YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ VE GÜVENLİĞİ

Elektrik Mühendisi Mustafa GÜLMÜŞ

FBE Elektrik Mühendisliği Anabilim Dalı Elektrik Makinaları ve Güç Elekroniği Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof. Dr. İbrahim ŞENOL

İSTANBUL, 2010

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

FW	Firewall- Güvenlik Duvarı
R	Router yönlendirici
G	Gizlilik
B	Bütünlük
K	Kullanabilirlik (Erişebilirlik)
TD	Tehdit Değer
AD	Açıklık Değeri
GS	Gizlilik Seviyesi
BS	Bütünlük Seviyesi
KS	Kullanabilirlik Seviyesi
GRD	Gizlilik Risk Değeri
BRD	Bütünlük Risk Değeri
KRD	Kullanabilirlik Risk Değeri

KISALTMA LİSTESİ

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 Sirketi

BBS Bulletin Board System, Mesaj Pano Sistemleri

BGYS Bilgi Güvenliği Yönetim Sistemi

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 Geçis Arayüzü

CMMI Capability Maturity Model-Integration; Bütünleşik Yetenek Olgunluk Modeli

COBIT The Control Objectives for Information and related Technology- Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri

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 Engelleme

DDoS Distributed Denial of Service, Dağıtık yapı ile Servis engelleme

EAP Extensible Authentication Protocol, Genişletilebilir Kimlik Doğrulama Protokolü

EMEA Europe, the Middle East and Africa, Avrupa, Ortadoğu ve Afrika

FBE Fen Bilimleri Enstitüsü

FBI Federal Bureau of Investigation, Federal Araştırma Bürosu

FIN Finish Packet, Bitis 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

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 işaret 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

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 Information Security Forum, Bilgi Güvenliği Forumu

ISN Initial Sequence Number, Baslangıç 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

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

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

PHP Hypertext Preprocessor, Hipermetin Ön İşlemci Betik Dili

PIN Personal Identification Number, Kişisel Kimlik Numarası

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 Reseaux IP Network Coordination Center, IP dağıtım merkezi

RSH Remote Shell, Uzaktan komut çalıstırma

RST Reset, Sıfırlama

SAN Storage Area Network, Veri Depolama Ağı

SATAN Security Administrator Tool for Analyzing Networks, Ağların Çözümlenmesi için 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

SSI Server Side Includes, Sunucu Taraflı Betik

SYN Synchronize, Senkronize

TCB Trusted Computing Base, Güvenli Hesaplama Esasları

TCK Türk Ceza Kanunu

TCP Transmission Control Protocol, İletim Kontrol Protokolü

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

URL Uniform Resource Locator, Tekdüze Kaynak Konumlayıcı

US-CERT The United States Computer Emergency Readiness Team, ABD Bilgisayar Acil Durum Hazırlık Ekibi

YTÜ Yıldız Teknik Üniversitesi

VPN Vitual Private Network, Sanal Özel Ağı

WASC The Web Application Security Consortium, Web Uygulamaları Güvenlik Konsorsiyumu

WEP Wired Equivalent Privacy, Kabloya Eşdeğer Mahremiyet Güvenlik Protokolü

WG Working Group, Çalısma Grubu

WPA Wireless Fidelity (Wi-Fi) Protected Access, Kablosuz Bağlantı Korumalı Erişim

XSS Cross Site Script, Çapraz Site Kod Çalıştırma

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Bu tezi hazırlamamda beni devamlı olarak yönlendiren ve bilgilendiren sevgili hocam Prof. Dr. İbrahim Şenol ve bilgilerinden çok faydalandığım Vural Yılmaz'a, beni daima destekleyen Eşim Gamze Gülmüş'e ve beni motive eden kızım Bahar Gülmüş'e çok teşekkür ederim.

Bu tezin içindeki tüm bilgiler, akademik kurallar çerçevesinde elde edilerek ve mümkün olduğunca tez yazım kurallarına uygun olarak düzenlenmiştir. Bu çerçevedeki tez çalışmasında orijinal olmayan her türlü kaynağa da eksiksiz olarak atıf yapılmıştır.

ÖZET

Bu çalışmada bilgi güvenliği ve unsurları incelenerek, kurumsal bilgi güvenliği ve standartları değerlendirilmiştir. Bu çerçevede kurumların bilgi güvenliğini zaafa uğratacak tehditler, riskler gözden geçirilerek, ülkemiz bilişim hukuku ve bilişim mevzuatı incelenmiş ve risk altındaki uygulamalar değerlendirilip web ve veri tabanları üzerinde yoğunlaşmıştır. Bu kapsamda kurumların en değerli varlıklarından sayılan bilgi varlıklarının korunması için alınacak önlemler belirlenerek sunulmuştur.

Makul seviyede bilgi güvenliğinin sağlanması için önemli olan işlemler tekrar gözden geçirilmiş ve kurumsal bilgi güvenliği yönetimi üzerindeki etkisi araştırılmış, tesbit edilen risklerin giderilmesi ve yönetilmesine yönelik çözüm önerileri sunulmuştur.

Bu tez çalışmasının ülkemiz kurumsal bilgi güvenliği yönetimi alanında yapılan kapsamlı bir çalışma olması nedeniyle ülkemizde bilgi güvenliğine gereken önemin verilmesine katkı sağlayacağı, kurum ve kuruluşlar için bir uygulama ve farkındalık kaynağı olacağı, ve bilgi güvenliği bilincinin yükseltilmesine katkıda bulunacağı tahmin edilmektedir.

ABSTRACT

In this study , information security and the elements of information security have been examined. Enterprise information security and its standards have been evaluated. In this context, the threats and risks of a company are reviewed for information security weaknesses. Turkish Legislation about information systems has been reviewed and applications that are subject to risks are assessed with a special focus on web and database applications. In this perspective measures for protection of information assets, that are considered to be the most valuable assets of a company, are determinedand presented.

Significant processes for attaining a reasonable level of information security have been reviewed and their impact on corporate information security management has been researched. Solution suggestions are proposed to avoid threats and to manage existing risks properly.

As this study is a comprehensive study in the field of Enterprise Information Security in Turkey it is expected to contribute to the importance attributed to information security, to be a resource for implementation to enterprises and for a greater awareness on the topic and to improve the overall consciousness on information security.

1. GİRİŞ

Bilgi; her zaman insanoğlunun en değerli varlığı olmuştur. Bilgi insanlığın yaşamını, düşüncesini, davranışını, iletişimini, gelişimini, üretmesini, tüketmesini belirleyen faktörlerin başında her zaman yerini korumuştur. Bilgi, en basit benzetme ile para gibi bir varlıktır. Kişiler, kurumlar, kuruluşlar ve ülkeler için bilgi, elde edilmesi ve aynı zamanda elde tutulması da zor olan bir varlıktır. Fikri mülk olarak tanımlanan bu varlık, bir kurumun bilgi ve özbilgi (knowledge) varlığıdır. Bu önemli varlığın korunması, tarih boyunca hayati bir önem arz etmiş ve daha ilkel zamanlarda bile korumak için çeşitli şifrelemeler kullanılmıştır. Bu önem, tarihteki en eski uygarlıklardan günümüze kadar devam etmiştir. Günümüzde ise bilginin iletişim teknolojisinin hızla gelişmesi ve gelişmesine devam edilmesiyle bilginin insanoğlunun hayatında daha da önemli hale gelmiştir. Her yeni günde bilgi, iletişim ve teknoloji ile iç içe geçmekte ve kullanımı artmaktadır. Bu gelişmeler doğrultusunda, elektronik ortamlarda bulunan bilgiler, her geçen gün katlanarak çoğalmakta, dolayısıyla da bilgi güvenliğinin en üst düzeyde sağlanmasına yönelik ihtiyaçlar, kişisel ve kurumsal olarak en üst seviyelere çıkmaktadır.

Günümüzde işler neredeyse tamam bilgi ve iletişim ile yönetilmektedir. İletişim ve bilişim teknolojilerinin hızla gelişmesi ve yaşantımızın birer parçası olması ile; bilginin yönetilmesi, iş verimliliğin artması, iş akışlarının hızlandırılması, insanlar ile insanlar, insanlar ile kurumlar ve kurumlar ile kurumlar arasında daha hızlı iletişim kurulabilmesi sağlanmış, hayatımız kolaylaşmış ve üretim ve tüketimde gelişmiştir. Bilişim teknolojilerin gelişmesi ile bilgilerin işlenmesi, taşınması, saklanması ve gerektiğinde geri çağırılmasında da büyük kolaylıklar sağlanmıştır.

Bilginin gelişen elektronik ortamlarda işlenmesi ve iletişimin gelişmesi ile bilgiye erişim kolaylaşmış ve mekandan erişmesi bağımsız hale gelmiştir. Günlük yaşantımızda yapmakta olduğumuz birçok iş ve işlemler kolaylıkla ve hızlıca yapılabilir hale gelmiştir. Örneğin Devlet kurumlarından bilgi edinmek için bazen devlet dairelerine gitmeden istediğimiz bilgileri elde edebilmekteyiz. Bankacılık işlemlerini bankaya gitmeden evimizde, iş yerimizlerdeki bilgisayarların veya mobil cihazları ile seyahat halinde bile yapmak, borç sorgulamak, fatura ödemek, pasaport ve vize başvurusunda bulunmak, çeşitli rezervasyonları yapmak, uçak bileti satın almak, araç kaza ve sigorta durumlarını sorgulamak, sınav sonuçlarını öğrenmek, öğrenci kayıtlarını yaptırmak, hastane tetkik sonuçlarını almak ve

uzaktan eğitim almak veya vermek, bilgi ve iletişimde varılan noktaya verilebilecek örneklerdir.

bilgi, iletişim ve araçları hayatımızın bir parçasına dahil olduğuna göre bu bilginin ve bilgiyi taşıyan veya depolayan ortamlarının da korunmasını önemli kılmıştır. Elektronik ortamlarda bulunan, kişi ve kurumların sahip olduğu bilgilerin mahremiyetlerinin korunması, bu ortamların yaygınlaşmasının önünün açılması ve bu ortamlarda herhangi bir kaybın veya zararın meydana gelmemesi için bu ortamlarda bulunan bilgilerin güvenliğinin sağlanması gereklidir.

Bilişim ve bilişim ağların yaygınlaşması, internet ortamı ve internet ortamında kullanılan uygulamaların yaygınlaşması ile bilgi güvenliğini sağlamak toplumda sadece bilgi güvenliğiyle uğraşan kişi ve kuruluşların uğraşması ile mümkün olamamaktadır. Bilgi ve bilişim çağı olarak adlandırılan günümüzde, bilgi sistemlerinin küresellesmesi sonucunda bu sistemlerle doğrudan veya dolaylı yönden ilişkisi olan ve bu sistemleri kullanan tüm birey ve kurumların katkıda bulunması gerekmektedir. Bunun önemli sebepleri iş veya günlük özel yaşamın bir parçası haline gelen uygulamaların artması, ihtiyaç duyulan bilgilerin ağ ve internet sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit olusturması, elektronik ortamında organize suçların hergün artması ve en daha önemlisi kisişel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir. Ağların birbirine bağlı bilgisayarlardan oluştuğunu düşünürsek, bir ağın kendisine bağlanan bilgisayarlardan daha güvenli olmadığı kolayca anlaşılabilir (Locahart, 2006). Dolayısıyla işimizi ve yaşantımızı kolaylaştırmasını sağlayan işlemlerin hızlandırılmasına katkılar sağlayan bilgisayar ortamları, insan hayatında günden güne daha da önem kazanmakta ve her geçen gün de beraberinde güvenliği üst düzeyde tesis etmeyi sağlanan güvenilir bilgi sistem platformlarına ihtiyaç vardır.

Herhangi bir bilgisayar ve dolayısıyla ağında meydana gelen güvenlik ihlali bir anda bu ağın bağlı olduğu diğer ağları etkileyebilmektedir. Bu güvenlik ihlali, çeşitli uygulamalara zarar verebileceği gibi bazende bu uygulamaların erişilebilirliğini imkansızlaştırıp bunları servis veremez duruma getirebilmektedir. Bu kurumsal ağları üzerinden işlemlere gerçekleştiren, iletişimi sağlayan uygulama ve bilgilerin değeri düşünüldüğünde bilgi güvenliğinin tesis etmenin önemi daha iyi anlaşılacaktır.

Günümüzde bilgi ve bilgisayar güvenliğine önem vermemenin, bize, çocuklarımıza, işyerimize ve ülkemize maliyeti, zannettiğinizden çok daha fazladır (Canbek ve Sağıroğlu, 2006).

Günümüzde bilgi, iletişim ve teknoloji ile iç içe geçmekte ve kullanımı artmaktadır. Bu gelişmeler doğrultusunda, elektronik platformlarda bulunan bilgiler, her geçen gün katlanarak çoğalmakta, dolayısıyla da bilgi güvenliğinin önemi en üst düzeyde sağlanmasına yönelik ihtiyaçlar da hem kişisel hemde kurumsal olarak en üst seviyelere çıkmaktadır.

Günümüzde tüm işler artık bilgi ve bilgi araçlarıyla yürütülmektedir. Bilginin bir kısmı herkes tarafından bilinen(public)dir ve bu genel olarak da adlandırılabilir. Diğer bir kısmı ise herkesçe bilinmeyen veya bilinmemesi gereken bilgi olup bu da özeldir (privat). İş bu kısım da özel korumayı ve yetkilendirmeyi gerektirir.

Elektronik platformlarda sunulan hizmetlerin (internet bankacılık, e-fatura, e-bilet, e-ticaret, e-devlet vs.) sayısı her geçen gün artmakta ve bu platformları kullananlarının sayılarını da çoğalmaktadır. Elektronik platformlarda hizmet veren kurumların uygulamaları artıkça bu ortamlardan nemalanmak isteyen kötü niyetli kişiler yani saldırganların bu ortamlara erişme isteği veya cazibesi de artmaktadır. Hatta bu ortamlar zamanla saldırganların cazibe merkezi haline bile gelebilmektedir.

Günümüzde kişilerin güvenliğinin yanında kişisel verilerinin de artık kişiler gibi korunması gerektiği bilinmektedir. Kişisel veriler artık ekonomik bir meta haline gelmiştir (Yıldırım, 2010). Özellikle içerisinde önemli bilgiler bulunduran bilgi sistemlerinin güvenliğinin sağlanması ve yönetimi önem kazanmıstır.

Bilgi teknolojileriyle birlikte geliştirilen elektronik uygulamalar bir yandan hayatımızın işleyişini kolaylaştırırken diğer yandan da yeni güvenlik tehditlerini ve yeni suç tiplerini beraberinde getirmektedir. Kişilerin, kurumların ve hatta devletlerin sahip oldukları önemli bilgiler, bilgi hırsızlığı, korsan atakları, bilgi sızdırmalarını ve kurumların kötü niyetli çalışanlarınca oluşturulabilecek bilgi suistimalleri ve atakları gibi çok geniş bir yelpazeye sahip kaynaklardan gelen tehditlerle karşı karşıya gelebilmektedir. Bilgi güvenliğini tehdit eden durumlar sadece elektronik platformlardan yapılan ataklarla sınırlı değildir. Çeşitli doğal afetler, insan hataları, yangın, sel, deprem, terör saldırıları, sabotaj gibi olaylar sonucunda da bilgi ve bilgi sistemleri zarar görebilmektedir.

Günümüzde elektronik platformlar üzerinde yapılan güvenlik ihlal ve suistimalerinden neredeyse her gün yenisi eklenmektedir. Bu durumdan elektronik platformlarda hizmet sunan kuruluşlar ve hizmet alan kullanıcılar da etkilenmektedir. Örneğin e-ticaret yapan bir alış-veriş firmasının kullanıcılar bir ihlal veya sahtekarlıkla dolandırıldığında parasını kaybederken, hizmeti veren sitenin itibari de kullanıcılar nezdinde düşer. Buna benzer tehdit ve tehlikelerden etkilenmeyi en aza indirmek için kurumlara, organizasyonlara ve kullanıcılara düşen önemli görevler vardır. Kullanıcıların bilgi güvenliği konusunda bilinçli olmaları gerekirken, kurumların da bilgi güvenliği kültürünü kurum geneline yerleştirmesi ile beraber kurumsal olarak önlemler alması gereken görevler düşmektedir.

Kullanıcılar bilgi güvenliği hakkında edinecekleri bilinçlendirme ve bilgilendirme eğitimleri sayesinde kendi üzerine düşen görevleri anlayıp ve uygulayarak gerekli korumayı yapmış olacaklardır. Kurumlar ise kurumsal bilgi güvenliği anlamı ve öneminin temel gereği olan bilgi güvenliği yönetim ve denetim standartlarına uyumluluk kapsamında altyapılarını gözden geçirmeli ve gözden geçirme sonucunda ortaya çıkan riskler ve ihtiyaçlara bağlı olarak alınması gereken önlemleri almalıdır.

Bilgi güvenliği sağlamak için bireyler ve kurumların dışında sosyal sivil örgütlere, üniversitelere ve eğitim kurumlarına da düşen görevler vardır. Bu kuruluş ve örgütler, vatandaşlarımızı bilinçlendirme çalışmaları yütürmelidirler.

Bilgi güvenliği sağamak için ayrıca devletimize de önemli görevler düşmektedir. Özelikle bilgi güvenliğinin sağlanmasıyla ilgili yasa ve düzenlemelerin zamanında çıkartılarak hukuksal boşlukların doldurulması gerekmektedir. Diğer önemli bir konu da bilgi güvenliği eğitimlerinin verilebilmesi ve bunu tüm ülke geneline yayması ile bilgi güvenliği bilincinin yaygınlaştırılabilmesi amacıyla gerekli olan çalışmaların ve düzenlemelerin yapılmasıdır.

Vatandaşlarımızın sahip olduğu kişisel bilgi güvenliği önem arz ederken, bundan daha da önemlisi, vatandaşlarımızın bilgi ve güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğimizdir. Günümüzde hepimizin doğrudan veya dolayı yollardan üzerinde hizmet aldığımız bilgi sistemleri veya kurumsal bilgi platformların bilgi varlıklarının, güvenliği sağlanmadıkça, kişisel bilgilerinin de güvende olduğu düşünülemez.

Ülkemiz verilerini de içeren güvenlik raporlarında kurumsal bilgi güvenliği konusunda kurumlarımızın yeterince duyarlı olmadığı ve gerekli olan önlemleri genellikle bilgisizlik,

maddi gerekçeler, personel yetersizliği gibi nedenlerden dolayı alamadıkları tespit edilmiştir. 2008 yılından itibaren etkisini hissidelen global krizin etkisiyle kurumlar yeni teknolojileri veya kendi uzmanlıkları dışında uzmanlık gerektiren alanları takip etmeyi ve kurumsal altyapılarını buna uyarlama çalışmalarını yapamamaktadırlar [1]. Kurumların kendi kurumsal bilgi güvenliği yönetim sistemlerini oluşturmları için bilgi güvenliği konusunda uzman olan güvenlik elemanlarına ihtiyaçları vardır. Ülkemizde kurumların kendi bünyesinde bilgi güvenliği alanında yetişmiş eleman barındırması çok azdır. Bazı kurumlar, bilgi işlemle ilgili her işi yapacak elemanlar ile bilgi güvenliği sistemini kurmaya çalışmaktadırlar. Bazı kurumlar ya bünyesinde bilgi güvenliği alandaki uzman kişiler barındırarak yada bu açığını dış kaynak kullanmaları ile bilgi güvenliği işini yürütmektedirler.

Bilgi güvenliği sisteminin etkinliğini ve güvenliğini kontrol edilmesi için güvenlik testleri (penetrasyon) yapan kurumların sayısı ise yok denecek kadar azdır. Aslında penetraston testlerinin zaman zaman yapılması son derece önemlidir. Bu işi yapan firmaların doğru seçilmesi önemlidir. Ülkemizde bu penetrasyon testi yapan bazı firmalar mevcuttur[*]. Penetrasyon testlerini yaptıran kurumlar kendi network yapısı ve uygulama zaafiyetlerini önceden görme şansına sahip olabilirler. Böylece birçok önlem alabilirler.

Öte yandan geliştirilen birçok yeni donanım ve yazılıma rağmen bilgi teknolojilerine yönelik güvenlik saldırıları her geçen gün artmaktadır. Bilginin gizliliğine (confidentiality), bütünlüğüne (integrity) veya kullanılabilirliğine (availability) karşı yapılan saldırılar ciddi risklere neden olabilmektedir[**]. Bilişim sistemlerinde bu riskleri tamamen yok etmek mümkün değildir. Ancak bu riskler, çeşitli güvenlik önlemleri ile kontrol altına alınabilir ve kayıpları en aza indiririlebilir. Kurumlar tarafından güvenlik önlemleri alınırken göz önüne alınması gereken önemli noktalar vardır. Öncelikli olarak alınan önlemlerin kurum çalısanları tarafından benimsenmesi ve sahiplenilmesi gerekmektedir.

Diğer bir önemli nokta ise korunması gereken bilgi varlıklarının koruma maliyetinin göz önünde tutulmasıdır. Varlığı koruma maliyetinin, varlığın değeri, varlığın zarar görme

---

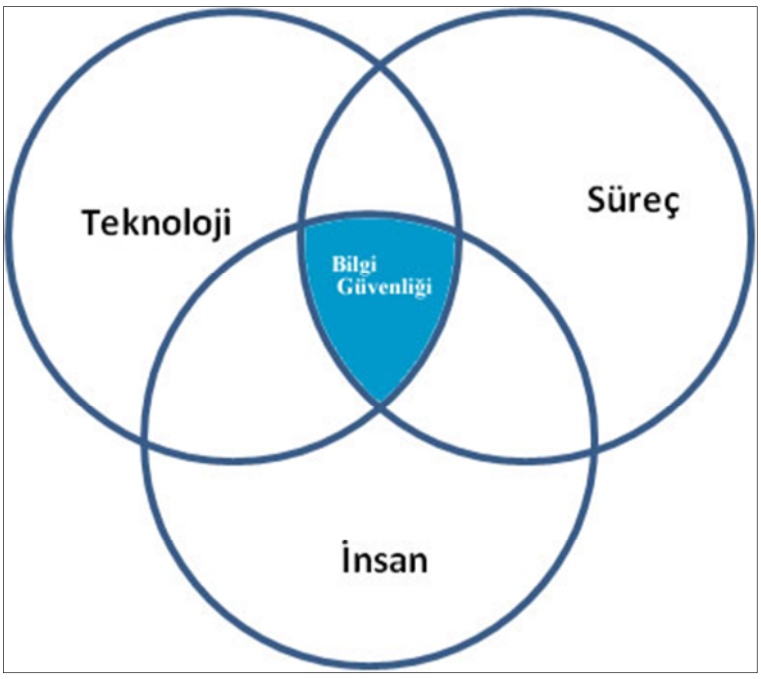
[*] Penetrasyon testi yapan kurumların listesi tezin 8. Bölümünde verilmiştir.

[**] Confidentiality, integrity ve availability kavramları ilerde açıklanacaktır.

olasılığı (tehdit değeri) ve varlığın zarar görebilme zayıflığının çarpımından büyük olmasına önem verilmesi uygun olur. Aksi takdirde varlığı korumak çok maliyetli olacaktır.

Bilgi güvenliğinin sağlanmasına yönelik kurumlar tarafından maddi yatırımlar yapılmadığında meydana gelen zararların ekonomik boyutu her geçen gün katlanarak artmaktadır. Bilgi güvenliği ihlallerinin meydana getirebileceği 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 3. bölümünde olarak yer verilmiştir.

Kurumsal bilgi güvenliği gözönünde insan faktörün de bulundurulması ve buna göre önlemler alınması gerekmektedir. Şekil 1.1'de görüleceğ üzere bilgi güvenliğinin halkalarından birisi insandır. Hatta bunun en zayıf halkası insandır [2]. Her türlü güvenlik önleminin alınmasına karşın, insanın içinde yer aldığı her sistemde mutlaka bir aksamanın meydana gelmesi, bir açığın oluşması mümkündür. Çünkü, insan bilgisayar sistemleri gibi çalışmamakta, karar alırken sadece mantık değil duygusal değerleri de göz önünde bulundurduğundan dolayı zaman zaman hataya düşebilmektedir. Bu hatalar ve insanların kuralları tam olarak uygulamaması sistemlerde ciddi güvenlik açıklarının oluşmasına sebep olmaktadır. Bu yüzden, kullanıcıların güvenlik konusunda bilgilendirilmeleri ve sistem kullanımı sırasında almaları gereken önlemler konusunda eğitilmelidirler.



Şekil 1.1 Bilgi güvenliğinde insan-teknoloji-süreç ilişkisi

Bilgi güvenliği, bilginin üretildigi, işlendiği, taşındığı ve saklandığı her ortamda sağlanmak zorundadır. Bilginin korunmasına çalışıldığı ilk günden itibaren güvenlik zincirinin en zayıf halkasını her zaman insanlar oluşturduğu yukarıdaki paragrafta zikredilmişti. 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 (Kabay, 2007). Bilgi güvenliğini en üst düzeyde tehdit eden ve güvenlik kontrollerinin aşılmasını sağlayan önemli risklerin basında 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 (Munro, 2005).

Sosyal mühendislik* 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 (Mitnick vd, 2003). 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.

Kurumsal bilgi güvenliğinin tesis edilmesi ile ilgili olarak bu tez çalışmasında da güvenliğin sadece bir uygulama, ürün veya hizmet olmadığı aslında bunun bir süreç olduğu bu sürecin insan, eğitim, teknoloji ve işlem (proses) olarak algılanması ve uygulanması ile makul seviyede bilgi güvenliğinin sağlanmasınının mümkün olabileceği açıklanmıştır. Bu amaç ile bu bölümde insan faktörü üzerinde fazla durulmuştur.

---

* Sosyal Mühendislik, insanları kendilerinin yararına olmayan hareketler yapmaya teşvik etmek, kandırmak ve bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan işlere verilen isimdir

Bilgi güvenliğinin sağlanmasında eğitimin önemi büyüktür. Teknoloji ve iletişim çağı ile beraber özellikle de internet ortamındaki sosyal ağların gelişmesi ile birlikte gerek kişisel bilgilerin korunması gerekse kurumsal bilgilerin korunması bir hayli zorlaşmaktadır. Bundan dolayı ülkemizde bilgi güvenliği eğitiminin verilmesiyle ilgili olarak üniversitelerimiz, okullarımız ve Milli Eğitim Bakanlığımıza önemli görevler düşmektedir.

Okul müfradatlarında bilişim güvenliği ile ilgili derslerin konulması ve uygulanması kişisel ve kurumsal olarak bilgi güvenliği bilincini geliştirecektir.

Yukarıda şu ana kadar özetlendiği üzere, kurumsal bilgi güvenliği konusu bir zincirin halkaları misali birbirleriyle alakalı eğitim, insan, teknoloji, işlem, süreçler, standartlar gibi birçok unsuru içinde barındırmaktadır. Bundan dolayı ülkemizde elektronik ortamları kullananları ilgilendiren önemli bir konudur.

Bu tez çalışması kapsamında bilgi, bilgi varlığı, bilgi güvenliği, kurumsal bilgi, kurumsal bilgi güvenliği, bilgi güvenliği yöntem ve standartları, Bilgi sistemleri risk yönetimii bilgi güvenliğini istirmas eden zaafiyetler ve tehditleri, penetrasyon testleri ve ülkemizde sızma testleri yapan firmaları, bu testlerde kullanılan araçlar, web ve veritabanı uygulamalarına ilişkin tehditler, bilgi güvenliğinin sağlanmasına etki eden ünsürlar gibi konu başlıkları altında araştırmalar sunulmuş ve yapılan uygulamalar açıklanmıştır.

Bu tez kapsamında; kurumsal bilgi güvenliğinin anlaşılabilmesi için öncelikle geniş bir anlama sahip olan bilgi ve bilgi varlığı kavramının açıklanması gerekmektedir. Bu kavramlar **bölüm 2**'de "Bilgi Ve Bilgi Varlıkları" başlığı altında açıklanmıştır.

Bilgi sistemlerinin tarihçesi ve geçmisten günümüze kadar bilginin güvende tutulması için geliştirilen yöntemlerin anlaşılabilmesi için bilgi güvenliğinin gelişimi hakkında bilgi sahibi olunması gereklidir. Bu konular **bölüm 3**'de "Bilişim Sistemleri Güvenliği" başlığı altında anlatılmıştır.

Bilgi güvenliği yönetim sistemleri oluşturulurken dünya genelinde kabul görmüş standartların uygulanması ve kurum ve kuruluşlara uyarlanması amacıyla kurumsal bilgi güvenliği politikalarının, standartların ve prosedürlerin ve süreçlerinin yazılması gerekmektedir. Bu durum gösteriyor ki bilgi güvenliğinin sağlanmasında bilgi güvenliği sürecinin sürekliliği ve yönetimi daha fazla önem kazanmaktadır.

Kurumların standartlaşma sağlaması için kabul gören standart ve çerçevelere (Framework)

göre bilgi işlem iş ve süreçlerini organize etmesi gerekmektedir. Bilgi güvenliği ve yönetimi ile ilgili kabul gören uluslararası standart ve çerçevelerin başlıcaları ISO 27001, ITIL, PCI, HIPAA, COBIT, CMMI, PRINCE2, BS25999 vs 'dir.

Bu çalışmada bu konunun önemi gözetilerek kurumsal bilgi güvenliğinin sağlanmasında önemli bir yeri olan bilgi güvenlik yönetimi sistemleri ve standartları "Kurumsal Bilgi Güvenligi Yönetim Sistemleri" konu başlığı altında **Bölüm 4'**de anlatılmıştır.

Standartlasma konusuna önderlik eden Ingiltere 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 [3].

Ülkemizde Avrupa Birligi Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmalar yapılmakla beraber standartı denetimi yaptırıp sertifi alan kurum sayısı sadece 20 dir. Bu kurumlardan birkaç tanesi de kamu kurumudur[4].

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.

ISO 27001 standardı kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde sağlanabilmesi amacıyla bir dizi prosedür ve uygulamaların pratikte çalışması gerekmektedir. Bu konuyla ilgili olarak ISO 27001 standardının kendisi ve uygulama adımları "Iso/Iec 27001:2005 Bilgi Güvenliği Yönetim Sistemi (BGYS)" başlığı altında **bölüm 5**'te kapsamlı açıklanmıştır

Bilişim teknolojileri sürekli gelişen ve değisen bir yapıda olduğundan, bilgi güvenliğinin kurumsal bilgi güvenliğinin sağlanması amacıyla bilgi güvenliği yaşayan bir süreç olarak ele alınmalı, sistemler güncellenmeli, eğitimler alınmalı, oluşabilecek yeni tehdit ve riskler karşısında yatırımların zamanında ve doğru bir şekilde yapılması gerekmektedir. Karmaşık süreçlerden oluşan kurumsal bilgi güvenliğinin sağlanması ve bilgi güvenliği yaşam döndügünün döndürülebilmesi amacıyla bilgi güvenliği yönetim sistemleri bilgi sitemlerinin risklerinin yönetilmesi gerekmektedir. Bu konu" Kurumsal Bilgi Güvenliği Risk Yönetimi" başlığı altında **bölüm 6**'da açıklanmıştır

Günümüzde kurumsal bilgi güvenliğinin sağlanabilmesi için bilişim sistemleri için risk meydana getiren zaafiyet ve tehdit sınıflarının açıklanması alınması gereken önlemlerin

planlanması açısından önem taşımaktadır.

Yukarıda da bahsedildiği üzere internet hız kapasiterlerinin artması ve iletişimin geçmişe nazaran maliyetlerinin düşmesi ile bir çok uygulama internet üzerinden ulaşılabilir duruma gelmiştir. Bununla birlikte beraberinde çeşitli zaafiyetleri ve tehditler de getirmiştir. Özellikle web uygulama ve servislerin sayısının artmasıyla internet üzerinden bilgilere erişim kolaylaşmış ve çeşitli hizmet ve işlemler mekân ve zamandan bağımsız hale gelmiştir. Bilgiye erişimin internet gibi açık ortamlardan yapılması üst seviyede bilgi güvenliğinin sağlanmasını zorunlu kılmaktadır. Ülkemiz ve dünya genelinde bilgi güvenliği zafiyetlerinin web ve veritabanı uygulamalarında yoğunlaştığı ve tehditlerin arttığı tespit edilmiştir. Bu konu ”Kurumsal Bilgi Güvenliğini İstismar Eden Tehditler” başlığı altında **bölüm 7**’de açıklanmıştır

Kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında zaafiyetlerin ve eksikliklerin erken teshisinin önemi büyüktür. Yapılabilecek saldırılardan önce güvenlik zaafiyet ve açıkların tespit edilmesini sağlayan penetrasyon(sızma) testlerinin yapılması kurumsal bilgi güvenliğinin sağlanması açısından önem taşımaktadır. Yine bir uygulamanın da çalışma ortamına (Prodection ortamına ve kısaca Prod ortamına) alınmadan önce zaafiyet ve güvenlik testlerininin yapılması da çok önemlidir. Ülkemizde kısmen kullanılan sızma testlerinin tanımı, hangi amaçla kullanıldığının kurumlar tarafından bilinmesi kurumsal bilgi güvenliğinin sağlanması ve sızma testlerinin yaygınlaşması açısından gereklidir. Kurumsal bilgi güvenliğinin sağlanmasında önemli bir role sahip olan, ülkemizde bu alanda kısmen kullanımı mevcut olan penetrasyon testleri bu testlerde kullanılan araçlar ve bu testi yapan firmların listesi hakkındaki konular “Bilgi Varlıklarıklarını Korumayı Amaçlayan Peneterasyon Testleri” konu başlığı altında **Bölüm 8**’de açıklanmıştır.

Dünyada ve ülkemizde bilişim güvenliğinin ilerleme yönlerini görerek önleyici tedbirleri alabilmek amacıyla güvenlik firmalarının yayınlandığı raporların bilinmesinde fayda vardır.

Bilişim ve iletişim ortam ve teknolojilierinin hızla gelişemesi, ağ kapasitelerinin artması ve sosyal ağların gelişmesi ile kişiler ve gruplar arasında sanal ortamların arttığı bilinmektedir. Bu ortamlardan kamuya yararlı hizmetler ve bilgiler paylaşılmasının yanında çıkar amaçlı ortamlarda oluşmaktadır. Bu tip bilgi güvenliği ihlallerinin önlenmesinde caydırıcı güç olarak veya meydana gelen güvenlik ihlallerinin cezalandırılmasında kullanılmak üzere bilgi

güvenliğiyle ilgili mevzuata hâkim olunmalıdır. Yukarıda sıralanan ihtiyaçların açıklanması amacıyla bilinmesi gerekenler "Bilgi Güvenliği Mevzuatı ve Ülkemizde bilişim Hukuku" konu başlığı altında **Bölüm 9'**da anlatılmıştır.

Tez çalışmasının bir bütün olarak değerlendirilmesi, elde edilen bulgular, ülkemiz açısından sağlanan katkılar, çalışmalar sırasında karsılaşılan güçlükler, kazanımlar ve sunulan öneriler "Sonuç ve Öneriler" konu başlığı altında **Bölüm 10'de** verilmiştir.

2. BİLGİ ve BİLGİ VARLIKLARI

Bilgi teknolojilerinin yaygınlaşması ile beraber bilgi üretimi de ciddi boyutlarda artış göstermiştir. Bilgi teknolojileri yaygınlaşmadan önce, bilginin büyük bir çoğunluğu basılı dokümanlarda iken, günümüzde bilgi teknolojileri tarafından işlenir duruma gelmiştir. Bu nedenle günümüzde bilgiye erişme imkânları geçmiş ile karşılaştırılamayacak seviyede artmıştır. Bu durum, birçok dezavantajı beraberinde getirmektedir. Bilgi teknolojileri üzerinde bilinçli veya bilinçsiz yapılan hataların çok ciddi sonuçlar doğurması olasıdır. Bilgi teknolojilerindeki açıklıklar ve dikkatsiz yapılandırmalar bilgiye yetkisiz erişime yol açabilir. Bu durumda bilginin yetkisiz imhası, değiştirilmesi ve görülmesi söz konusu olabilir. Geçmişte sadece fiziksel güvenliğin tesis edilmesi ile sağlanan bilgi güvenliği, günümüzde kurumların en çok zorlandıkları ihtiyaçların başında gelmektedir.

Bilgi çağı [5] olarak olarak adlandırılan günümüzde bilginin çok daha önem kazanması ile birlikte bilginin korunması ve güvenliğinin sağlanmasıda beraberliğinde gelmektedir. Bilgi üretilip işlendiği, taşındığı ve saklandığı bilişim sistemlerinin güvenliği dünyada ve ülkemizde güncel yerini korumuştur. Birinci bölümde önemi vurgulandığı üzere günümüzdeki toplumların temel hammaddesi olan bilgiler elektronik ortamlarda işlendikçe, taşındıkça ve saklanıkça bu ortamlarda alınması gereken önlemlerin, emek, metodoloji, güvenlik seviyeleri, değer, maliyet ve boyut açısından da farklılıklar gösterebilmektedir. Bilgi güvenliğinin doğru oranda sağlanması için bilgi varlıklarının sınıflandırılması ve bu sınıflandırmaya göre değerinin iyi tespit edilmesi, iyi derecede bir bilgi güvenliği bilincinin yerleşmesi, kullanılan yazılım ve donanım zayıflıklarının iyi takip edilmesi, meydana gelen zayıflıkların her an izlenmesi ve giderilmesi, meydana gelebilecek zayıflıkların önceden tespit edilerek zamanında giderilebilmesi, bu önlemlerin alınması için çalışanların eğitim ve beceri sahibi olması, sistemleri ve bilgileri belirli politikalar çerçevesinde korumak ve bu bilinçle güvenliğin dinamik bir süreçte ele alınması gerektigi artık bilinen veya bilinmesi gereken konulardır.

Tez çalışmasının bu bölümünde konunun öneminin daha iyi anlatılması ve bilgi güvenliği farkındalığın oluşturulması için bilgi ve bilgi varlığı incelenmiştir.

2.1 Bilgi

Bilgi (information) kelimesinin menşei, Latince'deki herhangi bir şeye sekil vermek anlamına

gelen “informare” kelimesinden gelmektedir (Floridi, 2010). Bilgi insan ile obje (nesne) arasındaki karşılıklı ilişkiden çıkan bir sonuçtur. Sözlük anlamıyla bilgi; öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü, insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü gibi anlamları bulunmaktadır. Bilgi literatürde çok farklı şekillerde tanımlanmaktadır. Bilgi, doğruluğu ispatlanmış inançlardır. Bilgi, sosyal olaylarda karşımıza çıkan eylem ve olayları anlamamıza yardım eden işaret ve kodlamalardır (Argyris, 1993).

Bilgi, günümüzde işletmeler için önemli bir varlık durumuna gelmiştir. Tek başına maddi ve finansal varlıklar, işletmelerin uzun dönemli başarısı için artık yeterli değildir. En iyi bilgi ve enformasyona sahip olan, istikrarlı bir şekilde yeni bilgi yaratan, bu bilgiyi organizasyonun her yerine geniş ölçüde yayan, yeni teknolojilerde ve ürünlerde hızla kullanan ve inovasyana oluşturabilen firmaların başarılı olduğu görülmektedir (Nonaka ve Takeuchi, 1995).

Üretim kavramının ortaya çıktığı ilk zamanlardan beri var olan, hissedilen ancak fiziksel bir niteliği olmamasından dolayı görünmeyen bir varlık olan bilgi, son yıllarda özellikle bilgi teknolojilerine dayalı sistem ve uygulamaların gelişmesi ve buna paralel olarak bu kurumlarda üretilen ürün ve hizmetlerin değerlerinin tam olarak belirlenemesi bu değerlerin ancak bilgi sistem araçları ile ortaya çıkma sonucu, bu varlığın fark edilmeye başlanmasına neden olmuştur. Bunun sonucunda gelişmiş kurumlarda bilgi artık bir varlık olarak tanımlanmaya başlanmıştır (Calder ve Watkins, 2007).

Bilgi günümüzde artık bir varlık olarak tanımlanmalı ve kişi, kurum ve kuruluşlar için önemli ve değerli olan bir kaynak gibi muamamele görmeli ve korunmalıdır.

2.1.1 Bilgi Varlıkları

ISO standartları bilgi varlığını, kişi ve kurumların sahip olduğu ve kendisi için maddi veya manevi değer ifade eden ve bu nedenle uygun korunmayı gerektiren tüm unsurlar şeklinde tanınlamışlardır (Iso, 2005).

Bir kurumun sahip olduğu dokümanlar raporlar, defterler, para kasası, sermayesi, veritabanları, müşteri bilgileri, personel dosyaları, öğrenci bilgileri,not kayıtları, rekabet bilgileri, web sayfaları, sistem odaları, sunucu, bilgisayar, ağ, telefon gibi bilişim sistemler gibi varlıklar, bilgi varlığına örnek verilebilir.

2.1.1.1 Kurumsal Bilgi Varlıklarının Sınıflandırılması ve Korunması

Bilgi varlığı, kişi, kurum ve kuruluşlar için önemli ve değerli olan bir kaynaktır ve korunması gerekir. İçeriğine göre bireysel ve kurumsal olmak üzere ikiye ayrılabilir. 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 (Bhatt, 2001).

Bilgi güvenliği açısından kurumsal olarak güvenlik risk seviyelerine göre korunması gereken varlıklık aşağıdaki gibidir (Iso, 2005):

Bilgi varlıkları:

Kuruluşun tüm bilgi sistemlerinde işlenen ve saklanan tüm bilgilerdir. Bu varlıklar, fiziksel ve mantıksal ortamlarda bulunabilir. Veritabanı, data dosyaları, müşteri bilgileri,çalışan özluk bilgileri, sözleşmeler, sistem dökümanları, kullanıcı rehberleri, araştırma dökümanları, kurum rekabet araştırmaları vs. örnek verilebilir. Sınıflandırması aşağıdaki şekilde yapılabilir:

- **Yazılımlar:** İşletim sistemleri, uygulama yazılımları, veritabanlarında duran bilgileri, geliştirme araçları, çizim ve hesap araçları vb.
- **Fiziksel varlık ve donanımlar**: Sunucular, PC'ler, fax-fotokopi, telefonlar vb.
- **İnsan Kaynakları**: Çalışan personel.
- **Hizmetler:** Bilgi sistemlerinin bağımlı olduğu iletişim ve bilgisayar hizmetleri, enerji, ısıtma, soğutma gibi genel hizmetler, iş süreçleri gibi.
- **Maddi olmayan varlıklar:** Entellektüel varlıklar, imaj ve itibar örnek verilebilir..

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 makul seviyede bir bilgi güvenliğinin sağlanması için önemlidir. Günümüzde kurumlar açısından kurumsal bilginin önemini göstermesi açısından 1998

yıllında kurulan ve 2004 yılında halka açılan (Borsada işlem gören) Google firması buna örnek olarak verilebilir [6]. Günümüzde neredeyse yüzyıllık **şirket**leri piyasa değerleri ile kıyaslandığında Google firmasının piyasa değerinin çok daha yüksek olduğu görülmektedir [7]. Bilginin günümüz rekabetçi pazarlarında son derece büyük bir role ve öneme sahip olduğunu ve gelecekte daha da öneminin artacagını kanıtlayan buna benzer örnekler her geçen gün daha fazla ortaya çıkmaktadır.

Kurumsal bilginin rekabeti körükleyici, itici, üretken gücünü doğru ve yerinde kullanan kurumlar, dünyanın her bölgesinde rekabet edecek duruma gelebilmektedirler. Kurumsal bilgi yönetiminin bu derece önemli olduğu günümüzde kurumsal bilgilerin güvende olması ve güvenli şekillerde taşınması çok önemlidir. Kurumsal bilgi güvenliğinin sağlanması her kurum için olmazsa olmazların başında gelmektedir.

Bu tez çalışmasında bunun gerekçelerini ortaya koymak ve alınması gereken önlemleri sunmak, ülkemizde tam olarak henüz önem verilmeyen kurumsal bilgi güvenliği yönetimi süreçlerini ele alıp kurumların bilgi güvenliği ihlallerinden doğabilecek kayıplarının azaltılmasında dikkat edilmesi gereken hususları göstermek de hedeflenmiştir.

3. BİLİŞİM SİSTEMLERİ GÜVENLİĞİ

3.1 Bilgi Güvenliğine Genel Bakış

Bilgi güvenliği, bilgiyi yetkisiz erişimlerden koruyarak gizliliğini(confidentiality) sağlamak, bilginin bozulmadan tamlığını(bütünlük) ve doğruluğunu (integrity) temin etmek ve istenilen zamanda erişilebilirliğini(availability) garanti etmekdir (Isaca, 2009).

Bilgi güvenliğinin denince için gizlilik, bütüntük ve erişilebilirlik kavramları ön plana çıkmaktadır.

Bilginin gizliliği(confidentiality) ile kastedilen, bir bilgiye sadece o bilgiye erişmesi gereken kişi veya kişilerin erişimine izin verilmesidir.

Bilginin bütünlüğü(integrity), o bilginin tahrif edilmeden, değiştirilmeden olduğu gibi orjinal hali ile durmasıdır.

Bilginin erişilebilirliği veya kullanılabilirliği(availability) bilgiye istenilen ve makul olan zamanda erişilmesi ve kullanılmasıdır.

Bu üç kelime ingilizce olarak **CIA** (**C**onfidentiality, **I**ntegrity, **A**vailability) kısaltılıp Türkçe **GBK**(**G**izliliğini, **B**ütünlük, **K**ullanılabilirlilik) olarak da kullanılır.

3.2 Bilişim Korsanlığının Tarihi

Bilgi ve bilgi güvenliği öneminin daha iyi anlaşılması için bilgi ve bilişim hırsızlığının da bilinmesinde yarar vardır. Bilişim, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimidir. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalıdır. Bilişim, bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır [8].

Bilişim korsanlığı(hırsızlığı) bilgi ve bilişim sistemelerine yetkisi olmadığı halde bu bilgi ve

sistemlere giren, girmeye çalışan, sistemlere saldırarak devre dışı bırakan(DoS ve DdoS denial of service*), bilgi ve sistemlere zarar veren, kendisine ait olmayan bu bilgiyi ifşa eden diye tanımlanabilir (Shahim, 2009).

Bilişim güvenliği denildiğinde insan faktörü, teknoloji ve sürecin birarada değerlendirilmesi gerekir. Bilgi güvenliği öneminin anlaşılabilmesi, bilgi varlıkları ve hizmetlerinin zaafiyetlerini kullanan tehditleri ve önlemleri konusunda geçmiste yaşanan olayları ve bu olayların sonucunda 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. Bu zaafiyetleri en iyi anlama yolu sistem veya uygulamaları güvenlik testlerine (güvenlik-sızma testleri veya penetrasyon) tabii tutmaktır. Bu testleri yaparken dikkat edilmesi gereken önemli nokta testlerin gerçeğe yakın olmasının sağlanmasıdır. Sızma testleri yapılırken gerçek bir saldırgan gibi düşünerek saldırganların kullandığı araç, yöntem ve becerilerle kurumsal bilgi varlıklarının güvenlik sevileri test edilmelidir.

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

1960'lar, ilk bilgisayar hackerları Amerika'da M.I.T.'de (Massachusetts Institute of Technology) ortaya çıkmıştı. Elektrikli trenleri kurcalayıp daha hızlı ve farklı çalışması için değiştiren yani "hack" eden model tren hobi grubunun üyelerini temsil eden "hacker", aynı işi bilgisayarlar üzerinde, yazılımda yapan grubun üyelerinin de kullandığı bir isim haline geldi. Korsan (hacker) teriminin doğdugu yıllar olarak literatüre geçmistir (Shinder ve Tittel, 2002).

1970'lar, bilişim korsanlığı daha sonra telefon hatları üzerinde ücretsiz görüşme yapılması ile başlanmıştır.

John Draper "Cap'n Crucnh" lakabını aldı. Draper bu adı taşıyan kahvaltı gevreği kutularından çıkan oyuncak düdüğün çıkarttığı 2600 hertz'lik sinyalin, AT&T'nin uzun mesafeli telefon görüşmelerinde kullandığı sistemle aynı frekansta olduğunu öğreniyor. Ardından bu buluşu bedava telefonla konuşmak için kullanıyor. Bu yıllarda telefon korsanları (phreaking) ücretsiz

* DoS ve DdoS, hizmeti devre dışı bırakmak olup ilerki bölümlerde anlatılacaktır.

görüşme yapabilmek için uluslararası telefon şebekelerine sızmaya başlamıstır. 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) çıkardıgını tespit etmiş ve mavi kutu (Blue Box) adı verilen cihazı geliştirmiştir. Bu cihaz sayesinde çok sayıda insana para ödemeden telefonla milletlerarası görüşme yaptırmıştır. Draper gerçeklestirdigi 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 yazdırmıstır (Wozniak ve Smith 2006). 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'ler, bu yıllarda bilgisayarların gelişmesiyle beraber telefon korsanları yavaş yavaş bilgisayar alanına kaymaya başlamıştır. Ayrıca ilk elektronik mesaj pano sistemleri ortaya çıkmıstır. 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 iş ortamlarında yapılan işlemlerin performansının ölçülmesi amacıyla ilk defa solucanlar (worm) kullanılmıştır bu wormlar daha sonra 1998 epostalarla yayılarak dünyada büyük zararlara neden olmuştur. 1983 yılında ise "Bilgisayar Virüsü" terimi DEC-VAX sistemleri üzerinde akademik deneylerini yapan Fred Cohen tarafından resmen tanımlanmıstır (Gelbstein ve Kamal, 2002).

1983 yılında Savaş Oyunları (War Games) isimli sinema filmi saldırı ve korsan efsanesini geniş kitlelere tanıtmıstır.

1985 yılında bilgi teknolojilerinin hizmet yönetimi ile ilgili olan ITIL* (Bilgi Teknolojileri Alt Yapı Kütüphanesi- Information Technology Infrastructure Library)' in birinci sürümü (version-v1) yayımlanmıştır.

1986 yılında korsan grupları bilgilerini para karşılığında satmaya başlamıştır. Bu alanda bilinen ilk olay olan 1986 yılında Almanya Hannover sehrindeki Chaos Computer Club üyesi olan birkaç korsan ABD'deki kamu (Enerji Bakanlığı, Savunma Bakanlıgı, NASA) ve özel

* ITIL ve CMMI bu tezin 4. Bölümünde anlatılacaktır.

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 geçmistir (Rattray, 2001).

1990'lı yıllar, 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 [9].

1991 yılında yazılım süreci olgunluk modellemesini olan CMMI (Capability Maturity Model-Integration; Bütünleşik Yetenek Olgunluk Modeli)'nin birinci sürümü (version 1-v1) yayımlanmıştır.

1993 yılında dünyanın dört bir yanındaki korsanların ve korsan olmaya hevesli bilgisayar meraklıları DefCon adı altında ilk defa toplanmıştır. Aynı yıl bir zamanlar "dark dante" takma adıyla anılan eski hacker yeni gazeteci-blogger Kevin Poulsen, Pacific Bell telefon şirletini hack ederek, KISS-FM adındaki radyo istasyonunun düzenlediği yarışmada, 102. arayan olmayı başararak Porsche 944 S2 kazanmış ve adını tüm ülke çapında duyurmuştu. Ancak hemen sonra yakalanan ve belli bir süre hapis yatan Poulsen, artık güvenlik raporları hazırlayan bir uzman olarak hayatına devam etmektedir (Hoath, 1998).

Kimilerine göre Dünyanın en büyük hackerı veya en çok tanınan hackeri Kevin Mitnick bu FBI'ın en çok arananlar listesine girmeyi başarmış ilk hacker olma ünvanına bu yıl sahip olmuştur. Kredi kartı veritabanlarını, telefon ağlarını hack ettikten sonra bilgisayar güvenlik uzmanı T.Shimomura'nın evindeki bilgisayara sızmaya çalışırken yakalanmıştır. Fujitsu, Motorola, Nokia ve Sun Microsystems gibi şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak 5 yıl hapis cezası almıştır. "The art of deception" adında bir kitabı bulunmakta. ayrıca zamanında kendisi için "free kevin mitnick" diye bir site de açılmıştı. kendi hayatını anlatan "Freedom Downtime" isimli bir filmde kendisini canlandırdı.. 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 sapkalı bir

bilgisayar korsanı olarak güvenlik danışmanlığı yapmakta ve dünya çapında bilgi güvenliğiyle ilgili kongrelere katılmaktadır [10].

1995 yılında ilk zafiyet tarama programı olan SATAN (Security Administrator Tool for Analyzing Networks) programı yazılmış ve güvenlik zafiyetlerini tanımlayabilecek hale gelmiştir (Chen vd, 2005).

Bu yıllarda kurumsal bilgi güvenliği bilinci iyice artmaya başlamıştır.Üniversiteler ve kurumlar tarafından standartlar* geliştirmeye başlanmıştır. Yine aynı yıl içerisinde çok önemli olan kurumsal bilgi güvenliğinin sağlanmasında kullanılacak olan ve ingiliz standart enstitüsü (British Standards Institution-BSI) tarafından geliştirilen BS-7799 standardı hazırlanmış ve kurumsal bilgi güvenliği standardı olarak olarak kabul edilmiştir.

1996 yılında HIPAA (The Health Insurance Portability and Accountability Act) Sağlık Sigortası Taşınabilirlik ve Sorumluluk olan yasa Amerikada çıkmıştır. Bu yasanın yani Hipaa'nın amaçlarından bir tanesi de özel sağlık bilgilerini korumak ve kişisel bilgileri dispersiyon için tek tip bir standard oluşturmaktır.

Aynı yıl içerisinde çıkış noktası bilgi teknolojilerinde proje yönetimi metodolojisi olan PRINCE2* (**PR**ojects **IN C**ontrolled **E**nvironments) tüm proje türlerinde kullanılmak üzere genelleştirilmiş ve PRINCE2 adını almıştır. [11]

Yine aynı yıl bilgi teknolojileri yönetimi için en iyi uygulamalar kümesi olarak kabul edilen COBIT* (The Control Objectives for Information and related Technology- Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (COBIT) ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından geliştirilmiştir. COBIT yöneticilere, denetçilere ve Bilgi Teknolojileri (BT) kullanıcılarına iş hedeflerinin bilgi işlem hedeflerine dönüşümünü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirirken, aynı zamanda bilgi teknolojileri alt yapılarını da etkin kullanmayı amaçlamıştır (Shahim, 2009).

---

* Standardlar bu tezin 4 ve 5. Bölümlerinde detaylı anlatılacaktır.

* PRINCE2 ve COBIT bu tezin 4. Bölümünde anlatılacaktır.

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 bakabilmişlerdir. Geliştirilen bu yazılımla birlikte bilişim güvenliği için yeni tehlikeli 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 tecrübeli korsanlar yerine onların yazmış olduğu yazılımları ustalıkla kullanan acemi korsanlarda artık önemli bir tehdit unsuru haline gelmiştir (Garfinkel, 1995).

1998 yılı içerisinde BS–7799 standardının ikinci kısmı yayınlanmıştır. BS 7799–2 daha çok BS-7799 uygulamasının nasıl yapılacağı anlatan bir rehber niteliğini taşımaktadır. 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 isletim sistemini çıkarmasıyla birlikte, 1999 saldırıların çok olduğu ve bilgi güvenliğinin gerekliliğinin fazlaca hissedildiği bir yıl olmustur. 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 gerçekleştirilmistir. Belge alan ilk kuruluş İgiltere’de bulunan The Co-Operative Bank isimli e-bankacılık yapan bir isletme olmustur (Numanoğlu, 2005).

2000’li yıllar, kurumsal açıdan güvenlik kaygılarının en üst seviyeye çıktığı, saldırıların ve korsanların çok tehlikeli olduğu ve artık saldırıların daha organize yapıldığı yeni bir döneme girilmiştir. Bu yeni dönemde kötücül kodlar internet aracılıgıyla hızla yayılmış milyonlarca bilgisayara bulaşmış ve milyonlarca dolarlık maddi hasara yol açmıstır. Saldırılar ve etkileri hızla artarken Marty Roesch ve Ron Gula tarafından Snort ve Dragon isimli saldırı tespit sistemleri hakkında ilk defa bilgi vermişlerdir (Ruiu, 2006).

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 dişer 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.

Ülkemizde de buna paralel olarak TSE (Türk Standartları Enstitüsü) tarafından çalışmalara başlanmıştır. Kuruluşların içerisinde bilgi teknolojisi güvenliğine ulaşmak ve sürdürmek için bir Bilgi Güvenliği Yönetim Sistemi üzerinde çalışılmıştır. ISO/IEC 17799:2000 Uygulamalar için tavsiyeler ve örnek yönetmeler içeren referans bir doküman olarak tasarlanmıştır. Kullanılmakta olan en iyi bilgi güvenliği uygulamalarını temel almıştır.

2002 senesinde çıkartılan BS 7799-2 (Bölüm 2) standardı ile ortaya konan kullanım kılavuzu ile kurumların ISO 17799 sertifikasyonu alması hedeflenmiştir. TSE, ISO 17799'u Kasım 2002'de BS 7799-2'yi ise Şubat 2005'te standart olarak kabul edip türkçe olarak yayınlamıştır.

Kurumsal bilgi güvenliğinin sağlanmasında olmazsa olmaz bir faktör olan standartlar konusu Bölüm 4 ve 5'te kapsamlı olarak anlatılmıştır.

2000 yılından sonra özellikle sanal gruplar oluşmuş ve daha organizeli ve gelir yaplaşımlı bilişim ihlalleri meydana gelmiştir. 2000 yılından günümüze kadar birçok saldırı olmuş ve kurumlar yüksek oranda bu saldırılardan etkilenerek maddi manevi zararlar görmüstür. 2000 yılından sonraki yıllarda otomatik saldırı araçlarının hızla yayılması sonucunda yapılan saldırılara burada yer verilmemiştir. Bunun baslıca sebebi saldırıların çoğalmasıdır. Hatta son yıllarda devletlerin hizmetlerini aksatan ve durduran saldırılar da meydana gelmiştir. Günümüzde otomatik programcık ve programların artması sonucu birçok saldırı yapılabilinmektedir.

Sonuç olarak son 50 yılda saldırganların geldiği nokta kurumsal bilgi güvenliğini üst düzeyde tehdit etmekte ve kurumların ve bireylerin bilgi güvenliğini sağlamaları konusunda üzerine

---

* Bilgi güvenliği standardı olup bu tezin 5. Bölümünde uygulaması da anlatılacaktır.

düşen görevlerini eksiksiz yerine getirmeleri gerekmektedir. Bundan dolayı bilgi güvenliği kurumsal kültürün bir parçası yapmayan kurumların ciddi riskler taşıdığı görülmektedir.

3.3 Bilgi Güvenliğinin Gelişimi ve Güvenlik Türleri

Bilgi güvenliğinin sağlanması için tarih boyunca çesitli güvenlik yöntemleri kullanılmıştır. Günümüzde hemen hemen tüm kurumlar kendi içlerindeki gereksinimlere göre bilgi akışını sağlayabilmek için bilişim altyapıları oluşturmaya başladılar. Artık bilgiye erişmek, bilgiyi saklamak gibi sıradanlaşan işler için çoğunlukla bilişim sistemleri kullanılmaktadır. Bir işletmenin bilgi varlığını artırması ve koruması o işletmeyi rekabet ortamında bir adım öne geçirmektedir. Giderek kritik bir değer haline gelen bilginin iç ve dış tehditlerden koruması ve zarar görmesinin engellemesi için kurumların bilgi güvenliği politikaları ve uygulamaları oluşturması gerekmektedir. Bilginin güvenliğinin sağlanmasının günümüze kadar olan değişimi ve gelişimi bilgi güvenliğinin sağlanmasında izlenilen yöntemlerin anlaşılabilmesi açısından önemlidir. Geçmisten günümüze bilgi güvenliğinin sağlanması için sırasıyla başta fiziksel ve çevresel güvenlik, haberlesme güvenliği, bilgisayar güvenliği, ağ güvenliği, uygulama güvenliği, veritabanı güvenliği, web güvenliği gibi konularında çalışmalar yapılmıştır (Lockhart, 2006).

Günümüzde bilgi güvenliğinin sağlanabilmesi için yukarıda bahsedilen güvenlik önlemlerinin hepsinin bir arada düşünülmesi gerektiğinden bu önlemler takip eden alt baslıklarda sırasıyla açıklanmıştır.

3.3.1 Fiziksel ve Çevresel Güvenlik

Güvenlik insanoğlunun hep önem verdiği bir konu olagelmiştir. Geçmis zamanlarda insanlar için önemli bilgilerin, çeşitli işaretlerle kayalara taşlara kazıyarak daha sonra madenlere işleyerek saklanmışlar. Daha sonraların ise ağaçlara, derilere ve sonrasında kâğıtlara yazılarak fiziksel güvenliği sağlanan ortamlarda saklanmıstır. Günümüzde artık bu yazma sanal medialara işlenmektedir. Fiziksel güvenliğin sağlanabilmesi amacıyla, duvarlar örülmüs, kale ve hendekler çekilmis, surlar ve sedler yapılmış, 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 (Boran, 2000).

Günümüzde de fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar

yapılmaktadır. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi, bina giriş-çıkış ve çevresinin kameralar ile izlenmesi gibi önlemler kullanılmaktadır.

Fiziksel ve çevresel güvenlik, bilgi güvenliği açısından değerlendirildiğinde pratikte kuruma yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunması olarak algılanabilir.

Konu ile ilgili bir takım işler artık standard hale olagelmiştir . Bu işler aşağıda özetlenerek sıralanmıştır. Bu işlerin uygulaması bilgi güvenliği açısından gereklidir.

- Bilgi işleme servis merkezlerini korumak amacıyla bir fiziksel bir sınır güvenliği tesisi (yetki kontrollu kart sistemi, güvenlik elemanlı nizamiye gibi) kurulmuş olmalıdır.
- Fiziksel sınır güvenliği, içindeki bilgi varlıklarının güvenlik ihtiyaçları ve risk değerlendirme sürecinin sonucuna göre olusturulmuş olmalıdır.
- Kurum içerisinde belli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol mekanizmaları kurulmalıdır.
- Ziyaretçilerin giriş ve çıkış zamanları kaydediliyor olmalıdır.
- Önemli ve hassas bilgilerin bulunduğu alanlar yetkisiz erişime kapatılmalıdır.
- Tüm personel ve ziyaretçiler güvenlik elemanları tarafından rahatça teşhis edilmelerini sağlayacak kimlik kartlarını devamlı takıyor olmalıdırlar.
- Güvenli alanlara erişim hakları düzenli olarak gözden geçiriliyor olmalıdır.
- Ofisler ve odalarla ilgili fiziksel güvenlik önlemleri alınmalıdır.
- Personel güvenliği ve sağlığı ile ilgili yönetmelikler uygulanmalıdır.
- Kritik tesisler kolayca ulaşılamayacak yerlere kurulmuş olmalıdır.
- Binada bilgi işlem faaliyetlerinin yürütüldüğüne dair işaret, tabela vb. bulunmamasına dikkat edilmelidir.
- Bilgi işlem merkezlerinin konumunu içeren dâhili/harici telefon rehberleri halka kapalı olmalıdır.
- Harici ve Çevresel Tehditlerden Korunma
- Yangın, sel, deprem, patlama ve diğer tabii afetler veya toplumsal kargaşa sonucu oluşabilecek hasara karsı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

- Komşu tesislerden kaynaklanan potansiyel tehditler göz önünde bulundurulmalıdır.
- Yedeklenmiş materyal ve yedek sistemler ana tesisten yeterince uzak bir yerde konuşlandırılmış olmalıdır.
- Güvenli bir alanın mevcut olduğu ile ilgili olarak veya burada yürütülmekte olan çesitli faaliyetlerle ilgili olarak personel ve üçüncü parti çalışanları için "İhtiyacı kadar bilme" prensibi uygulanmalıdır.
- Kayıt cihazlarının güvenli alanlara sokulmasına engel olunmalıdır.
- Kullanılmayan güvenli alanlar kilitleniyor ve düzenli olarak kontrol ediliyor olmalıdır.
- Kötü niyetli girişimlere engel olmak için güvenli bölgelerde yapılan çalışmalara nezaret edilmelidir.
- Halka Açık Alanlardan, Yükleme ve Dağıtım Alanlarından Erişim
- Bilgi işlem servisleri ile dağıtım ve yükleme alanları ve yetkisiz kişilerin tesislere girebileceği noktalar birbirinden izole edilmiş olmalıdır.
- Ekipman yerleşimi yapılırken çevresel tehditler ve yetkisiz erişimden kaynaklanabilecek zararların asgari düzeye indirilmesine çalışılmalıdır.
- Ekipman, gereksiz erişim asgari düzeye indirilecek şekilde yerleştirilmelidir.
- Kritik veri içeren araçlar yetkisiz kisiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.
- Özel koruma gerektiren ekipman izole edilmiş olmalıdır.
- Nem ve sıcaklık gibi parametreler izlenmelidir.
- Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır.
- Paratoner kullanılmalıdır.
- Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır.
- Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır.
- Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.
- Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.

- Su bağlantısı iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.
- Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmış olmalıdır.
- Kurum bu konuda yasal yükümlülüklerini yerine getirmelidir.
- Güç ve iletişim kablolarının fiziksel etkilere ve dinleme faaliyetlerine karsı korunması için önlemler alınmış olmalıdır.
- Kablolar yeraltında olmalıdır.
- Karışmanın ("interference") olmaması için güç kabloları ile iletişim kabloları ayrılmış olmalıdır.
- Hatalı bağlantıların olmaması için ekipman ve kablolar açıkça etiketlenmiş ve işaretlenmiş olmalıdır.
- Hassas ve kritik bilgiler için ekstra güvenlik önlemleri alınmalıdır.
- Alternatif yol ve iletişim kanalları mevcut olmalıdır.
- Fiber optik altyapı yapılandırılmalıdır.
- Bağlantı panelleri ve odalara kontrollü erişim altyapısı kurulmuş olmalıdır.
- Ekipmanın bakımı doğru şekilde yapılmalıdır.
- Ekipmanın bakımı, üreticinin tavsiye ettiği zaman aralıklarında ve üreticinin tavsiye ettiği şekilde yapılmalıdır.
- Bakım sadece yetkili personel tarafından yapılıyor olmalıdır.
- Tüm şüpheli ve mevcut arızalar ve bakım çalışmaları için kayıt tutulmalıdır.
- Ekipman bakım için kurum dışına çıkarılırken kontrolden geçirilmelidir.
- İçindeki hassas bilgiler silinmelidir.
- Ekipman sigortalıysa, gerekli sigorta şartları sağlanıyor olmalıdır.
- Kurum alanı dışında bilgi işleme için kullanılacak ekipman için yönetim tarafından yetkilendirme yapılıyor olmalıdır.
- Tesis dışına çıkarılan ekipmanın başıboş bırakılmamasına, seyahat halinde dizüstü bilgisayarların el bagajı olarak taşınmasına dikkat edilmelidir.
- Cihazın muhafaza edilmesi ile ilgili olarak üretici firmanın talimatlarına uyuluyor olunmalıdır.

- Evden çalışma ile ilgili tedbirler alınmış olmalıdır. Sigorta cihazların tesis dışında korunmasını kapsıyor olmalıdır.
- Kurum alanı dışında kullanılacak ekipmanlar için uygulanacak güvenlik önlemleri, tesis dışında çalışmaktan kaynaklanacak farklı riskler değerlendirilerek belirlenmiş olmalıdır.
- Ekipman imha edilmeden önce gizli bilginin bulunduğu depolama cihazı fiziksel olarak imha edilmelidir.
- Depolama cihazının içerdiği bilginin bir daha okunamaması için klasik silme veya format islemlerinin ötesinde yeterli düzeyde işlem yapılmalıdır.
- Ekipman, bilgi veya yazılımın yetkilendirme olmadan tesis dışına çıkarılmamasını sağlayan kontrol mekanizması oluşturulmuş olmalıdır.
- Kurum varlıklarının yetkisiz olarak kurum dışına çıkarılıp çıkarılmadığını saptamak için denetleme yapılmalıdır.
- Kurum çalışanları bu tip denetlemelerden haberdar olmalıdır.

3.3.2 Haberleşme (iletişim) Güvenliği

Karşılıklı olarak bilgi alısverişinde güvenli bir haberleşme ortamını oluşturmak üzere yapılan faaliyetlerin ortak adı haberleşme olarak adlandırılır [12]. Haberleşme anında fiziksel olarak bilgilerin güvenliğinin sağlanması, güvenlik açısından yeterli değildir. İletisim sırasında bilginin hedefe ulaşmadan önce başka kişiler tarafından ele geçirilmesi ve içeriğin öğrenilmesi riski her zaman vardır. Haberlesme güvenliğinin sağlanmasında kullanılan yöntemler tarih boyunca değişmemis fakat bu güvenliği sağlamak için kullanılan teknikler ve yöntemler sürekli olarak gelişmistir (Fry, 2001).

Haberleşme güvenliğinin sağlanmasında kriptografi ve steganografi yöntemleri kullanılmaktadır.

Steganografi, veri içerisinde veri saklama" anlamına gelip Yunanca "gizli yazı" veya iletişimin varlığını saklayan yöntem olarak bilinir.

Kriptografi, gizli mesajın anlaşılamaz hale getirilmesi yani mesajın varlığı bilinir ancak, içeriği anlaşılamaz. Kriptografi mesajın içeriğini anlaşılmaz hale getirirken, steganografi mesajı görülemeyecek şekilde saklar (Artz, 2001).

Kriptografi, veriyi yalnızca okuması istenen şahısların okuyabileceği bir şekilde saklamak ve göndermek amacıyla kullanılan bir teknolojidir. Kriptografi'de veri, matematiksel yöntemler kullanılarak kodlanır ve başkalarının okuyamayacağı hale getirilir. Bu matematiksel kodlamaya "kripto algoritması" adı verilir. İlk bilinen kripto algoritmaları 4000 yıl kadar önce ortaya çıkmıştır. Zaman geçtikçe, kullanılan teknikler ve cihazlar gelişmiş ve her geçen gün yeni teknikler kullanılır ve yeni algoritmalar üretilir olmuştur. Bu teknoloji şu anda bilişim güvenliğinin vazgeçilmez bir parçasıdır. Şifrelenmemiş bir bilgiye "açık metin" (clear text) denir. Açık metin, bir insanın okuyabileceği bir yazı ya da bir bilgisayarın anlayabileceği çalıştırılabilir (.exe, .com) bir program ya da bir veri dosyası (.txt) olabilir. Bir kripto algoritması kullanılarak, herkesin okuyamayacağı bir şekilde kodlanmış bilgiye ise "şifreli metin" (ciphered text) denir (Sunay, 2003).

3.3.3 Bilgisayar Güvenliği

Bilgisayarların ortaya çıkması ve kullanımının yaygınlaşmasıyla hemen hemen tüm veri ve bilgi günümüzde bilgisayar ortamlarında tutulmaya başlanmıştır. Fiziksel güvenlik, haberleşme (iletişim) güvenliğinden sonra bilgisayar güvenliği, bilgi güvenliğinin sağlanması açısından önem kazanmıştır. İlk elektronik bilgisayar geliştirildiğinde, eğitimli kişilerin çok az olması ve bu kişilerin sadece işin gereksinimlerinin yapması dolayısı ile, fiziksel tehditler dışında pek fazla güvenlik problemi ortaya çıkmamıstır. Bilgisayarlar iş dünyasında kullanılmaya basladığında, bilgisayarların güvenliğini korsan saldırıları ve bilgisayarlardan sorumlu olan kişilerin kötü niyetli ve çıkar amaçlı davranışları tehdit etmeye başlamıstır. 1970'li yılların başında David Bell ve Leonard La Padula bilgisayar güvenliğine iliskin bir model geliştirmişlerdir (Bell ve Padula, 1995). 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) olusmasını saglamıstır (Abrams ve Joyce, 1995). Bu kitapta, bilgisayar sistemlerinin güvenliğini test etmek için oluşturulan güvenlik seviyeleri asağıdaki gibi özetlenebilir (Pfleeger, 2006):

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 islemleri, güvenlik olaylarının izlenmesi ve kaynak tahsisiyle kullanıcıların her birinin kontrol edilebilmesini gerektirmektedir.

Etiketlenmis 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 genisletilmeli ve sisteme düzeltme islemleri eklenmelidir.

Onaylanmıs 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 dogru ve güvenilir bir şekilde gerçekleşir.

Günümüzde bazı kurumların bu gibi seviyelerin risk analizi sonucu belirlediği ve buna göre kontroller ve önlemler uygulandığı bilinmektedir (Calder, 2005). 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 cihaz ve ortamlardan oluşmaktadır. Bilgisayar güvenliğini doğal olaylar (deprem, sel, vb.), kazalar (yangın, vb.), hizmet kesintileri (güç kaynağının arızalanması, vb.) ve insan faktörü gibi değisik kaynaklardan oluşan tehditler olumsuz yönde etkilemektedir. Bu tehditler ve zaafiyetler ilerleyen bölümlerde kapsamlı olarak ele alınmıştır.

3.3.4 Ağ (Network) Güvenliği

Ağ (Network) ikiden fazla bilgisayarın birbirleriyle iletişim (kablolu veya kablosuz) halinde olmasıdır. Bu iletişim yanyana iki bilgisayar veya cihaz olabileceği gibi internet üzerinden farklı kıtalardaki iki bilgisayar veya cihaz da olabilir. Ağ ortamlarının temelinde yatan paylaşım ve uzaktan erişim imkânlarının kullanılması sonucunda yeni güvenlik açıkları meydana gelmistir. Bu açıklar, kötü niyetli veya meraklı kişiler tarafından kullanıldığında; bilgilere yetkisiz erişim, sistemler ve servislerin kullanılamaz olması, bilgilerin değiştirilmesi veya açığa çıkması gibi güvenlik ihlâlleri oluşmaktadır. Bilgisayar ağlarının yaygınlaşmasıyla güvenlik ihlâlleri artmış, bilgi güvenliği için alınması gereken önlemler fazlalaşmıştır.

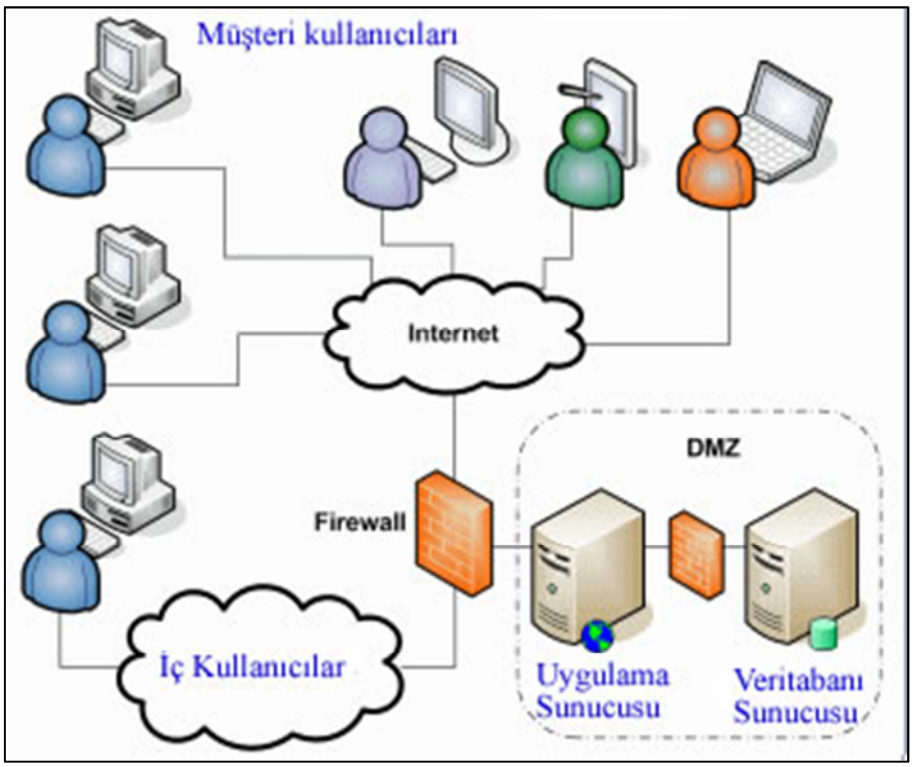
Bilgisayarlar, ağlar aracılığıyla kablolu veya kablosuz olarak birbirleriyle iletişim kurmaktadır. Kablolu ve kablosuz ağ ortamlarının güvenliğinin sağlanmasıyla ilgili farklı çözümler geliştirilmiştir. Bu bölümde öncelikle genel olarak ağ güvenliğinin sağlanmasında aşağıda sıralanan temel çözümler açıklanacak, sonrasında ise kablosuz ağlara ilişkin geliştirilen güvenlik çözümlerinden bahsedilecektir.

- Güvenlik duvarı (Firewalls),
- Saldırı tespit sistemleri (IDS),
- Saldırı önleme Sistemleri (IPS)
- DoS Ataklarını önleme Sistemleri (DoS appliances)
- Kablosuz ağ güvenliği çözümleri
- NAC (Network Access Control-Ağ Erişim Kontrolu) çözümleri

3.3.4.1 Güvenlik Duvarı (Firewall)

Bir ağın dış dünya ile bağlantısı router denilen cihazlar üzerinden yapılmaktadır. Routerlar, dış dünyadan kendisine gelen veya iç ağdan dışa ağa giden paketleri yönlendirmeye yarayan cihazlardır. Bu yüzden, kötü niyetli saldırılara karşı önlem alınacak ilk nokta dış dünya ile

bağlantıyı gerçekleştiren bu cihazlardır. Bu cihazların konfigürasyonlarında çeşitli kısıtlamalar yapılarak adres ve paket analizini yapmazlar. Adres ve paket analizi yapmak, paket geçişlerine izin vermek (permit) veya paketleri engellemek (drop) için güvenlik duvarı (Firewall) kullanılır. Güvenlik duvarı güvenilir ağların (kurumsal ağlar) sınır kısmında filtreleme (denetleme) noktaları oluşturarak, bu denetleme noktalarından güvensiz ağlara (internet) doğru giden veya güvensiz ağlardan gelen ağ trafiğini, kurumsal güvenlik politikalarında belirlenen kurallar (rules) veya filtrelere göre denetleyerek hangi isteklerin kabul (permit) veya red (drop) edileceğine karar veren yazılım veya donanım çözümleridir (Zwicky ve Cooper, 2000). 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 3.3.4.1.1'de verilmiştir.



Şekil 3.3.4.1.1 Güvenlik duvarı genel yapılandırması

Güvenlik duvarları, dış ağlardan (güvensiz ağ- internet) 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 karsı 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 en önemli bileşenlerdir.

3.3.4.2 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. Saldırı Tespit Sistemleri, Internet dünyasının gelişim sürecinde özellikle tüm dünyada kullanılan web trafiğinin artması ve de web sayfalarının popüler hale gelmesi ile birlikte kişisel ya da tüzel sayfalara yapılan saldırılar sonucu ihtiyaç duyulan önemli konulardan biri haline gelmiştir. Bununla birlikte kurum ya da kuruluşların sahip oldukları ve tüm dünyaya açık tuttukları mail, dns, database gibi sunucularının benzeri saldırılara maruz kalabilecekleri ihtimali yine Saldırı Tespit Sistemlerini Internet Güvenliği alanının vazgeçilmez bir parçası haline getirmiştir. Kurumların sahip oldukları çalışan sayısı ve bu çalışanların kendi kurumlarındaki kritik değer taşıyan yapılara saldırabilme ihtimalleri de iç ağın ya da tek tek kritik sunucuların kontrol altında tutulma gerekliliğini beraberinde getirir.

IDS (Intrusion Detection System) genel olarak iki tip olarak karşımıza çıkar; Sunucu tabanlı (host ids)IDS ve Ağ tabanlı IDS.

Ağ tabanlı IDS in görevi, bir kurum yada kuruluşun sahip olduğu ağ yada ağlara yönlenmiş olan tüm trafiği algılayarak, bu ağa doğru geçen her bir data paketinin içeriğini sorgulamak, bir atak olup olmadığına karar vererek kaydını alabilmek, kendisi ya da konfigüre edebildiği başka bir aktif cihaz tarafından atakları kesmek, sistem yöneticisini bilgilendirmek ve ilgili raporlar oluşturabilmektir. IDS bir data paketinin atak olup olmadığını, kendi atak veritabanında bulunan atak tipleriyle karşılaştırarak anlar ve karar verir. Sonuç olarak bir IDS in en önemli bileşeni bu atak veritabanıdır. Söz konusu Atak veritabanı nın içeriği, ne kadar

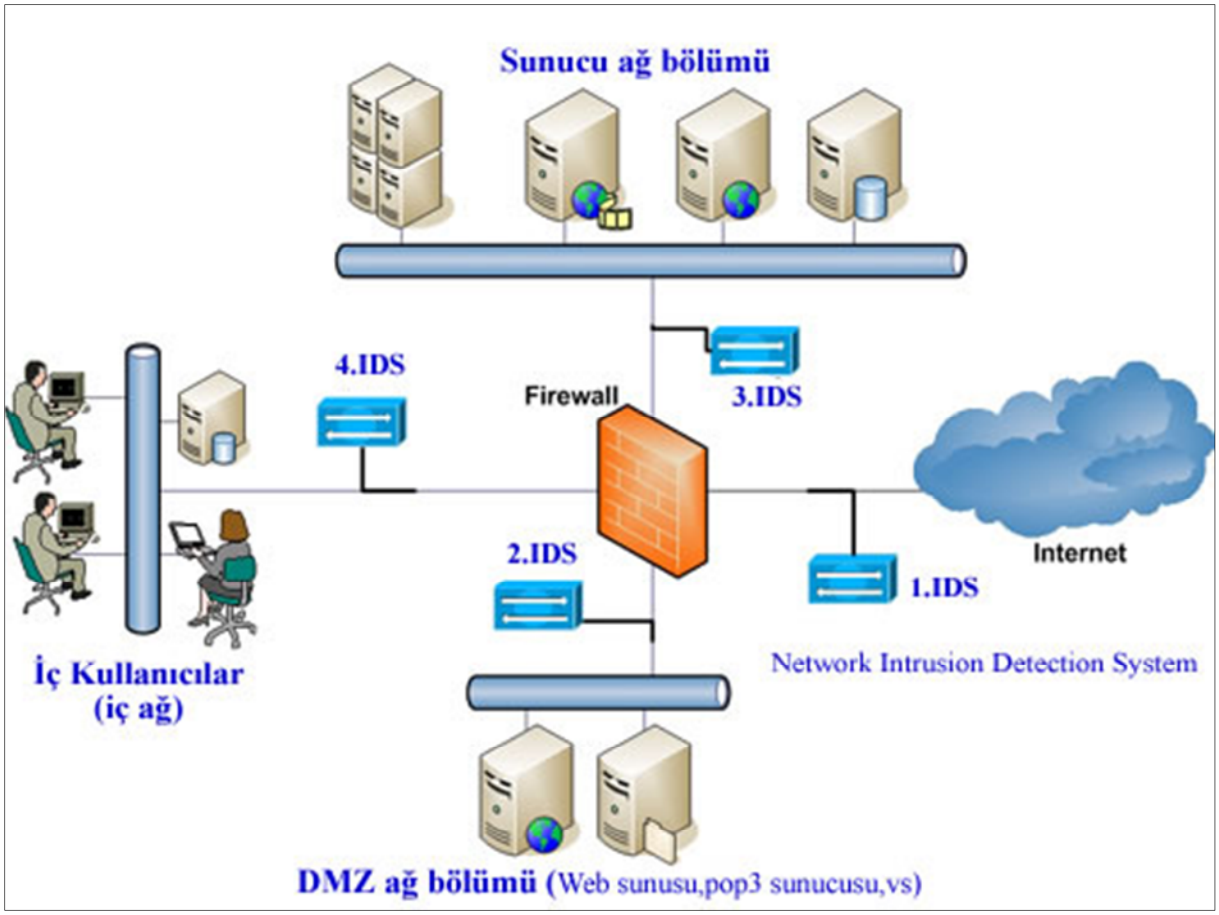
sıklıkla ve doğrulukla güncellendiği ve kimin tarafından oluşturulduğu/güncellendiği en önemli noktadır.

Sunucu Tabanlı IDS in görevi ise kurulu bulunduğu sunucuya doğru yönlenmiş bulunan trafiği yine üzerinde bulunan atak veritabanı baz alınarak dinlemesi ve atakları sezerek cevap vermesidir.

IDS' ler, dinlediği trafiğin kaydını tutarak, gerektiğinde bu kayıtları baz alarak istenilen şekilde raporlar çıkartabilmektedir. Atak sezdiklerinde atakları önleyebilir, yöneticilerine mail yada benzeri yollarla haber verebilirler, önceden oluşturulmuş bir program çalıştırabilir Tüm bu özellikleriyle IDS ler sistemin güvenli bir şekilde işlemesine yardımcı olur ve sistem yöneticilerinin sistemi güçlü bir şekilde izlemesine yardımcı olmaktadırlar.

İmza tabanlı saldırı tespit sistemleri günümüzde yaygın olarak kullanılmaktadır. Antivirüs sistemleri gibi ağ üzerinde yakalanan paketleri inceleme seklinde çalıstıkları için saldırının imza tanımının önceden tanımlanmış olması gereklidir. Bu yöntemin can alıcı noktası, saldırı imza listelerinin sistem tarafından otomatik (Auto Update) olarak güncellenmesinin sağlanmasıdır aksi takdirde güncel saldırılara karşı koruma sağlanamayacaktır.

Kurumsal bilgisayar aşlarında yer alan saldırı tespit sistemine bir örnek şekil 3.3.4.2.1'de verilmiştir.



Şekil 3.3.4.2.1 Saldırı tespit sisteminin genel yapılandırması

Şekil 3.3.4.2.1'de 1.IDS, 2.IDS, 3.IDS,4.IDS üzerinde bulunduğu ağdan olabilecek saldırıları anlamaya çalışacaktır. 1 ve 2.IDS daha çok internet (dışardan) gelebilecek saldırıları tespit edecektir. 3. ve 4.IDS ise daha çok iç ağda olabilecek saldırıları tespit edecektir.

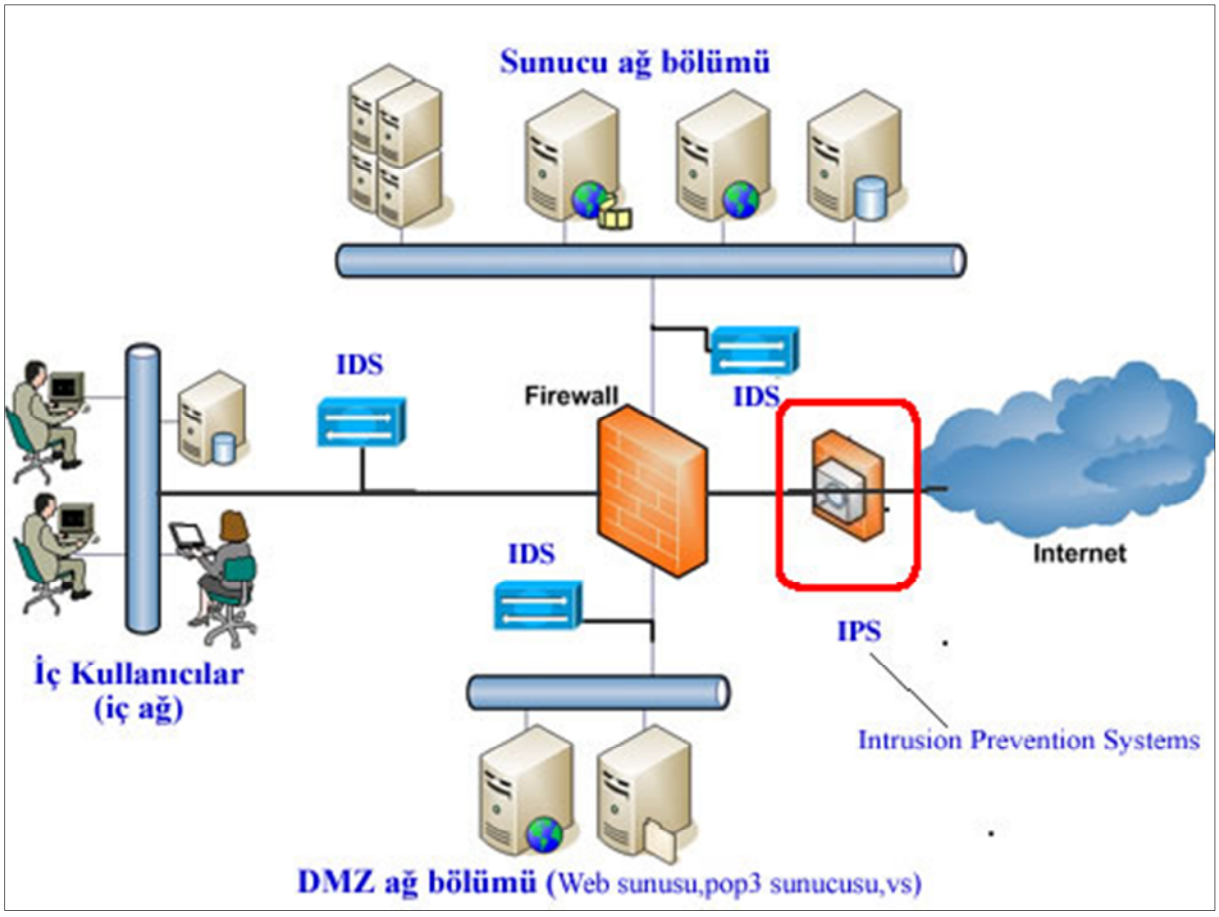
Saldırı tespit sistemlerinin kullanımında en fazla karşılaşılan problemlerden birisi saldırı tespit sistemlerinin sistemdeki normal bir davranışı saldırı olarak tespit etmesidir (False Positive). Bu hatadan dolayı saldırı tespit sistemlerinden beklenen başarı elde edilememektedir. Ancak yinede günümüzde sistem analizini iyi yapan uygulamalar bulunmaktadır.

3.3.4.3 Saldırı Önleme Sistemleri (IPS)

Günümüzde internetten saldırı teknikleri o kadar karmaşık bir hal almıştır ki bazen sadece bir güvenlik duvarı ile bu saldırıları engellemek pek mümkün olmamaktadır. Bu nedenle internetten gelen veri paketlerini inceleyen (Saldırı Tespit Sistemi) bu paketlerdeki veriyi önceki paketlerle karşılaştıran ve saldırı olma ihtimali olan ve belirli bir şablonda gelen

paketlerin geçmesini engelleyecek sistemlere ihtiyaç olmuştur. Bu tip sistemlere Saldırı Önleme Sistemleri (***I**ntrusion **P**revention **S**ystems*) denmektedir [59]. IPS, güvenlik güvarları ile beraber çalışırlar. Güvenlik duvarları geçen paketleri incelemez sadece geçip geçmeyeceğine izin verir, Saldırı Önleme Sistemleri de geçen paketleri inceleyerek zararlı olup olmayacağına karar verir ve buna göre aksiyon alırlar. Hatta günümüzde IPS cihazları güvenlik duvarından önce önde konumlandırmakta olup paketleri inceler. Eğer paketler zararlı kodlar (kurtçuklar, Truva atları, uygulama seviyesi saldırılar, önbellek taşmaları gibi) içeriyorsa IPS, tehditlere karşı kapsamlı koruma sağlamaktadır.

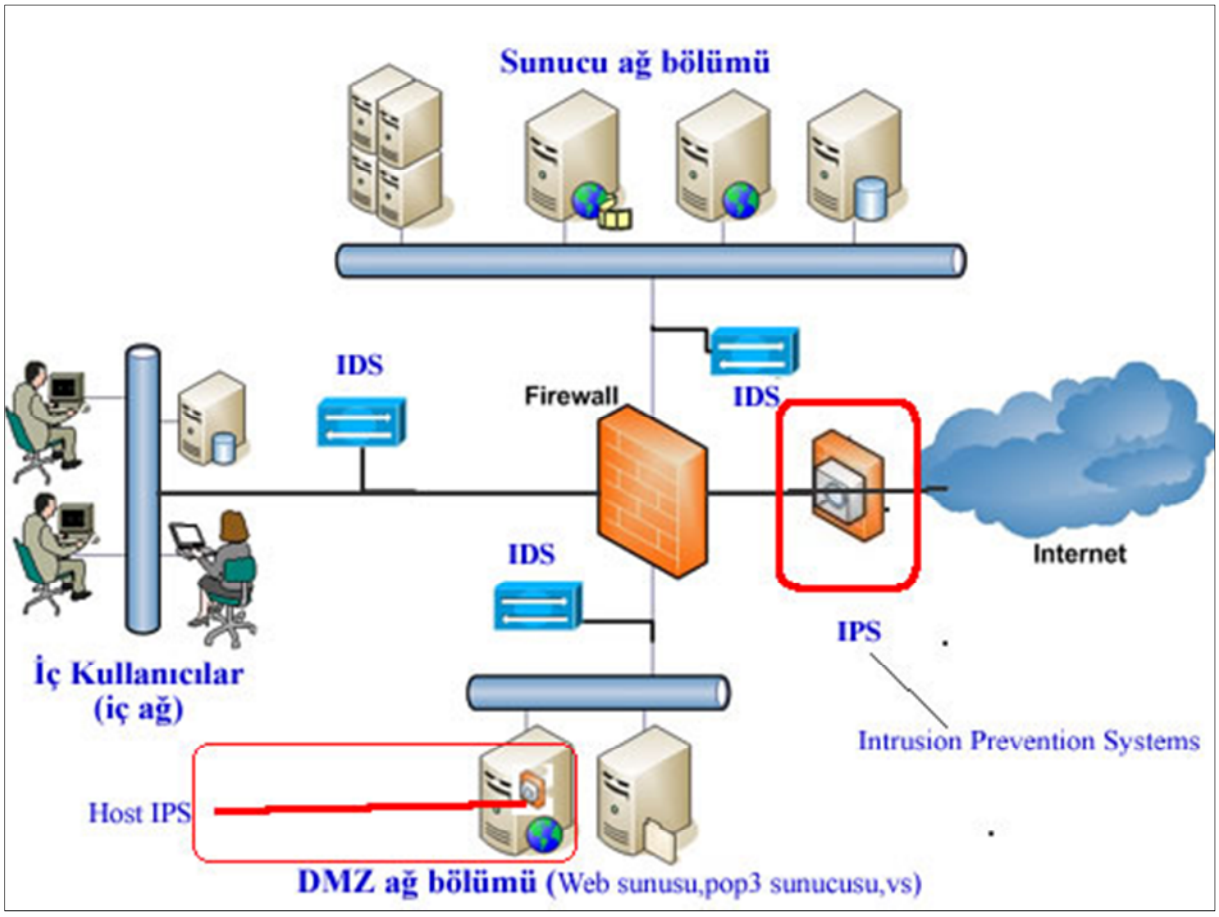
Kurumsal bilgisayar ağlarında yer alan saldırı önleme sistemine bir örnek şekil 3.3.4.3.1'de verilmiştir.



Şekil 3.3.4.3.1 Saldırı önleme sisteminin genel yapılandırması

IPSler içinde bulunduğu ağ ortamının farkında olma özelliği ile, ortamdaki değişikliklere adapte olabilmektedir. Bu da güvenlik yöneticilerinin saldırı önleme sistemi yönetimine ayırmaları gereken zamanı azaltmaktadır.

Kritik uygulamaları çalıştıran sunucular üzerinde saldırı önleme sistemi ayrıca sunucu üzerinde de çalıştırılabilmektedir ve bu sisteme host(client veya terminal) IPS denilmektedir. Bu yapıda daha da güvenli olmaktadır. Şekil 3.3.4.4'de görülen host IPS web sunucusu üzerinden konumlandırılmıştır.



Şekil 3.3.4.4. Terminal (Host IPS) saldırı önleme sisteminin genel yapılandırması

3.3.4.4 DoS ve DdoS Atakları Önleme Sistemleri (DoS Appliance)

DoS(Denial of Service) ve DDoS (Distributed Denial of Service) saldırısında internetteki bir bilgisayar veya bir ağın aşırı yük yoğunluğu sayesinde hizmetinin durdurulması veya servis dışı kalsmasıdır.Bu CPU, RAM veya Ağ donanimi normalinden çok daha fazla bir şekilde kullanılması sonucu ile bilgisayar işlevini doğru bir şekilde yerine getiremez olur yada çöker.

Bugüne kadar gerçekleşmiş en büyük DDOS saldırısının, 6 Şubat 2007 tarihinde 2,5 saat sürdüğü belirtilen bu saldırı sonucunda, 6 DNS server içerisinden 2'sinin etkisiz hale getirildiği ve dünyadaki internet erişiminde büyük uzun süre boyunca büyük sorun yaşandığı açıklanmıştır (Gaudin, 2007). Bu saldırıların daha hizmet veren bilgisayarlara gelmeden kesilmesi saldırı önleme sistemleri (IPS) ile kesilebilmektedir. Ancak aşırı yok yoğunluğu sonucu IPSLer de devre dışı bırakılabilir. Bu yüzden daha perdormanslı ve sadece bu DoS saldırılarından anlaması için programlanan ve buna göre donanım içeren cihazlar son zamanlarda üretilmektedir. Bu cihazlara Dos Appliance adı verilmektedir. İçinde Anormal trafiği anlayan dedektörleri barındırılan bu cihazlar olası bir DDoS saldırısı varlığını tespit edebilir ve ve gerçek zamanlı olarak zararlı trafiği bloklar (Davis, 2005).

3.3.4.5 NAC Ağ Erişim Kontrolü

NAC, Network Access Control kelimelerin kısaltmasından oluşup Türkçe "ağ erişim kontrolü" olarak çevilebilir. NAC bir donamım veya yazılımdan ibarettir. NAC'ın amacı ağa bağlanacak terminallerin güvenlik kriterlerine ve tanımlanan politikalara(policy) göre dahil dahil etmek veya bloklamaktır.

Sayıları günden güne artan güvenlik açıkları, virüsler, solucanlar, casus yazılımlar ağlar için büyük sorunlar oluşturuyor ve her yıl şirketlerin milyonlarca dolar zarar etmelerine neden oluyor. Bu durum sadece bu tehditleri önlemek için oluşturulan koruma sistemlerinin maliyetleri olarak algılanmamalı, herhangi bir şekilde bu tehditlerin ağ içerisinde ortaya çıkması durumunda yaşanan iş gücü kaybı ve vereceği zararlarda hesaba katılmalıdır. Cisco Systems'ın önderliğini yaptığı ve güvenlik alanında önde gelen şirketlerin desteklediği Network Admission Control (NAC) çözümü ağların karşı karşıya oldukları tehlikeleri en aza indirmeyi amaçlıyor [13].

Geleneksel güvenlik teknolojileri bu tehditler karşısında zaman zaman engelleyici çözümler sağlayamıyor ve ağ üzerinde bu gibi tehditlerle zaman zaman karşılaşılabiliyor. Bu gibi durumlar için daha iyi bir alternatif çözüm oluşturan NAC teknolojisi ağ altyapısını kullanarak kullanıcıların gerekli güvenlik politikalarına uyup uymadıklarını kontrol ederek ağları tehlikelerden koruyor [14].

NAC'ın amacı ağ kaynaklarına erişmek isteyen cihazların bu istekleri sırasında kurumsal güvenlik politikalarına uygunluğunu belirlemek ve uygun olmayan cihazların uygunluğunun

sağlanarak virüs, solucan ve casus yazılım gibi tehditlerin yaratacağı zararları sınırlamaktır. NAC sadece güvendiği ve uygunluğu belirlenmiş uç cihazların (Masaüstü, dizüstü, avuç içi bilgisayarlar, sunucular vs) ağa erişimine izin verir ve bunun dışındaki sistemlerin erişimini kısıtlar.

3.3.4.6 Kablosuz Ağ(wireless) Sistemleri

Son yıllarda özellikle ADSL ve DSL (daha çok amerika kıtasında kullanılır) hizmetinin genişlemesi ile birlikte kablosuz ağ destekli modemlerin kullanımı da artmıştır. Bu tip modemlerdeki kablosuz ağ özelliğinin sağladığı esneklikler ve kolay kullanımı ve düşük maliyeti sayesinde artık her işyerinde ve her evde bir kablosuz ağ oluşmaya başlanmıştır. Kablosuz ağlarda kurumlarda kullanılan kablolu ağlardan farklı bazı önemli noktalar vardır. 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 (Gürkas vd, 2005). Kimlik doğrulama mekanizması olmayan WEP algoritması, kablosuz ag güvenliğini sağlamada (bütünlük, gizlilik) sonradan yapılan iyilettirmelere rağmen başarısız olmustur. 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. 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 (Edney ve Arbaugh, 2003).

WPA2 şuan bulunan en güncel güvenlik standardıdır. Kablosuz ağların standartlaşması çerçevesinde WPA, IEEE (Institute of Electical and Electronic Engineers) tarafından 802.11i ismiyle geliştirildi. WPA'nın güzel tarafı AES (Advanced Encryption Standard) şifreleme standardını kullanıyor olmasısır. Bunu yaparken de doğal olarak 128, 192 veya 256 Bit şifreleme yöntemini kullanmaktadır. WPA ve WPA2 temel olarak birbirleri ile uyumlu; bu yüzden baz istasyonları bir karışık mo içinde çalıştırılabilmektedir.

Kablosuz Ağların Güvenliği:

Son yıllarda özellikle ADSL hizmetinin genişlemesi ile birlikte kablosuz ağ destekli modemlerin kullanımı da artmıştır. Bu tip modemlerdeki kablosuz ağ özelliğinin sağladığı esneklikler ve kolay kullanımı sayesinde artık her evde ve kurumda bir kablosuz ağ oluşmaya başladığını görülmektedir. Özellikle fiyat/kullanım özelliği oranındaki başarım kablosuz ağların yaygınlaşmasında önemli rol oynamıştır. Teknolojiye direnmek mümkün değildir. Avantajlarından "zarar görmeden" maksimum seviyede yararlanmayı her kişi ve kurum ister.Ancak bu sistemleri ve açıklarının iyi bilmek gerekmektedir. Kablosuz ağların çalışma mantıkları, güvenlik açıkları ve korunma yolları üzerinde durmak gereklidir.

Kablosuz ağlarda en çok kullanılan güvenlik opsiyonları aşağıdaki gibidir:
Open Security,

- WEP,
- WPA,
- WPA2 (en kullanılan yöntemdir.)
- RADIUS / WPA-RADIUS,
- Wireless Gateway.

Open Security, open security olarak geçen güvenlik modeli şifre gerektirmeyen bağlantı demektir. Aslında bu bir güvenlik modeli değildir. Yani herhangi biri bu kablosuz ağlara asitçe bağlanabilir.

WEP, Açık anahtar (şifre) kullanan modeldir. Kablosuz ağların güvenliğini sağlamak için kullanılır. Geliştirilmesine rağmen çok büyük açıkları bulunmaktadır. Açık anahtarı(şifre) bulmak kolaydır.

WPA/WPA2, Yine açık bulunan ancak WEP' e göre çok daha güçlü bir şifre yapısına sahiptir.

WPA (Wi-Fi Protected Access- Wi-Fi Korumalı Erişim)

WPA kablosuz ağlar için geliştirilmiş bir şifreleme standardıdır. Bu standart daha önceki WEP (Wired Equivalent Privacy- Kabloya Eş Güvenlik) sisteminin yetersizliğine karşılık geliştirilmiştir. WPA, veri şifreleme ve kullanıcı kimlik denetimi alanlarında bilgi güvenliği sunmaktadır. WPA, veri şifreleme işlemini geliştirmek için bu konuda yeni bir yöntem sunarak şifreleme anahtarlarını otomatik olarak dağıtır. Bir bit veri bile şifreleme

anahtarlarıyla korunur. Bu çözüm aynı zamanda, veri üzerinde bütünsel bir kontrol yaparak, verileri ele geçirmek isteyen kişilerin bilgileri değiştirmesini engeller. WPA, kurumsal kullanıcıların korunması için, ağ üzerindeki her bir kullanıcıya kimlik denetimi uygularken, bu kullanıcıları veri hırsızlığı amacıyla düzenlenmiş ağlara geçişini de engeller. WPA, IEEE 802.11i taslak standardının bir altkümesidir. 802.1x EAP (Extensible Authentication Protocol-Genişletilebilir Kimlik Doğrulama Protokolü) ile Değişken Anahtar Dağıtım (Dynamic Key Distribution) şekillerini Michael doğrultusunda birleştirmiştir [15].

WPA2 (Wi-Fi Protected Access 2)

WPA2, WPA'nın devamı niteliğinde kablosuz ağlar için geliştirilmiş bir güvenlik metodudur. IEEE 802.11.x standardına dayanır. WPA2 girişimciye ve müşteriye sadece yetkili kişilerin ağlara girebilmesi konusunda büyük bir güven vermektedir. WPA2'nin iki sürümü mevcuttur: WPA2-Personal (kişisel) ve WPA2-Enterprise (girişimci). WPA2-Personal yetkisiz kişilerin ağlara girişini bir kurulum şifresi kullanarak engellemeyi amaçlar. WPA2-Enterprise ise ağ kullanıcılarını bir sunucu yardımıyla denetler (Cache ve Liu, 2007).

WPA-WPA2 Personal, WPA ve WPA2 kişisel sürümü ev ve küçük ofisler gibi kimlik doğrulama sunucuları olmayan kullanıcılar için tasarlanmıştır. Kimlik doğrulama için IEEE 802.1X yerine önceden paylaşımlı bir şifre kullanır. WPA-WPA2 kişisel sürümü WPA-WPA2 Enterprise sürümü ile aynı şifreleme yöntemlerini kullanır. WPA , TKIP yoluyla WPA2 ise AES yoluyla kullanıcı, oturum, paket başına şifrelemeyi destekler.

WPA-WPA2 Enterprise, WPA, WPA2 personal ile aynı şifreleme özelliklerini desteklemektedir.

WPA-WPA2 ile ağ saldırılarından korunma

WPA ve WPA2 kablosuz ağı korsan saldırılara, zayıf şifrelere, kullanıcılarla ilgili saldırılara karşı korur. WPA, WEP'in hatalı şifreleme anahtarından kaynaklanan zayıflıkları belirler. WPA ve WPA2 ile birlikte TKIP ve AES şifrelemeleri geliştirildiği için saldırılar ve saldırılardan etkilenme olasılığı en aza indirgenmektedir (Vacca, 2006).

RADIUS, Bağlantı kuran istemci (client) bir bilet (ticket) sistemi ile kablosuz ağa bağlanır. Ortak bir server olduğundan doğru implemantasyonda gayet güvenli bir kablosuz ağ deneyimi sağlayabilir. Ancak ev kullanıcıları ya da küçük organizasyonlar için çok kullanışsızdır. **RADIUS-WPA** ise aynı sistemin WPA desteklisidir.

Wireless Gateway, Özellikle halka açık yerlerde kablosuz ağ sunan firmaların kurduğu sistemlerdir. Ağ ile kablosuz cihazlar arasında bir bağlantı noktası oluşturur, giren kişiler bu sistemden bir defa onay aldıktan sonra ilgili kota ve ayarlara göre gerçek ağa (internet) erişebilirler. Ülkemizde TTNet' in sunduğu TiWinet kablosuz internet erişimlerinde de bu metod kullanılır.

Ağ güvenliğinin sağlanması için aşağıdaki kuralların uygulaması yerinde olacaktır [16]:

1. Kurumsal ağ kaynaklarınızı iç ve dış tehditlere karşı korumak: Günümüzde kurumlar için yerel ağ kavramı artık, iç ağ/dış ağ ayrımı yapılmaksızın, kurumdaki herhangi bir kişiye, herhangi bir yerden erişebilmek anlamında genişlemiştir. Ama bu gelişime paralel olarak, güvenlik uzmanları da ağlarına karşı olan tehditlerle başa çıkabilmek için daha komplike güvenlik politikaları uygulamak zorunda kalmaktadır. Bu tehditleden en başta geleni, önemli ağ kaynaklarını Internet'ten veya yerel ağdan gelebilecek muhtemel saldırılara karşı korumaktır.

Ağ üzerinden erişim kontrolü, mevcut ağ kaynaklarını korumak için temel yoldur. Ölçeklenebilir kapsamlı erişim denetimi kuralları sayesinde, ağ güvenliği yöneticileri ağ bağlantıları için kaynak sistem, hedef sistem, ağ trafik türü ve uygulama zamanını belirlemek suretiyle esnek ağ erişim hakları belirleyebilirler.

Ağ güvenliğini korumak tabi ki sadece spesifik kaynaklara erişim denetimi sağlamaktan ibaret değildir. Bundan başka, komple bir ağ güvenliği çözümü aşağıdakileri sağlamalıdır:

- Ağ kullanıcıların kimliklerinin belirlenmesi,
- Aktarım esnasında veriyi şifreleme,
- Kayıtlı IP'leri optimize şekilde kullanma,
- Ağ trafiğinin tümünün içeriğine güvenlik politikasını uygulama,
- Saldırıları gerçek zamanlı olarak belirleme ve önlem alma,
- Denetim bilgilerinin tümünün kayıtlarını tutma.

Ayrıca güvenlik politkası, kurum içerisinde kullanılan mevcut ve ileride kullanılması muhtemel bütün uygulamalara tatbik edilebilmeli ve bağlantı sorunlarına, ağ performans düşüklüklerine yol açmamalıdır.

2. Mobil ve uzak kullanıcılar için ağ bağlantısı sağlamak: Birçok şirket uzak kullanıcılarının bağlantıları için, büyük modem bağlantıları gerektiren geleneksel uzaktan erişim çözümleri ve pahallı dial-up telefon bağlantıları ile karşılaştırıldıklarında çok ekonomik çözümler sunan Internet üzerinde geliştirilen ağ uygulamalarının farkına vardılar. Uzak ve mobil kullanıcılarını kurumsal ağlarına Internet bazlı özel sanal ağlar (VPNler) aracılığı ile bağlamak isteyen firmaların sayısı arttıkça, bu kritik bağlantıların güvenliğinin sağlanması da büyük önem kazanmıştır.

Bilgilerinizin Internet gibi herkese açık ağlar üzerinden iletimi sırasında güvenliğinden emin olabilmek için iki temel unsurun yerinde uygulanması gerekir. Birincisi, hem uzak istemci, hem de kurumsal Internet ağgeçidi seviyesinde mümkün olan en güçlü tanılama sağlanmalıdır. İkincisi ise, bütün kullanıcı kimlikleri belirlendikten sonra, bütün veri trafiği gizlilik açısından şifreli olarak iletilmelidir.

Hem tanılama hem de şifreleme uygulamaları, ağ güvenlik çözümü çerçevisinde kesintisiz ve uyumlu olarak çalışmalıdır. Erişim denetimi gibi ağ güvenlik kriterleri sanal özel ağ iletişimlerinde de çok önemli role sahiptir. Uzak bir kullanıcının VPN ile kurumsal ofisine bağlantı kurması demek, buradaki tüm ağ kaynaklarına erişim hakkı kazanması anlamına gelmemelidir.

Bir firma için uzak ağ bağlantı ihtiyacı arttıkça, ağ güvenlik yöneticileri yönetilebilir ve kullanımı kolay VPN çözümlerine ihtiyaç duyarlar. Ve seçilecek çözüm, kurulumu kolay, ileride eklenebilecek yüksek sayıda uzak kullanıcı sayısını destekleyebilecek esneklikte, son kullanıcı için ise kesintisiz ve transparan olmalıdır.

3. Internet'i kullanarak kurumsal veri iletişim masraflarını düşürmek: Güvenli ağ erişimi sağlamak amacıyla istemciler ve ağlar arasında kurulan VPN bağlantıları pahalı çözümler oldukları için, firmalar uzak ofis bağlantılarını sağlamak için Internet aracılığı ile ağlar arası veya bölgeler arası VPN bağlantılarını tercih ederek tasaruufa giderler. Ayrıca herkese açık hatlar üzerinden güçlü tanılama ve veri şifreleme özellikleri kullanarak, bilgi güvenliğinden ödün vermeksizin ticari iletişimleri de sağlamak mümkün olur. Bu sayede, frame-relay ve kiralık hatlara yüksek miktar yatırımlar yapmaya gerek de kalmaz.

Gözden kaçırılmaması gereken bir konu ise, uzaktan erişim çözümü olarak güçlü tanılama ve şifreleme teknolojileri seçildiği vakit, bu seçimin beraberinde yeni güvenlik yönetimi

zorlukları getirebilmesidir. Bu tip muhtemel zorlukları yaşamamak veya minumum seviyeye indirgemek için, tüm VPN bağlantı noktalarını merkezi bir konsol aracılığı ile yönetebilecek güvenlik çözümleri tercih edilmelidir.

Internet üzerindeki VPN uygulamalarının sağladığı maliyet düşüklüğünün yanı sıra, ağ iletişimlerini özel dedike hatlardan Internet üzerine taşınması, beklenmedik performans düşüklüklerine ve erişim sorunlarına yol açabilir. Bu yüzden, sanal özel bir ağ bünyesinde öncelikli bağlantılar için entegre bantgenişliği yönetimi ve yüksek erişilebilirlik desteklenmelidir.

4. Güvenli bir extranet üzerinden iş ortaklarına ağ erişimi sağlamak: Kendinize ait ağ kaynaklarınızı (uzak ve mobil kullanıcılar, branch ofisler) güvenli şekilde birbirine bağladıktan sonra, sıra kurumsal ağınızı extranet uygulamaları aracılığı ile değerli iş ortaklarınıza ve müşterilerinize kontrollü bir biçimde açmaya gelir. Endüstri standartlarında protokollere ve algoritmalara bağlı kalarak gerekli extranet bağlantıları güvenli şekilde sağlanabilir. Ama bu tür bağlantılar için kesinlikle tescilli teknolojiler tercih edilmelidir.

Internet bazlı VPN uygulamaları için kabul edilen standarda IPSec (Internet Protocol Security) adı verilir. IPSec, şifrelenmiş ve tanılanmış bir IP paketinin formatını ifade eder ve gelecek nesil IP iletişimi için gereklidir. Şifrelenmiş anahtarların yönetimini otomatikleştirmek için genellikle IPSec ile IKE (Internet Key Exchange) ile kullanılır.

Standart bazlı bağlantı kurulduğu zaman, dışardan erişecek kullanıcıların (iş ortakları, özel müşteriler) ihtiyaçlarına göre özel haklar sadece ilgili ağ kaynakları için tanınmalıdır. Kurumsal ağ kaynaklarının dışarıya açılma oranı arttıkça, bununla ilgili uygulanması gereken kapsamlı güvenlik politikası da periyodik olarak revize edilmelidir.

5. Kurumsal ağınızın yeterli performans, güvenilik ve yüksek erişilebilirliğe sahip olması : Kurumsal ağ bağlantılarında artan Internet kullanımının doğal sonuçlarından biri olan ağ tıkanıklıkları sonucu kritik uygulamalarda performans sorunları yaşanabilir. Ortaya çıkabilecek bağlantı hataları, ağgeçidi çökmeleri, ağ bağlantı gecikmeleri ve diğer performans düşüklükleri neticisinde firmalar büyük ekonomik kayıplar yaşayabilirler.

Internet ve Intranet hatlarının gereğinden fazla istemci ve sunucu tarafından kullanılması sonucu, trafik miktarına göre bağlantı kopuklukları, zayıf ‘response’ zamanları ve yavaş Internet kullanımı sorunları ile karşı karşıya gelmek normaldir. Bu gibi durumlarda, sınırlı

bantgenişliği üzerinde mevcut hattı aktif olarak paylaştırmaya yönelik bir yönetime gidilmelidir.

Eğer yerel ağınız bünyesinde yoğun trafik yaşanıyorsa, birçok kaynağınız (halka açık popüler bir Web sunucusu gibi) negatif yönde etkilenebilir. Bir uygulama için bir sunucuya güvenmek, zayıf 'response' zamanlarına hatta bağlantı kopukluklarına yol açabilir. Sunucu yük dengelemesi bir uygulama sunucusunun işlevini birçok sunucu üzerine dağıtarak ölçeklenebilir bir çözüm sağlar. Bu yolla ayrıca, sunucular üzerindeki performanslar da arttırılmış olur.

Performansın yettiği durumlarda dahi, ağgeçidi seviyesinde meydana gelebilecek bir hatayı tolere edebilecek güvenli bir ağ altyapı sistemi oluşturulmalıdır. Günümüzde artık çoğu kurum, ağgecidinde yaşayacakları anlık erişim sorunları yüzünden dahi büyük mali kayıplar yaşaycaklarından emin olarak yüksek erişilebilirliği destekleyen ağ güvenlik ürünlerini tercih etmektedir.

Yüksek erişilebilirliği destekleyen ürünler hem yazılım, hem donanım bazında yedeklemeli sistemler ile yüzde yüze yakın seviyelerde erişilebilirliği garanti ederler. Bir sorun meydan geldiği zaman, yüksek erişilebilirliği sağlayan bileşenler ağınızın güvenli olmasını sağlamalı ve son kullanıcıya tamamen transparan şekilde devam ettirilmelidir. Gerçek etkili çözümler sunacak ağ yöneticileri, iç ve dış kullanıcılarına daimi güvenilir servisler sağlamalıdır.

6. Kullanıcı bazında güvenlik politikalarını ağ seviyesinde uygulamak : Kurumsal ağ konseptinin genişlemesi, birçok ağ için kullanıcı, uygulamalar ve IP adres kullanımı sayılarında aşırı artışlara yol açmıştır. Bu tür dinamik ağ ortamlarında emniyetli ağ politikalarının uygulanması, kullanıcı bazında güvenlik politikalarının oluşturulmasıyla sağlanır. Bu politikalar çerçevesinde, ağ kullanıcıları için kişisel erişim denetimleri, tanılama prosedürleri ve şifreleme parametreleri belirlenir. Yüksek miktarda kullanıcı bilgisi içeren bu uygulamalarla uğraşmak ağ ve güvenlik yöneticileri için bazen kolay olmayabilir.

Kullanıcı seviyesinde güvenlik bilgilerini ölçeklenebilir şekilde merkezi bir yerde depolamak için LDAP protokolü kullanmak en uygun çözümdür. LDAP sayesinde, bütün kullanıcı bilgileriniz tek bir veritabanında tutulup diğer ağ uygulamaları tarafından paylaşılır. Bununla birlikte ağ ve güvenlik yönetimleri paralel çalışarak güvenlik ile ilgili zaman harcatıcı rutin prosedürlerin aşılması sağlanır.

Güvenlik denetimlerini en üst düzeyde tutmak için kullanıcı seviyesinde uygulanan güvenlik politikaların kayıtlarının tutulması ve bunların denetlenmesi gerekir. Kişisel güvenlik politikalarının uygulandığı ortamlarda DHCP protokolünün kullanılması etkili bir yol değildir. Bunun sebebi IP adres atamalarının dinamik olarak yapılmasıdır.

7. Ağınıza karşı yapılan atakları ve şüpheli aktiviteleri anında algılamak ve bunlara cevap vermek: Kurumsal ağ güvenliğinizi ancak ağınızı ve kullanıcılarınızı korumak için uyguladığınız güvenlik politikaları belirler. Ağ korumanızı devamlı olarak ayakta tutmanın yolu yetkisiz aktiviteleri gerçek zamanlı olarak tespit etmektir.

Etkili bir saldırı tespit sistemi, atak ve şüpheli ağ aktivitelerini yetkin bir şekilde tespit ederek kurumsal ağ güvenliğinizin bir bacağını oluşturur. Ama bu istenmeyen trafiğin sadece saptanması yeterli değildir. Kullandığınız saldırı tespit uygulaması öte yandan belirlenecek bu tür istenmeyen bağlantılara anında yanıt verebilmeli ve ağ kaynaklarına yetkisiz erişimi engellemelidir.

İyi dizayn edilmiş bir saldırı tespit uygulaması, gerçek zamanlı karşılıklara ek olarak kapsamlı kayıt tutabilme, komple denetim ve gerektiğinde ilgili kişileri ikaz edebilecek gelişmiş uyarı mekanizmalarına sahip olmalıdır.

8. Ağınızın IP adres altyapısını güvenli ve etkili bir biçimde yönetmek :Ağlar üzerindeki kullaınıcı ve uygulama sayısı arttıkça, ağ cihazları ve kullanıcıları için gereken IP adres adres sayısı gittikçe daha çok artmaktadır. Buna paralel olarak da hızlı gelişen ağlarda IP adres ve isim alanı yönetimi zorlaşmaktadır.

Eskisi gibi her bilgisayar ve ağ cihazının IP adres konfigürasyonunu manuel olarak kontrol etmek artık uygulanmamaktadır. Bunun sebebi, bu tip bir yönetimin günümüz ağları üzerinde hataya açık, zahmetli ve entegrasyon eksikli bir yapı oluşturacak olmasıdır. Böyle bir yapı da doğal olarak çok pahalı olmasının yanında, merkezi kontrol, ölçeklenebilme ve güvenilirlikten uzak olacaktır.

Kurumsal bazlı IP ağ altyapınız için merkezi idare ve esnek yönetim sağlayan IP adres yönetim çözümleri ancak genel ağ altyapısı ile tamamen entegre olduklarında güvenlik politikaları için optimum kullanılmış olurlar. Daha spesifik olmak gerekirse, dinamik paylaşımlı dahi olsalar, mevcut IP adreslerini kullanıcılara birebir olarak eşlemek kullanıcı bazlı daha güçlü çözümler yaratmayı sağlayacaktır.

9. Entegrasyona yönelik açık platform güvenlik çözümleri kullanmak :Ağ güvenlik yöneticileri, korudukları ağ üzerinde kullanacakları yazılım uygulamaları ve ağ altyapısında kullancakları donanımları baş döndürücü bir devinim içinde gelişen bilişim teknolojileri pazarından seçmektedirler. Bu noktada dikkat edilmesi gereken husus, bütün ürünlerin birbirleri ile teknik olarak entegrasyon sorunu olamaksızın yüksek performans ile çalışması gerekliliğidir.

Alternatif olarak, seçeceğiniz çözümleri geniş yelpazede çalışan üretici tek bir firmadan temin edebilirsiniz. Bu sayede ürünlerin sistemleriniz üzerinde entegrasyon sorunu olmadan çalışacağından emin olabilirsiniz ama bu aşamada da tercih edebileceğiniz uygulama sayısında daralma yaşarsınız. Bütün güvenlik ihtiyaçlarınızı temin edebilecek spektrumda hizmet veren tek bir üretici firma bulmanız pek muhtemel değildir.

Ağ güvenliği için tercih edeceğiniz çözümler neler olurlarsa olsun, hepsinin seçiminde açık mimari platformu destekleyecek çözümler olmalarına dikkat edilmelidir. İyi tanımlanmış arayüzlere sahip açık bir mimari, genel güvenlik politikası çerçevesinde kullanılacak bütün ürünlerin birbirleri ile sorunsuz çalışmasını sağlayacaktır. Buna ek olarak size özel ağ güvenlik ihtiyaçları yaratmanız için uygulama programlama arayüzleri (API'ler) kullanılabilirsiniz.

10. Güvenli bir ağa sahip olmanın maliyet ve zahmetlerini azaltmak :Kurumsal ağınızın güvenliğini sağlamak için, seçtiğiniz çözümleri yönetecek ve denetleyecek kişilere önemli miktarda ücret ödemek durumundasınızdır. Bu yüzden bu kişilerin işlerini, entegre konsollar üzerinden merkezi olarak idare edebilecekleri çözümler tercih edilmelidir. Böylelikle büyük bir kurumsal ağ için dahi, tek bir kişi ağ güvenlik yöneticisi olarak ağ güvenliği denetimi yapabilir. Bundan başka güvenlik politikasında meydana gelecek çözümleri bütün uygulama noktalarına hemen aktarmak gerekir.

3.3.5 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, transfer halindeki bilgilerin güvenliğinin sağlanması için iletişim güvenliğinin, bilgisayarlarımıza erişimin kontrol altına alınması için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir. Bilginin güvenliğinin yüksek seviyede sağlanabilmesi için yukarıda açıklanan güvenlik türlerinin tamamının organize bir şekilde uygulanması gerekmektedir. Bilgi güvenliği ile ilgili literatürde çesitli tanımlamalar yapılmıstır.

Bu tanımlardan bazıları aşağıdaki 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 (Canbek ve Sağıroğlu, 2006).

Bilgi güvenliği, yetkisiz erişim ve kullanım, açığa çıkarma, yok etme, deşistirme, bozma gibi saldırı tehditlerinden verilerin korunması sürecidir [17].

Bilgi güvenliği, Bilginin bir varlık (asset) olarak ele alınması ve olası hasarlardan korunması olarak tanımlar (Çağlayan, 2003).

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 (Iso, 2005).

Bilgi güvenliği, kurumsal BT (Bilgi Teknolojileri) kaynaklarının erişilebilirlik, bütünlük ve gizliliği üzerindeki risk etkilerinin azaltılarak disiplinize edilmesidir (Solms, 2006).

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 sürekliliği sağlamak, iş hasar ve zararlarını asgari düzeyde tutmak ve yatırım geri dönüşü ve getirilerini ve iş fırsatlarını azami düzeye çıkartmak amacıyla, bilgiyi çok çesitli tehditlere karşı korur (Tioia, 2006).

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 sürecine bilgi güvenliği olarak tanımlanabilir.

Bilgi güvenliğinin sağlanmasında uyulması ve uygulanması gereken birçok güvenlik bileşeni vardır. Öncelikle üç ana ilke olan gizlilik, bütünlük ve erişilebilirlik(kullanılabilirlik) ilkelerine uyulması sonrasında da bu ilkelere ek olarak değerlendirilebilecek giriş kontrolü, emniyet, inkâr edememe, güvenirlik, kayıt tutma, kimlik tespiti gibi ilkelere uyulması bilgi güvenliğinin üst düzeyde sağlanmasına yardımcı olur (Çağlayan, 2003).

Bilgi güvenliği tanımlayan bileşenleri açıklamakta yarar vardır:

Gizlilik(Confidentialy):

Elektronik ortamlarda bulunan veya taşınan bilginin; yetkisi ve izni olmayan kişiler veya süreçler tarafından elde edilmesinin 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 anlasılmasını veya çözülmesini zorlaştıracak yaklaşımlar kullanılarak bulunan veya taşınan bilgi çözülemeyecek başka bir formata dönüştürülür. Gizlilik ilkesinin sağlanmasında şifreleme algoritmaları ve steganografi yöntemleri kullanılmaktadır (Sağıroğlu ve Tunçkanat, 2002; Sağıroğlu vd,2002; Yerlikaya vd, 2006).

Bütünlük (integrity):

Bilginin göndericiden çıktığı haliyle bozulmadan bir bütün olarak alıcısına ulaştırılmasını garanti eden bir güvenlik unsurudur. Bilgi iletişim sırasında geçtiği yollarda değiştirilmemiş,eksiltip çoğaltılmamış şekilde alıcısına ulaştırılarak bütünlüğü sağlanır. Bilginin bütünlüğünün garanti edilmesi için hashing (özetleme) algoritmaları kullanılmaktadır.

Erişilebilirlik(Kullanılabilirlik- Availability):

Gerktiği zaman bilgiye kullanıcıların yetkisi dâhilinde zamanında erişimine imkan verilmesi olarak tanımlanabilir. Erişilebilirlik bilişim sistemlerini kullanan kişiler veya süreçler tarafından büyük bir önem taşımaktadır.

Kayıt (Log) tutma:

Bilişim sistemlerinde gerçekleşen olayların daha sonra analiz edilmesi ve hukuki olaylara kanıt teşkil etmesi için işlemlerin kayıt altına alınması olarak tanımlanabilir. Kullanıcının parolasını yazarak sisteme girmesi, veritabanlarından bir bilgi çağırması, web sayfasına bağlanması, eposta göndermesi veya alması gibi örnekler kayıt altına alınması gerekenolaylara örnek olarak verilebilir.

Kimlik tespiti (kanıtlama ve doğrulama- Identity):

Bilişim sistemlerinden hizmet alan alıcının, iddia ettiği kişi olduğundan emin olunması olarak tanımlanabilir. Örneğin, giriş izniniz olan herhangi bir elektronik ortama eriştiginizde 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 gelmistir. Akıllı kartlar, tek kullanımlık parolalar (one time password), elektronik imza kartları, biyometrik teknolojiler kimlik tespitinde kullanılan teknolojilerden bazılarıdır.

Güvenirlik (reliability):

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 çalıstırıldığında da aynı sonuçları vermesi olarak tanımlanabilir.

İnkâr edememe(nonrepudiation):

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 ve e-devlet bilgi sistemlerinde yoğunlukla kullanılmaktadır. Pratikte inkâr edememe unsuru elektronik imza ve açık anahtar altyapısı kullanılarak sağlanmaktadır.

Giriş kontrolü (Erişim listeleri-Access Control):

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.

4. KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ

Dünyada ve Türkiye'de yüksek seviyede kurumsal bilgi güvenliğinin sağlanmasında önemli bir rol oynayan güvenlik yönetim sistemleri ve bilgi güvenliği standartları bu bölümde açıklanmıştır.

Bilgi güvenliği ve yönetimi ile ilgili kabul gören uluslararası standart ve çerçevelerin başlıcaları aşağıdakilerdir (Shahim, 2009).

- ISO 27001,
- ITIL,
- COBIT,
- PCI DSS,
- HIPAA,
- CMMI,
- PRINCE2,
- BS25999

Bu standart, çerçeve (Framework) ve rehber (Guideline) arasında bilgi güvenliğini ön planda tutan standart, yeni adı ile ISO /IEC[†] 27001'dir. Standartlaşma konusuna önderlik eden İngiltere standart enstitüsü tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799 sonrasında ise ISO/IEC 27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir [18].

Bu kapsamda yukarı adı geçen standartlar hakkında kısa bilgi verilecek ve ülkemizde de en çok kullanılan ve hatta elektornik imza yasasında geçen ISO/IEC 27001 standardının detayları bölüm 4'de detaylıca incelenecektir.

4.1 ITIL

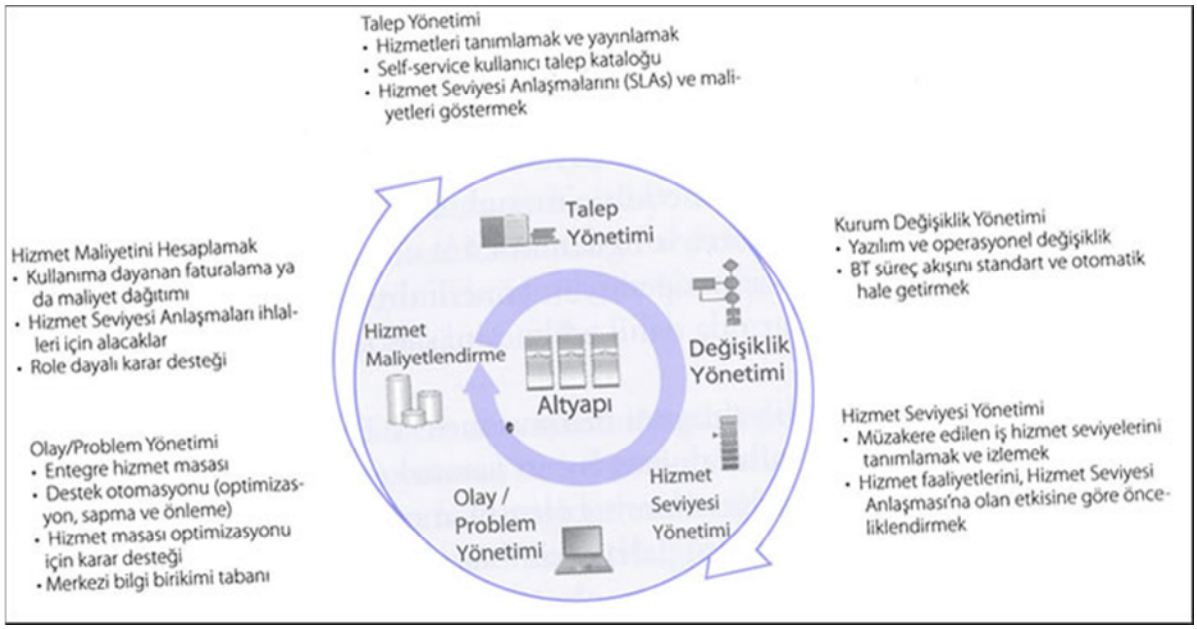
ITIL(Information Tehnologies Infrastructure Library) en iyi uygulamaların (best practices) ve deneyimlerin bir araya getirilmesi ile oluşturulmuş bir kütüphanedir. Ancak şuanda kütüphane olmaktan çıkıp BT yönetim metodoloji olmuştur.

[†] IEC: International Electrotechnical Commission

ITIL; 1980'li yılların sonlarında, İngiltere Ticaret Bakanlığı tarafından başlatılan, Bilgi Teknolojileri altyapı ve hizmet süreçlerinin standartlaştırılması çalışmaları ile ortaya çıkan bir kütüphanedir. Standartların belirlenmesi aşamasında oluşturulan yordamlar zamanla bir kütüphaneye dönüşmüştür. 1990'lı yılların başlarında, özellikle Avrupa ülkelerinde, pek çok büyük şirketin ve kamu kuruluşunun ITIL standartlarını benimsemesi ve kendi bünyelerinde uygulamaya başlaması ile ITIL, tüm dünyada kabul edilen bir endüstri standardı durumuna gelmiştir. ITIL temel şeması şekil 4.1.1 de verilmiştir (Johnson ve Higgins, 2007).

ITIL, IT altyapı ve hizmet süreçlerinin nasıl olması gerektiğinin anlatıldığı ve gerçekleştirilmiş en iyi örneklerden yola çıkılarak standartların tanımlandığı bir süreç ve yordam kütüphanesidir.

ITIL yordamlarında; IT hizmetlerinin, bir bütün olarak, maksimum kalitede, düzende, ve süreklilikte yürütülmesi, kurumların iş hedefleri ile maksimum seviyede uyumlu hale getirilmesi ve müşteri beklentilerinin en iyi biçimde karşılanması için hizmetlerin nasıl bir yapıda yürütülmesi gerektiği konularına yönelik süreçler ve yordamlar tanımlanmaktadır.



Şekil 4.1.1 ITIL genel süreci (Johnson ve Higgins, 2007)

ITIL, operasyonel bilgi işlem hizmetlerinin verimli ve etkin bir şekilde yürütülmesi için geliştirilmiş kalite yönetim metodolojisidir. ITIL operasyonel hizmetlerin, uçtan uca bütünleşik süreçler olarak yürtülmesinde esas alınacak ilkelere açıklık kazandırır. ITIL'ı uygulayan firmalar BT servislerinde gözle görülür bir iyileşme elde etmişlerdir. Genelde bu

iyileşmeler hizmet seviyesi kalitesinin yükselmesi, erişebiliriliğin artması, doğru kapasite planlamasının yapılarak maliyetlerin kontrol altına alınması gibidir.

ITIL metodolojisi küçük yada büyük ölçekli bütün firmalara uygulanabilir. Asıl işi bilgi teknolojileri olmayan firmalarda bilgi işlem bölümleri genellik harcama yapan bölüm olarak algılanır. Bu birimlerin yaptığı işin kurum hedefleri doğrultusunda yapıldığının yolu ITIL gibi süreçlerin oturtması ile bilgi teknolojilerine para harcayan bir müdürlük veya birim imajından çıkarabilir. Asıl hedefin hizmetlerin ölçülebilir olması , süreçlerle yönetim ve iş tarafı ile aynı olduğunun göstergesi olarak kullanılabilir.

ITIL'ın genel olarak amaç ve faydalarını aşağıdaki şekilde sıralayabiliriz.

- Maliyetleri düşürmek,
- Erişilebilirliği arttırmak,
- Kapasiteyi ayarlamak,
- İş gücünü arttırmak,
- Kaynakların verimli kullanılmasını sağlamak,
- Ölçülebilirliği artırmak,
- Yüksek kalitede bilgi teknolojileri hizmeti vermektir.

ITIL'ın Sürümü, ITIL, 1985, 2001 ve 2007 yılında olmak üzere 3 sürüm halinde yayımlanmıştır (Malone vd, 2009).

4.2 COBIT

COBIT, kelime olarak Control Objectives for Information and related Technology kelimelerinin kısaltmalarından oluşturulmuşdur. Cobit, türkçe olarak "Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri" olarak tanımlanabilir[19].

Cobit, ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından 1996 yılında geliştirilmiş, Bilgi Teknolojileri Yönetimi için en iyi uygulamalar kümesidir. COBIT yöneticilere, denetçilere ve Bilgi Teknolojileri (BT) kullanıcılarına iş hedeflerinin bilgi işlem hedeflerine dönüşümünü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirirken, aynı zamanda bilgi teknolojileri alt yapılarını da etkin kullanmayı sağlar.

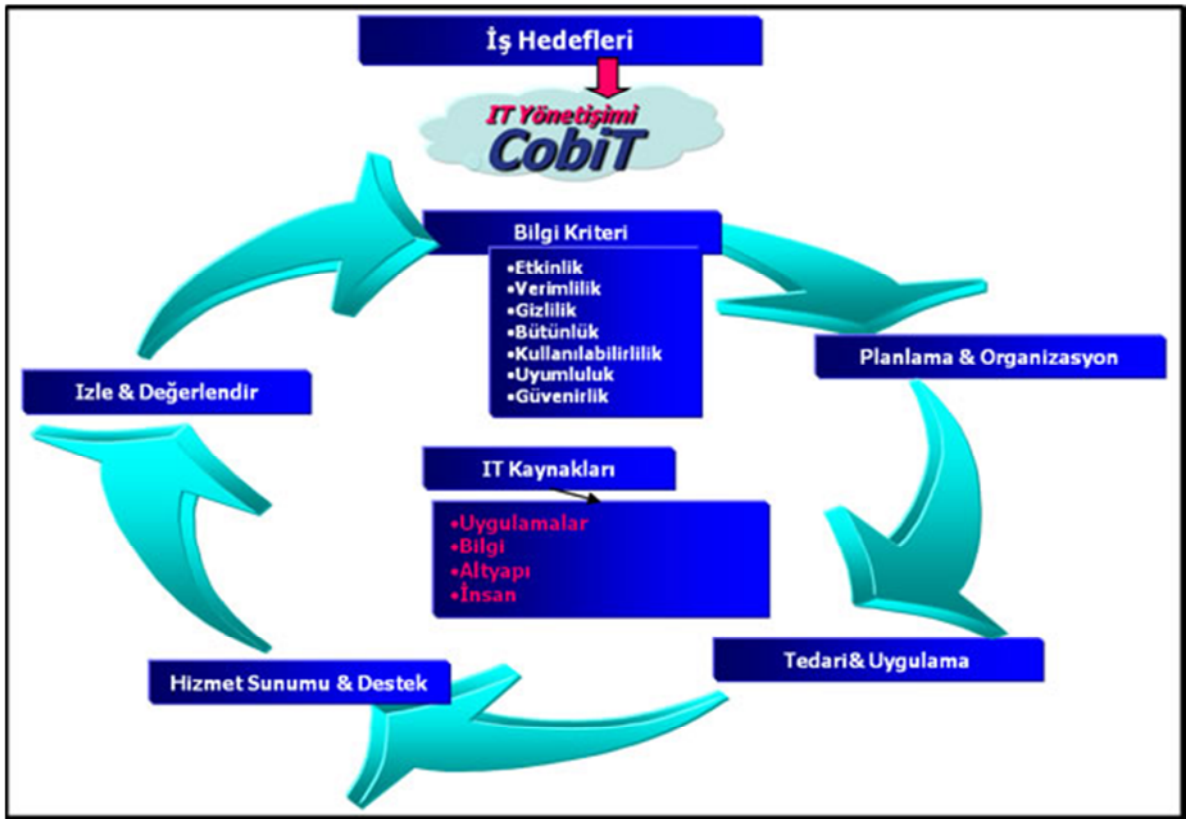
Kısaca bilgi teknolojileri yönetişimi için sunulmus bir modeldir. Bir standart değil, bir referansdır. Bircok standartı özümsemiş, örneklemiş ve en iyi uygularını içerisine sindirmiştir. CobIT kurumumun iş (Bussiness) gereksinimini destekleyen bir aractır. İş ve bilgi teknolojileri yönetimi arasındaki köprü görevini gören bir metodolojidir. CobIT kurum hedeflerine bilgi teknolojileri alt yapılarını etkin kullanarak ulaşmayı sağlayan bir araçtır [20].

CobIT'in mevcut 4.1 sürümü 4 ana alan (domain) ve34 farklı sürece ilişkin kontrol hedefleri barındırmaktadır.

CobIT de 4 ana domain aşağıdaki gibidir:

1. Planlama & Organizasyon,
2. Tedari & Uygulama,
3. Hizmet Sunumu & Destek,
4. Izle & Değerlendir

Bu domainlerin kapsadığı süreçler aşağıdakişekilde gösterilmiştir.



Şekil 4.2.1 COBIT ana süreci

4.3 PCI DSS

PCI DSS (Payment Card Industry Data Security Standard- Ödeme Kartları Endüstrisi Veri Güvenliği Standardı), kartlı ödeme sistemlerinde veri güvenliğini sağlamak amacıyla uluslararası kabul görmüş ödeme markaları olan American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. International kurumlarınca oluşturulmuş PCI Komitesi tarafından geliştirilmiştir.

PCI DSS, kartlı ödeme sistemlerinde yer alan kurum ve kuruluşlarda bilgi güvenliğini sağlamak için bilgi sistemlerinde bilgi iletimini, bilgi işleyişini ve bilgi depolamayı esas alan 6 temel kriter baz alınarak oluşturulmuş 12 gereksinim kategorisi ve bu kategoriler altında yer alan 200 üzerindeki kontrolden oluşmaktadır [21].

PCI DSS kapsamına, kart çıkaran ve kabul eden tüm bankalar, ödeme kartlarını kabul eden tüm perakendeciler ve kart ve işlem verilerini kendileri için saklayan veya ileten tüm hizmet sağlayıcıları girer. Bunun yanında bankalar, temsil ettiği perakendeciler ve iş yaptığı tüm üçüncü şahısların bu standarda uyumlu olmalarının sağlanmasında da sorumlu bulunmaktadırlar.

PCI DSS uyumu kontrolleri için gerek banka, gerek perakendeciler, gerekse hizmet sağlayıcılarla ilgili kriterler VISA ve MasterCard kuruluşlarının web sitelerinde detaylandırılmıştır.

PCI DSS yararları: Günümüz koşullarında bilgi güvenliği her türlü işletmede, özellikle kartlı ödeme sistemlerinde dikkate alınması gereken hassas bir konudur. PCI DSS içeriğindeki 12 kategori ile kart bilgisini taşıyan, işleyen ve saklayan kurum ya da kuruluşların bilgi güvenliğine uyum süreçlerini yönetmekte ve bu kurum ya da kuruluşlarda bilgi güvenliği disiplininin oluşmasına katkıda bulunmaktadır. Kartlı ödeme sistemi içerisinde yer alan kurum ve kuruluşlarda gerek kart kabul eden, gerek kart çıkaran gerekse kart işlemlerini çalıştıran tarafların her hangi birinde bilgi güvenliğinin sağlanmadığı durumda kart bilgilerini açığa çıkma olasılığı nedeniyle bu sistem içerisinde yer alan diğer kurum ve kuruluşlarda da güvenlik riski oluşmaktadır. PCI DSS uyumu ile kartlı ödeme sistemleri içinde yer alan tüm kurum ve kuruluşların veri güvenliği riski en aza inebilecektir.

PCI DSS uyumu, PCI DSS uyumu kontrolleri, VISA ve MasterCard kuruluşlarınca belirlenmiş kriterler doğrultusunda PCI DSS uyumu için gerekli PCI Council tarafından

onaylanmış yetkili firmalar (Approved Scanning Vendor - ASV) tarafından; ya uzaktan yapılan güvenlik tarama testleri (Vulnerability Scan) ya da hem vulnerbility scan hem de standarddaki 12 gereksinim kategorisi altında yer alan 200'den fazla kontrol için hazırlanmış olan güvenlik değerlendirme prosedürleri (Security Assessment Procedures) baz alınarak yapılan yerinde denetimler ile gerçekleştirilmektedir (Özinal, 2009).

4.4 HIPAA

Hippa, Health Insurance Portability and Accountability Act demektir. Sağlik kurumlarının hastaların gizli sağlık belgelerinin gizliliğini, güvenliğini ve standartlarının korunması için elektronik işlemlerde belli normlarda uyulmasını şart koşan Amerika'da 1996 yılında çıkan bir yasadır. Önemli olan noktaları tüm hasta ve sağlık kurumlarının datalarının gizliliği, tuturlığının sağlanması ve bu bilgileri izinsiz erişimlere karşı korunmasını temin etmektir ve güvenliğini sağlamaktır (Beaver ve Herold, 2005).

4.5 CMMI

CMMI (Capability Maturity Model Integration Yetenek Olgunluk Model Entegrasyonu), bir süreç modeli olup, örgütlerin yazılım süreçlerinin (Yazılım planlama, geliştirme, yapılandırma vb.) olgunluğunu değerlendirme modelidir. CMMI, Carnegie Mellon Üniversitesi'ne bağlı Yazılım Mühendisliği Enstititüsü tarafından Amerikan Savunma Bakanlığı'nın isteği üzerine 1986 yılında geliştirilmeye başlanmıştır.

CMMI , kurumlara süreçlerini iyileştirme konusunda gereken temel adımları gösteren bir süreç iyileştirme yaklaşımıdır. Ne yapılması gerektiğini açıklar. Nasıl sorusuna kesin bir cevap vermez. Bu yaklaşım bir projeye, bir kuruma ait departmana ya da büyük bir organizasyona süreçlerini iyileştirme ve geliştirme konusunda rehberlik eder. Olgun olmayan bir süreçten olgun ve disiplinli bir sürece giden evrimsel bir yol çizer. Ortaya konulan seviyelere göre olgunluk gelişimi sağlanır. Her olgunluk modelinin kendine özel sürecleri bulunur. Boylece sürekli bir iyileşme söz konusu olur. CMMI, geleneksel yapıda ayrı olan organizasyonel fonksiyonların entegre edilmesine, süreç iyileştirme için gerekli hedef ve önceliklerinin belirlenmesine, kalite süreçleri için kılavuz oluşturulmasına ve mevcut süreçlerin değerlendirilmesi için bir referans noktası oluşturulmasına yardım eder.

CMMI, dünyada ve Türkiye'de daha çok IT sektöründe ve özellikle yazılım geliştirme yapılan kurum, departman ve projelerde, yazılım kalitesini arttırmak için kullanılan bir referans model

olarak uygulanmaktadır. Donanım ve network alanlarında da uygulanan model, özellikle savunma sanayi başta olmak üzere; Ar-Ge ve yeni ürün geliştirme konusunda hizmet veren kurumların aradıkları bir standarttır (Atasever, 2007).

4.6 PRINCE2

PRINCE, İngilizce "PRojects IN Controlled Environments" ifadesinin kısaltılmış halidir. Metot 1970′li yıllardan bugüne geliştirilmektedir. Çıkış noktası bilgi teknolojilerinde proje yönetimi olsa da, 1996 yılında tüm proje türlerinde kullanılmak üzere genelleştirilmiş ve PRINCE2 adını almıştır. En son, Haziran 2009′da güncellenmiştir.

PRINCE2 proje yönetimi metodolojisi olup proje yönetimindeki metodolojilerin en yaygınıdır. PRINCE2 proje yönetimi metodolojisi olarak iyi tanımlanmış süreçlere, proje süresince gözetilmesi gereken prensiplere sahiptir. Bunun yanında, proje yönetimi ile ilgili roller ve sorumluluklar tanımlanmış, proje süresince üretilecek proje yönetimi çıktıları (risk-sorun kayıtları, durum raporları, iletişim planı vb) için de şablonlar ve kullanım kılavuzu içermektedir.

ITIL ve PRINCE2 arasında aynı kurum tarafından geliştirilmiş olmaları ve kendi alanlarında en iyi uygulamaları içermeleri dışında kavramsal olarak pek ilişkileri yoktur (Borman, 2009).

4.7 BS 25999

BS 25999 İş sürekliliği yönetimi (BCM- business continuity management) standardı olup İngiliz standard enstitüsü tarafından geliştirilmiştir [22].

Bu standart, bir BCM sisteminin temellerini uygulamaya koymanıza yardımcı olarak en zorlu ve en beklenmedik durumlarda bile işlerinizin devamını sağlamak, çalışanlarınızı korumak, itibarınızı sürdürmek ve faaliyetlerinize ve ticari etkinliklerinize devam etmenize yardımcı olmak için tasarlanmıştır.

BS 25999, İş Sürekliliği Yönetimi işlemlerini, prensiplerini ve terminolojisini oluşturmak için endüstrinin farklı sektörlerini ve yönetimi temsil eden, dünyanın en iyi uzmanlarından oluşan bir grup tarafından geliştirilmiştir.

BS 25999, her sektörden büyük küçük tüm kuruluşlar için uygundur. Finans, telekomünikasyon, ulaşım ve kamu sektörü gibi yüksek risk içeren ortamlarda faaliyet

gösteren ve faaliyetleri sürdürmenin kuruluşun kendisi, müşterileri ve hissedarları için hayati önem taşıyan kuruluşlar için özellikle gereklidir.

BS 25999, iki bölüm halinde geliştirilmektedir:

•Bölüm 1 olan Uygulama Kurallari yayınlanmış ve bu sadece rehber niteliği taşıyan bir dokümandir.

•Bölüm 2 olan Spesifikasyon, İş Sürekliliği Yönetim Sistemi için en iyi uygulamalara ait gereklilikleri sağlar. Standardin bu bölümü uygunluğun kanıtlanması amacıyla tetkik ve belgelendirme kriteri olarak kullanılabilmektedir (British Standard, 2005).

5. ISO/IEC 27001:2005 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

5.1 ISO/IEC 27001:2005 Standardı

İlk olarak İngilizler tarafından 1995 de geliştirilen BS 7799 adındaki ilk İngiliz standardı olup bilgi güvenliği yönetimi standardı olarak tarihe geçti Ancak uluslararası bir standart niteliğinde değildi. Daha sonra BS 7799-1 ve BS 7799-2 olarak yayımlandı. Daha sonra ISO trafından ele yeniden revizyonlarla ISO 17799 Standartı olarak yayımlandı. Bilgi güvenliği standardı olan BS 7799-2'nin revize edilip 2005'in sonlarında **ISO/IEC 27001:2005** olarak değiştirilmesiyle yürürlüğe giren bu standart kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlamaktadır (Iso, 2005).

Tarihçesi aşağıdaki gibidir.

- BS 7799-1: Şubat 1995'te ilk yayınlandı,
- BS 7799-2: Şubat 1998'te ilk yayınlandı,
- BS 7799-1 ve -2: 1999'da revizyonu yapıldı,
- ISO 17799: Kasım 2000'de yayınlandı,
- BS 7799-2:2002 yayınlandı,
- ISO 27001:2005 yayınlandı ve halen yürürlüktedir.

ISO 27002 uygulama rehberi olarak olarak yayımlandı. ISO 27005 'de Risk Yönetimi rehberi olarak yayınlandı. Ancak Belgelendirme ISO 27001:2005'e göre yapılmaktadır (Calder, 2006).

Bu standard, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. Süreçlerinin güvenliğini sağlamayı hedefleyen bir bilgi güvenliği standardıdır. İşin içinde sadece bilgisayar, bilişim güvenliği yoktur. Bunların yanında, kâğıttaki dokümanların güvenliği, her tür sürecin güvenliğini de kapsar.

Bunun yanı sıra ISO 17799:2002 numaralı standart ISO 17799:2005 "bilgi teknolojileri güvenlik teknikleri en iyi uygulamalar rehberi" olarak revize edilip yayınlanmış ve ISO 27001'e göre kurulacak bir BGYS'nin nasıl gerçekleştirilebileceğine dair açıklamaları içerir.

Yani ISO 27001:2005 bilgi güvenliği yönetim sistemi standardır ve ISO 27002:2005 ise bir uygulama rehberidir ve bu rehber ISO 27001:2005 nasıl uygulanacağını izah eder.

Ülkemizde de bu standart gelişimi paralel çalışmalar ve çeviriler Türk Standartlar Enstitüsü(TSE) tarafından yapılmıştır. Bu standard, ISO tarafından kabul edilen, ISO/IEC 27001 (2005) standardı esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubu'nca hazırlanmış ve TSE Teknik Kurulu'nun 02 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek yayımına karar verilmiştir. Bu standardın kabulü ile TS 17799-2 iptal edilmiştir (Tse, 2006).

5.1.1 Bilgi Güvenliği Yönetim Sistemi (BGYS)

Bilgi güvenliğini sağlamak, planlamak, tasarlamak, gerçekleştirmek, işletmek, izlemek, denetlemek, sürdürmek ve geliştirmek için, riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak tanımlanmaktadır (Iso, 2005).

Günümüzde bilginin önemi iyi niyetli veya kötü niyetli kullanıcını düşünüldüğünde 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 kurumların üst yönetimine işin içine katan ve üst yönetimde destek alan 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, bilgi güvenliği farkındalık eğitimlerin verilmesi, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçeklestirilmesi anlamına gelmektedir.

BGYS'nin kurumlara saglayacağı faydalar ana hatlarıyla aşağıda belirtilmektedir (Tbd, 2005). Bunlar;

- Bilgi varlıklarını ihtiyaca en uygun şekilde koruma altına alması,
- Bilgi varlıklarına yönelik tehditlerden koruyarak iş sürekliliği sağlaması,
- Tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması,
- Kurumsal saygınlığın korunması,
- Uluslararası temsillerde kurumsal bilgi güvenliğine verdiği önemi kolayca anlayabilmesi,
- Bilgi kaynaklarına erişimin denetlenmesi,

- Üçüncü taraflarla yapılan çalışma ortamından kaynaklanacak risklerin tanımlanması,
- Kurumun risk bilincine katkıda bulunması,
- 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,
- Çalışanların, müşterilerin ve yüklenicilerin görevlerini yerine getirirken, bilgi sistemleri kaynaklarını kötü amaçlı olarak kullanma ve/veya kaynakları suistimal etmelerinin engellenmesi,
- Personelin, baskaları tarafından yapılabilecek olan suistimal ve tacizlere karşı zan altında kalmasının engellenmesi,
- Yasalara, düzenlemelere, sözleşme şartlarına uyumma zorunluluğunun getirmesi,
- Kuruma rekabet avantajı sağlaması,
- Kurum imajina olumlu etki etmesi,
- 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 bir daha tekrar etmemesi için iyileştirme sürecinin olması olarak sıralanabilir.

Kurumsal bilgi güvenlik politikalarının oluşturulması, BGYS kapsamının belirlenmesi, risk yönetim metodolojisinin belirlenmesi, denetim kontrollerinin seçilmesi, düzeltici ve önleyici faaliyetleri için politikaların oluşturulması, uygulanabilirlik beyannameleri gibi unsurlar BGYS kurulabilmesi için, yapılması gereken adımlardır (Humphreys, 2007). Bilgi güvenliğinin yönetiminin kurulmasında izlenmesi gereken adımlar bu bölümde sırasıyla takip eden baslıklarda açıklanmıştır.

5.1.1.1 Kurumsal Bilgi Güvenliği Politikaları

Bilgi güvenliği 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 (Arnason ve Willett, 2008). 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 çalısanların uymaları gereken kuralları içeren resmi bir belge niteliğindedir.

Bilgi güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından da benimsenmelidir. En tepede kurumun ana bilgi güvenliği politikası olup bu politika, kullanıcılar tarafından uygulanabilir ve anlaşılabilir, güvenlik yöneticileri tarafından yönetilebilir kısa ve öz olmalıdır. Bilgi Güvenliği Politikası kurumda bilgi güvenliğine yön veren temel dokümandır. Bu doküman, kurumun tüm paydaşları tarafından erişilebilen ve bilinen bir doküman olacaktır. Bu nedenle, politikayı yazarken, dikkat edilmesi gereken ilk konu, politikanın kısa, öz ve anlaşılabilir olmasıdır. Politika çok uzun olursa, kurum kullanıcıları tarafından okunmayacaktır. Politika, tüm kullanıcılar tarafından anlaşılır ve net olmalıdır; teknolojik terimlerin kullanılmasından da mümkün olduğunca kaçınılmalıdır. Bilgi güvenliği politikası kurum çalışanları tarafından uygulanması beklenen bir politikadır. Politikanın gerçekçi olması önemlidir. Uygulanması zor veya imkânsız ifadelere yer verilmemelidir (Barman, 2001).

Iso 27001 standardında göre kurumsal bilgi güvenliği ana politikaları, kuruluşların ihtiyaçları doğrultusunda temel güvenlik ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) ve risklerin kontrol altına alınacağını beyan eden ifadeleri içermelidir (Calder, 2005).

Örneğin bir internet servis sağlayıcının bilgi güvenliği ana politikası şöyle olabilir:

“Şirketimizin tabi olduğu yasal mevzuat çerçevesinde, başta müşteri ve çalışanlarımızın bilgileri olmak üzere, ilgili tüm bilgi varlıklarımızın belirlenen risklerini kontrol altında tutarak gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamaktır. Bu doğrultuda amacımız, bilgi güvenliği yönetim sistemimizi, çalışanlarımızın katılım, katkı ve uyumları ile sürekli geliştirip iyileştirmektir.”

Bu tepedeki bilgi güvenliği ana politikasını destekleyen alt politikalar olabilir. Politikalar 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.

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 bölümden oluşmalıdır.

Belli konularda çalışanların daha fazla bilgilendirilmesi, dikkat etmesi gereken hususlar, ilgili konunun detaylı bir şekilde ifade edilmesi istendiğinde alt politikalar geliştirilmelidir. Örneğin kullanıcı şifre yönetim politikası, unutma, şifre değiştirme, yeni şifre tanımlama gibi durumlarda uyulacak kurallar alt politikalar aracılığıyla açıklanmalıdır.

Bir başka örnek ise, e-posta gönderme ve alma konusunda, şirket yönetimin kararlarını, haklarını, kullanıcının uyması gereken kuralları alt politika içerisinde ifade etmek daha uygun olacaktır. Bu alt politikayla şirket yönetimin, gerekli gördüğünde çalışanlarının şirket işleri için kullandığı 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.

Alt politikalar aşağıdaki örnekler verilebilir.

- Erişim politikası,
- Yedek alma politikası,
- Şifre yönetim politikası,
- Kullanıcı tanımlama politikası
- Antivirüs politikası,
- İnternet kullanım politikası,
- Ağ yönetim politikası
- Uzaktan erişim politikası,
- Fiziksel güvenlik politikası
- Sunucu kurulum politikası.

5.1.1.2 Bilgi Güvenliği Yönetim Sistemlerinin Kapsamı

Bilgi Güvenliği Yönetim Sistemleri (BGYS) kapsamına dâhil edilecek bilgi varlıkları kurumların belirlediği ihtiyaçlar doğrultusunda tespit edilir. BGYS'nin kapsamı ve sınırları belirlenmelidir. BGYS'nin kapsamı kurumun belli bir kısmı olabileceği gibi, kurumun bütünü de olabilir. Ancak, her iki durumda da, kurumun BGYS kapsamını ve sınırlarını eksiksiz ve doğru bir biçimde tanımlaması gerekmektedir Kapsamlar aşağıda gösterilen kategorilerde sınıflandırılabilir (Landoll, 2006).

- Kurumun sahip olduğu bilgi sistemlerinin tamamı,
- Bilgi sistemlerinin bir kısmı,
- Belli bir yerleşim birimindeki bilgi sistemleri (Merkez bina, Genel
- Müdürlük, A kampüsü vb.),
- Odaklanılmış bir bilgi sistemi (bilgisayarlar, ağ sistemi, sunucu bilgisayarlar, web sunucusu, vb.) olabilir.

Önerğin bir bir finans kuruluşunda müşteri verisi ile ilgili bir kapsam şöyle olabilir:

Finans Port uygulması kapsamındaki yatırımcı kayıtlarını korumak ve güvenli bir ortamda saklamak amacıyla Bilgi Güvenliği Yönetim Sistemi kurulmuştur.

5.2 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 için Uygulama Prensipleri Türk standardı olarak kabul edilmistir. 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 Subat 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 (Tbd, 2005).

TS ISO/IEC 27001:2006 standardı, tüm kuruluş türlerini kapsar. Bu standart, bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçeklestirmek, izlemek, gözdengeçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçeklestirilmesi için gereksinimleri belirtir. Bu standart ISO/IEC 27001:2005 standardından yararlanarak hazırlanmıstır. ISO/IEC 27001:2005 standardın tercümesidir. Dünyada ve ülkemizde belgelendirme konusunda yapılan çalışmalar bir sonraki bölümde anlatılmıştır.

5.3 BGYS'de Belgelendirme Hazırlık ve Başvuru

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 değistirilmiştir. 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 gerçeklestirilmiştir. Ancak, bu süre içerisinde yayınlanmış olan yeni bir BS 7799–2:2002 sertifikasının, Nisan 2007 tarihine kadar ISO/IEC 27001:2005'e geçişi tamamlanmıştır. Nisan 2007 tarihinden sonra bütün denetimler ve belgelendirmeler ISO/IEC 27001:2005 standardına göre gerçekleştirilmiştir.

Kurumların ISO/IEC 27001 sertifikası almasının avantajları aşağıda maddeler halinde listelenmiştir [23].

- İç denetimlerinizin bağımsız bir şekilde sağlandığını gösterir ve kurumsal yönetişim ve iş devamlılığı gereksinimlerini karşılar,
- Geçerli yasa ve düzenlemelere uygun davranıldığını bağımsız bir şekilde gösterir,
- Yasa ve Sözleşmeden doğan gereklilikleri karşılayarak ve müşterilerinize bilgilerinin güvenliğine gösterdiğiniz özeni göstererek bir rekabet avantajı sağlar,

- Bilgi güvenliği işlemleriniz, prosedürleriniz ve belgeleriniz biçimlendirilirken kurumsal risklerinizin gerektiği gibi tanımlandığını, değerlendirildiğini ve yönetildiğini bağımsız bir şekilde doğrular,
- Üst yönetiminizin bilgilerinin güvenliğine olan taahhüdünü kanıtlar,
- Bilgi güvenliği farkındalık eğitimleri ile çalışanların bilgi güvenliği bilincini canli tutar,
- Düzenli değerlendirme işlemi performansınızı sürekli izlemenize ve geliştirmenize yardımcı olur.

5.3.1 BGYS'de Belgelendirme Hazırlığı

Kurumsal bilgi güvenliği yönetim sistemi (BGYS) kurmak için hazırlanan proje planı aşağıdaki adımlardan oluşmaktadır [24]:

1.Standardın alınması: ilk olarak standardlar edinilebilir. Bu standartlar, www.bsi-global.com adresinden Ingilizce ve www.tse.gov.tr adresinden Türkçe olarak edinilebilir. Yapılması düşünülen BGYS çalışması ile standardın uyumu kontrol edilmelidir.

2.Ön ekibin eğitimi: BGYS kurmanın yararları, uygulanabilecek yöntemlerin de yer aldığı bir eğitim programı ile kurum içindeki "BGYS Yöneticisi" ve ön ekip ilk hazırlığını tamamlar. Eğitim programı, farkındalık, uygulama ve baş tetkikçi eğitimlerini içerebilir. Ekip içinde en az bir kişinin baş tetkikçi eğitimini almış olması, yaratılan sistemin belgelendirme denetimine hazırlığı kolaylaştırır.

3.Ekip ve Stratejinin kesinleştirilmesi: Kurum içinde ilk BGYS ekibinin kurulması ve üst yönetim bilgi/desteği ile hedefin ortaya konmasıdır. Ekip, BGYS ekibi içinde gerekli kaynakların aktarılması ve görevlendirme için üst yönetim temsilciliğini de yapacak olan "BGYS Sponsoru", projenin yönetimini yapacak olan "BGYS Yöneticisi" ve gerekli süreç sahiplerinden oluşabilir.

4.Kapsamın belirlenmesi: BGYS'nin hangi sınırlar içinde uygulanacağı kapsam dokümanı içinde belirlenir. Kapsam seçenekleri, tüm kurum, tek bir süreç, bir departmanın tüm süreçleri olabilir. Kapsamı belirlerken işin karakteristik özellikleri, organizasyon, yerleşim, varlıklar ve teknoloji düşünülmeli, kapsam dışında bırakılan her şey ayrıntıları ve gerekçeleri ile belirtilmelidir.

5.Gerektiğinde Danışmanlık kararının verilmesi: Kapsam belirlendikten sonra, bu kapsama giden yolda kendi BGYS'nizi kurarken dışarıdan alınabilecek destek seçeneklerini değerlendirilir. Danışmanlık, BGYS süresince ekibi yönlendirme ve doğru sonuçları üretme hedefinde olmalıdır. Sizin adınıza bir başka kurum çalışan bir BGYS yaratamaz.

6.Politika Beyannamesinin yazılması ve onaylanması: Yukarıda detayların anlatılan güvenlik politika beyannamesi, tüm şirket çalışanlarının ve ilişki içinde bulunan kişilere bilgilerin güvenliği ile ilgili hedeflerin gösterilmesi amacıyla yazılır. Kurumun bilgi güvenliği anayasası gibi hareket görür. Üst yönetim tarafından onaylanmış bilgi güvenliği beyannamesinin anlaşılması kolay, uygulanabilir, gerçekleştirmesi kolay, yürürlüğe koyulabilir, iş hedeflerini karşılayan yapıda olması önemlidir.

7.Bilgi Varlıklarının belirlenmesi: Bilgi güvenliğini sağlayabilmek için, korunması gereken bilgi varlıklarının listelenmesi, sahiplerinin belirlenmesi gereklidir. Süreçleri takip ederek ilişki içinde olan bilgi ve kaynakları çıkartılır. Böylece bilgi varlıklarının eksiksiz listelenmesi sağlanabilir. Bilgi kaynakları kağıt üzerine basılmış ya da yazılmış, elektronik olarak saklanıyor, posta ya da elektronik ortamlarla aktarılmakta, kurumsal videolarda gösterilmekte ya da söyleşiler sırasında sözlü olarak aktarılmakta olabilir.

8.Varlıkların Değerlendirmesi: Her varlık aynı değerde değildir. Her varlığın da korunması için benzer çaba gösterilmesi anlamlı değildir. Bu yüzden varlık sahiplerinin, varlıkları önceliklendirmesi gereklidir. Bu önceliklendirme varlığın Gizlilik, Bütünlük ve Kullanılabilirlik ihtiyacına göre yapılabilir.

9.Risk Değerlendirmesi: Her varlığın Gizliliğini, Bütünlüğünü ve Kullanılabilirliğini (GBK) tehdit eden unsurlar ve bu tehdide "çanak tutan" zayıf noktalar vardır. Bu tehdit ve zayıf noktalar birleşerek varlıkların GBK'ları için riskleri oluştururlar. Risklerin doğru, tekrarlanabilir ve kurum ihtiyaçlarını karşılayabilir olması BGYS'nin başarısını direk etkiler.
10.Risk Ele Alınış + Kontrol Seçimi: Önceki aşamada belirlenen riskler, ya yeterince düşük bulunur ve "kabul edilir" ya da kabul seviyesine gelmesi için çeşitli kontroller uygulanarak "ortadan kaldırılır", "azaltılır" ve "devredilir". Seçilen kontroller için ISO 27001 ve ISO 27002 (ISO 17799)'dan yararlanılabilir.

11.Politika ve Prosedürlerin yazılması: Seçilen kontrollerin nasıl kullanılacağı, BGYS'nin nasıl çalışacağı hazırlanan dokümanlar içinde belirlenir. Bu dokümanlar "politikalar", "standartlar", "kılavuzlar" ve "süreçler adlarını alırlar".

12.BGYS Dokümantasyonu + Uygulamanın gerçekleştirilmesi: Dokümantasyon yönetim kararlarının kayıtlarını içermeli, eylemlerin yönetim kararları ve politikalarına izlenebilir olmasını sağlamalı ve kaydedilen sonuçların yeniden üretilebilir olmasını sağlamalıdır. Önceki maddelerde anlatılanların dışında "uygulanabilirlik beyannamesi" hazırlanmalıdır.
13.Farkındalık Eğitimlerinin verilmesi: Hazırlanan BGYS kağıt üstünde ne kadar başarılı olursa olsun, kurum çalışanları tarafından uygulanmadıkça etkili olamaz. Hazırlanan politika, süreç ve diğer BGYS dokümanları, standart tehdit ve zayıf noktalar ve çözümlerle birlikte tüm (tam ve yarı zamanlı) yöneticileri, çalışanları, teknik ve teknik olmayan personel, kapsam dışı ama kapsamla ilişkisi olan kişiler (müşteriler ve tedarikçiler vb.) farkındalık eğitimlerine katılmalıdır. Farkındalık eğitimleri web tabanlı olabileceği gibi, sınıf eğitimi ya da diğer yöntemlerle yapılabilir.

14.Gözden Geçirme, Denetim ve Önlemler : ISO 27001 standardında yer alan PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) döngüsü içinde yer alan "kontrol et", gerçekleştirilen tüm süreçlerin gözden geçirilmesini kastetmektedir. Burada yapılan izleme süreçlerinin çalıştırılması, BGYS'nin etkinliğinin gözden geçirilmesi, planlanan aralıklarla risk değerlendirilmesinin gözden geçirilmesi ve üst yönetiminin BGYS'yi gözden geçirmesidir. Bulgulara göre karar verilen önlemlerin alınması ve sistemin güncellenmesi gereklidir.

15.ISO 27001 Sertifika Başvuru & Alım: Bu aşamaya geldiğinizde sahip olduğunuz sistemi belgelendirmek, avantajlara kavuşmak için önemlidir.

5.3.2 BGYS'de PUKÖ Döngüsü ve Süreç Yaklaşımı

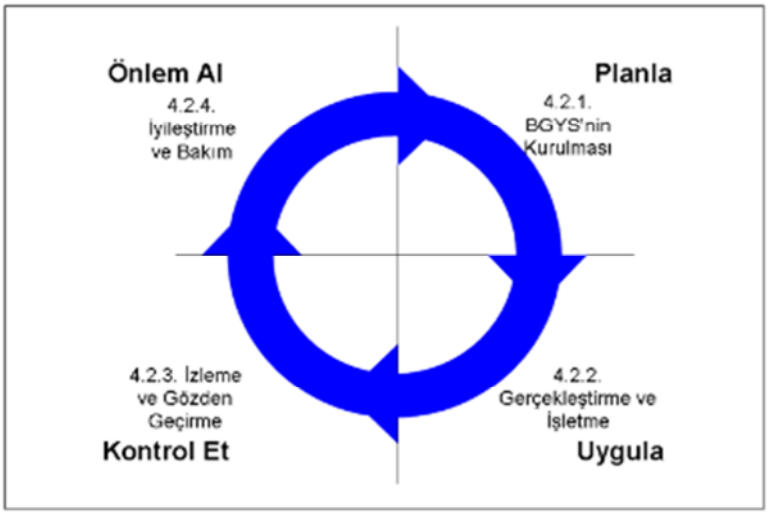
PUKÖ : **P**lanla-**U**ygula-**K**ontrol Et-**Ö**nlem Al kelimelerin kısatlmasından türemiştir. PUKÖ döngüsü şekil 5.3.2.1'de gösterilmiştir.

ISO 27001 standardı, BGYS'nin süreçlerden oluşan bir sistem olarak algılanması gerektiğini vurgulamaktadır. Buna ilave olarak, BGYS'nin kendisi de bir süreçtir. ISO 27001 standardına göre "Girdileri çıktıya çevirmek için kaynak kullanan ve yönetilen faaliyetler süreç sayılır". Dolayısıyla sürecin,

-Girdisi ve çıktısı; girdiyi çıktıya dönüştürmekte kullandığı bilgisi ve yöntemi olacaktır.

Bunlara ilave olarak süreç çalışırken kaynak kullanacaktır. Standart "yönetilen faaliyet" ifadesi ile yönetim tarafından tanımlanmış faaliyetin, - Yönetim tarafından atanmış sorumlular ve belirlenmiş roller uyarınca gerçekleştirilmesini anlışılmaktadır. Her iki konu ISO 27001 ve ISO/IEC 27002:2005 standardında açıkça vurgulanmaktadır [25].

BGYS sürecinin girdisi "Bilgi güvenliği ihtiyaç ve beklentileri", çıktısı "Yönetilen bilgi güvenliği"dir.

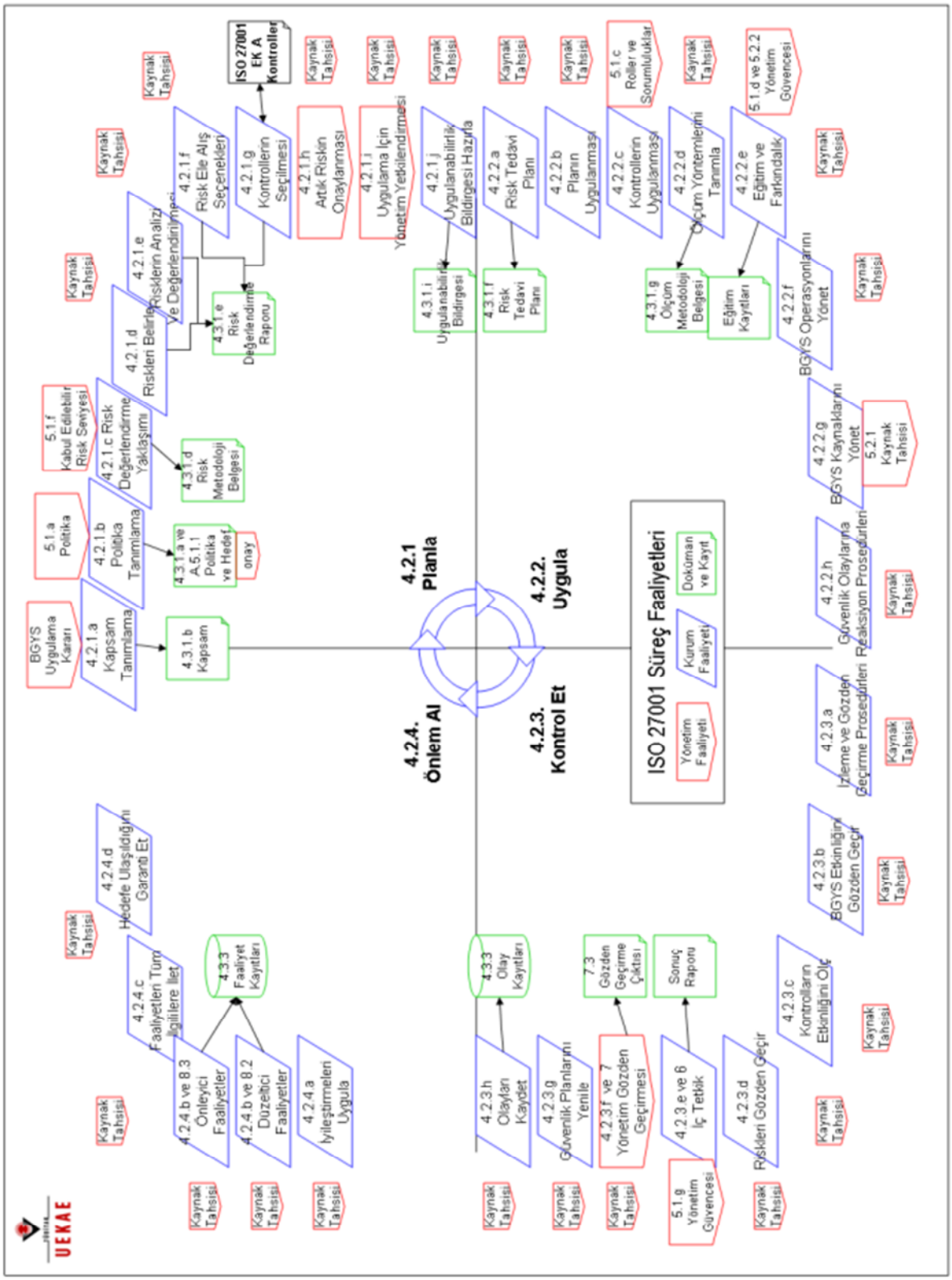


Şekil 5.3.2.1 PUKÖ adımları ve BGYS döngüsü

Şekil 5.3.2.1'deki bu dört adımın gerçekleştirilmesi ile PUKÖ döngüsü tamamlanmış olmaktadır.

ISO/IEC 27002:2005 standardının 4.2 başlığı altında BGYS döngüsünün çok yoğun bir özeti yapılmaktadır. Bu başlık altından standardın "dokümantasyon gereksinimleri", "yönetim sorumluluğu", "iç tetkik", hatta ISO 27002 kontrollerinin özetlendiği "Ek A. Kontrol Amaçları ve Kontroller" bölümlerine göndermeler yapılmaktadır.

Şekil 5.3.2.2'de PUKÖ döngüsü altında bahsi geçen faaliyetler daha detaylı olarak gösterilmiştir.



Şekil 5.3.2.2.Detaylandırılmış üç katmanlı BGYS süreci [25].

5.3.3 BGYS'de Belgelendirme Aşamaları

ISO/IEC 27001:2005 belgelendirmesi için geçilmesi gereken altı aşama aşağıda kısaca açıklanmıştır [26].

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

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

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

4.Aşama: Denetimi gerçekleştirecek olan kurum belgelendirme kapsamını, güvenlik politikasını, risk metodolojisi dokümanlarını, risk eylem planını, uygunluk beyanını (SOA) ve güvenlik prosedürlerini içeren dokümantasyonu gözden geçirir.

5.Aşama: Denetçi firma tarafından masa üstü denetim 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.

6.Aşama: Denetimin başarı ile tamamlanmasının ardından, Bilgi Güvenliği Yönetim Sisteminin kapsamını açık bir şekilde tanımlayan bir sertifika düzenlenir ve kuruluşa gönderilir.

Bu sertifika rutin değerlendirme (takip denetimi ile)ziyaretlerindeki uygunlukla 3 yıl boyunca geçerliliğini korur.

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 işleyisi açısından bir zorunluluk olarak değerlendirilmektedir.

5.4 BGYS Sertifikasını Veren Kurumlar ve Sertifikayı Alan Kurumlar

5.4.1 Akredite Edilmiş BGYS Sertifikasını Veren Kurumlar

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 5.4.1'de gösterilmiştir [27].

Çizelge 5.4.1.1. ISO27001 için akredite edilmiş sertifikasyon kurumları

Akredite Edilmiş Sertifikasyon Kurumları			
Sıra No		Sıra No	
1	AJA Registrars Ltd	34	LGAI Technological Center
2	BM TRADA Certification Limited	35	LRQA
3	BSI	36	LTSI SAS (France)
4	BSI-J (BSI Japan K.K.)	37	Moody
5	Bureau Veritas Certification	38	MSA
6	Center Teknologisk AS (Norway)	39	National Quality Assurance
7	Certification Europe	40	Nemko (Norway)
8	CIS (Austria)	41	PJR (Perry Johnson Registrars)
9	Comgroup GmbH (Germany)	42	PJR-J

10	CQS (Czech Republic)	43	PricewaterhouseCoopers
11	datenschutz cert GmbH (Germany)	44	PSB Certification (Singapore)
12	Defense Procurement Structure.(BSK)	45	QSCert, spol. s.r.o
13	DNV (Det Norske Veritas)	46	RINA S.p.A. (Italy)
14	DQS GmbH (Germany)	47	SAI Global Limited (Australia)
15	DS Certification	48	SEMKO-DEKRA Certification AB
16	ENAC	49	SFS-Inspecta Certification (Finland)
17	HKQAA	50	SGS ICS Limited
18	ICMS	51	SGS Pakistan (Pvt) Limited
19	Intertek Systems Certification	52	SGS Philippines Inc.
20	ISOQAR	53	SIRIM QAS International
21	JACO-IS	54	SQS (Swiss Quality System)
22	JATE	55	STQC IT Certification Services (India)
23	JICQA (JIC Quality Assurance Ltd)	56	TCIC Ltd
24	JMAQA (JMA QA Registration Center)	57	TECO
25	JQA	58	TÜV Austria Hellas
26	JSA	59	TUV NORD CERT GmbH (Germany)
27	JUSE-ISO	60	TÜV Rheinland Group (Germany)
28	J-VAC	61	TÜV RJ (TUV Rheinland Japan Ltd.)
29	KEMA Quality BV	62	TÜV SAAR CERT (Germany)
30	KPMG Audit plc	63	TÜV SÜD Gruppe

31	KPMG Certification	64	UIMCert (Germany)
32	KPMG RJ (KPMG Registrar Co., Ltd.)	65	United Registrar of Systems Limited
33	KPMG SA		

Çizelge 5.4.1.1'de Türkiye'de BGYS sertifikası veren TSE'nin adının geçmemektedir. Ancak TSE, Bilgi Güvenliği Yönetim Sistemi (TS ISO/IEC 27001) Belgelendirme faaliyeti ile ilgili ISO/IEC 17021 standardına akreditasyon çalışmalarımız tamamlanmış ve Nisan 2009 itibariyle TÜRKAK tarafından akredite edilmiştir [28].

5.4.2 ISO/IEC 27001 BGYS Sertifikası Alan Kurumlar

Belgelendirilen BGYS sistemi her geçen gün hızlı bir şekilde artmaktadır. Ülkelere göre belge sayısı incelendiginde dünya genelinde toplam 6573 adet ISO/IEC 27001 sertifikası olduğu görülmektedir [29].

Çizelge 5.4.2.1. Ülkelere göre sertifika alan firma sayısı

Dünya'da ISO/IEC 27001 alan firma Sayısı					
Japan	3572	Philippines	15	Peru	3
India	490	Pakistan	14	Portugal	3
UK	448	Iceland	13	Argentina	2
Taiwan	373	Saudi Arabia	13	Belgium	2
China	373	Netherlands	12	Bosnia Herzegovina	2
Germany	138	Singapore	12	Cyprus	2
Korea	106	Indonesia	11	Isle of Man	2
USA	96	Bulgaria	10	Kazakhstan	2
Czech Republic	85	Norway	10	Morocco	2
Hungary	71	Russian Federation	10	Ukraine	2
Italy	61	Kuwait	9	Armenia	1

Poland	56	Sweden	9	Bangladesh	1
Spain	43	Colombia	8	Belarus	1
Malaysia	39	Iran	8	Denmark	1
Ireland	37	Bahrain	7	Dominican Republic	1
Austria	35	Switzerland	7	Kyrgyzstan	1
Thailand	34	Croatia	6	Lebanon	1
Hong Kong	32	Canada	5	Luxembourg	1
Romania	30	South Africa	5	Macedonia	1
Australia	29	Sri Lanka	5	Mauritius	1
Greece	28	Vietnam	5	Moldova	1
Mexico	24	Lithuania	4	New Zealand	1
Brazil	23	Oman	4	Sudan	1
Turkey	21	Qatar	4	Uruguay	1
UAE	20	Chile	3	Yemen	1
Slovakia	19	Egypt	3		
France	18	Gibraltar	3		
Slovenia	16	Macau	3	**Total**	**6573**

5.4.3 Ülkemizde ISO/IEC 27001 Sertifikasını Alan Firmalar

Özellikle iş süreçlerini elektronik ortamlara taşıyan kurumlarda bu ihtiyacın daha da fazla olacağı tahmin edilmektedir. Türkiyedeki sertifika sayısı dünya geneline bakıldığında yetersiz olduğu görülmektedir. Türkiye'deki kurumlar ve sahip oldukları sertifikalar ise Çizelge 3.5'de gösterilmiştir [30].

Çizelge 5.4.3.1 Ülkemizde BGYS sertifikasını alan kurumlar

Sertifika Alan Kurum	**Ülke**	**Certification Body**	**ISO/IEC 27001:2005**
Anadolu **Bilişim** Hizmetleri A.S.	Turkey		ISO/IEC

			27001:2005
Atlas Medıcal Servıces Ltd.	Turkey		ISO/IEC 27001:2005
Bankalarasi Kart Merkezi A.S., Istanbul	Turkey	Bureau Veritas Certification	ISO/IEC 27001:2005
Beko Elektronik A.Ş.	Turkey	SGS United Kingdom Limited	ISO/IEC 27001:2005
Borcelik Celik Sanayii Ticaret A.S.	Turkey		ISO/IEC 27001:2005
Bursagaz Bursa A.S.	Turkey	SGS United Kingdom Limited	ISO/IEC 27001:2005
Corbuss Kurumsal Telekom	Turkey		ISO/IEC 27001:2005
E-Kart Elektronik Kart Sistemleri	Turkey	Bureau Veritas Certification	ISO/IEC 27001:2005
Global Bilgi Pazarlama, Danisma Ve	Turkey		ISO/IEC 27001:2005
Haci Omer Sabanci Holding A.S.	Turkey		ISO/IEC 27001:2005
İgdaş İstanbul Gaz Dağıtım	Turkey	Bureau Veritas Certification	ISO/IEC 27001:2005
Koc.Net Haberlesme Teknolojileri	Turkey		ISO/IEC 27001:2005
Merkezi Kayıt Kuruluşu A.Ş	Turkey	SGS United Kingdom Ltd.	ISO/IEC 27001:2005
National Ministry Of Education, Education Technologies Department	Turkey		ISO/IEC 27001:2005
Pwc / Basaran Nas Smmm A.S.	Turkey	Bureau Veritas Certification	ISO/IEC 27001:2005

Siemens AG	Turkey		ISO/IEC 27001:2005
Teknosa Ic Ve Dis Ticaret A.S.	Turkey		ISO/IEC 27001:2005
TEMSA SANAYI Ve TICARET A.S.	Turkey	SGS United Kingdom Limited	ISO/IEC 27001:2005
Turk Traktor Ve Ziraat Makineleri A.S	Turkey		ISO/IEC 27001:2005
Türktrust Bilişim Güvenliği A.Ş.	Turkey	SGS United Kingdom Limited	ISO/IEC 27001:2005
Tusas Aerospace Industries, Inc., Ankara	Turkey	Bureau Veritas Certification	ISO/IEC 27001:2005

Çizelge adı olmayan Türk şirketleri olabilir. Bu şirketler adını http://www.iso27001certificates.com/ ancak bu şirketler 1-2 adedi geçmez. Bunlardan bir tanesi Sermaye Piyasası Kurulu'dir.TSE tarafından Sermaye Piyasası Kurulu'na, belge TS ISO/IEC 27001 standardına göre verilmiştir.

5.5 BGYS Standartları Hakkında 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 çalısanların 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 çalısanların ve yöneticilerin eğitilmesi konusunda kuruluşların danımmanlık hizmetleri almaları işi hızlandıracak ve kolaylaştıracaktır.. 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 saglamadığı, 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 penetrasyon testleri ile testleriyle test etmekten geçmektedir.

6. KURUMSAL BİLGİ GÜVENLİĞİNDE RİSK YÖNETİMİ

ISO 27001 Bilgi Güvenliği Yönetim Sisteminin en önemli unsurlardan biri risk yönetim sürecidir.

Risk, sözlük anlamı olarak zarara uğrama tehlikesidir ve öngörülebilir tehlikeleri ifade eder. Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliği, ticari müesseseler içinse öncelikle karlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Finans dünyası başlıca risk faktörlerini Piyasa Riski, Kredi Riski ve Operasyonel Risk olarak üç ana başlık altında toplamaktadır. Bilişim Teknolojilerinde ise daha çok Operasyonel Risk ön plana çıkmaktadır (Egan, ve Mather, 2004).

6.1.1 Bilişim Teknolojilerinde Risk Yönetimi

Öncelikle Operasyonel Risk'den ne anlaşılması gerektiğini netleştirmemiz gerekmektedir. Genel literatür taramasında, Kredi ve Piyasa Riskleri dışındaki tüm risklerin Operasyonel Risk olarak tanımlandığı görülmektedir. Diğer taraftan, yetersiz ya da sorunlu iş süreçleri, personel ve sistemlerden kaynaklanabilecek doğrudan ya da dolaylı kayıpları da operasyonel riskler olarak tanımlamak mümkündür.

Teknolojinin hızlı gelişmesi, ürün ve hizmetlerdeki çeşitliliğin artması, iş süreçlerinin buna bağlı olarak karmaşıklaşması sistem ya da sistemler üzerindeki denetimi zorlaştırmaktadır. Bunun sonucunda hata ve dolandırıcılığa karşı tedbirlerin önceden alınması zorunlu hale gelmektedir. O nedenle, kurum ve kuruluşlar olası bir zarara karşı gerekli altyapı yatırımlarını önceden yapmış olmalıdırlar.

Kurum ve kuruluşlar için Bilişim Teknolojilerine dayalı süreçler, artık kurum ve kuruluşların varlıklarını devam ettirebilmeleri açısından vazgeçilmezler arasında önemli bir yer tutmaktadır. Bilişim Teknolojilerine dayalı iş süreçlerinin herhangi bir sebeple olumsuz yönde etkilenmesi aynı zamanda kurum ya da kuruluşların asli işlevlerini sürdürememesi anlamına gelmektedir.

6.1.2 Bilişim Teknolojileri Boyutuyla Riskler

Bilişim Teknolojileri hizmetlerini olumsuz yönde etkiliyerek kurum ya da kuruluşları, asli görevlerini kısmen veya tamamen yerine getiremez duruma getirebilecek riskleri beş ana

başlık altında toplamak mümkündür.

1. **Personel riski** (çalışan sorunları, insan hataları, eksik bilgi ve yetkinlikler),
2. **Teknolojik risk** (hatalı tasarlanmış sistem mimarileri, hatalı modellemeler, güvenlik zaafiyetleri, iletişim problemi, yazılım ve/veya donanım hataları, veri ve sistem kayıpları),
3. **Organizasyon riski** (BT ve iş birimleri arasında yetersiz iletişim, yetersiz bütçeleme/planlama, projelendirme hataları, yanlış kaynak kullanımı),
4. **Yasal riskler** (Üçüncü şahıs (firma) iflasları veya anlaşmazlıkları),
5. **Dış riskler** (Doğal afetler, sabotaj, terörist saldırılar, siber saldırılar, savaş hali, yangın, su basması gibi fiziksel tehditler).

Başarılı bir risk yönetimi için, kuruluşların bilgi varlıklarına ve hedeflerine yönelik risklerin belirlenerek, analiz edilmesi, tanımlanan risklerin kontrol altında tutularak izlenmesi gereklidir. Riski yönetmenin en doğru yolu, gerçekleşme olasılığı ve gerçeklestiğinde 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 değişir. 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 isleyiş yöntemlerinin oluşturulması gereklidir. Öncelikle kuruluşun uzun dönemdeki hedefleri üzerinde çalışılmalı ve gelecekteki hedefleri tehlikeye atacak risklerin tanımlanarak kontrollerin 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 kontrollerin 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 kontrolerin dengesidir. Gereksiz veya iyi bir risk planlaması yapılmadan oluşturulan kontroller sonucunda iş yapılamaz duruma gelinmesi de kurumlar için önemli bir risk faktörüdür.

Risk tanımlaması yapıldıktan sonra, riskler karşısında alınacak kararlar aşağıdakiler olabilir (Egan, ve Mather, 2004).

- **Riskin Kontrol Edilmesi (Azaltılması):** Riskin kontrol edilmesine karar verildiği durumda, mevcut kontrollerin yetersiz olduğu, ilave tedbir veya kontrollere ihtiyaç duyulduğu anlamına gelmektedir. Tanımlı risklerin kabul edilebilir seviyeye çekilmesi için yapılması gerekenler ve ek güvenlik kontroller (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.
- **Riskten kaçınma** : Risklerin çeşitli nedenlerle kontrol edilememesi ve kabul edilememesi durumunda uygulanır. Riskin kaynağı olan tehdidin gerçekleşme olasılığının ve iş etkisinin çok yüksek olduğu durumlarda riske neden olan bilgi işlem olanağı devreden çıkarılabilir veya riske neden olan işlem veye faaliyete son verilebilir.
- **Riskin aktarmarılması :** Kurum ve kuruluşların yönetiminde ve kontrolünde olmayan varlık ve fonksiyonlarla ilgili ve kurum ve kuruluşun müdahale edemeyeceği konularla ilgili riskler başka kurumlara transfer edilir. Örneğin yangın, doğal afet, hırsızlık gibi tehditlerin azaltılması için yapılan kontrollerden sonra kalan artık risk itfaiye, sigorta şirketi, emniyet güçleri vb. kurumlara aktarılır. 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.

- **Riskin Kabulü:** Risk kabul kararı, mevcut önlemlerin yeterli olduğu, ilave tedbir veya kontrol uygulanmasına gerek olmadığını ifade etmektedir. 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.

Risk Analizi:

Risklerin tanımlanması, hesaplanması ve değerlendirilmesi süreçleri risk analizi olarak tanımlanmaktadır. ISO 27001 standardının gereği olarak değerlendiriecek risk analizi ve yönetimi aşağıdaki adımlardan oluşmaktadır (Tipton ve Krause,2004):

1. Varlıkların belirlenmesi,
2. Belirlenen varlıkların sahiplerinin belirlenmesi (Risk değerlendirmesi yapacak),
3. Bu varlıklara ilişkin tehditlerin belirlenmesi,
4. Tehdit sıklık durumunun belirlenmesi,
5. Bu tehditler tarafından istismar edilebilecek zayıflıklarının (açıklıklar) tespiti,
6. Tehdidin açıklığı istismar etme olasılığının belirlenmesi,
7. Bu varlıkların tehdit ve açılıklarından etkilenme derecesinin Gizlilik, Bütünlük ve Kullanılabilirlik açısından değerlendirmesi,
8. Gizlilik risk seviyesi, bütünlük risk seviyesi ve Kullanılabilirlik risk seviyesi değerlerinin çıkarılması,
9. Risk değerlerine göre risk kararının verilmesi (Risk değeri, risk kabul kriterinin altındaysa ek herhangi bir kontrole gerek yoktur),
10. Eğer Risk kararı "kontrol" ise riski indirgemek için ek önlemlerin gereklidir.

Literatürde iki farklı risk analizi yöntemi mevcuttur. Bunlar, nicel (Quantitative) ve nitel (Qualitative) yöntemlerdir (Landoll, 2006).

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.

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 Kritik, yüksek, orta gibi tanımlayıcı değerler kullanılır.

Her kurum kendisine uygun standart risk analizi yöntemi bulamaya bilir. Her kurumun kendine özel bir varlık envanteri, bu varlıkların güvenliğini tehdit eden farklı tehlikeler vardır.

6.1.3 Bilgi Varlığının Maruz kalabileceği Risk Değerinin Hesaplanması:

Risk, bir tehdidin potansiyel bir zayıflıktan istifade etme olasılığı ve bunun organizasyon üzerinde negatif bir etkiye neden olmasının bir fonksiyonu olarak tanımlanmaktadır.

ISO 27001 standartına uygun hesaplanan risk metodolojilerinden birisi aşağıdaki gibidir (Calder ve Watkins, 2007):

Risk = f(varlığa etkisi, olasılık).

Risk için varlık (varlığın etkisi), varlığın zayıflığı (zaafiyeti, açıklığı) ve bu açığı sömürebilecek tehditler bulunmaktadır. Bu üç unsurdan risk değeri elde edilir.

Varlık, 2. Bölümde anlatıldığı üzere ISO standartları bilgi varlığını, kişi ve kurumların sahip olduğu ve kendisi için maddi veya manevi değer ifade eden ve bu nedenle uygun korunmayı gerektiren tüm unsurlar şeklinde tanınlamışlardır.

Zayıflık (Zaafiyet-Açıklık), varlığa özgü zaafiyetlerdir.

Tehditler, bilinçli veya bilinçsiz olarak varlığa özgü zayıflıkları kullanarak varlığa zarar verebilecek eylem veya durumlardır.

Örneğin 5 skala ile belirlenir aşağıdaki tehdit, zayıflık ve varlık etkisine değerlendirmelerin nasıl verildiğinin ve risk değerlerinin nasıl hesaplandığını anlatmakta yarar bulunmaktadır:

1. **Tehdit sıklığının değerlendirilmesi**

Bir varlık üzerindeki tehditlerin çokluğu, tehditlerin motivasyonu, yaygınlığı, tehditlerin gerçekleşme kolaylığı, tehditlerin karmaşıklığı ve hakkındaki bilgi azlığı gibi durumlar nedeniyle seviyelendirilmeleri gerekir. Seviyelendirme aşağıdaki skalaya göre yapılır. Tehdit

sıklığı belirlenirken, geçmiş deneyim ve istatistikler ile teknolojik gelişmeler göz önünde bulundurulmalıdır. Tehdidin şimdiye kadar hiç gerçekleşmemiş olması sıklığının çok düşük olduğu anlamına gelmez. Dünyada yaşanan deneyimler ve tehdidin özelliği dikkate alınarak sıklık belirlenmelidir.

Tehdidin gerçekleşme sıklığı aşağıdaki tablo örnek verilebilir:

Tehdit sıklık belirleme tablosu

Çizelge 6.1 Tehdit sıklık belirleme tablosu

Seviye	Değer	Tehdit Sıklık
Kritik	5	3 ay bir kez gerçekleşebilir.
Yüksek	4	6 ayda bir kez gerçekleşebilir.
Orta	3	1 yılda bir kez gerçekleşebilir.
Düşük	2	3 yılda bir kez gerçekleşebilir.
Çok Düşük	1	5 yılda bir gerçekleşebilir.

2. **Zayıflık (Zaafiyet, açıklık) değeri (Tehdidin zayıflığı istismar etme olasılığı):**

Açıklık (zaafiyet) değerleri 5 skala ile belirlenir. Bu değerler geçmiş zaman istatistikleri ve teknolojik gelişim gözönde tutularak belirlenir. Örneğin web sayfasının bir zaafiyetten yararlanılarak hackedilmesinin olasılık değer hesaplanırken sadece geçmiş zaman istatikleri baz alınamaz. Geçmiş zaman istatistiklerinin yanında teknolojik gelişim de göz önde tutulur. Geçmişte bir zaafiyettin bir tehdit tarafından istismar edilmemesi veya kırılmaması zaafiyet olasılığının çok düşük olduğu anlamına gelmez. Dünyada yaşanan deneyimler ve zaafiyetin doğası dikkate alınarak olasılık belirlenmelidir.

Açıklık değerlendirme tablosu:

Çizelge 6.2 Açıklık değerlendirme tablosu

Seviye	Değer	Açıklama
Kritik	5	İstismar edilme olasılığı %75'ten büyüktür.
Yüksek	4	İstismar edilme olasılığı %50-75 arasındadır.
Orta	3	İstismar edilme olasılığı %30-50 arasındadır.
Düşük	2	İstismar edilme olasılığı %10-30 arasındadır.
Çok Düşük	1	İstismar edilme olasılığı %10'dan küçüktür.

Tehdidin varlık üzerindeki iş etkisinin belirlenmesi:

Etki, bir tehdidin bir açıklıktan yararlanarak sebep olabildiği negatif sonucun veya zararın büyüklüğünü ifade eder. Etkinin düzeyi, etkilenen kaynak ve varlıkların gizlilik, bütünlük ve kullanabilirlik seviyesinin ne kadar zarar göreceğine bağlıdır.

GBK Seviyesi : Gizlilik Seviyesi (GS), Bütünlük Seviyesi (BS), Kullanılabilirlik Seviyesi (KS) bileşenlerinden oluşur. GS, BS ve KS, 1 ile 5 arasında değer alır. 1 çok düşük , 2 düşük, 3 orta, 4 yüksek, 5 kritik seviyeleri ifade eder.

Bir varlık için tespit edilen ve yukarıdaki gibi tanımlanan GBK seviyeleri ile tehditler ve zayıflıklar eğer açığa çıkarsa o varlığın gizliliği, bütünlüğü ve kullanılabilirliği bundan hangi derecede etkilenir sorusunun cevabı aranır.

3. **Varlık GBK (Gizlilik, Bütüntük,Kullanılabilirlik) Seviyeleri Değerlendirme Tablosu:**

Çizelge 6.3 Varlık GBK seviyesi değerlendirme tablosu

Seviye	Değer	Gizlilik	Bütünlük	Kullanılabilirlik (Erişebilirlik)

Kritik	5	Varlığın yetkisiz kişiler tarafından görülmesi veya ele geçirilmesi: • Cezai yaptırımlara veya düzenleyici kurumlar tarafından çok önemli idari tedbirler uygulanmasına neden olur. • Ulusal çapta medyada çok olumsuz ve ısrarla devam eden haberler çıkmasını ifade eder.	Varlığın doğruluğu ve bütünlüğünün bozulması: • Kurumun işleyişini durdurur. • Cezai yaptırımlara veya düzenleyici kurumlar tarafından çok önemli idari tedbirler uygulanmasına neden olur. • Ulusal çapta medyada çok olumsuz ve ısrarla devam eden haberler çıkmasını ifade eder. • Geri alınması mümkün olmayan varlık transferleri veya varlık zarar/kayıplarına neden olur.	Varlığın ihtiyaç duyulduğunda erişilemez veya kullanılamaz olması: • Kurumun işleyişini durdurur. • Cezai yaptırımlara veya düzenleyici kurumlar tarafından çok önemli idari tedbirler uygulanmasına neden olur. • Ulusal çapta medyada çok olumsuz ve ısrarla devam eden haberler çıkmasını ifade eder. • Varlığa hiçbir şekilde erişilemez.
Yüksek	4	Varlıklığın yetkisiz kişiler tarafından görülmesi veya ele	Varlık doğruluğu ve bütünlüğünün	Varlığın ihtiyaç duyulduğunda erişilemez veya

		geçirilmesi: • Düzenleyici kuruluşların idari para cezasına vermesine veya orta dereceli idari tedbirlerine neden olur. • Ulusal çapta medyada negatif haber çıkmasına neden olur. •	bozulması: • Düzenleyici kuruluşların idari para cezasına vermesine veya orta dereceli idari tedbirlerine neden olur. • Ulusal çapta medyada negatif haber çıkmasına neden olur. • Varlığın eski haline getirilmesi veya geri alınması için büyük tutarlı ilave finansal harcamalara neden olur.	kullanılamaz olması: • Düzenleyici kuruluşların idari para cezasına vermesine veya orta dereceli idari tedbirlerine neden olur. • Ulusal çapta medyada negatif haber çıkmasına neden olur. • Varlığın kullanılabilir duruma getirmek için büyük tutarlı ilave finansal harcamalara neden olur.
Orta	3	Varlığın yetkisiz kişiler tarafından görülmesi, veya ele geçirilmesi, düzenleyici kuruluşun eleştirisine veya sınırlı tedbirlerine neden olur.	Varlığın bütünlüğü ve doğruluğunun bozulması: • Düzenleyici kuruluşun eleştirisine veya sınırlı tedbirlerine neden olur. • Varlığı eski haline getirmek veya geri	Varlığın ihtiyaç duyulduğunda erişilemez veya kullanılamaz olması: • Düzenleyici kuruluşun eleştirisine veya sınırlı tedbirlerine neden olur.

			almak ilave zaman ve çaba gerektirir.	• Varlığın kullanılabilir durum getirmek için ilave zaman ve çaba gerektirir.
Düşük	2	Varlık, kurum içi çalışanlar açısından gizlilik değeri bulunmamaktadır. Kurum çalışanları dışındakilerin elini geçmesi Kurum politikalarını olumsuz etkiler.	Varlığın doğruluğu ve bütünlüğünün bozulması maddi kayıba neden olmaz, ancak kurum içi motivasyon kaybına neden olur.	Varlığın kullanılabilir durumda olmaması maddi kayıba neden olmaz, ancak kurum içi motivasyon kaybına neden olur.
Çok Düşük	1	Varlığın gizlilik değeri bulunmamaktadır.	Varlığın doğruluğu ve bütünlüğünün bozulmasının etkisi bulunmamaktadır.	Varlığın kullanılabilir olmaması herhangi bir etkisi bulunmamaktadır.

6.1.4 Varlığın Risk Değerinin Hesaplanması

Risk(GRD) = varlığın etki değeri x zayıflık değer x tehdit sıklığı 6.1.4.1

Risk(BRD) = varlığın etki değeri x zayıflık değer x tehdit sıklığı 6.1.4.2

Risk(KRD) = varlığın etki değeri x zayıflık değer x tehdit sıklığı 6.1.4.3

varlığın etki değeri: 3 olsun, zayıflık değer : 4 olsun, tehdit sıklığı: 2 olsun:

Risk Değeri = 3 x 4 x2 = 24 olur. Risk değeri 125 (5 x 5 x 5) üzerinden 24'tür. Değer 24 risk kabul kriterin altında ise bu varlığın riski mevcut önlemler ile korunması yeterlidir. Ancak eğer risk kabul kriterinden yüksek ise bu riski azaltmak için ek önlemler gereklidir.

7. KURUMSAL BİLGİ GÜVENLİĞİNİ İSTİSMAR EDEN TEHDİTLER

7.1 Tehdit

Bilgi güvenliği dünydasında tehdit, bilgi varlıklarının doğası gereği etkisinde bulunduğu zaafiyeti sömürüp varlığın gizlilik, bütünlük ve kullanılabilirliğini olumsuz yönde etkileme olasılığı olan tanımlı risklerdir [31]. Tehditlerin bilgi sistemlerinde etkili olabilmesi için bilgi sistemleri üzerindeki var olan zafiyetleri kullanmaları gereklidir.Tehditlerin bilgi varlıklarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki açıklık 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 sistemlerine zarar vermektedir.

Tehditler, tehdit kaynağı açısından bakıldığında;

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

7.2 Tehdit Örnekleri

Bilgi güvenliği ile ilgili güncel tehdit örnekleri aşağıdaki gibidir:

- Deprem, sel, hortum, yangın gibi doğal afet ile ilgili çevresel tehditler,
- İş ile ilgili tehditler: finansal zayıflıklar, iflas, pazar problemleri
- Log dosyalarının yanlışlıkla yada kasten değiştirilmesi
- Yedekleme medyalarında bozulma
- Gizli kanallardan bilgi sızdırılması
- Kaza veya arızalardan oluşabilecek hasar
- Kablo hasarları
- Disipline edilmemiş aksiyonlar veya tehditin farkedilemesi
- Hizmet kesintisi tehdidi
- Ekipmanın tahrip edilmesi tehdidi
- Gizli bilginin ortaya çıkması
- Şifreleme anahtarının ele geçirilmesi

- Bilginin ele geçirilmesi
- Tozlanma, kirlenme
- Çevresel kirlilikten (gürültü, haberleşme dahil) etkilenme
- Çevresel felaketler
- Güvenlik politikası içerisinde hatalar ve unutmalar
- Destek servislerinin kesintisi
- Yangın
- Su taşması, su basması
- Kötü niyetle istifade (fraud)
- Hardware arızası
- Rutubet ve aşırı sıcaklık
- Kanıt toplanmasının sağlanamaması
- Hatalı bilgi girişi
- Hatalı bilgi çıkışı
- Şifreleme anahtarının/algoritma sının yetersiz duzeyde olması
- Kriptografi (şifreleme) politikası eksikliği
- Bilgi alışverişindeki yetersiz anlaşmalar
- Bilginin sınıfılandırılması hatası
- Kaza/Arıza bilgilendirme eksikliği
- Kaza/arıza yönetiminin ele alınışında zayıflıklar
- Veri medyalarının elden çıkarılması sırasında güvenlik eksikliği
- Yetersiz ve test edilmemiş veri yedekleri
- Yetersiz güvenlik yönetimi önlemleri
- İş aktivitelerinin kesintisi
- İş sürekliliği plan zayıflıklıkları, prosedürel ve yönetimsel eksiklikler
- Çalışanın bil güv. Farkındalığında zayıflık
- Arıza/kaza bildirimlerinde çalışanlarda farkındalık eksikliği
- Bilgi kaybı
- Hizmet kaybı
- Kötü niyetli yazılımlar (virus, trojan, worm v.b.)

- Yanlış ve yeniden yönlendirilen mesajlar (re-route, mis)
- Yanlış yere dial edilme, yanlış yere faks gönderme
- Audit veya sistem tool'larının yanlış kullanılması
- Bilgi işlem olanaklarının yetkisiz veya yanlış kullanımı
- Sistem geliştirmede karışık ve anlaşılmayan testler
- Yasal düzenlemelerle uyumsuzluk
- Güvenlik kontrolleri ile uyumsuzluk
- Operasyonel zorluklar, tedarik zincirinde eksiklik, yoğun işgücü
- Unutulmuş erişim hakları
- Gizli dinleme
- Fiziksel müdahele
- Güç sağlayıcı, klima arızaları, elektiriksel anaomaliler
- Kuruma ait bilgilerin özel amaçlarla kullanımı
- Bilgi işlem süreç hataları
- Onaylanmamış doğru olmayan bilginin yayınlanması
- İnkar
- Internet, email, elektronik ticaret riskleri
- Teleworking (tele satış) riskleri
- Çalışanın güvenlik ihlaleri
- Dış kaynakla ilgili güvenlik ihlaleri (destek firmaları)
- Güvenlik politikası ile ilgili ihlaller
- İştirakler, üçüncü taraf kuruluşların yönetimi ile ilgili güvenlik ihlalleri
- Sistem hataları
- Bilgi hırsızlığı
- Ekipman ve medya hırsızlığı
- Onaylanmamış ve test edillmemil bilgi sistem değişiklikleri
- Bilgisayara yetkisiz erişim
- Ekipmana yetkisiz erişim
- Bilgiye yetkisiz erişim
- Mobil ekipmana yetkisiz erişim

- Network ve network servislerine yetkisiz erişim
- Taşıma sırasında yedekleme medyasına gizli ulaşım veya kopyalama
- Yazılım kaynak kitaplığına yetkisiz erişim
- Sistem dökümanlarına yetkisiz erişim
- Mesajların değiştirilmesi veya mesajlara yetkisiz erişim
- Bilgi sistem süreçlerine yetkisiz erişim
- Yazılım lisans bilgilerini yetkisiz kopyalama
- Yetkisiz yazılım kurma veya yazılımda değişiklik
- Yetkisiz olduğu halde bilgiyi değiştirme
- Yetkisiz fiziksel erişim
- Yetkisiz olduğu halde medyanın veya yazılımın silinmesi
- Bilgiye ulaşılamama durumu
- Bilgi işlem süreçlerine ulaşılamama durumu
- Personele ulaşılamama durumu
- Kaynaklara ulaşılamama
- Servizlere ulaşılamama
- Sorumlulukların yanlış kişiye aktarılması veya kaldırılamaması
- İşletim ortamında kontol dışı değişiklikler
- Zayıf gözlem nedeniyle tespit edilemeyen güvenlik zaafları
- Uygun olmayan kimlik tanıma mekanizması (authenticate)
- Kullanıcı hataları
- İş sürekliliği planlarının olmaması
- Görev tanımlarının yapılmamış olması

7.3 Kötücül Yazılımlara Dayalı Tehditler

Kötücül yazılımlara dayalı tehditler çok kullanıldığındanda ve her yeni gün bu tehdit türlerine rastlandığından dolayı bu konu biraz detaylandırılmıştır.

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 çoğunlugu kötücül yazılımlar (Malicious Programs) olarak adlandırılan programlar aracılığıyla yapılmaktadır. Kötücül yazılımlara dayalı olarak yapılan saldırılarda kullanılan yaygın tehditler başlıklar halinde takip eden paragraflarda verilmiştir.

7.3.1 Virüsler:

Virüsler üzerinde ilk ciddi çalışmaları yapmış olan matematikçi Dr.Frederick Cohen virüsü "başka programların içine kendisini kopyalayarak bulaşan bir bilgisayar programı" olarak tanımlamıştır (Canbek ve Sağıroğlu, 2006). Virüsleri bilgisayar sistemlerine,ortamlarına ve bilgilere zarar vermek üzere gelistirilmiş 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, girdigi sistemlere kendilerini, kullanıcının farkında olmadan isteği dışında kopyalayarak sistemlere zarar vermesidir. Kullanıcı tarafından çalıstırılmadan 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, usbler, cdler, dvdler, disketler, ağ paylaşımı, internet (e-posta, dosya indirme,vb. En tercih edilen yöntemdir. Çünkü çok yaygındır) yollarıyla yayılırlar. Aktif olduklarında dosyaları silebilirler, verileri değiştirebilirler, bilgisayarı yavaşlatabilirler, müzik çalabilir, ekrana çesitli 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 çesidi bulunmaktadır. Günümüzde bankacılık işlemlerine odaklanan virüsler coğunluktadır.

7.3.2 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 dagıtırlar. 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

7.3.3 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 islemlerin yapılmasını, uzaktan komut çalıştırılmasını, klavye tuslarının kontrol edilmesini sağlarlar. Truva atları daha çok kullanıcılar tarafından ragbet gören oyunlar ve yazılım güncellemelerinde, msn gibi mesajlaşma programları vasıtasıyla yayılırlar. *Truva atları*; insanların meşru bir kaynaktan geldiğini düsündükleri 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.

7.3.4 Casus Yazılım (Spyware)

Tanıtım, kişisel bilgi toplama veya kullanıcı onayının alınmadan bilgisayar yapılandırmasını değiştirme, kullanıcı bilgisayarının her türlü aktivitesini takip etme gibi çok farklı islemleri kullanıcının bilgisi olmadan gerçeklestiren yazılımlar için kullanılmaktadır (Canbek ve Sağıroğlu, 2006). İstenmeyen zamanlarda açılan reklâm pencereleri, tarayıcıların ilk açtıgı sayfa (giris sayfanız) veya arama ayarları istem dışı değişmisse, 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 çesitli yolları vardır. Müzik veya video dosyası paylaşım programı gibi istediğiniz baska bir yazılımı yüklerken, bu yüklenen yazılımın gerisinde gizlenmiş ve bu işlemle sisteme gizlice yüklenme, çok karsılaşılan yöntemlerdendir.

7.3.5 Arka Kapılar (Back Door)

Bilgisayar programlarına veya bilgi sistemlerine gizli giriş amacıyla kullanılan gizli bağlantı noktalarıdır. Arka kapılar önceden belirlenen yöntemlerle güvenlik kontrollerinin asılarak 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 oluştugunda 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.

7.3.6 Mantıksal Bombalar (Logic Bombs)

Daha önceden programlanan koşullar olustuğunda zarar verecek işlemler yapan zararlı programlardır. Koşullar bir tarih (Ocak ayının 22. günü), günün belli bir saati (23:00), belli bir kullanıcının sisteme girişi, işten çıkarılan bir çalısanın 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.

7.3.7 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 (örneğin www.akbank.com.tr yerine www.akbank.tr.com.tr adresi ile arayüzü orjinal site ile aynı olan bir websitesi açılması) hazırlayarak kandırma ve kullanıcıların gizli bilgilerini elde etme için yapılan kandırmaca girisimlerinin tümüne verilen addır.

Günümüzde 2000- 2007 yılları arasında çok kullanıldı ve bir çok kullanıcı olumsuz etkilendir. Günümüzde halen kullanılmaktadır.

7.4 Zararlı Kodlara Karşı Koruma Yöntemleri:

Kurumsal olarak;

- Kurumsal olarak zararlı kodlar ile mücade edilmesi için bir politika geliştirilmelidir.
- Kurumun internet bağlantı nokları kontrol edilmeli gelen tüm internet ve ağ trafiğinde zararlı kod taraması yapılması ve zararlı kodlar doğrudan bloklanmalıdır.
- Kuruma bağlanacak tüm cihazlar (Pc, USB disk, vb.) belli bir politika çerçevesinde taramalı ve böylece bağlantıya izin verilmelidir.

Bireysel olarak;

- Bilgisayarlarda muhakkak firewall programı yüklenmelidir.
- Bilgisayarda muhakkak olarak bir antivirüs, antimalware yazılımları yüklenmeli ve daima güncel tutulmalıdır.
- İşletim sistemimin yamaları zamanında yapılmalıdır. (Auto Update seçilmelidir)
- Bilgisayarlara lisansız programlar yüklenmemelidir.
- Güvenli olmayan sitelerden yazılım indirilmemelidir.
- Kullanılan tüm programların güvenlik güncellemeleri takip edilmeli ve zamanında yüklenmelidir.
- E-mail ve eklentilerine dikkat edilmelidir. Bilinmeyen e-posta ve eklentiler açılmadan silinmelidir.

Her siteye girilmemelidir. Açılan pencereler (popuplar) tıklanmamalıdır.

7.5 DoS ve Ddos Saldırıları

Dos: DoS (Denial Of Service) yani rervislerin devre dışı bırakımadır. DoS saldırılarından korunması oldukça zordur ancak saldırması kolaydır. DoS için en basit şekilde karşı sistemde işlemekte olan servisleri bloke etmek için yapılan saldırıdır.

DdoS: DdoS (Distributed Denial Of Service)'un işleyiş tarzı DoS ile aynıdır tek farkı birden fazla noktadan gerçekleştirilmesidir. Birden fazla noktadan saldırmanın en önemli amacı güçlü bir saldırı gerçekleştirmek ve saldırıyı düzenleyen kişiyi gizlemektir.Saldırgan güvenliği zayıf bilgisayarlara "zombi" adı verilen bir çeşit uzaktan erişim aracı yükler ve saldırıyı bu zombi bilgisayarlar sayesinde gerçekleştirir.

Özellikle DDoS atakları servis sağlayıcılarının korkulu rüyalarından biridir. DDoS tipi saldırılar özellikle büyük firmaların bu tür saldırılardan etkilenmesi DDoS adını ön plana çıkardı Hatta 2008 yılında Rus hackerlar tarafından Estonya'ya bu saldırılar yapılarak özellikle kamu hizmeti sunan bir çok kurum iş yapamaz duruma gelmişti (Ramses, 2009).

7.6 Güncel Web Tehditleri

Günümüzde ve yakın gelecekte bir çok kurum iş ve işlemlerini web ortamında yürüttüğü veya yürüteceğinden dolayı bu web uygulamalarına dayalı tehditler de her gün çoğalmaktadır. Dolayısı ile bu bu konu da biraz detaylandırılmıştır.

Web uygulamalarının güvenliğiyle ilgili birçok çalışma yapılmaktadır. Bu çalışmalardan birisi olan, Mark Curphey tarafından 2001 yılında kurulan, kâr amacı gütmeyen 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. 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). Kurumsal Bilgi Güvenliğini üst seviyede etkileyen güncel tehditler takip eden alt başlıklarda kısaca açıklanmıştır [31].

7.6.1 Kimlik Doğrulama Tehditleri

Web uygulamalarında yer alan kimlik doğrulama mekanizmasın atlatmak veya istismar etmek için kullanılabilecek zafiyetlerin oluşturduğu tehditlerdir. Kimlik doğrulamasında "sahip olunan bir nesne", "bilinen bir bilgi" veya "sahip olunan bir özellik" kullanılmaktadır. Kimlik doğrulama saldırıları, web sitesinin kullanıcı, servis veya uygulama kimliğini doğrulayan sistemleri hedef alan tehditleri kapsar.

7.6.2 Yetkisiz Erişim Tehditleri

Yetkilendirme saldırıları, bir web uygulamasının kullanıcı, servis veya uygulamanın istenen bir işlemi gerçekleştirmesi için gereken izinleri belirlemek için kullanılan yöntemleri hedef almaktadır. Yetkilendirme tehditlerini, oturum bilgisi tahmin etme, yetersiz yetkilendirme, yetersiz oturum sonlandırma, oturum sabitleme olmak üzere kendi arasında dört grupta sınıflandırmak mümkündür. Yetki veya oturum bilgisi tahmin etme, web uygulamasının kullanıcısı rolüne girme veya söz konusu kullanıcının oturumunun ele geçirilmesi yöntemidir. Yetersiz yetkilendirme, web uygulamalarının daha geniş erişim kontrol kısıtlamaları gereken hassas bilgiye, yapılandırma hatalarından kaynaklanan zayıflıklardan faydalanılarak erişme yöntemidir. Yetersiz oturum sonlandırma, web uygulamalarının yetkilendirme için kullanılan eski oturum kimlik bilgisini tekrar kullanma imkan vermesinden kaynaklanmaktadır. Oturum sabitleme, daha önceden belirlenen bir oturum numarasının çeşitli yöntemlerle kullanıcılara tahsis ettirilmesini sağlamaktadır.

7.6.3 Kullanıcı Taraflı Tehditler

Kullanıcı taraflı tehditler, 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 uygulamalarının geçerli içerik sunmasını beklerken web uygulamasından herhangi bir saldırı gelmesini beklemez. İçerik sahteciliği (Content Spoofing) ve siteler arası kod çalıştırma (Cross Site Script-XSS) kurumsal bilgi güvenliğini etkileyen kullanıcı taraflı tehditlerdir. İçerik sahteciliği, kullanıcının ziyaret ettiği dinamik içerikli web sitesinde harici olarak çalışan web uygulamasının ziyaret edilen web sitesinin resmi içeriği olduğuna inandırılmasın sağlayan saldırı 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. Siteler arası

kod yazma, kullanıcı ile web sitesi arasındaki güven ilişkisi istismar edilerek, web sitesinin saldırgan tarafından belirlenen çalıştırılabilir kodu kullanıcıya göndermesi ve bu kodun kullanıcı web tarayıcısında yüklenerek çalışmasıyla gerçekleşmektedir.

7.6.4 Komut Çalıştırma

Komut çalıştırma, web uygulamalarında uzaktan çalıştırılan komutlar yardımıyla yapılan tehditlerdir. 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.

7.6.5 Bilgi Açığa Çıkarma

Bilgi açığa çıkarma, web uygulamalarının kendisi veya çalıştığı platformlarla ilgili sisteme özel (versiyon, çalıştığı platform, yama seviyesi, yedek veya geçici dosyaların yeri, vb.) bilgilerin elde edilmesi için yapılacak işlemleri kapsamaktadır. Çoğu durumda, web uygulamaları kendileri hakkında bir kısım bilgiyi gösterecektir. Ancak burada önemli olan mümkün olduğunca, uygulamalar hakkında gösterilen bilgilerin boyutu en aza indirgenmektedir. Uygulamalar ve çalıştığı platformlar hakkında ne kadar çok bilgi toplanırsa saldırganlar tarafından zafiyetlerin belirlenmesi ve kullanılması da o kadar kolay olur.

7.6.6 Web Uygulamalarını Tehdit Eden Saldırılar

7.6.6.1 Web Uygulamalarına Yapılan Saldırılar

Kurum ve kuruluşlar bilgilerini elektronik ortamlara açtıkça, elektronik ortamlarda yapılan iş ve işlemler artmakta karşılaşılan tehdit ve tehlikelerde de doğal olarak artışlar gözlenmektedir. Son yıllarda yapılan araştırmalar ve çalışmalar incelendiğinde kurumsal bilgi güvenliğinin üst seviyede tehdit eden ve korunmasızlık seviyesinin en yüksek olduğu güncel tehditleri içeren ortam olan web uygulamaları olarak ifade edilebilir.

Web uygulamaları, güncel bilgiye kurum, kuruluş veya bireylerin kolayca erişebilmesi için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır. Web denilince akla ilk olarak

kurumların vitrini ve itibarı haline gelmiş kurumsal web siteleri gelmektedir. Web üzerinden verilen hizmetler çoğaldıkça web'e yönelik tehditler ve saldırılar da artışlar gözlemlenmektedir. Bunun nedeni, web uygulamaları güvenliğinin ilgisizlikten ve bilgisizlikten kaynaklanan sebeplerden ötürü yeterince ciddiye alınmaması ve güvenli yazılım geliştirme tekniklerinin bilinmemesi veya kullanılmaması olarak açıklanabilir. Web sitelerinin çalışma prensipleri güncel web tehditlerinin daha iyi anlaşılabilmesi amacıyla kısaca aşağıda açıklanmıştır.

Web uygulamalarının üzerinde çalıştığı Web dinamik veya statik yapıda çalışan içerikler sunmaktadırlar. Statik yapıda çalışan web siteleri, kullanıcıdan gelen talepler üzerine ilgili web sayfalarının gösterilmesini sağlayan statik html kodların içermektedirler. 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 üç katmanlı bir yapı içerisinde çalışmaktadır.

Bu katmanlar aşağıda maddeler halinde kısaca açıklanmıştır:

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

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

3. Web uygulamaları tarafından kullanılan verilerin depolandığı veri tabanlarıdır (My SQL, Oracle,MS SQL, Informix, DB2 Sybase,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 [32]. Web uygulamalarında oluşabilecek bir zafiyet, güvenlik önlemlerini (güvenlik duvarı, saldırı tespit ve önleme sistemleri, vb.) devre dışı bırakarak güvenilir bölgede yer alan sistemleri üst

düzeyde tehdit etmektedir.

7.6.6.2 Web Uygulama Saldırılarına (tehdit) Örnekler

a.1 XSS Saldırıları

XSS saldırıları, web sitesinin saldırgan tarafından belirlenen çalıştırılabilir kodu normal bir kullanıcıya göndermesi ve bu kodun kullanıcı web tarayıcısında yüklenerek çalışmasıyla gerçekleşen bir saldırı çeşitidir.

a.2 İçerik Sahteciliği

İçerik sahteciliği, kullanıcıya bir web sitesindeki belirli içeriğin meşru olduğuna ve bu içeriğin harici bir kaynağa ait olmadığına inandırılmasını sağlayan bir saldırı tekniğidir.

a.3 Komut Çalıştırılarak Gerçekleştirilen Saldırılar

Uzaktan çalışan komutlarla yapılan saldırılardır. Bütün web siteleri talepleri karşılamak için kullanıcı girdilerinden faydalanır. Çoğu zaman bu kullanıcı girdileri dinamik web sitesi içeriği hazırlamada kullanılan komutların oluşturulmasında kullanılır. Eğer bu işlem güvenli bir şekilde yapılmazsa, saldırgan komut çalıştırma işlemini değiştirebilir

a.4 Ara Bellek Taşması - Buffer Overflow

Buffer overflow saldırıları, hafızanın bazı bölümlerinin üzerine yazarak uygulamanın akışını değiştiren saldırılardır. Hata ile sonuçlanan genel bir yazılım kusurudur. Bu hata durumu, ayrılan yerden daha çok veri hafızada bir yere yazıldığında oluşur. Bellek taştığında, komşu hafıza bölgelerinin üzerine yazılarak hatalara veya çökmelere neden olunur. Bellek taşmasının, hafızayı bozması yazılımın çökmesi ile sonuçlanır ve bu şekilde hizmet dışı saldırısı olarak kullanılabilir.

a.5 SQL Enjeksiyonu

SQL enjeksiyonu, kullanıcı kaynaklı girdilerden SQL cümleleri oluşturan web sitelerini sömürmek için kullanılan bir saldırı tekniğidir.

7.7 Veritabanı Güvenliği

7.7.1 Veritabanı

Veri tabanı, en geniş anlamıyla; birbiriyle ilişkili verilerin tekrara yer vermeden, çok amaçlı kullanımına olanak sağlayacak şekilde depolanması olarak tanımlanabilir.

Veri tabanı veya Veritabanı düzenli bilgiler topluluğudur. Kelimenin anlamı bilgisayar ortamında saklanan düzenli verilerle sınırlı olmamakla birlikte, daha çok bu anlamda kullanılmaktadır. Bilgisayar terminolojisinde, sistematik erişim imkânı olan, yönetilebilir, güncellenebilir , taşınabilir, birbirleri arasında tanımlı ilişkiler bulunabilen bilgiler kümesidir. Bir başka tanımı da, bir bilgisayarda sistematik şekilde saklanmış, programlarca işlenebilecek veri yığınıdır.

7.7.2 Veri Tabanı Yazılımları

Verileri sistematik bir biçimde depolayan yazılımlara verilen isimdir. Birçok yazılım bilgi depolayabilir ama aradaki fark, veri tabanın bu bilgiyi verimli ve hızlı bir şekilde yönetip değiştirebilmesidir. Veri tabanı, bilgi sisteminin kalbidir ve etkili kullanmakla değer kazanır. Bilgiye gerekli olduğu zaman ulaşabilmek esastır.

Örnek yazılımlar aşağıdaki gibidir:

- MySQL
- Oracle
- MS-SQL
- Sybase
- DB2
- Informix
- Postgresql
- Filemaker
- Berkeley
- Firebird
- Ms access

7.7.3 Veri Tabanına Erişim ve Güvenlik

Kurum ve kullanıcılara hizmet veren, ürün sunan, sipariş alan, satış yapan, başvuru alan, kayıt yapan, sorguya izin veren web uyglamaları ve diğer özel kullanıcı arayüzü üzerinden hizmet veren uygulamaların beslendiği bir veritabanı günümüzde artık neredeyse uygulamaların arayüzlerinin tamamı web arayüzü üzerinden hizmet vermektedir. Genel olarak, web sitelerindeki form aracılığı ile alınan girdi ile veritabanındaki bilgiler filtrelendikten sonra

sonucu kullanıcıya gönderme işlemine veribanına erişim işlemi olarak algılanır. Bu genellikle yapısal sorgulama dili (Structured Query Language - SQL) yapılmaktadır. Uygulama içerisinde kullanılacak parametre değerleri alınırken kullanılan formun SQL deyimini yeniden yapılandırabilecek bazı özel karakterlere izin vermesiyle güvenlik problemleri ortaya çıkmaktadır. Bu güvenlik problemleri günümüzde en güncel ve en çok suistimale açık durumlardır.

Bu güvenlik problemleri kullanılarak bir uygulamanın arkasında, bu uygulamaya destek veren veri tabanı üzerindeki bütün bilgilere ulaşılabilir veya bilgiler üzerinde değişiklik yapılabilir. Veya veri tabanı sisteminin komutları kullanılarak kullanılan sunucular üzerinde uygulama harici istenen işlemler de yapılabilir. Bu problemlerden korunmak için de uygulama girdilerini bu tür karakterlere karşı kontrol eden fonksiyonların kullanılmalı ve geniş çaplı uygulamaların bu güvenlik açıklarını taşıyıp taşımadığını anlamak için güvenlik denetimine tabi tutulmalıdır.

Veritabanı güvenliğini, sistem güvenliği ve veri güvenliği şeklinde iki kategoriye ayırabiliriz. **Sistem güvenliği**, kullanıcı yaratma, değiştirme, silme vb. yetkileri tanımlayan ve veritabanının sistem seviyesinde kullanımıyla ilgili mekanizmaları kontrol eder. Sistem güvenliği mekanizmaları şunları kontrol eder:

Örneğin, doğru kullanıcı adı ve şifreleri, kullanıcıya ait şema nesneleri için ayrılan yer miktarı, kullanıcı için ayrılan kaynak miktarları.

Veri güvenliği, veritabanının şema nesneleri seviyesinde kullanımıyla ilgili mekanizmaları kontrol eder. Örneğin, kullanıcı hangi şema nesnelerine erişebilir, kullanıcı belli bir şema nesnesi üzerinde hangi işleri yapmaya yetkilidir.

7.7.4 Veritabanı Güvenliğini İçin Yönetilmesi Gereken Unsurlar

7.7.4.1 Veritabanı Kullanıcıları ve Şemaları

Bir kullanıcının veritabanına bağlanabilmesi için veritabanında tutulmakta olan geçerli bir kullanıcı adı ve şifresi vermelidir. Kullanıcının yapabileceği işlemlerin oluşturduğu kümeye kullanıcının güvenlik alanı denir. Default (kurulumla beraber gelen) gelen kullanıcıların hakları kısıtlanmalı ve şifreleri değiştirilmelidir. Kullanılmayan kullanıcılar devre dışı bırakılmalıdır.

7.7.4.2 Yetkilenedirme ve Yetkiler

Yetki, belli bir tipteki SQL cümlesini çalıştırabilme hakkıdır. Örneğin, veritabanına bağlanabilme, kendi şeması içinde tablo yaratabilme veya bir başkasına ait olan tabloyu sorgulayabilme. İki tür yetki vardır. Bunlar sistem yetkileri ve şema yetkileridir. Sistem yetkileri, sistem genelinde yapılacak işler içindir ve genelde sadece sistem yöneticilerine verilir. Şema yetkileri, belirli bir şemadaki belirli bir nesne üzerinde yapılabilecek işler için verilir. Bu yetkiler direk olarak kullanıcalara verilebildiği gibi yetkiler kümesi olarak tanımlanabilecek olan roller aracılığıylada verilebilir. Ancak yetkilerin roller üzerinde verilmes güvenlik açısından daha yararlıdır.

7.7.4.3 Roller

Roller, kullanıcılara ve diğer rollere verilecek, birbiriyle alakalı, isimlendirilmiş yetkiler kümesidir. Yetkilerin yönetimini roller aracılığıyla yapılması hem yönetimi kolaylaştırmakta hem de daha güvenli bir yapıya geçmeye izin vermektedir.

7.7.4.4 Depolama Ayarları ve Kapasite Limitleri

Her kullanıcı yaratılırken bir varsayılan birde geçici tablespace ile ilişkilendirilmelidir. Bir nesne yaratılacağı sırada eğer tablespace adı belirtilmezse kullanıcının varsayılan tablespace'inde yaratılır. Bir SQL cümlesi çalıştırılırken geçici segmente ihtiyaç duyulursa bu kullanıcının ilişkilendirilmiş olduğu geçici tablespace içinde yaratılır. Kullanıcıların tablespaceler içinde kullanabilecekleri yer miktarı ise o kullanıcıya o tablespace üzerinde verilmiş kotayla sınırlı olmalıdır.

7.7.4.5 Profiller ve Kaynak Limitleri

Veritabanı kaynaklarının gereksiz yere harcanmaması için her kullanıcıya kaynak kullanım limitlerini belirleyen bir profil atanmalıdır. Kaynakların kullanımı ve limitleri güvenlik açısından önemlidir. Profilin içereceğindeki kaynaklardan bazıları şunlardır:

- Kullanıcının aynı anda açabileceği maksimum oturum sayısı
- Kullanıcının oturumu ve çalıştıracağı SQL cümleleri için kullanabileceği CPU zamanı ve manatıksal giriş çıkış miktarı
- Kullanıcının bir iş yapmadan bekleyebileceği süre
- Kullanıcının bağlı kalabileceği süre

- Kaç başarısız bağlanma denemesinden sonra kullanıcı hesabının kilitleneceği, şifrenin ne kadar süre geçerli olduğu veya ne tür şifrelere izin verileceği gibi şifre kısıtlamaları

7.7.4.6 Kullanıcını Hareketlerinin Denetlenmesi

Üç farklı seviyede denetleme yapılabilir. Bunlar cümlelerin, yetkilerin ve şema nesnelerinin denetlenmesidir. Cümle denetlemesi, belli veya tüm kullanıcıların belirli tipteki SQL cümlelerinin denetlenmesini sağlar.

Yetki denetlemesi, belli veya tüm kullanıcılaların sistem yetkilerini kullanımlarının denetlenmesini sağlar. Şema nesnelerinin denetlenmesi, belli şemalardaki belli nesneler üzerinde yapılacak işlerin denetlenmesini sağlar.

Denetlemeler sonucunda elde edilen bilgiler denetleme tablolarına yazılır. Kullanıcılar tanımlayacakları veritabanı tetikleri ile daha karmaşık denetleme mekanizmaları kurabilirler.

7.7.4.7 Detaylı Denetleme

Erişilen verinin içeriğine göre denetleme yapılmasını sağlar. Denetleme sırasında önceden belirlenen durumlar tespit edildiğinde kullanıcının bu durum için tanımladığı veritabanı prosedürlerinin çağrılması sağlanabilir.

7.7.5 Veritabanlarını Tehdit Eden Durumlar

İnternet üzerinden veri paylaşımı arttıkça veri güvenliğinin sağlanması önemli bir olgu

haline gelmiştir. Bilişim sistemlerini çökertmek, yavaşlatmak üzerine yapılan saldırılarla birlikte değerli olan bilgilerin çalınmasına yönelik saldırılar daha tehlikeli hale gelmiştir. Değerli olan bilgilere günümüzde örnek olarak kredi kartı bilgileri ve banka hesapları verilebilir [33].

Dış saldırılara karşı güvenlik duvarı, saldırı önleme sistemleri, antivirus ve antispyware gibi çeşitli programlar, SSL (secure socket layer) benzeri şifreleme yöntemleri ve kullanıcı hakların kısıtlanması gibi yaptırımlar mevcuttur .Veri tabanından bilgi hırsızlığına karşı yapılabilecek hazır yazılım tarzında çok fazla ürün bulunmaktadır. Tasarımlarına bağlı olarak güvenlik duvarları genelde iç bilgisayarlara her türlü hakkı verirken, SSL tarzında uygulamalar verinin şifrelenmesi ve başka kişiler tarafından okunmasını engellenmesi amacına yönelik olduğundan veri tabanlarına karşı yapılan saldırılara yaptırımları çok fazla değildir.

Veri sorgulamasına ve girişine izin verilen herhangi bir kullanıcı sistemin içinde kabul edilir. Veritabanı uygulamalarında veritabanı genelde sunucu bilgisayar (server) üzerinde bulunmakta ve istemci bilgisayarlardan (client) veri girişi veya sorgulaması yapılmaktadır. İnternete ortamına hizmet veren sunucu tabanlı uygulamalardan ASP (Active Server Page) ve PHP (Hypertext Preprocessor) en fazla bilinenleridir. ASP ve PHP tabanlı web programları, derlenmiş kendi başına çalışabilen (executable binary) dosya yaratmadan web üzerinde kullanım sağlarlar (Clarke, 2009).

ASP ve PHP sunucu tabanlı uygulamalarla beraber çalışan SQL (Structured Query Language) veri tabanları veri girişini ve sorgulamasını kolaylaştırır. SQL veri tabanlarına MySQL, PostgreSQL,MS SQL ve Oracle örnek gösterilebilir. Microsoft Internet Explorer veya Firefox gibi herhangi bir tarayıcı (browser) aracılığıyla bu veri tabanlarına veri girilebilir veya veri tabanlarından veri sorgulanabilir. Veri girişinin ve sorgusunun hızlandırılması amacıyla sunucu tabanlı bilgisayarlarda PHP ve ASP gibi kolay hayata geçirilen uygulamalar bazı temel kurallara dikkat edilmezse veri tabanına karşı saldırılara açık vermektedir.

Sunucu temelli SQL veri tabanları ile beraber kullanılan PHP ve ASP uygulamaları programcılık hatalarından (bug) başka güvenlik sorunları olabilmektedir.

ASP ve PHP temelli uygulamalarda veri tabanlarındaki değerli bilgilere izinsiz ulaşmaya olanak veren tasarım boşlukları bulunabilmektedir. Veri girişi ve sorgulaması için geliştirilen uygulamanın bir an evel uygulamaya konulma isteği güvenlik açıklarını ortaya çıkarabilmektedir.. Veri tabanlarında ihtiyaç duyulan güvenliğinin sağlanması, kullanılacak uygulamanın tamamlanma süresini uzatmaktadır. Tasarım aşamasında uygulamada yapılan güvenlik açıklıkları, uygulamanın kullanılması sırasında sorunlara yol açabilmektedir.

Veri tabanlarındaki açıklar kredi kartı bilgileri gibi değerli bilgilerin veya adli sicil gibi kişisel bilgilerin çalınmasına neden olmaktadır.

Yukarıda bahsedilen açıklardan yararlanarak SQL injeksiyonu ile araya girerek SQL cümlecikleri ile verileri izinsiz bir şekilde alma riski en güncel konulardan birisidir

7.7.5.1 SQL Enjeksiyon Tehditlerine Karşı Uyulması Gereken Kurallar

Veritabanlarına yönelik güvenlik çözümleri veya uyulması gereken kurallar aşağıda

Listelenmiştir [33].

1. Veri girişi ve sorgulamasında kullanılacak uygulamasının Web Tarayıcısı (Web Browser örnek Microsoft İnternet Explorer, Firefox) üzerinden girilirken adres çubuğunun kaldırılması. Adres çubuğu internet tarayıcısından kaldırılarak bütün işlemlerin internet tarayıcısı üzerinden yapılmasının sağlanması, dışarıdan yapılacak müdahalelerin büyük bir kısmını engelleyecektir.

2. Veri tabanına bağlandıktan sonra SQL ifadelerine bağlı herhangi bir hata mesajının (error message) internet tarayıcısına veya uygulamaya yönlendirilmemesi. Hata mesajının internet tarayıcısına yönlendirilmemesi veritabanına sızmak isteyen kişilerin hangi konumda olduklarını öğrenmemelerini sağlayacaktır.

3. ComboBox ve ListBox'lardaki veri tabanı ismi ile sunucu veri tabanı isminin aynı olmaması ve veri girişi yapılan yer adları ile veri tabanındaki değişken (variable) isimlerinin aynı olmaması. İnternet tarayıcılarının tercihlerini bulunduran ComboBox ve ListbBox'lar veritabanı ve değişkenlerle aynı isime sahip olursa veritabanına ulaşılması kolaylaşacaktır.

4. Veri tabanlarında veri girişinde ve sorgulanmasında çapraz veritabanları ve tabloların kullanılması. Veritabanından bilgi istendiğinde veya bilgi gönderildiğinde bir yerine birkaç veri tabanı kullanılması ve bunlar arasında doğruluk karşılaştırılması yapılması güvenliği arttıracaktır.

5. Kullanıcı haklarının çapraz veri tabanları için ayrı ayrı tanımlanması. Kullanılacak birden fazla veritabanı için her aşamada kullanıcı haklarının ayrı ayrı tanımlanması gerekmektedir. Eğer bu işlem bir tek veritabanı üzerinden yürütülürse ve güvenliğin sağlandığı veritabanına sızılacak olursa bütün veritabanının güvenliği tehlikeye düşecektir. Eğer diğer veritabanlarında da güvenlik tedbirleri olursa sızma işlemi gerçekleştirilmeyecektir. Diğer veritabanlarında güvenlik sağlayacağından bir veritabanına sızmak bilgi sızdırmak için yeterli olmayacaktır.

6. Veri girişi yapan kişinin okuma (read access), yazma (write access) hakkının olması değiştirme hakkının süreli olması.

7. Veri girişi yapan kişilerin yanlızca kendi girdikleri verileri okuyabilmesi. 6. ve 7. maddeler temelde analizlere yönelik istatistksel veritabanları için geçerlidir. Daha önce girilmiş ve doğruluğu kabul edilmiş bilgilerin yanlışlıkla silinmesini engelleyecektir. Hatalı girişler için

değişterme hakkı süreli olduğundan daha sonra doğru kabul edilen bilgi üst makamlarca değiştirilebilecektir.

8. Veri girişi hakkı, okuma hakkı, değiştirme hakkı yanlızca bir yönetici (veya merkez) tarafından verilmesi ve hakkların verileceği kişilerin önceden belirlenmesi. Bu yöneticinin veri tabanı güvenlik denetleme (auditing) işine dahil edilmemesi. Kullanıcıların hakları bir tek merkezden verilmeli ve verilen okuma, yazma, değiştirme hakları kayıt altına alınmalıdır.

9. Veri girişinde veri girenlerin kullandıkları SQL ifadelerinin (SQL statement) hepsinin ayrı ayrı seyir dosyasına (log file) yazılması. Veri tabanıyla yapılacak her türlü işlem sunucu tarafından kayıt edilmelidir. Bu sayede veritabanında meydana gelecek hata takip edilebilecektir.

10. Tarayıcıdan gelebilecek SQL komutları uzunlukları yazılım tarafından kontrol edilmelidir. Veritabanına sızmak isteyen birisi SQL komutunu değiştirecektir. İnternet üzeriden gelen SQL komut uzunlukları kontrol mekanizması altına alınacak olursa bir çok saldırgan devre dışı kalacaktır.

11. Güvenlik denetleyecilerin hatalı veri girişlerini, veri girişçisinin işi bittikten sonra veriyi kontrol etmesi. İstatistiksel veri tabanlarında güvenlik denetçileri girilen veriyi kontrol ederek kullanıma hazır bir hale getirmeleri gerekmektedir.

12. Veri girişçi kendisine ait veri girişi parçasını bitirdikten sonra veri güvenlik denetçisinin yedekleme (backup) işlemi yapması. Sayısal ortama kaydedilen bilgileri güvenlik altında tutmanın en iyi yolu yedeklenmesi ve yedeğin yedeklenmesidir.

13. İstatistiksel analiz için kullanılacak veritabanının, web uygulamalarından elde edilecek ve asıl olarak kullanılacak veri veritabanından izole edilmesi. Asıl verinin veri tabanına yönetici ve güvenlik denetçileri tarafından düzenlenmesi.

14. Asıl olarak kullanılacak veri tabanı üzerinde yönetici hariç hiç bir veri güvenlikçinin yazma ve silme hakkının olmaması, değiştirme hakkının ise aynı anda iki veya üç veri güvenlikçinin şifresi girildikten sonra veya veri güvenlikçisi ve yönetici şifresiyle elde edilebilmesi.

Internet üzerinden geliştirilen uygulamalarda, veritabanları uygulamanın son noktasıdır. Bilgili ve deneyimli bir saldırgan eğer uygulama üzerinde bir boşluk bulursa veritabanındaki

bilgilere ulaşmakta zorlanmayacaktır. Saldırgan elde edebileceği yetkilerle girişlerini standart kullanıcı gibi gösterecek ve saklanması kolaylaşacaktır. Veritabanlarını korumak için uygulanacak önlemler uygulamanın işleme konma ve kullanıma açılama süresini ayrıca maliyeti arttıracaktır. Artan süre ve maliyete karşılık eldeki değerli bilgilerin dışarı sızmasını engelleyecektir diğer bir deyişle güvenliğin derecesi artacaktır.

7.7.6 Veritabanı Zaafiyetlerini Ölçmeye Yarayan Araçlar

1.Metasploit Framework, üretilmiş güvenlik araçları ve exploit'ler için geliştirilmiş bir platformdur. Network ve güvenlik uzmanları tarafından penetrasyon testleri gerçekleştirmek, sistem uzamanları için patch kurulumlarını kontrol etmek, ürün geliştirenler için regression testleri gerçekleştirmek için kullanılabilecek bir framework'tür. Bu framework Ruby programlama diliyle yazılmış ve C ve assembker 'da yazılmış kompanetler içerir.

2.Scrawlr – SQL Injection arama aracıdır.

3.DB Audit v4.2.24.8, Database Denetleme Uzmanlarının Oracle, Sybase, DB2, MySQL ve Microsoft SQL Server database'leri için profesyonel bir denetleme çözümüdür. Bu araçla database güvenlik ihtiyaçlarınıızı çoklu denetleme metodlarıyla iyi bir yapıya getirilebilir.

4.Sqlmap , SQLmap Python programlama dilinde geliştirilmiş bir otomatik SQL Injection aracıdır. Web uygulamalarındaki SQL Injection açıklarını tespit edip yararlanmayı hedeflemektedir. Hedef sistemde bir veya daha fazla SQL Injection tespit ettiğinde, kullanıcı arka-plandaki veritabanı sunucusu bilgisi alma, DBMS oturumu kullanıcı ve veritabanı alma, kullanıcı listesi alma, şifre hash'lerini alma, imtiyazlar, veritabanları ve DBMS tablo/kolonlarının tamamının listesini alabilme, kendi istediği SQL SELECT komutlarını çalıştırabilme, dosya sistemindeki istediği dosyayı okuyabilme gibi çok çeşitli seçenekler arasından istediğini seçebilmektedir.

7.8 Sosyal Mühendislik Tehditleri

Sosyal Mühendislik, Bilgisayar güvenliği terimleriyle Sosyal Mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklıklar olarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir.

Diğer bir deyiş ile teknik olmayan yöntemler ile bilgi elde etmektir.

Tehditleri tipleri aşağıdaki gibidir.:

- Sahte senaryolar uydurmak kullanıcılardan bilgi elde etmek (pretexting),
- Güvenilir bir kaynak olduğuna dair kullanıcıları ikna etmek (phishing),
- Truva atları (trojan) kullanarak kendini olduğundan başka (arkadaşı, müdür gibi tanıtmak ve bilgi alacağı kullanıcıyı ikna etmek) göstererek bilgi elde etmek,
- Güvenilir bilgi karşılığında yardım, para, eşantiyon, hediye, önermek
- Güven kazanarak bilgi edinmek,
- Omuz sörfü (kullanıcı farketmeden arkadan izlemek),
- Eski ve kullanılmayan donanımları incelemekle içindeki bilgilere erişmek,
- Çöp kutuları karıştırırak bilgi veye bilgiye erişim yöntemleri hakkında bilgi elde etmek gibi.

7.9 Güncel Tehditlerle İlgili Genel Değerlendirme

Kurumsal bilgi güvenliği tehditlerinin ağ ve sistemlerden web uygulamalarına doğru hızlı bir şekilde kaymakta olduğu görülmektedir. Dünyada olduğu gibi ülkemizde en fazla güvenlik açığına web uygulamalarında rastlanmaktadır. Kurumların genelde sınır ağ güvenliğinin sağlanmasıyla ilgili çözümleri olarak farkında oldukları güvenlik sistemleri güvenlik duvarı, saldırı tespit sistemleri, saldırı önleme sistemleri, anti-virüs programlardır. Öte yandan son 2008 ‘den beri de veri kaybı önleme (Data Loss Prevention) sistemleri gelişmektedir. Ancak web uygulama güvenliği kavramının dünyada olduğu gibi ülkemizde de, uygulamayı geliştiren yazılımcılarında dahil olduğu büyük bir çoğunluk tarafından tam olarak uygulanamadığı görülmektedir.

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için standartlar çerçevesinde teknik önlemlerin uygulanmasının 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.

2005- 2006 yılında yaygın olarak kullanılan ve özellikle 2006 yılının son aylarına damgasını vuran sazan avlama (phishing) saldırganlar tarafından kullanılan etkili bir saldırı yöntemidir. Ülkemizede özellikle bankalarımız bu phishing konusunda zaman zaman zor durumda kaldırılar. Bununla ilgili olarak banka müşteri de zaman zaman bu saldırıların kurbanı oldular.

zor durum Bu yöntem günümüzde de halen kullanılmaktadır . 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 (Carver ve Ferguson,2007).

Bilgi güvenliği alanında yaşanan güvenlik ihlallerinin giderek artan bir bölümü ağ, ve sistemlerden uygulamalara hatta veritabanlara 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 [34]. Yıllar içerisinde ağ ve sistemlerin güvenliğinin sağlanmasına ilişkin geliştirilen yöntemler kurumlar tarafından başarıyla uygulanmış ve Sınır Ağ Güvenliği (Perimeter Network Security) kavramının önemi çoğu kurum tarafından anlaşılmış ve gerekleri yerine getirilmiştir. Ancak benzer durumu uygulama ve veritabanı güvenliği için belirtmek henüz zordur. Bilgi güvenliğinin sağlanmasında uygulama ve veritabanı güvenliği merkezi kritik bir öneme sahiptir (Mcgraw, 2010).

Cenzic firmasının OWASP, SANS, OSVDB, Symantec ve US-CERT kaynaklarına dayanarak hazırladığı raporlar günümüzde ağ ortamlarında çalışan kişiler ve diğer uygulamalar tarafından erişilebilen uygulama yazılımlarındaki güvenlik zafiyetleri bilgi güvenliği tehditlerinin başında geldiği ve web uygulamalarında güvenlik zaafiyetlerin ve tehditlerin zamanla attığı görünmektedir [35].

Şekil 7.9.1.Web uygulamalarının zaafiyetleri artışı

Gartner, IDC ve Deloitte raporları incelendiğinde 2008 yılından itibaren gelişmiş ülke ve ekonomileri dahil tüm dünyayı etkileyen ve halen devam eden global krizle ile beraber kurum ve kuruluşların güvenlik teknolojilerine yeterli ölçüde yatırım yapmadıkları görülmektedir. Deloitte firmasının Teknoloji, Medya ve Telekomünikasyon (TMT) şirketlerini kapsayan bilgi ve bilişim güvenliği konusunda ilginç bulgulara erişen Küresel Güvenlik 2010 Araştırması'na göre; son bir yılda bu şirketlerin %10'u bilişim güvenliği bütçelerinde %10'dan fazla artışa giderken, %36'sının güvenlik yatırımı ise bir önceki yıla oranla %10'un altında kalmıştır [36].

Denetim ve danışmanlık şirketi Ernst & Young´ın 11´incisini düzenlediği "Küresel Bilgi Güvenliği Anketi" sonuçlarına göre de ülkemizde de güvenlik yatırımlarının yeterli yapılmadığı görülmüştür. Türkiye'nin de içinde bulunduğu 50 farklı ülkede yapılan araştırma sonuçlarına göre, şirketlerin bilgi teknolojileri ve güvenliğine dönük yaptığı yatırımlar arttığı halde hâlâ ihtiyacı karşılamıyor. Ayrıca ankete katılan çoğu katılımcı (yüzde 85), bilgi güvenliğinde yaşanan sorunların şirket itibarını doğrudan etkilediği inancını taşıdığı görülmüştür [37].

8. BİLGİ VARLIKLARIKLARINI KORUMAYI AMAÇLAYAN PENETRASYON TESTLERİ

Bilgi güvenliği yönetim sistemlerinin en önemli unsurlarından birisi denetim ve penetrasyon testleri (Sızma testleri)dir. Bilginin her gün önemini artırdığı günümüzde bilgiyi korumaya yönelik yapılan penetrasyon testleri de en popüler konularından biri olmuştur.

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 uygulanmadıgını anlamanın en iyi yolu bilgi sistemlerini denetim ve sızma testleriyle (Penetration Testing) test etmektir. 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 testlerini yapan birçok firma bulunmaktadır [38].

Ülkemizde bu testi yapan bazı firmlar ile sızma testleri konusunda görüşmeler yapılmış ve izlediği yöntemler hakkında bilgiler edinilmeye çalışılmıştır. Sızma testlerini yapanların geçmiş bilgilerini ve piyasadaki hazır araçlar (Nmap, Nesssus,Hping, Unicornscan, Scanrand, Xprobe, Snort, Qualys, Mcafee Foundstone, Nexpose, Eyee Retina, Inguma, W3af , vs) kullanarak yaptıkları tespit edilmiştir. Tez kapsamında yapılan sızma testleri sonucunda kurumlarda görülen en büyük güvenlik açığının literatür ve güvenlik firmaların yaptığı araştırmalarda vurgulandığı gibi web uygulamaları ve arkasındaki veritabanı açıklarınadan kaynaklandığı tespit edilmiştir. Özellikle kullanıcıdan girdi alınarak dinamik içerik sağlamak amacıyla veritabanı desteği sağlayan uygulama kodları (asp, jsp, php, cgi, vb.) web sitelerinin en zayıf halkalarını oluşturmaktadır. Ülkemizde kobi olarak tanımlanan orta ve küçük işletmelerin sunduğu web uygulamalarında bu açıkların büyük ölçekli firmalara göre daha yüksek olduğu tespit edilmiştir.

8.1 Penetrasyon Testi

Penetrasyon (Sızma) testi, Belirlenen bilişim sistemlerine mümkün olabilcek her yolun denenerek sızılmasıdır. Penetrasyon testinde amaç güvenlik açıklığını bulmaktan öte bulunan açıklığı değerlendirip sistemlere yetkili erişimler elde etmektir.

Penetrasyon test çeşitleri, Whitebox, blackbox, graybox olmak üzere genel kabul görmüş üç çeşit test vardır. Bunlardan blackbox genelde bilinen ve uygulanan penetrasyon test yöntemidir. Bu yöntemde testleri gerçekleştiren firmayla herhangi bir bilgi paylaşılmaz. Firma ismi ve firmanın sahip olduğu domainler üzerinden firmaya ait sistemler belirlenerek çalışma yapılır. Diğer yöntemlerde ise penetrayon testi yapacak firmayla belirli bilgiler paylaşılır.

Penetrasyon test, Vulnerability assessment kavramlarından farkı nedir?

Vulnerability Assessment(zaafiyet tarama), Belirlenen sistemlerde güvenlik zaafiyetine sebep olabilecek açıklıkların araştırılması. Bu yöntem için genellikle otomatize araçlar kullanılır(Nmap, Nessus, Qualys vs).

8.2 Penetrasyon Testi Bilgi Güvenliği İçin Neden Önemlidir

Kurumlarına sahip olduğu bilişim sistemlerindeki güvenlik zaafiyetlerinin üçüncü bir göz tarafından kontrol edilmesi ve zaafiyetlerin raporlanması ile kurumda bir farkındalık oluştururur ve kurum hemen önlem alabilir. Kurumsal bilgilerin ve sistemlerin artması ile bu sistemleri yönetenlerin gözden kaçırdığı zaafiyetlerin tespit edilmesi için açısından penetrasyon testlerin yapılması önem arzetmektedir. İletişim ortamların gelişmesi ve hackerlerin sayısı, bilgisi ve becerisi artması ile bu önem daha da atrmaktadır. Kurum hackerlara yem olmadan kendi güvenliği için beyaz şapkalı hackerlara kendi sisteminin önceden test ettirmesi yerinde bir önlem olacaktır.

8.3 Penetrasyon Testi Sonrası İzlenmesi Gereken Yol

Penetraston testi yaptırmak ne kadar önemliyse sonuçlarını değerlendirip aksiyon almak o kadar önemlidir.

- Penetsyon testin raporlarının üst yönetimle paylaşılıp yönetim desteğinin alınmalı,
- Sonuçlarının basit açıklıklar olarak değil, bir risk haritası kapsamında yönetime sunulması

- Açıklık hackerlar tarafından değerlendirilmesi durumunda kurumun kayıpları ortaya çıkarmalı ve yönetime sunulmalı,
- Raporu detaylıca inceleyip her bir açıklığın kimin ilgi alanına girdiğinin belirlenmesi yapılmalı,
- Açıklıkların kapatılmasının sağlanmalıdır.
- bir sonraki penetrasyon test tarihi belirlenmelidir.

8.4 Ülkemizde Penetrayon Testi Yapan Kurumlar

Ülkemizde de bu test her gün önemli hale geliyor. Test yapan firmalar aşağıdaki gibidir (Önal, 2009).

- **Lostar B.G** – http://www.lostar.com.tr/
- **Pro-G** http://www.pro-g.com.tr/
- **Nebula Bilişim Hizmetleri** http://www.nebula**bilişim**.com.tr/tr/home.aspx
- **ADEO** http://www.adeo.com.tr/
- **BizNet** http://www.biznet.com/
- **GamaSec -** http://www.gamasec.net/
- **Tubitak UEKAE** http://www.uekae.tubitak.gov.tr/

8.5 Penetrayon Testi İçin Kullanılan Yazılımlar

Test için birçok yazılım kullanılmaktadır. Bunlardan bazıları aşağıdaki gibi.

Açıkkod penetrasyon test yazılımları: Nmap, Nessus, Metasploit, Inguma, hping, Webscarab, jtr, W3af, Kismet,...

Ticari penetrasyon test yazılımları: Immunity Canvas, Core Impact, HP Webinspect, Saint Ssecurity Scanner, Retina, OpenVAS, AppDetective, gibi.

9. BİLİŞİM MEVZUATI ve ÜLKEMİZDEKİ BİLİŞİM HUKUKU

9.1 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 (Tbd, 2005).

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 sekilde veri islenmesine 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 Tasınabilirlik 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 Dernegi (NASD) Kuralları: Komisyoncuların ve hisse senedi alım-satımcılarının, kamuya duyurular da dâhil olmak üzere tüm aktivitelerinin kontrolü için bir sistem kurmak zorundadır. Bu sart, tüm elektronik iletişimin düzenli olarak araştırılması ve incelenmesine yönelik bir süreç gerektirir. Ayrıca, üye firmaların, tüm müşteri kayıtları ve islem 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 saglayacak 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.

9.2 Ülkemizde Bilişim Sistemleri ve Güvenliği İle Madde İçeren Kanunlar

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 yasalar aşağıda sıralanmıştır.

- İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında 5651 sayılı Kanun
- Elektronik Haberleşme Kanunu
- Elektronik imza kanunu
- Araştırma ve Geliştirme Faaliyetlerinin Desteklenmesi Hakkında Kanun
- Basma Yazı ve Resimleri Derleme Kanunu

- Basın İlan Kurumu Teşkiline Dair Kanun
- Basın Kanunu
- Basın Ve Yayın Yoluyla İşlenen Suçlara İlişkin Dava Ve Cezaların Ertelenmesine Dair Kanun
- Yeni Türk Ceza Kanunu
- Entegre Devre Topoğrafyalarının Korunması Hakkında Kanun
- Fikir ve Sanat Eserleri Kanunu
- Sermaya Piyasası Kanunu
- Sosyal Sigortlar ve Genel sağlık Sigortası Kanunun (Hasta bilgilerin gizliğini içeren kanun)
- Adli Sicil Kanunu (bilgilerin gizliliği ve cezai sorumluluk)
- Bilgi Edinme Hakkı Kanunu (Gizli bilgileri ayırarak bilgi veya belge verme)

9.3 Türkiye'de Bilişim Suçları Hukuku

İletişim ortam, uygulamaları, bu uygulamaları kullanların artması ve bu uygulamalarda yapılabilecek suistimalerin artması sonucunda özellikle bilgi güvenliğinin sağlanmasında caydırıcı rol oynaması açısından yukarıda yasa ve yönetmeliklerin yanında bilişim suçları tanımları yapılmıştır.

Bilgisayar, çevre birimleri, pos makinesi, cep telefonu, mobil cihaz gibi elektronik ortamlarda teknolojinin kullanılması ile işlenilen suçlar bilişim suçları olarak tanımlanmaktadır. Bilişim vasıtasıyla islenen suçlara, internet ve diğer bilişim sistemleri üzerinden de gerçeklestirilebilen küfür, hakaret, dolandırıcılık gibi klasik suçların yanında bilişime özgü suçlar olan verilerin tahrip edilmesi veya değiştirilmesi, sistemlere yetkisiz girişler, sistemin isleyişini değiştirmek örnek olarak verilebilir.

2002 yılından itibaren Emniyet Genel Müdürlüğü bünyesinde İnternet ve Bilişim Suçları Şube Müdürlüğün kurulması sonucu taşra teşkilatı olarak Şube Müdürlüğü içerisinde Bilişim Suçları Büro Amirliği adı altına çalışmalar sürdürülmüştür. Ülkemizde Bilişim Suçları ile yapılan mücadelede yaşanan yoğunluk, bilişim alanında hizmet veren birçok firma ve kurumun genel merkezlerinin veya temsilciliklerinin İstanbul'da bulunması nedeni ile Mali Suçlarla Mücadele Şube Müdürlüğü bünyesinde faaliyet gösteren Bilişim Suçları Büro

Amirliğinin kapatılması ve Bilişim Suçları Ve Sistemleri Şube Müdürlüğünün kurulması İçişleri Bakanlığının 25/04/2007 tarihli onayı ile uygun görülmüştür.

İstanbul Valiliğinin 29/05/2007 tarihli onayı ile ilde Bilişim Suçları ve Sistemleri Şube Müdürlüğü 03/09/2007 tarihinde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına bağlı olarak İstanbul Emniyet Müdürlüğü bünyesinde faaliyete geçirilmiştir [39].

9.4 Türk Ceza Kanunu Bilişim Suçları Bölümündeki Suçlar

Türk Ceza Kanununun bilişim suçları bölümünde suçlar 4 grubunda ele alınmıştır.

1. Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalma suçu (m.243)
2. Bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçu (m.244)
3. Bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu (m. 244/4)
4. Banka veya kredi kartlarının kötüye kullanılması suçu (m.245)

Bu suçların işlenmesi durumunda; duruma göre 2 yıldan 5 yıla kadar hapis ve adli para cezası da öngörülmektedir.

9.4.1 Bilişim Araçları İle İşlenebilecek Diğer Suç Tipleri

- Bilgisayar yoluyla dolandırıcılık
- Bilgisayar yoluyla sahtecilik
- Kanunla korunmuş bir yazılımın izinsiz kullanımı
- Yasadışı yayınlar
- Kişisel verilerin kaydedilmesi suçu
- Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu
- Verilerin yok edilmemesi suçu
- Haberleşmenin engellenmesi suçu
- Hakaret suçu
- Haberleşmenin gizliliğini ihlal suçu
- Nitelikli hırsızlık suçu
- Nitelikli dolandırıcılık suçu
- Kumar oynanması için yer ve imkan sağlanması suçu

9.4.2 Ülkemizde En Çok Karşılaşılan Bilişim Suçları

Bilişim Suçları alanında Ülkemiz başta olmak üzere Dünya genelinde en sık karşılaşılan suç türleri aşağıdaki gibidir [40]:

- İnternet Banka Dolandırıcılığı
- Banka ve Kredi Kart Dolandırıcılıkları
- BOTNET saldırıları
- Bilgisayar Korsanlığı (Bilişim sistemine girme, engelleme, değiştirme, verileri yok etmek vs.)

Bu maddeler aşağıdaki gibi detaylandırılabilir [40]:

- İnteraktif bankacılık dolandırıcılığı suçlarını işleyen şahısların kullandığı yöntemler zamana göre farklılık göstermesine rağmen; temelde kullanıcıyı aldatarak sahte internet sayfalarının taklit edilmesi, sahte e-posta bildirimleri, cep telefonlarına gönderilen mesajlar ya da banka operatörü gibi müşterileri arayan dolandırıcıların bankacılık işlemleri için gereken kişisel bilgiler ile hesap ve kredi kartlarına ait bilgilerin çalınması biçiminde karşımıza çıkmaktadır
- Başkalarının adına e-mail göndererek özellikle ticari ve özel ilişkileri zedeleme.
- Başkalarının adına web sayfası hazırlamak ve bu web sayfasının tanıtımı amacıyla başkalarına e-mail ve mesaj göndermek ve bu mesajlarda da mağdur olan şahsın telefon numaralarını vermek.
- Kişisel bilgisayarlar yada kurumsal bilgisayarlara yetkisiz erişim ile bilgilerin çalınması ve karşılığında tehdit ederek maddi menfaat sağlanması,
- Şirketlere ait web sayfalarının alan adının izinsiz alınması ve bu alan adlarının karşılığında yüklü miktarlarda para talep etmek.
- Özellikle pornografik içerikli CD/DVD kopyalamak ve satmak.
- Sahte evrak basımı gibi çok farklı konuları içerebilmektedir.

9.4.3 Bilişim Suçları İle İlgili Olarak Mağdur Olmadan Önce Yapılabilecek

Bilişim suçları ile ilgili olarak mağdur olmadan yapılanmasında yarar bulunanlar aşağıda sıralanmıştır [41].

- Şirketinize veya şahsınıza ait önemli bilgilerinizin yer aldığı bilgisayarınız ile özel güvenlik önlemleri almadan internete bağlanılmamalı.
- İnternet ortamında %100 güvenliğin hiçbir zaman sağlanamayacağını unutulmamalı.
- Özellikle anlık mesajlaşma (Chat) ortamında bilgisayarınıza saldırılabileceğini; chat de tanıştığınız kişilere şahsınız, aileniz, adres, telefon, işiniz v.s. konularda şahsi bilgilerinizi vermemeniz gerektiğini unutulmamalı.
- İnternet ortamında tanıştığınız kişilere hesap ve kredi kartı bilgilerinizi verilmemeli.
- İnternet üzerinden yapılan yazışmalarınızda karşınızdaki kurumlarla özel bir yöntemle yazışma yapılmasının yararlı olabilmektedir.

9.4.4 Bilişim Suçu İle Karşılaşıldığına Yapabilecekler

- Yasadışı siteler (web sayfaları) ile ilgili şikayetleri 155@iem.gov.tr adlı e-mail ihbar adresine bildirilebilir.
- Şahış veya kurumla ile ilgili şikayetçi olunan konular ile ilgili elde edebileceği tüm deliller ile birlikte Cumhuriyet Başsavcılığına müracaat ederek şikayetçi olunabilir.
- Şikayetçi olunan konular ile ilgili olarak yapılacak çalışma neticesinde ISP(İnternet Servis Sağlayıcının) yurt dışında bulunması durumunda Adli Makamlar tarafından yapılacak olan Adli İstinabe ile konunun takibi yapılabilmektedir.

10. SONUÇ ve ÖNERİLER

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 ve uygulamaları konusunda verilen dersler, 17 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 yazılacaktır.

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.

Kurumların günümüzde saldırganların teknolojik hızına yetişebilmesi ve kurumsal bilgi varlıklarını saldırılardan koruyabilmesi için bu tez çalışmasında da açıklanan kurumsal bilgi güvenliği yönetimini 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 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 bu 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 katkılar sağlayacağı beklenmektedir.

Bilginin bir kuruluşun faaliyetleri ve devamı için büyük bir önem taşıdığı yukarıda bahsedilmiştir. Bu kapsam ile bilginin güvenliğini sağlamak ve yönetmek için ISO/IEC 27001 Standardı ve bu standardın gereklilikleri, değerli bilgi varlıklarınızı yönetmenize, korumanıza ve özellikle de müşterilerinize güven vermenize yardımcı olacağı yine yukarıda habsedilmişti.

10.1 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 tam olarak 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 de 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. Yukarıda habsi geçen 2008 yılında Rus hackerlar tarafından Estonya'ya yapılan saldırıların özellikle kamu hizmeti sunan bir çok kurumun iş yapamaz duruma getirmesi, bilgi güvenliğine yönelik tehditlerin nitelik ve boyut değişimine uğradığı bir yıl olmuştur. Geçmis yıllarda saldırılar, yaygın ve hedef gözetmeksizin yapılmaktayken artık nokta hedefi gözeten ve bölgesel olarak düzenlenebilen organize saldırılar yapılmaktadır. Son yıllarda bilgi ve bilgisayar güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, kurumlar ve hatta devletler 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.

- Özellikle son zamanlarda gittiçe artış gösteren ve ülkelerin tüm internet alt yapılarını tehdit eden DDoS (Distributed Denial Of Service) henüz bir çözüm bulunamamıştır. DoS ve DdoS saldırılarına karşı özellikle ülkemizin kritik kurumlarının ağları ve hizmetleri kesintiye uğramaması için ülkemize yapılan network trafiği izlenmelidir.
- 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 sürekliligi planlarının uygulanması gibi stratejiler, kurumlar tarafından uygulanmalıdır.
- Bilişim sektöründeki gelişmelere bağlı olarak ülkemizde ve dünyada hukuksal sorunlarda gün geçtikçe artmaktadır. Tez kapsamında yapılan çalışmalar 2006-2007 yıllarına kadar yapılan saldırıların daha çok düzenleme amaçları geçmiste olduğu gibi şan, söhret, hava, kişisel tatmin iken günümüzde ekonomik ve hatta stratejik amaçlı saldırılar daha ön plana çıkmaktadır. Saldırganlar tarafından yazılan kötücül yazılımlar, artık maddi çıkar sağlamak için kullanıldığı gibi günümüzde devletler arasında çıkan sorunlardan sonra hackerler organize olup sanal savaşlar başlatmaktadır. Örneğin geçmis 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 isbirliği yapmaya ve örgütlenmeye baslamışlardır. Saldırılar artık organize ve planlı olarak yapılmaktadır. Bunun yanında saldırganlar bir araya gelerek, belirli organizasyonlar adı altında teşkilatlanmakta, bilgi alısverişi 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 (adli bilişimciler) sayısının artmasına ihtiyaç duyulmaktadır.

- Tez kapsamında yapılan araştırmalar sonucunda ülkemizde bilişim suçları konusunda kanunların ve adli bilişimcilerin henüz yetersiz olduğu değerlendirilmiştir.
- 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. Tez çalışmasında yapılan inceleme sonucunda İstanbul Bilgi Üniversitesi'nin 16 Mayıs 2010 tarihli Resmi Gazete'de yayımlanan Yönetmeliği ile faaliyete geçen, ülkemizin ilk Bilişim ve Teknoloji Hukuku Enstitüsü'nün master programı YÖK tarafından onaylandığı görülmüştür.
- 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 2010 yılında gelinen noktaya bakıldığında ISO–27001

standardının dünya genelinde 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 geçmis 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 iş 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, kurum içinde farkındalık eğitimlerin verilmesi 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 zorlağtıracak 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 standardı bu tez kapsamında kapsamlı olarak incelenmiş ve sonuç olarak farklı sektörler için:
    - GBK(**G**izlilik, **B**ütünlük, **K**ullanılabilirlik veya Erişebilirlilik) risklerinin yönetildiğine emin olmak,
    - GBK yönetimindeki hukuksal yaptırımların ve önlemlerin yasalara uygunluğundan emin olmak,
    - GBK altyapısının içerdiği uygulamaların ve denetimlerin, kurumların amaçladığı güvenlik seviyesi ile uyuştuğunu göstermek,
    - GBK 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 edilmistir.

- BGYS standartlarının kurumlara uyarlanması, anlatılması, kullanıcı, teknik çalısanların ve yöneticilerin eğitilmesi konusunda kuruluşların danışmanlık hizmetleri almalarının daha yararlı olabilmektedir.
- 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 değerlendirildiginde 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 denetim ve penetrasyon testleriye test edilmesi gerekmektedir.
- Penetrasyon testleriyle denenen bilgi sistemleri teknik (bilgisayar ağları, doküman yönetim sistemleri, süreç analizleri, vb.), insan ve teknik olmayan (çalısanların bilinci, kurum kültürü, yönetimsel prosedürler, fiziksel güvenlik, vb.) etkenler dikkate alınarak bir bütün olarak degerlendirilmelidir. Denetim ve penetrasyon 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.
- 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 penetrasyon 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 çalısanların bu konuda yeterli bilgiye sahip olmadıkları tespit edilmiştir. Bu tez çalışmasının sosyal mühendislik konusunda da kurumlar ve çalısanlar nezdinde farkındalık yaratması beklenmektedir.

- Dünyada olduğu gibi ülkemizde de en fazla güvenlik açıklarına web ve webi destekleyen uygulama ve veritabanlarında olduğu tespit edilmiştir.. 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 gerektigi fikrine varılmıstır.
- 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 çalısanlarına hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabilecegi 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, açıkların takip edilip güncellemesi, 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 isçilik kurumun kendi bünyesinde mevcut değilse dış kaynak kullanımına gidilmelidir. Aksi takdirde teknoloji seçiminin doğru yapılmasına rağmen insan faktörü ve eğitimlere gerekli hassasiyetin gösterilmemesi, teknolojik yatırımlarından tam olarak yararlanamayacağı hatta boşa çıkartacağı gibi daha çok güvenlik ihlallerinin meydana gelmesine neden olacak ve yatırımların boşa gitmesi ve kaynakların israf edilmesi sonucunu doğuracaktır.

10.2 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.

- İncelenen tez konusunun güncel olması ve daha önce bu konuda yapılan bir detaylı çalışmalara 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 kurumların, sivil toplum örgütlerinin ve eğitim kurumlarının sitelerinden olmasına özen gösterilmesi nedeniyle uzun soluklu araştırmaların yapılması,

- Tez konusunda yaralanılan kaynakların genelinin ingilizce olması, Türkçeye çevrilmesi sırasında anlam kayıplarının yaşanmaması ve bilgilerin doğru aktarılabilmesi için özverili çalışmalara ihtiyaç duyulması gibi zorluklarla karşılaşılmıştır.

Tez çalışması sırasında ilk günden son güne kadar birçok kazanım elde edilmiştir. Bu kazanımlardan önemlileri aşağıda maddeler halinde açıklanmıştır:

Bunlar:

- 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 bilgi güvenliğiyle ilgili akademik ve ticari alanda ülkemizde söz sahibi olan uzmanlarla görüşmeler yapılmış ve bunun sonucunda kurumsal bilgi güvenliği yönetimi konusu gibi çok değerli olan bir konu üzerinde ciddi bilgi paylaşımları yaşanmıştır.
- Tez çalışması tez yazarının iş yerindeki bakış açısını değiştirerek kuruma ve kariyerine yarar sağlamış ve kurumun bilgi güvenliği yönetim sistemine yarar sağlamıştır.
- 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 sağlanabilecegi dolayısıyla güvenliğin süreklilik arz ettiği daha iyi kavranmıştır.

10.3 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 güvenlik sistemlerine yönelik milli yazılımlar ve yöntemler üretilmeli ve geliştirilerek kullanılmalıdır.
- Ülkemizde kurumsal bilgi güvenliği konusunda daha fazla çalışma yapılmalıdır. Özellikle üniversiteler ve araştırma kurumlarında “Kurumsal Bilgi Güvenliği” dersleri açılmalıdır.

- Bu tez çalışmadında bir kez daha ortaya konuldugu gibi "yüksek seviyede bir GBK sağlanması için teknoloji, eğitim ve insan faktörlerine gerektiği kadar önem verilmelidir.
- Penetrasyon testleri ve denetimler yılda enaz bir kez yapılmalıdır.
- Kurumların ekipman ve yazılım güncellemelerine bağlı olarak bu denetimler ve testler sıklaştırılmalıdır.
- Denetimler risk tabanlı yani riski yüksek olan daha detaylı ve sık denetlenmeli biçiminde yapılmalıdır.
- Güvenlik bilinci ilk öğretimden başlamalı ve işyerinde de güncelliği korumayacak şekilde geliştirilmedir.
- Ülkemizde penetrasyon testleri ücretsiz yapan devlet destekli merkezler oluşturulmalı veya bu hizmet üniversiteler üzerinden 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 bir kaynak olması nedeniyle, bu alanda yapılacak diğer çalışmalar ve kurumsal bilgi güvenliğinin sağlanmasını önemseyen kuruluşlar için rehber bir kaynak olarak kullanılabilecegi ümit edilmektedir.

Kurum veya kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları için standartlar çerçevesinde teknik önlemlerin uygulanmasının 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.

KAYNAKLAR

Abrams, D. M. ve Joyce, V. M., (1995) "Trusted System Concepts", Computers & Security, 14(1):45-56.

Argyris, C., (1993), Knowledge For Action: A Guide To Overcoming Barriers To Organizational Change, Jossey-Bass, San Francisco.

Arnason, S. ve Willett K., (2008), How To Achieve 27001 Certification: An Example Of Applied Compliance Management, Auerbach Publications, New York.

Artz, D., (2001), Digital Steganography: Hiding Data Within Data, Internet Computing Publications, San Francisco.

Atasever, M., (2007), "Cmmı Süreç İyileştirme Yaklaşımı", Yazılımda Toplam Kalite Çalışması Konferansı, Ankara.

Barman, S., (2001), Writing Information Security Policies, New Riders Publishing,Indianapolis.

Beaver, K. ve Herold, R., (2005), The Practical Guide To Hıpaa Privacy And Security Compliance, Auerbach Publications, Washington Dc.

Bell, D. ve Padula, L., (1975), "Secure Computer System: Unified Exposition And Multics Interpretation", The Mitre Corporation Technical Report :75-81, Bedford.

Bhatt, G. D., (2001), "Knowledge Management İn Organizations: Examining The Interaction Between Technologies, Techniques And People", Journal Of Knowledge Management, 5 (1):71-76.

Boran, S., (2000), It Security Cookbook, Boran Consulting Press, Blonay.

Borman, J., (2009), Pmp Project Management Knowledge Areas & Processes. Art Media, Boston.

BS., British Standard, (2005), Business Continuity Management : Part 2- The Specification, BS Media, London.

Cache, J. ve Liu,V., (2007), Hacking Exposed Wireless: Wireless Security Secrets & Solutions, Mcgraw-Hill Osborne Media, Chicago.

Calder, A. ve Watkins S., (2007), Information Security Risk Management For Iso27001/17799, It Governance Press, London.

Calder, A., (2005), Nine Steps To Success: An Iso 27001 Implementation Overview, It Governance Publishing, Cambridgeshire.

Calder, A., (2006), Implementing Information Security Based On Iso 27001 And Iso 17799: A Management Guide, It Governance Publishing, Cambridgeshire.

Canbek, G. ve Sağıroğlu S., (2006) "Bilgi, Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9(3):69-72.

Canbek, G. ve Sağıroğlu, S., (2006), Bilgi Ve Bilgisayar Güvenliği: Casus Yazılımlar Ve Korunma Yöntemleri, Grafiker Yayıncılık, Ankara.

Carver, C.R. ve C., Ferguson, J. A., (2007), "Phishing For User Security Awareness", Computers & Security, 26(1): 73-75.

Chen, M. T., Elder, M. ve Thompson, J., (2005), Electronic Attacks: The Handbook Of Information Security, John Wiley & Sons, New York.

Clarke, J., (2009), Sql Injection Attacks And Defense, Syngress Publishing, Burlington.

Çağlayan, U., (2003), "Bilgi Güvenliği: Dünyadaki Eğilimler", Ulaknet Sistem Yönetimi Konferansı, 5-6.05.2003, Ankara.

Davis, Z. (2005), Network Intrusion Prevention Systems Product Comparison Guide,Tips-It Publishing, New York.

Edney, J. ve Arbaugh, W. A., (2003), Real 802.11 Security: Wi-Fi Protected Access And 802.11i, Addison Wesley, Boston.

Egan, M. ve Mather, T., (2004), The Executive Guide To Information Security: Threats-Challenges-And Solutions, Addison-Wesley Professional, Massachusetts.

Floridi, L., (2010), Information: A Very Short Introduction, Oxford University Press, New York.

Fry, S., (2001), "Information Security Guidelines For The Deployment Of Deployable Switched Systems", Chairman Of The Joınt Chiefs Of Staff Instruction, Part-2:3-6.

Garfinkel, S. L., (1995), "Aohell", The Risk Digest, 17(42):3-5.

Gaudin, S., (2007), "Anycast And Communication Foiled February's Root Server Attack", Infomationweek, 23(1):23-26.

Gelbstein, E. ve Kamal, A., (2002), "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, 47-59, New York.

Gürkas, G. Z., Durukan, S., Zaim, A. H., Demir, A. ve Aydın, M. A., (2005), "802.11b Kablosuz Ağlarda Güvenliğin Ağ Trafigi Üzerindeki Etkilerinin Analizi", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, 8-10-11.2005, İstanbul.

Hoath, P., (1998), "Telecoms Fraud, The Gory Details", Computer Fraud And Security, 20(1):10–14.

Humphreys, E., (2007), Implementing The Iso/Iec 27001 Information Security Management System Standard, Artech Print On Demand, Norwood.

Isaca, (2009), Cisa Review Manual 2009, Isaca Press, Rolling Meadows.

ISO., Organizastion, (2005), Iso 27002:2005 Information Technology — Security Techniques — Code Of Practice For İnformation Security Management, ISO Publication, Switzerland.

Johnson, B. ve Higgins, J., (2007), Itıl And The Software Lifecycle: Practical Strategy And Design Principles, Van Haren Publishing, Amersfoort.

Kabay, E.,(2007) "Social Engineering İn Penetration Testing :Penetration Tests With A Social-Engineering Angle", Network World, 201:13-17.

Landoll, J.D., (2006), The Security Risk Assessment Handbook: A Complete Guide For Performing Security Risk Assessments, Auerbach Publications, New York.

Lockhart A. , (2006), Network Security Hacks, O'reilly Media, Ca Sebastopol.

Malone,T., Menken, I. ve Blokdijk, G., (2009), Itıl V3 Foundation Complete Certification Kit - 2009 Edition: Study Guide Book And Online Course, Emereo Pty Ltd Publishing, Brisbane.

Mcgraw, G., (2010), "Software Security", Security & Privacy Magazine Ieee, 2(2):80 – 81.

Mitnick, K. D., Simon, L. W. ve Wozniak, S., (2003) , The Art Of Deception: Controlling The Human Element Of Security, Wiley Publishing, New York.

Munro, K., (2005). "Social Engineering", Infosecurity Today, 2(3):44.

Nonaka, I. ve Takeuchi, H.,(1995), The Knowledge-Creating Company", Oxford University Press, New York.

Numanoğlu, E., (2005), "Bs7799 Bilgi Güvenligi Yönetim Sistemi", Önce Kalite Dergisi, 13(93):43-46.

Önal, H.,(2009),"10 Soruda Pentest(Penetrasyon Testleri)", Netsec Güvenlik Bülteni,VI:7-11.

Özinal, S., (2009), "Ödeme Kartları Endüstrisi Veri Güvenliği Standardı", Bthaber Dergisi, (702):12-15.

Pfleeger, P. C., (2006), Security İn Computing, Fourth Edition, Prentice Hall, Westford.

Ramses, A., (2009), "New treat : DDoS", Rsa Information Security Conference 2009, 21-26 Nisan 2009, San Francisco.

Rattray, J. G., (2001), "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 Report, 85-92, Colorado.

Ruiu, D., (2006),"Learning From Information Security History", Ieee Security & Privacy, 4(1):78-79.

Sağıroğlu, S. ve Tunçkanat, M., (2002), "Gizli Bilgilerin İnternet Ortamında Güvenli Olarak Aktarımı İçin Yeni Bir Yaklaşım" , Popüler Bilim Dergisi, 9(105), 12-17.

Sağıroğlu, S., Tunçkanat, M. ve Altuner, M., (2002),"Kriptolojide Yeni Bir Yaklaşım Resimli Mesaj", Telekomünikasyon Ekseni Dergisi, Telekomünikasyon Kurumu, 2(2):22-24.

Shahim, A., (2009), It Governance Attestation, Sdu Uitgevers Press, Den Haag.

Shinder, L. D. ve Tittel, E., (2002), Scene Of The Cybercrime: Computer Forensics Handbook, Syngress Publishing Inc., Rockland.

Solms, B., (2006) “Information Security – The Fourth Wave”, Computers & Security, 25(3):166-167.

Sunay, S., (2003), “Bilişim Güvenliği”, Pro-G Oracle Security White Paper, V.1, 31-33.

Tbd, (2005), E-Devlet Uygulamalarında Güvenlik Ve Güvenilirlik Yaklaşımları 4. Çalısma Grubu Sonuç Raporu, Türkiye Bilişim Derneği.

Tbd., (2006), Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0, Türkiye Bilişim Derneği Yayınları, Ankara.

Tioia, The Institute Of Internal Auditors, (2006), Information Technology Controls, Iaa Gtag, Florida.

Tipton, F. H. ve Krause, M, (2004), Information Security Management Handbook, Auerbach Publications, New York.

Tse, (2006), Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, TSE, Ankara.

Vacca, J., (2006), Guide To Wireless Network Security, Springer, New York.

Wozniak S. ve Smith G. , (2006), Computer Geek To Cult Icon,Ww Norton And Company Press, New York.

Yerlikaya, T., Buluş, E. ve Buluş, N., (2006), Kripto Algoritmalarının Gelişimi Ve Önemi”, Akademik Bilişim 2006, Pamukkale Üniversitesi Yayınları, Denizli.

Yıldırım, B, (2010), "Bilgi Güvenliği Stratejisi", ODTÜ IV. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, 6-8 Mayıs 2010, Ankara.

Zwicky, E. ve Cooper, S. ve Chapman B, (2000), Building Internet Firewalls, O'reilly Media, Ca Sebastopol.

İNTERNET KAYNAKLARI

[1.] "2010 Tmt Global Security Study", Http://Www.Deloitte.Com/View/Tr_Tr/Tr/Sektorler/Tmt/5ab7df0a273f8210vgnvcm100000ba42f00arcrd.Htm, (16.06.2010).

[2.] Computerworld Dergisi , Http://Www.Computerworld.Com/S/Article/77360/How_To_Toughen_The_Weakest_Link_İn_The_Security_Chain , (Erişim Tarihi :30.10.2009).

[3.] "Information Security Standards", Http://En.Wikipedia.Org/Wiki/Iso/Iec_27001, (08.07.2010).

[4.] "İso27001certificates and Turkey" , Http://Www.İso27001certificates.Com/Taxonomy/Certificatesresults.Asp, (02.26.2010.

[5.] "Bilgi Çağı", Http://Tr.Wikipedia.Org/Wiki/Bilgi_%C3%A7a%C4%9f%C4%B1, (12.01.2010).

[6.] "Google Corporate Information", http://Www.Google.Com/İntl/En/Corporate/Facts.Html, (16.03.2010).

[7.] "Google Market Value", Http://Www.Nasdaq.Com/Reference/Barchartsectors.Stm, (7.6.2010).

[8.] "Bilişim", Http://Tdkterim.Gov.Tr/?Kelime=Bili%Feim&Kategori=Terim&Hng=Md, (03.04.2010).

[9.] "Operation Sundevil", Http://En.Wikipedia.Org/Wiki/Operation_Sundevil, (13.11.2009).

[10.] "Kevin Mitnick", Http://en.Wikipedia.Org/Wiki/Kevin_Mitnick , (05.12.2009).

[11.] "Prince2", Http://Www.Prince-Officialsite.Com/Home/Home.Asp, (10.11.2009).

[12.] "Communications_Security", Http://En.Wikipedia.Org/Wiki/Communications_Security, (05.01.2010).

[13.] "Dos Appliance" , Http://Www.Cisco.Com/En/Us/Products/Ps5888/ , (02.04.2010).

[14.] "Nac", Http://Www.Cisco.Com/En/Us/Solutions/Collateral/Ns340/Ns394/Ns171/Ns466/At_A_Glance_C45-542749.Pdf, (15.12.2009).

[15.] "Once Thought Safe, Wpa Wi-Fi Encryption İs Cracked", Http://Www.Pcworld.Com/Businesscenter/Article/153396/Once_Thought_Safe_Wpa_Wifi_Encryption_is_Cracked.Html , (19.03.2010).

[16.] "Ağ Güvenliği İçin 10 Kural", Http://Www.Cyber-Security.Org.Tr/Madde/135/A%C4%9f-G%C3%Bcvenli%C4%9fi-%C4%B0%C3%A7in-10-Kural, (03.03.2010).

[17.] "Information Security", Http://En.Wikipedia.Org/Wiki/Information_Security, (15.03.2010).

[18.] "Information Security Standards", Http://En.Wikipedia.Org/Wiki/Iso/Iec_27001, (08.07.2010.

[19.] "Cobit", Http://Tr.Wikipedia.Org/Wiki/Cobit, (18.03.2010).

[20.] "Cobit Framework", Http://Www.isaca.Org/Knowledge-Center/Cobıt/Pages/Overview.Aspx, (19.12.2009).

[21.] "Payment Card Industry Data Security Standard", Https://Www.Pcisecuritystandards.Org/index.Shtml, (05.11.2009).

[22.] "Bs 25999 Business Continuity", Http://Www.Bsigroup.Com/En/Assessment-And-Certification-Services/Management-Systems/Standards-And-Schemes/Bs-25999/, (19.01.2010).

[23.] "Iso/Iec 27001 Sertifikası Almasının Avantajları", Http://Www.Bsi-Turkey.Com/Tr/Tetkik-Ve-Belgelendirme-Hizmetleri/Yonetim-Sistemleri/Standartlar-Ve-Urunlerimiz/Iso-Iec-27001/, (27.11.2009)

[24.] "Iso 27001 Bgys'ye Hazırlık Çalışmaları", Http://Blog.Lostar.Com/2009/03/Kurumlara-iso-27001-Uygulanmasi.Html, (14.02.2010).

[25.] "Çok Katmanlı Iso 27001 Süreci", Http://Www.Bilgiguvenligi.Gov.Tr/Teknik-Yazilar-Kategorisi/Cok-Katmanli-iso-27001-Sureci.Html, (12.04.2010).

[26.] "Iso/Iec 27001 Belgelendirme Yöntemi", Http://Www.Bsi-Turkey.Com/Tr/Tetkik-Ve-Belgelendirme-Hizmetleri/Yonetim-Sistemleri/Standartlar-Ve-Urunlerimiz/Iso-Iec-27001/, (19.12.2009).

[27.] "Current List Of Certification Bodies in International Register Of Isms Certificates", Http://Www.iso27001certificates.Com/Certification_Directory.Htm, (11.01.2010).

[28.] "Tse Akreditasyon", Http://Www.Tse.Org.Tr/Turkish/Kaliteyonetimi/27001.Pdf, (11.01.2010).

[29.] "Number Of Certificates Per Country in International Register Of Isms Certificates", Http://Www.iso27001certificates.Com/Register%20search.Htm, (15.01.2010).

[30.] "Turkey Certified Company in International Register Of Isms", Http://Www.iso27001certificates.Com/, (19.01.2010).

[31.] "Kurumsal Bilgi Güvenliği Ve Güncel Tehditler", Http://Www.Cyber-Security.Org.Tr/Madde/183/Kurumsal-Bilgi-G%C3%Bcvenli%C4%9fi-Ve-G%C3%Bcncel-Tehditler, (11.04.2010).

[32.] "The Goal Of Attacks İs Going To Where", Http://Www.Gartner.Com/Technology/Analysts.Jsp, (12.10.2009).

[33.] "Veri Tabanlarını Bekleyen Tehlikeler: Şırınga Edilen Sql İfadeleri", Http://Www.Enderunix.Org/Docs/Sql_İnjection.Pdf, (12.11.2009).

[34.] "Gartner Magic Quadrant On Static Application Security Testing- Feb. 2009", Http://Www.Dragoslungu.Com/2009/02/15/Gartner-Magic-Quadrant-On-Static-Application-Security-Testing-Feb-2009/, (05.11.2009).

[35.] "Cenzic Web Application Security Trends Report – Q3-Q4, 2009", Http://Www.Cenzic.Com/Downloads/Cenzic_Appsectrends_Q3-Q4-2008.Pdf, (07.05.2010).

[36.] "2010 Tmt Global Security Study: Bounce Back", Http://Www.Deloitte.Com/View/Tr_Tr/Tr/Sektorler/Tmt/5ab7df0a273f8210vgnvcm100000ba42f00arcrd.Htm, (16.06.2010).

[37.] "Internet: Ernst & Young´In "Küresel Bilgi Güvenliği Anketi ", Http://Www.Ey.Com/Publication/Vwluassets/Bilgi_Guvenligi_Anketi_Bb/$File/Ernst%20&%20young%20bilgi%20g%C3%Bcvenli%C4%9fi%20anketi%202008%20-%20b%C3%9clten.Pdf, (03.03.2010)

[38.] "10 Soruda Pentest", Http://Blog.Lifeoverip.Net/2009/10/06/10-Soruda-Pentestpenetrasyon-Testleri/, (10.07.2010).

[39.] "Bilişim Suçları ve Sistemleri Şube Müdürlüğü", Http://Bilisimsuclari.İem.Gov.Tr/, (15.03.2010).

[40.] "Kaçakçılık Ve Organize Suçlarla Mücadele- Bilişim Suçları Ve Yükselen Trentler", Http://Www.Kom.Gov.Tr/Tr/Konudetay.Asp?Bkey=64&Kkey=172 , (25.05.2010).

[41.] "Ego Genel Müdürlüğü- Ülkemizdeki Bilişim Suç Tipleri", Http://Web.Ego.Gov.Tr/İnc/Newsread.Asp?Id=247, (12.04.2010).

ÖZGEÇMİŞ

Doğum tarihi	01.11.1973	
Doğum yeri	Şanlıurfa	
Lise	1988-1991	Gaziantep Atatürk Lisesi
Lisans	1992-1996	Yıldız Teknik Üniversitesi. Elektrik Mühendisliği
Yüksek Lisans	2009-2010	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elekt Mak. ve.Güç Elektoniği Anabilim Dalı

Çalıştığı kurum(lar)

1994-1997	IBM (Part time)
1997-2001	TURKCELL- ENTER
2001-2002	New York NESTECH
2002–2006	SUPERONLINE, Istanbul
2006-Devam ediyor	MKK