

İNTERNET GÜVENLİĞİ KAVRAMLARI VE
TEKNOLOJİLERİ

**T.C. YÜKSEKÖĞRETİM KURULU
DOKÜMANTASYON MERKEZİ**

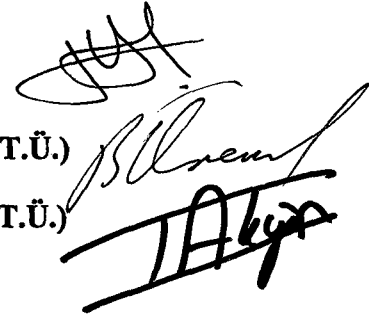
YÜKSEK LİSANS TEZİ
Müh. Osman KARAAHMETOĞLU
504961641

104119

104119

Tezin Enstitüye Verildiği Tarih : 11 Haziran 2001
Tezin Savunulduğu Tarih : 22 Haziran 2001

Tez Danışmanı : Doç.Dr. A.Coşkun SÖNMEZ
Diğer Jüri Üyeleri : Prof.Dr. Bülent ÖRENCİK (İ.T.Ü.)
Doç.Dr. B.Tevfik AKGÜN (Y.T.Ü.)



HAZİRAN 2001

ÖNSÖZ

Bilgi toplumuna geçmeden önceki zamanlarda, insanlar değerli eşyalarını ve evraklarını kasalarına kilitlemekte veya bankalarda saklamaktayken, atm kartlarına kredi kartlarına ve hesap cüzdanlarına, çalınma tehlikesine karşı gözleri gibi bakmaktaydılar. Bugün, bilgi toplumunda, bilgi insanların sahip olduğu en değerli varlıktır. Artık öyle bir çağda yaşıyoruz ki, bilgi kurumların, kişilerin itibarı olmuştur. İnsanların yararı için varolan teknolojinin insan hayatına zarar vermesinin yaşandığı bu çelişkili dönemde gerçekleştirmiş olduğum bu çalışmada, insanların itibarını (bilgiyi) koruyacak teknolojileri araştırarak, uygulanabilir bir bilgi güvenliği çözümü geliştirmeyi amaçladım.

Bu çalışmada bana engin tecrübeleriyle yol gösteren tez danışmanım sayın Doç. Dr. A.Coşkun SÖNMEZ' e, yakın arkadaşlarım Ebru EROĞLU, Lütfi YELKENCİ, Savaş KÖSE' ye ve bugünlere gelmemde çok büyük emekleri olan abim Erol KARAAHMETOĞLU ve 1997 yılında beyin metastazından kaybettiğim babam Lütfi KARAAHMETOĞLU' na sonsuz teşekkürlerimi sunarım.

Haziran 2001

Osman KARAAHMETOĞLU

İÇİNDEKİLER

KISALTMALAR.....	XII
TABLO LİSTESİ.....	XIV
ŞEKİL LİSTESİ	XV
ÖZET	XVII
SUMMARY	XVIII
1 GİRİŞ	1
1.1 Güvenlik Hedefleri.....	1
1.1.1 Kişiy e özellik	2
1.1.2 Bütünlük	2
1.1.3 Hazır bulunabilirlik	3
1.2 Güvenlik Seviyeleri	4
1.2.1 Güvenilen bilgisayar güvenliği değ erlendirme ölçütleri (Trusted computer security evaluation criteria – TCSEC).....	5
2 İLETİŞİM AĞ LARI BİLEŞ ENLERİ VE PROTOKOLLERİ	6
2.1 İletişim Ağ ları.....	6
2.1.1 İletişim ağ ları yapısal modeli.....	6
Açık sistem bağlantıları (Open systems interconnection-OSI) başvuru modeli.....	6
Bağ lantı aygıtları.....	8
2.2 Protokoller	12
2.2.1 TCP/IP protokol kümesi	13
İnternet protokolü (IP)	13
İletişim denetleme protokolü (TCP).....	14
Kullanıcı veri birimi iletişim protokolü(UDP)	14
Kapı(Port)	15
Yuva(Socket).....	15
2.2.2 Seri hat internet iletişim protokolü (Serial line internet protocol – SLIP)	15
2.2.3 IPX/SPX Protokolleri.....	16
2.2.4 NWLINK	16

2.2.5	NetBEUI protokolü	16
2.2.6	Apple talk protokolü	16
2.2.7	Veri bağlantı denetleme (Data link control – DLC) protokolü	16
2.3	İnternet.....	17
2.3.1	İnternet hizmetlerinin yapısı	17
2.3.2	İsimlendirme	17
3	BİLGİSAYAR SALDIRILARI	20
3.1	Bigisayar Saldırılarının Tarihsel Gelişimi	20
3.2	Saldırgan Tipleri	22
3.2.1	Meraklı Joe' lar	23
3.2.2	Kod parçası çocukları	23
3.2.3	Wannabes	23
3.2.4	Seçkinler.....	23
3.3	Program Saldırıları	24
3.4	Geçmişten Bugüne Gündem Oluşturan Bilgisayar Saldırıları.....	25
4	GÜVENLİK TEKNOLOJİLERİNE GİRİŞ	28
4.1	İnternet' e Bağlanıldığında Karşılaşabilecek Güvenlik Sorunları.....	28
4.1.1	Gizli bilgiyi korumak	28
	Ağ paket dinleyicileri	29
	IP taklidi.....	30
	Şifre saldırıları	30
	Hassas bilginin dağıtımı.....	31
	Ortakdaki adam (Man-in-the-middle) saldırıları.....	31
4.1.2	Ağınızı korumak: İç ağ sistem bütünlüğünü sağlamak	31
	Ağ paket dinleyicileri	32
	IP taklidi.....	32
	Şifre saldırıları	33
	Hizmet dışı bırakma.....	33
	Uygulama katmanı saldırıları	33
4.2	TCP/IP'nin Zayıf Noktaları.....	34
4.2.1	TCP sıralama numarasının tahmini.....	34
4.2.2	Kaynak yönlendirme (Source routing).....	36
4.2.3	Bilgi yönlendirme protokolü (Routing information protokol–RIP) saldırısı.....	36
4.2.4	ICMP saldırısı	36
4.2.5	Kimlik doğrulama sunucusu	36

4.2.6	Posta ofisi protokolü (Post office protocol-POP)	37
4.2.7	Alan isimlendirme sistemi (Domain name system-DNS)	37
4.3	Bilinen Güvenlik Gedikleri	37
5	KRİPTOGRAFİK KAVRAMLAR VE TEKNOLOJİLER.....	39
5.1	Giriş	39
5.2	Şifreleme ve Deşifreleme	40
5.2.1	İşlem biçimleri.....	40
5.2.2	İlkel şifreleme algoritmaları	41
5.2.3	Simetrik anahtarlı şifreleme	41
	Simetrik anahtarlı şifreleme algoritmaları	42
5.2.4	Açık anahtarlı şifreleme	44
	RSA Algoritması	45
5.2.5	Anahtar uzunluğu ve şifreleme kuvveti.....	45
5.3	Sayısal İmzalar	46
5.3.1	Çarpma Algoritmaları.....	47
5.3.2	Sayısal imza standardı	48
5.4	Sertifika ve Kimlik Doğrulama	49
5.4.1	Kimlik doğrulama	50
	Şifre temelli kimlik doğrulama	51
	Sertifika temelli kimlik doğrulama	52
5.4.2	Sertifikalar nasıl kullanılır?	53
	Sertifika tipleri	53
	SSL Protokolü.....	54
	SET Protokolü	54
	İmzalanmış ve şifrelenmiş elektronik postalar	55
	Form imzalama	56
	Nesne imzalama	56
5.4.3	Sertifika içeriği	56
	Kimlik doğrulama algoritmaları	59
6	FIREWALL	62
6.1	IP Adresinin Süzgeçten Geçirilmesi.....	62
6.1.1	TCP/UDP kapı süzgeçleme	63
	Sunucu tarafı TCP/UDP kapı süzgeçleme	64
	İstemci tarafı TCP/UDP kapı süzgeçleme	64
6.2	Uygulama Vekil Sunucuları	65

6.3	Durumsal İnceleme Süzgeçleme veya Devingen Paket Süzgeçleme..	66
6.4	Firewall Mimarileri.....	67
6.4.1	İkili konumlandırılmış geçityolu (Dualhomed Gateway)	67
6.4.2	İzleyen yönlendirici (screening router) ve bastion konak (bastion host)	68
6.4.3	İzleyen yönlendirici ve ikili konumlandırılmış geçityolu	68
6.4.4	İzlenen alt ağ (screened subnet) ve bir DMZ.....	69
6.4.5	İzlenen alt ağ (screened subnet) ve iki DMZ	70
6.4.6	Güvenli sunucu ağı.....	70
7	YETKİSİZ ERİŞİMLERİ SEZME (INTRUSION DETECTION).....	73
7.1	Yetkisiz Erişimleri Sezme Çalışmalarının Tarihçesi.....	73
7.2	Endüstriyel Kurumların Tecavüzkar Saldırı Çekincesi	74
7.2.1	Saldırılarda gözlenen artış	74
7.2.2	Kurum içi saldırıların maliyetinin diğerlerine oranla daha yüksek olması.....	74
7.2.3	Kurum içerisinde insandan fazla bilgisayarın olması sonucu riskin artması	75
7.2.4	Sisteme yetkisiz erişimin insanlarda bir zevk haline dönüşmesi	75
7.2.5	Güvenlik tehditlerini umursamamanın pazar üstünlüğünü kaybettirmesi	75
7.3	Geleneksel Saldırı Sezme Sistemleri	76
7.3.1	Çevre temelli izleme ve kontrol aletleri.....	76
7.3.2	Ağ temelli trafik izleyicileri	76
7.3.3	Konak temelli bilanço kaydı izleyicileri	78
7.4	Saldırı Sezme Sistemlerinde Düşünülmesi Gereken Önemli Elemanlar.....	79
7.4.1	Yetenek seviyesi.....	79
7.4.2	Cevap verme mekanizmaları	81
7.5	Sezilemeyen Saldırıları ve Yanlış Sezgiler.....	81
7.5.1	Ölçeklenebilirlik ve ortamları kapsayabilirlik	82
7.5.2	Merkezi yönetim	82
7.5.3	Başarım	83
8	GÜVENLİK POLİTİKASI	84
8.1	Giriş	84
8.2	Güvenlik Politikasının Özellikleri	84
8.3	Temel Yaklaşım	85

8.3.1	Güvenlik politikası kimler tarafından belirlenir?	86
8.3.2	Güvenlik politikası kimleri kapsar ve sorumluluklar nedir?.....	86
8.4	Tehlike Değerlendirmesi	86
8.4.1	Varlık tespiti.....	86
8.4.2	Tehditlerin tespiti	87
8.4.3	Maliyeti hesaplamak	87
8.5	Güvenlik Politikasının Önemli Noktaları	87
8.6	Ağ Sunucularının Güvenliğinin Sağlanması.....	89
8.6.1	Güvenli bir geçiş planının oluşturulması.....	89
8.6.2	Sunucu seçiminde göz önüne alınması gereken güvenlik gereksinimleri	90
8.6.3	İşletim sistemi ve uygulama yazılımlarının güncel tutulması	91
8.6.4	Sunucu makinesi üzerinde sadece gerekli ağ ve işletim sistemi hizmetlerinin sunulması	92
8.6.5	Bilgisayarlar üzerinde kullanıcı kimlik doğrulama yapılandırmasının yapılması	93
8.6.6	İşletim sisteminin uygun nesne, alet ve dosya erişim kontrolleri ile yapılandırılması	94
8.6.7	Sistem ve ağ kayıt mekanizmalarının çalıştırılması.....	94
8.6.8	Bilgisayar dosya yedekleme mekanizmalarının yapılandırılması.....	95
8.6.9	Bilgisayarların virüs ve benzeri programsal tehditlerden korunması	95
8.6.10	Bilgisayarların uzaktan güvenli sistem yönetimi için yapılandırılması	96
8.6.11	Bilgisayara sadece uygun fiziksel erişimlere izin verilmesi	97
8.7	Web Sunucu Güvenliğinin Sağlanması.....	97
8.7.1	Web sunucusunun genel ağlar ve kurumun iç ağlarından ayrılması.....	97
8.7.2	Web sunucusunun uygun nesne , alet ve dosya erişim kontrolleri ile yapılandırılması	98
8.7.3	Web sunucusuna özel kayıt mekanizmalarının tanımlanması ve etkin kılınması.	99
8.7.4	Web Sunucusu için program kod parçaları ve plug-in'lerin seçiminde güvenlik imalarının düşünülmesi.....	100
8.7.5	Plug-in' ler, kod parçaları ve programların işlevselliğini azaltmak için web sunucusunun yapılandırılması	101
8.7.6	Web sunucusunun gerekli olduğunda kimlik doğrulama ve şifreleme tekniklerini kullanacak şekilde yapılandırılması	102

8.7.7	Web sunucusunun içeriğinin yetkili bir kopyasının güvenli bir sunucuda saklanması	103
8.7.8	Web sunucusunun bilinen saldırılara karşı konunması	103
8.8	Firewall' ın Gerçek Ortama Geçişİ.....	104
8.8.1	Bir firewall sisteminin tasarlanması	104
8.8.2	Gerekli firewall yazılım ve donanımının belirlenmesi.....	104
8.8.3	Firewall ile ilgili teknik bilgiler içeren belgeler, eğitim ve teknik desteklerin edinilmesi	105
8.8.4	Firewall yazılımı ve donanımının kurulması	105
8.8.5	IP yönlendirmenin yapılandırılması	105
8.8.6	Firewall paket süzgeçlemenin yapılandırılması	106
8.8.7	Firewall kayıt tutma ve uyarı mekanizmalarının yapılandırılması....	106
8.8.8	Firewall sisteminin denenmesi	106
8.8.9	Firewall sisteminin kurulması	107
8.8.10	Firewall sisteminin işletim evresine geçirilmesi	107
8.9	Saldırlara Cevap Verilmesi	107
8.9.1	Saldırlara cevap vermek için politika ve yordamların oluşturulması	107
8.9.2	Saldırlara cevap vermeye hazırlanılması	108
8.9.3	Saldırının özelliklerini belirlemek üzere mevcut tüm verilerin analiz edilmesi	109
8.9.4	Saldırı ve saldırının gelişimden haberdar edilmesi gerekenlerin tümü ile iletişim kurulması.....	110
8.9.5	Saldırı ile ilgili bilgilerin toplanması ve korunması	110
8.9.6	Saldırıyı kontrol altına almak için kısa vadeli çözümlerin uygulanması	111
8.9.7	Her türlü saldırgan erişiminin engellenmesi	112
8.9.8	Sistemin normal işletimine geri döndürülmesi	112
8.9.9	Öğrenilen güvenlik derslerinin tanımlanması ve gerçekleşmesi	113
9	BİLGİ GÜVENLİĞİNDE HUKUKSAL YAKLAŞIM	114
9.1	Giriş	114
9.2	Türk Hukukunda İmzaya İlişkin Hükümler:.....	115
9.3	1991 Yılında Türk Ceza Kanuna Eklenen Hükümlerle Tarif Edilen Bilişim Alanında Suçlar ve Cezaları	116
10	ÖNERİLEN GÜVENLİK ÇÖZÜMÜ	118
10.1	Giriş	118

10.1.1	Önerilen DNS sunucu yapısı.....	120
10.1.2	Saldırı sezme sistemleri karşılaştırması	124
10.2	Genel Güvenlik Politikası Taslağı	127
10.2.1	Tanıtım ve amaç.....	127
10.2.2	Konu	127
10.2.3	Tanımlar	127
10.2.4	Bilgi sistemleri güvenliği için sorumluluklar	127
10.2.5	Kullanıcı tanımları ve şifreleri.....	128
10.2.6	İşe alma uygulamaları.....	128
10.2.7	Çalışanların sorumlulukları	129
10.2.8	Cihazlara erişim.....	130
10.2.9	Veriye erişim.....	130
10.2.10	Özel erişim	130
10.2.11	Yazılım kontrolü.....	131
	Virüs kontrolü.....	131
	Etkileşimsel yazılım kontrolü	133
10.2.12	Şifreleme	133
10.2.13	Güncelleme politikası.....	133
10.2.14	Saldırı sezme politikası.....	133
10.2.15	Acil durum planı	134
10.2.16	Onay.....	134
10.3	Windows NT Güvenliği.....	134
10.3.1	Güncellemeler	134
10.3.2	Kurulum	135
10.3.3	Genel politikalar	135
10.3.4	Dosya sistemi ve kayıt erişim kontrolü ayarları	138
10.3.5	Kullanıcı hesapları	140
10.3.6	Gruplar	140
10.3.7	Şifreler	141
10.3.8	Kullanıcı hakları	141
10.3.9	Ağ güvenliği.....	141
10.3.10	Uzaktan erişim hizmeti (Remote access service – RAS).....	142
10.4	UNIX ve NT İşletim Sistemlerinin Karşılaştırılması	143
10.5	“Checkpoint Firewall-1”	146
10.5.1	Kurulumdan önce yapılması gerekenler.....	146
10.5.2	Kurulum	147
10.5.3	Kayıt komutları.....	150

	"Excessive log grace period (sec)"	150
10.5.4	Uyarı komutları:	150
	"Popup alert command"	150
	"Mail alert command"	150
	"SNMP trap alert command"	152
	"User defined alert command"	153
	"Anti spoof alert command"	153
	"User authentication alert command"	154
	"IP options drop track"	154
	"Log established TCP packets"	154
10.5.5	Hizmetler	154
	"Enable FTP PASV connections"	154
	"Enable RSH/REXEC reverse stderr connections"	154
	"Enable RPC control"	154
10.5.6	Diğer Güvenlik önlemleri.....	155
	"Log viewer resolver properties"	155
	"Security server settings"	155
	"SYNDefender settings"	155
	"Ping-Of-Death" saldırısı	156
	"Java Applet" lerin engellenmesi	157
10.5.7	Önerilen Kurallar.....	157
	İstemcilerden dışarıya DNS sorguları.....	157
	İçsel DNS sunucudan internet' e alan iletimi	157
	"Firewall-1" sisteminin korunması	158
	Kural veritabanındaki en son kural.....	158
	"Firewall-1" de "Drop" ve "Reject" farkı.....	158
10.5.8	Implicit kurallar.....	158
	"DNS rule zero rules"	158
	"Firewall-1 control connections"	159
	"TCP session timeout"	159
	"Accept UDP replies"	159
	"Reply timeout"	159
	"Accept outgoing packets"	159
	"Accept RIP"	159
	"Accept ICMP"	160
10.5.9	Başarım	160
10.6	"RealSecure"	160
10.6.1	Ağ yapılandırmasının sıkılaştırılması	160

	"RealSecure" gizlilik biçimi.....	160
	Erişim kontrollerinin kullanılması.....	161
10.6.2	"Firewall-1" ile "RealSecure" un bütünleştirilmesi.....	161
10.6.3	"RealSecure" kurulumu.....	162
	"RealSecure" istemci kurulumu.....	162
	"RealSecure" motor kurulumu.....	163
	Kurulum sonrası.....	163
	"RealSecure" kullanımı.....	164
	"RealSecure" başarımı.....	165
10.6.4	"Mailsweeper" Elektronik Posta Vekili.....	166
	Yapılandırma.....	167
10.6.5	SSL 128 bit sertifika kurulumu.....	169
	Sertifika isteğinin üretilmesi.....	169
	Sertifikanın kurulması.....	169
11	SONUÇ.....	171
	KAYNAKLAR.....	174
	ÖZGEÇMİŞ.....	178

KISALTMALAR

TCSEC	: Trusted Computer Security Evaluation Criteria
TTAP	:Trust Technology Assessment Program
LAN	: Local Area Network
WAN	: Wide Area Network
OSI	: Open Systems Interconnection
TCP/IP	: Transmission Control Protocol/Internet Protocol
FTP	: File Transfer Protocol
SMTP	: Simple Mail Transfer Protocol
TCP	: Transmission Control Protocol
IP	: Internet Protocol
UDP	: User Datagram Protocol
SNMP	: Simple Network Management Protocol
IANA	: Internet Assigned Number Authority
DHCP	: Dynamic Host Configuration Protocol
DNS	: Domain Name Service
HTML	: Hypertext Markup Language
HTTP	: Hypertext Transfer Protocol
RIP	: Routing Information Protocol
DES	: Data Encryption Standard
IDEA	: International Data Encryption Algorithm
SHA	: Secure Hash Algorithm
SSL	: Secure Socket Layer
DMZ	: Demilitarized Zone
RAS	: Remote Access Service

ODBC	: Open Database Connectivity
NTFS	: Network File System
DNA	: Distributed Internet Architecture
TCO	: Total Cost of Ownership
RPC	: Remote Procedure Call
ICMP	: Internet Control Message Protocol
vb.	: ve benzeri
bknz.	: bakınız
diğ.	: diğerleri



TABLO LİSTESİ

	<u>Sayfa No</u>
Tablo 2.1 İnternet hizmetleri	18
Tablo 5.1 RSA Algoritması ile şifreleme ve deşifreleme	46
Tablo 6.1 Firewall kural veritabanı	65
Tablo 6.2 Firewall mimarilerinin karşılaştırılması	71
Tablo 7.1 Saldırı sezme sistemlerinin saldırı aileleri açısından karşılaştırılması ..	80
Tablo 10.1 Firewall ürünleri karşılaştırması	122
Tablo 10.2 Saldırı sezme sistemlerinin karşılaştırması	126
Tablo 10.3 Önerilen nesne erişim hakları	139
Tablo 10.4 TCO (yıl başına, kurum başına)	144
Tablo 10.5 Windows NT ve UNIX güvenlik özellikleri karşılaştırması	145
Tablo 10.6 İç DNS sunucu kuralı	157
Tablo 10.7. "Firewall-1" koruma kuralı	158
Tablo 10.8. En son kural	158

ŞEKİL LİSTESİ

	<u>Sayfa No</u>
Şekil 2.1	OSI başvuru modeli 7
Şekil 2.2	Tekrarlayıcı ve OSI başvuru :modeli 9
Şekil 2.3	Köprü ve OSI başvuru modeli 10
Şekil 2.4	Bir köprü uygulaması 10
Şekil 2.5	Yönlendirici ve OSI başvuru modeli 11
Şekil 2.6	Bir yönlendirici uygulaması 11
Şekil 2.7	Geçityolu ve OSI başvuru modeli 12
Şekil 2.8	Üç yollu el sıkışma protokolü 15
Şekil 4.1	Üç yollu el sıkışma protokolü 35
Şekil 4.2	TCP sıralama numarasının çalınması 35
Şekil 5.1	Simetrik anahtarlı şifreleme 42
Şekil 5.2	Açık anahtarlı şifreleme 44
Şekil 5.3	Veri bütünlüğünün sağlanmasında sayısal imza kullanımı 47
Şekil 5.4	MD5 ve güvenli çırpı algoritması 48
Şekil 5.5	Çırpılmış mesaj doğrulama kodu MD5 ve SHA Algoritmaları 48
Şekil 5.6	Şifre kullanılarak istemcinin kimliğinin doğrulanması 52
Şekil 5.7	Sertifika kullanılarak istemcinin kimliğinin doğrulanması 52
Şekil 5.8	SSL sertifikası örneği 58
Şekil 5.9	Şekil 5.8.'deki sertifikanın 64 bit olarak kodlanmış şeklidir. 59
Şekil 5.10	Needham-Schroeder kimlik doğrulama protokolü 60
Şekil 5.11	Kerberos protokolü 61
Şekil 6.1	IP adresi süzgeçleme 63
Şekil 6.2	IP trafiğinin firewall tarafından kesilmesi 64
Şekil 6.3	Sunucu tarafı TCP/UDP kapı süzgeçleme 65
Şekil 6.4	İkili konumlandırılmış geçityolu (Dualhomed gateway) 67
Şekil 6.5	İzleyen yönlendirici ve bastion konak 68
Şekil 6.6	İzleyen yönlendirici ve ikili konumlandırılmış geçityolu 69
Şekil 6.7	İzlenen alt ağ (screened subnet) ve bir DMZ 70
Şekil 6.8	İzlenen alt ağ (screened subnet) ve iki DMZ 70
Şekil 6.9	Güvenli sunucu ağı 72
Şekil 7.1	1998 CS/FBI çalışması : saldırı ve kötüye kullanım tipleri 75
Şekil 7.2	1998 CS/FBI bilgisayar suçları ve internet güvenliği 76
Şekil 7.3	Ağ temelli saldırı sezme yöntemi 77
Şekil 7.4	Konak temelli bilanço kaydı izleyicileri 79
Şekil 10.1	Uygulanabilir güvenlik çözümü 121
Şekil 10.2	Özel erişim istek belgesi örneği 131
Şekil 10.3	Özel erişim sözleşmesi örneği 132
Şekil 10.4	Windows NT IP iletme seçim ekranı 147
Şekil 10.5	Windows NT ağ bağlamaları ekranı 148
Şekil 10.6	"Firewall-1" kurulum tipi seçme (Selecting setup type) ekranı 149
Şekil 10.7	"VPN-1 & Firewall-1 gateway/server module" ekranı 151
Şekil 10.8	Lisans bilgileri ekranı 151
Şekil 10.9	GUI istemcisi yönetici tanımlama ekranı 152
Şekil 10.10	Dışsal arabirim ekranı 153

Şekil 10.11 "Real Secure" motor seçenekleri ekranı	161
Şekil 10.12 Windows NT TCP/IP güvenliği ekranı	162
Şekil 10.14 Motor yerleşimi tanımlama ekranı	164
Şekil 10.16 Real Secure Başarımı	166
Şekil 10.17 Gereksiz elektronik posta (antispam) yapılandırması	167
Şekil 10.18 Taklit önleme (antispoofing) yapılandırması	168
Şekil 10.19 Virüs tarama yazılımı tanıtma	169



Üniversitesi	: İstanbul Teknik Üniversitesi
Enstitüsü	: Fen Bilimleri
Anabilim Dalı	: Kontrol ve Bilgisayar Mühendisliği
Programı	: Kontrol ve Bilgisayar Mühendisliği
Tez Danışmanı	: Doç. Dr. A.Coşkun SÖNMEZ
Tez Türü ve Tarihi	: Yüksek Lisans – Haziran 2001

ÖZET

İNTERNET GÜVENLİĞİ KAVRAMLARI VE TEKNOLOJİLERİ

Osman KARAAHMETOĞLU

Bu çalışmada, internet güvenliği kavramları ve teknolojileri üzerine yapılan yoğun bir araştırmadan sonra uygulanabilir bilgi güvenliği çözümü elde edilmiştir. Bu bilgi güvenliği çözümü, maliyet, ölçeklenebilirlik, tutarlılık, gizlilik ve güvenilirlik ölçütlerini sağlamaktadır. Bu bilgi güvenliği çözümünün oluşturulmasında ilk olarak kurumun güvenlik ihtiyaçları belirlenmiş ve bu ihtiyaçlar doğrultusunda, bilgi güvenliği çözümlerinin vazgeçilmez elamanları olan firewall, saldırı sezme sistemleri, virüs tarama sunucuları, şüpheli durum sezme sunucuları ve yüksek şifreleme teknolojileri kullanılmıştır. Firewall' lar ile, yerel ağ ile internet arasında iki katmanlı bir koruma duvarı oluşturulmuş, bu duvarın aşılması olasılığı da düşünülerek, hassas bilginin değiş tokuş edildiği bölmelerde saldırı sezme sistemleri ve yüksek şifreleme teknolojileri kullanılmıştır. Bilgi güvenliğinde iyi ürünlerin kullanılmasından daha önemli olan bu ürünlerin çalıştığı ortamdır. Bu çalışmada bilgiyi korumak için oluşturulan sistemin maliyetinin bilginin değerinden daha fazla olmaması gerçeğini unutmayarak, Windows NT işletim sistemi sunucu işletim sistemi olarak seçilmiştir.

Anahtar Kelimeler: İnternet güvenliği, Uygulanabilir çözüm, Bilgi güvenliği elamanları , Uygulama ortamı, Maliyet

Bilim Dalı Sayısal Kodu: 619

University : İstanbul Technical University
Institute : Institute of Science and Technology
Science Programme : Control and Computer Engineering
Programme : Control and Computer Engineering
Supervisor : Ass. Prof. A.Coşkun SÖNMEZ
Degree Awarded and Date : MSC – June 2001

ABSTRACT

INTERNET SECURITY CONCEPTS AND TECHNOLOGIES

Osman KARAAHMETOĞLU

In this study, after an intensive research about internet security concepts and technologies, a feasible information security solution is proposed. This information security solution provides the criterions of the confidentiality, integrity, availability, reliability, scalability and cost. In the first phase of developing this information security solution, the security needs of an organization are determined and in according to this needs, firewalls, intrusion detection tools, antivirus servers, anomaly detection tools and high encryption technologies which are inalienable elements of the information security are used. Two layered protection wall are build between local network and internet by firewalls and and by taking the possibility of this wall being passed over into account, the intrusion detection tools and high encryption technologies are used at the segments which sensitive information are exchanged. The more important thing than using good products in information security is the platform on which these work. By not forgetting the fact that the cost of the system created for protecting the information is not higher than the value of it, the Windows NT operating system is selected as the server operating system.

Keywords: Internet security, Feasible solution, Information security elements, Application platforms, The cost

Science Code: 619

1 GİRİŞ

Kısa bir zaman öncesine kadar bilgi güvenliği, sadece büyük firmalar tarafından önemsenmekteydi. Sahip oldukları bilgilerin güvenliğini sağlamak amacıyla harcamış oldukları çabalar, bilgi güvenliği alanındaki çalışmaların temelini oluşturmaktaydı. Teknolojideki hızlı gelişmelerin sonucu olarak, günlük hayatımızda bilgisayar kullanımının yaygınlaşması, bu durumu değiştirmiştir. Artık bilgisayarlar stok değiş tokuşunu içeren ticari sistemlerden, maç sonuçlarını gösteren web sayfalarına kadar birçok işin çekirdeğinde kullanılır hale gelmiştir. Örneğin, bilgisayarlar banka hesaplarının, hastahane kayıtlarının, motorlu taşıtlar bölümünün raporlarının, kredi bilgilerinin tutulması vb. işleri yerine getirmede kullanılmaktadır. Açıkçası, kredi kartı olan veya ATM kartı kullanan herkes kişisel bilgilerinin gizliliği ve doğruluğu ile yakından ilgilidirler, doğal olarak da bilgi güvenliği ile yakından ilgili olmalıdırlar.

Bilgi güvenliği kaygısı neden vardır?

Bilgi güvenliği ile ilgili sorunların farkedilirliğini artıran birçok faktör vardır. Kişisel bilgisayarlar artık işyerlerinden çok ev kullanıcıları tarafından kullanılır hale gelmiştir. Ev kullanıcıları web, haber grupları ve elektronik posta gibi kaynaklara ulaşmak üzere internet kullanmayı tercih etmektedirler. Aynı zamanda ev kullanıcıları ve işyerleri basitliği ve uygunluğu açısından anında alışveriş ve elektronik ticareti ilgi çekici bulmaktadırlar. Bilgisayar kullanımındaki bu yaygınlık, sahip oldukları veriyi tehlikeye atabilecek yeteneğe sahip kişilerin sayısını artırmıştır.

Buna ek olarak, bilgisayar fiyatlarının düşmesi, insanları teknolojiyi daha yakından tanımaya getirmekle birlikte, bilgisayar temelli kaynakların kullanımını artırmıştır. Bunun sonucu olarak ortaya çıkan güvenlik açıkları, insanları olası finansal kayıp tehlikesiyle karşı karşıya bırakmıştır. Bir güvenlik açığı en kötü ihtimalle zaman kaybına ve verim düşüklüğüne sebep olur. Daha kötü ihtimaller göze alındığında güvenlik açığı finansal kayıplara da yol açabilir. Örneğin, bir avukatlık firması müşterilerine ait özel bilgileri çaldırırsa, itibar ve müşteri kaybına uğrar. Hatta para cezası ve tazminat gibi yasal zorunluluklarda da karşı karşıya kalabilir.

1.1 Güvenlik Hedefleri

Bilgi güvenliğinin üç ana görünüşü vardır:

1. Kişiy e özellik,
2. Bütünlük,
3. Hazır bulunabilirlik.

1.1.1 Kişiy e özellik

Kişiy e özellik, bilginin bilgiye erişim hakkı olan kişilere açık tutulmasıdır. Sadece bilgiye erişim hakkı olan kişilerin bilgiye erişmesini sağlayacak bir sistem, çok katı kontrollilerin konulmasını gerektirir. Kişiler güvenilir ve gizli bilgilerine, sadece yaptıkları işte kullanılması gerektiği zaman erişmelidirler. Bilgi ve kaynaklara erişim hakkının sadece ihtiyaç duyanlara verilmesi kavramına erişim kontrolü denir.

Erişim kontrolünü sağlamada kullanılan, en yaygın olarak bilinen yöntem şifre kullanımıdır. Şifrenin çaldırılması ise en yaygın olarak bilinen güvenlik gediğidir. Şifre güvenliğini sağlamak için akıllı kart ve tek kullanımlı şifre aletleri kullanmak gereklidir. Bu kaynakları yetkisiz erişime karşı engelleme konusunda alınacak önlemlerin ilk aşamasıdır.

Bir anlık işinizi tipik bir varoş evi olarak, evin anahtarını da şifreniz olarak düşününüz. Anahtar olmadan kimse eve giremez; fakat anahtar çok kolay bir şekilde kaybolabilir veya çalınabilir. Kuvvetli bir şifre politikası oluşturmakta çok zor bir şey olmamakla birlikte kesinlikle oluşturulmalı ve çalışanlarda bu konuda eğitilmelidir.

Erişim kontrolünün diğ er bir tarafı, kurumun bilgisayar ağlarında kimliği doğrulanan kurum çalışanının kaynak erişim yetkilerine sınırlamaların getirilmesidir. Örneğin, tüm insan kaynakları çalışanları, kişi ve kurum elemanları ile ilgili adres ve doğum günü gibi tüm bilgilere erişim yetkisine sahip olabilir; fakat tazminat bilgilerine sadece bir kısım yetkili kişiler erişebilir. Aynı zamanda, bazı kullanıcılara bu bilgiler üzerinde sadece görüntüleme yetkisi verirken, diğ er kullanıcılara hem görüntüleme, hem de güncelleme yetkisi verilecek durumlarla da karşılaşılabilir. Bu tipik bir erişim denetleme senaryosudur. Yine varoş evi örneğine gelinirse, hizmetçiniz ön kapının anahtarına sahip ve evinizi temizlemek için eve girebilmektedir. Hizmetçinizin görmesini istemediğiniz belgeleri çalışma odasına koyup farklı bir anahtarla odayı kilitleyiniz. Hizmetçideki anahtar çalışma odanızın kapısını açamadığından, hizmetçinin ev içerisindeki yetkileri kısıtlanmış olur.

1.1.2 Bütünlük

Bütünlük ölçütü, bilginin beklenmeyen yollarla güncellenememesini garanti eder. Bütünlük kaybına, insan hataları, kasıtlı kurcalamalar veya çok kötü olaylar neden olur. Şüphesiz ki, herhangi bir işte yanlış bilgilerin kullanılması istenmeyen sonuçlar

doğurabilir. Uygunsuz bir şekilde güncellenmiş verinin işe yaramaz veya tehlikeli olması gerçeği, verinin doğruluk ve tutarlılığın korunması için, çok büyük çabanın sarfedilmesini gerektirmektedir.

Verinin geçerliliği çok önemli ise bunu garanti edecek kontrollerin tasarlanması ve verinin doğruluğun kontrol edilmesi gereklidir. Eğer veri bir şekilde çalınmışsa veya yetkisiz kişiler tarafından değiştirilmişse, bunun tespit edilmesi sistemin bütünlüğü açısından elzemdir. Şifreleme, verinin yetkisiz kişiler tarafından erişilmesi ve değiştirilmesini, veriyi gizli bir biçime çevirerek, engellemede kullanılan bir yöntemdir.

Olgunlaşmış bir bilgi güvenliği politikası, etkin önlem alma (proactive) ve tepki oluşturma (reactive) işlevlerini içermelidir. Etkin önlem alma, kuvvetli güvenlik denetimlerinin konulmasını gerektirirken, tepki oluşturma bu kontrollerin kayıtlanması ve izlenmesini gerektirmektedir. İyi bir sistem yöneticisi, sistem içerisindeki hareketleri kayıt dosyalarından izleyerek, gerçekleşen olaylardan sonuçlar çıkarıp, yeni önlemler oluşturmaktadır. Etkin kayıt almanın önemi şu şekilde açıklanabilir: Bir odaya giriş çıkışların bir deftere not edildiğini düşününüz. Odaya giren her bir kişi için, isim ve odaya giriş ve çıkış saatleri gibi bilgilerin tutulduğunu varsayalım. Oda ile ilgili herhangi bir sorun çıktığında bu kayıtlara dönerek sorunun olduğu gün ve saatlerde odaya kimlerin çıktığına kolayca erişebilecektir. [1]

1.1.3 Hazır bulunabilirlik

Hazır bulunabilirlik, kaynakların silinmesi veya erişilemez hale gelmesine engelleyen ölçüttür. Bu ölçüt, sadece bilgi değil, diğer tüm teknoloji altyapısı ve ağa bağlı makineler için geçerlidir. Bu gerekli kaynakları kullanamama durumu, hizmet dışı bırakma (denial of service) olarak adlandırılır. Kasıtlı saldırıların çoğu, veri çalmaktan çok bu tip olup, politik veya ekonomik sebepli olarak başlatılır. Elektronik posta adreslerinin protesto amaçlı olarak yasa dışı gereksiz postalarla doldurulması veya bir internet bankacılık sitesinin hizmet dışı bırakılması gibi biçimlerde karşılaşılır.

Bilgisayar ağının veya sistemin fiziksel güvenliğinin sağlanması, hazır bulunabilirliği sağlama yöntemlerinden biridir. Önemli makine ve veri kaynaklarına fiziksel erişim kısıtlanarak, sistemin hazır bulunabilirlik sorunu azaltılabilir. Aynı şekilde elektronik bilgi ağının dışarıdan gelecek tehlikelere karşı, firewall olarak adlandırılan ürünlerle korunmalıdır. Güvenli geçit, iki bilgisayar ağı arasında hangi tip verinin akacağını düzenler ve kısıtlar. [1]

Evinize giden yol üzerinde bir güvenlik görevlisi tarafından korunan bir kapı olduğunu düşününüz. Güvenlik görevlisi bir güvenli geçit gibi davranarak, bahçeye girişleri kısıtlayacaktır. Saldırgan (intruder) ön kapının anahtarını bir şekilde ele geçirmiş olsa dahi, güvenlik görevlisi kendisini kapıya yaklaştırmayacağı için içeri giremeyecektir.

Diğer yönden, hazır bulunabilirlik, kaynakların ihtiyaç duyulduğu zaman ve yerde kullanılabilirliğini garanti etmelidir. Bu nedenle sistemin kırılması durumunda anında geri dönmeye sağlayacak yedek sunucuların bulunması ve veri yedeklemesinin düzenli olarak yapılması gereklidir. Aynı zamanda yedek sunucuların ve veri yedeklerinin de saldırılarından arındırılmış bir ortamda, tüm güvenlik önlemleri alınmış şekilde tutulması gereklidir.

Bir kurumun güvenlik stratejisi yukarıda bahsedilen üç ölçüt doğrultusunda değerlendirilmeli ve kurumun ihtiyaçlarına göre ölçütler değişik seviyelerde incelenmelidir. Örneğin, milli savunma sistemlerinde güvenilirliğe daha çok önem verilmesi gerekirken, fon aktarım sistemlerinde bütünlüğe daha çok önem verilmelidir.

1.2 Güvenlik Seviyeleri

Bir uygulamanın içerebileceği özelliklere göre sınıflandırılmış, dünyaca bilinen ve sistem güvenliğinin ölçümünde standart olarak kabul edilen güvenlik seviyeleri vardır. Örneğin, Hemen hemen herkesin kulağına yabancı olmayan, “C2 güvenlik seviyesi” terimi gibi. internet’ te uygulamaların güvenlik seviyeleri, NCSA (National Computer Security Center) tarafından, TPEP (Trusted Product Evaluation Program) programı yürütülerek belirlenir. Bir uygulamanın güvenlik seviyesinin belirlenmesi sürecinde, uygulamalar, daha önceden belirlenmiş olan bir dizine göre sınıflandırılırlar TPEP’ in sıkça sorulan sorular bölümünde sınıf şöyle tanımlanmaktadır:

“Güvenilen Bilgisayar Güvenliği Değerlendirme Ölçütleri (Trusted Computer Security Evaluation Criteria – TCSEC)’ nin gerektirdiği özelliklerin toplanmış halidir.”

Bir sistemin güvenlik seviyesinde, burada ayrıntısına girilmeyecek olan, Güvenli Teknoloji Değerlendirme Programı (Trust Technology Assessment Program-TTAP) , Güvenilen Ürün Değerlendirme Programı (Trusted Product Evaluation Program - TPEP) ve Oransal Bakım Evresi (Rating Maintenance Phase - RAMP) gibi programlar, Ortak Ölçüt (Common Criteria - CC) ve TCSEC gibi ölçütler vardır. [2]

1.2.1 Güvenilen bilgisayar güvenliği değerlendirme ölçütleri (Trusted computer security evaluation criteria – TCSEC)

TCSEC bilgisayar sistemlerinin güvenlik seviyesinin belirlenmesinde kullanılan ölçüttür. Bu ölçüt basılı olduğu kitap renginden dolayı, Turuncu Kitap (Orange Book) olarak adlandırılır. Bu ölçüt sistem güvenliğini, aşağıdaki güvenlik seviyeleri ile sınıflandırır.

- D seviyesi (En düşük koruma düzeyi): Daha üst düzeydeki ölçütleri sağlayamayan sistemler, bu sınıfa girerler ve güvensiz ürünler olarak adlandırılırlar.
- C1 seviyesi (Ayrık (Discretionary) güvenlik seviyesi): Sistem kullanıcılarını, veriden ayıran güvenlik seviyesidir. Kişisel seviyede erişim sınırlamasına olanak tanınması, kullanıcıların özel bilgilerini istenmeyen erişimlere karşı korunması gereken durumlar için uygun bir sistemdir.
- C2 seviyesi (Kontrollü erişim seviyesi): C1' e göre daha fazla ve daha alt düzeyde erişim kontrolü sağlayan bu seviye, bağlantı yordamları, güvenlik olaylarının izlenmesi ve kaynak ayırımlarıyla, kullanıcıların tek tek kontrol edilebilmesini gerektirmektedir.
- B1 seviyesi (Etiketlenmiş güvenlik seviyesi): B1 seviyesi, C2 seviyesinin tüm özelliklerini ek olarak, resmi olmayan güvenlik politikası modeli, veri etiketleme ve isimlendirilmiş nesneler üzerinde zorunlu erişim kontrolü gerektirmektedir.
- B2 seviyesi (Yapısal güvenlik seviyesi): Güvenlik politikasının resmleştirilmesinin gerektiği B2 seviyesinde, B1 seviyesindeki tüm özellikler yer almalı ve zorunlu erişim kontrolü, veri işleme sistemindeki tüm olay ve nesnelere kadar genişletilmelidir.
- B3 seviyesi (Güvenlik alanları): B3 sınıfı, Güvenilen Hesaplama Tabanı(Trusted Computing Base - TCB)' nin gerektirdiği başvuru izleme gereksinimlerini sağlamalıdır gerekmektedir. Bir güvenlik yöneticisi desteklenmeli, bilanço mekanizması tüm güvenlikle ilgili olayların kontrol edilmesi için genişletilmeli ve sistem onarım prosedürleri oluşturulmalıdır.
- A1 sınıfı (Onaylanmış tasarım seviyesi): İşlevsellik açısından B3 seviyesiyle aynı olan A1 sınıfının farklılıkları TCB'nin tasarım ve gerçekleştirme tekniklerinde yatmaktadır.

2 İLETİŞİM AĞLARI BİLEŞENLERİ VE PROTOKOLLERİ

Teknolojinin gelişimine paralel olarak, sayısal dünyada iletişimin gelişmesi, iletişim ihtiyaçlarının artmasına neden oldu. Bu duruma firmaların, geliştirmiş oldukları yeni teknolojiler ve ürünlerle karşılık vermesi, birçok protokolü ortaya çıkarmıştır. Öyle ki, küçük bir ofis ortamında bile, birden fazla protokol kullanılır hale gelmiştir. Özellikle internet kullanımının yaygınlaşması, internet üzerinde iletişim için çeşitli protokollerin geliştirilmesi sonucunu doğurmuştur.

2.1 İletişim Ağları

Birden fazla bilgisayarın birbirlerine doğrudan ve/veya telefon hatları ile bağlanmasıyla oluşan sisteme ağ denir. Ağ üzerindeki bilgisayarlar birbirleriyle çeşitli yöntemlerle haberleşirler. Kabaca iki farklı ağ çeşidi vardır:

1. Yerel Ağ (Local Area Network - LAN) : Fiziksel olarak aynı binada bulunan bilgisayarları birbirlerine bağlayarak oluşturulan ağlardır.
2. Geniş Alanlı Ağ (Wide Area Network – WAN) : Şehiriçi, şehirlerarası, ülkelerarası bilgisayar bağlantılarıyla oluşturulan ağlardır. Örneğin, bir bankanın merkezi ile şubesi arasındaki bağlantıyı sağlayan ağ geniş alanlı bir ağdır. Ayrıca Eran, internet ve Bitnet, geniş alanlı ağa örnek olarak gösterilebilir.

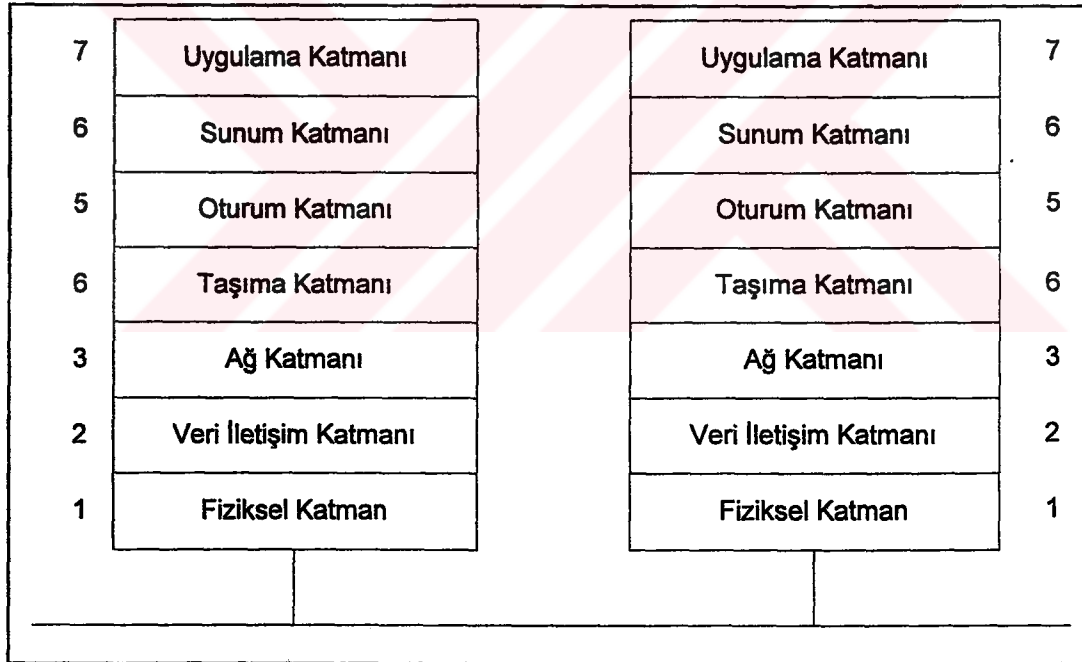
2.1.1 İletişim ağları yapısal modeli

Bu bölümde bilgisayar ağlarının birbirleri ile olan iletişimi (internetworking) konusunda bazı temel kavramlar hakkında bilgi verilecektir.

Açık sistem bağlantıları (Open systems interconnection-OSI) başvuru modeli

Bilgisayarlar arası iletişimin başladığı günden itibaren farklı bilgisayar sistemlerinin birbirleri arasındaki iletişimi daima en büyük problemlerden birisi olmuş ve bu sorunun üstesinden gelebilmek için uzun yıllar boyunca çeşitli çalışmalar yapılmıştır. 1980' li yılların başında Uluslararası Standartlar Organizasyonu (International Standards Organization-ISO) bilgisayar sistemlerinin birbirleri ile olan iletişimde ortak bir yapıya ulaşmak amaçlı çabaları sonuca bağlamak için, bir çalışma

başlatmıştır. Bu çalışmalar sonucunda 1984 yılında Açık Sistem Bağlantıları (Open Systems Interconnection-OSI) başvuru modeli ortaya çıkarılmıştır. Bu model sayesinde değişik bilgisayar firmalarının ürettikleri bilgisayarlar arasındaki iletişimi bir standarda oturtmak ve farklı standartlar arası uyumsuzluk sebebi ile ortaya çıkan iletişim sorununu ortadan kaldırmak hedeflenmiştir. OSI başvuru modelinde, iki bilgisayar sistemi arasında yapılacak olan iletişim sorununu çözmek için, yedi katmanlı bir ağ sistemi önerilmiştir. Bir başka deyişle, bu temel sorun yedi adet küçük soruna parçalanmış ve her bir sorun için, ayrı ayrı çözüm yaratılmaya çalışılmıştır. Bu yedi katmanın en altında yer alan iki katman, yazılım ve donanım, üstteki beş katman ise genelde yazılım yolu ile çözülmüştür. OSI başvuru modeli, bir bilgisayarda çalışan uygulama programının, iletişim ortamı üzerinden başka bir bilgisayarda çalışan diğer bir uygulama programı ile olan iletişiminin tüm adımlarını tanımlar. En üst katmanda görüntü, ya da yazı şeklinde yola çıkan bilgi, alt katmanlara indikçe makine diline dönüşür ve sonuç olarak, 1 ve 0' lardan ibaret elektrik işaretleri halini alır. [3] Şekil 2.1' de OSI başvuru modeli katmanları ve bir yerel ağ üzerindeki durumu gösterilmektedir.



Şekil 2.1 OSI başvuru modeli

OSI katmanlarının tanımlanan temel görevleri:

1. **Fiziksel:** Bu katman ağın elektriksel ve mekanik davranışlarını belirler. Ayarlama teknikleri, çalışma voltajı, frekansı vb. bu katmanın temel özelliklerindendir. OSI başvuru modeli bir ağ uygulaması değildir. OSI sadece her katmanın görevini tüm ayrıntıları ile tanımlar. Bu model bir gemi ya da ev projesine benzetilebilir. Nasıl aynı gemi planını alıp farklı firmalar

gemi yapabilirse OSI modeli de böyledir. Nasıl aynı gemi planından iki farklı firma gemi ürettiğinde, en azından kullanılan çiviler farklı yerlere çakılırsa, OSI modeli de gerçekleştiren firmadan firmaya farklılık gösterebilir.

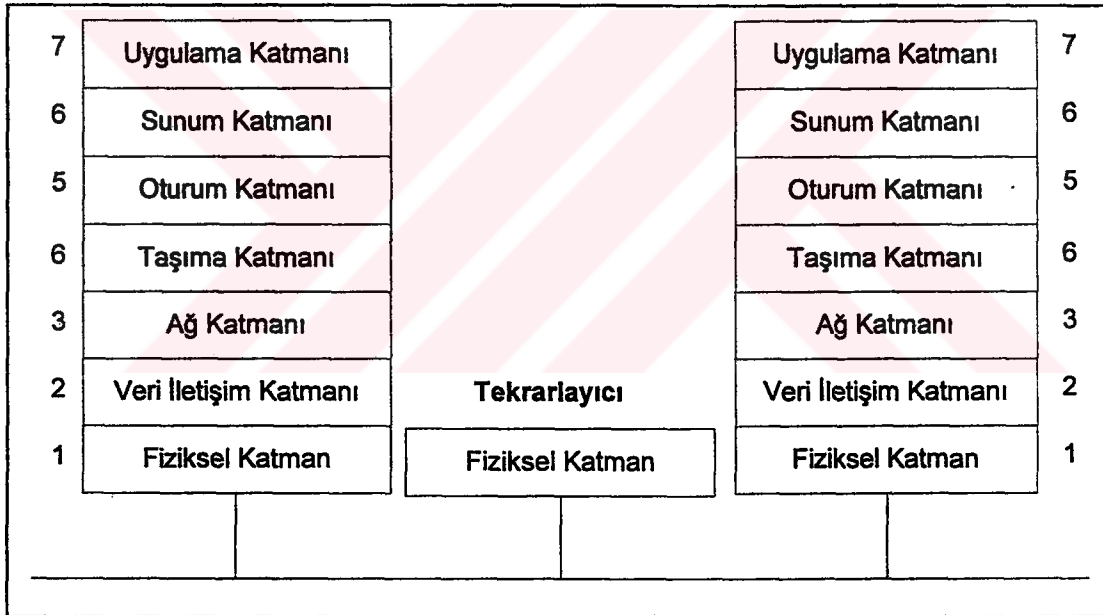
2. **Veri iletim:** Bu katman fiziksel katmana ulaşım stratejisini belirler. Fiziksel adresleme, ağ topolojisi, akış kontrolü vb. bu katmanın görevlerindendir. Köprü cihazları bu katmanda çalışır.
3. **Ağ:** Bağlantıyı sağlayan ve ulaşmak istenen bilgisayara giden yolu bulan katmandır. Yönlendirme protokolleri bu katmanda çalışır.
4. **Taşıma:** Bu katman gelen bilginin doğruluğunu kontrol eder. Bilginin taşınması esnasında oluşan hataları yakalar ve bunları düzeltmek için çalışır.
5. **Oturum:** İki bilgisayar üzerindeki uygulamaların birbirini farketmediği katmandır.
6. **Sunum:** Bu katmanda gelen paketler bilgi haline dönüştürülür. Bilginin karakter kümesi çevrimi veya değiştirilmesi, şifreleme vb. görevlerini bu katman üstlenir.
7. **Uygulama:** Kullanıcıya en yakın olan katmandır. Tablolama, kelime işlemci, banka aptal ekran programları vb. bu katmanın parçalarıdır.

Bağlantı aygıtları

Bilgisayar ağı erişiminde genel olarak dört tip bağlantı aygıtı kullanılır: Bunlar, tekrarlayıcı (repeater), köprü (bridge), yönlendirici (router) ve geçityolu (gateway).

- **Tekrarlayıcı (Repeater):** Tekrarlayıcılar, Şekil 2.2' den de görüleceği gibi fiziksel katmanda çalışan cihazlardır. Tekrarlayıcının temel görevi, bir fiziksel ortamdaki (kablo, fiber-optik, radyo dalgası vb.) sinyali alıp kuvvetlendirip bir diğer fiziksel ortama vermektir. Ağların fiziksel büyüklük sınırlarını daha da genişletmek amacı ile kullanılan bu cihazlar ile kuramsal olarak bir bilgisayar ağı sonsuza kadar genişletilebilir. Ancak çeşitli bilgisayar ağlarındaki tasarım sınırlamaları nedeni ile gerçekte bu genişleme belli sınırlar içinde kalmaktadır. Temelde bir ağın genişletilmesi amacı ile kullanılan tekrarlayıcılar, çok kolay kurulmaları, çok az bakım gerektirmeleri ve fiyatlarının ucuz olması sebepleri ile çok rağbet gören cihazlardır.
- **Köprü (Bridge):** Çağdaş, protokol-şeffaf köprüler, Şekil 2.3' te görüldüğü gibi OSI başvuru modelinin veri iletim (data link) katmanında çalışırlar. Köprü cihazları temelde bağımsız iki ağın (farklı ağ teknolojilerini kullanabilirler - Ethernet ve Token-Ring gibi) birbirine bağlantısı için kullanılırlar. Şekil 2.4' te

iki Ethernet ve bir Token-Ring ağının birbirlerine köprüler vasıtası ile yapılan bağlantısı gösterilmektedir. Bir köprü, bağladığı alt ağlar üstündeki tüm trafiği yürütür. Her paketi okur, paketin nereden geldiğini ve nereye gittiğini görmek için MAC (Media Access Control) katman kaynağını ve varış (destination) adresini inceler. Bu süzme yeteneği mesajları yayınlamak, ya da yerel veri trafiğinin diğer ağ üzerine geçmesini engellemek için etkili bir yol sağlar. Bazı köprüler adres süzmenin ve protokol tipine bağlı süzgeçin de ötesine gider. Bir köprü, DECnet, TCP/IP, XNS gibi farklı iletişim protokollerini kullanarak, protokol uyumluluğunu göz önüne almadan ağlar arasında fiziksel bağlantı sağlayabilse de, bu uygulamalar arasında işletilebilirliği garanti etmemektedir. Bu, OSI başvuru modelinin yüksek katmanlarında işleyen ve farklı işlem ortamları arasında çevrim yapabilen protokol çeviricilerin işidir. Köprülül ağlar, protokol çevrimlerinin olmadığı, güvenlik gereksinimlerinin en az olduğu ve gereken tek şeyin basit yönlendirme olduğu durumlarda başarılıdır.

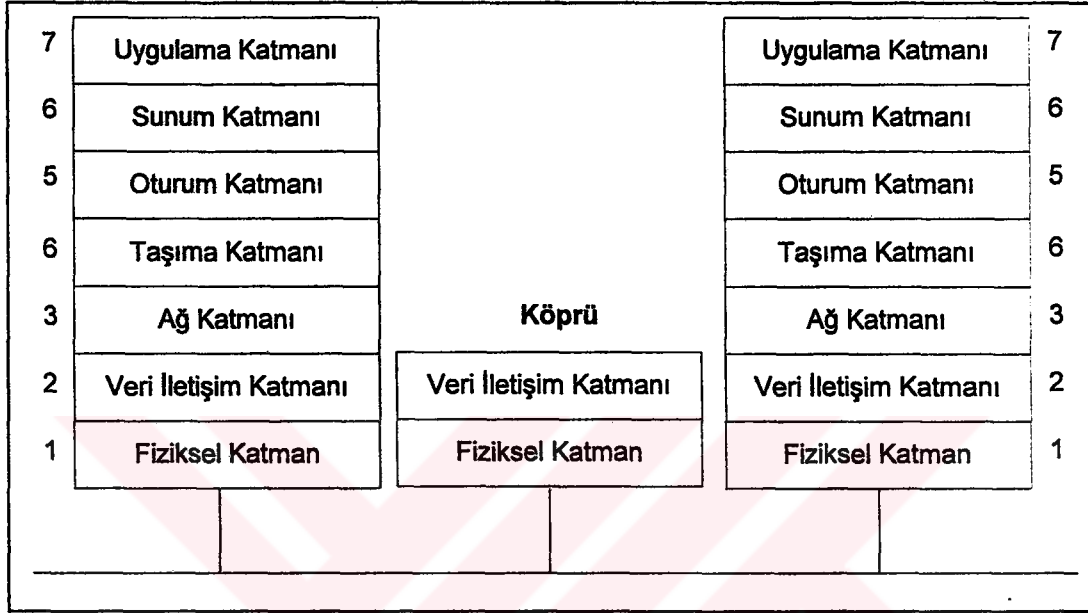


Şekil 2.2 Tekerlayıcı ve OSI başvuru :modeli

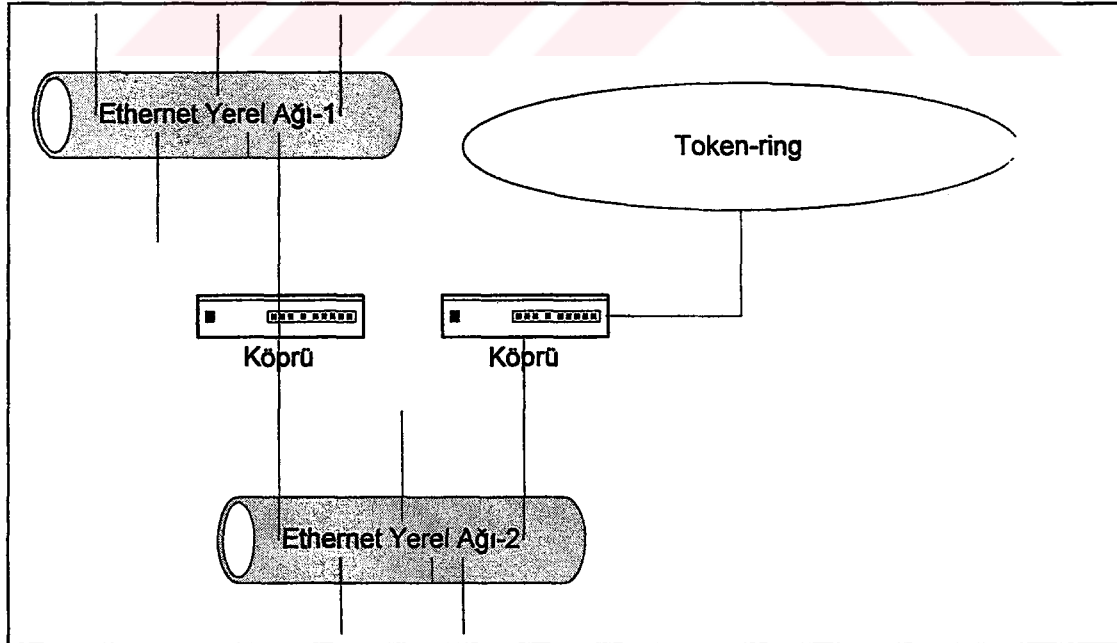
- Yönlendirici (Router): Yönlendiriciler Şekil 2.5' te görüldüğü gibi OSI başvuru modelinin ağ katmanında çalışırlar. Bir köprü sadece paketlerin kaynağını ve gittiği yerin adresini kontrol ederken, bir yönlendirici ağın tüm haritasını tutar ve paketin varış adresine en iyi yolu belirleyebilmek için, tüm yolların durumunu inceler.

Yönlendirici farklı fiziksel yapıda olan ve farklı protokolleri çalıştıran yerel, ya da geniş alan ağlarının birbirleri ile olan bağlantısında başarı ile kullanılabilir.

Bir yönlendirici, OSI başvuru modelinin ağ katmanında genel olarak tanımlanan protokollerle, yerel bölge ağlarını, geniş bölge ağlarına bağlar. Bu özellikleri sayesinde, örneğin, yönlendirici TCP/IP kullanılarak bir Ethernet ağının X.25 paket ağına bağlanmasını sağlar. Eski yönlendiriciler protokol bağımlı olduklarından, kuruluşların ağ işletim ihtiyaçlarını karşılamak için birden fazla yönlendirici gerekmekteydi. Yeni yönlendiriciler birden fazla ve değişik protokolü aynı anda idare edebilmektedirler.

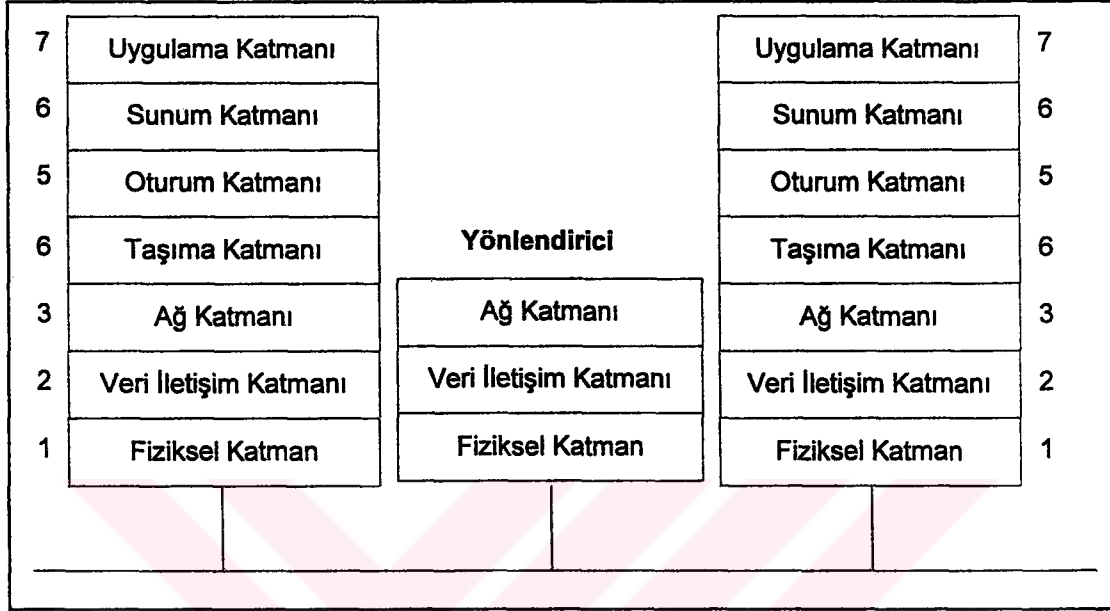


Şekil 2.3 Köprü ve OSI başvuru modeli

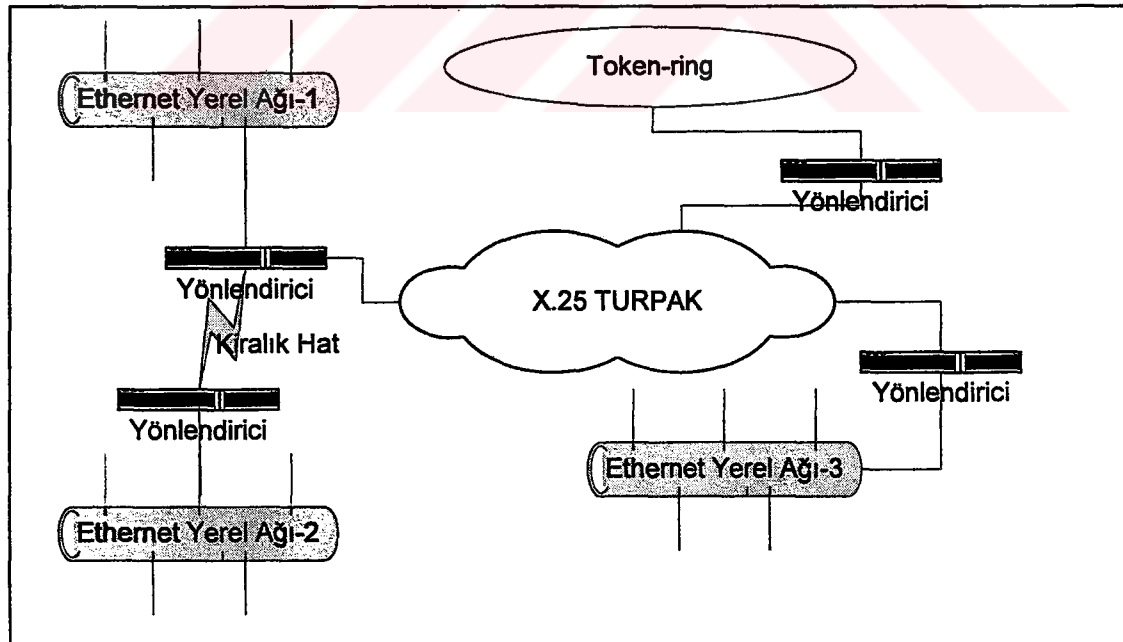


Şekil 2.4 Bir köprü uygulaması

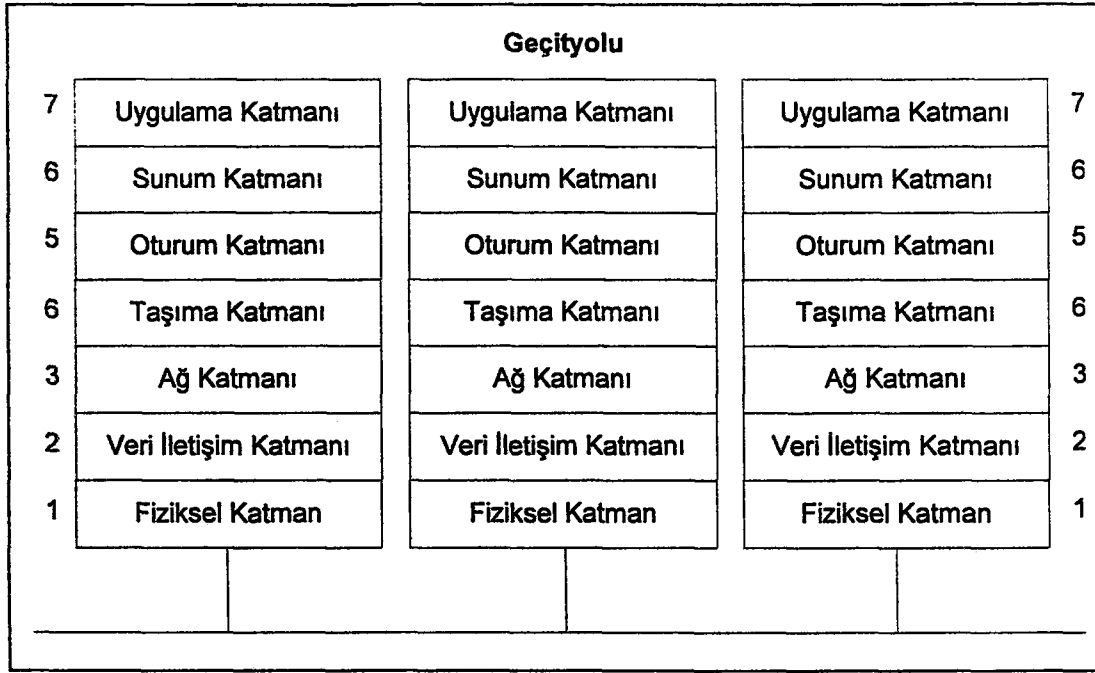
Yönlendiriciler paketleri iki istasyon arasındaki en iyi yolu gösteren yönlendirme çizelgesine göre ilerleterek, ağ üzerindeki yolları en iyi şekilde kullanırlar. Yönlendiriciler kendi yönlendirme tablolarını oluşturdıklarından, ağ trafiğindeki değişikliklere hemen ayak uydururlar ve böylelikle veri yükünü dengelerler. Aynı zamanda, yönlendiriciler ağdaki değişiklikleri tespit ederler; aşırı yüklü ve işlemeyen bağlantıları önerler.



Şekil 2.5 Yönlendirici ve OSI başvuru modeli



Şekil 2.6 Bir yönlendirici uygulaması



Şekil 2.7 Geçityolu ve OSI başvuru modeli

- **Geçityolu (Gateway):** Geçityolları köprü ve yönlendiricilerden daha geniş yeteneklere sahiptirler. Şekil 2.7' den de görülebileceği gibi, geçityolları, OSI başvuru modelinin üst katmanlarında işlerler. Geçityolları sadece farklı noktalardaki ağları bağlamakla kalmaz, aynı zamanda bir ağdan taşınan verinin diğer ağlar tarafından anlaşılmasını da sağlarlar. Bu bir sunucuda, kişisel bilgisayarda veya anaçatı bilgisayarda bulunan protokol çevirim yazılımı ile yapılır. İnternet protokolleri farklı ağlar arasındaki veri iletimini, geçityollarıyla bağlı alt ağlardan oluşmuş bağımsız sistem (Autonomous System - AS) gruplarını birbirine bağlayarak gerçekleştirirler. Yani internet, her biri merkezi olarak yönetilen ağ ya da alt ağlar serisi olan AS serisinden oluşmaktadır. Her AS, diğer AS' lere bağlantı sağlayan bir geçityolu sunar. Geçityolları tüm farklı ağları birlikte tutan bir yapıştırıcıdır. İnternet protokolleri, alt ağların nasıl birbirine bağlı olduğunu ve bağlantı araçlarının nasıl çalıştığını tanımlarlar. [3]

2.2 Protokoller

Ağ üzerindeki bilgisayarların tam ve doğru bir şekilde birlikte haberleşebilmeleri için uymak zorunda oldukları kurallar ve standart anlaşmalar bütününe protokol denir. İnternet üzerinde TCP/IP, Bitnet üzerinde NJE protokollere örnek olarak verilebilir.

Protokoller tipik olarak birbirleriyle uyumlu protokol yığınları içinde düzenlenir ve ilişkilendirilirler. Bir yığın yedi seviyeli, Açık Sistem Mimarisi (Open System Interconnection – OSI) katmanının çeşitli seviyelerinden protokoller içerir.

İletişim protokolleri, özellikleri açısından iki temel tipe ayrılabilirler:

1. **Bağlantı temelli protokoller:** İletişimden önce kaynak ile varış arasında sanal bir devre ile bağlantı kurulur. Bu bağlantı gönderilen paketin varışa erişimini garanti ettiğinden, bağlantı temelli protokoller güvenilirdir. Genellikle düşük seviyeli hızlarda ve bant genişliklerinde tercih edilir. Dosya transfer protokolü (File Transfer Protocol – FTP) örnek olarak gösterilebilir.
2. **Bağlantısız Protokoller:** Veri, varışa bağlantı kurulmadan gönderilir. Bu tip protokollerde verinin varışa ulaştığının garantisi verilemez. Elektronik posta protokolü (Simple Mail Transfer Protocol - SMTP) örnek olarak gösterilebilir.

2.2.1 TCP/IP protokol kümesi

İnternet üzerinde ağların birbirleriyle iletişimini sağlayan kurallar bütünü TCP/IP protokol kümesi olarak adlandırılır. İnternet üzerinde birbirleriyle iletişim kurmak isteyen bilgisayarların TCP/IP protokol kümesini desteklemesi veya bu protokole destek veren geçityolunu kullanması gereklidir.

TCP/IP protokol kümesini oluşturan protokoller katmanlı yapıdadırlar ve herbirinin görevi ve sunduğu hizmetler birbirinden bağımsızdır. Düşük düzeyli protokoller temel işlevleri yerine getirirken, yüksek düzeyli protokoller daha gelişmiş işlevler sunarlar. TCP/IP protokol kümesi,

- İnternet Protokolü (IP),
- İletişim Denetleme Protokolü (Transmission Control Protocol – TCP),
- Kullanıcı Veri Birimi İletişim Protokolü (User Datagram Protocol - UDP)

gibi temel protokollerden oluşur. [4]

İnternet protokolü (IP)

Bağlantısız bir protokol olan IP, iletişim paketlerinin adreslenmesi ve konaklar arasında yönlendirilmesinden sorumludur. Bağlantısız bir protokol olması, IP' nin paket dağıtımının doğruluğunu garanti edememesi sonucunu doğurmaktadır. IP her paket dağıtımını denemesinde yapabileceğinin en iyisini yapmasına karşın, dağıtım sırasında paketlerin kaybolması, sıralarının karışması, gecikmesi ve aynı paketin iki kez gönderilmesi gibi durumlarla karşılaşmak olağandır. IP protokolünde verinin alındığına dair bir onay mesajı göndericiye gönderilmediğinden, gönderici veya alıcı

verinin karşı tarafa doğru olarak erişip erişmediği konusunda bilgi sahibi olamaz. Paketlerin varışa doğru eriştiğine dair onay mesajının gönderilmesi daha üst seviyedeki TCP gibi bir protokolün görevidir.

İletişim denetleme protokolü (TCP)

Kullanıcıdan gelen iletileri parçalara böler ve her bir parçayı veri birimi (datagram) adı verilen paketler halinde varışa gönderir. TCP' de paketler varışa gönderilmeden önce, kaynak ile varış arasında sanal devre ile oturum açılır ve paketler bu bağlantı üzerinden gönderilir. İletişim Denetleme Protokolü, ağ katmanı (Network Layer) veri birimlerinin doğru şekilde gönderildiğini garantilemediğinden, veri birimlerine ait oldukları bağlantı ile ilgili başlıklar ekleyerek numaralandırır. Varışta bulunan taşıma ögesi (transport entity) ayrılmış veri birimlerini birleştirir ve kendisine doğru olarak erişen veriler için kaynağa onay mesajı gönderir. Onay alınmayan mesajlar kaynak tarafından yeniden gönderilir. Bu şekilde paketin doğru olarak dağıtımını garanti edilir.

TCP protokolünde veri aktarımı başlamadan açılan oturumu gerçekleştirmede üç yollu el sıkışma protokolü kullanılır. Üç yollu el sıkışma protokolü paketlerin gönderilişinin ve alınışının aynı zamanlı olarak çalışmasını sağlamak, diğer konağa tek seferde alabileceği veri boyutu ile ilgili olarak bilgilendirmek ve kaynak ile varış arasında sanal bir devre kurmak amaçlı olarak kullanılır. [4]

Şekil 2.8' de gösterimi yapılan üç yollu el sıkışma protokolü şu aşamaları içerir:

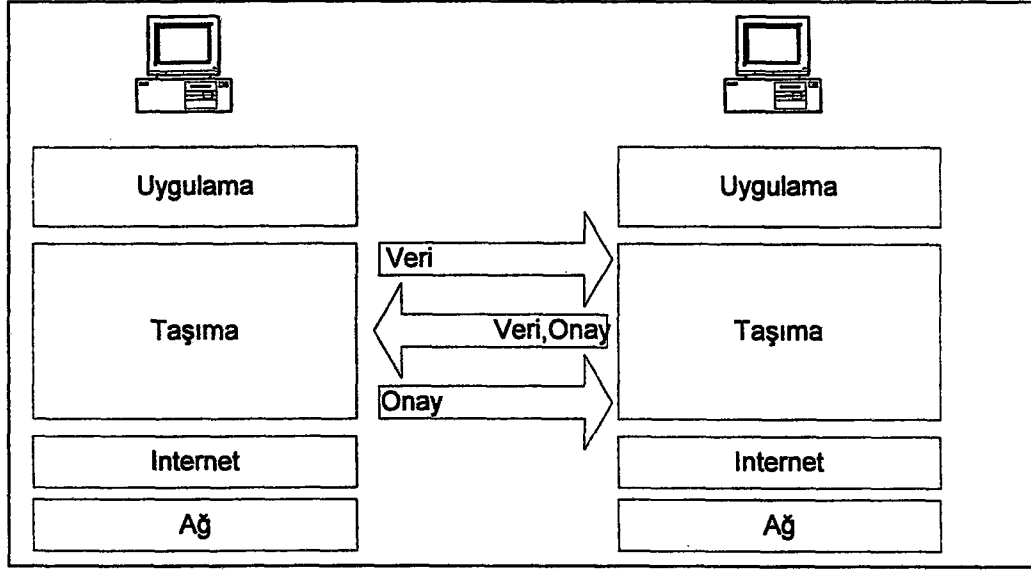
1. Bağlantı başlatmak isteyen konak zamanlama (synchronization – SYN) bayrağını aktif yapar ve varış konağına gönderir.
2. Varış konağı kaynak konağın bağlantı isteğinin veri kısmını, zamanlama bayrağı aktif, göndereceği veri parçasının başlangıç adresini işaretleyen sıralama numarası ve beklediği diğer veri kısmının sıralama numarası ve onay mesajı ile birlikte geri göndererek onaylar.
3. İstekte bulunan kaynak konağı, veri kısmını onaylanmış sıralama numarası ve onay mesajı numarası ile birlikte varış konağına gönderir.

Kullanıcı veri birimi iletişim protokolü(UDP)

TCP/IP protokol kümesinin bağlantısız taşıma protokolü olan UDP, kullanıcı iletilerini veri birimlerine ayırarak, sıralama ve yerine ulaşma garantisi olmadan varışa gönderir.

UDP protokolü onay mesajı gerektirmeyen ve küçük boyutlu verilerin iletiminde kullanılır. Ağ Temel Giriş Çıkış Sistemi (NetBIOS) isimlendirme hizmeti, Basit Ağ

Yönetim Protokolü (Simple Network Management Protocol – SNMP), UDP protokolüne örnek olarak gösterilebilir.



Şekil 2.8 Üç yönlü el sıkışma protokolü

Kapı(Port)

Yuva(socket) uygulamaları bilgisayar üzerinde kendilerini protokol kapı numaraları kullanımı ile tanırlar. Örneğin, bir FTP sunucu uygulaması diğer uygulamalarla iletişim kurabilmek için bilinen bir TCP kapı numarası kullanır.

Kapılar 0 ile 65.536 arasında herhangi bir numarayı kullanabilirler. İstemci uygulamaları için kapı numaraları, hizmet için istekte bulunulduğunda işletim sistemi tarafından otomatik olarak atanır. Bilinen sunucu uygulamaları için kapı numaraları, İnternet Atanmış Numaralar Makamı (İnternet Assigned Number Authority - IANA) tarafından önceden atanır ve bir daha değişmez.

Yuva(Socket)

Kavramsal olarak dosya tutamaçı (handle) ile benzerlik gösteren yuvalar, ağ iletişimde son nokta olarak görev görürler. Bir uygulama iletişim kurmak istediği konağın IP adresi, hizmet tipi (TCP veya UDP) ve uygulamanın kullandığı kapı numarasını tanımlayarak yuva oluşturur. Bir uygulama yuva yaratıp, uzak uygulamaya bağlantısız veri trafiği gönderebildiği gibi, diğer uygulamanın yuvasını bağlanıp, bağlantı kurar ve veriyi bu bağlantı üzerinden güvenli bir şekilde gönderir.

2.2.2 Seri hat internet iletişim protokolü (Serial line internet protocol – SLIP)

Seri Hat İnternet İletişim Protokolü (SLIP) normal olarak UNIX sunucuları tarafından kullanılan eski bir uzaktan erişim standardıdır. Windows 2000 Ağ ve Çevirmeli

Bağlantılar tarafından desteklenen SLIP standardı kullanılarak, uzaktaki erişim sunucusuna bağlantı yapılabilir.

2.2.3 IPX/SPX Protokolleri

IPX ve SPX Novell Netware ağlarında kullanılan taşıma iletişim protokolleridir. Bu iki iletişim protokolü TCP/IP protokol kümesindeki iletişim denetleme ve internet protokollerine karşılık gelir.

2.2.4 NWLINK

NWLINK, Novell' in IPX/SPX iletişim protokolünün Ağ Sürücü Arabirimi Belirtimi (Network Device Interface Specification – NDIS) uyumlu uygulamasıdır. NWLINK NetBIOS ve Windows yuvaları olarak isimlendirilen iki ağ uygulama programlarına arabirimlerini (Application Programming Interface – API) destekler. NWLINK protokolü windows işletim sistemi çalıştıran bilgisayarlar arasında veya windows işletim sistemi çalıştıran bir bilgisayar ile Netware sunucuları arasında iletişim kurmada kullanılır.

2.2.5 NetBEUI protokolü

NetBIOS Gelişmiş Kullanıcı Arabirimi (NetBEUI), 50' den az bilgisayarlı tek bir ağ kesiminden oluşan ağlarda kullanılmaya uygun, yönlendirilemeyen bir ağ taşıma iletişim protokolüdür. NetBEUI, Windows' un önceki sürümlerinde ağ ad çözümü için gereken NetBIOS kullanımını desteklemek için kullanılan iki ağ çözümünden biridir. Daha büyük ve yönlendirmeli ağlar için kullanılan NetBIOS tabanlı diğer çözüm, TCP/IP üzerinden NetBIOS (NetBT)' tur. NetBEUI küçük çalışma gruplarında veya yerel ağlarda kullanım için uygundur. NetBIOS ağ geçidi ve NetBEUI istemci iletişim protokolü, Windows NT/2000 Sunucusu çalıştıran tüm uzaktaki erişim sunucularına ve windows ağ istemcilerine kurulabilir.

2.2.6 Apple talk protokolü

Macintosh makinelerin dosya ve yazıcı paylaşımını sağlayan protokoldür. Ethernet ve Local Talk ağlarda çalışır ve yönlendirmeyi destekler.

2.2.7 Veri bağlantı denetleme (Data link control – DLC) protokolü

DLC IBM tarafından Ağ Sistem Mimarisi (Network System Architecture) için geliştirilmiş bir protokoldür. Anaçatı (mainframe) sistemler arasında kullanılan bu protokolün SDLC ve HDLC olmak üzere iki sürümü çıkmıştır. Bu iki protokolde yüksek seviyeli veri denetiminde kullanılır.

2.3 İnternet

İnternet aynı protokol ile anlaşılan bilgisayar ağlarının birleşimidir. Ağlar arasındaki ortak protokol genellikle TCP/IP protokol kümesi olup, ağlar yüksek hızlı telefon hatları ile birbirlerine bağlıdır. İnternet bağlantısına sahip yaklaşık üç milyon bilgisayar çeşitli bilgi ve hizmet sunmakta ve bunlara bağlı üniversitelerden, ticari kuruluşlardan milyonlarca insan birbirleriyle haberleşip veri alışverişinde bulunmaktadır.

İnternet üzerinde üç tür öge bulunmaktadır:

1. Bilgi Sağlayıcılar (Information Provider) : Bilgiyi kullanıcıların hizmetine sunar.
2. Kullanıcılar : Bilgiye sağlayıcıdan ulaşır.
3. Hizmet Sağlayıcılar (Service / Connection Provider) : Bilgi sağlayıcı ve kullanıcı arasındaki bağlantıyı sağlar.

2.3.1 İnternet hizmetlerinin yapısı

İnternet üzerinde verilen hizmetlerin büyük bir çoğunluğu istemci/sunucu yapısındadır. İstemci/sunucu yapısında bulunan iki bileşenden istemci, kullanıcı ile etkileşimli veri girişi ve gösteriminden sorumludur; kullanıcıdan gelen sorgulama isteklerini ve kullanıcının sağladığı veriyi sunucuya gönderdikten sonra, sunucuda isteğe karşı oluşan cevabı kullanıcıya uygun biçimde aktarır. Sunucu ise, istemci tarafından kendinden istekte bulunan görevleri yerine getirir; sorgulamaları ve verileri alır, dosyalardan okuma yaparak, komutlar işletir ve sonuçları veya durumları istemcilere bildirir. İstemci ve sunucu aynı makine üzerinde olabileceği gibi farklı makineler üzerinde de olabilir. [5]

Çeşitli internet hizmetleri Tablo 2.1' de gösterilmektedir.

2.3.2 İsimlendirme

İnternet' e bağlı tüm bilgisayarları tekil olarak tanımlayan bir adres ve isim mevcuttur. Tekil bir adrese sahip olan bir bilgisayar birden fazla isme sahip olabilir; fakat tüm bu isimler tek bir adresi işaret ederler. İsimlendirme 32 bit uzunluğundaki noktalı IP adreslerini, insanların kolayca hatırlayabileceği isimlere çevirme işlevini yerini getirmektedir.

Tablo 2.1 İnternet hizmetleri

Hizmet İsmi	Açıklaması
Devingen Konak Yapılandırma Protokolü (DHCP)	IP adreslerinin devingen olarak bilgisayarların hizmetine sunmak görevini yerine getirir.
Alan İsmiendirme Hizmeti (DNS)	Bilgisayarlara IP adresi üzerinden değilde, metin biçimindeki bir isim üzerinden hitap etmeyi olanaklı kılan hizmettir.
Dosya Aktarım Protokolü (FTP)	Dosyaların bir bilgisayardan diğer bir bilgisayara aktarılması görevini yerine getirir.
Gopher	Gopher verileri optik olarak hazırlamak ve aramayı kolaylaştırmak konusundaki ilk denemeydi. Fakat web ile anlamını yitirdi.
Hypertext Aktarım Protokolü (HTTP)	Web' in temelini oluşturan protokoldür. Sorgulanan web sayfaları ve içeriklerinin aktarımı görevini yerine getirir.
İnternet Sohbet Hizmeti (İnternet Relay Chat - IRC)	Anında sohbet gerçekleştirmek üzere kullanılan hizmettir.
Ağ Haber Aktarım Protokolü (NNTP)	Haber grupları, internet' teki kara tahtalar bu protokol üzerinden çalışır.
Elektronik Posta Hizmetleri (SMTP, POP)	İnternet üzerinden elektronik posta alışverişi görevini yerine getiren hizmetlerdir.
Telnet	Uzaktan komut satırı oturum yapısına sahip başka bir bilgisayar üzerinde çalışmayı olanaklı kılan hizmettir.
Basit Ağ Yönetim Protokolü (SNMP)	Ağ yönetimini gerçekleştirmek amaçlı olarak geliştirilmiştir.

IP adreslerinin isimlere dönüştürülmesi internet' in Alan İsmiendirme Hizmeti (Domain Name Service – DNS) tarafından gerçekleştirilir. Sıra düzensel isimler kullanan DNS, baştan sona doğru, özelden genele gider ve alan isimleri noktalarla

ayrılmış sözcüklerden oluşur. Örneğin, www.fbe.itu.edu.tr ismi Türkiye' de bir eğitim kurumu olan İstanbul Teknik Üniversitesi' nde fbe (Fen Bilimleri Enstitüsü)' nde www isimli bilgisayarın ismidir. İsimlerin en sonunda ISO 3166 standardına göre belirlenen ülke kodu (tr Türkiye, uk İngiltere gibi) bulunur. Ülke kodundan önce, bilgisayarın bulunduğu kurumun türünü gösteren com ticari kuruluş, mil askeri, edu eğitim kurumu gibi etkinlik grupları tanımlanır.

İsimleri adreslere çeviren hizmet birimlerine Alan İsimlendirme Sunucusu ismi verilir. DNS istemcileri bir isme karşılık gelen adresi bulabilmek için Alan İsimlendirme Sunucusu' na sorgular gönderir. DNS hizmet birimi, gerekirse diğer DNS hizmet birimleri ile bağlantı kurar ve yanıtı istemciye iletir.

Bazı alan isimleri başka alan isimlerini işaret eden takma isimler olabilirler; bu tür isimlendirme, sunulan hizmetlerle makineler arasında anlamsal bir bağ kurabilmek için yapılır. Örneğin, iki ayrı hizmet olan FTP ve WWW' nin sunulduğu bir bilgisayar hem ftp.hp.com, hem de www.hp.com isimleriyle hp.com alanına bağlantı sağlayabilmektedir.

3 BİLGİSAYAR SALDIRILARI

3.1 Bigisayar Saldırılarının Tarihseel Gelişimi

Bilgisayar saldırıları bilgisayarların icadı ile başlamıştır. Bilgisayar saldırılarının tarihçesine kronolojik olarak bakıldığında çok fazla olayla karşılaşılması, burada kabaca üzerinde durulmasını gerektirmektedir. Bilgisayar saldırılarının tarihsel gelişimi aşağıda aşamaları ile birlikte incelenmiştir.

- **Başlangıç.** Daha sistemlerin iletişim ağıları ile birbirlerine bağlanmadığı çağlarda, saldırganlar anaçatı, commodore 64 ve elma (apple) yazılımcılarıydılar. Bu devirde yazılımcılar arasında kırılmış yazılımlar ve saldırgan/kaçık araçlarının ticareti yapılmaktaydı. Bu ticari işleri düzenleyen kurallar vardı ve anti-sosyal davranışlar sergileyen saldırganlar ticari işlerden men edilmekteydi. Bunun yanında saldırganların bilinen önde gelen kişisel özellikleri, meydan okuma ve rekabet etme önceliğiydi.

Yazılım firmaları ürettikleri yazılımları kopyalamaya karşı korumak üzere çok üstün yeteneklere sahip güvenlik teknikleri kullanmaya başladılar. Buradan da anlaşılabilirceği gibi, saldırganların bu programları kırabilmek için, bilgi dağarcıklarını ve yetenek seviyelerini çok üst noktalara taşımaları gerekmektedir.

- **BBS çağı.** Bilgisayarların modemlerle birbirine bağlandığı BBS ağlarının kullanımının yaygınlaşması ile, dünyanın dört bir yanındaki yüzlerce bilgisayar birbirine bağlanmıştır. BBS ağlarının yaygınlaşması sonucu bilgi ve yazılım iletişiminin kolaylaşması, saldırı araçlarının dağıtımını kolaylaştırmıştır.

BBS ile birlikte yeni nesil, çağdaş saldırganlar ortaya çıkmıştır. BBS ile uzaktan diğer sistemlere erişim olarak tanımlanacak, yeni bir saldırı yöntemi ortaya çıkmıştır. Aynı zamanda web sitelerini ele geçiren, anti-sosyal davranışlar sergileyen ve sistem üzerindeki dosyaları yok eden zararlı saldırganlar ortaya çıkmaya başladılar. Artık saldırganlar ile güvenlik sistemleri arasındaki mücadelenin yer aldığı ikinci bölüm başlamıştı.

Birçok kuruluş ve üniversite üzerinde önemli bilgiler sakladıkları ve modemlerle birbirlerine bağlı bilgisayarlara sahiplerdi; bu bilgisayarlar saldırganların hedefi durumundaydı. Kısacası bilgisayar saldırıları artık kuruluşlar ve üniversiteler için büyük bir tehdit haline dönüşmüştü.

BBS, aynı zamanda, modern saldırı araçlarının da doğduğu bir çağdır. Artık saldırganlar "dialer" gibi güçlü saldırı araçları geliştirmeye başladılar. "Dialer" girilen belirli bir telefon aralağındaki tüm telefon numaralarını çevirerek, hatta bağlı modem olup olmadığını tespit eden bir araçtır. Ayrıca kullanıcı ismi ve şifre denemeleri yapan daha başarılı araçlarda görülmeye başlandı.

- **Mavi kutu.** Mavi kutu ve "dialer" yazılımlarının birleştirilmesi ile saldırganlar telefon sistemlerini kullanarak yerel ağlarından dışarıya dağıldılar. Telefon hatlarının yasa dışı kullanımı, telefon şirketlerini harekete geçirdi ve bilgisayar suçlarını ilgilendiren yasalar düzenlendi.
- **Ağ çağı.** Bilgisayar ağları binlerce bilgisayarı içine alacak büyüklüğe ulaştı; daha internet servis sağlayıcıları oluşmamasına rağmen, birçok üniversite ve kuruluş birbirine bağlanmış durumdaydı. Kabuk hesaplarının doğmasıyla saldırganlar kişisel bilgisayar ve modemler kullanarak sistemlere erişmeye, kendilerine sistem üzerindeki tüm erişim haklarını sağlamaya ve diğer sistemleri ele geçirmek üzere bu sistemleri kullanmaya başladılar.

Bilgisayar ağlarının gelişmesi, saldırganların gelişmesi ve saldırı eylemlerinin artması sonuçlarını oluşturdu. Artık kötü niyetli saldırganlar dosyaları silerek, sistemi göçerterek, sisteme zararlar vermekteydi.

- **Web çağı.** Alan isimlendirme sisteminin icadı ile web sistemi doğdu; web' in icadı ile, web üzerinde aktif olan kullanıcı sayısında büyük bir patlama gerçekleşmiştir. Web' in BBS' in yerini alması saldırı araçları ve yöntemlerinin dağıtımını daha da kolaylaştırdı. Windows ve grafiksel kullanıcı arabiriminin yarattığı kullanım kolaylığı, kod parçası çocukları (script kiddies) olarak adlandırılan yeni bir saldırgan tipini doğurmuştur. Bu tip saldırganların bilgi dağırcığı çok geniş değildi; zaten yeni saldırı araçlarının kullanımı da çok büyük yetenekler gerektirmemekteydi. Ayrıca web' de herkesin isimsiz olması, kod parçası çocuklarının kimliklerini ele vermeden istediklerini yapabilmeleri sonucunu doğurmuştur. Bu nedenle zararlı ve anti-sosyal davranışlarda (virüs, truva atı, hizmet dışı bırakma) artışlar gözlemlendi. Artık bilgisayar saldırıları genelde kötü niyetli olmaktaydı; meraktan gerçekleşen saldırılar ise yok olmaktaydı. Zararlı saldırıların yoğunlaşması sistem

güvenliğini en önemli konu haline getirdi; fakat kapatılan bir gedik, iki yeni gediğin oluşmasına sebep olmaktadır. Kabuk hesapları ve saldırıda izinizi saklamak çok önemlidir; fakat kolaylıkla izinizi saklayabilmekteydiniz. Bu durumla başedebilmek üzere yasalar çıktıktan sonra, FBI ve SS saldırganlar ile mücadeleye girişti. Ancak sadece saldırılarının izini gizlemede ihmalkar davrananlar yakalanabilmekteydi. Oysaki iyi bir saldırgan, bilgisayar üzerinde yaptıkları işlerin izini bırakmayanlardır. Dünyanın en ünlü ve eski saldırganlarından olan Kevin Mitnick gerçekleştirmiş olduğu saldırılar sonucunda, birçok firmayı binlerce dolar zarara uğratmak suçundan hapse bulunmaktadır. Ünlü telefon sistemlerine düzenlediği saldırılardan alan Mitnick, son olarak internet' e bağlı firmaların bilgisayarlarına girerek bilgilerin kopyalanması, silinmesi gibi maddi zarar veren hareketlerde bulunmuştur. [6]

- Artık saldırganlar yeteneklerini ve bilgilerini genişlettiler; böylelikle sistem yöneticilerinden daha üst seviyede bilgiye sahip oldular. Bir çoğu büyük paralara diğer tarafa geçerek ağ güvenlik uzmanı oldular. Diğerleri ise gerçek bir suç ögesi haline dönüştüler.

3.2 Saldırgan Tipleri

Saldırganlar yaptıkları işlere göre birkaç farklı tipte adlandırılırlar:

- Saldırgan (Hacker): Bilgisayarlar hakkında çok geniş bilgi ve yeteneğe sahiptirler.
- Kaçık (Cracker): İşleri bilgisayar sistemini kırmaktır. İşletim sistemi ve işletim sistemi güvenliği hedefleridir.
- Şifre pankçısı (Cypherpunk): Kriptografi uzmanlarıdır.
- Phreaker: Telefon sistemini kullanarak istenmeyen bir şekilde sisteme erişmenin inceliklerini çok iyi bilirler.
- Kod parçası çocukları: Bilgi dağarcıkları ve yetenekleri sınırlı yeni nesil saldırgan grubudur. Kullandıkları saldırı aracından öte bir güçleri yoktur.

İyi bir saldırgan tüm bu alanlarda bilgi sahibi olmakla birlikte, içinden birinde uzmanlaşmalıdır. Saldırganlara sistemi ele geçirmede ve geçirdikten sonra yapacağı işlemlerde kullanacağı araçları sağlarlar; kaçıklar sisteme girecek kapıları bulur ve açarlar; şifre pankçıları hayatı kolaylaştıracak anahtarları sağlarlar; phreaker' lar ise saldırı izlerini örtmek için telefon sistemini yanıtlırlar. [7]

Bilgisayar sistemlerinin ele geçirilmesi, günler, haftalar, hatta aylar alacak sabırlı ve dikkatli bir çalışma gerektirir.

Aşağıda saldırganlar yetenek seviyeleri ve amaçlarına göre gruplanmışlardır:

- Meraklı Joe' lar
- Kod Parçası Çocukları
- Wannabes
- Seçkinler
 1. Beyaz Şapkalar
 2. Siyah Şapkalar
 3. Gri Şapkalar

3.2.1 Meraklı Joe' lar

Bilgisayar ağlarının (telnet, ftp vb.), web' den daha geniş olduğunu keşfeden saldırganlardır. Bu tip saldırganlar çok meraklıdır; bununla birlikte bilgi dağarcıkları ve yetenek seviyeleri çok geniştir. Meraklı Joe' ların sisteme herhangi bir zarar verme amaçları yoktur. İzlerine kolayca erişilebilecek kabuk hesaplarını kullanmazlar ve eriştikleri sistemde izlerini belli etmezler.

3.2.2 Kod parçası çocukları

Birçok soruna yol açan kod parçası çocukları kendilerini saldırgan olarak adlandırırlar, fakat değildirler. Tüm bilgi ve yetenekleri kullandıkları programlardır; bunlardan daha ötesi yoktur. Günümüzde öyle yetenekli saldırı araçları vardır ki, bir sistemi ele geçirmek için kod parçası çocuklarının daha ileri bilgi ve yeteneğe ihtiyacı da yoktur.

3.2.3 Wannabes

Kod parçası çocuklarından çok daha üstün düzeyde yeteneklere sahiptirler. Tek hedefleri seçkin sınıfından bir saldırgan olmaktır. Bunu da çok büyük bir sistemi ele geçirip, kendilerinin yaptığını belirten imzalarını bırakarak gerçekleştirebileceklerini düşünürler.

3.2.4 Seçkinler

Beyaz, siyah ve gri olmak üzere üç sınıfa ayrılırlar. Tümü çok yüksek bilgi ve yetenek seviyesine sahiptirler. Bunları birbirlerinden ayıran özellikler, amaçları, davranışları ve eksiklikleridir.

- **Beyaz Şapkalar:** Bu grup güvenlik danışmanı olarak görev yapanlardan oluşur. Sistem yöneticileri ve siber polis gibi. Bu işi yapma nedenleri, bir nevi oyunculuk, para ve gururdur.
- **Siyah Şapkalar:** Bilgisayar ağlarının kötü çocuklarıdır. Bunlar virüs yaratıcıları, siber casuslar, siber teröristlerdir.
- **Gri Şapkalar:** Siber savaşlarda yerine getirmiş oldukları çekirdek görevi onları diğerlerinden farklı kılar. Kod parçası çocuklarının kullandıkları kod parçalarını gri şapkalar yazarlar. Genellikle bilgisayar ağlarındaki güvenlik eksiklikleri, devlet ve kuruluş saldırıları ile ilgilenirler. Genel olarak zararlı olmamalarına rağmen tahrik edildiklerinde zararlı olabilirler. Sistemi kendilerinin bazı amaçları veya ilgilendikleri bilgileri elde etmek için kullanırlar.

3.3 Program Saldırıları

Bilgisayar saldırılarının oldukça ilgi çeken bir konu haline gelmesi, bu alanda bir çok iş ortaya çıkarmıştır. Genellikle 14 yaş civarında olan ve yeni yetişen saldırganlar bilgisayar sistemlerine zorla girerek yazılımları kırarak sistemlere saldırmaktadırlar.

Saldırı olaylarının boyutlarının genişlemesi, ciddi bir koruma ihtiyacını doğurmuştur. Kuruluşlara ve kullanıcılara ait bilgilerin mahremiyetinin önemli olduğu noktada, bilgisayar saldırılarına karşı güvenliğin sağlanması önemli bir konu haline dönüşmektedir. Bilgisayar saldırılarına karşı iyi bir koruma, mevcut saldırı tiplerinin değerlendirilerek, bir saldırgan gibi düşünebilme yetisinin kazanılabilmesiyle gerçekleştirilir. Saldırının ne zaman, nereden, nasıl geleceğini tahmin edebiliyorsanız, o kadar iyi bir koruma planı oluşturabilirsiniz.

Bilgisayarlara saldırı düzenlemek meraklı kişiler için eğlenceli zararsız bir iştir; fakat kötü düşünceli bilgisayar saldırganları sistemlere büyük zararlar verebilmektedir. Genelde insanların bilgisayar saldırganları ile ilgili görüşü, saldırganların ahlaki olarak zararlı insanlar olduğudur. Bilgisayar suçlarına karşı oluşturulan yasalarda, bir sistemi yasal olmayan yollardan ele geçirmenin cezası on yıldır.

Basitçe, bilgisayar sistemleri ve yazılımlarının yasal olmayan yollardan ele geçirilmesi olarak tanımlanabilecek bilgisayar saldırılarının, genel nedenleri aşağıda listelenmiştir: [8]

- Saldırganlar kendi zevkleri ve yaptıkları ile övünmek için sisteme saldırılar düzenlerler.

- Yazılımların yasal olmayan yollardan kullanımını engellemek için geliştirilen kopya koruma sistemlerini kırmak amaçlı olarak düzenlenir.
- Sisteme erişimde kullanılan şifreleri kırmak amaçlı olarak düzenlenir.
- Gençlerin casusluk merakı sonucu olarak da saldırı düzenlenir.

Sonuç olarak, bilgisayar sisteminizi saldırılardan korumak için alacağınız en basit önlemler aşağıda listelenmiştir:

- Sisteme bağlanmak için kullanılan şifreler ve sistem üzerindeki mantıksal işlevler şüpheli bir duruma karşı belirli aralıklarla kontrol edilmelidir.
- Kaynaklara erişimde şifre kullanımı alışkanlık haline getirilmeli ve saldırganın tahmin edemeyeceği karışıklıkta şifreler kullanılmalıdır.
- Sistem üzerinde çalışan "exe" ve "dll" dosyaları kontrol edilmeli ve emin olunmayan kaynaklardan elde edilen programlar bilgisayarlara yüklenmelidir.

3.4 Geçmişten Bugüne Gündem Oluşturan Bilgisayar Saldırıları

Bugüne kadar gerçekleştirilen önemli saldırı olaylarının bazıları aşağıda listelenmiştir: [9]

- Captain Zap: Arkadaşları arasında Captain Zap olarak bilinen Ian Murphy, 1981'de AT&T' nin bilgisayarlarına girip, dahili saatleri değiştirerek, fatura oranlarının değişmesine sebep olmuştur. "Sneakers" filminin de ilham kaynağı olan Murphy şimdi "IAM/Secure Data System" 'in başkanlığını yapmaktadır.
- Morris Worm: 2 Kasım 1988 yılında Robert Tappan Morris, internet' in onda birini çalışmaz hale getiren bir solucan yaymıştı; bu solucan yaklaşık 6000 bilgisayar sistemini etkilemişti. Morris Worm adıyla bilinen bu saldırı, hükümetin anti siber-terorizm takımı olan CERT (Computer Emergency Response Team)' in kurulmasına neden olmuştur. Morris, Bilgisayar Dolandırıcılık ve Yolsuzluk Kanunu ile tutuklanan ve ceza alan ilk kişi olmuştur; ancak solucanın bulaştığı bilgisayarlara zarar vermemesi nedeniyle, sadece ceza ödemesine ve amme hizmetinde bulunma cezasına çarptırılmıştır.

Morris' in babası Robert Morris Sr. o zamanlarda NSA' de bilgisayar güvenlik uzmanıydı.

- **MOD ve LOD Takımları:** Hile uzmanları (Masters of Deception - MOD) genellikle telefon sistemleriyle eğlenen "telefon phreaker" larıydı. Onlar bedava uzak mesafe telefon görüşmeleri yapmakla ve özel konuşmaları dinlemekle ünlüydüler. Ayrıca bir çok insanın birlikte sohbet etmesini sağlayan hatlar yaratmayı başarmışlardır.

MOD NSA, AT&T ve Amerika Bankası'na ait veritabanlarına girmişlerdir. Ayrıca kredi kartı kayıt raporlarını tutan, TRW' nin bilgisayar sistemlerine de girerek zengin ve ünlülerin kredi kartı raporlarına erişmişlerdir.

MOD, en ünlü saldırganların karargahı olarak bilinen başka bir saldırgan grubu olan, ünlü Kıyamet Lejyonları (Legion of Doom - LOD) ile yaptığı savaşlarla da tanınır.

- **Kevin Mitnick:** Mitnick devlet bilgisayarlarına suç amaçlı girdiği için tutuklanan ilk kişidir. Mitnick ayrıca FBI' ın, "en çok arananlar" listesinde yer alan ilk kaçıktır.

Mitnick bilgisayar sistemlerinden bir milyon dolar değerinde gizli bilgi çalmak, internet' ten erişime açık veritabanlarından, binlerce kredi bilgisini çalmak, California motor araçları veritabanına girmek ve New York ve California' nın telefon anahtarlama "hub" larını uzaktan kontrol etmekle suçlanmıştır.

Mitnick, "War Games" filmine ilham veren ve onun yaptığı iddia edilen Kuzey Amerika Hava Savunma (North American Air Defense - NORAD) bilgisayarlarının kırılması olayını reddetmiştir.

Mitnick, ayrıca, saldırganlar arasında sosyal mühendislik olarak bilinen ve basitçe, istenilen bilgilere ulaşmak için insanlara soru sormak yönteminde de bir dahi idi. Çoğu zaman Mitnick girdiği sistemlerin şifrelerini yararlı işler için kullanacağını söyleyerek ikna ettiği sistem yöneticilerinin kendilerinden almıştır.

- **Büyük Banka Soygunu:** 1995 yılında St. Petersburg Üniversitesi mezunu Vladimir Levin, Citibank' ın bilgisayarlarına girerek müşterilerin hesaplarından, yaklaşık 10 milyon doları kendi hesabına aktarmıştır. Levin Heathrow havaalanında Interpol tarafından yakalanmış ve Citibank paranın büyük bir kısmını geri almıştır.
- **Virüsler:** 20. yüzyılın en kötü iki elektronik posta virüsü, "LoveBug" ve "Melissa" olmuştur. "LoveBug" geçen mayıs ayında ortaya çıkmış ve "Manila's AMA Computer College" inden yayıldığı tahmin edilmiştir. 1999

yılının Nisan ayında yayılan Melissa, bir kaç saat içinde 100.000' den fazla elektronik posta kullanıcılarını etkilemiş ve yazarı olan David Smith' e kötü bir ün kazandırmıştır.

- **Kod Parçası Çocukları:** 2000 yılının, Şubat ayında MafiaBoy adında Kanada' lı bir çocuk, bir çok internet sitesine hizmet dışı bırakma saldırısı düzenlemekten tutuklanmıştır.

MafiaBoy, Amazon, eBay ve Yahoo sistemlerini 6-14 Şubat tarihleri arasında çalışmaz duruma getirmeyi başarmıştı. Avukatı Yan Romanowski'nin "eğer MafiaBoy tüm gücünü kullansaydı, tahmin edilemez zararlara neden olabilirdi" iddialarına karşın, MafiaBoy' un bir dahi olduğuna inanan pek yoktur; o bilgisayar ağlarına rastgele veri göndermek ve etkilemek için sadece bir kod kullanmıştı. MafiaBoy 52 ağda 75 bilgisayara izinsiz erişim sağlayıp, hizmet dışı bırakma aracı yüklemiş ve 11 internet sitesine saldırıları bu araç vasıtasıyla yapmıştır.

- **Beyaz şapkalılar:** Beyaz şapkalılar arasında, yazılımın kaynak koduyla birlikte gelmesi gerektiğini düşünen ve "Free Software Foundation" ın kurucusu olan Richard Stallman, bilgisayar alamadığı için kendisi bilgisayar yapmaya karar veren ve ilk Apple kişisel bilgisayarı ortaya çıkaran Steve Wozniak ve Linux' un babası Linus Torvalds sayılabilir.

4 GÜVENLİK TEKNOLOJİLERİNE GİRİŞ

İnternet' e olan ilginin hızla artmasıyla ağ güvenliği , tüm dünya genelinde internet üzerinde faaliyet gösteren kurumlar için büyük endişe kaynağı haline geldi. Şirket ağlarının güvenliğini aşmaya yardımcı olan bilgi ve araçların yaygın hale gelmesi, bu endişeyi daha da arttırdı .

Ağ güvenliğine odaklanan bu ilgiden dolayı , ağ yöneticileri mevcut ağ kurulumu ve yönetiminden çok, ağları korumaya çaba harcamaktadırlar . Güvenlik yöneticisi (SATAN) gibi , sistem zayıflıklarını araştıran yeni araçlar bu çabalara yardım etmektedirler; fakat bu araçlar, ağları korumak yerine ağların zayıf alanlarını belirtmektedirler . Buna karşın, ağ yöneticileri düzenli olarak bugünün dünyasında karşılaşılabilecek birçok ağ güvenliği sorununa karşı bilgili olmak zorundadırlar. Yerel ağ internet' e açıldığında oluşacak güvenlik sorunlarının bazıları ilerleyen satırlarda incelenecektir.

4.1 İnternet' e Bağlanıldığında Karşılaşılabilecek Güvenlik Sorunları

Özel ağınıza internet' e bağlamak, ağınıza 50.000 bilinmeyen ağ ve kullanıcıyı özel ağınıza fiziksel olarak bağlamak demektir. Her ne kadar böyle bağlantılar, çok yararlı uygulamalara imkan tanısa ve bilgi paylaşımında büyük olanaklar sağlasa da, yerel ağlar, genellikle internet üzerindeki kullanıcılar ile paylaşılması gereken bir çok bilgiyi içermektedirler. Bununla birlikte her internet kullanıcısının kurallara uygun davrandığı da düşünülemez. Bu iki neden, internet dünyasında güvenlik konusunun arkasındaki anahtar sorunları gösterir:

- Yetkisiz kişilerden özel bilgilerinizi nasıl korursunuz?
- Dışardaki kötü niyetli kullanıcılar ve saldırılardan ağınıza ve kaynaklarınızı nasıl korursunuz?

4.1.1 Gizli bilgiyi korumak

Gizli bilgi , ağda iki durumda bulunabilir: Sabit disk sürücüsü veya bellek gibi fiziksel ortamlarda veya ağ paketleri formunda fiziksel ağ üzerinde iletim halinde bulunabilir. Bilginin fiziksel ortamdaki bu iki durumu, internet üzerindeki kullanıcılardan olabileceği gibi, iç ağdaki kullanıcılardan da gelebilecek saldırılara

birçok olanak tanır. Ağ güvenlik konusunu içeren ikinci durum ile öncelikle ilgilenilmelidir. Aşağıda, özel ağınızdaki bilgilere ulaşmak için kullanılan beş yaygın saldırı yöntemi listelenmiştir: [10]

1. Ağ paket dinleyicileri,
2. IP taklidi,
3. Şifre saldırıları,
4. Dış kaynaklara hassas iç bilginin dağıtımı,
5. Ortadaki adam (Man-in-the-middle) saldırıları.

Bu saldırılardan bilginizi korumak istediğinizde, dikkat etmeniz gereken, hırsızlığı, hassas ve gizli bilginin bozulmasını ve düzeltilemeyecek şekilde zarara uğratılmasını engellemek olmalıdır. Yaygın saldırı yöntemleri ve gizli bilgilere nasıl ulaşılabildiği aşağıda örnekler ile anlatılacaktır.

Ağ paket dinleyicileri

Ağ üzerindeki bilgisayarlar seri olarak iletişimde olduklarından, büyük bilgiler küçük parçalara bölünür. Bu küçük parçalar, ağ paketleri olarak adlandırılmaktadır. Çeşitli ağ uygulamaları, ağ paketlerini açık metin olarak dağıtmakta olup, ağ üzerinde bir uçtan diğer uca gönderilen bilgi şifrelenmemektedir. Şifrelenmemiş ağ paketleri, ağ üzerinde onları okuyabilen herhangi bir uygulama tarafından işleme tabi tutulabilir ve anlaşılabilir.

Ağ protokolü, hangi paketin hangi bilgisayar için gönderildiğini belirlemek için, paketlerin nasıl tanımlandığı ve etiketlendiğini belirtmektedir. TCP/IP gibi ağ iletişim protokollerinin tanımlarının yaygın bir şekilde bilinmesi sebebiyle, üçüncü bir kişi tarafından ağ paketlerinin yorumlanması ve ağ paket dinleyicilerinin geliştirilmesi oldukça kolaydır. Paket dinleyici, yerel ağ üzerinde gönderilen bütün ağ paketlerini yakalamak için her geleni kabul eden (promiscuous) ağ uyarlayıcı kartını kullanan yazılım uygulamasıdır.

Birçok ağ uygulamasının bilgiyi ağ üzerinde açık metin olarak göndermesinden dolayı, ağ dinleyicisi kullanıcısına kullanıcı hesapları ve şifreleri gibi birçok faydalı bilgiyi sağlar. Eğer ağ üzerinde veritabanları kullanılması durumunda paket dinleyici, veritabanından sorgulanan bilgiyi saldırgana sağlamakla birlikte kullanıcı hesapları ve şifreleri gibi veritabanına erişimde kullanılan bilgileri de elde edebilir. Kullanıcı hesapları ve şifrelerini elde etmek ile karşılaşılan bir diğer önemli sorun, aynı hesapların ve şifrelerin, kullanıcılar tarafından birçok uygulamada da kullanılmasıdır. Buna ek olarak, birçok ağ yöneticisi ağ ile ilgili sorunları bulmak ve çözmek için

paket dinleyicilerini kullanır. Ağ yöneticileri bu esnada ağ üzerinden, saldırıya karşı hassas olan bilgileri inceleme olanağı bulmaktadırlar.

Kullanıcıların çoğu, kendisine ait kullanıcı hesapları ve uygulamaların tümü için tek şifre kullanmaktadır. Saldırganlar, insanların farklı nesneler için tek şifre kullanma zaafından faydalanarak hassas bilgiye erişim kazanmada sık sık başarılı olurlar.

IP taklidi

IP taklidi saldırısı, ağ dışındaki saldırganın ya ağın güvendiği IP adres alanından birini ya da güvenilen ve bazı kaynaklara erişim yetkisi verilmiş bir harici IP adresini kullanarak güvenilen sisteme sızmaya teşebbüs etmesidir.

Normal olarak, IP taklidi saldırısı , istemci sunucu arasındaki veya uçtan uca ağ bağlantısındaki veri akışı içerisine komut veya veri eklenmesiyle sınırlıdır. Çift yönlü iletişimi sağlamak için, saldırgan taklit edilen IP adresine erişimin sağlanması için tüm yönlendirme çizelgelerini değiştirmelidir. Diğer bir yaklaşım ise saldırganın uygulamadan herhangi bir cevap beklememesidir.

Saldırgan yönlendirme çizelgelerini, taklit edilen IP adresine yönlendirilecek şekilde değiştirebilirse, taklit edilen adrese gönderilen tüm paketleri alabilir ve herhangi bir güvenilen kullanıcı gibi cevap verebilir. Paket dinleyicileri gibi, IP taklidi de, ağ dışından olan kişilere kısıtlanamaz. [10]

Şifre saldırıları

Şifre saldırıları brute-force (ardarda bir çok şifrenin denenmesi) saldırıları, truva atı programları, IP taklidi ve paket dinleyicileri gibi birçok farklı yöntem kullanılarak gerçekleştirilebilir. Her ne kadar paket dinleyicileri ve IP taklidi , kullanıcı hesapları ve şifrelerini ele geçirmeyi sağlasa da, genellikle şifre saldırısı, kullanıcı hesabını ve/veya şifresini tanımlamak için artarda süregelen birçok çabayı içerir. Bu tekrarlanmış çabalar , brute-force saldırısı olarak adlandırılırlar.

Brute-force saldırısı, genellikle sunucu gibi, paylaşılmış kaynağa erişmek için ağ üzerinde çalışan bir program kullanılarak gerçekleştirilir. Saldırgan kaynağa erişim hakkı kazandığında hesabını kullandığı kullanıcıyla aynı haklara sahip olur. Eğer bu hesap, yeterli ayrıcalıklara sahip ise, saldırgan, kullanıcı hesabında meydana gelebilecek durum veya şifre değişikliğinden endişe duymaksızın gelecekteki erişimleri için sistemde arka kapı oluşturabilir.

Hassas bilginin dağıtımı

Hassas bilginin dağıtımını kontrol etmek, ağ güvenlik planının çekirdeğindedir. Böyle bir saldırı size anlaşılabılır gelmese de, firmaların yaşadığı bilgisayar saldırılarının çoğunluğu memnuniyetsizlik duyan mevcut veya eski çalışanlar tarafından gerçekleştirilmektedir. Bu güvenlik gediklerinin çekirdeğinde, hassas bilginin, onu zararınıza kullanabilecek rakiplerinize veya diğer insanlara dağıtımı vardır. Dışarıdan gelecek bir kullanıcı (saldırgan), bilgiyi kopyalamak için şifre ve IP taklidi saldırılarını kullanabilir, ve içerdeki kullanıcı da hassas bilgiyi kolaylıkla dışardaki bir bilgisayara ya da paylaşılmış bir ağ sürücüsüne yerleştirebilir.

Örneğin; içerdeki kullanıcı masasından bile kalkmadan dosyayı dışarıya açık bir FTP sunucusuna yerleştirebilir veya bu bilgiyi bir elektronik postaya ekleyerek dışarıdaki bir kullanıcıya gönderebilir.

Ortadaki adam (Man-in-the-middle) saldırıları

Ortadaki adam saldırısı , saldırganın ağ üzerindeki paketlere erişimini gerektirir. Böyle bir duruma örnek olarak ağınızla, diğer ağlar arasında iletilen tüm bilgi paketlerine erişim kazanabilecek, internet servis sağlayıcınızda çalışan biri gösterilebilir. Böyle saldırılar, genellikle ağ paket dinleyicileri, yönlendirme ve iletişim protokolleri kullanılarak gerçekleştirilir. Böyle saldırıların olası kullanımları, bilgi hırsızlığı, dahili ağ kaynaklarına erişim için mevcut oturumun ele geçirilmesi, mevcut ağ yapısı hakkında bilgi elde etmek için trafiğin izlenmesi, hizmetin engellenmesi, iletilen bilginin bozulması ve ağ oturumlarına yeni bir bilginin eklenmesi olabilir.

4.1.2 Ağınızı korumak: İç ağ sistem bütünlüğünü sağlamak

Bilginizi korumak, belki sizin için en yüksek önceliğe sahip olabilir, ancak ağınızın bütünlüğünü sağlamak onun içerdiği bilgiyi korumayı sağlamada en büyük öneme sahiptir. Ağınızın bütünlüğünde oluşacak bir açık, vakit ve çaba yönünden aşırı derecede pahalıya mal olabilir ve süregelen saldırılar için birçok yeni imkan oluşturabilir. Ağ bütünlüğüne zarar vermek için kullanılan beş saldırı yöntemi aşağıda incelenecektir: [10]

1. Ağ paket dinleyicileri,
2. IP taklidi,
3. Şifre saldırıları,
4. Hizmet dışı bırakma,

5. Uygulama katmanı saldırıları.

Ağınız içinde neleri korumayı düşündüğünüzde, öncelik vermeniz gereken; fiziksel ağınızın, ağ yazılımınızın, diğer ağ kaynaklarının ve itibarınızın bütünlüğünü devam ettirmek olmalıdır. Bu bütünlüğü devam ettirmek, bilgisayarların ve kullanıcıların doğrulanabilir birer kimliğe sahip olmasını, ağın sağladığı hizmetlerin doğru şekilde faaliyet göstermesini ve en üst seviyede ağ başarımının sağlanmasını içerir. Tüm bunların sağlanması üretken bir ağ çevresinin oluşmasında büyük öneme sahiptir. Önceden bahsedilen saldırı yöntemleri ve bu yöntemlerin ağ bütünlüğüne zarar vermede nasıl kullanılabileceği anlatılacaktır.

Ağ paket dinleyicileri

Daha önceden bahsedildiği şekilde, ağ paket dinleyicileri, kullanıcı bilgileri ve şifreleri gibi önemli sistem bilgisine erişim sağlamada kullanılmaktadırlar. Saldırgan doğru hesaplara eriştiğinde ağınızı ele geçirebilir. En kötü durumda her zaman ağa erişimde arka kapı olarak kullanılabilecek yeni bir kullanıcı hesabı açmayı sağlayabilecek sistem seviyesindeki bir hesaba erişim kazanabilir. Saldırgan sistem yöneticisi hesabının şifresi, hizmetlerin listesi, dosya sunucusuna erişim hakkı ve özel bilgi içeren bilgisayarlara erişim bilgisi içeren dosyalar gibi büyük öneme sahip dosyaları düzenleyebilir.

Paket dinleyicileri, ağ topolojisi hakkında birçok saldırganın faydalı bulacağı bilgileri sağlarlar. Hangi bilgisayarda hangi hizmetlerin çalıştığı, ağ üzerinde kaç bilgisayarın bulunduğu, hangi bilgisayarların hangilerine erişim hakkı olduğu ve benzeri bilgiler günlük işlemlerin sonucunda gönderilen ağ paketlerinden elde edilebilir.

Buna ek olarak, ağ paket dinleyicisi var olan ağ paketlerindeki bilgileri değiştirmekte veya ağ üzerine yeni paketler eklemekte de kullanılabilir. Böylelikle saldırgan paketlerdeki kritik bilgileri değiştirmekle birlikte ağ iletişiminin kopmasına da sebebiyet verir. Saldırganın, muhasebe sisteminize eklenen bilgiyi değiştirdiğinde olabilecekleri düşünün. Böyle saldırıların etkilerini saptamak zordur ve düzeltmek çok pahalı olabilir .

IP taklidi

IP taklidi , kullanıcı hesapları ve şifrelerine erişim hakkı sağlayabildiği gibi birçok farklı şekilde de kullanılabilir. Örneğin, saldırgan kurumunuzu zor durumda bırakacak şekilde kullanıcılarınızdan birini taklit edebilir, saldırgan iş ortaklarınıza elektronik posta yollayarak bunu kurumunuzdan bir kişi tarafından gönderilmiş gibi gösterebilir. Saldırganın, kullanıcı hesabı ve şifresine sahip olması, bu tür saldırıları

daha da kolaylaştırır. Fakat iletişim protokolleri hakkında sahip olunacak basit bir bilgi ile de kolaylıkla IP taklidi saldırılarını gerçekleştirmek mümkündür.

Şifre saldırıları

Paket dinleyicileri ve IP taklidi gibi, brute-force şifre saldırıları da kritik ağ dosyalarını ve hizmetlerini değiştirmekte kullanılabilecek hesaplara erişim sağlayabilir. Ağınızın bütünlüğüne zarar verebilecek bu konuya, saldırganın ağ yönlendirme tablolarını değiştirmesi örnek olarak verilebilir. Böylelikle, saldırgan tüm ağ paketlerinin varış noktalarına ulaşmadan önce kendisine yönlendirildiğine emin olur. Böyle bir durumda, saldırgan bütün ağ trafiğini takip edebilir, etkin bir şekilde ağ trafiğinin ortasındaki adam (man in the middle) durumundadır.

Hizmet dışı bırakma

Hizmeti engellemeye yönelik saldırılar diğer saldırılardan çok farklıdır; çünkü bu saldırılar ağınıza veya ağınızdaki bilgiye erişim kazanmayı hedeflemezler. Bu saldırılar, ağ veya sistem kaynaklarını aşırı şekilde kullanarak hizmetin diğerleri tarafından kullanılmasını engellemeye yöneliktir. Bu saldırılar, HTTP ya da FTP gibi özel sunucu uygulamaları söz konusu olduğunda, sunucu tarafından desteklenen tüm mevcut olan bağlantı kaynaklarını açık tutarak o anki, kullanıcıları kilitlemeye odaklanır. Bu tür saldırılar, TCP/IP ve ICMP gibi yaygın internet protokolleri kullanılarak da uygulanabilir. Hizmetin engellenmesine yönelik saldırılar, genellikle yazılım hatası veya güvenlik açığından ziyade saldırılan sistemin bütünlüğünden kaynaklanan zayıflıklardan faydalanır. Buna karşın, bazı saldırılar ağa istenmeyen ve genellikle faydasız olan paketlerin aşırı derecede yollanması sonucu ağ başarımının düşürülmesi ve ağ kaynakları hakkında yanlış bilgi verilmesi gerçekleştirilir. [10]

Uygulama katmanı saldırıları

Uygulama katmanı saldırıları, çeşitli farklı yöntemlerin kullanılmasıyla gerçekleştirilir. En sık kullanılan yöntem, Sendmail, PostScript ve FTP gibi sunucu üzerinde bulunan uygulamaların çok iyi bilinen zayıflıklarının kullanılmasıyla gerçekleşir. Bu zayıflıkları ortaya çıkaran saldırgan, bu uygulamayı çalıştıran hesabın (genellikle yetkilendirilmiş sistem düzeyinde bir hesap) yetkileriyle bu bilgisayara erişim kazanır.

Truva atı programı saldırıları, saldırganın yaygın programların yerine, bu programları yerleştirmesi ile gerçekleşir. Bu programlar, normal programın sağladığı bütün işlevselliği sağlayabilir ve bundan başka, kullanıcı hesabi ve şifre bilgisini

yakalamak gibi saldırgan tarafından bilinen diğer özellikleri içerebilir. Bu programlar, hassas bilgiyi yakalayabilirler ve saldırgana bu bilgiyi geri döndürebilirler. Bu programlar, uygulamaların özelliklerini de değiştirebilir ve tüm kurum bünyesinde gönderilen elektronik postaların bir kopyasını da saldırgana göndermek gibi bir fonksiyona sahip olabilirler.

En eski truva atı uygulaması, kullanıcının gerçek olduğunu düşündüğü bir sisteme bağlantı ekranı gösteren programdır. Kullanıcı gerçek olduğunu düşündüğü bu ekrana kullanıcı adını ve şifresini girer; uygulama bu bilgiyi ele geçirerek saldırgana iletir ve ya normal sistem işlemine devam eder (çağdaş sistemlerde gerçekleştirilmesi imkansızdır) ya da yanlış kullanıcı ismi/şifresi gibi bir hata mesajı döndürerek kendini sonlandırır ve asıl sisteme bağlantı uygulamasını çağırır. Kullanıcı normal olarak hata yaptığını düşünerek kullanıcı ismini ve şifresini yeniden girer ve uygulama olması gerektiği gibi normal şekilde devam eder.

En yeni uygulama katmanı saldırılarına HTML, web tarayıcısı fonksiyonları ve HTTP gibi birçok yeni teknoloji olanak tanır. Bu saldırılar Java applet' lerini ve ActiveX kontrollerini içeren zararlı programların ağ üzerinden iletilip kullanıcının internet tarayıcısına yüklenmesiyle gerçekleşir.

ActiveX kontrolleri kullanıcıları, Microsof tarafından tanıtılan "Authenticode" teknolojisine güven duyarak yanlış yönlendirilebilirler. Buna karşın, saldırgan hali hazırda bir truva atı programını nasıl doğru şekilde imzalanmış ve hatadan arındırılmış bir ActiveX kontrolü haline getireceğini bilmekte olabilir. Bu teknik ile saldırgan, dosyaların üstüne yazmak ve diğer programları çalıştırmak gibi kirli işlerini yapmak için VBScript kullanır. Bu yeni tür saldırılar iki açıdan farklıdır;

1. Bu uygulamalar saldırgan tarafından değilde, zararlı kodu içeren HTML sayfasının kullanıcı tarafından yüklenmesiyle başlatılır.
2. Saldırıları, programlama dillerinin ortam bağımsız olmasından dolayı donanım ortamlarıyla ve işletim sistemleriyle sınırlandırılmamışlardır.

4.2 TCP/IP'nin Zayıf Noktaları

4.2.1 TCP sıralama numarasının tahmini

TCP sıralama numarasının tahmini, sunucudan hiçbir mesaj almadan TCP paket sıralama numarasının üretilmesidir. Bu saldırgana yerel ağdaki bir konağın kimliğini çalması olanağını verir. Normal bir TCP bağlantısının kurulması üç yollu el sıkışma protokolü ile gerçekleşir. Üç yollu el sıkışma protokolünün şematik gösterimi (Şekil 4.1) ve açıklaması aşağıdadır:

```

C → S : SYN(ISNc)
S → C : SYN(ISNs) , ACK(ISNc)
C → S : ACK(ISNs)
C → S : veri
      ve/veya
S → C : veri

```

Şekil 4.1 Üç yönlü el sıkışma protokolü

İstemci rastgele bir sayı üretir (ISN_c) ve sunucuya gönderir. Sunucu bu mesajı aldığı anda, kendisi bir sıralama numarası üretir ve bu numarayla birlikte istemciden almış olduğu sıralama numarasının onay mesajını istemciye gönderir. Bu mesajı alan istemci sunucunun sıralama numarasına onay gönderir. Sunucu cevabı aldığı anda bağlantı kurulmuş olur.

```

X → S : SYN(ISNx) , SRC = T
S → T : SYN(ISNs) , ACK(ISNx)
X → S : ACK(ISNs) , SRC = T
X → S : ACK(ISNs) , SRC = T , nasty = veri

```

Şekil 4.2 TCP sıralama numarasının çalınması

ISN_s sıralama numarası, saldırgan X tarafından tahmin edilebildiğinde, saldırgan kendi kimliğini saklayarak T konağının kimliği ile sunucuya bağlanır ve böylece T konağının kimliğini çalmış olur (Şekil 4.2). ISN_s sıralama numarası tahmin edilmesi ise, şöyle gerçekleşir: Herhangi bir sunucu ISN_s sıralama numaralarını üretirken 0' dan başlar ve her defasında daha önce üretmiş olduğu numaraya belirli bir sayı ekleyip yeni bir numara üretir. Bu artım belirli zaman aralıklarıyla gerçekleşir. Saldırgan bu zaman aralığını ve son üretilen sayıyı, ağı dinleyerek elde ettiği örnek değerlerden belirlemektedir. Buna karşı kullanılacak savunma yöntemleri, yeni sayı üretirken kullanılan artım değerinin rastgele seçilmesi veya ISN_s sıralama numaralarının üretilmesinde, kriptografik algoritmaların kullanılmasıdır. [11]

4.2.2 Kaynak yönlendirme (Source routing)

Kaynak yönlendirmede, saldırgan yerel ağdan bir ip adresi kullanarak hedef konağa bağlantı kurar ve mesaj paketleri güvenilen bir kaynaktan geliyormuş gibi, yönlendiriciye ve onun arkasındaki yerel ağa erişebilir.

Buna karşı yapılabilecek en basit savunma yöntemi, kaynak yönlendirme mevcut ise önceden doğrulanmış bağlantıların reddedilmesidir. Bu yöntem, aynı şirketin farklı yerdeki şubeleriyle olan bilgisayar bağlantılarını, internet gibi güvensiz bir ağ ortamı üzerinden yapmakta ise çözüm olmaktan çıkar. [11]

4.2.3 Bilgi yönlendirme protokolü (Routing information protokol–RIP) saldırısı

Bilgi yönlendirme protokolü (RIP), yerel ağda yönlendirme bilgilerinin iletilmesinde kullanılır. RIP protokolünün yarattığı sorun, herhangi bir saldırganın hedef konağa zararlı yönlendirme bilgileri göndererek, güvensiz konağın kendini gizlemesine olanak vermesidir. Buna karşı kullanılabilecek en basit savunma, daha önce hiç kullanılmamış olan yönlendirme bilgilerinin ağa eklenmesine izin vermemektir. Ağ iyi izleyen bir yönlendirici karşılaşılabileceği zararlı bir yönlendirme bilgisini kolayca farkedebilecektir. Diğer bir çözüm yolu ise RIP paketlerinin doğrulanmasıdır. [11]

4.2.4 ICMP saldırısı

ICMP protokolündeki saldırı bakımından odak nokta, ICMP yeniden yönlendirme (redirect) mesajıdır. Bu mesaj yönlendiriciler tarafından, en iyi yol üzerindeki konakları belirtmek için kullanılır. ICMP protokolünde de RIP protokolünde olan saldırılara benzer saldırılarla karşılaşılabılır. ICMP saldırılarının zorluğu kurulmuş bir bağlantının varlığıdır. Bu durumda konağın yönlendirme çizelgesine yasal olmayan yönlendirme bilgileri eklemek mümkün değildir. Varolan bir bağlantı için yönlendirme değişikliklerini kabul etmeyerek, bu saldırı tipine karşı bir savunma sağlanabilir. Fakat bu bağlantıda başarımlı düşüklüğüne yol açabilir. [11]

4.2.5 Kimlik doğrulama sunucusu

İstemcinin kimliğini öğrenmek isteyen sunucu, istemci konağın kimlik doğrulama sunucusu ile bağlantı kurar ve belirli bir bağlantıya ait kullanıcı ile ilgili bilgiler alır. Sunucu ile istemci konağın kimlik doğrulama sunucusu arasındaki bu haberleşme saldırganların tehditi altındadır. En başta, tüm konaklar kimlik doğrulama sunucusu kullanmamaktadırlar. Ayrıca, istemci konak güvenli değilse, kullanıcının kim olduğunun kanıtlanmasının hiç bir anlamı olmayacaktır. Kimlik doğrulama sunucusu, yönlendirme çizelge ve TCP sıralama numarası tahmini saldırılarına maruz kalabilir.

4.2.6 Posta ofisi protokolü (Post office protocol-POP)

Bu protokolde kimlik doğrulama, hem kullanıcı adı hem de şifresini içeren tek bir komutla gerçekleştirilmektedir. Bunun doğurduğu güvenlik açığı tek bir metin ele geçirildiğinde kullanıcının kimliği çalınmış olmaktadır. Buna çözüm olarak tek zamanlı şifreler kullanılmalıdır.

4.2.7 Alan isimlendirme sistemi (Domain name system-DNS)

DNS' in TCP sıralama numarası tahmini saldırısına uğraması ihtimal dahilindedir. Hedef kullanıcı, kendi DNS sunucusundan bağlantı kurmak istediği uzak makinenin ip adresi için DNS sorgulaması yaptığında, saldırgan araya girerek, bir DNS cevabı üreterek hedef kullanıcıya gönderebilir. Bu saldırının gerçekleşmesi için istemci çözümleyicisinin UDP kapısının ve sorgulama için kullanılan DNS sıralama numarasının bilinmesi gerekir. [12]

4.3 Bilinen Güvenlik Gedikleri

Bilinen önemli 14 güvenlik gediği aşağıda listelenmiştir: [13]

- Yetersiz yönlendirici erişim kontrolü: Yanlış yapılandırılmış yönlendirici erişim listeleri, ICMP, IP ve NETBIOS protokollerinde bilgi kaçağına neden olur ve DMZ bölgesindeki hizmetlere yetkisiz erişim ile sonuçlanır.
- Bu bilgi kaçağı saldırganlara işletim sistemi ve uygulama sürümleri, kullanıcı grupları, ağ paylaşımları, alan iletimi ile DNS bilgileri ve, SNMP, finger, SMTP, telnet, rusers, sunrpc, NETBIOS gibi çalışan hizmetler ile ilgili bilgiler verir.
- İzlenmeyen ve güvenli olmayan uzaktan erişim noktaları kurumsal ağlara en kolay erişim şeklini sağlar.
- Gereksiz hizmetler (sunrpc, FTP, DNS, SMTP) çalıştıran konaklar, sisteme sızılacak yolları açık bırakırlar.
- İş istasyonu seviyesinde, zayıf, kolayca tahmin edilebilen ve tekrar kullanılan şifreler, sunuculara erişim yollarını açarlar.
- Gereğinden fazla imtiyazlara sahip kullanıcı ve deneme hesapları sistem üzerinde tehlike oluştururlar.
- Yanlış yapılandırılmış internet sunucuları, özellikle web sunucuları üzerinde CGI kod parçaları ve isimsiz FTP erişimine izin veren sunucular sistem güvenliğini tehlikeye sokarlar.

- Yanlış yapılandırılmış firewall ve yönlendirici erişim kontrol listeleri, iç sistemlere doğrudan erişime izin verirler.
- Güncel olmayan, güvenlik gedikleri bulunan veya yanlış yapılandırılmış yazılımlar sistem güvenliğini tehlikeye sokar.
- Aşırı dosya ve izin erişim kontrolleri (NT/95 paylaşımları, UNIX NFS ihraçları) sistem güvenliğinde tehlike oluştururlar.
- NT alan güveni gibi aşırı güven ilişkileri, UNIX “.rhosts” ve “hosts.equiv” dosyaları saldırganlara, hassas sistemlere yetkisiz erişim hakkı sağlayabilir.
- “X Windows” gibi doğrulanmamış hizmetler sistem üzerinde güvenlik tehlikesi oluştururlar.
- Ağ ve konak seviyesinde, yetersiz kayıt tutma, izleme ve sezme yetenekleri, güvenlik gediği oluştururlar.
- Kabul edilebilir ve yeterli güvenlik politikaları, yordamları ve kılavuzları eksikliği sistem güvenliğini tehlikeye sokar.

5 KRİPTOGRAFİK KAVRAMLAR VE TEKNOLOJİLER

5.1 Giriş

İnternet altyapısında bilginin bir düğümden diğer düğümlere iletimi, bir dizi düğümler üzerinden TCP/IP protokol kümesi sayesinde gerçekleşir. TCP/IP protokol kümesinin sahip olduğu esnek yapı, kendisini internet ve yerel ağ üzerinde bilgilerin iletiminde dünyaca kabul edilmiş bir standart haline getirmiştir. TCP/IP’ de iletilen bilgilerin varış noktasına erişene kadar birçok ara düğümlerden geçmesi, iletişim ile ilgisi olmayan varlıkların iletişime karışmasına imkan vermektedir. İstenmeyen varlıkların iletişime karışması aşağıdaki biçimlerde gerçekleşebilir:

- Gözetlemek (Eavesdropping): İletişimin, iletilen bilgiler üzerinde herhangi bir değişiklik yapılmadan izlenmesi ve kaydedilmesidir. Kişiye ait kredi kartı numarasının öğrenilmesi veya gizli bir konuşmanın kaydedilmesi örnek olarak verilebilir.
- Kurcalamak (Tampering): İletilen bilgiler üzerinde, istenmeyen kişilerce değişiklik yapılarak alıcıya gönderilmesidir. Kullanıcının bir ürün almak üzere verdiği siparişin değiştirilmesi veya kişiye ait özgeçmişin değiştirilmesi örnek olarak gösterilebilir.
- Taklit Etmek (Impersonation): Bilginin kendini alıcının kimliği ile tanıtan kişiye gönderilmesi durumudur. İki biçimde karşılaşılır:
 1. Taklit Etmek (Spoofing): Bir kişinin kendini başka birinin kimliği ile tanıttırmasıdır. Elektronik posta adresi osmank@hotmail.com olan birinin kendini, erogluebru@hotmail.com olarak tanıttırması örnek olarak verilebilir.
 2. Yanlış Tanıtmak (Misrepresentation): Bir kişi veya kurumun kendini olduğundan farklı olarak tanıttırmasıdır. Adresi https://esnet.esbank.com.tr olan internet bankacılık sitesinin, kendini gerçek zamanlı araba satış sitesi olarak tanıttırması örnek olarak verilebilir.

İnternet üzerinden iletişimi gerçekleşen bilgilerin güvenilirliği, açık anahtar kriptografi olarak adlandırılan tekniklerce sağlanır. Açık anahtar kriptografinin gerçekleştirdiği faaliyetler aşağıdadır: [14]

- **Şifreleme ve Deşifreleme:** Güvensiz bir ortamda birbirleriyle konuşan iki tarafın bilgiye sadece kendilerinin anlayacağı bir biçim vermesi tekniğidir. Gönderilmeden önce gönderici tarafından şifrelenen veri, alıcı tarafından açılır ve veri elde edilir. İletilen verinin şifreli olması saldırganın veriye erişimini engeller.
- **Kurcalama Sezme:** İletişim sırasında veri üzerinde gerçekleştirilecek olası değişikliklerin sezilmesinde kullanılan tekniklerdir.
- **Kimlik Doğrulama:** Bilginin alıcısına, bilginin kaynağının ve göndericinin kimliğinin doğrulanması imkanını verir.
- **İnkâr Edememe (Nonrepudiation):** Bilginin göndericisinin sonradan, gönderdiği bilgiyi inkâr etmesini engeller.

5.2 Şifreleme ve Deşifreleme

Şifreleme, bilginin alıcı haricindeki kimse tarafından anlaşılmayacak bir şekile çevrilmesidir. Deşifreleme ise, özel bir anahtar yardımıyla anlamsız bilgiye, şifrelenmeden önceki anlamlı halinin geri verilmesidir. Şifreleme ve deşifreleme kriptografi algoritması olarak adlandırılan matematiksel işlevlerce gerçekleştirilir. Şifreleme yönteminin kuvveti algoritmanın bilinmezliği ile değil, kullanılan anahtarın uzunluğu ile ilgilidir. Şifrelenen veri anahtar kullanımı ile rahatlıkla açılmakta iken, anahtarın bilinmemesi durumunda verinin elde edilmesi matematiksel işlemlerin yoğunluğu açısından imkansızdır.

5.2.1 İşlem biçimleri

Şifreleme ve deşifrelemede en çok kullanılan şifreleyici biçimi, genellikle 64 bitlik uzunlukta olan sabit uzunluklu parçaların, yine olası 64 bitlik uzunlukta sabit uzunluklu parçalara, bir anahtar ve işlev kullanımı ile çeviren parça şifreleyicileridir. Giriş ve çıkış parçalarının tümünün anahtar uzunluğu n bit ise, parça şifreleyici, n bit tamsayılardan , n bit tamsayaların permütasyonlarına bire bir bir ilişkilendirme tanımlar.

Verinin aynı parçası, aynı anahtar ile üst üste iki kez şifrelendiğinde oluşan şifreli metin parçalarının da birbirine eşit olması durumuna Elektronik Kod Kitabı (Electronic Codebook – ECB) denir. Bu bilgi, sisteme saldırıda bulunma amacını güden kişiler için, çok önemli bilgidir. Aynı içerikli parçaların farklı şifreli metinlere dönüşmesini sağlamak için, iki farklı işlem biçimi kullanılır:

- Şifreleyici parça zincirlemesi (cipher block chaining – CBC): Şifreleyici parça zincirlemesinde şifreli metin, açık metin parçalarının, daha önceki şifreli parça ile XOR işlemine tabi tutulduktan sonra şifrlenmesi ile elde edilir.
- Şifreleyici geri beslemesi (cipher feedback - CFB): Bu yöntemde k' nıncı şifreli parça, (k-1)' inci şifreli metnin şifrlenip, k' nıncı açık metin parçası ile XOR işlemine tabi tutulması sonucunda elde edilir.

Diğer bir şifreleyici biçimi ise, akış şifreleyicileridir. Akış şifreleyicileri her geçişte bit bitlik bilgi çıktısı veren bir durum makinesi içerirler. Bu çıktı bitleri genel olarak koşan anahtar (running key) olarak adlandırılırlar. Şifreleme işlemi bu koşan anahtarların, açık metin ile şifrlenmesi ile gerçekleştirilir. [15]

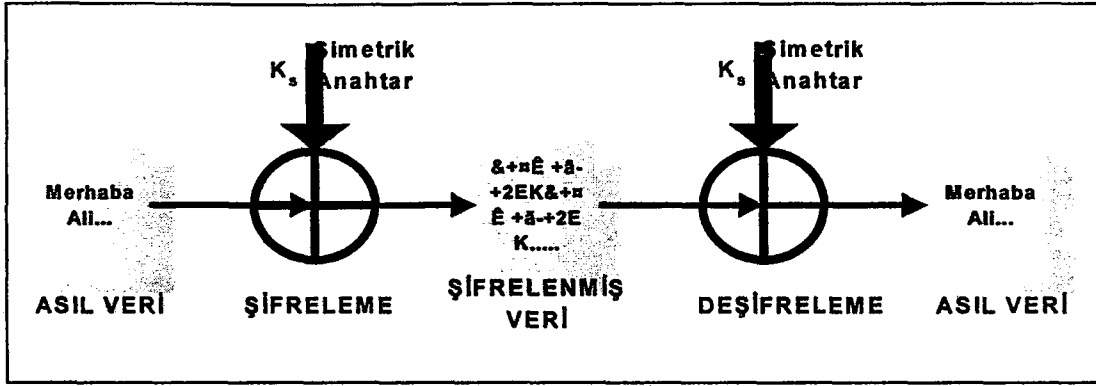
5.2.2 İlkel şifreleme algoritmaları

- Ceasar şifresi: Mesaj içerisindeki bir harfin, kendisinden 3 harf sonra gelen harf ile değiştirilmesidir.
- Monoalfabetik şifre: Bir harfin, rastgele seçilmiş diğer bir harf ile değiştirilmesidir.
- Eşit oyun (playfair) şifresi: Bir anahtar kelime seçilir ve 5X5' lik bir matrise soldan sağa ve aşağıdan yukarıya olmak üzere ve aynı harfleri sadece bir kez kullanmak kaydıyla yerleştirilir. Matrisin boş kalan diğer kısımleri, alfabenin diğer harfleri ile doldurulur. Açık metin aynı anda 2 harf olarak şifrlenir ve aynı metin içinde tekrar eden aynı harfler, "X" gibi bir ayraç tarafından ayrılır. Matrisin aynı satırını düşen harfler sağındaki harfler ile değiş tokuş edilirken, aynı sütununa düşen harfler aşağısındaki ile değiş tokuş edilir.
- Yer Değiştirme (Transposition) Şifresi: Açık metin harflerinin özel bir sıra ile yazılıp, diğer bir sıra ile okunmasından ibarettir.

5.2.3 Simetrik anahtarlı şifreleme

Şifreleme anahtarının, deşifreleme anahtarından elde edilebildiği şifreleme yöntemidir. Çoğu simetrik algoritmalarda, Şekil 5.1' de görüldüğü gibi şifreleme ve deşifreleme anahtarları aynıdır.

Simetrik anahtarlı şifreleme, verinin şifrlenmesinde ve deşifrlenmesinde herhangi bir gecikmeye neden olmaz. Simetrik anahtarlı şifrelemede bir anahtar ile şifrelenen veri diğer bir anahtarla açılmadığından, anahtarın gizli tutulması durumunda bir derece kimlik doğrulama sağlanır.



Şekil 5.1 Simetrik anahtarlı şifreleme

Simetrik anahtarlı şifrelemede, simetrik anahtarın gizli tutulması vazgeçilmez şarttır. Simetrik anahtarın gizli tutulmadığı durumlarda, hem verinin güvenilirliği, hem de kimlik doğrulama ölçütleri tehlikeye girer. Başkasına ait bir simetrik anahtar saldırganın hem kişiye ait gizli bilgilere erişmesini, hem de anahtar sahibinin kimliğiyle başkalarına veri göndermesini sağlar. [14]

Simetrik anahtarlı şifreleme algoritmaları

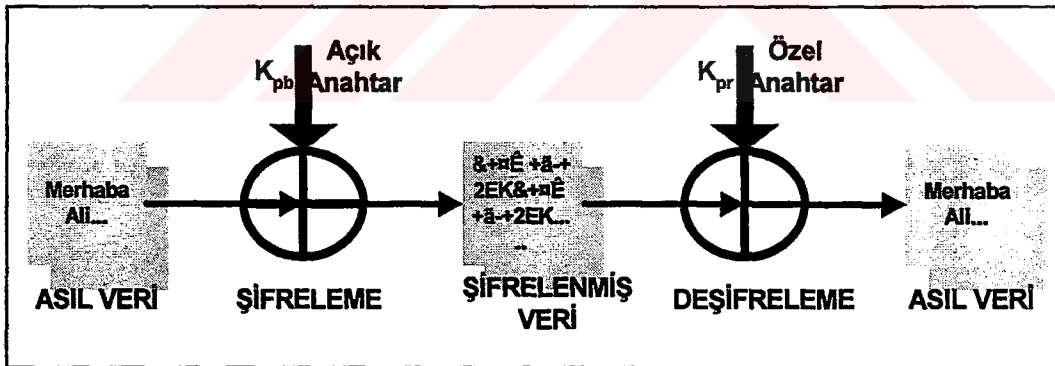
- Veri Şifreleme Standardı (Data Encryption Standard – DES) : Milli Standardlar Bürosu (National Bureau of Standards) tarafından yayınlanmış DES algoritmasının aşamaları aşağıda sıralanmıştır. [16]
 1. Mesajı 64 bitlik parçalara bölünüz.
 2. Bu bölmeleri bir başlangıç permütasyonundan geçiriniz.
 3. 56 bitlik anahtarı kullanarak, 16 adet 48 bitlik anahtar elde ediniz.
 - a) 56 bitlik anahtar üzerinde permütasyon gerçekleştirerek, 2 adet 28 bitlik anahtar elde ediniz.
 - b) Her iki bölmeyi, 1, 2, 9 ve 16. aşamalarda sola doğru bir, diğer aşamalarda 2 bit döndürme (rotate) işlemine tabi tutunuz.
 - c) Herbir bölmeyi ayrı ayrı permütasyondan geçirip, birinci anahtarın 9, 18, 22 ve 25' inci, ikinci anahtarın 35, 38, 43 ve 54' üncü bitlerini eleyiniz ve 48 bitlik anahtarı elde ediniz.
 4. DES aşamalarını gerçekleştirmek üzere, 16 adet 48 bitlik anahtarın herbirini kullanınız.
 - a) 64 bitlik giriş değerini 32 bitlik iki parçaya bölünüz.
 - b) DES aşamasına giriş değerinin sağ tarafı, aşama çıkış değerinin sol tarafı olur.

- c) Aşamaya giriş değerinin sağ tarafına parçalayıcı işlevi, aşamaya ait anahtarla uygulanır.
 - d) Parçalayıcı işlevin sonucu, aşamaya giren değer sol tarafı ile aşamadan çıkan değer sağ tarafının XOR işleminden geçirilmesidir.
5. Dördüncü aşamayı 16 kez tekrar ediniz.
 6. Sonucun sol ve sağ parçalarını yer değiştiriniz.
 7. Son permütasyonu gerçekleştirin.
- Üçlü (Triple) DES Algoritması: Üç anahtar kullanarak, DES algoritmasının üç kez çalıştırılmasını içeren üçlü DES algoritması, anahtar 1, anahtar 2, anahtar 3 olarak adlandırılan, üç adet 56 bitlik bölmelere ayrılan 168 bitlik anahtar kullanır. Bu algoritmanın aşamaları aşağıdadır:
 1. Açık metni, anahtar 1' i kullanarak şifreleyiniz.
 2. Birinci aşamada elde edilen şifrelenmiş metni, anahtar 2 ile deşifreleyiniz.
 3. İkinci aşama sonucunda elde edilen metni, anahtar 3 ile şifreleyiniz.
 - Uluslararası Veri Şifreleme Algoritması (International Data Encryption Algorithm – IDEA) : İsviçre' de, ETH Zurich' de, Xuejia Lai tarafından geliştirilen IDEA, 128 bitlik anahtar kullanarak, 64 bitlik açık metni 64 bitlik şifreli parçalar halinde şifreleyen bir algoritmadır. Feistel yapısının ilkel bir genelleştirilmesini temel alan IDEA, bir çıkış çevrimi tarafından takip edilen, hesapsal olarak birbirinin aynı 8 aşama içerir.
- Uzun zamandır bilinen IDEA algoritması, uzun zamandır üzerinde incelemeler yapılmasına karşın herhangi bir saldırı teşebbüsüne maruz kalmamıştır. Biham, Shamir ve Biryukov tarafından IDEA' ya gerçekleştirilen saldırı teşebbüsü, algoritmanın ancak dördüncü seviyesine kadar ulaşmış, algoritmanın 8 aşamalı toplam bölümü yine güvenli olarak kalmıştır. [15] Amerika ve birçok Avrupa ülkesinde patentlenmiş olan IDEA algoritmasının kabaca aşamaları aşağıdadır:
1. Şifrelenecek mesajı 64 bitlik parçalara bölünüz. Herbir açık metin parçası, şifreli parça haline dönüşecektir.
 2. 64 bitlik parçaları, 16 bitlik 4 bloğa ayırınız.
 3. 52 adet 16 bitlik anahtar oluşturmak üzere, 128 bitlik bir anahtar kullanınız.

4. Tek sayılı aşamalarda dörtlü, çift aşamalarda ikili kümelerde anahtar kullanarak 17 aşama gerçekleştiriniz.
 5. 16 bitlik blokları, 64 bitlik şifreli bloklar olarak birleştiriniz.
- RC4: RSA Veri Güvenlik Firması ve Ron Rivest tarafından geliştirilen RC4 algoritması, biri kaynak kodunu haber gruplarına postalayana kadar ticaret sırrı olarak kullanılmaktaydı. Çalışma hızının çok yüksek olması güvenlik seviyesinin bilinmemesine rağmen bazı hız gerektiren uygulamalarda RC+ algoritmasının kullanımını uygun kılmıştır. İstenildiği kadar anahtar uzunluğu kabul eden RC4 aslında, bir pseudo rastgele sayı üreticisi ve bu sayı üreticisinin çıktısının, şifrelenecek veri ile XOR işlemine tabi tutulmasından ibarettir. Bu nedenle, aynı anahtar iki farklı veri kümesini şifrelemede kullanılmamalıdır.

5.2.4 Açık anahtarlı şifreleme

Açık anahtarlı şifreleme de biri açık anahtar, diğeri özel anahtar olarak adlandırılan bir anahtar çifti kullanılır. Bu anahtar çifti verinin imzalanması, şifrenmesi ve kimlik doğrulamada kullanılır. Şifreleme yönteminde açık anahtar herkese dağıtılırken, özel anahtar, sadece anahtar sahibi tarafından bilinir. Açık anahtar ile şifrelenen veri sadece özel anahtar ile açılırken, özel anahtar ile şifrelenen veri ise, sadece açık anahtar ile açılabilir. [14]



Şekil 5.2 Açık anahtarlı şifreleme

Şekil 5.2' den de görüldüğü gibi gönderici veriyi, alıcının açık anahtarı ile şifreler ve alıcıya gönderir. Alıcı şifrelenmiş veriyi özel anahtarı ile açar.

Açık anahtarlı şifreleme, simetrik anahtarlı şifrelemeye göre daha fazla matematiksel işlem gerektirir. Bu nedenle büyük uzunluklu verilerin şifrenmesinde kullanılması uygun değildir. Bu tarz veri boyutlarında açık anahtarlı şifreleme ve simetrik anahtarlı şifreleme birlikte kullanılmalıdır. Çoğunlukla karşılaşılan yöntem, simetrik

anahtarın deęiřiminde açık anahtarlı řifrelemenin kullanılması, verinin deęiřiminde ise simetrik anahtarlı řifrelemenin kullanılmasıdır.

Açık anahtarlı řifreleme kimlik doęrulamada da kullanılmaktadır. Kimlięi doęrulanacak olan gönderici, özel anahtarı ile veriyi řifreler. Özel anahtar ile řifrelenen veri sadece açık anahtar ile açılabildeęi için, göndericinin kimlięi doęrulanır.

RSA Algoritması

1977 yılında R. Rivest, A. Shamir and L. Adleman tarafından bulunmuřtur. Şifreleme ve deřifreleme iřlemlerinin her ikisinde de kullanılan RSA algoritmasında, ilk önce řifreleme ve deřifrelemede kullanılacak açık ve gizli anahtar çiftinin oluřturulması gereklidir. RSA algoritmasının ařamaları ařaęıda gösterilmiřtir:

1. Tipik olarak 10000' den daha büyük p ve q gibi iki büyük asal sayı seęiniz.
2. $n = p * q$ ve $z = (p - 1) * (q - 1)$ iřlemlerini geręekleřtiriniz.
3. z sayısına göre, aralarında asal bir d sayısı belirleyiniz.
4. $e * d = 1 \text{ mod } z$ olacak řekilde, bir e sayısı belirleyiniz.
5. Şifrelenecek metini $2k < n$ olacak k bit uzunluklu bloklara ayırınız ve her bir bloęu P olarak adlandırınız.
6. P mesajını řifrelemek için, $C = P^e \text{ (mod } n)$ iřlemini geręekleřtiriniz.
7. Mesajı deřifrelemek için ise, $P = C^d \text{ (mod } n)$ iřlemini geręekleřtiriniz.

RSA algoritmasının iřlem ařamaları ve sonuęları Tablo 5.1' de gösterilmektedir. Tablo 5.1' deki RSA algoritması örneęinde, $p=3$, $q=11$, $n=33$, $z=20$, $d=7$ olarak alınmıřtır. [16]

5.2.5 Anahtar uzunluęu ve řifreleme kuvveti

Şifreleme yönteminin kuvveti anahtarın bulunması ile ilgilidir. RSA algoritmasında anahtarın bulunması, çok büyük basamaklı sayıların çarpanlara ayrılması iřlemidir. Şifreleme yönteminin kuvveti anahtarın uzunluęu ile doęru orantılıdır. Örneęin 128 bitlik RC4 algoritması, 40 bitlik RC4 algoritmasından daha kuvvetlidir. Kabaca 128 bitlik RC4 algoritması, 40 bitlik RC4 algoritmasından $3*10^{26}$ kat daha kuvvetlidir. Buna ek olarak, farklı řifreleme yöntemleri, aynı řifreleme kuvvetini saęlamak için farklı uzunlukta anahtar uzunlukları gerektirebilir.

Tablo 5.1 RSA Algoritması ile şifreleme ve deşifreleme

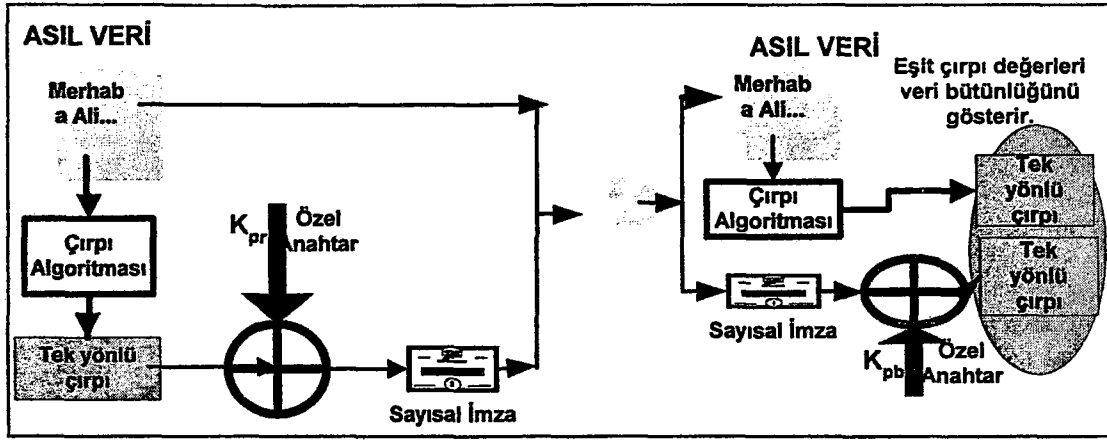
Açık Metin (P)		P^3	Şifreli Metin(C)	C^7	Deşifreleme işleminden sonra	
Sembolik	Sayısal		$P3(mod33)$		$C7(mod33)$	Sembolik
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	1	1	1	1	1	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	5	125	26	8031810176	5	E

5.3 Sayısal İmzalar

Şifreleme ve deşifreleme teknikleri verinin internet üzerinde iletiminde karşılaşılan sorunlardan sadece gözetlemeyi engellemektedir. Sayısal imzalar ise, kurcalama ve taklit etme sorunlarına çözüm getirmektedir.

Kurcalama sezme ve kimlik doğrulama teknikleri tek yönlü çırpma (one-way hash) olarak adlandırılan bir matematik işlevine bağlıdır. Tek yönlü çırpma işlevinin özellikleri aşağıdadır:

- Veriden elde edilen çırpı değeri tektir. Veride yapılan bir bitlik değişiklik çırpı değerini de değiştirir.
- Çırpı değerinden, çırpılan veri elde edilemez. Bu nedenle çırpma işlevi tek yönlü işlev olarak adlandırılmıştır.
- Sayısal imza, veriye tek yönlü çırpı işlevi uygulanarak elde edilen çırpı değerinin, kullanıcının özel anahtarı ile şifrelenmesi ile elde edilir.
- Şekil 5.3' den de görüldüğü gibi, veri tek yönlü çırpı işlevinden geçirilerek tek yönlü çırpı değeri elde edilir. Elde edilen çırpı değeri özel anahtar ile şifrelenir ve sayısal imza elde edilir. Elde edilen sayısal imza veri ile birlikte alıcıya gönderilir. Alıcı sayısal imzayı göndericinin açık anahtarı ile açar



Şekil 5.3 Veri bütünlüğünün sağlanmasında sayısal imza kullanımı

ve gönderici tarafından hesaplanmış tek yönlü çırpı değerini elde eder. Daha sonra elindeki veriden tek yönlü çırpı değerini hesaplar ve diğer çırpı değeri ile karşılaştırır. İki değerin eşitliği durumunda göndericinin kimliği doğrulanır.

5.3.1 Çırpma Algoritmaları

Geniş olarak kullanımda olan iki çırpı işlevi, MD5 ve güvenli çırpı algoritması (secure hash algorithm – SHA)'dır. MD5, Ron Rivest tarafından tasarlanmıştır. Güvenli çırpı algoritması, MD5 algoritmasından esinlenilerek, Milli Standartlar Enstitüsü (National Institute of Standards) ve Milli Güvenlik Acentası (National Security Agency) tarafından Sayısal İmzalama Standardı (Digital Signature Standard - DSS) ile birlikte kullanılmak amacıyla tasarlanmıştır.

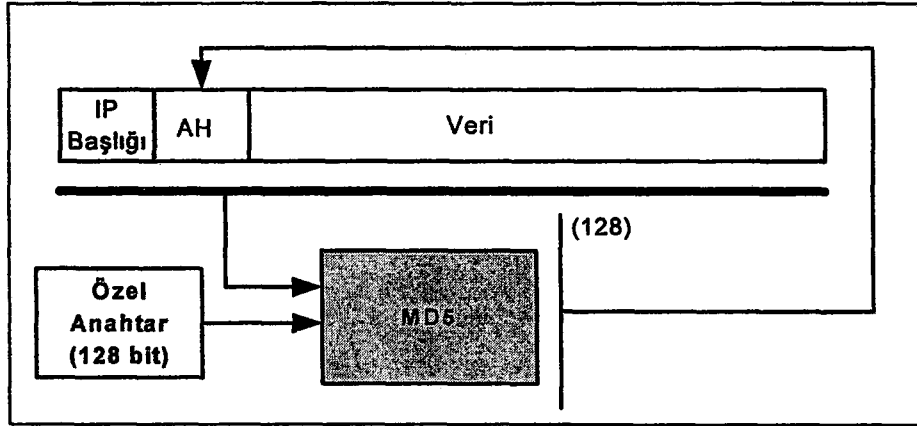
- MD5 ve Güvenli Çırpı Algoritması (Secure Hash Algorithm – SHA): MD5 ve güvenli çırpı algoritmasında 128 bitlik gizli anahtar ve veri birimi çırpı algoritmasına giriş değeri olarak girer. Algoritma sonucunda oluşan çıktı değeri, veri birimi başlığının kimlik doğrulama sahası (AH)'na yerleştirilir. Algoritmanın şekilsel gösterimi Şekil 5.4'te bulunmaktadır.

Güvenli çırpı algoritmasının MD5'den tek farkı, oluşan çırpı değerinin 160 bit olmasıdır.

- Çırpılmış Mesaj Doğrulama Kodu (Hashed Message Authentication Code – HMAC) MD5 ve SHA Algoritmaları: IBM tarafından sunulmuş güçlü bir çırpı değeri oluşturma yöntemidir. Çırpılmış mesaj doğrulama kodu kendi kendine bir çırpı işlevi olmaktan ziyade, mesaj doğrulama kodu hesaplaması için özel bir çırpı işlevi kullanan güçlü bir kriptografi yöntemidir. Örnek olarak MD5 algoritmasının kullanıldığı düşünüldüğünde, HMAC temel çırpı işlevinin üst üste iki kez uygulanmasından ibarettir. İlk seferde veri birimi ve anahtar, çırpı işlevine giriş değerleri olurken, ikinci seferde, birinci çırpı işlevinin çıktısı ve

anahtar deęerleri giriř deęeri olmaktadır. Sonu olarak oluřan 128 bitlik ırpı deęerinin ilk 96 biti MAC deęeri olarak kullanılır. Algoritmanın řekilsel gsterimi, řekil 5.5' te yer almaktadır. [16]

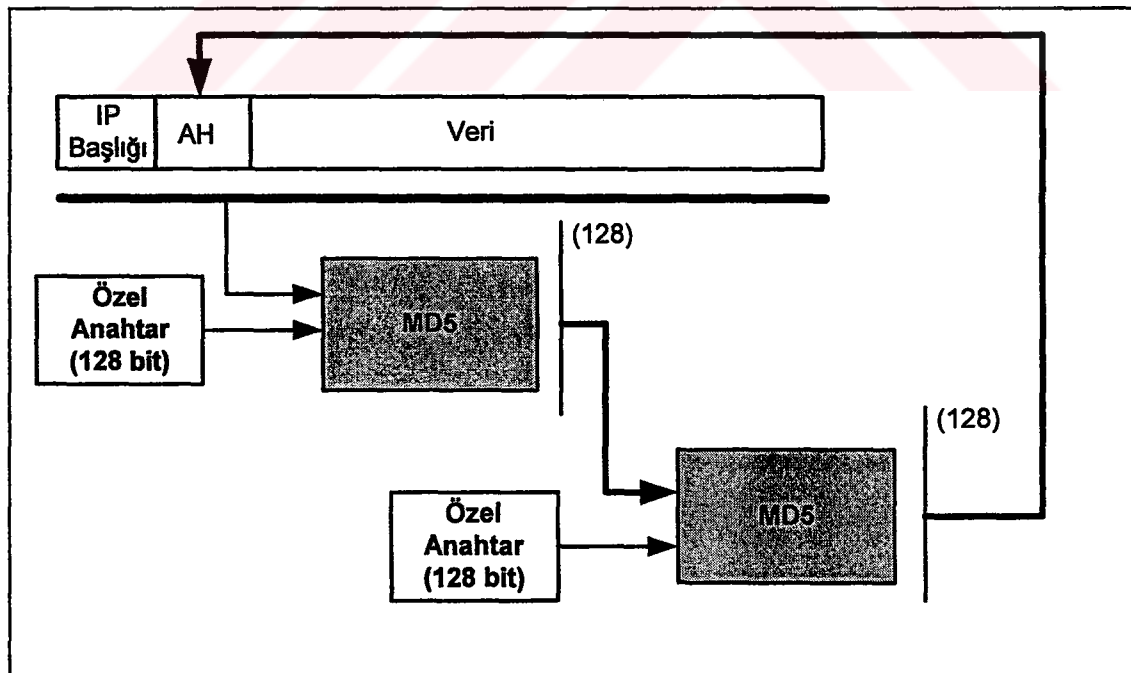
SHA iin oluřan tek deęiřiklik ise, oluřan ara deęerlerin 160 bit uzunlukta olmasdır.



řekil 5.4 MD5 ve gvenli ırpı algoritması

5.3.2 Sayısal imza standardı

- Gizli anahtar ile řifrelenmiř ırpı deęeri sayısal imza olarak adlandırılır. NIST ve NSA tarafından Amerika' nın sayısal kimlik doęrulama standardı olarak seilen, sayısal imza standardının ierięi ařaęıda gsterilmektedir: [16]



řekil 5.5 ırpılmıř mesaj doęrulama kodu MD5 ve SHA Algoritmaları

1. Uzunluğu genellikle 512 ve 1024 bit arasında olan, büyük bir p asal sayısı seçilir.
2. (p-1) sayısının 160 bit uzunluğunda olacak bir q çarpanını bulunur.
3. $h^{(p-1)/q} > 1$ eşitliği doğru ve h, (p-1) sayısından küçük iken,

$$g = h^{(p-1)/q} \text{ mod } p,$$
eşitliği hesaplanır.
4. Göndericinin özel anahtar olarak q' dan, küçük diğer bir x sayısı seçer.
5. $y = g^x \text{ mod } p,$
eşitliğini hesaplanır ve göndericinin açık anahtarı olarak kullanılır. (x,y) oturumdan oturuma değişmeyen, uzun ömürlü bir anahtar çiftidir.
6. Gönderici aşağıdaki işlemleri yaparak mesajı imzalar:
 - a) q' dan küçük bir rastgele k sayısı üretir.
 - b) $r = (g^k \text{ mod } p) \text{ mod } q,$
 $s = (k^{-1} (\text{SHA1}(m) + xr)) \text{ mod } q,$
eşitlikleri hesaplanır. (k,r) anahtar çifti oturum boyunca geçerli bir anahtar çiftidir. Her bir oturum için yeniden oluşturulur. Sayısal imza (r,s) anahtar çifti ile gösterilir.
 - c) Gönderici (m,r,s) sayılarını gönderir.
 - d) Alıcı imzayı şu şekilde onaylar:
 - I. $w = s^{-1} \text{ mod } q,$
 $u_1 = (\text{SHA1}(m)/w) \text{ mod } q,$
 $u_2 = (rw) \text{ mod } q,$
 $v = ((g^{u_1} y^{u_2}) \text{ mod } p) \text{ mod } q,$
eşitlikleri hesaplanır.
 - II. Eğer $v=r$, gerektirmesi doğru ise imza onaylanır.

5.4 Sertifika ve Kimlik Doğrulama

Sertifika bir kişinin, sunucunun, firmanın kimliğinin tanımlanması ve bir açık anahtarın bu kimlikle ilişkilendirilmesinde kullanılan elektronik belgedir. Sürücü belgesi, pasaport veya nüfus cüzdanı gibi belgeler kullanıcının kimliğini kanıtlamak

için kullanılan belgelerdir. Açık anahtarlı şifreleme taklit etme sorununu çözümlmek üzere sertifikaları kullanır.

Sürücü belgesi almak için, kimliğinizi, taşıt sürme yeteneklerinizi ve diğer bilgileri belgeleyecek Emniyet Müdürlüğü' ne, öğrenci numarası almak üzere, okul parasını ödeyip ödemediğiniz, okulun öğrencisi olup olmadığınız gibi bilgileri kontrol edecek okula başvurmanız gereklidir. Sertifika alma işleminde de benzer süreçler yaşanır. Sertifika makamları sertifika dağıtan ve kimlik doğrulayan kurumlardır. Makamlar bağımsız (third party) bir kurum olabildikleri gibi, kurumlarda kendi çalışanlarına ve müşterilerine Netscape sertifika sunucusu gibi bir yazılım kullanarak sertifika makamı olabilmektedirler. Her kurumun farklı politikaları olduğu gibi, sertifika makamları da, sertifika verme işleminde birbirlerinden farklı doğrulama yöntemleri kullanabilirler. Genel olarak sertifika makamları, sertifika dağıtırken önceden yayınlamış oldukları doğrulama yöntemlerini kullanırlar.

Sertifika makamı tarafından verilen sertifikanın, açık anahtar sunucu veya çalışanın ismi gibi nesnenin ismiyle ilişkilendirilir. Bu sayede sertifikalar, taklit etmeyi engeller. Sertifika ile ilişkilendirilen açık anahtar, sadece kendisine karşılık gelen özel anahtar ile çalışır.

Sertifika açık anahtarın yanında, nesneyi tanıtan isim, geçerlilik süresi, sertifikayı veren makamın ismi, seri numarası ve benzeri bilgileri içerir. Sertifikanın içerdiği en önemli bilgi sertifika makamının sayısal imzasıdır.

5.4.1 Kimlik doğrulama

Kimlik doğrulama, bilgisayar ağları üzerinde iki tarafın birbirlerinin kimliklerini doğrulamasıdır. Bilgisayar ağlarında iletişim, istemci ile sunucu arasında gerçekleşir. İstemci kimlik doğrulama, istemcinin kimliğinin sunucu tarafından doğrulanması olarak tanımlanırken, sunucu kimlik doğrulama ise, sunucunun kimliğinin istemci tarafından doğrulanmasıdır.

Sertifikalar, istemci ve sunucu kimlik doğrulama dışında, elektronik posta mesajında kullanıcının kimliğini, "activex" ve "java applet" programlarının güvenilirliğini kanıtlamak üzere kullanılırlar.

İki tip istemci doğrulaması vardır:

- **Şifre temelli kimlik doğrulama:** Bu kimlik doğrulama yönteminde sunucu isim ve şifrelerden oluşan bir veritabanı tutar. İstemcinin girmiş olduğu isim ve şifre, veritabanındaki bilgilerle karşılaştırılarak kimlik doğrulama işlemi gerçekleştirilir. Kimlik doğrulama istemcinin girmiş olduğu isim ve şifre

çiftinin, sunucunun veritabanındaki çiftle aynı olduğu durumda başarıyla sonuçlanır. Tüm sunucu yazılımları şifre temelli kimlik doğrulamayı destekler.

- Sertifika temelli kimlik doğrulama: Sertifika temelli kimlik doğrulama, SSL protokolünün bir parçasıdır. İstemci rastgele üretilmiş veriyi, sayısal imzası ile imzalar ve sertifikası ile birlikte sunucuya gönderir. Sunucu açık anahtarlı kriptografi tekniklerini kullanarak sayısal imzayı doğrular ve sertifikanın geçerliliğini onaylar.

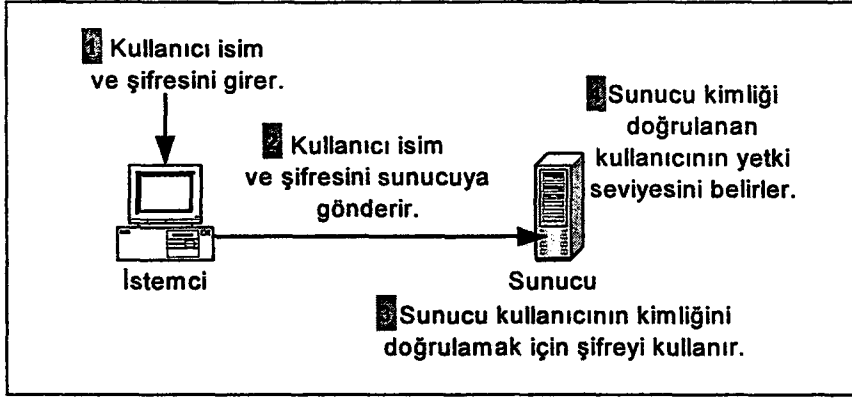
Şifre temelli kimlik doğrulama

Şifre temelli kimlik doğrulamada yer alan aşamalar Şekil 5.6' da gösterilmiştir. Şekil 5.6 şu varsayımları yapmaktadır:

- SSL ile kimlik doğrulama gerçekleşmiş olsun veya olmasın, kullanıcı sunucuya güvenmektedir.
- Kullanıcı sunucu tarafından denetlenen kaynaklara istekte bulunmaktadır.
- Sunucu kullanıcıya, istekte bulunduğu kaynağı kullanma izni vermeden istemcinin kimliğini doğrulamak istemektedir.

Şekil 5.6' da gösterilen aşamaların açıklaması aşağıdadır:

- Sunucudan gelen kimlik doğrulama isteğine karşılık olarak, istemci, kullanıcının ekranında isim ve şifre isteğinde bulunan bir iletişim kutusu gösterir. Kullanıcı oturum esnasında çalışmak istediği her bir sunucu için ayrı bir isim ve şifre çifti sağlamak zorundadır.
- İstemci kullanıcı ismi ve şifre çiftini bilgisayar ağı üzerinden sunucuya gönderir.
- Sunucu istemciden almış olduğu kullanıcı ismi ve şifre çiftini, kendi yerel veritabanında sorgular ve eşleniği varsa kullanıcının kimliğini doğrulama üzere kanıt olarak kabul eder.
- Sunucu, tanınan kullanıcının istekte bulunduğu kaynağa erişim hakkı olup olmadığını erişim kontrol listelerinden belirler ve erişim hakkı varsa istemcinin erişimine izin verir.



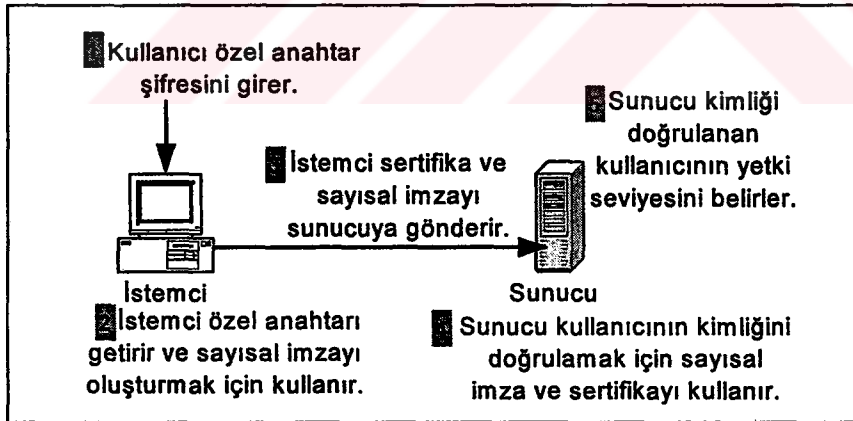
Şekil 5.6 Şifre kullanılarak istemcinin kimliğinin doğrulanması

Sertifika temelli kimlik doğrulama

Sertifika temelli kimlik doğrulamada, istemci kimlik doğrulama, sertifika ve SSL protokolünün kullanımıyla gerçekleşir. Kullanıcının sunucu tarafından doğrulanması için, istemci rastgele üretilmiş veri parçasını sayısal imzası ile imzalar ve sertifika ile birlikte sunucuya gönderir. Sunucu, sayısal imzasından kullanıcının kimliğini doğrular.

Sertifika temelli kimlik doğrulama, şifre temelli kimlik doğrulamaya, kullanıcının bildiği birşey (şifre) değil de, kullanıcının sahip olduğu birşey (özel anahtar) gerektirdiğinden tercih edilir.

Şekil 5.7' de gösterilen aşamaların açıklaması aşağıdadır:



Şekil 5.7 Sertifika kullanılarak istemcinin kimliğinin doğrulanması

- İstemci yazılımı, kullanıcıya ait açık anahtarlara karşılık gelen özel anahtarları veritabanında tutar. Bu veritabanına erişmek istendiğinde, özel anahtar için bir şifre girmek gereklidir. Aynı oturum içerisinde şifreyi bir defa girmek yeterlidir.
- İstemci özel anahtar veritabanından kullanıcı sertifikası için gizli anahtarı getirir ve rastgele üretilmiş veri parçasını sayısal imza ile imzalar. İmzalanmış veri parçası ve sayısal imza, özel anahtarın geçerlilik kanıtını

oluşturur. Bu sayısal imza, sadece bu özel anahtar ile sağlanır ve SSL oturumunda tekil olan açık anahtar ile doğrulanır.

- İstemci kullanıcı sertifikası ve imzalanmış veriyi sunucuya gönderir.
- Sunucu, sertifika ve imzalanmış veriyi kullanarak istemcinin kimliğini doğrular.
- Kimlik doğrulamadan sonra sunucu, LDAP dizininde kullanıcıyı sorgular ve kullanıcının erişim haklarına göre istemciye erişim isteğinde bulunduğu kaynağa izin verir veya reddeder.

5.4.2 Sertifikalar nasıl kullanılır?

Sertifika tipleri

- İstemci SSL sertifikaları: İstemcinin SSL protokolü ile sunucu tarafından kimliğinin doğrulanmasında kullanılır. Bankanın müşterilerine, banka sunucularının müşterileri tanımasını sağlamak ve erişim yetkilerini belirlemek üzere sertifika vermesi örnek olarak gösterilebilir.
- Sunucu SSL sertifikaları: Sunucunun kimliğini istemciye tanıtmak amaçlı olarak kullanılır. Sunucu SSL sertifikaları, istemci SSL sertifikaları ile birlikte veya olmaksızın kullanılabilir. Sunucu ile istemci arasında SSL oturumu açabilmek için, sunucu SSL sertifikası kullanımı şarttır. Örneğin, bir internet bankacılık sitesinin müşteri bilgilerinin güvenliği için, SSL ile şifrelenmiş bir oturumundan bilgi akışı, sunucu SSL sertifikası kullanımı ile sağlanabilir.
- S/MIME Sertifikaları: Elektronik postaları şifrelemek ve imzalamak için kullanılır. İstemci SSL sertifikalarında olduğu gibi, istemcinin kimliği bir insanın kimliği ile aynı özelliklere sahip olarak varsayılmıştır. S/MIME, SSL ve nesne imzalama sertifikaları , tekil bağlantı (single sign-on) çözümü oluşturmak için, tek sertifika olarak kullanılabilirler. Bir firma çalışanların kimliğinin doğrulanması, elektronik postaların şifrelenmesi ve imzalanması için tek bir sertifika kullanılması örnek olarak gösterilebilir. Bir diğer örnek S/MIME sertifikasının, sadece elektronik postaları şifrelemek ve imzalamak için kullanılmasıdır.
- Nesne imzalama sertifikaları: Java ve Javascript kodlarının veya diğer imzalanmış dosyaların imzalayıcısını tanıtır. Bir yazılım firmasının internet üzerinden dağıttığı yazılımları imzalaması örnek olarak gösterilebilir.

- **Sertifika Makamı Sertifikaları:** Sertifika makamlarının doğrulanmasında kullanılır. İstemci ve sunucu yazılımları, hangi sertifikanın güvenileceğini anlamak için sunucu sertifikalarını kullanır. Örneğin, Netscape Communicator' da saklanan sertifika otoritesi sertifikaları, tarayıcının kimliğini doğrulayabileceği sertifikaları gösterir. Sistem yöneticisi, kurumsal güvenlik politikasının bir yönünü tarayıcının kullanıcı kopyalarında saklanan sertifika makamı sertifikalarını kontrol ederek sağlar.

SSL Protokolü

Netscape tarafından geliştirilen SSL (Secure Socket Layer) protokolü, sunucu ve istemci kimlik doğrulamasını ve sunucu ile istemci arasındaki şifrelenmiş iletişimi yöneten kurallar kümesidir. SSL genel olarak internet üzerinde, kredi kartı gibi gizli bilgilerin değiş tokuşunda kullanılır.

SSL sertifikası gerektiren SSL protokolünde, el sıkışma sürecinin ilk aşaması olarak, sunucu sertifikasını kimliğini tanıtmak üzere istemciye sunar. Kimlik doğrulama sürecinde açık anahtarlı şifreleme ve sayısal imza kullanılır. Sunucunun kimlik doğrulama süreci tamamlandıktan sonra, sunucu ve istemci arasındaki bilgi değiş tokuşu daha hızlı olan simetrik anahtarlı şifreleme algoritması ile olur.

İstemci kimlik doğrulamanın gerektiği durumda, sunucu kimlik doğrulama başarıyla tamamlandıktan sonra, istemci sertifikasını sunucuya verir. İstemcinin kimliği de doğrulandıktan sonra SSL oturumu açılır.

SET Protokolü

Set protokolü, MasterCard ve VISA tarafından geliştirilmeye çalışılan GTE, IBM, Microsoft, Netscape, RSA, SAIC, Terisa ve Verisign firmalarının projeye danışmanlık ve destek verdiği açık bir protokoldür. Amaç, internet üzerinde kredi kartıyla güvenli ödeme yapabilmektir. Kullanıcının kredi kartı, alışveriş süreçleri içerisinde yer alan ikinci taraflara geçmemeli ve ödeme emrindeki diğer sipariş bilgileri, hem alıcı hem satıcı hem de aracı kurum olarak banka tarafından inkar edilemez nitelikte olmalıdır.

SET mesaj bütünlüğünü, bütün finansal bilginin doğrulanmasını ve hassas bilginin şifrelenmesini sağlar. Alıcının kredi kartı bilgileri şifrelenerek satıcıya bir sipariş emri ile gönderilir. Satıcı, alıcının şifreli kredi kartı bilgilerini, ödemenin gerçekleşmesi için alıcının bankasına gönderir. Ödemenin yapılacağı banka, kredi kartı onayını, kartı kullanıcıya veren bankadan alır ve onayı hem alıcıya hem de satıcıya bildirir. Böylelikle, kullanıcının kredi kartı bilgileri ilgili bankalar dışında satıcı veya ikinci

tarafarca açılmamış olur. Bu işlemin her adımında, ilgili taraflar kendi sayısal imzalarını ve elektronik kimlik belgelerini kullanırlar. Böylelikle, kredi kartı ile ödeme işlemi, ilgili tarafların tümü için bilgi güvenliği kuralları çerçevesinde yapılmış olur.

Burada ilgi çeken diğer önemli bir nokta, SET uygulamasını bir bölümünün internet üzerinde (alıcı-satıcı, banka-alıcı, ve/veya satıcı-banka iletişimi) bir bölümünün ise kapalı ağlar üzerinde gerçekleşmesidir (bankalar arası iletişim ve/veya satıcı-banka iletişimi). SET' in mevcut güvenlik sistemlerinden daha güçlü olmasının sebebi, alıcı ile satıcıyı bir finansal kurum ile ilişkilendiren sertifikaların varlığıdır.

SET protokolünün uygulaması bir takım alt yazılımların birleştirilmesi ile yapılır. Bunlardan ilki, internet tarayıcı cüzdanı (browser wallet) ya da elektronik cüzdandır. Tarayıcı cüzdanı, bir internet tarayıcısı ile birlikte çalışan ve kredi kartı sahibinin alışveriş yaparken kredi kartlarını ve elektronik kimlik belgelerini taşımasını sağlayan yazılımdır. Satıcıdan gelen SET mesajlarına cevap olarak, alıcıya hangi kredi kartıyla alışveriş yapmak istediğini sorar ve yukarıda tanımlı olan bütün SET protokolü işlemlerini gerçekleştirir. Öte yandan, satıcıların kullanmakta olduğu satıcı sunucusu yazılımı (merchant server), alıcı ödemelerini karşılar, satıcının iş yaptığı veya anlaşmalı bankası ile iletişime geçer, ödeme ve sipariş ile ilgili benzeri işlemleri yapar. Bankalar ise, satıcıların yaptığı kredi kartı işlemlerinin doğrulanması ve ödemelerin bankalar arası takasını sağlamak üzere başka bir yazılım kullanırlar. [17]

SET, güvenli bir iletişim altyapısı sağlamasına karşın, beklendiği hızda yaygınlaşamamıştır. Bunun nedenleri, kullanıcı kolaylığında yaşanan sıkıntılar ve yazılımların dağıtımı ile ilgili zorluklardır.

İmzalanmış ve şifrelenmiş elektronik postalar

Messenger ve Outlook gibi bazı elektronik posta programları S/MIME (Secure Multipurpose Internet Mail Extension) protokolünün kullanımıyla, sayısal olarak imzalanmış ve şifrelenmiş elektronik postaları destekler. S/MIME kullanarak elektronik postaları şifrelemek ve imzalamak için, S/MIME sertifikasına ihtiyaç vardır. Sayısal imza içeren bir elektronik posta, göndericinin postanın başlığında ismi yazılı kişi olduğu yönünde güven içerir.

Elektronik posta programı sayısal imzayı doğrulayamadığı durumda, kullanıcı bu konuda uyarılır. Sayısal imza tekildir ve mesaj üzerinde en küçük bir değişiklik yapıldıysa doğrulanamaz. Bu nedenle imzalanmış elektronik postalar yol üzerindeki değişikliklere karşı güvenlidir. Aynı zamanda, imzalanmış elektronik postalar, göndericinin, daha sonradan bu postayı gönderdiğini inkar etmesini engeller.

Bunlara ek olarak, S/MIME elektronik postayı şifreler ve sadece açık anahtara karşılık gelen özel anahtarın sahibi postayı okuyabilir.

Form imzalama

E-ticarete, genel olarak bir kişinin herhangi bir hareketi gerçekleştirme yetkisinin sürekli ispatı istenir. SSL protokolü istemcinin SSL bağlantısı süresince geçici doğrulanmasını sağlar. Fakat bu bağlantı süresince gerçekleşen hareketler için sürekli kimlik doğrulama sağlamaz. Form imzalama olarak bilinen Netscape teknolojisi, finansal hareketlerin sürekli doğrulanmasını sağlamaktadır. Form imzalama kullanıcıya, sayısal imzasını finansal bir hareketin sonucu olarak üretilmiş web temelli veriyle ilişkilendirme imkanı tanımaktadır. Örneğin İstemci S/MIME ve SSL sertifikası ile ilişkilendirilmiş bir özel anahtar, bu amaçla kullanılabilir.

Form imzalamayı destekleyen bir web sayfası üzerinde “submit” düğmesine basıldığında imzalanacak tam metni içeren bir iletişim kutusu ekrana gelir. Form tasarımcısı imzalamada kullanılacak sertifikayı belirler veya tarayıcı veritabanında saklanan sertifikalardan kullanıcının seçimine izin verir. Kullanıcı “OK” düğmesine bastığında metin imzalanır ve sunucuya gönderilir. Sunucu imza doğrulama aracını kullanarak sayısal imzayı doğrular.

Nesne imzalama

Nesne imzalama, internet’ ten indirilen kod hakkında güvenilir bilgi vermek üzere, açık anahtarlı kriptografinin bilinen tekniklerini kullanır. Nesne imzalama teknolojisiyle Java Applet’ leri, Javascript kodları, Plug-in’ ler ve benzeri nesneler imzalanabilir. İmzalanmış nesneler ve imzalar JAR uzantılı özel bir dosyada saklanırlar. Dosya imzalama için, öncelikle nesne imzalama sertifikasına sahip olmak gereklidir.

5.4.3 Sertifika içeriği

Sertifika içeriği, X.509 v3 standartına göre düzenlenir.

Farkedilebilir İsim (Distinguished Name): X.509 v3 sertifikası, farkedilebilir ismi açık anahtar ile ilişkilendirir. Farkedilebilir isim bir nesneyi tekil olarak tanıtan bir dizi isim ve değer çiftidir.

Aşağıda bir farkedilebilir isim örneği görülmektedir:

Uid=osmank, e=osmank@esbank.com.tr, cn=Osman KARAAHMETOĞLU,
o=Esbank T.A.S., c=TR

Kullanılan kısaltmaların anlamı aşağıdadır:

uid: Kullanıcı adı

e: Elektronik posta adresi

cn: Kullanıcının genel adı

o: Kurumun iadı

c: Ülke adı

Tipik bir sertifika veri ve imza olmak üzere iki kısımdan oluşur.

Veri kısmı şu bilgileri içerir:

- Sürüm numarası.
- Sertifika seri numarası: Sertifikayı verildiği sertifika makamı bazında tekil olarak tanıtan numaradır.
- Bilgi.
- Kullanıcının açık anahtarı ile ilgili bilgi. Bu bilgi kullanılan algoritma ve anahtarın gösterilimini içerir.
- Sertifikayı dağıtan sertifika makamının tanınır ismi.
- Sertifikanın geçerlilik süresi.
- Sertifikanın farkedilebilir ismi
- Seçimlik sertifika uzantısı: Örneğin sertifikanın istemci mi, sunucu mu yoksa S/MIME sertifikası mı olduğu ile ilgili bilgi bu bölüme yazılır.

İmza kısmı şu bilgileri içerir:

- Sertifika otoritesi tarafından kullanılan kriptografik algoritma
- Sertifika otoritesinin sayısal imzası
- Şekil 5.8' de bir sertifika örneği görölmektedir.

Şekil 5.9' da, Şekil 5.8.' deki sertifikanın 64 bit olarak kodlanmış şekli gösterilmektedir. [14]

Certificate:

Data:

Version: v3 (0x2)

Serial Number: 3 (0x3)

Signature Algorithm: PKCS #1 MD5 With RSA Encryption

Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US

Validity:

Not Before: Fri Oct 17 18:36:25 1997

Not After: Sun Oct 17 18:36:25 1999

Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US

Subject Public Key Info:

Algorithm: PKCS #1 RSA Encryption

Public Key:

Modulus:

00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
91:f4:15

Public Exponent: 65537 (0x10001)

Extensions:

Identifier: Certificate Type

Critical: no

Certified Usage:

SSL Client

Identifier: Authority Key Identifier

Critical: no

Key Identifier:

f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
26:c9

Signature:

Algorithm: PKCS #1 MD5 With RSA Encryption

Signature:

6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
dd:c4

Şekil 5.8 SSL sertifikası örneği

-----BEGIN CERTIFICATE-----

MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYDVQQGE
wJVUzERM8GA1UEChMITmV0c2NhcnGUxFTATBgNVBAsTDFN1cHJpeWEncyB
DQTAeFw05NzEwMTgwMTM2MjVaFw05OTEwMTgwMTM2MjVaMEgxCzAJBgN
VBAYTAiVTMREwDwYDVQQKEwhOZXRzY2FwZTENMA5GA1UECxEUHVicz
EXMBUGA1UEAxMOU3VwcmI5YSBTaGV0dHkkgZ8wDQYJKoZIhvcNAQEFBQ
ADgY0AMIGJAoGBAMr6eZiPGfjX3uRjG7SdATYazBcABu1AVyd7chRki
Q31FbXFOGD3wNktbf6hRo6EAmM5/R1AskzZ8AW7LiQZBcrXpc0k4du+2Q6xJu
2MPm/8WKuMOnTuvzpo+SGXelmHVChEqooCwfdiZywyZNMmrJgaoMa2MS6p
UkfQVAgMBAAGjNjA0MBEGCWCGSAGG+EIBAQQEAwIAgDAfBgNVHSMEGD
AWgBTy8gZZkBhHUFWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAOBQBTl
6/z07Z635DfzX4XbAFpjlRIAYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf91o3j3Ukd
GYpcd2cYRCgKi4MwqdWyltpuHAH18hHZ5uvi00mJYw8W2wUOsY0RC/a/IDy84
hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd1A==

-----END CERTIFICATE-----

Şekil 5.9 Şekil 5.8.'deki sertifikanın 64 bit olarak kodlanmış şeklidir.

Kimlik doğrulama algoritmaları

- Diffie-Hellman Anahtar Takası Algoritması: Birbirleriyle mesajlaşacak iki tarafın, güvenli bir şekilde gizli anahtarlarına takas etmesi işlemini yerine getirir. Algoritmanın içeriği aşağıda gösterilmiştir:

1. Birbirleriyle mesajlaşacak iki taraf, Alice ve Bob, a mod m ve büyük bir asal sayı olması gereken g tamsayısı olmak üzere, iki açık değeri paylaşmaktadırlar.

2. Alice rastgele çok büyük bir a sayısı belirler ve

$$X = g^a \text{ mod } m,$$

eşitliğini hesaplar.

3. Bob rastgele çok büyük bir b sayısı belirler ve

$$X = g^b \text{ mod } m,$$

eşitliğini hesaplar.

4. Alice X değerini ,Bob' a gönderir.

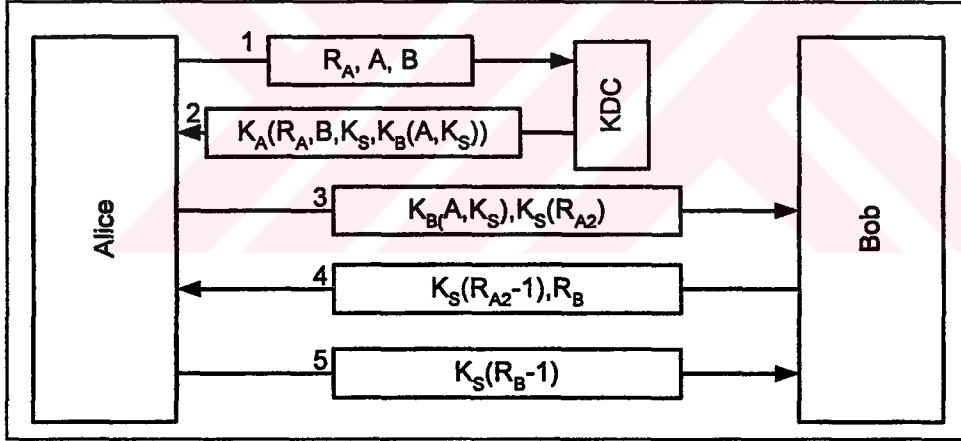
$$K1 = X^b \text{ mod } m,$$

eşitliği, Bob tarafından hesaplanır.

5. $K2 = Y^a \text{ mod } m,$

eşitliği, Alice tarafından hesaplar.

- Needham-Schroeder Kimlik Doğrulama Protokolü: 1978 yılında Needham ve Schroeder tarafından bulunmuştur. Şekil 5.10' da gösterimi yapılmış olan protokol, Alice' in anahtar dağıtım merkezine (key distribution center – KDC) Bob ile konuşmak istediğini, R_A rastgele sayısı ile bildirmesi ile başlar. KDC, Alice' in rastgele numarasını, oturum anahtarını ve Bob' a gönderilmek üzere bir bileti, bir mesajla (mesaj 2) Alice' e iletir. R_A rastgele sayısı KDC' nin gönderdiği mesajın yeni bir mesaj olduğunu anlamak üzere kullanılır. KDC, birinci mesajdaki B' yi kendi kimliği ile değiştirerek sisteme saldırıda bulunmaya çalışanlara karşı, bileti K_T ile şifreler. K_B ile şifrelenmiş bilet şifreli mesajın içindedir. Bileti alan Alice, yeni bir R_{A2} sayısı üretir ve bileti K_S oturum anahtarı ile şifreleyerek Bob' a gönderir. Mesajı alan Bob kendisinin Bob olduğunu Alice' e kanıtlamak için $K_S(R_{A2}-1)$ mesajını Alice' e gönderir. $K_S(R_{A2})$ geri gönderilme işlemi tekrar çalışmaz. Çünkü saldırgan daha önceki seferden $K_S(R_{A2})$ mesajını elde edebilir. Alice artık Bob ile konuştuğundan emindir. Fakat $K_S(R_{A2})$ mesajının gönderilmesinin üstünden birkaç milisaniye geçmiştir. Şekilden de görüldüğü gibi 5 numaralı mesajın gönderilme sebebi, gerçekten Bob' un Alice' le konuştuğundan emin olmasıdır. [16]

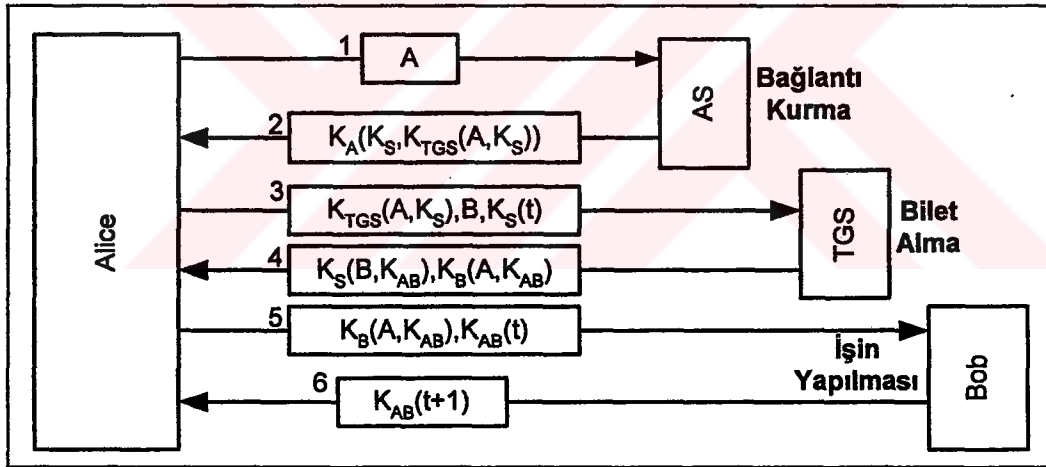


Şekil 5.10 Needham-Schroeder kimlik doğrulama protokolü

- Kerberos Protokolü: M.I.T. tarafından tasarlanan Kerberos protokolü, kullanıcıların ağ kaynaklarına güvenli bir şekilde erişimini sağlamaktadır. Needham Shroeder protokolünden ana farkı, ağ üzerindeki tüm saatlerin eş zamanlı olduğunu varsaymasıdır. Kerberos protokolü, Alice istemcisine ek olarak üç sunucu gerektirir.:
 1. Kimlik Doğrulama Sunucusu (Authentication Server – AS), kullanıcı kimliklerini doğrulama işlemini gerçekleştirir.
 2. Bilet Atama Sunucusu (Ticket Granting Server – TGS), tanımlayıcı biletlerin ispatını yayınlamaktadır.

3. Bob, Alice' in isteklerine göre görev gördüğünden, sunucu olarak düşünölmüştür.

- Kerberos protokolünde oturum, iletişim kurmak isteyen Alice' in bir iş istasyonu aracılığı ile AS' ye ismini göndermesi ile başlar. Bu mesaja AS, Alice' in gizli anahtarı ile şifrelenmiş, bir oturum anahtarı ve bilet ($K_{TGS}(A, K_S)$) ile cevap verir. Bu mesajı alan iş istasyonu Alice' in Alice olduğunu gösterecek şifreyi sorar. İş istasyonu almış olduđu şifreyi, K_A gizli anahtarını oluşturmada kullanır. Bu işlemden sonra Alice iş istasyonundan, Bob ile iletişim kurma isteğinde bulunur. Bu isteği alan iş istasyonu TGS' den, Bob ile iletişimde kullanmak üzere bir bilet isteğinde bulunur. TGS' nin göndericinin Alice olduğunu anlaması için, $K_{TGS}(A, K_S)$ mesajı, TGS' ye gönderilir. TGS, Alice' in Bob ile iletişimde kullanması için, K_{AB} oturum anahtarını oluşturur. TGS, bu anahtarın bir kopyasını, Alice'in okuyabilmesi için, K_S gizli anahtarı ile, diğerini ise Bob' un gizli anahtarı, K_B ile şifreler. Bundan sonra Alice Bob ile iletişime başlamak üzere, K_{AB} oturum anahtarını Bob'a gönderir. Bob' un bu mesaja gönderdiği cevap ise, Alice'in Bob ile konuştuğunun kanıtıdır. [16]



Şekil 5.11 Kerberos protokolü

6 FIREWALL

Firewall gelen ve çıkan bilgi paketlerinin geçtiği bir süzgeç görevini yerine getirir. Firewall' lar tanımı dışında, kısıtlama listelerine göre erişim kontrolü gibi ek işlevleri de gerçekleştirirler. Kabaca, tüm firewall' lar bir nevi kabul etme ve reddetme işlevi görürler. Bağlantı isteği olduğu zaman açılan bir ethernet köprüsü, firewall' ın çok basit bir biçimi olarak düşünülebilir. Bir ethernet köprüsü saldırganı güvenilir bilgilerin tutulduğu ağ ortamından uzak tutabilir; fakat böyle bir firewall' ın yönetimi hiç de kolay değildir.

Tasarım açısından çok farklı biçimlerde firewall' larla karşılaşmak mümkündür. Bunlar aşağıda listelenmiştir: [18]

- Yüklendiği sistemin TCP/IP yığınına değiştiren veya mevcut yığın ile iletişim kuran yazılım modülleri.
- İnternet güvenliği hedef alınarak, yeniden yazılmış bir işletim sistemi.
- SMTP ve HTTP gibi belirli tip internet bağlantısı için, koruma sunan uygulamaya özel firewall' lar.
- Gelen ve çıkan bağlantılar için süzgeç görevi gören yönlendirici gibi, donanım tabanlı firewall' lar.
- Bu sınıflamaya giren tüm ürünler, gelen ve çıkan paketleri yakalama, değerlendirme, geçişine izin verme veya reddetme işlevlerini yerine getirdikleri için firewall olarak adlandırılırlar.
- Bugünün firewall ürünleri paket süzgeçleme, uygulama vekilleri ve durumsal inceleme (stateful inspection) süzgeçleme işlevlerini içerirler.

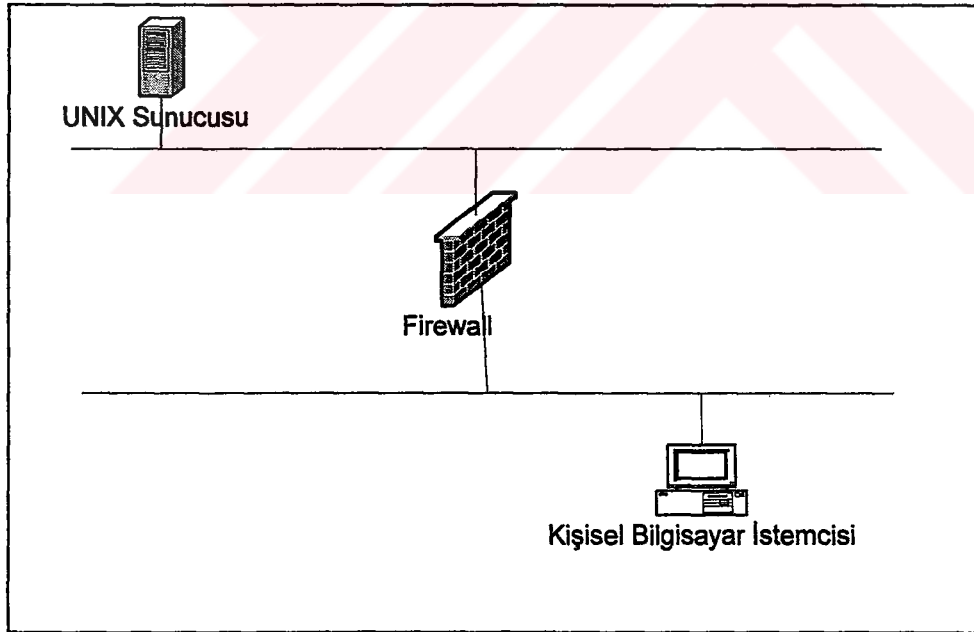
6.1 IP Adresinin Süzgeçten Geçirilmesi

Hemen hemen tüm firewall' lar, IP adreslerinin süzgeçten geçirilmesi işlevini sunarlar. Bu süzgeçler IP paketinin başlığını inceleyerek, kaynak ve varış adresine göre paketin geçişi için, kabul veya red kararı verirler. Bu süzgeçlerin çalışma mantığı Şekil 6.1' de gösterilmektedir. Bir kişisel bilgisayar istemcisi, UNIX sunucusuna Telnet protokolü ile erişmek istediğinde, kişisel bilgisayardaki Telnet istemcisi bir TCP paketi oluşturur ve varışa ulaştırması için kendi yerel TCP/IP

yığınınına verir. Yığın TCP paketini, IP paketi içerisine yerleştirir ve kendi üzerinde tanımlı yol doğrultusunda, UNIX sunucusuna gönderir. Şekil 6.1' de kişisel bilgisayar istemcisi paketi, UNIX sunucusuna göndermesi için, Firewall' a gönderir. Firewall üzerinde, UNIX sunucusuna yapılan tüm paketlerin reddedilmesini söyleyen bir kural varsa, istemciden sunucuya giden Telnet isteği geri çevirilecektir. Firewall üzerinde UNIX sunucusuna hiçbir IP paketi iletilmediğinden, sunucuya, sadece sunucuyla aynı bölme (segment)' de olan istemciler tarafından erişilebilecektir.

IP adreslerinin süzgeçlenmesi ile ilgili diğer bir örnek, Şekil 6.2' de gösterilmektedir. Bu örnekte kişisel bilgisayar dışındaki tüm istemciler, UNIX sunucusuna bağlanabilmektedir. Kabul veya red süzgeçlerinin ip adresleri bazında konulması, basit bir yerel ağda karşılaşılan en temel koruma şeklidir. İstemci kaynak adresi veya varış adresi nedeniyle iletişim hakkına sahip değilse, istemciye ait bilgi paketleri firewall tarafından reddedilir.

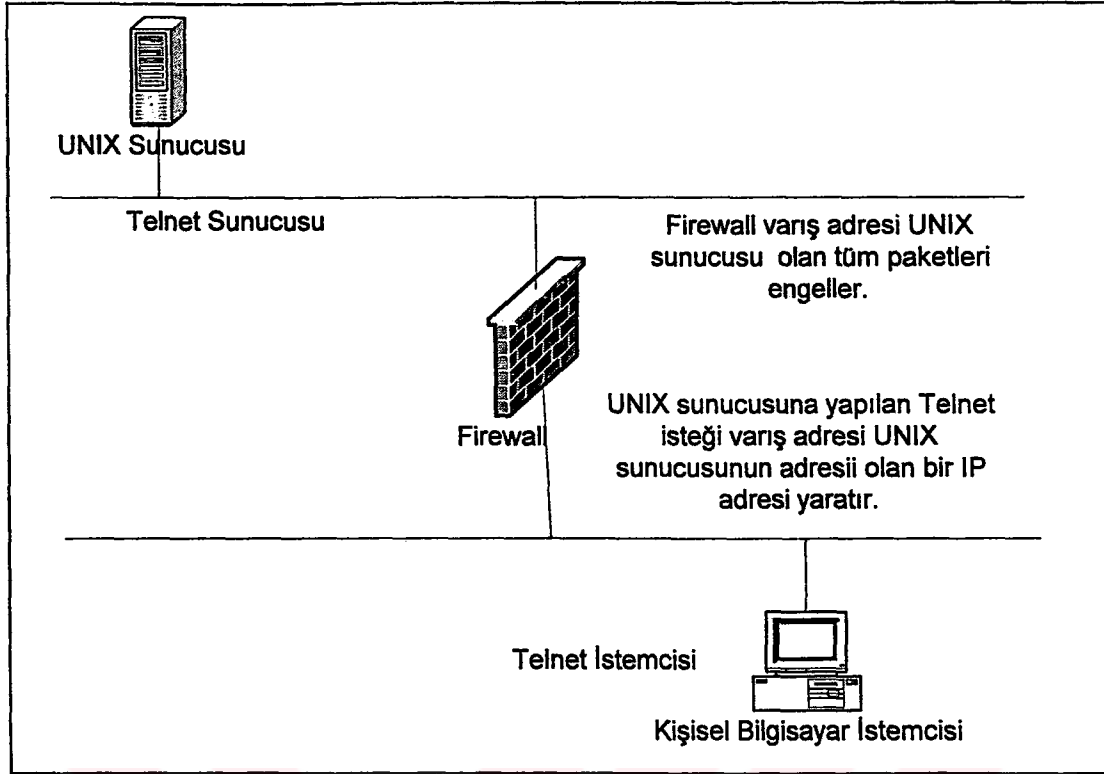
Küçük ölçekli firmalarda kullanıcıların erişim kontrolü, bu tip süzgeçleme yöntemleri ile sağlanmaktadır. Fakat IP taklidi gibi saldırılar nedeniyle, IP paket süzgeçleme çok güvenli bir koruma yöntemi değildir. Bunun yanında, bu süzgeçler firewall tasarımının temelini teşkil etmekte olup, toplam savunma altyapısının önemli bir parçasıdır.



Şekil 6.1 IP adresi süzgeçleme

6.1.1 TCP/UDP kapı süzgeçleme

Bilgi paketlerinin kabul veya reddine, sadece IP adresi kontrolü ile karar verilmesi doğru bir yöntem değildir. Örneğin, bir sunucu üzerinde sadece belli bir hizmete erişimin engellenmesi, diğer hizmetlerin erişime açık olması gereken bir durumda,



Şekil 6.2 IP trafiğinin firewall tarafından kesilmesi

sunucuya olan tüm trafiği engellemek, Telnet dışındaki hizmetlerinde engellenmesi anlamına gelecektir. Bu nedenle süzgeçlemede kullanılan kurallarda, IP adresinin yanında hizmete ilişkin TCP ve UDP kapı numaraları da kullanılır.

Sunucu tarafı TCP/UDP kapı süzgeçleme

Şekil 6.3' teki örnekte, kişisel bilgisayar istemcisinin UNIX sunucusuna Telnet protokolü ile erişimini engellemek için, Firewall'ın kural veritabanına UNIX sunucusuna, 23 numaralı kapıdan gelecek tüm istekleri reddedecek, bir kural girilmesi gereklidir.

Güvenlik açısından, sadece bir kapıyı kapamak iyi bir yöntem değildir. İzlenmesi gereken yöntem, önce tüm kapıları kapatan bir kuralın firewall kural veritabanında tanımlanması, daha sonra izin verilmesi uygun görülen kapılar için kural girilmesidir. Tablo 6.1' de buna ilişkin düzenleme gösterilmektedir. Tüm kapılar üç numaralı kural yardımıyla kapandıktan sonra, UNIX sunucusu üzerinde erişimine izin verilen, SMTP ve POP hizmetleri bir ve iki numaralı kurallar yardımıyla gerçekleştirilmiştir.

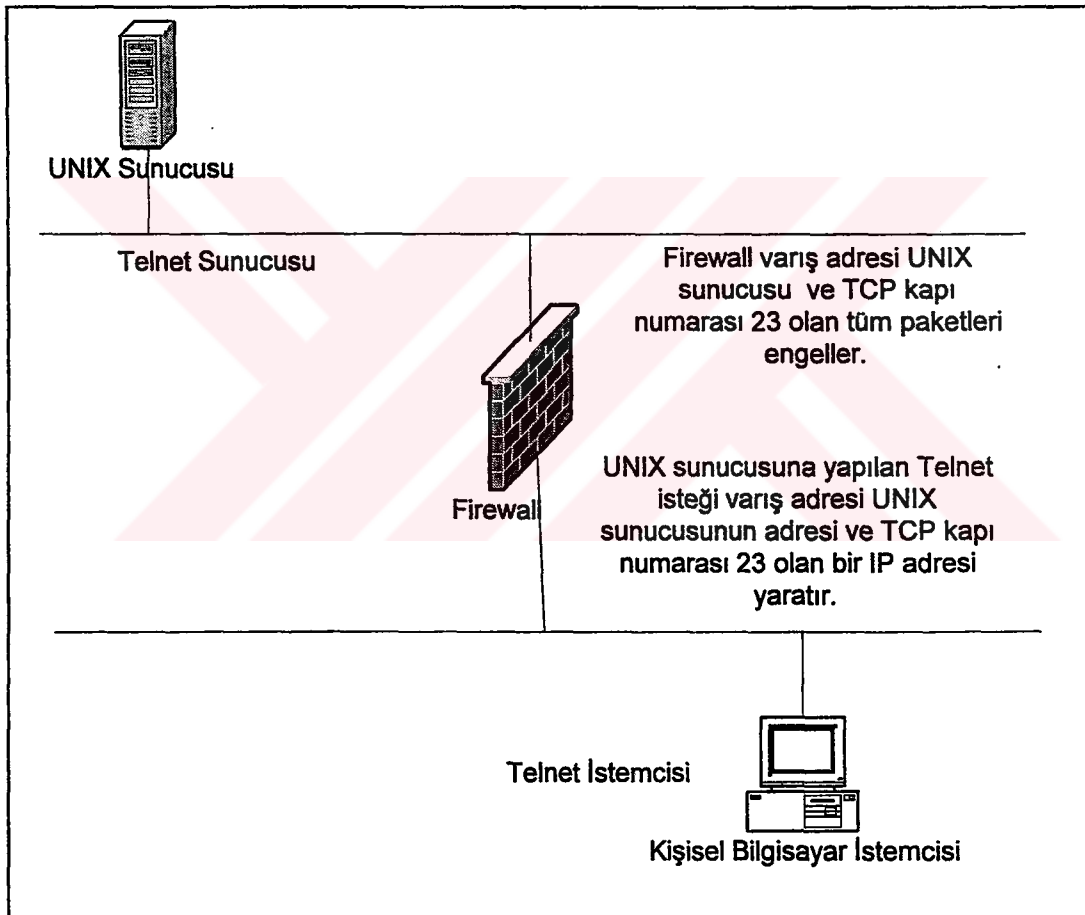
İstemci tarafı TCP/UDP kapı süzgeçleme

TCP/IP, uçtan uca bir protokoldür ve birbirleriyle konuşan her bir düğümün tekil bir adresi vardır. İstemci ve sunucular birbirleriyle TCP ve UDP kapı numaraları üzerinden bağlantı kurarlar. Bir sunucu hizmetine erişmek isteyen istemci 1023' ün

üzerinde bir kapı numarasını rastgele seçer. Bu nedenledir ki, iletişimin sağlanması için, istemiciye gelen paketlerin geçişine izin verecek kuralların da firewall kural veritabanına eklenmesi gereklidir.

Tablo 6.1 Firewall kural veritabanı

Numara	Kaynak	Varış	Kapı	Kural
1	PC	UNIX	25	Kabul
2	PC	UNIX	110	Kabul
3	Hepsi	Hepsi	Hepsi	Red



Şekil 6.3 Sunucu tarafı TCP/UDP kapı süzgeçleme

6.2 Uygulama Vekil Sunucuları

Uygulama vekil sunucuları, iki ağ arasına yerleşmiş firewall üzerinde çalışan uygulama programlardır. Vekil sunucularının çalıştığı konakların, yönlendirici gibi davranması gerekli değildir. İstemci program vekil sunucusu üzerinde herhangi bir

varışa bağlantı kurmak istediğinde, ilk olarak vekil sunucusu ile bağlantı kurmak zorundadır. İstemci ile vekil sunucusu arasında bağlantı kurulduktan sonra, istemci vekil sunucusundan kendisi için, varış hizmetlisine bağlantı kurmasını talep eder. Bu işlemler başarıyla sonuçlandırıldığında, biri istemciden vekil sunucusuna, diğeri vekil sunucusundan varış hizmetlisine olmak üzere iki bağlantı vardır. Bu bağlantı kurulduğundan itibaren, vekil sunucusu istemci ile sunucu arasında paketleri iki yönlü olarak alır ve iletir. Vekil sunucusu, bağlantı kurma ve paket iletme ile ilgili kararların tümünü verir; fakat konak üzerindeki herhangi bir yönlendirme işlemi ile ilgilenmez.

Vekil sunucuları hem özel amaçlı vekil makinelerinde, hem de genel amaçlı bilgisayarlarda bulunmaktadır. Vekil sunucuları paket süzgeçleyen yönlendircilere göre, daha yavaş olmasına rağmen, daha güvenli olduğundan tercih edilirler. Paket süzgeçleyen yönlendiriciler, işletim sisteminin yönlendirme gerçekleştirmesindeki yanlışlıklar ve gediklerden büyük sıkıntı çeker.

Çok karışık süzgeçleme ve erişim kontrol kararlarının verilmesi, uygulama vekil sunucularının pahalı hesaplama kaynakları ve güçlü bir konak gerektirmesi sonucunu doğurmuştur. Örneğin, UNIX işletim sistemi üzerinde çalışan bir firewall teknolojisi aynı anda 200 HTTP oturumunu desteklemeye ihtiyaç duyarsa, konağın aynı anda 200 HTTP vekil sürecini, kabul edilebilir başarımla sağlaması gereklidir. Buna 100 FTP oturumu, 25 SMTP, bazı LDAP, bazı DNS hareketlerini katarsanız, 500 ve 1000 arası vekil süreçlerini kotarması gereken bir konağa ihtiyacınız olur.

6.3 Durumsal İnceleme Süzgeçleme veya Devingen Paket Süzgeçleme

Paket süzgeçleme yönteminin daha yetenekli süzgeçleme işlevleri içeren şekline, durumsal inceleme süzgeçleme veya devingen paket süzgeçleme denir. Paket süzgeçleme daha önceki paketleri düşünmeden, mesajın içeriğine bakarak, süzgeçleme gerçekleştirmekle sınırlıdır. Durumsal inceleme süzgeçleme karar vermede, hem paketin içeriği, hem de daha önceki paketlerden etkilenir. Durumsal inceleme süzgeçleme paket süzgeçlemede olduğu gibi yönlendirme işlevlerine ek olarak üretilmiştir; durumsal inceleme süzgeçleme işlevlerinin çalıştığı konaklar, aynı zamanda yönlendirici işlevlerine sahiptirler. Durumsal inceleme süzgeçleme, bir yönlendirme eklentisi olduğundan, vekil sunucularında çok yüksek bir başarımla sağlarlar. Paket süzgeçlemede, karar verme sürecinde vekil sunucularındaki çok kapsamlı ve karışık ölçütlerin yer alması, yüksek kalitede bir yönlendirme altyapısı gerektirmektedir.

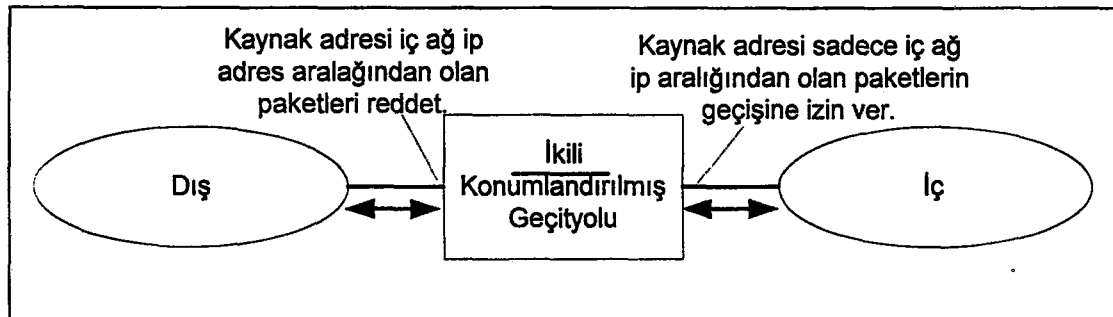
6.4 Firewall Mimarileri

Tüm firewall mimarilerinde firewall, ağın sınırlarında, ağı dış tehlikelerden korumak üzere, erişim kontrolü görevini gerçekleştirir. Tamamen iç ağ içinde kullanılan firewall' lar ise, alt ağlar arasında koruma görevi görür. Alt ağlar arasında erişim kontrolü yapmanın, ağ ile internet arasında erişim kontrolü yapmaktan hiç bir farkı yoktur. Bu nedenledir ki, firewall mimarileri iç ağlarda da kullanılabilir. Topolojilerine göre firewall mimarileri şu şekilde sınıflandırılabilir: [19]

- İkili konumlandırılmış geçityolu (dualhomed gateway)
- İzleyen yönlendirici (screening router) ve bastion konak (bastion host)
- İzleyen yönlendirici ve İkili konumlandırılmış geçityolu
- İzlenen alt ağ (screened subnet) ve bir DMZ
- İzlenen alt ağ (screened subnet) ve iki DMZ
- Güvenli sunucu ağı

6.4.1 İkili konumlandırılmış geçityolu (Dualhomed Gateway)

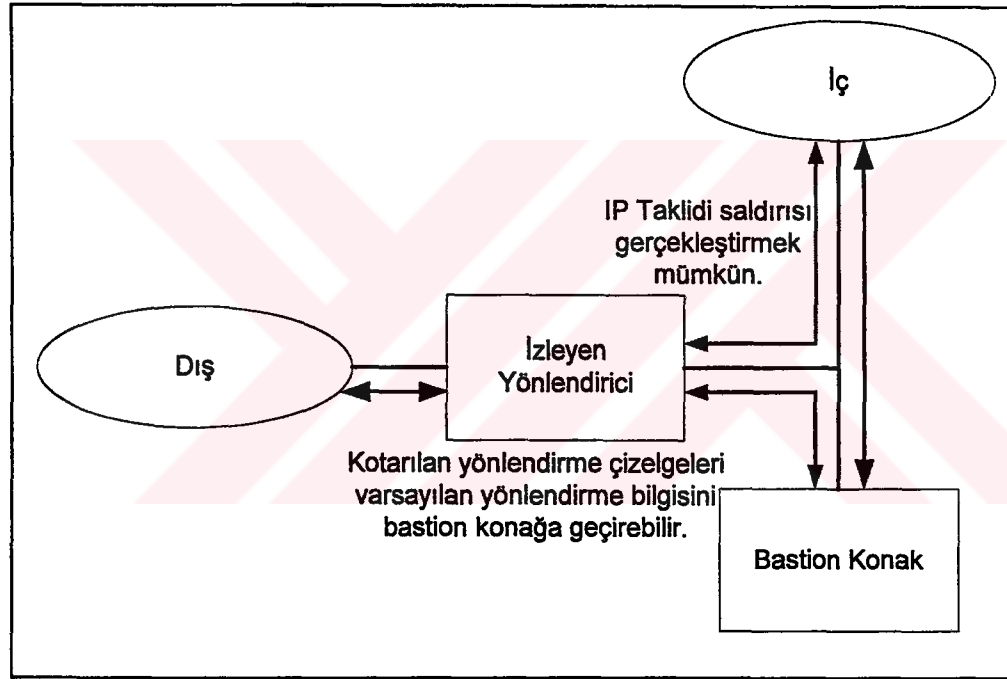
Genellikle, küçük çaplı kurumlarda kullanılan bir firewall mimarisidir. Dışarıdan gelen bağlantı istekleri, doğrudan geçityolunun dış arabirime gelirken, içerden dışarıya bağlanan makinelerde geçityolunun iç arabirimine bağlantı kurmaktadır. Geçityolunun iç ve dış arabirimine gelen bağlantı istekleri, tanımlanmış süzgeçlere göre incelendikten sonra, kabul veya reddedilir. Şekil 6.4' de yapısal gösterimi bulunan bu mimaride, iç arabirimin kaynak adresi iç ağ adres aralığından bağlantı isteklerine izin vermesi, dış arabirimin de iç ağda olduğu kanıtlanan kaynak adresi ile ağa erişmek isteyen bağlantı isteklerini kesmesi durumunda ip taklidi saldırısı engellenir.



Şekil 6.4 İkili konumlandırılmış geçityolu (Dualhomed gateway)

6.4.2 İzleyen yönlendirici (screening router) ve bastion konak (bastion host)

Özellikle, iç ağdan gelecek tehlikelerin önemslenmediği, iç ağın dışarıdan gelecek tehlikelere karşı korunması düşünülen durumlarda kullanılması uygun, bir firewall mimarisidir. Şekil 6.5' de yapısal gösterimi bulunan bu mimaride, dışarıdan içeriye bağlantı istekleri, ilk olarak izleyen yönlendiriciye gelir ve izleyen yönlendirici üzerinde tanımlı kurallara göre süzgeçten geçirilir. Buradaki süzgeçlerden geçiş izni alan paketler, bastion konağına iletilirler. Burada uygulama seviyesi süzgeç kurallarına göre süzgeçten geçirilen paketler, geçiş izni alırlarsa iç konaklara iletilirler. İç kullanıcılardan gelen erişim istekleri ise, ilk olarak, bastion konakta uygun uygulama seviyeli geçityoluna gelirler ve burada uygulama seviyeli süzgeçlerden geçirilirler. Geçiş izni alan paketler, izleyen yönlendiriciye iletilir ve burada da bir süzgeçten geçirilir. Geçiş izni alan paketler dış konaklara iletilirler.



Şekil 6.5 İzleyen yönlendirici ve bastion konak

6.4.3 İzleyen yönlendirici ve ikili konumlandırılmış geçityolu

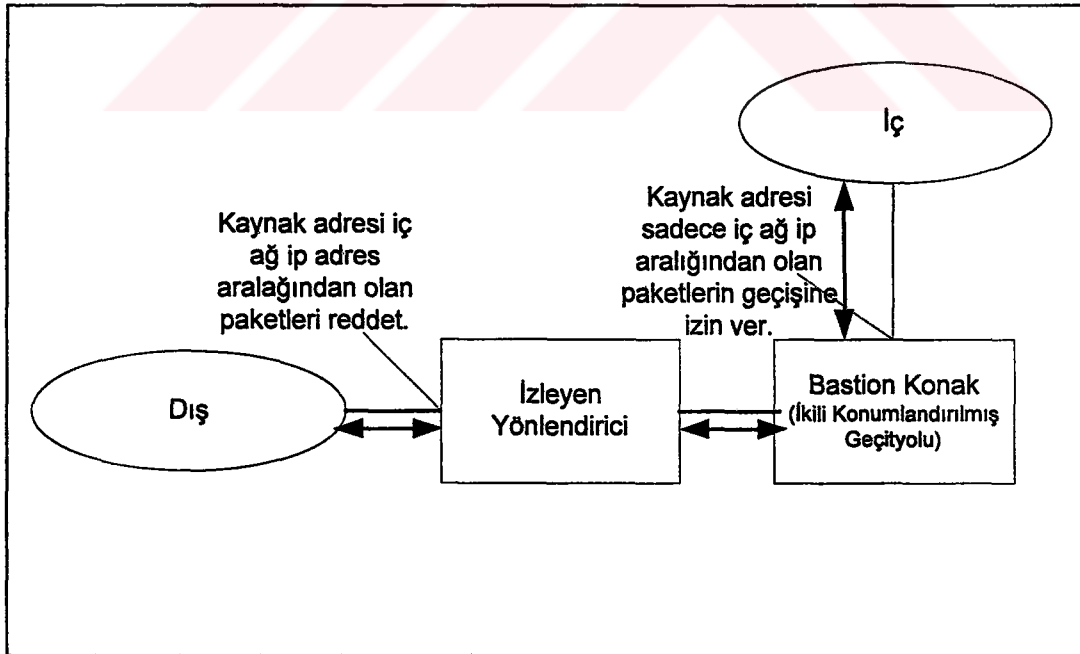
İç ağın dışarıdan gelecek tehlikelere karşı korunması gereken durumlarda, içeriden ip taklidi saldırısı ve dışarıdan izleyen yöndericinin ele geçirilme tehlikesi olduğu durumlarda kullanılan firewall mimarisidir. İçeriden gelecek IP saldırılarına karşı, bastion konak üzerinde yapılan kaynak adresi kontrolü sayesinde güvenlidir. İzleyen yönlendirici üzerinde içeriden bir adresin kaynak adresini kullanan paketlere geçiş izni vermeyecek bir süzgeç kullanıldığı durumda dışarıdan gelecek IP taklidi

saldırılarına karşı da güvenlidir. Şekil 6.6' da yapısal gösterimi bulunan bu mimaride, veri akışını izleyen yönlendirici ve bastion konak mimarisi ile aynıdır.

6.4.4 İzlenen alt ağ (screened subnet) ve bir DMZ

İç ağın dışarıdan gelecek tehlikelere karşı korunması gereken durumlarda ve iç ağın firewall' a karşı düzenlenecek saldırılar açısından güvensiz olduğu veya iç ağın firewall üzerinde yaratabileceği tehlikelerin olanak dahilinde olduğu durumlarda kullanılan firewall mimarisidir. Şekil 6.7' de yapısal gösterimi bulunan bu mimaride dışarıdan gelen bağlantı isteği, ilk olarak dış izleyen yönlendiriciye gelir. Bilgi paketleri izleyen yönlendiricideki uygulama seviyesi süzgeçlere göre, bastion konağına yönlendirilir. Bastion konağına gelen paketler, buradaki protokol bağımlı uygulama seviyesi geçit yollarında, uygulama seviyesi süzgeçlerden geçirilir. Geçiş izni alan paketler, iç izleyen yönlendiriciye iletilir. İç izleyen yönlendirici üzerindeki süzgeçlerden geçirilen paketler, geçiş izni aldıkları durumda içeriye iletilirler. İçeriden dışarıya veri akışı, aynı sürecin sondan başa doğru gelişmesidir.

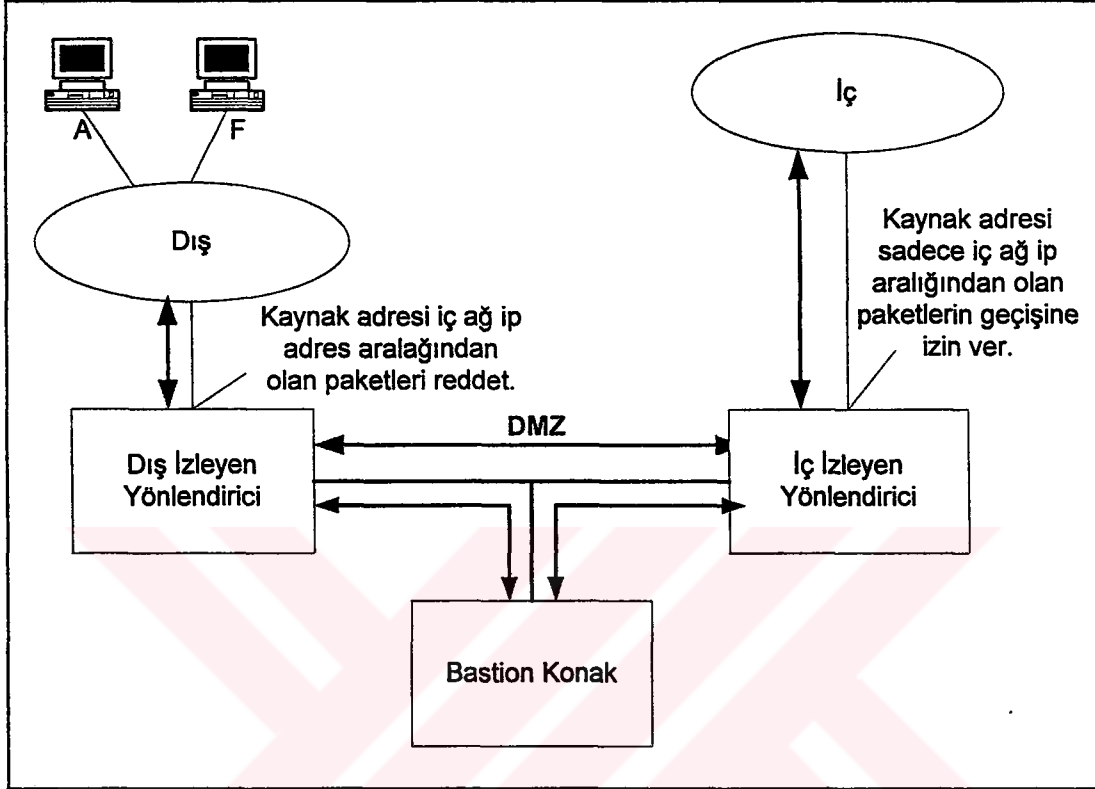
Dışarıdan içerideki bir ip adresini kaynak adresi kullanılarak yapılan bağlantı istekleri, dış izleyen yönlendirici üzerine konulacak bir süzgeç, içeriden dışarıya dışarıdaki bir kaynak adresi kullanılarak yapılan bağlantı istekleri, iç izleyen yönlendirici üzerine konulacak bir süzgeç ile engellenirse ip taklidi saldırısı ihtimali ortadan kalkacaktır.



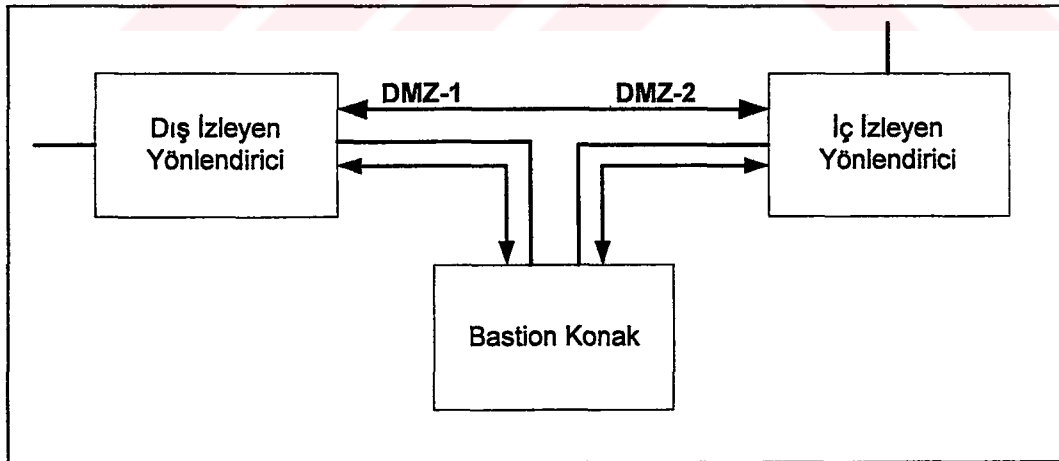
Şekil 6.6 İzleyen yönlendirici ve ikili konumlandırılmış geçit yolu

6.4.5 İzlenen alt ağ (screened subnet) ve iki DMZ

İzlenen alt ağ ve bir DMZ firewall mimarisinin kullanıldığı durumlara ek olarak, izleyen yönlendirici ele geçirilmesi durumunun imkan dahilinde olduğu durumlarda kullanılır. Şekil 6.8' de yapısal gösterimi bulunan bu mimaride veri akışı, izlenen alt ağ ve bir DMZ firewall mimarisi ile aynıdır. IP taklidi saldırılarına karşı güvenlidir.



Şekil 6.7 İzlenen alt ağ (screened subnet) ve bir DMZ



Şekil 6.8 İzlenen alt ağ (screened subnet) ve iki DMZ

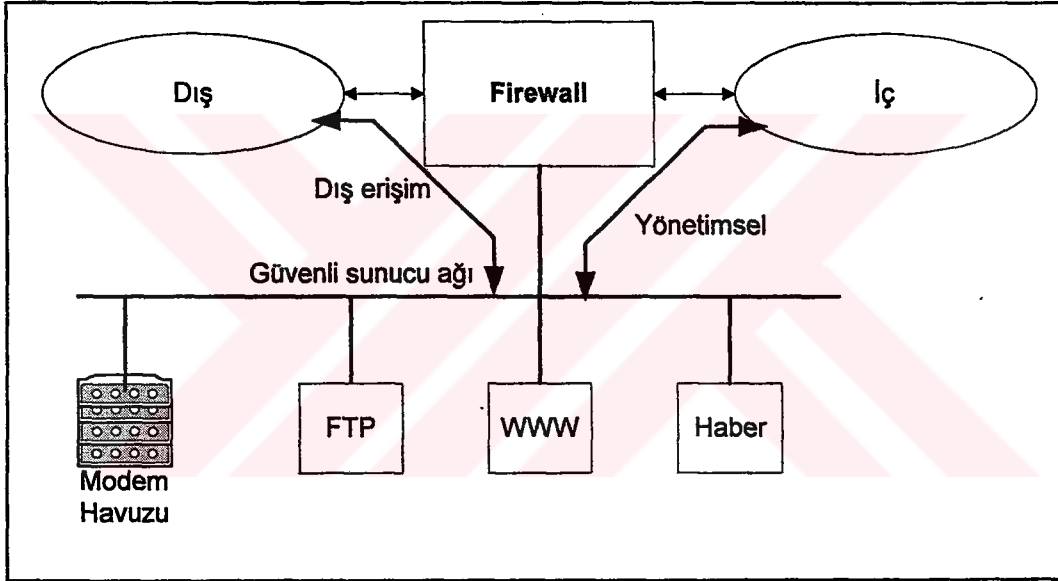
6.4.6 Güvenli sunucu ağı

Özellikle www, ftp, news, pop, imap vb. hizmetlerin kullanıcılara, iç ağı tehlikeye düşürmeden güvenli bir şekilde sunulması gereken durumlarda kullanılan firewall

Tablo 6.2 Firewall mimarilerinin karşılaştırılması

	Güvenlik	Başarım	Maliyet	Kayıt tutma mekanizmaları	Ölçeklenebilirlik
İkili Konumlandırılmış Geçityolu	Saldırgan tarafından IP iletimi açılabilirse saldırı gerçekleştirilebilir.	Tek bir geçityolu tüm kararları vermek zorunda olduğu için başarım düşüktür.	Sadece bir geçityolu gerektirdiği için maliyeti düşüktür.	Merkezi kayıt tutma mekanizmaları mevcuttur.	
İzleyen yönlendirici ve bastion konak	IP takilidi saldırıları gerçekleştirilebilir. Ayrıca saldırıyan izleyen yönlendiriciye ele geçirebilir. Güvenliği düşüktür.		Maliyet düşüktür. İzleyen yönlendiricinin tüm mimarilerde olduğu düşünüldüğünde, tek gerekli ek donanım bastion konaktır.	Bastion konak üzerinde merkezi kayıt tutma mekanizmaları kurmak mümkündür. Kayıt mekanizmaları izleyen yönlendiriciye yapılan saldırıları sezemezler.	Birden fazla bastion konak kullanarak ölçeklenebilirlik artırılabilir.
İzleyen yönlendirici ve ikili konumlandırılmış geçityolu	IP takilidi saldırısı imkansızdır. Bastion konağı ele geçirmek imkansızdır. Güvenliği yüksektir.		Ek bir ağ arabirimine gerek duyulur. Maliyet biraz artar.		Birden fazla bastion konak kullanarak ölçeklenebilirlik artırılabilir.
İzlenen alt ağ ve bir DMZ	Bastion konak üzerindeki ek bölme bastion konak ele geçirilse bile iç trafiğin dinlenmesini engeller. IP takilidi saldırısı ihtimal çok düşüktür. İzleyen yönlendiricilerden biri ele geçirilirse diğeri de tehlikeyededir.		Ek donanım gereklidir. İç izleyen yönlendiricinin donanımı ve yönetim maliyeti, maliyeti artırır.	Merkezi kayıt tutma mekanizmaları mevcuttur.	
İzlenen alt ağ ve iki DMZ	İzlenen alt ağ ve bir DMZ mimarisine göre iyi tarafı, saldırıyanın iç ağa erişmek için dış izleyen yönlendiriciye ele geçirmesi yeterli değildir; bastion konağı da ele geçirmelidir.		İzlenen alt ağ ve bir DMZ ile aynı	İzlenen alt ağ ve bir DMZ ile aynı	
Güvenli sunucu ağı	Yayın yapan sunuculardan birinin ele geçirilmesi iç ağın güvenliğini tehlikeye sokmaz. Proxy kullanımı iç ağı, dışarıdan saklar.	Firewall üç bölmenin bant genişliğini kotarmak zorunda olduğu için başarım düşebilir.	Her bir bölme için bir ağ arabirimi ve ek kablo gerektirdiği için pahalı bir çözümdür.		

mimarisidir. Şekil 6.9' da yapısal gösterimi bulunan güvenli sunucu ağı mimarisi, Bordeware firması tarafından geliştirilmiştir. Şekilde gözüken firewall için, üçlü konumlandırılmış geçityolu, izleyen yönlendirici ve üçlü konumlandırılmış geçityolu ve bastion konağı mimarileri kullanılabilir. Bu mimaride dışarıdan içeriye veri akışında, bağlantı isteği ilk olarak, protokol bağımlı vekiller çalıştıran firewall' a gelir. Bilgi paketleri firewall üzerindeki süzgeçlerden geçiş izni aldığı durumda, güvenli sunucu ağındaki konaklara iletilir. Dışarıdan bakıldığında, vekil prensiplerine göre, bağlantının firewall üzerinde sona erdiği görünür. Böylece güvenli sunucu ağı dışarıdan gizlenmiş olur. Güvenli sunucu ağına bir modem havuzundan ve dışarıdan firewall üzerinden erişime izin, çok kuvvetli bir kimlik doğrulama mekanizması gerektirir. Modem üzerinden gelen kullanıcılar ve iç kullanıcılar internet' e, uygulama seviyesi vekiller sayesinde saydam bir şekilde bağlanırlar. Bu şekilde iç ağ, dış kullanıcılara karşı saklı kalır.



Şekil 6.9 Güvenli sunucu ağı

7 YETKİSİZ ERİŞİMLERİ SEZME (INTRUSION DETECTION)

Yetkisiz erişimleri sezme, herhangi bir sistemin, yetkisiz eylemler ve tecavüzkar davranışların keşfedilmesi amacıyla, denetlenmesi olarak tanımlanabilir.

Bir sistemin içerisindeki, yetkisiz erişimleri sezme üç farklı yaklaşım ile şekillendirilebilir:

1. Güvenlik Geçitleri(Firewalls)
2. Ağ Analiz Araçları(Network Analysis Tools)
3. Konak Tabanlı Denetim Sistemleri (Host-based Monitoring Systems)

Kötü niyetli kullanımlara ve saldırılara karşı, sistemin güvenli hale getirilmesi, saldırıların en erken biçimde sezilmesi ve en az zararla sonlandırılabilmesi için, sistem üzerinde güvenlik ile ilgili olarak gerçekleşen tüm olayların kaydının tutulması yöntemi seçilmiştir. Bugün tüm işletim sistemleri, veritabanları ve ağ araçlarının yapmış oldukları işlemlerle ilgili kayıtlar tutulur. Bu kayıtların tutulmasındaki ana fikir, sistem yöneticisinin daha sonra bu kayıtları izleyerek, sistem üzerinde şüpheli herhangi bir olay olup olmadığını sezmesidir. Böyle bir yöntemle ancak, kullanıcı sayısı ve kayıt miktarının az olduğu durumlarda başarılı olunabilir. Bu nedenle kayıtları inceleyerek, şüpheli durumlarda gerekli eylemleri gerçekleştirecek yazılım veya donanım ürünlerine ihtiyaç vardır.

7.1 Yetkisiz Erişimleri Sezme Çalışmalarının Tarihçesi

1980' li yıllarda daha bilgisayar ağları temelli ticaret ve iletişim, bebeklik çağında iken, bilgi sistemi yöneticileri, sistemlerinin ne kadar güvenli olduğu ve uğradıkları saldırıları püskürtmek için, hangi yolları izlemeleri gerektiği konularında araştırma yapmaktaydılar. Geleneksel bilgeliğin gösterdiği yol, sistem üzerinde meydana gelen güvenlik ile ilgili olayların tümünün, kayıt ve bilançolarının tutulması gerekliliğidir. Bugün tüm işletim sistemleri veritabanları ve araçları, kayıt ve bilanço tutmaktadırlar. Bunun tutulmasının arkasındaki özgün fikir, güvenlik yöneticisinin bu kayıtları incelemesi ve sistem üzerinde şüpheli bir olayın gerçekleşip gerçekleşmediğine karar vermesiydi. Fakat bu ancak, çok az sayıda sistemi olan firmalar için mümkün olmaktaydı; çünkü kayıt ve bilanço dosyaları çok büyük uzunluktaydılar.

Bu durumun kısa sürede anlaşılması üzerine, firmalar kayıt ve bilanço dosyalarını inceleyip raporlar üretecek değerlendirme araçları ürettirler. 1984 yılında Clyde Sayısal Sistemler tarafından üretilen, OpenVMS bilanço ve kayıt dosyalarını şüpheli olayları belirlemek için inceleyen AUDIT ve Amerikan hükümeti tarafından desteklenen Stanford Araştırma Enstitüsünde sistem bilanço bilgileri üzerinde normal kullanım desenleri çıkaran ve bu desenlerden sapmaları rapor eden IDES programları değerlendirme araçlarına örnek olarak gösterilebilirler.

1990' lı yılların ilk yarısında, yetkisiz erişimleri sezme konusundaki araştırmalar, olay sonrası (post-event) bilanço bilgileri tutma yönteminde odaklandı. Fakat iki önemli nedenden ötürü bu tarz ürünler firmalardan itibar görmediler: [20]

1. Bu araçlarla gedikler ve saldırıların tiplerinin anlaşılması, tamamen kullanıcıların yeteneklerine bağlıdır.
2. Kullanıcı, işletim sistemi, veritabanı ve uygulama sayısı arttıkça bilanço kayıtlarının sayısı da artmakta ve sistem üzerinde çok büyük veri alanı kaplamaktadır. Bunun sonucu olarak hizmet dışı kalma sorunları oluşmaktadır.

1990' lı yılların diğer yarısında ise, yönlendirici, ağ trafik izleyicileri, firewall' lar vb. araçların bilanço bilgilerini izleyecek yeni uygulama yazılımları üretilmiştir.

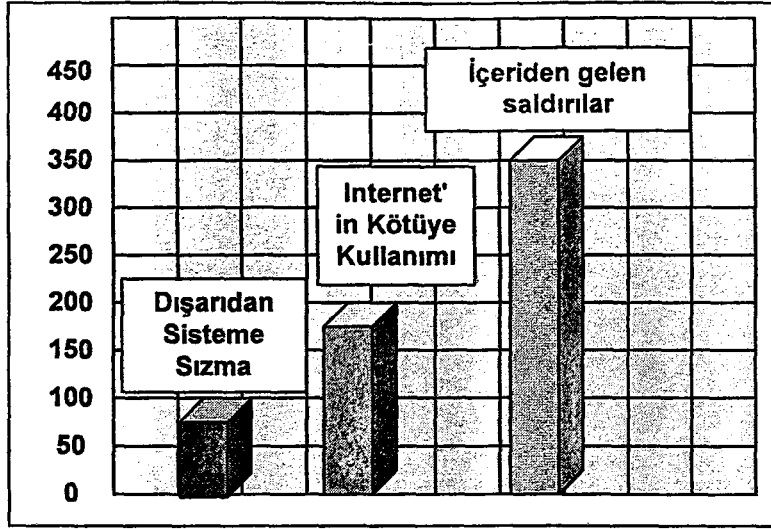
7.2 Endüstriyel Kurumların Tecavüzkar Saldırı Çekincesi

7.2.1 Saldırılarda gözlenen artış

Bugünün bilgi sistemlerinde, kurumların sistem saldırılarına uğraması kaçınılmazdır. 1998 yılında CSI tarafından yapılan bir araştırmaya göre, sistemlere yapılan saldırılar bir yıl içerisinde %16 oranında artmıştır. Bu araştırmaya göre, saldırılar içerisinde kurum içi saldırılar %70' in üzerinde oran tutmaktadır. Ayrıca 1997 yılına göre kurum içi saldırılar %22 oranında artmıştır. FBI bilgisayar suçları ekibi 1998 yılında yaptığı açıklamasında, "Kurumların ticari rakiplerinin kiraladığı saldırganlar, kolaylıkla kurum ağlarına sızmakta ve istediklerini almaktadırlar." demektedir.

7.2.2 Kurum içi saldırıların maliyetinin diğerlerine oranla daha yüksek olması

Geçen yıllarda içeriden, kurumun kendi kullanıcılarından gelen saldırılar ve internet' in kötüye kullanımındaki artış, dışarıdan gelen saldırılardaki düzenli artışa karşı baskın gelmiştir. Şekil 7.1' deki grafikten de görülebileceği gibi, içeriden gelen saldırılar üçte bir, internet' in kötüye kullanımı ikide bir oranında, dışarıdan gelen tehlikelerden baskın çıkmıştır.



Şekil 7.1 1998 CS/FBI çalışması saldırı ve kötüye kullanım tipleri

7.2.3 Kurum içerisinde insandan fazla bilgisayarın olması sonucu riskin artması

Bir kurumun büyüklüğü arttıkça, bilgisayarlar, web sunucuları ve yönlendirici vb. ağ araçlarının artması sonucu olarak daha karmaşık bir ağ yapısının ortaya çıkması, hem ağın yönetimini zorlaştırmakta, hem de sistem içerisindeki tecavüzkar saldırıyı sezme ve önlemeyi zorlaştırmaktadır. Firmaların bilanço bilgilerine takip edebilecek sayıda elaman istihdam edememesinin sonucu olarak, en azından başarıyı artırmak için bilanço ve kayıt tutma mekanizmaları etkisiz kılınabilmektedir.

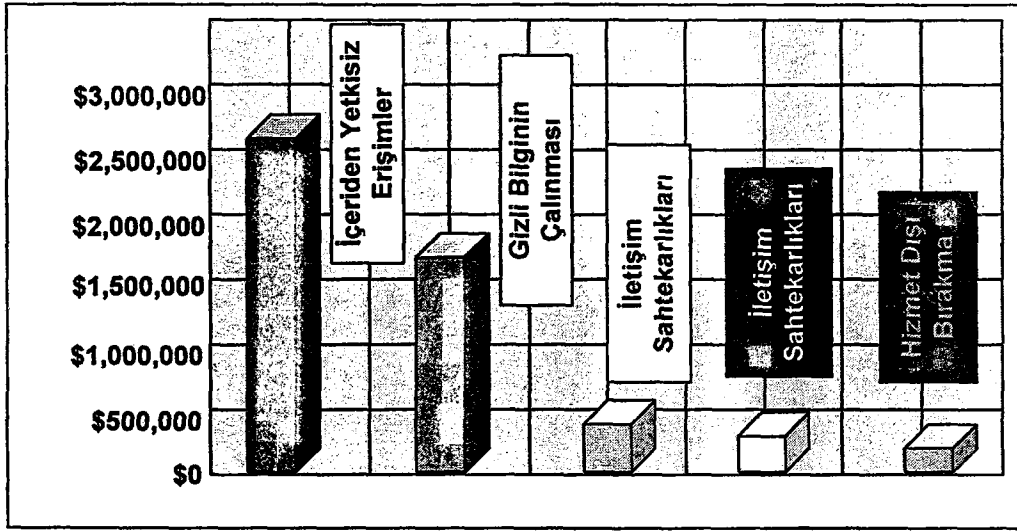
7.2.4 Sisteme yetkisiz erişimin insanlarda bir zevk haline dönüşmesi

Kısa bir zaman öncesine kadar sisteme saldırı düzenleme, çok uzun zaman ve emek isteyen bir işti. Fakat şimdi internet üzerinde "hacking, password cracking, Internet security" vb. sözcüklerle arama motorlarında yapacağınız bir arama sonucunda, UNIX ve Windows NT gibi işletim sistemlerinin nasıl ele geçirileceğine, aşama aşama anlatan belgeleri içeren sitelere dahi ulaşabilirsiniz. Bu sitelerde sistemi saldırı gerçekleştirmede kullanılacak programlar, araçlar bulmak mümkündür. CSI ve FBI' nın bilgisayar suçları ve güvenlik başlığı altında yaptığı araştırmada şöyle denilmektedir:

"Sisteme içeriden gelen tehlikelerde herhangi bir azalma kaydedilmemiştir. Fakat dışarıdan internet bağlantılarıyla gelen tehlikelerde artış gözlenmektedir."

7.2.5 Güvenlik tehditlerini umursamamanın pazar üstünlüğünü kaybettirmesi

Şekil 7.2' deki çizimde, CSI ve FBI' nın ortak çalışmasında güvenlik tehditlerine karşı önlem alınmamasının yarattığı finansal zararlar gösterilmektedir.



Şekil 7.2 1998 CS/FBI bilgisayar suçları ve internet güvenliği

7.3 Geleneksel Saldırı Sezme Sistemleri

Geleneksel saldırı sezme sistemleri aşağıdaki şekillerde karşılaşırlar:

- Çevre temelli izleme ve kontrol aletleri (firewall' lar ve yönlendirciler vb.).
- Ağ temelli trafik izleyicileri.
- Konak temelli bilanço hareketleri izleyicileri.

7.3.1 Çevre temelli izleme ve kontrol aletleri

Firewall ve yönlendirici gibi aletler, dışarıdan gelecek saldırılara karşı ilk koruma noktasını oluştururlar. Bu ürünlerin korumadaki etkinliği, nasıl tasarlandığı, yapılandırıldığı ve ağ üzerinde nasıl gerçekleştirildiğine bağlıdır. Firewall ve yönlendirciler, istenmeyen ağ trafiği ve ağ saldırılarını engelleyecek şekilde yapılandırılabilirler. Ancak, genellikle sisteme saldırı durumunda uyarı verme yeteneklerine sahip değildirler. Üstelik bu aletler içeriden gelecek tehlikelere karşı herhangi bir koruma sağlayamazlar.

Ağ güvenliği açısından düşünüldüğünde, firewall' lar saldırı sezme sisteminden ziyade bir erişim kontrol aleti olarak düşünülürler. Ancak, uygun bir şekilde yapılandırıldığında, paket temelli saldırılara karşı hatırı sayılır bir sezgi yeteneği sergilerler.

7.3.2 Ağ temelli trafik izleyicileri

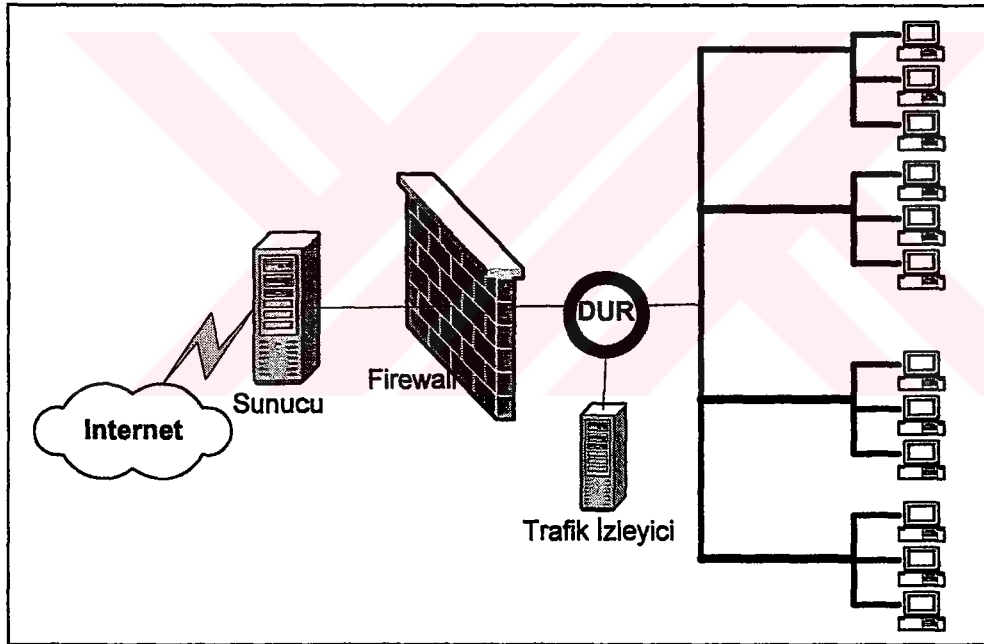
Ağ temelli trafik izleyicileri tek bir ağ bölümünde hareket eden bilgi paketlerini izlemek üzere, adanmış bir sisteme gereksinim duyarlar. Trafik izleyici yazılımları ağı dinleyerek elde ettiği paketlerin IP taklidi, bozuk paket ve paket bombardmanı

gibi ağ saldırılarına ait olup olmadığını, yapay zeka teknikleri kullanarak algılayan bir motora sahiptirler. Motor herhangi bir saldırı izine rastladığında, saldırıyı engellemek üzere elektronik posta, cep telefonuna mesaj, bağlantıyı kesme vb. uyarı ve eylemleri gerçekleştirir. Ağ temelli trafik izleyecilerinin saldırı sezmesindeki başarı derecesini belirleyen iki önemli nokta, saldırı sezme sisteminin saldırı imzaları taşıyan bir veritabanı ve bu veritabanının belirli aralıklarla güncellenmesidir.

Paket izleyicilerinin genellikle yerleştirildikleri ağ konumları aşağıda listelenmiştir:

1. Firewall'ın arkasına,
2. Önemli göreve sahip sunuculara,
3. İşlem yönlendicilerine,
4. Sunucu fabrikalarına (server farms) ve anahtar çalışma gruplarına (workgroups).

Trafik izleyicilerin tipik bir gerçekleşme şekli, Şekil 7.3' de görünmektedir.



Şekil 7.3 Ağ temelli saldırı sezme yöntemi

Ağ temelli trafik izleyicilerin sağladığı avantajlar arka sayfada listelenmiştir:

- Hizmet dışı bırakma saldırılarını (kapı tarama, ping saldırısı, SYN saldırıları gibi) hedef alan ağ izleyecilerinin daha önceden sisteme tanıtılmış paket katmanını hedef alan saldırı imzalarını izleyebilmektedir.
- Paketleri cepte tutma ve saklama gibi özellikleri olmadan, sadece paketi alıp ilettiğinden başarımlı düşümüne neden olmaz.

- Çoğu ağ temelli saldırı sezme sistemleri, saldırıları sezmenin yanında saldırılara cevap verme yeteneklerine de sahiptirler.
- Yeni nesil ağ temelli saldırı sezme sistemlerinde kullanıcılar kendilerine özel saldırı imzalarına tasarlayabileceklerdir.

7.3.3 Konak temelli bilanço kaydı izleyicileri

Tekil sistem ve yönetici/ajan olmak üzere, iki farklı bilanço kaydı izleyicileri vardır. Tekil sistemde bilanço kaydı izleyicisi, sadece tek makineyi, o makine üzerindeki kayıtlardan saldırıları sezerek korur.

Yönetici/ajan sistemde ise, ağ üzerinde korunacak tüm konaklara bir ajan yerleştirilir. Bu ajanlar ile yöneticiler arasında bağlantı kurulur, sonrada tüm sistem merkezi bir ekrana bağlanır. Bu yapıda ajanlar, üstünde çalışmakta olduğu sistemin bilanço kayıtlarını toplayarak, yöneticilere gönderirler. Böyle bir yapıda güvenlik mühendisi, tek bir merkezi noktadan kurallar tanımlama ve bunlara tüm sisteme dağıtma olanağına sahip olur.

Sistem üzerinde herhangi bir şüpheli olayla karşılaşıldığında, saldırı sezme yazılımı, kullanıcı hesabını etkisiz kılma, elektronik posta gönderme, cep telefonuna mesaj gönderme, bağlantıyı kesme vb. eylemleri gerçekleştirirler.

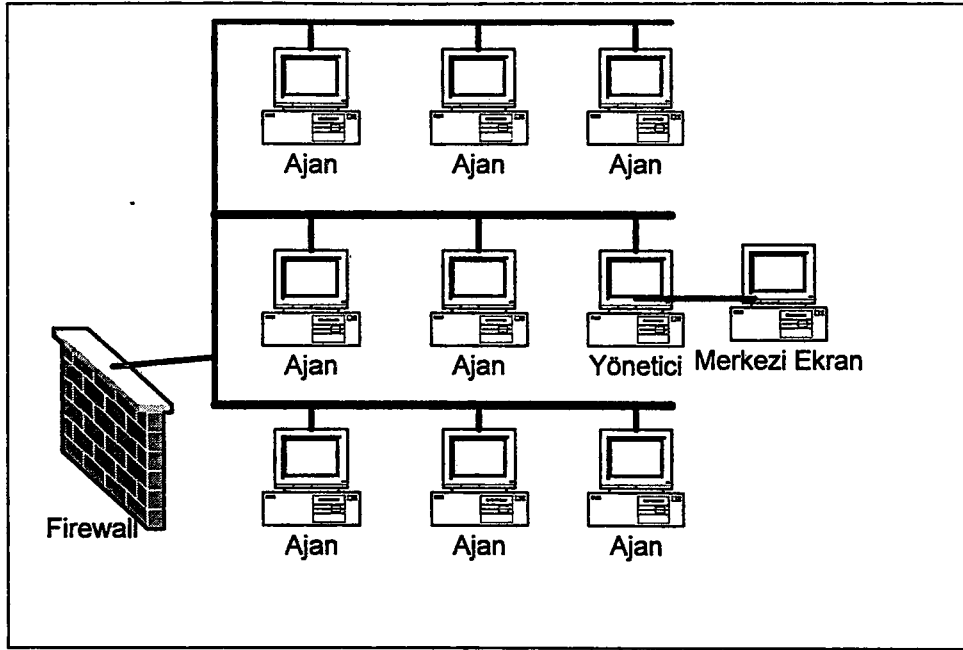
Şekil 7.4' de gösterimi yer alan, bu tarz bir saldırı sezme sisteminin başarıya ulaşmasında dikkat edilmesi gereken faktörler aşağıda listelenmiştir:

- Ölçeklenebilirlik,
- Çoktürel (Heterogeneous) ortamlarda çalışabilirlik,
- Sistem başarımına tehlikeye düşürmeyecek yük dengesinin sağlanması.

Konak temelli bilanço kayıt izleyicilerinin sağladığı avantajlar, aşağıda listelenmiştir:

Konak temelli saldırı sistemi, kuruluşun bilanço kayıtlarını inceleme ve değerlendirmede karşılaştığı güçlükleri ortadan kaldırmaktadır. Çoğu zaman böyle bir ürün alımı, bilanço kayıt yönetiminin merkezileştirilmesi ve azaltılması yoluyla maliyette indirim sağlar.

Diğer bir fayda ise, sistem yöneticisinin kayıtlar üzerinde, sistem üzerinde gerçekleşmiş olayları izlemek ve saldırı tiplerinin ait kayıt desenlerini çıkarmak üzere geçmişe yönelik tarihsel değerlendirmeler gerçekleştirebilmesidir.



Şekil 7.4 Konak temelli bilanço kaydı izleyicileri

7.4 Saldırı Sezme Sistemlerinde Düşünülmesi Gereken Önemli Elemanlar

Saldırı sezme sistemlerinde düşünülmesi gereken önemli elemanlar, aşağıda listelenmiştir: [20]

- Yetenek seviyesi,
- Cevap verme mekanizmaları,
- Sezilemeyen saldırılar ve yanlış sezgiler,
- Ölçeklenebilirlik ve ortamları kapsayabilirlik (platform coverage),
- Merkezi yönetim,
- Başarım.

7.4.1 Yetenek seviyesi

Saldırı sezme sistemleri ile ilgili cevaplandırılması gereken soru, hangi saldırı tiplerini yakalayabildikleridir. Yetenekli bir saldırı sezme sisteminin, diğer ölçütleri de sağlaması gerekir; fakat tanıyabildiği saldırı tiplerinin genişliği en önemlisidir.

Sürekli yeni saldırı tiplerinin çıkması, saldırı sezme sistemlerinin bir uzman sisteme veya veritabanına sahip olması gerekliliğini doğurmuştur. Böylelikle yeni çıkan saldırı tipleri, yazılım kodu üzerinde herhangi bir değişiklik yapmadan sisteme tanıtılabilir.

Tablo 7.1' den de görüleceği gibi, etkin saldırı sezme sistemi hem konak, hem de ağ temelli saldırı sezme yöntemlerini kullanmalıdır. Paket izleyicileri hizmet dışı bırakma gibi bazı saldırıları mükemmel bir şekilde sezebilmelerine rağmen, birçok diğer saldırı konaklarda mükemmel bir şekilde sezilmektedir. Bu konudaki genel kural, saldırının en iyi şekilde, saldırının hedefine yakın ortamların izlenmesiyle seziyeceğidir. Kısacası verilerin saklandığı ortam konak olduğuna göre, birçok saldırının hedefi konaklardır. [20]

Tablo 7.1 Saldırı sezme sistemlerinin saldırı aileleri açısından karşılaştırılması

Saldırıları	Paket İzleyicileri	Konak Temelli Saldırı Sezme Sistemleri
Hizmet Dışı Bırakma	Mükemmel Çözüm	İyi Çözüm
Araştırma ve Tarama	Mükemmel Çözüm	Kötü Çözüm
Şifre Saldırıları	Mümkün	İyi Çözüm
İmtiyaz Yakalama		Mükemmel Çözüm
Zararlı Kod Ekleme	Mümkün	Mükemmel Çözüm
Siber Vandallık	Mümkün	Mükemmel Çözüm
Gizli Bilgi Hırsızlığı		İyi Çözüm
Sahtekarlık, İsrar ve Kötüye Kullanmak		İyi Çözüm
Sistem Bilanço Kayıtlarının Kurcalanması	Mümkün	Mükemmel Çözüm
Güvenlik Yöneticisi Saldırıları		Mükemmel Çözüm

Milli Güvenlik Acentası (National Security Agency)' nın 1996 yılında yaptığı araştırmada, "Düzensizlik Sezme (Anomaly Detection)" ve "Kötüye Kullanım Sezme (Misuse Detection)" olarak adlandırılan iki önemli saldırı sezme yaklaşımı tanımlanmıştır. 1996 yılında, UC Davis INFOSEC Üniversitesi Araştırma Programı' ndan Nicholas J. Puketza, bu iki yaklaşımı şöyle tanımlamaktadır:

“Düzensizlik sezme yaklaşımı, saldırıya maruz kalan bilgisayar sisteminin, normal bir sistemden farkedilebilir derecede farklı olması gerçeğini temel alır. Kötüye kullanım sezme yaklaşımında ise, saldırı sezme sistemi özel ve açıkça temsil edilen bilgisayar sistemi kötüye kullanım tekniklerinin belirtisini arar.”

7.4.2 Cevap verme mekanizmaları

Sezilen saldırıya karşı verilecek önerilen cevap şekilleri aşağıda listelenmiştir:

- Saldırının gerçekleştiği oturumu sonlandırma.
- Elektronik posta veya SMS yoluyla mesaj gönderme.
- Sürekli izlenen bir ekrana alarm mesajı gönderme.
- Ağ hizmetlerini durdurma. Bu seçenek saldırı sezme açısından hem faydalı hem sakıncalıdır. Saldırı gerçekleştiği anda, saldırıyı önlemek açısından sistemin hizmetini durdurmak yarar sağlayacaktır. Fakat bu sistemin kandırılması durumunda saldırı sezme sistemi, hizmet dışı bırakma saldırılarını gerçekleştiren bir saldırgan aracı haline dönüşebilir.
- Ağ üzerinde meydana gelen olay ve eylemleri kaydetme.
- Komut çalıştırma ve kod parçası koşturma.

7.5 Sezilemeyen Saldırıları ve Yanlış Sezgiler

Pfaff ve Newsham saldırı sezme sistemleri ile ilgili yayınlamış oldukları makalesinde ağ merkezli saldırı sezme sistemlerinin gizli saldırı ve yanlış sezgilere aşırı bir şekilde maruz kalabileceğine işaret etmektedir. Bu savların dayanak noktası iki önemli faktördür:

“(1) Ağda kullanılan makinelerde gerçekleşen olaylar hakkında çıkarımlar yapacak kadar, bilgi mevcut değildir. (2) Sistemlerin edilgen olması gerçeği, doğal olarak hatalara açık kapı bırakır.”

Genellikle, saldırganlar ağ merkezli saldırı sezme sistemlerinden, temel paket mimarisi ilkelerini istismar ederek sıvışırlar. Bir saldırganın saldırı sezme sistemlerinden nasıl sıvıştığını gösteren üç tane örnek aşağıda listelenmiştir:

1. Paket içeriğini değiştirerek,
2. Saldırı elamanlarının sırasını değiştirerek,
3. Saldırı sistemini aşırı yükleyecek kadar gürültü oluşturarak.

Yanlış sezgide de, yine saldırgan paket mimarisini istismar ederek alışılmış, zararsız yanlış alarmlar oluştururlar ve sonunda şüpheli olmayan kişinin saldırı sezme sistemini kapatmasına neden olurlar.

Bu tarz saldırılara karşı alınacak önlem, paketin hizmet dışı bırakma saldırısının normal bir ağ trafiğinden ayıran verilerin bulunduğu, başlık kısmını incelemek olacaktır.

7.5.1 Ölçeklenebilirlik ve ortamları kapsayabilirlik

İyi bir saldırı sezme sistemi modeli, mimarisinde aşağıda listelenen faktörleri içermelidir:

- Girişim(enterprise) genişliğinde ölçeklenebilirlik. Saldırı sezme sistemi, girişim sınırları içerisindeki tüm sistemleri, sistemin büyüklüğü ve coğrafik sınırlarını dikkate almaksızın izleyebilmelidir.
- Çoklu ağ bölmeleri. Saldırı sezme sistemi girişim içerisindeki tüm ağ bölmelerini olası güvenlik tehlikelerine karşı düşünmelidir.
- Şalterlenmiş (switched) ve ATM ağ işlevselliği. Bir saldırı sezme sistemi modelinin uzun vadede başarılı olması için, bağlantıdaki ileri kavramları göz önüne alması gereklidir. Bugün ağ temelli saldırı sistemleri, her iki ağ altyapısında da çalışmaktadır.

Birçok büyük ölçekli kuruluşlar, birden fazla işletim sistemi kullanmaktadır. Dolayısıyla uygun saldırı sezme sisteminin çoklu ortamlardan veri toplama ve bilgileri özetleyerek yönetilebilecek tek bir çözüm oluşturma yeteneğine sahip olması gereklidir.

7.5.2 Merkezi yönetim

Kuruluşun tümünü etkin bir şekilde izleyebilmek için, akıllı bir saldırı sezme sistemi, güvenlik eylemlerini tek bir noktadan izlemeli ve düzenlemelidir. Merkezi bir ekranda elde edilen verilerden çizilen gerçek zamanlı çizimler, kuruluş bazında meydana gelen tüm güvenlik olayları için başvuru kaynağı oluşturur. Böyle bir başvuru kaynağı, güvenlik mühendisine, sistemi saldırılara karşı izlemesi olanağını sağlar.

Bir saldırı sezme sisteminde, görüntüleme programı ile motor programını ayırma kararı verilirken kullanılan dört önemli faktör aşağıda listelenmiştir:

1. Görüntüleme programı etkisiz kılınsa bile, sistemin çalışmaya devam etmesi gereklidir.

2. Çoklu motor tek bir görüntüleme programından kantarılmalıdır.
3. Ayrı bir görüntüleme programı sistemin uzaktan yönetimini mümkün kılar.
4. Ayrı bir görüntüleme programı sistem ve ağ araçları ile bütünleşme sürecini verimlileştirir.

7.5.3 Başarım

Ağ izleyecileri bazı paket tabanlı saldırı sezmelerine rağmen, içerik taramada sık sık başarım sorunlarıyla karşılaşır. Çünkü konak bağlamını yeniden oluşturmaya teşebbüs ederler. Aşağıda 60k paket büyüklüğünde, saniyede 64 sekizli paket çalıştıran, tek bölmeli, bir ağ izleyicisi ile elde edilen başarım değerleri gösterilmektedir:

- %20 ağ kullanımı.
- %40 kullanımda işlev durdurdu.
- Arka plandaki ağ trafiğini kotaramadı ve kendi kendine hizmet dışı bırakma saldırısı gerçekleştirdi.
- Ağ üzerindeki trafik patlamaları sırasında, hizmet dışı bırakma saldırılarını başlatan, bilinen saldırı desenlerini kotaramadı.
- Şalterlenmiş (switched) ve ATM ortamlarında çalışamadı.
- Şifrelenmiş veriyi göremedi.

Konak izlemede, gelen tüm paketleri izlemeye çalışan konak ajanları merkezi işlem birimini aşırı yükler. Buna rağmen konak ajanları, ağ izleyecilerde konak bağlamının oluşturulmasına göre daha az başarım kaybına neden olurlar.

8 GÜVENLİK POLİTİKASI

8.1 Giriş

Güvenlik politikası, kurumun ağırları içerisindeki korunacak varlıklar, bu varlıkların karşı karşıya oldukları tehlikeler ve bu tehlikelere karşı alınacak önlemleri belirler. Güvenlik politikası ile kurum çalışanları, maruz kalabilecekleri tehlikeler konusunda bilgilendirilirler ve üzerlerine düşen sorumlulukların farkına varırlar.

İyi bir güvenlik politikası oluşturmak, kurumun karşı karşıya olduğu tehlikelerin doğru bir şekilde belirlenmesine bağlıdır. Diğer bir deyişle, başarılı bir güvenlik politikasının oluşturulması, kuruma ait bilgisayar sistemlerinin maruz kalabileceği tehlikelerin, bu tehlikelerin sebep olabileceği maliyetin ve bunlara karşı alınabilecek önlemlerin neler olduğunun doğru belirlenmesine bağlıdır. Güvenlik politikasının başarısını sağlayan diğer bir faktör ise, yönetim desteğidir. Yönetim tarafından desteklenmeyen ve kapsamında belirlenen sorumlulukların gerektiği gibi yerine getirilmediği, güvenlik politikalarının başarıya ulaşmaları beklenemez. Tüm bunlara ek olarak, bir güvenlik politikasının başarıyla uygulanması için, etkin bir kurum içi iletişim gereklidir.

Kurumca kabul edilen bir güvenlik politikasına, tüm kurum çalışanlarının uyması ve oluşan ihlallere sebep olan kişilerin işten çıkarma ve hakkında yasal işlem başlatmaya varan cezalara çarptırılması gereklidir.

8.2 Güvenlik Politikasının Özellikleri

- Kolaylıkla anlaşılır bir yazım dili kullanılmalıdır.
- Aranılan bilgilere erişim kolay olmalıdır.
- İlk yazıldığı halin ve izleyen güncellemelerin tarihleri ve sürüm bilgileri belirtilmelidir.
- Kurum bünyesinde güvenlik ile ilgili resmi başvuru belgesi olarak kabul edilmelidir.
- Sistemin güvenliğinin sağlanması için gerekli vazgeçilmez doğruları belirlemelidir.

- Kavramlar açık, doğru ve anlaşılır şekilde kullanılmalıdır. Kavramların açıklanmasında kullanılan sözcükler doğru seçilmelidir.
- Bilgi sistemleri ile ilgili diğer temel kuralları içeren belgelerin, temel belgesi olarak düşünölmelidir.
- Güvenlik politikası, sistem güvenliğı açısından yapılması gerekenlerin yanısıra, yapılmaması gerekenleri de içermelidir.
- Güvenlik politikasının içeriğı, tüm kurum çalışanlarına duyurulmalıdır. Ayrıca, kurum çalışanlarına nasıl duyurulacağı ile ilgili de bir bölüm içermelidir.
- Değışen ihtiyaçlara göre, gerekli durumlarda güvenlik politikasında güncellemeler yapmak gereklidir. Bu güncellemelerin ne kadar sıklıkla ve ne şekilde yapılacağı güvenlik politikası belgesinde belirtilmelidir.

8.3 Temel Yaklaşım

Güvenlik politikası ve prosedürlerini belirlemek, gerçek anlamda bilgisayar güvenliğı ile ilgili neler yapacağımıza dair bir planın geliştirilmesini kapsar.

Bu konuda aşğıdaki gibi bir plan geliştirilebilir:

- Korunması gereken varlıkların belirlenmesi.
- Varlıkların kimlere karşı korunacağını belirlenmesi.
- Sistemin karşı karşıya olduğı olası tehditlerin belirlenmesi.
- Ağ güvenliğini sağlayacak etkin önlemlerin belirlenmesi.
- Güvenlik politikası ve prosedürlerinin sürekli olarak gözden geçirilmesi ve gerekli göröldüğünde güncellenmesi.

Uygulanabilir bir güvenlik politikası, veriyi korumanın maliyetinin verinin değerinden yüksek olmadığı politikalaradır.

Güvenlik politikası oluştururken dikkate alınması gereken gerçekler aşğıda listelenmiştir:

- Güvenlik politikası kurumun amaçları gözetilerek düzenlenmelidir. Kurumun vermiş olduğı hizmet cinsine ve yapısına göre güvenlik politikası da değışecektir.
- Güvenlik politikası kurumun uymak zorunda olduğı yasalar, kurallar ve düzenlemeler ile ihtilaf oluşturmamalıdır.

- Güvenlik politikasında, yerel ağlar ve dış ağlar bir bütün olarak düşünülmelidir.

8.3.1 Güvenlik politikası kimler tarafından belirlenir?

Güvenlik politikası, politikanın oluşturulmasının ve uygulanmasının gerekliliğini kavramış olan teknik eleman ve politikanın uygulamaya konulmasına yetkili karar alıcılardan oluşan bir grup tarafından belirlenmelidir.

8.3.2 Güvenlik politikası kimleri kapsar ve sorumluluklar nedir?

Güvenlik politikası kurum bünyesinde çalışanların tümünü kapsar. Örneğin, bilgisayar kullanıcıları, bilgisayarlarına, güvenlik açığı oluşturacak yazılımlar kurmamak ve şifrelerini korumak gibi sorumluluklara sahiplerken, sistem yöneticileri, güvenlik açıklarını belirlemek, kapamak, sisteme karşı geliştirilen saldırıları sezmek ve engellemek gibi sorumluluklara sahiptirler.

Güvenlik politikasının başarıya ulaşmasında, belirlenen sorumlulukların doğru kişilere atanması büyük öneme sahiptir. Bir güvenlik politikasının başarıya ulaşması, herkesin üzerine düşen sorumlulukları, harfiyen yerine getirmesine bağlıdır. Bir güvenlik politikası, olası tüm güvenlik sorunlarına çözüm bulmaktan ziyade, bu sorunların herbiri ile ilgilenecek kişileri belirlemeyi amaçlar.

8.4 Tehlike Değerlendirmesi

Tehlike değerlendirme, kurumun tehdiye açık varlıklarının, bu varlıkları tehdit eden kişilerin, varlıkların bu kişilerden nasıl korunacağını belirlenmesini ve tüm bu işlemlerin oluşturduğu zararın tespiti içerir.

8.4.1 Varlık tespiti

Tehlike değerlendirmesinde, kurumun korunması gereken varlıklarının belirlenmesini içeren süreçtir. Tehlikelere karşı korunması gereken varlıklar aşağıda listelenmiştir:

1. Donanımsal varlıklar: İşlemci, anakart, klavye, ekran, kişisel bilgisayar, sunucu, sabit disk, iletişim kabloları, yönlendirici, modem vb.
2. Yazılımsal varlıklar: Kaynak programlar, nesne yazılım kodları, uygulama araçları, işletim sistemleri.
3. Veri: Alınmış yedekler, veritabanları.
4. İnsan: Kullanıcılar, sistemin çalışmasında gerek duyulan tüm çalışanlar.

8.4.2 Tehditlerin tespiti

Korunması gereken değerlerin tespiti tamamlandıktan sonra yapılması gereken, bu değerlerin maruz kalabileceği tehditlerin tesbitidir. Aşağıda maruz kalınabilecek tehditlerden bazıları listelenmiştir:

- Yetkisiz giriş,
- Bilginin açıkta bırakılması,
- Hizmet dışı kalma.

8.4.3 Maliyeti hesaplamak

Güvenlik önlemleri, özellikle basit kullanıcılar için kullanılabilirliği azaltır. Güvenlik, işlerin gerçekleşmesini erteleyebilir; yönetim ve eğitim açısından büyük bir gider oluşturabilir. Aynı zamanda, büyük miktarda bilgisayar kaynaklarını tüketir ve adanmış donanım gerektirebilir.

Güvenlik tedbirlerinizi tasarladığınızda, ortaya çıkan maliyeti ve bu maliyet karşısında elde edeceğiniz ihtimal dahilinde olan kazançları tartmalısınız. Bunu gerçekleştirmek için, bir yanda başlı başına güvenlik önlemlerinin maliyetini görmeli, bir yanda da güvenlik olmadığı zaman ortaya çıkabilecek kayıpların maliyetini düşünmelisiniz. Eğer güvenlik önlemlerinin maliyeti güvenlik olmadan olabilecek maliyetleri aşmakta ise, güvenlik önlemleri olmadan gitmeyi tercih etmek daha mantıklı olacaktır.

8.5 Güvenlik Politikasının Önemli Noktaları

Bir güvenlik politikası geliştirilirken belirlenmesi gereken bir çok önemli nokta bulunmaktadır. Bunlar aşağıda inceleneceklerdir:

- Kaynakları kullanmaya kimler yetkilidirler? Güvenlik politikasında, kaynaklara kimler tarafından, hangi erişim yetkileri ile erişilebileceği belirtilmelidir.
- Kaynakların doğru kullanımı nasıldır? Kaynakları kullanım hakkına sahip kişilerin, kaynakları nasıl kullanması gerektiğinin belirlenmesi gereklidir. Farklı kişilerin aynı kaynaklar üzerinde, farklı yetkilere sahip olabilirler. Bir güvenlik politikası, yapılabileceklerin yanısıra, yapılamayacakları da içermelidir. Buna ek olarak, güvenlik politikasında, kaynakların kullanım şekillerinin, kullanıcının sorumluluğu altında olduğu belirtilmelidir. Ayrıca, güvenlik politikasında belirtilen kuralların ihlal edilerek, güvenliğin aşılmasının, yine güvenlik politikasınca yasaklandığından iyice bahsedilmelidir.

- Kim sistem yöneticisi haklarına sahip olabilir? Güvenlik politikasında kullanıcılara, kurumun verdiği hizmetlere erişim ve kullanım hakkını verecek bir kişinin belirlenmesi gereklidir. Kullanıcılara, sisteme erişim hakkı verme yetkisine sahip olanların sıkıca kontrol edilmesi gereklidir. Aksi takdirde, sistemin kimler tarafından kullanıldığı kontrol edilemez.

Sisteme gelen saldırıların büyük bir yüzdesinin iç kullanıcılardan geldiği düşünüldüğünde, sistem yöneticilerinin seçiminde çok dikkatli davranılmalıdır. Yerel kullanıcıların haklarının sınırlandırılması, yerel kullanıcılardan gelecek tehlikeleri engelleme yöntemi olarak kullanılmalıdır.

Buna ek olarak, özel haklara sahip kullanıcı hesaplarına sahip olanların, sorumluluk duyacakları bir makam olmalıdır ve bu güvenlik politikasında belirtilmelidir. Aksi takdirde, sistem üzerinde kontrol kaybedilir ve güvenlik tehdidinin kaynağını bulmak zorlaşır.

- Kullanıcıların hakları ve sorumlulukları nelerdir? Güvenlik politikası, kullanıcıların, kurumun bilgisayar sistemlerini ve hizmetlerini kullanırken, ne tür haklara ve sorumluluklara sahip olduğunu açık bir şekilde ifade etmelidir. Kullanıcı hakları ve sorumlulukları belirlenirken göz önünde bulundurulması gerekenler aşağıda listelenmiştir:

1. Kullanıcılar, kullanıcı hesaplarını paylaşabilir veya diğer kullanıcıların kendi hesaplarını kullanmasına izin verebilir mi?
2. Önemli yetkiye sahip kullanıcılar şifrelerini nasıl saklamalıdır?
3. Kullanıcılar şifrelerini ne kadar sıklıkla ve hangi şartlarda değiştirmelidir?
4. Yedekleme işlemi bir merkezden mi gerçekleştirilecek yoksa her kullanıcı kendi yedek alma işleminden mi sorumlu olacaktır?
5. Gizli bilgiler erişime açık bulunabilirler mi?

- Sistem yöneticisinin kullanıcılara karşı sorumlulukları ve hakları nelerdir? Güvenlik politikası, sistem yöneticisinin sorun çözmeye yönelik, ya da başka bir amaçla kullanıcılara ait dosyaları, ne dereceye kadar inceleme yetkisine sahip olduğunu ve kullanıcılara verilmiş hakları tanımlamalıdır. Burada cevap verilmesi gereken sorular şunlar olabilir:

1. Sistem veya güvenlik yöneticisi herhangi bir sebepten dolayı kullanıcı dosyalarını gözetleyip okuyabilir mi?

2. Engeller nelerdir?
3. Ağ yöneticisi ağ trafiğini izlemeye yetkili midir?

8.6 Ağ Sunucularının Güvenliğinin Sağlanması

8.6.1 Güvenli bir geçiş planının oluşturulması

Ağ sunucularının gerçek ortam yerleşimi gerçekleştirilmeden önce güvenilir bir şekilde yapılandırılması, daha sonradan oluşabilecek birçok sorunu ortadan kaldırmaktadır. Genellikle sunucuların varsayılan yapılandırmaları sistemin tüm özelliklerini içermektedir. Bu nedenle, sistem üzerinde güvenliği tehlikeye düşürecek yapılandırmaların üzerinde değişiklikler yapmak gereklidir. Bu değişikliklerin önceden oluşturulan kapsamlı bir geçiş planı çerçevesinde yapılması, sistem üzerinde ulaşabilecek gedikleri en aza indirecektir.

Güvenli bir sistem oluşturmada ve sistemin güvenliğinin devamında tutarlılık faktörü büyük rol oynamaktadır. Aynı zamanda tutarlılık, oluşabilecek güvenlik sorunlarının tespitinde büyük kolaylıklar sağlamaktadır.

Güvenli bir geçiş planının gerçekleştirilmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir. [21]

- Her bir bilgisayarın kullanım amacını tanımlayınız.
- Bilgisayar üzerinde çalışan ağ hizmetlerini belirleyiniz.
- Bilgisayar üzerinde kurulu ağ yazılımlarını belirleyiniz.
- Bilgisayar kullanıcıları veya kullanıcı kategorilerini belirleyiniz.
- Bilgisayar üzerinde kullanıcı kategorilerinin sahip oldukları imtiyazları belirleyiniz.
- Kullanıcı kimliğinin nasıl doğrulanacağına ve kimlik doğrulama verisinin nasıl korunacağına karar veriniz.
- Bilgi kaynaklarına uygun erişimin nasıl zorlanacağını belirleyiniz.
- Bilgisayarlar için saldırı sezme yöntemlerini geliştiriniz.
- Bilgisayar üzerinde saklanan bilgileri yedekleyiniz ve onarımı ile ilgili yordamları belgeleyiniz.
- Çeşitli hatalardan sonra ağ hizmetlerinin bakımının ve yeniden eski haline getirilmesinin nasıl sağlanacağını belirleyiniz.

- İşletim sistemi kurulumu ile ilgili yordamların geliştirilmesi ve kurulumun bu yordamlara göre yapınız.
- Bilgisayarın ağa nasıl bağlanacağına karar veriniz.
- Bilgisayarın günlük yönetimi ile ilgili güvenlik meselelerini belirleyiniz.
- Artık kullanımda olmayan makinelerde bilgi güvenliğini tehlikeye düşürecek bilgilerin korunmasına ilişkin eylemleri tanımlayınız.
- Bilgisayar geçiş planını güncel tutunuz.

8.6.2 Sunucu seçiminde göz önüne alınması gereken güvenlik gereksinimleri

Bilgisayar teknolojilerinin seçiminde genel olarak işlevsellik , fiyat , performans ve kapasite gibi etkenler dikkate alınmaktadır. Bunlara ek olarak, kurumunuz için gerekli sunucunun seçiminde, güvenlik gereksinimlerinin kullanılması şarttır.

Ürünlerinin güvenlik yetenekleri değişen birçok satıcı vardır. Bilinen ağ saldırıların çoğu belirli işletim sistemleri ve uygulamalarına gerçekleştirilmektedir. Sunucu seçiminde güvenlik gereksinimleri bir ölçüt olarak kullanıldığında, güvenlik gedikleri daha az olan ve daha az saldırı gerçekleştirilmiş sunucuların seçilmesi uygun olacaktır. Bu şekilde sistem yönetiminin ve saldırılarla uğraşmanın yaratacağı maliyet en aza indirileceğinden, ekonomik olarak uygun karar verilmiş olacaktır.

Güvenlik gereksinimlerinin içeriği aşağıdadır:

1. Sunuculara karşı yapılan, bilinen saldırı biçimlerinin oluşturduğu güvenlik gediklerinin olmaması.
2. Sistem yönetimi işlemlerinin sadece bir yetkili kullanıcı ile sınırlanabilmesi yeteneğine sahip olunması.
3. Sunucu üzerindeki bilgilere yetkisiz erişimin engellenebilmesi.
4. İşletim sistemi veya sunucu yazılımının kurduğu gereksiz ağ hizmetlerinin kaldırılabilme yeteneğine sahip olunması.
5. Çalışabilir programlara yapılabilecek erişim isteklerinin kontrol edilebilmesi yeteneğine sahip olunması.
6. Sistem saldırıları sezme amaçlı olarak, uygun sunucu hareketlerin kaydedilebilmesi yeteneklerine sahip olunması.

Sunucu seçiminde izlenecek yol ve göz önüne alınacak ölçütler aşağıda listelenmiştir: [21]

- İşlevsellik ve başarımlar gereksinimlerini belirlemek.
- Yapılandırma ve sunucu ürününün çalışmasını gösteren uygulamaları incelemek.
- Kurumun güvenlik ihtiyaçlarına göre, seçilecek sunucuda olması istenecek güvenlik ile ilgili özellikleri belirlemek.
- Olay verilerinin oluşturduğu mevcut kaynaklar kullanılarak, özel tipte olayların ve belirli sunuculara ait güvenlik gediklerinin sezilebilme olasılığını belirlemek.
- Kurumun işlevsellik, başarımlar ve güvenlik gereksinimlerini karşılayacak aday ürünleri belirlemek.
- Olası güvenlik olaylarının oluşturacağı iş bedeli ve ürünün işletiminde harcanacak emek doğrultusunda, aday ürünlerin işletme giderleri arasındaki farkları tahmin etmek.
- Genel maliyet, işlevsellik, başarımlar ve güvenlik açısından en iyi çözüm sunacak teknolojiyi seçmek.

8.6.3 İşletim sistemi ve uygulama yazılımlarının güncel tutulması

Kullanmakta olduğunuz ürünün satıcısı tarafından ürün ile ilgili yapılan güncellemelerin yakından takip edilmesi gereklidir. Ürüne yeni bir eklenti çıkarıldığında, bu eklentinin kurum tarafından incelenmesi ve eğer kurum sistemi için uygulanabilir ise kurulması gereklidir.

Yazılım sistemlerinin çok karışık olması, güvenlik ile ilgili sorunların genelde, yazılım geniş kitlece kullanıma geçtikten sonra bulunması sonucunu doğurmaktadır. Satıcılar güvenlik gediklerini tam vaktinde giderme çabasında olmalarına rağmen, her zaman sorunun ortaya çıkışı ile çözümü arasında bir zaman farkı vardır. Bu zaman aralığı olası bir saldırıya, güvenlik açığından faydalanarak sisteme karşı bir saldırı düzenleme şansını vermektedir. Bu zaman aralığının mümkün olduğu kadar kısaltılabilmesi için şu işlemler gerçekleştirilmelidir:

- Kurumun sistemine uygulanabilecek güvenlik sorunları ile ilgili duyuruları yakından izlemek.
- Etkilenen yazılımın kaldırılması gibi güvenlik açığından etkilenme oranını azaltacak acil önlemleri almak.
- Satıcı tarafından dağıtılan yamaları yakından takip etmek.

İşletim sistemleri ve uygulama yazılımlarının güncel tutulması için izlenmesi gereken aşamalar arka sayfada listelenmiştir: [21]

- Kullanılan sistem ve uygulama yazılımlarının yazılım güncellemeleri ve güvenlik sorunları ile ilgili bilgi kaynaklarının listesini oluşturmak ve bakımını sağlamak.
- Bu bilgi kaynaklarını izleyecek yordamları oluşturmak.
- Ürün güncellemelerinin sisteme uygulanabilirliğini değerlendirmek.
- Uygulanabilir güncellemelerin kurulumunu planlamak.
- Güncellemeleri belgelenmiş bir plan doğrultusunda kurmak.
- Yeni bilgisayarların gerçek ortama geçişini, güncellenmiş yazılım ile gerçekleştirmek.
- Bilgisayarın yapılandırması ve bilgi içeriğinde bir değişiklik yaptıktan sonra, yeni kriptografik kontrol toplamı (checksum) ve tutarlılık kontrol bilgilerini oluşturmak.

8.6.4 Sunucu makinesi üzerinde sadece gerekli ağ ve işletim sistemi hizmetlerinin sunulması

Herşeyin mükemmel olduğu bir ortamda, her bir ağ hizmeti kendisine adanmış tek amaçlı bir konak üzerinde çalışmalıdır. Birçok bilgisayar varsayılan olarak özel bir ağ hizmetinin gerektirdiğinden daha geniş uygulama ve hizmet ile yapılandırıldığından, bu hizmetleri elemek ve ortadan kaldırmak için, bilgisayarı yeniden yapılandırmak gereklidir.

Herhangi bir konak üzerinde sadece gerekli ağ hizmetlerinin çalıştırılması güvenliği birçok yönden artırır: [21]

1. Diğer gereksiz hizmetler kullanılarak sisteme saldırıda bulunulamaz.
2. Farklı hizmetler farklı sistem yöneticileri tarafından işletilebilir. Hizmetleri farklı konaklarda çalıştırarak sistem yöneticileri arasında oluşacak anlaşmazlıklar ortadan kaldırılır.
3. Konak üzerinde çalışan hizmetlinin gerektirdiği en uygun ayarlar ile yapılandırılabilir. Aynı konak üzerindeki farklı hizmetler, güvenlik açıkları oluşturabilecek farklı uygulama ve farklı donanım ayarları yapılandırılırlar.

4. Hizmet sayılarının azalması ile, kütük sayıları ve kütük içerisindeki giriş sayıları azalır ve sistem üzerindeki olağan dışı durumların sezilmesi kolaylaşır.

İş ihtiyaçlarını karşılayacak en az hizmet yapılandırması içerecek işletim sistemi yapılandırmasının sağlanmasında izlenmesi gereken aşamalar aşağıda listelenmiştir:

- Ağ sunucusu ile desteklenmesi tasarlanan işlevleri belirlemek.
- Aynı işlevi sağlamanın daha güvenli bir yolu varsa, onu seçmek.
- Konak için gerekli en küçük hizmet ve uygulama kümesine belirlendikten sonra, konak üzerinde sadece o kümeyi çalıştırmak.
- Gereksiz tüm açık ağ kapılarını kapamak.
- Bilgisayar üzerindeki tüm yapılandırmaları yaptıktan sonra, yeni kriptografik kontrol toplamı ve tutarlılık kontrol bilgilerini oluşturmak.

8.6.5 Bilgisayarlar üzerinde kullanıcı kimlik doğrulama yapılandırmasının yapılması

Bir kurumun güvenlik politikası çerçevesinde, bilginin güvenliği açısından bilgisayarlara, sadece üzerinde işlem yapma yetkisine sahip kullanıcılarca ulaşılması gereklidir. Bu amaca, bilgisayarın kullanıcı kimlik doğrulaması gerçekleştirecek şekilde yapılandırılmasıyla ulaşılır.

Bir bilgisayarın kimlik doğrulama yapacak şekilde yapılandırılması, işletim sistemi, donanım veya uygulama yazılımları üzerinde yapılandırma değişiklikleri gerektirebilmektedir. Kimlik doğrulama sunucusunun kullanılması, ayrı bir bilgisayar üzerinde de yapılandırma değişiklikleri gerektirecektir. Ayrıca özel durumlarda kimlik doğrulama için tek zamanlı şifre, token ve biyometrik aletler kullanılmaktadır.

Kimlik doğrulama politikasının uygulanmasında izlenmesi gereken aşamalar aşağıda listelenmiştir: [21]

- Eğer mevcutsa, sistem donanım tabanlı erişim kontrol mekanizmaları kullanacak şekilde yapılandırılmalıdır.
- Gereksiz kullanıcı hesap ve grupları sistemden silinmelidir.
- Etkileşimsiz hesapları iptal edilmelidir.

- Eriřim haklarını, ayrı ayrı kullanıcıları vermek yerine, her bilgisayar için bir kullanıcı grubu yaratıp, kullanıcıyı bu gruba atmak ve gerekli hakkı gruba vermek tercih edilmelidir.
- Uygun bir řifre politikası oluřturulmalı ve kullanıcıların bu politikaya uyması saęlanmalıdır.
- Bilgisayarlar iřlemsiz geen belirli bir sreden sonra yeniden kimlik doęrulama iřteęinde bulunacak řekilde yapılandırılmalıdır.
- Bilgisayarlar kk sayıda bir hatalı sisteme baęlanma denemesinden sonra sisteme baęlanma iřteęini reddedecek řekilde yapılandırılmalıdır.
- Kurumun ihtiyalarına gre SSL veya SSH gibi dięer kimlik doęrulama mekanizmalarını kullanmak gereklidir.
- Aę sunucuları için, eęer mevcut ise, aę hizmet yazılımının sunduęu kimlik doęrulama yntemleri kullanılmalıdır.

8.6.6 İřletim sisteminin uygun nesne, alet ve dosya eriřim kontrolleri ile yapılandırılması

Eriřim kontrollerinin dikkatli bir řekilde yapılandırılması, kasıtlı veya kasıtsız olarak oluřabilecek gvenlik gediklerinin kapanmasında nemli rol oynar. rneęin, bir belgeye okuma eriřim yasaęının konulması, bilginin gvenilirlięini saęlarken, yazma yasaęının konulması bilginin tutarlılıęını saęlar.

Saęlıklı bir eriřim kontrol yapılandırmasının saęlanması için, ařaęıdaki ařamaların izlenmesi gereklidir: [21]

- Bilgisayar zerinde yer alan tm nesneler için gerekli korumaları belirlemek.
- Gerekli kullanıcı gruplarını yaratmak.
- Eriřim kontrollerini yapılandırmak.
- nemli veriler için dosya řifreleme yeteneklerini kurmak ve yapılandırmak.

8.6.7 Sistem ve aę kayıt mekanizmalarının alıřtırılması

Sistem, aę, uygulama ve kullanıcı hareketleri sonucu retilen verilerin toplanması ve analiz edilmesi, saldırıların sezilmesi ve varlıkların gvenlięinin saęlanması aısından byk nem tařır. Kayıt dosyaları sistem zerinde gemiř hareketler ile ilgili bilgileri iermekte olup, oęu zaman řpheli durumların tek belirleyicileridir. Kayıt dosyalarının faydaları ařaęıda listelenmiřtir: [21]

1. Sistem üzerinde meydana gelen şüpheli durumların sezilmesi, kayıt dosyaları üzerinde yapılan analizler sonucu belirlenirler.
2. Saldırganın sistem üzerinde gerçekleştirdiği eylemlerin ayrıntısının belirlenmesinde kullanılırlar.
3. Sistemin herhangi bir sorun sonrası, yeniden eski haline getirilmesinde kullanılırlar.

İyi bir kayıt planının oluşturulmasında izlenecek aşamalar aşağıda listelenmiştir:

- Kaydı tutulacak bilgileri belirlemek.
- Sistem ve ağ tarafından sağlanan kayıt mekanizmalarının yeterli olup olmadığını belirlemek, eğer yeterli değil ise ek araçlar kullanmak.
- Sistemin kayıt tutma yeteneğini aktif etmek.
- Kayıt bilgilerinin güvenliğini sağlamak.
- Kayıt dosyalarının kotarılmasında kullanılacak yönetim planını belgelemek.

8.6.8 Bilgisayar dosya yedekleme mekanizmalarının yapılandırılması

Meydana gelen güvenlik saldırılarından sonra sistemin eski haline dönmesi için, dosya yedekleme mekanizmalarının kullanımı kaçınılmazdır. Bir sistem hatası veya güvenlik saldırısı sonucu zarar görmüş bir sistemin, yedek olmadan eski haline dönmesi imkansızdır.

İyi bir yedekleme sisteminin kurulmasında izlenmesi gereken aşamalar aşağıda listelenmiştir: [21]

- Dosya yedekleme ve onarım planı oluşturmak.
- Dosya yedekleme araçlarını kurmak.
- Yedekleme araçlarını yapılandırmak ve zamanlanmış yedekleme işlemlerini başlatmak.
- Zamanlanmış yedekleme işlemlerinin doğru bir şekilde gerçekleştiğini teyit etmek.
- Yedeklerde geriye dönebilme yeteneğini denemek.

8.6.9 Bilgisayarların virüs ve benzeri programsal tehditlerden korunması

Bilgisayar güvenliğine zarar veren birçok tip program vardır. Genel olarak, bu programlar üç farklı sınıfta toplanırlar:

- **Virüs:** Kendisini diğer programlara ekleyerek çoğalan bir kod parçacığıdır. Virüsler ya doğrudan veriye zarar verirler, ya da sistem başarımını düşürerek, sistemin yetkili kullanıcılara hizmet vermesini engellerler.
- **Kurtçuk (Worm) :** Genellikle ağ üzerinde, kendisini bir sistemden diğer sisteme kopyalayarak çoğalan programlardır. Aynı virus gibi, ya doğrudan veriye zarar verirler , ya da sistem başarımını düşürerek, sistemin yetkili kullanıcılara hizmet vermesini engellerler.
- **Truva atı (Trojan horse) :** Kendini yararlı bir işlev görüyormuş gibi gösteren, fakat içersinde zararlı bir programı saklayan bağımsız programlardır. Yetkisiz kullanıcı bu işlevi çalıştırdığında, truva atı da yetkisiz işlemleri yerine getirecektir.

Programsal tehditler sisteme bilginin izlenmesi, çalınması ve değiştirilmesi, bilgisayar yapılandırmalarının değiştirilmesi ve neticede saldırının oluşması gibi çok önemli zararlar verebilirler. Aynı zamanda, programsal tehditlerin sebep olduğu yıkımların örtülmesinin de maliyeti büyüktür. Bu nedenledir ki, programsal tehditlere karşı iyi bir korunma sistemi oluşturmak gereklidir. Böyle bir sistemin oluşturulmasında izlenecek aşamalar aşağıda listelenmiştir:

- Bilgisayarları programsal tehditlerden koruyacak bir plan geliştirmek. .
- Uygun virüs temizleme (anti-virus) yazılımlarını kurmak ve çalıştırmak.
- Kullanıcıları virüsten uzak durma ve tanıma konularında eğitmek.
- Belirli zaman aralıklarıyla, tehdit sezme araçlarını denetlemek ve güncellemek, özellikle yeni bir tehdit bulunduğunda.

8.6.10 . Bilgisayarların uzaktan güvenli sistem yönetimi için yapılandırılması

Bir iş istasyonunun veya ağ sunucusunun yönetimi, kullanıcı hesap bilgilerinin güncellenmesi, kayıtların incelenmesi, yeni veya güncellenmiş yazılımların kurulması ve uygun yapılandırmaların sağlanması gibi işlemleri içerir. Bu işlemler, ya yerel olarak makine üzerinde, ya da makineye uzaktan erişim gerçekleştirilerek gerçekleştirilir. Yerel yönetim tamamen güvenli olmasına rağmen, maliyet açısından uzaktan yönetim daha çok kullanılmaktadır Uzaktan erişimde maruz kalınabilecek güvenlik tehlikeleri iyi bir uzaktan erişim planını gerektirmektedir. Bu planın aşamaları aşağıda sıralanmıştır:

- Bilgisayara sadece kimliği doğrulanmış sistem yöneticisinden, sistem yönetim komutlarının sağlandığını garanti etmek.
- Bilgisayarın sistem yönetimine, sadece kimliği doğrulanmış konak üzerinden izin verdiğini garanti etmek.
- Tüm sistem yönetim işlemlerinin en düşük imtiyaz seviyesinde çalıştığını garanti etmek.
- Gizli bilginin saldırgan tarafından kesilemediğinden, okunamadığından veya değiştirilemediğinden emin olmak.
- Doğrulanmış kopyadan, firewall dışındaki açık sunuculara veri iletimi sağlayacak taşınabilir saklama birimleri kullanmak.
- Tüm kayıt dosyalarını incelemek için güvenli bir yöntem kullanmak.
- Bilgisayar üzerindeki tüm yapılandırmaları yaptıktan sonra, yeni kriptografik toplam kontrolü ve tutarlılık kontrol bilgilerini oluşturmak.

8.6.11 Bilgisayara sadece uygun fiziksel erişimlere izin verilmesi

Yetkisiz bir kullanıcı bir bilgisayara fiziksel olarak erişebiliyor ise, bu sistemin bütünlüğünün tehlike altında olduğu düşünülebilir. Özellikle sistem iç ağına bağlı ise, saldırgan tüm koruma ölçütlerini aşarak kaynaklara erişebileceğinden tehlike daha büyüktür. Bu nedenle verinin var olabilirliğini ve güvenilirliğini korumak için bilgisayar ve saklama birimini yetkisiz kullanıcıların faaliyetlerinden uzak tutmak gereklidir. Bunun sağlanması için gözetilmesi gereken hususlar aşağıda listelenmiştir:

- Yetkisiz donanım kurulumunu ve yetkili donanımların değiştirilmesini engellemek.
- Bilgisayar geçişlerinde güvenli faaliyetler kullanmak.

8.7 Web Sunucu Güvenliğinin Sağlanması

8.7.1 Web sunucusunun genel ağlar ve kurumun iç ağlarından ayrılması

Kurumsal ağ içerisinde web sunucusu yerleştirmek için, birçok seçeneğiniz vardır. Web sunucusunun korunulan ayrı bir alt ağda yerleştirilmesi uygundur. Böylece, internet ile sunucu arasındaki trafik hiç bir şekilde iç ağdan geçmeyecek ve iç ağ dışarıdan tamamen ayrılmış olacaktır.

Web sunucusu dünyanın dört bir yerinden istemcilerin erişeceği, genel erişim için planlanmış bir konaktır. Konak ve üzerinde çalışan programlar, ne kadar iyi

yapılandırılırsa yapılandırılın, her zaman yeni bir gedik bulmak ve sunucuya yetkisiz erişim kazanmak şansı vardır. Bu şans gerçek olursa, ilişkili olarak gerçekleşme ihtimali doğan olayların gerçekleşmemesi için aşağıdaki olayların engellenmesi gerekir: [22]

1. Saldırgan iç konaklar arasında akan ağ trafiğini gözleyebilir veya yakalayabilir. Bu trafik kimlik doğrulama bilgisi , tescilli iş bilgisi , kişisel veri vb. bilgiler içerebilir.
2. Saldırgan iç konakları ele geçirebilir ve onlar hakkında geniş bilgi sahibi olabilir . İç ağı bu iki tehdite karşı korumak için, güncel web sunucusunu, iç ağ ve iç ağ trafiğinden ayırmak gereklidir.

Bunu gerçekleştirmek için izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Web sunucusunu genel ve iç ağlardan ayrı bir alt ağa yerleştiriniz.
- Web sunucusu ile iç ağlar ve genel ağlar ile web sunucusu arasındaki trafiği engellemek için firewall teknolojisini kullanınız.
- Hizmet sağlayan sunucu konağı, genel ve iç ağlardan ayrılan, diğer bir alt ağa yerleştiriniz.
- Genel web sunucusunu koruyan tüm firewall ve yönlendiricilerde kaynak yönlendirmeyi etkisiz kılınız.
- Destekleyeci hizmet veren sunucular ve web sunucusundaki IP ileletme ve kaynak yönlendirmeyi etkisiz kılınız.

8.7.2 Web sunucusunun uygun nesne , alet ve dosya erişim kontrolleri ile yapılandırılması

Web sunucu ve konak işletim sistemlerinin çoğu, konak üzerinde saklanan dosyalar, aletler ve diğer veriler veya kod nesneleri için, erişim imtiyazları tanıma yeteneğine sahiptirler. Web sunucusu bu erişim kontrolü ile erişebileceği tüm bilgileri, web sunucusuna erişebilecek tüm kullanıcılara dağıtabilir.

Genel web sunucularında saklanan bilgileri koruyacak erişim kontrollerinin en iyi nasıl yapılandırılacağına iki açıdan düşünülmesi gerekir:

1. Web sunucu yazılımlarının erişimleri sınırlandırılmalıdır.
2. Web sunucusuna özel erişim kontrolleri uygulanmalıdır. Erişim kontrollerinin uygun kurulması, genel dağıtım için planlanmayan hassas ve kısıtlanmış bilgiyi yetkisiz erişimlerden önler.

Genel web sunucuları, genellikle herkese yayına açık bilgileri saklarlar. Bunun yanında aşağıdaki gibi kısıtlanmış erişim gerektirmeyen bilgileri barındırırlar: [22]

- Sunucu kayıt dosyaları,
- Sistem yazılımı ve yapılandırma dosyaları,
- Uygulama yazılımı ve yapılandırma dosyaları,
- Şifre dosyaları ve yapılandırma dosyaları.

Hem işletim sistemleri hem de web sunucu yazılımları tarafından sağlanan erişim kontrollerinin kullanımı, gizlilik ve bütünlüğün ihlal edilmesi, bilgilere zarar verilmesi olasılıklarını azaltır. Buna ek olarak, kaynaklara erişimi sınırlayacak erişim kontrolleri, hizmet dışı bırakma (DOS) saldırısı ve hazır bulunabilirliğin ihlali etkilerini azaltır.

Uygun erişim kontrollerinin oluşturulmasında izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Web sunucusunu, tek kişisel kullanıcı ve grup kimliği altında işletecek şekilde yapılandırınız.
- Web sunusuna özel nesneler , aletler ve dosyalar için gerekli korumaları tanımlayınız.
- Hizmet dışı bırakma saldırılarının etkisini azaltmak için, web sunucu konak işletim sisteminin kaynak kullanımını sınırlayınız.
- Hizmet dışı bırakma saldırılarının etkisini azaltmak için, vazgeçme süresi (time- out) ve diğer kontrolleri yapılandırınız.
- Web sunucusunu dış kullanıcıları açılması düşünülmeyen dosya dizini ağaçlar dışında kalan dosyaları, dış kullanıcılara sunmayacak şekilde yapılandırınız.
- Web sunucusu yazılım erişim kontrollerini yapılandırınız.
- Web sunucu dosya izin listelerinin sunulmasını etkisiz kılınız.

8.7.3 Web sunucusuna özel kayıt mekanizmalarının tanımlanması ve etkin kılınması.

Web sunucusu tarafından üretilen verinin toplanması, saldırı izlerinin sezilmesi ve web sunucusunun güvenilirliğinin analizinde temel olan önemli bilgileri sağlar.

Web sunucu yazılımını kurduğunuzda, kurulum programı kayıt yapılandırma ile ilgili birçok seçenek sunar. Farklı sistemler, bir çok değişik tipte kayıt bilgisi sağlar; bazı sistemler varsayılan yapılandırmasında yeterli bilgiler içermezler.

Kayıt dosyaları sistem üzerindeki şüpheli davranışların tek kayıtlarıdır. Kayıt mekanizmalarının etkin kılınmasında ve buna bağlı olarak uyarı mekanizmalarının tetiklenmesinde yapılan hatalar, saldırı teşebbüslerinin ve saldırının başarıyla sonuçlanıp sonuçlanmadığının anlaşılması yeteneklerini bertaraf edecektir. [22]

Web sunucu kayıtlarına ihtiyaç duyulmasının nedenleri aşağıda listelenmiştir:

- Geniş inceleme gerektirecek şüpheli davranışların uyarılması.
- Saldırgan eyleminin uzantısının belirlenmesi.
- Sistemin onarılmasına yardım edilmesi.
- İncelemelerin idare edilmesine yardımcı olunması.
- Yasal takipler için gereken bilgilerin sağlanması.

Uygun bir kayıt mekanizması sağlamak için izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Kaydı tutulacak web sunucusu yazılım bilgilerini tanımlayınız.
- Programlar, kod parçaları ve plug -in' ler için ek kayıt mekanizmalarına gerek olup olmadığını belirleyiniz.
- Web sunucu kayıt tutma yeteneğini etkin kılınız.
- Web sunucu kayıt dosya analiz araçlarını seçiniz ve yapılandırınız.

8.7.4 Web Sunucusu için program kod parçaları ve plug-in'lerin seçiminde güvenlik imalarının düşünülmesi

En temel şekilde web sunucu talep için dinler ve istekleri istemciye istenen dosyayı göndererek yanıtlar. Herhangi bir isteğe cevap olarak programlar çalıştırıp, kullanıcılar tarafından sağlanan veriyi işleyerek, veri üretmede ek mekanizmalar kullanırlar. Bunlar aşağıda listelenmiştir:

- CGI (Common Gateway Interface): CGI özel bir URL'e, istekte bulunarak çağrılan dış programları ekleyerek, web sunucusu yazılım uzantısını destekleyen kabul edilmiş bir standarttır.
- Kod parçası (Script): VBScript, JavaScript, PHP vb. gibi programlama dillerinde yazılan ve bir yorumlayıcı tarafından çalıştırılan programlardır.

- Plug-in: Plug-in' ler diğ er bir programın uzantısı olarak hizmet verirler. Plug-in' ler ek bir işlevsellik (SSL gibi) veya iyileştirilmiş sunucu başarımı (PERL gibi) sağlarlar.

Güvenlik gedikleri, programların, kod parçalarının, plug-in' lerin kurulumu, yapılandırılması, geçişi ve işletiminde kolaylık oluşturulabilir.

Web sunucusu yöneticisi olarak, dış program ve web sunucu yazılım geliştiricileri tarafından denenmemiş bir yapılandırmada dış program kurabilirsiniz. Gedikler genellikle geniş ölçekli kullanım amaçlı olmayarak kötü yazılan veya aynı bilgisayar üzerinde kullanımı amaçlanmayan programların, aynı bilgisayar üzerinde kullanımı sonucunda oluşan yan etkiler nedeniyle ortaya çıkar. Örneğin, web siteleri üzerinde gerçekleş en başarılı saldırıların önemli bir bölümü, CGI kod parçaları üzerinde bilinen gediklerin kötüye kullanımı sonucu gerçekleş ir.

Web sunucusu için program kod parçaları ve plug-in' lerin seçiminde güvenlik imalarını düşünerek izlemeniz gereken yolun aşamaları aşağıda listelenmiştir:

- Dış program seçmeden önce gerekli maliyet ve fayda analizini gerçekleştiriniz.
- Güvenilir kaynaklardan sağlanan program, kod parçaları ve plug-in' leri kullanınız.
- Dış programın sağladığı işlevlerin tümünü anladığınızdan emin olunuz.
- Kullanmayı düşündüğünüz programdaki gedikleri belirlemek için mevcut bilgileri inceleyiniz.

8.7.5 Plug-in' ler, kod parçaları ve programların işlevselliğini azaltmak için web sunucusunun yapılandırılması

Plug-in' ler , programlar ve kod parçaları genel web sunucusuna değerli ve yararlı işlevler ekleyebilirler. Bunları web sunucusuna istediğiniz zaman, sunucu kodunu değiştirmeden ekleyebilirsiniz.

Bu programların oluşturduğu, sisteme karşı tehlikeleri azaltmak için izlemeniz gereken yöntemler aşağıda listelenmiştir: [22]

- Dış programın gerekli kopyasının, kimliği doğrulanmış kopya olduğunu onaylatınız.
- Kullanımı gerekli tüm programları kullanmadan önce, iç ağınızdan ayrı bir deneme makinesinde deneyiniz.
- Zaman kod dağıtma tehlikesini azaltır.

- Dış programlardaki gediklere maruz kalma ihtimalini sınırlayacak araçları çalıştırınız.
- Sunucu tarafı kod işlevselliklerinin kullanımını sınırlayınız veya etkisiz kılınız.
- Web sunucusu yapılandırmasında yer alan dış programların çalışmasını etkisiz kılınız.
- Dış programlara erişimi kısıtlamak için, web sunucusu konak işletim sistemi ve web sunucusu yazılım erişim kontrollerini yapılandırınız.
- Sadece yetkili kullanıcıların dış programlara erişebildiğinden emin olunuz.
- Web sunucusunu, dış programları tekil bir kişisel kullanıcı ve grup tanımlayıcısı altında çalıştıracak şekilde yapılandırınız.
- Dış programların erişimlerini sadece temel dosyalarla kısıtlayınız.
- Tüm dış programların kriptografik kontrol toplamalarını ve bütünlük denetleme bilgilerini oluşturunuz.

8.7.6 Web sunucusunun gerekli olduğunda kimlik doğrulama ve şifreleme tekniklerini kullanacak şekilde yapılandırılması

Web sunucusunun, bilgiye erişim için farklı imtiyazlı kullanıcıların tanınması ve kimlik doğrulamasında, bir dizi farklı teknolojileri desteklemesi gerekir. Bu teknolojilerin bazıları, web tarayıcı istemcisi ile web sunucusu arasında şifrelenmiş bir kanal sağlayan kriptografik işlevleri temel alırlar. SSI, SET, S1 ve HTTP gibi teknolojiler buna örnek olarak verilebilir.

Kullanılması gerekli kriptografi teknolojilerine karar veremede izlemeniz gereken adımlar aşağıda listelenmiştir. [22]

- Web sunucusu üzerinde yayınlanacak hassas ve kısıtlanmış bilgilerin erişim gereksinimlerini belirleyiniz.
- İstemci ve web sunucusu arasında güven oluşturulmasının önemini kavrayınız.
- Adres temelli kimlik doğrulamanın sınırlamalarını kavrayınız.
- Kimlik doğrulama, şifreleme teknolojileri ve herbirinin ne zaman kullanılması gerektiğini kavrayınız.
- Gizlilik gerektiği durumlarda web sunucusunu, SSL kullanacak şekilde kurunuz ve yapılandırınız.

- SSL sunucu anahtar ve sertifika isteđi oluřturunuz ve SSL sunucu anahtarınızı sertifika makamından sertifika almak üzere hazırlayınız.
- Eđer kullanıcı kimlik dođrulama gerekliyse, web sunucu yazılımını SSL temelli kimlik dođrulama kullanacak řekilde yapılandırınız.
- Kuvvetli bir kimlik dođrulamaya ihtiyaç duyulacaksa, web sunucu yazılımını SSL istemci sertifikası kullanımını destekleyecek řekilde yapılandırınız.
- Eđer kredi kartı bilgisi iletimi gerekliyse, web sunucusunu SSL veya SET kullanacak řekilde yapılandırınız.

8.7.7 Web sunucusunun ięeriđinin yetkili bir kopyasının güvenli bir sunucuda saklanması

Web sunucusundaki bilgilerin bütünlüğü bozulduğunda bilgiler, yetkili kopyadan güvenli iletişim kuralları bütünü ile yeniden kopyalanır.

Web sunucusunun ięeriđinin yetki kapsamının güvenli bir biçimde sağlanması için izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Web sunucusunun ięeriđinin yetkili kopyasına erişim hakkı olan kullanıcı sayısını kısıtlayınız.
- Web ięerik alt izinleri seviyesinde erişim kontrolleri gerçekleyiniz ve uygulanmasını sağlayınız.
- Yetkili kopyaya erişim hakkı vermeden önce kuvvetli bir kullanıcı kimlik dođrulama kullanımını mecbur kılınız.
- Web sunucusunu, yetkili kopyayı barındıran güvenli sunucu tarafından başlatılacak řifrelenmiş ve dođrulanmış bağlantıyı kabul edecek řekilde yapılandırınız.
- Ağ kullanım imkanı olmadığı durumda yetkili kopyayı taşımak için gerekli kurallar oluřturunuz.

8.7.8 Web sunucusunun bilinen saldırılara karşı korunması

Web sunucusunun bilinen saldırılara karşı korunması için yapmanız gerekenler aşağıda listelenmiştir:

- Güvenlik gedikleri ve olayları ile ilgili bilgileri düzenli olarak takip ediniz.
- Yeni saldırı ve gedikleri engellemek için güvenlik kontrollerinizi yenileyiniz.
- Uyarı prosedürlerinizi genişletiniz.

- Dağıtık hizmet dışı bırakma saldırılarının oluşturduğu zararlarda, kurumunuzu nasıl koruyacağınızı belirlemek için ağ sağlayıcınızla çalışınız.

8.8 Firewall' ın Gerçek Ortama Geçişi

8.8.1 Bir firewall sisteminin tasarlanması

Bir firewall sisteminin tasarlanması, bilgisayar ağlarındaki güvenlik alanları arasındaki sınırların belirlenmesini gerektirir. Bir ağ güvenlik alanı, tekil bir güvenlik politikası altında işletilen ağ bölgesidir. Bu güvenlik alanlarının kesişmesi durumunda güvenlik politikalarında çıkan sorunlar firewall teknolojisi kullanılarak aşılır.

Bir firewall sisteminin tasarlanmasında izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Ağ, ağ araçları, güvenlik alanları vb. parçalardan oluşan ortamınızı belgeleyiniz.
- Kullanacağınız firewall'ın işlevlerini belirleyiniz. Kullanabilecek firewall işlevleri, paket süzgeçleme, uygulama vekilleri, durumsal inceleme veya devingen paket süzgeçlemedir (bkz. firewall bölümü).
- Kullanacağınız firewall topolojisini seçiniz (bkz. firewall bölümü).
- Varolan firewall mimarisi seçeneklerini, başarımlı, hazır bulunabilirlik, güvenilirlik, güvenlik, maliyet, yönetilebilirlik, yapılandırılabilirlik ve işlevsellik ölçütlerini temel alarak karşılaştırınız.
- Firewall sisteminizi yetkisiz erişimlerden koruyunuz.

8.8.2 Gerekli firewall yazılım ve donanımının belirlenmesi

Uygun firewall yazılımı ve donanımının seçilmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir. [23]

- Firewall için, gerekli donanım bileşenlerini belirleyiniz.
- Firewall için, gerekli yazılım bileşenlerini belirleyiniz.
- Deneme (test) ortamı için, gerekli deneme bileşenlerini belirleyiniz. Firewall sistemini gerçek ortama geçirmeden önce tüm sistem denemelerinin yapılması, gerçek ortamda sorun çıkma olasılığını azaltacaktır.
- Firewall sisteminin gerçek ortama geçişini gerçekleştirmeden önce, gerekli yazılımsal ve donanımsal tüm sistem parçalarını edininiz.

8.8.3 Firewall ile ilgili teknik bilgiler içeren belgeler, eğitim ve teknik desteklerin edinilmesi

Tasarlanan firewall mimarisine göre, firewall sistemini gerçek ortama geçişinin gerçekleştirilmesinde, bazı eğitimlere ve/veya satıcının teknik desteğine ihtiyaç duyulabilir. Bir firewall' ın gerçek ortama geçiş işleminin gerçekleştirilmesi için ne gibi bilgi ve hizmetlere ihtiyaç duyulduğunun belirlenmesinde izleyeceğimiz aşamalar aşağıda listelenmiştir:

- Eğitim gereksinimlerinize karar veriniz. Örneğin TCP/IP, ağ mimarisi, ağ güvenliği, ağ izleme vb.
- İhtiyaç duyulacak teknik destek gereksinimlerine karar veriniz.

8.8.4 Firewall yazılımı ve donanımının kurulması

Firewall güvenliğinin kırılmasının ana nedeni, firewall sistemlerinin yanlış yapılandırılmasıdır. Sisteme sızma denemeleri, denenen firewall sistemlerinin yarısından fazlasının yanlış yapılandırıldığını göstermektedir.

Firewall sistemi ve üzerinde koştuğu işletim sisteminin gerekli en az hizmet yapılandırması ile yapılandırılmadığı ve gerekli eklentiler uygulanmadığı durumda,

- kurum ağınızın, eklentileri mevcut, bilinen saldırılara maruz kalması,
- satıcınızdan verimli bir teknik destek alamama,
- firewall yazılımını çalıştıracağınız kararlı bir sisteme sahip olamama,

tehlikeleri ile karşı karşıya kalırsınız.

Firewall yazılım ve donanımının kurulmasında izlemeniz gereken aşamalar aşağıda listelenmiştir: [23]

- İşletim sistemini bir firewall sistemi için kabul edilebilecek, en az hizmet yapılandırması ile kurunuz.
- Sisteme uygulanabilir tüm eklentileri kurunuz.
- Firewall sistemine kullanıcı ve konak erişiminde kısıtlamalar yapınız.
- IP iletme işlevini etkisiz kılınız.
- Sisteminizin yedeğini alınız.

8.8.5 IP yönlendirmenin yapılandırılması

Doğru ip yönlendirme yapılandırmasının gerçekleştirilebilmesi için izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Firewall sisteminin herbir arabirimi için, tekil bir ip numarası belirleyiniz.
- Yönlendirme yapılandırmasını gerçekleştiriniz.

8.8.6 Firewall paket süzgeçlemenin yapılandırılması

Paket süzgeçleme yapılandırmasının gerçekleştirilmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Paket süzgeçleme kurallarının kurum ağlarına verilmesi düşünülen hizmetlere göre yapılandırın.
- Belirlenen paket süzgeçleme kurallarını belgeleyiniz.
- Paket süzgeçleme kurallarını kurunuz.

8.8.7 Firewall kayıt tutma ve uyarı mekanizmalarının yapılandırılması

Kayıt tutma ve uyarı mekanizmalarının yapılandırılmasında izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Kayıt dosyalarının yeri, uzunluğu, kimlerin erişeceği, yedeklenmesi vb. ölçütlerce oluşan kayıt tutma ortamını tasarlayınız.
- Paket süzgeçleme kuralları ile ilgili kayıt tutma seçeneklerini seçiniz.
- Uyarı mekanizması yapılandırmalarını tasarlayınız.
- Kayıt tutma ve uyarı mekanizmalarına destek sağlayacak araçları geliştiriniz veya edininiz.

8.8.8 Firewall sisteminin denenmesi

Firewall sisteminin gerçek ortam geçirilmeden denenmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir: [23]

- Bir deneme planı hazırlayınız.
- Deneme işlemi gerçekleştirmek için, kullanılacak araçları edininiz.
- Deneme ortamınızda firewall işlevlerini deneyiniz.
- Gerçek ortamda firewall işlevlerini deneyiniz.
- Kayıt dosyaları ile ilgili özellikler seçip, deneyiniz.
- Firewall sistemini deneyiniz.
- Güvenlik gediği için, sistemi tarayınız.
- Sistem durumlarını gösteren veri kümeleri tasarlayınız.

- Sistemi gerçek ortamda kullanıma hazırlayınız.
- Sistemi sürekli izleyecek sistemler hazırlayınız.

8.8.9 Firewall sisteminin kurulması

Firewall sisteminin kurulmasında izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Yeni bağlantıyı kurunuz. Firewall' ın kurulması sırasında, firewall üzerinden süzgeçlenmeyen ağ trafiğinin geçmesini engellemek için, firewall sistemini kapatınız. Tüm kurulum ve yapılandırma işlemleri sona erdikten sonra sistemi yeniden başlatınız.
- Yeni sistemi kurarken, eski sistemin çalışmasına herhangi bir etkide bulunmamalısınız. Eğer yeni sistemin kurulumunda herhangi bir sorun ile karşılaşırsanız, eski sisteme geri dönünüz.

8.8.10 Firewall sisteminin işletim evresine geçirilmesi

Firewall sisteminin işletim evresine geçirilmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Firewall sistemlerinin değiştirilmesinde kullanılacak geçiş planını hazırlayınız.
- Firewall sisteminin işletimi geçtiğini kullanıcılara bildiriniz.
- Özel trafiğin firewall sisteminiz üzerinden geçmesini etkin kılınız.

8.9 Saldırlara Cevap Verilmesi

8.9.1 Saldırlara cevap vermek için politika ve yordamların oluşturulması

Güvenlik politikası, bir kurumun güvenlik hedeflerini gerçekleştirmek üzere bilgisayar kaynaklarını nasıl yöneteceğini ve koruyacağını düzenleyen kuralları tanımlar. Saldırıları cevap vermede en öncelikli amaç, korunulması düşünülen tehlikelerin ve başarılı bir saldırı karşısında yapılması gereken eylemlerin belirlenmesidir.

Belgelenmiş, duyurulmuş ve uyulmaya zorlanmış politikalar ve destekleyen yordamlar, saldırılara zamanında ve kontrollü bir şekilde cevap vermeyi sağlar. Bu politika ve yordamların oluşturulmasında izlemeniz gereken aşamalar aşağıda listelenmiştir: [24]

- Saldırlara cevap vermek için, yönetim seviyesinde sorunun ana hatları ve kurallarını oluşturunuz ve bunları kurumunuzun ağ sistemleri güvenlik politikası içerisine yerleştiriniz.

- Yedek sistem ve yedekleme politikalarını belgeleyiniz. Sisteme herhangi bir saldırı düzenlendiğinde, hasar gören sistemin yerini alacak yedek sistemlerin oluşturulması ve bilgilerin yedeklenmesi sistem devamlılığını sağlamak açısından önemlidir.
- Saldırıya cevap verme politikalarını gerçekleyen cevap verme yordamlarını belgeleyiniz.
- Oluşturulan politika ve prosedürlerin kanunlara uygunluğunu kontrol ediniz.
- Oluşturulan politika ve yordamların uygulanmasında görev alacak çalışanlara politika ve yordamlar konusunda eğitim veriniz.

8.9.2 Saldırlara cevap vermeye hazırlanılması

Saldırlara cevap vermek için hazırlanmak, cevap verme süreci içerisinde yararlanılacak ve saldırı ile ilgili verileri toplayacak ve düzenleyecek, araçların seçilmesi, kurulması ve bu araçlara aşına olunmasından ibarettir. Saldırıyı sezmeden önce, uygun veriye ve araçlara sahip olunmadığı durumlarda, saldırıya cevap vermede başarısızlığa uğranılabilir.

Saldırlara cevap vermeye hazırlanma işleminde izlemeniz gereken aşamalar aşağıda listelenmiştir: [24]

- Kullanılan tüm işletim sistemleri ve sürümleri için, açılış disketi ve kurulum dosyaları arşivi oluşturunuz.
- Tüm uygulamalar, işletim sistemleri ve sürümleri için, güvenlik ile ilgili eklentiler arşivi oluşturunuz.
- Yedekleme prosedürlerinizin sistemin uğrayacağı her türlü zararı onaracak kadar yeterli olup olmadığından emin olunuz.
- Sistemin beklenen durumları ile ilgili bilgi veren deneme sonuçlarının arşivini oluşturunuz.
- Sistem yedeklerinin alınması ve dönülmesinde kullanılmak üzere, yüksek hacimli, tak-çıkart, donanımsal yazma korumalı saklama ortamları ve destekleyici teçhizatların varlığından emin olunuz.
- Güvenli veri iletişim mekanizmaları kurunuz.
- Dizinler ve diğer temas bilgileri kaynaklarına erişimde kullanılacak araçları belirleyiniz ve kurunuz.

- Saldırlara cevap verme süreci içerisinde kullanılacak araçlar ve donanım aletlerinden oluşan bir kaynak takımı oluşturunuz.
- Deneme sistemi ve ağının doğru bir şekilde yapılandırıldığından ve hazır bulunabilir olduğundan emin olunuz.

8.9.3 Saldırının özelliklerini belirlemek üzere mevcut tüm verilerin analiz edilmesi

Saldırı sezme mekanizmaları tarafından sistemin saldırıya uğradığı belirlendiği zaman, sistem ve sistem üzerinde saklanan verinin, bu saldırıdan ne kadar etkilendiği belirlenmelidir ki, saldırıya ne ölçüde cevap verileceği belirlensin. Sistem üzerinde yapılan analizler sırasında elde edilen ve yorumlanan bilgiler, cevap verme sürecinde alınacak kararlar ve eylemlerde anahtar ölçüt olacaktır. Sistem üzerinde yapılan analizlerin amacı,

- Sisteme erişim sağlamada kullanılan saldırıların ne olduğunu,
- Saldırgan tarafından erişilen veriler ve sistemlerin hangileri olduğunu,
- Saldırganın sisteme erişim sağladıktan sonra ne yaptığını,
- Saldırganın şu anda ne yaptığını,

belirlemektir. [24]

Bir saldırıya karşı etkin önlemler alabilmek için, saldırının boyutunu, etki alanını iyice belirlemek ve yapılması gereken eylemlere öncelik kazandırmak gereklidir. Bunun gerçekleşmeside, sistem üzerinde gerçekleşen olaylara ilişkin mevcut tüm bilgilerin değerlendirilmesi ile mümkün olacaktır. Bu bilgilerin değerlendirilmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Yedekleme işlevlerinin gerçekleştirilmesi sırasında, saklanmayan veya kaybolan sistem bilgilerini yakalayınız ve kaydediniz.
- Saldırıya uğramış sistemin sakladığı bilgileri ve yapılandırmaları yedekleyiniz.
- Saldırıya uğramış sistem üzerinden almış olduğunuz yedek dosyalarını gerçek ortamdaki sistemden ayrı bir deneme sistemine alınız ve ana sistemle arasında bağlantı olmadığına emin olduktan sonra, değerlendirme işlemlerini gerçekleştiriniz.
- Diğer sistemlerde saldırı izlerini araştırınız.

- Ağ izleyicileri, yönlendiriciler ve firewall' lar tarafından tutulan kayıt dosyalarını inceleyiniz.
- Sisteminize erişim sağlayan saldırıyı tanımlayınız.
- Saldırganın sisteminize erişim sağlarken yapmış olduklarını belirleyiniz.

8.9.4 Saldırı ve saldırının gelişimden haberdar edilmesi gerekenlerin tümü ile iletişim kurulması

Saldırıya cevap verme sürecinde, anahtar görevleri olanların saldırı ile ilgili olarak zamanında bilgilendirilmesi, sorumlulukların uygun bir şekilde yerine getirmeleri açısından önemlidir. Yönetimin onayını gerektiren saldırı cevap vermede,

- Gediğin kapanıp kapanmaması ve işin devam edip etmemesi,
- Saldırganın eylemleri ile ilgili veri toplamaya devam edilip edilmemesi,
- Hangi tip ve miktarda bilgilerin iletilmesi,
- Kimlerin bilgilendirilmesinin gerektiği,

konusunda karar alınması gereklidir.

Saldırıya cevap verme süreci içerisinde görev alacak kişilerin zamanında bilgilendirilmemesi, sistemlerin, ağların ve verilerin büyük zararlara maruz kalmasına sebep olabilir. Hatta, saldırının uygun bir şekilde kotarılmadığının kamuoyu tarafından duyulması, kurumun finansal kayıplara uğramasına ve itibar kaybetmesine neden olabilir. [24]

Saldırıya cevap verme sürecinde görev alacak kişiler arasında etkin iletişimin sağlanması için izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Saldırının özelliklerini hesaba katarak, bilgi dağıtma kurallarınızı çalıştırınız.
- Güvenli iletişim mekanizmaları kullanınız.
- Sistemin, saldırı ile ilk ve en son temas edecek taraflarını bilgilendiriniz.
- Geniş içerikli temas kayıtları tutunuz.
- Sistem ve taraflarınızla ilgili şu anki temas bilgilerini içeren kayıtlar tutunuz.

8.9.5 Saldırı ile ilgili bilgilerin toplanması ve korunması

Saldırı ile ilgili elde edilen tüm verilerin toplanarak, güvenli bir ortamda saklanması, bu verilerin sistem güvenliğinden sorumlu elamanların eğitiminde kullanılması ve saldırının değerlendirilmesi açısından önemlidir. Bu bilgilerin toplanması ve güvenli bir ortamda saklanması için izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Saldırı ile ilgili mevcut tüm bilgileri toplayınız.
- Saldırı ile ilgili kanıtları toplayınız ve koruyunuz.
- Kanıtların güvenli bir şekilde yakalandığından ve korunduğundan emin olunuz.
- Saldırganın peşine düşmek ve hakkında yasal takipte bulunmak istiyorsanız, emniyet güçlerine başvurunuz.

8.9.6 Saldırıyı kontrol altına almak için kısa vadeli çözümlerin uygulanması

Kontrol altına alma, saldırganın sistem üzerinde daha büyük zararlar vermesine engellemek üzere alınan kısa vadeli önlemlerdir. Kontrol altına alma,

- Kullanıcılar, müşteriler ve/veya iş ortaklarının, sistemin beklenmedik olaylardan dolayı bir süre hizmet veremeyeceğinin duyurulması,
- İletişim araçlarının bir şey olduğu ile ilgili olarak uyarılması,
- Saldırganın, kendisinin ve sistem üzerinde gerçekleştirmekte olduğu eylemlerin farkedildiği konusunda uyarılması,

gibi eylemleri içerir.

Saldırıyla karşılaşıldığında uygulamaya alınacak kontrol altına alma süreci sırasında gerçekleştirilecek işlemler konusunda karar almada, hesaba katılması gerekli ölçütler aşağıda listelenmiştir:

- Saldırının genel değerlendirmesi.
- Değerlendirmelerden elde edilen diğer önemli bilgiler (saldırının kaynağı gibi).
- Kurumun cevap verme sürecini yöneten amaç ve öncelikleri.
- Kurumun iş devamlılığı planı.

Kontrol altına almanın ana hedefleri, sistemin karşı karşıya kaldığı sorunu sonradan değerlendirip, sistemin kontrolünü yeniden ele geçirip, sistemi normal haline döndürmek ve saldırganın sisteme erişimini engelleyerek, sisteme daha fazla zarar vermesini engellemektir.

Kontrol altına alma sürecinde izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Saldırıya uğramış sistemi geçici olarak kapatınız.
- Saldırıya uğramış sistemin, ağ ile olan bağlantısını koparınız.

- Eğer mümkünse, sistem hizmetlerini etkisiz kılınız.
- Şifreleri değiştiriniz ve kullanıcı hesaplarını etkisiz kılınız.
- Sistem ve ağ faaliyetlerini inceleyiniz.
- Yedek sistem ve verilerin saldırıdan etkilenmediğini teyit ediniz.

8.9.7 Her türlü saldırgan erişiminin engellenmesi

Sistemi daha önceden etkilemiş olan bir saldırı tipine karşı, sistemin bundan sonra güvende olduğu garanti edilmelidir. Sisteme birkez erişen saldırgan sisteme daha sonrada erişmek için çeşitli arka kapılar oluşturur. Bu arka kapıların mümkün olduğu derecede elenmesi için izlemeniz gereken aşamalar aşağıda listelenmiştir: [24]

- Saldırganın erişim sağlamış olduğu tüm sistemlerdeki şifreleri değiştiriniz.
- Saldırı öncesi sistemin tutarlılığını belirlemede kullanılacak bilgilerle ilgili hazırlıkları yapmadıysanız, sistemi tamamen yeniden kurunuz.
- Sistem üzerinde, saldırganın sisteme erişimine neden olacak tüm arka kapıları kapatınız.
- İkili (binary) dosyaları ve çalışabilir programları, asıl kurulum dosyalarından yeniden kopyalayınız.
- Sistem yapılandırmasının tutarlılığını belirlemek üzere, sistemi gözden geçiriniz.
- Sisteminiz güvenlik açıkları olup olmadığına ve bu açıkların kapatılıp kapatılmadığına karar veriniz.
- Sistemin ve ağın saldırılarla olan temasını sınırlamak için, koruma mekanizmalarınızı iyileştiriniz.
- Saldırıların daha iyi bildirimini sağlamak için, sezme mekanizmalarınızı iyileştiriniz.

8.9.8 Sistemin normal işletimine geri döndürülmesi

Saldırı sonucunda etkilenmiş bir sistemin normal haline döndürülmesi, çalışanların sisteme yeniden erişimlerini sağlamaktan ibarettir. Bu işlemin gerçekleştirilmesinde izlemeniz gereken aşamalar aşağıda listelenmiştir:

- Sistemi normal işletim düzenine getirmedeki gereksinimler ve zaman aralıklarını belirleyiniz.
- Kullanıcı verilerinin güvenilen yedekleme ortamlarından yeniden kopyalanız.

- Sistem ve uygulama hizmetlerini aktif ediniz.
- Yedeklerden dönülen sistemi ağa bağlayınız.
- Yedeklerden geri dönülen sistemin tutarlılığını teyit ediniz.
- Saldırganın geri dönüşünü işaretleyen olası izler için sistemi takip ediniz.

8.9.9 Öğrenilen güvenlik derslerinin tanımlanması ve gerçekleştirilmesi

Kurumlar karşılaşmış oldukları, saldırılardan bazı dersler çıkarmazlarsa, yine tehlike altında çalışma süreçlerini devam ettirirler ve aynı veya benzer saldırı tipleri ile tekrar tekrar uğraşmak zorunda kalırlar. Karşılaşılan saldırı olaylarından ders alma noktasında yapmanız gerekenler aşağıda listelenmiştir:

- Daha ileri tebliğlere gerek duyulduğunda, “Daha önce bağlantı kurduğunuz sitelere bağlanınız” gibi bir tebliğ yayınlayınız.
- Saldırının görünüşü ile ilgili süregelen bilgilendirmeleri yönetiniz. İlgili tüm tarafları, saldırı ve saldırının gelişimi konusunda bilgilendiriniz.
- Saldırı esnasında, sistemin ve sistemden sorumlu kişilerin, saldırıya karşı davranışlarını değerlendiriniz ve saldırıya cevap verme sürecine katılan tüm taraflarla yapılan görüşmeleri gözden geçiriniz.
- Saldırının yeniden meydana gelmesini engellemek için, güvenlik planlarını, politikalarını, yordamlarını ve kullanıcı ve sistem yöneticisi eğitimlerini yeniden gözden geçirip düzeltiniz.
- Saldırı şiddet ve etkilerini temel alan yeni bir tehlike değerlendirmesi gerçekleştirip gerçekleştirmeyeceğinize karar veriniz.
- Sistem ve ağ varlıklarının yeni bir sayım çizelgesini çıkarınız.
- Eğer uygulanabilir ise, bir soruşturma ve kovuşturma başlatınız.

9 BİLGİ GÜVENLİĞİNDE HUKUKSAL YAKLAŞIM

9.1 Giriş

Kamuoyunda açık ağ sistemlerine karşı güvenin sağlanması açısından, taraflar arasında iletilen bilginin gizliliği, bütünlüğü ve tarafların kimliklerinin doğruluğu, kurulacak olan teknik ve yasal altyapı ile garanti edilebilmelidir. Bu amaca ulaşmada kullanılacak olan sertifikalar ile ilgili mevzuatların düzenlenmesi, bütün dünya ülkelerinin ilk önceliğidir. Sertifika yasaları halen Almanya, Singapur gibi ülkeler ile ABD' nin birçok eyaletinde uygulanmaktadır.

Sertifikalar, bir bilginin herhangi bir şekilde tutarlılığı, bütünlüğü, güvenilirliği bozulmadan karşı tarafa eriştiğini garanti eden harf ve karakter kümelerinden oluşan ve tekil olarak kişiyi tanımlayabilen belgelerdir.

Sayısal imza, elektronik imzanın özel bir çeşidi olup, bir anahtar çifti (açık ve özel anahtarlar) ile elektronik ortamda iletilen veriye vurulan bir mühüredir. Elle imza atma işleminin elektronik ortamda gerçekleştirilmesi için ortam oluşturma amacını güden sayısal imzalar, elektronik ortamda kişilerin taklit edilerek, bilgilere yetkisiz erişim sağlanmasını engelleme işlevini gerçekleştirirler. [25]

Birleşmiş Milletler Genel Kurulunun 28 Mayıs-14 Haziran 1996 tarihleri arasında New York' da yapılan 29. Toplantısında Elektronik Ticarete ilişkin Model Kanun ve konuya ilişkin Yasal Rehber'in kabul edilmesinden sonra, "sayısal imza ve onay makamları (certification authorities)" ile ilgili olarak diğer ülkelerin mevcut düzenlemelerinden de yararlanılmak suretiyle oluşturulan taslak metinde güvenli imzaların standart özellikleri şu şekilde özetlenmiştir:

1. "Teklik: Açık bir sistemde haberleşen kişilerin herbirinin, kendisini tekil olarak tanımlayacak bir imzası olmalıdır. Teklik şartı, biyometrik yöntemler (parmak izi, retina taraması) veya çift anahtar kullanımıyla sağlanabilmektedir."
2. "Kimlik Tespiti: Sertifika sahibinin kimlik tespiti, sertifika üzerinden rahatlıkla yapılabilmelidir."
3. "Güvenilirlik: Sertifika ile imzalanmış mesajın gerçekten, sertifika sahibi tarafından imzalandığının garanti edilmesi gereklidir. Burada, Verisign gibi sertifika makamlarının önemi ortaya çıkmaktadır."

4. "Bağlantı: Mesaj üzerinde gerçekleşecek bir bitlik değişim, sayısal imzanında değişmesine sebep olacaktır. Bu MD5, SHA gibi çırpı algoritmaları kullanımı ile sağlanmaktadır."

Yine taslakta yer alan ve henüz aksi ispat edilememiş önermeler aşağıda listelenmiştir:

1. "Mesaj sertifika ile imzalandığından itibaren mesaj değişmemiştir."
2. "Sertifika, sahibinin elektronik ortamda bir imzasıdır."
3. "Sertifika, mesajı imzalamak amaçlı olarak kullanılır."

İspat hukuku açısından, sertifika ile imzalanmış mesajı alan taraf yukarıdaki önermelere dayanarak kendini güvenceye alırken, ispat yükü sertifika sahibinin üzerine yüklenecektir.

Taslakta, sahiplik konusunda aşağıdaki hüküm üzerinde anlaşmaya varılmıştır;

"Kişiye veya kuruma ait bir sertifikanın yetkisiz olarak kullanıldığı ispatlanmadıkça, imzalayan taraf ile güvencelenen taraf arasında, sertifikanın imzalayan tarafa ait olduğunu kabul eden bir anlaşma vardır. "

Değişik ülkelerdeki uygulamaların birbirleri ile uyumunun sağlanması amacıyla, her ülkedeki açık anahtar uygulamasında, aşağıdaki hususların belirlenmesi gerektiği öngörülmektedir. [26]

1. Açık anahtar veritabanı ile ilgili kurumların hiyerarşisi, sayısı ve statüsü,
2. Sertifika ile mesajların imzalanmasının altyapısında kullanılacak şifreli anahtar çiftleri (açık ve özel anahtar) 'nin açık anahtar veritabanına sahip kurumlar tarafından mı, yoksa kullanıcılar tarafından mı düzenleneceği,
3. Sertifika makamlarının kamu kuruluşu olarak mı, yoksa özel teşebbüs olarak mı faaliyet gösterecekleri,
4. Sertifika makamlarına yetki verme işleminin, devlet tarafından lisans verme biçiminde mi, yoksa akredite edilme şeklinde bir yöntemlemleri olacağı,
5. Resmi kurumlara, şifrelenmiş bilgilere ulaşım konusunda verilecek yetkinin kapsamı ve sınırları.

9.2 Türk Hukukunda İmzaya İlişkin Hükümler:

Türk hukukunda, imzaya ilişkin hükümler Borçlar Kanununda düzenlenmiş bulunmaktadır. Söz konusu Kanunun 13' üncü maddesinde;

"Tahriri olması icap eden akıterde, bor deruhte edenlerin imzaları bulunmak lazımdır.

Hilafı kanunda yazılı olmadıka imzalı bir mektup veya aslı borcu zerine alanlar tarafından imza edilmiř olan telgrafname tahriri řekil makamına kaim olur." hkm yer almaktadır.

Aynı Kanun'un "İmza" bařlıklı 14' nc maddesinde;

"İmza zerine bor alan kimsenin el yazısı olmak lazımdır. Bir alet vasıtasıyla vazolunan imza, ancak rf ve adete kabul olunan hallerde ve hususiyle ok miktarda tedavle ıkarılan kıymetli evrakın imzası lazım geldiėi takdirde kafi addolunur.

Amaların imzaları usulen tasdik olunmadıka yahut imza ettikleri zaman muamelerin metnine vakıf oldukları sabit olmadıka onları ilzam etmez." hkm bulunmaktadır.

Ayrıca, aynı Kanun'un "İmza Makamına Kaim Olacak İřaretler" bařlıklı 15' inci maddesinde de;

"İmza vaz'ına muktedir olmayan her řahıs, imza yerine usulen tasdik olunmuř ve el ile yapılmıř bir alamet vazetmeye, yahut resmi bir řahadetname kullanmaya mezundur. Kambiyo poliesine mteallik hkmler mahfuzdur" denilmektedir

9.3 1991 Yılında Trk Ceza Kanuna Eklenen Hkmlerle Tarif Edilen Biliřim Alanında Sular ve Cezaları

Kiřisel ve/veya aė zerindeki herhangi bir bilgisayar sistemi zerinden izinsiz bilgi, veri, program vb. herhangi unsurun alınması, bunların nakli oėaltılması, bařkasına zarar vermek zere kullanılması, Trk Ceza Kanunu' nun 525 a maddesinde hapis ve aėır para cezasıyla cezalandırılmıřtır.

"T.C.K. md. 525 a- Bilgileri otomatik olarak iřleme tabi tutmuř bir sistemden, programları, verileri veya diėer herhangi bir unsuru hukuka aykırı olarak ele geiren kimseye bir yıldan  yıla kadar hapis ve bir milyon liradan onbeř milyon liraya kadar aėır para cezası verilir.

Bilgileri otomatik olarak iřleme tabi tutmuř bir sistemde yer alan programı, verileri veya diėer herhangi bir unsuru bařkasına zarar vermek zere kullanan, nakleden veya oėaltan kimseyede yukarıdaki fıkrada yazılı ceza verilir."

Kiřisel ve/veya aė zerindeki herhangi bir bilgisayar sistemine kendisine veya bařkasına yarar saėlamak amacıyla mdahale eden, zarar veren veya doėru ve beklenen řekilde alıřmasını engelleyen ve bilgisayar kullanımı ile hukuka aykırı

yarar sađlayan kimseler, Türk Ceza Kanunu' nun 525 b maddesinde hapis ve ağır para cezasıyla cezalandırılmıştır.

“T.C.K. md. 525 b- Başkasına zarar vermek veya kendisine veya başkasına yarar sađlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diđer herhangi bir unsuru kısmen veya tamamen tahrip eden veya deđiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sađlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan elli milyon liraya kadar ağır para cezası verilir. “

Kişisel ve/veya ađ üzerindeki herhangi bir bilgisayar sisteminde sahte belge tanzim eden, sisteme geçek dışı veri yerleştiren ve gerçek verileri gerçek dışı olanlarla deđiştirenler Türk Ceza Kanunu' nun 525 c maddesinde hapis ve ağır para cezasıyla cezalandırılmıştır.

“T.C.K. md. 525 c- Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tutan bir sisteme, verileri veya diđer unsurları yerleştiren veya var olan verileri, diđer unsurları tahrip eden kimseye bir yıldan üç yıla kadar, tahrip edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir.

Yukarıdaki suçları işleyenlerin, bu konuda meslekleri veya görevleri geređi, bu suçu işleme imkanına gerek bilgileri, gerekse çalışma ortamları bakımından diđer insanlardan daha yakın ve suçu daha kolaylıkla işleyebilecekleri, bu suretle kendilerine tanınan özel imkanları suistimallerinde bilimsel ve teknolojik manada daha az engel ile karşılaşacakları ve bunları daha rahat bertaraf edecekleri öngörüldüğünden bu kişilerin suçu işlemeleri halinde TCK md 25 c' ye göre diđer cezaların yanında, ayrıca kamu hizmetinden veya meslek ve sanat icrasından belirli bir süreyle yasaklanırlar.

“TCK md. 525 d- 525 a ve 525 b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak, meslek icrası sırasında veya icrasıyla suçun işlendiđi bir kamu hizmetinden veya meslek veya sanat veya ticaretinden altı aydan üç yıla kadar yasaklanma cezası da verilir.

10 ÖNERİLEN GÜVENLİK ÇÖZÜMÜ

10.1 Giriş

Sunulan güvenlik çözümü iki katmanlı bir yapıdan oluşmaktadır. Bu yapıdaki dış katman Checkpoint Firewall-1 ile korunacaktır. Checkpoint Firewall-1 ürünü tarafından oluşturulan DMZ bölgelerinden birinde, firewall üzerinden geçen iç ve dış trafik üzerinde içerik adresleme yöntemi ile incelemeler yaparak, akan paket toplulukları içerisinde virüsleri, truva atları, aktif içerikler gibi zararlı kodları sezecek bir antivirüs sunucusu yer almaktadır. Diğer DMZ bölgesinde kurumun internet üzerinden devingen işlemlerini (elektronik ticaret, internet bankacılığı vb.) gerçekleştireceği bir web sunucusu yer almaktadır. Parasal işlemlerin yoğunlukta olduğu böyle sistemlerde, sistem kullanıcılarına ait gizliliği yüksek ve korunması hayati bilgiler (kredi kartı, müşteri numarası vb.) değiş tokuş edilmektedir. Bu hareketsel işlemlerin yüksek şifreleme teknolojilerinin korunması altına alınması gereklidir. 128 bit' lik SSL kullanımı ile bu hassas bilgiler çalınmaya karşı korunmuş olur. Ayrıca buradaki web sunucusunun ele geçirilmesi, işletimsel sisteme, erişimde bir kademenin atlatılması ve kurum açısından hayati önemdeki, işletimsel sistemin veritabanlarına erişim yolu açmaktadır. Bu nedendir ki bu bölgede çok yüksek güvenlik önlemleri alınmalıdır.

Bu güvenlik önlemleri ilk bazda Checkpoint Firewall-1 üzerinde alınacaktır (Firewall ürünlerinin seçiminde kullanılan ölçütler ve ürünlerin denemeler sonunda sağladığı değerler Tablo 10.1' den görülmektedir. [27]). Bölüm 6' da bahsedildiği üzere firewall' lar yerleştiği iki taraf arasındaki trafiğinin geçişini kontrol altına alırlar. Fakat günümüzdeki gelişmiş birçok firewall bu görev dışında, bazı saldırı sezme özelliklerini de içlerinde barındırmaya başlamışlardır. Özellikle Checkpoint Firewall-1 bugün birçok ek ürünü (Checkpoint RealSecure, Şüpheli Durum Sezme Araçları, Raporlama Araçları vb.) içermektedir.

Bu DMZ bölgesinde alınabilecek ikinci önlem, saldırı sezme sistemlerinin kullanılmasıdır. Saldırı sezme sistemleri (bkznz. Bölüm 7) dinlemekte olduğu ağa üzerinde hareket eden paketleri yakalar, yapay zeka tekniklerini kullanarak paket desenlerini belirler ve kendisine önceden tanıtılan saldırı izlerine rastladığı zaman kendisine tanıtılan gerekli eylemleri yerine getirir. Genel olarak iki tip saldırı sezme

yöntemi vardır. Bunlar konak ve ağ temelli saldırı sezme sistemleridir. Önerilen bu iki yöntemin karışımının kullanımıdır. Sistem üzerindeki DMZ bölgeleri ağ temelli bir saldırı sezme sistemi olan RealSecure tarafından dinlenmelidir. Sistem dahilindeki gizliliği hayati önem taşıyan bilgilerin yer aldığı önemli sunucularında aynı ürün ailesinden "System Agent" tarafından izlenmesi gerekecektir.

Öte yandan, saldırı sezme açısından burada sadece Firewall-1' in DMZ bacağına çözüm bulunmuş durumdadır. Firewall-1' in kendini arındırma (stealth) kuralı ile koruyabilmesine rağmen, Firewall-1 diğer bacaklarındaki olağan dışı durumları sezebilmek için, yine aynı ürün ailesinden Şüpheli Durum Sezme (Anomaly Detection) ürününe ihtiyaç duyulacaktır.

Kurumun dışarı ile dosya alışverişi yapması gereken durumlarda kullanılacak olan FTP sunucusunun da dış DMZ bölgesine yerleştirilmesi doğru olacaktır. FTP sunucularının barındırdığı önemli güvenlik gedikleri ("FTP bounce" saldırısı gibi) böyle bir çözümü gerekli kılmaktadır.

Güvenlik politikalarında iki katmanlı yapı kullanımının amacı sistemin güvenlik seviyesini artırmaktır. Bu sistem üzerindeki her bir katmanın farklı firewall ürünlerince korunması, kademeli savunma anlayışı düşünüldüğünde mantıklı bir çözümdür. Çünkü, her iki katmanda da aynı firewall ürününün kullanılması durumunda, dış katmandaki "Checkpoint Firewall-1" in ürün içerisindeki bir güvenlik gediğinden dolayı aşılması sistemin topyekün aşılması boyutlarına varabilir. Oysaki farklı firewall ürünlerinin kullanılması, birinin kaçırdığı zararlı eylemlerin, diğeri tarafından engellenmesi açısından önemlidir. Gerçek dünyadaki eski savaşlardaki cephe örneğine bakılacak olunursa, önde süvariler, arkada okçular, daha arkada da yayan askerler olmak üzere üç katmanlı bir cephe oluşturulmaktadır. Bu nedenle ikinci katmanda Microsoft Firewall kullanımı uygun olacaktır. Microsoft Firewall Windows NT alan güvenliği ile bütünleştirilmiş olarak çalışabilmekte olup, Checkpoint tarafından patentlenmiş durumsal inceleme (stateful inspection) teknolojisine destekleyen ve çeşitli saldırı sezme mekanizmalarını içerisinde barındıran güçlü bir firewall' ır.

Dışarıdan elektronik posta alışverişini sağlayan elektronik posta sunucusu, kurum içerisindeki ofis otomasyonu ve iş akışı uygulamaları ile bütünleşik olarak çalışması gerektiğinden iç firewall üzerindeki DMZ bölgesine yerleştirilmesi, kurum açısından önemli belgelerin güvenliğini sağlayacaktır. Kuruma gelen ve kurumdan çıkan elektronik postalar dağıtılmadan önce "MailSweeper" programı yardımıyla içerik taraması, "Netshield" programı ile de virüs kontrolünden geçirilmelidir.

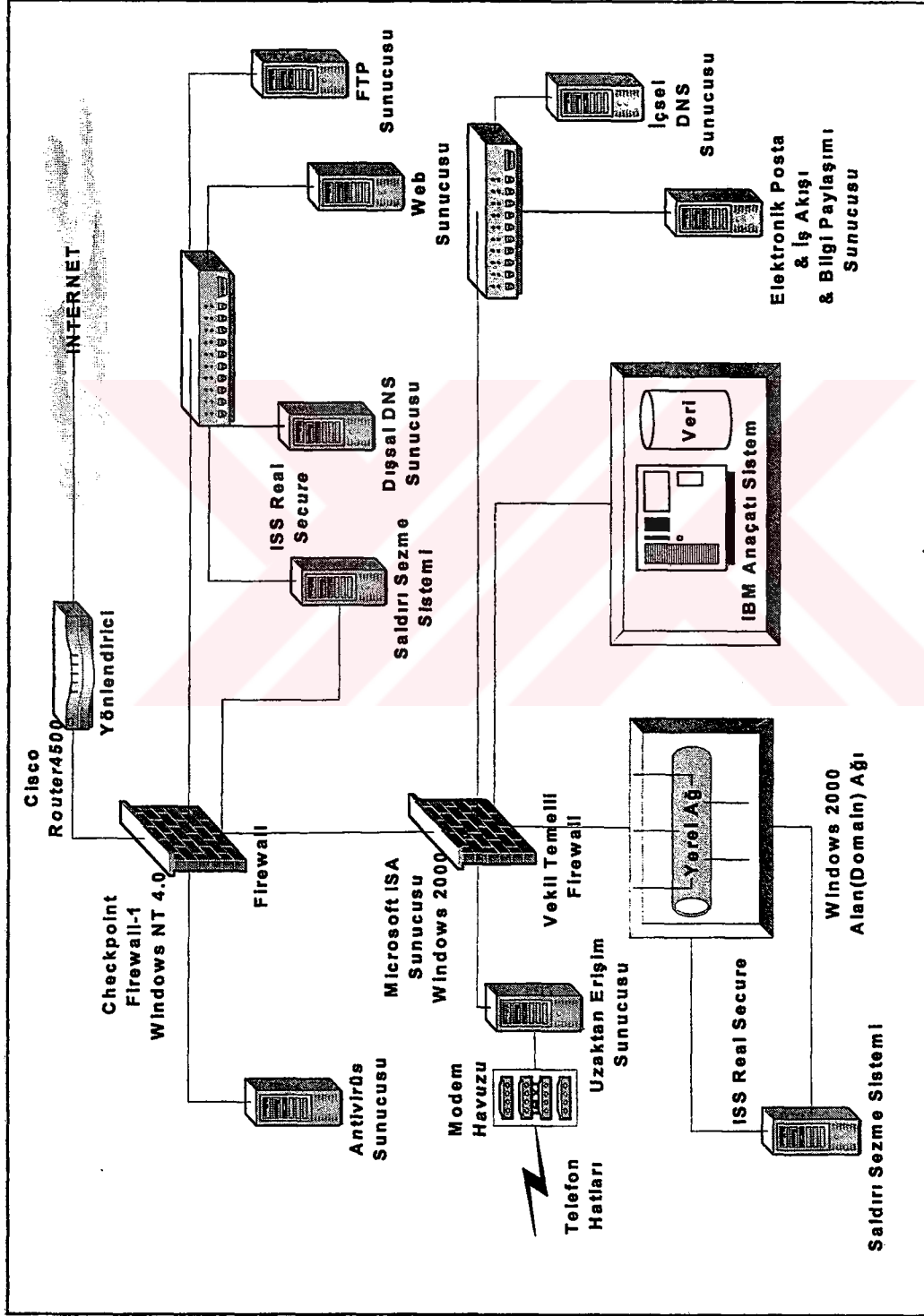
Kurum kendi kullanıcılarına, iştiraklerine ve iş ilişkilerinin bulunduğu diğer kurumlara kendi sisteme ile etkileşim sağlamak, kendi internet sistemleri üzerinden hizmet vermek veya kendi sistem sorumlularının sorun durumunda sisteme uzaktan müdahale etmesine sağlamak için, uzaktan erişim sistemi (Remote Access Service - RAS)' ne ihtiyaç duyabilir. Kurum içi sistemlere erişimde de kullanıldığı için, iç katmandaki DMZ bölgesine bağlanması, kurum içi bilgilerin gizliliği açısından faydalıdır.

Sistem üzerinde güvenlik tehdidi oluşturan saldırılar arasında iç kullanıcıların düzenlediği saldırılarının sayısının önemli bir yer tutması gerçeğinin yadsınamaz olması, iç ağda sıkı bir güvenlik politikası kullanımı ve iç ağdaki hareketlerin saldırı sezme sistemlerince izlenmesini gerektirmektedir.

Önlem alınması gereken diğer bir nokta, işletimsel sistemin güvence altına alınmasıdır. Genellikle kurum ağlarında işletimsel sistemler (IBM Anaçatı) yerel ağa direk olarak bağlanmaktadır. Bugün bu tarz sistemlerin çoğu, TCP/IP protokolünü desteklemeye başlamışlardır. İstemci tarafı sistemler ile bu sistemler, ODBC, yordam çağırma, kuyruklar, arabirim yazılımları ve diğer dosya sistemi nesneleri ile birbirleri ile konuşmaktadırlar. Bu noktada bu sistemlerin güvenliği kendi üzerlerinde alınan güvenlik önlemlerine bağlıdır. Bu çoğu zaman yeterli olmamaktadır. Bu nedenle yerel ağa bağlı olan işletimsel sistemi, iç katmandaki firewall' ın arkasına almak, bu sisteme erişim kısıtlaması getirmek açısından yararlı olacaktır.

10.1.1 Önerilen DNS sunucu yapısı

Güvenlik açısından ayırık (split) DNS sunucusu yaklaşımını kullanmak doğru olacaktır. Ayırık DNS sunucu yaklaşımında iç ve dış olmak üzere iki DNS sunucusu vardır. İnternet yapısı içerisinde DMZ bölgesinde, dışarıyla etkileşimde bulunan konakların girişleri dış DNS sunucusunda, yerel ağ içerisinde yer alan sunucuların DNS girişleri iç DNS sunucusunda bulunmalıdır. Bu şekilde iç ağ altyapısının dış kullanıcılarca öğrenilmesi engellenmiş olacaktır. Ayrıca DNS saldırılarına önlem olarak, kurum IP adres aralığının ters DNS girişleri de yapılmalıdır. Ters DNS girişine gereksinim duyan sunucular, kullanıcının DNS ismini alırlar ve bu DNS ismine karşılık gelen IP adresinin ters DNS girişi ismini bulurlar ve karşılaştırırlar. Eğer ikisi birbirinin aynı ise bağlantıya izin vererek basit bir DNS saldırısına karşı önlem alınmış olur. Kurum DNS sunucusundaki bilgilerin doğruluğunun sağlanması için, DNS sunucusunun sadece güvenirli DNS sunucuları ile alan iletimi yapmasına izin verilmelidir.



Şekil 10.1 Uygulanabilir güvenlik çözümü

Tablo 10.1 Firewall ürünleri karşılaştırması

Firma	AXENT Technologies	CyberGuard	Elron Software	IBM	MEMCO	Microsoft	NetGuard	Network Associates	Checkpoint S.T. Ltd.
Ürün İsmi	Raptor EagleNT 5.0.1	Firewall for Windows NT 4.1	Firewall for NT 2.5	eNetwork Firewall 3.2	SessionWall -3 2.1	Proxy Server 2.0	Guardian 3.01	Gauntlet Firewall 2.0	Checkpoint Firewall-1 4.01
Fiyat	\$3,995, 100 kullanıcı;\$12,500, sınırsız kullanıcı	\$3,245, 50 kullanıcı;\$9,995, sınırsız kullanıcı	\$2,995, 50 kullanıcı;\$9,995, sınırsız kullanıcı	\$4,499, 50 kullanıcı;\$16,500, sınırsız kullanıcı	\$1,495, 125 kullanıcı;\$14,950, sınırsız kullanıcı	\$995, sınırsız kullanıcı	\$3,980, 50 kullanıcı;\$8,980, sınırsız kullanıcı	\$4,400, 50 kullanıcı;\$18,000, sınırsız kullanıcı	\$3,250, 50 kullanıcı;\$9,000 sınırsız kullanıcı
Tasarım									
Paket Süzgeçleme	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet	Evet
Uygulama vekili	Evet	Evet	Hayır	Evet	Evet	Evet	Hayır	Evet	Evet
Devre seviyeli vekil	Evet	Hayır	Hayır	Evet	Hayır	Evet	Hayır	Hayır	Hayır
Durumsal İnceleme (Stateful inspection)	Hayır	Evet	Evet	Hayır	Hayır	Evet	Evet	Hayır	Evet

Önerilen Donanım									
CPU	Pentium *	Pentium 133	Pentium 100	Pentium 133	Pentium 100	Pentium 133	Pentium 166	Pentium 100	Pentium 100
RAM	32MB	32MB	32MB	64MB	32MB	32MB	64MB	32MB	32MB
Saklama Ortamı	1GB	2GB	200MB	87MB	100MB	250MB	1GB	512MB	1 GB
Özellikler									
Ağ Adres Çevrimi	Evet	Evet	Evet	Evet	Hayır	Evet	Evet	Evet	Evet
Uzaktan Yönetim	Evet	Evet	Evet	Evet	Hayır	Evet	Evet	Evet	Evet
Trafik Sınırları	Hayır	Hayır	Hayır	Hayır	Hayır	Hayır	Evet	Hayır	Hayır
İçerik izleme	Evet	Hayır	Hayır	Hayır	Evet	Evet	Hayır	Evet	Evet
Kullanıcı Kimlik Doğrulama	Evet	Evet	Evet	Evet	Hayır	Evet	Evet	Evet	Evet
Kayıt Süzgeçleme	Evet	Evet	Hayır	Evet	Evet	Hayır	Hayır	Hayır	Evet
VPN Özellikleri	Evet	Hayır	Evet	Hayır	Hayır	Evet	Evet	Hayır	Evet

10.1.2 Saldırı sezme sistemleri karşılaştırması

Uygun saldırı sezme sisteminin seçilmesinde göz önüne alınması gereken ölçütler şunlardır:

- Gerçekleme kolaylığı,
- Gerekli yönetim seviyesi,
- Saldırı tanıma yetenekleri,
- Saldırlara cevap verme hızı ve raporlardaki ayrıntı seviyesi,
- Teknik destek kalitesi,
- Sahiplik maliyeti.

Yukarıdaki ölçütler dahilinde Abirnet, IBM, ISS ve Network Flight Recorder/Anzen saldırı sezme sistemi çözümleri incelenmiş ve bu ürünlerin iyi ve kötü özellikleri belirlenmiştir. Bu incelemeler sonunda elde edilen bilgiler şöyledir: [28]

Abirnet çözümünün iyi özellikleri,

- Kolay kullanılabilir olması,
- Oturum engelleme ve süzgeçleme yeteneklerine sahip olması,
- Kolay yönetilebilir olması,
- En ucuz çözüm olması

iken,

- Dağıtık yönetime destek vermemesi,
- Saldırı sezme yeteneğinin diğer ürünlere göre zayıf olması,
- Gerçek anlamda bir saldırı sezme raporunun olmaması,
- Küçük trafik izleme hatalarının olması

kötü özellikleridir.

IBM tarafından üstlenilen taşeron çözümünün iyi özellikleri,

- Gereğinden fazla bir yönetim yükünün olmaması,
- Bilgili ve tecrübeli çalışanlarca desteklenmesi,
- İyi ve esnek bir müşteri hizmetinin ve düşük bakım yükünün olması,
- Hizmet ile bütünleşik olarak aylık yoğun bir gedik tarama işleminin olması

İken,

- Geniş ölçekli saldırıların uzak izleyiciyi devre dışı bırakabilmesi,
- Kendi güvenlik grubunuzu kiralamaya eşit üç yıllık bir maliyete sahip olması

kötü özellikleridir.

ISS çözümünün iyi özellikleri,

- Saldırıları doğru tanıyabilmesi,
- Esnek ve güvenli dağıtık yönetim özelliğine sahip olması,
- Kolay kullanılabilir Windows grafik arayüzüne sahip olması,
- İlginç oturum kaydetme aracı ile kaliteli rapor oluşturma olanağı sunması

iken,

- Gereğinden yoğun bir politika uygulandığında kayıt dosyalarının şişmesi ve başarımların düşüklüğüne sebep olması

kötü özelliğidir.

Network Flight Recorder/Anzen çözümünün iyi özellikleri,

- N-kod trafik değerlendirme motoruna sahip olması,
- %100 tanıma ile sonuçlanan güçlü bir dile sahip olması,
- Grafik ve güçlü sorgulama araçları içeren zengin özellikli raporlama yeteneklerine sahip olması,
- Java tabanlı grafik arayüzünün sağladığı ortam bağımsızlığına sahip olması

iken,

- N-kod öğrenme eğrisine sahip olması,
- Dağıtık yönetim desteğinin olmaması,
- SNMP veya diğer herhangi bir karşı eylem mekanizmasına sahip olmaması

kötü özellikleridir.

N-kod, trafik değerlendirme motoruna uygulanabilen süzgeçler oluşturulmasına izin veren, ele geçirilebilir (preemptive), olay tabanlı bir programlama dilidir. N-kod dilinde yazılan süzgeçler, derlenir, sekizli (byte) koduna çevrilir ve motora yüklenir.

Tablo 10.2' de saldırı sezme sistemlerinin belirli bazı ölçütlerle karşılaştırılması görülmektedir. Bu saldırı sezme sistemlerinden, RealSecure saldırı sezme ürünü,

Checkpoint ile olan uyumluluğu, saldırı sezmedeki doğruluk oranının yüksekliği, kullanıcı dostu olması ve güçlü raporlama araçlarına sahip olması özelliklerinin bütünün diğer ürünlere sağladığı üstünlük nedeniyle saldırı sezme sistemi olarak seçilmiştir.

Tablo 10.2 Saldırı sezme sistemlerinin karşılaştırması

Çözümler	Abirnet Çözümü	IBM Çözümü	ISS Çözümü	Network Flight Recorder/Anzen Çözümü
Ürün	"SessionWall-3"	"Internet Emergency Response Service IBM"	"RealSecure for Windows NT"	"Anzen Flight Jacket for NFR"
Başarım ve güç				
Gerçekleme (%5)	İyi (3)	İyi (3)	İyi (3)	Yeterli (2)
Yönetim ve Güvenlik (%20)	Çok iyi (16)	Çok iyi (16)	İyi (12)	Yeterli (8)
Bilinen saldırıları tanıma (%20)	Yeterli (8)	Yeterli (8)	Yeterli (8)	Mükemmel (20)
Cevap verme ve Raporlama (%20)	İyi (12)	İyi (12)	Çok iyi (16)	İyi (12)
Belgeleme (%5)	Çok iyi (4)	Çok iyi (4)	Yeterli (2)	Zayıf (1)
Destek ve Fiyat				
Teknik Destek (%10)	İyi (6)	İyi (6)	Zayıf (2)	İyi (6)
Teknik destek politikaları (%10)	Mükemmel (10)	Mükemmel (10)	Mükemmel (10)	Yeterli (4)
Projelendirilmiş temel sahiplik maliyeti (%10)	Yeterli (4)	Mükemmel (4)	Mükemmel (10)i	Mükemmel (10)

10.2 Genel Güvenlik Politikası Taslağı

10.2.1 Tanıtım ve amaç

- Kuruluşumuz bilgi sistemlerine, veri ve bilgi işleme yeteneklerine bağlı olarak hizmet vermektedir.
- Verinin bozulması, değiştirilmesi, çalınması, doğruluğunu kaybetmesi ve bu veriyi işleme yetisinin kaybolması sonucunda kuruluşumuz..... (<riskler anlatılır>)
- Her çalışan bu risklerin farkında olmak ve kuruluşumuzu bu çerçevede içinde koruyacak şekilde davranmak zorundadır.
- Bu güvenlik politikası bilgi sistemlerinin güvenliği için çalışanların sorumluluklarını belirler.

10.2.2 Konu

- Güvenlik politikası, tüm çalışanları, sözleşmelileri ve geçici olarak hizmet verenleri kapsar.
- Güvenlik politikası, tüm sunuculara, kişisel bilgisayarlara ve harici veri sağlayıcılara uygulanır.
- Güvenlik politikası tüm kuruluş verisine ve bu verilerden elde edilen raporlara uygulanır.
- Güvenlik politikası, kuruluş çalışanları tarafından, kuruluşun kaynakları kullanılarak, kuruluş bünyesinde geliştirilen tüm programlara uygulanır.

10.2.3 Tanımlar

Bu kısımda güvenlik politikasında kullanılan özel isimler ya da kavramların tanımı yapılır.

10.2.4 Bilgi sistemleri güvenliği için sorumluluklar

1. _____ sorumludur.
2. Her çalışan, bilgi sistemlerinin verisi ve ekipmanını da içerecek şekilde kuruluşun sahip olduğu mal ve değerleri korumaktan sorumludur.
3. Her çalışan güvenlik politikasına karşı olan bir faaliyeti tespit ettiğinde _____ haberdar etmek zorundadır.

10.2.5 Kullanıcı tanımları ve şifreleri

1. Hiç kimse yetkili bir kullanıcı hesabı olmadan bilgi sistemlerini kullanamaz.
2. Kullanıcı hesapları ve erişim hakları "bilmesi gereken" prensibi temel alınarak belirlenir.
3. Kullanıcı hesabı almak _____ onayını gerektirir.
4. Kullanıcı hesabı ve şifreler her bir yetkili kullanıcı için tekildir.
5. Her kullanıcı kendi kullanıcı hesabındaki hareket ve işlemlerden sorumludur.
6. Tüm kullanıcı hesapları gerekli görüldüğü takdirde iptal edilebilir.
7. Kullanıcı ayrıldığında veya başka bir birime geçtiğinde kullanıcı hesapları iptal edilir.
8. Kullanıcı şifreleri en az 8 karakterden oluşur. Ayrıca şifreler en az bir rakam ve büyük harf içermelidir.
9. Kullanıcı şifreleri gizli tutulacaktır. Herhangi bir kimse ile paylaşılmayacak ve program içerisine kodlanmayacaktır.
10. Kullanıcı hesapları 90 gün boyunca kullanılmadıkları takdirde iptal edilir.
11. Kullanıcı hesapları, şifre art arda 3 kere yanlış girildiği takdirde iptal edilir.
12. Herhangi bir oturum içerisinde eylemsiz geçen her bir 15 dakikalık süreden sonra kullanıcıdan şifresini yeniden girmesi istenecektir.
13. Sisteme başarıyla bağlanıldığında, sisteme son başarılı bağlantı ve sistemden ayrılma zamanları ekranda gösterilecektir.
14. Her kullanıcı en az her 90 gün içerisinde şifresini değiştirmek zorundadır. Bilgi sistemlerinin uygulamaları bunu gerektirecektir.
15. Kuruluş bünyesindeki programlar sadece yetkili kullanıcı hesabına sahip olanların o programı kullanabilecekleri şekilde düzenlenecektir.

10.2.6 İşe alma uygulamaları

1. Her çalışan, sözleşmeli ve geçici çalışan bu belgenin bir kopyasına sahip olmalıdır.
2. Her yeni çalışana, oryantasyon süreci içerisinde bilgi sistemlerinin güvenliğinin önemi ve bundaki rolleri anlatılacaktır.

3. Çalışanların bölüm değiştirmelerinden, terfilerden ve işten çıkarılmalarından _____ haberdar edilerek bilgi sistemlerine erişimdeki gerekli düzeltmeleri yapması sağlanacaktır.
4. Her çalışan bu belgeyi okuduğuna, anladığına ve kabul ettiğine dair belgeyi imzalayacaktır.

10.2.7 Çalışanların sorumlulukları

1. Kurum sistemlerinde ve hesaplarında kullanılan ve saklanan tüm bilgilerin korunması çalışanların sorumluluğundadır.
2. Sistem kullanıcıları, sistem üzerinde gördüğü herhangi bir zayıflığı, firmamın sistem güvenliği ekibine bildirmekle yükümlüdürler.
3. Kullanıcılar erişim hakkına sahip olmadıkları, sistem veya verilere erişim teşebbüsünde bulunmamalıdır.
4. Kullanıcılar uzaktan erişim sunucusu telefon numaralarını kimseye vermemelidirler.
5. Kullanıcılar telif haklarını ihlal ederek, kuruma ait yazılımların izinsiz kopyalarını oluşturmamalıdır.
6. Kullanıcılar kendilerine ve başkalarına yetkisiz kişisel kullanımlar sağlamak için, sistem dosyalarının kopyalarını almamalıdır.
7. Kullanıcılar, diğer kullanıcılara zarar verecek, sistem başarımını düşürecek, başka kullanıcıların kurum kaynaklarına yasal erişim yetkisini engelleyecek, kendisine atanandan daha fazla kaynak elde edecek, bilgisayar güvenliği sınırlamalarını aşarak erişim yetkisine sahip olmadığı kurum sistemlerine erişim yetkisi kazanacak eylemlerde bulunmamalıdır.
8. Kurumun elektronik iletişim faaliyetleri, hükümetçe izin verilen şekillerde kullanılmalıdır. Başkalarına zarar verici, düzenbazlık içeren, açık-seçik mesajlar ve maddelerin kurum sistemlerinden iletilmesi yasaktır.
9. Hiçbir kullanıcı kurum bünyesinde kullandığı bilgisayarına bilgi sistemleri merkezinden onay almaksızın üçüncü parti yazılımları yükleyemez, internet' ten indiremez.
10. Kullanıcıların internet' e erişim ihtiyaçları belirlenerek sınırlandırılacaktır. Tüm kullanıcılar iş dışı konularda, mesai saatleri dışında ve/veya öğle arasında internet' e erişebileceklerdir.

11. Pornografik içeriğe sahip internet sitelerine bağlanmak, bu sitelerden pornografik içeriğe sahip dosya indirmek yasaktır.

10.2.8 Cihazlara erişim

1. Sadece gerçekleştirdiği faaliyetin gerektirdiği kaynaklara erişim hakkı olan çalışanlar bilgi sistemlerinin kaynaklarına erişebilir.
2. Tüm bilgi sistemleri kaynakları, yangına, suya, elektrikteki voltaj değişimlerine, fiziksel zararlara ve hırsızlığa karşı korunmalıdır.
3. Bilgi sistemlerinin kaynaklarına erişimin kontrolünden ve yeterli korunmanın sağlanmasından _____ sorumludur.

10.2.9 Veriye erişim

1. Kuruluş bünyesindeki bilgi sistemlerinde tutulan tüm dosyalar yetkisiz kişiler tarafından yapılabilecek değişikliklere karşı korunacaktır.
2. Hassas veri dosyaları, yetkisi olmayan kişiler tarafından okunmaya veya değiştirilmeye karşı koruma altındadır.
3. Kuruluş bünyesindeki bilgi sistemleri uygulamaları hangi kullanıcı hesabının hangi dosyalardan okuyabileceği, hangi kullanıcı hesaplarının hangi dosyalara yazabileceğini kontrol edecek şekilde programlanmalıdır.
4. Her dosyanın sahibi, dosyanın ne derece hassas bilgiye sahip olduğunu ve kimlerin hangi haklarla bu dosyaya erişeceğini tanımlamakla yükümlüdür.
5. İnternet üzerinden dağıtılan kurum verilerine erişimde, kullanıcı ve sunucuya tanımlayacak kimlik doğrulama araçları (sertifika, akıllı kart, token gibi) kullanılacaktır.
6. Kişisel bilgisayarlarda tutulan sayısal setrifikalara erişim, şifre ve geçiş sözcükleri ile korunacaktır.

10.2.10 Özel erişim

1. Kurum sistemlerinde özel erişim, özel erişim veri tabanlarının kullanımı ile kurum işletmenleri ve güvenlik yöneticisi tarafından izlenir ve yönetilir.
2. Özel erişim hesaplarının şifreleri, kurum işletmenleri ve güvenlik yöneticilerinin kararlaştırdığı gibi düzenli bir şekilde gerçekleştirilir.
3. Özel erişim, işi gereği özel erişime gereksinimi olan çalışanlara verilir.
4. Özel erişim imtiyazlarının herhangi bir şekilde yanlış kullanımı hiç zaman kaybetmeden, kurumun güvenlik yöneticisine bildirilmelidir.

5. Özel erişim hakkı isteyen her kullanıcı, Şekil 10.2' de gösterilen özel erişim istek belgesini doldurmalı ve ayrıntısı Şekil 10.3' te gösterilen özel erişim sözleşmesini imzalamalıdır.
6. Özel erişim sözleşmesini imzalamayanlar özel erişim hakkına sahip olamazlar.
7. Özel erişim hakkına sahip olanlar, özel erişim gereksinimleri değiştiğinde, bu konuyla ilgili olarak, sistem işletmenleri ve güvenlik yöneticisini haberdar etmelidirler.
8. Kişi, işten ayrılma, görev değişikliği, özel erişim sözleşmesini ihlal gibi nedenlerden dolayı özel erişim veritabanından silinebilir.
9. Kişi, güvenlik yöneticisi veya şube yöneticisinin kararı ile özel erişim veritabanından silinebilir. [29]

ÖZEL ERİŞİM İSTEK BELGESİ	
Sicil No	
İsim Soyad	
Bölüm/Müdürlük	
Ünvan	
Görev	
İstenen Erişim Hakkı	
Nedeni	
İmza: Çalışan	İmza Müdür

Şekil 10.2 Özel erişim istek belgesi örneği

10.2.11 Yazılım kontrolü

Virüs kontrolü

1. Kullanıcılar internet üzerinden virus ve diğer zararlı kodları alabileceği ve virus tarama programları kullanımı konusunda eğitilecektir.
2. Yazılımlar sadece sistem yöneticisi tarafından indirilecek ve yüklenecektir.
3. Virüslerin sistem üzerinde yayılımını engellemek için dosya sunucuları üzerinde antivirüs yazılımları kurulacaktır.

4. Sistem üzerinde anında kontrol özelliklerine sahip virüs tarama programları kullanılacak ve yeni geliştirilen viruslerin oluşturacağı tehlikelere önlem olarak antivirüs yazılımı her gün güncellenecektir.
5. Virüs tarama programlarının kayıtları, virüs olasılığına karşı sistem yöneticiler tarafından incelenecektir.
6. Kullanıcılar sistem üzerinde karşılaşılan herhangi bir virus veya normal olmayan olayları sistem yöneticisine bildirmekle yükümlüdür.
7. Virüs belirlendiği zaman sistem yöneticisi virüsün yayılmasını engellemek için, diğer kullanıcıları bulunan virus ve sebep olan program konusunda uyaracaktır.
8. Virüslerden etkilendiği belirlenen makinenin hiç zaman kaybetmeden ağla bağlantısı kesilecektir.

ÖZEL ERİŞİM SÖZLEŞMESİ

Bu sözleşme _____ firmasının bilgisayar sistemlerinde özel erişim haklarının kullanımları ile yapılabilecekleri ve yapılamayacakları belirler. Bu özel erişim sözleşmesi, kullanıcıların özel erişim haklarını, sorumlu ve güvenli bir şekilde kullanmalarına yardım etmek için geliştirilmiştir. Bu sözleşmeyi imzalamaya reddeden kimse, özel erişim haklarına sahip olamayacaktır.

Genel Kurallar

1. Kurumun bilgisayar sistemlerinin yapısının farkına varınız.
2. Özel erişim haklarını sadece, gerekli olduğu zaman kullanınız.
3. Önemli eylemlerin tümünü belgeleyiniz ve gerekli kişileri bilgilendiriniz.
4. Birşeylerin kötü gitmesi ihtimaline karşın, bir yedekleme planına sahip olunuz.
5. Herhangi bir sorun oluştuğunda kiminle temasa geçmeniz gerektiğini biliniz.

Özel Kurallar

1. Özel erişim şifrelerinizi kimse ile paylaşmayınız.
2. Özel erişim şifrelerinizi ve güncel algoritmayı hiç bir yere yazmayınız.
3. Özel erişim hakkına sahip şifre ile rutin olarak sisteme bağlanmayınız.
4. Özel erişim gerektirmeyen işlemler yaparken, özel erişim şifrenizi kullanmayınız.
5. Özel erişim şifreniz ile kendi işinizin gerektirdiği görevleri ilgilendirmeyen sistemler üzerinde değişiklik yapmayınız.
6. Özel erişim haklarını kullanarak, kendi özel işlemlerinizi için geçici dosya ve dizinler oluşturmayınız.

Yukarıda yazılı tüm şartları ve herhangi bir ihlal durumunda tüm haklarımın elimden alınmasını kabul ederim.

İmza:

Tarih:

Şekil 10.3 Özel erişim sözleşmesi örneği

Etkileşimsel yazılım kontrolü

1. "Applet" lerin güvenilen kaynaklardan geldiğini ispatlayan kimlik doğrulama teknolojilerinin kullanılmadığı durumlarda, eğer engellenebilmekteyse firewall üzerinden, yoksa tarayıcı üzerinde "applet" kullanımı engellenecektir.
2. Eğer uygunsa "applet" kullanımı geliştime ortamı ile sınırlandırılmalı gerçek ortamda kullanılmamalıdır.

10.2.12 Şifreleme

1. Veri dosyaları _____ durumunda şifrlenmelidir.
2. Şifre dosyaları _____ durumunda şifrlenmelidir.
3. _____ şifreleme kullanımı ve kullanıcıları eğitmek konusunda yordamlar geliştirmekten sorumludur.
4. Şifreleme anahtarları kurumun gizliliği en önemli bilgileri arasında sınıflandırılacak ve kolayca elde edilemeyecek matematiksel karmaşıklığa sahip olacaktır.

10.2.13 Güncelleme politikası

1. Bu güvenlik politikası _____ aralıklarla gözden geçirilecektir.
2. _____ güvenlik politikasını gözden geçirip düzeltme hakkına sahiptir.
3. Güvenlik politikasındaki değişiklikler _____ ile beraber sonuçlandırılacaktır.

10.2.14 Saldırı sezme politikası

1. Normal kayıt tutma süreçleri tüm konak ve sunucu sistemleri üzerinde çalıştırılacaktır.
2. Ağ güvenlik sistemi içerisindeki tüm uyarı mekanizmaları aktif kılınacaktır.
3. Büyük öneme sahip tüm sunucular üzerinde "Tripwire" gibi ek izleyici araçlar çalıştırılmalıdır.
4. Güvenlik sistemi içerisinde yer alan tüm konak, sunucu ve güvenlik araçlarının tutarlılık kontrolü düzenli olarak yapılacaktır.
5. Güvenlik sistemi kayıtları saldırı tehlikesine karşı günlük olarak izlenecek ve raporlar oluşturulacaktır.
6. Kullanıcılar sistem üzerinde gerçekleşen olağan dışı durumları sistem yöneticisi ve güvenlik yöneticilerine bildirmeleri konusunda eğitilecektir.

7. Sistem yöneticisi tarafından alınan her bir sorun raporu sistem saldırısı ihtimaline karşı en ince ayrıntılarına kadar incelenecektir.
8. Ağ güvenlik ekibi diğer saldırı cevap verme kuruluşları ile ilişki içerisinde olacaktır.
9. Saldırı esnasında, önemli sistemler ele geçirilmediği sürece, güvenlik ekibi sistemi düzeltmeden saldırıyı izleyecektir.

10.2.15 Acil durum planı

1. Bilgi sistemlerine yönelik bir saldırı gerçekleştiğinde, saldırıya yönelik gösterilecek eylemden, zararın telafi edilmesine yönelik çalışmaların planlanması ve gerçekleşmesinden _____ sorumludur.
2. İçerisinde üst düzey yöneticilerinde bulunduğu bir acil durum ekibi kurulacaktır.
3. Saldırı sırasında ile ilgili tüm gerekli çalışanlar haberdar edilmesinden _____ sorumlu olacaktır.
4. Saldırı cevap verme sürecinde bağımsız kuruluşlardan alınacak yardımlarda temas _____ tarafından sağlanacaktır.
5. Saldırı ile ilgili olarak basına bilgi _____ tarafından verilecektir.
6. Sistem üzerinde alınacak ciddi kararların onayı _____ tarafından verilecektir.

10.2.16 Onay

1. Kuruluş üst yönetiminin imzası ve tarih.
2. Bilgi sistemleri yönetiminin imzası ve tarih.
3. Güvenlik yöneticisinin imzası ve tarih.
4. Güvenlik politikasında öneme sahip diğer personelin imzası ve tarih. NIST (2001)

10.3 Windows NT Güvenliği

10.3.1 Güncellemeler

- İşletim sistemi ile ilgili en son güncellemelerin kurulması işletim sisteminin hem güncel olmasını, hem de bilgisayarınızın işlevselliğini artırarak, geri kalmış olma endişesinin ortadan kalkmasını sağlayacaktır.

10.3.2 Kurulum

- Kullanılmayan gereksiz donanım aletleri (örneğin, COM ve LPT kapıları) ya kurulmamalı ya da BIOS' dan etkisiz kılınmalıdır.
- Sistem donanımlarının fiziksek güvenliğinin sağlanması gereklidir. Bilgisayarların, kilitli kasalara konulması, sistem odasına giriş çıkışların, otomatik kilit sistemleriyle kontrol edilmesi, giriş çıkışların kaydedilmesi vb. önlemlerin alınması gereklidir.
- Window NT İşletim sistemi kurulum araçlarından, kurulum disketleri veya CD' den başlatılarak kurulmalıdır. Windows 95, Windows 98 veya DOS işletim sistemleri üzerinden kurulmamalıdır.
- Makinenin farklı işletim sistemleri veya ortamlardan başlatılmasına, güvenlik gereksinimlerinden dolayı izin verilmemelidir. İzin verildiği durumda, bu işletim sistemleri üzerinde çalışan programlar, Windows NT işletim sistemi dosyalarının bulunduğu saklama ortamlarına, Windows NT işletim sisteminin güvenlik önlemlerince (NTFS dosya biçimi erişim kontrol listeleri) engellenmeden erişecektir.
- Windows NT işletim sisteminin kurulu olduğu makine üzerinde, Linux, Windows 9x veya DOS gibi işletim sistemlerinde kurulu olmasına izin verilmemelidir. Hatta işletimsel olarak çok gerekli olmadığı sürece aynı makine üzerinde, birden fazla NT işletim sistemi kopyası kurulumuna izin verilmemelidir.
- Windows NT işletim sisteminin kurulu olduğu, sabit disklerin tümü NTFS dosya biçiminde biçimlenmelidir. NTFS dosya sistemi, FAT dosya sisteminde farklı olarak, güvenlik açısından çok büyük öneme sahip olan erişim kontrol listelerini desteklemektedir.
- Windows NT işletim sistemi üzerindeki POSIX ve OS/2 alt sistemleri,
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\Subsystems
kayıt girişinde güvenlik tehdidi oluşturduğu için, "Optional" sahasından "Posix" ve "Os2" değerleri silinerek kaldırılmalıdır. [30]

10.3.3 Genel politikalar

- Disket Okuyucu (Floppy) ve CD-ROM' lara erişim

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon

kayıt girişindeki "AllocateFloppies" ve "AllocateCDRoms" parametreleri "1" yapılarak, o anda sisteme bağlı olan kullanıcıya kapanmış olur.

- IP taklidine önlem olarak, CD-ROM' ların otomatik çalıştırma özelliği,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom

kayıt girişindeki REG_DWORD "Autorun" parametresine 0 değeri girilerek iptal edilir.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System

kayıt girişindeki REG_DWORD "DisableRegistryTools" parametresine 1 değeri girilerek bilinen kayıt programının çalışması engellenebilir. Yalnız bu diğer programlarla sistem kayıtlarına erişimi engellemez.

- Koruma Modu: Windows NT kullanıcı programlarının birçok veri nesnelerine erişimine izin veren iç bir hiyerarşiye sahiptir. Tüm programlar, bu hiyerarşide erişim kontrol listelerine sahip nesneler oluşturabilmektedirler. Ancak temel nesneler olarak isimlendirilen bu nesnelerin çoğu, erişim kontrol listelerine sahip değildir.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager

kayıt girişindeki REG_DWORD "ProtectionMode" parametresine "1" değeri atanarak oluşturulan bir nevi erişim kontrol listesi ile nesneler üzerinde sağlanan koruma, kullanıcı programlarının, sistem yöneticisi ve nesne yaratıcısına erişimini sınırlandırır. [30]

- Varsayılan olarak misafir ve doğrulanmamış kullanıcılar, işletim sisteminin sistem ve uygulama kayıtlarını görüntüleyebilmektedirler.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\Application

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\System

kayıt girişlerindeki REG_DWORD "RestrictGuestAccess" parametresine 1 değeri atanarak bu erişim engellenebilir. [31]

- Sisteme yazıcı eklenmesi,

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers
\LanMan Print Services\Servers

kayıt girişindeki REG_DWORD "AddPrinterDrivers" parametresine 1 değeri atanarak, sadece sistem yöneticisi, yazıcı işletmeni ve güç kullanıcısı ile kısıtlanır.

- Ekran koruması kilitlemesini aktif hale getirmelidir.
- Çırpılmış Şifrenin Korunması: Windows NT işletim sistemi kullanıcı şifreleri yerine, bu şifrelerin tek yönlü çırpı işlevinden geçirilmiş değerlerini saklamaktadır. Windows NT sistemi kullanıcılarının çırpılmış şifreleri, sistem kayıtlarında SAM dosyasında tutulmaktadır. Çırpılmış değer kullanılarak sisteme bağlantı kurulamasa bile, "brute force" saldırısı kullanarak bu değerden asıl şifreyi elde edebilecek uygulamalar mevcut olabilmektedir. SAM kayıtlarına sadece sistem yöneticisine erişim hakkı verilerek, kullanıcı şifreleri güvenlik altına alınabilir; fakat "rdisk /s" komutu ile SAM dosyalarının bir kopyası başka saklama ortamlarına (disket gibi) kopyalanabilmektedir.

Öte yandan, "syskey" komutu ile yerel olarak saklanan şifrelerin korunması artırılmaktadır. Bu komut ek bir önlem olarak, çırpılmış şifrelerin 128 bitlik şifreleme algoritmaları ile şifrelenmesini sağlamaktadır.

- Windows NT, bir alanda kullanıcı hesaplarını görme hakları dahi olmayan kullanıcıların, o alan kullanıcı hesaplarını görmeye izin vermektedir. Bu sorunun giderilmesi için,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

kayıt girişindeki REG_DWORD "RestrictAnonymous" parametresine 1 değeri atanmalıdır.

- Sisteme son bağlanan kullanıcının kim olduğu,

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\Current
Version\Winlogon

kayıt girişindeki REG_SZ "DontDisplayLastUserName" parametresine 1 değeri atanarak gizlenir.

- Sisteme bağlanılmadan kapatılabilmesine izin vermek için,

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon

kayıt girişindeki REG_SZ "ShutdownWithoutLogon" parametresine 1 değeri atanmalıdır. Bu durumda bağlantı ekranında "Shutdown" düğmesi aktif olacaktır.

10.3.4 Dosya sistemi ve kayıt erişim kontrolü ayarları

1. Windows NT yardım dosyaları çalıştırılabilir kod içerdiğinden, taklit saldırılarını önlemek için, normal kullanıcıların yazmasına açık olmamalıdır.
2. *.ini ve *.pnf dosyaları uygulamaların kurulumu ve eylemleri ile ilgili bilgiler içerdiğinden, herkes tarafından yazmaya açık olmamalıdır.
3. "Repair" dizinindeki dosyalar çırpılmış şifre değerleri içerdiği için kimseye erişim hakkı verilmemelidir.
4. "System32" birçok önemli güvenlik dosyasını barındıran dizindir. Aynı zamanda, birçok uygulama nereye koyacağını bilmediği tüm dosyaları bu dizine kopyalamaktadır. Taklit saldırıları nedeni ile normal kullanıcıların bu dizine yeni dosya kopyalamalarını izin verilmemelidir. Bazı yedekleme programlarının bu dizin üzerinde geçici dosyalar oluşturması nedeni ile yedekleme işletmenlerine bu dizin üzerinde değiştirme hakkı verilmelidir.
5. Sistem üzerinde kurulu sürücü bilgilerinin tutulduğu "drivers" dizininde, sistem yapılandırmasındaki bütünlüğü bozacak değişikliklerin engellenmesi için, bu dizin üzerinde kimseye değiştirme yetkisi verilmemelidir.
6. Bu dizinde yer alan "ntconfig.pol" gibi bazı dosyalar, çok sıkı oluşturulmuş erişim kontrol listelerine ihtiyaç duyarlar. Bu dizin genelde replikasyon hizmeti tarafından kullanılır. Replikasyon işlevini gerçekleştirmesi için sunucu işletmenine tüm yetkileri vermek mantıklı olacaktır.
7. "System" dizini, kurulum sırasında "*.drv" ve "*.dll" dosyalarının tutulduğu dizindir. Kurulmdan sonra, sistem yöneticisinin arama yolundan (search path) çıkarılmalıdır.
8. RAS sisteminin yönetilmesi, sistem kurucusunun görevi dışında olduğu için "RAS" dizininde, herhangi bir özel yetkiye sahip olmamalıdır. Güç kullanıcısının sistemin "dial-in" ağlara açmadığı durumda, herhangi bir yetkiye ihtiyacı olmayacaktır.

Tablo 10.3 Önerilen nesne erişim hakları

Nesneler	Olması Gereken	Varsayılan NT Kurulumu	Açıklama
C:\	Kurucular: Değiştirme Herkes: Okuma Sunucul İşletmenleri: Değiştirme Güç Kullanıcıları: Ekleme*	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	
IO.SYS MSDOS.SYS	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme	Herkes: Değiştirme	
BOOT.INI, NTDETECT.COM NTLDR		Herkes: Okuma	
AUTOEXEC.BAT, CONFIG.SYS	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme	Herkes: Değiştirme	
C:\WINNT\	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	
\WINNT\config\	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	
\WINNT\help\	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme Güç Kullanıcıları: Değiştirme	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	1
\WINNT\inf\	Kurucular: Değiştirme Herkes: Okuma	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	2
\WINNT\repair\		Herkes: Okuma Sunucu İşletmenleri: Full Güç Kullanıcıları: Değiştirme	3
\WINNT\system\	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	7
\WINNT\System32\	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Değiştirme Yedekleme İşletmeni: Değiştirme	Herkes: Değiştirme Sunucu İşletmenleri: Değiştirme	4
\WINNT\System32\config\	Herkes: Listeleme	Herkes: Okuma Sunucu İşletmenleri: Değiştirme	
\WINNT\System32\drivers\	Herkes: Okuma	Herkes: Okuma Sunucu İşletmenleri: Bütün	5
\WINNT\System32\Repl	Herkes: Okuma Sunucu İşletmenleri: Bütün	Herkes: Okuma Sunucu İşletmenleri: Bütün	6
\WINNT\System32\RAS	Herkes: Okuma Sunucu İşletmenleri: Değiştirme	Herkes: Değiştirme Sunucu İşletmenleri: Bütün Güç Kullanıcıları: Değiştirme	8
\WINNT\System32\spool	Kurucular: Değiştirme Herkes: Okuma Sunucu İşletmenleri: Bütün	Herkes: Okuma Sunucu İşletmenleri: Bütün Yazıcı İşletmeni: Bütün	

	Yazıcı İşletmeni: Değişirme Güç Kullanıcıları: Değişirme	Güç Kullanıcıları: Değişirme	
WINNT\System32\wins	Herkes: Okuma Sunucu İşletmenleri: Değişirme	Herkes: Değişirme Sunucu İşletmenleri: Değişirme	9
\\printers\\ \\tmp\\	Kurucular: Değişirme Herkes: (RWX) Sunucu İşletmenleri: Bütün Yazıcı İşletmeni: Değişirme Güç Kullanıcıları: (RWXD)(WXD)	Herkes: Okuma Sunucu İşletmenleri: Bütün Yazıcı İşletmeni: Bütün	11
C:\...*.EXE	Herkes: X	N/A	
C:\...\\ *.BAT *.COM *.CMD *.DLL	Herkes: Okuma	N/A	

9. Ağ dizini olan bu dizine, uygulama kurucularına erişim izni vermemek doğru olacaktır.
10. Bu konudaki genel prensip, sunucu işletmenlerine tüm hakları vermek, yazıcı işletmenleri ve güç kullanıcılarına sadece değişirme hakkı vermektir.
11. "Printers" dizinini Windows NT için varsayılan "spool" klasörüdür. Buradaki kullanıcı sınırlamaları, normal bir kullanıcının diğer kullanıcıların bilgilerini görmesini engellemektedir. "Tmp" dizini geçici olarak yazma işlemleri için kullanılır. Güç kullanıcıları için kullanılan erişim dosyaları, güç kullanıcılarının, diğer kullanıcıların "spool" dosyalarını görmesini engeller.

10.3.5 Kullanıcı hesapları

- "Log on locally" hakkı, ciddi gereksinimi olan kullanıcılara verilmelidir.
- Kullanıcıların sisteme bağlanmalarına izin verilecek zamanlar gereksinime göre belirlenmelidir.
- Sistem üzerindeki "guest" hesabı etkisiz kılınmalıdır.
- Kullanım gereksinimi olmayan kullanıcı hesapları incelenerek, artık kullanım gereksinimi olmayan hesaplar iptal edilmelidir.

10.3.6 Gruplar

- Genel gruplar ve kullanıcılar, alan kontrolcülerindeki "Replicator" grubuna konulmamalıdır.
- "Guest" grubu doğrulanmış bir bağlantıyı aktif edemez.
- Windows NT alanında "Users" grubuna üye olan kullanıcılar, kendilerine ait gruplar üretebilirler. Kullanıcıların kendi gruplarını oluşturabilmesi erişim yeteneklerini genişletmektedir. Kullanıcıların grup oluşturmalarını kısıtlamak

istemekteyseniz, "Users" grubundan çıkarınız. Fakat bu da bazı nesnelere erişimde sorunlara sebep olabilir.

10.3.7 Şifreler

- Hesap poltikasında şifre tekilliği (password uniqueness) seçeneği aktif edilmelidir.
- Hesap poltikasında en az şifre yaşı (minimum password age) parametresini 2 gün olarak tanımlanmalıdır ki, kullanıcının eski favori şifrelerini tekrar dönmek için, aradan uzun zaman geçmesi gereksin ve kullanıcı eski şifrelerini tekrar tekrar kullanmasın.
- Yeni bir kullanıcı tanımlandığında kullanıcının sisteme ilk bağlantısında şifresini değiştirmesi için "User Must Change Password at Next Logon" seçeneği seçilmelidir.
- Bir önceki şifresi zaman aşımına uğradığı zaman, kullanıcının yeni bir şifre almasını engellemek için "User must log on in order to change password" seçeneği seçilmelidir.
- Kullanıcıların bağlantı saatleri dışında yeni bağlantı açmalarını engellemek için "Forcibly disconnect remote users from server when logon hours" seçeneğini kullanınız. Bu seçenek bağlantı zamanı geçmeden önce varolan bağlantılar için sorun çıkarmaz.
- Zayıf şifre kullanan kullanıcıları belirlemek için, belirli aralıklarla Windows NT şifre tahmin etme programları çalıştırınız.

10.3.8 Kullanıcı hakları

- "Log on locally" ve "Access this computer from the network" kullanıcı hakları sadece gereksinim duyan kullanıcılara verilmelidir.
- Yedekleme ve yedekten dönme haklarından, sunucu işletmenlerini çıkarınız ve bu hakları sadece, yedekleme işletmenlerine veriniz.

10.3.9 Ağ güvenliği

- Sistemin niteliğine göre kullanımına ihtiyaç duyulmayan ağ hizmetlerini sistem üzerinden kaldırınız.
- Windows NT, Windows ailesinden olmayan bazı işletim sistemlerine açık metin olarak şifre gönderme özelliğine sahiptir. Bu özellik,

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDR
\Parameters

kayıt girişindeki REG_DWORD "EnablePlainTextPassword" parametresine 1 değeri atanarak iptal edilebilir.

- Windows NT alan ağında oturum bilgilerinin çalınmasını önlemek ve sistem bütünlüğünü sağlamak için kullanılan SMB imzalama yöntemi,

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
\LanManServer\Parameters

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
\Rdr\Parameters

kayıt girişlerindeki REG_DWORD "EnableSecuritySignature" ve "RequireSecuritySignature" parametrelerine 1 değeri atanarak aktif edilir.

- Windows NT LANMAN biçiminde, kimlik doğrulamada kullanıcı şifrelere ağ üzerinde taşınmaktadır. Bu durum Windows NT işletim sistemini saldırılar karşısında güçsüz bırakmaktadır. Windows NT işletim sisteminin bu biçimi kullanmasını engellemek için,

HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA

kayıt girişindeki REG_DWORD "LMCompatibilityLevel" parametresine 2 atanmalıdır.

- Temel Windows NT hizmetlerinin intranet' ten ayrılması: Windows NT alan ağında yönlendirilemeyen NETBEUI protokolü kullanılarak, Windows NT alan ağında dolaşan bilgilerin, intranet üzerindeki yönlendiricilerin çoğu tarafından alınmasını engellenebilir.

Öte yandan, TCP/IP gibi yönlendirilebilen bir protokol kullanılması durumunda ise, bu temel hizmetler tarafından kullanılan TCP ve UDP kapıları (137-139) yönlendiriciler tarafından engellenerek, intranet' teki diğer elamanların temel Windows NT hizmetlerine erişimi engellenir.

- Windows NT TCP/IP protokolünün güvenlik seçeneklerinden TCP ve UDP kapı sınırlaması yapılabilmektedir. [30]

10.3.10 Uzaktan erişim hizmeti (Remote access service – RAS)

- Kullanıcıların kurum ağına uzaktan erişimi sadece, uzaktan erişim sunucuları ile sınırlandırılabilir. Bu ağa erişimle ilgilenmeyen bir kullanıcı için mantıklı bir

sınırlamadır. Bir Windows NT ağında yerel hesaplar sadece tanımlandıkları makineye erişim hakkına sahiplerdir. Buradaki senaryoda bu makine RAS makinesidir. Windows NT alan ağına bu erişim

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
RemoteAccess\Parameters\NetbiosGateway

kayıt girişindeki "NetbiosGatewayEnabled" parametresine aktif edilmesi gereklidir.

- İstemci kullanıcısı tarafından yapılandırılması gereken RAS parametreleri mevcuttur. Örneğin kullanıcı şifreleme açısından "Accept only Microsoft encrypted authentication" seçeneğini seçilmeleir.

10.4 UNIX ve NT İşletim Sistemlerinin Karşılaştırılması

Windows NT sabit bir çalışma ortamı sağlayan açık bir sistemdir. UNIX' ten farklı olarak, herkese açık uygulama programlama arabirimi (Application Programming Interface – API) ile tekil ve tutarlı bir geliştirme ortamı sunar. Yine UNIX işletim sisteminden farklı olarak, standart donanımlarda çalışma ve üzerinde çalışan birçok uygulamanın varolması özelliklerine sahiptir. UNIX işletim sistemlerinin bir tipinde yazılan uygulamalar diğer tipinde çalışabilmek için derlenmeden önce önemli değişiklikler gerektirebilir.

Windows Dağıtık İnternet Mimarisi (DNA) ve COM ölçeklenebilir ve dağıtık uygulamaların geliştirilmesi sürecini kolaylaştırmıştır. Windows Parça Hizmetleri (Windows Component Services) katmanı iş iplikleri (thread), kaynaklar, dağıtım ve paralelliği sağlamaktadırlar. Uygulamalar Windows hizmetlerinin kullanımı ile kolayca yüklenmekte ve merkezi olarak yönetilebilmektedir. COM ve DCOM varolan ortamların sayısal sinir ağı ile bütünleşmesini sağlamak ve bütünleştirilmiş bir geliştirme ortamı oluşturmaktadır.

Öte yandan, UNIX çağırma seviyesi API' ler kullanır ve bütünleştirme bağımsız yazılım geliştirici firmalara bırakılmıştır. COM' un rakibi olan CORBA ile yazılım geliştirmek kolay olmakla birlikte, bu yazılımları başka ortamlara yüklemek uzun ve zor bir iştir. Bu nedenledir ki son yıllarda EJB teknolojisi üzerinde yoğunlaşılmaktadır.

Windows NT sunucusu bağlı olduğu ağ ve sunucularının güvenilirliğini ve hazır bulunabilirliğini artırır; böylelikle sistemin hizmet verememe zamanını azaltır. Computerworld tarafından 102 kurum bilgi sistemleri yöneticisi arasında yapılan

araştırmada, bilgi yöneticilerinin %45' i Windows NT işletim sisteminin toplam maliyet sahipliği (total cost of ownership – TCO) koruması bakımından en iyi seçenek olarak bildirmişlerdir. Cahners In-Stat Group/BRG tarafından yapılan diğer bir araştırmada ise, Windows NT, SPARC sunucuları üzerinde çalışan Solaris işletim sistemine göre %37 daha düşük TCO' ya sahip olarak çıkmıştır (bknz Tablo 10.4) [32]

Firewall' lar, şifreleme aletleri ve diğer parçalar sistem güvenliğinde önemli bir yer tutsalar dahi, sunucu işletim sistemi sistem güvenliğinin en önemli parçasıdır. Şirketlerin birbirleriyle rekabetlerini sürdürmesinde önemli olan, ürünleri sadece sağladığı güvenlik özelliklerine göre değerlendirmemeli, değerlendirmeye ürünlerin maliyeti ve güvenlik sisteminin ticaret üzerindeki etkisi de katılmalıdır.

Windows NT işletim sisteminde güvenlik, temel işletim sistemi ile bütünleştirilmiştir. Windows NT işletim sisteminin güvenlik özellikleri, işletim sisteminin grafiksel yönetim araçları ile bütünleştirilmiş olmakla birlikte, komut istemcisi ve kod parçası araçlarından da erişilebilir. Windows kullanılan donanıma bağlı olmaksızın tekil ve birbirleriyle ilişkili yönetim ve güvenlik araçları sağlar. Bu iş işletimlerinde en az etkiyle gerekli güvenlik seviyesinin sağlanmasının maliyetini büyük ölçüde azaltır.

Tablo 10.4 TCO (yıl başına, kurum başına)

Yıllık Maliyet	Windows NT Server/ Compaq	Sun Solaris/ SPARC	% Difference
İlk sistem satın alma ücreti	367,250	791,190	54%
İlk sistem kurulumu, bütünleştirilmesi ve eğitim	13,300	17,860	26%
Sistem ve ağ artırımları (upgrade)	10,310	17,190	40%
Sistem ve ağ yönetimi insan kaynağı maliyeti	439,520	605,990	27%
Uygulama geliştirme ve bakım maliyeti	392,870	664,060	41%
Yıllık teknik destek ve artırım maliyeti	25,040	40,320	38%
Toplam yıllık sahiplik maliyeti	1,248,290	2,136,620	42%
TCO (sunucu başına)	42,130	56,270	25%
TCO (kullanıcı başına)	1,350	2,160	37%

Tablo 10.5 Windows NT ve UNIX güvenlik özellikleri karşılaştırması

	Windows NT	UNIX
Kimlik Doğrulama	- Sisteme erişimden önce gereklidir. - Güvenilen yol (CTR-ALT-DEL tuş kombinasyonu) ile sistem truva atlarına karşı korunur. - Kimlik doğrulama kullanıcı ismi ve şifre ile gerçekleştirilir. - Şifre dosyalarını şifreleyebilir. - Dağıtık uygulama kimlik doğrulamasını destekler.	- Sisteme erişimden önce gereklidir. - Güvenilen yol yoktur. - Kimlik doğrulama kullanıcı ismi ve şifre ile gerçekleştirilir. - Şifre dosyalarını saklar. - Kerberos eklentisine destek verir.
Erişim Kontrolü	- Ayrık erişim kontrollerini destekler. - Güvenlik Başvuru İzleyicisinde gerçekleşmiştir. - Erişim hakları, erişim kontrol listelerinde saklanır. 27 farklı kullanıcı hakkı vardır.	- Ayrık erişim kontrollerini destekler. - Dosya sistemi ve diğer çekirdek yerleşimlerinde gerçekleşmiştir. - Erişim hakları, kullanıcı, grup ve diğer biçim bit'lerinde saklanır. "Setuid" dosya üzerinde işlem yaparken bir kullanıcının diğer bir kullanıcı gibi davranmasını sağlar.
Eylem Sorumlularının Belirlenebilmesi	Kullanıcıları tekil olarak tekil olarak tanımlayan, kullanıcı ismi ile ilişkilendirilmiş güvenlik tekil tanımlayıcıları kullanılır.	Kullanıcıları tekil olarak tanımlayan kullanıcı tekil tanımlayıcıları kullanılır.
Raporlama	- Sistem üzerinde meydana gelen güvenlik olaylarının kaydedildiği, olay kayıtları mevcuttur. - Sistem bazında, tüm uygulamalar için tek bir kayıt dosyası vardır.	Olaya özel, birden fazla kayıt dosyaları mevcuttur.
Güvenlik Bölmeleme	- Güvenlik alanları ayrılmıştır. - Kullanıcı ve çekirdek adres alanları birbirinden ayrılır. - Çekirdeğin işlevselliği tek bir modülde gerçekleşir. - Nesneler tekrar kullanılmadan önce temizlenir.	- Güvenlik alanları ayrılmıştır. - Kullanıcı ve çekirdek adres alanları birbirinden ayrılır. - Çekirdeğin işlevselliği dağıtık olarak gerçekleşmiştir. - Nesneler tekrar kullanılmadan önce temizlenir.
Bütünlük	- Erişim kontrol listeleri işletim sistemini korur. - Yazılım kaynak kodlarının doğrulanması için "Authenticode"	- İşletim sistemini korumak için biçim bitleri kullanılır. - Yazılım kaynak kodlarını doğrulayacak bir mekanizmaya

	teknolojisi kullanılır. • Bütünlüğü sağlamak için standart bir kriptografik arabirim (CAPI) kullanılır. • Hazır bulunabilirlik için bütünleşik dosya sistemi araçları kullanılır.	sahip değildir. • Kriptografik olarak güçlü kontrol toplamları ve sayısal imzalar sağlayan GSS-API kullanırlar. • Hazır bulunabilirlik için ek dosya sistemi araçları kullanılır.
Gizlilik	• CAPI kullanır. • Güvenli RPC kullanır. • PPTP ve SSL kullanımını destekler. • IPSEC eklentisine destek verir.	• GSS-API kullanır. • Güvenli RPC kullanır. • SSL yardımcı araçları vardır. • IPSEC eklentisine destek verir.
Yönetilebilirlik	• Varsayılan olarak düşük güvenlik seviyesinde kurulur. • Tek bir araçtan tüm sistem güvenliği yönetilebilir. • Düşük seviyede bir yetenek yeterlidir.	• Varsayılan olarak düşük güvenlik seviyesinde kurulur. • Birçok satıcı tarafından üretilmiş araçlarca sistem yönetimi gerçekleştirilir. • Çok yüksek seviyede yetenek gerektirir.

Windows NT kurumsal güvenlik ihtiyaçlarını UNIX kadar iyi bir şekilde sağlamakla birlikte raporlama ve erişim kontrollerinde UNIX işletim sisteminden daha iyidir (bkz. Tablo 10.5). Windows NT işletim sisteminin güvenlik yönetimi, UNIX işletim sistemine göre daha kolaydır. Çünkü Windows NT güvenlik özellikleri işletim sistemi yönetim araçları ile bütünleştirilmiştir. [33]

10.5 “Checkpoint Firewall-1”

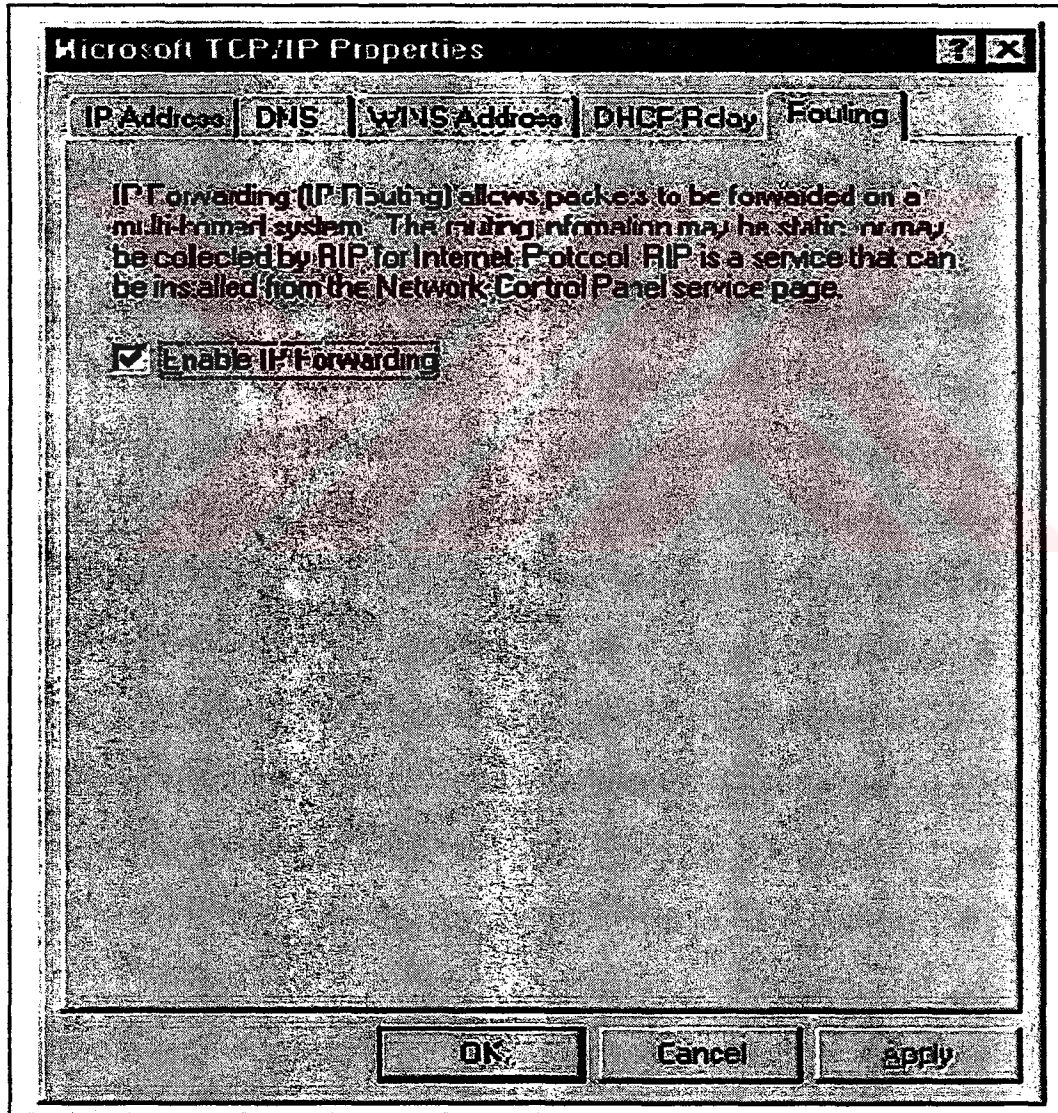
10.5.1 Kurulumdan önce yapılması gerekenler

1. Ağ bağdaştırıcısı kurulurken sadece TCP/IP protokolü kurulmalıdır. “Firewall-1” için statik bir IP kullanılmalıdır; dolayısıyla DHCP kullanılmamalıdır. DNS sunucusu kullanımı aktif değil ise, kurulum sırasında aktif edilmemelidir. DNS kullanılması gerekirse “Firewall-1” kurulduktan sonra aktif edilebilir.
2. Windows NT işletim sistemi kurulduğunda, Bilgisayar Tarayıcı (Computer Browser), NetBIOS Arabirimi (Interface), RPC Yapılandırma (Configuration), Sunucu (Server), İş İstasyonu (Workstation) varsayılan olarak kurulmaktadır. “Firewall-1” çalışmak için bu hizmetlerin hiçbirine ihtiyaç duymaması ve bu hizmetlerin olası güvenlik tehlikeleri içermesi nedeniyle, bu hizmetlerin sistem güvenliği açısından iptal edilmesi gereklidir. [34]

3. Windows NT işletim sisteminde Şekil 10.4' teki ekrandna IP iletme seçeneği seçilmelidir. Aynı zamanda sadece dış ağ bağdaştırıcısı için varsayılan geçityolu (default gateway) adresi tanıtılmalıdır. İç arabirimler için varsayılan geçityolu tanımlanmamalıdır.
4. Şekil 10.5' teki ekrandaki, Ağ bağdaştırıcısı üzerinde WINS istemcisi etkisiz kılınmalıdır. Ayrıca Windows NT hizmetler (services) penceresinde WINS istemcisi hizmetinin başlama seçeneği elle başlatma (manual) olarak seçilmelidir. [35]

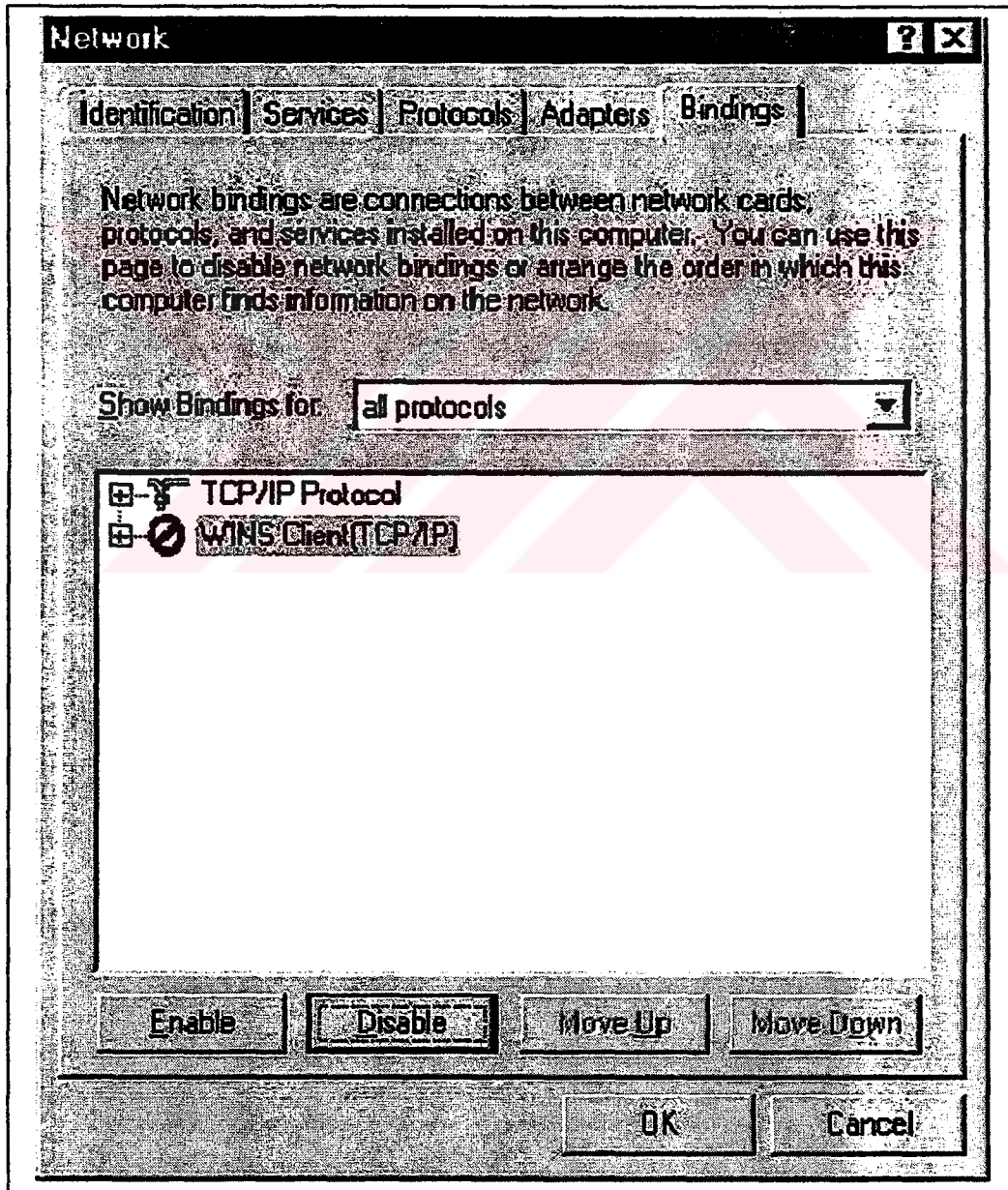
10.5.2 Kurulum

1. Kurulum dosyaları arasından "Setup" uygulaması çalıştırılarak, kurulum başlanır



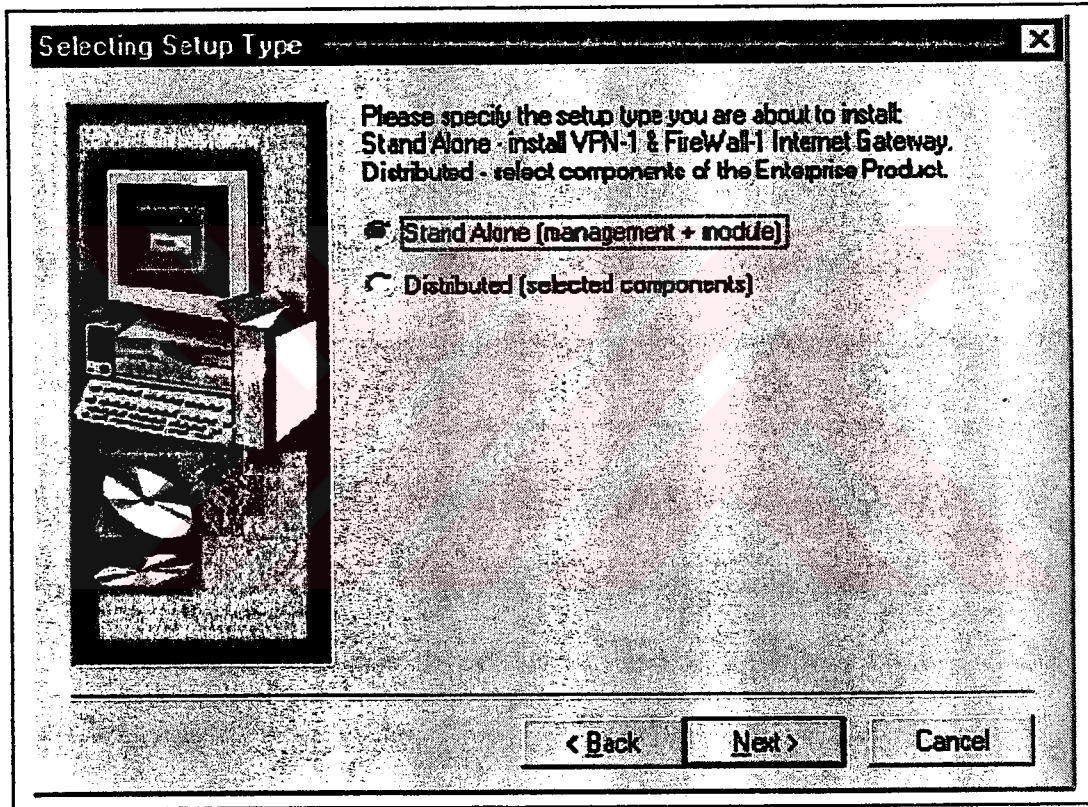
Şekil 10.4 Windows NT IP iletme seçim ekranı

2. Hoşgeldiniz (Welcome) penceresinde ileri (next) düğmesine basılarak kurulum devam edilir.
3. Kurulum tipinin seçilmesi (Selecting Setup Type) ekranında (bkz. Şekil 10.6), "Stand alone" seçeneği seçilir. "Stand alone", firewall ve yönetim modülünün aynı makineye kurulması durumunda seçilmelidir. Diğer seçenek "Distributed" bu modüllerin farklı makinelere kurulması anlamına gelmektedir.
4. Şekil 10.7' deki ekrandan, kuracağınız firewall ürününün tipini seçiniz. Ekrandan da görüldüğü gibi "VPN-1 & Firewall-1 Gateway Moudle-Limited hosts(25 to 100)" seçeneği seçilmiştir. Bu ürün tipleri lisans tiplerine göre oluşmaktadır.



Şekil 10.5 Windows NT ağ bağlamaları ekranı

5. Bu ekrandan sonraki ekranlarda, kurulacak ürün tipleri "Firewall module" ve "Inspection Module" seçilir.
6. Şekil 10.8' de görülen ekranda, ürün lisans bilgileri sisteme tanıtılır.
7. Şekil 10.9' daki ekranda GUI istemcisi yöneticisi tanımlanır. Bu ekranda tanımlanan yönetici, GUI istemcisine bağlanma ve bu sayede de "Firewall-1"i yönetme hakkına sahiptir. Bu ekranda tanımlanacak kullanıcının ismi şifresi ve "Firewall-1" üzerindeki erişim hakları sisteme tanımlanır. [36]
8. "Firewall-1" ürünün kurulduğu makinenin IP adresi Windows NT işletim sisteminin "hosts" dosyasından getirilir ve ekranda gösterilir. Eğer bu IP adresi doğru ip adresi değil ise kurucuya değiştirme imkanı tanınır.



Şekil 10.6 "Firewall-1" kurulum tipi seçme (Selecting setup type) ekranı

9. "Firewall-1" in uzak bilgisayarlardan yönetilmesi gerektiği durumlarda, GUI istemcisi ekranında "Firewall-1" i uzaktan yönetecek konağın adı yazılır.
10. Şekil 10.10' daki ekranda, "Firewall-1" in kurulu olduğu makinenin dış arabirimi ismi girilir. Ağ bağdaştırıcısının arabirim ismini öğrenmek için, işletim sisteminin komut istemcisinde "ipconfig" komutunu çalıştırınız. Ekranda oluşan çıktının "Ethernet Adapter EPRO1" satırındaki "EPRO1" ağ bağdaştırıcısının arabirim ismidir.

11. Daha sonraki ekranda, "Firewall-1" in IP iletmesini kontrol edip etmeyeceği seçilir. Seçilmesi gereken seçenek "Firewall-1" in IP iletmesini kontrol etmesidir. Çünkü "Firewall-1" in çalışması durduğunda, makine üzerinden kontrolsüz paket geçişinin de drudurulması gereklidir. Bu da makine üzerinde IP iletme seçeneğini kapalı olmasını gerektirmektedir. "Firewall-1" çalışması durduğunda, makinenin ağ bağdaştırıcıları üzerindeki ip iletme seçeneğini de kapatarak, ip paketlerinin ağ bağdaştırıcıları arasında ilettilmesini engeller.
12. "Key Hit Sessions" ekranında, rastgele anahtar üretimi için rastgele karakterler ekrana girilir ve ileri (next) tuşuna basarak anahtar üretilir.
13. Bitir (finish) düğmesine basılarak kurulum ve yapılandırma işlemi sona erdirilir. [37]

10.5.3 Kayıt komutları

"Excessive log grace period (sec)"

Firewall üzerinden geçen benzer aynı paketlerin kayıtlarının birkez alındıktan sonra, ikinci kez ne kadar zaman sonra alınacağını gösterir. Bu sürenin uzun olması, sistem üzerinde daha az kayıt oluşturmakla birlikte, sisteme gerçekleştirebilecek saldırının sezilmesi olasılığını azaltmaktadır. Bu değerin düşürülmesi kayıt değerlendirmelerindeki doğruluk oranını artıracaktır. Bu değerin 30 saniye, mümkünse daha düşük olması gereklidir.

10.5.4 Uyarı komutları:

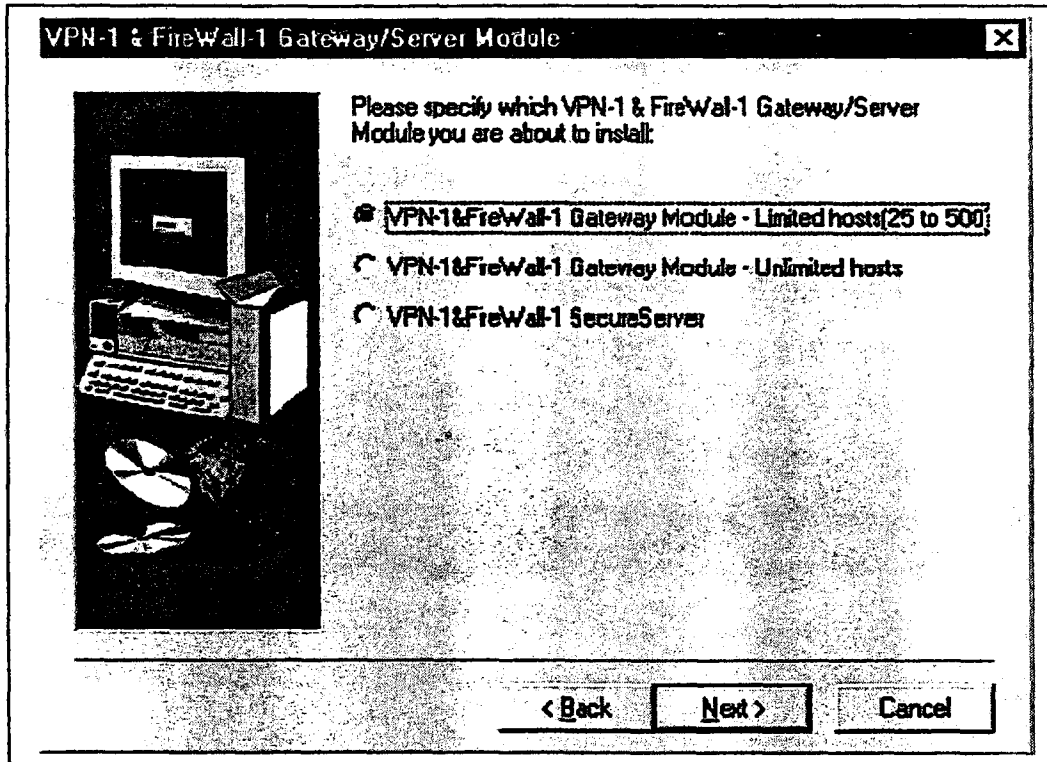
"Checkpoint Firewall-1" de uyarı, aşağıdaki şekillerde gerçekleştirilir:

"Popup alert command"

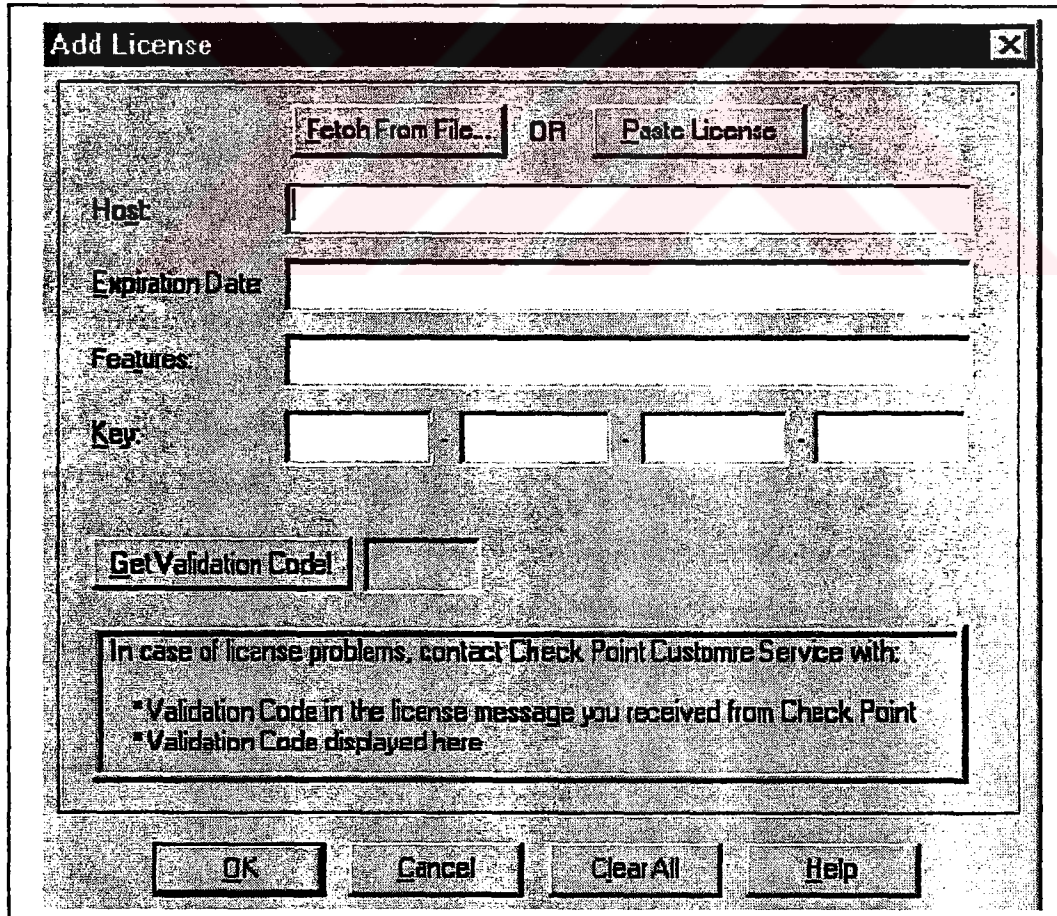
Varsayılan değeri "ok" olan bu uyarı mekanizması, uyarı oluştuğunda çalıştırılması gereken komutu belirtir.

"Mail alert command"

Herhangi bir uyarı oluştuğunda, sistem yöneticisine elektronik posta ile haber verilir. Windows NT sistemlerinde, "Firewall-1" ürünü üzerinde, elektronik posta sunucusu mevcut değildir. Bu işlemi kullanmak için "Firewall-1" makinesi üzerinde SMTP sunucusu kurmak gerekirse, güvenlik gediği oluşması olasılığı nedeniyle, bu işlem "Firewall-1" kurulumundan önce gerçekleştirilmelidir. Elektronik posta göndermek için başka makine üzerindeki, SMTP sunucuları da kullanılabilir.



Şekil 10.7 "VPN-1 & Firewall-1 gateway/server module" ekranı



Şekil 10.8 Lisans bilgileri ekranı

Add Administrator

Administrator Name:

Password:

Confirm Password:

Management Clients Permissions:

☒ **Read/Write All**
This is the only permission that enables editing policy objects.

☐ **Customized:**

- ☒ Edit Users database(s)
- ☒ Security Rules
- ☒ Bandwidth Rules
- ☒ Compression Rules
- ☒ Log Viewer
- ☒ System Status

☐ No permissions

Reporting Clients Permissions:

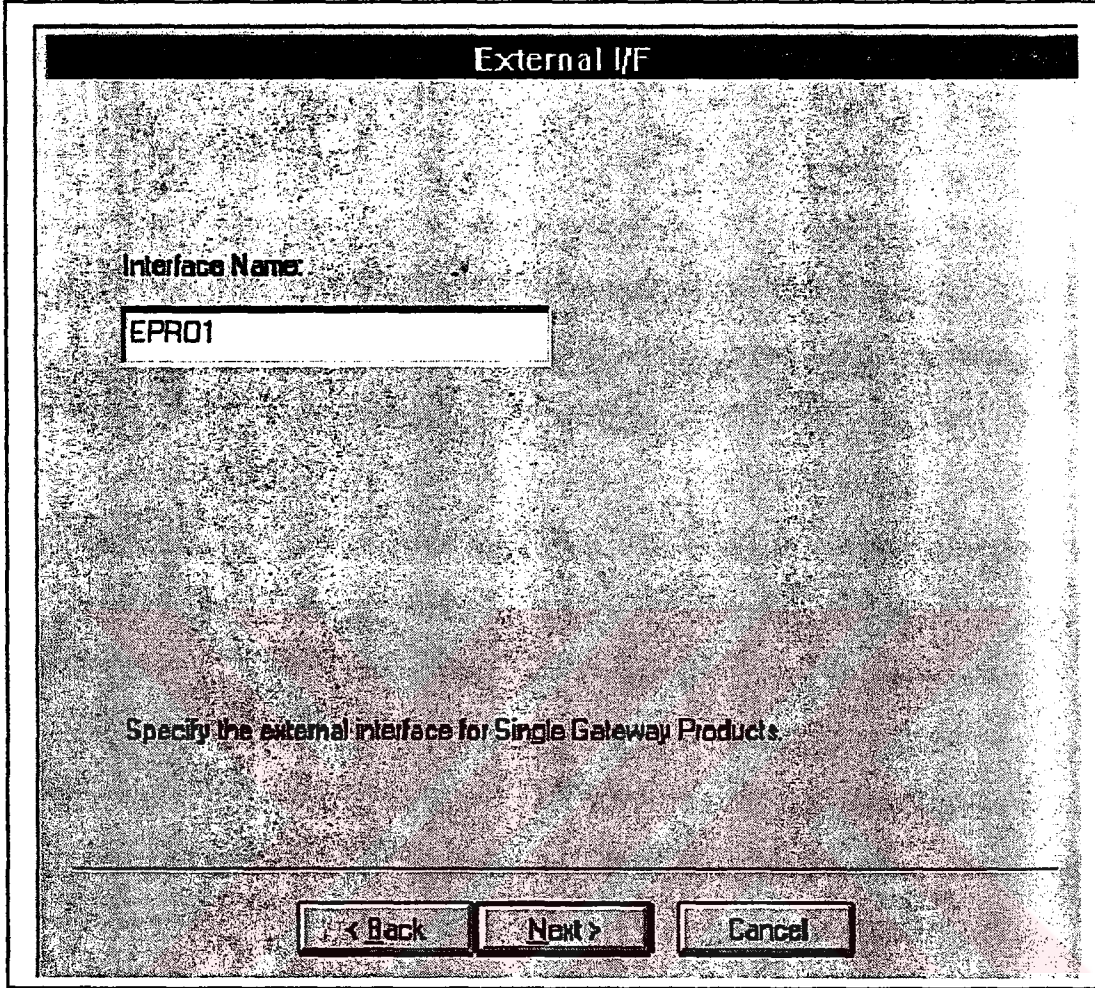
- ☒ Reporting Tool
- ☒ Log Consolidator

Şekil 10.9 GUI istemcisi yönetici tanımlama ekranı

“SNMP trap alert command”

SNMP tuzak gerekli eylem olarak seçildiğinde çalışması gerekli komutları belirtir. UDP temelli hizmet olan ve uyarı mesajının alıcısından onay beklemeyen SNMP ve SNMP tuzaklarda, SNMP tuzakların gönderileceği makine “localhost”, yani firewall makinesinin kendisi olarak seçilmiştir. Bunun yerine, SNMP kontrol biriminin olduğu makinenin IP adresi girilmelidir. SNMP kontrol biriminin

adresinde DNS isimleri kullanılmamalıdır. Çünkü, saldırgan gerçekleştirebileceği bir DNS saldırısı ile firewall sistemini kandırır ve SNMP tuzakların başka makinelere gönderilmesine neden olabilir.



Şekil 10.10 Dışsal arabirim ekranı

"User defined alert command"

Uyarı gerektiren bir durum oluştuğunda kullanıcı tarafından tanımlanmış bir program "Firewall-1" tarafından çalıştırılır. SMS veya çağrı mesajları gibi üçüncü parti yazılımların kullanımı bu şekilde sağlanabilir.

"Anti spoof alert command"

IP taklidi saldırıları sezilince gerçekleştirilecek eylemler tanımlanır. Taklit edilen IP adreslerinin kullanımı, "Firewall-1" makinesinde tüm arabirimler üzerinde IP taklidi saldırısı yapılandırması yapılarak engellenir. Herhangi bir IP taklidi saldırısı teşebbüsü, elektronik posta, SNMP tuzak veya üçüncü parti bir uygulama kullanılarak sistem yöneticisine bildirilir.

“User authentication alert command”

Kullanıcı kimlik doğrulamada oluşan hatalar, hata uyarı mekanizmalarınca sistem yöneticilerine bildirilir. Bu hatalar, yine elektronik posta, SNMP tuzak veya üçüncü parti bir uygulama kullanılarak sistem yöneticisine bildirilir.

“IP options drop track”

Seçenek sahasında veri içeren IP paketleri, “Firewall-1” tarafından otomatik olarak düşürülür. Böyle paketler için kaydetmenin yanı sıra, yüksek öncelikli uyarılar üretmek doğru bir karar olacaktır.

“Log established TCP packets”

Kurulmuş veya zaman aşımını uğramış TCP bağlantılarında hareket eden paketlerin kaydı tutulmalıdır. Bunun içinde “Log established TCP Packets” seçeneği seçilmelidir.

10.5.5 Hizmetler

“Enable FTP PORT Data Connections”: “Firewall-1” in koruduğu ağdaki kullanıcıların FTP kullanarak, internet’ ten dosya indirmesini sağlamak için bu seçeneğin aktif edilmesi gereklidir.

“Enable FTP PASV connections”

Kullanıcıların, web tarayıcısı ile dosya indirmelerin sağlanması için aktif edilmesi gereklidir. Bunun yanında “FTP PASV” bağlantılarına izin verilmesi yüksek seviyede güvenlik tehdidi oluşturabilir. Dışarıdaki kullanıcılara dosya indirme imkanı tanıyan bir FTP sunucusuna, dışarıdan “FTP PASV” bağlantılarına izin verilmemesi gereklidir.

“Enable RSH/REXEC reverse stderr connections”

“RSH” ve “REXEC” komutlarına “stderr” dosyası için ters bağlantı açmalarına izin verilmesi gereken durumlarda aktif edilir. Bu hizmetin aktif edilmesi birçok güvenlik tehlikesini de beraberinde getirir. Bu nedenle kullanımı belgelenmiş nedenlerden ötürü gerekmediği durumlar dışında kullanılmamalıdır.

“Enable RPC control”

Aktif edildiğinde sistem için tehlike oluşturan bir seçenektir. Belgelenmiş bir gereksinim olmadığı sürece aktif edilmemelidir. Bu hizmet girilen konak üzerinde hangi hizmetlerin çalıştığı ile ilgili bilgi almak için kullanılır.

10.5.6 Diğer Güvenlik önlemleri

“Log viewer resolver properties”

“Firewall-1” deki kayıt değerlendirmelerindeki başarımların düşüklüğünün ortadan kaldırılması için iptal edilmesi gereklidir.

“Security server settings”

“Firewall-1” in, FTP, Telnet, Rlogin gibi uygulama seviyesi vekilleri olan güvenlik sunucuları çalıştırıldığında, “Firewall-1” bağlantı sırasında, varlığını belirten bir sloganı istemci ekranında gösterir. Bu da saldırıya sistem üzerindeki Firewall ürününün tipi hakkında bilgi verir. Böyle bir durumda ekranda tüm erişimlerin kaydının tutulduğunu belirten bir uyarı mesajı yayınlanmalıdır.

“SYNDefender settings”

SYN saldırısı, bir konağa taklit edilmiş bir ip adresinden büyük miktarlarda SYN paketleri gönderilerek düzenlenir. Birçok durumda, bu paketler sistem başarımlarını düşürür, hatta işletim sistemini çökertir. “Firewall-1” SYN saldırısına karşı iki farklı yaklaşım içerir.

1. “SYN Defender Relay”: “Firewall-1” A konağına giden SYN paketini keser.

1 Z ———— SYN ———— → FW-1 A

“Firewall-1” SYN paketini A'ya geçirmez ve A konağının yerine Z' ye SYN/ACK mesajı gönderir.

2 Z <——— SYN/ACK ——— FW-1 A

Eğer Z'den ACK cevabı alınırsa Firewall SYN paketini A' ya geçirir.

3 Z ———— ACK ———— → FW-1 ———— SYN ———— → A

FW-1 <——— SYN/ACK ——— A

FW-1 ———— ACK ———— → A

Eğer “Firewall-1” bu aşamaların herhangi birinde saniyelerce cevap alamazsa veya ACK veya SYN/ACK mesajı beklerken RST mesajı alırsa bağlantıyı sonlandırır.

2. “SYN Defender Gateway”: Firewall SYN paketini keser ve bu olayı durum tablosuna kaydederken SYN paketinin A konağına geçmesine izin verir.

1 Z ———— SYN ———— → FW-1 ———— SYN ———— → A

Firewall A' nın cevabını keser.

2 Z FW-1 ←-----SYN/ACK-----A

Firewall SYN/ACK paketini Z' ye gitmesine izin verir. Bu arada A' ya da ACK gönderir.

3 Z ←-----SYN/ACK-----FW-1 A

Eğer bağlantı geçerli ise firewall Z' den ACK cevabı alır ve A' ya ACK gönderir. A ikinci ACK olduğu için bunu gözardı eder.

4a Z-----ACK-----→ FW-1 -----ACK ----→ A

Eğer bağlantı geçerli değilse zaman aşımı olur ve firewall A' ya RST mesajını yollar.

4b Z FW-1-----RST-----→

Bu saldırıya karşı "Firewall-1" in sunduğu çözüm, "SYN Defender Gateway" dir. Önerilen "SYNDefender" ayarları aşağıda gösterilmektedir:

- Yöntem = "SYN Gateway"
- Zaman aşımı = "10 saniye"
- Uyarı mesajıgörüntüleme = "Evet"
- En az oturum sayısı = "5000"

"Firewall-1" kayıtlarında böyle bir hata mesajı görüntülendiğinde, ağ paket izleyici yazılımları kullanılarak, taklit edilen IP adresi ve kaynak kapısı belirlenir ve aşağıdaki iki kural ile "Firewall-1" üzerinde önlem alınabilir:

1. Belirli IP adresine sahip IP paketlerinin durdurulması,
2. Kaynak adresinde geçerli bir IP adresi bulunmayan , IP paketlerinin durdurulması.

"Ping-Of-Death" saldırısı

64K' dan büyük "ping" paketlerini engellemek için yapılması gerekenler aşağıda sıralanmıştır:

1. Aşağıda sıralanmış parametrelere sahip generik servis tanımlanır.

Name: "long-icmp"

Type:"other"

Match field: "icmp, (ip_off & 0x2000)".

2. Tüm kaynak adreslerinden tüm varış adreslerine "long-icmp" paketleri durduran bir kural, kural veritabanına eklenir.

Ip_off & 0x2000 64 K' dan büyük paketlerin geçmesini engeller. Bunun çalışabilmesi için "property" panelindeki "accept ICMP packet without checking" seçili olmamalıdır. Aynı zamanda normal ICMP paketlerinin geçmesi için kural tabanında bu kuralın hemen ICMP paketlerini kabul eden bir kural girilir.

"Java Applet" lerin engellenmesi

Buradaki amaç herhangi bir Java applet' inin iç ağa girmesini engellerken, http protokolü ile dışarıya çıkışta sınırsız ve yetkisiz erişim sağlamaktır. "Firewall-1" de "URI resource" kuralların bir uzantısıdır. Burada her iki yönde http protokolünün geçişine izin veren ve java kodlarını engelleyen bir "URI resource" u tanımlanır. Bu işlemi gerçekleştirecek "URI resource" u aşağıdaki gibi tanımlanır:

Ekranın "general" bölümünde "URI Match Specification" kısmında "Wild Cards" seçilir. "Match" bölümünde "Schemes" kısmında "http", "Methods" kısmında "GET" ve "POST" seçilir. "Action" kısmında "Block JAVA code" seçeneği seçilir. "HTTP" protokolünü erişim izni vermek için tanımlanan kurala, "Add with resource" ile java kodlarını engelleyen kaynak eklenir.

10.5.7 Önerilen Kurallar

İstemcilerden dışarıya DNS sorguları

Güvenlik açısından, internet' e bağlanan tüm kullanıcıların internet' e DNS sorgusu yapmasına izin vermek yerine, cep görevi gören bir içsel DNS sunucusu kullanmak, sadece bu sunucunun dışarıdaki DNS sunucularına sorgu yapmasına firewall üzerinden izin vermek ve içsel kullanıcılarında bu DNS sunucusunu kullanmasını sağlamak doğru bir yaklaşım olacaktır. Bunun için firewall üzerinde tanımlanması gereken kural Tablo 10.6' da gösterilmektedir. [38]

Tablo 10.6 İç DNS sunucu kuralı

Kaynak	Varış	Kapı	Karar
DNSSunucu	İçDNSSunucu	53	Kabul

İçsel DNS sunucudan internet' e alan iletimi

İçsel bir DNS sunucunun olması durumunda, içsel DNS sunucudan, internet' teki diğer DNS sunucularına alan iletimi olasılığı da var olacaktır. Böyle bir durumda, kurumun iç ağ yapısı yetkisiz kullanıcılarca öğrenilebilme tehlikesini yaşayacaktır.

Bu nedenledir ki, ayrıık DNS sunucusu yapısı kullanılmalıdır. Bu yapıda, birincil ve ikincil DNS bilgileri, dışsal DNS sunucusunda tutulurken, içsel DNS sunucusuda sadece UDP sorgularına cevap veren ve cep işlevini yerine getiren bir DNS suncusu olarak kullanılmalıdır.

“Firewall-1” sisteminin korunması

“Firewall-1” kendini dışarıdan gelecek tehlikelere karşı, kendine gelecek tüm bağlantı isteklerini Tablo 10.7’ deki kural ile durdurarak korur. 256-259 arası kapı numaralarında, “Firewall-1” yönetim ajanları çalışmaktadır. Dışarıdan gelecek tehlikeleri karşı bu kapı numaralarına erişim kontrollü olarak verilmelidir.

Tablo 10.7. “Firewall-1” koruma kuralı

Kaynak	Varış	Kapı	Karar
Herkes	Firewall-1	Herkes	Red

Kural veritabanındaki en son kural

Tablo 10.8’ deki kuralın anlamı, bu en son kuraldan önceki hiçbir kuralın paketi kabul etmemesi durumunda paketin düşürüleceği anlamına gelmektedir.

Tablo 10.8 En son kural

Kaynak	Varış	Kapı	Karar
Herkes	Herkes	Herkes	Red

“Firewall-1” de “Drop” ve “Reject” farkı

“Drop”, kuralca kabul edilmeyen paketi hiç kimseye bildirmeden yok ederken, “Reject” kabul edilmeyen paketin sahibine, mesajın akibeti ile ilgili “Firewall-1” in varlığını belli edecek bir mesaj gönderir. Bu nedenle “Firewall-1” in gizliliğini sağlamak için “Drop” kullanımı tercih edilmelidir.

10.5.8 Implicit kurallar

“DNS rule zero rules”

Bu kurallar sistem için büyük bir güvenlik tehlikesi oluşturmaktadır. Bu nedenle bu kuralları etkisiz kılmak için, hem TCP, hem de UDP bağlantılar için “Accept Domain Name Queries” kontrol kutucuğunu iptal etmek gereklidir. Bunun yanında “Firewall-1” kural veritabanına girilecek kurallar ile de DNS sorguları kontrol altına alınmalıdır. Implicit DNS kuralları firewall’ ı baştan sona hiçbir engelle

karşılaşmadan geçen ve sistem güvenliği için büyük tehlikeler oluşturan Backorifice gibi araçlar doğurmuştur.

“Firewall-1 control connections”

“Firewall-1” in uzaktan yönetilebilmesini engellemek için bu bağlantıları iptal etmek gereklidir. Bu bağlantılar firewall üzerinde şu kapıların aktif olmasına neden olurlar:

- TCP Kapıları: 18181-18184, 256-259 ve 261.
- UDP Kapıları: 161.
- IP Tipi: 94 (IP çevrelemesi (encapsulation) içinde IP).

“TCP session timeout”

Varsayılan olarak seçilen 3600 saniye (1 saat) önerilen değerdir. Bu değer daha altına inildiğinde birçok kırılan bağlantı sorunu yaşanmaktadır. Diğer yandan bu sürenin gereğinden yüksek bir değere çıkarılması, saldırgan tarafından oturum bilgilerinin çalınabilmesi olasılığını artırmaktadır.

“Accept UDP replies”

Kaynak ve varış arasında bir UDP iletişimi başladığında, varış ile kaynak arasında da bir UDP cevap kanalı açılır. “Accept UDP Replies” seçeneği aktif edildiği durumda UDP cevap kanalının firewall üzerinden geçmesine izin verilir.

“Reply timeout”

UDP cevap kanalının herhangi bir paket gelmediği halde açık tutulacağı süredir. UDP cevap kanalından iletişim sona erdiğine ilişkin herhangi bir mesaj “Firewall-1” e gönderilmez. “Firewall-1” belirtilen sürede hiçbir mesaj alınmayan UDP cevap kanalını kapatarak UDP bağlantısını sona erdirir. Burada “Firewall-1” in vereceği varsayılan değer güvenli olan değerdir.

“Accept outgoing packets”

“Firewall-1” tarafından üretilen tüm trafiğin kabul edilmesine izin veren kuraldır. Ağ adres çevrimlerinin gerçekleştirildiği veya güvenlik sunucularının kullanıldığı durumlarda bu kural kullanılmalıdır. Bu seçeneğin aktif olması gereklidir. Aksi takdirde “Firewall-1” üzerinden hiçbir paket geçemez.

“Accept RIP”

Aktif olduğu durumda, bir dinamik yönlendirme bilgileri dağıtım protokolü olan RIP paketlerinin “Firewall-1” üzerinden geçmesine izin veren kuraldır. RIP bilgilerinin

“Firewall-1” üzerinden geçmesi zorunlu olmadığı durumlar dışında aktif edilmemelidir.

“Accept ICMP”

Bölüm 4’ te, TCP/IP potokolünün zayıflıklarında bahsedilmiş olan ICMP protokolü paketlerinin geçişini izin vermek içindir. Güvenlik açısından önerilen yapılandırma ICMP paketlerinin “Firewall-1” üzerinden geçişine izin verilmemesidir.

10.5.9 Başarım

“Firewall-1”, Checkpoint tarafından patentlenmiş durumsal inceleme (stateful inspection) teknolojisi ile inşa edilmiştir. Bu teknoloji ile uygulama seviyeli firewall’ lar gibi eski kuşak firewall’ lar tarafından gereksinim duyulan bağlam değiştirme yükünün ortadan kalkması, tüm iletişimin ağ katmanının altında kesilmesine olanak sağlaması ile gecikmenin azalması ve durumsal inceleme motorunun işletim sistemi çekirdeğinde çalışması ile CPU yükünün azalması sonucunda “Firewall-1” başarım yönünden çok büyük bir rekabet gücü kazanmıştır.

Windows NT 4.0 işletim sistemi kurulu, iki işlemcili (PIII 600), 256 MB Ram ve 4x10/100 ethernet arabirimli bir sistem üzerinde 4-6 istemcinin yarattığı ağ trafiği ile yapılan değerlendirmede, “Firewall-1”, 151.88 Mbps’ lik bir çıkış verimliliği (throughput) sağlamıştır.

10.6 “RealSecure”

10.6.1 Ağ yapılandırmasının sıkılaştırılması

“RealSecure” gizlilik biçimi

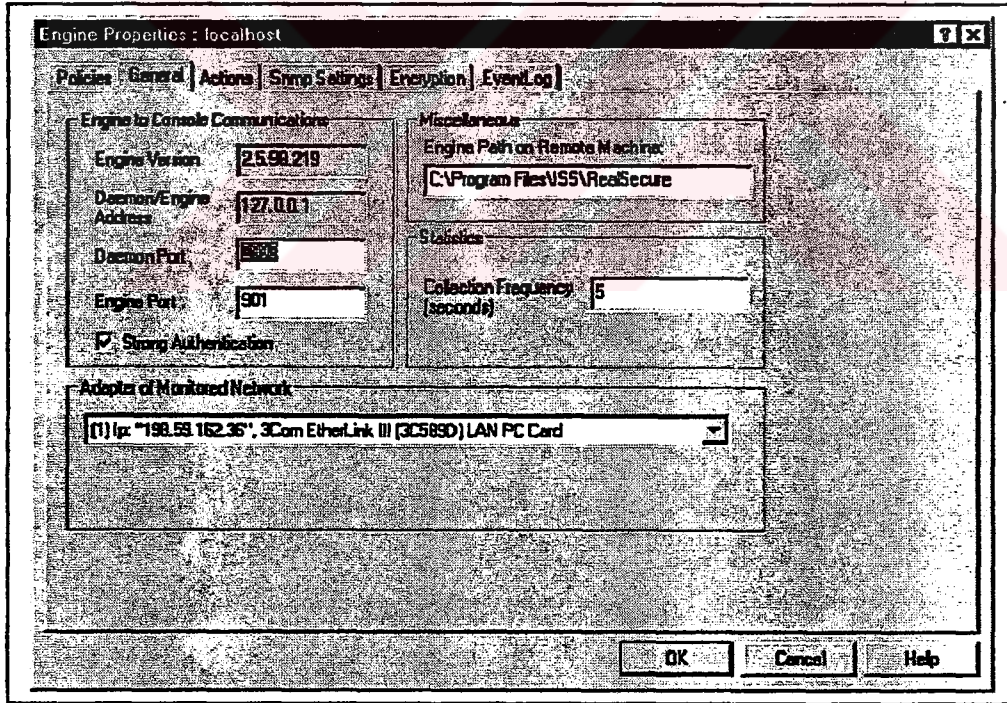
“RealSecure” saldırı sezme yazılımının gizliliğini sağlamak için aşağıdaki işlemlerin yapılması gerekecektir: [39]

- “RealSecure” motorunun çift ağ bağdaştırıcısı kullanması gerekecektir.
- İzlenen bölmedeki arabirim ile hiçbir ağ protokolü ilişkilendirilmeyecektir.
- Firewall üzerinde adanmış ağ arabirimi kullanımı gereklidir.
- Motor ve firewall arasında ayrılmış bir bölme oluşturulmalıdır.
- Bu gizlilik biçiminin kullanılması birçok yararı beraberinde getirmiştir. Motor üzerinde iki arabirim kullanılması, her bir arabirimin tek bir hedefi olması sonucunu doğurmuştur. Arabirimlerden hiçbir protokol ile ilişkilendirilmemiş olan izleme işlevini yerine getirirken, diğeri istemci yönetim programı (console) ile iletişimi kurar. Firewall üzerinde atanmış bir ağ arabirimi

kullanımı, ana internet trafiği ile motor ve istemci yönetim programı arasındaki ağ trafiğinin birbirine karışmasını engellemektedir. Ayrıca internet'e bağlı firewall arabirimi üzerinde, ek bir bağlantıya ihtiyaç yoktur. Firewall üzerinden içeri doğru bağlantı, internet üzerinden hiçbir şekilde erişilemeyen ayrılmış bir bölmeden geçer. Kısacası izlenen ağ üzerindeki arabirime erişilemez ve adreslenemez. Ayrılmış bölmedeki motordan veya motora iletişim firewall tarafından kontrol edilir. "RealSecure" daemon' unun hangi arabirim üzerine kurulması gerektiği ve motor ve daemon kapıları gibi parametrelerin seçildiği ekran Şekil 10.11' de gösterilmektedir.

Erişim kontrollerinin kullanılması

- "RealSecure" motor ve istemci programını aynı makinede kullanmak mümkün olmasına rağmen, başarımlı açısından önerilmemektedir. Bu nedenle "RealSecure" makinesi için sadece kullanılması gerekli protokol kapı ve hizmetlerin açık tutulması gereklidir. Şekil 10.12' deki TCP/IP güvenliği ekranında, "RealSecure" motor ve daemon kapı numaraları olan 901 ve 2998 numaralı kapılar iletişime açılır, diğerleri kapatılır. [40]



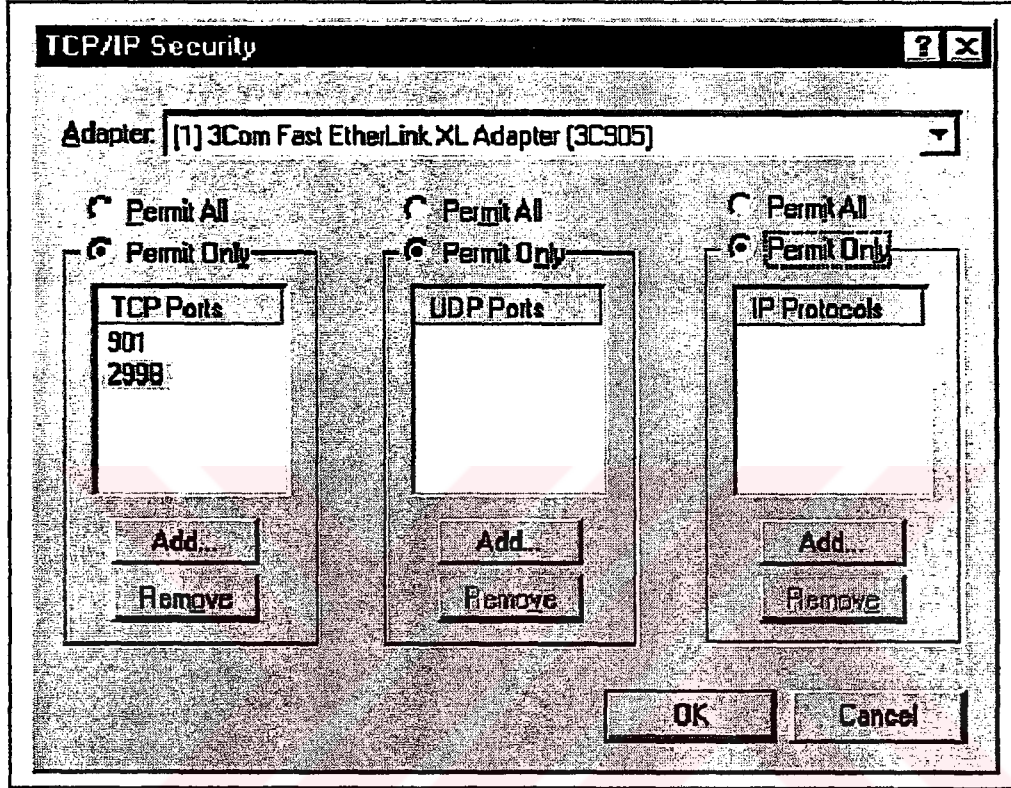
Şekil 10.11 "Real Secure" motor seçenekleri ekranı

10.6.2 "Firewall-1" ile "RealSecure" un bütünleştirilmesi

"RealSecure" herhangi bir saldırı girişimini sezdiğinde gerçekleştireceği eylemlerden birisi de, bu saldırı ile ilgili olarak "Firewall-1" i bilgilendirmektir. "RealSecure" motoru saldırı gerçekleştiren kaynak adresi, kapı ve/veya hizmeti kullanıcı tanımlı bir süre

kadar engellemesi için "Firewall-1" yönetim sunucusuna mesaj gönderir. "Firewall-1" kullanıcı tarafından tanımlanan bu süre sona erdiğinde ilgili kuralı, kural veritabanından siler. "RealSecure" ve "Firewall-1" arasındaki bu bağlantı, Şüpheli Eylem İzleme Protokolü (Suspicious Activity Monitoring Protocol – SAMP) tarafından sağlanır. İstek halinde bu bağlantı üzerinde kimlik doğrulamada gerçekleştirilebilir.

[41]



Şekil 10.12 Windows NT TCP/IP güvenliği ekranı

10.6.3 "RealSecure" kurulumu

"RealSecure" istemci kurulumu

1. Kurulumu başlamadan önce Microsoft Veritabanı Erişimi Parçaları (Microsoft Database Access Components – MDAC) 2.5 RTM ve "Internet Explorer 4SP1" veya daha ileri bir sürüm kurulmalıdır.
2. "Setup.exe" çalıştırılarak kurulumu başlanır, lisans bilgileri ekranı geçilir ve "Install RealSecure Console" seçeneği seçilir.
3. Programın kurulum klasörü seçildikten sonraki ekranda, eğer sistem üzerinde istemci programın eski sürümü kurulu ise yükseltme (upgrade) seçeneği ekranı görüntülenir. Bu ekranda "Use existing Log Database", "Back up existing Log Database", "Use existing Asset Database" ve "Back up existing Asset Database" seçeneklerinden bazıları seçili olarak gelecektir. Bu

seenekler seildiėinde varolan veritabanları kullanılırken, seilmemesi durumunda yeni veritabanları oluşturulacaktır.

4. Kurulum programı varolan gizli anahtarlar için sistem üzerinde bir araştırma gerçekleştirecektir. Araştırma sonuçları "OK" tuşuna basarak kabul edilir.
5. Daha sonraki ekranda şifreleme altyapısını oluşturacak kriptografik sağlayıcılar eklenir ve sıralanır.
6. "RealSecure" istemci programının kurulduğu, sistemin güvenliğini artırmak için "Setup to harden the files and registry entry for you" seeneėi için "Evet" seilir.
7. Daha sonraki ekranda bitir (finish) düğmesine basılarak kurulum sonlandırılır. [42]

"RealSecure" motor kurulumu

1. Kurulumu başlamadan Windows NT İş İstasyonu (Workstation) hizmeti açılır.
2. "Setup.exe" çalıştırılarak kurulumu başlanır, lisans bilgileri ekranı geçilir ve "Install RealSecure OS Sensor" seeneėi seilir.
3. Kurulum klasörünü seiniz ve kimlik doğrulama kuvveti seim ekranından kullanıcı kimlik doğrulama kullanıp kullanmayacağınıza seiniz.
4. Kurulum programı varolan gizli anahtarlar için sistem üzerinde bir araştırma gerçekleştirecektir. Araştırma sonuçları "OK" tuşuna basarak kabul edilir.
5. Daha sonraki ekranda şifreleme altyapısını oluşturacak kriptografik sağlayıcılar eklenir ve sıralanır.
6. Gizli anhtarın arşivlenmesi ekranında, gizli anahtarın bir kopyası, zarar görmesi ve silinmesi olasılığına karşı arşivlenir.
7. Daha sonraki ekranda, sadece sistem yöneticisinin "RealSecure" un hassas dosyalarına erişimine izin sağlamak için, sistem güvenliğinin artırılması seeneėi seilir.
8. Daha sonraki ekranda bitir (finish) düğmesine basılarak kurulum sonlandırılır.

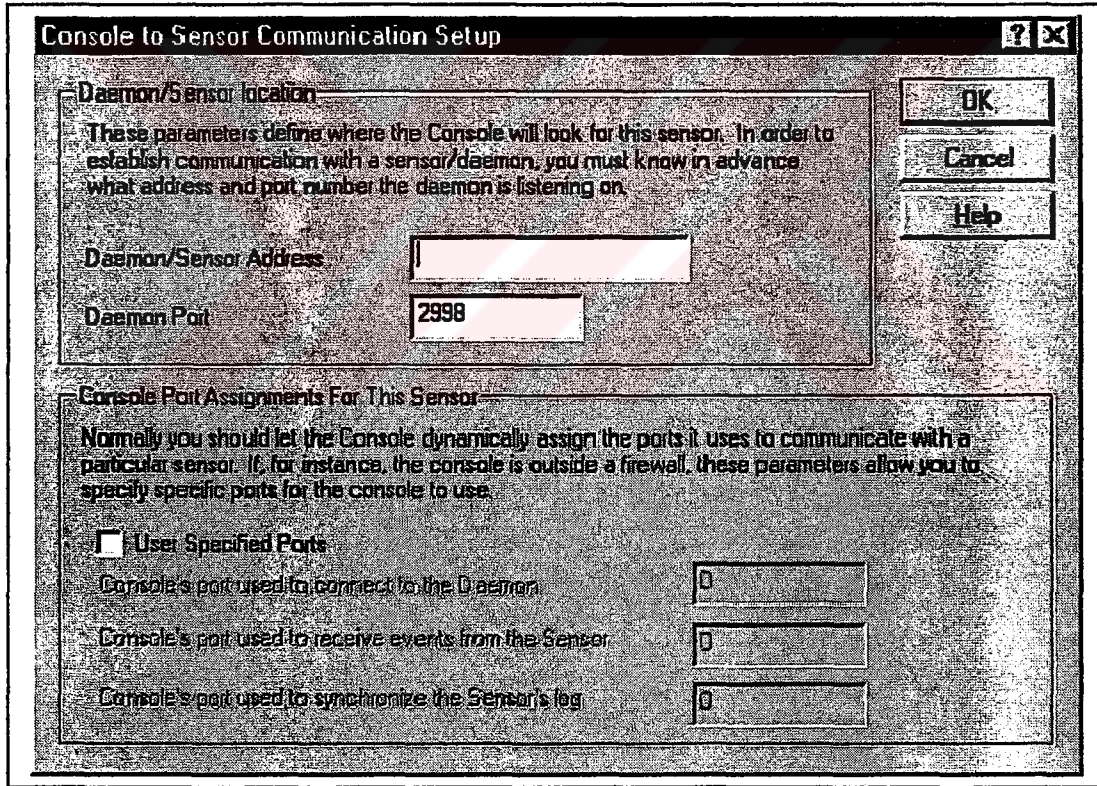
Kurulum sonrası

Kurulum sonrası "RealSecure daemon" unun kontrolü Windows NT hizmetler ekranından yapılabilir. Motorun, istemci program tarafından yönetiminin sağlanabilmesi için istemci program gizli anahtarının, motor programına tanıtılması gereklidir. Bunun için yapılması gereken işlemlerin aşamaları şunlardır:

1. İstemci program çalıştırılır, açık kimlikli doğrulama anahtarını ihraç et (export public authentication key) seçeneği seçilir ve gizli anahtar ihraç edilir.
2. Motor programı çalıştırılır, açık kimlik doğrulama anahtarını yükle (load public authentication key) seçeneği seçilir ve istemci programdan ihraç edilen gizli anahtar motora yüklenir.

“RealSecure” kullanımı

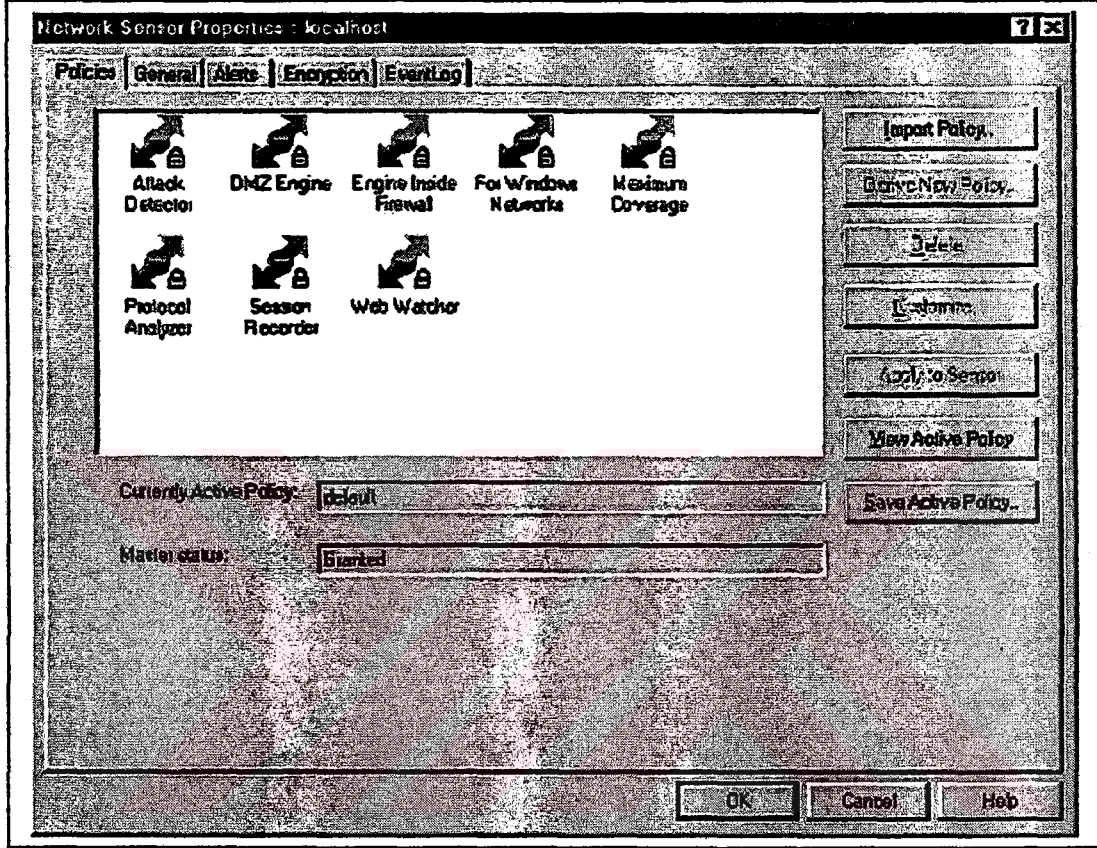
“RealSecure” istemci programı başlatıldığında motor sunucusuna bağlanabilmek için lisans bilgileri dosyasına ihtiyaç duyacaktır. Lisans bilgileri dosyası, “RealSecure” programının hangi IP numaraları üzerinde çalışabileceğini gösterir bilgiler içerir. Bu işlem gerçekleştirildikten sonra, Şekil 10.13’ teki ekrandan motor tanımlama işlemi gerçekleştirilir. Şekil 10.14’ teki ekranda “Deamon/Sensor Address” alanına motorun çalıştığı sunucunun IP numarası seçilir. Yine aynı ekranda görüldüğü gibi, “Real Secure” motoru 2998 kapı numarasından hizmet verir.



Şekil 10.14 Motor yerleşimi tanımlama ekranı

Saldırı sezme motoru “Sensors->Start” menü elamanına basarak başlatılır. Saldırı sezme motoru “RealSecure” istemci programından çıkılsa dahi çalışmaya devam eder. “RealSecure” motorunu durdurmak için “Sensors->Shutdown” menü elamanını seçmek gereklidir.

"RealSecure" ürününün çalışmasındaki diğer önemli bir nokta, kullanılan saldırı sezme politikası ve bu politikanın sisteme nasıl tanıtılacağıdır. "RealSecure" bilinen güvenlik sisteme gerçekleştirme tiplerine uygun bir takım, saldırı sezme politikalarına sahiptir. "RealSecure" motorunun hangi politikayı kullanacağı, Şekil 10.15' teki ekrandan seçilir. Motora uygulanacak politika seçildikten sonra, "Apply to Sensor" düğmesine basılarak, "RealSecure" motoruna yüklenir.



Şekil 10.15 Politika uygulama ekranı

Tüm bunlara ek olarak "Real Secure" ürünü kullanıcıların kendi politikalarını oluşturmalarını da izin verir.

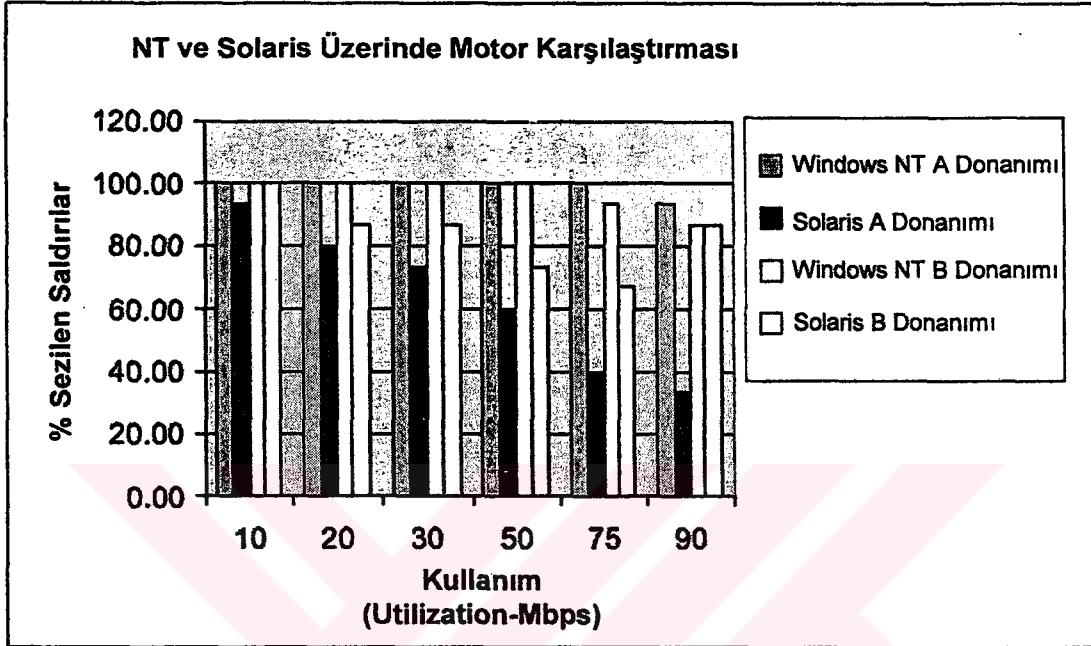
"RealSecure" başarımı

"RealSecure" saldırı sezme ürününün Solaris ve Windows NT işletim sistemi ile yapılan başarımlar ölçümleri sonucunda elde edilen karşılaştırmalı değerler Şekil 10.16' da görülmektedir. Bu başarımlar denemelerinde deneme altına alınan sistemlerin özellikleri aşağıda gösterilmektedir. [43]

- Windows NT A Donanımı: 1 Intel PIII, 550 MHZ işlemci, 128 MB bellek, Windows NT 4.0 SP 5, PCI veriyolu, Intel Pro/100 Ethernet Kartı.
- Windows NT B Donanımı: Çok işlemcili.

- Solaris A Donanımı SPARC Ultra II, 1 266 MHZ işlemci, 128 MB RAM, Sun Solaris 2.6, Sun 100 MB PCI Ethernet Kartı.
- Solaris B Donanımı: Çok işlemcili.

Bu sistem üzerindeki denemeler sırasında, "Real Secure" motorunda saldırı sezme (attack detector) politikası kullanılmıştır.



Şekil 10.16 Real Secure Başarımı

Şekil 10.16' daki başarımlar değerlerinde Windows NT işletim sistemi, %90 kullanım oranında, %85 saldırı sezebilme yeteneği ile çok yüksek yakalama oranlarında çalışmaktadır. Solaris işletim sisteminin düşük başarımlar vermesinin iki ana nedeni şunlardır:

1. Solaris 2.5.1-7 DLPI paket sürücüsünü düşük başarımlar,
2. Sun Sparc işlemcilerin, Intel işlemcilerden daha düşük saat hızlarında çalışmasıdır.

10.6.4 "Mailsweeper" Elektronik Posta Vekili

Bugün birçok firma internet üzerinden elektronik posta ile birbirleri ile haberleşmekte ve elektronik postaları günlük işlerinde kullanmaktadırlar. Bu veri akışı, elektronik postalar ile gelecek tehlikelere karşı firmaların kendilerini koruma gereğini doğurmaktadır.

Elektronik posta ile internet' ten gelebilecek tehlikeler şunlardır:

- Virüsler ve makro bombaları,

- Çöp (junk) elektronik postalar,
- Gizli bilginin yetkisiz iletimi,
- Uygun olmayan bilginin iletimi (kutsal şeylere saygısızlık gibi),
- Yasal sorumluluk.

“Mailsweeper” elektronik postalar için çok ayrıntılı bir içerik güvenliği sağlar. Kullanılan elektronik posta altyapısına göre elektronik posta yönlendiricisi olarak çalışır. “Mailsweeper” işlenmeyi bekleyen herhangi bir mesaj olup olmadığını anlamak için belli zamanlarda, elektronik posta sistemini kontrol eder. İşlenmeyi bekleyen her bir mesaj saklama ortamından alınır, parçalara ayrılır, doğrulanır ve tanımlanan kurala göre gerekli işleme tabi tutulur.

Yapılandırma

- Gereksiz elektronik posta (:anti-spam) yapılandırması: “Mailsweeper” bilinen kaynaklardan gelen elektronik postaları sezme ve engelleme yeteneklerine sahiptir. Şekil 10.17’ de listserver@company.com elektronik posta adresinden *@your_company.com adresindeki tüm kişilere gelen elektronik postalar için “DeleteJunk” cevabı oluşturulur. “DeleteJunk” cevabı ise “MIMESWP.CFG” dosyasında tanımlanmıştır. Buna ek olarak, elektronik postalar içerisinde geçen herhangi bir sözcüğe görede taranabilirler.

```

AUTHFILE.TXT dosyası:

RESPONSE allow
...
RESPONSE DeleteJunk PRIORITY 3

FROM *@*
TO *@* allow
FROM listserver@company.com
TO *@your_company.com DeleteJunk

FINISH

MIMESWP.CFG dosyası:

[Disposal]

DEFAULTDISPOSAL=Clean
DeleteJunk=JustDelete
LoadFailure=FailedLoad

```

Şekil 10.17 Gereksiz elektronik posta (antispam) yapılandırması

- Taklit önleme (antispoofing) yapılandırması: "Mailsweeper" gelen mesajları inceler ve bilinen taklit yöntemlerine göre bir taklit olasılığı belirler. Bu olasılık kullanıcı tarafından tanımlanan olasılık değerini aşmışsa veya eşitse, mesaj taklit edilmiş olarak işaretlenir ve bunu belirten bir mesaj elektronik postaya eklenir. Taklit edilmiş mesajların seçilmesi için yapılması gereken yapılandırmalar Şekil 10.18' de gösterilmektedir.

MIMESWP.CFG dosyası:

```
[Clean]
Edit=AppendIfSpoof
Edit=AppendOutwardDisclaimer
Deliver=

[AppendIfSpoof]
PerformIf=PossibleSpoof==TRUE
AppendToBody=C:\MSWConfig\POSSPOOF.TXT
```

POSSPOOF.TXT dosyası:

Bu mesajın başlığındaki bilgiler mesajın taklit edildiğini ve doğrulanması gerektiğini önermektedir.

SMTP.CFG dosyası:

```
[SMTP]
ContainerClass=Container
...
SpoofThreshold=10
```

Şekil 10.18 Taklit önleme (antispoofing) yapılandırması

- Eklentilerin (attachments) engellenmesi: "Mailsweeper" eklenti içeren elektronik postaları sezecek ve engelleyecek şekilde yapılandırılabilir. Bu özellik, "VALIDATE.CFG" dosyasında, "[Validation]" kısmındaki, "DetectAttachments = VALATTR" satırının önündeki, yorum işareti (;) kaldırılarak sağlanır.
- Elektronik posta mesajı boyut sınırlaması: Mesaj boyutu "VALIDATE.CFG" dosyasında, "[Validation]" kısmındaki, "DetectSize = VALATTR" satırı girilerek sağlanır. Mesaj boyutu sınırı ise, "[DetectSize]" bölümüne, "HaveSize=MessageSize>1048576" satırı eklenerek 1 MB olarak belirlenir.
- Virüs tarama yapılandırması: "VALEXE" doğrulayıcısı sayesinde, Mailsweeper üçüncü parti yazılımlar ile ilişkiye geçerek, virüs tarama işlevlerini bu yazılımlara gerçekleştirir. Bu işlem için gerekli yapılandırma Şekil 10.19' da gösterilmektedir. Şekilden de görüldüğü üzere virüs tarama

yazılımı olarak hızlı güncelleme çıkarması, geniş virüs tabanına sahip olması ve virüs sezmedeki başarısı nedeniyle "McAfee Netshield" seçilmiştir.

```
VALIDATE.CFG dosyası:  
  
[Validation.CFG]  
  
McAfee32=VALEXE  
  
[McAfee32]  
PerformIf=ContainerClass==Executable  
PerformIf=ContainerClass==Document  
PerformIf=ContainerClass==Text  
PerformIf=ContainerClass==Binary  
ExeName=C:\NETSHIELDNT\SCAN32.EXE  
CmdLine=%s /ALL /UINONE /CONTINUE /NOMEM /NOBOOT  
/LOGSUMMARY /LOG %s  
FilePos=0  
LogPos=1  
0=SUCCESS  
1=SCANFAILED  
2=VIRUSPRESENT
```

Şekil 10.19 Virüs tarama yazılımı tanıtma

10.6.5 SSL 128 bit sertifika kurulumu

Sertifika isteğinin üretilmesi

1. Anahtar yöneticisi (key manager) ekranında, WWW ikonu üzerinde sağ tuşa basarak yeni anahtar oluştur (create new key) seçeneği seçilir.
2. Daha sonraki ekranda üretilcek anahtarın boyutu seçilir; 128 bitlik SSL için 1024 bit anahtar boyu seçilmelidir.
3. Bir sonraki ekranda bilinen isim (common name) girilmelidir. Bu isim SSL sertifikası alınacak sunucuyu internet' te tekil olarak tanımlayacak bir isim olmalıdır. Örneğin internet bankacılığı yapılacak bir site için, "internetbank.testbank.com.tr" gibi.
4. Ülke, eyalet, adres ve temas bilgileri gibi bilgiler girilerek sertifika isteği üretimi tamamlanır.
5. Bu sertika isteği ile sertifika makamından sertifika isteğinde bulunulur.

Sertifikanın kurulması

1. Almış olduğunuz sunucu sertifikası metin dosyası olarak saklanır.
2. Daha sonra "SGCinst.exe" programı aracı kök sertifika makamını (intermediate root CA) kurmak için çalıştırılır (sgcinst cert.txt mycert.txt).

3. Daha sonra bu dosyayı IIS 4.0 anahtar yöneticisi (key manager) programından kurulur.
4. Açılan sunucu bağlama (server binding) ekranından, eğer aynı makine üzerinde başka güvenli sunucu yoksa "Any unassigned" seçeneği seçilir. Başka güvenli sunucularında olması durumunda, sertifikayı bir IP numarasına bağlamak gereklidir.



11 SONUÇ

Teknolojide büyük gelişmeler sonrası, ağır sanayi hamlesinin yapılmasından sonraki devrim, insanlığın bilgi çağına geçişidir. Bilgi ve bilginin güncelliği insan hayatındaki en önemli öge durumuna gelmiştir.

Önceki zamanlarda, dünyanın farklı yerlerinde yaşamakta olan insanlar birbirleri ile bilgi iletişimini haberci, posta güvercini, daha sonraki çağlarda, telgraf, mektup ve kargo hizmetleri ile sağlamaktaydılar. Fakat tüm bu sistemlerde bilginin bir kişiden diğerine erişimi gözardı edilemeyecek bir zaman almaktaydı.

Telefon hatlarının icadı iletişim alanında yepyeni bir devrimin işaretçisiydi. Telefon anında iletişimin en ilkel şeklidir. Bilgisayarların birbirine telefon hatları üzerinden bağlanması, dünyanın iki farklı ucundaki bilgisayarların birbirleriyle ses, görüntü ve dosya iletimleri gerçekleştirmeleri olanağını doğurdu. Tüm bu süreçleri bir standarda oturtacak TCP/IP protokolünün icadı ile bugün internet olarak adlandırdığımız dev ağ oluştu. Firmalar tüm iş süreçlerini, önceleri sadece akademik ve eğlence amaçlı olarak kullanılan bu yeni teknolojiye uyarladılar.

Teknoloji iyiye kullanıldığı zaman insanların yararınadır gerçeğini, hiçbir zaman unutmamak gerekir. İnternet üzerinden birbirleriyle iletişim içindeki bilgisayarlar arasında veriler, çıplak olarak hiçbir korumaya tabi tutulmadan aktığı için, trafiği kesen kötü niyetli kişilerce ele geçirilmesi işten bile değildi. Ayrıca TCP/IP protokolünün tasarım yönünden güvenlik zayıflığı tehlikeyi kat kat artırmaktaydı. Kısacası yeni gelişen teknoloji bilginin çalınması ve kişilerin, kurumların aleyhine kullanılması tehlikelerini de beraberinde getirmişti.

Zamanın kişiler, kurumlar ve hükümetlerce en değerli öge haline geldiği bu çağda (bilgi çağı) internet' ten vazgeçmek doğru bir davranış olmayacaktı. O zaman yapılması gereken internet üzerinde bilginin güvenliğini sağlayacak kavramları, yöntemleri ve teknolojileri geliştirmektir. İşte bu çalışmada bu güvenlik teknolojileri ve kavramları araştırılarak uygulanabilir bir güvenlik çözümü sunulmuştur. Bölüm 10' da bu çözüm ayrıntılı olarak anlatılmıştır. Burada da kısaca değerlendirmeleri yapılacaktır.

Bu çözümde iki katmanlı bir yapı kullanılmıştır. İki katmanlı yapının tek katmanlı yapıya karşı faydası, katmanlardan birinin çökmesi durumunda, ikinci katmanın

sistem savunmasına devam etmesidir. Meydan savaşlarında savaşa katılan orduların, önde süvariler, arkada okçular, onların arkasında da yayan askerler olarak kümelenmesi çok katmanlı yapı için iyi bir örnektir. Buradaki her katmanın farklı yeteneklere sahip ürünlerce korunması, bir katmanın çökmesine neden olan zayıflığı diğer katmanında içermesi olasılığını azaltmaktır.

Sunulan güvenlik çözümünde durumsal inceleme yeteneklerine sahip "Firewall-1" ürünü ile kurumun internet ile olan ilk temas noktası korunmaktadır. Durumsal inceleme teknolojisi diğer paket süzgeçleme yöntemlerine göre daha akıllı bir süzgeçleme yöntemidir. Çalışma mekanizmasında her bir bağlantı için karar çizelgeleri tutması ve bağlantının akibetine bu durum çizelgelerine göre karar vermesi ürün başarımını artırmaktadır.

Firewall' ı aşarak sistem üzerinde tehlike yaratabilecek eylemleri algılamak ve engellemek için saldırı sezme sistemleri kullanılmıştır. Temelde konak temelli ve ağ temelli olarak iki farklı saldırı sezme sistemi vardır (bkz. Bölüm 7). Bu iki farklı saldırı sezme sistemlerinin birbirlerine çeşitli yönlerden üstünlükleri vardır. Meydana gelen bir eylemin sezileceği yerin olayın gerçekleştiği yer olduğu gerçeğinden yola çıkılırsa konak temelli saldırı sezme sistemleri, konak temelli saldırı sezme sistemlerinin sadece üzerine kurulu olduğu makine üzerinde meydana gelen olayları sezdiği, ağda hareket eden diğer ağ trafiği ile ilgilenmediği gerçeği gözönüne alınırsa, ağ temelli saldırı sezme sistemleri kullanılmalıdır. Doğal olarak, her iki saldırı sezme yöntemini faydalı özelliklerini içeren saldırı sezme sistemi oluşturuldu.

İnternet üzerinden akan elektronik posta ve web trafiğinin virüs, vbscript ve java applet gibi zararlı kod parçalarına karşı korunmasına sağlamak üzere içerik tarama yöntemleri çözümün içine dahil edilmiştir.

Sistem üzerinde hareketsel işlemlerin yapıldığı web sunucularının yüksek şifreleme teknolojileri ile korunması gerekli görüldü. 128 bit sunucu SSL sertifikası kullanımı ile sistem güvenlik altına alınmıştır.

Burada sunulan güvenlik çözümü, maliyet, ölçeklenebilirlik, gizlilik, güvenilirlik, hazır bulunabilirlik gibi ölçütlerce uygulanabilir bir çözümdür. Güvenlik çözümlerinde unutulmaması gereken ana gerçek, 10 liralık bir veriyi korumak için 20 lira harcanılmamasıdır.

Zamanın çok önemli bir konuma geldiği günümüzde, firmalar üretimini aksatmamak için belli seviyelerde hammadde stoku tutmaktadırlar. Artık dünyadaki birçok firma anında (just-in-time) stok yöntemi kullanarak, ürünü stokta tutmak yerine ihtiyaç duyduklarında sipariş vermektedirler. Bu sistemin otomatik olarak çalışması için

retici firma ile tedariki firma arasında internet zerinden gerekleen iletiimin, sanal zel aĖlar (virtual private network) kullanımı ile korunması gereklidir. İleriki bir alıma olarak, burada sunulan gvenlik zmn sanal zel aĖlara cevap verecek ekilde yapılandırılabilir.

Elektronik ticaretin hızla gelitiĖi gnmzde, firmalar arasındaki tedarik zincirinde kullanıcı kimlik doĖrulamada XML sayısal imzaları kullanılmaya balanmışır. Tm bu tedarik zincirinde mteriyi tekil olarak tanımlayacak ve sistem genelinde tek baĖlantıyı saĖlayacak XML sayısal imza yapısı oluturmak ve gvenlik zmnn bu yapıya destek verecek ekilde gelitirmek mmkn olabilir.



KAYNAKLAR

- [1] **Cooper N., Feinman, T., Goldman, D., and Wong R., 1996.** Security Basics, PricewaterhouseCoopers LLP Resource Protection Services.
- [2] **Köse, S., 2000.** Nedir Bu Güvenlik Seviyeleri?, <http://www.guvenlikhaber.com/makaleler.htm>.
- [3] **Çağıltay, K., 1994.** Internet nedir?, ODTÜ Bilgi İşlem Daire Başkanlığı, Ankara, Türkiye.
- [4] **Microsoft Education and Certification, 1997.** Internetworking with TCP/IP in Microsoft Windows NT 4.0, Microsoft Corporation United States of America.
- [5] **Leblebici, B. ve Karaahmetoğlu, O., 1996.** Internet Teknolojilerinin Araştırılması ve Denenmesi, *Diploma Projesi*, Yıldız Teknik Üniversitesi, İstanbul, Türkiye.
- [6] **Cyber Warriors, 2000.** A Brief History of Hacking, <http://www.accessorl.net/~cyberwar/hackhist.html>.
- [7] **Cyber Warriors, 1996.** Hackers, <http://www.accessorl.net/~cyberwar/hackers.html>.
- [8] **Cyber Warriors, 1996.** Code Hacks, <http://www.accessorl.net/~cyberwar/codehacks.html>.
- [9] **Köse, S., 2001.** Tüm Zamanların En İyi Hacking Olayları, <http://www.guvenlikhaber.com/yazilar.htm>.
- [10] **Ford, M., Lew, H.K., Spanier, S. and Stevenson T., 1999.** Security Technologies, in *Internetworking Technology Overview*, pp 47.1-47.12, Cisco Systems, http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm.
- [11] **Bellovin S.M., 1989.** Security Problems in the TCP/IP Protocol Suite, *Computer Communication Review*, **19**, 32-48.
- [12] **Perkins, C. and Strebe, M., 1999.** TCP/IP from a Security Viewpoint, Firewalls, in *Firewalls 24seven*, pp 97-125, Sybex, Inc.
- [13] **Kurtz, G., McClure, S. and Scambray, J., 1999.** Hacking Exposed, Osborne/McGraw-Hill, Berkeley, California, USA.
- [14] **Netscape Communication Corporation, 1998.** Introduction to Public-Key Cryptography, *Security Documentation*, <http://developer.netscape.com/docs/manuals/security/pkin/index.htm>.

- [15] **Menezes, A., Van Oorschot, P., Vanstone, S.,** 1996. Handbook of Applied Cryptography, CRC Press, New York.
- [16] **Tanenbaum, A.S.,** 1996. Application Layer, in *Computer Networks*, pp 577-621, Prentice-Hall, Inc.
- [17] **BİLTEN ve İGEME,** 1999. Türkiye İçin Elektronik Ticarete Geçiş Durum Değerlendirmesi ve Pilot Uygulama Projesi, *E- Ticaret : Dünyada ve Türkiye'de Durum Değerlendirilmesi*, ODTÜ Kültür ve Kongre Merkezi, Ankara, Türkiye, 14 Haziran.
- [18] **Hall, E.,** 1996. Internet Firewall Essentials, *Network Design Manual* <http://www.networkcomputing.com/netdesign/wall1.html>.
- [19] **Veit, T.,** 1998. Internet Security Concepts, Diploma Projects, Hochschule für Technik, Wirtschaft und Kultur Leipzig, Leipzig, Germany.
- [20] **Clyde, R.A. and Williams, D.,** 1998. Enterprise-wide Intrusion Detection, AXENT Technologies, Inc.
- [21] **Allen, J., Ford, G., Konda, S., Kossakowski, K.P. and Simmel, D.,** 1999. Securing Network Servers, Carnegie Mellon Software Engineering Institute, Pittsburgh, USA.
- [22] **Allen, J. and Kossakowski, K.P.,** 1999. Securing Public Web Servers, Carnegie Mellon Software Engineering Institute, Pittsburgh, USA.
- [23] **Allen, J., Fithen, W. and Stoner, E.,** 1999. Deploying Firewalls, Carnegie Mellon Software Engineering Institute, Pittsburgh, USA.
- [24] **Alberts C., Allen, J., Cohen, C., Ford G., Fraser B., Hayes, E., Kochmar, J., Konda, S., Kossakowski, K.P. and Wilson, W.,** 1999. Responing to Intrusions, Carnegie Mellon Software Engineering Institute, Pittsburgh, USA.
- [25] **Ankan, S., Aslan N., Atalay, M., Eriş, İ., İnce, M., Pakbeşe, O. ve Özaygen, M.,** 1998. Elektronik Ticaret Koordinasyon Kurulu *Hukuk Çalışma Grubu Raporu*, Elektronik Ticaret Koordinasyon Kurulu Çalışmaları, Ankara, Türkiye.
- [26] **Akünel, T., Bayraktar, K., Beler, Ö., Güran, S., Kendigelen, A., Sözer, B. ve Yurtcan, E.,** 2000. İnternet ve Hukuk, *İnternet Haftası*, Lütfi Kırdar Spor ve Sergi Sarayı, İstanbul, Türkiye, 12-19 Nisan.
- [27] **Null, C.,** 1998. Firewall Product Comparisions, *InternetWeek*, 15, 71-95.

- [28] **Broderick, J.**, 1998. Network intrusion detection solutions, *Infoworld*, 20, 65-79.
- [29] **NIST**, 2001. Internet Security Policy: A Technical Guide, <http://csrc.nist.gov/isptg/html/ISPTG-Contents.html>.
- [30] **Suton, S.**, 1999. Windows NT Security Guidelines: Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments, *NSA Research*, Trusted System Services, USA.
- [31] **Espinola, M.**, 1998. The hardening of Microsoft Windows NT 4.0, *Santeria Systems Report*, Salem NH.
- [32] **Microsoft Corporation**, 1998. Why Windows NT Server Platform Is the Strategic Choice Over UNIX, *Windows NT Whitepaper*, <http://www.microsoft.com/NTServer/nts/techdetails/overview/WpGlobal.asp>.
- [33] **Microsoft Corporation**, 1998. Meeting Enterprise Security Needs: Microsoft Windows NT and UNIX, *Windows NT Whitepaper*, <http://www.microsoft.com/NTServer/nts/techdetails/overview/WpGlobal.asp>.
- [34] **Fieldman, J.**, 1999. Securing/Configuring Windows NT Server, *Checkpoint Howto Documents*, USA.
- [35] **Checkpoint Courseware**, 1998. CCSA Student User Guide Firewall-1 Version 4.0 Revision A, Checkpoint Software Technology Ltd., USA.
- [36] **Checkpoint Courseware**, 1999. Advanced Firewall-1 Student User Guide Management (CCSE) Version 4.0 Revision B, Checkpoint Software Technology Ltd., USA.
- [37] **Checkpoint Techwriters**, 2000. CheckpointVPN-1/Firewall-1 Administration Guide, Checkpoint Software Technology Ltd., USA.
- [38] **Technical Incursion Countermeasures**, 1999. The Firewall Hardening Guide, <http://www.ticm.com>.
- [39] **De Vries, S. and Sokol, M.**, 1998. Secure Intrusion Detection Deployment using an Isolated Segment and Secure DMZ, ISS RealSecure Technical Center: Tech Notes, http://www.iss.net/customer_care/resource_center/realsecure_tech_center/technotes/index.php.
- [40] **Internet Security Systems**, 1998. Windows NT 4.0 Security Configuration: Locking Down a Windows NT Host for Intrusion Detection, *ISS Whitepaper*, http://www.iss.net/customer_care/resource_center/how_to_guide/.

- [41] **Internet Security Systems**, 2001. RealSecure Frequently Asked Questions, *ISS Faqs*, http://www.iss.net/customer_care/resource_center/faq/.
- [42] **Internet Security Systems**, 2000. RealSecure Getting Started Guide, *ISS Online Documentation*, http://www.iss.net/customer_care/resource_center/online_doc/.
- [43] **Internet Security Systems**, 2000. RealSecure Network Sensor 5.0 Performance Testing and Configuration White Paper, *RealSecure Network Performance Testing*,



ÖZGEÇMİŞ

Osman KARAAHMETOĞLU, 1974 yılında Trabzon' da doğdu. Lise ve ortaokulu İstanbul' da okudu. 1991 yılında Yıldız Teknik Üniversitesi Bilgisayar Bilimleri ve Mühendisliği Bölümü' ne girmeye hak kazandı. 1996 yılında mezun oldu. 1996 yılında İstanbul Teknik Üniversitesi Kontrol ve Bilgisayar Mühendisliği Bölümü' nde yüksek lisansa başladı. 1999 yılında Yeditepe Üniversitesi İşletme Bölümü' nde yüksek lisansa başladı. Bir yıl süresince MDA A.Ş.' de sistem analisti ve programcı olarak çalıştı. Üç yılı aşkın süredir Esbank Bilgi Teknolojileri Merkezi' nde internet teknolojileri ve web uygulama geliştiriciliği konusunda çalışmaktadır. İyi derecede ingilizce bilmektedir.

