146162

T.C.
DUMLUPINAR ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı

Yüksek Lisans Tezi

İŞLETMELERİN AĞ – BİLGİ SİSTEMLERİNDE BİLGİ GÜVENLİĞİNİN YÖNETİMİ VE BİR UYGULAMA

Danışman

Yrd.Doç.Dr.Hakan ÇELİKKOL

146162

Hazırlayan

Faik BAŞHAN

0291013137

Kütahya – 2004

İŞLETMELERİN AĞ – BİLGİ SİSTEMLERİNDE BİLGİ GÜVENLİĞİNİN YÖNETİMİ VE BİR UYGULAMA

(Yüksek Lisans Tezi)

Faik BAŞHAN

Kütahya - 2004

Yüksek lisans tezi olarak sunduğum "İşletmelerin Ağ – Bilgi Sistemlerinde Bilgi Güvenliğinin Yönetimi Ve Bir Nato Biriminde Uygulaması" adlı çalışmamın, tarafımdan bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım kaynakların kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılanlardan yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

28/06/2004

Faik BAŞHAN

Kabul ve Onay

Faik BAŞHAN'ın hazırladığı "İşletmelerin Ağ – Bilgi Sistemlerinde Bilgi Güvenliğinin Yönetimi Ve Bir Uygulama Kooperatifçilik Kapsamında Konut Yapı Kooperatiflerinin Sorunları Ve Çözüm Önerileri" başlıklı Yüksek Lisans tez çalışması, jüri tarafından lisansüstü yönetmeliğin ilgili maddelerine göre değerlendirilip kabul edilmiştir.

28. / 06/ 2004

Tez Jürisi

Yrd. Doç. Dr. Hakan ÇELİKKOL (Danışman)

Yrd. Doç. Dr. Derya ERGUN

Yrd. Doç. Dr. Hayrettin ÖZLER

Prof. Dr. Ahmet KARAASLAN

Sosyal Bilimler Enstitüsü Müdürü

ÖZGEÇMİŞ

Faik BAŞHAN, 1971 yılında Ankara'da doğmuştur. İlk ve orta öğretimini Merzifon AMASYA'da tamamladıktan sonra 1988 yılında Kuleli Askeri Lisesinden, 1993 yılında da Hava Harp Okulu Yönetim bölümünden mezun olmuştur. 1993 ve 1995 yılları arasında İZMİR'de 2nci Ana Jet Üs Komutanlığında ve Hava Teknik Okullar Komutanlığında eğitimini tamamlamıştır.

1995 yılında ESKİŞEHİR 1nci Ana Jet Üs Komutanlığına atanmış ve 2001 yılına kadar çeşitli görevlerde bulunmuştur. Halen görev yapmakta olduğu NATO CAOC6 Komutanlığında Görev Analiz Subayı olarak çalışmaktadır.

2002 yılı güz döneminde Kütahya Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü Yönetim – Organizasyon Yüksek Lisans programına başlamıştır.

ÖZET

Bilişim çağına ve bilgi toplumuna geçiş süreci ile birlikte "değişimin değişmezliği" temel ilkesi paralelinde organizasyonlar faaliyetlerini sayısal ortama taşımışlardır. Bu gelişim sürecinin kaçınılmaz bir etkisi olarak tüm kurum ve kuruluşlar için bilgisayar ağı yapılanmasıyla birlikte intranet veya internet ortamlarında bilgi paylaşımı zorunlu hale gelmiştir. Elbetteki bu zaruret, bilgiye erişim, bilgiyi işleme, çabuk karar alabilme ve çabuk sonuca varabilme konularında her seviyedeki kurum ve kuruluşlara yüksek fayda sağlamakla birlikte, bilgi güvenliği ihlallerini ve bu konuda alınması gereken önlemleri ve organizasyon yapılanmalarında bir güvenlik yönetimini de gündeme getirmiştir.

Yapılan tez çalışmasında bilgi güvenliği yönetiminin esasları, önemi ve hangi konuları kapsaması gerektiği üzerinde durularak, kapsamlı bir bilgi güvenliği yönetim yapısı oluşturulmaya çalışılmıştır. Bölüm 1, ağ sistemleri, ağ sistemlerinin güvenliği, işletmelerin karşılaşacakları tehditler ve alınacak önlemler üzerine yoğunlaşmıştır. Bu bölümde bilgi güvenliğinin teknik kısmı öne çıkmaktadır. Bölüm II'de ise ağ bilgi güvenliği, yönetimsel açıdan incelenmiş ve bilgi güvenliği yönetim modellerini kapsayan konular açıklanmaya çalışılmıştır.

İşletmelerin ağ yapılarındaki bilgi güvenliğinin yönetiminin uygulaması, bilgi ağ yapılanmasında önemli bir birikime ve altyapıya sahip olan NATO sistemleri üzerinde yapılmıştır. Uygulama esnasında konu ile ilgili uluslararası standartlar esas alınmıştır.

ABSTRACT

The organizations transferred their activities into digital environment through the principle of " unchanging of changing" during the process of passing to the information age and information community. Information sharing became compulsory in the intranet and internet environment for all kinds of organizations by the computer network structuring as an inevitable side effect of this developing process. Absolutely this necessity figured out the information security breaches, precautions required for handling the security issues and management of security in the organizational structuring while providing high level advantages to the organizations about accessing to the information, processing of information, quick decision making and rapidly resulting of managerial issues.

In this study, a comprehensive information security management structure was tried to form by emphasizing the information management basics, importance and which topics should be covered. Part I focused on the network systems, network system security, possible threats for organizations and precautions to be taken. Technical dimensions of information security are highlighted in this part. In Part II, network information security was examined through the managerial aspect and the issues, which are covering the information security management models, were tried to explain.

The implementing of information security in the organizations' network structures was practiced on the NATO systems, which have great background and infrastructure on information management structuring. During the implementation of the study, international standards were taken into consideration related to the subject examined.

İÇİNDEKİLER

Sayfa

İKİNCİ BÖLÜM
BİLGİ GÜVENLİĞİ VE YÖNETİMİ

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

GRAFİKLER LİSTESİ

KISALTMALAR

ADP	Automated Data Process – Otomatik Bilgi İşlem
AES	Advanced Encryption Standard – Gelişmiş Şifreleme Standardı
ANS	Advance Network Services – Gelişmiş Ağ Hizmetleri
CD	Compact Disc
COMPUSEC	Computer Security – Bilgisayar Güvenliği
COMSEC	Communication Security – Haberleşme Güvenliği
CRYPTOSEC	Şifre güvenliği
DES	Data Encryption Standard – Veri Şifreleme Standardı
DNS	Domain Name System
DVD	Digital Video Disc
EMSEC	Yayım güvenliği
E-Posta	Elektronik Posta
E-Ticaret	Elektronik Ticaret
FAN	Family Area Network – Aile Alan Ağı
FTP	File Transfer Protocol – Dosya Transfer Protokolü
GAA	Geniş Alan Ağı
HTTP	Hyper Text Transfer Protokol
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
ISP	Internet Servis Provider (İnternet Servis Sağlayıcı)
LAN	Local Area Network – *Bkz. YAA*
P2P	Peer to Peer
RAM	Read Access Memory (Bellek)
SMTP	Simple Mail Trasfer Protocol
TCP/IP	Transmission Control Protocol/ Internet Protokol
TRANSEC	İletim güvenliği

UPS	Uninterrupted Power Source
USB	Universal Serial Buss
VPN	Virtual Private Network (Sanal Özel Ağ)
WAN	Wide Area Network – *Bkz.GAA*
WWW	World Wide Web
YAA	Yerel Alan Ağları

TEZ HAKKINDA

Araştırmanın Problemi

Bilgi güvenliği nedir? Bilgisayar ağlarına ve bilgiye karşı olan tehditler nelerdir? Bilgisayar ağlarının güvenliğinin sağlanması için ne gibi önlemler alınmalıdır? İşletmelerin bilgi güvenliği yapılanması nasıl olmalıdır? İşletmelerde bilgi güvenliği yönetimine neden ihtiyaç duyulur? Bilgi güvenliği politikası nasıl oluşturulmalıdır? Bilgi güvenliği yönetim sisteminin fonksiyonları nelerdir? Bilgi güvenliği sağlanırken risk yönetimi ve değerlendirmesi nasıl yapılır? Bilgi güvenliğinde dış kaynak kullanılabilir mi?

Araştırmanın Amacı

Araştırmanın temel amacı, işletmelerin bilgisayar ağlarında bilgi güvenliğinin sağlanmasına neden ihtiyaçları olduklarını ortaya koymak, gelişen teknoloji paralelinde bilgi güvenliği yönetimine olan ihtiyacı vurgulayarak, nasıl bir yönetim tarzı sergilenmesi gerektiğini açıklamaktır.

Araştırmanın Önemi

Araştırma, bilgi güvenliği ihlalinden kaynaklanacak yüksek maliyetin, alınan bilgi güvenlik tedbirleri ve etkin bilgi güvenliği yönetimi vasıtasıyla bertaraf edilmesini sağlaması, işletme kaynaklarının makul bir şekilde yönlendirilmesi suretiyle olumlu bir gelişimin tesis edilebilmesi ve işletmeye duyulan güvenin pekiştirilmesi açısından önem arz etmektedir.

Araştırmanın Hipotezleri

H_{10}: Gelişen teknolojiler ile daha karmaşık bir yapıya bürünen bilgi güvenliği ihtiyacı, bütünsel bir bilgi güvenliği yönetimini gerektirmektedir.

H_{20}: İşletmelerde ağ bilgi güvenliği ile ilgili tedbirlerin alınabilmesi için ağ yapısına olabilecek tehditlerin neler olduğu bilinmeli ve işletme için kapsamlı bir risk analizi yapılmalıdır.

H_{30}: Hassas bilgi içeren ağlara sahip olan işletmeler, organizasyon yapılarında bilgi güvenliği yönetim süreçlerini göz önüne alarak, uygun bir organizasyon yapısı oluşturmalıdır.

Araştırmada Varsayımlar

Araştırmada herhangi bir varsayımda bulunulmamıştır.

Araştırmanın Sınırlılıkları

Araştırmada bilgisayar ağları üzerindeki bilginin güvenliği ele alınmıştır. Basılı doküman veya video, kaset gibi farklı ortamlarda tutulan bilginin güvenliği konu kapsamı dışında tutulmuştur. Ağ bilgi güvenliğini doğrudan veya dolaylı olarak etkileyebilecek "Fiziki Güvenlik" ve "Personel Güvenliği" konuları araştırmaya dahil edilmemiştir.

Araştırmanın Yöntemi

Tez çalışmasında literatür taraması konuyu tüm boyutlarıyla ortaya koyacak şekilde yapılmış, güncel makale ve konu hakkında basılan kitaplar incelenmiştir. Uygulama, 1 adet Unix ve 1 adet Intel tabanlı iki ağ sistemi üzerinde, gözlem; çalışanlar ve muhabere bilgi sistemleri personeli ile görüşme ve karşılıklı mülakat yöntemleri uygulanarak yapılmıştır.

GİRİŞ

Bilgisayar sistemlerinin 1945'lerden itibaren gelişmeye başlaması, bilgi çağı olarak tabir edilen yeni bir çağın da başlangıcı olmuştur. İlk kullanılmaya başlandıklarında devasa boyutları ve yüksek maliyetleriyle geliştirilmesi bile düşünülmeyen bu sistemler, günümüzde hemen her eve ve ofise girerek, neredeyse hayatımızı tam anlamıyla yönlendiren tekno – sosyal bir olgu haline gelmiştir.

Bilgisayarların bu derece küçülmesinde ve herkesin alabileceği bir maliyete indirgenmesinde en önemli etken olarak 1980'lerin ortalarından itibaren başlayan teknolojik değişim ve rekabet süreci sayılabilir. Yaşanan bu süreçte güçlü bir etki unsuru olarak da telefon hatları üzerinden iki yönlü data aktarımına olanak tanıyan modemlerin kullanılmaya başlanması ifade edilebilir. Modemlerin kullanılması ile birlikte hemen bütün ev ve iş yerleri internet ortamına taşınarak, dünyaya açılmak istemişlerdir. Elbette bu durumu değişimin tek etkeni ve öncüsü olarak saymak mümkün değildir. Gelişim çok boyutlu bir ortamda başlayarak bütün yönlere doğru bir yayılım göstermiştir. Sürekli olarak diğer değişimleri, yenilikleri tetikleyen bir mekanizma iş başı yapmıştır.

Gelişimin öncülüğünü yaptığını söylediğimiz internet sistemi, aslında büyük bir ağdır. Yazılım ve donanım anlamında uygun koşulları sağlayan herkes bu büyük ağ'a dahil olabilmekte, ticaret, tanıtım, eğitim – öğretim, akademik çalışmalar, haberleşme ve diğer iş sahaları gibi her alanda dünyaya bir pencere açabilmektedir. Bu olanaklar, işletmelerin iş gücünü katlayarak artırırken, maliyetleri de inanılmaz ölçülerde düşürmekte ve çok büyük örgütsel faydalar sağlamaktadır. İnternet'in tüm bu güzel özelliklerini sıralarken, açık pencereden içeriye rüzgar girdiğini de belirtmek gerekir. Her türlü faaliyet alanında işletmeleri büyük imkanlara kavuşturmasına rağmen internet, sayısal saldırılar, virüsler, truva atları ve daha birçok şekliyle işletme bilgilerinin kaybına yol açabilecek birçok tehlikeye karşı hassas bir ortam oluşturmaktadır. Zira işletme bilgilerinin kaybı, ağ sisteminin çökertilmesi, kötü propaganda yapılması gibi sayısal dünya kabusları hem maddi hem de manevi kaybı beraberinde getirmektedir. Bilgi kaybının oluşması, veritabanlarının, müşteri veya

işletme bilgilerinin kaybedilmesi veya çok hassas bilgilerin kötü niyetli kişilerin eline geçmesi tarzında oluşturacağı maddi kayıp, işletmelerin boyutu ve faaliyet alanlarıyla doğru orantılıdır. Bunun yanında örgüt prestijinin sarsılması, örgüte olan inancın kaybolması, kötü propaganda sonucu müşteri ve vizyon kaybı, sonuçları hemen görülmese de orta ve uzun vadede örgütü sarsabilecek manevi kayıplar olarak tanımlanabilir.

Bilginin dış tehditlere maruz kalması, güvenliğinin sağlanması gerekliliği ise başka bir kavramı ortaya çıkarmıştır. **"Bilgi güvenliği"**. Şüphesiz ki bilgisayarın yaygınlaşmaya başlaması ile birlikte gündeme oturan bir konu olan "Bilgi güvenliği", yaşanan teknolojik değişimlerle birlikte basit bir konu olmaktan uzaklaşmıştır. Ağ teknolojilerinin gelişmesi, yerel ağ şebekelerinin, geniş alan şebekelerinin ve benzeri şekillerde farklı bilgisayar sistemlerinin bir birine bağlanmasına duyulan ihtiyaç, bağlantı şekillerinin telefon hatlarından, uydu bağlantı şekillerine kadar uzanan bir çeşitlilik göstermesine yol açmış, bilgi güvenliğinin yönetilmesine olan ihtiyacı ortaya çıkarmıştır. 80'li yıllarda ve 90'lı yılların başlarında bireysel bazı girişimlerle bilgisayarların ve bilgisayar sistemlerinin güvenliğini sağlamak mümkün olabilmekteydi. Bugün ise, yukarıda bahsi geçen teknolojik değişimin paralelinde bilgi güvenliği konusuna tamamen profesyonel bir şekilde yaklaşmak gerekmektedir. Bu kapsamda uzman bilgi güvenliği (infosec) personeli istihdam edilmekte, işletme yönetiminin politikası dahilinde bilgi güvenliği de işletmede bilgi güvenliğinin sağlanmasından ve idame ettirilmesinden sorumlu olmaktadır. Hatta bu konuda dış kaynak kullanımına (outsourcing) gidilmesi bile birçok zaman karşımıza akılcı bir çözüm olarak çıkmaktadır. Bu yaklaşımlar bize işletmelerin, ağ yapılarının güvenliğinin sağlanmasının önemini her geçen gün daha fazla idrak ettiklerini, günümüzde bilginin rekabet ortamında en fazla üstünlüğü sağlayan olgu olduğuna olan inançlarının arttığını anlatmaktadır. Bu maksatla birçok kurum tarafından bilgi güvenliği eğilimlerini ortaya koyabilmek amacıyla, her yıl yinelenen araştırmalar yapılmaktadır. Türkiye'de ise bu konuda kapsamlı bir çalışma sonucunda ortaya konulan bir rapor bulunmamaktadır. Özel sektörde faaliyet gösteren bazı firmalar işletmelerin güvenlik yönetimlerine talip olmakta hatta bu konuda seminerler ve diğer bazı bilgilendirici faaliyetlerde bulunmaktadırlar. Alan araştırması olarak dikkat çekici nitelikli çalışmaların sayısı ise

çok azdır. Bu çalışmalardan bir tanesi Koç.net'in Ağustos – Eylül 2003 tarihlerinde yaptığı güvenlik denetimi çalışmasıdır. Ücretsiz güvenlik denetimi kampanyası ile birlikte yapılan çalışmada 1000 civarında, büyüklü küçüklü, farklı sektörlere ait firmanın güvenlik riskleri tespit edilerek istatistik amaçlı olarak raporlanmıştır. Buradan elde edilen bulgulara göre incelenen bilgi sistemlerinin;

- %87'si farklı düzeylerde güvenlik riski taşımaktadır.
- %56'sının web sunucu bilgileri kolaylıkla çalınabilir, ana sayfaları değiştirilebilir veya bir başka adrese yönlendirilebilir.
- %43'ünün DNS sunucularındaki açıklardan dolayı şirket mail'leri ele geçirilebilir veya çalışanların internet üzerinden eriştiği bankacılık gibi işlemlerde kullanılan şifreler çalınabilir.
- %28'inin güvenlik duvarları konfigürasyonu kötü olduğu için by-pass edilerek her türlü bilgiye erişilebilir.
- %29'unun sistemlerinde çok yüksek seviyede açıklar bulunmaktadır.

Çıkan sonuçlar incelendiğinde tehditlerin büyük bölümünün iletişime açık durumda bırakılması zorunlu olan http, ftp, smtp ve dns servislerinden kaynaklandığı görülmektedir. Birçok işletmenin ürün tanıtımı, pazarlama, araştırma, iletişim gibi birçok işletme faaliyeti için interneti kullandığı göz önüne alındığında, kötü niyetli kişiler tarafından verilebilecek zararların telafisinin mümkün olmayacağı bir boyuta ulaşması yüksek bir ihtimal olarak karşımıza çıkmaktadır. Bilgi güvenlik sistemlerinde ciddi açıkları bulunan bu işletmelerin durumu kilidi ve anahtarı olmayan bir evde yaşayan insanların durumuna benzemektedir. İşletmeye ait tüm dosyalar, veri tabanları, diğer hassas bilgiler, kontrolsüz bir şekilde tüm dünyaya açık durumda bulunmaktadır.

Uluslar arası bir yazılım firması olan Symantec tarafından 2003 yılının ilk altı ayını kapsayan bir araştırmanın sonuçlarına göre Amerika'daki şirketlerin güvenlik riskleri ile ilgili olarak şu noktalar tespit edilmiştir.

- Açıkların %80'i uzaktan sistemlere zarar vermek için kullanılabillir.

- Şirketlerin %12'sinde web uygulama açığı bulunmaktadır.
- Solucan saldırılarındaki artış bir önceki seneye göre %20 artmıştır.
- Halka açık olmayan uygulamalara (veritabanı erişimi gibi) saldırılar bir önceki seneye göre çok artmıştır.
- Solucan saldırıları çok fazla zarara yol açmıştır. 2003 Ağustos ayında solucan saldırılarından dolayı şirketler 2 milyar $ zarara uğramışlardır.

Bu çalışmadan elde edilen bulgular Koç.net'in yaptığı çalışma bulgularıyla karşılaştırıldığında Türkiye'deki şirketlerin Amerika'daki şirketlerden 4 kat daha fazla güvenlik açığına sahip olduğu anlaşılmaktadır.

Bu anlamda riskin büyüklüğü çok ciddi boyutlardadır. Güvenlik risklerinin sektörlere göre dağılımında ise enerji ve sağlık sektöründe nispeten daha az risk unsuru bulunduğu, kamu, eğitim kurumları ve perakende sektörlerinde ise çok daha yüksek güvenlik risklerinin bulunduğu gözlenmektedir.

Belirtilen bu durum işletmelerin ciddi yatırımlarla birlikte ciddi önlemlere başvurmaları gerektiğini dikte ettirmektedir. Bu anlamda bilgi güvenliğinin sağlanması ve yönetilmesi profesyonel bir yaklaşımla yüksek derecede uzmanlık gerektiren bir faaliyet sahası olarak karşımıza çıkmaktadır.

Yapılan tez çalışmasında da, bilgi güvenliğinin ve yönetiminin boyutları kapsamlı olarak ortaya konmaya çalışılmıştır. Bilgi güvenliği yönetiminin, bilgi yönetimi ve güvenlik yönetimi fonksiyonları ayrı ayrı incelenmiş, kesişen noktaları ortaya konmuştur.

Bilginin güvenliğini sağlayabilmek için bilginin nasıl bir yapıda hareket ettirilip, saklandığına, hangi ortamda ve hangi kurallara bağlı olarak kullanıldığına vakıf olmak gerekmektedir. Bundan sonra ise karşımızdaki tehdit nedir ve ne gibi önlemler almalıyız soruları cevaplanmalıdır. Çalışmada bu konular ortaya konmaya çalışılmıştır.

Bilgi güvenliği ve yönetimi konusuna bütünsel bir yaklaşım sergilenerek risk değerlemesi ve risk yönetimi konularının da kapsanması sağlanmıştır.

Bu anlatılanlar ışığında ağ sistemlerindeki bilgi güvenliğinin sağlanması ve yönetilmesi amacıyla öncelikle bilinmesi gereken konunun Ağ sistemlerinin gelişiminin ve sistem güvenliğinin ne olduğunun anlaşılması olduğu düşünülmektedir. Bu maksatla tez çalışmasının 1nci bölümünde ağ sistemlerinin ve güvenlik olgusunun tanımı, fiziki, donanım ve yazılım olarak farklılık gösteren boyutları tanımlanmaya çalışılmış, bu kapsamda tehdit oluşturan olgular ve bunlara karşı alınabilecek önlemler açıklanmıştır. İkinci bölümde ise yönetim boyutu ele alınarak ortaya konulan bilgiler ışığında ağ güvenliğinin yönetim boyutu ele alınarak yönetim sürecini ve risk analizi ve risk yönetimini de içeren bütünsel bir yaklaşım izlenmeye çalışılmıştır. Üçüncü ve son bölüm ise bilgisayar ağları ve güvenliğinin sağlanmasına yönelik teknik bilgilerle bilgi güvenliği yönetimi sürecinin sentezini amaçlayan bir anlayışla metodolojik bir saha uygulama çalışmasını içermektedir.

TEZ METNİ

BİRİNCİ BÖLÜM

AĞ SİSTEMLERİ VE AĞ SİSTEMLERİNDE GÜVENLİK

1.1. AĞ SİSTEMLERİNİN GELİŞİMİ VE TANIMLANMASI

Bilgisayar ve ağ güvenliği konusunun daha iyi anlaşılabilmesi amacıyla öncelikli olarak bilgisayar ve ağ teknolojilerinin gelişim sürecini açıklamakta yarar görülmektedir. Teknolojik gelişime paralel olarak devam eden bu süreç, günümüzdeki bilgisayar ve bilgi güvenliğinin karmaşık yapısının anlaşılmasına da ışık tutacaktır.

1.1.1. Ağ Tarihçesi

Bilgisayar ağlarında temel nokta, iki bilgisayarın bir biri ile iki yönlü iletişim kurmasıdır. Bu iletişimde iki bilgisayar arasında data alış verişi olur ve bu da bilgisayarların daha işlevsel olarak kullanılabilmesine olanak tanır. Bilgisayar ağlarının ortaya çıkışı ve gelişimi, bilgisayarın gelişimi ile paralellik gösterir.

Bilgisayar bağlantısının köklerini 1962 yılında J.C.R. Licklider'in Amerika'nın en büyük üniversitelerinden biri olan Massachusetts Institute of Tecnology'de (MIT) tartışmaya açtığı "Galaktik Ağ" kavramında bulabiliriz. Licklider, bu kavramla küresel olarak bağlanmış bir sistemde isteyen herkesin herhangi bir yerden veri ve programlara erişebilmesini ifade etmiştir. Licklider 1962 Ekim ayında Amerikan Askeri araştırma projesi olan İleri Savunma Araştırma Projesi'nin (DARPA - Defense Advensed Research Project Agency) bilgisayar araştırma bölümünün başına geçmiştir. MIT'de araştırmacı olarak çalışan Lawrance Roberts ile Thomas Merrill, bilgisayarların ilk kez birbirleri ile 'konuşmasını' ise 1965 yılında gerçekleştirmiştir.[1]

1966 yılı sonunda Roberts DARPA'da çalışmaya başlamış ve "ARPANET" isimli proje önerisini yapmıştır. ARPANET çerçevesinde ilk bağlantı 1969 yılında dört merkezle yapılmış ve ana bilgisayarlar arası bağlantılar ile bilgisayar ağlarının ve bir anlamda internetin ilk şekli ortaya çıkmıştır. ARPANET'i oluşturan ilk dört merkez

---

[1] "İnternetin Tarihçesi", http://www.aydesign.net/internetintarihcesi.htm, Erişim Tarihi: 4 Nisan 2004.

University of California at Los Angeles (UCLA), Stanford Research Institute (SRI), University of Utah ve son olarak University of California at Santa Barbara (UCSB)'dır. Kısa süre içerisinde birçok merkezdeki bilgisayarlar ARPANET ağına bağlanmıştır.1971 yılında Ağ Kontrol protokolü (NCP-Network Control Protokol)ismi verilen bir protokol ile çalışmaya başlamıştır.[2] 1972 yılı Ekim ayında gerçekleştirilen Uluslararsı Bilgisayar İletişim Konferansı (ICCC- International Computer Communications Conference) isimli Konferansta, ARPANET'in NCP ile başarılı bir demontrasyonu gerçekleştirilmiştir. Yine bu yıl içinde elektronik posta (e-mail) ilk defa ARPANET içinde kullanılmaya başlamıştır. NCP'DEN daha fazla yeni olanaklar getiren yeni bir protokol, 1 Ocak 1983 tarihinde İletişim Kontrol Protokolu (Transmission Control Protokol/ internet protokol - TCP/IP) adıyla ARPANET içinde kullanılmaya başlamıştır. TCP/IP bugün varolan internet ağının ana halkası olarak yerini almıştır.[3]

1980'li yılların ortasında Savunma Bakanlığı'na bağlı (DoD) Amerikan askeri bilgisayar ağı, ARPANET'ten ayrılmış ve MILITARY NET adı ile kendi ağını kurmuştur. 1986 yılında Amerikan bilimsel araştırma kurumu 'Ulusal Bilim Kuruluşu' (NSF), ARPANET için ülke çapında beş büyük süper bilgisayar merkezi kurulmasını içeren kapsamlı bir öneri paketi öne sürmüştür. ARPANET Amerikan hükümetinin sübvansiyonu ile NSFNET olarak düzenlemiştir. 1987 yılında yeniden düzenlediği internet yapılanması planı ile NSFNET yedi bölgesel nokta üzerinde 1.5 Mb/s (daha önce 56 Kb/s idi) güçlü bir omurgayı işleteceğini duyurmuştur.[4]

NSFNET Merit olarak adlandırılan Michigan Eyaletindeki üniversitelerin organizasyonu ile NSF'in yaptığı bir anlaşma doğrultusunda işletilmeye başlanmıştır. NSFNET'in işletilmesine bir süre sonra Merit'in yanında ABD'nin dev bilgisayar firması IBM ve haberleşme firması MCI dahil olmuştur. NSFNET'in işletilmesine yönelik 1990 yılında oluşturulan bu birlik 'İleri Ağ Hizmetleri' (ANS-Advance Network

---

[2] "İnternet Tarihi", http://www.romannet.net/tr/domain/history.htm#top, Erişim Tarihi: 4 Nisan 2004.

[3] "İnternet'in Tarihçesi" www.kou.edu.tr/idari/bilgiislem/ders/inttarih.htm, Erişim Tarihi: 4 Nisan 2004.

[4] "İnternetin Tarihçesi", http://www.aydesign.net/internetintarihcesi.htm, Erişim Tarihi: 4 Nisan 2004.

Services)olarak adlandırılmıştır.[5] ANS'nin kuruluşu süreci ABD'de 1990'lara kadar devlet desteğinde gelişen internet omurgasının özelleştirilmesi sürecinin de başlangıcı olmuştur. 1990 yılında NSFnet ile özel şirketlerin ortak işletmesi ile başlayan özelleştirme süreci, 1995 yılı mayıs ayında NSF'nin internet omurga işletmeciliğinden tamamen çekilmesi ile tamamlanmış ve 1995 yılından itibaren ABD internet omurga işletimi tamamen özel işleticilerinin eline geçmiştir.

Ağ ve internet teknolojisi çok büyük bir oranda ABD'nin öncülüğünde gelişmiştir. Diğer ülkeler bu teknoloji yarışında geride kalmak istemeselerde üstünlüğün ABD'de olduğu açıktır. En azından TCP/IP protokolüne dayanan ve her bir makinenin internet üzerindeki kimliği gibi bir işlevi olan IP numaraları dahi ABD tarafından tahsis edilmektedir. Bu anlamda internete hükmetme konusunda en ileri ülke olma konumunu sürdürmektedir.

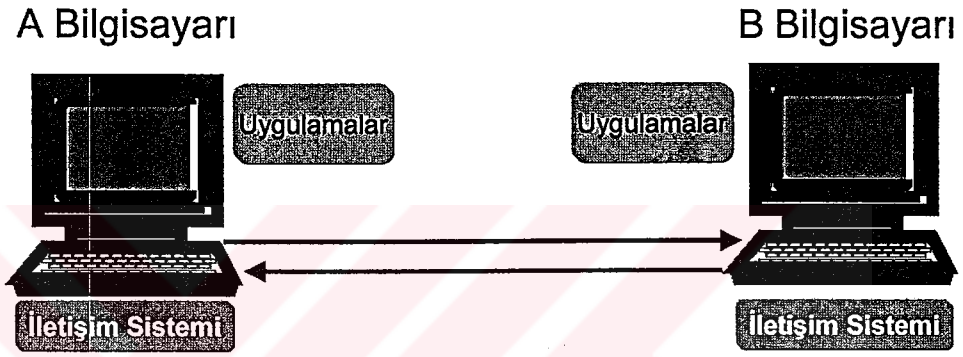
1.1.2. Ağ Sistemlerinin Tanımlanması

İşlevsel olarak bilgisayar ağları öncelikle bir bilgisayarda işlenen bir veriyi diğer bir bilgisayara veya kullanıcılara aktarmak suretiyle bir işin daha etkin ve kısa sürede yapılmasına imkan sağlar. Bilgisayar ağlarının veya daha geniş manada bütün ağ sistemlerinin mantığında aynı temel süreç yatmaktadır. Örnek verilecek olunursa; bankacılık sektöründe bir şubede yapılan işlemler saniyeler mertebesinde merkeze veya diğer banka şubelerine aktarılabilir. Bir firmanın bayileriyle arasındaki ilişki de benzer şekildedir. İşletmenin kendi bünyesinde de ayrı departmanların ayrı olarak yaptıkları işlerden haberdar olmaları, bunları paylaşımlı olarak işleyebilmeleri, yönetim kademesinin ise tüm bu süreci yakından takip ederek müdahale edebilmesi bilgisayar ağları ile mümkün olabilmektedir. Gerçekte, kurulan bir bilgisayar ağı tek başına bütün bu işleri gerçekleştiremez. Daha birçok sistem elemanından söz etmek gerekir. Ancak şu var ki bilgisayar ağları da bu mozaik yapının omurgasını oluşturan bir unsurdur.

---

[5] "İnternet Tarihi", http://www.romannet.net/tr/domain/history.htm#top, Erişim Tarihi: 4 Nisan 2004.

İki yönlü iletişim kuran bir bilgisayar ağı sistemi aşağıdaki şekilde görülmektedir. İki bilgisayar arasında veri aktarmanın en basit yöntemi noktadan noktaya veri aktaran bir ortam oluşturmaktır. Yani iki bilgisayarı birbirine kablo ile bağlamaktır. Fakat bu basit yöntemin bazı dezavantajları vardır. Birincisi, bilgisayarların birbirlerinden kilometrelerce uzakta olması durumunda bağlantı çok masraflı olacaktır. İkincisi ise ikiden çok bilgisayar olması durumunda her bilgisayarı birbirine bağlayan kablolar çekmek hem masraflı olacak, hem de karmaşaya yol açacaktır.[6]



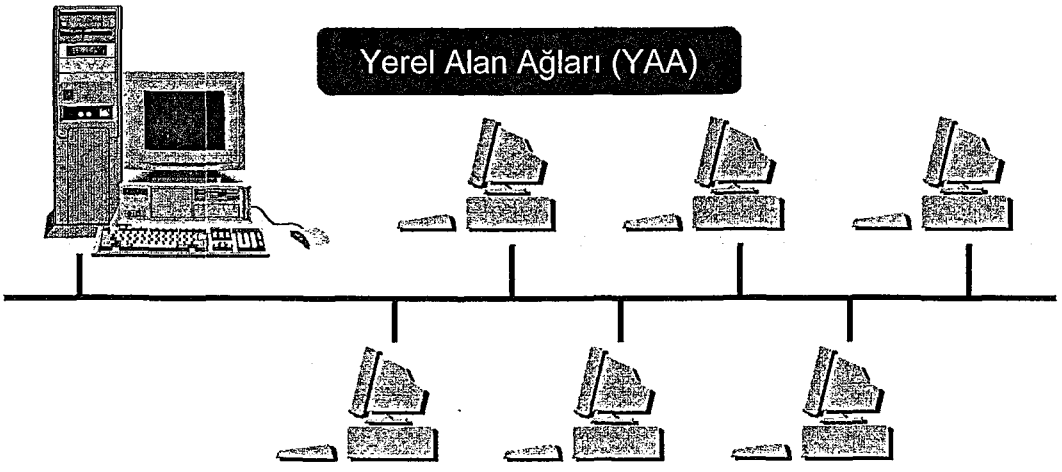
Şekil 1.1 : Temel İletişim Örneği

KAYNAK : Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.154

Noktadan noktaya bağlantı sağlamak yerine uygulanan yöntem, bir iletişim ağı oluşturmak ve her bilgisayarı bu ağa bağlamaktır. Bu şekilde oluşturulan ağları iki kısma ayırabiliriz. Birincisi "Yerel Alan Ağları" (LAN – Local Area Network) olarak tabir edilen ağ sistemleridir. Bu sistemlerde bağlantı genellikle ethernet kartı gibi bir arabirimle bilgisayarlar ağa dahil edilir.

---

[6] Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.154.

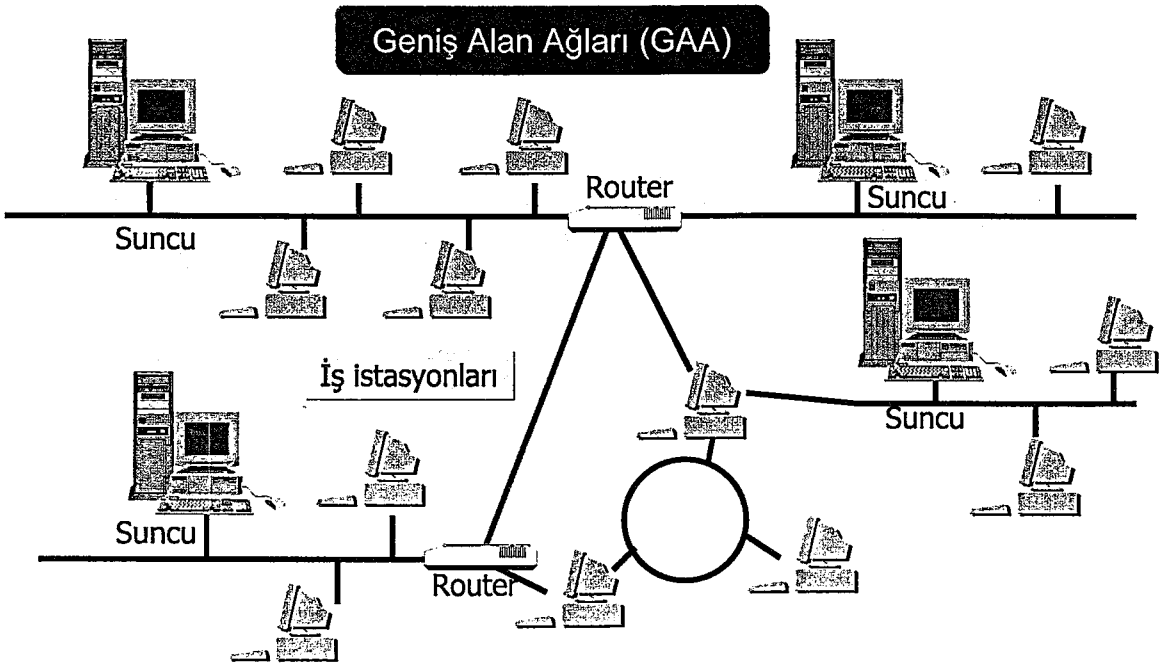


Şekil 1.2 : Yerel Alan Ağları (YAA)

KAYNAK : Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.156

İkinci ağ yapısı ise özellikle uzak mesafelerdeki istemcileri (client) birbirine bağlayan ağ şeklidir. Geniş Alan Ağları (WAN – Wide Area Network) olarak isimlendirilir. Bu şekildeki bağlantı sıklıkla telefon hatları kullanılarak, modem türü bir arabirim ile ağa dahil olmak şeklindedir. Telefon hatlarının yanı sıra geniş banttan yayın yapan kablolu TV, uydu yayınları veya doğrudan uydu bağlantısı da GAA'ların bağlantı şekillerindendir. Aşağıdaki şekil GAA'ların konumlanmasını göstermektedir.[7]

[7] Baykal, **a.g.e.**, s.156.



Şekil 1.3 : Geniş Alan Ağları (GAA)

KAYNAK : Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.156

Sözü edilen YAA ve GAA gibi bilgisayar ağlarının kullanılması, bilgisayarların yaygınlaşması ile birlikte bir miktar değişime de uğramıştır. Ağ sistemlerinin tarih içindeki gelişimi anlatılırken de değinildiği gibi öncelikle ortaya Yerel Alan Ağları (YAA) çıkmış ve bölgesel anlamda bilgisayar ünitelerini (bilgisayar, iş ünitesi, yazıcı gibi) birbirine bağlamış ve iletişimde bulunabilmelerini sağlamıştır. Daha sonra ortaya çıkan Geniş Alan Ağları (GAA) da aynı imkanları çok daha uzak mesafeler için sunmuştur. Bilgisayar hızlarının artmasına paralel olarak ağ sistemlerinin hızları da artış göstermiştir. Bir YAA'na yüzlerce makine bağlamak mümkündür. Bu gibi ağlarda veri aktarım hızı 10 ile 1000 bit/sn arasında değişebilmektedir. GAA ise mekandan bağımsız olarak milyonlarca bilgisayarın sisteme bağlanmasına izin

vermektedir. Veri aktarım hızı ise 64 kilobit/sn.'den gigabitler seviyesine kadar değişmektedir.[8]

2000'li yılların başında GSM ve diğer kablosuz ağ erişimlerini uygulamaya yoğun olarak geçmesiyle ağ gelişim evrelerine yeni bir madde eklenmiştir. Bu da kablosuz bağlantı/erişim ve kablosuz LAN (YAA)'dır. Artık LAN (YAA) ve WAN (GAA) şeklinde sınıflanan ağ yapılarına, Kişisel Alan Ağları (Personel Area Network – PAN) ve Aile Alan Ağları (Family Area Network – FAN) gibi yeni kavramlar eklenmiştir.[9]

1.2. AĞ SİSTEMLERİNDE GÜVENLİK VE BİLGİ GÜVENLİĞİ

Ağ sistemlerinde temel nokta verilerin bilgisayarlar arasında transfer edilmesidir. Bu transfer sırasında verilerin doğru bir şekilde gönderilmesi, aynı zamanda istenmeyen üçüncül kişilerin eline geçmemesi güvenlik kapsamında incelenecek olan konuları teşkil eder. Güvenlik konusu, çeşitli şekillerde ağa bağlanmış bilgisayarlardan, kişisel bilgisayarlara kadar geniş bir yelpaze içerisinde incelenebilir. Sistemlerin bağlantı şekillerine, yapılarına, faaliyet alanlarına göre farklılık gösterir. Bu nedenle ilk olarak "Güvenlik" tanımının yapılması gereklidir.

1.2.1. Güvenlik Tanımı

YAA'na yüzlerce ve GAA'na milyonlarca bilgisayarın aynı anda bağlanmasının mümkün olduğunu Ağ Sistemlerinin Gelişimi bölümünde ifade etmiştik. İnternet dahi mevcut haliyle GAA'dan başka bir şey değildir. Sadece kullanımına bir sınırlandırma getirilmemiştir. Bu kadar çok sayıda bilgisayarın aynı anda bağlandığı ve birbiriyle veri alış verişinde bulunduğu bir sistemde güvenlik anahtar unsur olarak

---

[8] Andrew S.Tanenbaum ve Maarten Van Steen, **Distributed Systems Principles and Paradigms,** Vrije Universiteit Amsterdam, Netherlands, 2002, s.1.

[9] Rifat Çölkesen ve Bülent Örencik, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri,** Papatya Yayınları, İstanbul, 2002, s24.

karşımıza çıkmaktadır. Her türlü tehlikeye açık bir yapı içerisinde bizim için çok kıymetli olan bilgilerin güvenliğini almamak düşünülemez. Dolayısıyla güvenli sistemlere ve bağlantılara ihtiyaç duymaktayız.

Bu konuda birbiriyle karıştırılan iki kavram vardır. **Güvenirlik** ve **Güvenlik.** Aslında bu iki terim tamamen farklı anlamlar taşımaktadır. Burada güvenilir güçlü, güvenli denetimli anlamındadır.[10]

1.2.1.1. Güvenilir Sistem

Güçlü sistem anlamına gelmektedir. Yoğun trafikte bile tüm sistem kendisinden beklenen performansı sergiler ve herhangi bir tıkanmaya, çökmeye sebep olmaz. Bunun için sistemde kullanılan aktif cihazların uygulamaya dönük dikkatli seçilmiş olması ve daha da önemlisi konfigürasyonunun iyi ve bilinçli bir şekilde yapılmış olması gerekir.

1.2.1.2. Güvenli Sistem

Denetimli sistem anlamına gelmektedir. Internet gibi genele açık bir ağa bağlanan kurumsal ağların dışarıdan gelebilecek tehlikelere karşı korunması, kurumun sahip olduğu bilgi ve verilere izin verildiği ölçüde erişilmesi ve kurumun kendi elemanları tarafından yapılacak iç ve dış erişimlerin denetlenebilmesini belirtir.

Bir ağ internete bağlandıktan sonra iç ve dış erişimler için koruma duvarı (firewall) gibi herhangi bir güvenlik sistemi içermiyorsa, sahip olunan bilgiler tehdit altındadır. Bir koruma duvarı olmadan kendi ağımızı kamuya açık bir ağa eklersek, ardından birtakım sorunlar da kendiliğinden gelir. Sisteme girilirken sistemlerin kullanıcı adı ve şifre sorgulaması yapmasının yeterli olacağını sanmak çok yanlış olur. Güvenlik konusunda ciddi önlemler alınmalıdır.

---

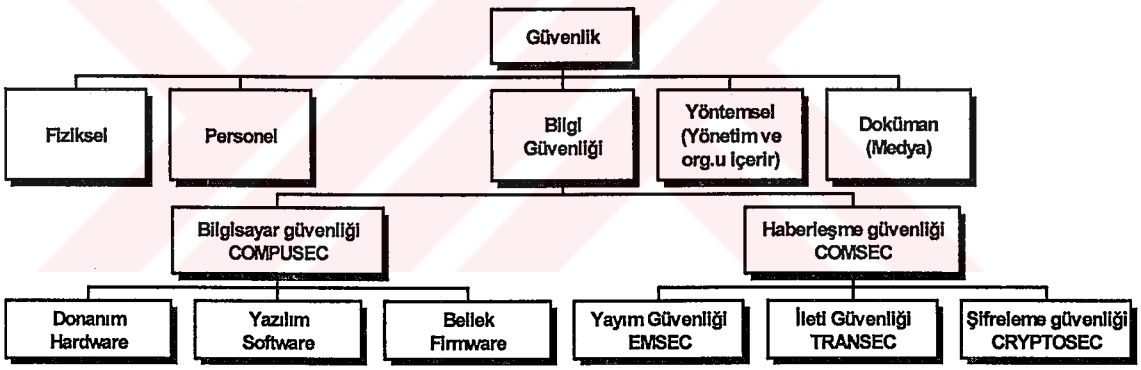
[10] Çölkesen ve Örencik, **a.g.e.,** s.311.

1.2.2. Bilgi Güvenliğinin Kapsamı

Güvenlik konusu sınıflandırma açısından organizasyonel anlamda iki tür yaklaşım sergilemektedir. Bunlardan ilki güvenlik yönetimidir. Bilgi güvenliği doğal olarak güvenlik yönetiminin bir parçasıdır. Bunun yanı sıra, bilgi güvenliği, bilgi yönetimi alt konuları içerisinde de geçmektedir. Bu nedenle bilgi güvenliğinin iki yönelimi ortaya çıkmaktadır.

1.2.2.1. Güvenlik Yönetiminde Bilgi Güvenliği Davranışı

Bilgi güvenliği tümden gelim (deductive) yöntemiyle ve bir bütün olarak ele alınmalıdır. Bütünsel bir yaklaşımda organizasyonlar için bilgi güvenliğini aşağıdaki şekilde sınıflandırabiliriz.



Şekil 1.4 : Güvenlik Alanlarının Tasnifi

KAYNAK : **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part V Chapter1, s.4

Yapılan bu sınıflandırmada olduğu gibi güvenlik tüm yönleriyle ele alınmalıdır. Bilgisayar ağlarındaki güvenlik büyük oranda bilgisayar güvenliği (COMPUSEC) sınıflandırmasının içine girmektedir. Bununla birlikte ifade edilen sınıflar arasında katı bir kesinlik bulunmamaktadır. Tüm sınıflar iç içedir ve birbirleriyle etkileşim içerisindedir. Tüm organizasyonların temelinde insan unsuru vardır. İnsana yönelik bilgi güvenliği belki de burada en fazla önem verilmesi gereken alanı

oluşturmaktadır. Bu çalışmada insan unsuru ikinci bölümde, yönetim bölümü içerisinde incelenmektedir.[11]

Dikkat edileceği gibi bilgisayar ve haberleşme güvenliği (COMPUSEC – COMSEC) güvenlik yönetiminin bilgi güvenliği alt başlığında incelenmektedir.

1.2.2.2. Bilgi Yönetiminde Güvenlik Yaklaşımı

Bilgi yönetimi, sayısal teknolojinin gelişmesiyle birlikte bir yönetim kavramı olarak ortaya çıkmıştır. Organizasyonların departmanlaşma süreci içerisinde de yerini almıştır. Bir departman olarak;

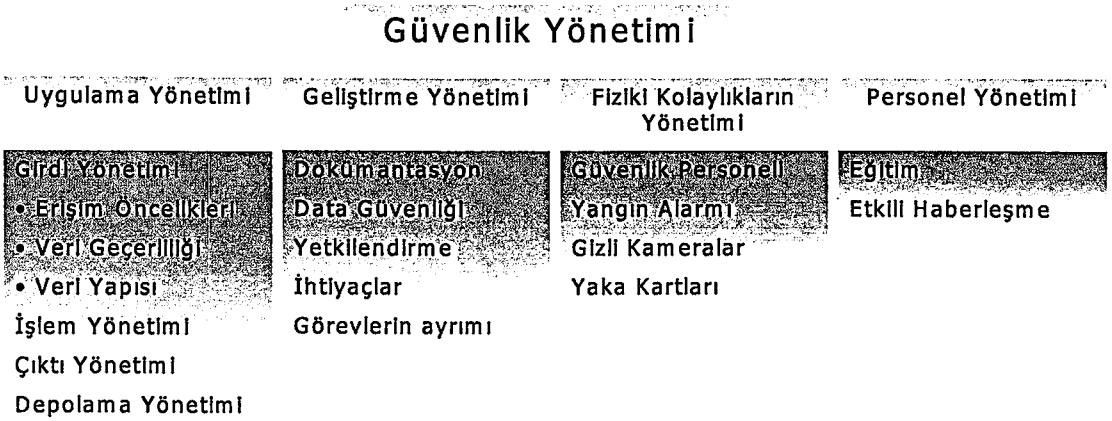
- Donanım Yönetimi,
- Yazılım Geliştirme,
- Eğitim ve Destek,

konularında sorumluluklar taşımaktadır. Bu sorumluluklar, ortak bilgi standartlarının oluşturulması, son kullanıcılara destek sağlanması, bilgi sistemlerine dayalı stratejilerin oluşturulması görevlerini içermektedir.[12] Bu bağlamda bilgi güvenliğini sağlama fonksiyonu da bilgi sistemlerinin yönetimini gerçekleştiren departmanın yetki ve sorumluluğundadır. Buna bağlı olarak güvenlik yönetimi aşağıdaki şekilde tasnif edilmiştir.

---

[11] ACE Security Directive AD 70-1, SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part V Chapter1, s.4.

[12] Gerald V. Post ve David L. Anderson, **Management Information Systems,** Richard D. Irwin, a Times Mirror Higher Education Group, Inc. Company, 1997 s.611.



Şekil 1.5 : Bilgi Yönetimine Bağlı Güvenlik Yönetimi

KAYNAK : Matt Bishop, **Computer Security,** Boston, Addison – Wessley, 2003, s.581.

Şekil incelendiğinde aslında iki yaklaşımda da konuların birbirinden çok farklı olmadığı görülmektedir. Sadece bakış açısı değişmektedir. Tez çalışmasında ortaya konulan sistematikte iki yaklaşım da etkin olarak kullanılmıştır. Bundan amaç iki yaklaşımın da çapraz kontrollü olarak incelenerek güvenlik sisteminin oluşturulmasıdır. Bu maksatla çoğu zaman gözardı edilen ve güvenlikle doğrudan ilgili bir konu olan fiziki sistem güvenliği öncelikli olarak incelenecektir.

1.3. FİZİKİ SİSTEM GÜVENLİĞİ

Fiziki Sistem Güvenliği, sistem kurulumu esnasında ve idamesi sırasında sürekli olarak göz önünde bulundurulması gereken bir unsurdur. Bir hırsızlık sonucundaki çalma olayında veya sabotörlerin sistemlere fiziki olarak zarar vermesi sonucunda ortaya çıkan maddi zararı hesaplamak olasıdır ve bu durum tahmin edilebilir bir düzeydedir. Bununla birlikte sisteme fiziki olarak sızarak ağ yapısına erişim sağlayan bir kişi sisteme kat ve kat daha fazla zarar verebilecektir. Bu açıklamadan da anlaşılabileceği gibi fiziki sistem güvenliği ile fiziki güvenlik arasında anlam olarak farklılık vardır. Fiziki güvenlik kapsam olarak tesislere giriş ve çıkışları kontrol altında tutmayı, tesislerin güvenliğini sağlamayı hedefler. Oysa fiziki sistem güvenliği, işletilen

sisteme çevresel arabirimlerden gelebilecek risklerin minimize edilmesini amaçlar. Bu doğrultuda fiziki arabirimler incelenerek, risk yapısı ortaya konulmaya çalışılacaktır.

Bir sisteme zarar vermek durumu söz konusu olduğu zaman bunun sadece veri transferi ile gerçekleştirileceğini düşünmemek lazım gelir. Elbetteki yazılımsal olarak veri transferi, bilgilerin silinmesi, karıştırılması, uygun olmayan şekillerde kullanılması şeklinde zarar verme yöntemleri mevcuttur. Bu konular 1.7 ve 1.8 no'lu bölümlerde detaylı olarak incelenecektir. Bunun yanı sıra çeşitli fiziki unsurları kullanarak bilgi kaybına sebebiyet vermek de olasıdır. Örneğin güç yedeklemesi olmayan bir ağ sunucusunda güç kaynağının veya elektrik hatlarının kesilmesi, işletim sisteminin çökmesi de dahil olmak üzere birçok bilginin kaybına yol açacaktır.[13]

Fiziki sistem güvenliği ile ilgisi bulunan çevre birimleri ve bunların muhtemel riskleri aşağıda açıklanmıştır.

1.3.1. Güç Hatları – Elektrik Tesisatı ve Yedek Güç Kaynakları

Güç, bir sistemin çalıştırılabilmesindeki en temel unsurdur. Bilgisayarların ve bilgi sistemlerinin çalıştırılmasında ana güç olarak elektrik enerjisi kullanılmaktadır. Sistemlerin işletilmesinde kullanılan elektrik enerjisinin akım ve voltaj olarak yeterli seviyede olması gerekmektedir. Sistemlerin istikrarı açısından bu durum çok önemlidir. Elektriğin istikrarlı bir düzeyde kullanılabilmesi temelde sağlanan şehir elektrik sistemine ve doğal olarak alt yapısına bağlıdır. Şehir elektriğindeki dalgalanmalar veya sıklıkla karşılaşılan elektrik kesintileri bilgi sistemlerine büyük zararlar verebilmektedir. Bu zararları aşağıdaki gibi özetleyebiliriz:

- İşletim sistemlerinin çökmesi,
- Hard disk gibi manyetik hafıza üniteleri başta olmak üzere kullanılan bütün donanımın fiziki zarar görebilmesi,

---

[13] Earl Crane, **Information Security Management at A-OK, Inc.,** A case study at Carnegie Mellon University, August 2000, s.4-5.

- İşleme esnasındaki verilerin kaybolması,
- Depolanmış verilerin kaybolması,
- İş ve zaman kaybı,
- Etkinliğin ve verimliliğin azalması,
- Personel üzerinde olumsuz moral etkisi,
- Sisteme ve örgüte duyulan güvenin azalması.

ABD'de yapılan bir araştırma çalışmasında kullanılan elektriğin kalitesinin mükemmel olduğu vurgulanmıştır. Voltaj dalgalanmalarının nominal değerin %10 limiti içerisinde olduğu ifade edilmiştir.[14] Aslında %10'luk bir dalgalanmayı birçok bilgisayar tolere edebilecek şekilde tasarlanmıştır. Ama bu durum, özellikle hassas bilgiler göz önüne alındığında risk almaya değecek bir özellik değildir. Özellikle şehir elektriğinin çok fazla güven vermediği durumlarda anılan etkileri bertaraf edebilmek için işletmeler tarafından ilave önlemler alınması gerekmektedir. Türkiye'de elektrik istikrarlı olmaktan çok uzaktır. Voltaj dalgalanması oldukça yüksek, elektrik kesintileri de çok sık yaşanmaktadır. Dolayısıyla bilgi sistemlerini, bilgisayar ağlarını sadece şehir elektriğine bağlı olarak kullanmaya çalışmak büyük bir hata olacaktır.

1.3.2. Kesintisiz Güç Kaynakları (UPS)

Özellikle ülkemizde öncelikle dikkat edilmesi gereken husus elektrik kesintileridir. Elektrik kesintisi halinde sistemin çalışmasını temin edecek bir yedekleme ünitesine ihtiyaç vardır. Kesintisiz güç kaynağı (UPS - Uninterruptible Power Sources) sistemleri güç kaybı durumunda devreye girerek kısa bir müddet sisteme takat sağlayabilmektedir. Günümüzde üretilen UPS'ler aynı zamanda bünyesinde bir regülatör modülü barındırarak ani voltaj dalgalanmalarına karşı da sistemi koruyabilmektedir. UPS seçiminde göz önüne alınması gereken hususların başında, sistemin büyüklüğü, çektiği akım ve hangi seviyelerde UPS kullanılacağı gelmektedir.

---

[14] James Arlin Cooper, **Computer and Communications Security,** İntertext Publications McGraw-Hill Book Company, 1989 s.68.

İkinci nokta UPS sistemi/sistemleri ne kadar bir süreyle takat sağlayacaktır? Normal olarak UPS'ler birkaç dakika gibi kısa bir süre için takat sağlayabilirler. UPS'ler sisteme uygun değerlerde güç üretebilen bataryalardır. Bu şarj durumuna bağlıdır. Birkaç dakikalık süre kısa gibi görünmesine rağmen yapılan işlerin kaydedilmesine ve bilgisayarların kapatılmasına olanak tanır. Tabi ki burada işletmeler için en akılcı çözüm, otomatik olarak devreye giren jeneratörlerdir. Genellikle sıvı yakıt kullanarak elektrik üreten jeneratörlerin üretime geçebilmeleri için birkaç dakikalık bir süreye ihtiyaç vardır. Dolayısıyla UPS sistemi birkaç dakika güç sağlayarak jeneratörlerin devreye girmesine kadar olan ihtiyacı karşılarlar. Bu düzenek sistemin kesintisiz olarak çalışmasını temin eder.

1.3.3. Voltaj Regülatörleri

Elektrik sisteminde dikkat edilmesi gereken diğer bir nokta daha önce de bahsedildiği gibi voltaj dalgalanmalarıdır. UPS sistemleri bu dalgalanmayı tolere edebilse de sadece bu maksat için üretilmiş voltaj regülatörleri de işletmeler için diğer bir alternatiftir. Voltaj regülatörleri, elektrik çıkışını sabit voltaj transformatörleri kullanarak ±%2V seviyesinde sabitleyebilmektedir. Bu da birçok uygulama için yeterli olabilecek bir değerdir.[15]

Genel olarak voltaj regülatörlerinin hedefi, şehir akımının %15'e kadar arttığı ve %25'e kadar düştüğü durumlarda güç çıkışını nominal gücün ±%8'i kadar bir değişim limiti içerisinde tutmaktır. Voltaj regülatörlerinin "dinamik düzenleme" olarak tabir edilen diğer bir fonksiyonu da ani voltaj değişimlerinin etkisini minimize etmektir. Bu sistemler ani voltaj değişikliklerini %10'luk bir seviyeye kadar indirgeyebilmektedir.

---

[15] James Arlin Cooper, **a.g.e.**, s.71.

1.3.4. Hat Monitörleri

Doğrudan koruyucu bir tedbir olmamakla birlikte işletmelerde kullanılan bir diğer araçta "hat monitörleri"dir. Hat monitörleri, hat güvenliğini tamamlayıcı bir özellik taşır. Güç hatları üzerinde meydana gelen anormalliklerin izlenmesine ve zamanında müdahale edilmesine, hataların tespitine imkan tanır. IBM ve AT&T tarafından açıklanan bilgilerde normal bir elektrik hattı üzerinde günde en az iki kere güç anormalliği yaşandığı, bilgisayar çökmelerinin ise yaklaşık %50 oranda bu anormalliklerden kaynaklandığı ifade edilmiştir. Yine AT&T Bell laboratuarlarında yapılan diğer bir çalışmada ölçülen anormalliklerin %87'sini voltaj düşüşü oluşturmuştur. Çalışmalara göre kesinti sırasında %75 oranında RAM'deki bilgilerin kaybedildiği, %25 oranında disk çökmeleri yaşandığı, %20 oranında da donanım arızaları oluştuğu açıklanmıştır. Yüksek voltaj olayı da dalgalanma kapsamına girmekle birlikte, tüm güç sapmasının %1'lik bir bölümünü oluşturmaktadır. Aşırı güç artışının ortaya çıkardığı sorun ise donanımda meydana gelen arızalardır.[16]

Güç kaynağı ve enerji sorunları bilgi sistemlerinin güvenliğinin ve istikrarının sağlanmasında en temel unsur olarak görülmektedir. İşletmelerin ise sistemde kullanılacak takat ile ilgili tedbirleri işletme yapısı, sistemleri, bilgi sistemi özellikleri ve işletmenin faaliyet gösterdiği sektöre göre planlamaları uygun olacaktır.

1.3.5. Aşırı Yük Koruyucuları ve Filtreler

Aşırı yük genellikle, bölgeye düşen bir yıldırımdan veya kaynak cihazı, klima, ısıtıcı gibi yüksek elektrik çeken cihazların kullanılması sonucu oluşur. Hatlarda aşırı yük oluşması durumunda sisteme bağlı cihazların arızalanması olasıdır. Böyle bir riskle karşılaşmamak için aşırı yük koruyucuları kullanılır. Birçok koruyucu, kapasitesi paralelinde oluşan aşırı yükü sönümler. Burada dikkat edilmesi gereken nokta, koruyucu sistemin kapasitesidir.

---

[16] James Arlin Cooper, **a.g.e.**, s.70.

Enerji (Jul) = Güç (watt) x Zaman (sn)

formülü, güç ve geçen zaman arasındaki bağıntıyı tanımlar. Kişisel bilgisayarlar gibi birçok cihaz bünyesinde 100 milijule kadar koruma sağlayan sistemler barındırır. Temelde yük koruyucu sistemler yaklaşık 1000 jullük bir sapmayı sorunsuzca telafi edebilirler.[17]

Filtreler de aşırı yük koruyuculara benzer bir prensiple çalışmaktadır. Filtreler istenmeyen enerjiyi zararsız bir yöne yönlendirir. Bu genellikle topraktır. Bu sayede aşırı yükün oluşturacağı zarar by-pass edilmiş olur.

İşletmeler faaliyet gösterdikleri sahaları ve durumlarını analiz ederek kendilerine gerekli olan sistemi kurma yoluna gitmelidir.

1.3.6. Topraklama

Topraklama konusu elektrik sisteminde hassasiyet arz eden bir diğer konudur. Elektrik topraklamasının yapılmasındaki amaç, sistemde biriken statik elektriğin, toprağa verilmesini öngörmektedir. Oluşan statik elektrik sisteme bağlı cihazlara zarar verebilmektedir. Bu zarar cihazların donanımsal olarak hasarlanması veya kararsız bir şekilde çalışmasıyla neticelenebilir. Bu durumda da depolanmış veya işlem görmekte olan bilginin kaybedilmesi olasıdır.

Topraklamada diğer bir konu, güvenlik topraklaması olarak tabir edilen, bilgi sızıntısına karşı uygulanan bir topraklama şeklidir. Güvenlik topraklamasında sistemlerden ortaya çıkan sızıntı ayrı bir toprak hattı vasıtasıyla toprağa aktırılır. Bu sayede sızıntı çalınmalara karşı koruma altına alınmış olur. Dikkat edilmesi gereken nokta bu toprak hattının mümkün olduğunca düşük bir direnç seviyesine sahip olmasının gerekliliğidir. Direnç düşükse, bilgi sızıntısı toprağa daha sorunsuz olarak aktarılabilecektir. Direnç, kabul edilen seviyenin üzerine çıktıkça, güvenli toprak hattından aktarılmaya çalışılan sızıntı kontrolsüz yönlere kaçış yapabilecektir. Direnç

---

[17] James Arlin Cooper, **a.g.e.**, s.76.

değeri yaklaşık 2 – 10 Ω arasında değişen bir değere sahip olmalıdır. Toprak hattının direncinin 3 aylık periyotlarla ölçülmesi bilgi güvenliği açısından önemlidir. Sızıntı konusu daha sonraki bölümlerde detaylı olarak incelenecektir.

1.3.7. Yangına Karşı Önlemler

Fiziki güvenlik ortamındaki en ciddi problemlerden bir tanesi yangındır. Bilgisayar sistemlerinin tümü yangına karşı çok hassastır. Dolayısıyla yangını önleyecek veya erken haber verebilecek usullerin önceden geliştirilmesi gerekir.[18] Örneğin yanıcı malzemelerin (kağıt, kimyasal gaz veya sıvı içeren materyaller, bant, koli, plastik gibi) yüksek sıcaklığa sahip bir ortam içinde bulundurulmamaları gerekir. Diğer bir tedbir olarak hassas bölgelerde manyezitten yapılan ve ateş tuğlası olarak tabir edilen malzeme ile yapılan ateşe dayanıklı duvarlar kullanılabilir.

Yangınla mücadelede göz önüne alınması gereken temel konular olarak; yangının tespit edilmesi, yangına karşı su kullanılması, yangın söndürme tüpleri, otomatik yangın söndürme sistemleri ve personel ve malzeme tahliyesi sayılabilir.

1.3.7.1. Yangının Tespit Edilmesi

Yangın ve duman tespit eden alarmlar aslında hepimiz tarafından yakınen tanınır. Türkiye'de evlerde ve işyerinde isteğe göre kullanılsa da Avrupa'da ve ABD'de kullanılması kanunlara tabidir. Yangın ve duman tespit sistemleri genel olarak üç kategoride incelenebilir: iyonlaşmanın tespiti, dağılan ışıkla duman tespiti ve ısı algılayıcılarıdır.

Bunlardan en çok kullanılanı iyonlaşmanın tespitine dayanarak yapılan alarmlardır. Bu cihazlar, küçük bir miktar radyoaktif madde kullanarak, algılama menzilindeki havayı iyonize eder. Duman ise havanın iyonlaşmasını azaltır. İyonlaşma

---

[18] **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part V Chapter 15 Annex A, s.3.

belirli bir eşik seviyesinin altına düştüğünde alarm devreye girer. Duman gözle görülür bir şekilde olmasa da, alevin oluşturduğu partiküllere karşı oldukça hassastır.

Dağılan ışık yöntemini kullanan detektörler gözle görülmeyen partiküllere karşı çok hassas olmamakla birlikte, duman tespitinde çok başarılıdırlar. Çalışma prensibi olarak, bir ışık kaynağından gelen ışık cihaza doğrudan yansıtılmaz. Ortamda duman olduğunda ise kaynaktan gelen ışık dağılır ve cihaza ışık düşer. Cihaza gelen ışık belirli bir ışık seviyesinin üstüne çıktığında alarm devreye girer.

Isı algılayıcı sistemlerde ise adından anlaşıldığı gibi, ısı belirli bir seviyenin üstüne çıktığında alarm devreye girer. Bu sistemler bilgisayar ortamında oldukça kullanışlıdır. Çünkü bilgisayarlar için ortam ısısının belirli bir derecede tutulması gerekir. Isı algılayıcılı sistemler bu anlamda ısının arzu edilen seviyenin üzerine çıkması durumunda gerekli tedbirlerin alınması imkanını sağlarlar.

1.3.7.2. Yangında Su Kullanılması

Yangınla mücadelede en çok uygulanan söndürme yöntemi su kullanarak söndürmedir. Bununla birlikte su bilgisayarlara ve çevre birimlerine karşı çok zararlıdır. Özellikle kendinden devreye giren sistemler personel güvenliğinde büyük bir etkinlik sağlarken, bilgisayar ünitelerinde büyük hasarlara neden olmaktadır. Ancak personelin emniyeti genel anlamda daha önemli bir durum arz eder. Bu yüzden etkinliği kanıtlanmış bir sistemden doğrudan vazgeçmek konusu daha dikkatli düşünülmelidir.

1.3.7.3. Yangın Söndürme Tüpleri

Yangın söndürme tüplerinde en çok kullanılan muhteviyat, su, CO2, kuru kimyasallar ve Halon 1211 gazıdır. Sulu tüpler, odun, kağıt ve plastik yangınlarında (A tipi yangın) çok etkilidir. Elektrik sistemlerinden kaynaklanan yangınlarda (C tipi yangınlar) ise bir o kadar tehlikelidir. Kuru kimyasallar ise genellikle ev tipi söndürücülerde kullanılır. Bilgisayar ortamı söz konusu olduğunda, bilgisayar ve ekipmanlarına zarar vereceğini belirtmek gerekir. Bilgisayar ve elektrik ortamı için kullanılabilen en uygun materyallerden bir tanesi CO2 tipi söndürücülerdir. CO2 tipi

söndürücüler, kağıt ve plastik kaynaklı yangınlarda çok elverişli değildir. Halon 1211 gazı nispeten diğerlerine göre pahalıdır. Ancak bilgisayarla teçhiz edilmiş yerlerde en etkili sonucu verir. Halon gazı aynı zamanda ağaç, kağıt ve plastik yangınlarına karşı da etkilidir. Elektrik ortamlarında güvenle kullanılabilir ve çökelti bırakmaz. Bu yüzden bilgisayar ve bilgi güvenliğinin önemli olduğu işletmelerde öncelikli düşünülmesi gereken yangın söndürme cihazları, Halon gazı içeren yangın söndürme tüpleri olmalıdır.

1.3.7.4. Otomatik Yangın Söndürme Sistemleri

Otomatik yangın söndürme sistemleri, yangının tespit edilmesi ile birlikte kendiliğinden devreye giren püskürtme tipi sistemlerdir. Yangın söndürme tüplerinde olduğu gibi su, CO2, Halon gazı püskürten otomatik sistemler mevcuttur. Daha önce de belirtildiği gibi su püskürtme sistemleri, personel sağlığı açısından en uygun sistem olmakla birlikte, bilgisayarlar gibi elektrikle çalışan donanıma zarar vermektedir. CO2 püskürtmeli sistemler ise personel sağlığı açısından ciddi sonuçlar doğurabilecek bir durum doğurabilmektedir. Ortama Halon gazı püskürtülmesi ise yangın söndürmede en etkili yöntemlerden bir tanesidir. Bu sistemlerde insanların boğulmasını engelleyebilmek amacıyla Halon gazının yoğunluğu düşürülür. Böylece personel tahliyesi en seri şekilde gerçekleştirilirken ortama yayılan Halon gazının da yangını söndürmesi hedeflenir.[19]

Birçok işletmede yangın departmanları bulunur ve sadece bir yöntem kullanılmaz. Yangın departmanları otomatik sistemlerin yanı sıra birçok durumda yangına el yordamı ile müdahale edecek sistemleri de bünyesinde bulundurur. İşletmede bazı bölümlerde su, bazılarında Halon gazı kullanılabilir. Söndürme sistemleri, personel ve malzeme güvenliğini tehlikeye düşürmeyecek şekilde bir sistematik dahilinde kullanılmalıdır.

---

[19] James Arlin Cooper, **a.g.e.**, s.86.

1.3.8. Personel ve Malzeme Tahliyesi

Personel ve Malzeme Tahliyesinin bilgi güvenliği konusuyla doğrudan ilgili olmadığı düşünülebilir. Ancak, personel de, malzeme de bilginin kullanılması ile doğrudan ilgilidir. Bu maksatla kurtulan personel ve kurtarılan malzemenin bilgi sürecine yeniden dahil olacağını düşünmek tahliye konusu ile bilgi güvenliğini bağdaştırmaktadır.

Yangın, deprem ve benzeri felaket durumunda personel ve malzemenin tahliyesini gerçekleştirebilmek amacıyla önceden planlar yapılır. Bina ve tesisler bu plana göre uygun çıkış ve kaçış noktalarına sahiptir. Tahliye edilen personel güvenli bir yerde toplanarak herkesin tam olarak kurtulduğundan emin olunmalıdır. Malzemenin tahliyesi tüm ofis materyallerini kapsamaz. Acil durum söz konusu olduğunda sadece hassas malzemenin kurtarılmasına özen gösterilir. Tahliye planlarında kimin hangi malzemeyi kurtaracağı ve hangi görev sorumlulukları yerine getireceği, departmanların bina içindeki yerleşimine göre neredeki personelin nereden tahliye edileceği önceden belirlenir. Tahliye planlarının tatbikatı işletme yönetimi tarafından mütemadiyen personele icra ettirilir. Bu tatbikatlar zamanlamanın sağlanabilmesi açısından önemlidir ve saat gibi işlemelidir. Bunun nedeni şöyle açıklanabilir: yangın, detektörler tarafından tespit edildikten sonra yaklaşık 30 sn. içinde Halon gazı ortama püskürtülecektir. Bu durumda personelin alarm ikazlarına süratle reaksiyon göstermesi önemlidir. Tatbikatlar olayın seriliğini artırır ve personelin bilgisini pekiştirir. Aksi taktirde gerçek bir durumla karşılaşıldığında çok büyük bir kargaşa yaşanacak ve muhtemel personel kayıplarıyla karşılaşılabilecektir.[20]

1.3.9. Suya Karşı Koruma

Yangına karşı önlemler konusunda suyun bilgisayar sistemlerine olabilecek zararından bahsetmiştik. Suyun bilgisayar sistemlerine karşı olabilecek zararları sadece

---

[20] **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part II Chapter 2, s.54.

yangın durumunda kullanılması ile sınırlı değildir. Su taşkınları, su borularının bilgisayar sistemlerinin üzerinden geçmesi ve sızıntı yapması, yağmur vs durumda çatının su sızdırması, personel tarafından kazara su, çay, kahve gibi sıvıların bilgisayarlar üzerine dökülmesi çoğaltılabilecek örneklerdendir.

Suya karşı korumayla ilgili olarak alınabilecek en etkili tedbirlerden bir tanesi bilgisayarların plastik kılıflarla korunmasıdır. Bu koruma birçok durumda etkili bir yöntemdir. Buna karşılık, 24 saat çalışan bir sistemde böyle bir korumaya gitmek mümkün olmaz. Diğer bir tedbir ise su detektörleridir. Piyasada çok geniş bir yelpazede su detektörleri bulmak mümkündür. Su detektörlerinin kullanılmasının işletmeler açısından söz konusu riski minimuma indirecek bir tedbir olduğu düşünülmektedir.[21]

1.4. AĞ GÜVENLİK MİMARİSİ

Önceki bölümlerde ifade edildiği gibi ağ mantığında iki bilgisayarın veri aktarımı suretiyle birbirine bağlanması vardır. Veri aktarımının güvenli olarak yapılması önem arz eder. Data aktarımında güvenliği sağlayabilmek için gerek data aktarım protokollerinde, gerekse işletim sistemi seviyesinde çeşitli tedbirler geliştirilmiştir. Bu tedbirler;

- Tanıma (authentication)
- Erişim kontrol (access control)
- Veri güvenliği (data confidentiality)
- Veri bütünlüğü (data integrity)
- Sayısal imza (digital signatures) ve
- Denetleme (auditing)

olarak sayılabilir. Ağ güvenlik mimarisinin ana unsurlarını oluşturan bu noktalar aşağıda açıklanmıştır.

---

[21] James Arlin Cooper, **a.g.e.**, s.88.

1.4.1. Tanıma (authentication)

Tanıma, iletişim kurmaya çalışan iki bilgisayarın bir birini tanıması esasına dayanır. Temel olarak, iletişimde kullanılan birçok protokolde tanıma için farklı matematiksel yöntemler kullanılsa da, sonuçta varılan nokta iki bilgisayarın birbirini tanıdığının ortaya konulmasıdır. Şayet bilgisayarlar birbirini tanımıyorsa iletişim kesilir. Böylece izinsiz girişlerin önüne geçilmeye çalışılır.

İki tür tanıma vardır. Kişi (entity) tanıma veya kimlik belirleme (identification).[22] Kişi tanıma dediğimiz yöntemde, ağa giriş yapmaya çalışan kişinin gerçekten o kişi olup olmadığı sorgulanır. Sonuç doğruysa ağa giriş işlemi sağlanır. Aynı kapsamdaki bir diğer tanıma şekli ise ileti tanıma diye adlandırılan ve bir kişi tarafından oluşturulan iletinin gerçekten de o kişi tarafından oluşturulduğunu ispata çalışan teknikler içeren tanıma şeklidir. İleti tanıma ve ileti bütünlüğü genellikle iletinin gerçekliğinin sağlanmasındaki en temel iki konudur ve birbirinde ayrılması, birinin sağlanıp, diğerinin ihmal edilmesi düşünülemez.[23] İleti bütünlüğü kavramı, veri bütünlüğü konusu içinde açıklanmaya çalışılacaktır. Bu vurgulamanın asıl amacı konu bütünlüğünün ifade edilmesidir.

Tanıma protokolleri incelendiğinde, basitten karmaşığa doğru farklı algoritmaların izlendiği görülmektedir. Adım adım bu yaklaşımları incelediğimizde, en basit şekliyle bir kullanıcı diğerine kendini tanıtır ve doğru beyan ettiği kabul edilerek tanıma gerçekleşir. Buradaki olası güvenlik problemi, başka bir kullanıcının kendisini adresi kontrol edilir. IP kontrolü, bilinen statik bir IP kullanılması durumunda yapılabilir. IP'nin statik olmaması durumunda ulaşılacak IP adresi internet servis sağlayıcısının (ISP – Internet Service Provider) IP aralığına veya bir ağ havuzundaki IP aralığına ulaşılabilir. Bilindiği gibi IP adresi, bir başka kullanıcının işletim sistemi kodlarına ve kernel bilgilerine ulaşmak suretiyle kopyalanabilir. Yani iletişim kurulan bilgisayara farklı bir IP adresinden ulaşılıyormuş gibi göstermek mümkündür.

---

[22] Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.346.

[23] Andrew S.Tanenbaum ve Maarten Van Steen, **Distributed Systems Principles and Paradigms,** Vrije Universiteit Amsterdam, Netherlands, 2002, s.433.

Dolayısıyla IP adresinin sorgulanmasına dayalı bu yöntem de suistimale açıktır.[24] Bu noktada düşünülen diğer bir kontrol unsuru şifre (password) uygulamasıdır. İki bilgisayar tanıma işlemi sırasında birbirlerine şifre sorar. Tanınacak bilgisayar bu şifreyi yanıtlar. Güvenlik açısından olasılıkları tahmin etmeye çalıştığımızda, şifrenin üçüncü kişi tarafından okunarak kaydedilmesi (read & store) suretiyle tespiti mümkündür. "Sniff" olarak adlandırılan bu hamleyle kullanıcı şifreleri çalınabilir. Kullanıcı şifrelerinin kriptolanması düşünülebilir. Ağa bağlanacak taraf kullanıcı şifresini kriptolayarak karşı bilgisayara gönderir ve bağlanılacak bilgisayar da kriptoyu çözerek sisteme girişe izin verir. Şifrelerin yakalanarak kaydedilmesi durumunda kriptolama işlemi yine bir çözüm olmayacaktır. Çünkü kriptolanmış şifre olduğu gibi kaydedilecek ve ağa kriptolu olarak gönderilecektir. Bu saldırı türü "playback attack" olarak adlandırılmaktadır.[25] Bu duruma karşı da geliştirilen bir dizi tedbir, anlık kontrol rakamları (nonce), genel anahtarlar (public key), özel anahtarlar (private key) olarak sayılabilir.

Anlık kontrol rakamları kullanılan protokolde bir defaya mahsus olarak üretilen bir rakamdır. Bu rakam bir daha asla üretilmez. Genel anahtarlar ve özel anahtarlar, günlük hayatta kapılarda kullandığımız anahtar kilit mekanizması gibi çalışırlar. İki bilgisayarda da anahtar ve kilit olarak tanımlayabileceğimiz fonksiyonlar vardır ve bunlar birbirini tamamlamaktadır. Fonksiyonlar karşılıklı tanımlanamazsa bağlantı da sağlanmamış olur.[26]

Gelişmiş tanıma protokollerinde bu usullerin bir kompozisyonu kullanılmaktadır. Birden fazla ağın birbirine bağlandığı durumlarda, eğer ağlar aynı derecede güvenlik seviyesine sahipse yeniden bir tanımlamaya ihtiyaç duyulmaz. Bu yüzden gerçekleştirilen mevcut tanıma işlemi diğer ağlar içinde geçerli olur. Farklı

---

[24] Beom-Hwan Chang, Dong-Soo Kimb, Hyun-Ku Kimb, Jung-Chan Naa, Tai-Myoung Chungb "Active security management based on Secure Zone Cooperation" **Future Generation Computer Systems,** Volume 20, South Korea, 2003, s.284.

[25] James F. Kurose & Keith W.Ross, **Computer Networking,** Pearson Education Inc., 2003, s.623.

[26] James F. Kurose & Keith W.Ross, **a.g.e.,** s.626.

güvenlik seviyeleri söz konusu olduğunda ise yeniden tanıma işlemine ihtiyaç duyulur.[27] Tanıma gerçekleştiğinde erişim kontrol olayı devreye girer.

1.4.2. Erişim kontrol (access control)

Ağ tarafından tanıma gerçekleştiğinde her kullanıcının sahip olduğu ağ öncelikleri işlenerek bir erişim denetimi gerçekleştirilir. Ağ öncelikleri kullanıcı profillerinde tanımlanır. Tanımlı olan ağ önceliklerine göre kullanıcının hangi dosyalara, klasörlere, sürücülere ne şekilde işlem yapabileceği ortaya konur.[28]

Erişim kontrol, literatürde yetkilendirme (authentication) olarak da nitelendirilmektedir.[29] Erişim kontrol veya yetkilendirme olarak adlandırılan bu usul, aşağıdaki şekilde en basit haliyle görülmektedir.

Şekil 1.6: Erişim denetiminde genel model

KAYNAK : Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.346

Buna göre kullanıcı tarafından gerçekleştirilen bir işlem isteği gözleme tabi tutulur ve işlemi yapmaya yetkili olup olmadığı sorgulanır. İşleme yetkili ise yetkilendirilmiş istek olarak nesneye gönderilir. Referans gözlem kullanıcıların erişim haklarını bünyesinde bulundurarak istekleri sorgulayabilen bir yapıdadır. Erişim hakları

---

[27] James Arlin Cooper, **Computer and Communications Security,** Intertext Publications McGraw-Hill Book Company, 1989 s.339.

[28] James Arlin Cooper, **a.g.e.,** s.339.

[29] Nazife Baykal, **a.g.e.,** s.346.

genel bir yaklaşım olarak erişim kontrol matrisi ile gerçekleştirilir. Bu matris, özneleri gösteren satırlar ve nesneleri gösteren sütunlardan oluşmaktadır. Buna göre kullanıcıların erişim yetkileri tanımlanır. Matris yapısının bir dezavantajı, binlerce kullanıcı ve milyonlarca nesne olması durumunda kontrolün neredeyse imkansız hale gelmesidir. Bunun için erişim kontrolünde uygulanan değişik yaklaşımlar geliştirilmiştir. Bu yaklaşımlardan bir tanesi de "erişim kontrol listesi" uygulamasıdır. Erişim kontrol listeleri her bir nesne için oluşturulur ve hangi kullanıcıların veya kullanıcı gruplarının ne seviyede yetkiye sahip olacağı belirlenir. Buna benzer farklı yaklaşımlar ağ mimarisinde kullanılmaktadır.[30]

1.4.3. Veri bütünlüğü ve güvenliği (data integrity & confidentiality)

Tanıma konusunda anlatıldığı gibi veri bütünlüğü ve güvenliği de güvenli kanallardan gerçekleştirilen bir veri koruma işlemidir. Burada veri bütünlüğü dendiğinde anlaşılması gereken bilgisayarlar arasında aktarılan verilerin dışarıdan yapılan tesirler neticesinde değiştirilmesinin engellenmesidir. Bu sayede aktarılan veri değişime uğramadan gönderilebilir. Veri güvenliği ise aktarılan verinin istenmeyen kullanıcı veya hariçten hatta girmeye çalışanların eline geçmeden ulaştırılmasını ifade eder. Bu maksatla kullanılan yöntemler tanıma, konusunda da anlatılan kriptolama, genel veya özel anahtar uygulaması gibi yöntemlerdir.[31]

1.4.4. Sayısal imza (digital signatures)

Veri bütünlüğü konusu ile çok yakından ilgili olan diğer bir uygulama ise sayısal imzalardır. Sayısal imzalar aslında, veri bütünlüğünün sağlanabilmesi için yapılan kriptolama tekniklerinden bir tanesidir. İnsan imzaları gibi bir karakteristik özellik taşırlar. Güvenilir, geçerli ve reddedilemez.[32] Dolayısıyla sayısal olarak

---

[30] Andrew S.Tanenbaum ve Maarten Van Steen, **a.g.e.**, s.448.

[31] Andrew S.Tanenbaum ve Maarten Van Steen, **a.g.e.**, s.441.

[32] James F. Kurose & Keith W.Ross, **a.g.e.**, s.627.

imzalanan bir bilginin güvenilir olduğu varsayılır. Bu yüzden güvenli iletişimde sayısal imzaların kullanılmasının önemi, gelişen teknoloji ve artan bilgisayar hızları paralelinde artmaktadır.

Konu kapsamından anlaşıldığı gibi sayısal imzalar, elektronik iletilerde kullanılır. Geleneksel elyazısı imzalarla sayısal imzalar arasında bazı farklılıklar vardır. Bu farklar şu şekilde özetlenebilir;

- Geleneksel imza, belgenin bir parçası halindedir. Sayısal imzalarda ise böyle bir olanak yoktur. Dolayısıyla imzanın bir şekilde ileti ile bütünleştirilmesi gerekmektedir.

- Geleneksel imzanın doğruluğundan emin olmak için üzerindeki imza, doğruluğundan emin olunan başka bir belgedeki imza ile karşılaştırılır. Sayısal imzanın doğruluğu ise herkesçe bilinen bir kanıtlama algoritması yardımıyla ortaya konulabilir.

- Elle imzalanmış bir kopya belge özgün belgeden kolayca ayırt edilebilir. Ama imzalanmış sayısal bir belgenin kopyası özgünüyle aynıdır.

- Gizli anahtar kriptografisine dayalı sayısal imzalar, yapısal sorunlar içerir. Açık anahtar (public key) kriptografisi tekniği ise daha iyi sonuçlar üretebilmektedir.

Bütün bunlarla birlikte sayısal imzalar hali hazırda, sadece küçük iletilerin imzalanmasında kullanılabilmektedir. Kripto sistemleri göz önüne alındığında, sayı kipi 512 veya 1024 bitlik bir sayıdır ve gönderilecek iletinin bu sayıdan küçük olması gerekmektedir. Bununla birlikte birçok doküman megabaytlarca uzunluğa sahip olabilmekte ve imzalanarak gönderilmek istenmektedir.

Bu duruma çözüm olarak akla gelen bir yöntem, dosyaları parçalamak ve her bir parçayı ayrı ayrı imzalayarak göndermektir. Bu yaklaşım bir çözüm olarak ortaya konsa da büyük iletilerde farklı sorunlar ortaya çıkmaktadır. Örneğin, ileti ile imzanın aynı boyutlara ulaşması, imza yöntemlerinde kullanılan algoritmaların modüler

üs alma gibi karmaşık ve zaman alan aritmetik işlemleri, sayısal imzaları küçük boyutlu olmayan iletiler için neredeyse imkansız hale getirmektedir.[33]

1.4.5. Denetleme (auditing)

Denetleme (auditing) işlemi, tanıma, erişim kontrol, yetkilendirme gibi fonksiyonların neticesinde ortaya çıkan sonuçların kayıt altına alınması olarak tanımlanmaktadır. Veri olarak kayıt altına alınan bu işlemler daha sonra başvurularak incelenebilmektedir.[34] Kayıtlar, günlük kayıt (kütük) dosyalarında saklanmaktadır.

Ağda yapılan işlemlerin kütük dosyalarında saklanması gereken bilgilerinin en azından şunları içermesi gerekmektedir.

- Tarih ve saat bilgisi,
- Gerçekleştirilen işlemler (güvenlik fonksiyonlarıyla ilgili olan bölümleri),
- İşlemi yapan kullanıcı kimliği,
- Yapılan işlemin başarılı olup olmadığı,
- Uygun olmayan işlem girişimleri,
- Kullanıcıların sisteme giriş ve çıkış bilgileri,
- Sistemin açılış ve kapanış bilgileri,
- Güvenlik parametrelerinde ve/veya politikalarındaki değişiklikler.[35]

---

[33] Nazife Baykal, **a.g.e.,** s.351.

[34] Jamer Arlin Cooper, **a.g.e.,** s.339.

[35] **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part V Chapter3, s.11.

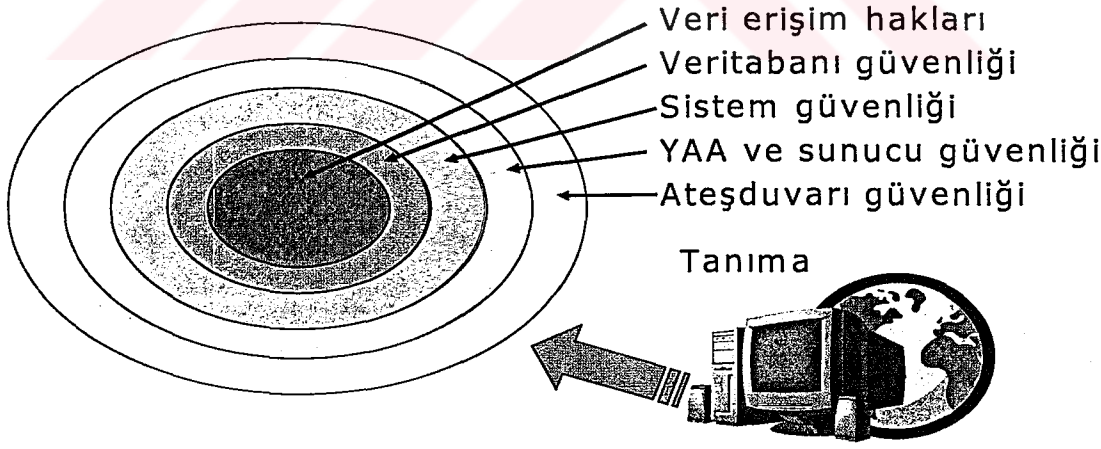
Kayıt dosyalarında saklanan bu bilgilerin özellikle yetkisiz personel erişimine karşı korunması gerekmektedir. Sistem bilgilerinin değiştirilmemesi ve gerçek haliyle saklanması için ayrı bir özen gösterilmelidir.

Kayıtların saklanma süresi de dikkat edilmesi gereken bir başka noktadır. Burada gizli veya çok gizli bilgiler için, önem arz eden bazı dosya ve belgeler için bir saklama süresi belirlenir. Saklanması çok elzem olmayan sıradan işlemlerin bilgileri ise daha kısa bir müddet süresince tutulmalıdır.

1.5. SİSTEM GÜVENLİĞİNİN SAĞLANMASI

"Ağ Güvenlik Mimarisi" konusunda sisteme giriş yapıldığı noktada güvenliğin tesis edilerek sistem giriş kontrollerinin nasıl bir mantıkla gerçekleştirilebileceği anlatılmıştır. Tüm kullanıcıların sisteme giriş yapmalarından sonra da güvenlik unsurları faaliyetlerini sürdürmeye devam ettirmektedir.

Bilgisayar ağlarında güvenlik tesisi ile ilgili olarak güvenlik katmanları oluşturulmuştur. Güvenlik katmanları aşağıdaki şekilde görülmektedir.



Şekil 1.7 : Güvenlik Halkaları

KAYNAK : Eduardo Gelbstein, **Managing Information Security,** International Computing Centre, Genava, Switzerland, s.16

Yukarıda oluşturulan modelde görüldüğü gibi, dışarıdan sisteme giriş yapmak için bütün güvenlik katmanlarından geçebilmek gerekmektedir.[36] Tanıma ve erişim hakları güvenlik katmanlarının çalışma mantığı bir önceki bölümde açıklanmıştır. Diğer güvenlik katmanları ise bu bölümde açıklanacaktır.

Güvenlik katmanlarının açıklanmasına geçmeden önce ne tip bir ağ yapısına sahip olunduğu ortaya konulmalıdır. Yapısal anlamda üç tip ağdan söz edilebilir;[37]

- Açık sistemler : İnternet
- Kapalı sistemler : İntranet
- Özel Sanal Ağlar (Virtual Private Networks - VPN)

1.5.1. Açık Sistemler : İnternet

Bilindiği gibi internet herkesin kullanımına açık bir sistemdir ve üzerinde gerçek anlamda bir denetim yoktur. Bununla birlikte çok geniş bir pazar ve bilgilendirme ağı olduğu açıktır. Bu nedenle birçok kişisel bilgisayar ve bilgisayar ağı bu devasa ağa kendini bağlamaktadır. İnternete bağlanan tüm bilgisayar ve ağlar her türlü riske, tehdide karşı açık bir konumda bulunmaktadır. Dolayısıyla bahsi geçen güvenlik önlemlerinin alınması çok daha önemlidir. Kriptolama, şifreleme, güvenlik duvarları, erişim haklarının tam denetimi internete bağlanan sistemlerinin olmazsa olmazlarıdır. Kişisel anlamda internet yoluyla gelebilecek tehlikeler bizlere çok fazla bir maddi külfet getirmeyebilir. Ama internet üzerinden işlem yaptıran bankaların çok özel müşteri bilgilerini, hesap numaralarını kaptırmaları veya bu bilgilerin değişikliğe

---

[36] Eduardo Gelbstein, **Managing Information Security,** International Computing Centre, Genava, Switzerland, s.16.

[37] Grant Kelly & Bruce McKenzie, **Security, privacy, and confidentially issues,** Computer Networks, Volume 17, s.131.

uğraması gerçek anlamda bir maddi kayba yol açacaktır.[38] Banka örneğinde olduğu gibi değişik iş kollarında faaliyet gösteren işletmeler için de durum çok farklı değildir. İnternete bağlı sistemlerde her zaman risk bulunmaktadır. Bu güne kadar yaşanan tecrübeler bunun böyle olduğunu dikte ettirmektedir. İnternete bağlanma zorunluluğunu hisseden işletmelerin güvenlik tedbirlerini en üst düzeyde tutmaları ve çok sık gözden geçirmeleri en akılcı davranış tarzı olacaktır.

1.5.2. Kapalı Sistemler : İntranet

İntranet sistemler, internet gibi herkese açık bir ağa dahil olmadan örgüt bazında, kullanıcı bilgisayarlarının birbirine bağlanması suretiyle oluşturulan ağlardır. Bu ağlar "Yerel Alan Ağları (YAA)" ve "Geniş Alan Ağları (GAA)" şeklinde olabilir. İntranet sistemleri, kapalı sistemler olduğu için internete bağlı sistemlere kıyasla daha az bir riske maruzdur. Bu yüzden daha güvenlidir diyebiliriz. Bu ifade daha önce bahsi geçen güvenlik tedbirlerine gerek yoktur şeklinde algılanmamalıdır. Neticede güvenlik bir bütündür ve tam anlamıyla yerine getirildiğinde ancak riskleri minimize etmek mümkün olabilir. Unutulmaması gereken nokta bir zincirin en çürük halkası kadar sağlam olduğudur. Bu zincirde oluşacak bir açık, zayıf bir nokta tüm güvenlik sisteminin çökertilmesi ve hassas verilerin kaybedilmesiyle sonuçlanabilir.

İntranet türü kapalı sistemlerde göz önünde tutulması gereken bir başka nokta ise işletme yönetiminde güçlü bir bilgi yönetim alt yapısı oluşturmasına rağmen, internet gibi pazarlama ve reklam unsurlarından yoksun olmasıdır. Yani intranet sistemler internetin oluşturduğu risklerden büyük anlamda korunmasına rağmen sağladığı avantajlardan da istifade edememektedir. Bu anlamda kapalı intranet sistemin yanında tamamen sistemden ayrılmış durumda bulunan internete bağlı diğer bir sistem işletmeler tarafından düşünülmesi gereken bir alternatiftir.

---

[38] Khalid S. Soliman, Brian D. Janz, "An exploratory study to identify the critical factors affecting the decision to establish Internet-based interorganizational information systems" **Information Management Journal,** Vol.41, Issue 6, USA, 25 June 2003, s.699.

1.5.3. Sanal Özel Ağlar (Virtual Private Networks - VPN)

Sanal özel ağ kullanımındaki temel amaç, herhangi bir kurum için özel bir ağın sağladığı olanakları, herkese ait açık bir ağ altyapısını kullanarak sağlamaktır. Extranet ve geniş alan İntranet, sanal özel ağların iki ayrı uygulama alanıdır.

Sanal özel ağ kullanımı, veri iletimini açık ağ üzerinden gerçekleştirmeden önce şifrelemeyi, verinin karşı tarafa ulaştığı anda ise şifre çözmeyi içerir. Daha fazla güvenlik, yalnızca verilerin değil, veri giriş ve çıkışının gerçekleştiği ağ adreslerinin de şifrelenmesi ile sağlanabilir. Bu yazılım genellikle, kuruma ait ateş duvarı sunucusunun bir parçası olarak kurulur.[39]

Sanal özel ağlarla mevcut kapalı bir sistemin internet üzerinden diğer kullanıcılara veya ağlara bağlanması da mümkün olmaktadır.[40]

1.5.4. Donanım Bütünlüğü

Ağ yapılarının kısaca tanımlanmasından sonra belki de sistem altyapısında en fazla öneme sahip olan donanım bütünlüğünden söz etmek gerekmektedir. Donanım bütünlüğü, güvenlik konusuyla ilgili olarak yapılan birçok çalışmada göz ardı edilmiş olsa da, veri güvenliğinin önemli unsurlarından birisidir.

"Bilgisayar çöktü..." veya "sistem bu kadar yükü kaldırmadı..." gibi yakınmalar donanım bütünlüğü kapsamında ele alınması gereken konulardır. Eğer donanım bütünlüğü sağlanamazsa alınacak güvenlik tedbirleri zincirin en çürük halkasında olduğu gibi çok fazla işe yaramayacaktır. Çünkü temelde yazılımlar, donanımlar için yazılırlar. Eğer yazılımlarda birçok güvenlik açığı bulunabiliyorsa, donanımlarda da güvenlik açıklarının bulanabileceğini düşünmek gerekmektedir.

---

[39] Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.346.

[40] Grant Kelly & Bruce McKenzie, **a.g.e.,** s.132.

Donanımdaki güvenlik açıkları bir yana, donanımsal olarak sistemin arıza yapması iş ve veri kayıplarına yol açabilecektir. Bu maksatla donanım bütünlüğünü öncelikle gerçekleştirebilecek unsurun "güvenli bilgisayar bileşenleri"nin kullanılması olduğunu söyleyebiliriz.[41] Bilgisayar bileşenlerinin seçiminde maliyet etkinlik analizi iyi yapılmalıdır. Zira ucuz olduğu için tercih edilen pek çok cihaz bütün bir sistemi felç edebilmektedir. Bu konuya bir örnek verecek olursak; ucuza alınan ve güvenli olmayan bir bilgisayar güç ünitesi arıza yaptığında bilgisayarın anakartını, işlemcisini, belleğini (RAM), sabit diskini ve daha birçok yongalarını kullanılamaz hale getirebilecektir. Oysa binlerce dolar vererek aldığımız bilgisayarlarda, güç ünitesi hiç önem vermediğimiz bir parçadır.

Maliyet – etkinlik analizinin yanı sıra dikkat edilmesi gereken bir başka nokta da alım yaptığımız sistem bileşenlerinin kapasitesidir. Kapasite tespit edilirken işletmenin uzun vadeli planlarında öngörülen değişiklikleri ve genişlemeyi de kapsayacak şekilde bir kapasite tercihi yapılmalıdır. Bu konuya da örnek verecek olursak; bulunduğumuz tesise döşenen elektrik hatları diyelim ki 10 bilgisayarı aynı anda çalıştıracak kapasitedeyse ve birkaç yıl sonra bilgisayar sayısını daha da artıracağımızı hedefliyorsak, elektrik tesisatının yeniden döşenmesi işletmeye ek bir maliyet getirecektir. Bunu göz önüne alarak baştan işletme hedeflerine uygun olacak şekilde tesisat döşenmesi veya genişlemeye olanak tanıyacak bir yapının kullanılması daha akılcı ve maliyeti düşüren bir çözüm olacaktır.

1.5.5. IP Güvenliği

IP adresleri bir bilgisayarın ağ üzerinde temsil ettiği adrestir. Her bilgisayarın kendisine ait bir IP numarası vardır ve bu numara tektir. Kullanılan IP adresinin güvenli olmasını istemek en temel hak olarak ortaya çıkmaktadır. Kendi güvenlik mekanizması bulunan programlarımızın haricinde kullandığımız, fakat

---

[41] James Arlin Cooper, **Computer and Communications Security,** Intertext Publications McGraw-Hill Book Company, 1989 s.157.

herhangi bir güvenlik unsuru içermeyen programlarımızın da güven altında olmasını isteriz. İşte bu noktada IP seviyesi güvenlik söz konusu olmaktadır.

IP seviyesi güvenlik üç fonksiyonel alanı kapsar. Bunlar; tanıma, güvenirlik ve anahtar yönetimi olarak sayılabilir.[42] Bu yöntemlerin yaklaşımı Ağ Güvenlik Mimarisi bölümünde açıklanmıştır.

IP adresleri internet veya herhangi bir ağ üzerinde bilgisayarı tanımlayan bir unsur olduğu için bilgisayara girmek veya zarar vermek isteyen bir üçüncü şahıs öncelikle işe bizim IP adresimizi tespit etmekle başlayacaktır. Hedef tespit edildikten sonrada sisteme giriş için diğer açıklar bulunmaya çalışılacaktır.

İnternette ve birçok ağ sisteminde halen kullanılmakta olan IP standardı IPv4 standardıdır. IPv4 içerdiği güvenlik unsurlarına rağmen gelişen yazılım ve donanım teknolojileri karşısında yetersiz kalmaktadır. Bu yüzden güvenlik tedbirlerinin yeterince düşünülmediği sistemlerden IP adresini bulup çıkarmak çok kolay bir hale gelmiştir. Çalıştırmakta olduğumuz birçok programda bulunan güvenlik açıkları da IP numaramızın istenmeyen kişilerin eline geçmesi için uygun bir zemin hazırlamaktadır.

IP adreslerinin güvenlik altında olması birçok kullanıcı için elzem bir konu haline gelmiştir. Bu nedenle geliştirilen bir yaklaşım IPsec olarak adlandırılmaktadır. IPsec özelliği oldukça karmaşık matematiksel fonksiyonlar içerse de, temelde IP yapısını parçalara bölerek çeşitli şekillerde şifreleyen ve karşılıklı sorgulayan bir seri işlem yürütür.

IPsec günümüzde kullanılan IPv4 standardı ile uyumludur. Birçok donanım üreticisi de IPsec özelliğini destekleyen donanımlar üretmektedir. 1995 yılında "Internet Engineering Tast Force (IETF) tarafından üretilen ve gelecekte kullanılması planlanan

---

[42] William Stallings, **Network Security Essentials** – ***Applications and Standards***, Pearson Education International, 2nd Edition, s.168.

IPv6 standardı IPsec özelliğini bünyesinde barındırmakta ve IP güvenliği konusunda daha güçlü bir nitelik vaat etmektedir.[43]

1.5.6. Web Güvenliği

"www (world wide web)" uygulamaları, temelde internet ve TCP/IP intranetleri üzerinde çalışan kullanıcı/sunucu uygulamalarıdır. İnternet iki yönlü bir yapıya sahiptir. Tüm elektronik yayınlar bu yapı içerisinde karşılıklı akarlar. İnternette bilgileri görüntülemenin en yaygın yolu internet gezgini (web browser) olarak adlandırılan görüntüleme yazılımlarının kullanılmasıdır. Gezginler kullanılması oldukça kolay, çok işlevli yazılımlardır. Bununla birlikte programın arkasındaki yapı çok karmaşık bir yazılımı içerir. Bugüne kadar edinilen tecrübeler, web gezginlerindeki bazı açıkların, kullanıcı bilgisayarlarına ve sunuculara ulaşmak için kullanıldığını göstermiştir.[44] Öyleyse web güvenliği denilince aklımıza gelmesi gereken bir nokta da gezginlerin güvenli iletişim kurmalarıdır.

Web üzerinden gelebilecek potansiyel tehditler sonraki bölümlerde açıklanacak tehditler konusunda kapsanacaktır. Burada bilinmesi gereken nokta, işletmelerin web güvenliği konusuna eğilirken öncelikle kendilerini tanıması, web üzerinde ne tür bir faaliyet gösterdiklerini ortaya koymasıdır.

1.5.7. Veritabanı Güvenliği

Veritabanları birçok işletme için hayati öneme haiz bir nitelik taşır. Bir anlamda işletme için her şeydir. Bir banka, telefon şirketi, internet servis sağlayıcı gibi birçok işletmede müşterilere ait bilgiler veri tabanlarında saklanır. Özellikle şirket veri tabanlarına internet üzerinden erişilmesine de müsaade ediyorsa, bu durumda güvenliğin tam anlamıyla sağlanması bir kat daha önemli hale gelir.

---

[43] William Stallings, **a.g.e.**, s.207 ve Nazife Baykal, **a.g.e.**, s.352.

[44] William Stallings, **a.g.e.**, s.214.

Veritabanları kendi bünyelerinde güvenlikle ilgili unsurları barındırırlar. Büyük ölçekli işletmeler de güvenliklerinden emin olabilmek için gelişmiş veritabanı yazılımlarını tercih etmektedirler. Piyasada veritabanı yazılımı ilgili çok fazla çeşit bulmak mümkündür. Ama bunlar arasında ciddi, profesyonel hizmet sağlayan, gerçek anlamıyla güvenli veritabanı yazılımı seçeneği sayısı çok fazla değildir. Burada işletmeler açısından karar verilmesi gereken birinci nokta güvenli veritabanlarıyla çalışmaktır. Bu husus işletmenin bütçesiyle doğrudan ilişkilidir.

İkinci nokta veritabanının yönetimidir. "Veritabanı Yönetim Sistemleri", veri girişi, veri değiştirme, okuma ve diğer güvenlik fonksiyonlarını yöneten yazılımlardır. Bu yazılımlar, maliyet olarak 50$'dan 10000$'a kadar değişen bir yelpaze içinde bulunmaktadır.

Veritabanı yönetim sistem yazılımları, erişim kontrol konusunda olduğu gibi, kimin hangi bilgiyi görüntüleyebileceği, değiştirebileceği, silebileceği konusunda da yetkileri belirlemektedir.[45] Dolayısıyla herkes yetkisi kadar işlem yapabilmektedir. Sistem aynı zamanda veritabanındaki hareketleri gözlemleyebilme yetisine sahiptir. Böylece sistem yöneticileri gerekli durumlarda müdahale edebilmekte, acil durumlarda, hatalı durumlarda yapılması gerekenler, iş işten geçmeden gerçekleştirilebilmektedir. Bu yapı yöneticilere, yönetim unsurlarının daha etkin bir şekilde yerine getirilmesinde büyük bir esneklik sağlamaktadır.

1.6. BİLGİ SİSTEMLERİNE YÖNELİK TEHDİTLER

Sistem güvenliği gereksinimlerinin ortaya konmasından sonra, muhatap olduğumuz tehditlerin de açıklanması ile güvenlik konusunun daha iyi anlaşılmasını sağlayacak, bu çerçevede alacağımız önlemler şekillenebilecektir.

---

[45] James Arlin Cooper, **a.g.e.**, s.266.

1.6.1. Zararlı Yazılımlar

Bilgisayar sistemlerine sızan zararlı yazılımlar oldukça karmaşık bir yapıya sahiptirler ve sisteme büyük zararlar verebilmektedirler. Zararlı yazılımların hazırlanış gerekçeleri, intikam duygusundan eğlenceye varana kadar geniş bir çeşitlilik gösterir. Gerekçesi ne olursa olsun bu yazılımlar sisteme çok büyük zararlar verdirebilme kabiliyetindedirler. Zararlı yazılımlar aşağıdaki şekildeki gibi tasnif edilebilirler.

Şekil 1.8 : Zararlı Yazılımların Tasnifi

KAYNAK : William Stallings, **Network Security Essentials** – ***Applications and Standards***, Pearson Education International, 2nd Edition, s.327

Şekilden de anlaşıldığı gibi zararlı yazılımları "konakçı bir yazılıma ihtiyaç duyanlar" ve "bağımsızlar" olarak iki grupta tasnif etmek mümkündür. Birinci grupta bulunanlar, işletim sistemi, bir uygulama yazılımı gibi özel bir yazılımın içine yuvalanırlar. Diğer gruptakiler ise her hangi özel bir yazılım içinde yuvalanmaya ihtiyaç duymaksızın faaliyet gösterirler. "Kendiliğinden çoğalabilirler" işareti ile gösterilen

grup ise bulaşma kabiliyetine sahiptir. Bir programdan diğerine, bir bilgisayardan öbürüne geçerek yaşamaya çalışırlar.[46]

1.6.1.1. Arka Kapılar

Arka kapılar, bazı kişilerin güvenlik erişim denetimlerine takılmadan doğrudan programların içine girmelerine olanak tanıyan gizli giriş noktalarıdır. Bu gizli giriş noktaları yıllardır programcılar tarafından hata ayıklamak, programı test etmek gibi gerekçelerle kullanılmıştır.

Programa giriş kodları art niyetli programcılar tarafından tespit edildiğinde ise güvenlik erişim kontrolü ortadan kalkacağı için üzerinde her türlü işlemi yapmak mümkün olacaktır.[47] Bilgi sızdırmak için çok uygun bir zemin hazırlayacaktır. Arka kapı girişlerinin tespit edilmesi de oldukça zordur. Bu anlamıyla gerçek bir risk yapısına sahiptir.

1.6.1.2. Mantık Bombaları

Mantık bombaları en eski yazılımlardan biridir. Herhangi bir programa gömülü olarak sisteme sokulur. Sisteme girdikten tetiklenmek için uygun şartların oluşmasını bekler. Bu şartlar, haftanın belli bir günün veya belirli bir tarihin gelmesi, belirli bir kullanıcının bir programı çalıştırması gibi olabilir. Belirlenen şartlar gerçekleştiğinde ise patlar. Patlama, bir virüsün ve kurtçuğun aktif hale geçmesi şeklinde görülebilir. Tetikleme gerçekleştikten sonra, sistemdeki veriler, silinebilir, değiştirilebilir, sistem çalışamaz hale getirilebilir veya başka şekillerde de zarar vermek mümkün olabilir.

---

[46] William Stallings, **Network Security Essentials** – ***Applications and Standards***, Pearson Education International, 2nd Edition, s.327.

[47] Sungwoo Taka & Sudhir Dixitb, E.K. Parka, "An end-to-end home network security framework" **Computer Communications**, USA, 2 Oct 2003, s.413.

1.6.1.3. Truva Atları

Bilgisayar dünyasında virüsler kadar ünlü olan zararlı yazılımlardan bir tanesi de Truva Atlarıdır. Yazılım, ismini aldığı tarihteki Truva atı gibi hareket eder. Asıl niyetini gizleyen uygulamalar olarak bilgisayar sistemlerine girmekte, yine kullanıcıya kendini hissettirmede faaliyetlerini sürdürmeyi amaçlamaktadır.

Truva atları genellikle bir taşıyıcıyla gelir. Elektronik posta ekinde gelen truva atları da son günlerde oldukça yaygındır. Aktive olduklarında öncelikle asıl görevlerini yerine getirmeye çalışırlar. Bu görevler genellikle güvenlikle ilgili görevlerdir. Sabit diskte kredi kartı bilgisi arama, arka kapı açma, güvenlik açıkları oluşturma, bunlardan bir kaçı olarak sayılabilir.

Truva atları birincil amaçlarını tamamladıktan sonra mantık bombaları gibi hareket ederek, gerekli şartların oluşmasına binaen ikincil amaçlarını faaliyete sokarlar. Bunlar; dosyaların silinmesi, makinenin formatlanması, ekrana çıkan bazı mesajlar, müzik çalınması gibi etkiler olabilir.

Yeni Truva atlarının bir çoğu bilgisayar korsanı araçları olarak geliştirilmiştir. Bilgisayar korsanları, truva atları vasıtasıyla girdikleri bilgisayarlardan gerekli bilgileri almakta, hatta sistemde açık kapılar bırakarak daha sonradan da defalarca girebilmektedirler. Truva atları, programlarla, e-postalarla, HTML (web sayfası formatında) koda gömülü olarak gelebilmektedir.[48] Nereden gelecekleri belli olmadığı için uygun güvenlik tedbirlerinin alınması sistem güvenliği açısından zaruridir.

1.6.1.4. Virüsler

En popüler zararlı yazılımlar virüs yazılımlarıdır. fark edilmemek ve kolayca yayılabilmek için mümkün olduğunca kısa yazılırlar. Virüslerin başarısı ile ilgili en önemli kriter, yayıldığı alan ve etkilediği bilgisayardır. Virüslerin en önemli

---

[48] Ziya Bahtiyar, **Virüsler ve Güvenlik,** Pusula Yayıncılık ve İletişim Ltd., İSTANBUL 2003, s.48.

amaçları bulaşmaktır. İkincil amaçları ise mesaj vermek, dosyaları silmek, format atmak, işletim sistemini çökertmek, güvenlik açıkları oluşturmak gibi faaliyetlerdir.

Virüsler günümüzde oldukça karmaşık bir yapıya sahiptirler. Bununla birlikte klasik bir tasnifini aşağıdaki tabloda görüldüğü gibi yapabiliriz.

Tablo 1.1 : Virüslerin Genel Tasnifi

VİRÜSLER		
Boot virüsü	Dosya virüsü	Makro Virüsü

Virüslerin başlıca zarar verme şekilleri şunlardır.

- Bulaşmak,
- Bilgisayarı yavaşlatmak,
- Dosyaları silmek, değiştirmek, bozmak,
- Sabit diski formatlamak ya da kısmen zarar vermek (veri kaybına yol açmak),
- İşletim sistemini çökertmek,
- Donanımsal sorunlara yol açmak,
- İtibar kaybettirmek,
- Güvenlik açıkları oluşturarak sistemin saldırılara açık hale getirilmesini sağlamak.

Virüsler tarafından kullanılan ortak bazı özel teknikler vardır. Bunlar virüsün karakteristik özelliklerini belirlemede önemli rol oynarlar. Aşağıda görülen tabloda bu özellikler açıklanmaya çalışılmıştır.

Tablo 1.2 : Virüslerin Kullandığı Ortak Teknikler

Virüslerin Kullandığı Ortak Teknikler	
Dosya Üzerine Yazma (Overwrite)	Daha çok ilkel virüsler tarafından kullanılan bir yöntemdir. Virüs kendini hedef dosyanın başına yazar. Dosyanın, virüs uzunluğu kadarki ilk kısmını tamamen siler. Böylece geri

	döndürülemez bir şekilde zarar verilmiş olur.
Saklı (Stealth)	Tespit edilmeyi engellemek için kullanılan saklanma veya kendini gizleme tekniklerine verilen genel addır. Birçok virüs kendisini gizleyebilmek için çaba gösterir.
Şifreli (Encrypted)	Tespit edilmeyi ve temizlenmeyi zorlaştırmak için virüs yazarlarını kullandığı bir tekniktir. Virüs kodunun mantıksal veya başka bir yöntemle şifrelenmesidir.
Şekil Değiştiren (Polymorphic)	Her bulaşmada içeriği değişerek imza (ya da parmak izi) temelli virüs tespit yöntemlerini atlatmayı hedefleyen bir yöntemdir. İleri düzey bir tekniktir. Pratikte uygulanması zordur.
Retro	Doğrudan anti virüs programlarına saldıran virüslere verilen addır. Bunlara tanıtılan anti virüs programlarına çeşitli yöntemlerle zarar verirler. Anti virüs programlarını doğrudan çalışamaz hale getirenleri olduğu gibi, çalışmasına rağmen virüs yakalayamayacak hale getirenleri de vardır.
Sahte yükleme (Fake Boot)	Ctrl-Alt-Del tuşlarına basılarak yapılan soft reset'te bellekte kalmayı başarabildiği iddia edilen virüslerin özelliğidir.

KAYNAK : Ziya Bahtiyar, **Virüsler ve Güvenlik**, Pusula Yayıncılık ve İletişim Ltd., İSTANBUL 2003, s.48

Virüslerle ilgi çok şey söylemek mümkündür. Bilgisayarın yaygınlaşmaya başladığı yıllardan itibaren virüslerin de ortaya çıktığını, çok büyük maddi ve manevi kayıplara yol açtığını bilmekteyiz. Her ortaya çıkan virüs için anti virüs yazılım şirketleri tarafından piyasaya sürülen temizleme programları mevcuttur. Anti virüsler, "önlemler" konusunda detaylı olarak anlatılmaya çalışılacaktır.

1.6.1.5. Kurtçuklar (Solucanlar)

Son yılların en popüler virüsümsüleri olan kurtçuklar, virüslere oldukça benzer özellikler taşırlar. Kurtçuklar bazı literatürlerde virüsler konusu altında incelenmektedirler. Kurtçukların virüslerle olan temel farkları yayılmak için bulaşmak zorunda oldukları bir dosyaya (konak) ihtiyaç duymamalarıdır. Bir anlamda bulaşmadan

kopyalanma yoluyla çoğalırlar ve yayılırlar. Yayılmak için ağları kullanırlar. Bu ağ kurumsal bir ağ (YAA veya GAA) olabileceği gibi internet de olabilir.

1.6.1.6. Zombiler

Zombiler, internet üzerinden başka bir bilgisayara yerleşen ve buradan diğer bilgisayarlara saldırmaya hazırlanan programlardır. Bu şekilde yayılması nedeniyle yaratıcısını bulmak oldukça güçtür. Genellikle hedef seçilen bir web sitesine saldırı amacıyla kullanılır. Zombi programın yayıldığı tüm bilgisayarlar hedef siteye karşı aynı anda taarruza geçer. Böylece sitenin çökertilmesi ve kullanılamaz hale gelmesi hedeflenir.[49]

1.6.2. Güvenlik Saldırıları

Bilgi sistemlerinin güvenliğini yönelik saldırıları sınıflandıracak olursak, bunu "aktif saldırılar" ve "pasif saldırılar" olarak ikiye ayırabiliriz. Pasif saldırılar, sistemde bulunan bilgileri çekmek için yapılmaktadır. Sistem kaynakları bu saldırılardan etkilenmez. Aktif saldırılarda ise sistem kaynakları değişikliğe uğrar.

1.6.2.1. Pasif Saldırılar

Pasif ataklar; dinleme, gözetleme, data aktarımı gibi faaliyetleri içerir. Amaç bilginin ele geçirilmesidir. Bunun için iki yoldan söz edilebilir. Birincisi gönderilen e-posta içeriklerinin yakalanması, ikincisi data trafiğinin analiz edilmesidir. Bu sayede gizlilik dereceli bilgiye sahip dokümanlar, yazışmalar ele geçirilir. Alınması gereken en etkili tedbir, posta içeriklerinin kriptolanmasıdır. Bu şekilde kriptolanan muhteviyatın ortaya çıkarılması düşük bir olasılığa sahiptir.[50]

---

[49] William Stallings, **a.g.e.**, s.328.

[50] William Stallings, **a.g.e.**, s.5.

Pasif ataklar, doğası gereği ortaya çıkarılması çok güç olan bilgi çalma teknikleridir. Bunun nedeni herhangi aktif bir faaliyet yürütmemeleri, bilgileri değiştirmeye çalışmamalarıdır.

1.6.2.2. Aktif Saldırılar

Aktif saldırılar, data akışı üzerinde değişiklik yapan saldırı türleridir. Bunlar dört kategoride incelenebilir; maskelemek, yeniden çalıştırmak, mesaj modifikasyonu ve servisin kilitlenmesi.

Maskeleme, üçüncü bir şahıstan gelen bilgiyi, tanınan birinden geliyormuş gibi göstermektir. Bu sistemin güvenlik katmanlarından geçebilmek için gerekli bilginin sağlanması, daha sonra da sisteme kolay giriş yapılması demektir.

Yeniden çalıştırmak, pasif bir saldırı ile elde edilen sistem güvenliği bilgilerinin yeniden çalıştırılarak yetkisiz giriş yapabilme işlemidir.

Mesaj modifikasyonu, mesaj tamamının veya bir kısmının değiştirilmesi, geciktirilmesi veya tekrar istenmesi gibi faaliyetlerdir. Bu sayede daha sonradan sistemdeki gizlilik dereceli bilgilere nüfuz edebilme imkanı ortaya çıkar.

Servisin kilitlenmesi, tüm mesaj trafiğinin belirlenen bir hedefe yönlendirilerek sistem yoğunluğunun artırılması ve normal servisin kullanılamaması gibi bir dizi faaliyeti içerir. Bu faaliyetlerden dolayı ağ kullanılamaz hale gelir veya performansı önemli ölçüde düşer.[51]

1.6.3. Bilgisayar Korsanlığı (Hacking)

Bilgisayar korsanlığı, bilgi sistemlerinin en büyük tehditlerinden biridir. Bilgisayarlara ve bilgisayar ağlarına izinsiz olarak girmek için çaba gösteren korsanlar,

---

[51] William Stallings, **a.g.e.,** s.8.

yaygın olarak "hacker" olarak tanınmaktadırlar. Bir önceki konuda açıklanan aktif ve pasif güvenlik saldırıları bu korsanlar tarafından yapılmaktadır.

Bu çalışma, ağ güvenliği konusu ile ilgili olduğu için korsanların hangi teknikleri kullandığı detaylı olarak açıklanmayacaktır. Bu konuda genel olarak bilgi verilecektir. Bilgisayar korsanları pasif ve aktif güvenlik saldırılarının tümünü gerçekleştirirler. Bununla birlikte genel bir yaklaşım olarak ilk öğrenmeye çalışacakları şey hedef bilgisayarın IP'si olacaktır. IP numarası öğrenildikten sonra da diğer sızma yolları denenecektir.[52]

IP numarasının ortaya çıkartılması ile birlikte sisteme giriş yapmak için bazı açık noktaların bulunması gerekmektedir. Bilgisayar korsanlığı profili incelendiğinde, genellikle genç, kendini ispat çabasında olan ve bazı bilgileri diğerlerinden daha çabuk öğrenerek ön almak isteyen meraklı insanların bu işlerle alakadar oldukları görülür. Yeni sürüm işletim sistemleri ve diğer bilgisayar programlarında bulunan güvenlik açıkları, korsanlar tarafından tespit edilmeye çalışılır.[53] Hatta bu konuda uygulanan bir yöntemde, programların internet sitelerinde yayınlanan güvenlik uyarılarını, yamaları takip ederek neler yapılacağını bulmaktır. Güvenlik ile uyarılar sitede yayınlansa da, bütün sistem yöneticileri veya bilgisayar kullanıcıları, sistemlerini, bilgisayarlarını bu güvenlik uyarılarına karşı güncellemezler. Bu durumdaki kullanıcılar, korsanlar için yeni potansiyel hedefleri oluşturur.[54]

IP numarasının tespiti ve sisteme giriş yapabilmek için birçok program ücretsiz olarak dağıtılmaktadır. ICQ, P2P gibi bütün dünyada yaygın olarak kullanılan iletişim yazılımları da IP adresinin gizlenmesi konusunda büyük güvenlik açıklarına sahiptirler.[55] Örneğin bu ücretsiz yazılımları kullanarak, eğer birisinin ICQ numarasını

---

[52] IP güvenliği ile ilgili daha fazla bilgi için 1.6.5 IP Güvenliği konusuna bakınız.

[53] Srinivas Mukkamala "Intrusion detection using an ensemble of intelligent paradigms" **Journal of Network and Computer Applications,** USA, 7 Jan 2004, s.3.

[54] **Hacker Avında Son Perde,** Chip dergisi, İstanbul, Haziran 2003, s.24.

[55] Vasileios Vlachos, "Security applications of peer-to-peer networks", **Science Direct,** Athens/Greece, 14 Jan 2004, s.196.

biliyorsanız, IP numarasını da saniyeler içinde tespit edebilirsiniz. Daha sonra da bilgisayara giriş yapacak uygun bir port bulmak gerekir. Bir bilgisayarda 65536 adet port bulunur. Yani internete bağlı bir bilgisayarı korumak 65536 kapısı bulunan bir kaleyi saldırganlara karşı korumaya çalışmak kadar zor olacaktır. "Port Scanner" türü yazılımlar, bütün bu portları tarayarak hangilerinin uygun olduğunu ortaya koymaktadır.

Portların tespit edilmesi de tamamlandıktan sonra, işletim sistemlerinin oluşturduğu dosya paylaşımı özelliği giriş için en uygun yeri oluşturur. Buraya ulaştıktan sonra da yapılacak iş parola ve şifreleri, dosya paylaşımlarını yeniden düzenlemek olacaktır. Bilgisayar kullanıcısı sonradan dosya paylaşımını kapatsa bile, korsan için diğer girişlerinde dosya paylaşımını yeniden kendisine göre değiştirmek sorun olmayacaktır.

Bilgisayar korsanları ile güvenlik personeli arasında çok sıkı bir mücadele devam etmektedir. Yakalanabilen korsanlar ülkelerin kendi hukuk sistemine göre cezalandırılmaktadır. Yalnız bilgisayar suçları konusunda standart bir hukuk kavramı, bu konu doğrultusunda geliştirilmiş kanunlar her ülkede bulunmamaktadır. Kanunlardaki açığın giderilmesi içinde hukukçular ve bilişimciler tarafından yoğun bir çalışma yürütülmektedir.

1.6.4. Bilgi Sızıntıları (Tempest)

Bilgi sızıntısı; monitör, kasa, data hatları gibi donanımlardan yayılan radyasyonun oluşturduğu tehlikeye denir. Bu donanımın yaydığı radyasyon uygun cihazların elde edilmesi ile data olarak yeniden dönüştürülebilir. Fiziki sistem güvenliği bölümünde hatlardan yayılan radyasyon hakkında bilgi verilmiştir.

Bilgi sızıntısı ile ilgili olarak, bulunulan bölgeye göre kullanılacak teçhizat kategorilendirilir. Bu kategorilendirmede, bölgenin hassasiyeti, cihazların durumu göz önüne alınır. Yayılan radyasyondan bilgi elde etmeye yarayan saldırı türleri pasif saldırılar kapsamında mütalaa edilebilir. Bu tarz bir hareket herhangi bir bilgi veya sistem kaynağını değiştirmeye çalışmaz.

Bu nedenle yayılan radyasyonun pasif saldırı türleri ile ele geçirilmesini engellemek gerekir. Radyasyonun bilgiye dönüştürülmesinde en belirgin iki ünite, monitörler ve data hatlarıdır. Monitörler, yaydıkları radyasyondan dolayı kolaylıkla izlenebilirler. Bu nedenle açık arazide, korumasız bölgelerde bulunan bilgisayarlarda gizlilik dereceli bilgiye nüfuz edilememesi gerekir. Diğer bir ifade ile gizlilik dereceli bilgilerin işlem gördüğü bilgisayarlar, korumalı bölgeler içinde bulundurulmalıdır. Bu sayede monitörlerden yayılan radyasyonun bilgiye çevrilmesindeki risk en aza indirilmiş olur.

Hatlardan yayılan radyasyonun okunabilmesi ihtimali ise göz önüne alınması gereken diğer bir noktadır. Bunun için en iyi önlem ise fiber optik kabloların kullanılmasıdır. Fiber optik kablolar ışık iletimiyle çalıştıklarından radyasyon yaymazlar. Bununla birlikte, hassas bölgelerde (giriş ve çıkışlarda) kullanılan fiberoptik kabloların üzerinde bulunan metal katmanın en az 2 metrelik bir bölümünün soyulması o bölgede oluşabilecek sızıntının dışarıya kaçmasının engellenmesi gerekmektedir. Bu yöntem bir nevi filtreleme görevi görmektedir. Bunun yanında bakır kabloların, fiber optik kablolarla olan bağlantısında da tedbir almak gerekir. Kriptolanmamış gizli bilgiyi taşıyan bakır kabloların metal kanallar içerisinde bulundurulması sızıntıyı önlemek için kullanılan bir yöntemdir. Bu metal kanallar ayrıca güvenli toprak hattına bağlanırlar ve herhangi bir sızıntı oluşması durumunda sızıntının güvenli bir şekilde toprağa aktarılmasını sağlarlar.

Korumalı bölgelerin seçimine titizlikle karar verilmelidir. Korumalı bölge dışında kullanılacak bilgisayarların ve donanımlarının sızıntı korumalı olması gerekmektedir. Bu da bilgisayar maliyetini 5 ila 10 kat artıracaktır. İşletmeler açısından diğer bir konu da sızıntı ölçümlerinin periyodik olarak yapılmasıdır. Periyodik olarak yapılan bu faaliyet risk değerlemesi ve analizinde önem taşır. Bu sayede oluşabilecek potansiyel riskler en aza indirilebilir.

1.6.5. Bilgi Kaçış Noktaları

Bilgi kaçış noktaları olarak tanımlanan yerler, bilginin sistemden çıktığı noktalardır. Bilginin sistemden çıktığı noktalar bir kaçak veya sızıntı gibi algılanmamalıdır. Bunlar normal sistem prosedürleri dahilinde olan işlemlerdir. Bu noktalar arasında bilginin sayısal ortamdan alınarak basılı doküman haline getirildiği yazıcılar, disket sürücüleri, CD/DVD yazıcıları, USB hafıza araçları, harici disk üniteleri gibi birçok donanım sayılabilir. Sistemden bilgi çıkışı olması dolayısıyla, belirtilen yerlerin kontrol altında olması gereklidir. "Güven kontrole mani değildir" prensibi doğrultusunda her ne kadar personelimize güveniyor olsak da, gerekli kontrolleri yapıp ilgili tedbirleri almak zorunda olduğumuzu unutmamalıyız. Bunun için kendi kedini düzenli olarak güncelleyen bir mekanizma geliştirmemiz gerekir.

1.6.5.1. Yazıcılar

Yazıcılar vasıtası ile sistemdeki bilgi basılı doküman haline getirilir. Bilgisayar ağları, bilgi yönetiminin en önemli aracı durumundadır. Dolayısıyla bilginin sayısal olarak hareket etmesi, dağıtımı ve işlenmesi istenir. Bunlara ek olarak bilgisayar vasıtasıyla basılı doküman maliyetinin en aza indirilmesi ve bürokratik engellerin ortadan kaldırılması hedeflenir. Böyle bir bilgi yönetim sisteminde yazıcılar ne kadar az kullanılıyorsa, sistem de o kadar güzel işliyor demektir. Bunun yanında, bilginin yedeklenmesi, güvence altına alınması, daha işlevsel olarak incelenmesi veya alışkanlık gibi sebeplerle basılı metin halinde kullanılması gerekebilir. İşte yazıcılar da bunun için vardır.

Yazıcıları güvenlik yönüyle incelediğimiz de ise, bilginin basılarak dışarıya taşınabilmesi anlamında, kontrol unsurunun ön plana çıktığını görmekteyiz. Bu ihtimal göz önüne alındığında, personelin yazıcıları mümkün olduğunca az kullanması tavsiye edilmelidir. Bunun hem ekonomik, hem de güvenlikle ilgili boyutu vardır.

Sistemde ağ yazıcıları kullanılmalı ve yazıcıların kurulacağı yerler, yazdırma yoğunluğuna, ergonomiye göre belirlenmelidir. Yazıcılar, kontrollü bir bölgede bulunmalıdır. Hangi bilgilerin basıldığı böylece gözlem altında tutulabilir.

Kesin bir önlem olarak, işletme giriş ve çıkışlarında periyodik veya örnekleme usulü güvenlik kontrolleri yapılabilir. Bu kontrollerin caydırıcılık gücü de yüksektir. Güvenlik personeli ne tür materyal arayacağı konusunda bilgilendirilir.

1.6.5.2. Disket Sürücüler

Disketler bilgi taşıma ortamlarından bir tanesidir. Yeni kullanılan teknolojilerde disket ve disket sürücü ortamları bulunmasa da kullanılan birçok sistem 3,5"lik sürücülere sahiptir. Disketler malzeme olarak kolaylıkla tespit edilemezler. Basılı materyallere nazaran daha küçüktür ve saklanması daha kolaydır. Aynı zamanda disket içeriğinin kontrol edilebilmesi için güvenlik noktalarında uygun donanımın ve ehliyetli bir güvenlik personelinin bulunması gereklidir.

Disket sürücülerin kontrol altında tutulması ise yazıcılara göre daha kolaydır. Bir bilgisayarda disket sürücü bulunsa bile, işletim sistemi üzerinden kullanımı iptal edilebilir. Hassas ve gizlilik dereceli bilginin bulunduğu işletmelerde disket sürücülerinin kullanılmasına ihtiyaç duyulan bilgisayarlar tespit edilir. Bu sayı güvenlik açısından kontrol altında tutulabilecek bilgisayar limitini geçmez. Diğer disket sürücülerin tamamı yazılımsal olarak kullanılamaz hale getirilir. Kullanıma açık disket sürücülerin de mekanik bir cihaz vasıtasıyla kilit altında tutulması uygulanan bir yöntemdir. Böylece disket sürücülerin ehliyetsiz kişiler tarafından kullanılması engellenebilir. Disketlerle ilgili olarak; işletme dahilinde kullanılan bütün disketlerin gizlilik derecelerinin üzerine basılı olarak bulunması güven duygusunu artırır. Üzerinde gizlilik derecesi olmayan bir disket asla bulunmaz ve kullanılmaz. Disketlere gizlilik derecesini belirten etiketlerin basılması sistem güvenlik personelinin sorumluluğunda bulunur.

1.6.5.3. CD/DVD Okuyucu ve Yazıcılar

CD/DVD gibi medyalar da bilginin kolaylık taşındığı bir ortam oluştururlar. Asıl itibariyle CD/DVD okuyuculardan medya üzerine yazmak mümkün değildir. Bu medyaya yazabilmek için CD/DVD yazıcıların kullanılması gerekir. Eğer sistemde

CD/DVD yazıcı kullanmıyorsanız veya sistem yöneticilerinin %100 kontrolünde yazma işlemleri gerçekleştiriliyorsa sorun çok büyük bir oranda çözülmüş demektir.

CD/DVD sürücülerde dikkat edilmesi gereken önemli bir husus da, okuyucu ve yazıcıların, bilgilerin kaçırılacağı bir ortam olarak düşünülmemesi gerektiğidir. Bu ortamlar aynı zamanda sisteme bilgi girişinin yapıldığı cihazlardır. Bu nedenle de sistem güvenliğine risk oluşturmaktadır. CD/DVD'lerde bulunan bilgilerde virüs olması durumunda, ağa virüs bulaşması ve büyük maliyetlere varan zararlara yol açması işten bile değildir. Yapılacak iş, disket sürücülerde olduğu gibidir. Sürücülerin kullanımı kısıtlanır ve kontrol altında tutulur.

1.6.5.4. Diğer Harici Medya

Diğer harici medyadan kasıt, disket ve CD/DVD gibi taşınabilir bilgi ortamları olan cihazları tanımlamaktır. Bu cihazlar teknolojileri yeni olan ve son birkaç yıl içerisinde kullanımı yaygınlaşan USB hafıza cihazları, hafıza kartları, harici disk üniteleri gibi medyalardır. Windows 2000, Windows XP gibi çıkan son işletim sistemleri bu tür cihazlara doğrudan destek vermektedirler. Bunun anlamı, cihazın bilgisayara takılır takılmaz, herhangi bir kurma işlemi ve denetimi olmaksızın kullanılabilir hale gelmesidir. Oldukça hızlı veri transferi yapan bu cihazların taşınması, kullanılması ve gizlenmesi çok kolaydır. Bir kalemin, saatin, kolyenin veya benzer şekilde günlük olarak kullandığımız bir eşyanın içine monte edilen ve piyasada rahatlıkla bulunan bu bilgi taşıma ortamları, profesyonel casusların kullandığı cihazlara benzer bir rahatlık ve esneklik sağlamaktadır.

Alınacak tedbir, sistem güvenlik yöneticileri tarafından USB portlarının kapatılması, kullanılamaz hale getirilmesi şeklindedir. Bu durum ise profesyonel, uzman personel istihdamını gündeme getirmektedir. Bu personelin sisteme hakim olması, son çıkan gelişmeleri ve güncellemeleri yakınen takip etmesi gerekir.

1.6.6. Bilinçsiz Kullanım

Bilinçsiz kullanım sistemdeki kullanıcıların sistem üzerindeki etkisi ile ilgilidir. Ağ üzerindeki bir kullanıcının sistemin bütün özelliklerini bilmesi veya görev konumuna göre bilgisayar uzmanı olması beklenemez. O sadece kendi üzerine düşen, sorumlu olduğu görevleri yapması gereken tanımlı bir kullanıcıdır. Bununla birlikte sistem dosyalarının silinmesi, veritabanı dosyalarında tahrifata yol açılması, sistem kaynaklarının uygun olmayan bir şekilde değiştirilmesi sıklıkla rastlanan örneklerdendir. Bu durum personelin bilgisayar ve ağ konusundaki bilgisiyle ve niyetiyle doğru orantılıdır. Belki de çok iyi niyetli ve masumane yapılan bazı işlemlerin sonucunda oluşan zarar, sisteme virüs bulaştığında verebileceği zarar kadar büyük olacaktır.

Bu bağlamda kullanıcıların erişim hakkının iyi analiz edilmesi ve doğru bir kullanıcı profili oluşturulması önem arz eder. Doğru kişilere doğru yetkilerin verilmesi sistem güvenliğini artıracaktır. İlave olarak bilgi çağında ve bilgi ağlarının kurulu olduğu modern işletmelerde bilgisayar bilgisi olmayan kullanıcıların mevcudiyeti çok fazla bağdaşmayan iki ayrı öğe gibi durmaktadır. Böyle bir durumda yapılması gereken en doğru seçeneğin, bilgi yönetim sistemlerini kullanma konusunda yetersiz olan personelin hizmet içi eğitime tabi tutulması olacağı düşünülmektedir. Eğitim süreklilik arz eden bir konudur. Eğitim süreci içerisinde, bilinçsiz kullanımdan kaynaklanan sorunların önüne geçmek mümkündür.

1.6.7. Sabotaj

Kötü niyetli kişilerce yapılan bir tahrifattır. Yazılımsal veya donanımsal olarak yapılabileceği gibi sistemi felç edecek diğer hassas bir bileşene karşı da yapılabilir. Failler işletme içinden veya dışından olabilir. İşletmenin rakipleri, bazı çıkar grupları veya maceraperest bazı insanlar potansiyel sabotörler olabilirler. İşletme içinden ise küskün, yönetime kızgın, işinden atılmış veya ayrılmış çalışanların da intikam, cezalandırma gibi çeşitli duygularla benzeri eylemlere giriştikleri bilinmektedir. 1996 yılında Omega Mühendislik Şirketi çalışanı Timothy Lloyd'un

eylemi hafızalar kazınmış bir örnektir. Lloyd, NASA ve donanma ile birlikte çalışan ve çok büyük bir şirket olan Omega'dan kovulduktan sonra intikam almak için yazdığı 6 satırlık bir kod ile üretim-operasyon sistemini çökertmiş ve eski şirketini tahmini olarak 10 ila 12 milyon dolar zarara sokmuştur.[56]

Sabotaj konusuyla güvenlik personelinin çalışma metotları, güvenlik konusuna yaklaşımları, bilgi seviyeleri, alınan tedbirler yakından ilgilidir. Güvenlik olayının kaba kuvvet kullanmak, insanları korkutmaya çalışmak olmadığı iyi anlaşılmalıdır. Güvenliğin yeni boyutu olan ağ ve bilgi güvenliği özellikle, risk analizi, doğru tahmin, yüksek bilgi seviyesi, işlevsellik, zamanında ve doğru kararlar alabilme gibi unsurlarıyla klasik yaklaşımlardan ayrılmaktadır. Bilgi güvenliği personelinin bu yeterliliğe sahip olması gerekmektedir.

1.7. BİLGİ SİSTEMLERİNDE ALINMASI GEREKEN ÖNLEMLER

Bilgisayar ağ yapısına olan tehditler bir önceki bölümde açıklanmıştır. Bu bölümde olası tehditlere karşı alınması gereken önlemler açıklanmaya çalışılacaktır. Tehditler bölümünde olduğu gibi önlemler bölümünde de konu bütünsel bir tarzda incelenecektir.

1.7.1. Kripto Sistemlerinin Kullanılması

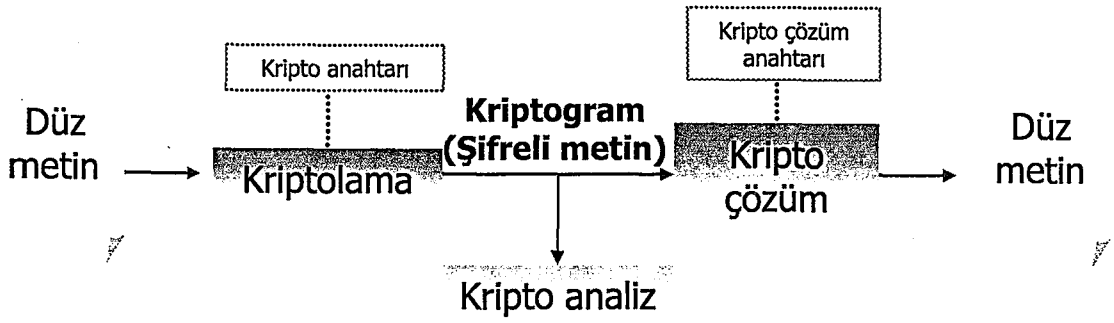
Kriptolama, iki bilgisayar arasında veya iki ağ düğümü arasında aktarılan bilginin çalınmaya karşı, istenmeyen üçüncü kişiler tarafından ele geçirilmesine karşı özel tekniklerle şifrelenmek suretiyle gönderilmesi olayıdır. Bu yüzden Kriptolama bilgi güvenliğinin en üst konusudur.

Kripto sistemi, bilgiyi kriptolayan ve kriptoyu çözen bir algoritmadan oluşur. Sistemde, kripto çözümünde bir kripto çözüm anahtarı bulunur. Simetrik yapıda anahtar, kriptolamada kullanılan anahtarla aynıdır. Asimetrik yapıda ise bu iki anahtar

---

[56] **"Hacker Avında Son Perde"**, Chip dergisi, İstanbul, Haziran 2003, s.22

farklıdır veya genel anahtar sistemi kullanılır. Her iki şekilde de kriptogramın (kripto algoritma yapısının) kriptoanalize (kriptonun analiz edilerek deşifre edilmesi) direnç gösterecek bir yapıda olması gerekir.[57] Kriptolama sisteminin çalışma prensibi aşağıdaki şekilde açıklanmaktadır.



Şekil 1.9 : Temel Kriptolama Yapısı

KAYNAK : James Arlin Cooper, **Computer and Communications Security,** Intertext Publications McGraw-Hill Book Company, 1989 s.311

Kriptolar, geçmişten günümüze büyük değişim göstermiştir. Bu değişimi şu şekilde özetlemek mümkündür;

Karakterler yerine bloklar halindeki bitlerle işlem yapılması,

Geniş bir anahtar aralığı kullanılması,

Anahtar aralığı önemli bir tasarım konusu haline gelmesi,

Karmaşık algoritmalar kullanılması.[58]

Gelişen teknolojiyle birlikte bilgisayar hızları her yıl katlanmaktadır. Bu durum, tasarlandıkları zaman güvenli olan yöntemlerin çok kısa bir süre sonra artık güvenli olmaktan çıkmasına yol açmaktadır. Yukarıda anılan maddeler, bu bağlamda kripto gelişimindeki yapıyı özetlemektedir.

---

[57] James Arlin Cooper, **Computer and Communications Security,** İntertext Publications McGraw-Hill Book Company, 1989 s.311.

[58] Nazife BAYKAL, **Bilgisayar Ağları,** SAS Bilişim Yayınları 2001, 1nci baskı, s.344.

Modern kriptografinin amacı, şifreleme algoritmalarını karmaşıklaştırarak, kriptoanalistlerin elinde çok miktarda şifrelenmiş metin olmasına karşın, bir şey yapamadığı sistemler tasarlamaktadır. Bu sistemlerden en yaygın olarak kullanılanlar;

- DES (Data Encryption Standard – Veri Şifreleme Standardı) ve
- AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı).

1.7.1.1. Veri Şifreleme Standardı (DES)

Ocak 1977'de ABD hükümeti, IBM tarafından geliştirilmiş olan bir kriptoyu tasnif dışı veriler için resmi standart olarak benimsemiş ve bu kriptoya DES adını vermiştir. DES, günümüze kadar banka işlemleri gibi birçok alanda yaygın olarak kullanılmıştır.

DES'in kripto algoritması ile 64 bitlik bloklar halinde şifrelenmiş bir metin elde edilir. Algoritma, 56 bitlik bir anahtar kullanır. 16 döngü içerir.[59]

DES'in güvenliği konusunda birçok tartışma halen süregelmektedir. Tartışmaların odak noktası, DES'in tasarlandığı yıldan bugüne kadar, bilgisayar hızlarının oldukça artması ve kriptonun analiz edilebilmesi ihtimalinin yükselmesidir. 1998 Haziranında Elektronik Öncü Kuruluşunun (Electronic Frontier Foundation – EFF) yaptığı bir açıklamada, 250000$'a mal edilebilecek DES kırıcı bir bilgisayarla, kriptonun kırılmasının üç günden az bir zaman alacağı belirtilmiştir.[60] DES'in uzun yıllardır kullanılıyor olması ve tamamen farklı bir algoritmaya geçilmesinin birçok DES donanımını kullanılamaz duruma düşüreceği bir diğer gerçektir. Bu nedenle üçlü DES gibi DES varyantı tasarımlar gündeme gelmiştir. Üçlü DES, 1 yerine 3 DES döngüsü ve 56 ikil yerine 112 ikil anahtar kullanan, çok daha güvenilir bir algoritmadır.

---

[59] Nazife BAYKAL, **a.g.e.**, s.345.

[60] William Stallings, **Network Security Essentials** – ***Applications and Standards***, Pearson Education International, 2nd Edition, s.35.

1.7.1.2. Gelişmiş Şifreleme Standardı (AES)

AES, DES'in yerine kullanılması düşünülen çok gelişmiş bir şifreleme standardıdır. Geliştirme çalışmaları halen devam etmektedir. Geliştirme çalışmaları açık bir yarışma şeklinde yapılmaktadır. Karar vermek için yarışmacı ve uzmanların yorumlarına başvurulmaktadır. Yarışma sırasında katılımcıların birbirlerinin tasarımlarını kırmaları için çaba göstermeleri istenmektedir.

Kripto, bir organizasyonda en üst düzeyde güvenliğe sahip bir unsurdur. Kriptoların kaybedilmesi, çaldırılması, yetkisiz kişilerin eline geçmesi çok büyük bir güvenlik ihlalidir. Böyle bir durumda aynı kripto ile çalışan bütün ağlar kriptolarını değiştirmek zorundadır. Değişim gerçekleşene kadar da tüm ağ yapısı güvensiz bir durumda bulunur. Bu nedenle kriptonun sağladığı güvenliğin anlamlı olabilmesi için, kriptonun güvenliğinin sağlanması gerekir. Bu kriptolamanın olmazsa olmaz prensibidir.

1.7.2. Kripto cihazlarının yerleştirilmesi

Kripto cihazları güvenlik açısından çok büyük öneme haizdir. Bu nedenle kripto cihazları sadece yetkili personelin girebileceği bir bölgede bulundurulmalıdır. Bulunduğu yer özel güvenlik tedbirlerine sahip olmalıdır. Giriş çıkış koruması, üç kombineli şifreli kilitlere sahip giriş kapısı, fiziki duvar koruması gibi unsurlar özel güvenlik tedbirlerinin arasında sayılabilir.[61] Kripto odası mutlaka korumalı bölgede olmalıdır. Korumalı bölgeden kasıt ise bölge korumasının silahlı özel güvenlik birimleri tarafından yapılıyor olmasıdır.

Kripto odalarının yerleştirilmesinde tek sınırlayıcı etken, bilgi güvenliğinin sağlanıyor olabilmesidir. Onun haricinde farklı bir kıstas içermez. Güvenlik kıstasını sağlayacak şekilde işletmenin herhangi bir bölümünde konumlandırılabilir.

---

[61] **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part II Chapter1, s.20-24.

1.7.3. Kriptoların değiştirilmesi

Kriptolar, en üst seviyede korumaya sahiptir. Bununla birlikte ağlarda kullanılan kriptolar en az 6 ayda bir değiştirilmelidir. Kripto değişimini dikte ettiren unsurlar arasında, kripto cihazının kabiliyeti, yapılan işin ve işletmenin yapısı ve bilginin hassasiyet derecesi sayılabilir. Bu paralelde kripto değişimi yukarıda sayılan unsurlara bağlı olarak 6 aydan 1 güne kadar değişen periyotlarda yapılır.

Kripto değişiminin en önemli gerekçesi, herhangi bir çalınma, kaybolma ve deşifre durumunun gerçekleşmesidir. Diğer bir gerekçe ise kripto anahtarlarının kullanıldığı zaman aralığının uzaması ile birlikte deşifre edilme riskinin artmasıdır. Bu prensip "bütün şifrelerin deşifre edilebileceği ama zamana bağlı olduğu" gerekçesini taşır. Örneğin evimizde kullandığımız bir bilgisayar ile DES algoritmasını normal insan ömrü içerisinde çözmek mümkün değildir. Artan bilgisayar hızları ve düşen maliyetler göz önüne alındığında bu süre daha da aşağı çekilecektir. Kripto değişim zamanına karar verirken muhtemel risk unsurları göz önünde bulundurulmalıdır.

1.7.4. Parola Yönetimi

Parola koruması ağın saldırganlara karşı korunmasında ön hattı oluştururlar. Çok kullanıcılı sistemlerde kullanıcının sadece kimlik bilgilerinin onaylanması yeterli olmaz. Aynı zamanda her kullanıcıya ait bir parola olmalıdır. Bu parola sunucuda da bulunur ve kullanıcı sisteme girmeye çalıştığında karşılıklı olarak sorgulanır.

Parola korumasına karşı farklı sistemler geliştirilmiştir. Bunlardan en yaygın olarak kullanılanı, kriptolamada ana mantığı açıklanmış olan parolanın özel anahtar – genel anahtar şifrelemesidir. Bu şifreleme, parolaların istenmeyen kişiler tarafından ele geçirilmesini önlemek için kullanılır.

Kripto algoritmasının sağladığı güvenlik unsuru, kriptoanalist olarak tabir edilen kripto çözücü sistemlerle deşifre edilebilir. Böyle bir risk hiçbir zaman gözardı edilemez. Bundan dolayı parola ve kripto güvenliğinin sağlanması için bazı kuralların

uygulanmasından hiçbir şekilde vazgeçilemez. Bu kuralları aşağıdaki gibi özetleyebiliriz.

Her kullanıcıya tahsis edilen bir kullanıcı ismi ve parolası mevcuttur. Bu bilgiler kişiye özel bir hassasiyettedir. Bütün kullanıcılar, kullanıcı kimliği ve parolasını saklamaktan, başkalarının eline geçmemesini sağlamaktan sorumludur. Başka birisinin kullanıcı adı ve parolayı elde ettiğinden şüphelenildiği her durumda bu bilgiler değiştirilmelidir.

Parolalar, en geç 6 ay içerisinde değiştirilmelidir. 6 ay aynı parolayı kullanmakta aşılmaması gereken süredir. Parola değişimi işletim sisteminin yönetici ayarlarından otomatik olarak yaptırılabilir.

Parola değişiminde ve seçiminde göz önüne alınması gereken kurallar da vardır. Öncelikle parola seçerken bilinen tarih, sicil numarası, ad soyad gibi kolaylıkla tahmin edilebilecek parolalar seçilmemelidir. Parola en az 8 karakterden oluşmalıdır. Harf, rakam ve özel karakterlerden oluşan bir kombinasyon kullanılmalıdır. Kullanılan son üç parola tekrar kullanılmamalıdır

Sisteme girişte parola yazarken her karakter arasında belli bir süre otomatik bekleme yapılmalıdır. Bunun gerekçesi, sistemi kaba kuvvet ataklarından (Brute Force Attacks) korumaktır. Normal bir insan her bir karakteri ortalama 0,5sn.'lik süre içerisinde girmektedir. Bir bilgisayar ağa taarruz ederse 1sn gibi bir sürede milyonlarca parola giriş denemesi yapabilir. Sistemin girişine bir bekleme zamanı konulursa, kaba kuvvet saldırıları büyük bir oranda önlenmiş olur.

1.7.5. Güvenlik Duvarlarının (Firewall) Kullanılması

Güvenlik duvarları işletmelerin ağ yapılarını, bilgilerini dışarıdan gelebilecek virüs, kurtçuk gibi zararlı verilere karşı korur. Aktarılan bilgilerin de güvenliğini sağlar. Kurum ağının dışarıya kapatılması elbette bir çözümdür. Ancak dışarıya açılmanın faydası göz önüne alındığında güvenlik duvarlarının kullanılması riski en aza indirir.

Ağdan dışarı çıkan ve içeri giren tüm verilerin güvenlik duvarı üzerinden geçmesini sağlamak genel olarak iki bileşeni içerir;

- Paket süzgeci, standart bir yönlendirici işlevlerinin yanı sıra, ölçütleri sağlayan paketlerin geçmesine izin veren, sağlamayanları ise durduran özelliklere sahiptir.

- Uygulama ağ geçidi (application gateway), uygulama katmanında çalışan ve yalnızca içeri giren veya dışarı çıkan ham paketi değil, bu paketlerin her birinin içeriğini de inceleyen bir ağ geçididir.[62]

Güvenlik duvarı içeriden dışarıya ve dışarıdan içeriye bütün geçişlerin kendi üzerinden yapılmasını sağlar. Bunun haricindeki bütün geçiş isteklerini fiziksel olarak engeller. Yerel güvenlik politikası gereğince sadece istenen trafiğin geçişine izin verir. Güvenliğin delinmesine karşı bir bağışıklık sistemi vardır. Elbette bu bağışıklık, güvenilir bir sistemin ve güvenli bir işletim sisteminin kullanılması ile doğru orantılıdır.[63]

Genel olarak güvenlik duvarlarının erişimi kontrol etmek ve güvenlik yönetim politikalarını uygulayabilmek için kullandıkları dört teknik vardır.

Servis kontrolü : Sistem içinden ve dışından erişilebilecek servisleri belirler. IP adresi ve TCP port numarasına göre trafiği süzer.

Yön kontrolü : Güvenlik duvarı üzerinden geçiş yapan kısmi servis taleplerinin yönlendirilmesini veya çalıştırılmasını kontrol eder.

Kullanıcı kontrolü : Hangi kullanıcının hangi servislere erişim sağlayacağını kontrol eder. Bu sayede belirli servislere yetkisiz kullanıcıların erişimi önlenerek bir güvenlik yapısı oluşturulur. Bu konuyla ilgili bilgiler erişim kontrolü bölümünde detaylandırılmıştır.

---

[62] Nazife BAYKAL, **a.g.e.**, s.342.

[63] William Stallings, **a.g.e.**, s.345.

Davranış kontrolü : Kısmi servislerin nasıl kullanılacağı ile ilgilidir. Örneğin güvenlik duvarı, e-posta kontrolü yaparak istenmeyen postaların geçişini engeller veya dışarıdan erişimde yerel bir Web sunucusu üzerindeki sadece belirli bilgilere erişimi kısıtlar.

Güvenlik duvarlarının güçlü güvenlik özelliklerinin yanı sıra, yetersiz kaldığı noktalar da vardır. Bilgi güvenlik personeli bu kısıtların farkında olmalıdır.

Güvenlik duvarı, duvarı bypass ederek yapılan güvenlik saldırılarına karşı etkisizdir. Örneğin, ağ sistemi dışarıdan numara çevirerek yapılan bir modem bağlantısına izin verebilir. Böyle bir sisteme seyahatte olan personelin ağa erişimini temin etmek için izin verilmiş olabilir. Bu durum ise sistemi dışarıdan yapılan saldırılara karşı korumasız bırakabilir.

Diğer bir nokta, güvenlik duvarı, dahili tehditlere karşı koruma sağlamaz. Dışardan bir saldırganla işbirliği yapan bir personel güvenlik duvarının aşılmasını sağlayabilir. Bunun yanında güvenlik duvarı dışarıdan veya içeriden sisteme bulaştırılan enfekte dosyaları, virüsleri %100 şekilde inceleme altında tutamaz.[64] Bunun için ilave bir anti virüs yazılımına ihtiyaç duyulmaktadır.

Güvenlik duvarı kullanımında dikkat edilmesi gereken en önemli nokta belki de ayarlarının uygun bir şekilde yapılmasıdır. Aksi taktirde koruma kabiliyeti yüksek ve oldukça etkin bir güvenlik duvarı, hatalı yapılandırmadan dolayı etkisiz bir kalkan haline dönebilir. Ayarların yapılabilmesi için sistem bilgi güvenliği konularına hakim personel istihdam edilmelidir.

1.7.6. Antivirüs Yazılımlarının Kullanılması

Antivirüs yazılımları kişisel bilgisayarları veya bilgisayar ağlarını virüs, kurtçuk, truva atları ve mantık bombaları gibi zararlı yazılımlara karşı koruyan algoritmalardır. Bilgi güvenliği açısından çok özel bir yere sahiptirler.

---

[64] William Stallings, **a.g.e.**, s.346.

Bütün virüs veya benzeri yazılımları %100 yakalayarak tesirsiz hale getirebilen bir yazılım şu ana kadar üretilmemiştir. Bununla birlikte antivirüs yazılımları oldukça başarılı olarak çalışmaktadırlar. İşletmeler için antivirüs yazılımlarının maliyeti artık neredeyse kaçınılmaz bir maliyet halini almıştır.

Antivirüsler temelde üç işlevi yerine getirirler;

Tespit : Virüs enfeksiyonu söz konusu olduğunda, program tarafından olayın gerçekleştiği teyit edilir ve virüsün konumu belirlenir.

Teşhis : Tespit işleminin akabinde virüsün ne olduğu ortaya konur.

Temizleme : Son aşama ise virüsün izleri ve sistemde yaptığı değişiklikler takip edilerek dosyalar orijinal konumuna geri getirilir.[65]

Antivirüsler bu işlemleri yaparken genellikle bünyelerinde bulunan virüs veritabanını kullanırlar. Tespit olayında ifade edildiği gibi sistem ayarlarını değiştirmeye çalışan bir program virüs davranışları gösterirse antivirüs yazılım tarfından bloke edilir. Daha sonra bloke edilmiş programın yapmak istedikleri veri tabanından kontrol edilir. Benzer davranışları tespit edilirse, antivirüs programı virüs bulunduğu alarmını verir.

Antivirüs programlarının kullandığı başka bir tarama yöntemi de sezgisel (heuristic) tarama yöntemidir. Bu yöntemi kullanan programların bünyesinde virüs davranışlarının kalıpları bulunur. Mevcut davranış kalıplarıyla virüs davranış kalıpları karşılaştırılır. Veri tabanında virüsün özellikleri tanımlanmamış olsa bile, davranışın karakteristiklerine bakarak kullanıcı ikaz edilir. Bu durum zaman zaman yanlış alarmlara sebebiyet verebilir. Örneğin, hard diskin formatlanmak istendiği tespit edilirse, uygulama derhal bloke edilerek kullanıcı bir mesaj ile uyarılır.bu duruma antivirüs programı, kullanıcının kendi isteği ile yapılan formatlama işlemini de bir virüs eylemi olarak değerlendirebilecektir.

---

[65] William Stallings, **a.g.e.,** s.336.

Yapılan bir araştırmada dünyada günde ortalama 15 virüsün ortaya çıktığı tahmin edilmektedir.[66] Bu durum virüs güncellemelerinin çok yakından takip edilmesini gerektirmektedir. Birçok antivirüs yazılımı güncellemelerini online olarak internet üzerinden sağlamaktadır. İşletmenin ağ güvenliği sorumlularının öncelikli görevlerinden birisi, virüs güncellemelerini sürekli takip ederek, ağı virüs saldırılarına karşı bağışık durumda bulundurmaktır.

Son nesil virüse karşı koruma yazılımları, e-postaları kontrol etme, spam filtreleme gibi güncel ihtiyaçlara cevap verecek tarzda üretilmektedir. Birçok yazılım, güvenlik duvarı yazılımları ile entegre olarak piyasaya sunulmaktadır. Bu yazılımlar aynı zamanda Explorer, Outlook gibi yaygın olarak kullanılan yazılımlarla entegre olabilmekte ve sistemi bir bütün olarak güvenlik şemsiyesi altına almaktadır.

Tüm çabalara rağmen sisteme virüs bulaşması durumunda ise yapılacak en doğru hareket, uygulamaları en kısa yoldan sonlandırarak sistemi kapatmak ve güvenli bir açılış disketi veya CD'si ile birlikte yeniden başlatmaktır. Daha sonra sistem, disket veya CD üzerindeki antivirüs yazılım ile temizlenebilir.

1.7.7. Bilginin Yedeklenmesi (Backup)

Birçok işletme için bilgilerinin kaybolması bir felakettir. Bilgi kaybı birçok sebepten kaynaklanabilir. Bir donanım hatası sonucu bilgi depolama ünitelerinin, işletim sisteminin çökmesi, virüs, kurtçuk veya dışarıdan yapılan saldırılar sonucunda sistemin anormalleşmesi olabilecek olaylardan sadece bir kaçıdır. Bu örnekler çoğaltılabilir. Bilgi kaybı, sitemdeki bilgiler periyodik olarak yedekleniyorsa büyük ölçüde önlenebilir. En azından kayıp minimum seviyede tutulabilir.

Bilginin yedeklenmesi ile ilgili olarak iki tip yöntemden söz etmek mümkündür. Tüm sistemin yedeğinin alınması (full backup), diğeri de değişikliklerin yedeklenmesidir (incremental backup). Tüm sistemin yedeğinin alınması yoğun bilgi

---

[66] **"PC'niz İçin Koruma Aşısı"**, Chip Dergisi, Haziran 2003, s.10.

akışının olduğu sistemlerde çok zaman almaktadır. Sadece sistemdeki değişikliklerin kaydedildiği değişiklik yedeklemesi daha kısa sürmekle birlikte daha az güvenlidir. Değişikliklerin yedeklenmesinde, sistemin istikrarlı bir şekilde çalışması çok önemlidir. Yedeklenen değişikliklerin kaybolması, bozulması gibi durumlar istenmeyen bilgi kaybına yol açar. Yedekleme ile ilgili yöntem seçiminde, tüm sistemin yedeklenmesi ile değişikliklerin yedeklenmesinin bir kombinasyonu düşünülebilir. Tercih konusundaki etkenler, işletmenin yapısına, işlenen bilginin türüne, sistemin kuruluşuna göre değişim göstermektedir.

Bilgi yedeklemesinde bir başka konu, bilgilerin ne kadar sıklıkla yedekleneceği ve ne kadar bir süre saklanacağıdır. Bu sorunun cevabını da işletmenin yapısı ve konumu belirlemektedir. Burada şunu söylemek mümkündür; bilgiler ne kadar sıklıkla yedeklenebiliyorsa o kadar iyidir. Haftada bir tüm sistemin yedeklenmesi ve günlük olarak değişikliklerin yedeklenmesi normal yapıda bir işletme için yeterli olabilecektir. Bununla birlikte kesin bir sürenin dikte edilmesi mümkün değildir. Bu süre işletmenin bilgi güvenlik politikası doğrultusunda tespit edilecektir.[67]

Bilgi yedeklemesi ile ilgili olarak kullanılan üniteler ise veri yoğunluğuna ve maliyete göre değişmektedir. En yaygın olarak kullanılan sistemler teyp yedekleme üniteleridir. Ortalama 40 – 80 Gb.'lık bir kapasiteye sahip olan bu üniteler, yedekleme konusunda oldukça kullanışlıdır. Bunun yanı sıra CD/DVD gibi yazılabilir medyalar da yedekleme ünitesi olarak kullanılabilir. CD/DVD gibi medyalar, kapasite olarak daha kısıtlıdır. Bu medyalara ilave olarak bazı sistemlerde Hard disk üniteleri de yedekleme ünitesi olarak kullanılabilmektedir.

Herhangi bir sistem çökmesi durumunda yedeklenen bilgiler yeniden sisteme sokulabilmektedir. Bu tip yedeklemede açıkça görüldüğü gibi, o anda işlem gören veya yedeklemeden sonra işleme tabi tutulan bilgilerin kaybı söz konusudur. Bu kaybın önüne geçmek için ise farklı yöntemler geliştirilmiştir. Örneğin çoklu sunucu

---

[67] **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part V Chapter11, s.13.

yapısına sahip bir sistemde, sunucular anlık olarak birbirlerini yedekleyebilmektedir. Bu ise sisteme büyük bir esneklik sağlamaktadır.

1.7.8. Çıktıların İmhası

"Bilgi kaçış noktaları" konusunda da işlendiği gibi, yazıcılar kesinlikle kontrol altında tutulması gereken noktalardandır. Bu yüzden yazıcılar titizlikle yerleştirilmelidir. Yazıcılardan alınan, fotokopi suretiyle çoğaltılan veya sair surette elde edilen basılı dokümanların saklanması belli kurallara tabi olmalıdır. Burada etkin olabilecek bir unsur, basılı her dokümanın bir gizlilik derecesi almasıdır. Doküman, aldığı gizlilik derecesine göre işleme tabi tutulur.

Dokümanların uygun şekilde muhafazasının yanında dikkat edilmesi gereken diğer bir başka nokta, basılı dokümanların imhasıdır. Gizlilik derecesine dikkat edilmeden çöpe atılan bir materyal [68], art niyetli insanlarca sisteme girmekte kullanılan veya kolaylıkla suiistimal edilebilecek bilgiler içerir. Bu nedenle iyi bir güvenlik anlayışına sahip işletmelerde gizlilik dereceli materyaller ile tasnif dışı materyal ayrı şartlarda imha edilir. Tasnif dışı materyaller, işletme ve sistemle ilgili olarak, başkalarının eline geçmesi durumunda bir tehlike veya güvenlik zafiyeti oluşturmayacak materyallerdir. Bunların doğrudan çöpe atılmasında herhangi bir mahzur yoktur. Gizlilik dereceli materyaller ise ele geçirilmeleri durumunda işletmeye zarar verebilecek bilgiler içerirler. Bu şekilde tasnif edilen materyaller özel şekillerde imha edilirler. Uygulanan en yaygın usul, işletme içinde belirli noktalara konulan kağıt kırpma makinelerinin kullanılmasıdır. Kağıt haricindeki malzemeler ise parçalanarak ve yakılarak imha edilir.[69] Eski bir usul olmakla birlikte birçok yerde geçerliliğini sürdüren başka bir yöntem de yakma fırınlarının kullanılmasıdır. Toplama noktalarında toplanan

---

[68] Materyal terim olarak, basılı, yazılı, çizili doküman, belge, CD/DVD/disket veya diğer ortamlarda bilgi içeren her türlü malzemeyi tanımlamaktadır.

[69] **ACE Security Directive AD 70-1,** SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, 1 January 1997 Part II Chapter1, s.19.

malzeme ve dokümanlar, belirli bir gün ve saatte bu fırınlarda yakılırlar. İmha işlemi yetkili kişiler tarafından yapılır ve imha tutanağı ile kayıt altına alınır.

1.7.9. Bilgi Güvenliğinde Personelin Konumu

Ağ güvenliğinde, sadece dışarıdan gelebilecek tehditlere karşı önlem almak yeterli değildir. İşletme içinden kaynaklanabilecek tehlikeler de bir o kadar önemlidir.[70] Bu kapsamdaki en yüksek riski personelin kendisi oluşturmaktadır. Bütün sistemler içeriden gelebilecek tehlikeler karşı daha zayıftırlar. İşletmeler için en etkili tedbir güvenilir personel çalıştırmaktır. Bunun yanında hatalardan kaynaklanabilecek riski en alt seviyeye indirmek için işletme içi ve dışı eğitim ve bilgilendirme çalışmaları yapılmalıdır.

Dokümanların gizlilik derecelerine göre tasnif edilmesi gibi, personel de aynı mantıkla tasnif edilir. Güvenlik kleransı (security clearance) vermek suretiyle, hangi personelin hangi gizlilik derecesine kadar nüfuz edebileceği belirlenir. Böylece herkes yetkisi derecesinde uygun bilgiye işlem yapabilir. Bu özellik, belirli bir güvenlik kleransına sahip şahsın o derecedeki bütün dokümanları görebileceği veya aynı gizlilik derecesindeki bütün bilgiye işlem yapabileceği anlamına gelmez. Personel, kendi sorumluluk sahasındaki bilgilerden gizlilik derecesinin müsaade ettiği kadarına ulaşabilir.

Güvenlik kleransları verilirken personel belirli bir süre denenir. Personel kleranslarında, kripto kleransı çok özel bir konuma sahiptir. Ağda kullanılan kripto, sadece kripto personeli tarafından işlem görür. Güvenlik anlamında genellikle uygulanan bir yöntem ise tek kişiye dayanan bir yapılanmadan uzak durmaktır. "İki kişi kuralı" olarak adlandırılan bu yöntemde kripto iki kişinin sorumluluğundadır ve tek personel bütün kripto bilgisine nüfuz edemez. Her kasanın iki adet üç kombineli kilidi

---

[70] Mark B. Desman "Building an Information Security Awareness Program" Boca Raton, FL: CRC Press LLC., **Journal of Government Information,** 2002, s.2.

vardır. Her bir kripto personeli sadece birinin şifresini bilmektedir. Böyle bir yapı işletme için daha güvenli bir ortam oluşturur.

İKİNCİ BÖLÜM

BİLGİ GÜVENLİĞİ VE YÖNETİMİ

2.1. İŞLETMELERDE BİLGİ GÜVENLİĞİ YÖNETİMİNİN ÖNEMİ

Çalışmada öncelikle "Bilgi Güvenliği"nin teknik boyutu ortaya konmaya çalışılmıştır. Gelişen teknoloji ve bilgi çağının gereksinimleri ile birlikte bilginin sayısal ortama taşınması, işletmelerin karşı karşıya oldukları risklerin boyutunu da değiştirmiştir. Bu değişim işletmeler açısından, hem teknik bilgisi kuvvetli, hem de yönetim unsurlarına vakıf personelin istihdamını zorunlu kılmaktadır.[71] "Bilgi Güvenliği", profesyonel bir şekilde ele alınmadığı taktirde işletme için bir sorun olmaya devam edecektir.

Bu bağlamda, sayısal ortamın teknik konularının yönetim unsurlarıyla nasıl bir uyum içerisinde çalıştırılacağı, yönetim kademelerinde hangi konuların göz önüne alınması gerektiği ortaya konulmalıdır.

İşletmelerde bilgi güvenliğinin önemi aslında çok yeni bir kavram değildir. İşletmelerin tarihteki yeri kadar eskidir. Günlük hayatta sık sık kullandığımız "meslek sırrı" tabiri de bunun bir sonucu olarak kullanılmaktadır. Yalnız, bilgi güvenliği, bilgi çağına giriş ve bilginin sayısal ortama taşınması ile birlikte yapısını ve şeklini değiştirmiştir.

Bilgi güvenliği yönetiminin önemini daha iyi açıklayabilmek için öncelikle bilgi toplumuna geçiş sürecini ve dünya elektronik ticaret hacmini ana hatlarıyla tanımlamak daha uygun olacaktır.

---

[71] İsmet Barutçugil, **Bilgi Yönetimi,** Kariyer Yayıncılık İletişim, Eğitim Hiz. Ltd. Şti., İstanbul, Nisan 2002, s.46.

2.1.1. Bilgi Toplumuna Geçiş

19ncu yüzyıldan 20nci yüzyıla geçerken, gelişmiş tarım toplumlarının üzerine, sanayi toplumlarının kurulmuş olduğu bilinmektedir. Benzer bir şekilde, 20nci yüzyıldan 21nci yüzyıla geçişte de bilgi toplumlarının, olgunlaşmış sanayi toplumlarının üzerine inşa edilmekte olduğu işlenmektedir. 19ncu yüzyılda tarım sektöründeki devrim, makinenin gelişmesi ve enerjinin etkin kullanımı ile olmuş; bilgi toplumuna geçişte de, sanayileşme sürecindeki elektro-mekanik ve elektronik teknolojilerindeki gelişmelerden ivme kazanmıştır.[72]

Bu gelişmenin bir sonucu olarak işletmeler, yeni teknolojileri kullanmaya başlamış ve örgüt yapıları da değişime uğramıştır. Örgüt yapılarının değişimi, yeni büyüme olanakları yaratmakta ve pazar yapıları buna bağlı olarak değişim geçirmektedir. Bilişim ve iletişim teknolojilerinin gelişmesi ve ağ yeterliliklerinin oluşturulması, büyüklü küçüklü tüm işletmeler için, daha az maliyetle, daha kolay ve esnek bir biçimde iş yapma olanağı yaratmaktadır.[73]

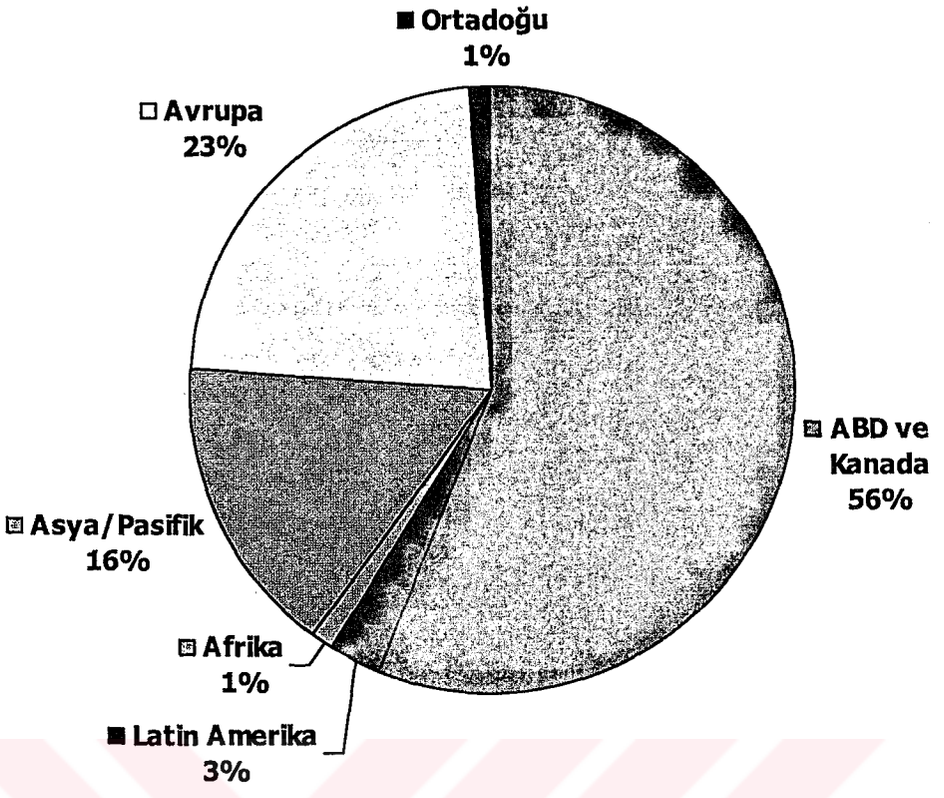
2.1.2. Elektronik Ticaret

Elektronik Ticaret, bilgi çağının en önemli oluşumudur. Bilgi teknolojilerinin bu kadar hızla gelişmesinin ve dünyanın her yerinde kullanılıyor olmasının en başta gelen sebeplerinden biri, internet üzerinden e-ticaret imkanının doğmasıdır.

---

[72] Eyüp İlyasoğlu, **Türk Bilgi Teknolojisi ve Gümrük Birliği,** Türkiye İş Bankası Kültür Yayınları, Temmuz 1997, s.59.

[73] Yakup Kepenek, **Ekonomik Yönleriyle Elektronik Ticaret,** Derleyen: Veysel Bozkurt, **Elektronik Ticaret,** Alfa Yayınları, Mayıs 2000, s.37.



Grafik 2.1 : Mayıs 1999'da internet erişimine sahip insan sayısı

KAYNAK : Sacit ERTAŞ, **Elektronik Ticaret: Tanımı, Gelişimi, Avantajları,** Güvenliği, Uludağ Üniversitesi İktisadi ve İdari Bilimler Fakultesi, Ekonometri Bölümü, Alıntı Yapılan Kaynak: http://www.nua.ie/surveys, Derleyen: Veysel Bozkurt, Elektronik Ticaret, Alfa Yayınları, Mayıs 2000, s.6

Bir internet araştırma firmasına göre Mayıs 1999'da dünyada 171 milyon insan internet erişimine sahiptir. Aşağıdaki tablodan da görüldüğü gibi internet erişimi en yüksek iki ülke ABD ve Kanada'dır. Veriler incelendiğinde, ABD, Kanada, İskandinav ülkeleri ve Avustralya'da nüfusa göre internet erişim oranlarının İngiltere, Almanya, Japonya ve Fransa'nın iki katı olduğu görülmektedir.[74] Bu tablo, internetin ne kadar hızlı bir şekilde gelişerek milyonlarca eve girdiğini çarpıcı bir şekilde göstermektedir. Görüldüğü gibi bu gelişimde de ABD ve Kanada dünyada baş rolü oynamaktadır.

---

[74] Maryan Jones Thompson, "My How We've Grown", **The Industry Standard,** April 26, 1999, (http://www.thestandart.com).

İnternet, birçok farklı amaca hizmet etmekle birlikte, özellikle ticaret anlamında çok uygun bir ortam oluşturmaktadır. Teknolojik değişim, bilgisayarların güçlenmesi, ağ bağlantılarının gelişmesi, ticareti çok daha kolay ve hızlı bir konuma getirmiştir. E-ticarettin iki kategorisi bu anlamda büyük bir gelişme göstermiştir. Bu kategorileri, firmadan firmaya ticaret ve firmadan tüketiciye ticaret olarak tanımlayabiliriz.[75]

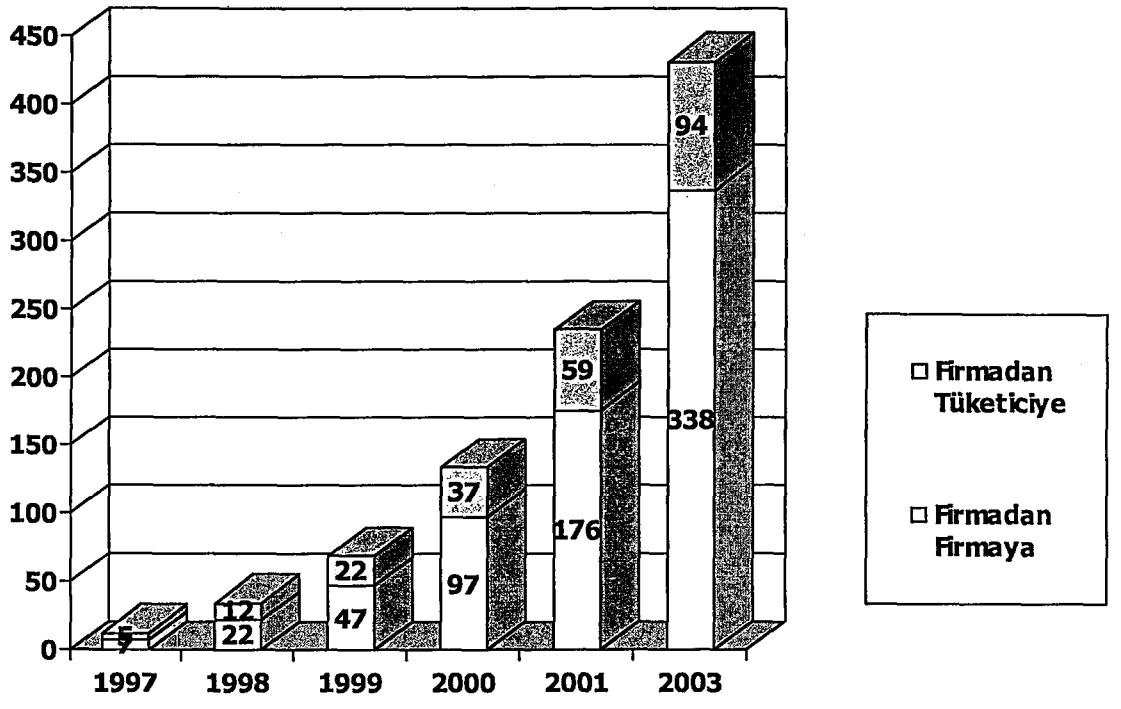
Dünyada ticaret hacmi yılda %69 büyümektedir. OECD ve IDC gibi kuruluşlara göre, 1997 yılında 11 milyar dolar olarak gerçekleşen elektronik ticaret hacmi, 2003 yılında 400 milyarı aşmış ve 2005 yılında da 1 trilyon doları bulacağı hesaplanmaktadır. Aşağıdaki tabloda bu veriler görülmektedir.

Tablo 2.1 : Elektronik Ticaret - İnternet Temelli Satışlarda Büyüme

Yıllar	Firmadan Firmaya (milyar $)	Firmadan Tüketiciye (milyar $)
1997	7	5
1998	22	12
1999	47	22
2000	97	37
2001	176	59
2003	338	94

KAYNAK : Veysel Bozkurt, **Bilgi ve Toplum, Elektronik Ticaretin Ekonomik ve Toplumsal Boyutu,** Alfa Yayınları, 1999/2

[75] Khalid S. Soliman, Brian D. Janz, "An exploratory study to identify the critical factors affecting the decision to establish Internet-based interorganizational information systems" **Information Management Journal,** Vol.41, Issue 6, USA, 25 June 2003, s.698.



Grafik 2.2 : Elektronik Ticaret - İnternet Temelli Satışların Gelişimi (milyar $)

KAYNAK : Veysel BOZKURT, Elektronik Ticaretin Ekonomik ve Toplumsal Boyutu, **Bilgi ve Toplum,** 1999/2 Uludağ Üniversitesi, Bursa.

Yukarıdaki şekilde e-ticaret hacmindeki büyüme açıkça görülmektedir. Bu durum, internet üzerinden elde edilen geliri ve bu alana yapılan yatırımı da paralelinde getirmektedir. Bu durum işletmelerin yatırım ve ticaretlerini her geçen gün artan bir oranda internet ortamına taşımak için çok cazip avantajlar sağlamaktadır. İşletmeler internet ortamına geçerken, internetin potansiyel tehditlerine maruz kalmaktadırlar. açık bir konuma gelmektedirler.[76] Bu yüzden bilgi güvenliğinin önemi her geçen gün artmaktadır.

---

[76] Internet temelli satışların gelişimi, **IDC,** 1998. http://www.pwcglobal.com/gx/eng/ins-sol/spec-int/knapp-05.htm.

2.1.3. Elektronik Ticareti Olumsuz Etkileyen Faktörler

Birçok avantajı ile birlikte çok cazip bir pazar haline gelen elektronik ticareti etkileyen olumsuz faktörler de vardır. Yapılan bir araştırmaya göre tespit edilen olumsuz etkenlerin oranları aşağıdaki tabloda görülmektedir.

Tablo 2.2 : Elektronik Ticareti Olumsuz Etkileyen Faktörler

Elektronik Ticareti Engelleyen Unsurlar	Oran (%)
Korsan Korkusu	21
Ürün Azlığı	16
Ürünü Görememek	15
Kişisel Bilgi Verme Zorunluluğu	13
Kötü Hazırlanmış Web Sitesi	8
Şirketin Adı	6
Ürünün ve Paranın Kaybolma Korkusu	6

KAYNAK : **"Hipermarketinizi Çöpe Atın"**, Milliyet Gazetesi, 29.07.1999

Tablo incelendiğinde, korsan korkusu, kişisel bilgi verme zorunluluğu ve ürünün ve paranın kaybolma korkusu doğrudan bilgi güvenliği ile ilgilidir ve toplam oranın %40'ını oluşturmaktadır.

Diğer yandan binlerce benzer ürünün ve firmanın bulunabileceği ortamda farklılık yaratarak internet kullanıcılarının internet sitesine uğramasını sağlamak oldukça zordur ve bu konudaki sıkıntıyı gidermek için işletmelerin sitelerini tanıtmaları önem kazanmaktadır. Bu yönde gerçekleştirilen tanıtım ve reklam faaliyetlerinin yatırım tutarları elektronik ticareti olumsuz yönde etkileyen diğer bir faktördür.[77]

2.1.4. Bilgi Güvenliği Yönetimi Gereksinimi

İnternet ortamında faaliyet göstermek birçok riski beraberinde taşımaktadır. Bu riskler daha önceki bölümlerde detaylı olarak açıklanmıştır. İşletmeler için kar ve büyüme amaçlı olarak düşünülen internet ortamı, yeterli güvenlik çözümleri

---

[77] Ahmet Araşan, İnternette Ticaret, **Hürriyet Gazetesi,** Finans'99 Eki, 24 Kasım 1999, s.13.

oluşturulmadığı taktirde, büyük bilgi kayıplarına yol açmakta ve dolayısıyla çok büyük zararlara sebebiyet vermektedir.

Bilgi kaybının maliyeti sadece internet ortamından kaynaklanmamakla birlikte, internetin risk potansiyeli de oldukça yüksektir. 1996 yılında Timothy Lloyd'un Omega mühendislikten ayrılırken yazdığı 6 satırlık bir kod ile 10 – 12 milyon dolarlık bir zarara sebep olması bilgi kaybı maliyetinin boyutlarını vurgulamak için iyi bir örnektir.[78]

Bu anlamda oluşturulacak güvenlik çözümleri, tamamen profesyonel bir yaklaşımla ele alınmalıdır. Bu amaçla oluşturulacak organizasyon yapısı, departmanlar, dış kaynak kullanımı gibi konular ilerleyen bölümlerde açıklanacaktır.

2.2. GÜVENLİK POLİTİKASI

Bilişim Teknolojilerinin uygulanmasındaki en kritik unsurlardan bir tanesi "Güvenlik Politikası'nın oluşturulmasıdır. Güvenlik politikası uyulacak kuralları, prosedürleri tanımlar. Hangi personelin hangi kaynaklara, veri tabanına veya gizlilik dereceli diğer bilgilere ne şekilde erişim sağlayacağı güvenlik politikası ile belirlenir.[79] Genel bir ifade ile güvenlik politikası, işletmede uygulanan ve uygulanması arzu edilen tüm güvenlik unsurlarının, hareket tarzlarının, güvenlik tanımlarının ve yetkilerinin yazılı hale getirilmiş bir ifadesidir.[80]

Bu çerçevede güvenlik politikası bileşenlerini;

- Kapsam
- Dokümantasyon
- Yayım

---

[78] "Hacker Avında Son Perde", **CHIP Dergisi,** 6/2003 s.22.

[79] Alistair Donaldson & Phil Walker, "Information governance—a view from the NHS" **International Journal of Medical Informatics,** 2003, s.282.

[80] Jack G. Albright, The Basics of an IT Security Policy, March 2002.

- İdame
- Uygulanabilirlik

başlıkları altında toplamak mümkündür.[81]

2.2.1. Kapsam

Güvenlik politikasının kapsamının ne olacağı, işletmenin büyüklüğüne, faaliyet gösterdiği sektöre, kullanılan teknolojiye ve gelirine göre değişim göstermektedir. Dikkate alınması gereken nokta, teknolojik değişime uyum sağlayabilecek, esnek bir yapıda olması gerektiğidir.[82]

Öncelikle işletmenin güvenlik vizyonu iyi tanımlanmış, açık bir şekilde ifade edilmiş olmalıdır. Örneğin;

"Güvenlik politikası, bilişim unsurlarının etkin kullanımı doğrultusunda veri ve kaynak güvenliğini sağlayarak, işletmenin güvenirlik ve bütünlüğünü temin etmeyi amaçlar..."

ifadesi genel bir şekilde işletmenin bilgi güvenliği vizyonunu tanımlamaktadır. Bu vizyon doğrultusunda diğer güvenlik tanımları daha detaylı bir biçimde yapılmaktadır.

Güvenlik Politikası, izlenecek prosedürleri kapsar. İşletmeye hangi cihazların getirileceği ve getirilmeyeceği bu prosedürler kapsamında değerlendirilir. Örneğin, işletmenin yapısına göre, kişisel cep bilgisayarlarının, dizüstü bilgisayarların getirilmesinin güvenlik açısından uygun olmayacağı değerlendirilebilir. Sayısal fotoğraf makinelerinin, cep telefonlarının yasaklanması gerekli görülebilir. Bu prosedürler,

---

[81] Eduardo Gelbstein, **Managing Informatin Security,** International Computing Centre, OECD, April 2001, s.11.

[82] Mark B. Desman "Building an Information Security Awareness Program" Boca Raton, FL: CRC Press LLC., **Journal of Government Information,** 2002, s.2.

güvenlik politikasının bir parçası olarak belirlenir. Aynı şekilde bir güvenlik ihlali olduğunda veya uygulamada yanlışlık yapıldığı taktirde ne şekilde bir işlem uygulanacağı bu prosedürler dahilinde telakki edilir.

Görev ve pozisyon tanımlarının yapılması, güvenlik politikasının önemli bir bölümünü oluşturur. Herkesin ilgileneceği konular açıkça ifade edilir. Burada, kullanıcıların bilgisayar kaynaklarına erişim hakları da tanımlanabilir.

Oluşturulan güvenlik profilleri ve bunların tanımı, güvenlik politikası içinde yer alır. İş istasyonlarında, sunucularda, kullanılan diğer ağ bileşenlerinde yapılacak rutin işler standart hale getirilir. Bu kapsamda uygulanan en yaygın yöntem güvenlik çeklist'lerinin kullanılmasıdır.[83] Çeklistler, standardizasyon ve uygulamanın yeknesaklığında önemli bir araçtır.

Düzenli ve düzenli olmayan güvenlik kontrolleri, takip edilen politikanın başarısını ortaya koyar. Kontroller sonucunda ortaya çıkan sonuçlar, güvenlik performansının değerlendirilmesinde de kullanılır. Güvenlik politikasının oluşturulmasında kullanılan fonksiyonlar, işletmenin yapısına göre artırılabilir.

2.2.2. Dokümantasyon

Dokümantasyon, "Güvenlik Politikası" kapsamına giren tüm unsurların yazılı olarak ifade edilmesini tanımlar. Politika ve kurallar yazılı hale getirildiklerinde uygulamaların ve görev tanımlarının standartlaştırılmasında etkili olurlar. Dokümantasyon, işletmeye kalıcılık ve görevi idame kabiliyeti kazandırır. Yönerge, yönetmelik türündeki dokümanlar, kullanılan form, çizelge, çeklist gibi basılı materyaller bu kapsamda mütalaa edilir.

Kuralların bu surette yazılı hale getirilmesi, personel moral ve motivasyonu için de önemlidir. Herkesin yaptığı ve yapacağı iş belirlidir. Belirsiz durumlar en aza indirilmiştir. Bu durum işletmeye duyulan güveni ve iş performansını artırıcı bir rol

---

[83] Jack G. Albright, **a.g.e.**, s.5.

oynar. Dokümantasyonun işletmeler için oluşturabileceği bir dezavantajdan söz etmek de mümkündür. Bu, dokümanların oluşturulmasında ve güncelliğinin sağlanmasında ilave personel kullanılmasının gerekli olabileceğidir. İlave personel istihdamı ise işletme için ilave maliyet anlamına gelmektedir. Bu kapsamdaki diğer bir unsur ise bürokrasidir. Uygulama değişikliklerinin, teknolojik gelişmelerin yazılı ve basılı hale getirilmesi, güvenlik politikasına adapte edilmesi süreci, belirli bir bürokratik gecikmeye maruz kalacaktır.

2.2.3. Yayım

Yazılı ve basılı hale getirilen dokümanların işletme içine, alt kuruluşlara veya işbirliği içinde bulunulan diğer kurum ve kuruluşlara gönderilmesini ifade etmektedir. Dokümanların yayımında dikkat edilmesi gereken en önemli nokta, istihbaratın da en önemli prensiplerinden olan *"Bilmesi Gereken Prensibi"*dir. Bu prensip, bilmesi gereken kişiye, bilmesi gerektiği kadar bilgi verilmesi esasına dayanır. Yani güvenlik kapsamında hazırlanan bir dokümanı gönderirken, gitmesine gerek olup olmadığı veya uygun olup olmadığı sorgulanmalıdır. Aksi taktirde yayım konusu kendi başına güvenlik ihlallerine yol açabilecek bir hareket tarzı olabilir.

2.2.4. İdame

İşletmenin güvenlik politikalarının uygulanmasında bir süreklilik olmalıdır. Bu sürekliliğin sağlanmasında aslında işletmede çalışan tüm birimler sorumludur. Üst yönetim kademesi de güvenlik politikalarının takibinde istekli olmalıdır. Politikaların idamesinde belki de en belirleyici etkenin personelin görevine bağlılığı olduğunu söyleyebiliriz. Uygulamaların personel tarafından benimsenmesi, güvenlik politikalarının başarıya ulaşmasında önemli bir rol oynayacaktır.

Güvenlik politikalarının idamesi ile ilgili sorumlu bir bölümün bulunması da gerekli olan diğer bir konudur. Bilgi güvenlik personeli, politikaların idamesinden doğrudan sorumludur. Üst yönetimin bilgi güvenlik personelini güvenlik politikalarının uygulanması konusunda desteklemesi ise çok önemlidir. Güvenlik politikaları bazı

durumlarda işletme içinde bir zorlama durumu oluşturabilir. Güvenlik kontrolleri genellikle personel tarafından çok hoş karşılanmayan bir durumdur. Bu kontroller, personel arasında, özlük haklarına, kişisel bilgi veya malzemelerine bir müdahale gibi algılanabilir. Kontroller esnasındaki bu zorlama eğilimi, üst yönetim tarafından doğrudan destek görmelidir. Personel, yapılan kontrol ve denetlemelerin gerekliliği, güvenlik personeline yardımcı olmaları konusunda bilgilendirilmeli ve ikna edilmeye çalışılmalıdır. Aksi taktirde, personel ile güvenlik arasında, tartışmaların yaşanması, sözlü ve fiziki çatışmalar, sıklıkla karşılaşılan bir problem olarak karşımıza çıkacaktır. Bu problem kendi haline bırakıldığında da, örgüt içi huzursuzluklar, yerli yersiz polemikler görülecek, gerginlik artacaktır. Doğal bir sonuç olarak da performans kaybı, işletmeye güvensizlik gibi istenmeyen durumlarla karşılaşılabilecektir.

2.2.5. Uygulanabilirlik

Uygulanabilirlik, güvenlik politikalarının kapsamı oluşturulurken başlayan ve devam eden bir konudur. Politikaların uygulanabilir olması zorunludur. Aksi taktirde bir anlam ifade etmez. Uygulanmaması durumunda ise güvenlik personelinin ve yönetici kesimin fevri davranışları ortaya çıkabilir. Sorunun önlenmesinin en iyi yolu işletme içinde yeniden değerlendirmelerin yapılmasıdır. Yeniden değerlendirme sonuçları, uygulanabilir konseptler halinde sisteme entegre edilmelidir.

Uygulanabilirlik, güvenlik politikasının bir başarı göstergesidir.[84] Eğer hazırlanan kurallar ve yöntemler başarıyla uygulanabiliyorsa, izlenen politika da başarılıdır. Başarıyla uygulanamıyorsa veya uygulanması için fazladan iş/saat, personel istihdamı, kırtasiyecilik, maliyet gibi gereksinimler oluşuyorsa, *"işletmenin bir güvenlik politikası var..."* tarzındaki ibareler gerçek anlamda bir değer içermeyecektir. Özetle, Güvenlik Politikası, uygulanabiliyorsa "Güvenlik Politikası"dır.

---

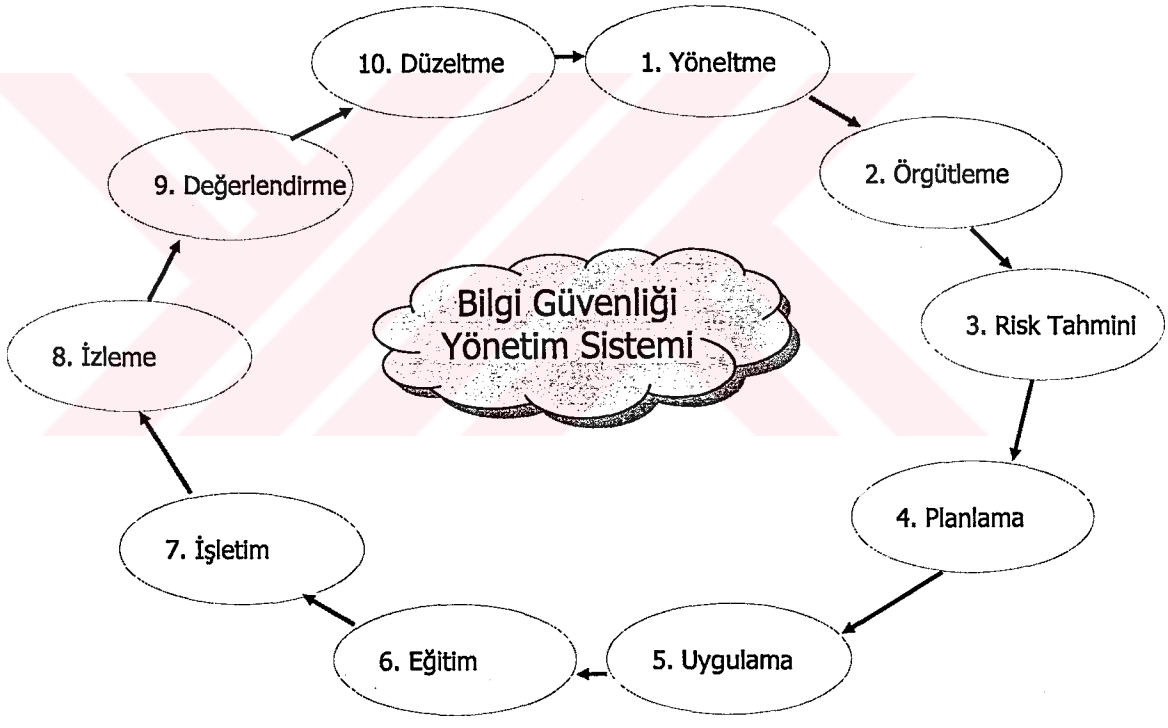
[84] Eduardo Gelbstein, **a.g.e.**, s.11.

2.3. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN FONKSİYONLARI

"Güvenlik", aslında gerçek hayatta olmayan bir kavramdır. Soyuttur. Kendimizi ve sahip olduğumuz varlıkları koruma çalışmalarını ifade eder. İşletmelerde, güvenlik ve bilgi güvenliği kavramlarının iç içe bir yapı oluşturduğunu ve kesin çizgilerle birbirinden ayırmanın mümkün olmadığını daha önceki bölümlerde açıklamıştık.

Bu bölümde "Bilgi Güvenliği Yönetimi"nin yönetim süreci içerisindeki fonksiyonları açıklanmaya çalışılacaktır.

Aşağıdaki şekil Bilgi Güvenliği Yönetiminin çevrimini ifade etmektedir.



Şekil 2.10 : Bilgi Güvenliği Yönetim Sistemi Çevrimi

KAYNAK : Rhein Hansen, **The Elements of a Security Management System,** IT University of Copenhagen, s.3.

Bilgi Güvenliği Yönetim sisteminin işletmelerde kurulması ve işletilmesi günümüzde zaruri hale gelmiştir. Güvenlik faaliyetlerinin yürütülmesinde, hangi seviyede bir güvenlik yapısına sahip olunması gerektiğine karar verilmesinde bilgi yönetim sisteminin yukarıdaki şekilde gösterilen disiplinleri kullanılır.

Bilgi güvenliği yönetimi sisteminin fonksiyonlarının iyi bilinmesi örgütsel anlamda büyük önem taşır. Aşağıda, bu fonksiyonlar tek tek açıklanmaya çalışılmıştır.

2.3.1. Yöneltme

Yöneltme, işletme çabalarının bilgi güvenliğinin sağlanabilmesine yönelik olarak teksif edilmesini ifade eder. Bilgi Güvenliği yönetimi için gerekli ilk şartların oluşturulması bu safhada başlar. Yönetim kademesinin vereceği direktifle birlikte, işletme hedef ve stratejisine uygun olarak güvenlik ihtiyaçları tespit edilir. Akabinde de işletmenin güvenlik politikası oluşturulur. Güvenlik politikasının hangi safhalarda oluşturulacağı ve kapsamının ne olacağı bir önceki bölümde açıklanmıştır.

Güvenlik politikası bütün güvenlik yönelimli davranışları betimleyen, hepsinin üstünde bir öncelik derecesine sahiptir.[85] Güvenlik politikasını işletme güvenlik yapısının omurgası olarak tabir etmek mümkündür. Yapılacak tüm eylemler bu politikanın sınırları içinde olmak durumundadır.

Güvenlik politikası ile birlikte, işletme güvenlik stratejisi de oluşturulur. Güvenlik stratejisi, işletmenin güvenlik hedeflerine nasıl ulaşılacağını gösterir. İcra edilen uygulamalarda güvenlik stratejisi takip edilir.

Bilgi güvenliği yönetim sistemi, bir çevrim süreci olduğundan, değerlendirmeler ve değişiklikler neticesinde olabilecek değişiklikler sisteme entegre edilir ve yeniden yöneltme uygulanır.

---

[85] Rhein Hansen, **a.g.e.**, s.3

2.3.2. Örgütleme

İşletme içinde bilgi güvenliği aktivitelerinin gerçekleştiği bütün çevrimi kontrol edebilmek için bir yönetim yapılanması gereklidir. Genellikle bilgi yönetimini esas alan modellerde bilgi güvenliğinin sağlanması ve diğer bilişim işlemleri, oluşturulacak bir takım tarafından yerine getirilir.[86] Bu organizasyonun gerçekleştirilmesinde dikkat edilmesi gereken bazı konular vardır.

2.3.2.1. Takım Organizesinde Dikkat Edilmesi Gereken Prensipler

Takım organizasyonunda en önemli düşünce "takım düşüncesidir". Bir takım yapısında, moral, grup normları, yönetim tarzı gibi konular önemli rol oynamaktadır. Bu anlamda, yapılan işin mahiyeti bir yerde ikinci planda kalmaktadır. Takım ne şekilde oluşturulursa oluşturulsun, başarı için öncelikle takım ruhunun bireylere aşılanması gereklidir. Örgütün takım yapısında dikkat edilmesi gereken genel prensipleri ise şu şekilde sıralayabiliriz.[87]

- Az sayıda ve kaliteli personel kullanın. Küçük grupların göreceli olarak daha verimli çalıştıkları görülmüştür. Kalabalık gruplarda genellikle daha fazla iletişim ihtiyacı ortaya çıkmaktadır. Bu durumun verimlilik üzerinde olumsuz bir etkisi olmakta ve daha fazla hataya yol açmaktadır.

- Görevleri personelin kabiliyeti ve motivasyonuna uygun olarak seçin. Birçok yönetim sisteminde çok iyi çalışan personel, yönetim kademelerine terfi ettirilerek ödüllendirilir. Bu mantık birçok durumda çökmektedir. Çok iyi çalışan bir personelin, iyi bir yönetici olabileceği yargısı yanlıştır. İki alanda farklı konular içermektedir. Bu yüzden çalışkan personel ödüllendirilmek istendiğinde kendi kariyer gelişimleri ile ilgili farklı pozisyonlar ve çözümler düşünülmelidir.

---

[86] Alistair Donaldson & Phil Walker, "Information governance—a view from the NHS" **International Journal of Medical Informatics,** 2003, s.283.

[87] Hans Von Vliet, **Software Engineering – Principles and Practice,** John Qiley & Sons Ltd. Baaffins Lane, Chichester, West Sussex 1019 1UD, England, Second Edition, 2003, s.97.

- Uzun vadeli terfi sistemi iyi planlanmalı. Personel terfi ettiğinde, uzmanlık alanındaki gelişmesi de muhtemel sekteye uğrayacak veya duracaktır. Bu durum hızlı değişen bilgisayar teknolojisinin doğal bir sonucudur. İkinci bir olasılık ise, personelin uzmanlık alanı dışındaki görevlerde kullanılmaması durumunda ortaya çıkmaktadır. Kendisine terfi için fırsat tanınmayan personel uzun vadede, aynı işi yapmaktan dolayı sıkılacak ve örgütten soğumaya başlayacaktır. Kariyer planlamasında bu iki olasılığın göz önünde tutularak, kişiye özel çözümler getirilmesinin akılcı bir çözüm olabileceği düşünülmektedir.

- Dengeli ve uyumlu çalışan bir takım için takım üyeleri iyi seçilmelidir. Bir takımda herkesin star olması beklenemez. Böyle bir oluşuma gitmek zaten takım mantığına yanlıştır. En üst seviyede uzman çalışanların yanında dengeyi ve uyumu sağlayacak normal seviyedeki personelin istihdamına dikkat edilmelidir. Takım yapısında uyum ve denge dikkat edilmesi gereken en önemli unsurdur.

- Takıma uyum sağlayamayanlar ayrılmalıdır. Takım, bütün bir yapıdır. Bütünlüğü bozan personelin bu yapıdan uzaklaştırılması gerekir. Genellikle yöneticiler, böyle bir durum karşısında bir müddet daha bekleyip, olayların düzelmesini bekleme eğilimindedirler. Ancak uzun vadede bu şekildeki olayların örgüte zarar verdiği bir gerçektir.

Takım içinde üyelerin aldığı roller farklı olabilir. Yürütülen projenin büyüklüğüne göre bir personele birden fazla görev de verilebilir. Tavsiye olarak kimin ne iş yapacağının kesin çizgilerle ayrılması ve denge unsurunun gözetilmesi performansa olumlu katkı sağlayacaktır. Büyük grupların yönetimi oldukça zordur. Bu nedenle, gruplar bölünerek küçültülür. Takım organizasyonu ile ilgili genel prensipleri ortaya koyduktan sonra örgüt yapılarını da aşağıdaki gibi inceleyebiliriz.

2.3.2.2. Hiyerarşik Organizasyonlar

Çok sık karşılaşılan bir yapılanma şeklidir. Organizasyonun veya projenin büyüklüğüne göre farklı yönetim seviyeleri uygulanabilir. Genellikle yapılanmada kaç alt sistem varsa, o kadar takım oluşturularak hiyerarşi düzenlenir. Hiyerarşi yapısı,

sistemin geneli hakkında da bilgi verir. Alt sistemlerin oluşumunda, proje bazlı fonksiyonel bölünmeler de görülen yapılanmalardır. Sistem yöneticileri, bilgi güvenlik elemanları bu kapsamda değerlendirilebilir.

Hiyerarşik yapılanmalarda koordinasyon mekanizması öne çıkan bir unsurdur. Asıl faaliyet alt basamaklarda yürütülür. Üst basamaklara çıkıldıkça, yapılan işin detayıyla ilgili bilgi azalır. Bununla beraber, konunun bütününe olan hakimiyet daha fazladır. Hiyerarşik yapılanmadan kaynaklanan koordinasyon problemleri en sık görülen problemlerdendir. Alt kademelerdeki bir sorunun üst kademelere ulaştırılabilmesi için bütün ara yönetim kademelerinden geçmesi gerekmektedir. Sorunun mahiyetinin ise iletişim kanallarından geçerken değişime uğraması genellikle karşılaşılan bir durumdur. Bu yapılarda üst yöneticinin yanlış bilgilendirilmesi olasılığını ortadan kaldırabilmek için iletişim kanallarının çok iyi kullanıldığı bir koordinasyon mekanizması kurulmalıdır.

2.3.2.3. Matriks Organizasyonlar

Matriks organizasyonlar, ürün bazlı yapılanmalarda genellikle karşılaşılan bir şekildir. Farklı departmanlarda çalışan bir ürünü ortaya çıkarmak veya hizmet üretmek maksadıyla, çoğunlukla part time bir araya gelerek çalışmayı yürütür. Bu şekilde işletme içinde bir veya birden fazla ünite oluşturulur. Oluşturulan üniteler, farklı uzmanlık alanlarındaki kişilerden oluşur. Ürünün en kaliteli ve seri şekilde ortaya çıkarılmasında oldukça kullanışlı bir yapı oluşturur.

Matriks organizasyonlarda, bir dezavantaj olarak, projenin gelişimini takip etmek zordur. Çalışanların farklı departmanlarda olması bu sonuca yol açar. Diğer bir nokta olarak ise çalışanlar proje ile ilgili olarak birden fazla yöneticiye karşı sorumlu hale gelir. Eğer çalışan birden fazla yerde görev yapıyorsa, hangi işi ne zaman yapacağı, ne kadar süre hangi konu üzerinde çalışacağı ve kimden izin alacağı konularında sürekli problemler yaşar.

Proje yöneticisi, projenin takibinden ve devam ettirilmesinden sorumludur. Matriks organizasyon yapısına uyan projeler, işletme içinde örgüt kültürü yüksek ise

çalışanlar, iş görmek için güdülenmiş ve paylaşmaya istekli iseler, yüksek oranda başarıya ulaşırlar. Proje yöneticisi başlangıç safhasında kimlerin hangi görevleri alacağını, çalışma sürelerini ve şartlarını belirler, bunları onaylanmış yazılı belgeler haline getirirse birçok belirsizliği ortadan kaldırmış olur. Proje yöneticisinin bu konudaki performansı, proje gruplarının başarısında önemli bir yer tutacaktır.

2.3.2.4. Takım Liderliği Yapısı

Takım Liderlği yapısı 1970 yılında Harlan Mills tarafından ortaya konmuştur.[88] Takımın çekirdeği üç kişiden oluşur. Şef, takım lideridir ve bütün konularla o ilgilenir. Şefin iki asistanı vardır. İlki, şefin ihtiyaç duyacağı yardımları yapar. Diğeri, idari konularla ve dokümantasyonla ilgilenir. Bunların yanında birkaç uzman daha takıma ilave edilebilir.

Bu yapıda, her şey şefin etrafında döner. Şefin, teknik konulara yeterince hakim bir kişi olması gerekmektedir. İlave olarak, yeterli seviyede yöneticilik kabiliyeti de bulunmalıdır. Bu yapı bir cerrah ve ekibini andırır. Tamamen uzmanlık isteyen bir iş yapılır ve takım da kendi konusunun uzmanlarından oluşur. Baş cerrah hem kendi konusunda en iyidir, hem de karizmatik bir liderdir.

Bu yapı özellikle bilgisayar yazılımı üreten işletmeler için uygundur. Farklı uzmanlık alanlarındaki (veritabanı, grafik tasarım, programcılık, kullanım testi gibi) personel bir ekip halinde bir araya getirilir. Bu ekibe eğitimi devam eden bir veya iki kişi, şefin yardımcısı rolünde ilave edilebilir.

2.3.2.5. SWAT Takımları

SWAT takımlarının genellikle yineleme veya revizyon gerektiren işlerde kullanılmaktadır. zaman zaman görülmektedir. SWAT kelimesi, "Skilled With Advanced Tools" (Gelişmiş Donanım Kabiliyetli) kelimelerinin baş harflerinden

---

[88] Hans Von Vliet, **a.g.e.**, s.95.

oluşturulmuştur. SWAT takımları yapısının bilişim sektöründe yazılım geliştirme projelerinde uygulandığı görülmektedir. Yapısal olarak nispeten daha küçük bir sayıya sahiptir. 4 veya 5 kişilik gruplardan oluşur. Aynı odada çalışırlar. Bu yüzden iletişim kanalları kısa tutulmuştur. Formallikten uzaktır. Resmi toplantılarla, brifinglerle zaman kaybı yaşanmaz. Genellikle seminer ve beyin fırtınaları ile bilgi alış verişi yapılmakta ve sorunlara bu yöntemler ile çözüm aranmaktadır.

Bu sistem yapısı itibariyle, yanlış anlaşılmalardan ve yönetim kademeleri arasında oluşabilecek anlam kaymalarından muzdarip olmamaktadır. Aslında "Takım Liderliği" yapısına benzer özellikler taşır. Grup üyeleri bu yöntemde de uzman kişilerden oluşmaktadır ve SWAT takımının lideri hem yönetici hem de çalışan teknik bir elemandır.

SWAT takımlarında motivasyon çok önemli bir unsurdur. Genellikle takımın vizyonunu yansıtan bir logo, slogan veya takma ad kullanılır. Bu tür bir uygulama takım ruhunu güçlendirir ve takım üyelerini bir birine bağlar.

2.3.2.6. Açık Yapılı Takımlar

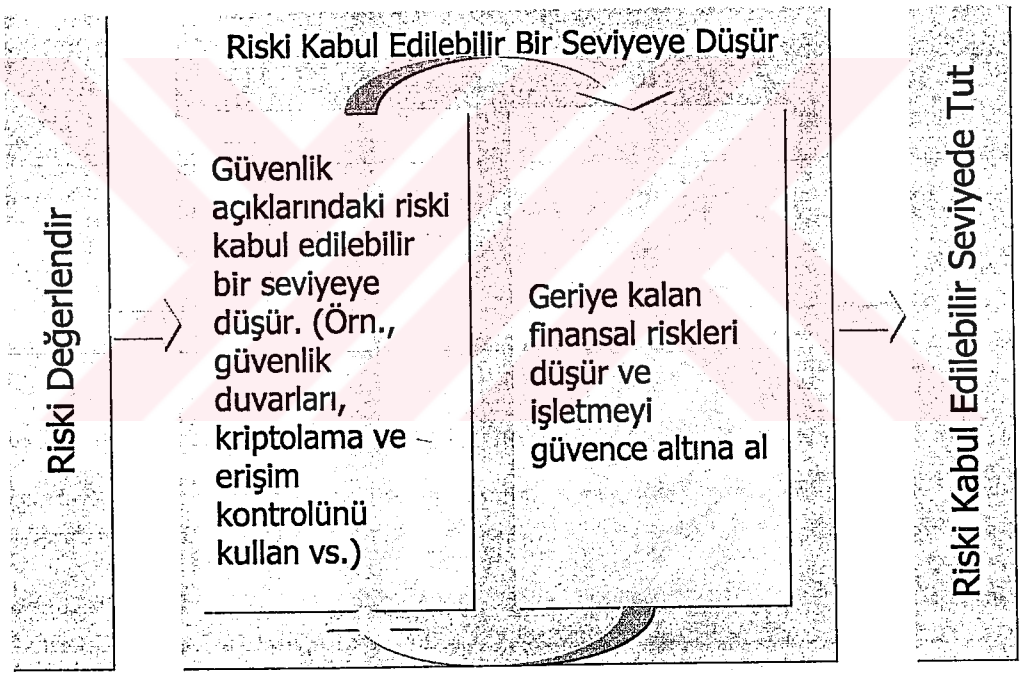
Bilişim sektöründe faaliyet gösteren işletmelerde veya işletmelerin bilişim ile ilgili faaliyet gösteren departmanlarında karmaşık problem çözümü ile ilgili olarak açık yönetim tarzları öne çıkar. Bu yaklaşım, işletmenin ve işin boyutlarına göre belirlenmekte olup bilişim konularına çok uygun bir yöntemdir.

Çalışanların da fikirlerinin alındığı modern organizasyon yapısında doğal olarak ortaya atılan bir görüşü destekleyen ve desteklemeyenler olacaktır. Destekleyenler, görüşü benimseyerek performans artışına katkıda bulunacak, desteklemeyenler performans artışına ya katkıda bulunmayacak veya performansı düşürecektir. Buna benzer problemleri ortadan kaldırmak için açık yapılı takımlar yöntemi uygulanmaktadır. Bu yöntemde bireyler arasındaki ilişkiye çok önem verilir. Teknik lider, hiçbir ortak görüşe varılmasa bile yönetici sıfatı ile olaylara uzlaşmacı bir çözüm bulmaktan sorumludur.

Açık yapılı takımlar, esasen farklı dünyaların en iyilerini birleştirmeye yöneliktir. Burada kişisel uzmanlığa ve proje hedeflerine odaklanılarak, proje amaçlarına zamanında ve etkin bir şekilde ulaşılması için merkezi eşgüdüm üzerinde durulmalıdır.

2.3.3. Risk Yönetimi ve Değerlemesi

Risk; muhtemel zarar, kayıp gibi organizasyona ve amaçlarına istenmeyen etkilerde bulunabilecek durumlar ve sonuçlardaki belirsizliği ifade eder.[89] Risk yönetimi ise bu belirsizlik ortamının yönetilmesi manasına gelmektedir. Bilgi güvenliği yönetimi, risk yönetimi ile özdeşleşmiş durumdadır. Aşağıdaki şekil, bilgi güvenliğinde risk yönetimini ifade etmektedir.



Şekil 2.11 : Bilgi Güvenliğinde Risk Yönetimi

KAYNAK : Lawrance A.Gordon & Martin P.Loeb, **Economic Aspects of Information Security,** University of Maryland, College Park, June 27, 2003 s.6

---

[89] **Information Security Management and Assurance,** The Institute of Internal Auditors, Critical Infrastructure Assurance Project, Washington DC., First report, April 2000, s.6.

Bu kapsamda önce işletmenin bilgi işletim yapısındaki riskler tespit edilir. Ağ yapısına olabilecek tehditler, daha önceki bölümlerde açıklanmıştır. Bilgi güvenliği ile ilgili departman, mevcut tehditlerin ağ yapısı için ne derecede bir risk oluşturduğunu ortaya koymalıdır.

Daha sonra risk öncelikleri belirlenmeli ve öncelik sırasına göre muhtemel risklere karşı gerekli tedbirler alınmalıdır. Bu şekilde risk oranı minimuma indirilebilir. Düşürülen risk oranı, değişen şartlara göre yeniden değerlendirilerek, ilave tedbirlerle kontrol altında tutulabilir.

Bir organizasyon bilgi riski yönetimi konusunda aşağıdaki hususları yerine getirmek zorundadır:

- Bilgi Risk Yönetim grubunun veya komitesinin oluşturulması,
- Bilişim varlıklarının ve her birinin değerlerinin tanımlanması,
- Varlıkların her birinin gizliliğine, bütünlüğüne ve kullanımına yönelik tehditlerin tanımlanması,
- Kabul edilebilir bir risk modeline göre varlıkların her birine ve hepsine birden olabilecek riskin analiz edilmesi,
- Her bir bilgi ünitesi için tanımlanan riskin nasıl yönetileceğinin (riski kabul etmek, transfer etmek veya riski azaltmak gibi) analiz edilmesi,
- Belirtilen sürecin periyodik bir şekilde tekrarlanarak, risk yönetimine devam edilmesi.[90]

Bu süreçte, üzerinde durulması gereken bir nokta, risk modelinin seçilmesidir. Risk modellerine girmeden önce riskin matematiksel bir eşitliğini yazmak, formülasyon açısından daha faydalı olacaktır.

---

[90] **California Counties"Best Practices" Information Security Program,** California County Information Services Directors Association, CCISDA Information Security Forum, March 2002, s.31.

Risk = (Bir bilişim varlığına karşı oluşacak tehdit olasılığı) x (Varlığın değeri) [91]

Bu formül riskin matematiksel bir ifadesini sağlayacak ve risk analiz grubuna önceliklendirme yapmasında yardımcı olacaktır. Model seçiminde en iyi yollardan bir tanesi her bir varlık için ortaya çıkabilecek riski niteleyen risk modelleri geliştirmek ve bunları sayısal hale getirerek ölçmektir. Bu modellerden bazıları, doğru sonuçlar çıkarabilmek için detaylı matematik ve istatistik analizleri içermektedir. Model seçiminde işletmenin veya departmanın ihtiyacına en uygun modelin seçilmesine özen gösterilmelidir. Sık kullanılan risk modellerinden bir tanesi şu şekilde ifade edilmektedir.

$$Risk = \frac{Tehdit}{Karşı\ tedbirler} \ x \ \frac{Hassasiyet}{Önlemler} \ x \ \frac{Hasar}{Dersler} \ x \ \frac{Değer}{Çaba}$$

Eşitlikteki değişkenlerin ifadeleri aşağıda açıklanmıştır.

Tehdit, saldırı amacı taşıyan bir metottur.

Karşı tedbirler, saldırılardan gelen tehdidi önleyebilmek amacı ile atılan adımlardır.

- ◊ Önlemler, hassasiyeti azaltmak için uygulanan adımlardır.
- ◊ Hasar, bir saldırı sonrası gerçekleşen maliyettir.
- ◊ Dersler, bir saldırı sonucunda gerçekleşen olumlu değerlerdir.
- ◊ Değer, risk altındaki unsurların maliyeti
- ◊ Çaba ise değeri korumak için sarf edilen emeğin tamamıdır.

Hassas bilginin karşılaştığı riskin her bir cihaz için ayrı ayrı ölçülmesinden sonra yapılacak işlem bu riskin / risklerin yönetilmesidir. Yönetim, ölçülen riskin nasıl yönetileceğini ve ne gibi bir yaklaşım sergileyeceğini ortaya koymalıdır. Her bir yaklaşım için maliyet analizi yapılır. Genellikle riskin yönetilmesinde üç yaklaşım söz

---

[91] California Counties"Best Practices" **Information Security Program,** March 2002, s.34

konusudur. Bunlar; *"Riskin kabul edilmesi", "Riskin transfer edilmesi" ve "Riskin azaltılması"* dır.[92]

2.3.3.1. Riskin Kabul Edilmesi

Temel olarak işletmenin mevcut riski kabul etmesini gerektirecek iki durum söz konusu olabilir. Birincisinde risk maliyeti düşüktür ve işletme tarafından kabul edilebilir bir düzeydedir. İkincisinde ise riskin transfer edilmesi veya azaltılması için oluşturulacak maliyet, riskin kendisinden daha yüksektir. Bu iki durumda da işletme riski kabullenebilir. Eğer riski kabul etme maliyeti, riskin azaltılması veya transfer edilmesinden daha yüksekse işletme riski kabul etmemelidir. Bu durumda diğer iki seçenek göz önüne alınmalıdır.

2.3.3.2. Riskin Transfer Edilmesi

Riskin transfer edilmesi, herhangi bir alandaki riskin üçüncü bir şahıs veya firma ile paylaşılmasını ifade etmektedir. Bu tür uygulamaları genellikle sigorta şirketleri yapmaktadır. Belirlenen risk, yapılan anlaşma şartları ve riskin oluşacağı durumun öngörüleri dahilinde uygun bir ücret karşılığında sigorta şirketi tarafından üstlenilir.

Bazı durumlarda riskin transfer edileceği üçüncü bir taraf bulunamayabilir. Veya risk üstlenici üçüncü taraflar, belirlenen riski almak istemeyebilir. Bu durumda riskin kabul edilmesi veya riskin azaltılması seçenekleri öne çıkar.

2.3.3.3. Riskin Azaltılması

Risk durumu yüksek bir ünitede riskin transferi gerçekleştirilemiyorsa, riskin kısmi veya tamamen azaltılması yönüne gidilmelidir. Azaltma süreci, muhtemel

---

[92] California Counties "Best Practices" **Information Security Program,** March 2002, s.35.

tehditlerin tanımlanması, araştırılması, tehditlere karşı etkili tedbirlerin geliştirilmesi safhalarını içerir.

Riskin azaltılması bazen en hızlı ve en ucuz yoldur. Bilgi sistemlerinin sağlayıcılarının sunduğu ücretsiz güvenlik yamaları, otomatik güncelleme mekanizmaları, tespit edilen hataların ücretsiz olarak giderilmesi bu kapsamda değerlendirilebilir. Riski azaltma maliyeti, riskin ne olduğuna göre değişiklik arz eder. İçinde hassas bilgi sistemleri bulunan bina, doğal afetlerden kolaylıkla etkileniyorsa, güçlendirilerek afete karşı korumalı hale getirilmelidir. Bu amaçla yapılacak harcamalar risk azaltma maliyetini artıracaktır.

Bu şekilde, karşı tedbirlerin kullanılması risk azaltmada etkili bir yöntemdir. İlgili tedbirler büyük oranda önlemler bölümünde açıklanmıştır. Karşı tedbirlerin alınması, ölçülen risk miktarının önemli oranda düşürülmesini sağlamaktadır.

2.3.4. Planlama

Risk değerlemesi safhasını müteakiben ortaya konan güvenlik gereksinimleri ve önlemleri planlanır. Planlamada temel olan işletmenin kendi ihtiyaçlarıdır. Risk değerlemesi sonucunda ölçülen risk ve maliyet, alınması gereken karşı tedbirleri de şekillendirecektir. Karşı tedbirlerin tam ve kapsamlı olarak hazırlanması, işletmeye bilgi sistemleri güvenlik mimarisinin oluşturulmasında da büyük avantaj sağlar.

"Temel Güvenlik Yaklaşımı" detaylı bir risk analizi yapılmadan, sadece güvenlik risk seviyelerinin ortaya konup, minimum koruma tedbirlerinin alınması ile ihtiyacın karşılanabileceğini ifade etmektedir. Bu görüş açısı ISO/IEC TR 13335 teknik raporu tarafından da desteklenmektedir.[93] Bununla birlikte minimum koruma tedbirlerinin neler olacağı konusunda varılmış bir ortak görüş bulunmamaktadır. Bu doğrultuda işletmelerin detaylı bir risk analizi yapmasının ve analiz sonrası ortaya çıkan

---

[93] Rhein Hansen, **a.g.e.**, s.3.

neticeler paralelinde güvenlik önlemlerini planlamasının daha doğru sonuçlar vereceği değerlendirilmektedir.

Planlama safhası, ortaya konan eylem tarzlarının dokümante edilmesi sürecini de içermektedir. Planların ve benzeri eylem tarzlarının dokümante edilmek suretiyle basılı ve yazılı hale getirilmesi, uygulanabilirlik oranını artırıcı bir rol oynar.

2.3.5. Uygulama

Güvenlik ile ilgili uygulamalar, hazırlanan güvenlik planı/planları paralelinde yürütülür. Planın uygulanmasından bütün işletme çalışanları, takibinden de güvenlik birimleri ile üst yönetim sorumludur. Uygulamada temel olarak kapsanacak konular;

- Güvenlik yönetimi
- Kritik iş uygulamaları
- Bilgi işleme
- Haberleşme ağları
- Sistem geliştirme

olarak tasnif edilebilir.

Tasnifi yapılan konular, birbirlerinden farklı riskler ve uygulama alanları içerebilmektedir. İşletme yapısına ve yapılanmasına göre oluşan eğilimler, bu konuda uygulanacak güvenlik yaklaşımlarını farklılaştırabilir.

Bilgi güvenliği tedbirleri ve uygulamaları ile ilgili uluslar arası standartlar, İngiltere'de uygulanmakta olan BS 7799 (Code of Practice for Information Security Management) standardından esinlenerek oluşturulmuştur. Türkiye'de ise "TS ISO/IEC 17799 Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi İçin Uygulama Prensibi" adıyla yürürlüğe girmiştir.

2.3.6. Eğitim

Örgüt çalışanlarına uygulanan eğitim genel olarak iki kategoride değerlendirilebilir. Bunlar; örgüt içi eğitim ve örgüt dışı eğitimdir. Örgüt içi eğitim, işletmenin imkan ve kabiliyetleri ile sağlayabileceği eğitimi kapsamaktadır. Çalışanların eğitilmesinde örgüt içi eğitimin büyük faydaları olduğu mülahaza edilmektedir. Örgüt içi eğitim mesleki eğitim kapsamında önemli yer tutar. Bunun yanında örgütün kendi bünyesinde sağlayamayacağı eğitim için örgüt dışı eğitim planlanır. Bu tip eğitimlerde personelin kariyer gelişimi göz önünde tutulduğu gibi, işletmenin gelişmesi, büyümesi, değişime uyumu gibi gerekçeler de önem arz eder.

Bilgi güvenliği ile ilgili olarak yapılacak eğitimin belirli periyotlar halinde planlaması yapılır. Bu planlama maliyet açısından önem taşıdığı gibi, gelişimin ve etkinliğin ölçülmesi, takibinin yapılabilmesi açısından da önemlidir. Bilgi güvenliği eğitimi, bilgi güvenliği politikası ve stratejisi doğrultusunda planlanır. Ferdi bazda ve toplu olarak yapılabilir. İşletmenin güvenlik politikalarının ve uygulamalarının çalışanlara anlatıldığı eğitimler, genellikle örgüt içi eğitim şeklinde planlanır. Yüksek uzmanlık gerektiren eğitimler ise örgüt dışı, uzman kişi ve kuruluşlarca verilir. Bilgi güvenliği personelinin eğitilmesi ve sertifikasyonu bu kapsamda değerlendirilir.

Bilgi güvenliği eğitimi uzman kurum ve kuruluşlar tarafından kurs ve seminer ile verilebilmektedir. Eğitim muhteviyatı ihtiyaca göre farklılaşabilmektedir. Bilgi Güvenliği Yönetim Standardı BS 7799 / ISO 17799 ile ilgili olarak verilen eğitimin, işletmelerin bilgi güvenliği yaklaşımlarını gözden geçirmeleri, yapısal ve teknik değişikliklere gidebilmeleri açısından önemli olduğu düşünülmektedir. Böyle bir eğitimde kapsam olarak;

- Güvenlik ihtiyacı ve tehlikenin tanımlanması,
- Güvenlik yönetim sistemi,
- Güvenlik nasıl yönetilir,
- BS 7799 / ISO 17799 standardı,
- Bilgi güvenliği yönetimi kapsamının belirlenmesi,
- Güvenlik politikasının kapsamı,

- Bilgi güvenliği yönetiminin çerçevesinin oluşturulması,
- Risk analizi ve değerlendirmesi,
- Kullanım uygunluğunun belirlenmesi ve yazılı hale getirilmesi,
- Kritik güvenlik kontrollerinin anlaşılması,
- Fiziksel, Mantıksa ve Prosedürel güvenlik,
- Sertifikasyon ihtiyacı ve BS 7799 sertifikasyonu süreci

konuları incelenmektedir[94]. Bu tip bir eğitim, işletmenin güvenlik konusundaki belirsizliklerini ortadan kaldırmasına yardım edecek, daha rasyonel yaklaşımlar ortaya koymasına yardımcı olacaktır. Bilgi güvenliği yönetimi eğitimine kimlerin katılacağı ile ilgili olarak;

- Kuruluşların kritik bilgi varlıklarına erişim olan tüm çalışanların,
- Birim yöneticilerinin,
- Güvenlik yöneticileri ve personelinin,
- Bilgi sistem yöneticilerinin,
- İnsan kaynakları yöneticileri ve personelinin,
- Dahili denetçilerin

katılabileceği bir profil ortaya koymak uygun olacaktır.

2.3.7. İşletim

İşletim, işletme faaliyetleri ile ilgili olarak her gün yapılan işlemleri ifade eder. Bilgi güvenliği ile ilgili olarak her gün yapılan faaliyetler güvenlik prosedürlerinde belirtilmiştir. İşlemler bu prosedürlere uygun olarak yapılır. Bu amaçla prosedürlerin eksiksiz takip edilip edilmediğini kontrol eden bir içsel denetleme mekanizması kurulmalıdır. Bu mekanizma güvenlik döngüsünde işletmenin bilgi güvenliğinin sağlanmasını garanti altına alır.

---

[94] Infosecure 201, BS 7799 / ISO 17799 **Bilgi Güvenliği Yönetim Sistemi Standardına Giriş,** http://www.infosecurenet.com/akademi.asp, Erişim Tarihi: 04 Nisan 2004.

Veri dosyalarının işlemler sırasında yedeklenmesi bilgi güvenliğinin önemli bir boyutudur. Yedeklenen bilgilerin tekrar kullanılabilir bir halde olup olmadıkları periyodik olarak kontrol edilir.

Yukarıda sayılan günlük işletim faaliyetlerine ilave olarak normal bir işletmede dikkat edilmesi gereken noktaları şu şekilde sıralayabiliriz.

- **Yapılanma yönetimi;** mevcut yapılanmanın, güvenlik açısından sürekli kontrol altında tutulması ve değişikliklerin uygun şekilde ele alınmasıdır. Sistemde meydana gelen bütün değişiklikler kayıt altında tutulur. Bu değişiklikler işletim sistemlerinin sistem yönetimi araçlarında bulunabileceği gibi, olmaması durumunda veya ilave bazı özelliklere ihtiyaç duyulması durumunda çeşitli ağ yönetim yazılımları vasıtasıyla takip edilebilir. Sistem değişiklik kayıtları belirli bir süre saklanmalıdır (3 ay / 6 ay gibi). Bu süreye güvenlik politikası ve güvenlik gereksinimleri doğrultusunda karar verilir. Değişiklik kayıtları sistem yöneticileri veya bilgi güvenlik sorumluları tarafından mütemadiyen analiz edilir. Analiz sonucunda ulaşılan bilgiler, yönetimin yeniden şekillenmesinde veya revizyonunda etkileyici rol oynar.

- **Değişiklik yönetimi;** bilgi sistemlerinde bir değişiklik olduğunda yeni güvenlik gereksinimlerinin ortaya çıkıp çıkmadığı ve değişim gereksinimlerinin ne şekilde ele alınacağı ile ilgilidir. Güvenlik ihtiyacı yeniden tanımlanır. Risk analizi bu kapsamda değerlendirilebilir. Değerlendirme sonucu ortaya çıkan durumun yönetilmesi, ihtiyaçların önceliklendirilmesi, maliyet analizlerinin yapılması ve sorunun halli bilgi sistemlerindeki değişikliğin yol açtığı sonuçlardır.

- **Problem yönetimi;** ortaya çıkan herhangi bir güvenlik sorunun yönetilmesidir. Yönetim mekanizması öncelikle en alt seviyeden başlar. Ortaya çıkan sorunların bu seviyelerde çözülebilecek bir mahiyette olması, sorunun büyümesini ve üst yönetim kademelerinin sorunla işba hale gelmelerini önler. Bununla birlikte sorun alt kademede çözülemiyorsa, silsileye uygun olarak üst kademelere taşınır. Problem çözümü ile ilgili olarak işletmenin yapısına göre farklı prosedürler takip edilebilir. Önemli olan takip edilecek prosedürlerin belirlenmiş olmasıdır.

- **Yedekleme ve afet kurtarma prosedürleri;** hassas bilginin yedeklenmesi, bilgi güvenliğinin en önemli ayrıntılarından birisidir. Yedekleme, bilginin kaybolma maliyetini ortadan kaldırmaya / en aza indirmeye yarayan bir tedbirdir. Bilgi yedeklemesinin önemi ve ne şekilde yapılacağı önceki bölümlerde açıklanmıştır. Günlük işletme faaliyetlerinde önem arz eden nokta, neyin, ne şekilde ve ne zaman yapılacağının belirlenmiş olması ve sorumluların bu konuya uymalarıdır.

Afet kurtarma prosedürleri de aynı kapsamda değerlendirilmelidir. Personel ve malzemenin tahliyesi, kimin hangi malzemeyi kurtaracağı, nerelerden tahliye edileceği önceden belirlenmeli ve bu prosedürlerin uygulanabilirliği zaman zaman test edilerek gözden geçirilmelidir.

2.3.8. İzleme

İzleme bilgi güvenlik yönetimi çevriminin başarılı veya aksayan noktalarını ortaya koyar. İzleme faaliyeti ile çevrim üzerinde sürekli bir denetim mekanizması kurulmuş olur. İzleme, yönetim sürecinin her safhasında devamlılık arz eden bir faaliyettir. Bu sürekli denetim mekanizması ile;

- Önlemlerin ve prosedürlerin amaçlandığı gibi çalışıp çalışmadığı değerlendirilir.

- Çevresel değişiklikler ile teknik altyapının korunup korunmadığı gözden geçirilir.

- Otomatik bir değerlendirme programı kurularak, gözlemde hassasiyet sağlanır ve işgücü tasarrufunda bulunulur.

- Ortak kabul edilmiş standartların bağımsız üçüncül birimlerce gözden geçirmesine müsaade edilir ve aksayan yönler, tarafsız bir şekilde ortaya konur.

2.3.9. Değerlendirme

İzleme süresince ortaya çıkarılan güvenlik sapmaları, düzenli bir şekilde yönetim kademelerine rapor edilir. Bu raporlar sonucunda bilgi sistemleri güvenlik yapısının başarılı bir şekilde çalışıp çalışmadığı ortaya konur. Güvenlik sisteminin nerelerinde ayarlama yapmak gerektiği tespit edilir. Değerlendirme safhasında;

- Yönetim tarafından geçmiş döneme ait değerlendirme ve gözden geçirme raporları incelenir.
- Değerlendirme, risk değerlemesi temeli üzerine yapılır.
- Yönetim, uygun hareket tarzlarına karar verir.

2.3.10. Düzeltme

Değerlendirme sonucunda düzeltici işlemlerin yapılmasına karar verilirse, işletme kaynakları bu yöne tahsis edilir. Düzeltme işlemi, işletme faaliyetleri arasında önceliğe sahiptir. Düzeltme faaliyetleri kapsamında;

- Bilgi sistemleri güvenlik politikası güncelleştirilir.
- Yeni önceliklere göre bilgi sistemleri güvenlik stratejisi değiştirilir.
- Gerekli uygulama projeleri başlatılır.

Bilgi güvenliği çevriminin 10 safhalık döngüsü yaklaşık olarak 6 ile 12 aylık bir süre içerisinde tamamlanmaktadır. Bu döngü ile üst yönetim çok fazla çaba sarf etmeden doğrudan yönetim sürecini yönlendirebilme imkanına sahip olmaktadır. Çalışanlar da günlük olarak uygulayacakları bir rehbere sahip olmaktadır.

Güvenlik yönetim sisteminin anlatılan şekilde kurulması ile işletmenin karşılaşacağı problemler büyük ölçüde azaltılır. Bununla birlikte aynı anda 10 madde üzerine odaklanmak her zaman mümkün olmayabilir. Bir konunun bile gözden

kaçırılması, bütün bir yönetim sistemini tehlikeye atabilir. "Bir zincir en çürük halkası kadar sağlamdır", prensibi bilgi güvenliği yönetiminin en önemli kuralıdır.

2.4. BİLGİ GÜVENLİĞİ YÖNETİMİNDE DIŞ KAYNAK KULLANIMI

İşletmelerin, sadece kendi sahip oldukları yetenek ve becerileri esas alan işleri yapmak istemeleri veya öz yeteneklerinin kullanılmadığı işleri , organizasyon dışındaki başka işletmelerden temin etmeleri, yaygın bir dış kaynak kullanımı uygulamasını ortaya çıkarmıştır.[95] Dış kaynak kullanımı son yıllarda bilgi teknolojilerinde de yaygınlaşmaya başlamıştır. Ancak bilgi sistem güvenliğinin sağlanmasında dış kaynak kullanımı nispeten yeni bir konudur. Bilgi teknolojileri her geçen gün çok daha karmaşık bir yapıya bürünmektedir. Bilgi teknolojilerine yönelik risk de gelişen teknoloji paralelinde bir artış göstermiştir. Tehditler daha baş edilemez bir hal almıştır. Bilgi güvenliği konusunda dış kaynak kullanımının artmasındaki en önemli etken budur.[96] Uzman personel istihdamı, aynı zamanda koruma maliyetlerini de artırmıştır. Buna paralel olarak bazı işletmeler için konuyu daha uzman bir firmaya veya gruba devretmek daha avantajlıdır.

Bilgi sistemleri güvenliğinde dış kaynak kullanımından beklenen avantajlar olarak şu şekilde sıralanabilir.[97]

- İşletme personel ve kaynaklarının işletme stratejisi doğrultusunda teksif edilmesi,

- Maliyet yönetimine ve para tasarrufuna olanak tanıması,

---

[95] Tamer KOÇEL, **İşletme Yöneticiliği,** Beta Yayınları, İstanbul, 8.Baskı, Mart 2001, s.315.

[96] Abdulwahed Mo. Khalfan, "Information security considerations in IS/IT outsourcing projects:a descriptive case study of two sectors" **International Journal of Information Management** sayı 24, UK, 2004, s.35.

[97] **Outsourced Information Security Management,** Internet Security Systems Publication, June 2002 Atlanta/USA, s.3.

- Bilgi güvenliğinin artırılması,
- Uzman personel ile çalışmanın işletmeye sağlayacağı güven,
- Güvenlik ihlalleri ve saldırıları sonucunda oluşabilecek yüksek maliyet ve güven kaybının önüne geçilmesi.

Orta ölçekli bir işletmenin, bilgi güvenliği ihtiyacını dış kaynak kullanarak karşılaması, kendisine ortalama yıllık %40 ile %60 arasında bir tasarruf sağladığı, bu konuda uzmanlaşmış firmalar tarafından beyan edilmektedir.[98]

İşletmeler dış kaynak kullanmaya, risk ve maliyet etkinlik analizleri sonucunda karar verirler. Böyle bir karar aşamasında dış kaynak kullanımının işletmelere olabilecek mahzurlarının da göz önüne alınması gerekir. Bunlar kısa veya uzun vadede ortaya çıkabilecek sorunlardır. Kısa vadede karşılaşılabilecek sorunlar, daha çok bilgi akışı ve iletişim konularıyla ilgilidir.

Uzun vadede karşılaşılabilecek sorunların başında, tedarikçi işletmelere aşırı bağlılık gelmektedir. Ortaklık seviyesine varabilecek bir dış kaynak kullanımı ilişkisi, firmayı tedarikçi işletmeye bağımlı hale getirir. Bu durum başlangıçtaki beklentinin aksine dış kaynak kullanan işletmenin esnekliğini kaybetmesine yol açar. İlişkilerde kontrolün kaybedilmesi ve fiyat konusunda istenilen şartları yerine getirme zorunluluğu, avantajlı bir konunun işletme için dezavantaj haline gelmesine yol açar.[99]

Diğer bir konu ise bilgi güvenliğinde dış kaynak kullanımının bilgi güvenliğinin kendisine tehdit teşkil etmesidir. Bunun önlenmesi için, tedarikçi firma ile yapılan sözleşmeye, örgütün haklarını hukuki olarak koruyacak maddeler eklenir. Başka bir ifade ile tedarikçi firmadan hassas bilgileri kötü amaçla kullanmayacağına dair, hukuki garanti alınır.

---

[98] Outsourced Information Security Management, **a.g.e.**, s.4.

[99] Tamer KOÇEL, **a.g.e.**, s.317.

Endüstriyel anlamda bir diğer olumsuz sonuç ise dış kaynak kullanımının bir nevi işletmenin içlerini boşaltmaları anlamına gelmesidir. İşletme içini boşaltarak, kendi ilgi alanına odaklanır. Böylece maliyetler büyük oranda azaltılır. Bu eğilim ise aynı zamanda faaliyet gösterilen endüstri dalının da içinin boşalmasına yol açacaktır.[100]

İşletmeler için diğer bir seçenek, bilgi güvenliği yönetiminde bütün olarak dış kaynak kullanımı yerine sadece belirli alanların ihale edilmesidir. Bu yöntem finans sektöründe sıklıkla uygulanmaktadır. Finansal danışmanlık şirketleri, bankalar, çeşitli yatırım kurumları internet üzerinde faaliyet gösterirken web sitelerinin güvenliğinden emin olmak istemektedirler. Web sitesinin güvenliği ile ilgili testler, bir firmaya veya kuruma anlaşma yapılarak devredilir. Böylece güvenlik olayı dışarıdan sınanır. İşletmedeki bilgi güvenliği işletme kaynaklarınca sağlanmaya devam edilir. Bu yöntemin işletme için önemli faydaları vardır. Bunlardan biri, güvenliğin işletme kaynaklarınca sağlanması ile, hizmet sağlayan firmanın hassas bilgilere doğrudan nüfuz edememesidir. Diğeri, firmanın web sitesini ve internet bağlantısını uzman kuruluşlara denettirerek, siber saldırılardan etkilenebilecek alanları çok daha düşük bir maliyetle tespit etmesidir.

Güvenlik danışmanlığı da son günlerde yaygınlaşan diğer bir sektördür. Güvenlik danışmanları, işletmelerin bilgi güvenlik yapısına sürekli olarak müdahalede bulunmazlar. Belirli bir periyot içerisinde güvenliği inceleyerek üst yönetime bulguları rapor halinde sunarlar.[101] Rapora göre işletme durumunu yeniden değerlendirerek, alınması gereken tedbirleri belirler.

Bilgi sistemlerinin sigortalanması da dış kaynak kullanımı kapsamında değerlendirilebilir. Risk yönetimi bölümünde de anlatıldığı gibi tespit edilen risk, bilgi sistemlerinin sigortalanması sayesinde başka bir kuruluşa aktarılır. İşletmeler bilgi güvenliğinin temini için bu ve buna benzer yöntemler doğrultusunda dış kaynak kullanmaktadır.

---

[100] Tamer KOÇEL, **a.g.e.,** s.317.

[101] Rick Davis, **The Unlikely Hereos of Cyber Security,** The Information Management Journal, May/June 2003.

Sonuç itibariyle, dış kaynak kullanımı da, diğer tüm yönetim tekniklerinde olduğu gibi, yerine ve zamanına göre kullanılmalı ve yönetilmelidir. Bu açıdan bakıldığında, dış kaynak kullanımının, işletmelerin başarılarına çok büyük katkı sağlayan bir işletmecilik tekniği olduğu görülür.

ÜÇÜNCÜ BÖLÜM

AĞ BİLGİ SİSTEMLERİNDE BİLGİ GÜVENLİĞİ YÖNETİMİNİN NATO CAOC 6 KOMUTANLIĞINDA UYGULANMASI

3.1. UYGULAMA YAPILAN CAOC 6 KOMUTANLIĞINA AİT GENEL BİLGİLER

CAOC 6 (Combined Air Operations Centre – Birleştirilmiş Hava Harekat Merkezi 6) Komutanlığı, NATO Komuta yapısında bir üst komutanlık olan İTALYA Napoli'de konuşlandırılmış AIRSOUTH karargahına bağlı olarak görev yapar. NATO yapısındaki değişiklikle birlikte Eylül 1999'tarihinde ESKİŞEHİR'de kurularak göreve başlamıştır. CAOC 6 güney bölgesindeki 5 CAOC'tan bir tanesidir.[102]

CAOC 6 Komutanlığının görevi, Bölge Hava Komutanlığı (AIRSOUTH) direktifleri paralelinde, barış, kriz ve çatışma durumlarında, kendisine tahsisli tüm birliklerin, hava harekatını planlamak, bu birlikleri görevlendirmek, koordine ve komuta etmek ve rapor etmektir. İlave olarak uygun Deniz ve Kara komutanlıkları ile irtibat görevi, Milli ve Nato komutanlıkları arasında koordinasyon görevini yürütür.

CAOC 6 Komutanlığı, diğer NATO birliklerinde olduğu gibi çok uluslu bir yapıya sahiptir. Türkiye haricinde diğer ülke mensupları, ABD, Almanya, İtalya, Macaristan, İspanya ve Yunanistan'dandır.

CAOC 6 Komutanlığı ve diğer NATO birlikleri güçlü bir ağ bilgi sistemleri alt yapısına sahiptir. Görevi ve konumu itibariyle de bilgi güvenliği son derece önemlidir ve titizlikle takip edilmektedir.

3.2. CAOC 6 KOMUTANLIĞINDA AĞ BİLGİ SİSTEMLERİNİN UNSURLARI

Alan çalışması, NATO CAOC 6 Komutanlığında, 1 adet Unix ve 1 adet Intel tabanlı iki ağ sistemi üzerinde, gözlem; çalışanlar ve muhabere bilgi sistemleri

---

[102] **NATO Handbook,** NATO Office of Information and Press, 1110 Brussels – Belgium, 2001, s.257.

personeli ile görüşme ve karşılıklı mülakat yöntemleri uygulanarak yapılmıştır. Bilgi güvenliği yönetimi konusunda uluslar arası bir standart olan BS 7799.2 2002 Kontrol Listesi uygulamada esas alınmış, elde edilen bulgular, bu listeye kaydedilmiş ve değerlendirilmiştir.[103]

Uygulama sonuçları 10 başlık halinde incelenmiştir. Varılan sonuçlar aşağıda açıklanmıştır.

3.2.1. Güvenlik Politikası

"Bilgi Güvenliği" politikası yönetim tarafından onaylanarak yayınlanmış ve bütün çalışanlar tarafından anlaşılmıştır. Bilgi güvenliği yönetiminde örgütsel bir yaklaşımla yönetim kararlılığı oluşturulmuştur. Bu kararlılık neticesinde mevcut politika, personel tarafından titizlikle uygulanmaktadır. Bilgi güvenliği ile ilgili aksaklıklar en üst yönetim seviyesinde ele alınarak mutlak çözüme ulaştırılmaktadır.

Güvenlik politikası Karargah Güvenlik subayı tarafından düzenli bir şekilde gözden geçirilmektedir. Konu ile ilgili olarak üst komutanlıklarca yılda bir defa güvenlikle ilgili görev ve sorumluluğu bulunan personel denetlenmektedir. Gözden geçirme işlemleri asli değerlendirmeye temel teşkil edecek şekilde yapılmaktadır.[104]

3.2.2. Örgütsel Güvenlik

Bilgi güvenliği, örgüt içersinde olmazsa olmaz yaklaşımı ile ele alınmakta ve güvenli olmayan hiçbir sistem ve yöntem kullanılmamaktadır. Örgüt içersinde yönetim forumunu sağlayacak ve güvenlik inisiyatifini destekleyen açık ve anlaşılır bir yönetim desteği vardır.

---

[103] Kontrol listesinin içerdiği konular için bakınız EK-1.

[104] Detaylı bilgi ve uygulama soruları için bakınız "EK-2 Güvenlik Politikası Kontrol Listesi ve Elde Edilen Bulgular".

Bilgi güvenliğinde koordinasyon sağlayabilmek amacıyla ilgili birim temsilcileri arasında çapraz kontrol mekanizması oluşturulmuştur Karargah Güvenlik Subayının altında ona karşı sorumlu olarak çalışan her branştan ilgili bir personel bulunmaktadır. Sorumlu olarak tespit edilen kişiler düzenli olarak toplantılar yapmakta ve bilgi sistemleri kullanıcılarına uyarıcı hatırlatmalarda bulunmaktadır.

Her bir bilgi sisteminin korunmasını sağlamak amacıyla sorumluluklar ve özgün güvenlik işlemleri açıkça tanımlanmıştır. Bütün bilgi sistemleri için Yerel Alan Ağı güvenlik sorumluları tespit edilmiştir. Bu sorumlular Çalışma Sahası Güvenlik Subayları ile eşgüdüm içersinde çalışmaktadırlar

Bilgi işleme kolaylıklarının yetkilendirme süreci ile ilgili olarak yeni bir bilgi sistemi kurulmadan önce sistemin yapısını ve bağlantılarını açık bir şekilde ifade eden ve güvenli bir sistem olduğunu belirten kontrol listeleri onaylanarak bir üst makama yetki için başvurulmaktadır. Bu işleme Güvenlik Akreditasyonu denilmektedir. Üst makamlarca ilgili gizlilik seviyesine uygun olduğu onaylanırsa sistemin kurulmasına ve ilgili Geniş Alan Şebekesine bağlanmasına müsaade edilmektedir. Yetkilendirme süreç yönetimi bütün yazılım ve donanım kolaylıklarını kapsamaktadır.

Çalışma Alanı Güvenlik Subayı bilgisayar ve güvenlik ile ilgili kişilerden seçilmekte ve daha sonra bu konuda özel eğitim almaktadırlar. Çalışma Alanı Güvenlik Subayları; Yerel Alan Ağı güvenlik Subayı, Bilgi Güvenliği Subayı, Haberleşme Güvenliği Subayı gibi konu üzerinde daha fazla uzman olan personel ile beraber eşgüdüm içersinde çalışmaktadır.

Herhangi bir güvenlik olayında hızlıca uygun eyleme geçilmesini sağlayacak ve tavsiyede bulunacak haberleşme uzmanları, bilgi hizmeti sağlayıcıları mevcuttur. Bilgi ve tecrübenin yetersiz kaldığı durumlarda daha üst komutanlıklarda bulunan uzman personele başvurulmaktadır. Askeri yapının haricindeki sivil veya resmi kurum ve kuruluşlardaki uzmanlarla da bağlantılar mevcuttur.

Örgüt içinde çalışan üçüncül şahıs ve firmalar ile ilgili güvenlik riski tanımlanmış ve uygun kontroller yapılmaktadır. Bu şahıs ve firmaların kontrollü sistemlere direk erişimi mümkün değildir. Sadece bakım sözleşmesi imzalanan firmalar

idarenin kontrolü altında, idarenin isteği üzerine sistemlere müdahale edebilmektedirler. Üçüncül şahıslar özellikle kontrollü sistemlerde, nezaretçisiz işlem yapamamaktadırlar. Kontrollü sistemlerin bakımlarının yapılması için yapılan sözleşmelerin içerisinde üçüncül şahısların idarenin güvenlik kurallarına kayıtsız şartsız uyacağı belirtilmektedir. Böylece örgütsel güvenlik politikaları ve standartları, güvenlik ihtiyaçları doğrultusunda resmi sözleşme metinleri içinde yerini almaktadır. Sözleşme yasal gereklerin nasıl karşılanacağını, örgütsel varlıkların güvenliklerinin nasıl idame ettirileceğini ve test edileceğini, denetleme haklarını, fiziki güvenlik konularını ve herhangi bir afet anında servis imkanlarının nasıl idame ettirileceği konularını kapsamaktadır.[105]

3.2.3. Varlıkların Sınıflandırılması ve Kontrolü

Bütün bilgi sistemlerin önemli parçalarının seri numaraları ayrı bir demirbaş listesi olarak tutulmaktadır. Her bir sistemin sorumlu personeli belirlenmiş olup, üzerinde etiketle gösterilmektedir. Sistemlerin yeri ilgili birimin izni ve onayı alınmadan değiştirilememektedir. Bütün sistemlerin üzerinde güvenlikle ilgili gizlilik derecesi sınıflandırması gözle görülebilecek şekilde etiketlenmiştir.

Her kurulacak bilgi sistemi kurulmadan önce hangi gizlilik seviyesine sahip olacağı bir üst yönetim kademesinin onayı ile belirlenmektedir. Bilgi sınıflandırmasının nasıl yapılacağına dair yönergeler mevcuttur. Sistemlerin kurulmasından sorumlu olan birimler bu rehberin uygulanmasından da sorumludur.

Örgütün sınıflandırma şemasına uyan bilgi işleme ve etiketleme için uygun yöntemler oluşturulmuştur. Belirli bir gizlilik seviyesinin üzerine çıkan harici hafıza üniteleri (Harddisk, Disket, CD vb.) özel kontrol numaraları ile kayda alınmaktadırlar. Belirli bir gizlilik seviyesinin altındaki harici hafıza üniteleri için kayıt işlemi uygulanmaz, ancak hangi gizlilik derecesine kadar bir bilgi ihtiva ettikleri, üzerlerindeki etiketle gösterilir.

---

[105] Detaylı bilgi ve uygulama soruları için bakınız "EK-3 Örgütsel Güvenlik Kontrol Listesi ve Elde Edilen Bulgular".

Bilgilerin nasıl işlem göreceğinin ve korunacağının belirlenmesine yardımcı olacak bilgi sınıflandırma rehberi ilgili dokümanlarda yer almıştır. Ağ'da bulundurulan bütün bilgiler için gizlilik tasnifi yapılmaktadır.[106]

3.2.4. Personel Güvenliği

Bilgi güvenliği ile ilgili örgüt için organizasyon şeması oluşturulmuş olup, her görev tanımı ile ilgili yapılacak işlerden kimin sorumlu olduğu belirlenmiştir. Sorumluluklar örgüt içerisindeki en üst yetkili tarafından kendilerine tebliğ edilmiştir. Verilen bu sorumluluklar belirli varlıkların korunmasına veya güvenlik faaliyetlerinin genişletilmesine ait sorumlulukları kapsadığı gibi güvenlik politikalarının yerine getirilmesi veya idame ettirilmesini de kapsamaktadır. Örgütün bilgi güvenliği politikasında bulunan güvenlik rolleri ve sorumlulukları görev tanım formlarına işlenmiş durumdadır.

Sürekli çalışan personel iş yaparken gözlenmekte ve güvenlik tasdikleri takip edilmektedir. Personelin hangi seviyedeki bilgilere haiz olacakları güvenlik kleransı ile belirlenmektedir. İlave olarak, çalışanlara örgüte katılım belgeleri içerisinde gizlilik kurallarına uymaları ile ilgili güvenlik belgesi imzalatılmaktadır. Bu belge her 6 ayda 1 kendilerine yeniden tebliğ edilmektedir. İstenilen gizlilik seviyesindeki kleransa haiz olmayan kimselerin işe başlamaları mümkün değildir. Personelin işten ayrılması bilgi saklama sorumluluğunu değiştirmemektedir. Bu durum özel kanunlarla korunmaktadır.

Kullanıcı Eğitimi ile ilgili olarak, örgüte yeni katılan personele ilk katılış brifingi sırasında bilgi güvenliği konusunda bilgi verilmektedir. Bilgi güvenliğine ait diğer detaylı eğitim ise örgüt çapında üç ayda bir yapılan periyodik eğitim ve seminerlerle verilmektedir. Üçüncül şahıslar örgüt içerisinde bulundukları sürece yapacakları işlemlerle ilgili eğitim almaktadırlar. Bu eğitim bilgi güvenliğini de

---

[106] Detaylı bilgi ve uygulama soruları için bakınız "EK-4 Varlıkların Sınıflandırılması ve Kontrolü Kontrol Listesi ve Elde Edilen Bulgular".

kapsamaktadır. Güvenlik olaylarının uygun yönetim kademesi vasıtasıyla mümkün olan en kısa zamanda bildirildiği resmi yöntemler oluşturulmuştur. Hangi güvenlik olayının hangi rapor formatı ile bildirileceği ve karşılığında ne gibi işlemler yapılacağı yönergelerde yer almaktadır. Örgüt içi haberleşme kanalları ile sistemlerde oluşabilecek herhangi bir güvenlik zafiyeti ilgili birimlere iletilmektedir.

Yazılım arızalarının bildirilmesi ile ilgili yöntemler de düzenlenmiştir. Yazılımlardaki aksaklıklar örgüt kabiliyeti ile giderilebilecekse muhabere bilgi sistemleri yardım masasında bulunan nöbetçi personele bildirilmektedir. Ancak arızalar, yazılımın yapısı ile ilgili ise yazılımı üreten firmaya veya birime bildirilmesi için özel rapor formatları kullanılmaktadır.

Örgütsel güvenlik politikalarını ve yöntemlerini ihlal eden çalışanlar hakkında disiplinle ilgili resmi süreçler bulunmaktadır. Bu süreç kanunlarla belirlenmiştir ve çok sıkı bir şekilde takibi yapılmaktadır. Bu konuyla ilgili örgüt içi istihbarat birimleri görev yapmaktadır.[107]

3.2.5. Fiziksel ve Çevresel Güvenlik

Fiziksel ve çevresel güvenlikle ilgili olarak birçok farklı kademelerde güvenli bölgeler ihdas edilmiş ve bilgi işlem cihazları çeşitli güvenlik tedbiri ile koruma altına alınmıştır.

Örgütün ana giriş kapısında güvenlik personeli tarafından giriş kartı kontrolü yapılmaktadır. Bina girişinde ise manyetik kartlı şifreli geçiş sistemi bulunmaktadır. Örgütün dış sınırları tel örgü ile çevrilmiş olup silahlı güvenlik personeli tarafından 24 saat gözetim altında tutulmaktadır. Örgüt içersindeki çeşitli alanlara sadece yetkili kişilerin girişine müsaade eden kontroller geliştirilmiştir. Manyetik kart

---

[107] Detaylı bilgi ve uygulama soruları için bakınız "EK-5 Personel Güvenliği Kontrol Listesi ve Elde Edilen Bulgular".

sistemi ile bir bölümden diğerine geçiş yapılmaktadır. Kartların yetki seviyesi ise bir merkez tarafından kontrol edilmektedir.

Bilgi işleyen hassa cihazların bulunduğu bölgelerde elektronik şifreli kapılar bulunmakta ve haricen kilitlenmektedir. Özel bilgi ve yüksek gizlilik derecesine haiz materyal üç kombineli şifreli çelik kasalarda muhafaza edilmektedir. Örgüt binası, örgütün faaliyet gösterdiği alan ile doğru orantılı olarak doğal felaketler ile savaş tehlikesine karşı en üst düzeyde korumaya sahiptir.

Bilgiler sadece bilmesi gereken kişiler içindir. Güvenli bölgelerde çalışan üçüncül şahıslar ve personel için güvenlik kontrolleri yapılmaktadır. Üçüncül şahıslara sadece bilmeleri gerektiği kadar bilgi verilmektedir. Güvenli bölgelerde ise örgüt içinde bir veya daha fazla personel üçüncü şahıslara nezaret etmektedir. Üçüncül şahısların güvenlik kontrolleri, güvenlik birimi tarafından yapılmaktadır.

Bilgi işleme bölgeleri güvenli bölgeler olarak tasnif edilmiştir. Dışarıya karşı izolasyonu tamdır. Malzeme giriş çıkışının yapıldığı kapılar hassas bölgelerden uzakta ve kontrol altındadır. Sunucu ve kripto cihazlarının bulunduğu alan özel bir oda haline getirilmiş, yetkisiz erişimlere tamamen kapatılmıştır. Üç kombineli kilitle muhafaza altına alınmış, duvarlar özel olarak güçlendirilmiştir. Ağa bağlı diğer cihazların bulunduğu yerler, yetkisiz personelin erişimine kapalıdır. 24 saat gözlem altında olmayan alanlarda bulunan hassas bilgiye haiz bilgisayarların hard diskleri mesai saati bitiminden sonra, üç kombineli kilitli çelik kasalarda saklanmaktadır. Mesainin bitiminden sonra bir güvenlik personeli bütün odaları tek tek inceleyerek uygun güvenlik önlemlerinin alındığını kontrol etmektedir.

Yangına karşı fiziki güvenlik önlemi olarak otomatik yangın algılama ve söndürme sistemi bulunmaktadır. Diğer doğal afetlere ve diğer fiziki tehditlere karşı 24 saat görev yapan izleme bölümü bulunmaktadır. Sunucu odalarında bir şeyler yiyip içmek yasaktır. Yedekleme ihtiyacı duyulmayan bilgisayarların yanında yeme-içme kontrolü yapılmamaktadır. Sigara içmek bütün binada yasaktır.

Güç kaynakları ile ilgili olarak, kesintisiz güç kaynağı, çoklu besleme ve yedek jeneratör gibi sürekli güç kaynakları kullanılarak cihazlar elektrik kesintisinden

korunmaktadır: Ağı destekleyen merkezi kesintisiz güç kaynakları şehir cereyanı kesilse bile sistemi beslemeye devam etmektedir. Şehir cereyanının kesilmesini takip eden 15sn. içinde jeneratörler devreye girmekte ve kesintisiz güç kaynaklarının üzerindeki yükü almaktadırlar.

Hassas ve kritik bilgiler için ek güvenlik kontrolleri uygulanmaktadır. Veri taşıyan haberleşme kabloları ile güç kabloları ayrı ayrı kanallar içerisinde bulunmaktadır. Bu kanallar özel metal bir yapıya sahip olup, elektrik ve bilgi kaçaklarını ayrı ayrı topraklara iletmektedirler.

Merkezi kesintisiz güç kaynağı belli bir güç seviyesinin üzerinde olduğundan ve güvenli toprağa bağlandığından şehir cereyanı üzerinden dışarıya bilgilerin kaçışı filtrelenmektedir.

Cihaz bakımları ise üretici firmanın tavsiye ettiği şekilde ve zaman aralığında yapılmaktadır. Arızalar ve bu arızalar ile ilgili yapılan düzeltici işlemler periyodik bakım formlarına kaydedilmektedir. Garanti kapsamında olan cihazlar için yapılan işlemler fatura ile beraber garanti bitimine kadar saklanmaktadır. Cihazlar kurum dışına gönderilirken ise gizli bilgi depolayan harici hafıza birimleri sökülmekte ve hangi parçaların gönderildiği teslim tutanağı ile kayıt altına alınmaktadır.bu cihazlar, taşıyıcı kargo şirketi veya cihazın gönderildiği firma tarafından sigorta ettirilmektedir.

Kurum veya bina dışına çıkartılan cihazların güvenliği güvenlik politikaları doğrultusunda alınmaktadır. Kontrollü cihazların örgüt dışına çıkartılması, üst yönetimin sorumluluğunda olup sürekli uygulanan bir yöntem değildir. Gerekli olduğu durumlarda ise takip edilecek prosedürler belirlenmiş durumdadır. Kurum dışına çıkartılacak cihazlar, bina içerisinde sağlanan güvenlikle eşit oranda güvenlik sağlamayan yerlerde kullanılamaz. Bu maksatla aynı güvenlik ortamını sağlayan yerlerde kullanılmak şartıyla kurum dışına çıkartılmasına müsaade edilebilir. Hassas

bilgi içeren cihazlar kurum dışına çıkartıldığında bilgi güvenliğinin temin edilmesinden cihazları teslim alan makam sorumlu olmaktadır.[108]

3.2.6. Haberleşme ve İşletim (Operation) Yönetimi

Güvenlik Politikası, yedekleme ve cihaz bakımı gibi işletimsel yöntemler tanımlamıştır. Ağ bilgi sistemlerinde kullanılan bütün programlar, bu programlarda yapılacak herhangi bir değişikliğin değişiklik kontrol yetkilendirmesinden geçme ihtiyacında olması gibi sıkı bir kontrol mekanizmasından geçmektedir. Örgüt içinde kullanılan programlarda örgüt personeli tarafından değişiklik yapılmamaktadır. Değişiklik ihtiyacı, ilgili ticari firmaya veya bunu üreten birime uygun usullerle bildirilmektedir. Program değişiklikleri ilgili firma veya üreten birim tarafından örgüte bildirilmekte ve alınan değişiklikler, alındığına dair kaydedilmektedir.

Güvenlik olaylarının nasıl ele alınacağına dair ilgili yönergelerde ekler mevcut olup, bu ekler düzenli olarak güncellenmektedir. Güvenlik birimleri 24 saat faaliyet gösterecek şekilde yapılanmıştır. Güvenlik ihlalleri olduğunda, ihlalin tipine göre hangi birimin sorumlu olacağı önceden bellidir. Olayla ilgili denetleme izleri ve kayıtları tutulmaktadır. İstenmeyen olayların tekrarlanmasını önleyecek aktif tedbirler alınmaktadır. Örnek olay yaklaşımı örgüt çapında yaygın olarak kullanılmakta, örgütün bağlı olduğu üst birimlerce gerekli önlemler alınarak tüm personelin müteyakkız olması temin edilmektedir. Her cihazın bulunduğu bölge ile ilgili güvenlik sorumluları vardır. Bu sorumlular, cihazların yetkilendirilmiş personel tarafından kullanılıp kullanılmadığını gözlemler. Cihazların yerlerinin değiştirilmesi, içlerinin açılması da dahil olacak şekilde tüm güvenlik ihlalleri bu sorumlular tarafından takip edilir. Karşılaşılan aksaklıklar, güvenlik organizasyon şemasında gösterilen hiyerarşik yapıya göre güvenlik birimlerine bildirilir.

---

[108] Detaylı bilgi ve uygulama soruları için bakınız "EK-6 Fiziksel ve Çevresel Güvenlik Kontrol Listesi ve Elde Edilen Bulgular".

Kapasite istekleri düzenli olarak takip edilmekte, gelecek ile ilgili kapasite ihtiyaçları öngörülmektedir. Bina içindeki merkezi kesintisiz güç kaynağı, mevcut kapasitenin üzerinde olup, artırma planları ile uyumludur. Yedekleme üniteleri, her bilgisayar sistemleri 5 yılda bir yenilenirken yeniden planlanmakta ve kapasitenin üzerindeki ihtiyaçları da karşılayacak şekilde satın alınmaktadır. Bunların haricinde ortaya çıkabilecek herhangi bir kapasite ihtiyacı bir sonraki yıllık bütçeye dahil edilerek temin edilmesi sağlanmaktadır.

Yeni sürüm, güncelleme ve yeni bilgi sistemleri için sistem kabul kriterleri düzenlenmiştir. Kabulden önce gerekli testler yapılmaktadır. Yeni sürüm, güncelleme yazılımları merkezi olarak takip edilmekte ve örgüte üst makamlar tarafından temin edilmektedir. Yerel alım ile karşılanan sistemler için standartlar merkezi olarak belirlenmekte, alınan cihazların standartlara uyup uymadığı ise yerel olarak kontrol edilmektedir. Kontrol sırasında sözleşme maddelerinin tek tek karşılanıp karşılanmadığı test edilmektedir.

Kötü niyetli yazılımlara karşı etkin koruma mekanizmaları geliştirilmiştir. Müsaade edilmeyen yazılımların kullanılması yasaklandığı gibi lisanslı yazılım kullanmayı öngören bir güvenlik politikası da oluşturulmuştur. Bu konular yönergelerde açık olarak belirtilmektedir. Kullanıcı personelin her bilgisayara girişi sırasında kötü niyetli yazılımların kullanılmaması gerektiğine dair uyarıcı bir mesaj yayınlanmaktadır. Bilgisayarlarda, sunucular tarafından kontrol edilen merkezi anti virüs yazılımları mevcut olup, bu yazılımlar düzenli olarak güncellenmektedir.

Bilgilerin yedeklenmesi, güvenliğindeki en önemli konulardan bir tanesidir. Yedekleme üniteleri yedekleme yöntemlerine uyumludur. Yedekleme birimleri mevcut kapasitenin tamamını bir gün içerisinde yedekleyebilecek kabiliyete sahiptir. Yedeklenen bilgiler, sunucuların bulunduğu yerden ayrı bir yerde depolanmaktadır. Düzenli bir test işlemi yapılmamakla beraber kullanıcı ihtiyaçları doğrultusunda ortaya çıkan durumlarda yedeklenen bilgilerin geri yüklenmesinin testi yapılmaktadır. Bütün bilgisayar sistemlerine servis sağlayan sunucuların her gün tam yedeklemesi yapılmaktadır.

İşletim sorumluları, yapılan işlemlerle ilgili bilgileri, kayıt defterlerine düzenli olarak kaydetmektedirler. Bu sayede her işletmenin yaptığı işlemden diğerlerinin de haberi olmaktadır. Arızalar muhabere bilgi sistemleri yardım masasına bildirilmekte ve buradaki görevli personel tarafından takip edilmektedir. Yapılan düzeltici işlemler bilgisayar üzerinde arıza kayıt dosyalarına işlemektedir.

Ağ yönetimi ile ilgili ağ ve korumalı sistemlerde veri işlemlerinin güvenliği ve bütünlüğü açısından gerekli kontroller oluşturulmuştur. Her bilgi sisteminin yerel alan ağı (YAA), kendi IP adresi menzilinde çalışmakta olup, birbirlerinden donanım ve yazılım olarak ayrılmış durumdadır. Hassas bilgi içeren YAA'lar hiçbir şekilde internete bağlanmamaktadır. Bu ağlar, uzaktan erişime kapalıdır. Hassas bilgi içeren YAA'lar, geniş alan ağına (GAA) bağlanmadan önce kriptolanmakta ve bu ağ üzerinde kriptosuz haberleşme yapılmamaktadır. GAA, merkezi olarak kontrol edilmekte ve muhtemel güvenlik açıklarına karşı denetime tabi tutulmaktadır.

Taşınabilir harici bilgisayar hafızalarının yönetimi ilgili yöntemler, ilgili dokümanlarda bulunmaktadır. Harici medya, belli bir gizlilik seviyesi üzerinde bilgi içerdiği taktirde, kontrollü evrak muamelesi görmektedir. Bu tip medyanın alınıp verilmesi, senetle yapılmakta ve her biri için ayrı bir kontrol numarası verilmektedir. Bu medya kontrol numaralarına göre düzenli olarak sayıma tabi tutulmaktadır. İhtiyaç duyulmayan harici hafızalar, yönergelerde belirtilen yöntemlerle imha edilmektedir. İmha edilen malzemenin kaydı ayrıca tutulmakta ve bunlar sayımdan düşülmektedir.

Sistem belgelerinin güvenliğini sağlayabilmek için sistem belgeleri yetkisiz erişimden korunmaktadır. Sistem belgeleri sadece muhabere bilgi sistemleri personeli tarafından kontrol edilebilmekte, diğer kullanıcılara bu konuda her hangi bir yetki verilmemektedir. Sistem kontrol dosyalarına yapılan işlemler, ağ güvenlik dosyalarına otomatik olarak kaydedilmektedir.

Örgütler arasındaki bilgi ve yazılım değişimi ilgili yönergeler gereği kontrollü olarak yapılmakta ve örgütler arasıdaki bu değişim, alındı onayı ile geri bildirilmektedir. Bu şekildeki değişim, bilginin gizlilik seviyesine göre belirlenmiş özel işlemlere tabidir.

E-posta iletimi, örgüt içinde haberleşmede büyük bir yer tutmaktadır. E-posta'ların yarattığı riski azaltmak için antivirus kontrolleri, güvenli olmayan potansiyel e-posta'ları izole etme ve istenmeyen e-posta aktarımının engellenmesi gibi kontroller uygulanmaktadır. E-posta sunucusu otomatik olarak gizlilik derecesi seçeneği sunan bir yazılım çalıştırmaktadır. Seçilecek gizlilik seviyesi, ağ gizlilik seviyesinin en üst limitine kadar olabilmektedir. E-postalar, anti virüs yazılımları ile kontrol edilmekte, şüpheli postalar otomatik olarak filtrelenmektedir. GAA internete açık olmadığı için, mevcut internet risklerinin büyük bir bölümü izole edilmiş olmaktadır.[109]

3.2.7. Erişim Kontrolü

Erişim kontrolü hakkında iş ihtiyaçları belirlenmiş ve belgeye dökülmüştür. Erişim kontrolü ihtiyacı çalışanların bulunduğu görev pozisyonuna göre ayarlanmaktadır. Her bölümün şube müdürlerinden gelen erişim kontrolü istekleri karşılanmakta olup, kullanıcıların şahsi başvuruları üzerine herhangi bir işlem yapılmamaktadır. Gruplar, şube müdürlerinin haftada bir yaptığı toplantı sonucunda belirlenmekte, gerek duyulduğunda da değişiklik yapılmaktadır.

Kullanıcı kaydı ile ilgili örgüte yeni katılışlar esnasında, yapılan kayıt işlemleri ile hangi bilgi sistemlerinden ne gibi hizmetler alacağı, kullanıcılara tebliğ edilmektedir. Yeni katılanlara örgüte katılışları esnasında güvenlik belgesi imzalattırılmakta ve bilgi sistemlerine ait kullanıcı şifresinin en üst seviyede gizliliğe haiz olduğu belirtilmektedir. Şifreler belirli bir süre içinde değiştirilecek şekilde sistem tarafından kontrol edilmektedir. Herhangi bir kullanıcı ile ilgili erişim hakkı güncellemesi esnasında mevcut diğer erişim hakları da gözden geçirilmektedir. Bu tip işlem en az ayda bir defa yapılmaktadır. Örgüt içerisinde bulunan bilgi sistemlerinin muhabere bilgi işlem personeli haricinde özel ayrıcalıklı kullanımı mümkün değildir.

---

[109] Detaylı bilgi ve uygulama soruları için bakınız "EK-7 Haberleşme ve İşletim Yönetimi Kontrol Listesi ve Elde Edilen Bulgular".

Kullanıcı sorumlulukları erişim kontrolünde ayrıcalıklı bir yere sahiptir. Şifre kullanımı, erişim kontrolü kapsamında değerlendirilmektedir. Şifrelerin ilk girişi ve güncellenmesi esnasında şifre kurallarına uymayan girişler, sebepleriyle birlikte kullanıcıya iletilmektedir. Kullanıcı bu kurallara uyan bir şifre girinceye kadar sisteme giriş yetkisi alamamaktadır. Her kullanıcı, işi bittiğinde kullandığı bilgisayarın ya ekranını kilitlemek veya sistemden çıkış yapmak zorundadır. Her ihtimale karşı maksimum 10 dak. İçerisinde bilgisayarın kendi ekranını kilitlemesi seçeneği, aktifleştirilmiştir. Ancak otomatik çıkış işlemi bazı sakıncaları dolayısıyla yapılmamaktadır.

Ağ erişim kontrolü konusunda, her bir ağın ağ güvenlik personeli ile sistem yöneticileri ilgili politikaların oluşturulmasında birinci öncelikli olarak sorumludur. Ağ hizmetlerinde esas olan politika sistem yönetimi ile ilgili işlemlerin sadece muhabere bilgi işlem personeli tarafından yapılmasına dayanmaktadır. Bu politikalar paralelinde her kullanıcının hangi bölümlere ulaşabileceği belirlenmekte olup, ilgili bölümlere kimlerin ulaşabileceği de ayrıca kontrol edilmektedir. Bu işlem için esas olarak sistem olay kütükleri düzenli olarak incelenmektedir. Kullanıcıların kendilerine ayrı bir yol oluşturmalarına müsaade edilmemektedir.

Harici bağlantılarda esas olan erişim iki tipte yapılmaktadır. Örgütün web sayfasına sadece misafir kullanıcı yetkileri dahilinde giriş yapılabilmektedir. Örgütün veri tabanına ulaşım, veri tabanı yetkilendirmesi ile kontrol edilmektedir. Düğüm kimlik kontrolü, emniyetli ve ortak bir bilgisayar kolaylığından grup olarak bağlanmış olan kullanıcıların kimlik kontrolü olarak hizmet verebilmektedir. Örgütün güvenlik yönetimi dışında herhangi bir bilgisayar sistemi bulunmamaktadır. Örgüt dışında güvenli bağlantılar üzerinden bağlantı kurulacağı zaman sadece belirli bir süre için geçici kullanıcılar tanımlanmaktadır. Bu kullanıcılar, telnet ve ftp servisleri ile kısıtlı işlemler yapabilmektedirler. İşlemin tamamlanmasından sonra bu tip kullanıcı hesapları sistemden kaldırılmaktadır.

Uzaktan hata kontrol işlemleri ile ilgili olarak GAA yöneticileri sorumlu olup, ihtiyaç duyduklarında sistemin GAA bağlantılarına müdahale edebilmektedirler. YAA'da bu tip müdahalelere müsaade edilmemektedir. GAA'ya bağlantının yapılması

için gelişmiş kripto cihazları kullanılmakta olup, bu bağlantı üçüncül şahıslar tarafından kullanılamamaktadır. Sistem internete bağlı olmadığından, güvenlik duvarı kullanılmamaktadır. Örgüt sınırlarının dışına uzanan ağ bağlantıları ilk kurulum aşamasından önce akredite edilmektedir. Akreditasyon işlemi sırasında GAA güvenliği, YAA güvenliği ve kullanılacak protokollerle ilgili onay alınmakta olup, sistem güvenliğini zafiyete uğratacak herhangi bir bağlantı türüne müsaade edilmemektedir. Akreditasyon gereklerinin yerine getirilip getirilmediği sistem kurulumundan önce örgütün bağlı olduğu üst birimlerce yerinde kontrol edilmektedir.

Hassas bilgi içeren bütün ağlar, umuma açık olmamakla birlikte, her bir ağın IP adres aralığı akreditasyon işlemleri sırasında belirlenmektedir. Her bir yazılımın kullandığı port numaraları belirli olup, bu portların haricinde kontrolsüz haberleşme yapılmamaktadır. Örgüt dışı kullanıcılar, kendi bulundukları bölgede güvenlik politikalarının uygulanmasından sorumludurlar. Her iki tarafında aynı şartlar altında güvenlik kurallarına uyması ağ adres dönüşümü gibi internet üzerinde kullanılan çeşitli güvenlik önlemlerine duyulan ihtiyacı ortadan kaldırmaktadır.

Sunucular ve routerlar GAA üzerindeki bütün sunucu ve routerları düzenli olarak kontrol etmekte, her bir sunucunun hangi sunucularla bağlantı yaptığı sistem kontrol tablolarından takip edilebilmektedir. Bilgi sistemlerine giriş için kullanılan her bir terminalin yakınında gözle görülebilecek şekilde kullanmaya yetkili personel isim listesi bulundurulmaktadır. Terminal bölgesi güvenlik sorumluları ve ilgili birimin kullanıcıları, yetkisiz personelin bilgi sistemlerine girişini gözlemlemektedir. Her kullanıcı kendi kullanıcı adı ve şifresi ile girdiğinden umuma açık kullanıcı adları ve şifreleri bulunmamaktadır.

Sistem yöneticileri ve diğer tüm teknik kullanıcılar, sisteme müdahale etmek için en üst seviyedeki yetkilere sahiptirler. Bu şekildeki sistem yöneticilerinin sayısı muhabere bilgi işlem teknik personelinin sayısı ile sınırlıdır. Sistem yönetimi ile ilgili veya hassas bilgiyi içeren bilgisayarlarda umumi kullanıcı bulundurulmamaktadır.

Ağ sisteminde güvenirlik ile ilgili kişisel şifreler, şifre değiştirme zorlaması, şifrelerin kriptolanmış formatta saklanması, şifrelerin ekranda görünmemesi vb. değişik

şifre kontrol yöntemlerine yönlendiren şifre yönetim sistemi kullanılmaktadır. Her bir kullanıcının ayrı ayrı şifresi mevcut olup bu şifreler minimum 8 karakterden oluşmaktadır. Şifrelerin içerisinde harf, sayı ve diğer işaretlerin kullanılma zorunluluğu vardır. Şifreler max. 180 gün içerisinde değiştirilecek şekilde otomatik olarak yeni girişe zorlanmaktadır. Hiçbir şifre ağ üzerinde bir yere kaydedilmemektedir. Şifreler girilirken ekranda kaç karakter girildiği gözükmemektedir.

Umumi kullanıcı alanlarındaki bilgisayarlar hiçbir işlem yapılmadığı taktirde max.10dak. içerisinde otomatik olarak kilitlenmektedir. Bu kilidi sadece ilgili kullanıcı veya sistem yöneticisi kaldırabilmektedir. Hassas bilgi içeren bilgi sistemleri ise fiziksel olarak koruma altında bulunan bölgelerde olduğu için zaman sınırlamasına ihtiyaç duyulmamaktadır.

İstisnai durumların ve erişim kontrollerinin saklandığı dosyalar, düzenli olarak yedeklenmekte, ihtiyaç duyulduğunda yedekler üzerinden kontrol edilebilmektedir. Gözlemleme faaliyetlerinin sonuçları düzenli olarak gözden geçirilmektedir. Sunucular üzerinde bulunan sistem kayıt dosyaları her bir kullanıcının hangi zaman aralıklarında sisteme dahil olduğunu ve ne gibi işlemler yaptığını kayıt altına almaktadır. Bu dosyalar düzenli olarak kontrol edilmekte ve yetkisiz herhangi bir giriş olup olmadığı ağ güvenlik sorumluları tarafından takip edilmektedir.

Dizüstü ve cep bilgisayarı gibi bilgisayar kolaylıkları ile ilgili olarak, Diz üstü ve cep bilgisayarı gibi mobil bilgisayar kolaylıklarının hassas bilgi içeren sistemlere bağlanmasına müsaade edilmemektedir. Bu tip bilgisayarlar örgüte ait resmi bilgisayarlar ise düşük seviyeli gizlilik derecesine haiz olmakta ve hassas bilgi içeren sistemlerden ayrı olarak akredite edilmektedir. Örgüt politikası olarak mobil bilgisayar sistemlerinin kullanımı sınırlandırılmış olup, kişisel mobil bilgisayarların örgüt içerisine getirilmesine müsaade edilmemektedir.[110]

---

[110] Detaylı bilgi ve uygulama soruları için bakınız "EK-8 Erişim Kontrolü Kontrol Listesi ve Elde Edilen Bulgular".

3.2.8. Sistem Geliştirme ve Bakım

Yeni sistemler veya mevcut sistemlerin geliştirilmesi için iş ihtiyaçlarının bir parçası olarak güvenlik gereksinimleri kapsanmaktadır. Aslen yeni sistemlerin ve mevcut sistemlerin geliştirilmesi örgütün yetkisi dahilinde olmayıp, merkezi olarak yürütülen projeler sayesinde yapılmaktadır. Böylece aynı seviyedeki diğer örgütlerle güvenlik standardizasyonu sağlanmaktadır. Sistem geliştirme aşamasındaki risk değerlendirmesi bağlı olunan en üst örgütün sorumluluğu altındadır.

Sisteme veri girişi için belli formattaki yapılar kullanılmakta olup, giriş esnasında verinin uzunluğu ve kullanılan karakterler sistem tarafından otomatik olarak kontrol edilmektedir. Yanlış veri girilmesi durumunda ilgili veritabanına kayıt yapılmayarak kullanıcıya yapılan hata hakkında otomatik uyarı mesajı gönderilmektedir. Doğru girilmiş olan veriler bazı durumlarda kasti hareketler veya işlem hatalarından dolayı bozulabilir. Kontroller, herhangi bir verinin bozulmasının işe etkisi ve uygulama yazılımının doğasına bağlıdır. Sistem veri girişlerindeki geçerleme kontrolleri kullanıcıların yapacağı hatalara karşı otomatik korumaya sahip olduğundan dolayı, yanlış formattaki bilgilerin girişi genellikle mümkün olmamaktadır. Her bir hata ile ilgili hata kodlarının açıklaması ve muhtemel düzeltici işlemler veritabanı yardım dosyalarında bulunmaktadır. Kontrol dışı yanlış girişler veritabanına kaydedildiğinde, hatalar sonradan tespit edilerek düzeltilebilmektedir.

Mesaj kimlik kontrolü, gönderilen elektronik mesajın içeriğinin yetkisiz bir şekilde değiştirilmesi veya bozulmasını tetkik etmekte kullanılan bir tekniktir.Her bir mesajın kendine ait mesaj kimlik numarası, uzunluğu, kaynak IP adresi, hedef IP adresi gibi teknik veriler, sistem tarafından otomatik olarak üretilmekte olup, ağ haberleşmesi standartlarına uymaktadır. Sistemlerde IPV4 IP adresleme tekniği kullanılmaktadır. Saklanan bilgilerin doğruluğu, checksum ve CRC hata tespit ve düzeltme mekanizmaları tarafından temin edilmektedir. Hatalı bilgiler, düzeltme işlemlerinden sonra sistem tarafından kullanıcılar uyarılmakta ve veriler yeniden kaydedilmektedir.

İletilmesi gereken bilginin koruma seviyesinin tanımında risk değerlendirmesi yapılmaktadır. Kriptografik kontroller bilgi güvenliğinin en hassas

noktası olup, güvenlik politikaları içerisinde tamamen ayrı bir şekilde tanımlanmaktadır. Her bir kriptonun gizlilik seviyesi hassas bilgi sistemlerinin sahip olduğu en üst gizlilik seviyesine uygundur. Verilerin GAA üzerinden gönderilmesinden önce donanımsal olarak kriptolanması sağlanmakta ve GAA'ya dahil olan bütün YAA'lar aynı güvenlik seviyesinde kriptolamaya tabidir.

Kriptolarla ilgili gizli anahtarlar hassas bilgi sistemleri üzerinden aktarılmayıp, özel kuryeler vasıtasıyla temin edilmektedir. Bu yüzden gizli anahtarların ağ üzerinden elde edilmesi mümkün değildir. Bu anahtarlar, kripto donanımının özelliğine bağlı olarak, her gün veya her hafta belli saatlerde güncellenmektedir. Güncelleme işlemi, karşılıklı olarak haberleşen iki kripto cihazı üzerinden aynı zamanda yapılmaktadır. Herhangi bir anahtar ihlaline karşı yedek anahtarlar mevcut olup, merkezi olarak, yapılan duyuruyu takiben, asli anahtarlar yerine yedek anahtarlar kullanılabilmektedir.

Bilgi sistemlerinin bozulmasına sebebiyet verebilecek oyun, şahsi uygulama yazılımları ve lisanssız ürünler sistemlere yüklenmemektedir. Böylece kontrolsüz değiştirmeler engellenmektedir. İşletim sistemi değişiklikleri yapılmadan önce mevcut durumun en son hali yedeklenmekte, herhangi bir sorunla karşılaşılırsa işletim sisteminin eski haline geri dönülmektedir. İşletim sisteminin bir önceki sürümü muhafaza edilmekte, sistemin tamamen çökmesi durumunda eski sürüm kullanılarak yeniden yükleme işlemi yapılmaktadır.

Yazılım paketleri örgüte ulaştığında mutlaka bir kopyası alınmakta, bozulmalara karşı bu kopya kullanılmaktadır. Yama ve servis paketleri sistem normal olarak çalıştığı sürece yüklenmemektedir. Ancak güvenlik sebebiyle yapılan özel duyurulardan sonra sistemde herhangi bir sorun olmasa da tavsiye edilen yama ve servis paketleri yüklenmektedir.

Gizli kanallar bazı belirsiz ve dolaylı yollarla bilgileri açığa çıkartabilir. Truva atları yetkilendirilmemiş bir yol ile sistemi etki altına almak için yazılmıştır. Sistemlerin güncelleştirilmesi için kullanılan yazılımlar merkezi olarak dağıtılmakta ve internet üzerinden herhangi bir güncelleştirme işlemi yapılmamaktadır. Bu yüzden

kullanılan yazılımlar güvenli olup, sistemlere şu ana kadar herhangi bir zarar vermemiştir. Merkezi olarak temin edilen yazılımlar üretici firmalardan ücreti karşılığında satın alındığından içlerinde truva atları gibi zarar verici yazılımlar bulunmamaktadır.[111]

3.2.9. İş Devamlılığı Yönetimi

İş devamlılığı ile ilgili olarak yönetilen süreçte, Belli zaman periyodu içerisinde yapılan işler ayrıca kayıt altına alınarak daha sonraki analizlerde kullanılmaktadır. Örgüt içerisinde bu tip uygulamalar "çıkarılan dersler" adı altında değerlendirilmektedir. Ortaya çıkan her bir sorun için düzeltici işlemler yapılmakta, kısa vadede düzeltilemeyen problemler için uzun vadeli planlama yapılarak uygun hal tarzları ile çözümlenmektedir.

İş süreçlerinin kesintiye uğramasına sebebiyet verebilecek olaylar gerçekleşme ihtimallerine göre sınıflandırılmaktadır. Her bir olay için alınacak tedbirler ayrı ayrı belirlenip acil durumlar uygulama planına ithal edilmektedir. Mevcut yapılandırma ile giderilmesi mümkün olmayan riskler için ayrıca bütçe planlanmakta ve bu bütçe bir sonraki yıla bırakılmadan kullanılmaktadır.

İş süreçlerini kesintiye uğratacak beklenmeyen acil durumlarda hareket tarzları belirlenmiş olup, gerektiğinde personelin ve teçhizatın tahliyesine kadar varan tatbikatlar yapılmaktadır. Her tatbikatı takiben çalışanlar, normal duruma geçmekte karşılaştıkları zorlukları ilgili birimlere bildirmektedir. Bu sayede planlar güncelleştirilmektedir.

İş devamlılığının ana çatısını örgütün tanımlanmış vazife analizleri oluşturmaktadır. Her bir görevin hangi birim tarafından yapılacağı görev tanım formlarında belirtilmiş olup, düzenli olarak yapılan tatbikatlarda ortaya çıkan durumlar

---

[111] Detaylı bilgi ve uygulama soruları için bakınız "EK-9 Sistem Geliştirme ve Bakım Kontrol Listesi ve Elde Edilen Bulgular".

görev analiz birimi personeli tarafından değerlendirilmeye tabi tutulmaktadır. Bu sayede sistemin aksayan yönleri ortaya çıkartılarak, düzeltici işlemlerin hangi birimler tarafından yapılacağı tanımlanmaktadır.

İş devamlılık planlarının etkin ve güncel olarak tutulması için diğer örgütlerden gelen ilave personelin tespit ettiği aksaklıklar ayrı bir analize tabi tutulmaktadır. Bu sayede örgüt içerisinde farkına varılamayan aksaklıklar ortaya çıkartılmaktadır. Buna benzer uygulamalar çapraz eğitim olarak adlandırılmaktadır.[112]

3.2.10. Uyum

Yasalara uyumla ilgili olarak, ihtiyaçları karşılamaya yönelik kişisel sorumluluklar ve özel kontroller tanımlanmış ve belgelenmiştir. Kanunların ilgili maddeleri yönergelere ithal edilmiş olup, kullanıcıların sorumlu oldukları hususlar, açık ve net bir biçimde belirlenmiştir. Bu konuyla ilgili düzenleyici maddeler, denetleme kontrol listesi haline getirilmiştir.

Örgütün sahip olduğu bilgi sistemleri üzerinde lisanssız herhangi bir yazılımın kullanılmasına müsaade edilmemektedir. Kullanıcı istekleri doğrultusunda yüklenecek yazılımların lisans belgesi ibrası talep edilmektedir. Telif hakları, tasarım hakları ve ticari haklar gibi fikri mülkiyet hakları (IPR - Intellectual Property Rights) bağlamında materyalin kullanımı ile ilgili yasal kısıtlamalara uyumu temin edecek yöntemler istisnasız uygulanmaktadır.

Örgüt tarafından kullanılacak bütün yazılımlar, merkezi olarak temin edilmekle beraber, istisnai durumlarda, ihtiyaç duyulan yazılım ticari piyasadan lisanslı olarak satın alınmaktadır. Örgütün eline ulaşan bütün yazılımlar, ilk kullanımdan önce kopyalanarak yedeklenmektedir. Dijital ortamda bulunan bütün kayıtlar da düzenli

---

[112] Detaylı bilgi ve uygulama soruları için bakınız "EK-10 İş Devamlılığı Yönetimi Kontrol Listesi ve Elde Edilen Bulgular".

olarak yedeklenmektedir. Diğer, basılı evrak, önemine binaen ilgili birimlerce fotokopi ile çoğaltılarak saklanmaktadır.

Kişisel bilgilerin gizliliği ve korunmasına yönelik yönetimsel yaklaşımda, genel olarak örgütle ilişkisi olmayan kişisel bilgilerin hassas bilgi sistemlerinde saklanmasına müsaade edilmemektedir. Ancak resmi manadaki kişisel bilgiler, sadece idari kısım personeli ve kişinin kendisi tarafından işlem görecek şekilde saklanmaktadır.

Bilgi işlem kolaylıklarının sadece örgütün resmi amaçlarına hizmet eden alanlarda, kullanılacağı, örgüt politikası olarak yönergelere işlenmiştir. Yönergelerin uygulanması en üst örgüt yönetimi tarafından zaman zaman denetlenmektedir.

Her sisteme giriş esnasında ekranda girilen sistemin hassas bilgi içeren bir sistem olduğu ve yetkisiz kullanımına müsaade edilmediği açık bir biçimde uyarı mesajı ile gösterilmektedir.

Kriptografik kontrol düzenlemeleri bölgesel ve milli mutabakata uymaktadır. Kriptografik kontroller yılda en az bir defa olmak üzere yapılmaktadır. Bu kontroller örgütün bağlı olduğu, daha üst kademelerce hazırlanmış yönerge esaslarına göre yapılmaktadır. Bu yönergeler, uluslar arası mutabakata dayanan standartlara göre hazırlanmıştır.

Güvenlik politikalarına uyum tamdır. Bütün denetleme, gözden geçirme ve yeniden değerlendirme işlemleri bilgi güvenliği politikası ve stratejisi paralelinde yapılmaktadır. Bilgi güvenliğini oluşturan politikalar, teknolojik gelişmelere uygun olarak yılda bir defa gözden geçirilerek güncellenmektedir.

Teknik uyumluluk kontrolleri yetkili ve uzman personelin kendisi tarafından veya bu personelin yönetimi altındakiler tarafından yapılmaktadır. Herhangi bir bilgi sistemi alınmadan önce kullanılacak bölgenin koruma seviyesine göre incelemeye tabi tutulmaktadır. Örgütün bulunduğu bölge bilgi güvenliği açısından tam korumalı alan olduğundan dolayı satın alınacak teçhizatta herhangi bir kısıtlama yoktur. Ancak herhangi bir intikal durumunda gidilecek bölgenin koruma durumuna göre alınacak teçhizat ayrıca belirlenmektedir. Tam korumalı olmayan bölgelerde kullanılacak

teçhizat tavsiye edilen ürün listesinden seçilmek zorundadır. Tavsiye edilen ürün listesinde bulunmayan bir teçhizat alınmak istendiğinde, merkezi kontrol birimine gönderilerek gerekli tetkiklerinin yapılması sağlanmaktadır.[113]

3.3. UYGULAMA SONUÇLARI

Elde edilen bulgular incelendiğinde üzerinde çalışma yapılan ağ sistemlerinin oldukça güvenli bir yapıya sahip olduğu uluslararası standartlara uygun olarak tasarlandığı ve işletildiği görülmektedir. Hazırlanan yönerge, kontrol listeleri ve uygulama rehberleri bilgi güvenliğini sağlayacak yeterliliktedir.

Bu standartların uygulanabilmesi için gereken güvenlik ihtiyaçları organizasyonun birinci öncelikli harcama kalemleri arasında bulunmaktadır. Güvenlik politikası ve stratejisi kapsamında tespit edilen tüm altyapı, donanım ve yazılım ihtiyaçları, ivedilikle karşılanmaktadır. Bilgi güvenliği ile ilgili olarak alınması veya uygulanması gereken unsurlar organizasyonun bağlı olduğu bir üst birime gönderilmekte, burada değerlendirilmekte ve en seri şekilde sonuçlandırılmaktadır.

Organizasyon bilgi güvenliği yönetimi anlamında da yüksek seviyede bir yapılanma sergilemektedir. Bütün yöneticiler ve organizasyon çalışanları bilgi güvenliği hassasiyetinin farkındadır. Yürürlükteki kurallar ve uygulamalar çalışanlara büyük sorumluluklar yüklemekte ve güvenlik konusunda kesinlikle taviz verilmemektedir. Güvenlik ile ilgili denetlemeler titizlikle yapılmakta, kontrol listelerinde bulunan tüm maddeler en ince ayrıntısına kadar aranmaktadır. Bu sayede örgütün bilgi güvenliği politikaları ve bu politikaların uygulanması, bir üst birimin denetim mekanizması tarafından doğrulanarak kontrol altında tutulmaktadır.

Bilgi güvenliği konusunda organizasyon açısından dezavantaj olarak değerlendirilen konular şu şekilde sıralamak mümkündür:

---

[113] Detaylı bilgi ve uygulama soruları için bakınız "EK-11 Uyum Kontrol Listesi ve Elde Edilen Bulgular".

Organizasyon çok kozmopolit bir yapı sergilemektedir. Çalışanların tamamının güvenlik kleransları olmakla birlikte, örgütsel anlamda bir personel seçimi yapılamamaktadır. Organizasyonda çalışacak personelin kimler olacağına uluslar arası anlaşmalar paralelinde katılımcı ülkeler karar vermektedir. Bu durum organizasyon yapısı içerisinde her zaman istenilen kalitede personel istihdamını mümkün kılmamaktadır. Personel istihdamı ile ilgili diğer bir konu ise organizasyon çalışanları, mensubu oldukları ülke politikaları uyarınca belirli rotasyonlar halinde görev yapmaktadırlar. Belirli rotasyon süreleri içerisinde görev yapan personelin örgüt kültürünü ve politikalarını benimsemeye yetecek kadar süreye sahip olmamaları, yapılan işin miktarı ve kalitesi üzerinde olumsuz etki yapmaktadır.

Örgüt içindeki teknolojik altyapı, ağ sistemleri ve bileşenleri, uluslar arası güvenlik standartlarını karşılayacak seviyededir. Uygulama sonuçları göz önüne alındığında ağ bilgi güvenliğinin yönetimi ile ilgili şu önerilerde bulunulabilir;

- Bilgi güvenliği konularını kapsayan günlük faaliyetler için detaylı kontrol listeleri hazırlanmalıdır.

- Hazırlanan kontrol listelerinin değişen şartlara ve ihtiyaçlara göre sürekli güncellenmesi sağlanmalıdır.

- Kontrol listelerinin bilgi güvenlik personeli tarafından uygulanıp uygulanmadığı, bir üst yönetim kademesi tarafından kontrol edilmelidir.

- Bilgi güvenlik personeli tarafından periyodik kontrollerle bilgi güvenliği denetlenmeli ve sonuçları kayıt altına alınmalıdır.

- Kontrol sonuçları, mütemadiyen analiz edilerek, yeniden değerlendirmeye tabi tutulmalıdır.

- Bilgi güvenlik personeli güncel değişiklikleri yakından takip etmelidir.

- Değişen durumlara uyum süreci hızlandırılmalıdır.

- Organizasyon çalışanları bireysel ve toplu olarak bilgi güvenliği eğitimine tabi tutulmalı, her an müteyakkız olmaları sağlanmalıdır.

Sonuç olarak, örgüt yapısı içerisinde teknolojik anlamda bilgi güvenliğini sekteye uğratacak açık bir noktaya rastlanmamakla birlikte, bilgi güvenliğini zafiyete uğratacak unsurlar içerisinde insan kaynaklarının ön plana çıktığı görülmüştür. Bu durumun şimdiye kadar önemli bir probleme yol açmadığı ancak, bilgi güvenliğinde önemli bir risk alanı olduğu değerlendirilmiştir.

SONUÇ VE GENEL DEĞERLENDİRME

Bilgi toplumuna geçiş sürecinde, işletmelerde bilgiye sahip olma, bilgi üretme / geliştirme, bilgiyi kullanabilme ve bilgiyi koruyabilme, bilgi sürecinin kritik faktörleri olarak ortaya çıkmıştır. Yapılan çalışmada, bu bilgi sürecinin son boyutu olan "bilginin korunması" konusu üzerinde durulmuş, bu kapsamda işletmelerin ağ bilgi sistemlerinde ağ bilgi güvenliğinin yönetimi incelenmiştir. Öncelikle ağ sistemleri ve ağ sistemlerinde güvenlik konuları vurgulanmış, daha sonra bu konular yönetim süreçleriyle birleştirilmiştir. NATO CAOC 6 Komutanlığında yapılan uygulama, literatür taramasından elde edilen sonuçları destekler niteliktedir.

Tez çalışmasının hipotezleri, çalışma sonuçları paralelinde analiz edilmiş ve aşağıdaki değerlendirmelere ulaşılmıştır.

H_{10}: Gelişen teknolojiler ile daha karmaşık bir yapıya bürünen bilgi güvenliği ihtiyacı, bütünsel bir bilgi güvenliği yönetimini gerektirmektedir.

Teknolojinin gelişmesi, ağ sistemlerinin oldukça karmaşık bir hale gelmesini sağlamıştır. Ağ ve bilgi teknolojileri karşısındaki tehdit ise aynı paralelde artış göstermiştir. Çalışmanın birinci bölümünde muhtemel risk alanlarını ortadan kaldırmak veya en aza indirmek için gerekli olan örgüt yapılanması ortaya konmuştur. Yönetim yaklaşımları ise ikinci bölümde ele alınmıştır. Yapılan uygulamada, CAOC 6 Komutanlığının ve bağlı bulunduğu diğer NATO karargahlarının, görev ve sorumluluklarını yerine getirebilmek amacıyla, gelişen teknolojiyi yakından takip ederek organizasyon bünyesine adapte ettiği görülmüştür. Bu değişime ayak uydurma sürecinde, bilgi güvenliğine tehdit teşkil eden en büyük riskin koordinasyon eksikliği olduğu belirlenmiştir. Bilgi güvenliğinin birbirine bağlı halkalardan oluştuğu ve en zayıf halkası kadar güçlü olduğu ve birimler arasındaki koordinasyonun, bütünsel yönetim yaklaşımını temin edecek en önemli unsur olarak ortaya çıktığı görülmüştür. Bu nedenle NATO Komuta kademelerinde yüksek seviyede koordine sağlanabilen bir yönetim yapısı oluşturularak, sözü edilen risk alanı minimum seviyede tutulmuştur. Alan çalışmasıyla da, gelişmiş ağ sistemleri üzerindeki bilgi güvenliğinin değerlendirilmesi

sonucunda sadece bütünsel bir güvenlik yönetiminin, arzu edilen güvenlik kriterlerini sağlayabileceği sonucuna ulaşılmıştır. Böylece elde edilen bulgular doğrultusunda H_{10} hipotezi kabul edilerek H_{11} hipotezi reddedilmiştir.

H_{20}: İşletmelerde ağ bilgi güvenliği ile ilgili tedbirlerin alınabilmesi için ağ yapısına olabilecek tehditlerin neler olduğu bilinmeli ve işletme için kapsamlı bir risk analizi yapılmalıdır.

Ağ'daki hassas bilgi, ağ bilgi güvenliği yönetiminin en öncelikli konusudur. Tehditler ise gün geçtikçe artmaktadır. Bu tehditlerin neler olduğu, öncelikle sistem yöneticileri ve bilgi güvenlik sorumluları tarafından bilinmelidir. Bütün ağ tehditlerine karşı önlem almaya çalışmak ise hem gereksiz, hem de mali olarak imkansız bir durum sergilemektedir. Bu yüzden işletmenin muhtemel risk alanlarının bir profili çıkartılmalıdır. Kapsamlı risk analizi gereksiz maliyetleri ve gayret sarfını önlemektedir. Risk analizi, işletme kaynaklarının ve gayretinin teksif edileceği bir önceliklendirilmiş liste oluşturulmasına yardımcı olmaktadır. CAOC 6 Komutanlığında yapılan uygulamada bilgi güvenliği personelinin risk analizi yöntemiyle muhtemel tehditlerin neler olabileceğini uygun bir şekilde tanımladığı ve gerekli önlemleri aldığı tespit edilmiştir. Tehditlerin belirlenmesiyle birlikte, ilgili persoenlin tehdidin muhteviyatı konusunda araştırma yaptığı ve bu paralelde gerekli önlemleri saptayarak etkili bir şekilde uyguladığı görülmüştür. Bu kapsamda literatür taraması ve uygulama sonuçlarından elde edilen veriler paralelinde H_{20} hipotezi kabul edilerek H_{21} hipotezi reddedilmiştir.

H_{30}: Hassas bilgi içeren ağlara sahip olan işletmeler, organizasyon yapılarında bilgi güvenliği yönetim süreçlerini göz önüne alarak, uygun bir organizasyon yapısı oluşturmalıdır.

Organizasyonun yapılanması bilgi güvenliğinin önem arz eden bir diğer boyutudur. Bilgi güvenliği yönetiminin en etkin şekilde uygulanabileceği organizasyon yapıları çalışma içerisinde incelenmiştir. Bu paralelde organizasyonlar kurulurken veya yeniden yapılanırken bilgi güvenliği yönetim mekanizması oluşturulmalı ve etkinliği sağlanmalıdır. Bu durum bütünsel güvenlik yaklaşımının gereğidir. Uygulama yapılan

CAOC 6 Komutanlığında dikey bir hiyerarşik yapı bulunmasına karşın, bilgi güvenliği yönetimiyle ilgili yatay bir yapı oluşturulduğu görülmüştür. Bu sayede görev ve sorumluluklar organizasyon çalışanları arasında uygun bir şekilde paylaştırılarak, haberleşme kanalları etkin olarak çalıştırılmıştır. Bütün görevlerin doküman ve yönergelerde açıkça tanımlandığı, yüksek seviyede bir koordinasyonun sağlandığı matriks tipi bir yapılanma uygulanmıştır. CAOC 6'da uygulanan bu yapı neticesinde bilgi güvenliği yönetim süreçleri kesintisiz olarak takip edilmiş ve şimdiye kadar ciddi bir güvenlik ihlali ortaya çıkmamıştır. İfade edilen gerekçelerle H_{30} hipotezi kabul edilerek H_{31} hipotezi reddedilmiştir.

Sonuç olarak, bilginin işletmeler açısından artan önemi ve bilginin korunması için yapılması gerekenler, işletmelerin yönetim kademelerinde yüksek bir teknoloji bilgisi ile yönetim gücünün birleştirilmesini gerekli kılmıştır. Bu doğrultuda, işletmelerin bilgi güvenliği yönetimi süreçlerini oluşturması ve bu süreçleri bütünsel bir yönetim yaklaşımıyla birleştirmesi, artan bilgi tehditleri karşısında en yüksek korumayı sağlayacaktır.

EKLER

EK-1 BS 7799.2 2002 Bilgi Güvenliği Yönetimi Kontrol Listesi Muhteviyatı

EK-2 Güvenlik Politikası Kontrol Listesi ve Elde Edilen Bulgular

EK-3 Örgütsel Güvenlik Kontrol Listesi ve Elde Edilen Bulgular

EK-4 Varlıkların Sınıflandırılması ve Kontrolü Kontrol Listesi ve Elde Edilen Bulgular

EK-5 Personel Güvenliği Kontrol Listesi ve Elde Edilen Bulgular

EK-6 Fiziksel ve Çevresel Güvenlik Kontrol Listesi ve Elde Edilen Bulgular

EK-7 Haberleşme ve İşletim Yönetimi Kontrol Listesi ve Elde Edilen Bulgular

EK-8 Erişim Kontrolü Kontrol Listesi ve Elde Edilen Bulgular

EK-9 Sistem Geliştirme ve Bakım Kontrol Listesi ve Elde Edilen Bulgular

EK-10 İş Devamlılığı Yönetimi Kontrol Listesi ve Elde Edilen Bulgular

EK-11 Uyum Kontrol Listesi ve Elde Edilen Bulgular

BS 7799.2 2002 Bilgi Güvenliği Yönetimi Kontrol Listesi Muhteviyatı

EK-2	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Güvenlik Politikası			
1.1	***Bilgi Güvenliği Politikası***		
1.1.1	Bilgi güvenliği politikası dokümanları	Bütün çalışanlar tarafından uygun şekilde anlaşılmış ve yönetim tarafından onaylanarak yayınlanmış "Bilgi Güvenliği" politikası var mıdır? Bilgi güvenliği yönetiminde organizasyonel yaklaşım ve yönetim kararlılığı var mıdır?	Bilgi güvenliği politikası mevcut olup, personel tarafından titizlikle uygulanmaktadır. Bilgi güvenliği ile ilgili aksaklıklar en üst yönetim seviyesinde ele alınarak mutlak çözüme ulaştırılmaktadır.
1.1.2	Gözden geçirme ve değerlendirme	Güvenlik politikasını tanımlanmış gözden geçirme işlemlerine göre gözden geçiren ve idamesini sağlayan ve sorumlu olan bir sahibi var mıdır? Gözden geçirme işlemleri asli değerlendirmeye temel teşkil edecek şekilde yapılmakta mıdır? Örneğin: Önemli güvenlik olayları, yeni zafiyetler, organizasyonel veya teknik altyapı ilişkin değişiklikler.	Güvenlik politikası Karargah Güvenlik subayı tarafından düzenli bir şekilde gözden geçirilmektedir. Konu ile ilgili olarak üst komutanlıklarca yılda bir defa güvenlikle ilgili görev ve sorumluluğu bulunan personel denetlenmektedir.

EK-3	Bilgi Güvenliği Yönetimi BS 7799 2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Örgütsel Güvenlik			
2.1	***Bilgi Güvenliği Altyapısı***		
2.1.1	Bilgi güvenliği forumunun yönetimi	Örgüt içersinde yönetim forumunu sağlayacak ve güvenlik inisiyatifini destekleyen açık ve anlaşılır bir yönetim desteği var mıdır?	Bilgi güvenliği örgüt içersinde olmazsa olmaz yaklaşımı ile ele alınmakta ve güvenli olmayan hiçbir sistem ve yöntem kullanılmamaktadır. Bu konudaki aksaklıklar yönetim kademesine bildirildiğinde öncelikle çözüm bulunmaktadır.
2.1.2	Bilgi güvenliği eşgüdümü	Bilgi güvenliği kontrollerinin eşgüdümünde ilgili birim temsilcileri arasında çapraz kontrol var mıdır?	Bilgi güvenliği ile ilgili olarak Karargah Güvenlik Subayının altında ona karşı sorumlu olarak çalışan her branştan ilgili bir personel bulunmaktadır. Bu kişiler düzenli olarak toplantı yapmakta ve bilgi sistemleri kullanıcılarına uyarıcı hatırlatmalarda bulunmaktadır.
2.1.3	Bilgi güvenliği sorumluluklarının tahsisi	Her bir varlığın korunmasında sorumluluklar ile özgün güvenlik işlemleri açıkça tanımlanmış mıdır?	Her bir Bilgi Sisteminin korunmasından sorumlu ilgili bilgi sistemi Yerel Alan Ağı güvenlik sorumlusu bulunmaktadır. Bu kişiler Çalışma Sahası Güvenlik Subayları ile eşgüdüm içersinde çalışmaktadırlar.

EK-2 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi

İlgi Denetleme sahaları, amaç ve sorular

Kontrol Listesi	Bölüm	Denetleme Sorusu	Bulgular
2.1.4	Bilgi işleme kolaylılarında yetkilendirme süreçleri	Yeni bilgi işleme kolaylıklarının yetkilendirme süreç yönetimi var mıdır? Bu bütün yazılım ve donanım kolaylıklarını kapsamalıdır.	Yeni bir bilgi sistemi kurulmadan önce sistemin yapısını ve bağlantılarını açık bir şekilde ifade eden ve güvenli bir sistem olduğunu belirten kontrol listeleri onaylanarak bir üst makama yetki için başvurulmaktadır. Buna Güvenlik Akreditasyonu denilmektedir. Üst makamlarca ilgili gizlilik seviyesine uygun olduğu onaylanırsa sistemin kurulmasına ve ilgili Geniş Alan Şebekesine bağlanmasına müsaade edilmektedir.
2.1.5	Bilgi güvenliği uzmanları	Uygun olan birimlerde bilgi güvenliği ile ilgili uzman bir danışman var mıdır? Bunun için belirli bir şahıs dahili bilgi birikimini ve tecrübeleri eşgüdümlemek için görevlendirilir ve güvenlik ile ilgili kararların alınmasında yardımcı olur.	Her bir birimin Çalışma Alanı Güvenlik Subayı kısmen uzman kişilerden seçilerek bunlara özel eğitim verilmektedir. Bunlar Yerel Alan Ağı güvenlik Subayı, Bilgi Güvenliği Subayı, Haberleşme Güvenliği Subayı gibi konu üzerinde daha fazla uzman olan personel ile beraber eşgüdüm içersinde çalışmaktadır.
2.1.6	Örgütler arasında işbirliği	Herhangi bir güvenlik olayında hızlıca uygun eyleme geçilmesini sağlayacak ve tavsiyede bulunacak haberleşme uzmanları, bilgi hizmeti sağlayıcıları, düzenleyici kimseler ile kanun uygulayıcıları ile uygun temaslar mevcut mudur?	Bu sahalarla ilgili personel mevcut olup, bilgi ve tecrübeleri yetersiz kaldığında daha üst komutanlıklarda bulunan uzman personele başvurulmaktadır. Ayrıca askeri yapının haricinde varolan ilgili uzmanlarla bağlantılar mevcuttur.
2.1.7	Bilgi güvenliğinin bağımsız denetimi	Bilgi güvenliği politikalarının yerine getirilip getirilmediği bağımsız bir şekilde düzenli olarak kontrol edilmekte midir? Bu örgütsel uygulamaların uygun bir şekilde politikalara yansıtılması için sigorta görevi görür, uygulanabilirdir ve	Konu ile ilgili olarak rasgele zamanlarda kontroller yapılmakta ve aksaklıklar sabah toplantılarında gündeme getirilmektedir.

EK-3 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi

İlgi Denetleme sahaları, amaç ve sorular

Kontrol Listesi	Bölüm	Denetleme Sorusu	Bulgular
2.1.4	Bilgi işleme kolaylılarında yetkilendirme süreçleri	Yeni bilgi işleme kolaylıklarının yetkilendirme süreç yönetimi var mıdır? Bu bütün yazılım ve donanım kolaylıklarını kapsamalıdır.	Yeni bir bilgi sistemi kurulmadan önce sistemin yapısını ve bağlantılarını açık bir şekilde ifade eden ve güvenli bir sistem olduğunu belirten kontrol listeleri onaylanarak bir üst makama yetki için başvurulmaktadır. Buna Güvenlik Akreditasyonu denilmektedir. Üst makamlarca ilgili gizlilik seviyesine uygun olduğu onaylanırsa sistemin kurulmasına ve ilgili Geniş Alan Şebekesine bağlanmasına müsaade edilmektedir.
2.1.5	Bilgi güvenliği uzmanları	Uygun olan birimlerde bilgi güvenliği ile ilgili uzman bir danışman var mıdır? Bunun için belirli bir şahıs dahili bilgi birikimini ve tecrübeleri eşgüdümlemek için görevlendirilir ve güvenlik ile ilgili kararların alınmasında yardımcı olur.	Her bir birimin Çalışma Alanı Güvenlik Subayı kısmen uzman kişilerden seçilerek bunlara özel eğitim verilmektedir. Bunlar Yerel Alan Ağı güvenlik Subayı, Bilgi Güvenliği Subayı, Haberleşme Güvenliği Subayı gibi konu üzerinde daha fazla uzman olan personel ile beraber eşgüdüm içersinde çalışmaktadır.
2.1.6	Örgütler arasında işbirliği	Herhangi bir güvenlik olayında hızlıca uygun eyleme geçilmesini sağlayacak ve tavsiyede bulunacak haberleşme uzmanları, bilgi hizmeti sağlayıcıları, düzenleyici kimseler ile kanun uygulayıcıları ile uygun temaslar mevcut mudur?	Bu sahalarla ilgili personel mevcut olup, bilgi ve tecrübeleri yetersiz kaldığında daha üst komutanlıklarda bulunan uzman personele başvurulmaktadır. Ayrıca askeri yapının haricinde varolan ilgili uzmanlarla bağlantılar mevcuttur.
2.1.7	Bilgi güvenliğinin bağımsız denetimi	Bilgi güvenliği politikalarının yerine getirilip getirilmediği bağımsız bir şekilde düzenli olarak kontrol edilmekte midir? Bu örgütsel uygulamaların uygun bir şekilde politikalara yansıtılması için sigorta görevi görür, uygulanabilirdir ve	Konu ile ilgili olarak rasgele zamanlarda kontroller yapılmakta ve aksaklıklar sabah toplantılarında gündeme getirilmektedir.

EK-3 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
		etkindir.	
2.2	***Üçüncül şahısların güvenliği***		
2.2.1	Üçüncül şahıs erişimlerinden gelen riskin tanımlanması	Üçüncül şahısların erişimleri tanımlanmış mıdır ve uygun güvenlik kontrolleri yapılmakta mıdır? Erişim sebepleri belirlenmiş midir? Örgüt içinde çalışan üçüncül firmalar ile ilgili güvenlik riski tanımlanmış mıdır ve uygun kontroller yapılmakta mıdır?	Üçüncül şahısların kontrollü sistemlere direk erişimi mümkün değildir. Sadece bakım sözleşmesi imzalanan firmalar idarenin kontrolü altında, idarenin isteği üzerine sistemlere müdahale edebilmektedirler.
2.2.2	Üçüncül şahıs sözleşmelerinde güvenlik ihtiyacı	Üçüncül şahıslar ile ilgili örgütsel güvenlik politikalarını ve standartlarını kapsayan güvenlik ihtiyaçlarını temin eden resmi sözleşme var mıdır?	Kontrollü sistemlerin bakımlarının yapılması için yapılan sözleşmelerin içerisinde üçüncül şahısların idarenin güvenlik kurallarına kayıtsız şartsız uyacağı belirtilmektedir.
2.3	***Dış Kaynak Kullanımı***		

EK-3 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
2.3.1	Dış kaynak kullanım sözleşmelerinde güvenlik ihtiyacı	Örgüt bilgi sistemlerinin, ağların ve/veya masaüstü bilgisayarların yönetimini ve kontrolünü başka dış bir firmaya yaptırdığında güvenlik gerekleri üçüncül şahıslara adreslenmekte midir? Sözleşme yasal gereklerin nasıl karşılanacağını, örgütsel varlıkların güvenliklerinin nasıl idame ettirileceğini ve test edileceğini, denetleme haklarını, fiziki güvenlik konularını ve herhangi bir afet anında servis imkanlarının nasıl idame ettirileceğini ifade etmelidir.	Üçüncül şahıslar özellikle kontrollü sistemlerde, nezaretçisiz işlem yapamamaktadırlar. Sözleşmede güvenlikle ilgili konular yer almakta ve üçüncül şahıslar bu gerekçelere uyacaklarını beyan etmektedirler. Harici bilgisayar hafızalarının içerisinde bulunan hiçbir bilgi örgüt dışına üçüncül şahıslar tarafından çıkartılamaz. Ancak sistemlerin bilgi depolayan kısımları hariç diğer parçaları, arıza olduğunda tamir için üçüncül şahıslarca izne binaen çıkartılabilir.

EK-4	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Varlıkların sınıflandırılması ve kontrolü			
3.1	***Varlıkların sorumluluğu***		
3.1.1	Varlıkların demirbaş listesi	Her bir bilgi sistemi için önemli varlıklarla ilgili demirbaş listesi veya kayıt defteri tutulmakta mıdır? Her bir varlığın belirlenmiş bir sahibi var mıdır, mutabık kalınmış ve tanımlanmış güvenlik sınıflandırması ve yeri belirlenmiş midir?	Bütün sistemlerin önemli parçalarının seri numaraları ayrı bir demirbaş listesi olarak tutulmaktadır. Her bir sistemin sorumlu personeli belirlenmiş olup, üzerinde etiketle gösterilmektedir. Sistemlerin yeri ilgili birimin izni ve onayı alınmadan değiştirilememektedir. Bütün sistemlerin üzerinde güvenlikle ilgili gizlilik derecesi sınıflandırması gözle görülebilecek şekilde etiketlenmiştir.
3.2	***Bilgilerin sınıflandırılması***		
3.2.1	Sınıflandırma rehberleri	Bilgilerin nasıl işlem göreceğinin ve korunacağının belirlenmesine yardımcı olacak Bilgi sınıflandırma şeması veya rehberi var mıdır?	Her kurulacak bilgi sistemi kurulmadan önce hangi gizlilik seviyesine sahip olacağı bir üst yönetim kademesinin onayı ile belirlenmektedir. Bilgi sınıflandırmasının nasıl yapılacağına dair yönergeler mevcuttur. Sistemlerin kurulmasından sorumlu olan birimler bu rehberin uygulanmasından da sorumludur.

EK-4 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
3.2.2	Bilgilerin etiketlenmesi ve işlenmesi	Örgüt tarafından uyarlanmış sınıflandırma şemasına uyan bilgi işleme ve etiketleme için uygun yöntemler var mıdır?	Belirli bir gizlilik seviyesinin üzerine çıkan harici hafıza üniteleri (Harddisk, Disket, CD vb.) özel kontrol numaraları ile kayda alınmaktadırlar. Belirli bir gizlilik seviyesinin altındaki harici hafıza üniteleri için kayıt işlemi uygulanmaz ancak hangi gizlilik derecesine kadar bir bilgi ihtiva ettikleri üzerlerindeki etiketle gösterilir. Ağ'da bulundurulan bilgiler için gizlilik tasnifi yapılmaktadır. E-posta uygulama yazılımı, kullanıcıları yeni ileti oluşturulduğunda gizlilik derecesi seçimine zorlamaktadır.

EK-5	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Personel Güvenliği			
4.1	***Görev tanımlarında bulunan güvenlik ve kaynaklandırma***		
4.1.1	Güvenliğin görev tanım formlarına işlenmesi	Örgütün bilgi güvenliği politikasında bulunan güvenlik rolleri ve sorumlulukları uygun bir şekilde yazıya dökülmüş müdür? Bu belirli varlıkların korunmasına özgün veya güvenlik faaliyetlerinin genişletilmesine ait sorumlulukları kapsadığı gibi güvenlik politikalarının yerine getirilmesi veya idame ettirilmesini de kapsamalıdır.	Bilgi güvenliği ile ilgili örgüt için organizasyon şeması oluşturulmuş olup, her görev tanımı ile ilgili yapılacak işlerden kimin sorumlu olduğu belirlenmiştir. Sorumluluklar örgüt içerisindeki en üst yetkili tarafından kendilerine tebliğ edilmiştir.
4.1.2	Personelin gözlenmesi ve politika	Sürekli çalışan personele iş sırasında dikkat edilerek güvenlik tasdikleri takip edilmekte midir? Bu ahlaki eğilimleri, teyit edilen akademik ve profesyonel niteliklerini ve bağımsız kimlik kontrollerini kapsamalıdır.	Sürekli çalışan personelin hangi seviyedeki bilgilere haiz olacakları güvenlik kleransı ile belirlenmektedir. Kişilerin bu kleranslara uyup uymadıkları düzenli olarak kontrol edilmektedir.
4.1.3	Gizlilik mutabakatı	Çalışanlara gizlilik mutabakatı ve sırları ifşa etmeme belgesi işe başlama şartı olarak bildiriliyor (imzalatılıyor mu) mu?	Çalışanlara örgüte katılım belgeleri içerisinde gizlilik kurallarına uymaları ile ilgili güvenlik belgesi imzalatılmaktadır. Bu belge her 6 ayda 1 kendilerine yeniden tebliğ edilmektedir.

Ek-5	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
4.1.4	İşe başlama şartları	İşe başlama şartları çalışanların bilgi güvenliği ile ilgili çalışanın sorumluluklarını kapsıyor mu? Duruma göre bu sorumluluk çalışan işi bıraksa bile belli bir süre daha devam edebilir.	İstenilen gizlilik seviyesindeki kleransa haiz olmayan kimselerin işe başlamaları mümkün değildir. Personelin işten ayrılması bilgi saklama sorumluluğunu değiştirmez. Bu durum özel kanunlarla korunmaktadır.
4.2	***Kullanıcı Eğitimi***		
4.2.1	Bilgi güvenliği eğitimi	Örgüt içindeki bütün kullanıcılar ile üçüncül şahıslar uygun Bilgi Güvenliği eğitimi alıyorlar mı ve örgütsel politika ve yöntemler hakkında güncelleniyorlar mı?	Örgüte yeni katılan personele ilk katılış brifingi sırasında bilgi güvenliği ile ilgili bilgi verilmektedir. Bilgi güvenliğine ait diğer detaylı eğitim ise örgüt çapında üç ayda bir yapılan periyodik eğitim ve seminerlerle verilmektedir. Üçüncül şahıslar örgüt içerisinde bulundukları sürece yapacakları işlemlerle ilgili eğitim almaktadırlar. Bu eğitim bilgi güvenliğini de kapsamaktadır.
4.3	***Güvenlikle ilgili olaylarının ve arızaların cevaplanması***		
4.3.1	Güvenlikle ilgili olayların rapor edilmesi	Güvenlik olaylarının uygun yönetim kademesi vasıtasıyla mümkün olan en kısa zamanda bildirildiği resmi yöntemler var mıdır?	Hangi güvenlik olayının hangi rapor formatı ile bildirileceği ve karşılığında ne gibi işlemler yapılacağı yönergelerde yer almaktadır.
4.3.2	Güvenlik zafiyetlerinin bildirilmesi	Güvenlik zafiyetlerinin veya sistem ve hizmetlere karşı olan tehditlerin kullanıcılar tarafından bildirilme yöntemi veya rehberi var mıdır?	Örgüt içi haberleşme kanalları ile sistemlerde oluşabilecek herhangi bir güvenlik zafiyeti ilgili birimlere iletilmektedir.

EK-5	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
4.3.3	Yazılım arızalarının bildirilmesi	Yazılım arızalarının bildirilmesi için yöntemler düzenlenmiş midir?	Yazılımlardaki aksaklıklar örgüt kabiliyeti ile giderilebilecekse muhabere bilgi sistemleri yardım masasında bulunan nöbetçi personele bildirilmektedir. Ancak arızalar, yazılımın yapısı ile ilgili ise yazılımı üreten firmaya veya birime bildirilmesi için özel rapor formatları kullanılmaktadır.
4.3.4	Olaylardan öğrenme	Olayların ve arızaların çeşitlerini, büyüklüklerini ve maliyetlerini ölçen ve gözlemleyen yöntemler mevcut mudur?	Arıza durumunda veya arıza ihtimali oluşturan bir risk durumu tespit edildiğinde maliyet analizi yapılarak, sorunun giderilmesine yönelik çalışmalar yapılmaktadır. Arızanın önem derecesine göre yapılan harcamalar artmaktadır.
4.3.5	Disiplinle ilgili süreçler	Örgütsel güvenlik politikalarını ve yöntemlerini ihlal eden çalışanlar hakkında disiplinle ilgili resmi süreçler var mıdır? Güvenlik yöntemlerini ihmal etmeye eğilimli çalışanları caydırmaya yönelik süreçler gibi.	Vardır. Bu süreç kanunlarla belirlenmiştir. Çok sıkı bir şekilde takibi yapılmaktadır. Bu konuyla ilgili istihbarat birimleri görev yapmaktadır.

EK-6	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Fiziksel ve Çevresel Güvenlik			
5.1	***Güvenli Bölge***		
5.1.1	Fiziksel güvenlik çemberi	Bilgi işleyen cihazlar ne gibi fiziksel olarak sınırlandırılmış güvenli bir yerde bulunmaktadır? Bunlara bazı örnekler; kartlı geçiş kapısı, duvarlar ve nöbetçili resepsiyon gibi...	Örgütün ana giriş kapısında güvenlik personeli tarafından giriş kartı kontrolü yapılmaktadır. Bina girişinde ise manyetik kartlı şifreli geçiş sistemi bulunmaktadır. Örgütün dış sınırları tel örgü ile çevrilmiş olup silahlı güvenlik personeli tarafından 24 saat gözetim altında tutulmaktadır.
5.1.2	Fiziksel giriş kontrolü	Örgüt içersindeki çeşitli alanlara sadece yetkili kişilerin girişine müsaade eden ne gibi kontroller vardır?	Örgüt içinde de manyetik kart sistemi ile bir bölümden diğerine geçiş yapılmaktadır. Kartların yetki seviyesi bir merkez tarafından kontrol edilmektedir.
5.1.3	Çalışma odalarının ve binaların güvenli hale getirilmesi	Bilgi işleyen cihazların bulunduğu odalarda kilit, kilitlenebilir dolap veya emniyetli kasalar var mıdır? Bilgi işleyen cihazlar doğal ve insani felaketlerden korunmakta mıdır? Komşu bina ve arazilerden kaynaklanan muhtemel tehditler var mıdır?	Bilgi işleyen hassa cihazların bulunduğu bölgelerde elektronik şifreli kapılar bulunmakta ve haricen kilitlenmektedir. Özel bilgi ve yüksek gizlilik derecesine haiz materyal üç kombineli şifreli çelik kasalarda muhafaza edilmektedir. Örgüt binası, örgütün faaliyet gösterdiği alan ile doğru orantılı olarak doğal felaketler ile savaş tehlikesine karşı en üst düzeyde korumaya sahiptir.

EK-6	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
5.1.4	Güvenli bölgelerde çalışma	Bilgiler sadece bilmesi gereken kişiler içindir. Güvenli bölgelerde çalışan üçüncül şahıslar veya personel için güvenlik kontrolü yapılmakta mıdır?	Üçüncül şahıslara sadece bilmeleri gerektiği kadar bilgi verilmektedir. Güvenli bölgelerde ise örgüt içinde bir veya daha fazla personel üçüncü şahıslara nezaret etmektedir. Üçüncül şahısların güvenlik kontrolleri, güvenlik birimi tarafından yapılmaktadır.
5.1.5	İzole edilmiş teslimat ve yükleme bölgeleri	Teslimat bölgeleri ve bilgi işleme bölgeleri herhangi bir yetkisiz erişim için birbirlerinden izole edilmişler midir? Bu tip bölgelerde güvenliğin temini için risk değerlendirmesi yapılmış mıdır?	Bilgi işleme bölgeleri güvenli bölgeler olarak tasnif edilmiştir. Dışarıya karşı izolasyonu tamdır. Malzeme giriş çıkışının yapıldığı kapılar hassas bölgelerden uzakta ve kontrol altındadır.
5.2	***Teçhizat Güvenliği***		
5.2.1	Cihaz yerleşim güvenliği	Cihazlar yetkisiz erişimi en aza indirecek çalışma bölgelerine yerleştirilmişler midir? Genel seviye korumasını azaltmak için özel koruma gerektiren cihazlar izole edilmiş midir? Hırsızlık, yangın, patlayıcılar, duman, su, titreşim, kimyasal etkiler, elektrik sağlayan arayüzler, elektromanyetik radyasyon ve su baskını gibi muhtemel tehditlerden kaynaklanan riskleri en aza indirmek için kontroller benimsenmiş midir? Bilgi işleyen cihazların yanında bir şeyler yemek-içmeye ve sigara içmeye karşı bir politika var mıdır? Bilgi işleyen cihazları negatif yönde etkileyecek çevresel	Sunucu ve kripto cihazlarının bulunduğu alan özel bir oda haline getirilmiş, yetkisiz erişimlere tamamen kapatılmıştır. Üç kombineli kilitle muhafaza altına alınmış, duvarlar özel olarak güçlendirilmiştir. Ağa bağlı diğer cihazların bulunduğu yerler, yetkisiz personelin erişimine kapalıdır. 24 saat gözlem altında olmayan alanlarda bulunan hassas bilgiye haiz bilgisayarların hard diskleri mesai saati bitiminden sonra, üç kombineli kilitli çelik kasalarda saklanmaktadır. Mesainin bitiminden sonra bir güvenlik personeli bütün odaları dolaşarak uygun güvenlik önlemlerinin alındığını kontrol etmektedir.

EK-6 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
		şartlar gözlemlenmekte midir?	kontrol etmektedir. Sunucu odalarında bir şeyler yeme-içmeye karşı politikalar geliştirilmiştir. Yedekleme ihtiyacı duyulmayan bilgisayarlar için yeme-içme kontrolü yapılmamaktadır. Sigara içmek bütün binada yasaktır. Yangına karşı fiziki güvenlik önlemi olarak otomatik yangın algılama ve söndürme sistemi bulunmaktadır. Diğer doğal afetlere ve diğer fiziki tehditlere karşı 24 saat görev yapan izleme bölümü bulunmaktadır.
5.2.2	Güç kaynakları	Kesintisiz güç kaynağı, çoklu besleme ve yedek jeneratör gibi sürekli güç kaynakları kullanılarak cihazlar elektrik kesintisinden korunmakta mıdır?	Ağı destekleyen merkezi kesintisiz güç kaynakları şehir cereyanının kesilse bile sistemi beslemeye devam etmektedir. Şehir cereyanının kesilmesini takip eden 15sn. içinde jeneratörler devreye girmekte ve kesintisiz güç kaynaklarının üzerindeki yükü almaktadırlar.
5.2.3	Kablolama güvenliği	Veri taşıyan haberleşme kabloları veya bilgi sistemlerini destekleyen kablolar ile güç kablolarının birbirlerine zarar vermeleri önlenmiş midir? Hassas ve kritik bilgiler için ek güvenlik kontrolleri uygulanmakta mıdır?	Veri taşıyan haberleşme kabloları ile güç kabloları ayrı ayrı kanallar içerisinde bulunmaktadır. Bu kanallar özel metal bir yapıya sahip olup, elektrik ve bilgi kaçaklarını ayrı ayrı topraklara iletmektedirler. Merkezi kesintisiz güç kaynağı belli bir güç seviyesinin üzerinde olduğundan ve güvenli toprağa bağlandığından şehir cereyanı üzerinden

EK-C Bilgi Güvenliği Yönetimi BS 7799:2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			dışarıya bilgilerin kaçışı filtrelenmektedir.
5.2.4	Cihaz bakımı	Cihazlara üretici firmanın tavsiye ettiği şekilde ve zaman aralığında bakım yapılmakta mıdır? Bakım sadece yetkili personel tarafından mı yapılmaktadır? Bütün gerçek ve şüpheli arızalar ile koruyucu ve düzeltici işlemler kayıt altına alınmakta mıdır? Cihazlar kurum dışına gönderilirken uygun kontroller yapılmakta mıdır? Eğer cihazlar sigortalandıysa sigorta ihtiyacı karşılamakta mıdır?	Bakım sözleşmeleri kapsamında ilgili firma tarafından periyodik bakım yapılmakta, muhabere personeli tarafından da sistem kayıt dosyaları, arızalar açısından haftalık olarak kontrol edilmektedir. Arızalar ve bu arızalar ile ilgili yapılan düzeltici işlemler periyodik bakım formlarına kaydedilmektedir. Garanti kapsamında olan cihazlar için yapılan işlemler fatura ile beraber garanti bitimine kadar saklanmaktadır. Cihazlar kurum dışına gönderilirken gizli bilgi depolayan harici hafıza birimleri sökülmekte ve hangi parçaların gönderildiği teslim tutanağı ile kayıt altına alınmaktadır. Cihazların kurum dışına gönderilmesi durumunda taşıyıcı kargo şirketi veya cihazın gönderildiği firma tarafından sigorta işlemleri yapılmaktadır.
5.2.5	Kurum dışına çıkartılan cihazların güvenliği	Bilgi işleyen herhangi bir cihazın örgüt binaları dışına kullanılmaları için yönetimden izin alınmakta mıdır? Bu cihazlar bina dışına çıkartıldıklarında bina içersinde sağlanan güvenlikten daha fazla güvenlik sağlanmakta mıdır?	Kontrollü cihazların örgüt dışına çıkartılması, üst yönetimin sorumluluğunda olup sürekli uygulanan bir yöntem değildir. Gerekli olduğu durumlarda ise takip edilecek prosedürler belirlenmiş durumdadır. Bu cihazlar, bina içerisinde sağlanan

EK-6 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			güvenlikle eşit oranda güvenlik sağlamayan yerlerde kullanılamaz. Bu maksatla aynı güvenlik ortamını sağlayan yerlerde kullanılmak şartıyla kurum dışına çıkartılmasına müsaade edilebilir. Hassas bilgi içeren cihazlar kurum dışına çıkartıldığında bilgi güvenliğinin temin edilmesinden cihazları teslim alan makam sorumlu olmaktadır.
5.2.6	Cihazların emniyetli imhası veya yeniden kullanılması	Hassas bilgi içeren harici bellekler fiziksel olarak imha edilmekte midir veya geri dönüşümü olmayacak şekilde silinmekte midir?	Hassas bilgi içeren harici bellekler, kırma, yakma ve asitle eritme gibi geri dönüşümü olmayan yöntemlerle imha edilmektedir. İmha edilen bellekler, hassas bilgi tutanaklarından düşülmektedir.
5.3	***Genel Kontroller***		
5.3.1	Temiz masa ve temiz ekran politikası	Otomatik bilgisayar ekranını kilitleme seçeneği kullanılmakta mıdır? Bu bilgisayar belli bir süre kullanılmadığında ekranı kilitleyecektir. Çalışanlar başında kimsenin olmadığı zamanlarda doküman ve disket gibi özel bilgi içeren malzemeleri kilit altında bulundurmaları konusunda uyarılmakta mıdır?	Bütün bilgisayar sistemlerinde otomatik bilgisayar ekranını kilitleme seçeneği maksimum 10 dak. olacak şekilde ayarlanmıştır. Bu konu düzenli olarak kontrol edilmektedir. 24 saat açık ve korumalı bölgelerde, hassas bilgi içeren doküman ve materyal açıkta bulundurulabilmekte, diğer bölgelerdeki doküman ve materyal üç kombineli kilitli çelik kasalarda saklanmaktadır. Masa ve dolaplarda kilitli olsa bile belli bir gizlilik seviyesinin üzerindeki materyal

EK-6 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			bulundurulmamaktadır.
5.3.2	Malzemelerin dışarıya çıkartılması	Cihaz, bilgi veya yazılım yetkisiz bir şekilde dışarıya çıkartılıyor mu? Bu tip malzemenin dışarıya çıkartılıp çıkartılmadığı düzenli denetleniyor mu veya rasgele kontrol ediliyor mu? Çalışanlar bu tip rasgele kontrol veya düzenli denetlemeden haberdar mı?	Cihaz, bilgi ve yazılımın dışarıya çıkartılması, ilgili birimlerin onayı ve kontrolünü müteakiben yapılabilmektedir. Bu konu giriş ve çıkışlarda, güvenlik personeli tarafından periyodik olmayan zamanlarda kontrol edilmektedir. Çalışanlara ve üçüncül şahıslara örgüt içerisine girişte üzerlerinde bilgi depolamaya müsaade eden teçhizat bulunup bulunmadığı sorulmaktadır.

EK-7 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi Denetleme sahaları, amaç ve sorular			
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Haberleşme ve İşletim (Operation) Yönetimi			
6.1	***İşletimsel Yöntemler ve sorumluluklar***		
6.1.1	Belgelenmiş işletimsel yöntemler	Güvenlik Politikası, yedekleme ve cihaz bakımı gibi işletimsel yöntemler tanımlamış mıdır? Bu gibi yöntemler belgelenmiş ve kullanılmakta mıdır?	Yedekleme ile ilgili yapılacak işlemleri gösteren dokümanlar hazırlanmış ve kullanılmaktadır. Cihaz bakımları hem dış kaynak, hem de bilgisayar teknik personeli tarafından yapılmaktadır. Bakım cihazların teknik dokümanlarına uygun olarak yapılmaktadır.
6.1.2	İşletimsel Değişiklik Kontrolü	Üretim sistemlerinde kullanılan bütün programlar bu programlarda yapılacak herhangi bir değişikliğin değişiklik kontrol yetkilendirmesinden geçme ihtiyacında olması gibi sıkı bir kontrol mekanizmasından geçmekte midir? Üretim programlarında yapılan herhangi bir değişikliğin denetleme kayıtları tutulmakta mıdır?	Örgüt içinde kullanılan programlarda örgüt personeli tarafından değişiklik yapılmamaktadır. Değişiklik ihtiyacı, ilgili ticari firmaya veya bunu üreten birime uygun usullerle bildirilmektedir. Program değişiklikleri ilgili firma veya üreten birim tarafından örgüte bildirilmekte ve alınan değişiklikler, alındığına dair kaydedilmektedir.
6.1.3	Olay yönetim yöntemleri	Güvenlik olaylarını ele alacak Olay Yönetim yöntemleri mevcut mudur? Yöntem olay yönetim sorumluluğunu güvenlik olaylarına sırasıyla ve hızlı cevap vermek için adreslenmiş midir? Yöntem hizmetin reddinden gizliliğin ihlaline kadar olan	Güvenlik olaylarının nasıl ele alınacağına dair ilgili yönergelerde ekler mevcut olup, bu ekler düzenli olarak güncellenmektedir. Güvenlik birimleri 24 saat faaliyet gösterecek şekilde yapılanmıştır. Güvenlik ihlalleri olduğunda,

EK-7 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
		farklı çeşitteki olayları ve ele alma yollarını adreslemekte midir? Olayla ilgili denetleme izleri ve kayıtları tutulmakta mıdır ve olayın tekrarlanmamasını sağlayacak bir yöntemle aktif eylem yapılmakta mıdır?	ihlalin tipine göre hangi birimin sorumlu olacağı önceden bellidir. Örnek olay yaklaşımı örgüt çapında yaygın olarak kullanılmakta, örgütün bağlı olduğu üst birimlerce gerekli önlemler alınarak tüm personelin müteyakkız olması temin edilmektedir.
6.1.4	Görevlerin gizlenmesi	Bilgilerin ve hizmetlerin kötü amaçlı kullanımını veya yetkisiz değişiklikleri daha aza indirmek için sorumluluk sahaları ve görevler ayrılmış mıdır?	Her cihazın bulunduğu bölge ile ilgili güvenlik sorumluları vardır. Bu sorumlular, cihazların yetkilendirilmiş personel tarafından kullanılıp kullanılmadığını gözlemler. Cihazların yerlerinin değiştirilmesi, içlerinin açılması da dahil olacak şekilde tüm güvenlik ihlalleri bu sorumlular tarafından takip edilir. Karşılaşılan aksaklıklar, güvenlik organizasyon şemasında gösterilen hiyerarşik yapıya göre güvenlik birimlerine bildirilir.
6.1.5	ARGE ve işletimsel kolaylıkların birbirlerinden ayrılması	ARGE ve test kolaylıları işletimsel kolaylıklardan ayrılmışlar mıdır? Örneğin ARGE yazılımlarının çalıştırıldığı bilgisayar ile üretim yazılımlarının çalıştırıldığı bilgisayarlarla ayrı olmalıdır. ARGE ile üretim YAA'ları (Yerel Alan Ağları) birbirlerinden zorunlu olarak ayrılmalıdır.	Örgütün yapısı itibariyle ARGE faaliyetleri yürütülmemektedir.

EK-7	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
6.1.6	Harici kolaylıkların yönetimi	Herhangi bir Bilgi İşlem kolaylığı harici (üçüncül) bir firma tarafından yönetilmekte midir? Böyle bir yönetim ile ilgili risk önceden tanımlanmış mıdır, üçüncül firma ile tartışılmış mıdır ve uygun kontroller şartnameye konmuş mudur? İş ve uygulama yazılımlarının sahiplerinden (sorumluları) onay alınmış mıdır?	Bilgi işlem kolaylıkları üçüncül şahıslar tarafından yönetilmemektedir. İhtiyaç olduğunda üçüncül şahıslar çağrılarak örgüt personelinin gözetimi altında yerinde müdahale yapılmaktadır.
6.2	***Sistem planlaması ve kabulü***		
6.2.1	Kapasite planlanması	Kapasite istekleri takip edilmekte midir, gelecek ile ilgili kapasite ihtiyaçları öngörülmekte midir? Bu yeterli güç ve yedekleme ünitelerinin mevcut olup olmadığından emin olmak için gereklidir. Örneğin: Kritik sunuculardaki hard disk kapasitesinin, RAM ve CPU'nun gözlemlenmesi.	Bina içindeki merkezi kesintisiz güç kaynağı, mevcut kapasitenin üzerinde olup, artırma planları ile uyumludur. Yedekleme üniteleri, her bilgisayar sistemleri 5 yılda bir yenilenirken yeniden planlanmakta ve kapasitenin üzerindeki ihtiyaçları da karşılayacak şekilde satın alınmaktadır. Bunların haricinde ortaya çıkabilecek herhangi bir kapasite ihtiyacı bir sonraki yıllık bütçeye dahil edilerek temin edilmesi sağlanmaktadır.
6.2.2	Sistem kabulü	Yeni sürüm, güncelleme ve yeni bilgi sistemleri için sistem kabul kriterleri düzenlenmiş midir? Kabulden önce gerekli testler yapılmakta mıdır?	Yeni sürüm, güncelleme yazılımları merkezi olarak takip edilmekte ve örgüte üst makamlar tarafından temin edilmektedir. Yerel alım ile karşılanan sistemler için standartlar merkezi olarak belirlenmekte, alınan cihazların standartlara uyup uymadığı ise yerel olarak

EK-7 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			kontrol edilmektedir. Kontrol sırasında sözleşme maddelerinin tek tek karşılanıp karşılanmadığı test edilmektedir.
6.3	***Kötü niyetli yazılımlara karşı koruma***		
6.3.1	Kötü niyetli yazılımların kontrolü	Kötü niyetli yazılımlara karşı herhangi bir kontrol var mıdır? Müsaade edilmeyen yazılımların kullanılmasını yasaklamak gibi lisanslı yazılım kullanmayı öngören bir güvenlik politikası var mıdır? Bütün uyarı belletenlerinin doğruluğunu kontrol eden bir yöntem var mıdır ve kötü niyetli yazılımların kullanımına engel olacak şekilde midir? Bütün virüs yazılımlarının bilgisayar ve harici hafızalardaki varlıklarını kontrol ve izole eden veya bunları uzaklaştıran antivirüs yazılımları bilgisayarlara yüklenmiş midir? Bu yazılımların imzaları en yeni virüslerin varlığını kontrol edecek şekilde düzenli olarak güncellenmekte midir? Güvenilir olmayan bir ağdan örgüte gelen tüm trafik virüsler açısından kontrol edilmekte midir?Örneğin e-posta, e-posta ekleri ve web'teki virüsler ile FTP trafiği kontrol edilmekte midir?	Ağ üzerinde anti virüs programları çalıştırılmaktadır. Lisanslı olmayan yazılımların ağ üzerindeki herhangi bir bilgisayara yüklenmesine müsaade edilmemektedir. Bu konu yönergelerde açık olarak belirtilmektedir. Kullanıcı personelin her bilgisayara girişi sırasında kötü niyetli yazılımların kullanılmaması gerektiğine dair uyarıcı bir mesaj yayınlanmaktadır. Bilgisayarlarda, sunucular tarafından kontrol edilen merkezi anti virüs yazılımları mevcut olup, bu yazılımlar düzenli olarak güncellenmektedir. Gelen her türlü e-posta, ftp trafiği ve diğer veri akışı filtrelenmektedir.

EK-7	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
6.4	***Toparlama***		
6.4.1	Bilgilerin yedeklenmesi	Üretim sunucusu, kritik ağ parçaları ve yapılandırma ayarları gibi zorunlu iş bilgileri düzenli olarak yedekleniyor mu? Örneğin: Pazartesi-Perşembe artan yedekleme ve Cuma: Tam yedekleme. Yedekleme üniteleri yedekleme yöntemlerine uyumlu mudur ve güvenli ve esas birimden yeterince uzak bir yerde saklanmakta mıdır? Yedeklenen bilgilerin işletimsel yöntemlerin öngördüğü zaman aralığında geri yüklenip yüklenemediği düzenli olarak test edilmekte midir?	Bütün bilgisayar sistemlerine servis sağlayan sunucuların her gün tam yedeklemesi yapılmaktadır. Yedekleme birimleri mevcut kapasitenin tamamını bir gün içerisinde yedekleyebilecek kabiliyete sahiptir. Yedeklenen bilgiler, sunucuların bulunduğu yerden ayrı bir yerde depolanmaktadır. Düzenli bir test işlemi yapılmamakla beraber kullanıcı ihtiyaçları doğrultusunda ortaya çıkan durumlarda yedeklenen bilgilerin geri yüklenmesinin testi yapılmaktadır.
6.4.2	İşletmen kayıtları	İşletmenler isim, arıza, düzeltici işlem vb. verilerin kayıt edildiği bir günlük tutuyorlar mı? İşletmen günlükleri işletim yöntemleri kapsamında düzenli olarak incelenmekte midir?	İşletmenler yapılan işlemlerle ilgili bilgileri, kayıt defterlerine düzenli olarak kaydetmektedirler. Bu sayede her işletmenin yaptığı işlemden diğerlerinin de haberi olmaktadır.
6.4.3	Arıza Kaydı	Arızalar bildirilmekte midir ve iyi bir şekilde yönetilmekte midir? Bu yapılan düzeltici işlemler, arıza kayıtları ve yapılan işlemlerin kontrolünü içermektedir.	Arızalar muhabere bilgi sistemleri yardım masasına bildirilmekte ve buradaki görevli personel tarafından takip edilmektedir. Yapılan düzeltici işlemler bilgisayar üzerinde arıza kayıt dosyalarına işlemektedir.

EK-7 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
6.5	***Ağ Yönetimi***		
6.5.1	Ağ Kontrolü	Ağların ayrılması ve sistem yönetim kolaylıklarının ayrılması gibi zorunlu etkin işletimsel kontroller oluşturulmuş mudur? Kullanıcı bölgelerindeki teçhizatı da kapsayan uzaktan kontrollü cihazların yönetimi için yöntemler ve sorumluluklar belirlenmiş midir? Umuma açık ağ ve korumalı sistemler ile ilgili veri işlemlerinin güvenliği ve bütünlüğü açısından gerekli korumanın özel kontrolü mevcut mudur? Örneğin: Özel Sanal Ağlar, diğer şifreleme ve kıymalama mekanizmaları vb.	Her bilgi sisteminin yerel alan ağı (YAA), kendi IP adresi menzilinde çalışmakta olup, birbirlerinden donanım ve yazılım olarak ayrılmış durumdadır. Hassas bilgi içeren YAA'lar hiçbir şekilde internete bağlanmamaktadır. Bu ağlar, uzaktan erişime kapalıdır. Hassas bilgi içeren YAA'lar, geniş alan ağına (GAA) bağlanmadan önce kriptolanmakta ve bu ağ üzerinde kriptosuz haberleşme yapılmamaktadır. GAA, merkezi olarak kontrol edilmekte ve muhtemel güvenlik açıklarına karşı denetime tabi tutulmaktadır.
6.6	***Harici hafıza işlemleri ve Güvenlik***		
6.6.1	Taşınabilir harici bilgisayar hafızalarının yönetimi	Teyp, kaset, disk, hafıza kartları ve raporları gibi taşınabilir harici bilgisayar hafızalarının yönetimi ile ilgili yöntemler mevcut mudur?	Harici medya, belli bir gizlilik seviyesi üzerinde bilgi içerdiği taktirde, kontrollü evrak muamelesi görmektedir. Bu tip medyanın alınıp verilmesi, senetle yapılmakta ve her biri için ayrı bir kontrol numarası verilmektedir. Bu medya kontrol numaralarına göre düzenli olarak sayıma tabi tutulmaktadır.

EK-7 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
6.6.2	Harici hafızaların imhası	İhtiyaç duyulmayan harici hafızalar güvenli ve emniyetli bir şekilde imha edilmekte midir? İlerideki denetlemelerde takip edilmek üzere hassas malzemenin imhası zorunu olarak kayıt altına alınmakta mıdır?	İhtiyaç duyulmayan harici hafızalar, yönergelerde belirtilen yöntemlerle imha edilmektedir. İmha edilen malzemenin kaydı ayrıca tutulmakta ve bunlar sayımdan düşülmektedir.
6.6.3	Bilgi İşleme Yöntemleri	Bilginin işlenmesi ve depolanması ile ilgili bir yöntem var mıdır? Bu yöntemler bilginin korunmasına ve yetkisiz ifşa veya suiistimal konularına da hitap etmekte midir?	Evet.
6.6.4	Sistem belgelerinin güvenliği	Sistem belgeleri yetkisiz erişimden korunmakta mıdır? Sistem belgelerine erişim listesi uygulama programının sorumlusu ile ilgili diğer kişileri en azda tutulacak şekilde midir? Örneğin: Sistem belgeleri müsaade edilenlerin bulunduğu Erişim Kontrol Listesin de bulunduğu ortaklaşa kullanılan ve sadece belirli sayıda kullanıcının ulaşabildiği sürücüde konulmalıdır.	Sistem belgeleri sadece muhabere bilgi sistemleri personeli tarafından kontrol edilebilmekte, diğer kullanıcılara bu konuda her hangi bir yetki verilmemektedir. Sistem kontrol dosyalarına yapılan işlemler, ağ güvenlik dosyalarına otomatik olarak kaydedilmektedir.
6.7	***Bilgi ve yazılım değişimi***		
6.7.1	Bilgi ve yazılım değişimi mutabakatı	Örgütler arasında bilgi ve yazılım değişimi ile ilgili resmi veya resmi olmayan mutabakatlar var mıdır? Mutabakat işe ait bilginin içerdiği hassasiyeti temel alan güvenliğe hitap etmekte midir?	Örgütler arasındaki bilgi ve yazılım değişimi ilgili yönergeler gereği kontrollü olarak yapılmakta ve örgütler arasıdaki bu değişim, alındı onayı ile geri bildirilmektedir. Bu şekildeki değişim, bilginin gizlilik seviyesine göre belirlenmiş özel işlemlere tabidir.

EK-7 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
6.7.2	Ulaşım Sırasında Harici Hafızanın Güvenliği	Ulaşım sırasında harici hafızaların güvenliği dikkate alınmakta mıdır? Harici hafızalar yetkisiz kişilerin erişimine, kötü amaçlı kullanımına ve bozulmaya karşı korunmakta mıdır?	Harici hafızalar bozulmaya karşı korumalı kutular içerisinde ulaştırılmakta ve yetkisiz kişilerin bu tip malzemeye erişimlerine müsaade edilmemektedir. Harici hafızalar da sahip olduğu gizlilik derecesine göre güvenlik açısından evrak muamelesi görmektedir.
6.7.3	Elektronik Ticaret güvenliği	Elektronik ticaret iyi bir şekilde korunmakta mıdır ve hileli faaliyetlere, anlaşmalı tartışma ve ifşaya veya bilginin değiştirilmesine karşı korumak için kontroller oluşturulmuş mudur? Kimlik denetimi ve yetkilendirme gibi güvenlik kontrolleri elektronik ticarette dikkate alınmış mıdır? Ticari ortaklar arasındaki elektronik ticaret düzenlemeleri güvenlik konularının detaylarını da içerecek ve her iki tarafı da anlaşmaya varılan ticari konular üzerinde bağlayacak olan mutabık kalınan belgelere dayanmakta mıdır?	Elektronik ticaret yapılmamaktadır.
6.7.4	E-posta Güvenliği	Kabul edilen e-posta kullanım politikası var mıdır veya güvenlik politikası e-posta kullanım konusuna hitap etmekte midir? E-posta'ların yarattığı riski azaltmak için antivirus kontrolleri, güvenli olmayan potansiyel e-posta'ları izole etme ve istenmeyen e-posta aktarımının engellenmesi gibi kontroller uygulamaya konulmuş mudur?	E-posta sunucusu otomatik olarak gizlilik derecesi seçeneği sunan bir yazılım çalıştırmaktadır. Seçilecek gizlilik seviyesi, ağ gizlilik seviyesinin en üst limitine kadar olabilmektedir. E-postalar, anti virüs yazılımları ile kontrol edilmekte, şüpheli postalar otomatik olarak filtrelenmektedir. GAA internete açık olmadığı için, mevcut internet risklerinin büyük bir bölümü izole edilmiş

EK-7	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			olmaktadır.
6.7.5	Elektronik ofis sistemlerinin güvenliği	Elektronik ofis sistemlerinin kullanımına hitap eden kabul edilebilir kullanım politikaları mevcut mudur? Elektronik ofis sistemlerinin etkin kontrolünü ve güvenlik risklerini belirten herhangi bir rehber oluşturulmuş mudur?	Hassas bilgi içeren ağlar, kripto ile GAA'ya bağlanmaktadır. Kullanım politikaları ilgili yönergelerde açıklanmaktadır. Güvenlik risklerini belirten her bir bilgi sistemine ait detaylı kontrol listeleri mevcuttur.
6.7.6	Umuma açık sistemler	Bilgilerin umuma açık hale getirilmesini sağlayan resmi herhangi bir yetkilendirme işlevi var mıdır? İş ve uygulama yazılımları sorumlularının ve yetkilerinin değiştirilmesi onayı gibi. Umuma açık bilgilerin yetkisiz erişime ve bütünlüğünün bozulmasına karşı korunması için herhangi bir kontrol var mıdır? Bunlar ateş duvarı, işletim sistemini sertleştirme ve zorla girişi tarama yazılımları gibi sistemi gözetleyen araçları içerebilir.	Hassas bilgi içerene sistemler, umuma açık hale getirilmemektedir. Örgüt içerisinde herkes bilmesi gereken prensibine göre yetkilendirilmektedir. Örgüt içerisinde ortak olarak kullanılacak bilgiler ayrı sürücülerde muhafaza edilmektedir. Buralardaki güncelleme işlemleri, sadece sınırlı sayıdaki yetkili personel tarafından yapılabilmektedir. Kripto kullanıldığından dolayı, ateş duvarı kullanılmamaktadır. Her bir ağın güvenlik ihtiyaçlarını karşılayacak ayrı rehberleri ve kontrol listeleri bulunmaktadır.
6.7.7	Bilgi değişiminin diğer şekilleri	Faks, ses ve video haberleşmesi gibi bilgi değişiminin yapıldığı yolları korumak için kontroller veya politika , yöntemler mevcut mudur? Çalışanlara bu tipte bir bilgi değişim sisteminin kullanımı ile ilgili olarak hassas bilginin gizliliğini korumak maksadıyla hatırlatmalar yapılıyor mu?	Faks, ses ve video haberleşmesi için ayrı ayrı kriptolama yapılmakta olup, bu tip haberleşmenin hangi birimlerle yapılabileceğinin belirtildiği ayrı bir telefon rehberi mevcuttur. Kriptosuz cihazların kullanılması sırasında kullanıcının gözüne hitap edecek alanlarda bu cihazlar üzerinden hassas bilgi göndermesi yapılamayacağına dair uyarı etiketleri

EK-7	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			bulunmaktadır.

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Erişim Kontrolü			
7.1	***İş İhtiyaçları ve Erişim Kontrolü***		
7.1.1	Erişim Kontrol Politikası	Erişim kontrolü hakkında iş ihtiyaçları belirlenmiş ve belgeye dökülmüş müdür? Erişim kontrol politikası her kullanıcı ve kullanıcı gurubuna ait kurallar ve haklara hitap etmekte midir? Kullanıcılara ve servis sağlayıcılara, erişim kontrolünün iş ihtiyaçlarını karşılaması konusu açıkça ifade edilmekte midir?	Erişim kontrolü ihtiyacı çalışanların bulunduğu görev pozisyonuna göre ayarlanmaktadır. Her bölümün şube müdürlerinden gelen erişim kontrolü istekleri karşılanmakta olup, kullanıcıların şahsi başvuruları üzerine herhangi bir işlem yapılmamaktadır. Gruplar, şube müdürlerinin haftada bir yaptığı toplantı sonucunda belirlenmekte, gerek duyulduğunda da değişiklik yapılmaktadır.
7.2	***Kullanıcı Erişim Yönetimi***		
7.2.1	Kullanıcı Kaydı	Çok kullanıcılı bilgi sistemleri ve servislerine resmi kullanıcı kaydı yapma ve silme işlemleri mevcut mudur?	Kullanıcıların örgüte katılışı esnasında, yapılan kayıt işlemleri ile hangi bilgi sistemlerinden ne gibi hizmetler alacağı, kendilerine tebliğ edilmektedir.
7.2.2	Özel Ayrıcalık Yönetimi	Çok kullanıcılı bilgi sistemlerinde özel ayrıcalıkların tahsisi ve kullanılması sınırlandırılmakta ve kontrol edilmekte midir? Örneğin özel ayrıcalıkların, bilmesi gereken prensibine göre ve resmi yetkilendirme işlevinden sonra verilmesi gibi.	Örgüt içerisinde bulunan bilgi sistemlerinin muhabere bilgi işlem personeli haricinde özel ayrıcılıklı kullanımı mümkün değildir.

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
7.2.3	Kullanıcı Şifre Yönetimi	Şifrelerin tahsisi ve yeniden tahsisi, resmi yönetim işlevlerine göre kontrol edilmelidir. Kullanıcılara şifreleri gizli tutmaları için bir belge imzalatılmakta mıdır?	Kullanıcılara örgüte katılışları esnasında güvenlik belgesi imzalattırılmakta ve bilgi sistemlerine ait kullanıcı şifresinin en üst seviyede gizliliğe haiz olduğu belirtilmektedir. Şifreler en fazla 180 gün içerisinde değiştirilecek şekilde sistem tarafından kontrol edilmektedir.
7.2.4	Kullanıcı Erişim Haklarının Gözden Geçirilmesi	Düzenli fasılalarla kullanıcı erişim haklarının kontrol edildiği bir işlev mevcut mudur? Örneğin: Özel ayrıcalıklı kullanım hakkı 3 ayda 1, normal ayrıcalıklı kullanım hakkı 6 ayda 1.	Herhangi bir kullanıcı ile ilgili erişim hakkı güncellemesi esnasında mevcut diğer erişim hakları da gözden geçirilmektedir. Bu tip işlem en az ayda bir defa yapılmaktadır.
7.3	***Kullanıcı Sorumlulukları***		
7.3.1	Şifre Kullanımı	Güvenli şifrelerin korunması ve seçilmesi için oluşturulmuş bir rehber var mıdır?	Şifrelerin ilk girişi ve güncellenmesi esnasında şifre kurallarına uymayan girişler, sebepleriyle birlikte kullanıcıya iletilmektedir. Kullanıcı bu kurallara uyan bir şifre girinceye kadar sisteme giriş yetkisi alamamaktadır.
7.3.2	Gözetimsiz Kullanıcı Teçhizatı	Kullanıcı ve yükleniciler gözetimsiz teçhizatın korunması ile ilgili olarak sorumlu oldukları gibi yöntem ve güvenlik ihtiyaçlarından haberdar mıdırlar? Örneğin; Oturum bittiğinde çıkış yapılması veya otomatik çıkışın ayarlanması gibi...	Her kullanıcı, işi bittiğinde kullandığı bilgisayarın ya ekranını kilitlemek veya sistemden çıkış yapmak zorundadır. Her ihtimale karşı maksimum 10 dak. İçerisinde bilgisayarın kendi ekranını kilitlemesi seçeneği, aktifleştirilmiştir. Ancak otomatik çıkış işlemi bazı sakıncaları dolayısıyla yapılmamaktadır.

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
7.4	***Ağ Erişim Kontrolü***		
7.4.1	Ağ Hizmetlerinin Kullanımındaki Politika	Ağ ve ağ hizmetlerini ilgilendiren bir politika var mıdır? Erişilecek Ağ kısımları; Kimin ne yapacağını tanımlayan yetkilendirme hizmetleri, Ağ bağlantıları ve ağ hizmetlerine erişimin kontrolüne dair yöntemler gibi.	Her bir ağın ağ güvenlik personeli ile sistem yöneticileri ilgili politikaların oluşturulmasında birinci öncelikli olarak sorumludur. Ağ hizmetlerinde esas olan politika sistem yönetimi ile ilgili işlemlerin sadece muhabere bilgi işlem personeli tarafından yapılmasına dayanmaktadır. Diğer konular önceki maddelerde belirtildiği gibidir.
7.4.2	Yönlendirilmiş Yol	Kullanıcı terminali ile kullanıcının erişime yetkilendirildiği bilgisayar hizmetleri arasındaki yol kısıtlamaları kontrol edilmekte midir? Örneğin; Riskin azaltılması için yolun yönlendirilmesi	Yol kısıtlamalarının oluşturulmasında her kullanıcının hangi bölümlere ulaşabileceği belirlenmekle birlikte ilgili bölümlere kimlerin ulaşabileceği de ayrıca kontrol edilmektedir. Bu işlem için esas olarak sistem olay kütükleri düzenli olarak incelenmektedir. Kullanıcıların kendilerine ayrı bir yol oluşturmalarına müsaade edilmemektedir.
7.4.3	Harici Bağlantılar için Kullanıcı Kimlik Kontrolü	Harici bağlantılar için herhangi bir kimlik kontrol mekanizması var mıdır? Örneğin; Kriptolama tabanlı teknikler, donanımsal anahtar, yazılımsal anahtar, karşılıklı sorgulama protokolleri	Harici bağlantılarda esas olan erişim iki tipte yapılmaktadır. Örgütün web sayfasına sadece misafir kullanıcı yetkileri dahilinde giriş yapılabilmektedir. Örgütün veri tabanına ulaşım, veri tabanı yetkilendirmesi ile kontrol edilmektedir.

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
7.4.4	Düğüm Kimlik Kontrolü	Örgütün güvenlik yönetimi dışındaki bilgisayar sistemlerine uzaktan bağlantı için kimlik kontrolü yapılmakta mıdır? Düğüm kimlik kontrolü, emniyetli ve ortak bir bilgisayar kolaylığından grup olarak bağlanmış olan kullanıcıların kimlik kontrolü olarak hizmet verebilmektedir.	Örgütün güvenlik yönetimi dışında herhangi bir bilgisayar sistemi bulunmamaktadır. Örgüt dışın güvenli bağlantılar üzerinden bağlantı kurulacağı zaman sadece belirli bir süre için geçici kullanıcılar tanımlanmaktadır. Bu kullanıcılar, telnet ve ftp servisleri ile kısıtlı işlemler yapabilmektedirler. İşlemin tamamlanmasından sonra bu tip kullanıcı hesapları sistemden kaldırılmaktadır.
7.4.5	Uzaktan Hata Kontrol Portlarının Korunması	Uzaktan hata kontrol portları bir güvenlik mekanizması tarafından korunması gibi, güvenli bir şekilde kontrol edilmekte midir?	Uzaktan hata kontrol işlemleri ile ilgili olarak GAA yöneticileri sorumlu olup, ihtiyaç duyduklarında sistemin GAA bağlantılarına müdahale edebilmektedirler. YAA'da bu tip müdahalelere müsaade edilmemektedir.
7.4.6	Ağların ayrılması	Ağ (iş ortaklarının veya üçüncü şahısların erişimine ihtiyaç duyduğu bilgi sistemleri) güvenlik duvarı gibi çevresel güvenlik mekanizmaları ile ayrılmış mıdır?	GAA'ya bağlantının yapılması için gelişmiş kripto cihazları kullanılmakta olup, bu bağlantı üçüncül şahıslar tarafından kullanılamamaktadır. Sistem internete bağlı olmadığından, güvenlik duvarı kullanılmamaktadır.
7.4.7	Ağ bağlantı protokolleri	Örgüt sınırlarının dışına uzanan ortak ağların herhangi bir ağ bağlantı kontrolü var mıdır? Örneğin; elektronik posta, web erişim, dosya aktarımı gibi...	Örgüt sınırlarının dışına uzanan ağ bağlantıları ilk kurulum aşamasından önce akredite edilmektedir. Akreditasyon işlemi sırasında GAA güvenliği, YAA güvenliği ve kullanılacak protokollerle ilgili onay alınmakta olup, sistem güvenliğini zafiyete uğratacak herhangi bir bağlantı türüne müsaade edilmemektedir.

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			Akreditasyon gereklerinin yerine getirilip getirilmediği sistem kurulumundan önce örgütün bağlı olduğu üst birimlerce yerinde kontrol edilmektedir.
7.4.8	Ağ yönlendirme kontrolleri	İş uygulama yazılımlarının erişim kontrol politikasını ihlal etmeyen bilgi akışı ve bilgisayar bağlantılarını emniyete alan her hangi ağ kontrolü var mıdır? Bu örgüt dışı kullanıcılar tarafından da ortaklaşa kullanılan ağlar için genellikle zorunludur. Yönlendirme protokolleri hedef tanıma mekanizmaları ve pozitif kaynak kontrolüne dayandırılmakta mıdır? Örneğin; Ağ Adres Dönüşümü (NAT - Network Address Translation)	Hassas bilgi içeren bütün ağlar, umuma açık olmamakla birlikte, her bir ağın IP adres aralığı akreditasyon işlemleri sırasında belirlenmektedir. Her bir yazılımın kullandığı port numaraları belirli olup, bu portların haricinde kontrolsüz haberleşme yapılmamaktadır. Örgüt dışı kullanıcılar, kendi bulundukları bölgede güvenlik politikalarının uygulanmasından sorumludurlar. Her iki tarafında aynı şartlar altında güvenlik kurallarına uyması ağ adres dönüşümü gibi internet üzerinde kullanılan çeşitli güvenlik önlemlerine duyulan ihtiyacı ortadan kaldırmaktadır.
7.4.9	Ağ hizmetlerinin güvenliği	Bütün hizmetler tarafından kullanılan güvenlik özelliklerinin açıkça tanımlandığı ve organizasyonun kullandığı genel ve özel ağ servisleri temin edilmiş midir?	Organizasyonda kullanılmakta olan ağ ve ağ bağlantıları için gerekli güvenlik özellikleri açıkça tanımlanmış durumdadır.
7.5	***İşletim sistemi erişim kontrolü***		
7.5.1	Otomatik terminal tanıma	Bağlantıların kimlik kontrolünü yapacak otomatik terminal tanıma mekanizması var mıdır?	GAA bağlantıları kriptolandığından dolayı örgüt dışı haberleşme kanallarından mevcut ağlara girilememektedir. Bununla beraber,

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			sunucular ve routerlar GAA üzerindeki bütün sunucu ve routerları düzenli olarak kontrol etmekte, her bir sunucunun hangi sunucularla bağlantı yaptığı sistem kontrol tablolarından takip edilebilmektedir.
7.5.2	Terminal giriş yöntemleri	Bilgi sistemlerine erişim sadece güvenli giriş işlemleri ile mi yapılmaktadır? Bilgi sistemlerine giriş için bir yöntem oluşturulmuş mudur? Bu yetkisiz erişim imkanını en aza indirmeye yarar	Bilgi sistemlerine giriş için kullanılan her bir terminalin yakınında gözle görülebilecek şekilde kullanmaya yetkili personel isim listesi bulundurulmaktadır. Terminal bölgesi güvenlik sorumluları ve ilgili birimin kullanıcıları, yetkisiz personelin bilgi sistemlerine girişini gözlemlemektedir. Her kullanıcı kendi kullanıcı adı ve şifresi ile girdiğinden umuma açık kullanıcı adları ve şifreleri bulunmamaktadır.
7.5.3	Kullanıcı tanıma ve kimlik kontrolü	Sistem yöneticileri işletmenler ve diğer tüm teknik kullanıcılar için tek bir tanımlayıcı temin edilmiş midir? Umumi kullanıcı hesapları sadece bariz iş faydası temin edileceği olağan dışı şartlarda verilmelidir. İddia edilen kullanıcı kimliğini, kimlik kontrolü yöntemleri doğrulamakta mıdır? Genellikle kullanılan yöntem: Sadece kullanıcıların bildiği şifrelerin kullanılmasıdır.	Sistem yöneticileri ve diğer tüm teknik kullanıcılar, sisteme müdahale etmek için en üst seviyedeki yetkilere sahiptirler. Bu şekildeki sistem yöneticilerinin sayısı muhabere bilgi işlem teknik personelinin sayısı ile sınırlıdır. Sistem yönetimi ile ilgili veya hassas bilgiyi içeren bilgisayarlarda umumi kullanıcı bulundurulmamaktadır.
7.5.4	Şifre Yönetim Sistemi	Güvenirlik ile ilgili kişisel şifreler, şifre değiştirme zorlaması, şifrelerin kriptolanmış formatta saklanması, şifrelerin ekranda görünmemesi vb. Değişik şifre kontrol yöntemlerine yönlendiren şifre yönetim sistemi mevcut mudur?	Her bir kullanıcının ayrı ayrı şifresi mevcut olup bu şifreler minimum 8 karakterden oluşmaktadır. Şifrelerin içerisinde harf, sayı ve diğer işaretlerin kullanılma zorunluluğu vardır. Şifreler max. 180 gün içerisinde değiştirilecek

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
		mudur?	şekilde otomatik olarak yeni girişe zorlanmaktadır. Hiçbir şifre ağ üzerinde bir yere kaydedilmemektedir. Şifreler girilirken ekranda kaç karakter girildiği gözükmemektedir.
7.5.5	Sistem araçlarının kullanımı	Bilgisayar kurulumlarıyla gelen fakat sistem ve uygulama yazılımı kontrollerini geçersiz kılan sistem araçları sıkıca kontrol edilmekte midir?	Sistem araçlarının kurulumu sadece sistem yöneticileri tarafından yapılmakta olup, kullanıcıların bu tip araçları bilgisayar sitemlerine yüklemelerine müsaade edilmemektedir.
7.5.6	Kullanıcıları korumak için zorlama alarmı	Zorlamaya maruz kalabilecek kullanıcılar hakkında zorlama alarm tedbirleri dikkate alınmakta mıdır?	Zorlamaya maruz kalabilecek kullanıcılar için ilk giriş esnasında aynı adda başka bir kullanıcının sistemde bulunup bulunmadığı kontrol edilmektedir. Aynı kullanıcı adıyla başka biri sisteme dahil olmuş ise bu durum kullanıcıya uyarı mesajı olarak gönderilmektedir.
7.5.7	Terminal zaman aşımı	Umumi kullanıcı alanlarında hiç kullanılmadan belli bir süre duran terminallerin ekranı kilitlenmeye veya otomatik olarak kapanmaya ayarlanmalıdır.	Umumi kullanıcı alanlarındaki bilgisayarlar hiçbir işlem yapılmadığı taktirde max.10dak. içerisinde otomatik olarak kilitlenmektedir. Bu kilidi sadece ilgili kullanıcı veya sistem yöneticisi kaldırabilmektedir.
7.5.8	Bağlantı zamanı sınırlaması	Yüksek riskli uygulama yazılımları için bağlantı zamanı sınırlaması mevcut mudur? Bu tip bir kurulum yüksek riskli bölgelerde kurulmuş olan hassas uygulama yazılımları için dikkate alınmalıdır.	Hassas bilgi içeren bilgi sistemleri fiziksel olarak koruma altında bulunan bölgelerde olduğu için zaman sınırlamasına ihtiyaç duyulmamaktadır.

EK-8 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
7.6	***Uygulama yazılımı erişim kontrolü***		
7.6.1	Bilgi erişim sınırlaması	Organizasyon içindeki çeşitli grup ve personelin uygulama yazılımlarına erişimleri kişisel iş uygulama yazılımlarına göre erişim kontrol politikası dahilinde tanımlanmalıdır. Bu işlem örgütün bilgi erişim politikaları ile tutarlı olmalıdır.	Bu uygulama daha önceki bölümlerde ifade edildiği şekilde yerine getirilmektedir.
7.6.2	Hassas sistem izolasyonu	Güvenilir uygulama yazılımı sistemleri ile kaynaklarını paylaşmak için tahsis edilen bilgisayar gibi teçhizatın, hassas sistemlerle izolasyonu sağlanmış mıdır?	Güvenilir uygulama yazılımları sadece sunucular üzerinde çalıştığından dolayı diğer bilgi sistemleri tarafından paylaşılmaya müsait değildir. Kullanıcılar, sunucu üzerinde kendilerine verilen yetki dahilinde bu yazılımları çalıştırabilmektedir.
7.7	***Sistem erişim ve kullanımının gözetlenmesi***		
7.7.1	Olay Kaydı	İlerideki araştırmalar ve erişim kontrollerinin gözlemlenmesi için istisnai durumlar ve diğer güvenlik olayları kayıt edilip, belirli bir süre zarfında saklanmakta mıdır?	İstisnai durumların ve erişim kontrollerinin saklandığı dosyalar, düzenli olarak yedeklenmekte, ihtiyaç duyulduğunda yedekler üzerinden kontrol edilebilmektedir.

EK-8	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
7.7.2	Sistem Kullanımının Gözlemlenmesi	Bilgi işlem kolaylıkları kullanımının gözlemlendiği yöntemler oluşturulmuş mudur? Yöntemler, kullanıcıların sadece açıkça yetkilendirildiği aktiviteleri yapmalarını sağlamalıdır. Gözlemleme faaliyetlerinin sonuçları düzenli olarak gözden geçirilmekte midir?	Sunucular üzerinde bulunan sistem kayıt dosyaları her bir kullanıcının hangi zaman aralıklarında sisteme dahil olduğunu ve ne gibi işlemler yaptığını kayıt altına almaktadır. Bu dosyalar düzenli olarak kontrol edilmekte ve yetkisiz herhangi bir giriş olup olmadığı ağ güvenlik sorumluları tarafından takip edilmektedir.
7.7.3	Saat Senkronizasyonu	Bilgisayar veya haberleşme cihazları gerçek zaman saatin işletme kabiliyetine sahip midir? Bu zaman yerel standart saat veya evrensel coğrafi saat gibi mutabık kalınan standart bir saate ayarlanmalıdır. Bilgisayar saatinin doğru ayarlanması, denetleme kayıtlarının doğruluğu açısından büyük öneme haizdir.	Bütün iş istasyonları gerçek zaman saatini sunuculardan almakta ve bu saat evrensel coğrafi saate (zulu saat) ayarlanmaktadır. Sunucularla iş istasyonları arasında zaman senkronizasyonu kaybolduğunda bazı programlar çalıştırılamamaktadır.
7.8	***Mobil bilgi işlem ve uzaktan işlem***		
7.8.1	Mobil bilgi işlem	Dizüstü ve cep bilgisayarı gibi bilgisayar kolaylıkları ile özellikle korunmasız ortamda çalışmanın riski, resmi politikalara uyarlanmakta mıdır? Riskin azaltılması için mobil bilgisayar kolaylıklarını kullanan personelin dikkatini kullanılan yöntemden dolayı oluşabilecek ek risklere çekmek amacıyla eğitim düzenlenmekte midir?	Diz üstü ve cep bilgisayarı gibi mobil bilgisayar kolaylıklarının hassas bilgi içeren sistemlere bağlanmasına müsaade edilmemektedir. Bu tip bilgisayarlar örgüte ait resmi bilgisayarlar ise düşük seviyeli gizlilik derecesine haiz olmakta ve hassas bilgi içeren sistemlerden ayrı olarak akredite edilmektedir. Örgüt politikası olarak mobil bilgisayar sistemlerinin kullanımı sınırlandırılmış olup, kişisel mobil bilgisayarların örgüt içerisine

EK-8 Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi			
İlgi Denetleme sahaları, amaç ve sorular			
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			getirilmesine müsaade edilmemektedir.
7.8.2	Uzaktan Çalışma	Uzaktan çalışma faaliyetlerinin kontrolü için her hangi bir politika, yöntem ve/veya standart mevcut mudur? Bu örgütün güvenlik politikası ile uyumlu olmalıdır. Bilgilerin yetkisiz ifşası, teçhizatın çalınması gibi tehditlere karşı uzaktan çalışan birim uygun bir şekilde korunmakta mıdır?	Uzaktan çalışma faaliyetleri sadece müsaade edilen uzak kullanıcıların ilgili veritabanına erişimi ile sınırlıdır. Veritabanlarında her bir kullanıcının yapabileceği işlemler ayrıca kısıtlanmaktadır. Uzak kullanıcıların kendi örgütleri içerisinde güvenlik standartlarını yerine getirmeleri düzenli olarak denetlenmektedir. Her bir uzak kullanıcı için belirli bir zaman periyodu içerisinde yetki verilmekte olup, bu yetki örgütün üst düzey yöneticileri tarafından onaylanmaktadır.

EK-9	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Sistem Geliştirme ve Bakım			
8.1	***Sistemlerin güvenlik ihtiyaçları***		
8.1.1	Güvenlik ihtiyaçları analizi ve özellikleri	Yeni sistemler veya mevcut sistemlerin geliştirilmesi için iş ihtiyaçlarının bir parçası olarak güvenlik gereksinimleri kapsanmalıdır. Tanımlanan güvenlik ihtiyaçları ve kontrolleri, bilişim varlıklarının ticari değerlerini ve güvenlik hatalarından doğacak maliyeti yansıtmalıdır. Sistem geliştirme aşamasından önce risk değerlendirmesi tamamlanmakta mıdır?	Yeni sistemlerin ve mevcut sistemlerin geliştirilmesi örgütün yetkisi dahilinde olmayıp, merkezi olarak yürütülen projeler sayesinde yapılmaktadır. Böylece aynı seviyedeki diğer örgütlerle güvenlik standardizasyonu sağlanmaktadır. Sistem geliştirme aşamasındaki risk değerlendirmesi bağlı olunan en üst örgütün sorumluluğu altındadır.
8.2	***Uygulama sistemlerindeki güvenlik***		
8.2.1	Veri girişi geçerleme	Uygulama sistemlerine veri girişinin doğruluğu ve uygunluğu geçerlenmekte midir? Hata mesajlarını kontrol etmek için değişik tipteki girişler, geçerleme hatalarını cevaplayan yöntemler, veri girişi işlevleri ile ilgilenen bütün personelin sorumluluklarının tanımlanması vb. kontroller dikkate alınmakta mıdır?	Veri girişi için belli formattaki yapılar kullanılmakta olup, giriş esnasında verinin uzunluğu ve kullanılan karakterler sistem tarafından otomatik olarak kontrol edilmektedir. Yanlış veri girilmesi durumunda ilgili veritabanına kayıt yapılmayarak kullanıcıya yapılan hata hakkında otomatik uyarı mesajı gönderilmektedir.

EK-9	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
8.2.2	Dahili işlemlerin kontrolü	Geçerleme kontrollerinin ve çevrim süreçlerinin dahil edildiği risk alanları tanımlanmış mıdır? Doğru girilmiş olan veriler bazı durumlarda kasti hareketler veya işlem hatalarından dolayı bozulabilir. Uygulama yazılımları için dahili işlemler sırasında riskleri azaltmaya yönelik uygun kontroller tanımlanmış mıdır? Kontroller, herhangi bir verinin bozulmasının işe etkisi ve uygulama yazılımının doğasına bağlıdır.	Sistem veri girişlerindeki geçerleme kontrolleri kullanıcıların yapacağı hatalara karşı otomatik korumaya sahip olduğundan dolayı, yanlış formattaki bilgilerin girişi mümkün olmamaktadır. Her bir hata ile ilgili hata kodlarının açıklaması ve muhtemel düzeltici işlemler veritabanı yardım dosyalarında bulunmaktadır. Kontrol dışı yanlış girişler veritabanına kaydedildiğinde, hatalar sonradan tespit edilerek düzeltilebilmektedir.
8.2.3	Mesaj kimlik kontrolü	Mesaj kimlik kontrolünün gerekli olup olmadığı güvenlik riski değerlendirmesi sırasında dikkate alınmakta mıdır ve en uygun yöntemin uygulanması tanımlanmakta mıdır? Mesaj kimlik kontrolü, gönderilen elektronik mesajın içeriğinin yetkisiz bir şekilde değiştirilmesi veya bozulmasını tetkik etmekte kullanılan bir tekniktir.	Her bir mesajın kendine ait mesaj kimlik numarası, uzunluğu, kaynak IP adresi, hedef IP adresi gibi teknik veriler, sistem tarafından otomatik olarak üretilmekte olup, ağ haberleşmesi standartlarına uymaktadır. Sistemlerde IPV4 IP adresleme tekniği kullanılmaktadır.
8.2.4	Çıkış verilerinin geçerlenmesi	Saklanan bilgilerin doğru ve uygun şartlarda işlem gördüğü uygulama sistemlerinin veri çıkışları tarafından geçerlenmekte midir?	Saklanan bilgilerin doğruluğu, checksum ve CRC hata tespit ve düzeltme mekanizmaları tarafından temin edilmektedir. Hatalı bilgiler, düzeltme işlemlerinden sonra sistem tarafından kullanıcılar uyarılmakta ve veriler yeniden kaydedilmektedir.
8.3	***Kriptografik Kontroller***		

EK-9	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
8.3.1	Kriptografik Kontrollerin kullanılmasındaki politika	Bilginin korunması için kriptografik kontrollerin kullanımında bir politika mevcut mudur? Verilmesi gereken bilginin koruma seviyesinin tanımında risk değerlendirmesi yapılmakta mıdır?	Kriptografik kontroller bilgi güvenliğinin en hassas noktası olup, güvenlik politikaları içerisinde tamamen ayrı bir şekilde tanımlanmaktadır. Her bir kriptonun gizlilik seviyesi hassas bilgi sistemlerinin sahip olduğu en üst gizlilik seviyesine uygundur.
8.3.2	Kriptolama	Verileri korumak için herhangi bir kriptolama tekniğe kullanılmakta mıdır? Gereken koruma seviyesi ve bilgi hassasiyetinin analizi için değerlendirmeler yapılmakta mıdır?	Verilerin GAA üzerinden gönderilmesinden önce donanımsal olarak kriptolanması sağlanmakta ve GAA'ya dahil olan bütün YAA'lar aynı güvenlik seviyesinde kriptolamaya tabidir.
8.3.3	Sayısal imzalar	Elektronik belgelerin bütünlüğünün ve kimlik kontrolünün korunması için sayısal imzalar kullanılmakta mıdır?	Sayısal imza tekniği örgüt içerisinde kullanılmamaktadır.
8.3.4	Reddetmesiz servisler	Bir olay veya eylemin oluşup oluşmamasındaki anlaşmazlığı zorunlu olarak çözen reddetmesiz servisler kullanılmakta mıdır? Örneğin; Elektronik ödeme veya sözleşme hakkındaki sayısal imzanın kullanımını içeren anlaşmazlık	Sayısal imza tekniği ve elektronik ödeme gibi uygulamalar örgüt içerisinde kullanılmadığından, bu tip servislere ihtiyaç duyulmamaktadır.
8.3.5	Anahtar yönetimi	Gizli anahtar tekniği ve umumi anahtar tekniği gibi örgütün kullandığı kriptografik teknikleri destekleyen yönetim sistemleri mevcut mudur? Anahtar yönetim sistemi, güvenli yol ve yöntemler ile mutabık kalınan standartlar dizisine dayanmakta mıdır?	Gizli anahtarlar hassas bilgi sistemleri üzerinden aktarılmayıp, özel kuryeler vasıtasıyla temin edilmektedir. Bu yüzden gizli anahtarların ağ üzerinden elde edilmesi mümkün değildir. Bu anahtarlar, kripto donanımının özelliğine bağlı olarak, her gün veya her hafta belli saatlerde güncellenmektedir. Güncelleme işlemi, karşılıklı

EK-9	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			olarak haberleşen iki kripto cihazı üzerinden aynı zamanda yapılmaktadır. Herhangi bir anahtar ihlaline karşı yedek anahtarlar mevcut olup, merkezi olarak, yapılan duyuruyu takiben, asli anahtarlar yerine yedek anahtarlar kullanılabilmektedir.
8.4	***Sistem dosyalarının güvenliği***		
8.4.1	İşletimsel yazılımın kontrolü	İşletimsel sistemlerin yazılım uygulamasına dair kontroller mevcut mudur? Bu işletimsel sistemlerin bozulmasına yönelik riskin en aza indirilmesine yöneliktir.	İşletimsel sistemlerin yazılım uygulamalarına ait yamalar, düzenli olarak güncellenmekte ve sistemin faaliyeti sağlanmaktadır.
8.4.2	Sistem test verilerinin korunması	Sistem test verileri korunmakta ve test edilmekte midir? Kişisel bilgileri içeren işletimsel veri tabanının test amaçlı kullanılmasından kaçınılmalıdır. Eğer böyle bilgiler kullanılıyorsa veriler kullanılmadan önce kişisel bilgilerden arındırılmalıdır.	Uygulama yazılımlarına ait testler merkezi olarak yapıldığından sistem test verileri örgüt içerisinde bulunmamaktadır. Bu yüzden kişisel bilgiler ile karışması mümkün değildir.
8.4.3	Program kaynak kütüphanelerine yönelik erişim kontrolü	Program kaynak kütüphanelerine erişim sıkı bir şekilde kontrol edilmekte midir? Bu bilgisayar programlarının bozulmasına yönelik potansiyelin azaltılması içindir.	Program kaynak kütüphanelerine erişim yetkisi, sistem yöneticileri haricindeki hiçbir kullanıcıya verilmemektedir.
8.5	***Destek ve geliştirme işlemlerindeki güvenlik***		

EK-9	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
8.5.1	Kontrol yöntemlerinin değiştirilmesi	Bilgi sistemlerinin değiştirilmesine yönelik sıkı kontrol yöntemleri oluşturulmuş mudur? Bu bilgi sistemlerinin bozulmasını en aza indirmek içindir.	Bilgi sistemlerinin bozulmasına sebebiyet verebilecek oyun, şahsi uygulama yazılımları ve lisanssız ürünler sistemlere yüklenmemektedir. Böylece kontrolsüz değiştirmeler engellenmektedir.
8.5.2	İşletim sistemi değişikliklerinin teknik olarak gözden geçirilmesi	İşletim sistemi değişikliklerinden sonra uygulama sistemlerini gözden geçirecek işlem ve yöntemler oluşturulmuş mudur? Son düzeltmeler, yamalar ve servis paketlerinin yüklenmesi gibi işletim sistemi düzenli olarak güncelleştirilmek zorundadır.	İşletim sistemi değişiklikleri yapılmadan önce mevcut durumun en son hali yedeklenmekte, herhangi bir sorunla karşılaşılırsa işletim sisteminin eski haline geri dönülmektedir. İşletim sisteminin bir önceki sürümü muhafaza edilmekte, sistemin tamamen çökmesi durumunda eski sürüm kullanılarak yeniden yükleme işlemi yapılmaktadır.
8.5.3	İşletim sistemi değişikliklerinin teknik olarak gözden geçirilmesi	Yazılım paketlerinin değiştirilmesine yönelik herhangi bir kısıtlama var mıdır? Mümkün olduğunca satıcı firma tarafından temin edilen yazılım paketleri hiçbir değişikliğe uğramadan kullanılmalıdır. Eğer değişiklik yapma zorunlu ise orijinal yazılım elde tutulmalı, değişiklikler temiz bir kopya üzerinde yapılmalıdır. Bütün değişiklikler, gelecekte yazılım güncellemeleri zorunlu hale gelirse, kullanılabilsin diye açıkça test edilmeli ve kayda alınmalıdır.	Yazılım paketleri örgüte ulaştığında mutlaka bir kopyası alınmakta, bozulmalara karşı bu kopya kullanılmaktadır. Yama ve servis paketleri sistem normal olarak çalıştığı sürece yüklenmemektedir. Ancak güvenlik sebebiyle yapılan özel duyurulardan sonra sistemde herhangi bir sorun olmasa da tavsiye edilen yama ve servis paketleri yüklenmektedir.
8.5.4	Gizli kanallar ve truva atları	Yeni veya güncelleştirilmiş sistemlerin içine truva atlarının veya gizli kanalların saklanmadığını garanti eden kontroller mevcut mudur? Gizli kanallar bazı belirsiz ve dolaylı yollarla bilgileri açığa çıkartabilir. Truva atları yetkilendirilmemiş bir yol ile sistemi etki altına almak için	Sistemlerin güncelleştirilmesi için kullanılan yazılımlar merkezi olarak dağıtılmakta ve internet üzerinden herhangi bir güncelleştirme işlemi yapılmamaktadır. Bu yüzden kullanılan yazılımlar güvenli olup, sistemlere şu ana kadar herhangi bir

EK-9	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
		yazılmıştır.	zarar vermemiştir. Merkezi olarak temin edilen yazılımlar üretici firmalardan ücreti karşılığında satın alındığından içlerinde truva atları gibi zarar verici yazılımlar bulunmamaktadır.
8.5.5	Dış kaynaklı yazılım geliştirme	Dış kaynaklı yazılımlar hakkında kontroller mevcut mudur? Dikkat edilecek noktalar: Lisans düzenlemeleri, yasal düzenlemeler, kalite güvencesi için sözleşme ihtiyaçları, Truva atlarını tespit etmeye yönelik yükleme öncesi testler vb.	Dış kaynaklı yazılımlar örgüt tarafından satın alınmadığı için herhangi bir risk mevcut değildir. Lisanslı olarak merkezi satın alma yöntemi ile alınmamış ve yasal olmayan hiçbir yazılım sistemlere yüklenmemektedir.

EK-10	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
İş devamlılığı yönetimi			
9.1	***İş devamlılığı yönetimine bakış açışı***		
9.1.1	İş devamlılığı yönetimi işlevleri	Organizasyon çapındaki iş devamlılığının idamesi ve geliştirilmesi için yönetilen bir süreç mevcut mudur? Bu bütün örgüt çapında iş devamlılığı plan düzenli testler ve planın güncelleştirilmesi, iş devamlılığı stratejisinin dokümantasyonu ve formüle edilmesini içerebilir.	Belli zaman periyodu içerisinde yapılan işler ayrıca kayıt altına alınarak daha sonraki analizlerde kullanılmaktadır. Örgüt içerisinde bu tip uygulamalar "çıkarılan dersler" adı altında değerlendirilmektedir. Ortaya çıkan her bir sorun için düzeltici işlemler yapılmakta, kısa vadede düzeltilemeyen problemler için uzun vadeli planlama yapılarak uygun hal tarzları ile çözümlenmektedir.
9.1.2	İş devamlılığı ve tesir analizi	İş süreçlerini kesintiye uğratabilecek olaylar tanımlanmış mıdır? Örneğin; cihaz arızaları, su baskını ve yangın. Bu tip bir kesintinin etkisini tanımlamak için herhangi bir risk değerlendirmesi yapılmış mıdır? İş devamlılığına bütünsel yaklaşımı tanımlamaya yönelik risk değerlendirme sonuçlarına dayanan strateji planı geliştirilmiş midir?	İş süreçlerinin kesintiye uğramasına sebebiyet verebilecek olaylar gerçekleşme ihtimallerine göre sınıflandırılmaktadır. Her bir olay için alınacak tedbirler ayrı ayrı belirlenip acil durumlar uygulama planına ithal edilmektedir. Mevcut yapılandırma ile giderilmesi mümkün olmayan riskler için ayrıca bütçe planlanmakta ve bu bütçe bir sonraki yıla bırakılmadan kullanılmaktadır.
9.1.3	Devamlılık planını yazma ve uygulama	İş süreçlerinin durmasını ve kesintiye uğramasını takiben ihtiyaç duyulan zaman süresi içerisinde ticari işlerin yeniden başlamasını sağlayacak planlar geliştirilmiş midir?	İş süreçlerini kesintiye uğratacak beklenmeyen acil durumlarda hareket tarzları belirlenmiş olup, gerektiğinde personelin ve teçhizatın tahliyesine kadar varan tatbikatlar yapılmaktadır. Her tatbikatı

EK-10	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
		Plan düzenli olarak test edilip güncelleştirilmekte midir?	takiben çalışanlar, normal duruma geçmekte karşılaştıkları zorlukları ilgili birimlere bildirmektedir. Bu sayede planlar güncelleştirilmiş olmaktadır.
9.1.4	İş devamlılığı planının çatısı	İş devamlılığı planının tek bir çatısı mevcut mudur? Bütün planların tutarlılığı ile test ve bakımları için önceliklerinin tanımlandığı bir çatı idame ettirilmekte midir? Bu, faaliyete ve planın her bir parçasının icra edilmesinden sorumlu kişilere ait şartları tanımlamakta mıdır?	İş devamlılığının ana çatısını örgütün tanımlanmış vazife analizleri oluşturmaktadır. Her bir görevin hangi birim tarafından yapılacağı görev tanım formlarında belirtilmiş olup, düzenli olarak yapılan tatbikatlarda ortaya çıkan durumlar görev analiz birimi personeli tarafından değerlendirilmeye tabi tutulmaktadır. Bu sayede sistemin aksayan yönleri ortaya çıkartılarak, düzeltici işlemlerin hangi birimler tarafından yapılacağı tanımlanmaktadır.
9.1.5	İş devam planının test edilmesi, idamesi ve yeniden değerlendirilmesi	İş devamlılık planlarının güncel ve etkin oldukları düzenli olarak test edilmekte midir? İş devamlılık planları, devamlılık etkinliğini güncelleştirme ve düzenli olarak gözden geçirmeyle idame ettirilmekte midir? Yöntemler, iş devamlılığı meselesine uygun bir şekilde hitap eden örgüt çapında program değişiklik yönetimini içermekte midir?	İş devamlılık planlarının etkin ve güncel olarak tutulması için diğer örgütlerden gelen ilave personelin tespit ettiği aksaklıklar ayrı bir analize tabi tutulmaktadır. Bu sayede örgüt içerisinde farkına varılamayan aksaklıklar ortaya çıkartılmaktadır. Buna benzer uygulamalar çapraz eğitim olarak adlandırılmaktadır.

EK-11	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
Uyum			
10.1	***Yasal ihtiyaçlara uyum***		
10.1.1	Uygulanabilir kanunların tanımlanması	Her bir bilgi sistemi için ilgili kanuni, düzenleyici ve yükleniciye ait ihtiyaçlar açıkça tanımlanmış ve belgelenmiş midir? Bu ihtiyaçları karşılamaya yönelik kişisel sorumluluklar ve özel kontroller tanımlanmış ve belgelenmiş midir?	Kanunların ilgili maddeleri yönergelere ithal edilmiş olup, kullanıcıların sorumlu oldukları hususlar, açık ve net bir biçimde belirlenmiştir. Bu konuyla ilgili düzenleyici maddeler, denetleme kontrol listesi haline getirilmiştir.
10.1.2	Fikri mülkiyet hakları (IPR - Intellectual Property Rights)	Telif hakları, tasarım hakları ve ticari haklar gibi fikri mülkiyet hakları bağlamında materyalin kullanımı ile ilgili yasal kısıtlamalara uyumu temin edecek yöntemler var mıdır? Yöntemlere iyi bir şekilde uyulmakta mıdır? Patentli yazılım ürünleri, belirlenen makinelerde kullanımını sınırlayan lisans anlaşmalarına uygun olarak temin edilmekte midir? Tek istisnai durum, yazılımın kendi kopyasının yedeklenmesidir.	Örgütün sahip olduğu bilgi sistemleri üzerinde lisanssız herhangi bir yazılımın kullanılmasına müsaade edilmemektedir. Kullanıcı istekleri doğrultusunda yüklenecek yazılımların lisans belgesi ibrası talep edilmektedir. Örgüt tarafından kullanılacak bütün yazılımlar, merkezi olarak temin edilmekle beraber, istisnai durumlarda, ihtiyaç duyulan yazılım ticari piyasadan lisanslı olarak satın alınmaktadır. Örgütün eline ulaşan bütün yazılımlar, ilk kullanımdan önce kopyalanarak yedeklenmektedir.
10.1.3	Örgütsel kayıtların muhafazası	Örgütün önemli kayıtları, yanlış işlev ve imha sonucunda kayıp olmasına karşı koruma altında mıdır?	Dijital ortamda bulunan bütün kayıtlar düzenli olarak yedeklenmektedir. Diğer, basılı evrak, önemine binaen ilgili birimlerce fotokopi ile

EK-11	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			çoğaltılarak saklanmaktadır.
10.1.4	Kişisel bilgilerin gizliliği ve verilerin korunması	Veri ve kişisel bilgilerin gizliliğini korumaya yönelik yönetim yapılandırması ve kontrolü oluşturulmuş mudur?	Örgütle ilişkisi olmayan kişisel bilgilerin hassas bilgi sistemlerinde saklanmasına müsaade edilmemektedir. Ancak resmi manadaki kişisel bilgiler, sadece idari kısım personeli ve kişinin kendisi tarafından işlem görecek şekilde saklanmaktadır.
10.1.5	Bilgi işleme kolaylıklarının kötü kullanıma karşı korunması	Bilgi işlem kolaylıklarının işle ilgisi olmayan ve müsaade edilmeyen amaçlar için yönetim onayı olmadan kullanımı bu kolaylığın uygun olmayan kullanımı olarak değerlendirilmekte midir? Sisteme giriş esnasında girilen sistemin özel bir sistem olduğunu ve yetkisiz erişime izin verilmediğini ikaz eden uyarı mesajı, bilgisayar ekranında gösterilmekte midir?	Bilgi işlem kolaylıklarının sadece örgütün resmi amaçlarına hizmet eden alanlarda, kullanılacağı, örgüt politikası olarak yönergelere işlenmiştir. Yönergelerin uygulanması en üst örgüt yönetimi tarafından zaman zama denetlenmektedir. Her sisteme giriş esnasında ekranda girilen sistemin hassas bilgi içeren bir sistem olduğu ve yetkisiz kullanımına müsaade edilmediği açık bir biçimde uyarı mesajı ile gösterilmektedir.
10.1.6	Kriptografik kontrollerin düzenlenmesi	Kriptografik kontrol düzenlemeleri bölgesel ve milli mutabakata uymakta mıdır?	Kriptografik kontroller yılda en az bir defa olmak üzere yapılmaktadır. Bu kontroller örgütün bağlı olduğu, daha üst kademelerce hazırlanmış yönerge esaslarına göre yapılmaktadır. Bu yönergeler, uluslar arası mutabakata dayanan standartlara göre hazırlanmıştır.

EK-11	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
10.1.7	Delillerin toplanması	İlgili işlevler hakkındaki delillerin toplanması yasal ve endüstriyel uygulamalara uygun mudur?	Herhangi bir olayla ilgili delil toplanması daha önceden belirlenmiş ve tamamen yasal olan özel kurallara tabidir.
10.2	***Teknik uyum ve güvenlik politikalarının gözden geçirilmesi***		
10.2.1	Güvenlik politikalarına uyum	Örgüt içindeki bütün alanlar, düzenli gözden geçirme işlemleri açısından, güvenlik politikaları, standartları ve yöntemlerine uyumluluk yönüyle dikkate alınmakta mıdır?	Bütün denetleme, gözden geçirme ve yeniden değerlendirme işlemleri bilgi güvenliği politikası ve stratejisi paralelinde yapılmaktadır. Bilgi güvenliğini oluşturan politikalar, teknolojik gelişmelere uygun olarak yılda bir defa gözden geçirilerek güncellenmektedir.
10.2.2	Teknik uyumluluk kontrolü	Bilgi sistemlerinin, güvenlik uygulama standartlarına uyumluluğu düzenli olarak kontrol edilmekte midir? Teknik uyumluluk kontrolleri yetkili ve uzman personelin kendisi tarafından veya bu personelin yönetimi altındakiler tarafından yapılmakta mıdır?	Herhangi bir bilgi sistemi alınmadan önce kullanılacak bölgenin koruma seviyesine göre incelemeye tabi tutulmaktadır. Örgütün bulunduğu bölge bilgi güvenliği açısından tam korumalı alan olduğundan dolayı satın alınacak teçhizatta herhangi bir kısıtlama yoktur. Ancak herhangi bir intikal durumunda gidilecek bölgenin koruma durumuna göre alınacak teçhizat ayrıca belirlenmektedir. Tam korumalı olmayan bölgelerde kullanılacak teçhizat tavsiye edilen ürün listesinden seçilmek zorundadır. Tavsiye edilen ürün listesinde bulunmayan bir teçhizat alınmak istendiğinde, merkezi kontrol birimine gönderilerek gerekli tetkiklerinin yapılması

EK-11	Bilgi Güvenliği Yönetimi BS 7799.2:2002 Denetleme Listesi		
İlgi	Denetleme sahaları, amaç ve sorular		
Kontrol Listesi	**Bölüm**	**Denetleme Sorusu**	**Bulgular**
			sağlanmaktadır.
10.3	***Sistem denetleme etkenleri***		
10.3.1	Sistem denetleme kontrolleri	İşletimsel sistemlerin kontrolleri hakkındaki faaliyetler ve denetleme ihtiyaçları dikkatlice planlanmakta ve iş işlevlerinin aksamasına dair riski en aza indirmek için konu hakkında mutabakat sağlanmakta mıdır?	Bilgi güvenliği ile ilgili denetlemeler, hiçbir şekilde işletimsel sistemlerin ve örgütün faaliyetinin duraklamasına sebebiyet verecek şekilde planlanamaz. Ancak zaruri olan işlemler, örgüt faaliyetinin en az olduğu zaman aralıklarında yapılacak şekilde planlanır. Bu konudaki yetki örgütün en üst kademe yöneticisine aittir.
10.3.2	Sistem denetleme araçlarının korunması	Muhtemel kötü kullanım ve kötü niyetli işbirliğinin önlenmesi için yazılım veya veri dosyaları gibi sistem denetleme araçlarına erişim korunmakta mıdır?	Sistem denetleme araçları sadece sistem yöneticisi yetkilerine sahip muhabere bilgi işlem personeli tarafından kullanılabilmektedir. Bu araçların çoğu sadece sunucular üzerinde çalıştırılabilmektedir. Sunuculara dışarıdan erişim mümkün değildir.

KAYNAKÇA

ACE Security Directive AD 70-1, SUPREME HEADQUARTERS ALLIED POWERS EUROPE, BELGIUM, Part V Chapter1, 1 January 1997.

Albright, Jack G., **The Basics of an IT Security Policy,** March 2002.

Araşan, Ahmet, İnternette Ticaret, **Hürriyet Gazetesi,** Finans'99 Eki, 24 Kasım 1999.

Bahtiyar, Ziya, **Virüsler ve Güvenlik,** Pusula Yayıncılık ve İletişim Ltd., İSTANBUL 2003.

Barutçugil, İsmet, **Bilgi Yönetimi,** Kariyer Yayıncılık İletişim, Eğitim Hiz. Ltd. Şti., İstanbul, Nisan 2002.

BAYKAL, Nazife, **Bilgisayar Ağları,** SAS Bilişim Yayınları, 1nci baskı, 2001.

Bozkurt, Veysel, **Bilgi ve Toplum,** Elektronik Ticaretin Ekonomik ve Toplumsal Boyutu, 1999/2.

California Counties"Best Practices" Information Security Program, California County Information Services Directors Association, CCISDA Information Security Forum, March 2002.

Chang, Beom-Hwan, Kimb, Dong-Soo, Kimb, Hyun-Ku, Naa, Jung-Chan, Tai-Myoung Chung, "Active security management based on Secure Zone Cooperation" **Science Direct,** South Korea, 2003.

Chip Dergisi, **PC'niz İçin Koruma Aşısı,** Haziran 2003.

Cooper, James Arlin, **Computer and Communications Security,** Intertext Publications McGraw-Hill Book Company, 1989.

Crane, Earl, **Information Security Management at A-OK, Inc.,** A case study at Carnegie Mellon University, August 2000.

Çölkesen, Rifat ve Örencik, Bülent, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri,** Papatya Yayınları, İstanbul, 2002.

Davis, Rick, **The Unlikely Hereos of Cyber Security,** The Information Management Journal, May/June 2003.

Desman, Mark B., "Building an Information Security Awareness Program" Boca Raton, FL:

CRC Press LLC., **Journal of Government Information,** 2002.

Donaldson, Alistair & Walker, Phil, "Information governance—a view from the NHS" **International Journal of Medical Informatics,** 2003.

Eduardo Gelbstein, **Managing Information Security,** International Computing Centre, Genava, Switzerland.

Gordon, Lawrance A. & Loeb, Martin P., **Economic Aspects of Information Security,** University of Maryland, College Park, June 27, 2003.

Hacker Avında Son Perde, Chip dergisi, İstanbul, Haziran 2003.

Hansen, Rhein, **The Elements of a Security Management System,** IT University of Copenhagen.

Hipermarketinizi Çöpe Atın, **Milliyet Gazetesi,** 29.07.1999.

Internet temelli satışların gelişimi, **IDC,** 1998. http://www.pwcglobal.com/gx/eng/ins-sol/spec-int/knapp-05.htm.

İnternet Tarihi", http://www.romannet.net/tr/domain/history.htm#top Erişim Tarihi: 4 Nisan 2004.

İnternet'in Tarihçesi" www.kou.edu.tr/idari/bilgiislem/ders/inttarih.htm Erişim Tarihi: 4 Nisan 2004.

İnternetin Tarihçesi, http://www.aydesign.net/internetintarihcesi.htm Erişim Tarihi: 4 Nisan 2004.

Kelly, Grant & McKenzie, Bruce, **Security, privacy, and confidentially issues.**

Khalfan, Abdulwahed Mo., "Information security considerations in IS/IT outsourcing projects:a descriptive case study of two sectors" **International Journal of Information Management** sayı 24, UK, 2004.

KOÇEL, Tamer, **İşletme Yöneticiliği,** Beta Yayınları, İstanbul, 8.Baskı, Mart 2001.

Kurose, James F. & Ross, Keith W., **Computer Networking,** Pearson Education Inc., 2003.

Mukkamala, Srinivas "Intrusion detection using an ensemble of intelligent paradigms" **Journal of Network and Computer Applications,** USA, 7 Jan 2004.

NATO Handbook, NATO Office of Information and Press, 1110 Brussels – Belgium, 2001.

Outsourced Information Security Management, Internet Security Systems Publication, Atlanta/USA, June 2002.

Post, Gerald V. ve Anderson, David L., **Management Information Systems,** Richard D. Irwin, a Times Mirror Higher Education Group, Inc. Company, 1997.

Solimana,Khalid S., Janz,Brian D., "An exploratory study to identify the critical factors affecting the decision to establish Internet-based interorganizational information systems" **Science Direct,** USA, 25 June 2003.

Stallings, William, **Network Security Essentials – *Applications and Standards*,** Pearson Education International, 2nd Edition.

Taka, Sungwoo, Dixitb, Sudhir, Parka, E.K., "An end-to-end home network security framework" **Computer Communications,** USA, 2 Oct 2003.

Tanenbaum, Andrew S. ve Steen, Maarten Van, **Distributed Systems Principles and Paradigms,** Vrije Universiteit Amsterdam, Netherlands, 2002.

Thompson, Maryan Jones, "My How We've Grown", **The Industry Standard,** April 26, 1999, (http://www.thestandart.com).

Vlachos, Vasileios, "Security applications of peer-to-peer networks", **Science Direct,** Athens/Greece, 14 Jan 2004.

Vliet, Hans Von, **Software Engineering – Principles and Practice,** John Qiley & Sons Ltd. Baaffins Lane, Chichester, West Sussex 1019 1UD, England, Second Edition.

DİZİN

I

K

M

O

P

R

S

T

U

V

W

Y

Z