler yapılmakta ve yasal olmayan yollarla ekonomik çıkarlar elde edilmektedir. Kötücül yazılım yazan saldırganlar, işin içine maddiyatın karışması nedeniyle birbirleriyle işbirliği yapmaya ve örgütlenmeye başlamışlardır. Saldırılar artık organize ve planlı olarak yapılmaktadır. Bunun yanında saldırganlar bir araya gelerek, belirli organizasyonlar adı altında teşkilatlanmakta, bilgi alışverişi yapmakta ve güvenliği yeterli seviyede sağlanamayan bilişim sistemlerini veya güvenlik bilinci olmayan kullanıcıları soymaya yönelik yazılımlar geliştirmektedir. Bu tür olayları tespit ederek kullanıcıları korumak için saldırganlara caydırıcı cezaların verilmesi amacıyla bilişim suçlarıyla ilgili yasalara ve uzman bilişim hukukçularının sayısının artmasına ihtiyaç duyulmaktadır.

Tez kapsamında yapılan araştırmalar sonucunda ülkemizde bilişim suçları konusunda kanunların yetersiz olduğu değerlendirilmiştir. Bilişim suçlarıyla ilgili olarak hazırlanan yeni kanun tasarısı ülkemiz açısından önemli bir gelişmedir. Ancak bu kanun tasarısının yasalaşması ve uygulanması gerekmektedir. Ayrıca uygulamada çıkacak aksaklıklar göz önüne alınarak eksikliklerin veya fazlalıkların giderilmesine yönelik çalışmalar yapılmalıdır.

Bilişim ile ilgili kanunların hazırlanması ve uygulanmasında bilişim hukukçularına ihtiyaç duyulmaktadır. Ülkemizde bu alanda uzmanların yetiştirilmesi konusunda üniversitelerimize önemli görevler düşmektedir. Bilişim hukuku ile ilgili dersler hem hukuk fakülteleri hemde bilgisayar mühendisliği ile ilgili bölümlerin müfredatına konularak bu alandaki bilgi altyapısının kurulması ve bilişim hukuku ile ilgili yüksek lisans programları aracılığıyla da uzman adli bilişimcilerin yetişmesi ülkemiz açısından önemlidir.

Kurumsal bilgi güvenliğini sadece saldırganlar, yapılan saldırılar veya oluşan güvenlik açıkları tehdit etmemektedir. Kurumsallaşmasını tamamlayamayan kurum ve kuruluşlardaki prosedürel eksikliklerden kaynaklanan hatalar veya çalışanların sebebiyet verdiği kazalar da bilgi güvenliğini en az saldırganlar kadar tehdit

etmektedir. Bu tip tehditlerin ve saldırıların önüne geçilebilmesi için kurumsal bilgi güvenliğinin sağlanmasında izlenmesi gereken süreçler, görev tanımları ve sorumluluklar, kişilerin uyması gereken politikalar, prosedürler, standartlar ve kılavuzlar tanımlanarak uygulanmaya konulmalıdır.

Bilgi güvenliği dünya genelinde benimsenmiş standartlara bağlı kalınarak yönetilmesi gereken bir süreçtir. Dünyada bilgi güvenliğinin yönetilmesi ile ilgili yapılan çalışmalar sonucunda 2007 yılında gelinen noktaya bakıldığında ISO–27001 standardının tüm dünya tarafından benimsendiği ve uygulamaya koymak için kurumlar tarafından çalışmalar yapıldığı görülmüştür. Ülkemizde bu konuda yapılan çalışmalar ve kurumların farkındalıkları yetersiz olduğundan bilgi güvenliği yönetimi konusunda büyük eksiklikler olduğu tespit edilmiştir.

Bilgi güvenliğinin sağlanması konusu birbirine bağlı ve iç içe geçmiş karmaşık süreçlerden oluştuğundan, bu süreçlerin yönetilemediği durumlarda bilginin güvenliğinden bahsetmek mümkün değildir. Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması; BGYS'nin kurumlarda hayata geçirilmesiyle mümkün olacaktır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir

BGYS'nin kurulmasında, kurumsal bilgi güvenliğinin sağlanmasında ve yönetiminde bilgi kaynaklarına erişimi olan kişilerin uyması gereken kuralların düzenlendiği bilgi güvenlik politikalarının önemli bir yeri vardır. Ülkemizde güvenlik politikaları çoğu kurum ve kuruluşta genellikle sözlü olarak veya e-postalar aracılığıyla kullanıcılara duyurularak kullanıma alındığından istenilen düzeyde etkiyi sağlamamıştır. Güvenlik politikalarının etkin olabilmesi için yazılı olması, yönetim tarafından onaylanması, kullanıcılar tarafından benimsenmesi, uygulanabilir ve kolay yönetilebilir olması, kurumun iş ihtiyaçları ve hedefleri doğrultusunda hazırlanması gerekmektedir.

Kurumsal bilgi güvenliği sağlanmasında, koruma maliyeti gözden kaçırılmamalıdır. Kurumlar tarafından verilmek istenen hizmetler, kullanım kolaylığı ve güvenliğin maliyeti ile uygulanacak olan güvenlik önlemleri arasında denge kurulmalıdır. Hizmetleri aksatacak, kullanımı zorlaştıracak ve maliyeti çok yüksek güvenlik önlemleri kuruluşların sistemlerden elde edeceği toplam faydayı azaltacaktır. Yüzde yüz güvenlik sağlanamayacağı bilinciyle, her zaman için bir bilgi sisteminde bilgi güvenliği ihlalinin oluşma riski vardır. Burada amacın, varolan bu riski önlemek yerine uygun bir maliyet-zaman analizi yaparak uygun kararlar alınması ve yüksek riski düşürmenin yüksek maliyet getireceğinin unutulmamasıdır. Bir bilgi sisteminin güvenliğinin sağlanmasında riski sıfırlamak için o kıymetin değerinden fazla güvenlik için kaynak ayırmak akılcı bir yaklaşım olmayacaktır. Bu nedenle kurumların riski önlemek yerine, risk ile birlikte yaşamayı öğrenmeleri daha uygun bir çözümdür. Bazen korunacak sistemin güvenlik ihtiyacı ile güvenlik sağlamanın maliyeti arasındaki ilişki, güvenlik önlemlerinden vazgeçmeyi gerektirebilecektir. Basit formülü ile sistemden elde edilecek fayda, sistemin maliyetlerinin altında kalmamalıdır. Bununla birlikte, itibar, prestij ve saygınlık gibi ticari ve psikolojik parametreler yüksek maliyetlere rağmen kurumlar açısından korunmak zorunda olan değerlerdir. Yüzde yüz güvenliğin sağlanamayacağı bilinciyle bilgi güvenliği ihlalinin ve riskin daima varolacağı göz önünde bulundurularak yüksek seviyede bilgi güvenliğinin sağlanmasının devamlılık gerektiren bir süreç olduğu unutulmamalıdır.

Bilgilerin düzenli olarak maruz kaldığı bir takım tehditlerin tanımlanmasına, yönetilmesine ve bunların minimize edilmesine yardımcı olan bilgi güvenliği yönetim sistemlerinin kurulması için gereklilikleri ortaya koyan ISO/IEC 27001:2005 (önceki adıyla BS 7799–2:2002) standardı bu tez kapsamında kapsamlı olarak incelenmiş ve sonuç olarak farklı sektörler için:

- KBG risklerinin ekonomik olarak yönetildiğine emin olmak,
- KBG yönetimindeki hukuksal yaptırımların ve önlemlerin yasalara uygunluğundan emin olmak,

- KBG altyapısının içerdiği uygulamaların ve denetimlerin, kurumların amaçladığı güvenlik seviyesi ile uyuştuğunu göstermek,
- KBG yönetim süreçlerini belirlemek ve açıklamak,
- Yönetim tarafından, bilgi güvenliği yönetimi faaliyetlerinin belirlenmesi ve gözlemlenmesini sağlamak,
- İç ve dış tetkikçiler tarafından, kurumun, bilgi güvenliğinin sağlanması konusunda beyan ettiği politikalara, prosedürlere ve standartlara uygunluğunu değerlendirmek,
- Kurumların iş yapmış olduğu diğer iş ortaklarına, bilgi güvenliği politikaları, prosedürleri ve standartları hakkında bilgi sağlanması,

gibi hususları içermesi gerektiği tespit edilmiştir.

BGYS standartlarının kurumlara uyarlanması, anlatılması, kullanıcı, teknik çalışanların ve yöneticilerin eğitilmesi konusunda kuruluşların danışmanlık hizmetleri almaları gerekmektedir. BGYS uygulamaları, kurumlar tarafından başarılı bir şekilde uygulandıktan sonra kuruluşların bilgi güvenliğini yönettiklerine dair uluslararası alanda geçerli olan belgeler alması bilgi güvenliğinin kritik olduğu kurumlar açısından önemli bir göstergedir.

Bu tez çalışması kapsamında yapılan araştırmalar değerlendirildiğinde dünyada ve ülkemizde BGYS konusunda istenen düzeyde yeterlilik ve farkındalık oluşmadığı anlaşılmaktadır. Bilgi güvenliği daha öncede birçok kez tekrarlandığı üzere mutlaka yönetilmesi gereken, idari ve teknik konuları içeren birçok karmaşık süreçten oluşmaktadır. Tüm dünyada kabul edilmiş olan, bir kuruluşun sadece teknik önlemlerle bilgi güvenliğini ve iş sürekliliğini korumasının mümkün olmadığı görüşü ve BGYS aracılığıyla alınacak önlem ve denetimlerin sağlanması gerekliliği konusu bu tez çalışmasında gösterilmiştir.

Kurumsal bilgi sistemlerinin güvenliğinin istenilen düzeyde sağlandığından emin olmak için teknik önlemlerin yanında teknik olmayan önlemlerinde bir bütün olarak ele alınmasını ve bilgi sistemlerinin güvenliğini tehdit eden risklerin ortaya çıkartılmasını sağlayan sızma testleriye test edilmesi gerekmektedir. Sızma testleriyle

sınanan bilgi sistemleri teknik (bilgisayar ağları, doküman yönetim sistemleri, süreç analizleri, vb.), insan ve teknik olmayan (çalışanların bilinci, kurum kültürü, yönetimsel prosedürler, fiziksel güvenlik, vb.) etkenler dikkate alınarak bir bütün olarak değerlendirilmelidir. Sızma testleri değişen risklere paralel olarak periyodik zaman aralıklarında tekrarlanmalıdır. Tekrarlama zaman dilimi kurumların bilgi dinamikleri dikkate alınarak belirlenmelidir. Genel kanaat yılda iki kere yapılması yönündedir.

Sızma testleri kurumsal bilgi sistemlerinin saldırganların gözüyle sınanmasını sağlayan, saldırganların kullandığı yöntem ve tekniklerin kullanıldığı kontrollü saldırıların yapıldığı bilgi güvenliği tatbikatlarıdır. Bu kapsamda bir değerlendirme yapıldığında sızma testleri bilgi güvenliği ihlallerinin önceden tespit edilmesini ve bilgi güvenliğinin sağlanmasında aksayan yönlerin ortaya çıkartılmasının bulunmasını sağlayan erken uyarı sistemleri gibi davrandığından kurumsal bilgi güvenliğinin sağlanmasında çok önemli bir yeri olduğu bu tez çalışması sonucunda elde edilen önemli bulgulardan birisidir.

Bu tez çalışmasının esasını teşkil eden sızma testlerinin kurumsal açıdan faydaları değerlendirilmiş olup çok çeşitli amaçlar için aşağıda maddeler halinde verilen alanlarda kullanılması bu tez kapsamında kurumsal bilgi güvenliğinin sağlanması açısından önerilmektedir

- Bilgi sistemlerindeki yeni ve varolan zafiyetlerin bulunması,
- Bilgi sistemlerindeki güvenlik tasarım zayıflıklarının belirlenmesi,
- Kurumsal bilgi güvenliğini tehdit eden risklerin varlığının ve derecesinin tespit edilmesi,
- KBG politikalarının oluşturulması,
- Kurumsal itibar ve imaj ve saygınlığın korunması,
- KBG yönetim sistemleri sertifikasyonlarına uyum,
- Etkili ve bilinçli güvenlik yatırımı,
- Güvenlik yatırımlarının geri dönüşümü,
- Teknik personelin verimliliğinin ölçümü

- İnsan faktörünün istenmeyen yönde devreye girmesine sebep olan bilgi güvenliği farkındalığının ölçümü ile
- Kurumsal bilgi sistemlerine yapılacak olan muhtemel saldırı veya saldırılara karşı güvenlimiyiz sorusunun cevaplanması

gibi çok geniş aralıkta kullanımı ele alınabilir.

Kurumsal bilgi güvenliğine etki eden unsurlar içerisinde en zayıf halka olarak adlandırılan insan faktörünün en tehlikeli güvenlik açığı olarak kabul edilen güvenlik bilinci zayıflığının belirlenmesinde sosyal mühendislik yöntemiyle yapılan sızma testleri önemli bir role sahiptir. Her geçen gün teknolojik önlemlerin ilerlemesi yazılım veya donanımdan kaynaklanan güvenlik açıklarının minimize edilmesi nedeniyle saldırganlar, insan zafiyetlerinden faydalanarak saldırılarını gerçekleştirmektedirler. Bu tür saldırıların kurumsal bilgi güvenliğini en az oranda tehdit etmesi amacıyla sosyal mühendislik teknikleri ve önemi kurumda her kademede çalışan kullanıcılar tarafından bilinmelidir. Bu tez çalışmasında elde edilen önemli bulgulardan birisi ülkemizde sosyal mühendislik kavramının henüz tam olarak anlaşılamadığı veya önemsenmediği, kurumların ve çalışanların bu konuda yeterli bilgiye sahip olmadıkları tespit edilmiştir. Bu tez çalışmasının sosyal mühendislik konusunda da kurumlar ve çalışanlar nezdinde farkındalık yaratması beklenmektedir.

Önceki paragraflarda açıklanan tespitlere ilaveten, bu tez çalışması kapsamında sızma testlerinin yapılma yöntemleriyle ilgili geniş bir literatür çalışması yapılmış, yapılan çalışmalar sonucunda, sızma testlerinin nasıl yapılacağına dair yeni bir bakış açısı bu tezde sunulmuştur. Bu yönteme göre, sızma testleri planlama, bilgi toplama, zafiyetlerin bulunması, zafiyetlerin kullanılması, raporlama olmak üzere beş aşamada gerçekleştirilmektedir. Bu yöntemle gerçekleştirilen sızma testleri sonucunda kurumsal bilgi güvenliğini en çok tehdit eden uygulamaların web uygulamaları olduğu tespit edilmiş ve bu konu detaylı olarak bir bölümde incelenmiştir.

Dünyada olduğu gibi ülkemizde de en fazla güvenlik açıklarına web uygulamalarında rastlanmaktadır. Bu tez kapsamında yapılan araştırmalar ve

çalışmalar sonucunda web uygulamaları konusunda ülkemizde, web uygulamalarını geliştiren yerli yazılım firmalarının web uygulamaları güvenliği adı altında bir eğitimden geçirilmesi gerektiği fikrine varılmıştır. Bu tez çalışmasının beşinci bölümünde web uygulama güvenliğini tehdit eden unsurlar kapsamlı olarak anlatıldığından, bu bölümdeki bilgilerin uygulama geliştiricilerin güvenli yazılım geliştirmelerine yardımcı olacak bir konudur.

Kurumsal bilgi güvenliğinin sağlanmasında, bilgi güvenliği sürecini etkileyen temeldeki üç unsurun insan faktörü, eğitim ve teknoloji olduğu bu tez kapsamında elde edilen önemli bulgulardan bir diğeridir. Kurumsal bilgi güvenliğinin sağlanmasıyla ilgili olarak bu tez çalışmasında güvenliğin bir ürün veya hizmet olmadığı, insan faktörü, teknoloji ve eğitim üçgeninde süreklilik arz eden yönetilmesi zorunlu bir süreç olduğu esas alınmış, bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviyede bir güvenlikten bahsedebilmenin mümkün olamayacağı saptanmıştır. Yüksek seviyede kurumsal bilgi güvenliğin sağlanması için yapılması gerekenler, alınması gerekli önlemler ve tedbirler bu çerçeve dâhilinde açıklanmıştır.

Tez kapsamında yapılan araştırmalarda çoğu kurumda güvenlik eğitimleri ve bilinçlendirme programının olmadığı ve olan kurumlarda ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi ve bilinçlendirmeyi başaramadığı tespit edilen bir diğer önemli bulgudur. Eğitimsizlik ve bilinçsizlik sonucunda insan faktöründen kaynaklanan güvenlik riskleri tamamen yok edilemese de iyi planlanmış güvenlik eğitimleri ve farkındalık çalışmaları ile insan faktöründen kaynaklanan risklerin kabul edilebilir bir seviyeye çekilmesi mümkündür. Bilgi güvenliği eğitimleri ve farkındalık çalışmalarıyla, kurum çalışanlarının kurumsal bilgilerin ve bilgi kaynaklarının bilgi güvenliği ana unsurları olan gizlilik, bütünlük, erişilebilirlik ve kimlik yönetimi konularında yapması gereken görev ve sorumlulukların neler olduğu konusunda bilinçlendirilmeli ve eğitilmelidir. Kurumlar eğitim ve farkındalık çalışmalarıyla çalışanlarına hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etkiyi anlatarak bilgi güvenliğinin en zayıf halkası olan insan faktörünün güçlenmesini sağlamalıdır.

Kurumsal bilgi güvenliğinin üst seviyede sağlanması amacıyla, güvenlik mimarisi ve ölçeklendirme açısından doğru teknolojilerin seçilmesi, seçilen teknolojilerin hatasız yapılandırılması, bakımlarının periyodik olarak yapılması, verimli ve etkin kullanımı ile karma yapıda ve katmanlı inşa edilmeleri teknoloji seçiminde ve yatırımında dikkat edilmesi gereken önemli hususlardır. Karma yapılarla kurulan katmanlı güvenlik mimarileri bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir katkı sağlamaktadır ancak burada dikkat edilmesi gereken en önemli husus karma yapıdaki katmanlı mimarilerin kurulum, bakım ve işletilmesinde üst düzeyde teknik bilgiye gereksinim duyulmasıdır. Eğer bu teknik işçilik kurumun kendi bünyesinde mevcut değilse dış kaynak kullanımına gidilmelidir. Aksi takdirde teknoloji seçiminin doğru yapılmasına rağmen insan faktörüve eğitimlere gerekli hassasiyetin gösterilmemesi, teknolojik yatırımları boşa çıkartacağı gibi daha çok güvenlik ihlallerinin meydana gelmesine neden olacak ve yatırımların boşa gitmesi ve kaynakların israf edilmesi sonucunu doğuracaktır.

7.2. Kişisel Kazanımlar

Tez çalışması sırasında birçok zorlukla karşılaşılmış ve bu zorlukların aşılmasıyla birçok değerli kazanım elde edilmiştir. İlk olarak tez çalışması boyunca karşılaşılan bazı zorluklar, sonrasında ise tez çalışması sonucunda elde edilen kazanımlar aşağıda maddeler halinde açıklanmıştır. Bunlar:

- İncelenen tez konusunun güncel olması ve daha önce bu konuda yapılan bir çalışmaya rastlanmaması nedeniyle, çoğunlukla internet üzerindeki kaynaklardan yararlanılması ve bu kaynaklarda sunulan bilgilerin doğruluğundan emin olunması için uzun araştırmalar ve denemeler yapılmıştır. İnternet kaynaklarından faydalanılırken ilgili kaynağın bilgi güvenliğinde dünyada ve ülkemizde söz sahibi olan ticari firmaların, sivil toplum örgütlerinin ve eğitim kurumlarının sitelerinden olmasına özen gösterilmesi nedeniyle uzun soluklu araştırmaların yapılması,
- Tez konusunun tüm boyutlarıyla ele alınması sebebiyle, neredeyse her bir bölümün hatta bazı alt bölümlerin tez konusu olabilecek çapta önemli konular olması

nedeniyle kapsamlı bir çalışma hazırlanması ve içeriğin zengin tutulması zorunluluğu,

- Tez konusunda yaralanılan kaynakların neredeyse tamamının İngilizce olması, Türkçe diline çevrilmesi sırasında anlam kayıplarının yaşanmaması ve bilgilerin doğru aktarılabilmesi için özverili çalışmalara ihtiyaç duyulması,
- Tez konusunun esasını teşkil eden sızma testlerinin uygulanması sırasında kurumlara özgü sızma testleri senaryolarının hazırlanması ve uygulanması zorunluluğu,
- Sızma testlerinin yapılması sırasında gerek hukuki boyutların, gerekse kurumsal bilgi sistemlerinin sahip olduğu açıkların mahremiyetleri ihlal edilmemesi için azami gayret gösterilme zorunluluğu,
- Kurumlara sızma testleri yapılmadan önce karşılıklı olarak imzalanmış anlaşmalar çerçevesinde "etik saldırı" senaryolarının defalarca karşılıklı olarak görüşülerek karara bağlanması,
- Sızma testleri konusunun çok hassas bir konu olması nedeniyle tez çalışmasında verilen bilgilerin içeriklerine çok dikkat edilme zorunluluğu ve çalışmanın saldırganlar tarafından kullanılmayacak formda verilmesi,
- Kurumsal bilgi güvenliği ve sızma testleri gibi iki yeni konunun bir tez çalışması altında toplanması,
- Tez içerisinde bu çalışmaya özgü olan ve ilk defa bu çalışma içerisinde yayınlanacak olan birçok grafik, temsili görünümler, vb. gibi görselleştirmelere azami olarak yer verilmesi ve bu çalışmalar sırasında görsel gösterimler son halini alıncaya kadar her biri üzerinde defalarca çalışılması

olarak sıralanabilir.

Tez çalışması sırasında ilk günden son güne kadar birçok kazanım elde edilmiştir. Bu kazanımlardan önemlileri aşağıda maddeler halinde açıklanmıştır. Bunlar:

- Tez çalışma konusu ilk belirlendiğinde "bilgi güvenliği" bilgisayar ağlarının sınır koruması olarak algılanmış ve tez kapsamında yapılan araştırmalar ve çalışmalar sonucunda sınır ağ güvenliği konusunun sadece kurumların ağ üzerinden gelecek

tehditlere karşı korunmasını sağlayan ve Bölüm 2'de anlatılan teknolojik denetim araçlarından ibaret olduğu anlaşılmıştır.

- Tez çalışması öncesinde web uygulama güvenliği denildiğinde web sitelerinin saldırganlar tarafından değiştirilmesi akla gelmekteyken çalışma sonucunda web uygulama güvenliğinin kurumları en az zarara uğratacak yönünün web sayfalarının değiştirilmesi olduğu anlaşılmış, aslında web uygulama güvenliğinin ayrı bir tez konusu olabilecek kadar geniş ve kapsamlı olduğu, kurumsal bilgi güvenliğini en üst seviyede tehdit eden riskler içerdiği anlaşılmıştır.
- Tez çalışması öncesinde Sosyal Mühendislik konusunun bilgi güvenliğini ne kadar etkilediği konusunda oluşan şüpheler 162 nolu kaynak başta olmak üzere birçok kitap, makale, web sayfası, vb. gibi güncel kaynakların incelenmesi ve sızma testleri sırasında yapılan pratik çalışmalar sonucunda, Sosyal Mühendislik konusunun insan faktörünü en ustaca kullanan, teknoloji denetimlerle engellenemeyen sinsi ve üst seviyeli ciddi bir tehdit olduğu anlaşılmıştır.
- Tez öncesinde kötücül kodların oluşturduğu tehditler ve verdiği zararlar konusunda var olan bilgi eksikliği tez çalışması sonucunda giderilerek, sazan avlama, anticasus, solucan ve virüs gibi kötücül kodların çoğunlukla bir arada kullanıldığı anlaşılmış hatta bazı durumlarda Sosyal Mühendislik testleriyle desteklendiği bu gibi durumlarda engellenmesinin hiç de kolay olmadığı anlaşılmıştır.
- Tez çalışması öncesinde bilgi güvenliği standartlarıyla ilgili bilgi ve kavram karmaşası çalışma sonucunda giderilerek bilgi güvenliği yönetim standartlarının kurumsal bilgi güvenliğinin üst seviyede sağlanabilmesi için gerekli olduğu anlaşılmıştır.
- Tez çalışması sırasında sızma testlerinin daha etkin ve gerçekçi yapılabilmesi için kaynakların yetersiz olduğu ve mevcut kaynaklardan faydalanılarak istenilen veya beklenilen bilgi edinilemeyeceği anlaşılmış ve bu amaçla saldırganlarla iletişim kurulması gerekmiştir. Bu çalışmalar sonucunda saldırganların çalışma şekilleri, yaşam tarzları, sosyal statüleri ve bilgi seviyeleri gibi konularda bilgi edinilmiştir.
- Tez çalışması sırasında bilgi güvenliğiyle ilgili akademik ve ticari alanda ülkemizde söz sahibi olan uzmanlarla görüşmeler yapılmış ve bunun sonucunda sızma testleri konusu gibi çok değerli olan bir konu üzerinde ciddi bilgi paylaşımları

yaşanmış ve tez çalışmasının bu çevrelerce takdir edildiği ve desteklendiği görülmüştür.

- Tez çalışması tez yazarının iş yerindeki kariyerini önemli ölçüde etkilemiş ve iş yerinde bilgi güvenliğinin sağlanmasına yönelik önemli katkıları olmuştur. Bu olaya verilebilecek en önemli örneklerden birisi, çalışılan kurum tarafından daha önceden ücretli olarak yaptırılan sızma testlerinin sonucunda herhangi bir güvenlik açığı tespit edilmemiş olmasına rağmen yazar tarafından önceden ticari firma tarafından yapılan sızma testlerinin yetersiz olduğu tespit edilmiş ve bu konuda yürütülen çalışmalar sonucunda açıklar tespit edilmiş giderilmesi yönünde ortaklaşa çalışmalar yapılmıştır.
- Tez çalışması sırasında yapılan çalışmalar, araştırılan kaynaklar ve incelenen materyallerden elde edilen bilgiler doğrultusunda internet üzerinden nasıl arama yapılması gerektiği, literatür tarama teknikleri, akademik disiplin içerisinde kaynaklardan yararlanma alışkanlığının edinilmesi, istenilen bilgilere ulaşabilmek için hangi yöntemlerle arama motorlarının kullanılması gerektiği gibi bilgiye erişim yöntemleri ve akademik etik açısından önemli kazanımlar elde edilmiştir.
- Yüksek seviyede bir bilgi güvenliğinin sağlanabilmesi için kurum ve kuruluşların bilgi güvenliğine geniş bir açıdan bakması gerektiği, güvenliğin bir takım çalışması olduğu ve bu takımda en zayıf halka kadar güvenliğin sağlanabileceği dolayısıyla güvenliğin süreklilik arz ettiği daha iyi kavranmıştır.

7.3. Öneriler

Bu tez çalışması sonucunda elde edilen bilgi ve deneyimlere göre ülkemiz bilgi güvenliğinin yüksek seviyede sağlanmasına yardımcı olacak bazı öneriler aşağıda maddeler halinde sıralanmıştır.

- Ülkemizde kurumsal bilgi güvenliği konusunda daha fazla çalışma yapılmalıdır. Özellikle üniversiteler ve araştırma kurumlarında Gazi Üniversitesi FBE Bilgisayar Müh. ABD'da açıldığı gibi "Kurumsal Bilgi Güvenliği" dersleri açılmalıdır.
- Bu konuda yapılacak tez çalışmalarında her bir konu daha detaylı ele alınmalıdır. Mesela Türk toplumunda sosyal mühendislik detaylı olarak incelenmeli ve toplumsal zafiyetler tespit edilip giderilmeye çalışılmalıdır.

- Bu tez çalışmadında bir kez daha ortaya konulduğu gibi "yüksek seviyede bir KBG sağlanması için teknoloji, eğitim ve insan faktörlerine gerektiği kadar önem verilmelidir.
- Sızma testleri yılda en az iki kez yapılmalıdır. Kurumların ekipman ve yazılım güncellemelerine bağlı göre bu daha da arttırılmalıdır.
- Güvenlik bilinci sadece üniversitelerde değil eğitimin her aşamasında dikkate alınmalı ve kullanıcılar bilgilendirilmelidir.
- Ülkemizde sızma testlerine yönelik milli yazılımlar ve yöntemler geliştirilerek kullanılmalıdır.
- Casus savar, virüs savar, güvenlik duvarı, saldırı tespit sistemleri, zafiyet tarayıcı gibi yazılımlar ülkemizde de geliştirilmelidir.
- Ülkemizde sızma testlerini ücretsiz yapan devlet destekli merkezler oluşturulmalıdır.
- İnternet kullanımının hızla yaygınlaştığı ülkemizde bilgi güvenliği konusunda devlet desteğinde üniversitelerimizde, halk eğitim merkezlerinde ve diğer eğitim kuruluşlarımızda halkımız ücretsiz olarak bilgi güvenliği konusunda bilinçlendirilmeli ve eğitilmelidir.
- Bilişim güvenliğiyle ilgili yasaların oluşturulması için toplumun her kesminden geniş bir katılımın sağlandığı çalışma grupları oluşturulmalı ve yasalar bu ortak akıl ile çıkarılmalıdır.

Sonuç olarak bu çalışmanın ülkemizdeki tüm kamu ve özel kurumlar için bilgi güvenliği, kurumsal bilgi güvenliği, bilgi güvenliği yönetim sistemleri, sızma testleri web uygulama güvenliği gibi önemli kavramların kapsamlı olarak anlatıldığı ilk kaynak olması nedeniyle, bu alanda yapılacak diğer çalışmalar ve kurumsal bilgi güvenliğinin sağlanmasını önemseyen kuruluşlar için rehber bir kaynak olarak kullanılabileceği ümit edilmektedir.

KAYNAKLAR

1. Schmidt, A. H., "Building a mosaic of security for a better world", Security Matters, ***Aspatore Books***, U.S.A., 24-26 (2004).

2. İnternet: Computer Incident Advisory Capability "PDF XSS Vulnerability" http://www.ciac.org/ciac/bulletins/r-096.shtml (07.03.2007).

3. Dodge, C. R., Carver, C., Ferguson, J. A., "Phishing for user security awareness" ***Computers & Security***, 26(1): 73, (2007).

4. İnternet: Netcraft "Phishing By The Numbers: 609,000 Blocked Sites in 2006" http://news.netcraft.com/archives/2007/01/15/phishing_by_the_numbers_609000_blocked_sites_in_2006.html (07.03.2007).

5. İnternet: Message Labs "2006: The Year Spam Raised Its Game and Threats Got Personal" http://www.messagelabs.com/portal/server.pt/gateway/PTARGS_0_5885_404_443_670_43/http%3B/0120-0176-CT01/publishedcontent/publish/about_us_dotcom_en / news events/press_releases/DA_174397.html (07.03.2007).

6. Stytz, M. R., Banks, S.B., "Dynamic software security testing", ***Security & Privacy Magazine IEEE*** , 4(3): 77, (2006).

7. McGraw, G., "Software security", ***Security & Privacy Magazine IEEE***, 2(2): 80 - 81, (2004).

8. Gilliam, D.P., Wolfe, T. L., Sherif, J. S.; Bishop, M., "Software security checklist for the software life cycle", ***Proceedings of the Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises***, Linz, 243-248 (2003).

9. İnternet: CERT "CERT/CC Statistics 1988-2006" http://www.cert.org/stats/ (04.03.2007).

10. Kudat, B., "Kötü adamların hızına yetişen daha güvenli", ***BThaber***, 604:15, (2007).

11. İnternet: Wikipedia, "ISO/IEC 27001", http://en.wikipedia.org/wiki/ISO_27001 (08.03.2007)

12. Barrett, N., "Penetration testing and social engineering: Hacking the weakest link", ***Information Security Technical Report***, 8(4):56-58 (2003).

13. Arce, I., "The weakest link revisited" ***IEEE Security & Privacy Magazine***, 1(2):72-74, (2003).

14. Munro, K., "Social engineering", ***Infosecurity Today***, 2(3):44, (2005).

15. Barber, R., "Social engineering: A People Problem?", ***Network Security***, 2001(7):9-1, (2001).

16. Mitnick, K. D., Simon, L. W., Wozniak, S., "The Art of Deception: Controlling the Human Element of Security", ***Wiley Publishing***, New York, 17-18 (2003).

17. Türkiye Bankalar Birliği, "İnternet Bankacılığı İstatistikleri", ***TBB-Eylül 2006,*** Ankara, 3-4, (2006).

18. Rocha, L. M., Schnell, S., "The Nature of Information-Lecture Notes", ***Indiana University***, Bloomington, 1, (2007).

19. İnternet: Türk Dil Kurumu "Güncel Türkçe Sözlük - Bilgi http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=bilgi (10.03.2007)

20. Nonaka, I., Takeuchi, H., "The Knowledge-creating Company", ***Oxford University Press***, New York, 58 (1995).

21. Argyris, C., "Knowledge for Action: A Guide to Overcoming Barriers to Organizational Change", ***Jossey-Bass***, San Francisco, 2-3, (1993).

22. İnternet: Wikipedia, "Bilgi", http://tr.wikipedia.org/wiki/Bilgi (10.03.2007).

23. Laudeman, G., "Information Technology and Community-level Socio-economic Development", ***Georgia Institute of Technology***, Atlanta, 2, (2005).

24. Sağıroğlu, Ş., Alkan, M., "Her Yönüyle Elektronik İmza", ***Grafiker Yayıncılık***, Ankara, 10-15 (2005).

25. Tuomi, I., "Data is More Than Knowledge: Implications of the Reversed Knowledge Hierarchy for Knowledge Management and Organizational Memory", ***Journal of Management Information Systems***, 16(3):105-107 (2000).

26. İnternet: Wikipedia, "Data", http://en.wikipedia.org/wiki/Data (11.03.2007).

27. Setzer, V. W., "Data, Information, Knowledge and Competency", 3rd CONTECSI ***International Conference on Information Systems and Technology Management***, Sao Paulo, 2-3 (2006).

28. Bhatt, G. D., "Knowledge Management in Organizations: Examining the Interaction between Technologies, Techniques and People", ***Journal of Knowledge Management***, 5 (1):71, (2001).

29. Barutçugil İ., "Bilgi Yönetimi", ***Active Bankacılık ve Finans Dergisi,*** Mayıs, 3- 5, (2000).

30. İnternet: Türk Dil Kurumu "Güncel Türkçe Sözlük - Bilişim" http://www.tdk.gov.tr/TR/sozbul.ASPX?F6E10F8892433CFFAAF6AA849816B2EF05A79F75456518CA&Kelime=bilişim (12.03.2007).

31. Shinder, L. D., Tittel, E., "Scene of The Cybercrime: Computer Forensics Handbook", ***Syngress Publishing, Inc.***, Rockland, 52 (2002).

32. McDonough, J., Pellegrini, M., Sutherland, P., Tran, D., "Designing Secure Software", ***Tufts University Department of Computer Science***, 1(1):4, (2006)

33. Gelbstein, E., Kamal, A., "Information Insecurity:A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security", ***United Nations ICT Task Force and the United Nations Institute for Training and Research***, New York, 47-59, (2002).

34. Levy, S., "Hackers: Heroes of the Computer Revolution", ***Penguin Group***, New York, 40-46, (1984).

35. Rattray, J. G., "The Cyber Threat", The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors, ***USAF Institute for National Security Studies US Air Force Academy***, Colorado, 85, (2001).

36. İnternet: Computer Emergency Responce Team "Meet CERT-Background" http://www.cert.org/meet_cert/meetcertcc.html#bkgd (12.03.2007).

37. Ingham, K., Forrest, S., "A History and Survey of Firewall Technology", ***UNM Computer Science Department Technical Report TR-CS-2002-37, New Mexico***,4-5,(2002).

38. İnternet: Wikipedia, "Operation Sundevil", http://en.wikipedia.org/wiki/Operation_Sundevil (13.03.2007).

39. Hoath, P., "Telecoms Fraud, the Gory Details", ***Computer Fraud and Security***, 20(1):10–14, (1998).

40. Solms, R., "Information Security Management (3): the Code of Practice for Information Security Management (BS 7799)", ***Information Management & Computer Security*** ,6(5):224, (1998).

41. Shepherd, S.J., "Lessons learned from security weaknesses in the Netscape World WideWeb browser", ***Public Uses of Cryptography-IEEE Colloquium***, 11:7/2-7/4, (1996).

42. İnternet: Wikipedia, "Kevin Mitnick" http://en.wikipedia.org/wiki/Kevin_Mitnick (13.03.2007).

43. Chen, M. T., Elder, M., Thompson, J., "Electronic Attacks", The Handbook of Information Security, ***John Wiley & Sons***, New York, 8, (2005).

44. Garfinkel, S L., "AOHell", ***The Risk Digest***, 17(42):3, (1995).

45. Skoudis, E., Zeltser, E., "Malware: Fighting Malicious Code", ***Prentice Hall***, New Jersey, 18, (2004).

46. Numanoğlu, E., "BS7799 Bilgi Güvenliği Yönetim Sistemi", ***Önce Kalite Dergisi***, 13(93):43, (2005).

47. Ruiu, D., "Learning from Information Security History", ***IEEE Security & Privacy***, 4(1):78, (2006).

48. Maiwald, E., "Network Security: A Beginner's Guide Summary", ***McGraw-Hill Osborne Media***, California, 4-11, (2003).

49. İnternet: "Communication" http://en.wikipedia.org/wiki/Communicati on (07.03.2007).

50. İnternet: Wikipedia "Kriptografi" http://tr.wikipedia.org/wiki/Kriptografi (07.09.2006).

51. Yerlikaya, T., Buluş, E., Buluş, N., "Kripto Algoritmalarının Gelişimi ve Önemi", ***Akademik Bilişim 2006, Pamukkale Üniversitesi***, 2, (2006).

52. Bilişim Sistemleri Güvenliği El Kitabı Çalışma Grubu "Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0" ***Türkiye Bilişim Derneği Yayınları,*** Ankara, 4, (2006).

53. Sağıroğlu, Ş., Tunçkanat, M., "Gizli bilgilerin internet ortamında güvenli olarak aktarımı için yeni bir yaklaşım" ***Popüler Bilim Dergisi***, 9(105), 21-24, (2002).

54. İnternet: Wikipedia "Steganografi" http://tr.wikipedia.org/wiki/Steganografi (07.09.2006).

55. Sağıroğlu, Ş., Tunçkanat, M., Altuner, M., "Kriptolojide Yeni Bir Yaklaşım Resimli Mesaj", ***Telekomünikasyon Ekseni Dergisi***, Telekomünikasyon Kurumu, 2(2):22-24, (2002).

56. Baykal, N., "Bilgi Teknolojisinin, Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile İlgili Boyutu", ***Hava Harp Akademileri Sempozyumu,*** 12, (2005).

57. Sevgi, L., "Elektromanyetik Uyumluluk- Elektromanyetik Kirlilik", ***Elektrik Mühendisleri Odası Dergisi***, 23, (2000).

58. İnternet: Wikipedia "Tempest" http://en.wikipedia.org/wiki/TEMPEST, (22.09.2006)

59. Bell, D., La Padula, L., "Secure Computer System: Unified Exposition and Multics Interpretation", ***The MITRE Corporation Technical Report ESD-TR-75-306,*** Bedford***,*** 5, (1975).

60. Abrams, D. M., Joyce, V. M., "Trusted System Concepts", ***Computers & Security***, 14(1):45-56, (1995).

61. Department of Defense, "Trusted Computer System Evaluation Criteria", ***DoD 5200.28-STD,*** Washington, 3-8, (1985).

62. Pfleeger, P. C., "Security in Computing, Fourth Edition", ***Prentice Hall***, Westford, 297-300, (2006).

63. Groth, D., Toby, S., "Network+ Study Guide, Fourth Edition", ***Neil Edde & Sybex, Inc.***, Alameda, 4, (2005).

64. Lehtinen, R., "Computer Security Basics, 2nd Edition" , ***O'Reilly***, Sebastopol, 302, (2006).

65. Strebe, M., Perkins, C., "Firewalls 24Seven, Second Edition" ***Neil Edde & Sybex Inc.***, Alameda, 7, (2002).

66. Abraham, A., Grosan, C., "Evolving Intrusion Detection Systems", Genetic Systems Programming Theory and Experiences, ***Springer***, Netherlands, 59, (2006).

67. Gürkaş, G. Z., Durukan, Ş., Zaim, A. H., Demir, A., Aydın, M. A., "802.11b Kablosuz Ağlarda Güvenliğin Ağ Trafiği Üzerindeki Etkilerinin Analizi", ***II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi***, İstanbul, 10-11, (2005).

68. Wi-Fi Alliance, "Deploying Wi-Fi Protected Access (WPA) and WPA2 in the Enterprise", ***Wi-Fi Alliance March 2005***, Austin, 7-8, (2005).

69. Edney, J., Arbaugh, W. A., "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", ***Addison Wesley***, Boston, 12-13, (2003).

70. Canbek G., Sağıroğlu Ş., "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", ***Politeknik Dergisi***, 9(3):169, (2006).

71. İnternet: Wikipedia "Information Security" http://en.wikipedia.org/wiki/Information_security (15.03.2007).

72. Türk Standardları Enstitüsü, "Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri", ***TSE-TS ISO/IEC 17799, Ankara***, 11, (2002).

73. Solms, B., "Information Security – The Fourth Wave", ***Computers & Security***, 25(3):166, (2006).

74. The Institute of Internal Auditors, "Information Technology Controls" ***IAA GTAG, Florida***, 29,(2006).

75. Lewandowski, J. L., "Information Security Fundamentals for DIAS Participants:Learning to be Safe in an Insecure World", ***Purdue University CERIAS K-12, West Lafayette***,1,(2004).

76. Gifford, E.A., "Electronic Information Security", ***IEEE-Potentials***, 7(4):26, (1998).

77. Beck, M., Plank, J. S., Millar, J., Atchley, S., Soltesz, S., Bassi, A., Liu, H., "Information Security on the Logistical Network: An End-to-End Approach", ***Second IEEE International Security in Storage Workshop (SISW'03)***, Washington, 31, (2003).

78. Pfleeger, C. P., "The Fundamentals of Information Security", ***Software, IEEE***, 14(1):15, (1997).

79. Shegai, I., "Some Aspects of Information Security Problems", ***The IEEE-Siberian Conference on Control and Communications (SIBCON-2003)***, Tomsk, 111, (2003).

80. Sharp, E. D., "Information Security in the Enterprise", Information Security Management Handbook Fifth Edition, Tipton, F. H., Krause, M., ***Auerbach Publications***, New York, 1199-1200, (2004).

81. Blanding, F. S., "An Introduction to LAN/WAN Security", Information Security Management Handbook Fifth Edition, Tipton, F. H., Krause, M., ***Auerbach Publications***, New York, 394, (2004).

82. Cohen, F., "Computer Viruses: Theory and Experiments", ***Computers & Security*** 6(1):22-23, (1987).

83. Szor, P., "The Art of Computer Virus Research and Defense", ***Addison Wesley Professional,*** Hagerstown, 12, (2005).

84. Canbek, G., Sağıroğlu, Ş., "Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri", ***Grafiker Yayıncılık***, Ankara, 182-183 (2006).

85. Solomon, M., Broom, N., Barrett, D., "Computer Forensics JumpStart", ***Sybex Inc.***, Alameda, 7, (2004).

86. İnternet: Wikipedia "Phishing" http://en.wikipedia.org/wiki/Phishing (17.03.2007).

87. Canbek G.,Sağıroğlu Ş., "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", ***Gazi Üniv. Müh. Mim. Fak. Der.***, 22(1):130, (2007).

88. Lininger, R., Vines, D. R., "Phishing: Cutting the Identity Theft Line", ***Wiley Publishing Inc.***, Indianapolis, 1, (2005).

89. İnternet: Bonisteel, S., "Two Arrested In Alleged $50 Million Web Fraud" http://findarticles.com/p/articles/mi_m0NEW/is_2001_Sept_7/ai_77984266 (17.03.2007).

90. Salus, H. P., "Casting the Net: From ARPANET to INTERNET and Beyond", ***Addison-Wesley Professional***, New York, 64, (1995).

91. İnternet: The Opte Project "Current Maps", http://www.opte.org/maps/ (17.03.2006).

92. İnternet: CERT "Incidents Reported" http://www.cert.org (17.03.2007).

93. Dunlevy, J. C., "Information Security Strategies: A New Perspective", ***CERT, Pittsburgh,*** 15, (2006).

94. Internet: World Stats "Top 20 Countries With The Highest Number Of Internet Users" http://www.internetworldstats.com/top20.htm (17.03.2007).

95. Symantec Corp., "Symantec Internet Security Threat Report Trends for July–December 06" ***Symantec Volume XI,*** Cupertino***,*** 24-64 (2007).

96. Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., "CSI/FBI, Computer Crime and Security Survey", ***FBI Computer Security Institute***, 1-26, (2005).

97. Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2005", ***Koç.net, İstanbul***, 5- 12, (2005).

98. Üneri, M., "BT Güvenliği Güncel Durum ve Eğilimler", ***TÜBİTAK-UEKAE Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü,*** Ankara 27- 35, (2006).

99. Eriş, M., "Türkiye Kamu Kurumları BT Güvenlik Analiz Sonuçları ve Çözüm Önerileri", ***TÜBİTAK–UEKAE Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü,*** Ankara***,*** 7- 9, (2006)

100. Eriş., M., "Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü Anket Sonuçları", ***TÜBİTAK–UEKAE Kamu Kurumları Bilgi Teknolojileri Güvenlik Günü,*** Ankara 10-32 (2006).

101. Türkiye Bilişim Derneği, "E-Devlet Uygulamalarında Güvenlik ve Güvenilirlik Yaklaşımları 4. Çalışma Grubu Sonuç Raporu***", TBD Kamu-BİB IV, Ankara,*** 9, 11, 17, (2005).

102. İnternet: İstanbul Emniyet Müdürlüğü "Bilişim Suçunun Tanımı" http://www.iem.gov.tr/iem/?s=51, (06.03.2007).

103. Ahi, G., "Bilişim ve Ceza Hukuku", ***Bilişim ve Hukuk Sempozyumu, Mersin,*** 3 (2006).

104. İnternet: Türkiye Büyük Millet Meclisi "Türk Ceza Kanunu Kanun No. 5237" http://www.tbmm.gov.tr/kanunlar/k5237.html (06.03.2007).

105. İnternet: Kanunlar Genel Müdürlüğü "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" http://www.kgm.adalet.gov.tr/bilisimkanunu.htm (18.03.2007).

106. Türk Standardları Enstitüsü, "Bilgi güvenliği yönetim sistemleri–Özellikler ve kullanım kılavuzu", ***TSE-TS 1779- 2,*** Ankara, 3, (2005).

107. Thow-Chang, L., Siew-Mun, K., and Foo, A., "Information Security Management Systems and Standards" ***Synthesis Journal***, 2(2):5,8 (2001).

108. Kalman, S., "Web Security Field Guide", ***Cisco Press***, Indianapolis, 36, 37 (2003).

109. İnternet: Türkiye Dil Kurumu "Güncel Türkçe Sözlük - Risk" http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=Risk (19.03.2007).

110. Purser, S., "A Practical Guide to: Managing Information Security", ***Artech House***, Boston, 27-28 (2004).

111. Craig, D. R., Jaskiel, P. S., "Systematic Software Testing", ***Artech House,*** Boston, 26, (2002).

112. Whitman, E. M., Mattord, J. H., "Principles of Information Security", ***Course Technology***, Boston, 109-113 (2002).

113. İnternet: Wikipedia "BS-7799" http://en.wikipedia.org/wiki/BS_7799 (19.03.2007).

114. Osborne, M., "How to Cheat at Managing Information Security", ***Syngress Publishing Inc.***, Rockland, 90, (2006).

115. British Standards Institute, "Information Technology — Security Techniques — Code of Practice for Information Security Management", ***BSI BS 7799-1:2005,*** Bristol **,** 4,5,7,9,19,23,29,37 (2005).

116. Türk Standardları Enstitüsü, "Bilgi Güvenliği Yönetim Sistemleri – Özellikler ve Kullanım Kılavuzu", ***TSE TS 17799-2,*** Ankara, 1-3 (2005).

117. İnternet: BSI "Information Security Management Systems Guidelines for Information Security Risk Management" http://www.bsi-global.com/en/Shop/PublicationDetail/?pid=000000000030125022&recid=2557 (20.03.2007).

118. İnternet: International Organization for Standardization-ISO "Overview of the ISO system" http://www.iso.org/iso/en/aboutiso/introduction/index.htm (20.03.2007).

119. İnternet: International Organization for Standardization-ISO "JTC 1 / SC 27" http://www.iso.org/iso/en/stdsdevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=143 (20.03.2007).

120. Saint-Germain, R., "Information Security Management Best Practice Based on ISO/IEC 17799", ***The Information Management Journal***, 39:61-62 (2005).

121. İnternet: BSI Eurasia "ISO/IEC 17799:2005 Nedir?" http://www.bsi-turkey.com/BilgiGuvenligi/Genel-bakis/BS7799nedir.xalter (20.03.2007).

122. İnternet: Wikipedia "ISO 27000 Series" http://en.wikipedia.org/wiki/ISO_17799 (20.03.2007).

123. Türk Standardları Enstitüsü, "Bilgi Teknolojisi–Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler", ***TSE- TS ISO/IEC 27001,*** Ankara, 3-13, (2006).

124. İnternet: ISO 27001 Security "ISO/IEC-17799&ISO/IEC-27002" http://www.iso27001security.com/html/iso17799.html (20.03.2007).

125. İnternet: ISO 27001 Security "ISO/IEC 27003" http://www.iso27001security.com/html/iso27003.html (20.03.2007).

126. İnternet: ISO 27001 Security "ISO/IEC 27004" http://www.iso27001security.com/html/iso27004.html (20.03.2007).

127. İnternet: ISO 27001 Security "ISO/IEC 27005" http://www.iso27001security.com/html/iso27005.html (20.03.2007).

128. İnternet: ISO 27001 Security "ISO/IEC 27006" http://www.iso27001security.com/html/iso27006.html (20.03.2007).

129. İnternet: ISO 27001 Security "ISO/IEC 27007" http://www.iso27001security.com/html/iso27007.html (20.03.2007).

130. İnternet: ISO 27001 Security "ISO/IEC 27031" http://www.iso27001security.com/html/iso27031.html (20.03.2007).

131. İnternet: BSI Eurasia "BSI Belgelendirme Yöntemi" http://www.bsi-turkey.com/BilgiGuvenligi/ISMStescil/BSItescilyontemi.xalter?print_only=1 (20.03.2007).

132. İnternet: BSI Eurasia "Bilgi Güvenliği Yönetim Sisteminin Belgelendirilmesi" http://www.bsi-turkey.com/BilgiGuvenligi/ISMStescil/index.xalter (20.03.2007).

133. İnternet: International Register of ISMS Certificates "Certification Bodies" http://www.iso27001certificates.com/certification_directory.htm (20.03.2007).

134. İnternet: International Register of ISMS Certificates "Certificate Search Page" http://www.iso27001certificates.com/Taxonomy/CertificatesResults.asp (20.03.2007).

135. Devlet Planlama Teşkilatı Müsteşarlığı, "E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları", ***DPT, KYR-22,*** Ankara***,*** 27 (2005).

136. The Australian High Tech Crime Centre, "Australian Computer Crime & Security Survey", ***AusCERT,*** Canberra, 12, (2006).

137. National ICT Security & Emergency Response Centre, "Malaysia ISMS Survey", ***NISER-ISMS Survey,*** Kuala Lumpur, 4, 35-40 (2003).

138. Federal Office for Information Security "A Penetration Testing Model" ***BSI,*** Bonn, 6-9, 93 (2002).

139. Cole, E., Krutz, R., Conley, J. W., "Security Assessments, Testing, and Evaluation", Network Security Bible, ***Wiley Publishing Inc.***, Indianapolis, 607-612 (2005).

140. Geer, D., Harthorne, J., "Penetration testing: a duet" ***IEEE 18th Annual Computer Security Applications Conference***, Las Vegas, 185 (2002).

141. Budiarto, R., Ramadass, S., Samsudin, A., Noor, S., "Development of Penetration Testing Model for Increasing Network Security", ***IEEE International Conference on Information & Communication Technologies: From Theory to Applications,*** Damascus***,*** 563 (2004).

142. Nilsson, J., "Vulnerability Scanners" Yüksek Lisans Tezi, ***Department of Computer and Systems Sciences Royal Institute of Technology***, Stockholm, 28-30 (2006).

143. Braden J., "Penetration Testing – Is it right for you?" ***SANS Institute***, Maryland, 1, (2002).

144. İnternet: Corsaire Limited "What is a Penetration Test?" http://www.penetration-testing.com (21.03.2007).

145. İnternet: Wikipedia "Penetration Test" http://en.wikipedia.org/wiki/Penetration_testing (21.03.2007).

146. Lammle, T., "CEH Certified Ethical Hacker Review Guide", ***Sybex Inc.***, Alameda, 8 (2005).

147. Harris, S., Harper, A., Eagle, C., Ness, J., Lester, M., "Gray Hat Hacking: The Ethical Hacker's Handbook", ***McGraw-Hill Osborne Media***, New York, 73 (2004).

148. Manzuik, S., Gold, A., Gatford, C., "Network Security Assessment From Vulnerability to Patch" ***Syngress Publishing Inc.***, Rockland, 104 (2007).

149. Dautlich, M., "Penetration Testing — the Legal Implications" ***Computer Law & Security Report***, 20(1):41, (2004).

150. Cohen, F., "Managing Network Security — Part 9: Penetration Testing?", ***Network Security,*** 1997(8):13, (1997).

151. Schultz, E., "Hackers and Penetration Testing", ***Network Security***,1997(10):10, (1997).

152. Midian, P., "Perspectives on Penetration Testing", ***Computer Fraud & Security***, 2002(6):15, (2002).

153. Weissman, C., "Security Penetration Testing Guideline", Handbook for the Computer Security Certification of Trusted Systems, ***Center for Secure Information Technology Naval Research Laboratory***,Washington, 2 (1995).

154. Dahl, M. O., "Using Coloured Petri Nets in Penetration Testing", Yüksek Lisans Tezi, ***Department of Computer Science and Media Technology Gjøvik University***, Gjøvik, 18, (2005).

155. Abrams, D. M., "FAA System Security Testing and Evaluation-Technical Report", ***MTR 02W0000059,*** Virginia, 3-7, (2003).

156. Schneier, B., "The Process of Security", http://infosecuritymag.techtarget.com/articles/april00/columns_cryptorhythms.shtm (21.03.2007).

157. İnternet: Wilson, M., "Demonstrating ROI for Penetration Testing (Part One)" http://www.securityfocus.com/infocus/1715 (22.03.2007).

158. İnternet: Memorial Sağlık Grubu "Sağlık Rehberi" http://www.memorial.com.tr/saglikrehberi.php?Id=271 (22.03.2007).

159. Landwehr, C. E., Bull, A. R., Mcdermott, J. P., Choi, W. S., "A Taxonomy of Computer Program Security Flaws" ***ACM Computing Surveys***, 26(3), 214-215, (1994).

160. Splaine, S., "Testing Web Security-Assessing the Security of Web Sites and Applications", ***Wiley Publishing Inc.***, Indianapolis, 3-4 (2002).

161. Heald, A., E., "Understanding Security Testing" ***Infosec Writers***, 8, (2005).

162. Mitnick, K. D., Simon, W. L., "Aldatma Sanatı", Nejat Eralp Tezcan, ***ODTÜ Yayıncılık,*** Ankara, 303, (2006).

163. Hürriyet Ekonomi, Haziran, 29, "Microsoft'la Oracle'ın Dedektifli Savaşı,", ***Hürriyet Gazetesi***, (29.06.2000).

164. Canbek, G., "Klavye Dinleme Ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme" Yüksek Lisans Tezi, ***Gazi Üniversitesi Fen Bilimleri Enstitüsü***, 23, (2005).

165. İnternet: Wikipedia "Brute Force Attack" http://en.wikipedia.org/wiki/Brute_force_attack (22.03.2007).

166. İnternet: Columbia University Computer Science Department "A Distributed Denial of Service Attack" http://nsl.cs.columbia.edu/projects/sos/ (22.03.2007).

167. Northcutt, S., Zeltser, L., Winters, S., Kent, K., Ritchey, W. R., "Inside Network Perimeter Security", ***Sams Publishing***, Indiana, 540-550, (2005).

168. Layton, P. T., "Penetration Studies – A Technical Overview", ***SANS Institute***, Maryland, 3-7, (2002).

169. National Infrastructure Security Co-ordination Centre, "Commercially Available Penetration Testing", ***NISCC-Best Practice Guide,*** London***,*** 24 (2006).

170. Long, J., "Google Hacking for Penetration Testers", ***Syngress Publishing Inc***., Rockland, 135- 137, (2005).

171. Potter, B., McGraw, G., "Software Security Testing" ***IEEE Security & Privacy Magazine***,2(5): 81 (2004).

172. Search Security Definitions, "Vulnerability analysis", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1176511,00.html (22.03.2007).

173. Knight, E., "Computer Vulnerabilities", ***Artech House***, Boston, 7-9 (2000).

174. Stanton, J., "Network Security-OS Fingerprinting" ***Department of Computer Science Lecture Notes,*** Washington, 3 (2007).

175. Trowbridge C., "An Overview of Remote Operating System Fingerprinting", ***SANS Institute,*** Maryland, 3, (2003).

176. Lippmann, R. P., Fried, D., Piwowarski, K., Streilein, W., "Passive Operating System Identification from TCP/IP Packet Headers", ***Workshop on Data Mining for Computer Security (DMSEC)***, Melbourne, 2-3 (2003).

177. Klevinsky, T. J., Laliberte, S., Gupta, A., "Hack I.T.: Security Through Penetration Testing", ***Addison Wesley First Edition,*** Hagerstown, 318, (2002).

178. Mueller, P. J., "Windows Administration at the Command Line for Windows2003, WindowsXP,and Windows2000", ***Wiley Publishing Inc.***, Indianapolis, 135-152 (2006).

179. İnternet: Internet Assigned Numbers Authority "Port Numbers" http://www.iana.org/assignments/port-numbers (22.03.2007).

180. İnternet: Microsoft TechNet "İletim Denetimi Protokolü (TCP)" http://www.microsoft.com/technet/prodtechnol/windowsserver2003/tr/library/ServerHelp/eeebf72d-4b09-4ba0-9cb5-c51bdce62673.mspx?mfr=true (22.03.2006).

181. İnternet: Microsoft TechNet "Kullanıcı Veri Birimi Protokolü (UDP)" http://www.microsoft.com/technet/prodtechnol/windowsserver2003/tr/library/ServerHelp/fbf87684-99c5-4f6e-a630-53fef58b03c1.mspx?mfr=true (22.03.2006).

182. Garfinkel, S., Spafford, G., Schwartz, A., "Practical Unix and Internet Security Third Edition", ***O'Reilly***, Köln, 281-283 (2003).

183. İnternet: Fyodor "Port Scanning Techniques", http://insecure.org/nmap/man/man-port-scanning-techniques.html (22.03.2007).

184. İnternet: Sanfilippo, S., "Dumb Scan" http://www.kyuzz.org/antirez/papers/dumbscan.html (23.03.2007).

185. Scambray, J., Mcclure, S., Kurtz, G., "Hacking Exposed: Network Security Secrets & Solutions Second Edition", ***McGraw-Hill/Osborne,*** New York 95-97 (2001).

186. Foster, J., C., Liu, V., "Writing Exploits and Security Tools", ***Syngress Publishing Inc.***, Rockland,, 16 (2006).

187. İnternet: SearchSecurity Definitions, "Zero-day Exploit", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html (23.03.2007).

188. İnternet: Stefan Frei "The Speed of (In) security" http://www.techzoom.net/paper-speed-of-insecurity-discovery-date.asp (23.03.2007).

189. Özavcı, F., "Metasploit Framework ile Güvenlik Denetimi", ***Linux Şenliği ODTÜ***, 4, 5, (2006).

190. Singh, P., Mookhey, K.K., "Metasploit Framework, Part 1" http://www.securityfocus.com/infocus/1789 (23.03.2007).

191. Tiller, J. S., "A Framework for Business Value Penetration Testing", ***Auerbach Publications***, New York, 288- 291, (2005).

192. İnternet: Fyodor "Top 10 Vulnerability Scanners" http://sectools.org/vuln-scanners.html (26.09.2006).

193. İnternet: ISECOM "The Open Source Security Testing Methodology Manual, http://www.isecom.org/osstmm (23.01.2007).

194. Herzog, P., "OSSTMM 2.2. Open-Source Security Testing Methodology Manual", ***ISECOM OSSTMM 2.2,*** Barcelona, ,44, 47, 49, 68, 71, 83, 99-101 (2006).

195. Wack, J., Tracy, M., Souppaya, M., "Guideline on Network Security Testing" ***NIST Special Publication 800-42,*** Washington, 1 (2003).

196. İnternet: Wikipedia "OWASP" http://en.wikipedia.org/wiki/OWASP (23.03.2007).

197. Jia, X., "Design, Implementation and Evaluation of an Automated Testing Tool for Cross-Site Scripting Vulnerabilities", Yüksek Lisans Tezi, ***Darmstadt University of Technology (TUD) - Computer Science Department***, 2-6 (2006).

198. Foster, C. J., Osipov, V., Bhalla, N., Heinen, N., "Buffer Overflow Attacks: Detect, Exploit, Prevent", ***Syngress Publishing Inc.***, Rockland, 4 (2006).

199. İnternet: OWASP "About The Open Web Application Security Project" http://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project (23.07.2007).

200. İnternet: Web Application Security Consortium "About Us" http://www.webappsec.org/aboutus.shtml (23.07.2006).

201. Hansche, S., "Official (ISC2) Guide to the CISSP Exam", ***Auerbach Publications***, New York, 12, (2003).

202. İnternet: Web Application Security Consortium "Weak Password Recovery Validation" http://www.webappsec.org/projects/threat/classes/weak_password_recovery_validation.shtml (23.03.2007).

203. İnternet: Application Defense Center "What is a Brute Force Attack" http://www.imperva.com/application_defense_center/glossary/brute_force.html (23.03.2007).

204. Barnett, C.R., "Mitigating the WASC Web Security Threat Classification with Apache", ***Addison Wesley Professional***, Indiana, 187 (2006).

205. Ellison, C., Hall, C., Milbert, R., Schneier, B., "Protecting Secret Keys with Personal Entropy", ***Future Generation Computer Systems***, 16(4):312 (2000).

206. Endler, D., "Brute-Force Exploitation of Web Application Session IDs", ***IDEFENSE Labs***,Chantilly, 4-5 (2001).

207. Fu, K., Sit, E., Faemster, N., "DoS and Donts of Client Authentication on the Web" ***USENIX Security Symposium,*** Washington, 258-260,(2001).

208. Kolsek, M., "Session Fixation Vulnerability in Web-based Applications", ***ACROS Security***, Maribor, 2- 4 (2002).

209. İnternet: Web Application Security Consortium "Cross-site Scripting" http://www.webappsec.org/projects/threat/classes/cross-site_scripting.shtml (23.03.2007).

210. İnternet: Amit Klein "DOM Based Cross Site Scripting or XSS of the Third Kind" http://www.webappsec.org/projects/articles/071105.shtml (23.03.2007).

211. İnternet: The World Wide Web Consortium (W3C) "Document Object Model FAQ" http://www.w3.org/DOM/faq.html#what (23.03.2007).

212. Donaldson, E. M., "Inside The Buffer Overflow Attack: Mechanism, Method, & Prevention", ***SANS Instutie***, Maryland, 2, (2002).

213. İnternet: Web Application Security Consortium "Format String Attack" http://www.webappsec.org/projects/threat/classes/format_string_attack.shtml (23.07.2007).

214. Carter, G., "LDAP System Administration", ***O'Reilly & Associates Inc***., Sebastopol, 5-7 (2003).

215. Chapela, V., "Advanced SQL Injection" http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt (23.03.2007).

216. Anley, C., "Advanced SQL Injection In SQL Server Applications", ***Next Generation Security Software Publication,*** Surrey, 18- 21 (2002).

217. Hotchkies, C., "Blind SQL Injection Automation Techniques The Database", ***Black Hat Briefings***, Las Vegas, 4 (2004).

218. İnternet: SQL Server 2005 Books Online "@@VERSION (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms177512.aspx (24.03.2007).

219. İnternet: SQL Server 2005 Books Online "@@SERVERNAME (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms187944.aspx (24.03.2007).

220. İnternet: SQL Server 2005 Books Online "FILE_NAME (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms181399.aspx (24.03.2007).

221. İnternet: SQL Server 2005 Books Online "DB_NAME (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms189753.aspx (24.03.2007).

222. İnternet: SQL Server 2005 Books Online "SYS.SYSOBJECTS (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms177596.aspx (24.03.2007).

223. İnternet: SQL Server 2005 Books Online "SYS.SYSCOLUMNS (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms186816.aspx (24.03.2007).

224. İnternet: SQL Server 2005 Books Online "UNION (Transact-SQL)" http://msdn2.microsoft.com/en-us/library/ms180026.aspx (24.03.2007).

225. İnternet: Wikipedia "Server Side Includes" http://en.wikipedia.org/wiki/Server_Side_Includes (24.03.2007).

226. İnternet: Web Application Security Consortium "SSI Injection" http://www.webappsec.org/projects/threat/classes/ssi_injection.shtml (24.03.2007).

227. İnternet: The World Wide Web Consortium (W3C) "XML Path Language (XPath)" http://www.w3.org/TR/xpath (24.03.2007).

228. İnternet: Web Application Security Consortium "XPath Injection" http://www.webappsec.org/projects/threat/classes/xpath_injection.shtml (24.03.2007).

229. İnternet: Web Application Security Consortium "Directory Indexing" http://www.webappsec.org/projects/threat/classes/directory_indexing.shtml (24.03.2007).

230. İnternet: Web Application Security Consortium "Information Leakage" http://www.webappsec.org/projects/threat/classes/information_leakage.shtml (24.03.2007).

231. İnternet: Web Application Security Consortium "Path Traversal" http://www.webappsec.org/projects/threat/classes/path_traversal.shtml (24.03.2007).

232. İnternet: Web Application Security Consortium "Predictable Resource Location" http://www.webappsec.org/projects/threat/classes/predictableresource_location.shtml (24.03.2007).

233. İnternet: Web Application Security Consortium "Abuse of Functionality" http://www.webappsec.org/projects/threat/classes/abuse_of_functionality.shtml (24.03.2007).

234. İnternet: Web Application Security Consortium "Denial of Service" http://www.webappsec.org/projects/threat/classes/denial_of_service.shtml (24.03.2007).

235. İnternet: Web Application Security Consortium “Insufficient Anti-automation” http://www.webappsec.org/projects/threat/classes/insufficient_antiautomation.shtml (24.03.2007).

236. İnternet: Web Application Security Consortium “Insufficient Process Validation” http://www.webappsec.org/projects/threat/classes/insufficient_process_validation.shtml (24.03.2007).

237. Carter, E., “CCSP Self-Study: Cisco Secure Intrusion Detection System (CSIDS)”, ***Cisco Press***, Indianapolis, 88-89 (2004).

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı	: VURAL, Yılmaz
Uyruğu	: Türkiye Cumhuriyeti
Doğum Tarihi ve Yeri	: 02.07.1974 - Kahramanmaraş
Medeni hâli	: Evli
Telefon	: (90536) 950 84 36
E-posta	: yvural@hotmail.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Lisans	TrakyaÜniversitesi	
	Bilgisayar Mühendisliği	1996
Lise	K. Maraş Sütçü İmam Lisesi	1991

İş Deneyimi

Yıl	**Yer**	**Görev**
2000 –	STM A.Ş.	Bilişim Teknolojileri Danışmanı
1997 –2000	K:Maraş Sütçü İmam Ünv.	Öğretim Görevlisi
1996 –1997	Tekstiplik A.Ş.	Yazılım Mühendisi

Yabancı Dil

İngilizce

Yayınlar

Hobiler

Basketbol, Türk Halk Müziği, Yüzme