İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

GÜVENLİK VE İNTERNET ERİŞİM POLİTİKALARI OLUŞTURULMASI: İSTANBUL ÜNİVERSİTESİ'NDE UYGULAMA SÜRECİ

Hakan AYSAL
Enformatik Bölümü

Danışman
Yard.Doç.Dr. Zerrin AYVAZ REİS

Ocak, 2007

İSTANBUL

İSTANBUL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

GÜVENLİK VE İNTERNET ERİŞİM POLİTİKALARI OLUŞTURULMASI: İSTANBUL ÜNİVERSİTESİ'NDE UYGULAMA SÜRECİ

Hakan AYSAL
Enformatik Bölümü

Danışman
Yard.Doç.Dr. Zerrin AYVAZ REİS

Ocak, 2007

İSTANBUL

Bu çalışma 14/02/2007 tarihinde aşağıdaki jüri tarafından Enformatik Anabilim Dalı Enformatik programında Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Jürisi

Yrd.Doç.Dr. Zerrin A. REİS (Danışman)
İstanbul Üniversitesi
Enformatik Bölümü

Doç.Dr. Sevinç GÜLSEÇEN
İstanbul Üniversitesi
Enformatik Bölümü

Doç.Dr. Hülya ÇALIŞKAN
İstanbul Üniversitesi
Enformatik Bölümü

Doç.Dr. Mehpare TIMOR
İstanbul Üniversitesi
İşletme Fakültesi

Yrd.Doç.Dr. Zuhal TANRIKULU
Boğaziçi Üniversitesi
Yönetim Bilişim Sistemleri Bölümü

ÖNSÖZ

Yüksek lisans öğrenimim sırasında ve tez çalışmalarım boyunca gösterdiği her türlü destek ve yardımdan dolayı çok değerli hocam Yard.Doç.Dr. Zerrin AYVAZ REİS'e en içten dileklerimle teşekkür ederim.

Bu çalışma boyunca desteğini ve fedakarlığını esirgemeyen kızım ve eşime, ayrıca teşekkürü borç bilirim.

Ocak, 2007 **Hakan AYSAL**

İÇİNDEKİLER

İÇİNDEKİLER

ŞEKİL LİSTESİ

TABLO LİSTESİ

ÖZET

GÜVENLİK VE İNTERNET ERİŞİM POLİTİKALARI OLUŞTURULMASI: İSTANBUL ÜNİVERSİTESİ'NDE UYGULAMA SÜRECİ

Bu çalışma, güvenlik ve internet erişim politikaları oluşturma sürecini, İstanbul Üniversitesi örneğini kendisine temel alarak, uluslararası standartlar ve konunun önde gelen hem yerli hem yabancı üniversitelerinin bu yönde geliştirmiş oldukları projeler ve tecrübeleri referans alınarak tanımlamayı hedef almıştır.

Bu hedef doğrultusunda hazırlanmış olan çalışma, üç ana bölümde incelenebilir. Birinci bölümde, çalışma sahası olması nedeniyle kurumsal altyapı tüm teknik yönleriyle ele alınmıştır. Kurumsal ölçekte en uygun altyapı örneğini teşkil eden üniversitelerin, kullandığı teknolojiler, ağ ve ağ bileşenleri kısaca incelenmiş, İstanbul Üniversitesi örnekleriyle konuyu tamamlar hale getirilmiştir.

İkinci bölümde, güvenlik kavramı tüm bileşenleriyle ele alınmış ve politikalar ile ilişkisi daha belirgin hale getirilmeye çalışılmıştır. Güvenliğin bileşenlerini ortaya koyma açısından, tehditler ve bunlara karşı alınabilecek tedbirler üzerinde durulmuştur. Kurumsal güvenliğin sağlanması hususunda bilgi teknolojileri sektörünün ortaya koymuş oldukları çalışmalar, getirmiş oldukları çözümler ve bu yönde geleceğe dönük eğilimler irdelenmiştir.

Çalışmanın üçüncü bölümünde, üniversitelerde kurumsal ölçekte bir güvenlik anlayışının tam olarak oturtulabilmesi ve istikrarlı bir şekilde sürekliliğini koruyabilmesi için en önemli unsurun, yönetimin de tam desteğini almış bir kurumsal güvenlik politikası oluşturulması gereği anlatılmıştır. Daha sonra bu alanda köklü ve kapsamlı projeler geliştirmiş olan üniversitelerin çalışmaları ve bu yönde hazırlanmış olan uluslararası standartlar esas alınarak, bir süreç ortaya konulmaya çalışılmıştır. Ortaya konulan süreç doğrultusunda İstanbul Üniversitesi'nde uygulanacak politika hazırlama çalışmalarına başlanmıştır. Çalışmanın en son bölümünde İstanbul Üniversitesi güvenlik politikası şablonu ve örnek güvenlik politikaları hazırlanmıştır.

SUMMARY

IMPLEMENTATION OF SECURITY AND INTERNET ACCESS POLICY: APPLICATION PROCESS IN ISTANBUL UNIVERSITY

This dissertation has aimed to describe the process of security and implementation of internet access policies concerning the example of Istanbul University and the projects that have been developed by the national and international leading universities of this field.

This study has three chapters. In the first chapter the institutional infrastructure has been examined with the all technical aspects since it is the main technical background. The technologies, network and network components used by the universities which constitute the most appropriate example of infrastructure at the enterprise grade briefly examined. Istanbul University example has been given to complete the subject.

In the second chapter, the concepts of security with all dimensions and the relation to the security policies have been clearly treated. In order to put forward the components of the security, the threats and the measures that can be taken against the threats have been emphasized. The works which are given by the information technology sector in order to acquire the institutional security and the suggested solutions and the future aims have been discussed.

In the third chapter, we have come to the conclusion that in order to establish a well security approach in the universities at the institutional scale and maintain the consistence of it, it is needed an institutional policy which is fully supported by the administration. After that the remarkable and extensive projects that are prepared by some universities have been examined concerning the international standards on this area to determine the process of it. In the direction of this process, which have been put forward, the policy preparations have been started at the Istanbul University. At the final section of the dissertation, an example of a security policy template of Istanbul University and the sample security policy has been prepared.

1. GİRİŞ

Kurumlarda bilgi ağı ve akışı, insan hayatı gibidir. Bu akışı sağlayan donanım, yazılım ve kullanıcılar gibi unsurların birleşiminden bir toplum ortaya çıkar. İnsanlık, hayatını düzenleyen ve hayatın kalitesini yükseltmeyi hedefleyen yazılı yasa ve kurallar oluşturduğu gibi yazılı olmayan kurallara da sahiptir. Üniversite toplumunun da sağlıklı, kaliteli ve kesintisiz bir erişime sahip olabilmesi, bilgi akışını sağlayan unsurlar arasındaki ilişkilerin düzenli ve kaliteli olabilmesi için yazılı kuralların ortaya konulması gerekmektedir.

Hem kurumlar hem de kullanıcılar bakımından uzmanlaşmanın günden güne artması, bilgiyi de özel ve değerli hale getirmektedir. Bu değer nedeniyle de bilgi teknolojilerine önemli yatırımlar yapılmaktadır. Ancak, söz konusu teknolojilerin, güvenilirliklerini yitirmeden yararlı olmayı sürdürmesi, yeni yatırımlardan çok, kullanıcı bilgisi ve kullanım disiplinine bağlıdır. Herhangi bir güvenlik sorunu nedeniyle, kurumun kullanıcılar karşısında güven kaybına uğramaması, kurum için değerli bilgileri kaybetmemesi, kurumun bu yönde imajını koruyabilmesi ve geleceğe güvenle hazırlanabilmesi için bilgi güvenliği altyapı ve politikalarını bugünden oluşturmak gerekmektedir.

Üniversite gibi açık bir ortamda kurallar yada politikaların sınırlarının ve kapsamının belirlenebilmesi ve kabul görmesi için de teknik, idari ve hukuki kıstasların herkesin anlayabileceği şekilde ortaya konulması gerekir. Burada dikkat edilecek husus konulan kuralların, ağın kuruluş amacı olan akademik çalışmaları sekteye uğratmadan düzenlemeler getirmesidir.

Çalışmanın içeriği oluşturulurken, dünyada ve Türkiye'deki üniversitelerde bu yönde yapılmış çalışmalar ile bu konuda özel sektörün ve çeşitli standart organizasyonlarının ortaya koymuş oldukları projeler referans teşkil etmiştir.

Öncelikle Üniversitelerde internet altyapıları konusunda giriş yapmak amacıyla, bilgisayar ağları ve ağ teknolojileri başlıkları teknik olarak incelenip, Türkiye'deki diğer üniversitelerin hemen hemen benzer ağ yapısına sahip olması sebebiyle İstanbul Üniversitesi Yerel Ağı örnek olarak gösterilmiştir. Daha sonra güvenlik kavramının ağ bağlantılarındaki yeri konusu ve politikalar ile ilişkisi irdelenip, güvenliğin sağlanabilmesi resminin yönetim ve kullanıcı tarafından görünen kısımları ayrı ayrı ele alınmıştır.

Güvenlik bileşenleri ortaya konulduktan sonra bunların yazılı kurallar ile bir çerçeveye oturtulmasının gerekliliği, amacı, planlanması, oluşturulması ve uygulanabilmesinin önemi ve bunun için de gereken kıstasların neler olduğu vurgulanmıştır.

Güvenlik politikaları; her kurum için olduğu gibi üniversiteler için de büyük öneme sahip kurallar dizisidir. Güvenlik politikası oluşturulması hususunda bütün üniversiteler farklı düzeylerde çalışmalar yapmıştır ancak bu çalışmalar tüm üniversitelerin uygulayabileceği ortak bir standarda oturtulamamıştır. Bu çalışmada hedef, güvenlik politikası oluşturulması hususunda temel alınacak bir süreç ortaya koymaktır. Umarım bu çalışma, bu konudaki önemli bir eksikliği gidermede, biz Bilgi Teknolojileri yöneticilerine yardımcı olacaktır.

2. BİLGİSAYAR AĞLARI

Bilgisayar ve iletişim teknolojilerinde yaşanan hızlı gelişmeler sonucu bu alanlar birbirlerine gittikçe yakınlaşmaya başlamış ve bilginin toplanması, iletimi, saklanması ve işlenmesi arasındaki farklar hızla yok olmaya başlamıştır. Bu değişen ve gelişen uygulamalar, bilginin çok daha kapsamlı ve hızlı işlenmesi ihtiyacını doğurmuştur.

Bütün kurumun bilgi işleminin tek bir merkezi ana bilgisayardan yürütülmesi kavramının modası geçmiş, yerine çok sayıda ve dağınık fakat birbirine bağlı bilgisayarlar kullanılmaya başlanmıştır. Bu, birbirinden bağımsız bilgisayarların toplanarak bir teknoloji vasıtasıyla bilgi alış verişi yapabildiği sistemlere, bilgisayar ağları denilmektedir. [Tanenbaum Andrew S., 1]

Ağları yayıldıkları coğrafi alan açısından yerel alan (Local Area Network: LAN) ve geniş alan (Wide Area Network: WAN) ağları olarak ikiye ayırabiliriz:

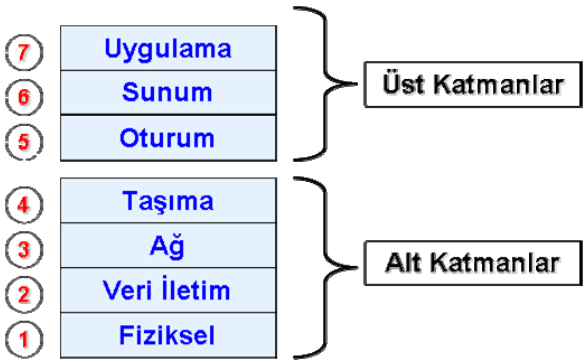
2.1. Genel Ağ Kavramları

2.1.1. OSI (Open System Interconnect) Referans Modeli

OSI referans modeli, farklı platformlarda çalışan ve farklı üreticilere ait uygulamaların ortak bir alanda çalışabilmelerini sağlamak amacıyla 1984 yılında Uluslararası Standartlar Organizasyonu (ISO) tarafından ISO/IEC 7498-1 numarasıyla geliştirilmiştir. [4] Türk Standartları Enstitüsü tarafından TS ISO/IEC 7498-1 belge numarası ve "Bilgi Teknolojisi-Açık Sistemler Ara Bağlantısı-Temel Referans Model-Bölüm 1:Temel Model" başlığı ile 27.11.2002 tarihinde kabul edilmiştir. [5]

OSI modeli, verilerin bir bilgisayarda bulunan yazılım uygulamasından ağ ortamını kullanarak başka bir bilgisayardaki yazılım uygulamasına nasıl taşındığını tanımlar. OSI modeli, ağ iletişiminin karmaşık yapısını işlevsellik ve verdikleri hizmet açısından yedi ana katmana böler. Her katman yürüttüğü görevler ve hizmetler olarak kendi

sorumluluğuna sahiptir. Böylece bir katmanda yapılan değişiklikler diğer katmanları etkilemez ve problemlerin tespiti ve çözümü kolaylaşır. Şekil 2.1.1.1. de bu katmanlar görülmektedir.



Şekil 2.1.1.1 : OSI referans modeli katmanları

Protokol kavramı: Protokoller, yazılım veya donanımların, verileri bir ağ üzerinde OSI modelinin talimatları doğrultusunda nasıl taşıyacaklarını tanımlarlar. Bir protokol, bir görevi yerine getiren tek bir eleman veya elemanlar kümesi olabilir. Bir protokol kümesi veya protokol takımı, bilgisayarlar arasındaki veri alışverişinde kullanılan birden çok protokolden meydana gelir. Küme içerisindeki bir protokol, ağ arayüz kartının (NIC) nasıl iletişim kurduğunu tanımlarken, bir diğeri bir bilgisayarın bu ağ arayüz kartından bilgileri nasıl okuyacağını tanımlayabilir.

Üst Katmanlar

OSI modeli üst katmanları uygulama konularıyla ilgili olup genellikle yazılımlara uygulanırlar.

- **Uygulama katmanı:** En üst katman olup kullanıcıya en yakın olan olanıdır. Uygulama katmanı bir bilgisayar üzerinde çalışan programlar ve bir ağ üzerindeki diğer hizmetler arasında veri alışverişinden sorumludur. Genel ağ erişimi, akış kontrolü, hata düzeltme ve dosya transfer konularıyla ilgilenir. Uygulama katmanı protokollerine örnek olarak aşağıdakiler verilebilir;
    - **FTP (File Transfer Protocol):** Dosya transfer protokolüdür. Protokolün ayrıntılı açıklaması RFC 959 belgesinde yapılmıştır. [6]
    - **SMTP (Simple Mail Transfer Protocol):** E-posta yollamak için kullanılan protokoldür. Protokolün ayrıntılı açıklaması RFC 2821 belgesinde yapılmıştır. [7]

- **HTTP (Hypertext Transfer Protocol):** Sunucu ve istemcilerin iletişimini sağlayarak kullanıcıların internet üzerinde dolaşabilmesine imkân tanıyan protokoldür. Protokolün ayrıntılı açıklaması RFC 2616 belgesinde yapılmıştır. [8]
- **TELNET (TCP/IP Terminal Emulation Protocol):** Uzak sistemlere bağlanmak ve bu sistemler üzerinde komutlar çalıştırmak için kullanılan protokoldür. Protokolün tanımı RFC 854 belgesinde yapılmıştır. [9]
- **TFTP (Trivial File Transfer Protocol):** Genellikle ağ cihazlarının ana yazılım (firmware), yapılandırma ve güncelleme dosyalarının transferinde kullanılan basit dosya transfer protokolüdür. Protokolün tanımı RFC 1350 belgesinde yapılmıştır. [10]

- **Sunum Katmanı:** Sunum katmanı, programların verileri anlayabilecekleri şekilde biçimlendirir. Bu katmanda şifreleme, sıkıştırma ve tekrar biçimlendirme hizmetleri verilmektedir. Sunum katmanı, gelen tüm paketlere içerisindeki verilerin nasıl kodlanacağını söyleyen bir alan ekler. Eğer bir sıkıştırma işlemi yapıldıysa, ayrıca ne tip bir sıkıştırma yapıldığına dair bir bilgi de eklenir. Böylece alıcı paketi düzgün bir şekilde açabilir. Sunum katmanı protokollerine örnek olarak aşağıdakiler verilebilir;
  - **ASCII (American Standard Code for Information Interchange):** Bilgisayarlar sadece rakamları anlarlar, bu nedenle "a, @ veya ├" gibi karakterlerin sayısal dönüşümü için ASCII kodları kullanılır. Latin alfabesi üzerine kurulu 7 bitlik bir karakter seti olup genellikle bilgisayar, iletişim aygıtları ve benzeri yazı (text) ile ilgili çalışmaları gerçekleştiren aygıtlarda kullanılır. 95 tane yazılır, 33 tane basılmayan olmak üzere toplam 128 adet karakter bulunur. [11]
  - **MPEG (Moving Picture Experts Group):** Film, video ve müzik gibi görsel-işitsel bilgilerin bir sayısal sıkıştırılmış biçim içine kodlanmasında kullanılan bir standartlar ailesi olup MPEG 1-4 e kadar uygulamaları vardır. MPEG, kullandığı çok gelişmiş sıkıştırma teknikleri sayesinde ses ve video uygulamalarını aynı kalitede ve çok küçük hacimlerde kodlayabilmektedir. [12]

- **JPEG (Joint Photographic Experts Group):** Fotoğrafik görüntülerin sıkıştırılmasında kullanılan yaygın bir yöntemdir. Standardın herkesçe bilinen "JPEG" resmi adı ISO/IEC IS 10918-1 belgesiyle yayınlanmıştır. [13]

- **Oturum Katmanı:** Bu katman oturumlar arasındaki bağlantıları destekler ve yönetimsel görevleri ve güvenliği yürütür. [Comer D., 14] Oturum katmanı protokollerine örnek olarak aşağıdakiler verilebilir;
  - **DNS (Domain Name Service):** Bilgisayar isimleri ile IP adresleri arasında çift taraflı çevirim için kullanılır. Protokolün uygulaması ve tanımları RFC 1035 belgesinde açıklanmıştır. [15]
  - **LDAP (Lightweight Directory Access Protocol):** LDAP, X.500 standardı ile tanımlanan dizin erişim protokolünün hafifletilmiş sürümüdür**.** Protokolün tanımı RFC 1777 belgesinde yapılmıştır. [16]
  - **NetBIOS (Network Basic Input/Output System):** NetBIOS, IBM tarafından küçük ağlar için geliştirilmiş olup bir ağdaki farklı bilgisayarlar üzerindeki uygulamaların iletişimini sağlayan protokoldür. Daha sonra Microsoft tarafından NetBEUI (NetBIOS Extended User Interface) olarak geliştirilmiş ve tüm Windows ağlarda kullanılmaya başlamıştır.

Alt katmanlar

OSI modelinin alt katmanları, veri taşıma konuları ile ilgilenirler. Fiziksel katman ve veri iletim katmanı hem yazılım hem de donanımlara uygulanırlar.

- **Taşıma Katmanı:** Taşıma katmanı sıradan bir katman olmayıp tüm protokol düzeninin kalbidir. Bu katman iletim sırasında oluşabilecek hataları tespit eder ve uçtan uca akış kontrolü yaparak verilerin güvenli bir şekilde alıcıya teslimini sağlar. Taşıma katmanı, uygulama mesajlarını *segment* adı verilen küçük paketlere dönüştürür. [Mir Nader F., 17] Gelen paketlerin incelenmesi, tekrar paketlenmesi ve mesajların daha küçük paketlere bölünmesi bu katmanda gerçekleşir. Taşıma katmanı protokollerine örnek olarak aşağıdakiler verilebilir;
  - **TCP (Transmission Control Protocol):** TCP, internet protokolleri arasındaki en önemli protokoldür. Ağ üzerinde bulunan bilgisayarlardaki

uygulamaların birbirleri ile bağlantı kurmalarını sağlar (connection oriented). Ayrıca vericiden alıcıya gönderilen verilerin, güvenilir ve sırasına bağlı kalarak teslimini sağlar. TCP protokolü, aynı sistem üzerinde çalışan eş zamanlı uygulamaların (web ve e-posta sunucu vb.) oluşturduğu çoklu bağlantı verilerini ayırt eder. Bu protokol RFC 793 belgesi tarafından tanımlanmıştır. [18]

- **UDP (User Datagram Protocol):** UDP protokolü verinin yerine ulaşıp ulaşmadığını kontrol etmez, bağlantı kurmayı gerektirmez (connectionless), güvenilir değildir fakat ağ üzerinde az yer kapladığından hızlı iletişim kurulması gereken yerlerde kullanılır. Bu protokol RFC 768 belgesi tarafından tanımlanmıştır. [19]

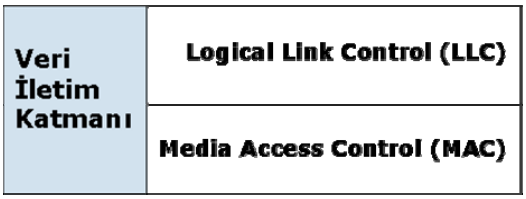
- **Ağ Katmanı:** Ağ katmanının en önemli işlevi, üst katmanlara bilmeleri gereken tüm iletim ve anahtarlama teknolojilerine ait bilgiler konusunda yardımcı olmaktır. [Prasad K.V., 20] Ağ katmanı, veri paketlerinin ağlar arasında, yönlendirme protokollerini kullanarak nasıl yönlendirilmesi gerektiğine karar verir. Bu katmanda kullanılan yönlendirme protokollerinin görevi ise yönlendirilecek paketin hedefe ulaşabilmesi için geçmesi gereken yolun hangisinin en uygun olduğunu belirlemektir. Bu katmanda tanımlanan protokollere örnek olarak X.25, IP (Internet Protocol) ve IPX (Internetwork Packet Exchange) verilebilir.

  - **IP (Internet Protocol):** IP protokolü, paket anahtarlamalı bilgisayar ağlarına bağlı sistemlerde kullanılmak üzere oluşturulmuştur. IP protokolü datagram adı verilen veri bloklarının, sabit uzunlukta adrese sahip kaynak ve hedef sistemler arasında iletimini sağlar. [Naugle M., 21] protokol paketlerin içeriği ile ilgilenmeyip paketlere adresler tanımlayarak hedefe doğru en iyi yönü belirler. Bu protokol çoğu zaman hata kontrolü ve doğrulaması yapmadığı için güvenilmez bir protokol olarak adlandırılır. Bu tip işlemler daha üst katmanlarda (TCP) uygulanmaktadır. Bu protokolün özellikleri RFC 791 belgesinde ayrıntılarıyla açıklanmıştır. [22]
  - **IPX (Internetwork Packet Exchange):** TCP/IP protokolünün her yere yayılmadan önceki dönemde, birçok ağ Novell NetWare sunucuları ile çalışmaktaydı. Her ne kadar NetWare'in son sürümü TCP/IP yi kullansa bile mevcut kurulu ağların NetWare ağlarındaki bilgisayarların paketlerinin

yönlendirilmesi ve adreslerinin kontrolünü Novell'in sahip olduğu IPX protokolü sağlar. [Zacker C., 23]

- **Veri İletim Katmanı:** Veri iletim katmanı, fiziksel katmana aktarılacak verilerin biçiminin ne olması gerektiğini belirler ve adresleme, hata giderimi ve akış kontrolü işlemleriyle beraber fiziksel ortama nasıl erişileceğini belirtir. Bu katmanda verilerin, aynı fiziksel ağ üzerindeki iki cihaz arasında taşınabilmesi için frame adı verilen çerçeveler içerisinde gruplandırılır. Bir frame, başlık ve taşıyıcı başlıklarından oluşur. Bir LAN ortamında kullanılan veri iletim katmanı protokollerine örnek olarak Ethernet, Token Ring ve Fiber Distributed Data Interface (FDDI) gösterilebilir. Ayrıca Geniş Alan Ağları (WAN) ortamlarında kullanılan protokollere örnek olarak Frame Relay, ve Asenkron Transfer Modu (ATM) gösterilebilir.

  Veri iletim katmanı, IEEE (Institute of Electrical and Electronics Engineers) tarafından Media Access Control (MAC) ve Logical Link Control (LLC) olmak üzere iki alt bölüme ayrılır:



Şekil 2.1.1.2 : Veri iletim katmanı

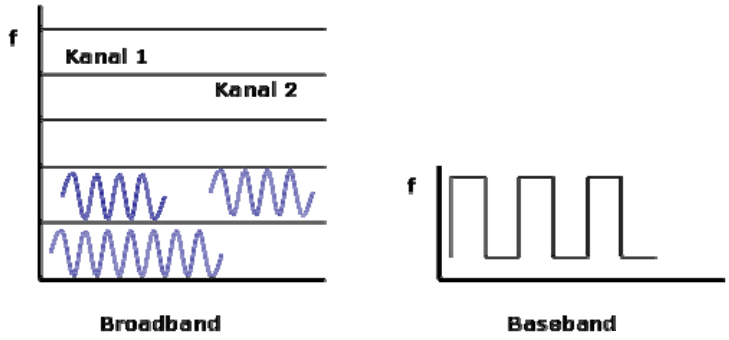
  - MAC alt katmanı, paketlerin ağ ortamı üzerine nasıl yerleştirileceğini tanımlar. Hata belirleme, frame'lerin sırasına göre teslimi ve ilave akış kontrolü bu alt katmanda kullanılır.
  - LLC alt katmanı, ağ katmanı protokollerini tanımlamak ve sonra da bunları kapsüllemekten (encapsulation) sorumludur. Bir LLC başlığı veri iletim katmanına, bir pakete ait ilk frame alındığında ne yapması gerektiğini söyler.

- **Fiziksel Katman:** Bu katmanda tanımlanan standartlar, taşınan verinin içeriğinden daha çok fiziksel ortamda kullanılacak konnektör türü, kablo türü gibi elektriksel, optik ve mekanik özelliklerle ilgilenir. Bütün ağ hizmetleri ve

cihazlarının fiziksel arayüzleri bu katmanda tanımlanır. [Barnes D. ve Sakandar B., 24]

2.1.2. Yerel Ağ İletim Teknikleri ve Standartları

Yerel ağ iletim teknikleri; broadband ve baseband olmak üzere ikiye ayrılır. Broadband, çok kanallı anlamına gelmektedir. Bu nedenle birden çok bağımsız kanal, sahip oldukları arayüzlere bağlı olarak analog veya sayısal bilgileri taşıyabilirler. [Goleniewski L. ve Jarrett Kitty W., 25]



Şekil 2.1.2.1 : Broadband ve baseband karşılaştırması

Baseband tek kanallı bir sayısal sistemi ifade eder. Bu tek kanal, bilgileri kullanılan LAN standardına göre tanımlanan paket veya frame'ler üzerinde taşır. En çok kullanılan LAN standartları, Ethernet, Token Ring ve Fiber Distributed Data Interface (FDDI) dir.

Tablo 2.1.2.1 : LAN Standartları karşılaştırması

Karakteristik	Ethernet	Token Ring	FDDI
Standart	IEEE 802.3	IEEE 802.5	ANSI X3T9.5, IEEE 802.6
Mantıksal topoloji	Bus	Ring	Ring
Fiziksel topoloji	Bus, yıldız	Ring, yıldız	Dual ring, dual bus
Fiziksel ortam	Coax, UTP, STP, fiber	Coax, UTP, STP	Fiber (CDDI)
İletim yöntemi	Baseband	Baseband	Baseband
Bant genişliği	10Mbps, 100Mbps, 1Gbps, 10Gbps	4 Mbps, 16 Mbps, 100 Mbps, 1 Gbps	100Mbps

Ethernet

Yerel ağların büyük çoğunluğu baseband Ethernet ağlarından meydana gelmiştir. IEEE 802.3 çalışma grubu tüm Ethernet standartları ailesini oluşturup tanımlarını belirlemiştir. [26] (Tablo 2.1.2.2)

Tablo 2.1.2.2 : Ethernet standartları

Ethernet Standardı	Tamamlandığı Tarih	Tanım	Fiziksel Ortam	Mesafe	Hız
802.3	1983	10BASE5	Kalın coax kablo	500 m	10 Mbps
802.3a	1985	10BASE2	İnce coax kablo	185 m	10 Mbps
802.3i	1990	10BASE-T	Sarmal çiftli kablo	100 m	10 Mbps
802.3j	1993	10BASE-F	Fiber kablo		10 Mbps
		100BASE-TX	Sarmal çiftli kablo	100 m	100 Mbps
802.3u		100BASE-FX	62.5/125 Multi mod fiber	400 m	100 Mbps
802.3z	1998	1000BASE-X	Fiber kablo		1 Gbps
802.3ab	1999	1000BASE-T	Sarmal çiftli kablo	100 m	1 Gbps
		1000BASE-LX	62.5 mic Multi mod fiber 50 mic Multi mod fiber Single mod fiber	440 m 550 m 3-10 km	1 Gbps
		1000BASE-SX	62.5 mic Multi mod fiber 50 mic Multi mod fiber	275 m 550 m	1 Gbps
802.3ak	2004	10GBASE-CX4	Çift eksenli kablo		10Gbps

İlk nesil Ethernet 1983 yılında IEEE 802.3 standardıyla 10 Mbps hızında kalın koaksiyel kablo üzerinden veri iletimini tanımlamıştır. Daha sonra 1995 yılında 802.3u standardı 100 Mbps veya Fast Ethernet tanımını yapmıştır. Bir sonraki atlama noktası 1998 yılında 802.3z standardıyla 1 Gbps Gigabit Ethernet tanımlanmıştır. En son resmi standart olan 802.3ae, 2003 yılında onaylanmış ve 10 Gbps Ethernet tanımını yapmıştır. 802.3 standartları hala tamamlanmamış olup 100 Gbps Ethernet hızına ulaşma ve bu ucuz ve her yerde bulunabilen teknolojiyi metro ve geniş alan ağlarının hizmetine sunma çalışmaları sürmektedir. [Norris M., 27]

Ethernetin bu kadar yaygın kullanımı ve donanımlarının ucuz maliyetinden dolayı, birçok üretici bugün Ethernet kartlarını direk olarak bilgisayarların anakartları üzerine yerleştirmektedirler. Ethernetin bu kadar hızlı gelişimine rağmen teknolojilerin benzer ve kolay uyum sağlayabilir olması yaygınlığını arttırmıştır.

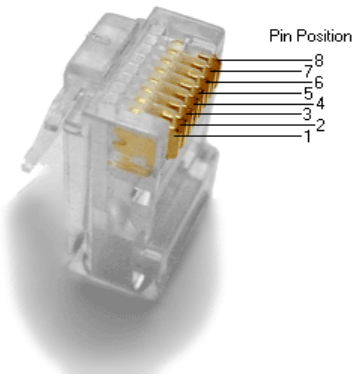
2.1.3. Yerel Ağ İletim Ortamları

Yerel ağlarda en yaygın olarak kullanılan kablo tipleri sarmal çift bakır ve fiber optik kablolardır.

Sarmal çiftli bakır kablolar

IEEE 802.3 çalışma grubu Ethernet teknolojisinin standartlarını değerlendirmek ve yenilerini geliştirmekle sorumludurlar. Fiziksel kablolama ve bağlayıcıların (connector) özelliklerini tanımlamak için Amerikan Milli Standartlar Enstitüsü (ANSI), Mühendislik Endüstrisi Kurumu (EIA) ve Telekomünikasyon Endüstrisi Kurumu (TIA) kurulmuştur. ANSI/TIA/EIA kurumları, sarmal çiftli bakır kabloların özelliklerini, yayınladıkları TIA/EIA-568-B belgesiyle duyurmuşlardır. Bu belgede en bilinen standart, 8 damarlı 100 ohm'luk sarmal çift kablonun renk dizilimine ait olan TIA/EIA-568-B.1-2001 standardıdır. (Tablo 2.1.3.1)

Tablo 2.1.3.1 : T568A ve T568B renk dizilimi

Pin	T568A Çift	T568B Çift	T568A Renk	T568B Renk	RJ-45 Bağlayıcı üzerindeki pinler
1	3	2	yeşil/beyaz	turuncu/beyaz	
2	3	2	yeşil	turuncu	
3	2	3	turuncu/beyaz	yeşil/beyaz	
4	1	1	mavi	mavi	
5	1	1	mavi/beyaz	mavi/beyaz	
6	2	3	turuncu	yeşil	
7	4	4	kahverengi/ beyaz	kahverengi/ beyaz	
8	4	4	kahverengi	kahverengi	

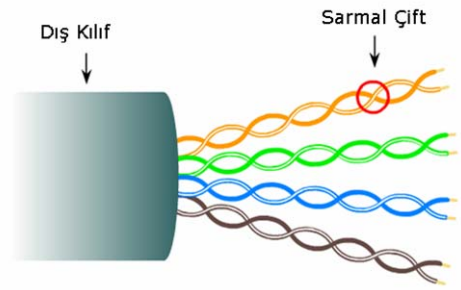
Sarmal çiftli bakır kablolar çeşitli formlarda kullanılmakta olup en yaygınları Category 3, 5, 5E ve 6'dır. Kategoriler kablolamanın radyo frekans gücünün onay belgesini temsil eder.

- Category 3 kablo, 16 MHz frekansa kadar 10 Mbps hızında verileri taşımak için uygundur.

- Category 5 kablo, 100 MHz frekansına kadar 10/100 Mbps hızında verileri taşımak için tasarlanmıştır.
- Category 5E (Enhanced) kablo, adından da anlaşılacağı üzere Cat 5 kablonun geliştirilmiş halidir. Hala 100 MHz ile sınırlı olmasına rağmen 1000BASE-T uygulamalarını destekleyebilmektedir.
- Category 6 kablo, mümkün olan en iyi performansa sahip olup frekans menzili 250 MHz' e kadar artmıştır. Cat 6 kablo daha sıkı standartlara sahiptir.

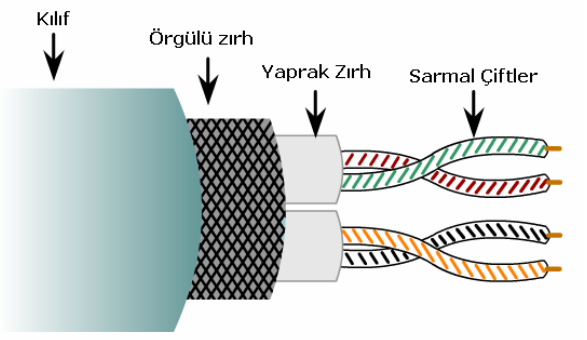
Sarmal çiftli kablolar, zırhlı (Shielded Twisted Pair: STP) ve zırhsız (Unshielded Twisted Pair: UTP) olmak üzere iki çeşittir.

- **Zırhı olmayan sarmal çiftli kablo (UTP):** UTP, hem kendi aralarında hem de dış ortamdan oluşabilecek sinyal bozulmalarını engellemek amacıyla birbirine sarılmış dört çift bakır tel halinde ve en dışta da plastik bir koruma olmak üzere üretilir. UTP kablolar, kolay döşenebilmesi ve maliyetinin düşük olması sebebiyle yerel ağ uygulamalarında en yaygın olarak kullanılan kablo türüdür.



Şekil 2.1.3.1 : UTP kablo yapısı

- **Zırhlı sarmal çiftli kablo (STP):** UTP kablonun manyetik gürültülerden etkilenmemesi amacıyla koaksiyel kablodakine benzer bir dış iletken koruyucu metal tabaka ile kaplanarak üretilmiş olanıdır.



Şekil 2.1.3.2 : STP kablo yapısı

Fiber optik kablo

Fiber optik kablolar, cam lifler üzerinden ışık vasıtasıyla veri iletimine olanak sağlarlar. Kablonun merkezinde nüve (core), etrafında ışığın geri yansımasını sağlayan bir örtü (cladding) ve en dış kısımda da fiziksel şartlardan koruyan bir kaplama bulunur. Bu kaplama kablonun bulunduğu mekân ve dış şartlara göre farklılık gösterir (yeraltı kabloları, deniz aşırı kablolar ve havai kablolar gibi). Şartlar ağırlaştıkça dış yüzeyin de kalınlığı ve kullanılan malzemenin yoğunluğu artmaktadır. Bina içi uygulamalarda kullanılan fiber optik kablolara *indoor* kablo, bina dışı uygulamalarda kullanılan fiber optik kablolara *outdoor* kablo denilmektedir.

Fiber optik kablolar, kaynak olarak elektrik sinyalleri yerine ışık kullandığı için elektriksel gürültülerden etkilenmezler. Bu nedenle veri ve ses iletimi için en ideal kablo türünü oluştururlar. Uygulamada özellikle ağ cihazlarının yüksek hızlarda birbirlerine bağlanmasında, ulaşılması gerekli uzak mesafedeki aktif cihazların mevcut ağa bağlantısında ve yüksek hızlı omurga bağlantılarının oluşturulmasında fiber optik kablolar kullanılmaktadır. Tablo 2.1.3.2.1. de fiber optik kabloların güçlü ve zayıf yönleri kısaca yer almıştır.

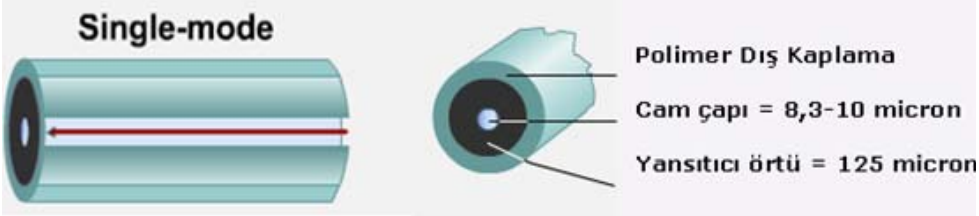
Tablo 2.1.3.2 : Fiber optik kablo güçlü ve zayıf yönleri

Avantajları	**Dezavantajları**
Yüksek hızlı veri iletimine sahiptir.	Yüksek kurulum maliyeti gerektirir.
Esnek trafik taşıma kapasitesine sahiptir.	Özel test cihazları gerektirir.
Elektromanyetik gürültülerden etkilenmez.	Fiziksel hasarların tespiti zordur.
Güvenli iletim olanaklarına sahiptir.	Doğa şartlarının oluşturabileceği zararlara açıktır.

Çok modlu (Multi-mode) ve tek modlu (single-mode) olmak üzere iki sınıf fiber optik kablo mevcuttur.

- **Single-mode fiber:** Single-mode fiber kablolar, lazer ışık darbelerini uzun mesafeler boyunca kırılmadan tek bir yol üzerinde sabit olarak taşıyarak, yüksek kapasitelerde veri iletimine olanak sağlarlar. Fiber ölçüsü nüve ve örtü çapı şeklinde ifade edilir. Örneğin 9/125 mikron ölçüsüne sahip fiberin nüve çapı 9 mikron, örtü çapı 125 mikrondur. Üniversite kampüslerinin en yakın Telekom

santraline ve uzun mesafe gerektiren kampüs içi yerel ağ omurga bağlantılarında single-mod fiber optik kablo kullanılır.

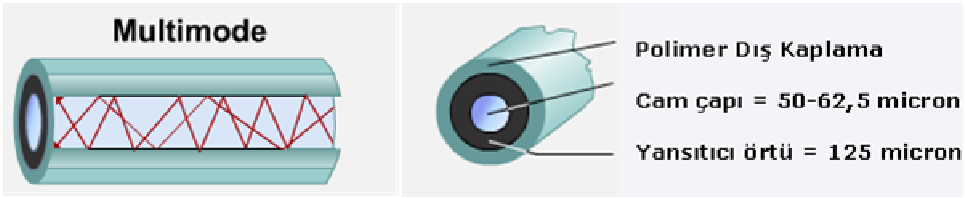


Şekil 2.1.3.3 : Single-mode fiber yapısı ve iletim şekli

Single-mode fiberin dezavantajı; nüve çapının çok küçük olması sebebiyle ışık yoğunluğu yüksek ve pahalı olan lazer ışık kaynağı kullanma zorunluluğu ve ek yapılabilmesi için çok daha hassas bağlantı elemanları gerektirmesidir.

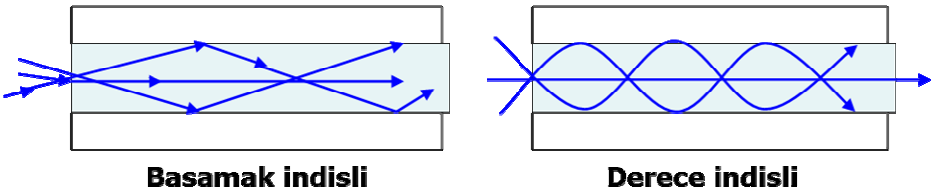
Single-mode fiber optik kablolar, Gigabit Ethernet için IEEE802.3z, 1000BASE-SX (kısa dalga boyu Gigabit Ethernet) 1000BASE-LX (Uzun Dalga Boyu Gigabit Ethernet, 5 km. ye kadar menzile sahiptir) ve IEEE802.3ae, 10GBASE-SR/SW, 10GBASE-LX4 (10 Gigabit Ethernet) protokollerini de içeren mevcut tüm yerel ağ uygulamalarını desteklemektedir.

- **Multi-mode fiber:** Bu kablo tipi Şekil 2.1.3.4. den de görüleceği üzere tek bir ışık kaynağını düz bir doğrultuda iletmeyip, farklı dalga boylarında birden fazla ışık kaynağını yansıtarak veri iletimi sağlar. Işık kaynağı olarak LED (Light Emitting Diot) kullanır.



Şekil 2.1.3.4 : Multi-mode fiber yapısı ve iletim şekli

Multi-mode fiber yansıtma şekline göre *basamak indisli* (step-index) ve *derece indisli* (graded-index) olmak üzere ikiye ayrılır. (Şekil 2.1.3.5)



Şekil 2.1.3.5 : Multi-mode fiber çeşitleri

Bina içi 100 metreyi aşan (bakır kablo için mesafe sınır) mesafelerde, katlar arası kabin bağlantılarında ve Gigabit Ethernet için 275 metreden daha kısa bina dışı uygulamalarda da multi-mode fiber optik kablo kullanılabilir.

Şekil 2.1.3.6 : Fiber optik bağlayıcı çeşitleri

Çeşitli ağ uygulamalarına ve aktif cihazlara göre değişen fiber optik bağlayıcılar Şekil 2.1.3.6. da görülmektedir.

2.1.4. Yerel Ağ Cihazları

Yerel ağ cihazları ve OSI referans modelinin hangi katmanlarında çalıştıklarına dair bir özet, Tablo 2.1.4.1. de görülmektedir.

Tablo 2.1.4.1 : Yerel Ağ (LAN) Cihazları

Cihaz	OSI Referans Modeli
Tekrarlayıcı	1. Katman (fiziksel)
Hub	1. Katman (fiziksel)
Köprü	2. Katman (veri iletim)
Anahtar	2. Katman (veri iletim) veya 3. Katman (ağ)
Yönlendirici	3. Katman (ağ)

Tekrarlayıcı (Repeater)

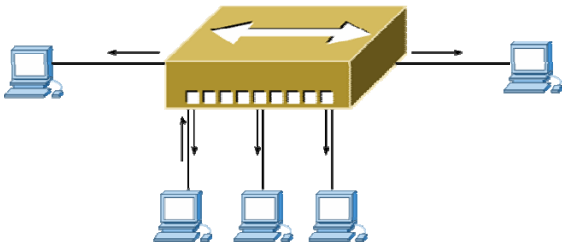
Bir verici (transmitter) cihazı sinyalleri göndermek, alıcı (receiver) cihazı sinyalleri almak ve tekrarlayıcı (repeater) ise alıcı ve verici arasında yol alan sinyalleri

kopyalamak veya güçlendirmek için kullanılan ağ cihazlarıdır. [Castelli Matthew J., 28] Ayrıca Ethernet ağında kullanılabilecek mesafeyi arttırmak, ağa bağlı bilgisayar adedini arttırmak ve farklı kablo tipleri kullanan ağları birleştirmek tekrarlayıcıların kullanım amaçlarıdır. Tekrarlayıcılar Şekil 2.1.4.1.1. de görüldüğü gibi OSI referans modelinin fiziksel katmanında yer almaktadırlar.

Şekil 2.1.4.1 : Tekrarlayıcının işlevi ve OSI modelindeki yeri

Hub

Hub' lar genellikle 24 veya daha da az cihazdan oluşan küçük LAN bölümlerini (segment) birleştirmek için kullanılır. Hub'lar birden çok giriş-çıkışa (multiport) sahip tekrarlayıcılar olup bir portuna gelen frame'leri diğer portlara tekrarlar. Böylece ağın tüm bölümleri bütün frame'leri görebilirler. Hub'lar da tekrarlayıcılar gibi OSI referans modelinin fiziksel katmanında yer almaktadırlar.



Şekil 2.1.4.2 : Hub

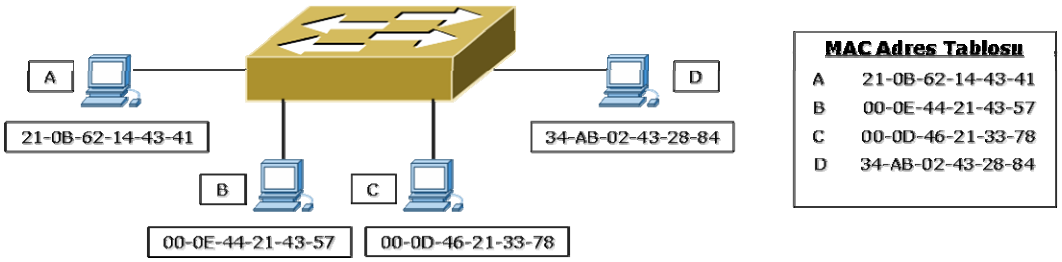
Köprü (Bridge)

Köprüler, iki benzer ağ bölümünü birbirine bağlamak için kullanılırlar. Köprüler, veri paketlerini fiziksel adresleri vasıtasıyla süzer ve iletir. Köprü cihazı bağlı olduğu ağın tüm bölümlerini dinler ve hangi fiziksel adresin hangi bölümde olduğunu gösteren bir tablo hazırlar. Bir bölümden bir veri iletilmek istendiğinde, köprü cihazı hedef adresin tablosunda yer alıp almadığını kontrol eder. Eğer hedef adresi tablosunda yoksa veriyi gönderildiği bölüm hariç tüm bölümlere iletir. [Casad J., 29] Köprüler OSI modelinin veri iletim katmanında çalışırlar.

Şekil 2.1.4.3 : Köprü cihazı

Anahtar (Switch)

Anahtarlar çok portlu köprü cihazlarıdır. Hub'lar aldığı veri paketini tüm portlarına iletirken aynı anda sadece tek bir veri paketi gönderebilir. Anahtarlar ise birden çok bağlantıyı aynı anda yürütebilir. Ağ üzerinde iki bilgisayar arasında iletişim oluyorsa işleyiş açısından hub ve anahtarın arasında fark yoktur. Fakat ikiden fazla bilgisayar var ise anahtar kullanmak çok daha performanslı olacaktır. [Null L., Lobur J., 30] Aynı köprü cihazlarında olduğu gibi anahtarlar da kendisine bağlı bulunan bilgisayarların fiziksel adreslerini bir tabloda tutar (MAC adres tablosu).



Şekil 2.1.4.4 : Anahtar cihazı

OSI modelinin ikinci katmanında çalışan anahtarlar olduğu gibi üçüncü katmanında da çalışan anahtarlar mevcuttur.

Yönlendirici (Router)

Bir yönlendirici kendisine bağlı olan uçlardaki trafiği ileterek bir anahtarın yaptığı her şeyi yapar. Fakat anahtarlar frame ve MAC adresler ile işlem yaparlar. Farklı ağlarla iletişim kurulmak istendiğinde veya internet üzerinde iletişim kurulmak istendiğinde yönlendirici kullanmak gerekir. Yönlendiriciler OSI modelinin üçüncü katmanında çalışırlar ve paketleri yönlendirirken IP protokolünü kullanırlar. Yönlendirici yerel ağdan bir Ethernet frame'i aldığında frame'in içinde veri alanında yer alan IP başlığına

bakar ve paketin gitmesi gereken hedefin IP adresini okur. [Axelson J., 31] Anahtarlar gibi yönlendiriciler de trafiği yönlendirmek için kullanılan IP adres tabloları tutarlar.

2.2. YEREL ALAN AĞLARI

Yerel alan ağı bir ev, ofis veya yerleşke gibi nispeten daha sınırlı bir coğrafi alandaki bilgisayar ve bileşenlerini yüksek hızlarla bağlandığı ağlardır. Yerel ağlar; bilgisayar kullanıcılarına uygulamalara ve cihazlara ulaşım, bağlı kullanıcılar arasında dosya değişimi, elektronik posta ve diğer uygulamalar yoluyla haberleşme gibi çeşitli avantajlar sağlar.

Daha çok üzerinde duracağımız üniversite altyapılarında kullanılan yerleşke ağları, adını birden fazla binayı bir ağ ile birleştiren ilk organizasyonlar olan üniversitelerden almaktadır. Birbirine yakın binalar arasında bilgi ve kaynak paylaşımını sağlarlar. Yeraltı ve yerüstü kabloları kullanılarak bir omurga çatısı altında tüm yerleşkeyi çevrelemektedirler. [Uçan Osman N. ve diğ., 2] LAN ile benzer özelliklere sahiptir. Aralarındaki fark ise daha uzak mesafelere sahip olması ve birden çok LAN' ı kapsayabilmesidir. Mesafe olarak bakır kablonun yeterli gelmediği durumlarda Single Mod veya Multi Mod fiber optik kablolar kullanılabilmektedir.

Yerel Alan Ağlarında iki ve ya daha fazla sayıdaki bilgisayar bir ağ topolojisi kullanarak 10/100/1000 mbit/s hızları ile veri iletişiminde bulunabilirler. Verimli ve etkin bir yerel ağın aşağıdaki özelliklere sahip olması gerekir; [Slone, 3]

- **Güvenilirlik:** Ağın tasarımını kablo güzergâhlarında elektromanyetik girişimlerden uzak tutarak, kabinlerde kullanılan cihazların özenle seçilip yapılandırılmasıyla ve tasarımda yedeklemeyi de göz önünde bulundurarak güvenilirlik sağlanabilir.
- **Bütünlük:** Kablolama altyapısını hazırlarken kurumun bütçesi, politikaları ve diğer sınırlamalar dahilinde her katı, birimi ve odaları kapsayacak şekilde bütün kurumu içine alan bir yaklaşım sergilenmelidir.
- **Genişleyebilme:** Kurumun doğabilecek yeni ihtiyaçlarına karşın genişlemeye uygun, esnek bir yapıda olmalıdır. Kablolama altyapısında kullanılacak cihazlar bu anlayışa göre seçilmelidir.

- **Maliyet etkinlik:** Ağ altyapısını oluştururken pasif kablolama elemanların ve aktif cihazların maliyetleri göz önünde bulundurulmalıdır. Kurumun ilerleyen teknolojik ihtiyaçlarına cevap verebilecek şekilde aktif cihazlar en az beş yıl, pasif elemanlar yirmi yıl etkinliğini koruyabilmelidir.
- **Standartlara uyumluluk:** Ağ altyapısı oluştururken pasif kablolama elemanların ve aktif cihazların hem ulusal hem de uluslar arası standartlara uyumluluğu göz önünde bulundurulmalıdır.
- **İzlenebilirlik:** Ağ altyapı cihazlarına kurum politika, yönerge ve talimatlarının uzaktan uygun bir yazılım veya donanım vasıtasıyla uygulanması mümkün olmalıdır. Ayrıca bu yönetim sayesinde cihazlarda oluşabilecek arıza ve uyarılar da gözlemlenebilmelidir.

2.2.1. Üniversitelerde Yerel Alan Ağı Altyapısı

İnternet ve internet bileşenlerinin (web, mail vb.) kullanımının hızla artması ile üniversiteler, ağ altyapılarında güncel teknolojileri uygulama ihtiyacı hissetmişlerdir. ULAKNET in yapısındaki gelişmelerin de bu uygulamalarda itici bir rolü olmuştur. Bu gelişmelerin ayrıntılarına "Dünden Bugüne UlakNet", http://www.ulakbim.gov.tr/hakkimizda/tarihce/ulaknet/dunbugun.uhtml adresinden ulaşılabilir. 2000 yılından sonra uygulanan projelerde yaygın olarak Gigabit Ethernet teknolojisi kullanılmaya başlanmıştır. Bu teknolojide anahtarlar arası bir yada birden fazla gigabit bağlantıya, kullanıcılar 10/100 Mbps hızlarında bağlantıya sahip olmuşlardır.

Üniversite internet altyapılarını yerleşke üniversiteleri ve şehir üniversiteleri olarak ikiye ayırmak mümkündür.

2.2.1.1. Yerleşke (Kampus)Üniversiteleri

Nüfus ve yerleşim olarak genelde tek yerleşkeden oluşan, tek bir çatı (omurga) altında toplanmış üniversitelerdir. Bu yapı yönetim ve kontrol açısından kolaylık sağlamaktadır. Örn: Koç, Sabancı, Bilkent, Yeditepe, Beykent, Bilgi, Işık Üniversiteleri vb.

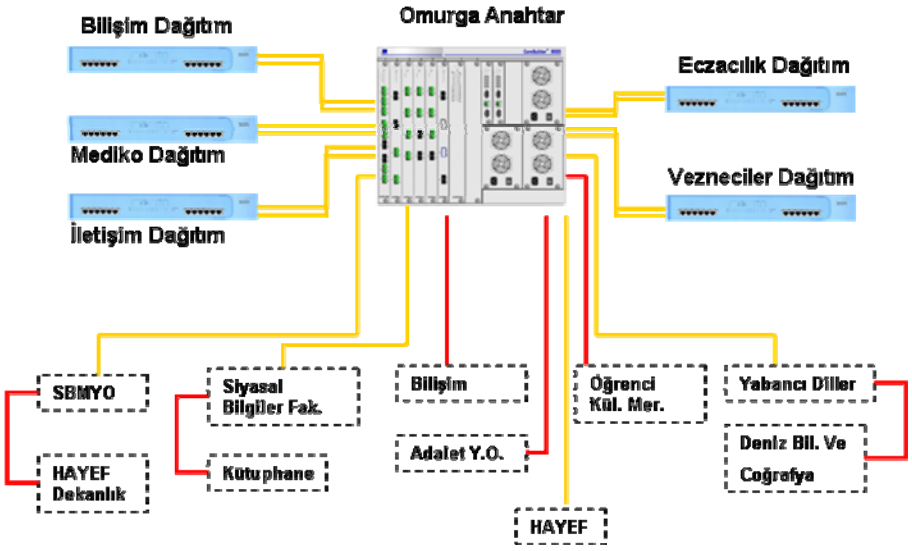
2.2.1.2. Şehir Üniversiteleri

Benzer büyüklüklerde birden fazla yerleşkeye sahip, birden fazla omurganın tek bir noktada merkez yerleşkede birleşip akademik ağa bağlantısının olduğu üniversitelerdir. Bu tip üniversiteler bulundukları şehrin içine dağılmış hatta bazı durumlarda başka şehirlere kadar uzanan şubelere (Yüksek Okullar, enstitüler, merkezler gibi) sahiptirler. Bu yapıda yönetim tek bir merkezden kontrol edilmekle beraber alt bölümlere ayrılarak kendi içlerinde ayrı bir kontrol merkezleri oluşturulmuştur. En büyüklerine örnek olarak, İstanbul Üniversitesi, Marmara, İTÜ, Ege, Selçuk Üniversiteleri gösterilebilir.

2.2.2. Örnek: İstanbul Üniversitesi Beyazıt Yerleşkesi Yerel Alan Ağı

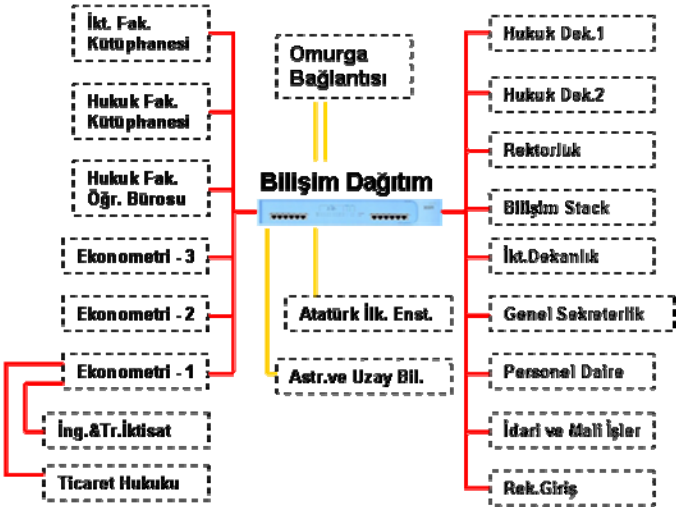
Merkez Kampüsü Beyazıt ve Vezneciler olarak ikiye ayırabiliriz. Yerel ağ omurgası Biyoloji Binasında bulunmaktadır. Fiber optik kablo altyapısının bu binada toplanması merkez olmasının en büyük etkenidir. Omurga anahtar şase tipinde ve üzerine modüller eklemek suretiyle genişleyebilen yapıdadır. Üzerinde yedekleme (redundancy) için gerekli olan yönetim, denetim, anahtarlama, supervisor modülleri mevcuttur. Omurga anahtar üzerinde ara dağıtım anahtarlarının bağlantısı için 9 adet 1000Base-SX, 16 adet 1000Base-LX ve Server Bağlantıları içinde 4 adet 1000Base-T port bulunmaktadır.

Dağıtım (distribution) noktaları kullanılarak, kenar anahtarların omurgaya olan bağlantısı sağlanmış böylece her bir fakültenin gerektiğinde omurga anahtardan bağımsız olarak çalışabilmesi mümkün kılınmıştır. Dağıtım anahtarları ağ tasarımı itibariyle her bir fakülte ve bunlara bağlı alt birimlerin kendi içlerinde haberleşebilmesini sağlamak üzere üçüncü katman yönlendirme yapabilecek şekilde yapılandırılmışlardır. Böylelikle her fakülte istenildiğinde kendi içindeki VLAN (Sanal Yerel Ağlar) lar arası iletişimini, dağıtım anahtarı üzerinde kayıpsız bir performansla yapabilecektir. Dördüncü katman TCP/UDP port bazında trafik önceliklendirmesi özelliği sayesinde, dağıtım anahtarının gelişen uygulamaları daha performanslı yönetebilmesi ve network kritik uygulamaların (Ses, SQL, SNMP vb.) ihtiyacı olan en az gecikme süresini sağlayabilmek mümkün olabilmektedir. Dağıtım noktalarından gelen trafik yoğunlukları göz önünde tutularak omurga bağlantıları, 2 Gbps hızında trunk hatlarıyla (iki link tek bir hatmış gibi yapılandırılarak) sağlanmıştır. Şekil 2.1.2.1. de Beyazıt Yerleşkesi Yerel Alan Ağı ana çatısı görülmektedir.



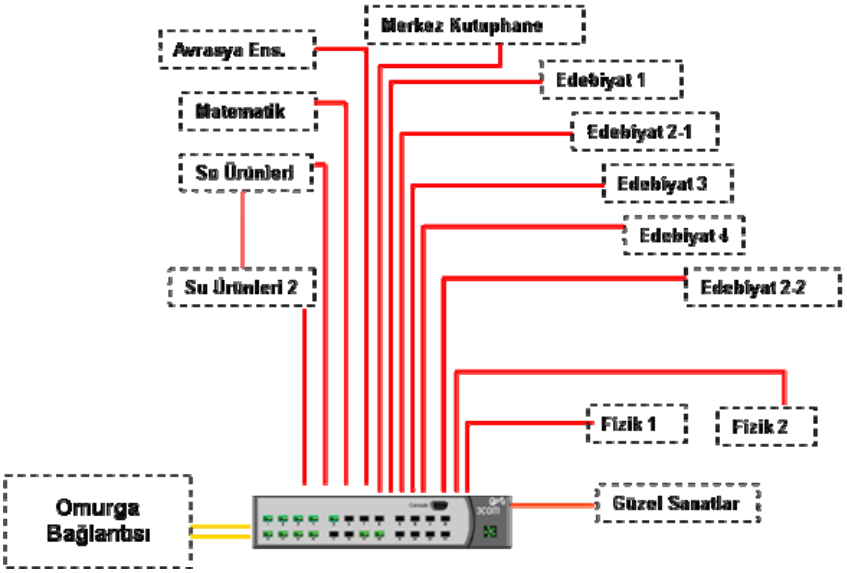
Şekil 2.2.2.1 : Beyazıt Yerleşkesi Yerel Alan Ağı ana çatısı

Sarı ile ifade edilen hatlar Single-mode fiber, kırmızı ile ifade edilen hatlar ise multi-mode fiber kabloları göstermektedir. Kablo seçiminde iki birim arası mesafeler etken olmuştur. 200 Metre'nin altındaki mesafelerde multi-mode 8 damarlı, outdoor, 62.5/125 mikron'luk çelik zırhlı fiber optik kablolar kullanılmış, 200 metrenin üstündeki mesafelerde single-mode 9/125 mikronluk 12 damarlı, outdoor çelik zırhlı fiber optik kablolar kullanılmıştır. Şekil 2.1.2.2. de omurgaya bağlı dağıtım merkezlerinden Bilişim Dağıtım anahtarı ve ona bağlı merkezler görülmektedir.



Şekil 2.2.2.2 : Bilişim Dağıtım anahtarı ve ona bağlı merkezler

Bina içi kablolamalarda, uygun mesafelere kablo toplama merkezleri (kabinet) yerleştirilerek her odadan gelen Cat5E UTP bakır kablolar bu merkezlerde sonlandırılmıştır.



Şekil 2.2.2.3 : Vezneciler dağıtım anahtarı ve ona bağlı merkezler

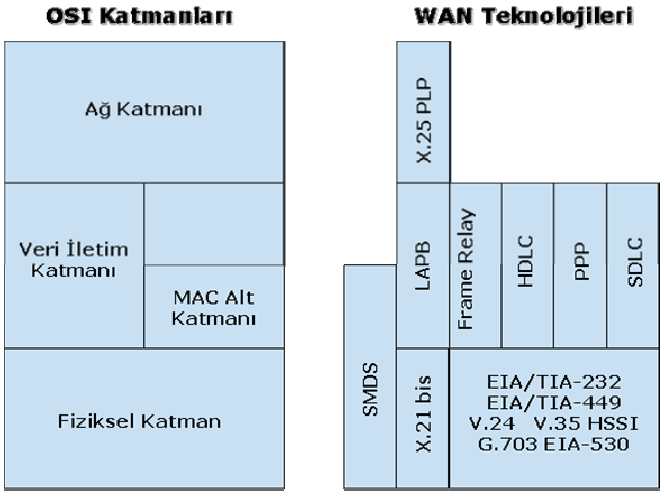
Ana dağıtım noktalarından Vezneciler Dağıtım anahtarı ve ona bağlı merkezler Şekil 2.1.2.3. de görülmektedir.

2.3. GENİŞ ALAN AĞLARI

Geniş alan ağları (Wide Area Network), geniş coğrafi bölgelerle ayrılmış yerel alan ağlarını, yerel alan ağlarına göre daha düşük hızlarla birbirine bağlar. Bunu yaparken Türk Telekom gibi servis sağlayıcılarının altyapılarını ve hizmetlerini kullanır. Türkiye'de tüm üniversite ve araştırma kurumlarını birbirine bağlayarak akademik bir ağ oluşturan ULAKNET geniş alan ağlarına en güzel örnektir.

Ekonomik ve teknik sebeplerden dolayı, LAN'lar uzun mesafeli iletişimler için uygun değildirler. [Çakır Ali Y. ve diğ., 32] Birbirinden farklı yerel alan ağları arası veri iletişiminde belirli şartları yerine getirebilmek için geliştirilmiş WAN hatları kullanılmaktadır. Bu belirli ağ ve uygulama ihtiyaçlarını karşılayabilmek için de birçok WAN tekniği geliştirilmiş ve yıllar boyunca yaygın bir şekilde kullanılmıştır. WAN teknolojileri genellikle OSI modelinin alt üç katmanı olan fiziksel, veri iletimi ve ağ

katmanlarında çalışmaktadırlar. [33] Şekil 2.3.1. de yaygın WAN teknolojileri ve OSI modeli arasındaki ilişki görülebilmektedir.



Şekil 2.3.1 : WAN Teknolojileri OSI modelinin en alt katmanlarında çalışırlar

- **Kiralık hatlar:** Kiralık hatlar (leased lines), en iyi ağ yönetim kontrolünü sağlarlar. Kiralık hatlarda kullanıcıya söz verilen miktarda bir bant genişliği tedarik edilir ve kullanıcıdan başkasının erişimi mümkün değildir. Fakat her zaman tümüyle kullanılamayan bir bant genişliği kapasitesi söz konusudur. Bu nedenle maliyetleri de yüksektir.

Kiralık hatların maliyetini düşürebilmek amacıyla IP tabanlı ağlarda Frame Relay hizmetleri kullanılmaya başlanmıştır. Çok sayıda servis sağlayıcı Frame Relay hatların sanal devrelerini ortak kullandıkları için kiralık hatlara nazaran çok daha uygun bir maliyet seçeneği sunmuştur. Yoğun mültimedya veya yüksek bant genişliği gerektiren uygulamalar içeren ortamlar için belki de en uygun çözüm ve kiralık hatlara diğer bir WAN alternatifi olarak Asenkron Transfer Modu (ATM) ortaya çıkmıştır. Yakın zamanda da daha düşük maliyetleriyle ve sunduğu hizmetler nedeniyle IP tabanlı ağlar önemli bir role sahip olmuşlardır.

Günümüzde WAN kullanımının bir amacı da ses, veri ve video trafiğini bütünleştirerek ortak bir platform ve ortak bir altyapı üzerinde çalıştırmaktır. Örneğin ATM'in amacı, mevcudu kullanıp cihaz ihtiyacını en aza indirerek, bir tümleşik geniş bant altyapısı oluşturmaktır. Bugün de bu rolü IP ağları üzerine almıştır.

Tüm bu çeşitli WAN seçenekleri, *devre anahtarlamalı* (circuit-switched) ve *paket anahtarlamalı* (packet-switched) olmak üzere iki ana başlık altında toplanabilir.

2.3.1. Devre anahtarlamalı ağlar

Devre anahtarlamalı geniş alan ağları; kiralık hat teknolojisini temel alanlar ve Tümleşik Hizmetler Sayısal Ağı (Integrated Services Digital Network) nı temel alanlar olmak üzere iki ana başlıkta incelenebilir.

Kiralık hatlar

Noktadan noktaya ve sabit bir bant genişliği ihtiyacı olduğu durumlarda kiralık hatlar kullanılmaktadır. Kiralık hatlar büyük çoğunlukta şehir içi bina bağlantılarında tercih edilmektedir. Kurumun kullanımına özel olarak tahsis edilen kiralık hatlarda, gecikmeler veya kapasitede dalgalanmalar olmaz fakat maliyetleri çok yüksektir.

- **T- ve E- taşıyıcı omurga:** Kuzey Amerikan Sayısal Düzeni (North American Digital Hierarchy) kullanan; Kuzey Amerika, Kanada, Kore, Hong Kong ve Tayvan' da, bakır kablo üzerinden tedarik edilen WAN bant genişliği, T- olarak adlandırılmıştır. [Alwayn V., 34] Bu düzen Tablo 2.3.1.1. de gösterilmiştir. Bu düzen içerisinde bir kanala sayısal akım (Digital Stream: DS) denilmektedir. Sayısal akımlar, çoklanarak yüksek hızlı WAN devrelerini oluştururlar. DS-1 ve DS-3 en yaygın olarak kullanılan kapasitelerdir.

Tablo 2.3.1.1 : DS seviyeleri ve bunların T- karşılığı

Sinyal	Kapasite	DS-0 adedi	İsim
DS-0	64 Kbps	1	Channel
DS-1	1.544 Mbps	24	T1
DS-1C	3.152 Mbps	48	T1C
DS-2	6.312 Mbps	96	T2
DS-3	44.736 Mbps	672	T3
DS-4	274.176 Mbps	4032	T4

Avrupa' da ise, Avrupa Posta ve Telefon İdaresi (Committee of European Postal and Telephone: CEPT) E- sistemi adı verilen bir düzen tanımlamıştır. Bu düzen Tablo 2.2.1.1.1. de gösterilmiştir.

Tablo 2.3.1.2 : E- seviyeleri ve bunların kapasiteleri

Sinyal	Kapasite	E adedi
E0	64 Kbps	N/A
E1	2.048 Mbps	1
E2	8.448 Mbps	4
E3	34.368 Mbps	16
E4	139.264 Mbps	64

- **SDH/SONET omurga:** Synchronous Digital Hierarchy (SDH), fiber optik kablolar üzerinden veri iletiminde kullanılmak üzere, Avrupa Telekominikasyon Standartları Enstitüsü (ETSI) tarafından Avrupa için geliştirilmiş daha sonra Kuzey Amerika ve Japonya dışında heryerde kullanılan bir uluslararası standarttır. [35] SDH, Senkron İletim Sinyali (Synchronous Transport Signal) seviye 1 veya STS-1 adı verilen 51.84 Mbps hızında standart bir iletim oranını tanımlar. Daha yüksek hızlarda yapılan iletim, STS-1 in katları şeklinde gösterilmektedir. SDH teknolojsinde ise SONET' in STS oranlarına karşılık olarak Synchronous Transport Module (STM) oranı tanımlanmıştır.

Tablo 2.3.1.3 : STS – STM Oranları ve Hızları

STS Oranı	STM Oranı	OC Seviyesi	Hız
STS-1	STM-0	OC-1	51.84 Mbps
STS-3	STM-1	OC-3	155.52 Mbps
STS-12	STM-4	OC-12	622.08 Mbps
STS-48	STM-16	OC-48	2.488 Gbps
STS-192	STM-64	OC-192	9.952 Gbps
STS-768	STM-256	OC-768	39.813 Gbps

- **SONET:** Synchronous Optical Network (SONET), paketlerin veya hücrelerin fiber optik kablolar üzerinden yüksek hızlı senkron iletiminde kullanılan bir fiziksel katman özelliğidir. SONET, Amerikan Milli Standartları Enstitüsü

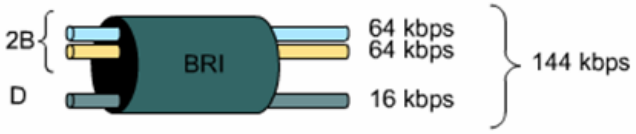
(ANSI) tarafından tanımlanmış ve Kuzey Amerika' da kullanılmaktadır. SONET, SDH sisteminin STS-1 seviyesini kendisne temel olarak almıştır. [Oppenheimer P., 36] Türkiye' de üniversitelerin bağlantısını sağlayan Ulusal Akademik Ağ (ULAKNET) ve Türk Telekom' un yüksek bant genişliğine ihtiyaç duyduğu omurga hatlarında bu teknolojiler kullanılmaktadır.

- **Dark fiber omurga:** Dark fiber deyimi, iki ucu da kullanıcıda sonlandırılmış fiber optik hatlar için kullanılmaktadır. Böylece Telekom santrallerine uğramadan iki binayı fiber optik ile yüksek hızlarla ve bant genişliğine karşılık ücret ödenmeksizin bağlamak mümkün olabilmektedir. Dark fiber uygulamasına geçmişte Türk Telekom tarafından, şirketlerin veya üniversitelerin, arasından cadde veya sokak geçen binaları arasında kullanılmasına izin verilmekteydi. Fakat son birkaç senedir Türk Telekom' un bu tip bağlantıların artık santraller üzerinden yapılması yönünde çalışmaları vardır.

Integrated Services Digital Network (ISDN)

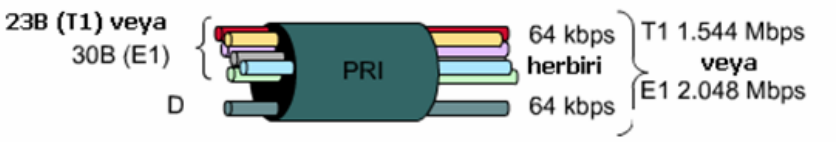
ISDN; ses, görüntü, veri gibi her türlü bilginin sayısal bir ortamda birleştirilip aynı hat üzerinden aynı anda iletilmesinin sağlandığı bir haberleşme ağıdır. ISDN, OSI referans modeline sıkı sıkıya bağlı kalınarak tasarlanmıştır. ISDN elemanları, tüm yedi katmana yayılmakla beraber çoğunlukla sadece 1. ile 3. katmanlar arasında kullanılmaktadır.

- **Basic Rate Interface (BRI):** BRI, ev ve küçük işletmelerin ihtiyacına cevap verebilecek şekilde, iki adet 64 kbps B kanalı ve bir adet 16 kbps D kanalından oluşmaktadır. (Şekil 2.2.1.2.1.)



Şekil 2.3.1.4 : ISDN BRI kanalları

- **Primary Rate Interface (PRI):** PRI, daha büyük işletmeler ve kurumların ihtiyaçlarına cevap verebilecek şekilde, otuz adet 64 kbps B kanalı ve bir adet 16 kbps D kanalından oluşmaktadır. (Şekil 2.2.1.2.2.)



Şekil 2.3.1.5 : ISDN PRI kanalları

2.3.2. Paket anahtarlamalı ağlar

X.25 Protokolü

Kiralık hatların yüksek maliyetlerine çözüm olarak paket anahtarlamalı ağlar geliştirilmiştir. Bu tip ağlara ilk örnek X.25 protokolü gösterilebilir. X.25 protokolü ister anahtarlamalı ister sabit olsun düşük bir bant genişliğinde, ortak paylaşılan bir kapasite sunar. X.25 ağları genellikle düşük kapasiteye sahip olup en fazla 48 kbps hızına ulaşabilirler. X.25, bağlantı süresi veya mesafe dikkate alınmayıp, iletilen veri miktarı temel alınarak ücretlendirildiği için maliyet açısından çok uygundur. X.25 ağları ilk olarak genellikle bankaların şube ve ATM bağlantılarında kullanılmıştır.

Frame Relay

Artan yüksek bant genişliği ve düşük gecikme değerli (latency) paket anahtarlama ihtiyaçları doğrultusunda Frame Relay teknolojisi geliştirilmiştir. Frame Relay, ağ altyapısı olarak X.25 ile benzer olup hata ve akış kontrolü yapmayarak daha basit bir protokol olması ve ağ katmanı yerine veri iletim katmanında çalışması ile X.25 ten farklılıklar gösterir. Frame Relay, ses ve veri trafiğini beraber taşıyan, sabit, ortak bir bant genişliği hizmeti sunar. Bu özelliği sayesinde kurumsal ölçekte, yüksek hız gerektiren yerel ağların bağlantısında kullanılır. Frame Relay, kurumların geniş alana çıktıklarında ihtiyaçları olan yüksek bant genişliğini sağlamak ve patlamalı (bursty) trafik profilini en iyi şekilde taşıyabilmek için geliştirilmiş, yüksek hızlı bir iletim teknolojisidir. Düşük hızlardan başlayarak, 2 Mbps, 34 Mbps, 50 Mbps'ye varan hız seviyelerinde servis vermektedir. [37] Üniversitelerin büyük kampüslerinin veya şehirlerarası iletişim gerektiren uzak merkezlerinin bağlantısı, Frame Relay ağların kullanım alanlarına örnek gösterilebilir.

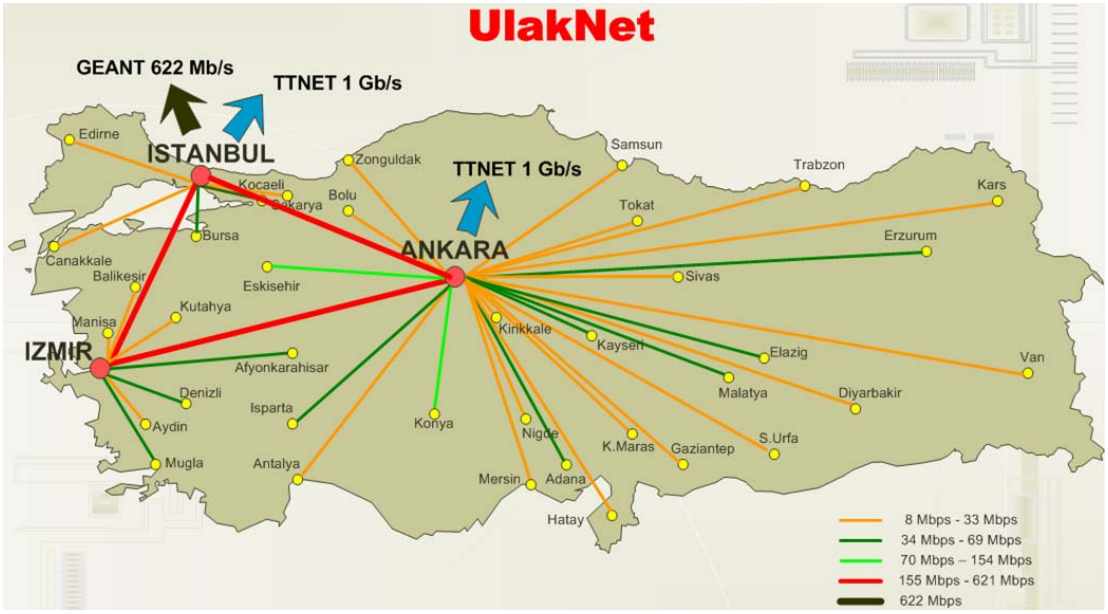
Asynchronus Transfer Mode (ATM)

ATM, ses, görüntü ve verilerin, yüksek hızlarda ve geniş ağlarda iletimi için tasarlanmış bir teknolojidir. Paketlerin iletiminde frame yerine, 5 byte başlık, 48 byte veri olmak

üzere 53 byte sabit uzunlukta hücreler kullanılır. [Bass M., 38] Bu küçük ve sabit uzunluktaki hücreler gecikmeye tahammülü olmayan ses ve görüntü trafiklerinin taşınmasına oldukça uygundur. ATM ile 2 Mbps ile 622 Mbps arası hızlarda veri iletimi mümkün olmaktadır. ATM, genellikle üniversitelerin, Türk Telekom hatları üzerinden Ulusal Akademik Ağ (ULAKNET) ile yüksek hızlarda bağlantısında kullanılmaktadır.

2.3.3. Üniversitelerde Geniş Alan Ağı Altyapısı

Üniversiteler şehir içi veya şehir dışı, yerleşke veya daha küçük birimlerini (fakülte, yüksek okul, enstitü, merkez, tesis vb.) tek bir merkezde bir araya toplarlar. Genelde kiralık hatlar (Leased Line) ve/veya frame relay teknolojiler ve 128 kbps ile 2048 kbps arası hızlarda bant genişlikleri kullanılır. Bu bant genişlikleri, yönetim, kaynakların paylaşımı ve ortak projelerin kullanılabilmesi (öğrenci, personel, maaş, hastane vb. otomasyon sistemleri) için gereklidir. Ayrıca ULAKNET bağlantısının tek bir noktadan yapılması gerekmektedir. Üniversitelerin ULAKNET bağlantılarında 8 Mbps ile 155 Mbps arası bant genişlikleri kullanılmaktadır. (Şekil 2.2.1.1.) Bu bağlantı hem ulusal akademik kaynaklara ve diğer üniversitelere erişimde hem de küresel internete çıkışta kullanılır.

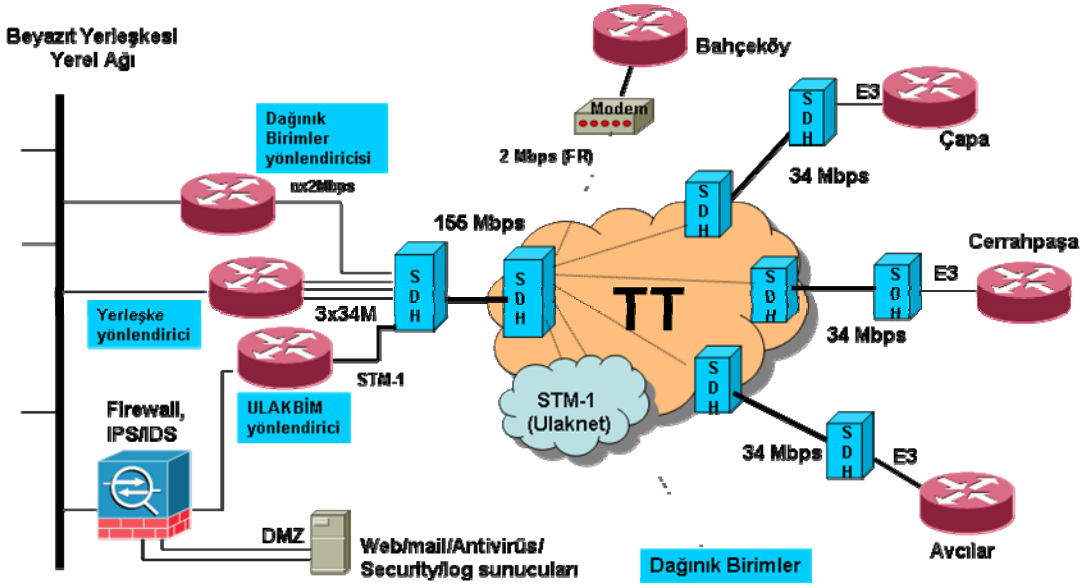


Şekil 2.3.3.1 : ULAKNET Altyapısı

2.3.4. Örnek: İstanbul Üniversitesi Geniş Alan Ağı

İstanbul Üniversitesi merkez Beyazıt olmak üzere Avcılar, Çapa, Cerrahpaşa, Bahçeköy yerleşkelerinden ve şehir içine yayılmış irili ufaklı birimlerden oluşmaktadır. Bu birimler ve 2006 yılı itibariyle merkez ile bağlantı hızları aşağıdaki gibidir;

- ULAKNET çıkış - 155 Mbps
- Avcılar yerleşkesi – Beyazıt arası - 34 Mbps
- Çapa yerleşkesi – Beyazıt arası – 34 Mbps
- Cerrahpaşa yerleşkesi – Beyazıt arası – 34 Mbps
- Bahçeköy yerleşkesi – Beyazıt arası – 2 Mbps
- Kadıköy ilçesinde Devlet Konservatuarı – 512 kbps
- Bakırköy ilçesinde Sağlık Yüksek Okulu – 512 kbps
- Şişli ilçesinde Florence Nightingale Hemşirelik Yüksekokulu – 1024 kbps
- Süleymaniye semtinde Fen Fakültesi Botanik A.B.D. – 512 kbps
- Haseki semtinde Kardiyoloji Enstitüsü – 512 kbps
- Bebek semtinde Baltalimanı Tesisleri – 128 kbps
- Horhor semtinde İlahiyat Fakültesi, Döner Sermaye İşletme Saymanlığı, Tıp Tarihi, Basımevi ve Film Merkezinden oluşan Horhor yerleşkesi, 54 Mbps hızında kablosuz (Wireless) teknoloji ile merkeze bağlıdır.
- Sakarya ili Sapanca ilçesinde bulunan Su Ürünleri Fakültesi Su Ürünleri Meslek Yüksekokulu – 256 kbps hızına sahiptir.



Şekil 2.3.4.1 : İstanbul Üniversitesi geniş alan ağı

Şekil 2.3.4.1. den de görüleceği üzere Avcılar, Çapa ve Cerrahpaşa yerleşke hatları ayrı bir yönlendirici, dağınık birimler ve Bahçeköy yerleşkesi ayrı bir yönlendirici, ULAKNET ve küresel internete çıkış hattı da ayrı bir yönlendirici vasıtasıyla yapılmaktadır. Böylece trafik yükü tek bir yönlendirici üzerinde toplanmamış yük paylaşımı ve dengelenmesi sağlanmıştır.

Ana yerleşkelerin en yakın Türk Telekom santraline bağlantıları fiber optik hatlar üzerinden SDH cihazları aracılığıyla sağlanmaktadır.

ULAKNET yönlendiricisi ve yerel ağ omurga cihazı arasına bir güvenlik ihlallerini tespit ve önleme cihazı (Intrusion Detect & Prevention System) konumlandırılarak giren ve çıkan her türlü trafik olabilecek saldırı ve tehditlere karşı süzülmektedir.

Ayrıca İstanbul Üniversitesi yönlendirici ve anahtarlarından alınan trafik ölçümleri http://mrtg.istanbul.edu.tr/ adresinden gözlemlenebilmektedir.

3. GÜVEN KAVRAMI VE POLİTİKA İLİŞKİSİ

Güven; Türk Dil Kurumu Güncel Türkçe Sözlüğünde "korku, çekinme ve kuşku duymadan inanma ve bağlanma duygusu, itimat" olarak ifade edilmiştir. [39] Politika ise; varılmak istenen hedef doğrultusunda atılacak adımlara ve verilecek kararlara rehberlik edip yön verecek kurallar dizisinden oluşan, bir hareket planı olarak tanımlanabilir. Burada hedef bir güvenlik politikası oluşturmak olunca, güvenli bir ortam sağlayabilmek için yapılması ve yapılmaması gerekenler politika içerisinde açıkça anlatılmalıdır.

Güven kavramı birçok politikanın temelini oluşturur. Bazı politikalar insanların doğru şeyleri yapacakları hususunda kuşku duyulmadığı için yazılmayabilir. Diğer taraftan insanların her zaman doğru şeyleri yapmayacaklarını bildiğimiz ve onlara güvenmediğimiz konularda da yazılı politikalara ihtiyaç duyarız. Aslında gerçek olamayacak kadar güzel olan bir şey var ise o da; insan, bilgi, yazılım ve donanım gibi korunması gereken tüm kaynakların güvenilir olmasıdır. Donanımlarda çıkan problemler ve yazılımların güvenlik açıkları artık sıradan hale gelmiştir. Bir arıza durumu ortaya çıktığında, önceden hazırladığımız kontrolleri ve yönergeleri uygulamak bu durumun olumsuz etkisini en aza indirecektir.

Kullanıcılar ve erişebilecekleri kaynaklar sınıflandırılmalıdır. Kullanıcılara ve çalışanlara güven duygusu, zamanla bilinç ve eğitim düzeyi yükseldikçe gelişecektir. Fakat başlangıçta değişik sınıflara ayrılmış olan çalışanlara farklı seviyelerde güvenilmelidir. İlk adım kimin, kaynaklara, ne kadar erişimine izin verileceği, yani güven seviyesinin belirlenmesi kararıdır. Güven seviyesinin kararı hassas bir dengedir. Çok fazla güven duymak beraberinde güvenlik sorunlarını getirebilir. Çok az güven duyulması ise çalışan bulma ve elde tutmayı zorlaştıracaktır.

3.1. GÜVENME ŞEKİLLERİ VE GÜVENLİK

Herkese her zaman güvenmek, günümüz dünyasında pek mümkün değildir. En kolay uygulanabilir olanıdır, fakat gerçeğe aykırıdır. Hiçbir zaman kimseye güvenmemek, genelde yüksek güvenlik seviyeli devlet kurumlarında mümkün olabilir. En sıkı

önlemleri içermesine karşın bunun da uygulanması mümkün gözükmemektedir. Belli kişilere belli zamanlarda güvenmek, en bilinen yöntem olup güven duygusunun zamanla oluşması beklenir. Ayrıca kurumun farklı birimlerinde farklı güvenlik seviyeleri uygulamak mümkündür.

İnsanların politikalara yaklaşımı pek sıcak olmamaktadır. İnsanlar, kurallara uymaktan ve faaliyetlerinin sınırlandırılmasından hoşlanmazlar. Ayrıca politikalara uyulmasının ve uygulanmasının zor olacağını düşünerek çekinirler. Güvenlik ihtiyaçlarına karşı, farklı bakış açıları vardır;

- Kullanıcılar, işlerini bu kadar çok kural ve kontrol altında yapamayacaklarını düşünerek endişelenirler.
- Sistem destek personeli, sistemlerin yönetiminin daha sıkı kontroller altında kolay olmayacağı hususunda endişe duyarlar.
- Yönetim, herkesin gönül rahatlığıyla bilgi alışverişi yapabildiği, çalışabildiği ve üretebildiği güvenli bir ortam sağlayabilmek için gereken yazılım, donanım ve en önemlisi insan yatırımı maliyetlerini düşünerek endişelenir.

Güvenlik politikaların hazırlanmasının en önemli amaçlarından biri, her ne kadar tüm çalışanlarının kurumsal bir hedef ve bakış açısı doğrultusunda davranmalarını sağlamak ise de, herkesin tam olarak fikir birliğine vardığı bir politika oluşturulmasının neredeyse imkânsız olduğu unutulmamalıdır.[Guel Michele D., 40]

“Güvenlik bir süreçtir, bir ürün değildir. Bir ürün gibi alıp, basit bir şekilde mevcut sisteminize ekleyemezsiniz. Sistemin maruz kalabileceği tehditleri anlamanız, bu tehditleri göğüsleyebilecek bir güvenlik politikası tasarlamanız ve uygun karşı önlemleri hayata geçirmeniz gerekir. Ürünler bir miktar koruma sağlarlar, ancak güvenli olmayan bir dünyada etkin olarak iş yapabilmenin tek yolu, işin içsel güvenlik risklerini fark edecek süreçleri yerleştirmektir. İşin sırrı, ürün ve yamalardan bağımsız olarak riske açık olma durumunu azaltabilmektir.” [Schneier B., 41]

3.2. RİSK NEDİR?

Risk güvenlik terminolojisi içerisinde ele alındığında kurum değer veya varlıklarının potansiyel olarak zarara veya tehlikeye uğrama olasılığıdır. Korunması gereken ve bir değere sahip olan her şey varlıktır. Bunlar başta bilgi, belge, yazılım, donanım, kurum çalışanları, kurumun saygınlığı ve kurumun imajıdır. [Bejtlich R., 42] Risk aşağıdaki şekilde formüle edilebilir;

Risk= tehdit x güvenlik boşluğu (zafiyet) x varlık değeri

Tehdit kaynaklarının ya da güvenlik boşluklarının azaltılması, tehdide ait riskleri de aynı oranlarda azaltacaktır.

Tablo 3.2.1 : Tehdit Kaynağı - Güvenlik Boşluğu - Risk İlişkisine Örnekler

Tehdit Kaynağı	**Etkileyebileceği Güvenlik Boşluğu**	**Oluşan Risk**
Virüs	Antivirüs yazılımının eksikliği	Virüs bulaşması
Hacker	Sunucu bilgisayar üzerinde çalışan güçlü hizmet programları	Gizli bilgilere yetkisiz erişim hakkının elde edilmesi
Kullanıcılar	İşletim sisteminde yanlış ayarlanmış bir parametre	Sistemin çalışamaz duruma gelmesi
Yangın	Yangın söndürme cihazının eksikliği	Bina ve bilgisayar sistemlerinin zarar görmesi ve can kaybı olasılığı
Çalışanlar	Erişim denetim mekanizmalarının yetersizliği	Görev-kritik bilgilerin zarar görmesi
İş ortağı olan bir firmanın yetkilisi	Erişim denetim mekanizmalarının yetersizliği	Ticari sırların çalınması
Saldırgan	Kötü yazılmış bilgisayar programları	"tampon taşması" hatasının alınması
Kötü niyetli ziyaretçi	Güvenlik Görevlisinin olmayışı	Kıymetli cihaz ve/veya bilgilerin fiziksel olarak çalınması
Çalışan	Tutulan kayıtlardaki yetersizlik	Veri işleme programına verilen giriş verileri ve çıkış olarak elde edilen veriler üzerinde değişiklikler yapılması
Saldırgan	Güvenlik Duvarı'nın ayarlarının iyi yapılmamış olması	Bir "hizmet durdurma" saldırısının gerçekleşmesi

Tablo 3.2.1. de tehdit kaynağı - güvenlik boşluğu - risk ilişkisine örnekler yer almaktadır. [43]

3.2.1.Risk Analizi

Risk analizi; güvenlik risklerinin, bu risklerin ölçeklerinin ve önlem alınması gereken alanların belirlenmesi sürecidir. Risk analizi ve yönetiminin hedefi, kurum içerisinde olabilecek tehlikelere uygun cevap verebilecek, kasıtlı ya da kasıtsız tehditlerin etkisini ve olma ihtimalini azaltacak hazırlıkları, adımları ve kontrolleri teşhis etmektir. [Stoneburner G. ve Goguen A., 44]

Risk analizi öncesi yapılacak temel hazırlıklar aşağıdaki gibidir;

- Analizin kapsamı belirlenir,
- Belirlenen kapsam dahilindeki süreçler ve bu süreçler arası ilişkiler ortaya konulur,
- Risk analizini yapacak takım oluşturulur,
- Risk analizi metoduna karar verilir. [Karabacak B., 45]

İki temel risk analizi yöntemi mevcuttur. Bunlar, kantitatif (quantitative) ve kalitatif (qualitative) yöntemlerdir.

- Kantitatif risk analizi, riski hesaplarken sayısal yöntemlere başvurur. Kantitatif risk analizinde tehdidin olma ihtimali, tehdidin etkisi gibi değerlere sayısal değerler verilir ve bu değerler matematiksel ve mantıksal metotlar kullanılarak risk değeri bulunur.

  $$Risk = Tehdidin\ Olma\ İhtimali\ x\ Tehdidin\ Etkisi$$

  formülü kantitatif risk analizinin temel formülüdür.

- Diğer temel risk analizi yöntemi ise kalitatif risk analizidir. Kalitatif risk analizi riski hesaplarken ve ifade ederken sayısal değerler yerine yüksek, çok yüksek gibi tanımlayıcı değerler kullanır.

Risk analizi; ekip çalışması ile gözlemleyerek, düzeltmeler yaparak ama sonuç alınıncaya kadar, ısrarla uygulanmalıdır.

3.2.2. Risk Yönetimi

Risk yönetimi; bir kişinin, bir proje veya şirketin, hedeflerine ulaşma sürecindeki belirsizliklerin tanımlanması, analizi ve etkilerinin değerlendirilmesidir. Sonuçta "uygun karşı planlar" ın oluşturulması riskin yönetilmesi demektir. Hedefe giden yoldaki tüm belirsizlikler, yönetimi gerektirecek risklere dönüşebilir. [Filiz A., 46]

Bilgi teknolojilerinde risk yönetimi ise kurumun bilgi kaynaklarını, güvenlik konusunda yaptığı yatırımları ve varlıklarını verimli bir şekilde kullanabilmeyi sağlar. Risk yönetiminde esas olan, riskin tümüyle engellenmesi değil, sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. [TBD Kamu-BİB, 47] Kurum olarak bu süreç doğrultusunda resmi bir risk yönetim planı ortaya konulmalıdır.

Risklerin ortaya konulması, analizi, değerlendirilmesi, azaltılması veya aktarılması işlemleri, risk yönetiminin genel özellikleridir. Risk yönetim işleminde temel teşkil edecek bir kaç anahtar soru mevcuttur:

- Ne olabilir (bir tehdit veya saldırı olayı)?
- Eğer olursa ne kadar kötü olabilir (tehdidin etkisi veya sonuçları)?
- Ne kadar sıklıkta olur (tehdidin periyodu)?
- İlk üç sorunun cevapları ne kadar kesin olur (belirsizliğin tanımlanması)?

Bu sorulara cevap bulunduğunda mevcut risklerin neler olduğu ve nasıl değerlendirilmesi gerektiği ortaya çıkmaktadır. [Tipton H. ve Krause M., 48]

3.2.3. Risk Değerlendirmesi

Risk değerlendirmesi, ilk önce açıklıkların ve tehditlerin belirlenmesi, sonrasında ise bu açıklıkların saldırganlar tarafından kullanılması durumunda ortaya çıkacak zararın ve bu zararın ortaya çıkma ihtimalinin belirlenmesi ve risklerin hesaplanması faaliyetlerinden

oluşmaktadır. Risk değerlendirmesi kapsamında mevcut güvenlik önlemlerinin belirlenmesi ve etkinliğinin saptanması çalışmaları da yapılmaktadır. Risk değerlendirmesi çalışmasının sonucunda, sistemin toplam risk değeri ve öncelikli olarak ele alınması gereken konular belirlenmiş olacaktır.

Risk değerlendirme işlemi, aşağıdaki adımlardan meydana gelmektedir: [Cole E. ve Krutz R., 49]

1. **Sistemin ortaya konulması:** Risk değerlendirme işleminin kapsamını tasvir ve tarif eder. Adım boyunca yazılım, donanım, veri, sistem arayüzleri, sistem kullanıcıları, sistem destek personeli, sistemin görevi, sistem verilerin önemi, hassasiyeti, işlevsel bir sistemin gereksinimleri, sistem güvenlik politikaları, sistem güvenlik mimarisi, ağ topolojisi, bilgi depolama koruması, sistem bilgi akışı, teknik güvenlik kontrolleri, fiziksel güvenlik ortamı ve çevre güvenliği gibi sistem hakkında bilgiler bir araya getirilir.
2. **Tehditlerin tanımlanması:** Bu adım potansiyel tehdit kaynaklarını tanımlar ve bu kaynaklar ile ilgili bir rapor oluşturur.
3. **Güvenlik boşluğu (vulnerability) tanımlaması:** Bu adım potansiyel tehdit kaynakları tarafından sömürülebilecek sistem güvenlik boşluklarını ortaya çıkarır. Yeni çıkan güvenlik boşlukları, web üzerinde bulunan çeşitli veri tabanlarından ve sitelerden takip edilebilir. (Örn: UlakCSIRT, olympos.org, NIST veritabanı vb.)
4. **Kontrollerin analizi:** Bu adım sistemde güvenlik boşluğunu kullanabilecek tehdit olasılığını en aza indirmek veya yok etmek için, sistem içine yerleştirilmiş kontrolleri analiz eder. Bu kontroller teknik olabildiği gibi, güvenlik politikaları, yönetimsel faaliyetler gibi teknik olmayabilirler.
5. **Olasılık tespiti:** Bu çalışma, tehditlerin kullanabileceği potansiyel güvenlik boşluklarının olasılığını oransal bir ifade şeklinde ortaya koyar. Olasılık seviyeleri yüksek, orta ve düşük olarak ifade edilir.
6. **Etki analizi:** Etki analizi, tehditlerin kurum üzerinde yaratacağı etkilerin belirlenmesi aşamasıdır. Etki analizinin yürütülebilmesi için gereken bilgiler, bir iş etki analizi (Business Impact Analysis: BIA) veya görev etki analizi raporu gibi mevcut kurumsal belgelerden sağlanabilir.
7. **Risk tespiti:** Bu adım sistemin risk seviyesini ortaya çıkarır.

8. **Kontrol önerileri:** Bu adım risklerin azaltılması için uygulanması gereken kontrolleri ortaya koyar. Bu kontrolleri belirlerken kurumsal politika, maliyet-kar analizi, uygulanabilirlik, emniyet ve güvenilirlik hususları dikkate alınmalıdır.
9. **Sonuçların belgelenmesi:** Risk değerlendirme işleminin son adımı, bir risk değerlendirme raporu oluşturulmasıdır. Bu rapor yönetime, bütçe, politikalar, yönergeler, idari ve mali işler konularında karar sürecinde destek olmalı ve yol göstermelidir.

Risklerin yukarıda belirtildiği şekilde tanımlanması ve önceliğinin belirlenmesinin yanı sıra, bu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli, gerekli önlemler planlanarak uygulanmalıdır. [TBD Kamu-BİB, 50]

3.3. BİLGİ GÜVENLİĞİ

Bilgi güvenliği; bilgilerin gizli veya açık olsun, üretilmesi, saklanması, korunması, iletişimi, işlenmesi ve kullanılması çerçevesinde, gözetilecek ilkeleri, politikaları, elektronik ve matematiksel yöntemleri içine alan üst bir kavramdır. [İnce F., 51]

Korunması gerekli bilginin, olası hasarların ve bunların değerlerinin saptanması ve koruma adımlarının tanımı ve bunların maliyetinin saptanması bilgi güvenliği tanımı ile ilgili konulardır. Koruma adımları; hasarı önleme, hasarı tespit etme ve bilgiyi hasardan önceki haline getirme olarak sıralanabilir. [Çağlayan M. Ufuk, 52]

"Bilgi birçok formlarda bulunabilir. Kâğıda basılabilir, elektronik olarak depolanabilir, posta veya elektronik yollar ile gönderilebilir, filmler üzerinde gösterilebilir, sohbetlerde konuşulabilir. Bilgi hangi biçimde olursa olsun, her zaman uygun olarak korunmalıdır." [53]

Bilgi güvenliği temel ilkeleri aşağıdaki gibi sıralanabilir:

- **Gizlilik (confidentiality):** Gizlilik, kurum için önem taşıyan hassas bilgilerin, sadece erişimine izin verilmiş yetkili kişiler tarafından ulaşılabilir olması durumdur.
- **Bilgi bütünlüğü veya bilgi doğrulaması (integrity):** Bütünlük, bilginin varlığının ve akışının doğru, kesin ve eksiksiz olduğunun güvence altına alınması ile sağlanır. Bu amaç doğrultusunda;
    - Bilginin, yetkisi olmayan kişiler tarafından değiştirilmesi önlenir.
    - Bilginin, yetkili kişiler tarafından istem dışı değiştirilmesi önlenir.
    - Bilginin, tutarlılığının korunması sağlanır.
- **Hizmet sürekliliği (availability):** Bilgilerin bir sistem veya ağ üzerinden, yetkili kullanıcılar tarafından istenildiği vakitte ve kesintisiz erişiminin sağlanmasıdır.

3.4. YAZILIM GÜVENLİĞİ

Ekonomi, devlet ve sosyal yaşam gün geçtikçe daha fazla internet üzerine taşındıkça, yazılım güvenliği çok daha önemli hale gelmektedir. Bilgi güvenliğinde olduğu gibi bir yazılımın güvenli olabilmesi için, gizlilik, bütünlük ve süreklilik temel ilkelerini sağlaması gerekmektedir.

Yazılım ürünü özelliklerinden en önemli üç tanesi kalite, maliyet ve zamandır. Maliyet ve zaman için rakamsal ölçülebilirlik olduğu halde, kalite için bu çok zordur. Yazılım kalitesi kavramı içerisindeki en önemli özelliklerden biri güvenilirlik olup, programlardaki en büyük maliyet kaynağı olan hataların oranından etkilenir. Bu nedenle güvenilirlik, belirli bir ortam ve sınırlı zaman dilimi içinde, yazılımın hatasız olarak çalışma olasılığı olarak tanımlanır. [Eren Ş., 54]

Güvenlik açıklarının hemen hemen tamamı yazılımların güvenli mimari ve kodlama teknikleri kullanılmadan yazılmasından kaynaklanmaktadır. Bu nedenle yazılım geliştirme sürecinin nasıl işlediği bu noktada çok önem taşımaktadır. [55] Web Uygulamaları Güvenlik Platformu (Open Web Application Security Project: OWASP) tarafından açıklanmış olan güvenlik açıklarında ilk 10 sıralaması şöyle oluşmaktadır:

1. Teyit edilmemiş girdi (Unvalidated Input):

Web uygulamalarında, kullanıcıdan alınan verinin kontrol edilmeden işleme sokulmasından doğan güvenlik açığıdır.

2. Kırılmış erişim kontrolü (Broken Access Control):

Yetkilendirilmiş kullanıcıların sistemde neler yapabileceğinin uygun şekilde belirtilmediği durumlardır. Bu durum başka kullanıcıların haklarını kullanma ve yetkisiz olduğu halde verilere erişebilme gibi sakıncalar doğurmaktadır.

3. Kırılmış yetkilendirme ve oturum yönetimi (Broken Authentication and Session Management):

Kullanıcı hesabının bulguları ve izlerinin korunmamış olduğu durumlardır. Saldırganın şifreleri, anahtarları ve oturum çerezlerini ele geçirerek yetki sınırlarını aşabilmesi ve diğer kullanıcı kimliklerine sahip olabilmesidir.

4. Çapraz site betikleri (Cross Site Scripting - XSS):

Saldırganların kişisel bilgilere ulaşabilmek amacıyla kullandığı gelişmiş yöntemlerden biridir. Bir web uygulamasının içine JavaScript, VBScript, ActiveX, HTML veya Flash kodları yerleştirme becerisidir. Web tabanlı e-posta istemcisinden çevrimiçi (on-line) forumlara veya alışveriş site uygulamalarına kadar birçok web uygulamasında kullanılabilir. [Hendrickx M., 56] Sonrasında banka hesabına girme, kullanıcı ayarlarını değiştirme, cookie hırsızlığı yada spam gönderme mümkün olmaktadır. Çevirim içi alış veriş sitesi Amazon.com, internet üzerinden ödeme yapmak için kullanılan PayPal veya bankaların internet üzerinden işlem yapılan siteleri gibi güvenlik açığı olma ihtimali düşük olarak görülen siteler bu yöntemle gerçekleştirilen saldırıların en yeni hedefleri olarak gözükmektedir. Kullanıcıların bu yöntemle yapılan saldırılardan, sadece erişmek istediği sitenin ana sayfasındaki linkleri takip ederek görmek istediği bilgilere ulaşmaları korunmalarının en kolay yolu olarak gözükmektedir. [Endler D., 57]

5. Tampon taşması (Buffer Overflow):

Tampon (buffer), hafızada ard arda dizili türdeş veri tipi (int, char gibi) depolayan hafıza bloğudur. Bu blok C programlama dilinde array olarak tanımlanmaktadır. Diğer bütün veri türleri gibi, array`ler de statik yada dinamik olarak sınıflandırılabilirler.

Statik değişkenler, program hafızaya yüklenirken, programın data segment`ine yerleştirilir, dinamik değişkenler ise, program hâlihazırda çalışırken, dinamik olarak 'stack' dediğimiz hafızada program için hazırlanmış özel bolümde yaratılıp, yok edilirler. İşte tampon taşması da, bu dinamik değişkenlerin taşıyabilecekleri veri miktarından fazlasını yükleyerek değişkenin sınırlarını aşmadır. Kaba bir tabirle, 10 byte veri taşıyabilecek bir array`a 20 byte kopyalamak bu tampon belleği taşırmak demektir. [Balaban M., 58]

Burada temel amaç sistem üzerinde bir açık kapı oluşturarak sisteme sızmaktır. İşletim sistemi gönderilen normal veriyi ara bellekte yer kalmadığı için bir kod gibi işlediği anda artık sistem savunmasız hale gelmiştir.

6. Araya yerleştirme açıkları (Injection flaws):

Saldırgan tarafından bu açıklar kullanılarak zararlı kodlar, uygulama aracılığıyla sistem sınırlarını geçer ve buraya başka bir sistemin bileşenlerini yerleştirir. Sistem sınırlarını hileyle geçebilmek mümkündür çünkü bir PHP uygulaması için zararsız bir kod satırı veritabanına ulaştığında çok tehlikeli bir silaha dönüşebilir. [Ristick I., 59]
Bu tip açıklara aşağıdakiler örnek olarak verilebilir:

- Pencere yerleştirme açığı (window injection flaw): [60]

Burada saldırganlar web tarayıcılarının açıklarından faydalanırlar. Kötü amaçlı bir site (genelde bedava mp3, yazılım vaat eden veya pornografik içerikli siteler) güvenilir bir sitenin üzerine, içeriğine zararlı kodlar yerleştirilmiş bir açılır pencere (pop-up) yerleştirir. Böylece saldırganlar tarayıcı sayfalarını ele geçirebilmekte ve o güvenilir web sitesinin içeriğini değiştirebilmektedir.

- SQL kodu yerleştirme (SQL injection):

Neredeyse bütün web uygulamaları bazı bilgilerin saklanabilmesi ve gerektiğinde çağırılabilmesi için veritabanlarını kullanmaktadır. Uygulama geliştiricileri, uygulamalarda SQL sorgularını oluşturmak amacıyla basit bir şekilde kelime dizilerini birbirlerine bağlarlar ve bazı durumlarda kullanıcılardan gelen verileri beklenen veri türü ile karşılaştırmayarak SQL sorguları içinde kullanmaktadırlar. Genel olarak problemler, uygulama geliştiricinin SQL sorgularında anlam ifade edebilecek “‘”, “;”, UNION” gibi kötü niyetli karakterlere karşı bir önlem almadığı zaman ortaya

çıkmaktadır. Bu durum kullanıcıya önceden planlanmamış, uygulama düzeyinde erişim sağlayabilir. SQL araya yerleştirme ile saldırgan tablo yaratabilir, değişiklikler yapabilir, veritabanı üzerinde erişim sağlayabilir veya veritabanı kullanıcısının hakları doğrultusunda sunucuda komut çalıştırabilir. [61]

Kullanıcıların bilgi gönderebileceği kullanıcı girişi, arama sayfası, yorum sayfası gibi sayfalar bu tip bir saldırı için uygundur. Genelde html sayfaları kullanıcı girdilerini gönderirken POST metodunu kullanırlar böylece sayfanın adresinde parametreler görülemez. Bu durumda sayfanın kaynak kodu incelenerek hangi parametreleri gönderdiği bulunabilir. Örnek olarak:

< form method="post" action="Search/search.asp">
< input type="hidden" name="A" value="C" />
< form>

form etiketleri arasındaki her şey potansiyel parametrelerdir. [62]

Kullanıcı girdi olarak "kullanıcı adı" ve "parola" girdiğinde veritabanında ilgili tablodan verilerin doğruluğu kontrol edilir. Örneğin; kullanıcı adı: hakan parola: aysal olsun. Bu girdinin SQL karşılığı,
SELECT count(*) FROM Users WHERE Kullanıcı adı = 'hakan' AND Parola = 'aysal'
şeklinde olur. Eğer saldırgan girdi olarak;
Kullanıcı adı: hakan, Parola: ' OR 1=1-- girer ise SQL karşılığı,

SELECT count(*) FROM Users WHERE Kullanıcı adı = 'hakan' AND Parola = '' OR 1=1 --'

olacaktır, bu durumda girişin sağlanması için şart "hakan" kullanıcı adına ait parolanın boş olması veya ikinci bir seçenek olarak 1=1 eşitliğinin sağlanmasıdır. Sonuçta 1=1 eşitliği sağlandığına göre saldırı başarıyla sonuçlanacak ve "Başarılı şekilde giriş yapıldı" mesajı alınacaktır.

Potansiyel SQL araya yerleştirme taşıyıcılarını keşfetmede aşağıdaki metotlar kullanılabilir:

Geçersiz karakterlerin denenmesi: Veritabanına bağlantı kuran her uygulamada her veri giriş alanı için “ ‘, “”, %, _, ||, +, ; “ gibi geçersiz karakterlere sahip girişleri denemek gerekir. Veritabanından alınan herhangi bir hata mesajı potansiyel bir SQL araya yerleştirme taşıyıcısının varlığını gösterir.

Kodların gözden geçirilmesi: Uygulama geliştiriciler ve kalite kontrol personeli potansiyel SQL araya yerleştirme taşıyıcılarına karşı veritabanı içerisindeki kodları tekrar gözden geçirmelidirler. SQL ifadelerinin dinamik olarak yaratıldığı alanlara özellikle dikkat edilmelidir. [Kevin Lam K., LeBlanc D., 63]

7. Uygun olmayan hata yönetimi (Improper Error Handling):

Hataların yanlış ele alınması bir web sitesinin güvenlik problemlerinden biridir. En yaygın sorun yığın taramaları, veritabanı çökmeleri ve hata kodları gibi ayrıntılı sistem hata mesajlarının saldırgan tarafından görüntülenmesi ile oluşur. Bu mesajlar asla açığa çıkmaması gereken, uygulamanın işleyişi ile ilgili ayrıntılar içerir. Bu gibi ayrıntılar saldırganlara sistemin potansiyel açıkları hakkında önemli ipuçları sağlar. [64]

8. Güvensiz ortamlarda saklama (Insecure Storage):

Birçok web uygulaması hassas bilgileri bir veritabanında veya dosya sisteminde depolamak zorundadır. Bu bilgiler şifreler, kredi kartı numaraları, hesap kayıtları olabilir. Kriptolama teknikleri genelde bu hassas bilgileri koruyabilmektedir. Kriptolamanın uygulanmasının ve kullanımının nispeten kolay olduğu durumlarda, yazılım geliştiricileri bu kriptolama işlemlerini web uygulamalarında kullanırken hata yapmakta, bu kriptolama tekniklerinin kullanılması ile kazanılan korunmayı küçümsemektedirler.

9. Hizmet Durdurma (Denial of Service):

Servis performans veya kısıtlamalar yönünden sistemi zorlayıp, sistemin doğru hizmet vermesini engellemektir. Bu konu, 4.2.3. Bölümde ayrıntılı olarak incelenecektir.

10. Güvensiz Yapılandırma Yönetimi (Insecure Configuration Management):

Web sunucuları ve uygulama sunucularının konfigürasyonları, bir web uygulamasının güvenliğinde anahtar rol oynar. Bu sunucular, içeriğin sunulması ve bu içeriklerin çağırdığı uygulamaların çalıştırılmasından sorumludurlar. Birçok uygulama sunucusu, web uygulamalarının kullandığı veri depolama, dizin hizmetleri, posta, mesajlaşma gibi çok sayıda hizmeti verebilmektedirler. Web hazırlama grubu ile siteyi işleten sistem grubu genelde farklıdır ve aralarında geniş bir boşluk vardır. Web uygulamalarının güvenliğinin sağlanması ile projenin iki taraf üyeleri arasında bir köprü oluşur.

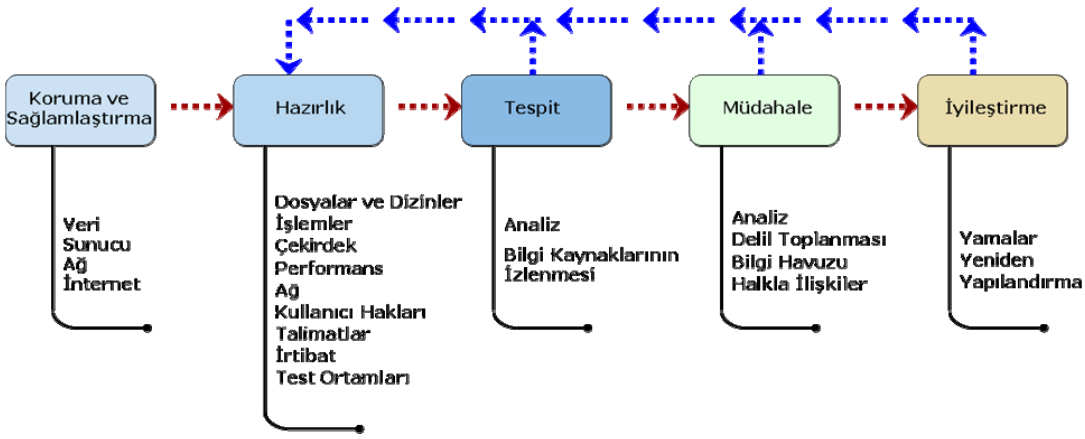
Sunucu güvenliğini tehdit eden yapılandırma problemlerine;

- Sunucu yazılımında yamanmamış güvenlik açıkları,
- Dizin listelendirmesi ve saldırılarına izin veren sunucu yazılım açıkları veya hatalı yapılandırmaları,
- Gereksiz betikler, uygulamalar, yapılandırma dosyaları ve web sayfalarının varsayılan, yedek veya örnek dosyaları,
- Hatalı dosya ve dizin izinleri,
- Uzaktan idare ve içerik yönetimi de dahil gereksiz servislerin açık bırakılması,
- Varsayılan hesapların varsayılan şifreleri ile bırakılması,
- Yönetimsel veya hata ayıklama fonksiyonlarının açık ya da erişilebilir bırakılması,
- Aşırı derecede bilgi veren hata mesajları,
- Hatalı yapılandırılmış SSL sertifikaları ve şifreleme ayarları,
- Kimlik denetimi için kendinden imzalı sertifikaların kullanılması ve ortadaki, adam koruması,
- Varsayılan sertifikaların kullanılması,
- Dış sistemlerle uygun olmayan yetki paylaşımı, örnek olarak gösterilebilir. [65]

3.5. AĞ GÜVENLİĞİ

Ağ güvenliği, ağ üzerinde dolaşan paketlerin duruma göre gizliliğini, bütünlüğünün korunmasını, dinlenen ve kaydedilen paketlerin tekrarının önlenmesini ve gönderen ile alıcının kimliklerinden tarafların emin olması demektir. [Levi A., 66]

Tehditler sürekli olarak yenilenmekte ve çeşitlilik kazanmaktadır. Kullanılan altyapılar, sık aralıklarla güncelleme, iyileştirme, genişleme ve benzeri çalışmalar sonucu değişikliklere uğramaktadırlar. Bunların yanına, yazılım sistemlerindeki sürekli değişimlerde eklenince herhangi bir anda güvenli kabul edilebilecek bir sistemin, bir sonraki kontrol arasında geçen sürede güvenli kalması garanti edilemez. Bu nedenle, güvenlik çalışmaları bir yaşam döngüsü ile modellenmektedir. (Şekil 3.5.1.)



Şekil 3.5.1 : CERT/CC Güvenlik Yaşam Döngüsü

Ağ güvenliği, güvenlik politikalarını temel alan yaşayan bir süreçtir. Kurum hedeflerinin ve kurumsal güvenlik politikasının belirlenmesinden sonra Uluslar Arası Bilgisayar Acil Durum Müdahale Ekipleri Koordinasyon Merkezi (Computer Emergency Response Teams Coordination Center - CERT/CC), tarafından önerilen güvenlik uygulamaları döngüsü ve bu çerçevede sunulan çözüm bileşenlerinin uygun bir biçimde bir araya getirilmesi, yol gösterici bir referans olacaktır.

CERT/CC, ağları ve sistemleri korumak için gerçekleştirilmesi gereken faaliyetleri beş ana başlık altında toplamıştır: [Allen J., 67]

1. Koruma ve sağlamlaştırma,

2. Hazırlık,
3. Tespit,
4. Müdahale,
5. İyileştirme, şeklinde bu adımlar sıralanabilir.

CERT/CC tarafından öngörülen bu beş adımlık güvenlik uygulaması firma, ürün ya da teknolojiden bağımsız olarak düzenlenmiştir. Tüm adımlarda, kurumun güvenlik ihtiyaçları için zemin oluşturacak kurumsal hedeflerinin ve kurumsal güvenlik programı ve politikasının önceden oluşturulmuş olduğu varsayılır.

3.5.1. Koruma ve Sağlamlaştırma

Satın aldığımız sistemler ilk bakışta çok kullanışlı ve her şeyin yerli yerine oturduğu bir ürün gibi görünseler de güvenlik açısından ele aldığımızda birçok zayıflık ve zafiyet (vulnerability) içerdiklerini görürüz. [68, 69] Üreticiler, ürünlerinin kuruluma ve kullanıma hazır olarak sunulduğundan ve her türden kullanıcıya hitap ettiğinden o kadar emindirler ki, genelde o ürüne ait servisler hâlihazırda (default) açık olarak gelir. Örneğin; dizüstü bilgisayarının kablosuz iletişim (wireless) olanağından faydalanmak için ofise, evde kullandığı kablosuz ADSL modemini kuran bir kullanıcı düşünelim. Kablosuz ADSL modemler, hâlihazırda üzerlerinde DHCP (havuzdan otomatik IP dağıtma hizmeti) hizmeti açık olarak gelirler. Bu modem kurumun yerel ağına bağlandığında sahip olduğu DHCP hizmetini tüm yerel ağ için vermek isteyecektir. Eğer bu konuda ağ üzerinde bir önlem alınmamışsa, modemin bağlı olduğu ağın o bölümü çalışmaz hale gelecektir. Bu da ağ güvenliğinden sorumlu kişilerin, sorunun ne olduğunu ve kaynağını tespit edebilmeleri için fazladan zaman harcamaları ve bu süre içerisinde kullanıcıların mağdur olması anlamına gelmesi demektir. Bu nedenle, ister kurumun en yetkili yöneticisi olsun ister sıradan bir kullanıcı olsun, sorumlu olduğu sistemin konfigürasyonunun, kurumun güvenlik gereklerine ve politikasına uyduğundan emin olması gerekmektedir. İhtiyaç duyulduğunda, sistemi bu doğrultuda yeniden yapılandırmalıdır.

Bu adım, bilinen saldırı ve tehditlere karşı güvenliği sağlanmış ve sağlamlaştırılmış bir sistem konfigürasyonu ve ağ yapısı oluşturmak adına atılacak adımları içerir:

- Sadece en düşük gereksinimlere cevap verecek şekilde işletim sistemleri kurulmalıdır. Bunlar sadece sistemin çalışabilmesi için gereken dosyalar ve dizinleri içeren paketlerdir.
- Bilinen eksiklikler ve güvenlik açıklarına karşı yamalar yüklenmelidir. Örneğin; Windows XP işletim sistemini yükledikten hemen sonra, Service Pack 2 paketi yüklenmeli ve ardından bütün yamalar için işletim sistemi güncellenmelidir.
- Yazılımların en güncel ve güvenli hale getirilmiş sürümleri yüklenmelidir. Her yeni sürümde, bir eksiklik veya açığın giderilmiş olabileceği unutulmamalıdır.
- Kurulumdan hemen sonra, yazılım tarafından hazır gelen tüm imtiyazlar ve erişim hakları kaldırılmalıdır. Sadece ihtiyaç duyulan miktarda erişim hakkı tanımlanmalıdır. Örneğin; Windows Xp işletim sistemi kurulduktan sonra, Administrator ve Guest kullanıcı adları ve hakları kaldırılmalı, kullanıcı ihtiyaçları doğrultusunda yeni kullanıcı adları ve hakları tanımlanmalıdır.
- Sistem hakkında ayrıntılı bilgilere ulaşabilmek için sistemin log'ları tutulmalıdır.

Diğer tüm adımlar bu adımın sonucunda ulaşılan düzeye göre geliştirileceğinden bu adımın etkin bir biçimde planlanması ve gerçekleştirilmesi son derece önemlidir.

3.5.2. Hazırlık

Hazırlık aşaması, koruma ve sağlamlaştırma aşamasında atılan adımlara rağmen hala belirlenememiş, mevcut olan güvenlik zafiyetlerini tespit edip, tanıma amacını taşımaktadır. Bu süreç, sistem yöneticisinin sorumlusu olduğu sistemi, tüm altyapısı, ayarları ve özellikleriyle tanıyarak nasıl çalıştığını anlayabilmesidir. Koruma ve sağlamlaştırma adımı ile hazırlığın tanıma aşaması arasındaki ayrım, sağlamlaştırma çalışmalarıyla, bilinen çözüm yollarını uygulayarak bilinen problemleri çözmektir. Tanıyarak hazırlanma aşaması ise oluşabilecek yeni problemleri fark edebilmek ve bunlara karşı yeni çözümler ortaya koymak için yardımcı olur.

3.5.3. Tespit

Bu adım, güvenlik duvarı veya bir web sunucudan elde edilen log'lar gibi kaynakların izlenmesi sürecidir. Bu süreçte, olağan dışı, beklenmeyen veya şüpheli bir faaliyetlere karşı tetikte olunur, kaynakların özellikleri hakkında yeni şeyler öğrenilir veya harici bir

kaynaktan bilgiler edinilir. Bu harici kaynaklar; bir kullanıcı raporu, diğer bir kurumdan gönderilmiş bir e-posta, bir güvenlik uyarısı veya bir güvenlik bülteni olabilir. Buralardan elde edilen veriler bazı şeylerin daha fazla analiz edilmesi gerektiğinin, sistemde bir şeylerin değiştiğinin veya yeni bir yamanın uygulanmasına gerek olduğunun birer göstergesidir. Bu beklenmeyen veya şüpheli faaliyetlerin incelenmesi sonucunda belki de sisteme yetkisiz bir erişimin olduğu ortaya çıkarılabilir.

3.5.4. Müdahale

Bu adımda, sisteme yetkisiz bir erişim veya bir güvenlik ihlali (intrusion) gerçekleştiğinde oluşan zararın tespiti, zararın kapsamı ve diğer sistemlere etkisi en kısa sürede belirlenir. Mümkün olduğunca bu etkiler bertaraf edilmeye çalışılır, gelecekte tekrar edilmesinin önüne geçilir ve sistemler eski çalışır hallerine geri döndürülür. Daha sonra bu izinsiz girişin veya saldırının delileri toplanır ve gerektiğinde saldırganlar aleyhine hukuki girişimlerin başlatılmasında kullanılır. Saldırıya hızla müdahale edebilmeye olanak sağlayacak mekanizmaları kurmak, eğitimli teknik uzmanlar yetiştirmek ve olay müdahalesi (incident response) ile ilgili politika ve talimatnameleri işletmek de bu adım kapsamında ele alınır.

3.5.5. İyileştirme

İyileştirmeye yönelik faaliyetler, genelde saldırıların tespiti ve müdahale çalışmalarını takiben gerçekleştirilir. Benzer türde saldırıların muhtemel etkisini azaltmak ve mümkün ise bu tür saldırıların gerçekleşmesini önlemek üzere ağ ve sistem güvenliğini arttırıcı önlemlerin alınması bu adım kapsamında ele alınır. Güvenlik ile ilgili politikalar ve talimatnameler gözden geçirilmeli ve güncellenmelidir. Önceki adımlarda elde edilen verileri, güvenlik çözümlerini güçlendirmek için kullanmak gerekmektedir. Müdahale sonrasında alınan önlemlerin genele yaygınlaştırılmasını sağlamak yapılabilecek bir çalışma da bu adım bağlamında değerlendirilir. [Dayıoğlu B., 70]

İyileştirme faaliyetleri, koruma ve sağlamlaştırma, hazırlık ve tespit adımlarının tekrardan gözden geçirilmesini sağlar. Bu adımların tekrarlı bir biçimde gerçekleştirilmesi sayesinde, sürekli olarak potansiyel sorunlar tespit edilebilir ve zamanında önlem alınarak sistem güvenliği azami seviyede korunmaya çalışılır.

4. NEDEN AĞ GÜVENLİĞİNE İHTİYAÇ VAR?

Güvenliğin tek bir amacı vardır o da kurumun değerlerini, varlıklarını korumaktır. Tarihte güçlü ve yüksek duvarlar inşa ederek düşmanları durdurmak, küçük ve iyi korunmuş kapılar ile de halkın güvenli bir şekilde giriş çıkışını sağlamak, güvenlik için dönemin şartları göz önünde bulundurulduğunda yeterliydi. Bu taktik, buzdolabı büyüklüğünde mainframe bilgisayarlar, binanın bir katını kaplayabilecek büyüklükte ve sıkı korunan sistem odaları ve kapalı ağların olduğu yakın geçmişte de oldukça işe yaramıştı. Ağların dış dünya ile bağlantısının olmaması güvenlik için yeterlidir düşüncesi hakimdi. Kişisel bilgisayarların, yerel ağların ve tüm dünyayı saran internetin gelişmesiyle ağlar günümüzde daha açık hale gelmiştir.

Tablo 4.1 : İnternet kullanımı ve nüfusa oranı

Ülke	**Nüfus (2006 yılı tahmini)**	**İnternet Kullanıcı Adedi**	**Nüfusa Oranı**	**Kullanım Oranı**	**Büyüme (2000-2006)**
Türkiye	74,709,412	16,000,000	21,4 %	64 % **(1)**	700 %
Avrupa	807,289,020	308,712,903	38,2 %	28,4 % **(2)**	193,7 %
Dünya	6,499,697,060	1,086,250,903	16,7 %	100 %	200,9 %

(1) A.B. Aday ülkeleri toplamı %100 olarak kabul edildiğinde

(2) Dünya ülkeleri toplamı %100 olarak kabul edildiğinde

Tablo 4.1. Dünya internet kullanıcıları ve nüfus istatistiklerinin tutulduğu "Internet Usage Statistics - The Big Picture" web sitesindeki verilerden derlenerek oluşturulmuştur. [71]

Tablo 4.2 : Cinsiyete göre Türkiye, kent-kır ayrımında bilgisayar ve İnternet kullanım oranları (%)

		Bilgisayar kullanım oranı			İnternet Kullanım oranı		
		Toplam	**Kadın**	**Erkek**	**Toplam**	**Kadın**	**Erkek**
Son üç ay içinde (Nisan-Haziran 2005)	Türkiye	17,65	5,77	11,88	13,93	4,33	9,60
	Kent	23,16	7,92	15,24	18,57	6,06	12,51
	Kır	8,28	2,12	6,16	6,05	1,39	4,66
Üç ay - bir yıl önce	Türkiye	1,88	0,71	1,17	1,52	0,54	0,99
	Kent	2,44	0,95	1,49	1,96	0,72	1,24
	Kır	0,92	0,29	0,63	0,78	0,22	0,56
Bir yıldan çok oldu	Türkiye	3,42	1,53	1,89	2,10	0,74	1,36
	Kent	3,98	1,83	2,16	2,54	0,92	1,61
	Kır	2,45	1,03	1,42	1,36	0,43	0,92
Hiç kullanmadı	Türkiye	77,06	42,28	34,78	82,45	44,68	37,76
	Kent	70,41	38,65	31,77	76,94	41,65	35,29
	Kır	88,35	48,45	39,90	91,81	49,84	41,97

Türkiye İstatistik Kurumu tarafından 2005 yılı Haziran ayında gerçekleştirilen "Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması" sonuçlarından, cinsiyete göre Türkiye, kent-kır ayrımında bilgisayar ve internet kullanım oranları yüzde olarak Tablo 4.2. de verilmiştir. [72] İlk tabloda % 700 ile Türkiye'nin internet ve bilgisayar kullanımının artışının son yıllarda ne kadar yüksek olduğu görülmektedir. Fakat ikinci tablo ise daha kat edilecek çok yol olduğuna dair iyi bir göstergedir.

E-ticaret ve internet uygulamalarının artmaya devam etmesi, iyiler ile kötülerin ayırt edilebilme kabiliyeti de düşünülerek, izole olmakla açık olmak arasındaki dengeyi bulmanın önemini de artmıştır. Mobil ticaret ve kablosuz ağlar, eski model kale duvarı güvenlik anlayışını parçalamış, kendi içinde bir bütünlüğe sahip, daha şeffaf ve daha esnek güvenlik çözümlerinin gerektiğini ortaya çıkarmıştır.

Saldırganlar bu yeni ve karmaşık ağların ve üzerinde çalışan karmaşık servislerin açıklarını avantaj olarak kullanmakta ve bu ortamda bulunan yönlendiriciler, anahtarlar, sunucular, istemciler, ağlar, uygulamalar, işletim sistemleri, güvenlik cihazları, uzak kullanıcılar da dahil olmak üzere neredeyse her şey hedef olabilmektedir.

Günümüz ağlarına yönelen bu tehditler, klasik güvenlik üreticileri ve çözümleri tarafından engellenemez hale gelmeye başlamış ve bütün bu hedefleri tek bir güvenlik cihazı, yazılımı veya çözümü ile korumak ise neredeyse imkânsız hale gelmiştir.

4.1. TEHDİTLER

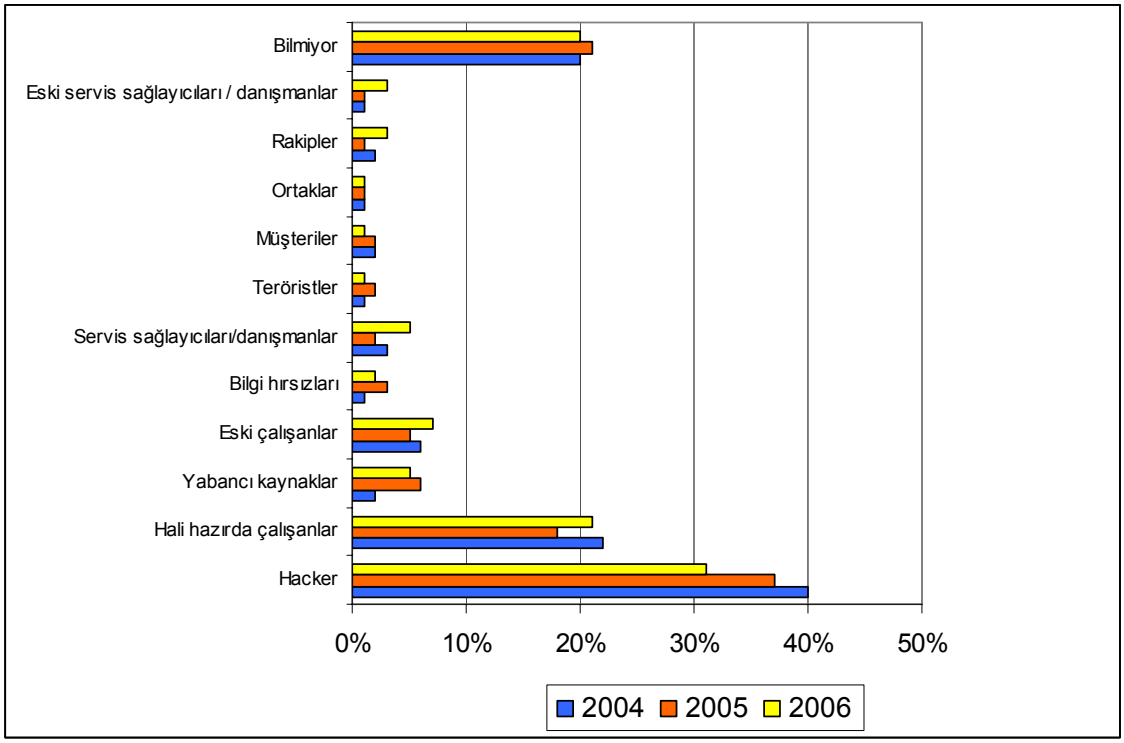
Sun Tzu usta Art of War isimli eserinde [73] "Eğer düşmanınızı ve kendinizi tanırsanız, yüzlerce savaşın sonucundan korkmanıza gerek yoktur. Eğer kendinizi tanır düşmanınızı tanımazsanız, kazanılan her zaferde ayrıca mağlubiyetin de ıstırabını çekersiniz. Eğer ne kendinizi ne de düşmanınızı tanırsanız, her savaşta mağlup olursunuz. (*If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.*)" demiştir.

Bu özlü sözün ışığında bilgisayarımızı, sistemimizi, ağımızı, kurumumuzu ve çevremizi tehditlerden etkin bir biçimde koruyabilme mücadelemizde başarılı olmak için, var olan tehditleri iyi anlamamız, tanımamız ve ona göre davranmamız gerekir.

Tehdit, bir bilgi sistemleri ortamının güvenliğini ihlal edebilecek eylem veya olay olarak tanımlanabilir. Tehdidin üç bileşeni vardır: [Maiwald E., 74]

- Hedefler (target); saldırıya maruz kalabilecek güvenlik durumudur.
- Aracılar (agent); tehdidi oluşturan kişi veya kurumlardır.
- Olaylar (event); tehdidi ortaya çıkaran eylem şeklidir.

Tablo 4.1.1 : CERT/CC Tehdit gruplarını belirleme anketi sonuçları



A.B.D. Gizli Servisi, Carnegie Mellon Yazılım Mühendisliği Enstitüsü CERT Koordinasyon Merkezi ve CSO Dergisi işbirliğiyle elektronik suçla savaş eğilimleri, teknikleri ve en iyi uygulamaları ortaya çıkarmak amacıyla her yıl e-suç takip araştırması yapılmaktadır. Bu araştırmalardan bilişim güvenliği konusunda son bir yıl içerisinde en büyük tehdidi en fazla hangi grubun oluşturduğuna dair sorunun 2004, 2005, 2006 yıllarında alınmış cevaplarına ait bir istatiksel dağılım Tablo 4.1.1. de görülmektedir. [CERT/CC, 75] Tabloya göre en büyük tehdidi saldırganlar (hacker) oluşturmaktadır.

Tehditler, tehdit kaynağı açısından bakıldığında insan kaynaklı ve doğa kaynaklı olmak üzere iki grupta incelenebilir.

4.1.1. İnsan Kaynaklı Tehditler

Bu tür tehditleri de kendi içinde iki alt gruba ayırabiliriz:

a) **Kötü niyetli olmayan davranışlar sonucu oluşanlar:** Bir kullanıcının, sistemi yeterli eğitime sahip olmadan, bilinçsiz ve bilgisizce kullanması sonucu sistemde ortaya çıkma olasılığı olan aksaklıklardır.

- Kullanıcıların kendilerine ait diz üstü veya cep bilgisayarlarını hiçbir önlem almadan kurumun internet ağına bağlamaları,
- Taşınabilir bellekler vasıtasıyla kişisel bilgilerini herhangi bir virüs taraması yapmadan kurumun bilgisayarlarına takmaları,
- Temizlik görevlisinin sunucunun fişini çekmesi veya sigortaları indirmesi,
- Konu ile ilgili yeterli eğitim almamış bir çalışanın veritabanını silmesi,

bilgisiz ve bilinçsiz kullanıma örnek gösterilebilir.

b) **Kötü niyetli davranışlar sonucu oluşanlar:** Sisteme zarar verme amacıyla, sisteme yönelik olarak yapılacak tüm kötü niyetli davranışlardır. Bu tür tehditlerde, tehdit kaynağı, sistemde bulunan güvenlik boşluklarından yararlanır.

4.1.2. Doğa Kaynaklı Tehditler

Bu tür tehditler genellikle önceden tespit edilemezler ve büyük bir olasılıkla olmaları engellenemez. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi ve yıldırım düşmesi bu tür tehditlere örnek olarak verilebilir.

Ayrıca tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre;

4.1.3. İç tehditler

İç tehditler, kurum içinden kuruma yönelik yapılabilecek saldırılar olarak tanımlanır. Ayrıca iç tehditler terimi, işinden kötü şekilde ayrılan, daha fazlasını hak ettiğini ve kendisine haksızlık yapıldığını düşünen ve çalıştığı kuruma zarar vermek için çeşitli faaliyetlerde bulunan kurum çalışanları için kullanılan bir terimdir. [76] Bu çalışanlar, sistemlere ait bilgileri başkalarına verebilmekte, uzaktan bağlantı sağlayarak, özellikle yüksek seviyede yetkilere sahip oldukları sistemleri sabote edebilmektedirler. Kendi bilgisayarlarına kurdukları paket dinleyiciler (sniffer), Truva atları veya klavye hareketlerini kaydedebilen (keylogger) yazılımlar sayesinde kurum çalışanlarının, dolayısıyla kuruma ait gizli bilgileri, yazışmaları elde edebilmektedirler. Ayrıca her türlü önlemin dışarıdan gelebilecek saldırılara karşı alındığı bir ortamda içeriden birisi kolaylıkla önemli sistemlere erişebilir kritik bilgileri silip değiştirebilir.

4.1.4. Dış tehditler

Kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanabilir. Dış tehditler, yapısal (structured) tehditler ve yapısal olmayan (unstructured) tehditler olarak iki başlıkta incelenebilir. [Bastien G. ve Degu Christian A., 77]

4.1.4.1. Yapısal Tehditler

Yapısal tehditler, belirli bir hedefin güvenliğini aşmak için bir plan dahilinde ve bir düzen içerisinde yürütülen faaliyetlerdir. Kendi içerisinde bir düzene sahip olmasından dolayı en tehlikeli tehdit sınıfıdır. Bir kişi veya grup tarafından, belirlenmiş bir hedefe daha önceden planlanmış bir saldırı düzenlemesi, bu tehditler kapsamındadır. Bir saldırganın dışarıdan kurum web veya posta sunucusunu ele geçirerek ona ait veritabanı kayıtlarını silmesi, değiştirmesi veya birçok saldırganın kurum internet çıkış yönlendiricisine, web veya mail sunucusuna hizmet durdurma saldırısı yapması, bu tehdit sınıfına örnek olarak gösterilebilir.

4.1.4.2. Yapısal olmayan tehditler

Yapısal olmayan tehditler, en yaygın olan tehditlerdir. Yapısal olmayan tehditler, belirli bir sistem, ağ veya kurumu hedef almayan, hedefin ele geçirilmesi hususunda fırsat yaratabilmek amacıyla internet üzerinden çeşitli araçlar vasıtasıyla yürütülen faaliyetler sonucu oluşur.

- Virüs saldırıları (Melissa, CIH – Çernobil, Vote),
- Solucan saldırıları (Code Red, Nimda, Blaster,Sasser),
- Truva atları veya arka kapılar (Netbus, Subseven, Black Orifice), yapısal olmayan tehditlere örnek olarak gösterilebilir.

4.2. TEMEL SALDIRI ŞEKİLLERİ

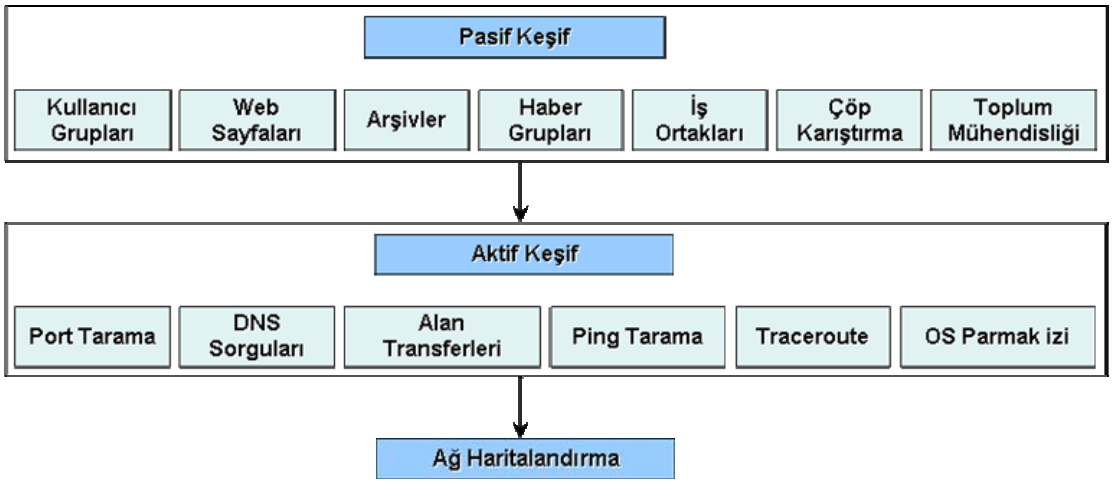
4.2.1. Keşif (Reconnaissance)

Keşif; sistemin, servislerin ya da güvenlik boşluklarının, yetkisiz bir şekilde taranması ve haritalandırılması şeklinde olur. Bu keşif faaliyetleri bir saldırı şekli olmaktan çok, arkasından yapılacak saldırılar için, saldırganın hedef hakkında bilgi toplamasıdır. Saldırı öncesi hazırlık safhasının yedi adımı Tablo 4.2.1.1. de görülmektedir. [Gregg M., 78]

Tablo 4.2.1.1 : Saldırı öncesi hazırlık safhasının yedi adımı

Adım	Başlık	Aktif/Pasif	En çok kullanılan araçlar
Bir	Bilgi toplama	Pasif	Sam Spade, ARIN, IANA, Whois, Nslookup
İki	Ağın büyüklüğünün tesbiti	Pasif	RIPE, APNIC, ARIN
Üç	Çalışan makinelerin tanımlanması	Aktif	Ping, traceroute, Superscan, Angry IP scanner
Dört	Açık port ve uygulamaların bulunması	Aktif	Nmap, Amap, SuperScan
Beş	İşletim sistemi parmak izinin alınması	Aktif / Pasif	Nmap, Winfigerprint, P0f, Xprobe2, ettercap
Altı	Parmak izi alma servisleri	Aktif	Telnet, FTP, Netcat
Yedi	Ağın haritalanması	Aktif	Cheops, traceroute, NeoTrace

Kullanılan materyallere göre keşif saldırısını, Şekil 4.2.1.1 den de görülebileceği üzere pasif ve aktif olmak üzere ikiye ayırabiliriz. [Whitaker A. ve Newman Daniel P., 79]



Şekil 4.2.1.1 : Pasif ve aktif keşif

Pasif keşif

Pasif keşif; kullanıcı grupları, web sayfaları, haber grupları, iş ortakları, çöp karıştırıcılık ve toplum mühendisliği teknikleri ile haber ve bilgi toplama şeklidir.

Aktif keşif

1. **DNS sorguları:**

- **nslookup**: DNS (Domain Name Service) işleminde normalde bilgiler bir DNS sunucusundan diğerine alan transferi şeklinde yapılır. Eğer etki alanında birden

fazla isim sunucusu varsa sunuculardan biri birincil (primary) olur. En basit DNS Sorguları nslookup komutu ile yapılabilir.

C:\>nslookup www.google.com
Server: dnsr1.sbcglobal.net
Address: 68.94.156.1
Non-authoritative answer:
Name: www.l.google.com
Addresses: 64.233.187.99, 64.233.187.104
Aliases: www.google.com,

- **dig**: DNS Sunucular üzerinde değişik türde sorgulamalar sağlayan ve aynı zamanda sistem yöneticileri tarafından DNS problemlerini belirlemek için kullanılan son derece kullanışlı bir uygulamadır. IP adresleri ile DNS isimleri arasında ters dönüşüm sorgularının yapılarak kimi zaman sistemlere görevleri doğrultusunda isim verilmesi nedeniyle, bilgisayarların yaptıkları görevlerin belirlenmesinde yardımcı olur. [Dirican Can O., 80]

2. **Traceroute komutu:** Tracert komutu, hedef bilgisayara giden yolu keşfetmek için kullanılır. Windows sistemlerde *tracert* şeklinde kullanılır.

C:\>tracert 192.168.1.200
Tracing route to 192.168.1.200:
1 10 ms <10 ms <10 ms
2 10 ms 10 ms 20 ms
3 20 ms 20 ms 20 ms 192.168.1.200
Trace complete.

3. **Ping taraması (ping sweep):** Ping komutu, iki sistem arasında 3. katman düzeyinde bir iletişimin kurulup kurulamadığına yönelik bir kontrol aracıdır. İki sistem arasında fiziksel bir bağlantı sağlanmışsa ve bu sistemlerde IP protokol yığını düzgün olarak çalışmakta ise bize bir uçtan diğerine yolladığı kontrol paketinin istatistiksel değerlerini geri döndürür. Bir saldırgan bunu kurban ağın sınırlarını belirlemede ve ağı keşfetme aşamasında kullanabilir.

4. **Port taraması (Port scan):** Port tarama, hedef sistemde hangi servis ve uygulamaların çalıştığını bulmak amacıyla TCP ve UDP portlarını tarama şeklinde olur. Tarama sonrasında, çalışan uygulamalar, açık portlar ve servisler keşfedilir böylece saldırgan sisteme saldırabilmek için en iyi yola karar verir. Toplamda 65,535 adet TCP ve UDP port vardır. Bu port numaraları gelen veya giden paketin hangi işlem için kullanıldığını tanımlar.

Tablo 4.2.1.2. : Bazı çok kullanılan portlar ve bunlara ait protokolleri

Port	Servis	Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

Nmap bugüne kadar geliştirilmiş en yaygın kullanıma sahip port tarama uygulamasıdır. [81]

5. **İşletim sistemi güvenlik boşlukları taraması:** Uç sistem cihazında çalışan uygulamalarda var olan açıklar günümüzde en popüler tehditlerden biridir. Bu, bir işletim sistemi veya web sunucusu uygulaması olabileceği gibi yönlendirici, ağ geçidi ve güvenlik duvarı gibi cihazlardaki yazılımlar da olabilir. Saldırgan hedefteki sistemde çalışan yazılımları ve bunların boşluklarını taramak suretiyle sistem hakkında daha ayrıntılı bilgiye erişmiş olur.

4.2.2. Erişim (Access)

Adından da anlaşılacağı üzere, bir saldırganın herhangi bir kullanıcı hesabı veya şifresinin olmadığı sistem veya ağlara erişim kazanmak için yürüttüğü faaliyetlerdir. Hedef ağ veya sisteme erişim sağlandıktan sonra saldırganın yapabileceği işlemler üç ana sınıfta toplanmıştır:

- **Araya girme (Interception):** Bu yöntemde saldırgan, bir kaynak ve hedef iki sistem arasındaki trafiği dinler ve daha sonra kullanmak üzere kayıt eder. Bu kayıt edilen veri trafiği, kişisel bilgiler, öğrenci notları, araştırma ve geliştirme projeleri olabileceği gibi sunucu ve ağ cihazlarının yönetiminde kullanılan parolalar olabilir.
- **Değiştirme (Modification):** Sisteme giren saldırgan artık kaynakları değiştirebilir. Bu durum sadece dosyaların içerikleriyle sınırlı kalmaz, sistem konfigürasyonlarının, yetki seviyelerinin, kullanıcı adları ve parolaların değiştirilmesine kadar uzanabilir.
- **Üzerine ekleme (Fabrication):** Sisteme erişim hakkı kazanmış olan saldırgan, girmiş olduğu sistemdeki dosyaların, veri tabanı nesnelerinin ve diğer çalışan uygulamaların sahtesini yaratabilir. Ayrıca ele geçirdiği bu sistem üzerinden, ağa ve başka sistemlere saldırı düzenlemek amacıyla virüs, solucan veya Truva atları yerleştirebilir.

Yukarıda bahsi geçen tüm bu işlemleri gerçekleştirebilmek için çeşitli yöntemler mevcuttur. Bunlar; şifre ele geçirme, güven istismarı, port yönlendirme, ortadaki adam ve toplum mühendisliği yöntemleridir.

Parola ele geçirme

Parola ele geçirme saldırıları; kaba kuvvet (brute-force) saldırıları, Truva atları, IP şaşırtma (spoofing) ve paket izleyiciler (sniffers) de dahil olmak üzere çeşitli metotlar kullanılarak yapılır.

Kaba kuvvet saldırıları, bir kişinin kullanıcı isminin, parolasının, kredi kart numaralarının veya kriptografik anahtarlarının, birer birer tahmin edilmesi için kullanılan otomatik bir deneme yanılma işlemidir. Saldırgan, şifre tahmin etme araçları veya kodları kullanarak iyi bilinen kullanıcı adı (admin, administrator, root vb.) ve şifrelerin kombinasyonlarını (aaaa, bbbb, 123456 vb.) sırayla denerler. Bu tip uygulamalar, çok kullanılan şifreleri içeren hazır şifre veritabanları veya sözlükleri kullanırlar (dictionary attack). Ayrıca şifre alanında kabul edilen karakter setinin bütün kombinasyonlarını denerler. [82]

Normal kaba kuvvet ve ters kaba kuvvet olmak üzere iki çeşit kaba kuvvet saldırısı mevcuttur. Normal kaba kuvvet saldırısı, bir tek kullanıcı ismini birçok parola için kullanır. Ters kaba kuvvet saldırısı ise birçok kullanıcı ismini tek bir parola için dener. Milyonlarca kullanıcı hesabına sahip sistemlerde, birden çok kullanıcının aynı parolaya sahip olması olasılığı çok yüksektir.

Kaba kuvvet saldırı teknikleri çok popüler olup çoğunlukla başarılı olurlar fakat bu saldırılar saatler, haftalar veya yıllar gerektirebilir. [83] Örneğin; ***John The Ripper*** programı da ***l0phtcrack*** programı gibi, çoğu Unix işletim sisteminde, Dos, Win32 ve BeOS işletim sistemlerinde çalışan hızlı bir şifre kırıcıdır. Ana amacı zayıf Unix şifrelerini tespit etmektir. [84]

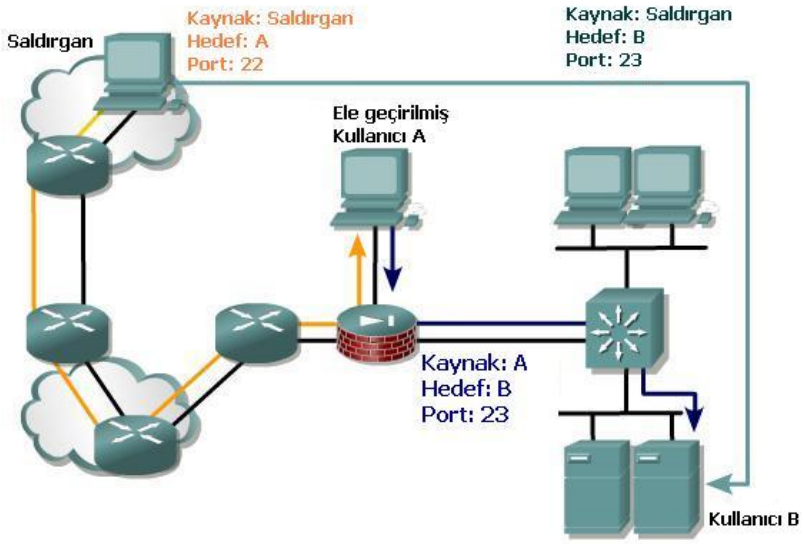
Bazı sistemlerde yetkiler ve izinler IP adresine göre verilmiştir ve bu erişimler sadece yetkili olan makinelerden yapılabilir. IP şaşırtma (spoofing) da saldırganlar kendi IP'leri yerine yetki verilen kişilerin IP'lerini kullanarak veya normalde iç ağda kullanılan IP'leri kullanarak sistemi yanıltırlar.

Güven istismarı (trust exploitation)

Bir kişinin ağdaki güven ilişkilerini kendi menfaati doğrultusunda kullanmaya çalışması olarak tanımlayabileceğimiz güven istismarı bir saldırı şeklinden daha çok bir tekniktir. Bir kurumun internet bağlantısını sağlarken kullandığı ağını düşünelim. Bu ağ, Alan Adı Sistemi (DNS), elektronik posta hizmeti (SMTP), ve web (HTTP) gibi sunucularına ev sahipliği yapmaktadır. Tüm bu sunucuların aynı segmentte yer alması nedeniyle bir sistemin diğer sistemler ile arasında güven ilişkisi vardır. Bir diğer örnek de güvenlik duvarının dışında yer alan bir sistem ile güvenlik duvarının içindeki sistem arasında oluşan güven ilişkisidir. Dışarıdaki sistem bu güven ilişkisini iç ağa saldırı olarak kullanabilecektir. Bir ağdaki güven seviyelerinde yoğun kısıtlamalara giderek bu tip saldırılar azaltılabilir. Güvenlik duvarının dışındaki bir sistem, iç taraftaki sistemlere tam bir güven içine sokulmamalı, belli protokollerle yada IP adresi dışında bir metotla sınırlandırılmalıdır. [85]

Port yönlendirme (Port Redirection)

Güven istismarı saldırısında olduğu gibi burada da ancak güvenlik duvarı üzerinden paket alış verişi yapabilen, güven ilişkisi yaratılarak ele geçirilmiş bir sistem kullanılmaktadır. (Şekil 4.2.2.1)



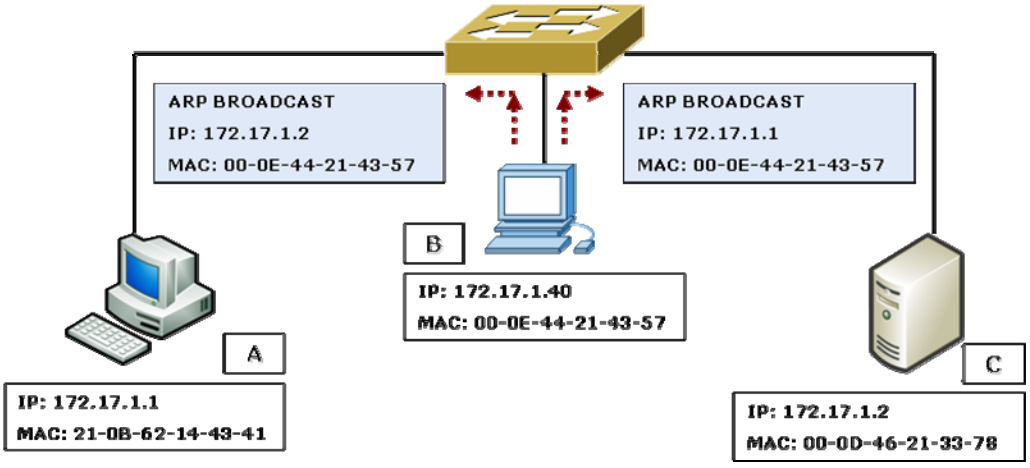
Şekil 4.2.2.1 : Port yönlendirme işlemi

Üç bacaklı ve her üçünde de bir kullanıcı olan bir güvenlik duvarı düşünelim. Dış bacaktaki kullanıcı, çeşitli hizmetlerde kullanılan sunucuların bulunduğu DMZ (Demilitarized Zone) segmentine erişebilmekte fakat iç bacaktaki sisteme erişememektedir. DMZ deki sistem ise hem içeri hem de dışarıdaki sistemlere erişebilmektedir. Eğer saldırganlar DMZ deki sisteme sızabilirlerse dışarıdaki sistemden direk içerideki sisteme yönlendirmeyi sağlayacak bir yazılım kurabilirler. Güvenlik duvarı üzerinde bu tip erişimleri kısıtlayacak kurallar da tanımlanmamışsa bağlantı kurulmuş olur. Böylece paket süzen güvenlik duvarlarının da süzme kuralları devre dışı bırakılmış olur. Bu tip bir bağlantıyı sağlayabilecek yazılımlara örnek olarak netcat [86] gösterilebilir. Sisteme bu tip bir saldırı düzenlendiğinde kullanıcı temelli bir güvenlik ihlal tespit sistemi (Intrusion Detection System: IDS) tarafından saldırganı tespit eder ve bu tip bir yazılımın kurulumunu önler.

Ortadaki adam (Man in the middle)

Bu saldırı türü yapılan bağlantıların arasına girip iki tarafa da sanki karşıdaki kişiymiş gibi davranarak veya bir tarafı devre dışı bırakarak yapılır. Bu yöntemde saldırganın,

bulunduğu ağdaki hedef cihaz ile bu cihazın iletişimde bulunduğu başka bir cihaz arasındaki trafiği kendi üzerinden geçirmek için, ağ ortamına veya kaynak ve hedef arasındaki cihazlara erişim sağlaması gerekir. Kablosuz LAN teknolojileri bu tip saldırılar için özellikle hassastırlar. Şifreli VPN (Virtual Private Network) bağlantılarının kullanımını zorunlu tutarak kablosuz ağların doğasında olan bu güvenlik zafiyetine karşı önlem olarak alınabilir. [Bruno A., 87]



Şekil 4.2.2.2 : ARP protokolü kullanarak ortadaki adam saldırısı düzenlenmesi

Saldırgan, gönderici IP adresi olarak bu uçbirimlerin adreslerini, fakat MAC adresi olarak kendi adresini içeren sahte ARP (Address Resolution Protocol) cevap mesajları yollar. Uçbirimler gelen bu ARP paketi sonucunda ARP geçici belleklerini güncellerler. Böylece bir uçbirim diğerine bir paket yolladığında bu paket aradaki saldırgana, oradan da hedef uçbirime iletilir. [Efe A., 88] Bunun sonucunda saldırgan elde ettiği paketleri okuyabilir, değiştirebilir yada yok edebilir. (Şekil 4.2.2.4.1.)

- **ARP:** IP yığınında, adres çözümlemesi yapan protokoller vardır. Adres çözümleme protokolü (ARP) IP adreslerinin fiziksel adreslere dönüştürülmesi sağlar ve bu fiziksel adresleri üst katmanlardan gizler. Genelde ARP, ARP belleği olarak bilinen, bir IP adres ile bir fiziksel adres arasında eşleştirme yapılmasını sağlayan tablolar ile çalışır. Bir yerel ağda, ARP, hedef IP adresini alır ve eşleştirme tablosundan buna karşılık gelen hedef fiziksel adresi arar. Eğer ARP, adresi bulursa, bulduğu fiziksel adresi; isteği yapan cihaza yollar.

IPSec (IP Security) protokolü ile bu tip saldırılar engellenebilir. IPSec protokolünün integrity (bütünlük) ve authentication (kimlik doğrulama) özellikleri, iletişimi gerçekleştiren bilgisayarların birbirlerinin kimliklerinin doğrulanmasını sağlayarak ortadaki adam saldırılarına karşı bir güvenlik önlemi sağlar. Bunun yanında IPSec'in IP paketlerini şifrelemesini sağlayarak bu paketlerin ağ üzerinde güvenli bir şekilde iletilmesini sağlanabilir. Böylece bu paketler ağ üzerindeki üçüncü bir kişi tarafından bir paket koklayıcı (sniffer) kullanılarak yakalansalar dahi paketlerin içeriği şifrelendiği için yakalanan paketler herhangi bir anlam ifade etmeyecektir. [Öztürkci H., 89]

Toplum Mühendisliği (Social Engineering)

Toplum mühendisliği, bilgisayar güvenliği konusunda ele alındığında; normalde insanların tanımadıkları biri için yapmayacakları şeyleri kişilere yapmalarını sağlatarak, insanların kişisel bilgilerine veya direk şifrelerine ulaşma yöntemidir. Çok basit bir yöntem olmasına rağmen en etkili ve en çok kullanılan yöntemdir.

Bir kurumda içeriden ya da dışarıdan gelebilecek saldırılara karşı güvenliği sağlamak için çeşitli güvenlik araçları (güvenlik duvarı, IDS/IPS, vb.) kullanılmaktadır. Bu tip güvenlik araçlarına oldukça yüksek maliyetlerde yatırımlar yapılmaktadır. Bu güvenlik araçlarını yapılandırıp yönetecek teknik personelin eğitimi konusunda gerekli yatırım yapılmamış ve çeşitli güvenlik politikaları ile de desteklenmemiş ise güvenliğin en zayıf halkası olan insan faktörü devreye girer. [Mitnick Kevin D., 90]

Tablo 4.2.2.1 : Toplum mühendisliği döngüsü

Hareket	**Açıklama**
Araştırma	Aralarında güvenlik delme testi kayıtları, yıllık raporlar ve pazarlama broşürleri, patent uygulamaları, basın kupürleri, sektör dergileri, internet sayfası içeriği olabilir. Ayrıca çöp karıştırıcılığı da uygulanabilir.
Dostluk ve güven uyandırma	İçeriden gelen bilgilerin kullanılması, başkasının kimliğine bürünme, kurbanın tanıdığı kişilerin adlarının sıralanması, yardım isteği veya otoriteye sahip olma faaliyetleridir.
Güveni kötüye kullanma	Kurbandan bir bilgi vermesinin veya bir işlem yapmasının istenmesidir. Ters dalaverede kurban saldırgandan yardım ister.
Bilgi kullanma	Eğer edinilen bilgi asıl amaçtan bir adım uzaktaysa saldırgan, amacına ulaşana kadar döngüdeki önceki adımlara geri döner.

Toplum mühendisliği; insan doğasında var olan başkalarına güvenme ve yardım etme eğiliminin, başka şekilde elde edilmesi zor olan şeylerin ele geçirilmesi amacı ile kullanılmasıdır.

Toplum Mühendisliği insan kaynaklı ve bilgisayar kaynaklı olmak üzere ikiye ayrılabilir:
İnsan kaynaklı toplum mühendisliğine örnek olarak;

- Başka bir çalışan veya yetkili biri gibi davranmak,
- Sorun çıktığı taktirde yardım isteyebileceğini söyleyip sonra sorunu kendisi yaratmak, böylece kurbanın yardım istemek için kendini aramasını sağlamak,
- Yardıma ihtiyacı olan, işe yeni girmiş biri gibi davranmak,
- Güven kazanmak için kurum içi terimleri kullanmak, verilebilir.

Bilgisayar kaynaklı toplum mühendisliğine örnek olarak;

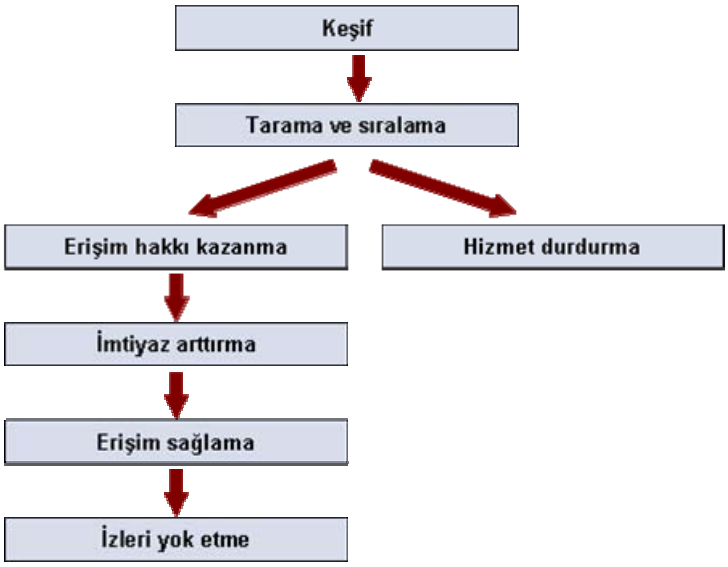
- Kurbanın yüklemesi için bedava yazılım veya yama göndermek,
- E-posta ekinde virüs veya Truva atı göndermek,
- Kullanıcının sisteme yeniden bağlanmasını veya parola girmesini isteyen sahte bir pencere kullanmak, gösterilebilir.

Etkileme sanatı, toplum mühendisliğinin en önemli kavramlarından biridir. Özellikle toplum mühendislerinin ilk aşamada uyguladıkları bir yöntem olan etkileme sanatı istenilen hedef ya da sisteme daha kolay erişim ve kullanım hakkı sağlamakta önemli rol oynar. Başarılı bir toplum mühendisinin en büyük özelliği karşı tarafa güven sağlayacak etmenler üretebilmesidir, bu nedenle iyi bir diksiyona, etkileme kabiliyetine ve düzgün cümle kurma yeteneğine sahip olması gerekir. Bunların yanı sıra diyalog esnasında kullanılan kelimeler, cümlelerin uyumu ve hitap şekli karşı tarafı etkilemede önemli etkenlerdir. Etkileme metodunu en iyi şekilde uygulayabilmek için, hedef hakkında, daha önceden bilgi edinmiş olmak yöntemin daha başarılı olmasını sağlayacaktır.

4.2.3. Hizmet Durdurma (Denial of Service)

Hizmet durdurma saldırıları, kurumlar için en büyük tehditlerden biri olup güvenliğin her zaman ulaşılabilirliği ve sürekliliği (availability) prensibini hedef alır. DoS saldırısı, çoğunlukla ağa sızma girişiminde başarılı olamayan saldırganlar için son bir çaba olarak

kullanılır. DoS saldırısının yöntem olarak saldırı gerçekleşme süreci içindeki yeri, Şekil 4.2.3.1. den görülebilir.



Şekil 4.2.3.1 : Saldırı gerçekleşme süreci

Normal işlemlerin ve normal iletişimin kesintiye uğratılması DoS saldırısının etkileridir. Çoğu durumda bir saldırgan için bu saldırıda başarılı olmak, ağa erişim hakkı kazanmaktan daha kolaydır. DoS saldırıları üç ana başlık altında toplanır:

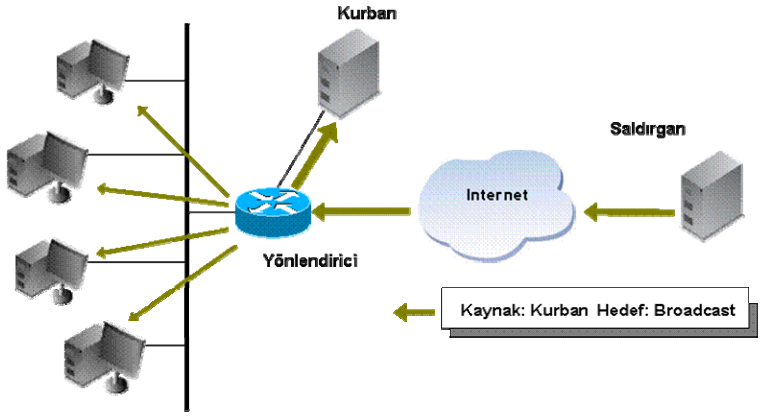
- Bant genişliği tüketimi
- Kaynak sömürme
- Programlama kusurları

Bant genişliği tüketimi

Bant genişliği, cihazların ağa bağlantı kapasitelerinin saniyede aktarılan bit (bps = bit per second) olarak ifadesidir. Bant genişliği tüketme saldırıları, tek bir cihazın veya cihaz grubunun ağa bağlantı kapasitesini kullanıp iletişim kabiliyetini keserek gerçekleşir. Ne kadar geniş olursa olsun her bant genişliğinin bir sınırı vardır. Eğer saldırgan bu bandı doygunluğa eriştirecek kadar meşgul edebilirse cihazın normal iletişimini de kesebilir. Bu tip saldırılara aşağıdakiler örnek olarak verilebilir:

- **Smurf saldırısı:** Internet Kontrollü Mesajlaşma Protokolü (ICMP = Internet Control Message Protocol) nün açıklarından faydalanılarak yapılır. Saldırgan o ağdan seçtiği kurbanın IP adresini kaynak adres, hedef olarak ta hedeflediği ağın broadcast adresi işlenmiş kandırılmış (spoofed) bir ping paketi gönderir.

Karşılığında da Şekil 4.2.3.1.1 deki gibi o ağdaki cihazlardan kurbana doğru cevap (reply) mesajları akmaya başlar.



Şekil 4.2.3.2 : Smurf saldırısı

Ağın Smurf saldırısına uğramasını önlemek için yönlendiricilerde

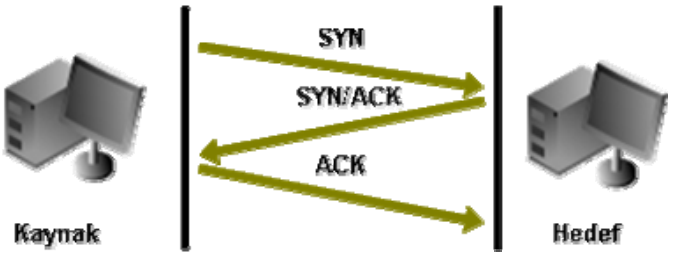
no ip directed-broadcast

komutu kullanılır.

Kaynak sömürme

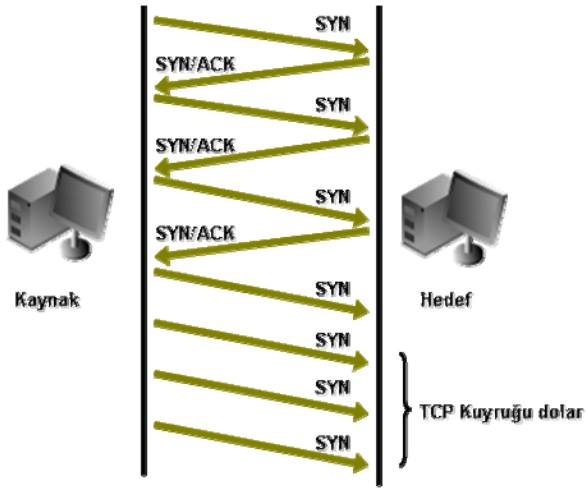
Kaynak sömürme saldırıları, bant genişliği tüketimi saldırılarının aksine tek bir sistemin kaynaklarını hedef alır ve sonucunda hedef sistem donar veya çöker. Bu tip saldırılara bir kaç örnek aşağıdakiler verilebilir:

- **SYN seli saldırısı**: Bir istemci sistem bir sunucuya telnet, web, e-posta hizmetlerinden faydalanmak amacıyla bir TCP bağlantısı kurmak istediğinde istemci ve sunucu arasında bir dizi mesaj alışverişi olur (three way handshake).
  - İstemci, sunucuya içinde kendisi hakkında bilgi bulunan bir SYN (Synchronize) paketi yollar.
  - Sunucu bu SYN paketini alır ve istemciye, gönderilen SYN'i aldığını belirten ACK (Acknowledgement) ile yine kendi hakkında bilgi içeren SYN paketini beraber yollar.
  - İstemci SYN+ACK paketini alır ve sunucuya ACK paketi ile bunu haber verir ve ikisi arasında bağlantı kurulmuş olur.



Şekil 4.2.3.3 : Normal TCP Trafiği (three-way handshake)

Saldırgan bir SYN, sunucuda buna yanıt olarak SYN+ACK paketlerini yollar ve ACK paketini beklemeye koyulur. Eğer ACK paketi gelmez ise bu bağlantıya "yarı-açık" bağlantı denir. [Klevinsky T.J. ve Laliberte S., 91]



Şekil 4.2.3.4 : TCP SYN Seli saldırısı

Sunucu ACK için beklerken, saldırgan sunucuya ACK yerine bir bağlantı talebinde daha bulunur ve bu işlem sürekli tekrarlanır. Sunucu açılan her bağlantının son ACK paketini bekleyeceği için her bağlantı hakkında bilgiyi hafızasına yerleştirir. Belli bir süre sonra bu bilgi boyut olarak hafızada taşma meydana getirecek kadar büyür ve sunucu dışarıdan gelecek hiçbir bağlantı talebine yanıt veremez hale gelir.

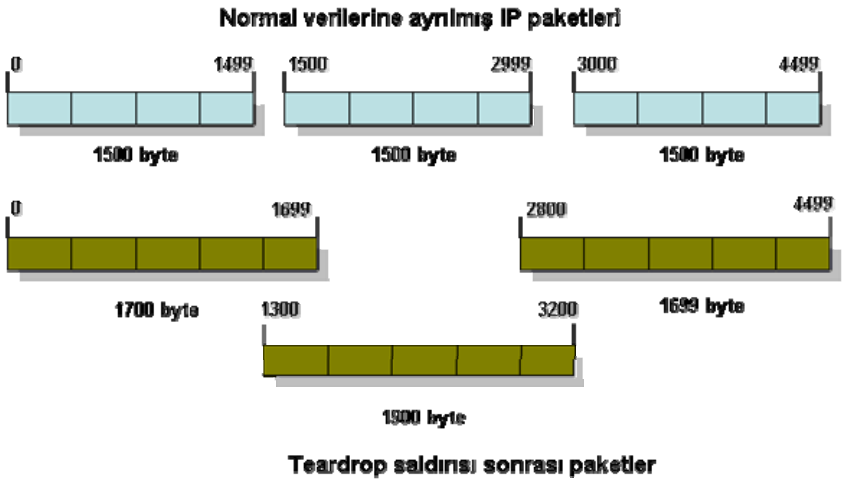
Güvenlik duvarları bu tip saldırıları önleme amaçlı temel IDS özelliklerini sağlayabilecek şekilde yapılandırılabilirler. Örneğin Cisco PIX güvenlik duvarı, Flood Defender olarak adlandırılan bir özelliğe sahiptir. Bu özellik belli bir

sunucuya açılmış cevapsız SYN (embriyonic) bağlantılarının miktarını sınırlandırır. Sınıra ulaşıldığında diğer bütün bağlantılar kesilmek suretiyle saldırı önlenir.

Programlama açıkları

Programlama açıkları saldırıları, sistemin işletim kabiliyetini durdurabilecek bir kritik hatadan meydana gelir. Bu tip saldırılar, saldırganın savunmasız bir programı yüksek miktarda veri veya bozuk paketler göndererek çalışmaz hale getirmesi sonucu ortaya çıkar.

- **Ping of Death saldırısı**: Bir paketin 65,536 byte lık standart boyutu verilere ayrılma (fragmentation) tekniği ile aşırı şekilde büyütülebilir. Saldırgan hedef sisteme bu şekilde büyük boyutta ve sıklıkta ping paketleri göndererek tampon belleğini doldurur. Sonrasında sistem cevap veremez hale gelir ve çöker.
- **Teardrop saldırısı**: Bir IP paketi karşı tarafa yollandığında bu paket tekrar verilere ayrılırken paketin içinde bulunan "offset" bilgisi kullanılır. Bu "offset" bilgilerinin birbirleriyle çakışmaması yani üst üste gelmemesi lazımdır. Özel ayarlanmış bir paket, bu senkronizasyonu bozabilir ve paketler üst üste gelirse ve bunu kontrol edebilecek bir mekanizma da mevcut değilse bu işletim sistemini çalışmaz duruma getirebilir. [Atabey O., 92]



Şekil 4.2.3.5 : Teardrop saldırısı

- **LAND saldırısı**: Bir LAND saldırısında, hedef sistemle aynı kaynak ve hedef port ve aynı IP adresine sahip bir TCP SYN paketi gönderilir. Bu paketi alacak

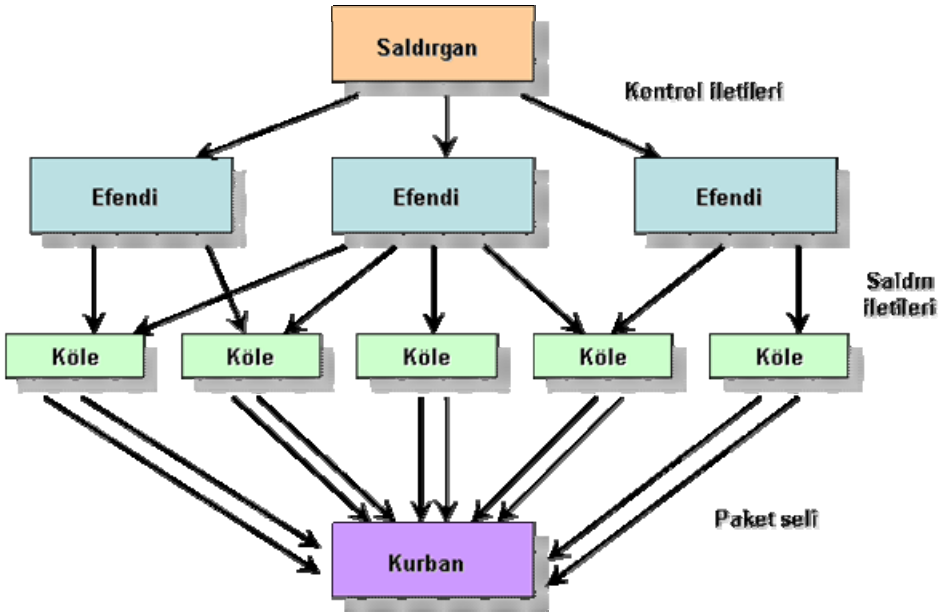
sistem bu bozulmuş paketlere nasıl davranacağını bilemez ve sonucunda donar, kilitlenir veya CPU kullanımı yüzde yüzlere tırmanır. 1997 yılından beri bilinen bir saldırı şekli olmasına rağmen Windows XP Service Pack 2 ve Windows Server 2003 işletim sistemleri eğer üzerlerindeki bütünleşik güvenlik duvarları kapalı olurlarsa bu saldırıya karşı hala savunmasızdırlar. [Whitaker A. ve Newman Daniel P., 79] Aynı zamanda TCP/IP analizi, güvenlik duvarı sınama, port tarama ve işletim sistemi saptama için kullanılan Hping programı ile bu tip SYN paketleri yaratılabilmektedir.

- **SMBdie saldırısı**: SMB (Server Message Block - Sunucu İleti Bloğu) protokolü Microsoft' un dosya, yazıcı ve seri bağlantı noktalarını paylaşmak için kullandığı protokoldür. Saldırgan 139 veya 445 portuna özel olarak hazırlanmış bir SMB paket isteği göndererek, hedef sunucunun hizmet dışı kalmasını sağlayabilir.

Dağıtık hizmet durdurma saldırıları (Distributed DoS)

Bir dağıtık hizmet durdurma saldırısı, DoS saldırısı ile benzer amaçları taşır, tek farkı DDoS saldırısının birden fazla kaynak saldırı noktasından yapılıyor olmasıdır.

Bir DDoS saldırısı iki aşamadan oluşur. İlk adım olan saldırı öncesi hazırlık döneminde, saldırgan interneti tarayıp kendisine saldırıda kullanılmak üzere bilgisayarlar bulur, ele geçirir ve saldırı yazılımlarını üzerlerine kurar. Üniversite ağları da dahil olmak üzere zayıf yapılandırılmış ağlar ve gerekli güvenlik önlemleri alınmamış, savunmasız bilgisayarlar bu tip bir saldırının hedefleridir. Bu ele geçirilen bilgisayarlara zombi veya köle adı verilir. Daha sonra kontrolün ve koordinasyonun sağlanabilmesi için makineler arasında iletişim kanalları oluşturur. Bu ya işletmeci/aracı (handler/agent) mimarisi veya IRC tabanlı bir komut ve kontrol kanalı vasıtasıyla yapılır. Bir kez DDoS ağı kurulduğunda istenildiği miktarda istenildiği değişik hedefler için saldırıda kullanılabilir. [Mirkovic J. ve Dietrich S., 93] Bu adım tamamlandığında gerçek saldırının gerçekleşeceği ikinci adım başlar. Saldırgan, Şekil 4.2.3.6. dan da görülebileceği gibi efendilere (master), köle bilgisayarların saldırıyı başlatması için gereken talimatları verir.



Şekil 4.2.3.6 : Dağıtık hizmet durdurma saldırısı

Kölelerden kurbana doğru trafik, sel olup akmaya başladığı zaman saldırı her yerden yapılıyormuş gibi gözükür. Bu nedenle kaynağının tespit edilmesi, kontrolü ve durdurulması da zordur. DDoS saldırılarından korunmak için ilk olarak saldırı fark edildiği anda saldırıda bulunan adreslerden gelen bağlantı isteklerinin iptal edilmesi gerekmektedir.

DDoS saldırısının bileşenleri yazılım ve donanımlardır. İki parçadan oluşan yazılımlar şunlardır:

- Saldırı yazılımı: Saldırganın efendilerle arasındaki koordinasyonu sağlayan komut ve kontrol paketlerini yönetir.
- Aracı yazılım: Köle bilgisayarlarda çalışan bu program saldırgandan gelen saldırı hakkındaki ayrıntılı bilgileri içeren komut paketlerini alır ve onlara göre davranır.

DDos saldırısı için gereken ikinci bileşen donanımlardır. Üç maddeden oluşur:

- Efendi: Saldırı yazılımının çalıştığı sistemdir.
- Köle: Saldırıda aracılık işlemini yürüten ikinci derecede sistemdir.
- Kurban: Saldırıya maruz kalan hedef sistemdir.

DDoS saldırısı için kullanılan bazı araçlar ve yöntemleri Tablo 4.2.3.1. de gösterilmiştir.

Tablo 4.2.3.1 : DDoS araçları ve yöntemleri

DDos Araçları	Saldırı yöntemi
Trin00	UDP
TFN	UDP, ICMP, TCP
Stacheldraht	UDP, ICMP, TCP
TFN2	UDP, ICMP, TCP
Shaft	UDP, ICMP, TCP
MStream	TCP
Trinitiy	UDP, TCP

DDos araçlarında dikkat edilecek husus genelde yüksek numaralı (1024 ve üzeri) açık portları kullandıkları ve trafiklerinin zorlukla tespit edilebilmesi için iletişimlerini şifreli yaptıklarıdır.

Bu saldırılara karşı en iyi savunma her zaman içerisine servis sağlayıcının da dahil olduğu bir plana sahip olmaktır. Böylece akan trafiği zamanında durdurarak bize yardımcı olabilirler. Bu tip bir saldırıda geçen her dakika vereceği zararlar açısından telafisi zor sonuçlar doğurabilecektir.

4.2.4. Kötü amaçlı program kodları (Malicious codes)

İnsanlar genelde bu kadar kolay saldırıya uğrayabildikleri ve sistemlerinin çalışmaz hale gelmesinden dolayı ilk önce donanım ve yazılım üreticilerini suçlarlar. Donanım ve yazılım firmalarının, ürünlerini daha güvenli yapma hususunda bazı sorumlulukları olduğuna şüphe yoktur, fakat tüm suçu da bilişim sektörüne yüklemek haksızlık olur.

Kötü amaçlı program kodları, bir sistemin veya ağ cihazının normal işlevini engellemeye yönelik her türlü yazılıma verilen genel bir tanımlamadır. Bu yazılımlar çoğunlukla kullanıcının rızası dışında çalışırlar.

Kötü amaçlı program kodlarının doğurduğu saldırıların başarılı olmasının birçok sebebi vardır;

- Yazılım mimarisindeki açıklar,

- Güvenliği yeterince test edilmemiş sistem ve ağ yapılandırmasından doğan güvenlik boşlukları,
- Saldırganlar tarafından kullanılan toplum mühendisliği metotları,
- İnsan hataları ve olayın ciddiyetini kavrayamamış kullanıcılar,
- Saldırganların bu konu üzerinde ısrarlı çalışmaları, bunlara örnektir.

On binlerce çeşit virüs, solucan ve Truva atı mevcut olduğu bilinmesine rağmen bunlardan çok azı dikkate değerdir. Kötü amaçlı kodların tehdit seviyesi (threat level) onun sahip olduğu potansiyel yayılma ve bulaşma düzeyini ifade eder. Genel olarak yok, düşük, orta ve yüksek olarak sınıflandırılır. Bir kodun yüksek miktarda bilgisayara bulaşarak hızla yayılmaya başlamasına virüs dolaşımda (in the wild) denir. İnternette bu dolaşımda olan kodların arşivinin ve bilgilerinin derlenerek tutulduğu *wild list* [94] gibi listeler mevcuttur.

Kötü amaçlı kodlar çok geniş bir yelpazede çeşitlilik göstermekte olup sürekli artan sayıda bulaşma mekanizmasıyla dağılmaktadırlar. Kötü amaçlı kod çeşitleri;

- Virüsler,
- Truva atları ve arka kapılar,
- Solucanlar (worm),
- Karışık tehditler (blended threats),
- Mantıksal bombalar (logic bombs) / Zaman bombaları (time bombs),
- Casus yazılımlar (spyware),
- Reklam pencereleri (adware),
- Hırsız yazılımlar (stealware),

olarak sıralanabilir. [Erbschloe M., 95]

Virüsler

Virüsler, başka programların içine kendisini kopyalayarak bulaşan bir bilgisayar programıdır. [Cohen F., 96] Virüs, bir bilgisayara bulaşarak genelde diğer bilgisayarlara ve ağ cihazlarına hasar vermek üzere dizayn edilmiş olup en büyük özellikleri kendi kendilerini kopyalayabilmeleridir. Çoğunlukla kullanıcının haberi olmadan bulaşır ve

iradesinin dışında çalışarak sisteme çeşitli boyutlarda zarar verirler. Virüsün aktif olabilmesi için öncelikle bulaştığı programın çalıştırılması gerekir.

Bilgisayar virüslerinin aktif oldukları kendilerine özgü çalışma ortamlarını tanımak, onları anlama yolunda en önemli adımlardan biridir. Kötü amaçlı bir kodun bir sisteme başarılı bir şekilde bulaşması ancak bu kodun bulaşma şartlarıyla o potansiyel ortamın uyuşmasına bağlıdır. [Szor P., 97]

Virüsler genelde yapılarında aşağıdaki bileşenlere sahiptir;

- Kopyalama mekanizması; bir bilgisayardan diğerine virüsün taşınabilmesini ve yeniden üremesini sağlar. [Ludwig, Mark A., 98]
- Tetik; virüsün görevini veya kopyalama mekanizmasını harekete geçirir.
- Görev veya görevler grubu; bir sistem üzerinde çalışarak dosyaları ya çalışmaz hale getirir veya değiştirir. İşletim sistemi ayarlarını veya yapılandırmasını değiştirir. Sistem veya ağ cihazının çalışmasını sekteye uğratır veya tamamen engeller.

Bu üç bileşen çok çeşitli şekillerde ve davranışlarda bulunabilirler. Sonsuz kombinasyonda çok çeşitli zararlar vermek üzere dizayn edilirler. Bazı popüler virüs çeşitlerine örnek olarak aşağıdakiler verilebilir:

- **Boot sector virüsleri**: Sabit veya disket sürücünün ilk sektörüne bulaşırlar. İlk sektör bilgisayar çalıştıktan hemen sonra işletim sistemi yüklenirken bilgisayarın konfigürasyonuna ait master boot kaydını tutar. Bilgisayar açıldığında virüs harekete geçip belleğe yüklenerek kontrolü ele geçirir. Disket sürücüye takılan tüm disketlere bulaşır. Ağ üzerinden diğer sistemlere yayılmazlar. En çok bilinen boot sektör virüsü 1991 yılında belirlenen Michelangelo virüsüdür.
- **Dosya silen virüsler**: Temel görevleri ve uygulamaları çalıştıran belli dosyaları silerler. Kelime işleme dokümanlarını (word), hesap tablolarını veya grafik dosyalarını silmek üzere tasarlanmışlardır.
- **Dosyalara bulaşan virüsler**: Genelde uzantısı .com, .exe, .dll, .ovr, veya .ovl olan çalıştırılabilir dosyalara kendilerini eklerler. Dosya çalıştırıldığında virüs yayılmaya başlar. Kodlarının bir kopyalarını bulaştıkları dosyanın sonuna eklerler. Grafik dosyalarına, html sayfalarına, video veya ses dosyalarına

eklenen veya içeriğine gömülü virüsler de bu gruba dahildirler. Bilinen bazı Windows çalıştırılabilir dosya tipleri Tablo 4.2.4.1.1 de görülmektedir.

Tablo 4.2.4.1 : Bilinen bazı Windows çalıştırılabilir dosya tipleri

Uzantı	**Açıklaması**
.bat	Windows toplu işlem dosyası
.com	Özellikle derlenmiş DOS/Windows binary çalıştırılabilir dosyası
.exe	Windows standart binary çalıştırılabilir dosya
.js	JavaScript dili kaynak dosyası
.mnu	Değişik uygulamalar ve çalışma ortamları için menü dosyaları
.ovl	Windows veya DOS overlay dosyası
.pif	Windows program bilgi dosyası
.prg	Her türlü Windows program kaynak dosyaları
.scr	Windows ekran koruyucu dosaysı
.sys	Windows veri dosyası, ayrıca Sysgraph, Sysstat ve SPSS uygulamaları
.vb	Visual Basic kod dosyası
.vbe	Visual Basic kod dosyası
.vbs	Visual Basic uygulamaları (bütün MS Office bileşenleri de dahil) kod dosyası
.ws	Windows Script dosyası
.wsc	Windows Script bileşeni
.wsf	Windows Script dosyası

- **Makro virüsler**: Microsoft Word veya Excel tabloları gibi ofis yazılımı uygulamalarında bulunan makrolar vasıtasıyla yayılırlar. Bu makrolar genelde bir doküman veya tablonun bir parçası gibi kaydedilir ve eğer bu dosyalar e-postaya eklenir, bir diskete kaydedilir veya başkalarının erişimi için dosya sunucusuna kopyalanırsa diğer sistemlere de bulaşabilir.

  Bu tip virüsler otomatik çalışabilen makrolardan yararlanılarak oluşturulurlar. Bu özellikte üç tip makro vardır:

  Autoexecute: Autoexec adında bir makro MS Word'ün başlangıç dizininde normal.dot yada global template'in içindeyse Word her açıldığında bu makro çalışacaktır.

  Automacro: Önceden tanımlanmış aç, kapa, Word'den çık, gibi bir olay olunca çalışır.

  Command: Makro global makro dosyasındaysa yada makro bir Word komutuyla aynı adı taşıyorsa kullanıcı komutu çalıştırınca makro uyanır.

Automacro yada command makrosu belgeye eklenir. Belge açılınca global makro dosyasına kendini kopyalar. Word'ün açtığı her oturumda global makro aktif olur ve çoğalarak hasar verir. [Grimes Roger A., 99]

Makro virüsleri hem çalıştırılabilir programlara hem de veri dosyalarına bulaşırlar. Makro virüslerine en bilinen örnek olarak Melissa' nın bulaşmış olduğu bir Word belgesini açıldığında, virüs Word' ün temel şablonu olan NORMAL.DOT' a bulaşır. Word bütün kişisel ayarları ve temel makroları bu şablon dosyada tutar. Dolayısıyla, kendini NORMAL.DOT'a kopyalayan Melissa, yaratılan bütün yeni belgelere de kendiliğinden bulaşır. Marker, Caligula, Triplicate, GaLaDRieL ve W2KM_PSD makro virüslerine diğer örneklerdir.

- **Kütlesel e-posta gönderen (mass mailer) virüsler**: Bu tip virüsler yayılma şekli olarak interneti kullandıkları için aynı zamanda solucan özelliği de göstermektedirler. Virüs bulaşmış olduğu bilgisayarın adres defterinde bulunan adreslere eklenerek kendi kendini gönderir. Genelde bulaşmış olduğu bir e-posta aracılığıyla sisteme girer. Bazı durumlarda virüs bulaşmış ekli bir posta otomatik olarak çalışabilir, aksi durumda virüsün bulaşması için kullanıcının bu eki çalıştırması gerekir. Virüs aktif olduğunda kendisini Windows sistem klasörüne kopyalar, kayıt defterinde (registry) kendisi için bir başlangıç anahtarı yaratır veya WIN.INI yada SYSTEM.INI dosyasını değiştirir ve bellekte aktif olarak kalır. Aktif olunca kullanıcının adres defterinden e-posta adreslerini toplar. HTML dosyaları gibi belli dosyaları tarar ve e-posta adreslerini buralara yerleştirir. Bu tip virüsler kendi içlerinde gömülü posta hizmet sunucuları (SMTP) sayesinde izlerini belli etmeden topladığı tüm adreslere kendi kendini gönderir. Bazı sürümleri sistemde bulunan e-posta yazılımını aracı olarak kullanabilmektedir. Eğer tek bir posta kutusunu hedef alırsa "…@m" uzantısı ile gösterilir. Birden fazla posta kutusunu hedef aldığını gösteren "…@mm" uzantısı bu tip virüsleri tanımlamak için kullanılır. En bilinen örnekleri; Klez, Nimda, Yaha, Sircam, Bugbear, Magistr, Braid, Badtrans, PrettyPark, Sobig tir.
- **Polimorfik virüsler**: Bulaştıkları her farklı sistemde görünüşlerini değiştirebilen virüslerdir. Genellikle virüs koruma yazılımlarından saklanmada çok başarılıdırlar. Örn: W32.Bacalid.B, W32.Polip, W32.Bakaver.A

- **Gizlenebilen (stealth) virüsler**: İşletim sistemi veya antivirüs programı ile tespit edilemeyip dosya büyüklüğünü veya dizin yapısını değiştirebilen virüslerdir.
- **Sahte (hoax) virüsler**: Genellikle doğru olmayan bir ifadeyi, şaka ya da gönderenin başka bir amacına yönelik olarak çok kişiye gönderen mesajlar anlamına gelmektedir. Bu tür mesajlar, "virüs, ödül, yardım, vb." konulardaki asılsız içerikleriyle heyecan yaratarak kullanıcıların zamanını boşa harcamalarına neden olmaktadır. Bu yöntem ayrıca, yoğun mesaj zinciri içinde geçen e-posta adreslerini ele geçirerek, daha sonra kullanıcılara istekleri dışında mesajlar göndermeyi amaçlayan kötü niyetli kişiler tarafından da yaygın biçimde kullanılmaktadır. Hoax virüs listeleri için birçok kaynak bulunmaktadır. [100, 101]

Truva atları ve arka kapılar

Truva atları; zararsız ve gerekli gibi görünen fakat çalıştırıldığında kullanıcının haberi olmadan saldırganların sisteme uzaktan erişim sağlamasına, sisteme arka kapı yerleştirmesine, klavye hareketlerinin kayıt edilmesini, hizmet durdurma saldırılarına ve antivirüs veya yazılım güvenlik duvarlarının devre dışı kalmasını sağlayabilen programlardır. Virüs veya solucanların aksine Truva atları kendi başlarına yayılamazlar.

Truva atları, genel olarak iki ayrı modülden oluşmaktadırlar. İlk modül, saldırganın kullanıcı bilgisayarına uzaktan erişimine ve kontrol sağlamasına izin vermesine ikinci modül ise saldırgan ile kullanıcı bilgisayarı arasında bağlantıyı kurabilecek bir port açılmasını sağlar.

Truva atlarını yedi ayrı sınıfta toplayabiliriz. Birçoğunun birden fazla işlevi olmasından dolayı bazılarını da tek bir sınıfa sokmak oldukça zordur. Truva atlarının neler yapabileceğini daha iyi anlayabilmek için bu sınıflar aşağıda gösterilmiştir:

- **Uzaktan erişim sağlayan**: Saldırgana sistem üzerinde uzaktan tam kontrol sağlarlar. En bilinen örnek Subseven Truva atıdır. Bu tip Truva atları genelde istemci/sunucu programlar şeklinde kurulur.
- **Veri gönderen (keylogger)**: Amacı verileri kayıt edip saldırgana yönlendirmektir. Aynı zamanda keylogger olarak ta bilinmektedirler. Bu

programlar klavye hareketlerini ve fare hareketlerini gizli bir dosyaya kayıt eder. Daha sonra ele geçirdiği parolaları, kredi kartı bilgilerini veya diğer bütün kişisel bilgileri önceden belirlenen bir e-posta adresine gönderir. Bu tip bir Truva atına örnek olarak Eblaster verilebilir.

- **Yıkıcı**: Bu Truva atları özellikle zarar vericidirler. Hard Disk Killer bu tip programlara örnektir. Amacı programlara zara vermek veya sistemden silmektir. Sabit diskin ışığının sürekli yanması veya ses çıkarması bulaştığının tek belirtisidir. Örn: Blackmal
- **Hizmet durduran (DoS)**: Sunucular üzerinde çalışan belirli bir hizmeti veya tüm sistemi durdurmayı amaçlayan programlardır. Örneğin DLoader_L Truva atı bir e-posta eki ile gelmektedir ve kendisini Microsoft Windows XP için acil bir güncelleme olarak tanıtır. Çalıştırıldığında ise bilgisayara karşıdan bir program yükler. Bu program internete her bağlanıldığında belirli bir web sitesine, cevap verebileceği bağlantı sayısından daha fazla istek göndererek onun hizmet dışı kalmasını (Denial of Service) sağlamak üzere bilgisayarın üçüncü kişilerce denetim altına alınmasına izin vermektedir. DDoS.Dest, DDoS.Win32.Kozog, DoS.Win32.DieWar, Trojan.Spector, Trojan.Storm diğer örneklerdir.
- **Proxy**: Bu tip Truva atları proxy hizmeti vermek üzere tasarlanmışlardır. Saldırganın saklanıp, hareketlerini kurban bilgisayar üzerinden internete bağlanarak yürütme olanağı sağlar. Böylece saldırganın takibi zorlaşır. Mitglieder.E, Jupillites, Satiloler.C, Cidra bu tip Truva atlarına örnektir.
- **FTP**: Bu tip Truva atları özellikle 21 numaralı porttan çalışmak üzere tasarlanmışlardır. Saldırgana kurbanın bilgisayarından dosya indirme, gönderme veya taşımaya olanak sağlar. Back Construction, Blade Runner, Doly Trojan, Fore, FTP trojan, Invisible FTP, Larva, WebEx, WinCrash, Cattivik FTP Server, CC Invader, Dark FTP, Juggernaut 42, MotIv FTP, Net Administrator, Ramen, Senna Spy FTP, Traitor 21, The Flu, Shaft, 21 numaralı porttan çalışan Truva atlarıdır.
- **Güvenlik yazılımını devre dışı bırakanlar**: Bu tip Truva atları yazılım güvenlik duvarlarına ve antivirüs programlarına saldırmak ve bunları devre dışı bırakmak üzere tasarlanmışlardır. Böylece saldırgan sistemin kontrolünü daha kolay ele geçirebilecektir. Trojan.Disabler bu sınıfa örnek olarak verilebilir.

Tablo 4.2.4.2 : Uzaktan erişim ve arka kapıların kullandığı portlar

Adı	**Default Protocol**	**Default Port**
Back Orifice	UDP	31337
Back Orifice 2000	TCP/UDP	54320/54321
Beast	TCP	6666
Citrix ICA	TCP/UDP	1494
Donald Dick	TCP	23476/23477
Loki	ICMP	NA
Masters Paradise	TCP	40421/40422/40426
Netmeeting Remote Desktop Control	TCP /UDP	49608/49609
NetBus	TCP	12345
Netcat	TCP/UDP	Any
pcAnywhere	TCP	5631/5632/65301
Reachout	TCP	43188
Remotely Anywhere	TCP	2000/2001
Remote	TCP/UDP	135-139
Timbuktu	TCP/UDP	407
VNC	TCP/UDP	5800/5801

Bazı bilinen Truva atları, ticari araçlar ve arka kapılara ait protokol ve port örnekleri Tablo 4.2.4.2 de verilmiştir. Bu konu ile ilgili daha fazla ayrıntılı bir tablo için kaynaklar mevcuttur. [102]

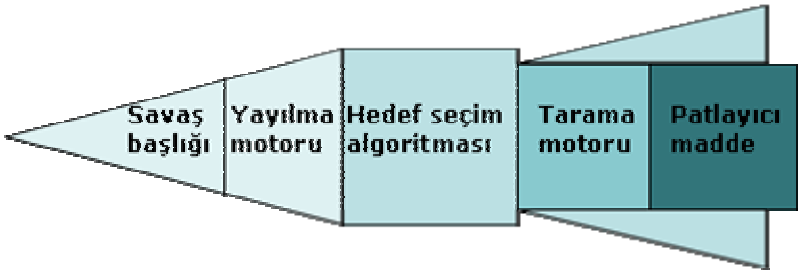
Arka kapılar: Bir arka kapı programı saldırganlara bir sistemin normal güvenlik kontrollerini devre dışı bırakarak saldırganın kendi istekleri doğrultusunda erişim kazanmasına olanak sağlayan programlardır. Eğer bir program bir arka kapı işlevi görerek sisteme gizli bir erişim sağlıyorsa arka kapıdır. Truva atları ile karıştırılmamalıdır. Elbette aynı zamanda hem arka kapı hem de Truva atı özelliklerine sahip bir takım araçlar mevcuttur.

- **Tini:** Windows için yazılmış basit ve küçük bir arka kapı Truva atıdır. Assembler dilinde yazılmış 3 kb boyutundadır. TCP 7777 portunu dinler ve uzaktan erişime olanak sağlar.
- **Qaz:** Notepad.exe nin adını Note.com olarak değiştirir ve kendisini bilgisayara Notepad.exe olarak kopyalar. Notepad.exe her çalıştırıldığında Qaz Truva atı aktif olur ve fark edilmemek için orijinal Notepad.exe yi çağırır. 7597 portundan

gelecek bağlantı isteklerini bekler. Bu portu açık bulan herhangi birisi sisteme giriş yapabilir.

Solucanlar

Solucanlar virüslerle benzerlik taşısa da bir program veya taşıyıcıya ihtiyaçları yoktur. Solucanlar kendi kendilerini kopyalar ve yayılmak için bilgisayarlar arasındaki bağlantıları kullanırlar. [Oldfield P., 103] Solucanlar başka diğer saldırıların kolayca ulaşamayacakları bir çapta etkili olmaları sebebiyle saldırganlar tarafından kullanılırlar.



Şekil 4.2.4.1 : Bir solucanın temel bileşenleri

Genel olarak solucanlar; Şekil 4.2.4.1 de görüldüğü gibi güdümlü bir füzeye benzetilerek, bileşenlerine ayırabilir. Savaş başlığı, bir sisteme giriş sağlayabilecek tampon taşması, dosya paylaşımı veya e-posta saldırıları gibi unsurlar içerir. Yayılma motoru, solucanı hedef sisteme taşır. Patlayıcı madde (payload), hedef üzerinde bazı işlemler gerçekleştirecek kodları içerir. Bazı solucanlar arka kapıları, hizmet durdurma saldırı araçlarını veya şifre kırma programlarını taşırlar. Hedef seçim algoritması ise güvenlik boşluklarını tespit etmek üzere yeni adresleri seçer. [Skoudis E. ve Zeltser L., 104]

E-postalar ve ağa bağlı bilgisayarların güvenlik boşlukları solucanların yayılmalarında en çok kullandıkları iki yoldur. Yayılmak için e-postaları kullanan solucanlar kütlesel mail gönderen solucanlar (mass-mailing worms) olarak bilinirler ve genellikle Visual Basic programlama dili ile yazılırlar. Windows işletim sisteminde Microsoft Outlook veya Outlook Express posta istemcilerinin açıklarını kullanırlar. Bu istemcilerdeki adres defterinde tutulan bütün e-posta adreslerine bir kopyasını gönderir. Bu tip solucanlara

Sober, Netsky, Novarg, Love Letter, Sircam, Sobig, BugBear, Beagle, Zotob ve Mydoom örnek olarak verilebilir.

Internet solucanları aksine bilinen bir açığa sahip işletim sistemi veya web sunucusu çalıştıran bilgisayarları tarayarak yayılır. Yeterince güvenlik önlemi alınmamış bir bilgisayar bulduğu anda solucan açıklardan faydalanarak hedef bilgisayara kendini kopyalar ve sonrasında bu bilgisayarı saldıracak başka hedefler bulmak üzere kullanır. [Wang W., 105] Bu tip solucanlara CodeRed, Nimda, Blaster, Sasser ve Welchia örnek gösterilebilir.

Karışık tehditler (blended threats)

Karışık tehditler, e-posta virüslerinin geleneksel zararları ile hızlı tarama yapan ve ağdaki güvenlik açıklarını bulabilen ağ tabanlı solucanların yeteneklerinin birleşmesi ile ortaya çıkmıştır. CodeRed ile başlayan karışık tehditler kavramı, Goner, Klez, BugBear ve belki de en yıkıcısı Nimda ile devam ederek bilgisayar güvenlik dünyasını kasıp kavurmuştur. Nimda, web sayfalarına bulaşmış, bu sayfaların ziyareti sonucunda savunmasız bilgisayarlarda readme.eml dosyasının otomatik olarak indirilmesi ve çalıştırılması mümkün olmuştur. Nimda, C ve D sürücülerini paylaşıma açar ve .exe uzantılı dosyalara eklenerek bulaşır. CodeRed C/D, Sadmind ve diğerlerinin bıraktıkları açık kapıları kullanır. En yakın örneklerden olan BugBear, bulaştığı Windows makinelerin e-posta adres defterleri vasıtasıyla global ağlara kendini kopyalayarak çok hızlı bir şekilde yayılmıştır.

Mantıksal bombalar (logic bombs) / Zaman bombaları (time bombs)

Mantıksal bombalar bir tetikleyici olaya bağlı olarak Truva atları gibi yıkıcı etkiler yapabilen başka amaçlar için hazırlanmış programlar içine gömülmüş yazılımlardır. Tetikleyici olay mantıksal bombayı içeren programın çalıştırılması ile gerçekleşir. [Stephenson P., 106] Belirgin bir tarih veya sistem olayı da tetikleyici mekanizma olarak kullanılabilir. Sistem kütüklerinde değişimlere yol açan özel bir tür mantıksal bomba da vardır. İşletim sisteminin özellikle kabuk bölümünde kullanıcılar tarafından sık kullanılan yazılımların yok edilerek yerlerine aynı adlı ama başka işlevli yazılımların yerleştirilmesi bu sınıfa girer. [Koltuksuz A., 107]

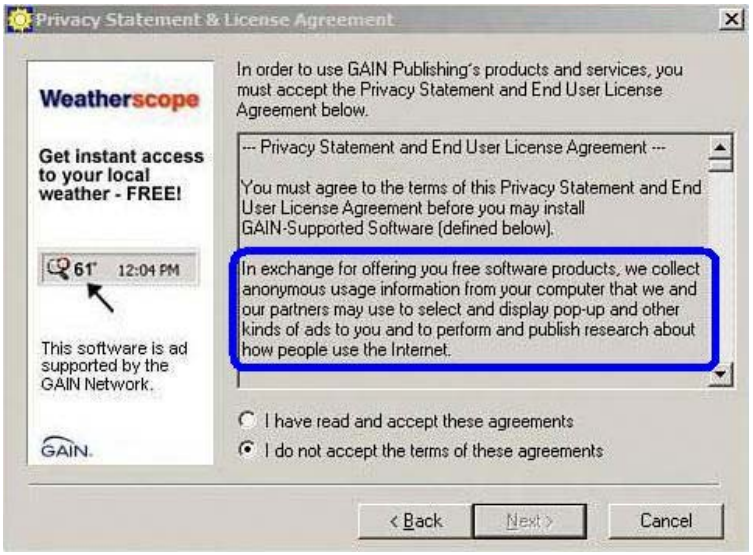
Casus yazılımlar (spyware)

Casus yazılımlar, kurbana ait bir sabit diskten kişisel bilgilerini haberi olmadan alarak başka bir bilgisayara gönderen programlardır. Casus yazılımlar, kullanıcının yaptığı işlemlerin ekran görüntülerini ve klavye ile yazdığı tüm bilgileri kayıt eder. Ayrıca kullandığı her programı takip ederek bu programların ne kadar süre kullanıldığının kayıtlarını tutar. İşverenler çalışanlarının kuruma ait bilgisayarlarda kişisel işleri için kullanıp kullanmadıklarını takip etmek, aileler çocuklarının yasak sitelere girip girmediğinden emin olmak ve saldırganlar da kurbanların kredi kartı numaralarını ve şifrelerini ele geçirmek için casus yazılımları kullanabilirler. Casus yazılımlar, virüsler, Truva atları ve solucanlarla beraber dünya çapında tehlike yaratan en büyük dört tehditten biridir.

Casus yazılımların en büyük özelliği gizlenme kabiliyetidir. Genellikle kullanıcının programı kolaylıkla sistemden kaldırabilmesi de mümkün olamamaktadır. Birçok casus yazılım kendisini sistemin açılışında çalıştırılmak üzere kurar. Yalnızca sistem kaynaklarını çalarak bilgisayarın performansını düşürmekle kalmaz, bant genişliğini de sömürerek ağ bağlantı hızını da düşürür. En yaygın casus yazılımlar, Bargain Buddy, GAIN, b3d projector, Gator, n-Case, SaveNow, Search Toolbar, Webhancer, ve Search Assistant' tır. Ayrıntılı bir listeye http://home.earthlink.net/~doniteli/index73.htm#list adresinden ulaşılabilir. [108]

Reklâm pencereleri (adware)

Program geliştiriciler hazırladıkları bir ticari yazılımın kullanıcılar tarafından denenmesi amacıyla ücretsiz (freeware) veya limitli kullanım (shareware) sürümlerini piyasaya çıkarırlar. Bu hazırlanan freeware veya shareware yazılımların yanına ekledikleri ücretsiz ayrı bir yazılımla veya içerisine kodlar eklemek suretiyle, kendisine destekleyici olan firmanın reklamını yaparlar. Bu tip küçük programlara, reklam pencereleri (adware) denir. Bunların bir kısmı, asıl programın menü barında yer alır kimisi de ayrı bir açılır pencere (pop-up) şeklinde ortaya çıkar. Bazı adware programlar ücretsiz yazılımın yanında ayrıca kurulurlar. Bu kurulum esnasında genellikle son kullanıcı lisans anlaşması (EULA) içerisinde kullanıcıyı uyarırlar. [Walker A., 109]



Şekil 4.2.4.2 : Weatherscope programının son kullanıcı lisans anlaşması ekranı

Kullanıcının, alışkanlıklarını, internette girdiği sayfaları izleyerek merkezi bir noktaya raporlamak, kullanıcıyı kendi üyesi olduğu sitelere yollayarak hit kazandırmak gibi korsan işlevleri olan genelde istenmeyen programlardır. Bu programlar kullanılmadığı veya programın sistemden kaldırıldığı durumlarda bile, mevcut yazılımın bilgileri toplamaya devam ettiği ve sunucularına gönderdiği saptanmıştır. Bu nedenle bu tür yazılımlar casus yazılımlarla aynı özellikleri göstermektedir. Bu tip yazılımların bir listesine SpywareGuide [110] ve Symantec [111] sitelerinden ulaşılabilir.

Hırsız yazılımlar (stealware)

Hırsız yazılımlara geçmeden önce gelir ortaklığı (affiliate program) programı kavramını anlamak faydalı olacaktır. Bir web site sahibi gelir ortaklığı programına katıldığında, kendisine bir dizi reklâm bandı ve link verilecek ve bunları web sayfasında yayınlaması istenecektir. Kullanıcılar bu bağlantılardan birine tıkladığında, bu işlem ortaklık yazılımı tarafından çerezler (cookie) vasıtasıyla kaydedilecek ve komisyon türüne bağlı olarak web sitesi sahibi komisyonunu alabilecektir. Eğer kendisine hırsız yazılım bulaşmış bir kullanıcı tarafından bu bağlantılara tıklanıldığında çerezler içine kayıt edilmiş gelir ortaklığı programı kimliği ve ayrıntıları hırsız yazılım tarafından

değiştirilecektir. Böylece web sitesi sahibinin alması gereken komisyonlar değişen bu bilgilerle hırsız yazılımın kontrolünü elinde tutan firmaya gönderilebilecektir.

Kazaa, Morpheus, Limewire gibi dosya paylaşım programları, ufak bir ekleme ile, online satış yapan bazı sitelerin, ortak sitelerine verdikleri komisyonları çalabilmektedirler. [112] Örneğin kullanıcı, Amazon' a bağlı alt bir siteden bir CD satın aldığında, yazılım Amazon' un sistemi kandırılmakta ve satıcı siteye verilecek olan komisyon, Kazaa' nın hesabına geçebilmektedir. Üstelik yazılımın içerdiği bu dolandırıcılık modülü, yazılım sistemden kaldırılsa bile sistemde kalıp çalışmaya devam edebilmektedir. [113]

Phishing (dolandırıcılık)

Genellikle e-posta ya da Web sitelerindeki açılır pencereler yoluyla kullanıcının karşısına çıkan ve hem kişisel hem parasal anlamda zararla sonuçlanabilme ihtimali yüksek bir bilgi hırsızlığı yöntemidir. Bu yolla kullanıcıların kişisel bilgilerini veya finansal şifrelerini çalmak için, banka, servis sağlayıcı ve devlet kurumları gibi hizmet alınan kurumların kurumsal kimliğini taklit eden mesajlar göndermektedirler. Tüm bu mesajların ortak amacı, bir nedenle kullanıcının hesabı ile ilgili bilgilerin güncellenmesi gerektiği konusunda onu ikna edebilmektir. Örneğin; kullanıcının sürekli alışveriş yaptığı bir siteden geliyormuş gibi bir mesaj gönderilmekte ve kullanıcının hesabına ait şifre bilgilerinin değiştirilmesi gerektiğini söylemektedir. Ayrıca gelen e-postada kullanıcının hızlı karar verip dikkatini dağıtmak için de üyeliğinin askıya alınacağı gibi bir an önce işlem yapmasını gerektiren bir ortam yaratılıyor. Kullanıcı çabuk karar verip mesajda yer alan sahte bağlantıya tıkladığında, bu sitenin taklit edilmiş bir kopyasına yönlendiriliyor. Yönlendirilen sahte sitedeki ilgili boşluklara kişisel bilgiler girildiği anda kullanıcıya ait tüm bilgiler karşı tarafın eline geçmiş oluyor.

E-posta kullanım oranının çok yüksek olması bu tür online dolandırıcılık işlemlerinin e-posta yoluyla gerçekleşmesinde temel etmenlerden biridir. Phishing ataklarındaki önemli artış internet tarayıcı uygulamalarının (Internet Explorer, Mozilla Firefox, Opera vb.) güvenlik sorunlarını da ön plana çıkarmıştır. [114]

Phishing saldırılarının bu kadar hızla yayılmasının en büyük sebebi dolandırıcıların banka hesaplarını ve kimlik bilgilerini ele geçirerek karşılığında büyük kazançlar elde etmesidir. İşin kötü yanı her yıl artan sayıda kullanıcıların bu tuzaklara düşüyor olmasıdır. Hızla artmasına rağmen bu tip saldırılardan korunmak zor değildir. Antispam yazılımları, e-posta istemcilerine ve tarayıcılara ilave edilen yazılımlar birçok phishing girişimini yakalayabilmektedir. Aslında en iyi korunma yolu, ne kadar masum görünürse görünsün, bir finans kurumundan geldiğini iddia eden ve kişisel bilgilerle ilgili düzenlemeler isteyen postaları tıklamamaktır. Dolandırıcıların ne kadar zeki olduğu düşünülürse gelen postanın gerçek veya sahte olup olmadığını anlamak oldukça zordur. [Gralla P., 115]

5. GÜVENLİK ARAÇLARI

Bir önceki bölümde ayrıntıları ile açıklanmış tehdit ve saldırılara karşı kurum içerisinde güvenliği sağlayabilmeyi, kurum ihtiyaçlarını karşılayabilecek uygun güvenlik araçlarına yatırım yapılması, politikaların oluşturulması ve uygulanması, kurum güvenlik bilincini ve farkındalığını sağlayacak eğitimlerin verilmesi olarak üçlü bir temele oturtabiliriz.

Bu konuda yatırım yapılırken bilinçli ve planlı hareket edilmelidir. Kurum ihtiyaçları belirlenip yapılacak satın alma kararından önce ayrıntılı bir araştırma yapılmalıdır. Genellikle aynı yapıya ve hacme sahip olan kurumlarda, kurumlar arasında daha önceden bilgi alışverişinde bulunularak destek alınması, avantaj ve dezavantajların denenmiş olmasından dolayı benzer sistemlerin kullanılması, uygun bir çözüm olarak görünmektedir. Kutu çözümler veya ticari yazılımlar ilk bakışta daha cazip görünebilir. Teknik bilgi gereksinimleri göz önüne alındığında uygun bile olabilir. Fakat açık kaynak (open source) yazılım alternatifini, genelde ücretsiz ve bütçenin kısıtlı olduğu durumlar için ideal olmaları nedeniyle maliyet ve verimlilik açısından değerlendirmeden karar vermemek gerekir. Açık kaynak kod dünyasında uzun zamandır kullanılan, belli bir kararlılığa ulaşmış ve kendini ispatlamış birçok güvenlik yazılımı bulunmaktadır. [116] Açık kaynak kodlu yazılımların avantajlarına, aşağıdakiler örnek olarak verilebilir:

- Bu güvenlik yazılımları ile ilgili hem Türkçe hem de İngilizce yeterince belge de bulunabilmektedir. (Bkz. www.enderunix.org, www.belgeler.org, www.acikkaynak.org)
- Hataları herkes tarafından kısa sürede fark edilebilir ve kısa sürede giderilebilir, kaynak kodlarında her türlü arka kapı ve kötü amaçlı kodlar kolayca fark edilebilir.
- Ayrıca istenildiği oranda özelleştirilip, ekleme ve çıkarmalar yapılabilir olması da başka bir avantajıdır.

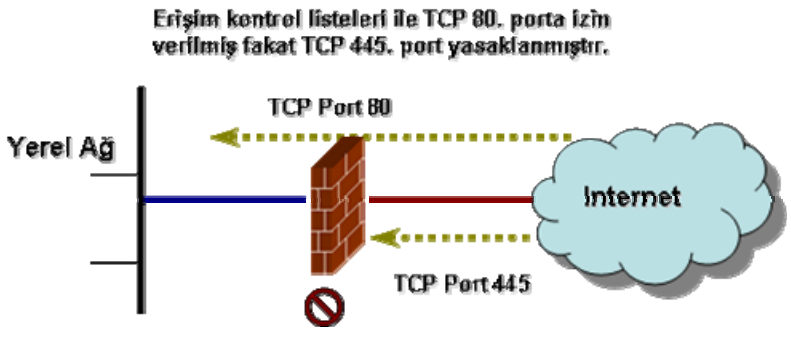
Tabii en uygunu her iki uygulamayı da dengeli bir şekilde kullanabilmektir.

5.1. GÜVENLİK DUVARLARI

Yapı teknolojisinde güvenlik duvarları (firewall=ateş duvarı), çıkabilecek bir yangının, binanın bir bölümünden diğerine yayılmasını engellemek için kullanılır. Teorik olarak bir internet güvenlik duvarı da benzer bir amaca hizmet eder; internet üzerinden gelip ve iç ağımıza yayılabilecek tehlikeleri önler. Pratikte ise daha çok ortaçağ kalelerinin su dolu hendekleri gibidir:

- Girmek isteyen kişileri dikkatlice kontrol edilen bir noktadan geçmeye zorlar.
- Saldırganların savunma hattımıza yaklaşmalarını önler.
- Ayrılmak isteyen kişileri dikkatlice kontrol edilen bir noktadan gitmeye zorlar. [Zwicky Elizabeth D. ve diğ., 117]

Güvenlik duvarı ağ güvenlik mimarisinin yapı taşlarından biri olarak kurum yerel alan ağı (güvenlik duvarının iç tarafı) ile internet (güvenlik duvarının dış tarafı) arasına konan ve çeşitli haklar düzenleyerek veri alış veriş trafiğini sınırlandıran yazılım veya donanım temelli bir ağ güvenlik sistemidir. [118] Güvenlik duvarının ana amacı, giren ve çıkan trafiği incelenmek ve değerlendirmek amacıyla bir geçitten geçirmeye mecbur bırakarak kurumsal bir ağ erişim politikası uygulanmasını sağlamaktır. Güvenlik duvarının sistem üzerinde tam olarak etkili olabilmesi için, ağ ortamı ile internet arasındaki tüm trafiğin güvenlik duvarı üzerinden geçirilmesi gerekir. [Çölkesen R., 119]



Şekil 5.1.1 : Ağ güvenlik duvarı, erişim kontrol listelerini uygular

Güvenlik duvarları kullanıcının erişim kontrol gereksinimlerini tanımlamasına olanak tanır ve sadece bu gereksinimleri karşılayan trafik veya veriler, güvenlik duvarından (ağ

temelli güvenlik duvarı) geçebilir. Şekil 5.1.1. de ağ temelli güvenlik duvarı kullanılarak trafiğin nasıl sadece korunan kaynaklara erişimine izin verildiğine örnek gösterilmiştir.

Temelde bir güvenlik duvarının aşağıdaki görevleri gerçekleştirmesi gerekir:

- Ağ trafiğini yönetir ve kontrol ederler.
- Kaynakları korurlar.
- Bir aracı gibi davranırlar.
- Giren ve çıkan trafiği kayıt eder ve raporlarlar.
- Ağa erişimi denetlerler.

5.1.1. Güvenlik Duvarı Uygulamaları

Ağ Adres Dönüşümü (NAT)

IP adres kavramı tasarlandığında bol miktarda adres olduğu ve fazlasıyla yeterli olduğu düşünülmüştü. Teoride IPv4 için en fazla 4,294,967,296 (2^{32}) adet gerçek (unique) IP adresi vardır. IP adreslerinin sınıflara ayrılmış ve bazılarının test veya özel amaçlar için rezerve edilmiş olması, kullanılabilir IP adreslerinin adedini daha da azaltmıştır (ortalama 3,3 milyar). İnternetin yaygınlaşması, ev ve işyeri ağlarının sayısındaki artış kullanılabilir IP adreslerini hızla tüketmiştir. Bunun en büyük sebebi de ağları daha küçük parçalarına bölerken açığa çıkan kullanılamayacak IP adreslerinden dolayı yaşanan kayıplardır. Sonuç olarak hiçbir IP adresi boşa harcanmasa bile mevcut IP adresleri hızla gelişen teknolojinin doğurduğu artan ihtiyacı karşılayamayacaktır.

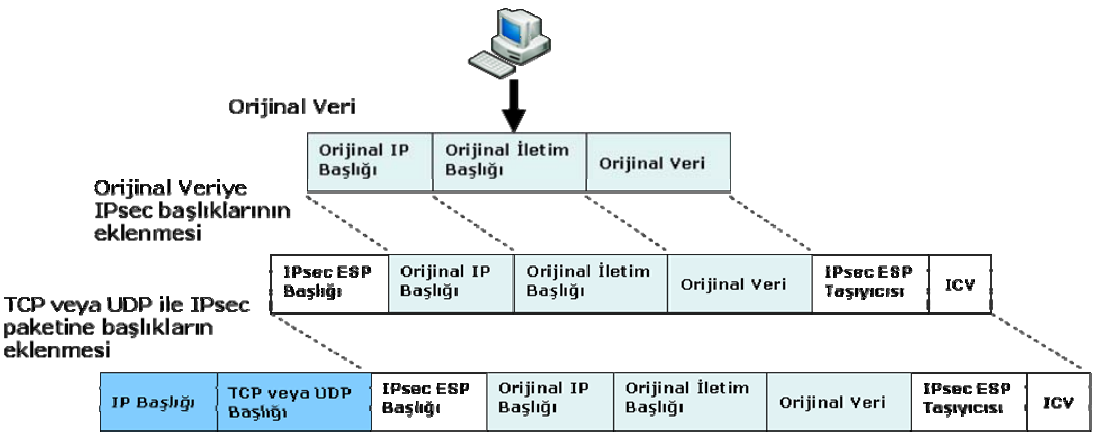
Daha fazla adres oluşturulmasına imkan tanıyan yeni bir tasarım geliştirmek bu adres krizine uzun vadede çözüm olacaktır. IPv6 adı verilen bu yeni tasarım birçok yeni ağ tarafından desteklenmektedir. Günümüzde internet altyapısını oluşturan yönlendiriciler yapılan güncellemeler ile bu yeni standardı tam olarak desteklemektedirler. Geçen zamana rağmen birçok ağ hala IP v4 adres şemasını kullanmaktadır.

IP adres krizine kısa vadede diğer bir çözüm ise bir yönlendirici veya güvenlik duvarı gibi tek bir cihazın Internet ile yerel ağlar arasında bir aracı rolü üstlenerek ağ adres dönüşümünü yapabilmesidir. Bu da tek bir gerçek IP adresi ile bütün bir ağın temsil edilebilmesi anlamına gelir. Bu durum NAT kullanılmasının sebeplerinden sadece

biridir. NAT sayesinde dış ağlara, ağın büyüklüğü, bu ağdaki cihazların tipleri, sayısı, ağın yapısı vb. konular hakkında herhangi bir bilgi gitmez. Böylece dış ağlardan gelebilecek saldırıları zorlaştırır ve belli bir miktarda güvenlik sağlar. NAT işlemini RFC 3022 [120] ve RFC 2663 [121] standartları tanımlar.

NAT Traversal (NAT-T)

NAT işlemi, veri paketini dönüşüm esnasında değiştirmesi nedeniyle IPsec uygulamalarında problem yaratır. IPsec in doğasından dolayı, NAT kullanılarak veri paketi yeniden oluşturulduğunda, alıcı güvenlik duvarı veya yönlendirici verinin değişmiş olduğunu (kaynak IP adres artık doğru kaynak IP adres değildir) saptar ve paketi çöpe atar. Bu sorunu ortadan kaldırmak için NAT traversal (NAT-T) işlemi geliştirilmiştir. NAT-T, TCP veya UDP paketi olsun bütün IPsec paketini *frame* ler içerisine yerleştirir (encapsulation). Bunu yaparken, orijinal IPsec verisinin değişmiş olması dikkate alınmaksızın trafik istendiği gibi dönüştürülür. Şekil 5.1.1.1. bu encapsulation işlemini göstermektedir. RFC 3947 standardı NAT-T işlemini tanımlar. [122]



Şekil 5.1.1.1 : NAT-T Encapsulation

NAT Terminolojisi

NAT işlemini, terminolojisinin üzerinden geçmeden açıklamak oldukça zordur. NAT birçok farklı şekilde uygulanabilir. NAT işlemi esnasında IP adreslerinin birçok değişik yolla kullanımı mevcuttur. NAT işlemini doğru bir şekilde uygulayabilmek için bazı tanımların yapılması gerekir. [Albanese J. ve Sonnenreich W., 123]

- **Kayıtlı (registered) ve kayıtsız (unregistered) IP adresleri:** Herkes tarafından erişilebilir IP adresleri *Internet Assigned Numbers Authority* (IANA) tarafından kayıt altında tutulur. Bu kurum genellikle geniş IP adres bloklarını, müşterilerine dağıtması amacıyla internet servis sağlayıcılarına (ISP) kayıt eder. Bir kısım kayıt altına alınmamış adres blokları ise iç ağlarda özel kullanımlar için ayrılmıştır. Bu ayrılan kayıt altına alınmamış adreslerin sadece yerel ağlarda kullanımı mümkün olup, internet ortamında hiçbir anlamları yoktur.

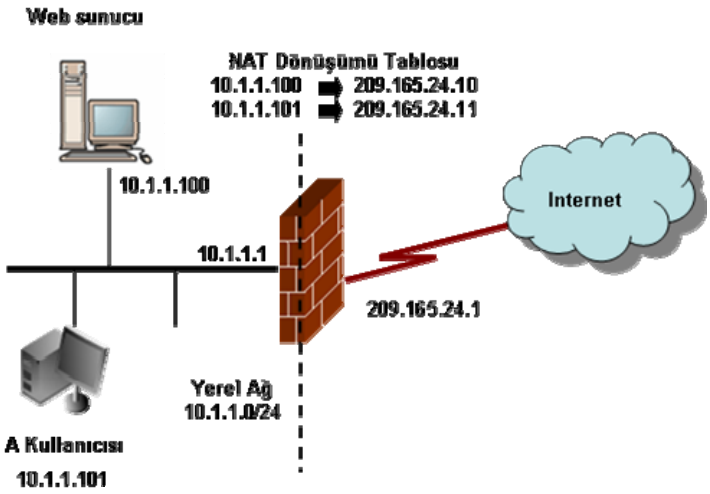
  Özel IP adresleri [124]:

  10.0.0.0 – 10.255.255.255

  172.16.0.0 – 172.31.255.255

  192.168.0.0 – 192.168.255.255

- **Global IP adresleri:** Bunlar internet üzerindeki herhangi birinin erişimine olanak sağlayan kayıt altına alınmış IP adresleridir. NAT kullanarak bir ağa global adresler atanmışsa bunlara iç taraf global adresler denir. Bu IP adreslerine gönderilen tüm paketler NAT yönlendiricisi tarafından işleme tabi tutulur. Internet üzerindeki diğer tüm adresler dış taraf global adresler olarak adlandırılır.
- **Yerel adresler:** NAT kullanılarak erişilebilen bir ağın iç tarafında yer alan IP adresleridir. Genelde kayıt altına alınmamış adreslerdir. NAT yönlendiricileri tarafından kullanılan çok az bir kısmına dış taraf yerel adresler denir. İç ağda kullanılan geri kalan kısmına iç taraf yerel adresler denir.
- **Statik NAT:** Bir iç taraf global adres ile bir iç taraf yerel adresin NAT tablosunda birebir eşleştirilmesi ile gerçekleşir. Statik NAT ağın dışındaki cihazların iç ağdaki bilgisayarlara bağlantı başlatmasını sağlar. Bu iç ağdaki bir sunucunun dış ağdan erişimini sağlayabilmek için özellikle kullanışlı bir yöntemdir. Şekil 5.1.2.1. deki örneğe göre statik NAT sayesinde iç taraf yerel adresi 10.1.1.100 olan bir web sunucusuna 209.165.24.10 iç taraf global adresi vasıtasıyla ulaşılabilmektedir.



Şekil 5.1.1.2 : Statik NAT ve Internet erişimine bir örnek

- **Dinamik NAT:** Bu tip NAT işleminde, birebir eşleşmeler yerine bir global IP adres havuzu bulunur. İç ağdaki kullanıcı, ilk gelen ilk dönüşür mantığıyla havuzdaki en düşük global IP adresini alarak internete çıkar.

#nat (inside) 1 10.1.1.50-10.1.1.99 netmask 255.255.255.0

Bu komutla dönüşüme uğrayacak yerel adresler tanımlanır.

#global (outside) 1 209.165.24.50-209.165.24.99 netmask 255.255.255.0

Bu komutla yerel adreslerin dönüşeceği global IP adres havuzu tanımlanır.

Örneğin 10.1.1.55 adresli kullanıcı internete bağlanmak isteyen ilk kullanıcı olsun. Havuzdan alacağı IP adresi 209.165.24.50 olacaktır. Bir sonraki iç ağ kullanıcısının alacağı adres 209.165.24.51 olur ve bu böyle devam eder. Bu statik bir dönüşüm değildir ve dönüşüm **timeout xlate hh:mm:ss** komutu ile tanımlanan hareketsiz kalma süresi (period of inactivity) dolunca sona erer.

- **Port Adres Dönüşümü (PAT):** Eğer iç ağda mevcut global adreslerden daha fazla kullanıcı var ise havuz dolar ve geri kalan kullanıcılar port adres dönüşümü vasıtasıyla internete çıkmaları mümkün olur. Eğer **global** komutunun yanında bir havuz yerine tek bir IP adresi tanımlanmışsa bu adres, port dönüşümüne uğramıştır. Bu sayede tek bir global IP adresi ile 65,535 kullanıcıya bağlantı sağlanabilir.

#global (outside) 1 209.165.24.100

Bu komut ile PAT işlemi uygulanacak global IP adresi tanımlanır.

PAT kullanımında dikkat edilecek birkaç husus vardır: [125]

- PAT için tanımlanan IP adresi başka bir global adres havuzu içerisinde bulunamaz.
- PAT işlemi H.323 uygulamaları, isim sunucularının bellekte tutulması ve Point-to-Point Tunneling Protocol (PPTP) ile beraber çalışmaz. PAT, alan adı hizmeti (DNS), dosya transfer protokolü (FTP) ve pasif FTP, http, posta, uzaktan işlem çağırımı (RPC), rshell, telnet, içerik filtreleme ve dışarı doğru traceroute işlemleri ile birlikte çalışır.
- Güvenlik duvarı üzerinden geçen multimedya uygulamalarında PAT kullanılmamalıdır. Multimedya uygulamaları PAT tarafından sağlanan port eşleşimi ile çakışmalar oluşturacaktır.
- Global komutu ile tanımlanan global adres havuzundaki IP adreslerine sahip sunuculara dışarıdan erişimin mümkün olabilmesi için ters DNS girişlerinin yapılması gerekir. Ters DNS eşleştirmesi için her global adres için adres-isim eşleştirmesinin yer aldığı DNS Pointer (PTR) kayıtları kullanılır.

Örneğin, global IP adresi 209.165.24.10 ve deneme sunucusu için alan adı deneme.test.com olan bir PTR kaydı;

10.24.165.209. in-addr.arpa. IN PTR deneme3.test.com

11.24.165.209. in-addr.arpa. IN PTR deneme4.test.com şeklinde olur ve böyle devam eder.

Perdelenmiş Alt Ağ (DMZ)

DMZ (Demilitarized Zone), güvenlik duvarı tarafından daha az korunan, daha fazla erişime izin verilen bir bölgedir. Güvenlik duvarına üçüncü bir ağ arayüzü eklenmesi ve internete servis verecek olan sunucuların buraya konulması ile oluşturulur. [125]

DMZ kullanımı güvenlik anlayışına çok katmanlı yaklaşımın yaygınlaşmasıyla beraber ihtiyaç duyulan bir yöntem haline gelmiştir. Sadece güvenlik duvarı, NAT ve paket süzme elemanlarından oluşan tek yönlü koruma metodu yöneticiye tüm bağlantıların

hizmet veya protokollerini tamamen kesme veya izin verme dışında başka bir seçenek sunmaz. Bu da yapılan işlemin esnekliğini yok eder. Bu esnek olmayan uygulama ise bilgi güvenliğinin süreklilik (availability) ilkesinin her zaman sağlanamaması demektir. İşte bu noktada DMZ yapısı, gereken esnekliğin yanında, yöneticiye iyi bir güvenlik sistemi oluşturması ve ihtiyacı duyduğu hizmetlerin kesintisiz olarak sağlanması konusunda büyük katkıda bulunur.

DMZ in farklı bir güvenlik seviyesinde oluşturulmasından dolayı saldırganlar bu bölgeden iç ağa geçiş yapamazlar. Ayrıca oluşturulacak erişim listeleri ile DMZ bölgesine iç ağdan erişim sınırlandırılabilecek ve belli bir miktarda koruma sağlanacaktır.

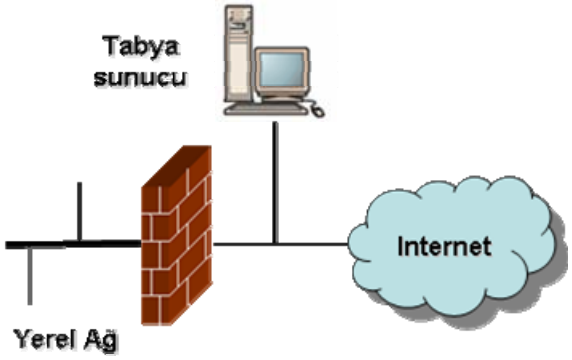
DMZ bölgesine yerleştirilen, dışarıdan rahatla erişilebilecek web, mail ve ftp gibi sunucular, ilave güvenlik önlemleri ile güçlendirilirler. Bu nedenle bu güvenliği sıkılaştırılmış sunuculara tabya sunucu (bastion host) denir. [126]

Temel DMZ yerleşimleri

a) **Tek güvenlik duvarı**:

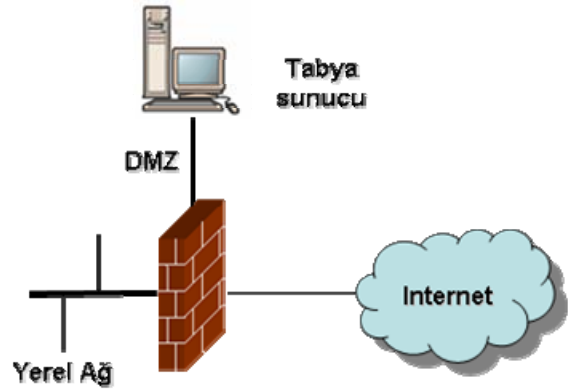
Şekil 5.1.1.3 : Tek güvenlik duvarı yerleşimi

b) **Tabya sunucu ile tek güvenlik duvarı**:



Şekil 5.1.1.4 : Tabya sunucu ile beraber tek güvenlik duvarı yerleşimi

c) **Tabya sunucu ile beraber perdelenmiş alt ağ (DMZ) güvenlik duvarı**:



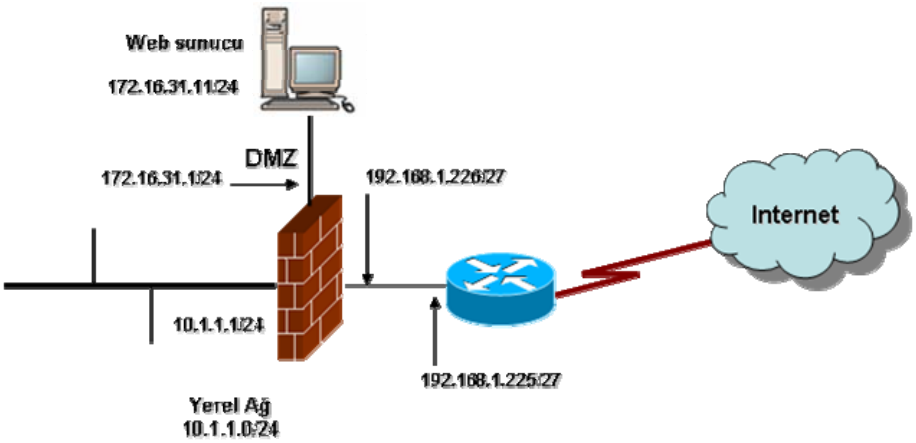
Şekil 5.1.1.5 : Tabya sunucu ile beraber perdelenmiş alt ağ (DMZ) güvenlik duvarı yerleşimi

Çeşitli tipte DMZ uygulamalarının avantaj ve dezavantajlarına ait ayrıntılar Tablo 5.1.3.1. de görülebilir. [Shimonski Robert J. ve diğ., 127]

Tablo 5.1.1.1 : Temel DMZ yerleşimlerinin avantaj ve dezavantajları

Temel Yerleşim	**Avantajları**	**Dezavantajları**	**Uygun kullanım**
Tek güvenlik duvarı	Ucuz, oldukça kolay yapılandırma, az bakım	Çok daha düşük güvenlik kabiliyeti, büyüme veya genişleme potansiyeli yok	Diğerlerine hizmet sağlamayan ev, küçük ofis-ev ofis (SOHO) ve küçük işletmeler
Tabya sunucu ile tek güvenlik duvarı	Daha sağlam alternatiflerine göre daha düşük maliyet	Tabya sunucu saldırılara karşı oldukça savunmasız, içerik güncellemesine elverişsiz, olmazsa olmaz hizmetler harici işlevselliği düşük, sonuç ihtiyaçlar karşısında genişleyemez	Daha sağlam uygulamalar için kaynakları olmayan küçük işletmeler veya sık güncelleme gerektirmeyen statik içerik sağlanması durumunda
Tabya sunucu ile perdelenmiş alt ağ (DMZ) güvenlik duvarı	Savunmasız bir tabya sunucunun potansiyel saldırıya uğrama ihtimaline karşın güvenlik duvarı hem iç ağa hem de tabya sunucuya koruma sağlar.	Tek nokta başarısızlığı; bu yapılandırmada bazı ürünler, DMZ için ağ adreslerinin gerçek adreslere dönüşümünü sınırlandırıyor, bu hem ekonomik değil hem de ağ uygulamaları için olanaksız	Bilgilerini güncelleyebilmesi için tabya sunucuya erişimi gereken ağlar

Örnek DMZ uygulaması



Şekil 5.1.1.6 : Örnek DMZ Uygulaması

Örneğimizden yola çıkarak güvenlik duvarı temel komutları aşağıdaki gibi oluşturulabilir.

```
interface Ethernet0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

interface Ethernet1
nameif outside
security-level 0
ip address 192.168.200.226 255.255.255.224

interface Ethernet2
nameif dmz
security-level 10
ip address 172.16.31.1 255.255.255.0

access-list dmz_int extended permit tcp host 172.16.31.11 any eq
http
```

Örneğimizde DMZ bölgesinin güvenlik düzeyi 10 belirlenerek iç tarafın ve dış tarafın güvenlik düzey değerleri arasında bir değer verilmiştir. Ayrıca 172.16.31.11 web sunucusuna sadece http portundan ulaşılabilmesi için de bir erişim kontrol listesi yazılmıştır.

Sanal Özel Ağ

Sanal Özel Ağ (Virtual Private Network : VPN), mevcut halka açık veya paylaşımlı bir ağ yapısı (WAN bağlantıları, internet gibi) üzerinde taşıdığı verinin güvenliğini sağlamak amacıyla şifreleme (encryption) veya kimlik denetimi (authentication) teknolojilerini kullanarak kurulan bir bağlantı biçimidir. Bir VPN bağlantısının arkasında yatan temel fikir şifreleme kullanarak ağın birçok farklı katmanında bir iletişim kanalını güvenli hale getirmektir. VPN bağlantıları kullanıcıdan kullanıcıya, kullanıcıdan ağ geçidine, ağ geçidinden ağ geçidine olmak üzere üç temel yapıda sınıflandırılabilir. [Northcutt S. ve diğ., 128]

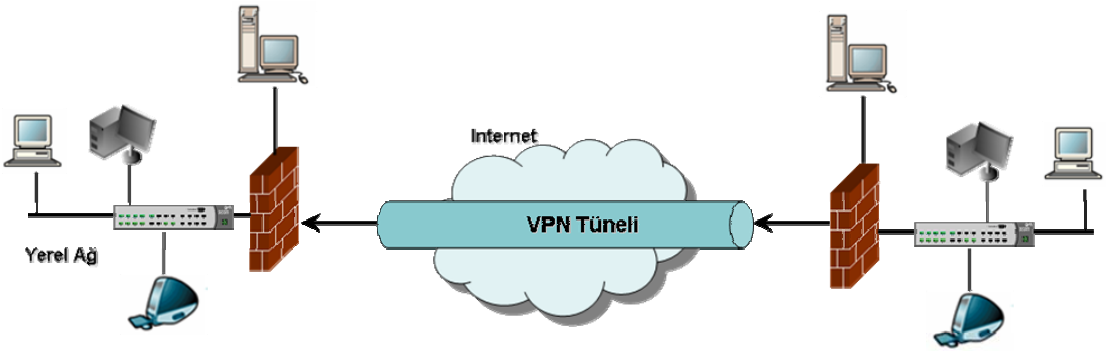
Uygulama katmanında Pretty Good Privacy (PGP) gibi programlar ile veya Secure Shell (SSH) gibi kanallar boyunca şifreleme uygulanabilir. Ayrıca uzak bağlantıları koruyabilmek için pcAnywhere gibi tek oturumlu uzaktan erişim veya Terminal Sunucu gibi çok oturumlu programlar şifreleme ile kullanılabilirler. Bu programların çoğu kullanıcıdan kullanıcıya VPN sınıfına girerler.

İletim katmanında, Secure Socket Layer (SSL) gibi protokoller kullanılır. [129] Bu tip bağlantı genellikle web tarayıcılar vasıtasıyla kullanılır. SSL ayrıca, Stunnel [130] denilen bir yazılım kullanarak diğer iletişim oturum şekilleri için bir tünel oluşturucu gibi de kullanılır.

Ağ katmanında IPsec gibi protokoller sadece paketin veriyi taşıyan kısmını şifrelemez bunun yanında TCP/IP bilgisini de şifrelerler. Paketler şifrelenirken veya şifresi çözümlenirken IP adres bilgisi doğru yönlendirme yapılabilmesi için gereklidir. Hedef sistemin IP adres bilgisi, eğer şifrelemeyi yönlendirici, güvenlik duvarı veya toplayıcı (concentrator) gibi bir ağ geçidi cihazı tarafından yapılıyorsa tünel oluşturma (tunneling) tekniği kullanılarak ta saklanır.

Veri iletim katmanında Point-to-Point Protokolü (PPP) üzerinden gönderilen paketlerin şifrelenmesi için PPP ye Layer 2 Tünel Oluşturma Protokolü (L2TP) ilave edilir. [131]

Şekil 5.1.1.7 de iki ağın her iki tarafında güvenlik duvarları ile sonlandırılan bir VPN bağlantısı görülmektedir.



Şekil 5.1.1.7 : İki ağın birbirine internet üzerinden sanal bir tünel vasıtasıyla bağlanması

VPN kısaca; gönderilmek istenen veriyi özel bir iletişim ağından diğerine göndermeden önce, hedef ağın veriyi göndermesi gereken ağ olup olmadığını kontrol etmekte, gönderilecek veriyi şifrelemekte ve iki ağ arasında sanal tünellere koyup, hedef sisteme göndermektedir.

Üniversite ortamlarında VPN; IP adresleri ile sınırlandırılmış ve lisanslandırılmış elektronik dergi ve veritabanlarına, dosya sunucularına, sadece yerel ağ kullanımına açık istemci-sunucu mantığıyla çalışan programlara, güvenlik duvarından engellenmiş ağda paylaştırılmış kaynaklara ve akademik amaçlı uzak masaüstü bağlantı erişimini sağlamak amacıyla kullanılabilmektedir.

5.1.2. Güvenlik duvarı çeşitleri

Güvenlik duvarları kontrol ettikleri protokol seviyelerine göre sınıflandırılabilirler. Bunlar; paket süzen güvenlik duvarı, devre düzeyli ağ geçidi, uygulama seviyeli güvenlik duvarı ve bu üçünün birleşiminden meydana gelen durum denetlemeli çok katmanlı güvenlik duvarlarıdır.

Paket Süzen Güvenlik Duvarı

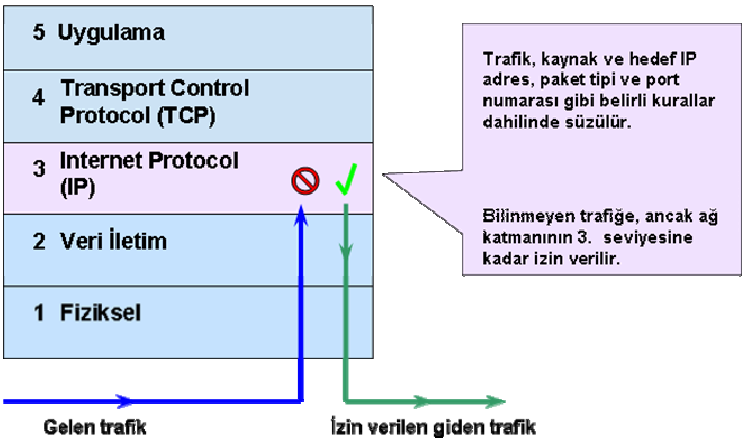
Paket süzen güvenlik duvarları genelde bir yönlendiricinin (router) parçasıdırlar. Yönlendirici, paketleri bir ağdan alıp diğerine ileten cihazlardır. Paket süzen güvenlik duvarları OSI modelinin ağ katmanında veya TCP/IP protokolünün IP katmanında erişim kontrol listeleri (Access Control List: ACL) kullanarak çalışırlar. Erişim kontrol

listeleri güvenlik duvarının gelen paketlere karşı uyguladığı text tabanlı kurallar setidir. Bu kurallar, kaynak ve hedef IP adres, kaynak ve hedef port numarası ve kullanılan protokollerden oluşur. Aşağıda trafiği süzmek amacıyla oluşturulmuş basit erişim kontrol listeleri görülmektedir.

access-list 101 permit icmp any 192.168.185.0 0.0.0.255 echo-reply
access-list 101 permit icmp any 192.168.185.0 0.0.0.255 ttl-exceeded
access-list 101 permit tcp any 192.168.185.0 0.0.0.255 established
access-list 101 permit udp any host 192.168.185.100 eq 53
access-list 101 permit udp any eq 123 192.168.185.0 0.0.0.255

Gelen tüm paketler erişim kontrol listeleriyle karşılaştırılır, eğer uyumlu bir satır bulunursa bu satırdaki hüküm sonucunda izin verilir (permit) veya ret edilir (deny). Eğer gelen paketlerle ilgili bir satır bulunmuyorsa tamamıyle ret edilir.

Düşük maliyeti ve ağ performansına etkisinin düşük olması paket süzen güvenlik duvarlarının avantajlarıdır. Birçok yönlendirici paket süzmeyi destekler.



Şekil 5.1.2.1 : Paket süzen güvenlik duvarının TCP/IP modeli üzerinde çalışma ortamı

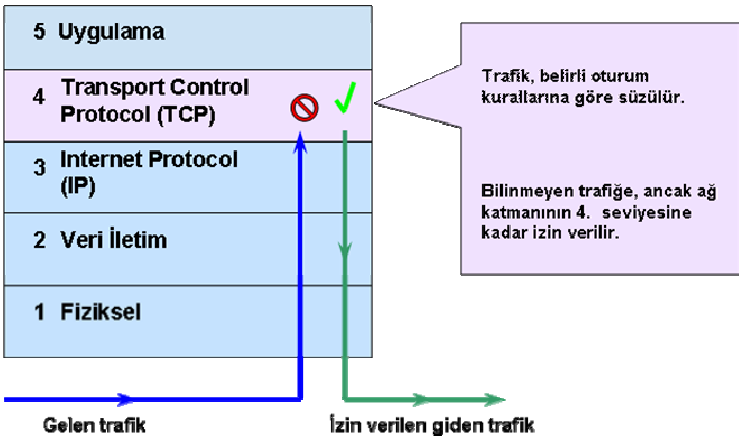
Bu tip güvenlik duvarları sadece ağ katmanında çalıştıklarından karmaşık kural tabanlı modelleri desteklemezler bu onların çok daha hızlı olmasını sağlar. İki bilgisayarın birbirleriyle iletişime geçtikleri anda oluşturulan TCP oturum bilgilerinin takibini yapmazlar. Bilgisayarlar TCP kullanarak birbirleriyle iletişime geçtiklerinde ilk olarak TCP oturumunun kurulabilmesi amacıyla three-way handshake adı verilen bir dizi işlem

kullanır. Bu oturumların paket süzen güvenlik duvarlarıyla takip edilmemesinden dolayı iç ağdaki bilgisayarlar, değiştirme (spoofing) tehlikesine karşı savunmasızdırlar.

Spoofing: Bir saldırganın bir standart paket süzen güvenlik duvarını devre dışı bırakmak niyetiyle IP paketlerinin kaynak bilgilerinin değiştirilmesi işlemidir. Güvenlik duvarı paketi inceler, kaynağı (değiştirilmiş) belirler, kabul eder ve geçirir. Bu da saldırgana saldırısını normal bir trafikmiş gibi gizlemesine (spoof) olanak sağlar. [Newman Daniel P., 132]

Devre düzeyli ağ geçidi (circuit-level gateway)

Devre düzeyli güvenlik duvarı OSI modelinin oturum katmanında veya TCP/IP modelinin TCP katmanında çalışırlar. Talep edilen oturumun doğru ve kurallara uygun olup olmadığını tespit için TCP iletişim kurma (handshaking) işlemini gözlerler. Karşıdaki bilgisayara giden bilgiler sanki devre düzeyli güvenlik duvarı tarafından üretiliyormuş gibi görünür. Bu korunan ağ için bilgilerin saklanması hususunda faydalı bir uygulamadır. Ancak kişisel paketleri süzmezler. [Noonan W. ve Dubrawsky I., 133]

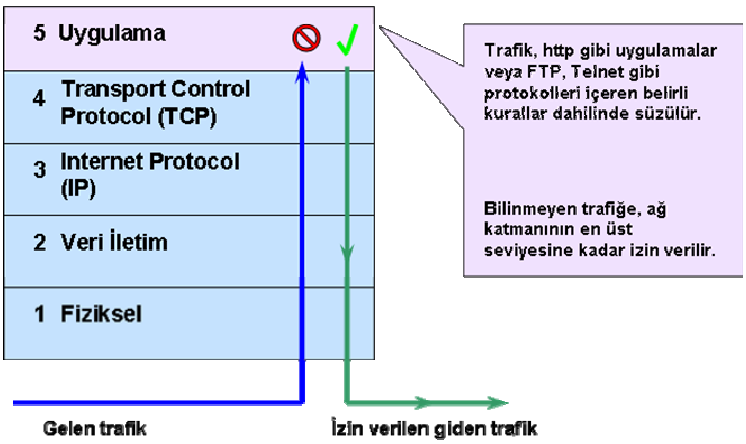


Şekil 5.1.2.2 : Devre düzeyli güvenlik duvarının TCP/IP modeli üzerinde çalışma ortamı

Bu türde oturum bir kez kurulup kabul edildikten sonra, her paket için denetim yapılmaz; paketler kurulan sanal devre üzerinden akar. Oturum kurulurken ilgili port sınamaları yapılır ve oturum kurulduktan sonra o portu, oturumun kurulmasını başlatan taraf sonlandırana kadar sürekli açık tutar.

Uygulama Düzeyli (Application-level) Güvenlik Duvarı

Uygulama düzeyli güvenlik duvarları, proxy de denilebilir, OSI modelinin uygulama katmanında paketleri süzer. Bir proxy hizmeti kullanıcıdan aldığı internet isteklerini alıp kullanıcı adına yürütür ve sonucu yine kullanıcıya iletir. Bir web proxy olarak yapılandırılan güvenlik duvarı, uygulama katmanında paketleri incelediğinden http:post ve get gibi uygulamaya özgü komutlarla süzer, bu nedenle ftp, gopher, telnet veya diğer trafiklerin geçmesine izin vermez. Bu tip güvenlik duvarları ayrıca kullanıcı hareketlerini ve oturum açma bilgilerini kaydetme (log) de kullanılır. Yüksek seviyede güvenlik sunarlar fakat ağ performansında da önemli bir düşüşe sebep olurlar.



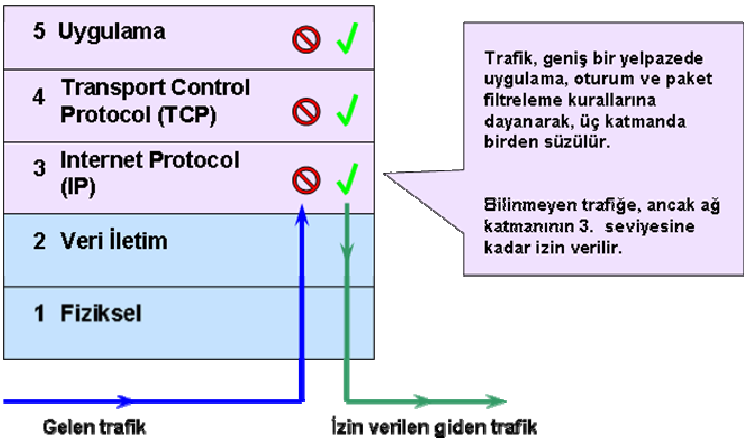
Şekil 5.1.2.3 : Uygulama düzeyli güvenlik duvarının TCP/IP modeli üzerinde çalışma ortamı

Durum denetlemeli çok katmanlı (stateful inspection multilayer) güvenlik duvarı

Durum denetlemeli çok katmanlı güvenlik duvarı diğer tip güvenlik duvarlarının özelliklerinin birleşiminden meydana gelmiştir. Bu sayede iletim, oturum ve ağ katmanlarından topladığı bilgilerle denetlediği protokolleri çok daha iyi anlayabilmektedir. Bu durum UDP veya RPC tabanlı uygulamalardaki gibi bağlantı sürekliliği gerektirmeyen protokolleri takip edebilmek amacıyla sanal oturumlar yaratma becerisi sağlar. Bu güvenlik duvarları trafiği, paket süzen güvenlik duvarlarının çalışma mantığında olduğu gibi süzerler. Ayrıca kurulan oturumun geçerli olduğundan emin olmak için oturum kontrolleri yaparlar fakat paketlerin içeriğine bakmazlar. Kullanıcılara üst seviyede bir güvenlik ve yüksek performans sağlarlar. Ayrıca pahalı olmalarının yanında karmaşık yapıları nedeniyle bilgi düzeyi yüksek personel tarafından

yapılandırılmadıkları sürece benzer tipteki güvenlik duvarlarına göre daha az güvenlik sağlayabilecektir.

Durum denetleme (stateful inspection) kavramı Check Point Yazılım Teknolojileri firması tarafından 1990 lı yılların ortalarında keşfedilmiş ve kurumsal anlamda ağ güvenlik çözümlerinde hızla bir endüstri standardı haline dönüşmüştür. [134] Günümüz güvenlik duvarlarının çoğunda bu teknoloji kullanılmaktadır.



Şekil 5.1.2.4 : Durum denetlemeli çok katmanlı güvenlik duvarının TCP/IP modeli üzerinde çalışma ortamı

Bir dinamik ve durum bilgili paketleri değerlendiren güvenlik duvarları, aktif TCP oturumlarının ve sahte UDP oturumlarının bir tablosunu tutar. Bütün oturumların kaynak ve hedef IP adreslerini, port numaralarını ve o an ki TCP sequence numarasının kaydını tutar. Girişler, ancak tüm o TCP veya UDP bağlantıları, tanımlanan güvenlik politikasını sağlıyorsa yaratılır.

Yazılım güvenlik duvarları

Açık kaynak kodlu güvenlik duvarları

Açık kaynak kod dünyası her çeşit büyüklükteki ağa uygun güvenlik duvarı yazılımı üretiminde yıllardır ileride olmuştur. Linux' un paketleri yönlendirme ve süzme kabiliyeti, kendi özünde vardır. Ipchains veya Iptables, Linux sistemlerde bu amaçlar için kullanılmaktadır.

Iptables: Linux 2.4 çekirdeği ve üzerini destekler. Iptables paketi 2.3 çekirdeğinde bulunduğu gibi paket maskeleme ve süzme işlemlerini desteklemektedir. Netfilter paket süzme yapısının alt yapısını oluşturmakta ve iptables için API görevini görmektedir. Kısaca iptables netfilter'ı kullanan bir arayüz diyebiliriz. Bu nedenle Iptables'ı

kullanmak için netfilter'in ardından Iptables paketinin kurulmuş olması dolayısıyla çekirdeğin yeniden derlenmesi gerekir. Ipfwadm ise hem Ipchains hem de Iptables'ın öncüsüdür ve daha eski Linux çekirdeklerinde kullanılmıştır.

IP tables, farklı çeşitlerde paket işleme görevi için ayrı kural tabloları kullanır. Bu kural tabloları, kurallar için **filter** tablosu, NAT için **nat** tablosu ve özel paket işlemeye özel **mangle** tablosu olmak üzere üç ana modülden oluşur. [Suehring S. ve Ziegler R., 135]

Örnekler:
Bir IP bloğundan gelen bütün www trafiğinin engellenmesi:

```
iptables -A FORWARD -p tcp –dport 80 -s 12.12.12.0/24 -d www.ubc.ca -j DROP
```

Tek bir kullanıcıdan gelen bütün Telnet trafiğinin engellenmesi:

```
iptables -A INPUT -p tcp -s bad.host.com -d my.host.com  --dport 23 -j DROP
```

RFC 1918 özel ağların iç tarafta engellenmesi:

```
iptables -A FORWARD -s 10.0.0.0/8 -i eth0 -j DROP
iptables -A INPUT   -s 10.0.0.0/8 -i eth0 -j DROP
iptables -t mangle -A PREROUTING -s 172.16.0.0/12 -i eth0   -j DROP
```

ssh oturumuna ve durumun devamına izin verilmesi:

```
iptables -A FORWARD -p tcp –dport 22   -i fxp0 -m state    --state NEW,ESTABLISHED -j ACCEPT
```

OpenBSD PF (Packet Filter): En gelişmiş açık kaynak kodlu güvenlik duvarı çözümüdür. PF, TCP/IP trafiğini süzme ve ağ adres dönüşümü (NAT) sağlayan bir OpenBSD sistemidir. PF, aynı zamanda TCP/IP trafiği üzerinde normalleştirme ve iyileştirme de yapabilir. Bant genişliğini kontrol eder ve paket önceliklendirmeyi de destekler. PF, OpenBSD 3.0'dan bu yana ana OpenBSD çekirdeğinin bir parçasıdır. [136]

Ayrıca CD ve disketten direk çalışan Linux güvenlik duvarları da mevcuttur. Bunlar;

- AstaroSecurityLinux, CensorNet, ClarkConnect Broadband Getaway, Devil-Linux, Euronode, Gibraltar, IPCop Firewall, Mandrake Security MNF, m0n0wall, redWall Firewall, Sentry Firewall, SmoothWall GPL

Ticari yazılım güvenlik duvarları

Kişisel kullanım için tasarlanmış yazılım güvenlik duvarları:

Kişisel kullanım için tasarlanmış yazılım güvenlik duvarları, kullanıcıların güvenlik çözümlerinden beklentileri doğrultusunda oluşan eğilimler sonucunda yeni bir yapılanmaya girmişlerdir. Bu eğilim neticesinde yazılım üreticileri güvenlik duvarı hizmetlerinin (paket süzme, uygulama seviyesi paket denetleme, proxy, NAT gibi) yanı sıra işletim sistemi güvenliği, antispyware ve içerik filtreleme gibi unsurları da bünyelerine eklemişlerdir. Bunlara örnek olarak aşağıdakiler verilebilir:

- Windows güvenlik duvarı,
- Zone Alarm Pro 6.5,
- Kerio WinRoute Firewall 6,
- CA Personal Firewall 2007,

Kurumsal kullanım için tasarlanmış yazılım güvenlik duvarları:

- **Check Point FireWall-1**: FireWall-1 erişim kontrolü, kimlik tesbiti, ağ adres dönüşümü, içerik güvenliği, denetleme gibi işlemleri gerçekleştirebilen kurumsal güvenlik çözümüdür. FireWall-1 ile kurumsal ağ kaynaklarının güvenliğini sağlayacak tek ve çok yönlü bir güvenlik politikası tanımlanıp uygulanabilir. Kendine ait patentli "Stateful Inspection" teknolojisi ve "Open Platform for Security" (OPSEC), internet güvenliğinin her aşamasına entegre olabilen ve bunları tek bir merkezden yönetebilen, çok sayıda konfigürasyon ve işletim platformu seçenekleri içeren bir çözüm sunar. [137]
- **Microsoft Internet Security and Acceleration (ISA) Server**: Politika tabanlı güvenlik uygulamaları sunan, ağ yapılarını hızlandıran ve bu yapıların etkin biçimde yönetilmesini sağlayan bir güvenlik duvarı ve Web önbellek (cache) sunucusudur. Güvenlik duvarı bileşeni; paket seviyesinde, anahtarlama seviyesinde ve uygulama seviyesinde süzme yapma, üzerinden geçen veri trafiğini kapsamlı biçimde inceleme ve trafiğin erişim politikalarını ve

yönlendirilmesini kontrol etme özelliğine sahiptir. Önbellek bileşeni ise sıkça kullanılan Web içeriğini önbellekte depolayarak ağ performansının ve kullanıcı deneyiminin artmasını sağlar. Güvenlik duvarı bileşeni ve önbellek bileşeni farklı sunuculara kurulabileceği gibi tek bir makine üzerinde de bulunabilir. ISA Server kullanıcılara Standart Edition ve Enterprise Edition olarak iki farklı versiyonla sunulmaktadır. Her iki versiyon da zengin özellikler içermektedir. Standart Edition, en fazla dört işlemciyi destekleyen tek bir sunucu için tasarlanmıştır. Daha geniş uygulama alanları için tasarlanan Enterprise Edition, sunucu grupları oluşturmak, çok katmanlı politikalar geliştirmek ve dört işlemciden daha fazla işlemciye sahip sistemler için uygundur. [138]

Donanım güvenlik duvarları

Donanım güvenlik duvarı çözümlerin artıları aşağıdaki gibidir:

- Uygulama için özel geliştirilmiş entegre devrelere (ASIC) sahip olduklarından daha yüksek performans elde edilebilmektedir.
- Genelde en kötü saldırılarda dahi cihazı kapatıp açınca yeniden çalışmaya devam ederler.
- Versiyon yükseltmeleri (upgrade) diğer sistemlere göre daha çabuk yapılır.
- Hizmet dışı kalma süreleri (downtime) azdır.
- İşletim sistemleri bilinmediğinden (Genelde UNIX türevleridir) ve az kullanıldığından açıkları fazla bilinmez. [Karaarslan E., 139]

Donanım (appliance) güvenlik duvarları, yazılım güvenlik duvarlarında olduğu sahip oldukları temel işlevlerin (durum denetlemeli güvenlik duvarı, NAT, VPN vb.) yanında yazılım güncellemeleri ve ilave moduller ile günümüz kullanıcı istek ve ihtiyaçlarına cevap verebilecek hale getirilmiştir. Üretici firmaların birçoğu da mevcut ürün yelpazelerine yeni modeller ilave etmişlerdir. Örnek olarak aşağıdaki ürünler verilebilir.

- **Juniper NetScreen**: NetScreen-500, NetScreen-5200, NetScreen-5400 güvenlik duvarı ve VPN çözümlerine ilave olarak ISG 1000, ISG 2000, ISG with IDP, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208 modelleri ile birlikte Güvenlik İhlallerini Tespit ve Önleme Sistemi (IPS) ihtiyaçlarına , Netscreen 5G ve SSG serisi ile de Birleşik Tehdit Yönetimi (UTM) ihtiyaçlarına cevap verebilecek duruma gelmiştir. [140]

- **Nokia Firewall/VPN**: Özel olarak tasarlanmış Check Point güvenlik duvarı/VPN teknolojisi ve güvenliğe özel tasarlanmış IPSO işletim sistemi ile güçlendirilmiş Nokia platformunun birleşiminden meydana gelmiştir.
- **Cisco PIX (Private Internet Exchange)**: PIX güvenlik duvarı ilk olarak Network Translation şirketinden Brantley Coile ve John Mayes tarafından tasarlanmış ve 1995 yılında şirketlerinin Cisco ile birleşmesinden sonra geliştirilmesine burada devam edilmiştir. Çeşitli büyüklükteki ağların giriş güvenliğini sağlamak üzere PIX 501, 506E, 515E, 525, 535 modelleri bulunmaktadır. Cisco daha sonra IPS de dahil olmak üzere bir çok özelliğin eklendiği ASA (Adaptive Security Appliance) ürün grubunu çıkarmıştır. [141]
- **WatchGuard** : Watchguarad firması ilk donanım güvenlik duvarı üreticilerindendir. Firebox serisi ürünleri artık güvenlik duvarı kavramının ötesinde VPN, NAT, IPS, içerik filtreleme, gateway antivirüs, antispam, ve antispyware özelliklerini kendine has Firewire Pro işletim sistemi ile karşılayabilecek bir yapıya gelmiştir. [142]
- **Secure Computing CyberGuard TSP Firewall/VPN**: Ürün ailesi 110, 210, 410, 510, 1100, 2100, 2150 ve 4150 modellerinden oluşmaktadır. [143]

5.1.3. Güvenlik duvarları ve ağ erişim politikası ilişkisi

Güvenlik duvarı ağ erişim politikasının uygulanmasına yardımcı olacak, savunma hattımızın en önünde yer alan araçlardan biridir.

- Kullanıcı gruplarının sınıflandırılması
- Ağ kaynaklarının sınıflandırılması
- Kullanıcı gruplarının ağ kaynaklarını nasıl ve ne kadar kullanacaklarının belirlenmesi,

ağ erişim politikasını oluşturma aşamasında izlenmesi gereken adımlardır.

Bu adımlar ayrıntıları ile belirlendikten sonra sıra bunun ağ güvenlik cihazlarında uygulanmasına gelir. Örnek:

- Kullanıcı gruplarının sınıflandırılması:
  - Akademisyenler,
  - İdari yöneticiler,

- İdari bürolar,
- Öğrenci laboratuvarları,
- Öğrenci yurtları,
- Sunucular,
- Bilgi Teknolojileri Ofisi,

- Ağ kaynaklarının tanımlanması
  - Web içeriği (content),
  - Online haberleşme (IM = Instant Messaging),
  - Internet erişimi kullanım kapasitesi (bandwidth),
  - Sunucular [web, mail, ftp, antiX (virüs, worm, trojan, spyware, adware) vb.],
  - Otomasyon programları (DA = Database Applications),
  - Protokoller ve portlar (P/P),
- Kullanıcı gruplarının ağ kaynaklarını nasıl ve ne kadar kullanacaklarının tanımlanması: İçerik süzme (CF = content filtering), erişim sınırlandırılması (BR = bandwith rate)

Tablo 5.1.3.1 : Basit bir ağ erişim politikası

	Content filtering	**Instant Messaging**	**Bandwith Rate**	**Database Applications**	**P/P**
Akademisyenler	Sınırlı	Kullanabilir	Uygulanmaz	Kullanamaz	Sınırlı
Yöneticiler	Sınırlı	Kullanabilir	Uygulanmaz	Kullanabilir	Sınırlı
İdari bürolar	Tamamen	Kullanamaz	Uygulanır	Kullanabilir	Sınırlı
Öğrenci lab.	Tamamen	Kullanamaz	Uygulanır	Kullanamaz	Sınırlı
Öğrenci yurtları	Tamamen	Kullanabilir	Uygulanır	Kullanamaz	Sınırlı
BTO	Uygulanmaz	Kullanabilir	Uygulanmaz	Sınırlı	Sınırlı
Dış kullanıcılar				Kullanamaz	Sınırlı

Tablo 5.1.1.1. de basit bir ağ erişim politikası çizelgesi görülmektedir. Tabloda yer alan sütunlar kendi içinde de sütunlara ayrılarak politika detaylandırılabilir. Örneğin protokol ve port sınırlandırılması yapılırken, öğrenci yurtlarında web (80 TCP), mail (25, 110 TCP) ve online haberleşme portlarının dışındaki tüm portlar kapalı tutulur. İdari bürolar, yöneticiler, akademisyenler için ise birkaç istisna dışında genellikle saldırıların yapıldığı 2000 üstü portlar kapalı tutulabilir. Bu tablodaki değerler, kullanılabilecek güvenlik politikası doğrultusunda farklı olabilecektir.

5.2. GÜVENLİK İHLALLERİNİ TESPİT SİSTEMİ (IDS)

Güvenlik duvarları, IDS ve IPS gibi farklı teknolojiler, birlikte çalışarak ağ üzerinde oluşabilecek ihlaller konusunda uyarılar verir ve bunları önler. IDS ve IPS'ler güçlü bir güvenlik programının sağlanmasında hizmet eden birçok yöntemden sadece ikisidir. Dikkatli bir risk analizi temel alındığında, ister katmanlardan oluşan bir yaklaşım, ister derinlemesine bir savunma (defense in depth) anlayışı kullanılsın, bir ağ en zayıf halkası kadar güvenlidir. Bu da demektir ki bir ağ, kurumun tüm güvenlik stratejisini bir bütün haline getirebilmek için kendi içlerinde işlevlere sahip, çok katmanlı bir güvenliğe sahip olmalıdır. [Endorf C. ve diğ., 144]

Bir güvenlik ihlal tespit sistemi, yetkisiz ve şüpheli ağ faaliyetlerini tanımlayan, değerlendiren ve kayıtlarını tutan araçlar, yöntemler ve kaynaklar olarak tanımlanabilir. IDS'ler, OSI modelinin ağ katmanında çalışırlar ve genellikle ağın boğum noktalarına yerleştirilen pasif ağ sensörleridir. Ağ trafiğindeki paketleri belirli örneklere göre analiz ederler.

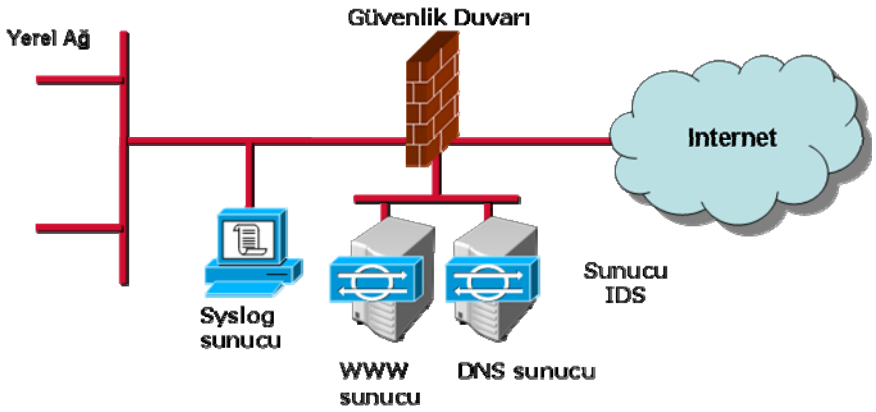
Analiz işlemleri imza tabanlı (signature based) ve anormal davranış tabanlı (anomaly based) olmak üzere iki şekilde yürütülür. İmza tabanlı durumlarda, gelen trafik dinlenir ve belirli bir diziye uyan saldırı paketleri tespit edilir. Anormal davranış tabanlı durumda ise ağda var olan hareketler incelenir ve bu trafiklerin karakteristikleri çıkarılır. Bu hareketlerin dışına çıkan bir olay gerçekleşirse, bu hususta uyarı mesajları üretilir. [Lockhart A., 145]

Her ne kadar alarmlar gerekli olsa da ağ güvenlik personelinin, IDS in yanlış olumsuz ve yanlış olumlu alarm üretimini en aza indirebilmesi çok önemlidir. **Yanlış olumlu** (false pozitive), geçerli bir trafik veya tehlikesiz bir olay olduğu halde IDS in ihlal olduğu kararına varması durumudur. **Yanlış olumsuz** ise bir ihlal olması veya saldırı trafiği iletilmesine rağmen IDS sensörün bunu ihlal olarak görmemesi ve geçirmesi durumudur. Bu ağ işletimi için çok kötü bir durumdur. Yanlış olumsuz durumların en aza indirilmesi en yüksek önceliğe sahip olmalıdır.

IDS ler yerleşimlerine göre üç temel sınıfa ayrılırlar: Sunucu tabanlı (HIDS), ağ tabanlı (NIDS) ve ikisinin karışımından oluşan hibrid ihlal tespit sistemi.

5.2.1. Sunucu tabanlı (Host Based) güvenlik ihlal tespit sistemi

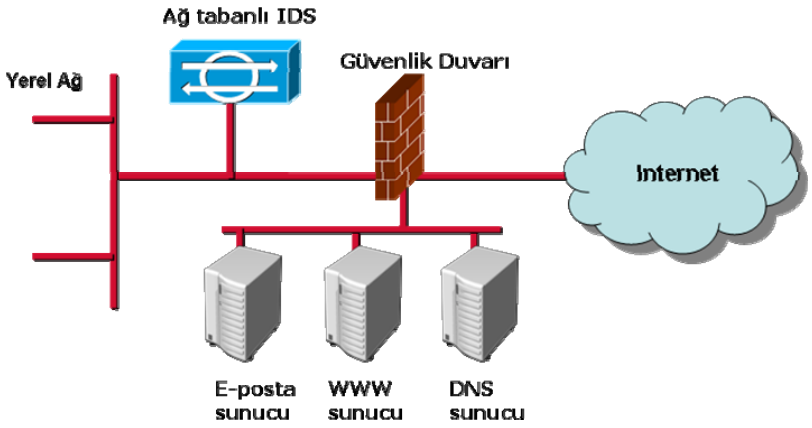
Bir sunucu tabanlı ihlal tespit sistemi, bir işletim sistemi üzerine kurulan ve tüm sunucu kaynaklarını tarayan bir yazılımdır. İyi bir saldırı tespit sistemi, çok az kullanıcı müdahalesi ile çalışabilmeli, sistem kaynaklarını en az düzeyde kullanmalı, sistemde zaman içinde yapılacak değişikliklere karşı uyum sağlayabilir olmalı, sistemdeki normal davranış ile normal dışı davranışı ayırt edebilmelidir.



Şekil 5.2.1.1 : Sunucu tabanlı ihlal sistemi yerleşimi

5.2.2. Ağ tabanlı (Network Based) güvenlik ihlal tespit sistemi

Bir ağ tabanlı ihlal tespit sistemi (NIDS) genellikle ağın iç tarafına yerleştirilir ve oluşabilecek saldırılara karşı ağ paketlerini analiz eder. Bir NIDS ağın belirli bir segmentinden port mirroring gibi yöntemlerle tüm paketleri alır. Şüpheli davranış örneklerine göre trafiği analiz eder ve elde edilen bulgulardan dikkatlice sonuç çıkarır. Birçok NIDS faaliyetlerinin kayıtlarını tutma, rapor verme ve alarm üretme özellikleri ile donatılmışlardır. Ayrıca birçok yüksek performanslı yönlendiriciler de NIDS kabiliyetine sahip olabilmektedirler.



Şekil 5.2.2.1 : Sunucu tabanlı ihlal sistemi yerleşimi

Ağ tabanlı ve sunucu tabanlı ihlal sistemlerinin karşılaştırılması Tablo 5.2.1. de yer almıştır.

Tablo 5.2.1 : Ağ tabanlı ve sunucu tabanlı ihlal sistemlerinin karşılaştırılması

NIDS	**HIDS**
Geniş bir ölçekte çalışırlar. (tüm ağ faaliyetlerini gözlerler)	Dar bir ölçekte çalışırlar. (sadece belirli bir sunucunun faaliyetlerini gözlerler)
Kurulumu kolaydır	Kurulumu daha zordur
Dışarıdan gelebilecek saldırıların tespitinde daha iyi bir konumdadır.	İçeriden gelebilecek saldırıların tespitinde daha iyi bir konumdadır.
Tüm ağ üzerinde kaydedilenlere göre tespit etme işlemi yapılır.	Tek bir sunucu üzerinde kaydedilenlere göre tespit etme işlemi yapılır.
Paket başlıklarını inceler.	Paket başlıklarını göremez.
Neredeyse gerçek zamanlı cevap verme kabiliyetine sahiptir.	Genellikle sadece şüpheli bir log girişi yapıldıktan sonra cevap üretilir.
İşletim sisteminden bağımsızdır.	İşletim sistemi bağımlıdır.
Trafik analiz edilir edilmez ağ saldırıları tespit edilir.	İç saldırıları ağı vurmadan önce tespit eder.
Başarısız saldırı girişimlerini tespit eder.	Saldırıların başarılı veya başarısız olduğunu onaylar.

Kendine has özelliklere sahip birçok farklı ağ tabanlı IDS mevcuttur. Cisco Secure IDS, Enterasys Dragon Network Sensor, ISS RealSecure Network Sensor, NFR Sentivist IDS, Snort, ve Sourcefire Intrusion Management System en çok bilinen ve yaygın olarak kullanılanlarıdır. Hepsi de alarm üretme, log'lama ve raporlama kabiliyetlerine sahiptirler.

5.2.3. Açık kaynak kodlu bir IDS örneği: Snort

Snort, Marty Roesch tarafından yazılmış, imza tabanlı ve en yaygın kullanıma sahip açık kaynak kodlu güvenlik ihlal tespit sistemidir. Kasım 1998 de sadece Linux te çalışan APE isimli, sadece 1600 kod satırı ve toplam iki dosyaya sahip bir paket koklayıcı (sniffer) olarak yazılmıştır. Şu an 2.6.1. versiyonu mevcuttur. IP ağında gerçek zamanlı trafik analizi, protokol analizi, içerik tarama, karşılaştırma ve paket loglama kabiliyetine sahiptir. [Babbin J. ve Biles S., 146]

Snort, üç modda çalıştırılmak üzere yapılandırılabilir:

- **Sniffer mod**: Ağdaki paketleri okur ve kullanıcıya konsol ekranından sürekli akar şekilde gösterir. İlk olarak ekranda TCP/IP paket başlıklarını görüntülemek için

  ./snort -v

  komutu kullanılır. Bu komut sadece snortu çalıştırır ve sadece IP ve TCP/UDP/ICMP başlıklarını gösterir. Eğer iletilen uygulama verisi görüntülenmek istenirse

  ./snort -vd

  komutu kullanılır. Bu komutla snort başlıklar gibi paket verisini de gösterir. Eğer veri iletim katmanı başlıkları gibi daha tanımlayıcı bir görüntü almak istenirse

  ./snort -vde

  komutu kullanılır.

  Aynı işleve sahip son komut aşağıdaki gibidir:

  ./snort -d -v -e

- **Paket loglayıcı mod**: Bir önceki modda görüntülenen verilerin belirlenen bir dizine otomatik olarak kayıt edilmesi için

  ./snort -dev -l ./log

  komutu kullanılır. Burada **log** dizini varsayılan dizin olarak kabul edilmiştir. Snort bu modda çalıştırılırsa gördüğü her paketi toplar ve IP adreslerine göre bir dizine yerleştirir.

  ./snort -dev -l ./log -h 192.168.1.0/24

Bu komut satırı veri iletim ve TCP başlığı ve uygulama verisini ./log dizinine gönderir ve paketleri 192.168.1.0. C sınıfı ağa göre loglar. Gelen tüm paketler log dizininin alt dizinlerine uzak sistemin IP adreslerine göre isimlerle kayıt edilir. Yüksek hızlı bir ağda bulunuluyor veya daha sonra analiz edilmek üzere paketler daha yoğun bir şekilde loglanmak istenirse binary mod kullanılabilir. Binary mod paketleri dizin içerisinde tek bir binary dosya şeklinde tcpdump formatında loglamaktadır.

./snort -l ./log -b

Binary mod tüm paketleri tek bir dosya içerisinde logladığı için ilave anahtar kullanmaya gerek yoktur. Binary dosya içine kayıt edilen paketler tcpdump binary formatını destekleyen tcpdump veya Ethereal gibi herhangi bir sniffer ile okunabilir. Binary olarak kaydedilen log dosyasini sniffer modunda okumak için

./snort -dv -r packet.log

komutu kullanılır. Sadece ICMP paketlerini göstermek için ise

./snort -dvr packet.log icmp

komutu kullanılır.

- **Ağ ihlal tespit sistemi (NIDS)**: Bu modu açabilmek için

  ./snort -dev -l ./log -h 192.168.1.0/24 -c snort.conf

  yazılır. Burada **snort.conf** kural dosyasının adıdır. Eğer hedef dizini yoksa **/var/log/snort** dizininin altına kayıt işlemi yapılır. Eğer snort uzun vadede NIDS olarak çalıştırılacak ise hız kazanabilmek için -v anahtarını komut satırından çıkarabiliriz. Birçok uygulama için veri iletim başlıklarına da ihtiyaç olmayacağı için ayni sekilde -e anahtarı da çıkarılabilir.

  ./snort -d -h 192.168.1.0/24 -l ./log -c snort.conf

  Bu komut satırı snortu en temel NIDS formunda çalıştırmak üzere yapılandırır.

Ayrıca yönetim için Apache web sunucu (SSL desteği olması çok önemlidir) gerektiren ihlal veritabanları için analiz konsolu (ACID) web arayüzü, PHP ve alarmların tutulacağı MySQL veya PostgreSQL gibi veritabanları kurulabilir.

Bazı yaygın snort eklentilerine aşağıdakiler örnek olarak verilebilir:

- ACID, Oinkmaster, SnortSnarf, SnortReport

İhlal veritabanları için analiz konsolu (ACID)

ACID (Analysis Console for Intrusion Databases), birçok PHP (Pretty Home Page) kodu ve konfigürasyon dosyasının birlikte çalışarak bir web arayüzü vasıtasıyla bir mySQL veritabanından alınan verileri toplama, analiz ve gösterme amacıyla kullanılan bir araçtır. [147] ACID, snort ile birlikte çalışabildiği gibi diğer güvenlik duvarı ve ağ görüntüleme cihazları gibi güvenlikle ilgili ürünlerle birlikte çalışabilir. [Rehman R., 148]

5.3. GÜVENLİK İHLAL ÖNLEME SİSTEMİ (IPS)

Bilgisayar ve ağ güvenlik cihazları canlılar gibi değişmekte, büyümekte ve ortam şartlarına karşı uyum sağlayarak evrim geçirmektedirler. Özellikle, her gün güvenliği tehdit eden yeni unsurların ortaya çıkması, güvenlik ürünlerinin bu yeni tehditlerin üstesinden gelebilecek şekilde uyum sağlaması için şartları zorlamaktadır.

Güvenlik ihlallerini önleme sistemleri (IPS), ağ cihazlarına karşı yapılabilecek bilinen veya bilinmeyen saldırıları önleyebilecek cihazlar veya uygulamalardır. Bu sistemler ilk olarak güvenlik duvarları ve antivirüs ürünleri gibi o günün ürünlerinin ilave özellikleri olarak ortaya çıkmış daha sonra gelişerek bağımsız bir ürün grubu haline gelmiştir.

Güvenlik ihlal önleme sisteminin en büyük özelliği kötü amaçlı trafiği hedef sisteme ulaşmadan önlemektir. Güvenlik tespit sistemleri (IDS), tepkisel (reactive) yapılarından dolayı kötü amaçlı trafiği tespit ederler ve uyarı gönderirler. İhlal önleme ise insiyatif kullanarak (proactive) ağı saldırılara karşı savunurken bir yandan da kurumun ağ güvenlik politikalarının uygulanmasında yardımcı olur. [Carter E. ve Hogue J., 149]

IPS, bu görevlerini yerine getirirken iki temel yaklaşım kullanır; korunacak sunucu sistemin üzerine yüklenen bir yazılım olan sunucu ihlal önleme sistemi (HIPS) ve bir ağ segmentine bağlanan, o segment ve alt segmentler üzerinde bulunan tüm sistemleri koruyan bir yazılım veya donanım sistemi olan ağ tabanlı ihlal önleme sistemi (NIPS).

5.3.1. Sunucu tabanlı ihlal önleme sistemi (HIPS)

Sunucu tabanlı IDS sistemlerde olduğu gibi, korunması gereken sistem üzerine direk olarak kurulan yazılımlardır. Sistem üzerinden geçen trafik denetlenir, uygulamaların ve işletim sisteminin davranışları bir saldırının etkilerine karşı incelenir. Bu programlar (agent) sadece işletim sistemini veya o sunucu üzerinde çalışan uygulamaları korur. Saldırı tespit edildiğinde sunucu tabanlı IPS yazılımı ya saldırıyı ağ katmanında engeller veya uygulama veya işletim sistemine verdiği gerekli komutlarla saldırının doğurduğu davranışı durdurur. [Rash M. ve Orebaugh A., 150] Örneğin tampon taşması (buffer overflow) saldırıları, adres satırına yazılan kodlarla kötü amaçlı program çalıştırılmasının engellenmesi ile önlenebilir. Internet Explorer gibi uygulamalar vasıtasıyla arka kapı programların kurulma girişimleri, Internet Explorer' a "dosyaya yaz" komutunun engellenmesi ve reddedilmesi ile önlenir.

5.3.1.1. Sunucu IPS özellikleri

Bir sunucu IPS ürününün tanımlanabilmesi ve sınıflandırılabilmesi için bir takım özelliklere sahip olması gerekir.

- Kötü amaçlı kod saldırılarını engelleyebilmelidir.
- Bir sunucuya yapılan saldırıyı engellemenin en kolay yolu ağ bağlantısını kesmektir fakat bu aynı zamanda ağ servislerini kullanan kullanıcıları bu hizmetlerden mahrum etmek demektir. Güvenliğin sağlanabilmesi için bağlantının kesilmesi, normal işlemleri kesintiye uğratacağı için çok kullanışlı bir yöntem değildir. IPS'lerde benzer olarak sistemin normal çalışmasını kesintiye uğratmamalıdır.
- Saldırılar ve normal olaylar arasındaki farkı yeterince doğru bir şekilde anlayabilmelidir.
- Sunucu tabanlı IPS'ler yeni ve bilinmeyen saldırıları tekrar bir konfigürason veya güncelleme gerektirmeden durdurabilmelidir.
- İzin verilen uygulamalardaki açıklara karşı korunma sağlamalıdır.

5.3.1.2. Sunucu IPS in faydaları

Sunucu IPS lerin uygun kullanımı ve doğru ürün seçimi, kurumun karşılaştığı problemler ile ürünün sağlayacağı faydalar birbirleriyle örtüşmelidir. Bu nedenle hangi ürünün kurumun yararına olduğu ve hangi problemleri çözdüğünün bilinmesi gerekir.

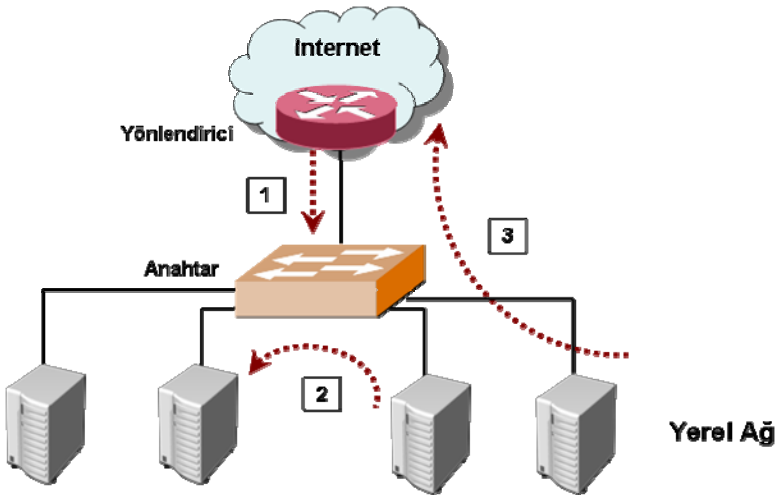
- Bir sistem üzerine direk olarak kurulmuş bir yazılım saldırılara karşı bir koruma sağladığı gibi o saldırının sonuçlarına karşı da bir korunma sağlar.
- Yerel ağın içinden gelebilecek saldırılara karşı bir korunma sağlar.
- Uygulamalardaki açıkların ve güncellenmemiş yamaların doğurduğu zaafiyetlere karşı bir korunma sağlar.
- Güvenlik risklerini azaltmak için hazırlanmış yönetmelik ve talimatnameleri içeren politikaların uygulanmasında da yardımcı olur. Örneğin, politikada hem ethernet portu hem de kablosuz iletişim portu bulunan makinelerin bunları beraber kullanmamalarına dair bir madde olsun. Bu durum belki sistemin kendisine bir zarar vermez ama ağ için bir güvenlik riski oluşturur. Sunucu tabanlı IPS, biri çalışırken diğerini kapatmak üzere yapılandırılabilir.
- Kurumsal politikaların bir tanesi de kabul edilebilir kullanım politikasıdır. Kabul edilebilir kullanım politikası içerdiği uygun kullanıma dair talimatlar nedeniyle güvenlik politikalarından farklıdırlar. Örneğin kabul edilebilir kullanım politikasında internet kullanımının sadece akademik amaçlar için olduğuna dair bir madde bulunsun. Lisanssız programlar veya pornografik materyallerin download edilmesi gibi başka amaçlar için interneti kullanan çalışanlar kontrol ve tespit edilebilmelidir. Sunucu tabanlı IPS, hangi kullanıcının hangi zamanlarda ve neler yaparak politikayı ihlal ettiğini tespit eder ve buna karşı uygulanacak soruşturmada delil oluşturur.

5.3.2. Ağ tabanlı ihlal önleme sistemi (NIPS)

Ağ tabanlı IPS, standart bir IDS, bir IPS ve güvenlik duvarının birleşiminden meydana gelen yerel ağın iç tarafına konumlandırılan cihaz veya yazılımlardır. Bir güvenlik duvarında olduğu gibi iç ve dış olmak üzere en az iki arayüze sahiptir. Herhangi bir arayüzüne gelen paketler incelenmek üzere tespit mekanizmasına geçerler. Eğer paketin zararlı kodlar taşıdığı tespit edilirse bir uyarı üretilmesinin yanı sıra paket düşürülür ve ona kötü damgası vurulur. TCP oturumunun geri kalan diğer paketleri IPS e ulaştığında onlarda hemen düşürülür. Zarasız paketler diğer arayüze geçer ve hedefine ulaştırılır. Bunu sağlamak için parçalanmış, sırası bozulmuş veya örtüşen (overlapping) IP parçalarından oluşan paketler hedef sisteme gönderilmeden önce tekrar dizilir ve temizlenir. Burada dikkat edilmesi gereken husus, TCP reset komutu göndererek veya

bir saldırı tespit edildiğinde güvenlik duvarını yeniden yapılandırarak IPS özelliklerine sahip olunamayacağıdır. [151]

Ağ tabanlı IPS sisteminin ağ üzerinde konumlandırılacağı yer saldırılara karşı başarı oranını büyük oranda etkileyecektir. Şekil 5.3.2.1. de ki gibi bir ağın korunduğunu varsayalım.



Şekil 5.3.2.1 : Örnek ağ yapısı

Ağa yapılan saldırıların önlenmesi IPS cihazı saldırgan ve kurban sistem arasında konumlandırılmadır. Şekil 5.3.2.1. den de görüleceği üzere üç saldırı şekli mevcuttur:

1) Internet tarafında bulunan saldırganın iç ağdaki bir sisteme düzenlediği saldırı

2) İç ağdaki bir saldırganın yine iç ağda bulunan başka bir sisteme düzenlediği saldırı

3) İç ağdaki saldırganın internette bulunan bir sisteme karşı düzenlediği saldırı

1 ve 3 numaralı saldırılara karşı korunma IPS cihazını yönlendirici ve anahtar arasına yerleştirerek kolaylıkla sağlanır. İç ağa giren veya iç ağdan çıkan trafik IPS cihazından geçer ve incelenir. Böylece bilgisayar tabanlı cihazların yanı sıra güvenlik duvarı, yönlendirici, ağ yazıcıları ve VPN cihazları da korunmuş olur. 2 numaralı saldırıya karşı IPS kullanarak korunma sağlamak daha zordur. Herhangi iki sistem arasındaki trafiğin IPS cihazı üzerinden geçirilmesini sağlayabilmek için anahtar ve her sistem arasına IPS cihazı yerleştirmek gerekir. Bu tip bir durumda sunucu tabanlı IPS sistemi ile ağ tabanlı IPS cihazı işbirliğine gitmek daha akıllıca gözükmektedir.

5.3.3. Örnek IPS sistemleri

- Snort yazılımına IPS özellikleri katan ilave yazılım olan SnortSam,
- IBM Proventia Network Intrusion Prevention System (IPS),
- McAfee IntruShield Security Manager Appliance,
- SecureWorks Network Intrusion Prevention Appliance, iSensor V5.3,
- Cisco ASA Serisi,
- SecureSoft Absolute IPS NP5G,

5.4. TUZAK SİSTEMLER (HONEYPOT)

Bir honeypot, taranarak, saldırıya uğrayarak veya ele geçirilerek verileri toplayan bir güvenlik kaynağıdır. Bu demektir ki honeypot olarak ne kurulursa kurulsun, beklenen ve amaçlanan bütün ideal yazılım veya donanımların tam tersine sistemin taranması, saldırıya uğraması ve ele geçirilmesidir. Tanımından da görüldüğü üzere honeypotlar ele aldıkları değişik amaçlar doğrultusunda birçok güvenlik aracından farklıdırlar. Günümüzde kullanılan birçok güvenlik teknolojisi belli problemleri çözmek üzere tasarlanırlar. Örneğin güvenlik duvarları kurum içerisine ve dışına çıkan trafiği kontrol ederek bir erişim kontrol cihazı gibi koruma sağlarlar. Genellikle kurum ağının sınırına yerleştirilerek yetkisiz erişimleri ve faaliyetleri engellerler. [Spitzner L., 152]

Honeypotlar tek bir belirli problemi çözmekle sınırlı olmadıklarından farklıdırlar. Farklı durumlara uygulanabilen oldukça esnek araçlardır. Bir çok farklı amacı olması ve farklı şekillerde bulunması tanımını da zorlaştırmaktadır. Örneğin saldırıları engellemek için kullanılan bir honeypot güvenlik duvarları ile aynı amacı paylaşırlar. Ayrıca IDS işlevlerine benzer bir şekilde, saldırıları tespit amacıyla da kullanılabilirler.

5.4.1. Honeypot Çeşitleri

Honeypotlar ürün ve araştırma honeypotları olmak üzere iki ana sınıfa ayrılırlar. Bu sınıfların ana fikri Snort un geliştiricisi Marty Roesch' ten gelmektedir. Ürün honeypotlar kurumların korunması için, araştırma honeypotları öğrenmek için kullanılırlar.

Ürün honeypotlar

Ürün honeypotlar belirli bir kurumun güvenliğine değer katar ve saldırıları tespit ederek risklerinin azaltılmasına yardımcı olur. Honeypot teknolojileri, ağın ve sistemlerin kanun koruyucuları olarak, kötü amaçlı kişilerle mücadele ederler. Ürün honeypotların genellikle daha az işlevsellik gerektirdiği için kurulumu ve yerleştirilmesi, araştırma honeypotlarına göre daha kolaydır. Fakat saldırılar ve saldırganlar hakkında daha az bilgi verirler. Saldırıların hangi sistemlerden geldiği veya ne tip bir saldırı yönelttikleri gibi bilgiler elde edilebilir fakat birbirleriyle nasıl iletişim kurdukları veya araçlarını nasıl geliştirdiklerine dair bilgiler öğrenilemez.

Araştırma honeypotları

Araştırma honeypotları belli bir kuruma direk değer katmazlar. Temel görevleri; kurumların karşı karşıya kaldıkları tehditleri, saldırganların kim oldukları, nasıl organize oldukları, saldırı yaparken kullandıkları araçları ve bu araçları nereden elde ettikleri hakkında araştırmalar yapmaktır. Ürün honeypotlarını kanun koruyucular olarak farz edersek, araştırma honeypotları, suçlular hakkında bilgi toplayan karşı istihbarat birimleri gibidir. Üniversiteler ve güvenlik şirketleri gibi araştırma kurumlarının yanı sıra askeri ve devlet daireleri de bu tip honeypotları sıkça kullanırlar. Araştırma honeypotları üzerinde gerçek işletim sistemleri ve uygulamalar kullanıldığından, artan işlevsellik, ona dezavantaj getirmektedir. Araştırma honeypotları, daha karmaşık, daha büyük risklere sahip ve yönetimi için daha fazla zaman ve gayret gerektirirler.

5.4.2. Honeypotların sınıflara ayrılması

Bir honeypotla ne yapılmak istenirse o şekilde yapılandırılır. Saldırganları suçüstü yakalamak, araçları ve taktikleri hakkında bilgi toplamak istenirse saldırganın etkileşime geçeceği gerçek bir işletim sistemi içeren karmaşık bir honeypot kurmak gerekir. Ağ taramaları gibi yetkisiz faaliyetler tespit etmek istenirse, sadece servislerin benzerlerinin çalıştığı basit bir honeypot kurulmalıdır. Saldırganlara karşı ortaya çıkan etkileşim seviyesi temel alınarak honeypot çeşitleri sınıflandırılabilir.

Düşük etkileşimli honeypotlar

Düşük etkileşimli honeypotlar, genellikle basit yapıları ve temel işlevselliği nedeniyle kurulumu, yapılandırılması, yerleştirilmesi ve sağlanması en kolay olanlardır. Ağ katmanında çalışır, portlar ve servisler ile sınırlı etkileşime imkan tanırlar. Örneğin bir saldırgan veya solucan ağ katmanında bir porta bağlanmayı dener ve reddedilir. Bu sürede honeypot bağlantı bilgisini yakalar. Bu bilgiler sayesinde kaynak IP adres, port numarası ve bu bağlantı girişiminin ne yapmaya çalıştığı ortaya çıkarılır. Slammer gibi internet solucanları ve port taramaları, düşük etkileşim honeypotları vasıtasıyla tanımlanabilirler. [Grimes Roger A., 153]

BackOfficer Friendly: İlk olarak Back Orifice Truva atı vasıtasıyla port taraması girişimlerinin tespit edilmesi amacıyla yaratılmıştır. Daha sonra gelişerek Telnet, FTP, SMTP, POP3 ve IMAP2 gibi diğer servislere bağlantı girişimlerini tespit eder hale gelmiştir. Bu servislerden birine bağlantı tespit ettiğinde saldırgana sahte cevaplar gönderir, saldırganın zamanını harcar ve sistem yöneticisine saldırganı durdurmak için zaman kazandırır. [154]

HoneyComb: Ağ tabanlı güvenlik ihlal tespit sistemleri (NIDS) için imza üretiminde kullanılan bir sistemdir. Honeypotlar üzerinden trafiği yakalayıp protokol analizi ve model tespit tekniklerini uygular. Linux, FreeBSD ve OpenBSD platformlarında çalışan Honeycomb özellikle solucanların belirlenmesinde faydalıdır. [155]

HoneyD: Honeyd Michigan Üniversitesinden Niels Provos tarafından Unix platformlar için açık kaynak olarak yazılmış ve geliştirilmiştir. Honeyd 1.5b 19.08.2006 da kullanıma sunulmuş ve bir sonraki versiyon üzerinde çalışmalar devam etmektedir. [156] Honeyd, ağ üzerinde sanal sunucular yaratan ve tek bir sunucuyu birden fazla adrese sahipmiş gibi gösteren küçük bir servistir. Ayrıca gerçek sistemleri sanal sistemlerin ortasına saklayarak saldırganları caydırır. Bu sanal sistemlere ping atmak ve traceroute uygulamak mümkündür. Sanal sunucu üzerindeki herhangi bir servis basit bir konfigürasyon dosyası ile taklit edilir.

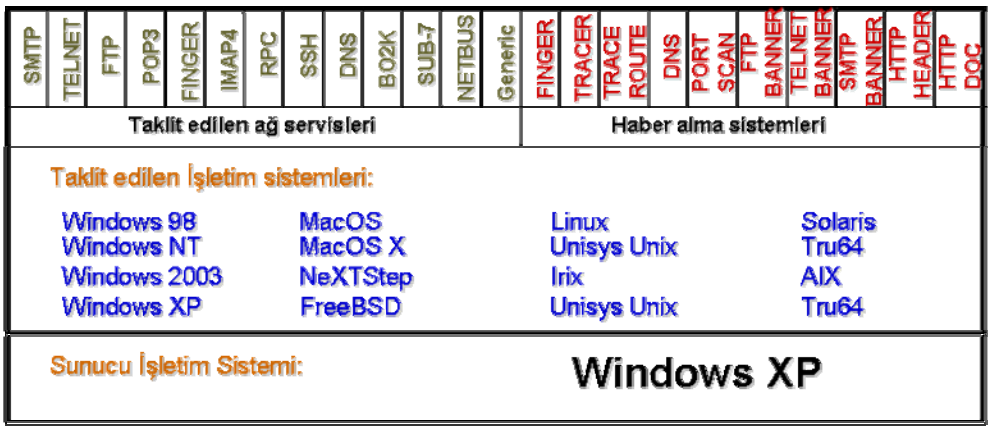
KFSensor: KFSensor Windows tabanlı bir honeypot güvenlik ihlal tespit sistemidir (IDS). Güvenlik açıklarına sahip bir sistem ve Truva atı taklidi yaparak saldırganları ve solucanları kendisine çeker ve tespit eder. Bir yem sunucu gibi davranarak hassas

sistemlere gelebilecek saldırıları saptırır ve güvenlik duvarları ve NIDS lerin kullanabileceği yüksek seviyede bilgiler edinilmesini sağlar. Uzaktan yönetim, Snort uyumlu imza motoru ve Windows ağ protokollerinin taklitleri gibi birçok yenilikçi ve kendine has özelliklere sahiptir. Yeni versiyon olan 4.2 16 Haziran 2006 da kullanıma sunulmuştur. [157]

Mwcollect: Linux ortamında solucanlar ve diğer müstakil yayılma gösteren kötü amaçlı yazılımlar hakkında bilgi toplamak için basit bir çözümdür. [158]

PatriotBox: Güvenlik ihlal tehditlerinin erken tespitinde etkin çözüm sağlayan, yem tabanlı basit kurulum ve yönetime sahip bir honeypot sunucu yazılımıdır. Çok yönlü saldırı tespiti, yönetilebilir bir konumlandırma, yanlış olumlu uyarıların elendiği, görünmez izleme, raporlama ve politika tabanlı saldırı azaltma özelliklerine sahiptir. Ayrıca bir Open Relay Posta Sunucu gibi çalışarak spamların önlenmesine de yardımcı olur. Spam göndericiler postalarının yönlendirildiğini düşünürler fakat PatriotBox a gelen postalar hiçbir yere gönderilmez ve yapılan her hareket loglanır. [159]

Specter: Specter güvenlik açıkları olan bir bilgisayar gibi davranarak saldırganları kendisine çeker. Saldırganlara normal gibi gözüken SMTP, FTP, POP3, HTTP ve TELNET gibi servisleri çalıştırıp boşa uğraşmalarını ve bu arada farkında olmadan izler bırakmalarını sağlar. Bu arada bütün her şey loglanır. Specter yoğun miktarda tuzak resim, mp3 dosyası, e-posta, parola dosyaları, belgeler ve her türlü yazılım içerir. Programların ve diğer içeriğin yasal olmayan şekillerde indirilmesiyle saldırgan, kendi bilgisayarına gizli bir delil koymuş olur. [160]



Şekil 5.4.2.3 : Specter yazılımının yapısı

Bubblegum: Bir açık proxy, internet bağlantılarını hiçbir şey sormadan herhangi bir yerden başka bir yere ileten sunucudur. Kötü amaçlarla bir şey yapmak isteyenler bu tip açık proxy'leri kullanırlar ve bu tip proxy'lerin kayıtları da ya kısa süreli olur veya hiç olmaz. Bir açık proxy honeypot (proxypot), bir açık proxy gibi davranarak bu kötü amaçlı kişilerin isteklerine cevap verir ve onları kandırarak yakalanmalarını sağlar. En büyük amacı spam postaları engellemek, gönderenlerin kimliklerini açığa çıkartmak ve yakalandıklarında mahkemede delil oluşturmak üzere bilgi toplamaktır. [161]

HOACD: HOACD, direk bir CD den çalıştırılan, loglarını ve yapılandırma dosyalarını sabit disk üzerinde saklayan ve temel olarak Honeyd yazılımını alan düşük etkileşimli bir honeypot uygulamasıdır. [162]

LaBrea Tarpit: LaBrea bir zift çukuru yaratan yapışkan honeypot ta denilen, ağda kullanılmayan IP adreslerini alıp, solucanlara, saldırganlara ve internetten gelen diğer davetsiz misafirler için çekici sanal sunucular oluşturan bir yazılımdır. Program bu tip bağlantı isteklerine bir şekilde cevap verip onları uzun süre oyalayabilmektedir. Yazılımın son versiyonu olan 2.5-stable-1, FreeBSD, Linux, Solaris, Windows 98/2K işletim sistemlerini desteklemektedir. [163]

LaBrea ARP isteklerini ve cevaplarını dinler. Program herhangi bir cevap gelmeyen, birkaç saniye aralıklı ardışık ARP isteklerini görürse, bu IP adresinin boş olduğuna karar verir. Daha sonra sahte bir MAC adresine sahip bir ARP cevabı yaratır ve geriye gönderir.

Tiny Honeypot: Tiny honeypot, iptables yönlendirmelerini ve xinetd dinleyicilerini temel alan basit bir programdır. Kullanımda olmayan tüm TCP portlarını dinler, tüm faaliyetleri loglar ve saldırgan hakkında bilgiler sağlar. [164]

Yüksek etkileşimli honeypotlar

Yüksek etkileşimli honeypotlar, honeypot teknolojilerinde en üst noktayı temsil ederler. Saldırganlar hakkında çok büyük miktarda bilgiler verirler fakat yüksek seviyede risk taşırlar. Amaçları saldırgana hiçbir şeyin taklit edilmediği veya sınırlandırılmadığı gerçek bir işletim sistemine erişim vermektir. Şekil 5.3.2.2.1. de görüldüğü üzere öğrenme olanakları inanılmazdır.

```
220-Serv-U FTP-Server v2.5h for WinSock ready...
220--------H-A-C-K T-H-E P-L-A-N-E-T--------
220-W3|_c0m3 T0 JohnA's 0d4y Ef-Tee-Pee S3rv3r.
220 -------H-A-C-K  T-H-E  P-L-A-N-E-T--------
USER johna2k
```

```
331 User name okay, need password.
PASS haxedj00
230 User logged in, proceed.
PORT 172,16,1,106,12,71
200 PORT Command successful.
RETR nc.exe
150 Opening ASCII mode data connection for nc.exe (59392 bytes).
226 Transfer complete.
PORT 172,16,1,106,12,72
200 PORT Command successful.
RETR pdump.exe
150 Opening ASCII mode data connection for pdump.exe
(32768 bytes).
226 Transfer complete.
PORT 172,16,1,106,12,73
200 PORT Command successful.
RETR samdump.dll
150 Opening ASCII mode data connection for samdump.dll
(36864 bytes).
226 Transfer complete.
QUIT
```

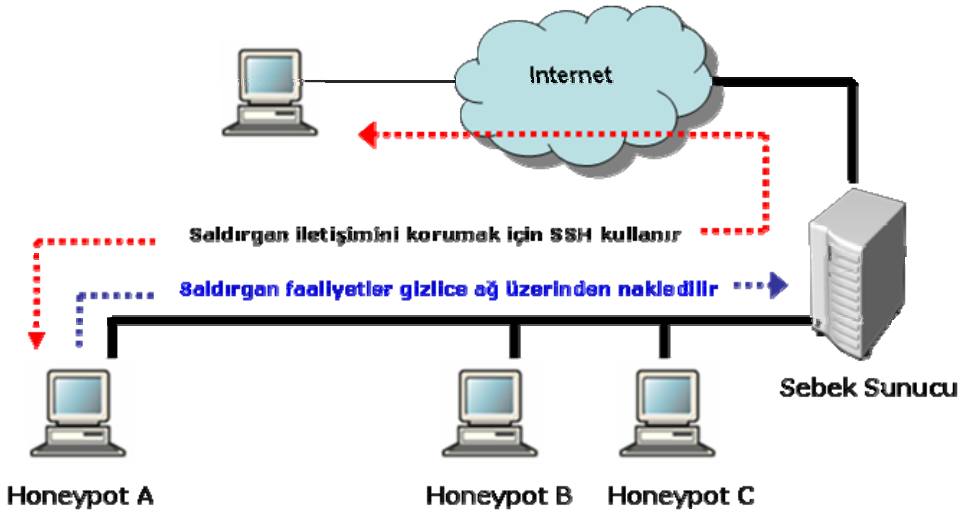
Şekil 5.4.2.4 : Yüksek etkileşimli bir NT tabanlı honeypot'tan alınan, gerçek bir FTP oturumu

Yüksek etkileşimli honeypotlar genellikle bir güvenlik duvarının arkası gibi kontrol altındaki ortamlara yerleştirilirler. Güvenlik duvarı, saldırgana arkasında yer alan honeypotlardan birinin ele geçirilmesine izin verir. Fakat bu durum saldırganın honeypotu kullanarak başka bir saldırı düzenlemesine imkân tanımaz. Kapsamlı kontrol mekanizmaları nedeniyle yüksek etkileşimli honeypotlar kurulumları ve yapılandırılmaları oldukça zor ve zaman alıcı olabilirler. Yüksek etkileşimli honeypotlar, güvenlik duvarı ve güvenlik ihlal tespit sistemleri gibi farklı teknolojileri bir araya getirir. Tüm bu teknolojiler dikkatlice ve düzgün bir şekilde ihtiyaçlara göre uyarlanmalıdır. Güvenlik duvarı erişim listelerinin ve IDS imza veritabanlarının güncelleştirilmesi ve honeypot faaliyetlerinin zamana karşı bir hızda izlenmesi gerektiği, bakımının da zaman aldığını göstermektedir. Bu karmaşık yapı beraberinde yüksek seviyede risk de getirmektedir. Saldırgana verilen daha fazla etkileşim daha fazla şeyin ters gitmesine sebep olabilir. Buna rağmen yüksek etkileşimli honeypot bir kez doğru olarak kurulduğunda, saldırganlara diğer honeypotların veremeyeceği imkanlar tanır.

Sebek: Sebek bir veri toplama aracıdır. Bir saldırganın sisteme giriş yaptığı zaman, nasıl yaptığı ve giriş yaptıktan sonra neler yaptığı hakkındaki bilgiler sayesinde saldırganın kim olduğu, neden yaptığı ve neler kullandığı ile ilgili veriler elde edilir. Eğer şifreleme kullanılmamışsa saldırganın ağ faaliyetleri yakalanarak klavye

hareketlerini izlemek mümkündür ve ethereal gibi bir araç kullanarak TCP akışı yeniden bir araya getirilir ve oturumun içeriği incelenir. Bu teknik saldırganın yazdıkları ile beraber çıktı olarak gördüklerini de verir. [165]

Sebek istemci ve sunucu olmak üzere iki bileşenden oluşur. İstemci sebek honeypotlar üzerine kurulur. Saldırganın tüm faaliyetlerini bir kernel modül veya yama gibi kopyalar ve Şekil 5.3.2.2.3. teki gibi sunucuya gönderir. Kernel modül honeypottan gönderilen bütün Sebek paketlerini ağ boyunca gizler. Böylece saldırganın herhangi bir paketi koklaması veya izlemesi mümkün olmaz.



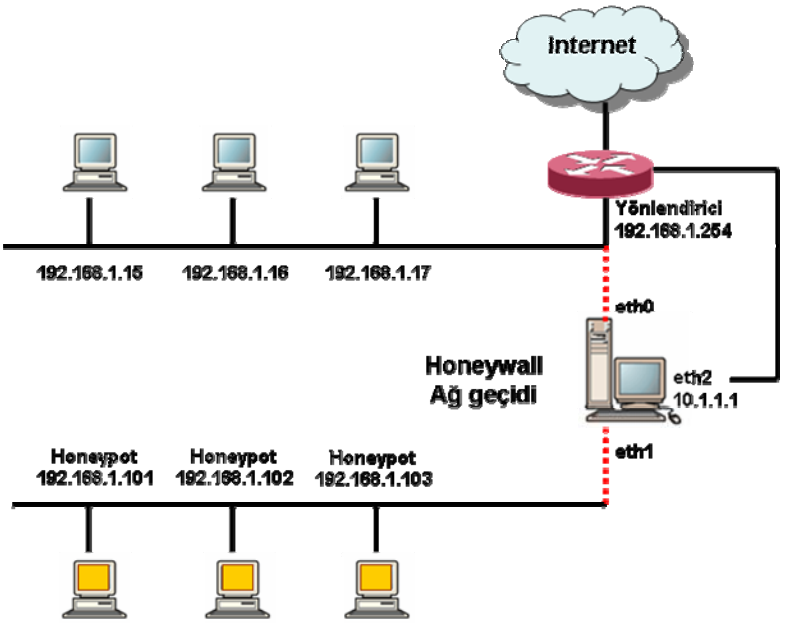
Şekil 5.4.2.5 : Genel bir Sebek yerleşimi

Sebek sunucu bütün Sebek paketlerini toplayan merkezi bir log sistemidir. Normalde Sebek sunucu Honeywall ağ geçidinin üzerine kurulur. Sunucu üç araçtan meydana gelmiştir; sbk_extract, sbk_ks_log.pl, sbk_upload.pl.

- **Sbk_extract**: Sebek paketlerini analiz etmek üzere toplayan bir C programıdır. Sebek paketlerini hem bir tcpdump dosyasından hem de gerçek zamanlı ağdan akan Sebek paketlerinden yakalayarak açar.
- **Sbk_ks_log.pl**: Sebek paketlerini alan ve saldırganın klavye hareketlerini STDOUT olarak veren bir Perl kodudur.
- **Sbk_upload.pl**: Sebek paketlerini alan ve daha gelişmiş analizler için yerel veya uzak bir veritabanına gönderen bir Perl kodudur.

HoneyWall: Honeywall, bir GenII honeynet ağ geçidi için gereken tüm araçları bünyesinde toplayan, kullanımı kolay ve güvenliği yüksek çalıştırılabilir bir CDROM

dur. [166] Amacı honeynet yerleşimini geniş ve dağıtık ağlar için basit ve etkin bir hale getirmektir.



Şekil 5.4.2.6 : Honeywall CD / Honeynet yerleşimi

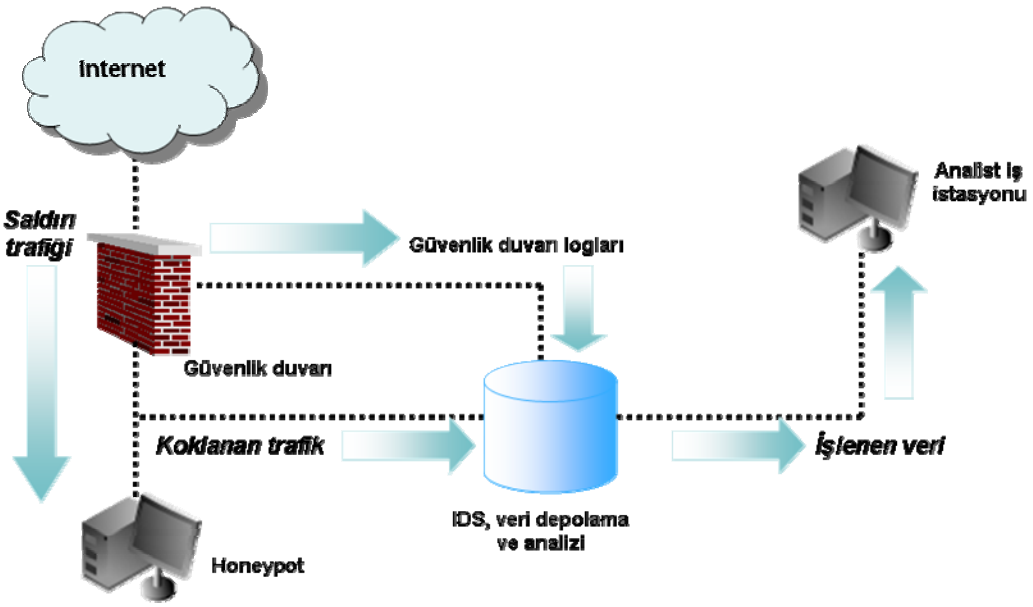
Bağlantıları sınırlandırmak ve hesaplamak için 2. katman köprüleme güvenlik duvarı (iptables) kullanır, IP adresi yoktur ve TTL azaltmaz. Libpcap yerine iptables dan paketleri kabul eden Snort un değiştirilmiş bir versiyonuna sahiptir. Böylece iptables a pakedin atılacağını, geri gönderileceğini, değiştirileceğini veya bir snort tabanlı kurallar çerçevesinde kabul edilip edilmeyeceğini söyler. [Kuehl K., 167] En büyük yeniliği Fedora Core 3 tabanlı bir işletim sistemini diske kurmasıdır. Honeynet e giren ve çıkan trafiği yakalar, kontrol ve analiz eder. Honeywall CDROM Roo'nun en son versiyonu 1.0hw-189 dur.

Honeystick: Tam bir işletim sistemi, GenIII honeywall ve bir veya birden fazla honeypotun, tek bir çalıştırılabilir 2 GB lık USB diske sığabilecek kadar sıkıştırıldığı taşınabilir bir honeynet uygulaması ve olay cevap aracıdır. [168]

5.4.3. Honeynet

Honeynet' ler yüksek etkileşimli honeypotlardır. Honeynet yapısı basittir; güvenlik duvarı gibi bir erişim kontrol cihazı arkasında normal sistemlerin yer aldığı standart bir ağ kurulur ve neler olup bittiği izlenir. Saldırganlar Honeynet içindeki gerçek işletim

sistemleri ve uygulamalarına sahip sistemlerle etkileşime geçerek tararlar, açıkları bulurlar ve buldukları açıklar üzerinden saldırırlar. Bir Honeynet içerisindeki sistemler her şey olabilir; Oracle veritabanı çalışan bir Solaris sunucu, IIS web sunucu çalıştıran bir Windows XP veya bir Cisco yönlendirici. Kısaca bir Honeynet içindeki sistemler gerçek sistemlerdir. Şekil 5.4.3.1. de basit bir honeynet konfigürasyonu görülmektedir.



Şekil 5.4.3.1 : Honeynet örneği

Bir honeynet altyapısı işletmek düşman hatlarının arkasında casus bir ağ çalıştırmakla benzerdir. Karşı konulamayan saldırıları savuşturabilmek için savunma hatları kurmak ve ağ üzerinde her zaman dikkat çekmeden gizlenmek zorundadır. Gözden uzakta emin bir şekilde çalışabilmek çok önemlidir. Üzerlerine gitmek yerine saldırganların gelmesini beklemek gerekir. [Chuvakin A. ve Peikari C., 169]

Honeynet mimarisi

Honeynet in hazır bir paket çözüm olmadığı, bir yapı olduğu bir önceki bölümde anlatılmıştı. Bu mimari; veri kontrol, veri yakalama ve veri toplama olmak üzere üç gereksinimle tanımlanır. Kurumların bu mimarileri uygulayabilecekleri birçok yol vardır. Bu mimarilerden GenI (ilk nesil) 1999 da geliştirilmiş, yerleştirilen ilk honeynet'lerdir. Bu nesilde, honeynet'lerin yerleştirilmesi ve kurulması oldukça zor olup basit veri kontrol ve yakalama yeteneklerine sahiptirler. Üçüncü katman

yönlendirme cihazları ile sınırlandırılmış, belli sayıda dış bağlantıları olan ve sadece şifrelenmemiş trafiği analiz edebilecek düzeydedirler.

GenI mimarisi amaçlarına ulaştığında, 2001 yılında GenII (ikinci nesil) Honeynet'ler geliştirilmiş ve bir takım gelişmeler tanımlanmıştır. İkinci katman köprüleme, ihlal önleme teknolojisi (snort-inline ile beraber) ve şifreli trafiğin analiz edilebilmesini sağlayan Sebek projesi geliştirilmiştir. Bu kadar artan yeteneklerine rağmen honeynet'ler hala kurulumu ve yerleştirilmesi zor ve vakit alan bir durumdadırlar. Geçen zamanda honeynet'lerin daha kolay yerleşimini sağlama çabaları devam etmiştir.

2003 Mayısında ilk Honeywall CDROM'u, Eyeore kullanıma sunulmuştur. Amacı GenII honeynet yerleşimleri için tüm araç ve gereksinimleri tek bir CDROM da biraraya getirmektir. Bu çözüm bir beta sunum olup birçok zayıflıklar içermekteydi. 2004 Eylülünde Roo adı verilen yeni bir tasarım, mimari ve çözüm geliştirildi. GenIII teknolojisine sahip bu çözüm GenII Veri Kontrol ve Veri Yakalama işlevlerini temel alıp ayrıca uzaktan grafik arayüzlü yönetim, Veri Analizi entegrasyonu, Sebek 3.x desteği, güçlü işletim sistemi tabanlı, otomatik güncellenebilme ve daha fazlasını içermektedir.

Honeynet ile ilgili riskler

Bütün honeypotlar arasında en büyük riske sahip oldukları bir gerçektir. Kurumlar Honeynet teknolojilerini kullanmadan önce bu durumlar hakkında iyice düşünmeli, tamamen bilinçli olmalıdırlar. Bu risklerden birincisi etkileşim seviyesidir. Saldırganlar gerçek işletim sistemlerine tam bir erişim sağlarlar. Saldırganlar Honeynet sistemlerini kod derlemek, saldırılar için üs olarak ve araçlarını dağıtmak için kullanabilirler. Saldırganın faaliyetlerini sınırlayan tek şey honeypotların dışındaki veri kontrol mekanizmalarıdır.

İkincisi ise çeşitli teknolojilerin bir arada çalışmasından dolayı karmaşık yapısının doğurduğu risklerdir. Güvenlik duvarı erişim listeleri doğru olarak yapılandırılmış olmalı, iç ve dış bağlantıları doğru olarak sağlanmalıdır. Uyarı üretme kodları çalışır durumda, yetkisiz faaliyetlere dair bilgiler loglanıyor ve uzak log sunucuya iletiliyor olmalıdır. Bu yapılandırmalar veya teknolojilerden birinde oluşacak bir hata Honeynet i

büyük bir risk altına sokacaktır. Örneğin yanlış yapılandırılmış bir kod dışarıya olan bağlantıları engelleyip saldırgana diğer sistemlere karşı saldırı düzenleme olanağı verecektir. Bir teknolojinin bu kadar bağımlılıklara sahip olması bir şeylerin ters gitme olasılığını da arttıracaktır.

Üçüncü sebep ise Honeynet'lerin belirli beklenen bir faaliyeti yakalamak ve kontrol etmek üzere tasarlandıklarıdır. Yeni ve beklenmeyen bir tehdit Honeynet'lerin güvenlik mekanizmalarını devre dışı bırakacaktır. Yapılan her şey oluşabilecek riskleri en aza indirebilmek içindir fakat her zaman bilinmeyen bir tehdidin mevcut güvenlik mekanizmalarını bertaraf etme olasılığı vardır.

5.4.4. Honeypot bilgi kaynakları

- Tracking Hackers (www.tracking-hackers.com), internetteki en iyi honeypot web sitesidir. Honeypot belgeleri ve yazılımlarının geniş bir kolleksiyonu ve ayrıca e-posta listelerine, organizasyonlara ve sıkça sorulan soru (FAQ) sitelerine linkler içermektedir.
- Honeyd Geliştirme web sayfası (www.honeyd.org), sanal honeypot olan Honeyd nin son versiyonlarına ait yazılımlar, belgeler ve kodlar içerir.
- Honeynet Projesi (www.honeynet.org), Ekim 1999 da bilgi güvenliği ve honeypot araştırmaları için kurulmuş kar gütmeyen bir organizasyondur. Amacı siyah şapkalıların araçlarını, taktiklerini ve saldırma nedenlerini öğrenmek ve öğrendikleri bu dersleri paylaşmaktır. Tüm çalışmaları açık kaynak kodlu olup tüm güvenlikle ilgili topluluklarla paylaşım halindedir.
- (www.honeypots.net) Bu site, güvenlik ihlal tespiti, honeypotlar ve olay yönetimi hakkında bilgi, belge, yazılım, kitap ve linkler içermektedir.

5.5. VİRÜS TARAMA VE TESPİT SİSTEMLERİ

Virüs tehditlerini önlemenin en ideal çözümü virüslerin sisteme girmesine izin vermemektir. Gerçekleştirilmesi günümüz şartlarında imkansız olsa da alınacak önlemlerle başarıya ulaşacak virüs saldırılarının sayısı azaltılabilecektir. Bir sonraki en iyi yaklaşım ise aşağıdakileri yapabilmektir: [Stallings W., 170]

- **Tespit etme**: Bulaşma olayı gerçekleşir gerçekleşmez, bulaştığının ve virüsün yerinin belirlenmesi
- **Tanımlama**: Belirleme işlemi başarıyla sonuçlandıktan sonra virüsün tam olarak tanımlanması
- **Temizleme**: Virüs tam olarak tanımlandıktan sonra, virüsün bulaştığı programdan tüm kalıntılarının temizlenmesi ve orijinal durumuna geri getirilmesi. Virüsü bulaştığı tüm bölgelerden temizleyerek daha fazla yayılması engellenmiş olur.

Antivirüs yazılımları sahip oldukları imzalar vasıtasıyla virüsleri ve solucanları tanıyabilen, temizleyen veya zararsız kılmak için karantinaya alan programlardır. Genel olarak iyi bir antivirus programı;

- Virüsleri tanımlamak üzere program tarafından kullanılan virüs imzalarına sahip olmalı.
- Yeni virüs imzalarını otomatik olarak gün içerisinde mümkün olabildiğince sık güncelleyebilmelidir.
- Program deneyim kazandıkça öğrenebilen bir kabiliyete (heuristic) sahip olmalıdır. Böylece program bir bulaşma yaşanmadan virüs benzeri bir davranış anlayışıyla virüsü tespit edip aktiviteyi durdurabilmektedir.
- Günlük, haftalık ve aylık periyotlarla planlanabilen günün belli bir saatinde otomatik olarak virüs taraması yapabilmelidir.
- Virüslerin çoğunluğunun e-postalarla bulaşmasından ve yayılmasından dolayı gelen ve giden postaları tarayabilmelidir.
- Sistemin korunmasını sağlarken işlemci ve bellek kaynaklarını en az düzeyde kullanmalıdır.
- Virüsleri durdurmakla kalmamalı, hızlı ve isteğe bağlı olarak temizleyebilmelidir.
- Casus yazılımlar ve phishing girişimi içeren e-postalar gibi diğer tehditlere karşı da savunma sağlayabilmelidir.

Antivirüs yazılımları e-posta sunucuları üzerine kurularak e-posta yoluyla gelebilecek virüsleri kullanıcılara ulaşmadan belli bir düzeyde engelleyebilmektedir. ClamAV [171] açık kaynak kodlu, Symantec Mail Security for SMTP [172] ise ticari, posta sunucu

üzerine kurulan antivirüs yazılımlarına örnektir. Ayrıca kullanıcıların bilgisayarlarına kuracakları antivirüs programları da virüslere karşı savunma anlayışına derinlik getirecektir. Avast, Grisoft AVG, Antivir ve ClamWin ücretsiz, F-Secure, Kaspersky Anti-Virus Personal, TrendMicro PC-Cillin Internet Security Suite, Panda Titanium Antivirus, Eset NOD32, McAfee VirusScan ve Norton AntiVirus programları da kişisel kullanıma uygun ticari yazılımlara örnek olarak gösterilebilir.

Kurum içerisinde kullanılacak olan antivirüs yazılımı; istemci/sunucu mimarisiyle çalışabilmeli, web üzerinden kolaylıkla kurulabilmeli, imza sunucuları ile otomatik olarak güncelliğini koruyabilmeli, kullanıcıların herhangi bir ayar yapmasını gerektirmemeli ve merkezi bir yönetim konsolu ile yönetilebilmelidir. Symantec Enterprise Edition, McAffee, Trend Micro, Sophos, NOD32, Panda Enterprise antivirüs yazılımları kurumsal antivirüs çözümlerine örnek olarak verilebilir.

5.6. KULLANICI KİMLİK DOĞRULAMA (AUTHENTICATION)

Kimlik doğrulama, kısaca bir nesnenin diğer bir nesneye iddia ettiği varlık olduğunu kanıtlama işlemidir. [Mao W., 173] Kimlik doğrulama deyince insanların aklına genelde parolalar gelmektedir. Her ne kadar kimlik doğrulama için en çok parolalar kullanılsa da birçok kimlik doğrulama mekanizması vardır. Bu mekanizmalar aşağıdakilerden birinin veya birden fazlasının doğrulanmasıyla sınıflarına ayrılabilir: [Burnett M. ve Kleiman D., 174]

- Kullanıcının bildiği bir şey ile
- Kullanıcının sahip olduğu bir şey ile
- Kullanıcıya özel bir şey ile

5.6.1. Kullanıcının bildiği bir şey ile kimlik doğrulama

Kullanıcının bildiği bir şey, kullanıcının kimlik doğrulama sistemleri için istediği zaman üretebileceği parola gibi gizli ve tahmin edilmesi zor bir şeydir. Parolalar bütün güvenlik sistemleri için ihmal edilmemesi gereken vazgeçilmez bir unsurdur. Diğer iki kimlik doğrulama yöntemi bir parola ile beraber kullanıldığında çok etkili olacaktır. Tüm bu çok bileşenli kimlik doğrulama mekanizması, güvenliğin birden çok katmanının

beraber çalışmasıyla sağlanır. Örnek olarak kullanıcının kartını geçirmesi sonrasında da bir parola girmesi gösterilebilir.

Kimlik doğrulamanın en önemli unsuru olan parolalar, zayıflıklara sahip olup tamamen parola sahibinin sağduyu ve öngörüsüne bağlıdır. Parolalar kolayca çalınabilir, kaybedilebilir, paylaşılabilir veya kırılabilir. Birden fazla parolayı yönetme ihtiyacından ve kullanılan parolanın etkin olarak kullanıldığını garanti etme zorunluluğundan kurumlar uyulması zorunlu parola kullanım politikaları kullanmaktadırlar. Bu durum daha karmaşık parolaların ortaya çıkmasına neden olmuş dolayısıyla parolaların akılda tutulmasını daha da zorlaştırmıştır. Bu durumun üstesinden gelebilmek için kullanıcılar parolalarını not etmeye başlamışlardır ki bu sağlanmak istenen güvenliği daha da kötü hale getirmektedir.

Güvenli parolalar oluşturmak

Parola oluşturma işleminde, parolanın uzunluğu ve karmaşıklığının zorunlu kılınmasıyla oldukça güvenli hale getirilebilir. Diğer bir zorunlu kılınması gereken husus parolaların düzenli olarak değiştirilmesidir. Parolanın uzun süre kullanılması başkaları tarafından öğrenilme olasılığını da arttırmaktadır. Genel olarak parola oluştururken;

- Parolalar tahmin edilmesinin zor olması fakat sahibinin de unutmaması için yeterli uzunlukta olmalıdır. Normal kullanıcılar için 8-10 karakterli fakat yönetim haklarına sahip kullanıcılar için daha uzun parolalar seçilmelidir. Böylece bir saldırganın parolayı kırma (crack) süresi de uzayacaktır.
- Parolalar sözlükteki kelimelerden seçilmemelidir.
- Parolalar harf, numara ve sembollerin karışımından meydana getirilmelidir.
- Parolalar kullanacak kişi tarafından belirlenmelidir.
- Parolalar kullanıcıların kolayca hatırlayabileceği şekilde olmalıdır.
- Parolalar kesinlikle bir yere not edilmemelidir.
- Parolalar belirli kurallar çerçevesinde düzenli olarak değiştirilmelidir.
- Parolalar herhangi bir şüphe duyulur duyulmaz değiştirilmelidir.
- Parola değiştirme politikaları kullanıcıların küçük değişikliklerle parola oluşturmalarını engellemelidir. Örneğin; Tag2mB yerine Tag3mB kullanılabilir. [Schinder D.L., 175]

5.6.2. Kullanıcının sahip olduğu bir şey ile kimlik doğrulama

Kullanıcının sahip olduğu bir şey, günümüzde internet kullanımı için en başarılı kimlik doğrulama şekli olup aynı anda sadece tek bir yerde olabilen fiziki bir cihazdır. Bunlar aşağıdakilerden herhangi biri olabilir;

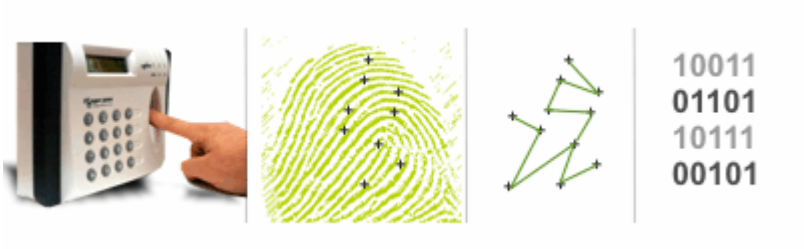
- **Manyetik kart**: Bir kredi kartı gibi arkasında statik temel hesap bilgilerini içeren siyah bir bant olan plastik bir karttır. Kart arkasında basılı olan CVS kodu gibi bilgiler içerebilir. Bu kodlar telefon veya internet üzerinden yapılan alış verişlerde karta sahip olunduğunun kanıtlanmasına yardımcı olur.
- **Akıllı kart**: Akıllı kartlar manyetik kartların daha gelişmiş bir versiyonudur. Üzerlerinde mikroişlemci ve bellek alanı içeren küçük bir çip bulunmaktadır. Bu sayede çip içerisinde bilgilerin saklanmasının yanında hesaplamalarda yapılabilmektedir. Manyetik kartların dış yüzeylerinde bulunan bilgilerin kopyalanabilmesi de güvenlik açısından akıllı kart kullanımının gerekliliğini ortaya koymaktadır. Bütün bilgilerin ve işlemlerin çip içerisinde yapılması ve çipin kopyalanamaması akıllı kartın en büyük artıları arasında yer almaktadır. Ayrıca akıllı kartın bilgilerine ulaşılabilmesi için kartın PIN (Personal Identification Number) koduna ihtiyaç duyulmaktadır. Oldukça güvenli bu sistemlerin tek dezavantajı akıllı kart okuyucuya ve yazılımına ihtiyaç duyulmasıdır.
- **Token**: Parolaların bu kadar kolay ele geçirilebilmesi veya parola denemeleri (brute force) nedeniyle parolaların bulunabilmesi, her seferinde başka bir parola üreten sistemlerin doğmasına yol açmıştır. Bunun için çeşitli yazılım veya fiziksel çözümler mevcuttur.

Şekil 5.6.2.1 : Token örneği

- Token, anahtar veya kart büyüklüğünde, bilgisayarın USB portuna takılabilecek içerisinde gizli bilgiler, parolalar, dijital sertifikalar saklayabilen akıllı bir karttır. Saldırgan tarafından ele geçirilse bile PIN kodu doğru olarak girilmedikçe hiçbir işe yaramaz. Ağın dinlenerek token veya akıllı kart tarafından oluşturulmuş şifrenin ele geçirilmesi durumunda ise bu şifre tek kullanımlık olduğu için saldırganın hiç bir işine yaramayacaktır.

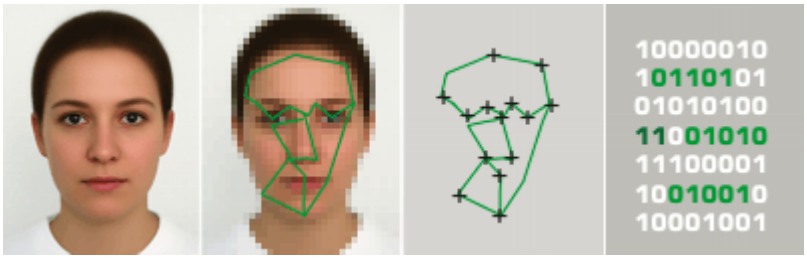
5.6.3. Kullanıcıya özel bir şey ile kimlik doğrulama

Kullanıcıya özel bir şey, kullanıcıya ait normalde değişmeyecek bazı fiziksel veya davranışsal özelliklerin ölçümüdür. Biyometrik sistemler de denilen kişinin tanımlanmasında kullanılan bu yöntemlerde, insan bedeninin bir parçasının ölçülmesi ile elde edilen fiziksel biyometriler; parmak izi, yüz, iris, retina, el izi ve damar tanımadır. Bir davranışın ölçülmesi ile veri elde edilen davranışsal biyometrilere ise ses tanıma ve imza tanıma örnek gösterilebilir.



Şekil 5.6.3.1 : Parmak izi tanıma sistemleri işleyişi

Biyometrik Sistemler bireyin belli biyolojik karakteristiklerini sadece o kişiye özel tek ve benzersiz bir koda dönüştürür. Bu kod elektronik ortama kaydedilir, kayıtlar ile ilgili kişi anında karşılaştırılır ve sonuca varılır.



Şekil 5.6.3.2 : Yüz tanıma sistemleri işleyişi

Biyometrik sistemler kişilerin kontrollü geçişini veya erişimini sağlamayı amaçlarlar. [Han Vinck A.J., 176] Kartlı veya parola kullanılan sistemlerin aksine biyometrik sistemlerde bireyin özelliklerinin kopyalanması veya taklit edilmesi neredeyse imkânsızdır. Ayrıca kimlik doğrulama kişinin fiziksel veya davranışsal özelliği ile yapıldığı için kişi özelliğini başkasına devredemez, unutamaz veya kaybedemez. Dolayısı ile kartlı veya parola kullanılan sistemlerde yaşanan kaybedilme, unutulma veya çalınma gibi problemler de yaşanmaz.

5.7. İÇERİK SÜZME SİSTEMLERİ (CONTENT FILTERING)

Internetin kullanımının artması web ortamını Google, Yahoo ve Altavista gibi geniş arama motorlarının bunların yarısını bile bilemediği sürekli ve hızla değişen bir dünya haline getirmiştir. Bu durumda sayfalar değiştikçe ve yerine yenilerinin türemesi web adresleri üzerinden süzme işlemini gittikçe zor hale getirmiştir. Burada webin daha güvenli ve daha temiz olabilmesi için ihtiyaç duyulan şey, ziyaret edilen her sayfada uyuşturucu, şiddet, silah, ırkçılık, terör ve pornografi gibi öğelerin tespitini ve istendiğinde engellenmesini sağlayacak bir yazılımdır. Bu tip yazılımlara içerik süzme yazılımı denir.

5.7.1. Kurumsal İçerik Süzme Yazılımları

İçerik süzme yazılımları kurumsal ağlarda bir proxy sunucu veya güvenlik duvarı ile beraber çalışarak ağın tüm kullanıcılarının http trafiğini kontrol eder, süzer ve girilen sayfaların kayıtlarını tutar. Böylece yaşanabilecek verim ve üretim kayıplarını en aza indirmekte kurum adına yardımcı olur. SurfControl Web Filter (www.surfcontrol.com), Websense Enterprise (www.websense.com), Web Inspector (www.zixcorp.com) ContentKeeper (www.contentkeeper.com), Secure Computing SmartFilter (http://www.securecomputing.com/gateway/content_filtering.cfm) ürünleri sunucu tabanlı içerik süzme yazılımlarına örnek olarak verilebilir.

5.7.2. Kişisel İçerik Süzme Yazılımları

Kişisel içerik süzme yazılımları, özellikle ebeveynler tarafından çocukların internette sakıncalı olarak görülen sayfalara erişememeleri için kullanılmaktadır. Bu tip yazılımlar, ayrıca küçük çaplı internet kafelerde de kullanılabilmektedir. PC tabanlı kişisel kullanıma uygun içerik süzme yazılımlarına örnek olarak AOL Parental Control, Arlington Custom Browser, Cyber Patrol, Cyber Sentinel, Cybersitter, Net Nanny, Bsafe Home ve Safe Eye gibi sadece bu amaç için hazırlanmış ürünler piyasada bulunabildiği gibi, Norton Internet Security, Trend Micro Internet Security, Kaspersky Internet Security gibi toplam bir koruma sağlayan yazılımların içine gömülü olarak ta sunulabilmektedir.

CensorNet: Linux tabanlı kurumsal, eğitim ve kişisel kullanımlar için internet web süzme ve yönetimi çözümü sunan açık kaynak kodlu bir yazılımdır.

DansGuardian: Linux, FreeBSD, OpenBSD, NetBSD, MacOS X, HP-UX ve Solaris üzerinde Squid gibi bir proxy ile beraber çalışabilen açık kaynak kodlu içerik süzme yazılımıdır. Cümle karşılaştırma, MIME süzme, dosya uzantısına göre süzme, POST sınırlandırma, PICS (Platform for Internet Content Selection) süzme ve adrese göre süzme de dahil olmak üzere birçok yöntem kullanarak ziyaret edilen sayfaların içeriğini süzer. Sadece yasaklı adresler veritabanından aldığı bilgilere göre süzme yapmadığından dolayı gerçek bir web içerik süzme yazılımıdır. [177]

Dansguardian, kullanıcı internet tarayıcısı ile Proxy arasında bulunur ve aradaki trafik üzerinde gerekli işlemleri yapar. Kullanıcıdan web sunucusuna giden istek dansguardin'a gelir. Gerekli filtreleme işlemelerinden sonra paket Proxy'ye oradan da web sunucusuna iletilir. Web sunucusu paketi işleyip gerekli cevabı Proxy'ye gönderir ve oradan da tekrar dansguardin'a iletilir. Gerekli filtreleme işlemlerinden geçirildikten sonra paket kullanıcıya geri döner. Dansguardian basit olarak bu şekilde çalışmaktadır.

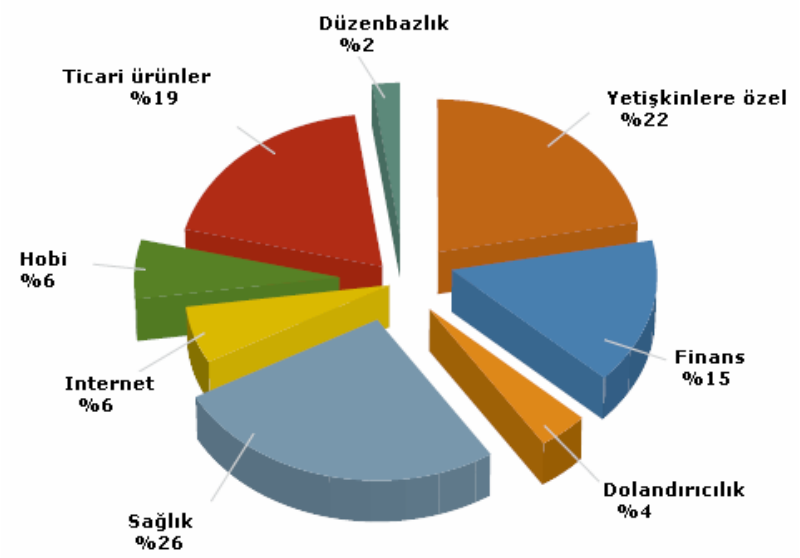
- **PICS (Platform for Internet Content Selection)**: PICS, etiketleri (metadata) internet içeriği ile ilişkilendiren bir özelliktir. Başlangıçta ailelerin ve öğretmenlerin, çocukların internet erişimini kontrol edebilmesi amacıyla tasarlanmış fakat ayrıca etiketlerin kod imzalama ve gizlilik gibi diğer kullanımlarını da kolaylaştırmaktadır. [178]

5.8. SPAM TESPİT VE ENGELLEME SİSTEMLERİ

Spam nedir?

SpamAssasin projesi spam tanımını, talep edilmeyen e-posta (Unsolicited Bulk Email: UBE) olarak yapmıştır. Spam sözcüğü ilk olarak Monthy Python komedi grubunun bir skeçinde, sunduğu akşam yemeği menüsünde spam marka salam kullanılan bir restoranı konu alarak sürekli spam kelimesini tekrar etmesiyle duyulmuştur. İlk örneği 3 Mayıs 1978'de görülmüş, günümüz anlamı ile ilk kullanımı 12 Nisan 1994'te Canter ve Siegel isimli şahısların 90 dakikadan az sürede yaklaşık 6000 Usenet haber grubuna göndermesiyle gerçekleşmiştir. [179]

Spam, kullanıcıları ve sistem yöneticilerini rahatsız eden Truva atları, virüsler, solucanlar ve phishing girişimlerinden sonra en büyük güvenlik sorunlarından biri haline gelmiştir. Ayrıca ağ kaynaklarının ve posta sunucularının hizmet verememesi veya performanslarının düşmesine de yol açmaktadır.

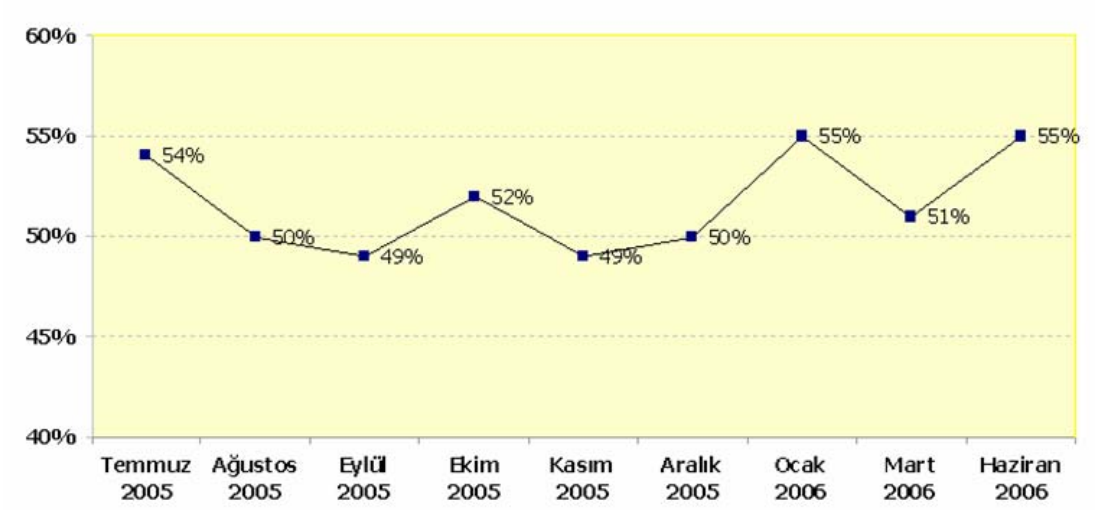


Şekil 5.8.1 : Spam kategorileri

Spam kategorilerinin oranlarının gösterildiği Şekil 5.7.1.1. de, 2006 yılının ilk altı ayında tespit edilen en yaygın spam tipi olarak %26 lık oran ile sağlık hizmetleri gelmektedir. Bir sonraki en büyük spam kategorisi ise %22 ile yetişkinlere özel konulu olanlardır. [180]

Neden spam gönderiliyor?

Bunun cevabı elbette para kazanmak amacıyla spam gönderiliyor olacaktır. Mevcut yazılımlar ve teknikler ile tek bir spam gönderici günde 200 milyon mesaj gönderebiliyor. Toplu olarak bakıldığında mali getirisinin yüksek olması artık spam göndermeyi bir uğraş olmaktan çıkarıp bir iş kolu haline getirmiştir. 2001 yılında e-postaların %8 i spam iken şu an %60 lar seviyesinde bir oranda spam içermektedir. Önümüzdeki yıl %70 ler seviyesinde olması bekleniyor.



Şekil 5.8.2 : Spam miktarının toplam e-posta miktarına oranının aylık dağılımı

Spam gönderenler e-postaları nasıl elde ediyorlar?

- **Web site tarama**: Web tabanlı e-posta siteleri üzerinde adres defterlerini tarayan yazılımlar bulunmaktadır. Ayrıca web sayfaları içerisine gömülü adresleri arayıp tespit eden ve liste oluşturan yazılımlar da mevcuttur.
- **Kelime tabanlı spam gönderme**: Rasgele kelimeleri ve sık kullanılan isimleri bir araya getirip geçerli bir e-posta adresi elde etmeye yarayan yazılımlar bulunmaktadır. Çok fazla kişinin e-posta kullandığı düşünülürse Mehmet Öztürk gibi sık görülen isimlere ait adresler birçok posta hizmeti veren büyük firmalarda tükenmiş durumdadır. Bu nedenle kullanıcılar kolay çağrışım yapan kelimeleri veya isim, soy isim veya her ikisinin sonuna doğum tarihlerini, doğum yerlerini getirerek kombinasyonlar oluşturmaktadırlar. Örneğin; mehmet@dotmail.com, mehmetozturk@dotmail.com, mozturk@dotmail.com,

mehmeto@dotmail.com, mehmet1972@dotmail.com, ozturk1972@dotmail.com vb. Kelime türeten ve milyarlarca denemeyi bir saat içerisinde yapan yazılımlar kullanan spam göndericileri kolaylıkla bu kombinasyonlara erişebilmektedirler.

- **Ticari e-posta listeleri**: Milyonlarca e-posta adresi çok düşük bir ücret karşılığında internetten indirilebilir şekilde veya CD-ROM üzerinde satılmak üzere mevcuttur.
- **Haber grupları, tartışma forumları ve interaktif web sayfaları**: Kullanıcı bir web sitesinden düzenli haber iletileri almak için e-posta adresini gönderdiğinde veya tartışma forumuna kayıt yaptırdığında bu tip haber gruplarından e-posta adreslerini toplayabilen yazılımlar vasıtasıyla kullanıcı adresi spam göndericiler tarafından kullanılabilir hale gelir.
- **Yarışmalar ve diğer ücretsiz promosyonlar**: Genellikle düzenlenen yarışmalar ve ücretsiz hediyeler için kayıt yaptırıldığında kullanıcıya ticari bir e-posta alacağı iletilir ve kullanıcı da bunu kabul eder. Bu yarışmalar e-postaların toplanabilmesi için kurulan bir düzenin parçasıdırlar.
- **E-posta iletimi**: Eğer düzinelerce kişiye bir e-posta iletilecekse kime (To) kısmına kendimizi göndereceğimiz bütün kişileri de Bcc (blind carbon copy) alanına yazmak gerektiği unutulmamalıdır. Böylece kişilerin adresleri görünmez bir şekilde gönderilir. Bcc'nin kullanılmadığı zamanlarda spam göndericiler için bu adresler, kolay hedefler haline gelmektedir.

Spam tespit ve önleme sistemleri

Gün içinde sürekli güncellenen ve ek olarak istendiğinde aktif olarak son kullanıcıların kendilerine özel kurallar tanımlamasına olanak tanıyan spam tespit çözümleri, spam saldırılarına karşı oldukça etkili bir koruma sağlamaya başlamışlarsa da spamların tam bir çaresi bulunmamaktadır. Bununla beraber birçok değişik tipteki spam için farklı filtreler kullanılmaktadır. Yenilenen çok katmanlı çözümlere rağmen spam göndericiler her katmandan kaçabilecek yollar bulabilmektedirler. Örneğin, son dönemlerde text tabanlı e-postalar yerine resim tabanlı spam e-postalar yaygınlaşmıştır. Spamları yakalamak ta çoğu zaman yeterli değildir. Normal postaların sahiplerine gittiğinden emin olabilmek için, antispam yazılımının yakaladığı spam adedinden daha çok, yüksek seviyede doğruluk oranına (accuracy) sahip olması önemlidir. Spam tespit ve önleme sistemleri, otomatik olarak güncellenebilmeli, çok fazla ayar gerektirmemeli, kolay

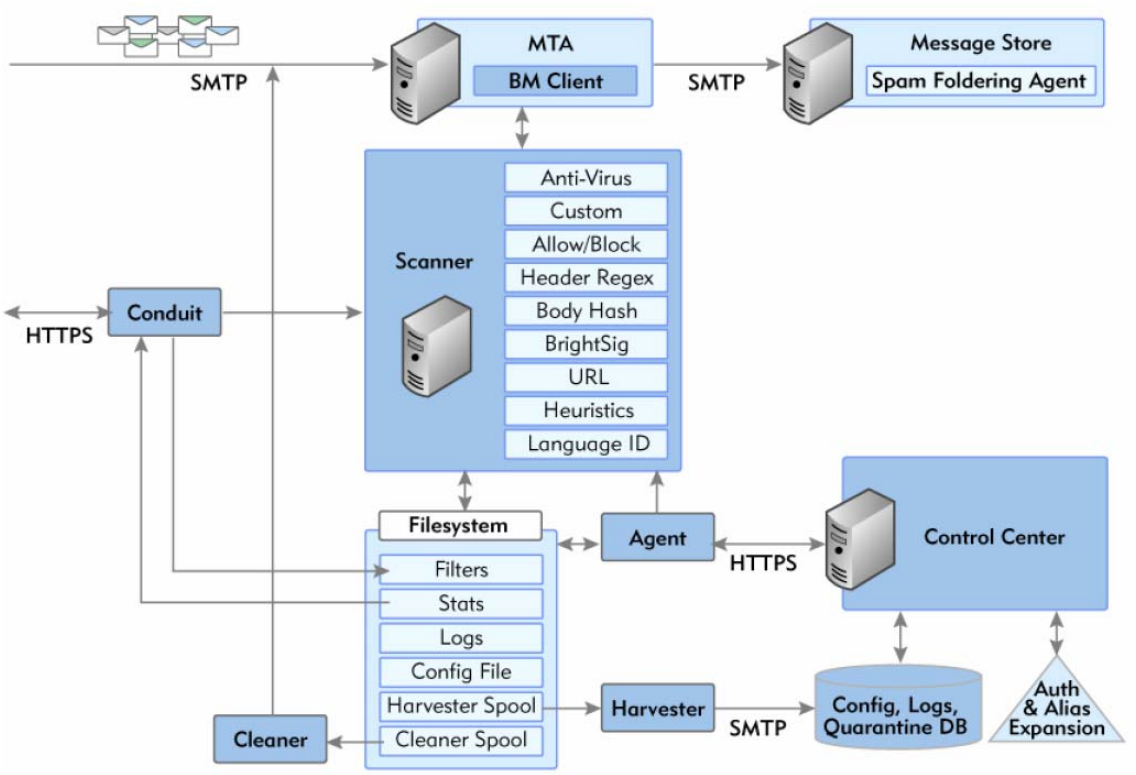
kurulabilmeli, kolay yönetilebilmeli ve yanlış olumlu (false positive) durumlarına üretici tarafından çözüm getirilebilmelidir. Bu yazılımlar, sistem yöneticisinin kendi kontrol, güvenlik ve yönetim esnekliğine sahip bir sunucu üzerine kurulabildiği gibi, güçlendirilmiş bir işletim sistemi, posta iletim programı (MTA) ve uygulama yazılımı içeren bir kutu üzerinde de kurulu olabilir.

Anti-spam yazılımları spamları tespit etmede genellikle aşağıdaki test ve teknikleri kullanırlar:

- **E-posta başlık analizi**:Ufak tutarsızlıklara karşı e-posta başlıklarını tarayıp postanın geçmiş veya gelecek tarihli, sahte ID ve benzeri durumları ortaya çıkarır.
- **Kelime kontrolü ve tekst analizi**: Posta gövdesi spam kelimeleri, büyük harf ile yazılmış kelimeler veya bir şeyi tıklamaya ve satın almaya davetler gibi bilinen içeriklere göre taranır.
- **Bayesian spam filtreleme**: Gelen postanın istatistiki olarak spam olabilirliğini hesaplar böylece benzer postalar gelecekte daha kolay tanımlanabilir.
- **Gerçek zamanlı DNS kara listeleri (DNSBL, RBL) kontrolü**: Postalar, servis sağlayıcılar ve sivil toplum örgütlerinden (www.spam.org.tr, www.mail-abuse.org, www.abuse.net, http://www.ordb.org) temin edilen e-posta adresleri ve gönderen IP adreslerini içeren kara listeler üzerinde kontrol edilir.
- **SPF (Sender Policy Framework)**: Postalardaki sahte "kimden" adreslerini tespit etmek üzere geliştirilmiş bir standarttır.
- **Grafik spam tespiti**: Sıradan spamlarda olduğu gibi grafik imzalar oluşturulur ve imza veritabanına eklenir.
- **Kullanıcı tarafından oluşturulan temiz ve kara listeler**

Antispam yazılımları kurumun e-posta sunucusu üzerine veya onun birlikte çalışacağı ayrı bir antispam sunucu üzerine kurulabilir. Bu durumlarda gelen ve giden postalar ilk olarak bu antispam (genelde antivirüs sunucu ile beraber çalışırlar) sunucuya gelir, daha önce bahsi geçen teknik ve testlerden geçerek posta sunucuya teslim edilir. Bu tip kurumsal ticari çözümlere örnek olarak Symantec Brightmail Antispam 6.0, Kaspersky Anti-Spam 3.0, McAfee SpamKiller for Mail Servers, Trend Micro Spam Prevention System 2.6 ve Sophos PureMessage for UNIX verilebilir.

- **Symantec Brightmail Antispam 6.0**: Kurumsal spam tespit ve önleme yazılımı olan Symantec Brightmail Antispam 6.0, Windows, Solaris, Linux (Red Hat Enterprise ve SuSe işletim sistemleri üzerinde ve Microsoft IIS SMTP, Exchange 2000, Exchange 2003, Sendmail 8.12, Sendmail Switch 3.1, Exim, Postfix 2.1.4, QMail (Q2/3 2004), Sun Messaging Server 5.2/6.0 posta iletim programları ile beraber çalışabilir. Antivirüs tarama, merkezi yönetim ve raporlama özelliklerine sahiptir. [181]



Şekil 5.8.3 : Symantec Brightmail Antispam 6.0 Mimarisi

Kaspersky Anti-Spam 3.0:

Kaspersky Anti-Spam yazılımının spam temizleme işlevi dört adımda yapılmaktadır:

- Spam laboratuvarı tarafından internette spam göndericilerin yoğunlukla kullandığı sitelere üye olunarak, ücretsiz e-posta servislerini kullanan üyelerden ve kullanıcılardan gelen geri bildirimlerden spam örneklerinin toplanması gerçekleştirilir.

- Toplanan spamlar dilbilgisi laboratuvarında başlıklarına ayrılır ve her mesaj için ayrı imzalar oluşturulup veritabanına kayıt edilir. İmzalar oluşturulduktan sonra deneme yanılma yoluyla (heuristic) analiz aşamasına geçilir.
- Her yirmi dakikada bir düzenli veritabanı güncellemeleri ile en yeni spam mesajlarına ait bilgiler temizleme sunucusuna gönderilir.
- Temizleme sunucusu: Spam filtreleri ağ geçidi üzerine kurulan ve gelen spam mesajları filtreleyen sunucu programlarıdır. Günde yüzlerce gigabaytlık trafiğe sahip kurumların etkili ve verimli şekilde korunmasını sağlar. [182]

Desteklediği posta sunucular: Sendmail 8.13.5, Postfix 2.2.2., Qmail 1.03., Exim 4.52., Communigate Pro 4.3.7

Desteklediği işletim sistemleri: RedHat Linux 9.0, RedHat Fedora Core 3, RedHat Enterprise Linux Advanced Server 3, SuSe Linux Enterprise Server 9.0, SuSe Linux Professional 9.2, Mandrake Linux version 10.1, Debian GNU/Linux version 3.1, FreeBSD version 4.10, FreeBSD version 5.4

Sunucular için açık kaynak kodlu spam engelleyici yazılımlara örnek olarak SpamAssasin (http://spamassassin.apache.org/), Razor (http://razor.sourceforge.net/), Anti-Spam SMTP Proxy (ASSP) (http://assp.sourceforge.net/), SpamBayes (http://spambayes.sourceforge.net/) gösterilebilir.

- **SpamAssassin**: Spamassasin içinde 800 den fazla kural içeren ve bu kurallara göre bir postanın spam olup olmadığına karar veren açık kaynak kodlu bir spam önleme aracıdır. Anti-spam testleri ve konfigürasyonu text dosyasında tutulduğu için yapılandırmak ve yeni kurallar eklemek oldukça kolaydır. Esnek ve gelişmiş programlama arabirimi sayesinde procmail, sendmail, Postfix, qmail ve birçok posta sunucusu ile çalışabilir. Ayrıca birçok spam önleme aracı ile de birlikte bir bütünlük içinde çalışabilir. Bunların başında Razor, Pyzor, Dcc gelir. Ayrıca RBL'leri (kara listeleri) kontrol edebilir ve MX kaydı sorgulaması yapabilir. En son versiyonu SpamAssassin 3.1.7 dir. [183]

Sunucular için kurumsal çözümler olduğu gibi kişisel kullanımlar için de hem ticari hem de ücretsiz anti-spam yazılımları bulunmaktadır. Bunlar ayrı ayrı olabildikleri gibi tek bir güvenlik paketi yazılımının içinde modül olarak ta kullanılabilmektedir.

Windows bilgisayarlar için ücretsiz anti-spam programlarına ait örnekler: http://www.snapfiles.com/Freeware/comm/fwspam.html
Açık kaynak kodlu anti-spam yazılımlarına örnekler: http://freshmeat.net/search/?q=anti-spam&orderby=&filter=2=26 sitelerinden elde edilebilir.

5.9. GÜVENLİK ÇÖZÜMLERİNDE YENİ EĞİLİMLER

Öncelikle eğilimleri belirleyen unsurlar olan tehditler ve güvenlik teknolojilerini incelemek yerinde olacaktır. Saldırganlar ve yarattıkları tehditler olmasa sahip olduğumuz, bizim için bir değer arz eden ağ ve bilgi kaynaklarımızı korumak için önlemler, yöntemler ve cihazlar geliştiren güvenlik sektörü ortaya çıkmaz bizim de bu kadar emek ve para harcamamıza gerek kalmazdı. Maalesef bu düşünce ne kadar güzel ve ideal olsa da gerçek olması mümkün değildir. Gerçek olan şudur; çeşitli bilgi düzeylerinde, kendilerine göre çeşitli nedenleri olan saldırganlar ve amaçlarını yerine getirecek araçları ve teknikleri vardır ve gelecekte de var olacaktır. Daha kısa süre öncesine kadar birçok hacker saldırısının hedefi bankalar ve devlet daireleri gibi yüksek güvenlikli kurumlar iken şimdi ister bir ister binlerce IP adresine sahip olsun internete bağlı bütün kurumlar hedef haline gelmiştir.

Saldırganların ana hedefinin kurumsal bağlantılar ve sunucular olduğu zamanlarda iyi yapılandırılmış bir güvenlik duvarı bir çok ağın güvenliğini sağlamak için yeterliydi. Daha sonra virüsler ve solucanlar bu derece yaygınlaşmaya başlayınca kurumlar e-posta üzerinden gelenlere önlem olarak smtp gateway yazılım ve donanım ürünlerine yöneldiler. Bunları, web üzerinden gelebilecek tehditlere karşı içerik filtreleme ve sonunda anti-spam yazılımları takip etmiştir. Sonuç olarak bu katmanlı güvenlik anlayışı beraberinde yönetim zorluğu ve kurulum maliyeti getirmiştir.

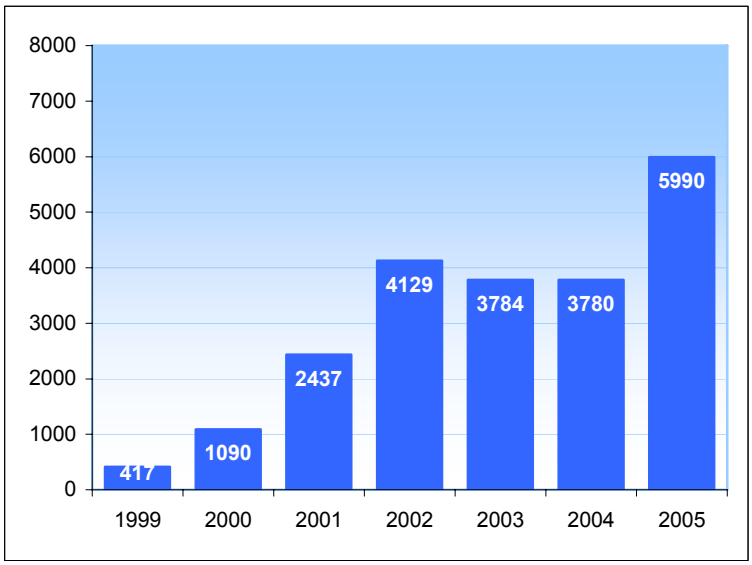
Son yıllarda geliştirilen programların ve uygulamaların Web tabanlı (ERP, CRM vb.) olması önümüzdeki yıllarda karşılaşacağımız tehdit ve saldırıların da büyük çoğunluğunun bu yönde olacağını göstermektedir. Bu tip tehditlere karşı güvenliği

sağlayabilmek için de uygulama katmanında analiz ve tespit yapabilecek ilave teknolojilere ihtiyaç vardır.

5.9.1. Risk artışına sebep olan faktörler

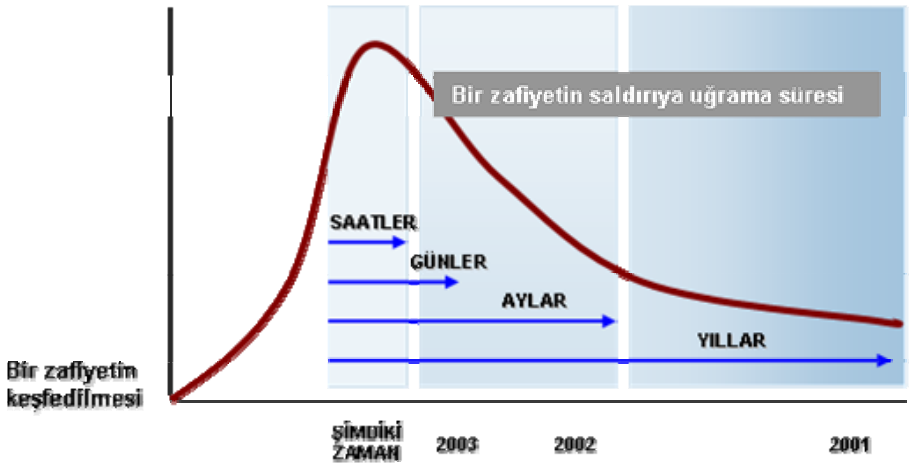
Kurumların yüzyüze geldiği ağ güvenliği problemlerinin artmasına sebep olarak aşağıdakiler gösterilebilir:

- Ağların sahip olduğu giriş noktaları hızla artmaktadır. Örneğin; evden bağlanmak isteyen kullanıcılar için VPN bağlantıları ve mobil kullanıcılar için kablosuz erişim noktaları gibi. Bu durumda kullanıcılar ev veya taşınabilir bilgisayarlarına bizim kontrol edemediğimiz yazılımlar kurarak ve bilgisayarlarının tam olarak güvenliklerini sağlamayarak tehditlerin ortaya çıkmasına neden olmaktadır.
- Ağlar ve uygulamalar daha karmaşık ve daha zor yönetilir bir hale gelmekte bununla beraber kalifiye güvenlik uzmanı az bulunmakta ve IT bütçeleri bu gelişmelere rağmen yerinde saymaktadır.
- Yazılım geliştirme süreçlerinin ekonomik nedenlerle kısalması ürünlerin yeterince testten geçmeden ve güvenlik açıklarının kapatılmadan piyasaya sürülmesine neden olmaktadır. Bunun sonucunda yeni keşfedilen güvenlik zafiyetlerinde son altı yılda on beş kat artış gözlenmiştir. (Şekil 5.8.1.1. Computer Emergency Response Team Güvenlik Zafiyetleri Raporu) [184]



Şekil 5.9.1 : CERT Güvenlik Zafiyetleri Raporu

- Saldırı araçlarının daha az beceri gerektirmesi, daha kolay bulunabilmesi ve daha otomatik hale gelmesi saldırganların başarı oranlarını da arttırmıştır. Bu saldırı araçlarının, geniş ölçekte saldırılar için programlanmış olması nedeniyle tek bir saldırgan çok daha fazla hasara sebep olabilmektedir.
- Kendi kendine çoğalıp yayılabilen solucan, virüs ve Truva atları gibi kötü amaçlı kodların, yaşam süreleri uzamakta ve hasarın katlanarak büyümesine neden olmaktadırlar.
- Ağ saldırılarının yaşam döngüsü gittikçe kısalmaktadır. Şekil 5.9.2. de görülebileceği gibi, bir zaafiyetin ortaya çıkması ve bunun kullanılarak saldırı düzenlenmesi süresi artık birkaç saatlik bir süreye inmiş durumdadır [185]. Bu nedenle, kurumların saldırganlar ve solucanlar tarafından kullanılmadan önce, bu zafiyetleri tanımlamak ve düzeltmek için daha az zaman kullanmak zorundadırlar.



Şekil 5.9.2 : Zafiyetlerin ortaya çıkması ve bunlar üzerinden saldırı düzenlenmesi arasındaki ilişki

5.9.2. Ağ geçitleri

Ağ ve bilgi güvenliğini tehdit eden unsurların evrimi doğal olarak ağ güvenlik cihazlarını da bu yönde bir gelişmeye zorunlu bırakmıştır. Güvenlik çözümlerine, uygulama katmanından gelebilecek tehditlere karşı içerik denetleme ve analiz yapabilecek güvenlik ağ geçitleri (gateway) eklenmiştir. Güvenlik ağ geçitleri yapı olarak uygulama katmanı proxy'lerdir. Uygulama katmanı proxy, kullanıcı tarafından

başlatılmış TCP oturumunu sonlandırır ve hedef sunucuya yeni bir TCP oturumu başlatır.

SMTP Ağ geçitleri

Güvenlik ağ geçitlerinin en yaygın kullanımı e-posta üzerinedir. E-posta sistemlerinin büyük çoğunluğu genelde "relay" veya MX (mail exchange) adı verilen adanmış bir SMTP proxy kullanır. E-posta sakla ve gönder yapısından dolayı bir ağ geçidi cihazı için doğal bir protokoldür. SMTP ağ geçidi cihazları spam, virüs, phishing ve hizmet durdurma saldırılarını önlemek için geliştirilen çok gelişmiş güvenlik sistemleri ile donatılmışlardır. Bununla birlikte yıllardır 25 numaralı port için geliştirilen savunma şekilleri gibi saldırganlar tarafından yürütülen taktikler de bu artan bilgi düzeyine uyum sağlamıştır. Son saldırı taktikleri birleşik tehditler (blended threats) de denilen SMTP, HTTP, FTP ve online mesajlaşma gibi diğer portlardan akan trafiğin kombinasyonunu kullanmaktadır. Buna en iyi örnek Sober-N ve devamı Sober-Q verilebilir.

HTTP Ağ geçitleri

Bu yöndeki saldırılarla mücadele edebilmek için birçok firma SMTP ağ geçitleri ve onların güvenlik algoritmaları ile işbirliği içinde çalışabilecek yüksek performanslı HTTP ağ geçitleri geliştirmişlerdir. Web ağ geçitlerinin çalışma mantığı e-postaların aksine asenkron olarak yapılmaktadır. HTTP protokolünün gerçek zamanlı bir protokol olması nedeniyle web ağ geçidi kullanımı son kullanıcının web erişimini etkilemektedir. İlginçtir web güvenliği ağ geçitlerinin gelişiminde yaşanan sorunlar on yıl önce web önbellekleme (caching) endüstrisinde yaşananlarla benzerdir. Web önbellekleme işleminin amacı, kullanıcıların içeriğe hızlı bir şekilde erişimini sağlayarak bant genişliği tasarrufu sağlamaktır. Web önbellekleme işlemi depolama alanı sorununun yanında ayrıca yüksek performanslı dosya sistemlerine ihtiyaç duymaktadır. Bu konuda en yaygın kullanım açık kaynak kodlu Squid Web önbellekleme yazılımı üzerine olmuştur. [186]

Yeni web güvenlik ağ geçitleri, bu Web önbellekleme platformları üzerine inşa edilmişlerdir. Fakat bu platforma yüksek performanslı içerik tarama, yüksek hızlı erişim kontrolü ve basit yönetim özellikleri ilave edilmiştir.

5.9.3. Tehdit Yönetim Cihazları

Bu kadar çok mükemmel yazılım tabanlı güvenlik uygulaması geliştirilirken neden kullanıcılar tehdit yönetim güvenlik cihazlarını tercih ediyorlar? (Örneğin; Marmara Üniversitesi, Selçuk Üniversitesi, Işık Üniversitesi vb.) Aslında bunun cevabını vermek kolay olmamakla beraber; rahatlık, kurulum kolaylığı ve merkezi yönetim gibi özellikler bu tip cihazların artı değerleri olarak öne çıkmaktadır. Aşağıda sıralanan faktörler bu sektörün büyümesinde etkili olmaktadır:

- Hepsi birarada yaklaşımı (all in one), ürün seçimini, entegrasyonunu ve sürekli destek sağlanmasını kolaylaştırıp karmaşıklığı azaltmaktadır.
- Cihazlar, genelde çok az kurulum ayarı gerektiren tak çalıştır ürünlerdir. Kullanıcı yapılandırma hataları ve değişiklikleri en aza indirgenmiştir.
- Uzak kampüsler gibi dağıtık yapılı ağların uç noktalarına yerleştirildiğinde, bu bölgede nitelikli güvenlik personeli bulundurma gerektirmeden, uzaktan yönetim kolaylığı sağlar.
- Uygulama tabanlı mimarileri (ASIC) sayesinde standart bir performansa sahiplerdir.
- Kutuda bir problem oluştuğunda, teknik olması gerekmeyen bir personel tarafından da kolayca yerine bir başkası takılarak çok çabuk arıza giderilebilir. Bu husus uzak kampüsler için daha da önemlidir.
- Cihazın işletimi, performans ve uygulama işlevselliği, merkezi bir yönetim konsolu tarafından sağlanabilir.

5.9.4. Birleşik Tehdit Yönetim Sistemleri (Unified Threat Management)

Ağ ve bilgi güvenliğine yönelik tehditlerin sürekli gelişip değiştiği bir ortamda, güvenliği sağlayabilmek ve koruyabilmek için iki temel yaklaşım ortaya çıkmıştır. Bu yaklaşımlardan bir tanesi; güvenlik duvarı, IPS, SMTP gateway, içerik filtreleme ve Anti X (virüs, spam, phishing, pharming gibi hepsini içeren) gateway gibi farklı işlevleri yerine getiren, alanında en iyi birkaç farklı çözümü bir arada kullanmaktır. Fakat kullanılan tüm bu çözümlerin kurulumlarını, bakımlarını ve güncel kalmalarını sağlamanın özellikle küçük ve orta boy işletmeler için pahalı ve zor bir yöntem olabileceği düşünülmektedir.

Diğer bir düşünce ise; kurumlara, güvenlik duvarı, saldırı önleme sistemi, anti-virüs, anti-spyware, SSL ve IPSEC VPN, Web uygulama güvenliği, P2P ve anlık mesajlaşma denetimi, VoIP güvenliği ve uzak PC'lerin güvenlik denetimi ihtiyaçlarını tek çatı altında karşılayan bir çözüm sunma fikridir. Bu fikir doğrultusunda ağ güvenlik teknolojileri sektöründe yeni bir eğilim oluşmuş ve buna da birleşik tehdit yönetim sistemi, UTM (Unified Threat Management) denmiştir.

UTM Kutu Çözümleri

UTM cihazları, mevcut güvenlik duvarı/VPN çözümlerine, IPS, ağ geçidi anti-X, içerik filtreleme, casus yazılım ve spam engelleme kabiliyetleri ilave edilerek oluşturulmuştur. UTM çözümleri ayrıca bütünleşik yönetim, gözlemleme ve loglama özelliklerine sahiptir. Secure Computing Sidewinder G2, SonicWall, ISS Proventia M50, Fortinet FortiGate serisi, TippingPoint X505 cihazları bu tip çözümlere örnek olarak gösterilebilir.

UTM Yazılım Çözümleri

UTM cihazlarının masa üstü bilgisayarlar için uygun yazılım olarak karşılıkları sektörde internet güvenlik paketleri olarak anılmaktadır. TrendMicro Internet Security, Symantec Internet Security, ZoneAlarm Internet Suite, McAffee Internet Security Suite bunlara örnek gösterilebilir.

6. GÜVENLİK POLİTİKALARI

Güvenlik politikaları her kurum için olduğu gibi üniversiteler için de büyük öneme sahip, kurumun iyi tanımlanmış ve düşünülmüş güvenlik stratejisini işler hale getirebilmek için neler yapılması gerektiğini yüksek seviyede ifadelerle anlatan kurallar dizisidir. Bu durum bir çok kurumun göz ardı ettiği bir husustur. Aslında kurumun güvenlik politikasının bütünü, belirli konuları, cihazları ve amaçları anlatabilmek için yazılmış kendi içinde bir bütünlüğe sahip birden fazla güvenlik politikasından meydana gelmiştir.

Önceki bölümlerde güvenliği tehdit eden unsurlar ve bunlara karşı alınabilecek teknik önlemler ayrıntılarıyla açıklanmıştı. Etkin bilişim güvenliği sağlayabilmek için teknolojinin gerekli bir bileşen olduğunu, ancak hiçbir zaman tek başına yeterli olamayacağı yadsınamaz bir gerçektir. Kurumsal ölçekte bilişim güvenliğini bir bütün olarak görüp tüm boyutlarını göz önüne alarak, bir kurumsal bilişim güvenliği yapısı oluşturmak temel hedef olmalıdır. [Özgit, A., 187] Bu hedef doğrultusunda, her kurumda olduğu gibi üniversitelerde de bir bilgi güvenliği çalışması yapılmasının gerektiği açıktır. Bu şekilde bir çalışma sonrası ortaya çıkarılacak güvenlik politikası, kurumun güvenlik ile ilgili ihtiyaçlarını, beklentilerini ve kurum yöneticilerinin bu konuda yürütülecek faaliyetlere olan desteğini açık bir biçimde ortaya koyacaktır.

Bir güvenlik politikasının hedefi, nelerin korunması gerektiğini (kurum değer ve varlıklarının belirlenmesi), kimin bu koruma işleminden sorumlu olduğunu (bilgi güvenliği sorumlulukları) ve bu koruma işleminin nasıl gerçekleştirileceğini (politikalar, standartlar, yönetmelikler ve talimatnameler) tanımlamaktır [188]. Bu, kurumun güvenlik fikri karşısındaki duruşunu yasallaştıran, ölçülebilir bir materyal sağlar.

Bir güvenlik politikası:

- Ortak kurallar kümesidir.
- Yüksek seviyede yönergeleri içerir ve bunlarla ortak davranış ve korunma biçimi sağlar.
- Güvenlik amaç ve hedeflerini belirler.

- Etikleri tanımlar ve sorumluluk yükler.
- Atılması gereken adımları belirler.
- Personele, kurum yönetiminin beklentilerini açıklar.
- Personelin neler yapmaları gerektiğini belirler.
- Kurumun mevcut güvenlik duruşunu bir temele oturtur [Brennan Linda L. ve Johnson Victoria E., 189].
- Güvenlik çözümlerini uygulamak için bir çatı oluşturur.
- İzin verilen ve verilmeyen davranış biçimlerini belirler [Laet G. ve Schauwers G., 190].
- Güvenliğin sağlanabilmesi için gerekli araç ve prosedürleri tanımlar.
- Ortak bir dil ve rolleri tanımlar.
- Güvenlik ihlallerinin nasıl ele alınacağını belirler.
- Olası bir güvenlik ihlali sonrasında oluşabilecek davalara karşı yasal destek oluşturur.

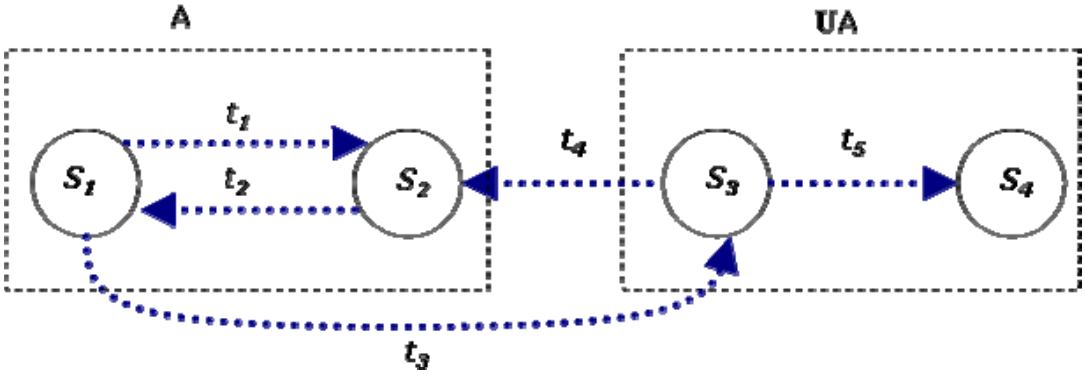
Etkin bir güvenlik politikası ayrıca kişileri de korur. Bilgi güvenliğini tehdit edecek bir risk oluştuğunda, karar verecek yada müdahale edecek kişilere bir sorumluluk yüklenmektedir. Güvenlik politikaları, zarar görme korkusu olmaksızın sorumlulara harekete geçme olanağı tanır. Böylece kurumun kaderini kendi kontrolleri altına almış olurlar. Güvenlik politikası, kullanıcıların kişisel insiyatiflerini yok ederek veya en azından azaltarak, verilerin kendi kendini korumasını sağlar. [191]

Bir bilgisayar sistemini, durum değiştiren geçiş fonksiyonlarına sahip bir sonlu durum özdevinirlik (finite-state automaton) yöntemi ile ifade ettiğimizi düşünelim. O zaman:

- Bir güvenlik politikası; durumları yetkili (authorized) veya güvenli ve yetkisiz (unauthorized) veya güvensiz durumlar olarak iki gruba ayırır.

Bir politikada güvenli olarak tanımlanan durum başka bir politikada güvenli olmayabilir. Bu bağlamda bir güvenlik politikası güvenli bir sistemin tanımının ne olacağını da belirler.

- Bir güvenli sistem, yetkili bir durumda başlar ve yetkisiz bir duruma geçiş yapmaz.



Şekil 6.1 : Basit bir sonlu durum makinesi

Bu anlattıklarımızı, Şekil 6.1. de görülen dört durum ve beş geçiş içeren bir sonlu durum makinesi üzerinde inceleyebiliriz. Bu sistemde güvenlik politikası durumları, A = { S_1, S_2 } yetkili durumları ve UA = { S_3, S_4 } yetkisiz durumları göstermek üzere iki bölüme ayırmıştır. Bu sistem, S_1 den S_3 e geçiş yaptığı için, yetkili bir durumla başlamasına rağmen yetkisiz bir duruma geçiş yaptığı için güvenli değildir.

- Güvenlik ihlali, bir sistem yetkisiz bir duruma geçiş yaptığında oluşur. Bu sistemde güvenlik ihlali t_3 geçişidir. [Bishop M., 192]

6.1. BİLGİ GÜVENLİĞİ POLİTİKASI

Bilgi güvenliği politikası kurumun sahip olduğu hassas bilgilerin neler olduğunu ve bu bilgilerin nasıl korunması gerektiğini tanımlar. Bu politika kurumda kullanılan bütün bilgileri kapsayacak şekilde inşa edilmelidir. Kurumun her çalışanı kendi sahip olduğu hassas bilgileri korumakla sorumludur. Bir kurumdaki bilgilerin hassasiyeti kurumun yaptığı işe göre farklılık gösterebilir. Kayıtlar, raporlar, tutanaklar, ürün tasarımları ve patent bilgileri hassas bilgiler sınıfına dahil olabilirler. Üniversite ortamında ise, öğrenci, personel ve akademisyen kişisel kayıtları, kurum içi yazışmalar, evraklar, tutanaklar, soruşturmalar, e-postalar ve web sayfaları hassas bilgilere örnek olarak verilebilir. Bütün üniversite mensupları bu hassas bilgilerin korunmasında kendi üzerlerine düşen sorumlulukları yerine getirmekle mükelleftirler. Kurumsal bilgi güvenlik politikası, bu sorumlulukların neler olduğunu bütün ayrıntılarıyla içermelidir. Bu sorumluluklar, 6.3. bölümde ayrıntılı olarak işlenecektir.

6.2. POLİTİKALARIN ÖNEMİ

Bundan yirmi beş yıl önce belki bu güvenlik politikalarına ihtiyaç yoktu fakat taşınabilir bilgisayarlar, kablosuz ağ teknolojileri ve cep telefonları da dahil olmak üzere bilgi tabanlı teknolojilerde yaşanılan patlama bu konuda bir değişime ön ayak olmuştur. Ortaya çıkan bu çok katmanlı ve işlevli yapıda, bilgi güvenliğinin sağlanmasına yardımcı olacak açık ve kesin talimatlara sahip olunması gerektiği çok açıktır. Milyonlarca otomobil sürücüsünün trafik kuralları olmadan yollarda sağlıklı ve düzgün bir şekilde otomobil kullanabileceğini nasıl düşünemiyorsak, bu sektörde çalışan milyonlarca kişinin de güvenlik politikaları olmadan işlerini düzgün ve eksiksiz yürütebilmelerini düşünmemiz de mümkün değildir.

Kurumların kendi güvenlik politikalarını yazılı olarak geliştirmeleri, bunu ulusal ve uluslar arası bilgi güvenliği standartlarına ve ilgili yasalarla yazılı olarak ilişkilendirmeleri, önemli ve göz ardı edilmemesi gereken bir husustur. Güvenlik politikasının tanımlanması, uygulanabilirliğinin değerlendirilmesi, uygulanmasının sağlanması ve güncel tutulması oldukça zor ve zahmetli bir süreçtir. Günümüzde birçok devlet kurumunda, güvenlik politikaları gibi iş hayatını düzenleyici kuralların önemi, üst yönetimlerce gittikçe daha fazla kabul görmeye başlamıştır. Bunun neticesinde, bakanlıklarca çeşitli yönetmelikler, mevzuatlar ve politikalar hazırlanmıtır. Bunlara; Adalet Bakanlığı bilgi sistemlerinin internet üzerinden gelecek tehlikelerden korunması ve veri güvenliğinin sağlanmasında uyulacak usul ve esaslar hakkında yönetmelik [193], Çalışma ve Sosyal Güvenlik Bakanlığının, ulusal çalışma ve sosyal politikalar kamu araştırma programı [194] ve Sağlık Bakanlığının, bilgi güvenliği politikası, kurumsal bilgi güvenliği yönetim politikası bildirimi [195], örnek olarak olarak gösterilebilir.

Açık ve net kurallar olmadan geliştirilen yeni bir sistemin, yönetimin düşündüklerine ve kurumun ihtiyaçlarına cevap verip veremeyeceği belirsizdir. Ayrıca yönetim de, güvenlik politikaları olmadan oluşturulan bilgi sistemleri altyapısının güvenli bir şekilde işletildiğinden emin olamaz.

6.3. BİLGİ GÜVENLİĞİ SORUMLULUKLARI

Bilgi güvenliği sorumlulukları; Şekil 6.3.1 den de görüldüğü gibi kamu kurumlarında, üstte yönetim ile başlayıp, kurumun Bilgi İşlem sürecini üstlenen Bilgi İşlem Daire Başkanlığı, Bilgi İşlem Merkezi Müdürlüğü ve/veya Bilgi Teknolojileri Ofisi birimleri ile kullanıcılar şeklinde sıralanabilir.

Şekil 6.3.1 : Sorumluluk akışı

6.3.1. Yönetimin sorumlulukları

Yönetimin sorumluluğunu; kuruma ait bilgi varlıklarının korunması ve iş sürekliliğinin sağlanması ve desteklenmesinin ötesinde olup kendisini bilgi güvenliği politikasının bir parçasıymış gibi düşünerek politikayı sahiplenmesi şeklinde ifade edebiliriz. Yönetimin, bu programın bir parçası olması, kurumun diğer işlerinde gösterdiği liderliği aynı manada bu konuda da göstermesi demektir. Ayrıca bu amaç için hazırlanan politikaların uygulanabilirliğinin sağlanması için ihtiyaç duyulan gerekli teknik donanım ve nitelikli personel istihdam maliyetlerini sağlamak ve bu aşamalarda çıkabilecek bürokratik engelleri aşmaya destek sağlamak ta yönetimin sorumluluklarındandır.

6.3.2. Bilgi İşlem Yönetimi Sorumlulukları

Bilgi İşlem çalışanları tüm kurumun internet ağının ve bu ağın üzerinde yaşayan yazılım (otomasyon programları,web ve mail programları vb.) ve donanımları (bilgisayar, sunucu, anahtar, yönlendirici, güvenlik duvarı vb.) kurumun ihtiyaçları doğrultusunda kesintisiz ve güvenli bir biçimde sağlamakla yükümlüdürler. Kurumdaki sunuculardan kişisel bilgisayarlara, mobil kullanıcılara hizmet veren kablosuz ağlardan kampüsler ve

şubeler arası bağlantılarına kadar tüm noktalarda ağ ve sistem altyapısının güvenliğini sağlayacak çözümleri tanımlar ve uygularlar.

Bilgi İşlem yönetimleri, kurumdan kuruma değişiklik göstermekle beraber, Bilgi İşlem Daire Başkanlığı, Bilgi İşlem Merkezi ve Bilgi Teknolojileri Ofisi olmak üzere üç ana teşkilat şeklinde kurum organizasyon şemasında yerini almışlardır.

Türkiye Bilişim Derneği (TBD) tarafından düzenlenen KAMU-BİB (Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği) Bilişim Platformu, çalışma grupları ve belge gruplarının gerçekleştirdiği değerlendirme toplantılarının ardından beş çalışma grubu tarafından raporlar hazırlanmıştır [196]. Çalışma grubunun "Başarılı Bilgi İşlem Merkezi Modeli" başlıklı raporuna ait aşağıdaki maddeler özet olarak verilebilir;

- Bilgi İşlem Merkezleri'nin biçim ve ilkeleri konusunda üst yönetimde bilinç yaratılması,
- BİM ile kurum ve kuruluşun diğer kademeleri arasındaki işbirliği eksikliklerinin giderilmesi,
- BİM'lerde verimlilik, kalite ve kullanıcı memnuniyetinin sağlanması,
- BİM'lerde kaynak planlaması yapılması,
- BİM'lerdeki kadro unvan kargaşasının çözülmesi amacıyla, ihtiyaç duyulan unvanların belirlenmesi ve gerekli düzenlemelerin yapılması,
- Bilgi Teknolojileri sektöründeki personel açığının, kalifiye elemanlarla giderilmesi; ek gösterge karmaşasının çözülmesi ve mali hakların sağlanması,
- E-dönüşüm Türkiye 5 Yıllık Eylem Planı'nda BİM adına yapılması gereken eylemlerin ele alındığı 68. ve 87. eylemlerin ilgili tüm taraflarca tartışılması ve takip edilmesinin sağlanması (68. eylem: BİM'lerin tek çatı altında toplanması; 87. eylem: Kamu Personel Kanunu'nun bilgi toplumu hedef ve eylemleri doğrultusunda revizyonu),
- Bilişim hizmetlerinde üst yönetim desteği sağlanmasıdır.

Bilgi işlem yönetimi ayrıca, kendi organizasyon şeması içerisinde, güvenlikle ilgili olarak, konu hakkında eğitimli ve uzman kişilerden meydana gelen bir ağ güvenlik birimi oluşturmalıdır.

6.3.2.1. Ağ Güvenlik Birimi

Ağ güvenlik biriminin başında mutlaka bir sorumlu olmalıdır. Sorumlunun kurum ihtiyaçlarına göre belirlediği cihaz alımı yada geliştirdiği projeler için hem yetkisi hem de yeterli bütçesi olmalıdır. Bu kişinin yetki ve sorumlulukları yönetimin de desteği ile tüm kuruma duyurulmalıdır.

Ağ güvenlik biriminin sorumluluklarına, aşağıdaki maddeler örnek olarak sıralanabilir;

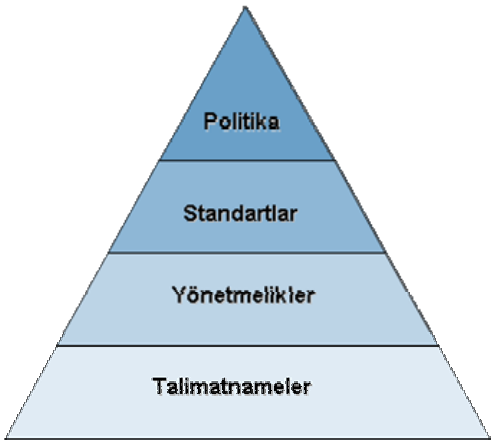
- İç güvenlik standart ve uygulamalarının tavsiyesi ve geliştirilmesine yardımcı olmak,
- Resmi güvenlik politikası ve dokümantasyonunun altyapısının oluşturulmasını, üretilmesini ve bakımını sağlamak,
- Muhtemel güvenlik açıklarına karşı ağları ve sistemleri monitör etmek, taramak ve test etmek,
- Güvenlik haber gruplarını, mesaj listelerini ve duyuruları takip etmek ve gerekenleri yapmak, (ör. gerekli güvenlik yamalarını kurmak)
- Güvenlik arttırma ve izleme araçlarının test edilmesini, kurulmasını ve bakımını sağlamak,
- Yetkisiz modem veya kablosuz cihazların bulunup bulunmadığını bulmak için periyodik olarak araştırmalar yapmak,
- Güvenlik log dosyalarını günlük olarak gözden geçirmek ve anormallikleri araştırmak,
- Tüm sunuculara ait yedekleme ve yedekten geri dönme politikası ve prosedürü hazırlamak,
- Yazılımlardaki güvenlik açıkları için üretici firma tarafından yayımlanan yamaların, öncelikle test edilmesini, sonrasında kurulumunu yapmak,
- Güvenliği tehdit eden unsurlar ve bunlar karşısında alınabilecek tedbirler konusunda güncelliği korumak,
- Ağdaki güvenlik ihlali olayları karşısında araştırma, koordinasyon, rapor ve takipler yapmak,
- Kurumun güvenliğine etki edebilecek iç projelerin inceleme ve analizlerine katılmak,
- Akademisyenlere, çalışanlara ve öğrencilere kurum bilgi güvenliği politikasını sağlamaktır.

6.3.3. Kullanıcı Sorumlulukları

Kullanıcılar, politikaları onların davranış şekillerini düzenleyen ve işlerini yapmalarını zorlaştıran kurallar zinciri olarak gördüklerinden, bu konuda en çok etkilenen gruptur. Bu nedenle güvenlik politikasının her bölümünde, kullanıcıların sorumlulukları ayrı seviyelerde hazırlanmalı ve açıkça tanımlanmalıdır. Kullanıcılar da, hazırlanan kural ve düzenlemelerin kurumun çıkarları doğrultusunda hazırlandığını bilerek ve yönetime duydukları güvenle hareket etmelidirler. Hazırlanan politikaları ihlal eden davranış ve olayları gözlemlediklerinde en hızlı biçimde birim sorumlularına haber vermelidirler.

6.4. GÜVENLİK POLİTİKASI BİLEŞENLERİ

Güvenlik politikalarının bileşenleri olan politikalar, standartlar, yönetmelikler ve talimatnameler arasındaki etkileşim en çok kafa karıştıran husustur. Bu terimleri ayrı ayrı örnekleriyle tanımlamak, aralarındaki ilişkiyi gösterme açısından faydalı olacaktır. Şekil 6.4.1. de politika ve bileşenlerinin yerleşimini gösteren piramit görülmektedir.



Şekil 6.4.1 : Politika ve bileşenleri piramidi

Piramitte alt basamaklara inildikçe belgeler daha ayrıntılı ve daha konuya özel hale gelmektedir. Yani politikalar, geniş anlamlı ve kolay kolay değişmezler, standartlar ve yönetmelikler daha ayrıntılı ve değişmeye yatkındırlar. Talimatnameler ise mümkün olduğunca ayrıntılı olup her yeni standart veya yönetmelik uygulandığında sıkça değişebilmektedir.

6.4.1. Politika

Politika uyulması gereken kuralları ve karşılanması gereken ihtiyaçların ana hatlarının belirlendiği bir belgedir. Politikalar genellikle standartları ve yönetmelikleri varlığının kaynağı olarak temel alırlar. Politikalar uygulanması gereken işlemleri geniş anlamlı ve yüksek seviyeli ifadeler ile anlatır. Bir Şifreleme Kullanım Politikası'nı örnek politika olarak ele alırsak ifademiz; "bu koşullarda şifreleme kullanılması zorunludur" şeklinde olacaktır.

6.4.2. Standartlar

Standartlar herkes tarafından uyulması zorunlu, genellikle teknoloji veya sisteme özel şartlar bütünüdür. İlgili alan veya teknolojiye ait gereksinimler standartların içeriğini oluşturur. Kurumlar birçok yerel ve ulusal standartları referans alarak kendi politikalarını hazırlamalıdırlar. Bilgi güvenlik politikaları standartlarla ters düşmemelidirler. Şifreleme Kullanım Politikası örneğimizde, standartlar başlığına örnek olarak şöyle bir ifade yer alabilir; "Şifreleme algoritması olarak sadece Triple DES (3DES) veya Gelişmiş Şifreleme Standardı (AES) kullanılacaktır."

Kurumsal bilgi güvenliği politikasının hazırlanması aşamasında TS ISO/IEC 17799 ve TS ISO/IEC 27001 standartları esas alınmalıdır. TS ISO/IEC 17799 ve TS ISO/IEC 27001 standartları, kurumsal düzeyde bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan bilgi teknolojileri uzmanlarının kullanımı için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri kapsamaktadır.

Donanım ve hazır yazılımlar için ürün bazında bilgi güvenliğine ilişkin olarak, TS ISO/IEC 15408 Ortak Kriterler (Common Criteria) standardı dikkate alınmalıdır. Güvenlik ihtiyaçların belirlenmesinde, ayrıca, Avrupa Komisyonu IDABC (Birlikte Çalışabilir Avrupa e-Devlet Hizmetlerinin İdareler, İşletmeler ve Vatandaşlara Sunumu) Programı tarafından geliştirilen Ortak İlgi Alanındaki Projeler İçin Güvenlik Anketi (PCI Security Questionnaire) kaynak ve referans olarak kullanılabilir. [197]

BS 7799-1:2000 / ISO-17799

Ürün ve hizmetlerin kalitesini geliştirmeye yönelik standartlar oluşturan ve bağımsız bir kuruluş olan İngiliz Standartlar Enstitüsü (BSI) tarafından belirlenmiş bir global bilgi

güvenliği standardıdır. “Bilgi Teknolojileri – Bilgi Güvenlik Yönetimi için Uygulama Kuralları” olarak adlandırılmıştır. Bu kısımda bilişim güvenliği için çalışma kuralları, güvenlik politikası geliştirme ve güvenlik denetlemesi yapma konuları anlatılmakta olup, içerdiği on alt bölüm içerisinde 127 ana kontrol maddesi bulundurmaktadır. Her bölümde, o bölümde anlatılan konunun, kurumsal güvenlik politikasına nasıl dahil edileceği ve bu faaliyetlerin nasıl denetleneceği ile ilgili bilgiler vardır. 2000 yılı Aralık ayında Uluslararası Standartlar Kurumu (ISO) tarafından benimsenerek birebir alınmış ve ISO-17799 olarak adlandırılmıştır. 11 Kasım 2002 tarihinde TS ISO/IEC 17799 adıyla Türk Standartları Enstitüsü (TSE) tarafından kabul edilmiştir.

1. İş Sürekliliğinin Planlanması: Kritik iş kaynakları tanımlanır ve bu kaynaklara zarar vermeye ve onların sürekliliğini etkilemeye yönelik olan faaliyetlerle mücadele için tedbirler alınmalıdır. Burada bahsedilen zarar, küçük ya da büyük bir zarar olabilir.
2. Sistem Erişim Denetimi: Erişim denetimine ihtiyacı olan kaynaklar belirlenir. Yetkisiz gerçekleşen faaliyetler tespit edilmeli ve uygun bir şekilde kotarılmalıdırlar.
3. Sistem Geliştirme ve Sürdürme: Bilginin gizliliği, bütünlüğü ve kimlik sınaması korunmalıdır. Tüm bilişim faaliyetleri güvenli bir şekilde gerçekleştirilebilmelidir. Uygulama yazılımların ve bunlara ilişkin verinin güvenliği de göz önünde bulundurulmalıdır.
4. Fiziksel Güvenlik ve Çevre Güvenliği: Kuruma ait bina ve benzeri yerlere giriş çıkışlar kontrol altında tutulmalıdır. Bu sayede verilerin, bilgisayar ve bilgisayar ağlarına ilişkin cihazların çalınmasını ve zarar görmesi engellenir.
5. Uygunluk: Yasal olarak yapılmış düzenlemelere, kurumsal olarak ortaya konulan politika ve kurallara uygunluk sağlanmalıdır.
6. Kurum Çalışanlarının Güvenliği: Kullanıcıların, potansiyel tehditler ve kurumsal güvenlik politikasını desteklemek üzere nasıl davranacağı hakkında bilgi sahibi olmaları sağlanmalıdır.
7. Güvenlik Organizasyonu: Kurum içinde bilgi güvenliğinin yönetimi yapılmalıdır. Bilgi-işlem hizmetleri, başka bir firma yardımıyla dış kaynaktan alınıyor olsa bile, kuruma özel bilgiler, yine kurum içersinde korunmalıdır.
8. Bilgisayar ve Ağ Yönetimi: Bilgi işlem ve iletişim kaynakları korunmalı ve bu kaynakların bütünlüğü ve sürekliliği sağlanmalıdır.

9. Kaynak Sınıflandırması ve Kontrol: Bilgi kaynakları için uygun sınıflandırma yapılmalı ve her sınıflandırma düzeyi için gerekli koruyucular devreye sokulmalıdır.
10. Güvenlik Politikası: Kurumsal güvenlik programının temeli olarak bir güvenlik politikası oluşturulmalıdır.

BS 7799-2:2005 / ISO-17799:2005

"Bilgi güvenliği yönetim sistemleri - Özellikler ve kullanım kılavuzu" olarak adlandırılmaktadır. 2005 yılında ISO-17799 revize edilmiş ve ISO-17799:2005 adını almıştır. TSE tarafından TS 17799-2 adı ile 17 Şubat 2005 tarihinde kabul edilmiştir. Daha sonra 21 Aralık 2006 tarihinde "Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" adı ile tekrar düzenlenmiş ve diğer standarlar yürürlükten kaldırılmıştır. [198]

ISO/IEC 27001

Bilgi güvenliği standardı BS 7799-2 revize edilmiş beş madde daha eklenerek toplam on beş ana maddeden oluşmuştur. Bu beş madde;

- Bilgi güvenliği yönetiminin sistemi, gereksinimleri, kurulumu, yürütülmesi, takibi, bakımı ve geliştirilmesi,
- Yönetimin sorumlulukları ve yerine getirmesi gerekenler,
- Dahili bilgi güvenliği yönetim sistemi denetlemeleri,
- Bilgi güvenliği yönetim sistemi konusunda, yönetimin gözden geçirmesi gerekenler,
- Bilgi güvenliği yönetim sisteminin sürekli geliştirilmesi, düzeltici ve önleyici faaliyetlerinin gerçekleştirilmesidir.

2005 Ekim ayında adının "ISO 27001:2005" olarak değiştirilmesiyle yürürlüğe girmiştir. Bu standart ISO-17799 içinde tanımlanan kontrollerin nasıl uygulanacağına, bilgi güvenliği yönetim sisteminin nasıl kurulacağına ve çalışır hale getirileceğine dair tanımlar içermektedir. ISO 27001, kurumların risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Bu standart, TS ISO/IEC 27001 adıyla 02.03.2006 tarihinde TSE tarafından kabul edilmiştir. [199]

6.4.3. Yönetmelikler

Standartlar uygulanması zorunlu olmasına rağmen yönetmelikler daha çok takip edilmesi gereken bir tavsiye ve rehber niteliği taşırlar. Yönetmelikler de standartlar gibi politikalar ve yasalarla ters düşmemelidirler. Resmi kurumların bağlı oldukları üst makamlar tarafından hazırlanması bakımından uygulanmasının zorunlu olduğu hallerde mevcuttur.

Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) Kullanım Politikası Sözleşmesi

Türkiye' de üniversiteler ve araştırma kuruluşlarının öğrenci, öğretim üyesi, araştırmacı ve diğer çalışanlarından oluşan kullanıcılarının, internete erişim için TÜBİTAK ULAKBİM tarafından sağlanan Ulusal Akademik Ağ (ULAKNET) hizmeti bulunmaktadır. Bu ağın kullanımında uyulması gerekli kurallar bir kullanım politikası sözleşmesi ile (Acceptable Use Policy - AUP) duyurulmuş ve tüm kullanıcıların imzasına açılmıştır. [200] Bu politika tüm üniversiteler için bir referans özelliği taşımaktadır. Üniversitelerin hazırlayacakları kullanım politikaları bu sözleşme ile uyumlu olmak zorundadır.

OECD Bilgi Güvenliği Politikası Rehberi

17/02/2003 tarihli ve 2003/10 sayılı Başbakanlık Genelgesi ile OECD Bilgi Güvenliği Politikası Rehberi yayınlanmış, bu rehber ile bilgi sistem ve ağları için güvenlik kültürü rehber ilkeleri tüm kamu kurum ve kuruluşlarının dikkatine sunulmuştur. [201] Bu genelge ile kurumların bilgi sistem ve ağlarının korunması için yürütülen çalışmalarda bu rehber ilkelerin göz önünde bulundurulması istenmiştir. Ayrıca rehber ilkelerin amacının güvenlik hususunda tek ve kesin bir çözüm ileri sürmek veya belli bir durumda hangi politika, uygulama, önlem ve prosedürlerin uygun olduğu hususunda net bir açıklama getirmek olmadığı belirtilmiştir. Bundan daha ziyade, kullanıcıların bir güvenlik kültürünü nasıl oluşturacağı ve aynı zamanda ondan nasıl yararlanacağı konusunda daha iyi bir anlayış yerleştirmek üzere, çerçeve ilkeler sunmak olduğu belirtilmiştir. Bu rehberde birbirini tamamlayan dokuz temel ilke oluşturulmuştur;

1. Bilinç: Kullanıcılar, bilgi sistemleri ve ağlarının güvenliğinin gerekliliği ve güvenliği artırmak için neler yapabilecekleri konularında bilinçli olmalıdır.
2. Sorumluluk: Tüm kullanıcılar bilgi sistem ve ağlarının güvenliğinden sorumludur.

3. Tepki: Kullanıcılar, güvenlik tehditlerini önlemek, saptamak ve bunlara tepki verebilmek için işbirliği içinde ve zamanında eyleme geçmelidir.
4. Etik: Kullanıcılar birbirlerinin yasal çıkarlarına saygı göstermelidir.
5. Demokrasi: Bilgi sistem ve ağlarının güvenliği, demokratik toplumun temel değerleri ile uyumlu olmalıdır.
6. Risk değerlendirmesi: Kullanıcılar risk değerlendirmeleri yapmalıdır.
7. Güvenlik tasarımı ve uygulama: Kullanıcılar, güvenliği, bilgi sistem ve ağlarının önemli bir unsuru olarak ele almalıdır.
8. Güvenlik Yönetimi: Kullanıcılar güvenlik yönetimi ile ilgili kapsamlı bir yaklaşım benimsemelidir.
9. Yeniden değerlendirme: Kullanıcılar bilgi sistem ve ağlarının güvenliklerini incelemeli ve yeniden değerlendirmeli; güvenlik ile ilgili politika, uygulama, önlem ve prosedürlerde gerekli değişiklikleri yapmalıdır.

e-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi

e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı, 4/12/2003 tarih ve 25306 sayılı Resmi Gazetede yayımlanan 2003/48 sayılı Başbakanlık Genelgesi ile hayata geçirilmiştir. Genelgede, kamu kurum ve kuruluşları arasında etkin ve güvenli bilgi paylaşımı amacıyla birlikte çalışabilirliğe imkan sağlayan güvenli bir altyapı kurulmasının önemi vurgulanmış ve kamu kurumlarınca uygulanan ya da hazırlık çalışmaları sürdürülen çevrimiçi hizmetlerin etkin şekilde sunulabilmesi için işbirliği ve bilgi paylaşımını sağlayacak böyle bir altyapının kurulması, Eylem Planı'nın temel önceliklerinden biri olarak kabul edilmiştir. [202]

e-Dönüşüm Türkiye Projesi Kısa Dönem Eylem Planı (KDEP)'nda yer alan 34 no'lu "Birlikte çalışabilirlik esaslarının belirlenmesi ve rehber yayımlanması" eylemi çerçevesinde Devlet Planlama Teşkilatı Müsteşarlığı koordinasyonunda hazırlanmıştır. Rehber'de; beş temel konuda esaslar ve kullanılacak standartlar belirlenmiştir. Bunlar;

1. **Veri sunumu ve değişimi:** Elektronik ortamdaki verilerin sunumu ve değişimi için gerekli standartlar ortaya konmuştur. Standartlar belirlenirken dikkat edilen temel noktalar; sunulan bilgilerin kullanıcı tarafında asgari derecede ek yazılım gerektirmesi, kullanılacak araçların mümkün olduğunca açık standartlara dayalı olması ve bu bilgilere farklı platformlardan ulaşılabilmesidir.

2. **Ara bağlantı ve ağ standartları:** Fiziksel altyapıya ait tanımlamaları içermektedir.
3. **Veri entegrasyonu ve içerik yönetimi:** Kamu hizmetlerinin elektronik ortamda birlikte çalışacak, ortak bir çözüm oluşturacak şekilde sunulması ve içerik yönetimi için bir metodoloji ve bu metodoloji için gerekli araçlar belirtilmiştir.
4. **Güvenlik:** Bilginin güvenli bir şekilde iletilmesi için kurumların uyması gerekli belli başlı bilgi güvenliği standartları tanımlanmış ve bilgi paylaşan tüm kurumların bu standartları yakalamasının gerekliliği anlatılmıştır.
5. **Çözüm yaşam döngüsü:** Bu bölümde, sistemlere, geliştirilen çözümlere ve güvenliğe ilişkin süreçlere ait olarak kullanılacak standartlar ortaya konmuştur.

6.4.4. Talimatnameler

Talimatnameler politika, standart veya yönetmelikte geçen uyulması, yapılması veya izlenmesi gerekenlerin nasıl gerçekleştirileceğini tam olarak adım adım anlatan, oldukça ayrıntılı belgelerdir. Bir kurumda bilgi güvenliği konusunda yüzlerce hatta binlerce talimatname bulunabilir. Talimatnameler direk olarak kurumsal iş akışı ile bağlantılı olup bu akışta yapılan değişiklikler sonrası talimatnameler de gözden geçirilmelidir.

Güvenlik politikaları ve talimatnameleri arasındaki farkı daha iyi anlayabilmek için bir yedekleme politikası ve yedekleme talimatnameleri arasındaki ilişkiyi incelemek faydalı olacaktır. Bir kurumun yedekleme politikasında “tüm veritabanı kayıtları yedeklenecek ve bu yedekler farklı bir binada tutulacaktır” ifadesi yer alsın. Talimatnamede ise bu yedeklemenin hangi sunucularda, ne zaman, ne sıklıkta, nasıl ve kimler tarafından yapılması gerektiği, kontrolü, taşınması, saklanması ve daha fazla ayrıntılı bilgilere ait ifadeler bulunur.

6.5. POLİTİKA ÇEŞİTLERİ

Politika hazırlama ve geliştirme çalışmasında, politikanın anlaşılmasını kolaylaştırmak için genellikle üçe ayrılırlar [Peltier Thomas R., 203]:

- Program politikaları
- Konuya özel politikalar
- Uygulamaya özel politikalar

6.5.1. Program Politikaları

Kurum yönetimi, kurumun bilgi güvenlik politikasını ve temel yapısını oluşturmak için bir Program Politikası yayınlamakla sorumludur. Bu yüksek seviyeli politika kurumdaki bilgi güvenliği programı amacını ve onun kapsamını tanımlar. Ayrıca politikanın oturtulması ve buna uyulması ile ilgili sorumlulukları belirler. Kurumsal güvenlik politikası ve kabul edilebilir kullanım politikası (Acceptible Use Policy - AUP) bu tip politikalara örnek olarak gösterilebilir. Kabul edilebilir kullanım politikası, kurumun ağ kaynaklarının kullanıcılar için, uygun ve uygun olmayan kullanımını açıkça ifade eder [Riggs C., 204]. Bir program politikası aşağıdaki maddelerde belirtilen konuları kapsamalıdır.

6.5.1.1. Amaç

Politikanın amaç kısmı normalde programın hedeflerini ve yapılmak istenenleri tanımlar. Bilgi güvenliği konusu ele alındığında, bütün program politikaları bilgi kaynaklarının gizliliği, bütünlüğü, erişilebilirliği ve güvenilirliğini korumak üzerine yoğunlaşmışlardır. Ayrıca bilginin kurumun bir değer varlığı olduğunu ve dolayısıyla yetkisiz erişimden, değiştirilme, ifşaat veya imhadan korunmasının gerekliliğini ifade eder.

6.5.1.2. Kapsam

Kapsam, kurumun hangi kaynaklarının politika tarafından ele alındığını belirtir. Bu amaç dahilinde, akademik, idari ve sözleşmeli personel, tam zamanlı ve yarı zamanlı çalışanlar tarafından yaratılmış veya erişilen, elektronik olarak depolanmış, işlenmiş, iletilmiş, çıktı olarak alınmış, faks olarak gönderilmiş veya müzakere edilmiş bütün bilgileri içerir.

6.5.1.3. Sorumluluklar

Politikanın bu bölümünde genelde üç veya daha fazla belirli rol ve bunlara ait sorumluluklar tanımlanır. İlk rol genelde programın uygulanması ve desteklenmesinden sorumlu olan yönetime aittir. Çalışanlar politikaya birebir uymakla zorunlu olup karşılaştıkları herhangi bir şüpheli durumu yönetime rapor etmekle sorumludurlar. Politika ayrıca kendisinin yedi gün yirmi dört saat yönetiminden sorumlu bir birimin tanımlarını da içerir.

6.5.1.4. Uyma

Politika uyma ile ilgili genelde iki konuyu ele alır;

- Politika hedeflerine uyumu sağlamakla kimin sorumlu olacağını söyler. Normalde iki belirgin grup tanımlanır:
  - İlk safha denetleme ve çalışanların faaliyetlerini takip etmedeki rolü
  - İç denetim personeli ve resmi incelemelerin idaresindeki sorumlulukları
- Politika ihlal edildiğinde neler olur? Politika hazırlama ve uygulama aşamasında politika ihlallerinin istenmeden yapılabileceği unutulmamalıdır. İhlal, eğitim eksikliği ve bilinçsizlik sonucu ortaya çıkmış olabilir. Bunun önüne geçebilmek için, ortaya çıkan her ihlali birer birer ele alan bir gözden geçirme işlemi oluşturmak gereklidir. Problemlerin gözden geçirilebilmesi sürecinde yönetime zaman tanınmalıdır.

6.5.2. Konuya özel politikalar

Program politikalarının aksine konuya özel politikalar, tek seferde tek konuyu ele alabilmek için odak noktalarını daraltırlar. Burada her bölümün başında kurumun politika ifadesi yer alır. Daha sonra bu politikayı desteklemek için gerekli adımlar tanımlanır. Sistem güvenlik, ağ güvenlik, yazılım ve donanım politikaları bu tip politikalara örnek olarak gösterilebilir. [Morimoto R. ve diğ., 205] Konuya özel politikalar aşağıdaki bölümlere sahiptirler:

6.5.2.1. Önerme ifadesi

Belirli bir konuda politika oluşturmak için yazar, yönetimle görüşmeli ve üzerinde durulacak ilgili maddeleri belirlemelidir. Program politikasının amaç kısmında olduğu gibi burada da politikanın hedefleri ve varmak istediği noktalar tanımlanmalıdır.

6.5.2.2. İlişki

Konuya özel politika ayrıca politikanın kimlere uygulanacağını da anlatmalıdır. Buna ilave olarak politika, yapılacakların nerede, nasıl ve ne zaman uygulanacağı hususlarına da açıklık getirmelidir.

6.5.2.3. Sorumluluklar

Görevler ve sorumlulukların ortaya konulması, konuya özel politikaların içeriğinde olmalıdır. Bir politika veya talimatnamede bir şahıs tanımı yapılmak istenildiğinde,

isminin kullanılması yerine mevkisi veya görev yerlerini tanımlamak daha faydalı olacaktır. Kişiler değişebilse de görev yerleri kalıcı olmaktadır.

6.5.2.4. Uyma

Burada kabul edilemeyen bazı davranışların ayrıntılı tarifi yapılması ve bu davranışın ortaya çıkaracağı sonuçların ele alınması uygun olacaktır. Bunların takibi ile ilgili sorumluluklar da ayrıca tanımlanmalıdır.

6.5.2.5. İlave bilgiler

Konuya özel politikalarda, kullanıcıların ilave bilgilere ulaşabilmeleri için gerekli şahıslar ve birimlerin tanımlanması gerekmektedir. Birbiriyle ilişkili talimatların kopyalarının nereden elde edilebileceğine dair bilgiler bu bölümde yer almalıdır.

6.5.3. Uygulamaya özel politikalar

Program seviyesinde ve konuya özel politikaların her ikisi de genelde bütün kurumu kapsayacak şekilde geniş bir topluluğa hitap etmektedir. Uygulamaya özel politikalar tek bir belirli sistem veya uygulama üzerine yoğunlaşmışlardır. Bir kurumun güvenlik mimarisinde son aşama olarak kabul edebileceğimiz uygulamaya özel politikalar, programın uygulama ve sistem seviyesinde açılımını sağlarlar. İnternet erişimi, e-posta, yedekleme, uzaktan erişim, antivirüs, şifre kullanım, acil durum yönetimi, fiziksel güvenlik, kimlik doğrulama ve yetkilendirme, veritabanı güvenlik ve bakım politikaları bu tip politikalara örnek olarak gösterilebilir [Sullivan C., 206] .

Birçok güvenlik hususunda karar, sadece uygulama veya sistem seviyesinde verilir. Bu konuda aşağıdaki örnekler verilebilir:

- Uygulama verilerini okuma veya değiştirme yetkisine kim sahiptir?
- Veriler hangi şartlar altında okunur veya değiştirilebilir?
- Uzaktan erişim nasıl kontrol altına alınabilir?

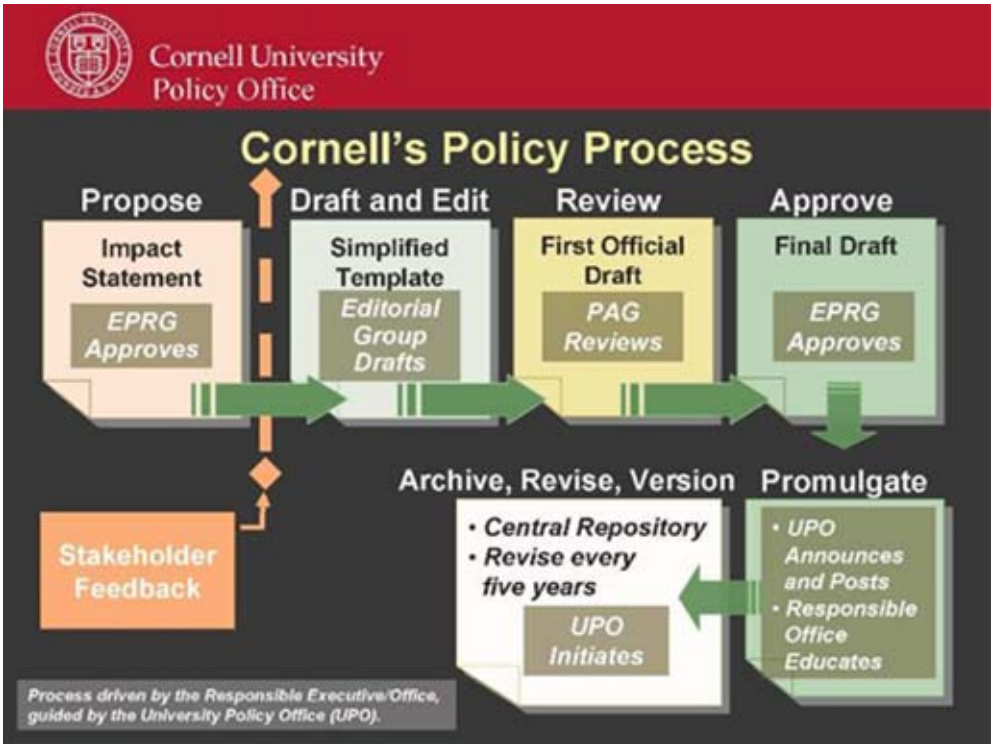
Çok yönlü bir sistem güvenlik politikaları geliştirebilmek için kurum hedeflerini ve amaçlarını sağlayan güvenlik kurallarını içeren bir yöntem kullanılmalıdır.

- Hedefler ve bu hedeflere ulaşabilmek için gerekli ne tür güvenlik araçları kullanılabilecek belirlenmelidir.
- Uygulama veya sistem işletimi için kurallar oluşturulmalıdır. Hangi kaynaklara ne zaman kim erişecek tanımlanmalıdır.

7. GÜVENLİK POLİTİKASI GELİŞTİRİLMESİ

Kurum olarak güvenlik hususundaki temel prensipler ortaya konulduktan sonra politika geliştirme safhasına geçilir. Yüksek öğretim kurumlarının da diğer kurumlar gibi bir yandan yasa, yönetmelik ve standartlara bir yandan da kendilerine internet hizmeti sağlayan ULAKBİM politikalarına uyum sağlayabilmeleri için uygun politikalar geliştirmeleri kurum adına faydalı olacaktır. Geliştirecekleri politikalar kurumun dış ağlarla ilişkisini ve bunun yanında kurum içi bilgi akışını da düzene koyabilecektir.

Yüksek öğretim kurumlarında politika geliştirme konusunda bir sistematik belirlemek için referans alınabilecek uluslararası birçok yaklaşım ve kaynak mevcuttur. Bazı kurumlar, politikaların nasıl biçimlendirileceğini, kimlerin oluşturacağını ve nasıl onay alabileceğini anlatan talimatlar dizisi ve kurumsal bir rapor sağlayan "politika oluşturma talimatları" ortaya koymuşlardır. Cornell Üniversitesi "Politikaların kaleme alınması ve yayınlanması" başlıklı bir politika geliştirme yöntemi tanımlamıştır [207].

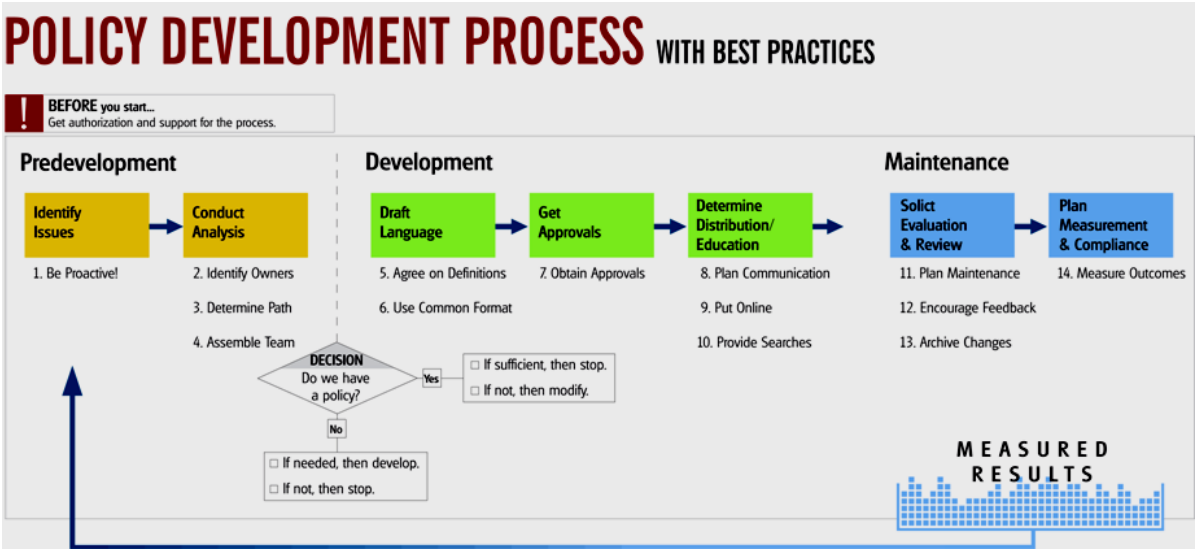


Şekil 7.1 : Cornell Üniversitesi'nin politika oluşturma akış şeması

Şekil 7.1. de Cornell Üniversitesinin politika oluşturma akış şeması görülmektedir [207]. Cornell Üniversitesinde yeni veya düzeltmeler yapılmış politikaları gözden geçiren ve onaylayan iki daimi komisyon bulunmaktadır. Bunlardan ilki olan, İdari Politika İnceleme Grubu (Executive Policy Review Group - EPRG), Rektör Yardımcıları ve dekanlardan oluşur. İkinci daimi komisyon olan Politika Danışma Kurulu (Policy Advisory Group - PAG), kıdemli yöneticilerden oluşur ve ayda bir kez toplanırlar. EPRG, üç ayda bir toplanarak politika oluşturma konusunda gelen teklifleri ve düzeltmeleri, kurumsal bakış açısı ile değerlendirirler. EPRG'nin onayından geçtikten sonra, politika hazırlama ekibi tarafından, tüm politikanın taslak çıkarma işlemi başlar. Ortaya çıkan ilk resmi taslak, gerçek testlere tabii tutulmak üzere PAG'ın denetimine sunulur. Bu son taslak, PAG'ın denetiminden sonra, nihai onay için EPRG'ye gönderilir. EPRG'nin onayından sonra politika, yayınlanmak ve duyurulmak üzere Üniversite Politika Ofisi (UPO)'ne gönderilir. UPO, bu işleyişin her aşamasında bütün komisyonlara destek vermektedir. Politika yayınlanıp duyurulduktan sonra, merkezi bir veri tabanında arşivlenir ve her beş yılda bir gözden geçirilir.

Minnesota Üniversitesi, her türlü konuya uyarlanabilecek kurumsal politikalar oluşturma hususunda kolaylık getirmesi açısından, bir "Politika Yazma Rehberi" hazırlamıştır [208]. Bu rehber politika geliştirme, dağıtma ve takip süreci hakkında bilgiler içermektedir. Ayrıca politika yazımı ile ilgili ipuçları, politika biçimi, maddeleri ve içeriği ilgili temel yapıyı tanımlar. Bu türde resmi bir yaklaşım, politika geliştirmeyi istikrarlı bir hale getirir ve politika geliştirme ve onaylama yetkililerine söz hakkı tanır. [Luker Mark A. ve Petersen R., 209]

Üniversite ve Yüksekokul Politika Yöneticileri Birliği (Association of College and University Policy Administrators - ACUPA) bir "en iyi uygulamalar ile politika oluşturma yöntemi" geliştirmişlerdir [210].



Şekil 7.2 : En iyi uygulamalar ile politika oluşturma yöntemi akış şeması

Bu yöntemin içerdiği adımlar;

1. Ele alınacak konuların ortaya konulması,
2. Analiz yönetimi,
3. Taslak hazırlanması,
4. Onay alınması,
5. Duyurulması, dağıtım ve eğitimi,
6. Taleplerin değerlendirilmesi ve gözden geçirme,
7. Takip ve uyum adımlarıdır. (Şekil 7.2)

Burada 1 ve 2. maddeler hazırlık, 3, 4 ve 5. maddeler geliştirme, 6 ve 7. maddeler bakım kısmını oluşturmaktadır. ACUPA nın tavsiye ettiği yöntem güvenlik politikaları geliştirme hususunda birçok faydalı özellik içermektedir. İlk olarak; ele alınacak konuların ortaya konulması adımı, mevcut bilgi veya veri güvenlik politikalarının tanımlanmasını da kapsayan bir güvenlik risk analizi gerçekleştirmek üzere tasarlanmıştır. İkinci olarak; politikayı oluşturabilmek için politika hazırlama ekibinin, izleyeceği yolun ve ekibin tanımlanması, güvenlik politikasının mükemmel bir şekilde başarıya ulaşmasında çok önemli bir yer tutmaktadır. Bir hukuk danışmanının, politika hazırlama ekibinin parçası olması ve politika belgesinin hukuki yeterliliğine karar verebilmesi için müteakip gözden geçirme işleminin bir parçası olması, politikanın yasal yönünün ifadesi açısından faydalı olabilecektir. Güvenlik politikasının çok ağır bir hukuki dile sahip olması veya yazılan terimlerin çok karmaşık olması, kullanıcılar veya

çalışanların politikayı okuma ve anlama heveslerini kırabilecektir. Diğer bir yandan da hukuki danışmanlar, güvenlikle ilgili yasal uygulamalar konusunda ayrıntılı bilgiye sahiptirler. Üçüncü olarak; taslak oluşturulması ve onay alınması süreci, birçok kurum için stratejik ve politik bir işleyiştir. Kurumlar için bilgi ve ağ güvenliğinin aciliyeti nedeniyle, kurumsal politikanın benimsenmesi ve resmi gözden geçirimi için paylaşılan idari işlemlerde, hukuki uyumluluğu sağlamak ve değerleri korumak adına, atılması gereken adımlarda ve bürokratik engellerde daha makul olunabilir. Dördüncü olarak, güvenlik konuları ve bununla alakalı politika ve talimatnameler hakkında artan bir şekilde eğitim ve bilinçlendirme çalışmaları ortaya koymak, önemli bir husustur. Kimsenin hakkında bir şey bilmediği bir politika veya daha da kötüsü, görmezlikten gelinen bir politika, faydasından çok zarar getirecektir. Son olarak da bakım aşamasında, güvenlik politikalarının etkinliğini koruması ve değişen teknoloji karşısında gelişimini sağlayabilmesi için düzenli olarak değerlendirilmesinin öneminin altı çizilmektedir.

Sektörün en iyi uygulamalarının yanında, tutarlı bir politika geliştirme amacıyla kullanılabilecek bir diğer yaklaşım ise, ISO17799 gibi güncel standartlarla bir taslak oluşturmaktır. Bu yaklaşımda genel olarak, en düşük veya temel güvenlik gereksinimlerini ve risklere karşı dayanma gücünü anlayabilmek için, idari ve teknik ortama ait bir risk değerlendirme işlemi kullanılır. Bu risk analizi, tehditlerin ve bunlara karşı alınabilecek tedbirlerin tanımlanması ve sonrasında kendine özel hazırlanmış politika ifadelerinin oluşturulmasını mümkün kılar. Güvenlik politikaları oluşturmada kullanılabilecek aşamalar genel hatlarıyla aşağıda belirtilmiştir.

1. Bütün sorumlu birimler ve rolleri, yükümlülükleri ve görevleri ayrıntılı olarak tanımlanır.
2. Başlıca kurumsal hedefler belirlenir.
3. Yönetimin güvenlik yaklaşımını ve hedeflerini yansıtan bir güvenlik ilkeleri listesi oluşturulur.
4. Bütün uygulanabilir veriler ve işleme tabi tutulan kaynaklar tanımlanır ve sınıflandırılır.
5. Temel verilerin sınıflandırılmasında, üretiminden silinmesine kadar süreci kapsayan bir veri akış analizi çalışması hazırlanır.
6. Başlıca tehditler belirlenir.

7. Başlıca gerekli güvenlik hizmetleri (yetkilendirme, kimlik belirleme, izlenebilirlik, bütünlük, gizlilik ve süreklilik vb.) tanımlanır.
8. Genel bir politika şablonu oluşturulur.

Tüm bu öneriler ve rehber çalışmaların ışığında ve bunları kapsayacak şekilde bir genel politika oluşturma aşamaları ortaya konulabilir. Bu aşamaları detaylandırmak istersek;

- Hazırlık
    - Kurum değer ve varlıklarının belirlenmesi
        1. Yazılım ve donanım
        2. Yazılı kaynaklar
        3. İnsan kaynakları
    - Ekibin belirlenmesi
    - Veri akış analizi çalışması
    - Tehditler ve karşı tedbirlerin ortaya konulması
- Oluşturma
    - Ortak bir şablon ortaya konulması
    - Taslak oluşturulması
    - Onay alınması
    - Duyurulması ve dağıtımı
    - Güvenlik bilinçlendirme programı
- Bakım
    - Taleplerin değerlendirilmesi ve gözden geçirme
    - Uyumun sağlanması ve takibi

7.1. HAZIRLIK

7.1.1. Kurum değer ve varlıklarının belirlenmesi

Bilgi güvenliği politikaları kurumun işleyişini, amaç ve hedeflerini korumak üzere hazırlanmalıdır. Burada genellikle düşülen hata, yazılım ve donanımların neden satın alındıklarını düşünmek yerine sadece teknik bir bakış açısı ile bunları değerlendirmektir. Eğer bilgisayarların kurumun bilgi varlıklarını işleyen araçlar olduğu, disklerin bu varlıkların depolanmasında kullanıldığı ve internet ağının bu

bilginin kurumun çeşitli ihtiyaçları doğrultusunda birimleri arasında akışını sağladığı göz önüne alınırsa, ancak o zaman tutarlı ve tatbik edilebilir bir güvenlik politikası yazılması için doğru bir yola girilmiş olabilir [Barman S., 211].

7.1.2. Yazılım ve Donanım

Kurumun iş akışını sağlayan ve altyapısını oluşturan yazılım ve donanımlar, politikalar vasıtası ile korunmalıdır. Bu nedenle tüm ağın haritasının da dahil olduğu kurum değer ve varlıklarının tam bir envanterinin çıkarılması önemlidir. Ağın haritasının ve sistem envanterinin oluşturulmasının birçok yöntemi vardır. Burada önemli olan hangi yöntemlerin kullanıldığı değil, her şeyin belgelendirildiği olmalıdır. Aşağıda Tablo 7.1.2.1. de dökümü yapılan bir envantere ait örnek bir donanım listesi görülmektedir.

Tablo 7.1.2.1 : Donanım liste örneği

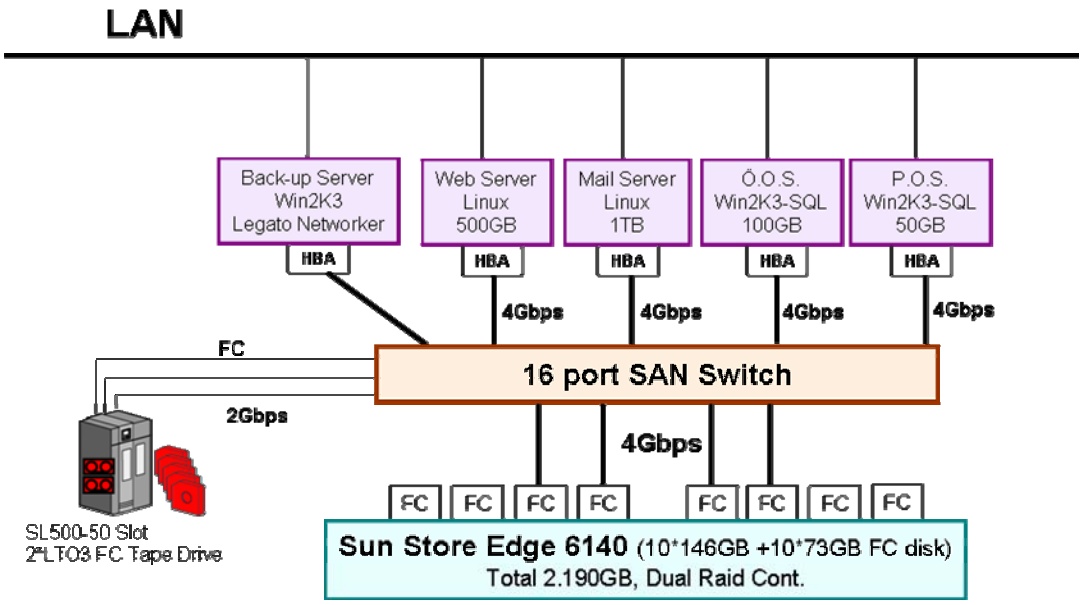
Bilgisayar	**Adet**	**Yerel Ağ Altyapısı**	**Adet**
Sunucu Masaüstü Dizüstü Diğer		Yerel Ağa Bağlı Bilgisayar Sayısı Yerel Ağ Bant Genişliği (Mbps) Yapısal Kablolama Türü (İç) Cat5 / Fiber vb. Hub/Switch (Uç sayısı) Kablosuz Yerel Ağ WLAN (Erişim Noktası Sayısı)	
Çevre Birimleri		**İnternet Bağlantısı**	
Yazıcılar		Router (Sayısı) Bağlantı Türü Bağlantı Hızı Donanım-Firewall sayısı İnternete bağlı olan bilgisayar sayısı	
Lazer Mürekkep Püskürtmeli Nokta Vuruşlu Çizici (Plotter) Projeksiyon			
Tarayıcı			
Kesintisiz Güç Kaynağı			

Bu liste, Tablo 7.1.2.2 de ki gibi detaylandırılabilir.

Tablo 7.1.2.2 : Donanım liste detayı

Sunucu	**İşlemci**	**Hafıza**	**Disk Kapasitesi**
Web Sunucu	Xeon 1.6 GHz 4 MB Önbellek	4 GB DDR2 SDRAM	6 x 300 GB 10 krpm SAS

Ağın haritasının çıkarılmasında, envanter dökümünün hazırlanmasından başka, diğer bir yol da verilerin her sistem üzerinden nasıl geçerek işlendiğini göstermektir. Bir veri akış haritası üzerinde kritik noktalar işaretlenerek, bu noktalarda güvenlik ve kontrol ölçümlerine çok daha dikkat edilebilir.



Şekil 7.1.2.1 : Sunucu veritabanları yedekleme topoloji örneği

Çıkarılan bu harita, verilerin veritabanlarına nasıl depolandığını, sistem üzerinde nasıl gezdiğini, yedeklendiğini, izlendiğini ve log olarak kayıt altına alındığını göstermek açısından da önemlidir. (Şekil 7.1.2.1)

7.1.3. Yazılı kaynaklar

Envanterler, politikalar gibi yazılım ve donanımın ötesinde bir içeriğe sahip olmalıdırlar. Programlara, donanımlara, sistemlere, yönetimsel işlemlere ve kurumun teknik işleyişini her yönüyle tanımlayan belgelere ait bir liste hazırlanabilir. Bu belgeler kurumun çalışma şeklinin nasıl olduğunu açıkladığı gibi hangi alanların saldırıya uğrayabileceğini gösteren bilgiler içerebilirler. Hazırlanan bu envanter aynı zamanda kurumun hazır basılı formlarını, antetli kağıtlarını ve kurumun adının yer aldığı resmi içerikli diğer bütün evrakları da kapsamalıdır. Boş antetli ve hazır mühürlü evraklar

kurumu zor durumda bırakabilecek, sahtecilik ve dolandırıcılık işlemlerinde kullanılabilirler. Tüm bu kaynakların envantere, dolayısıyla kurumun korunması gereken değerleri arasına dahil ederek yazılan politikalarla da korunması sağlanmış olur.

Tablo 7.1.3.1 : Yazılı kaynak örnek listesi

İşletim Sistemi	**Adet**	**Antivirüs**	**Adet**
Windows 95, 98 veya öncesi Windows NT WorkStation Windows 2000 Professional Windows XP Windows Server (NT- 2000-2003 - .NET) Linux UNIX Sun Solaris IBM Diğer **Toplam**		**Güvenlik Duvarı** **Veri Tabanı Yönetim Sistemi** ORACLE SQL Server IBM DB2 MySQL-PostGre SyBase Informix Diğer **Toplam**	
Ofis Paketleri		**Coğrafi Bilgi Sistemi ve CAD/CAM**	
Microsoft Office Open Office Star Office Diğer **Toplam**		ESRI (ArcView-ArcInfo-..) MapInfo InterGraph AutoDESK (AutoCAD) NetCAD Diğer **Toplam**	

7.1.4. İnsan kaynakları

İnsan kaynakları istihdamı ve yönetimi olarak tüm bu kaynakların arasında en pahalı olanıdır. İnsan kaynaklarının envanterinin çıkarılabilmesi için kullanılabilecek şablona örnek olarak Tablo 7.1.4.1. ve Tablo 7.1.4.2 gösterilebilir.

Tablo 7.1.4.1 : İnsan kaynağı profili

	İlköğretim	**Lise**	**Yüksel Okul**	**Üniversite**	**Yüksek Lisans**	**TOPLAM**
Kuruluş Personel Sayısı						
Bilgisayar Kullanıcısı Personel Sayısı						
TOPLAM						

Tablo 7.1.4.2 : Bilgi İşlem Birimi Personelinin Görev Dağılımı ve Yetkinlikleri Şablonu

	Mühendis	**Bilgisayar Programcısı (Ön-Lisans)**	**Bilgisayar Teknikeri (Teknik Lise)**	**Sertifikalı Personel**	**Diğer**	**TOPLAM**
Uygulama Geliştirme						
Sistem Yönetimi						
Veri Girişi-Kontrolü						
Teknik Destek						
Programlama						
Diğer						
TOPLAM						

7.1.5. Ekibin Belirlenmesi

Kurum için, genel bir bilişim güvenliği politikasının parçası olmayan, sadece teknik elemanların önerileri ile yapılandırılmış bir bilişim güvenliği politikasının oluşturulması ve uygulanması, yeterli olmayacaktır. Bu nedenle kurumun Bilgi İşlem ve Sistem Sorumlusunun yanında çeşitli görev sahalarından katılımcılardan meydana gelen bir politika geliştirme ekibi oluşturulur. Oluşturulacak ekip;

- İdari konularda üst yönetim ile köprü oluşturarak destek sağlanmasında ve bürokratik engellerin aşılmasında yardımcı olmak üzere bir Rektör Yardımcısı,
- Kurumsal güvenlik politikasının ihlal ve aksi uygulamalar karşısında kurumun uygulayacağı yaptırımların anlatıldığı uyum kısmını oluşturmak üzere Bilişim Hukuku veya Ceza Hukuku dallarından bir akademisyen,
- Politikanın ihlal edildiği durumlarda hukuki yaptırımlar ve adli soruşturmaları yürütme konusunda kurum adına yardımcı olmak üzere Hukuk Müşaviri veya kurum avukatı,
- Temel kullanıcı profillerinden örnekleri biraraya getirmek üzere öğrenci, akademik ve idari personel temsilcileri,

Bilgi İşlem Güvenlik Birimi sorumlusunun liderliğinde biraraya gelmelidir.

7.1.6. Veri akış analizi çalışması

Günümüz bilgi teknolojileri dünyasında veri, en önemli değer olup bu yaklaşımla ele alınmalıdır. Bu sayede kuruma ait verilerin ve işlem kaynaklarının sistematik olarak sınıflandırılması, kullanımları ve değerleri ile ilgili olarak doğru, düzgün ve nitelikli kararların daha kolay verilebilmesi mümkün olur. Bundan sonra ancak, bu değerler üzerinde en uygun maliyetli çözümü uygulanabilir.

Güvenlik politikası oluşturma aşamasında verinin üretiminden silinmesine kadar geçen süreci kapsayan bir veri akış analizi yapılması gerekir. Bunu yaparken kullanılabilecek yöntemlerden bir tanesi de veri odaklı (data-centric) modeldir. Veri akış analizinin amacı, veriye müdahale edilen bütün düğüm noktalarının tanımlanmasına olanak sağlamaktır. Örneğin bir hareket işleme sistemini (transaction processing system) ele alalım; veri, tarayıcılar, web ve diğer sunucular veya güvenlik duvarları üzerinden akar ve veritabanlarında depolanır. Verilerin, tabi tutulan işlem boyunca akışının takibinin yapılmasıyla bu kurumsal değerlerin korunmasında, mantıksal ve fiziksel kontrollerin şekli ve yerine, doğru bir şekilde karar verilebilir.

7.1.7. Tehditler ve karşı tedbirlerin ortaya konulması

Bir tehdit profili ortaya çıkartmak, ele alınan ortamlarda hangi tip tehditlerin mevcut olduğu, bir tehditin ortaya çıkma olasılığı, alt kollarının neler olduğu, sonuçları ve maliyeti konusunda fikir sahibi olmamızı sağlar. Farklı ortamlarda farklı tehditlerin oluşabildiği unutulmamalıdır. Bir web sunucuya yapılacak saldırının tehditi ve sonuçları ile bir bilgi sistemine ait otomasyon sunucusuna yapılacak saldırının tehditi ve sonuçları farklı olacaktır. Ortaya konulan bu tehditlere karşı farklı seviyelerde tedbirler alınması gerekir. Sunucu üzerinde yazılım güvenlik duvarı çalıştırmak, sunucuyu DMZ bölgesine yerleştirerek iç ağdan gelebilecek tehditlere karşı önlem almak ve sunucunun kullanılmayan servislerini ve portlarını kapatmak, alınabilecek tedbirlere örnek olarak gösterilebilir. Ayrıca alınacak tedbirler bütün ayrıntılarıyla belgelendirilmelidir.

7.2. GELİŞTİRME

7.2.1. Ortak bir biçim ortaya konulması

Standart bir politika biçimi yazılan politikalar arasında uyumu ve tutarlılığı sağlar. Her standart üniversite politikasının ilk sayfasında başlık bloğu bulunur. Başlık bloğu;

- Kurum anteti
- Politikanın başlığı
- Politikanın versiyon numarası
- Politikanın yürürlüğe girdiğe tarih
- Politikadan sorumlu kişi
- Politikadan sorumlu birim

Bir standart üniversite politikası, başlık bloğuna ilave olarak en azından aşağıdaki başlıklara sahip olmalıdır:

- **Politika:** Politika ifadesinde kısaca ne yapmak istediğimizi anlatıyoruz. Yapılan uygulamanın bir özeti, politikaya kimlerin uyması gerektiği, ne zaman politikanın uygulanması gerektiği ve başlıca koşullar ve sınırlandırmaların neler olduğuna dair bilgiler yer alır.
- **Amaç**: Politika ifadesinde yer alan hususların ne amaçla yapılmak istendiği ve politikanın yazılma nedeni açıklanır. Hukuki veya yönetmelik gereği düzenlemelerin neler oldukları belirtilir. Politikanın çözüme ulaştıracağı anlaşmazlıklar veya problemler tanımlanır. Herkes için meşru kullanımın nasıl olduğu ve bunun getireceği faydalar anlatılır.
- **İçerik**: Politikanın içerik kısmında listelenen bilgiler, politikanın kısa veya uzun formda olup olmamasına bağlı olarak değişiklik göstermektedir. Örneğin bir politika, Bağlantılı Bilgiler ve İrtibat kısımları tamamlanmadan önce ele alınmak zorunda ise bu kısımlar için sayfa numaraları İçerik kısmında listelenmez. Uzun formdaki bir politika da beşinci dereceden başlıklara kadar sayfa numaraları ile bir listeleme olmalıdır.
- **Bu politikayı kimler bilmelidir**: Politikaya kimlerin riayet etmesi ve bu politikaya ait talimatları kimlerin takip etmesi gerektiği anlatılır. Görevlerini yapabilmeleri için politikayı kimlerin anlaması gerektiği ve ayrıca bu politikadan kimlerin etkileneceği bu kısımda belirtilir.

- **Bağlantılı bilgiler:** Talimatları yerine getirebilmek için gerekli bilgiler, konu ile ilgili diğer üniversite politikaları, faydalı olabilecek belgeler, kanunlar, ilgili programlar ve eğitim materyalleri bu kısımda sıralanır.
- **İrtibat:** Konu ile ilgili sorulara cevap verebilecek veya istisnaları onaylayabilecek kişiler, bağlı oldukları birimler, çalışma saatleri, telefonları ve e-posta adresleri bu kısımda yer alır.
- **Ayrıntılı içindekiler tablosu:** Karmaşık uzun formdaki bir politikada ayrıntılı içindekiler tablosu okuyucuya gruplar halinde sıralanmış başlık ve bilgiler arasında kolaylıkla gezinme imkanı sağlar. Ana ve alt başlıklar sayfa numaraları ile verilmelidir. Kullanılan kelime işlem programının (Microsoft Word benzeri) stil kısmındaki başlık formatları bu konuda yardımcı olacaktır.
- **Hariç durumlar:** Politikadan hariç tutulan herhangi bir bölge, birim veya kurumların (Üniversite içinden veya dışından) ve ayrıca kaynakların veya görev sınıflarının listesi bu kısımda yer alır. Eğer herhangi bir hariç durum yok ise politikanın Üniversitedeki bütün herkese uygulanacağı varsayılır.
- **Tanımlar:** Bu kısımda okuyucuların politikanın ana fikrini anlayabilmeleri için sadece özel terimler açıklanır. Konuya özel terimler, Ekler kısmında bir sözlük şeklinde yer alır. Alışkın olunmayan, özel anlamlar içeren veya teknik terimler alfabetik olarak sıralanarak tanımlanır.
- **Talimatname Başlığı:** Bu kısımda uygulanabilir politika, talimatname numarası, sorumlu yönetici ve sorumlu birim yer alır.
- **Özel Durumlar:** Bu kısım çok az kimseyi etkileyen veya sıkça karşılaşılmayan koşullara ait bilgiler içerir. Bu bilgiler alt başlıklara ayrılarak önem sırasına göre listelenir.
- **Sorumluluklar:** Bu politikaya iştirak eden kişi veya kurumlara ait temel sorumluluklar özetlenir.
- **Ekler:** Diğer kısımlara geçişi engelleyebilecek ve konu bütünlüğünü bozabilecek uzunlukta veya karmaşık referans bilgileri içerir. Ayrıca tüm işleyişin bir akış şemasını ve değişken veya çok az kimseye uygulanan bilgiler de burada yer alır.
- **Geçmiş:** Bu kısımda politikanın daha önceki sürümleri isimleri ve tarihleriyle sıralanır.

- **Sıkça Sorulan Sorular:** Ne kadar ayrıntılı, özenli ve kapsamlı bir politika yazılmış olsa bile her zaman kişisel yorumlar içeren birtakım sorular olabilecektir. Bu kısım en çok karşılaşılabilecek soruları ve bunlara özel cevapları içermektedir.

7.2.2. Taslak Oluşturulması

Belirlenen politikanın kaleme alınması sürecinde uygun dilin kullanılması, doğru ayrıntı seviyesinin belirlenmesi, yetki ve sorumlulukların doğru biçimde devri ve politika kapsamında ele alınması gereken konuların belirlenmesi bu safhayı belirleyici unsurlardır. Politikalar basit, anlaşılır ve okunması kolay bir şekilde hazırlanmış olmalıdır. Bir politika kanun kitabı değildir ve yorumlayabilmek için hukuk bilgisine ihtiyaç duyulmamalıdır. Kelimeler dikkatlice seçilmeli, cümleler kısa, kesin ve net ifadeler içermelidir. Özet ifadelerden oluşmalı daha ayrıntılı bilgi almak isteyenler için başvuracakları linkler belirtilmelidir. Ayrıca ifadeler hazırlanırken kurum koşulları göz ardı edilmemelidir. Taslak oluştururken dikkat edilecek birkaç husus aşağıda sıralanmıştır:

- **Farklı seviyelerden kullanıcılara hitap etmelidir:** Politikaların oluşturulmasının ve yazılmasının temel amacı kullanıcılar tarafından okunması ve uygulanmasıdır. Politikaları hazırlarken kullanıcılar hiç bir zaman göz ardı edilmemelidir. Herhangi bir politika ifadesi yazılmadan önce hangi kullanıcıya hitap ettiği ve kullanıcının konu hakkındaki bilgi seviyesinin ne olduğu konusunda mutlaka çalışma yapılmalıdır.
- **Düzenli olmalıdır:** Kullanıcıların politikanın ifade etmek istediği hususları anlayabilmeleri için politikalar bir mantıksal ve gerçekleşme sırasına göre yazılmalıdır. Eğer maddeler düzgün planlanmazsa kullanıcıların beklenen şekilde açıkça anlaması mümkün olmaz. Cümleler kolayca sindirilebilir bilgilere bölünmelidir. Uzun ve neredeyse bir paragraf süren cümleleri kullanıcıların sıkılmadan okuyabilmesi ve sonrasında da bununla ilgili işlemleri başarıyla gerçekleştirmesi beklenemez.
- **Belgenin okunması ve düzenlenmesi:** Cümlelerin sadece dilbilgisi kurallarına uygun olup olmadığının kontrolü, onun yayınlanmaya hazır olduğunu göstermez. Bu durum özellikle bir yabancı dilden yapılan çevirilerde sıkça

rastlanılan bir durumdur. Bazen cümle özne, tümleç ve yüklem içererek imla kurallarına uygun olsa bile cümleden bir anlam çıkartmak oldukça güçtür. İfadeleri hazırlayan kişi öncelikle yazdıklarını anlayabilmeli ki kullanıcıların anlayabilmesi de mümkün olsun.

- **Konunun uzmanının bulunması:** Herhangi bir politika veya talimatname oluşturma işleminde ilk adım konuyu öğrenmek veya konuyu bilen ve bilgisi yazma işleminde kullanılabilecek birisini bulmaktır. Konunun uzmanı olan kişi politika yazma işlemi hakkında bilgi sahibi olmayabilir. Bu nedenle onunla birlikte çalışarak işleyişin nasıl olduğu ile ilgili notlar alınıp, sonrasında politikalar ve talimatnameler yazılır.
- **Açık ve bilinen kelimeler kullanılmalı:** Politikanın hitap ettiği kullanıcılar eğer alışkın olmadıkları kelimeler, deyimler ve kısaltmalarla dolu bir belge ile karşılaşırlarsa bu durumdan hiç hoşnut olmazlar. Tanımlar bölümünün bu amaçlar için kullanılabileceği unutulmamalıdır. Tüm kısaltmaların açıklandığından emin olunmalıdır. Eğer yazı içerisinde tanımlanmamış terimler yer alırsa kullanıcı ilgisini kaybedebilecek ve kavrama güçlüğü yaşayabilecektir.
- **Cümleler kısa ve basit olmalı:** Uzun cümleler kullanıcılarda hayal kırıklığı yaratabilecek ve anlama seviyesini düşürebilecektir. Talimatname ifadeleri için uygun bir ortalama cümle uzunluğu on ile onbeş kelimeden oluşur.

- **Fog Index:** Fog Index yazılı metinlerin ne kadar kolay okunur ve anlaşılır olduğunu görme açısından analizini yapmakta kanıtlanmış bir yöntemdir [212]. Bu yöntemde sis endeksinin hesaplanabilmesi için örnek olarak 7.1.7 bölümünü ele alırsak;
  1. Yazıdaki kelimelerin adedi çıkarılır, (103)
  2. Yazıdaki cümlelerin adedi çıkarılır, (6)
  3. Yazıdaki büyük kelimelerin adedi (3 ve daha fazla heceye sahip olanlar) çıkarılır, (34)
  4. Daha sonra kelime adedi, cümle adedine bölünerek ortalama cümle uzunluğu hesaplanır. (103/6 = 17)
  5. Büyük kelime adedinin toplam kelime adedi içerisindeki oran hesaplanır, (34/103 = %33)
  6. Ortalama cümle uzunluğu ve büyük kelime oranı toplanır, (17+33 = 50)
  7. Sonuç 0,4 ile çarpılır, (50x0,4 = 20) ve çıkan 20 sayısı endeksi ifade eder.

Robert Gunning tarafından oluşturulan bu matematiksel formüle dayanarak metinlerin anlaşılırlığı konusunda bir sis endeksi geliştirilmiştir. Bu endekse göre 3 ile 11 arasında olanlar iyi, 7-8 en ideali, 12-14 arası olanlar biraz fazla uzun, 15 ve yukarısı ise hukuk diline yakın, kabul edilmez ölçüde ağdalı bulunmuştur.

Bu formül, Türkçe pek çok metne uygulanmış ve tutarlı bir sonuç vermemiştir. Bunun üzerine yeni bir matematiksel çözüm aranmış, deneysel çalışmalar sonunda Sönmez tarafından, Sönmez Modeli adı verilen yeni bir matematiksel formül bulunup önerilmiştir [Sönmez V., 213]. Bu formülle, araştırma kapsamına alınan tüm metinlerin anlaşılırlık düzeyi güvenilir bir şekilde saptanmıştır. Formüle göre metindeki yabancı, bilinmeyen sözcük, deyim, terim, kavram, mecaz, benzetme formül, sembol vb. sayısı; metindeki tüm sözcüklerin sayısına bölünüp karesi alınmıştır. Bulunan rakamlar metne göre bir ile sıfır arasında yer almaktadır. Bire yaklaştıkça metin anlamsızlaşmakta, sıfıra yaklaştıkça ise, açık ve anlaşılır hale gelmektedir. [Sönmez V., 213]

- **Konuyu destekleyen çizimler kullanılmalıdır:** Metnin içerisine şekiller yerleştirerek bahsi geçen konunun anlatımı kolaylaştırılmış olur. Bu şekiller; resim, akış şeması, pasta veya çubuk şeklindeki grafikler olabilir. Ekran görüntülerinin kullanılmasıyla da resimler oluşturulabilir. Bu tip görüntüler, kullanıcıların bahsi geçen işlem veya programın neye benzediğini ve sonuç olarak karşısına neler çıkacağını görebilmesi açısından faydalı olabilecektir.
- **Cümlelerde etken çatı kullanılmalıdır:** Etken çatılı cümle yapısında vurgu yapılması gereken şeyin üzerinde yoğunlaşır. Hangi faaliyetten kimin sorumlu olduğu belirtilmiş olur. Örneğin edilgen çatıda olan cümle, “Bütün web sayfalarının yedeği web sorumlusu tarafından alınacaktır.” Bu cümlenin etken çatıdaki hali ise “web sorumlusu, haftada bir bütün web sayfalarının yedeğinin alınmasından sorumludur” şeklinde olacaktır.
- **Dilbilgisi ve noktalamaların doğruluğundan emin olunmalıdır**.

7.2.3. Onay alınması

Ortaya çıkan taslak politika üzerinde tartışılarak, Politika Hazırlama Ekibinin onayı alındıktan sonra karara varılır. Güvenlik ekibi yöneticisinin son gözden geçirmeleriyle politikanın son haline gelinir. Kurumdan kuruma değişmekle beraber, üniversiteler için Rektör Yardımcısının başkanlığını yaptığı bir Politika Onay Komisyonu oluşturularak, politikanın son hali üzerinde karara varılır. Politika üzerinde düzeltmeler yapılması gerekiyorsa Politika Hazırlama Ekibine geri gönderilir. Politika Onay Komisyonunun onayı ile kesinlik kazanan politika resmi onay için senatoya sunulur. Yönetimsel destek alınmayan, ayarlamaların ve kısıtlamaların birçok soruna yol açabileceği unutulmamalıdır. [Karaarslan E. ve diğ., 214]

7.2.4. Duyurulması ve uygulanması

Senatonun onayından sonra kurum yöneticisi tarafından güvenlik politikası, resmi yazı ile bütün birimlere duyurulmalıdır. Bu yazıda güvenlik politikasının oluşturulma nedenleri ve güvenlik politikasının ana hatları verilmeli, daha ayrıntılı bilgi için kullanılabilecek erişim bilgileri de belirtilmelidir.

Güvenlik politikasının en son sürümüne, bütün çalışanların erişimini sağlayabilmek için bütün yollar kullanılmalıdır. Bu amaç için posterler, seminerler, toplantılar, e-postalar ve web sayfaları kullanılabilir. Ayrıca kurumun güvenlikle ilgili bir web sayfası olmalı duyurular burada da yer almalıdır. Bir diğer yol da, ayda bir yayınlanabilen bir bülten veya broşür olabilir. Bu bültende yeni gelişmeler, güvenlik açıkları, tehditler ve politikadaki son güncellemeler akıcı ve anlaşılabilir dille yer alabilir. Çok fazla teknik olmayan ve kısa cümlelerden oluşmuş, renkli ve canlı bir bülten, kullanıcıların ilgisini cezp ederek, politikanın etkin bir şekilde duyurulması yönündeki hedefe bir adım daha yaklaştıracaktır. Hazırlanan bültenin en fazla kullanıcıya ulaştırılabilmesi amacıyla; giriş çıkış kapıları, yemekhaneler, kantinler ve yurtlar gibi kilit noktalarında dağıtılmalıdır.

Şekil 7.2.4.1 : California-Berkeley Üniversitesi “Be Secure” dergisine ait iki sayfa

Berkeley Üniversitesi’nin periyodik güvenlik eğitimi çalışmalarından biri olan “Be Secure” dergisinin son sayısına ait iki sayfa Şekil 7.2.4.1. de görülmektedir [215]. Dergide dört temel güvenlik standardı (antivirüs, güvenlik duvarı, yamalar ve güçlü şifreler) hakkında, sekiz sayfalık, takibi ve uygulaması kolay bir rehber hazırlanmış ve kampüste dağıtılmıştır.

Uzun ve zahmetli bir süreç sonucu hazırlanmış olan güvenlik politikası, yönetim tarafından onaylanıp, duyurulduktan sonra uygulama aşamasına geçilir. Bu aşama politikanın oluşturulma aşamasından daha zordur. Bu aşamada ilk olarak, bilgi teknolojileri ekibini; resmi güvenlik politikasının uygulanmasında dikkat edilmesi gereken bütün esas noktalar, kurumsal güvenlik anlayışı ve bakışı konularında bilinçlendirmek ve eğitmek gerekmektedir. Güvenlik politikasını tüm kullanıcıların benimseyip sahiplenebilmesi için, öncelikle onlara örnek alabilecekleri, bilgi ve beceri

olarak tam donanımlı bir bilgi teknolojileri ekibi oluşturulmalıdır. Ancak ekibin hazır hale getirilmesinden sonra, kullanıcıların bilinçlendirme süreci başlatılabilir.

7.2.5. Güvenlik Bilinçlendirme Programı

Güvenlik Bilinçlendirme Programı (Security Awareness Program), bir kurumsal güvenlik politikasının başarılı olarak uygulanabilmesi için anahtar unsurlardan biridir. Temel hedef, güvenlik politikasında belirtildiği şekilde kuruma ait değer ve kaynakların güvenliğinin sağlanmasında, her bir çalışanın veya kullanıcının rollerini ana hatlarıyla tanımlamaktır. Güvenlik Bilinçlendirme Programının hedefi, ayrıca bilgi güvenliği konusunda ilgiyi arttırmak, etkin ve kolaylıkla anlaşılır hale getirmektir. Bu program "bilinçlendirme" ve "eğitim" olmak üzere ikiye ayrılabilir. Başlangıç olarak aşağıdaki soruların cevaplandırılması gerekir:

- Bu programla varılmak istenen nedir? Burada kısa vadeli ve daha küçük ve belirgin hedefler belirlenebilir.
- Hedef kullanıcı kitlesi kimlerdir ve eğitim düzeyleri nelerdir? Burada programı ikiye bölerek, birini bilgisayarlar hakkında yeterli bilgisi olanlara, diğerini yeterli bilgisi olmayanlara yönelik olarak hazırlamak uygun olabilir.
- Kullanıcılara nasıl ulaşılabilir, motive edilebilir ve daha da önemlisi bu konu üzerine ilgileri nasıl çekilebilir? Kullanıcıların güvenlik bilincini ortaya koyabilecek anketler düzenlenebilir. Bu anketler bilinç seviyesini ölçtüğü gibi aynı zamanda kullanıcıların konu hakkındaki yanlış anlamalarını ve sıkça yapılan hatalarını görmek için de faydalı olur. Böylece düzenlenecek programın, kalitesini geliştirmek mümkün olur.

Güvenlik bilinci ölçüm anketinde kullanılabilecek sorulara aşağıdakiler örnek olarak verilebilir:

1. Aşağıdaki parolalardan hangisi en güvenli olanıdır, neden?
    a) abc123456
    b) 13041980
    c) HakaN
    d) $kst987ew
    e) Bilmiyorum

2. Aşağıdakilerden hangisi bir e-posta ile gelebilecek en tehlikeli uzantıya sahip dosyalardır, neden?
    a) *.exe
    b) *.com
    c) *.bat
    d) *.vbs
    e) Hepsi
3. Güvenlik politikasında, "Bilgi Teknolojileri Ofisinden (BTO) e-posta aracılığıyla hiçbir güncelleme gönderilmeyecektir" ifadesine rağmen bir e-posta aldınız, ne yaparsınız?
    a) E-posta guvenlik@iu.edu.tr den geliyor, bu e-posta bizim BTO ya ait, güvenir ve hemen çalıştırırım.
    b) Güvenlik politikasında herhangi bir ekli dosyayı taramadan açmamam gerektiği söyleniyor. Bu nedenle önce taratır sonra çalıştırırım.
    c) Bilgisayarımı güncellemem.
    d) Daha fazla bilgi alabilmek için hemen BTO' yu ararım.
    e) E-postaları okurum fakat bir işlem yapmam.
4. Bir arkadaşınız işyerindeki bilgisayarınızda kurup kontrol etmenizi istediği bir program CD si verdi. Ne yaparsınız?
    a) Arkadaşıma güveniyorum. Bana asla virüslü veya zararlı bir program içeren bir CD vermez, hemen kurarım.
    b) Her ne kadar arkadaşım vermiş olsa da, güvenlik politikasında "Tüm taşınabilir medyaların (USB disk, mp3 çalar, CD ve DVD vb.) kullanımları belli kurallarla sınırlandırılmıştır." başlığı altındaki talimatlara göre, çalıştırmadan önce virüs taramasından geçiririm.
    c) İş yerindeki bilgisayarımdan önce dizüstü bilgisayarımda çalıştırırım.
    d) İşyerindeki bilgisayarımı, kişisel uygulamalarım için kullanmam.
    e) Program kurmayı bilmiyorum.
5. BTO dan aradığını iddia eden bir kişi (hatta isim de veriyor), size bilgisayarınızda bir güvenlik problemi olduğunu ve uzaktan erişip düzeltebilmesi için de parolanıza ihtiyacı olduğunu söylüyor. Ne yaparsınız?

a) BTO, kurumumuzda bilgisayar güvenliğinden sorumlu birimdir. Parolam olmadan bilgisayarıma ulaşamazlar. Bu nedenle onlara parolamı veririm.
b) Bu konuda kendilerine geri döneceğimi söyleyip, teyit için BTO'yu ararım.
c) Ben zaten bilgisayarımın güvenliği için gerekli her şeyi yaptım. Bu nedenle onlara parolamı vermem.
d) Ben parolamı kimse ile paylaşmam, mümkün olduğunca gizli tutarım.
e) Bilgisayarım parolasız olarak açılmaktadır.

Bu örnek sorular, güvenlik politikası içerisinde yer alan, önemli birçok noktaya dikkat çekmektedir. Anketin kaç sorudan oluşacağı kararı, tamamen ilginin çekilmek istendiği ve değinilmek istenen konulara bağlıdır. Burada önemli olan, yürütülen programın etkinliğini ve ne düzeyde olduğunu gözlemleyebilmek için anketlerin belli periyotlarla düzenli olarak yapılması gerektiğidir.

Güvenlik bilincinin geliştirilebilmesi için tek yolun, kullanıcıların uygun ve düzenli olarak eğitilmesi gerektiği bir gerçektir. Elbette bu konuda elde edeceğimiz başarının seviyesi, eğitim hususunda geliştireceğimiz yöntemlerin çeşitliliğine bağlı olarak değişebilecektir. İçerik ve sunuş açısından kullanıcıların sürekli ilgisini ayakta tutabilecek ve onları öğrenmeye teşvik edecek, etkin eğitim seçenekleri geliştirmek gerekir. Bu seçeneklerden birkaçı aşağıda sıralanmıştır:

- Kullanıcıların ilgisini çekebilecek, güvenlikle ilgili konularda eğitsel yarışmalar düzenlenebilir. Bu yarışmalardan sonra başarılı olanlar, BTO' nun güvenlik web sayfasında duyurulabilir.
- Kullanıcılara, "size ihtiyacımız var" fikrini aşılayarak, kurumsal güvenlik içerisindeki yerleri konusunda bilinçli bir bakış açısı oluşturulabilir.
- Kullanıcıların fikirleri, önerileri ve kişisel tecrübeleri, güvenlik bilinçlendirme eğitimleri sürecinde değerlendirilebilir. Böylece onların da, bu işin bir parçası oldukları vurgulanmış olur. Bu tarz bir yaklaşım kullanıcılara az veya çok mutlaka olumlu yönde bir etki edecektir.
- Daha önce basılı materyal olarak sunulan güvenlik bülteni fikrini, bir adım daha ileri götürerek, e-posta kanalıyla tüm kullanıcılara ulaştırabileceğimiz, belirli bir

içeriğe sahip ve periyodik bir düzene kavuşturabiliriz. Burada temel amaç, kurumsal güvenlik politikasının ana hatlarını anlayabilmeleri için, kullanıcıların ilgisini çekecek ve onları cezp edecek bir yol uygulamaktır. Bu fikrin daha açık ifade edilebilmesi için örnek bir güvenlik bülteni şablonu aşağıda verilmiştir.

Örnek Güvenlik Bülteni:

İstanbul Üniversitesi Bilgi Teknolojileri Ofisi (BTO) Güvenlik Bülteni
Sayı:1, Tarih:
http://bto.iu.edu.tr/guvenlik
guvenlik@iu.edu.tr
Tel: 440 00 00 / 12345

1. **Yaklaşan etkinlikler:** Bu kısımda, en yakın tarihli güvenlik bilinçlendirme programı ile ilgili toplantı, seminer, yarışma ve eğitimler gibi tüm faaliyetler yer alır.

2. **Güvenlik ile ilgili bir makale:** Güvenlik bilinçlendirme programı çerçevesinde yapılmış bir toplantıdan sonra, kullanıcıların ilgisinin devamını sağlayabilmek için, son toplantıda işlediğimiz konu ile ilgili bir makale hazırlamak uygun görünmektedir. Makalede farklı bir konuyu ele almak, kullanıcıların kafalarını karıştırmaktan öteye gitmeyecektir. Makale kolay anlaşılabilir bir dille ve fazla ayrıntıya kaçmadan hazırlanmalıdır. Burada amaç, toplantının konularının özetlenmesi ve bir tekrar yapılmasıdır. Makaleye örnek teşkile edecek konular;

- Parola güvenliği: Bu konuda, kurumsal verilerin korunmasında parolaların önemi ve düzgün parolalar oluşturma yönünde örnekler anlatılabilir.
- Uygun internet kullanımı: Bu konuda, kurumun sahip olduğu internet bağlantısının kullanım amacı, internet ve e-postalar aracılığıyla gelebilecek tehlikeler, kurumun bu yönde aldığı önlemler anlatılabilir.
- Bilgi Teknolojileri Ofisinin kurumdaki yeri, sorumlulukları ve çalışma prensipleri hakkında bilgiler verilebilir.

3. **Nedir…?** Bu köşede, en son yapılan toplantıda ele alınmış konuya ait güvenlik ile ilgili bilinmesi gereken virüs, solucan (worm), güvenlik duvarı (firewall), olta yöntemi (phishing) ve benzeri terimlerin kısa ve teknik açıklamalarına yer verilebilir.

4. **Bize sorun**: Bu bölüm, kullanıcıların güvenlikle ilgili sorularını, doğrudan konunun uzmanlarına sorabilecekleri ve kullanıcılar ile BTO arasında bir köprü oluşturacak, çok önemli ve etkili bir bölümdür.
5. **Güvenlik kaynakları**: Bu bölümde güvenlik problemleri ve çözümleri ile ilgili bir veya iki haber, kolay anlaşılabilir bir şekilde ele alınabilir. Ayrıca güvenlikle ilgili referans teşkil edecek birkaç siteye ait linkler de bu bölümde yer alabilir.
6. **İletişim:** Bu bölümde ayrıca, hangi problemlerle hangi birimlerin ilgilendiğine dair sorumlu isimleri, e-postalar ve telefonları yer alabilir.
7. **Öneriler:** Bu bölümde, güvenlik bülteninin daha etkili olabilmesi için ele alınabilecek konularla ilgili kullanıcılardan gelen öneri ve geri bildirimlere yer verilebilir.

7.3. BAKIM

Güvenlik politikası geliştirme ve uygulama süreci, sürekli yinelenen canlı bir süreçtir. Aslında her şey politikanın yürürlüğe girdiği anda başlar. Güvenlik politikasında belirtilen hususlara, o ana dek, bazı kullanıcılar uymakta, bazı kullanıcılar bilinçli bazıları da bilinçsiz olarak uymamaktadırlar. Yapılan hatalı uygulamaların, tehdit ve saldırıların karşısında, teknik çözümlerle ancak belli bir noktaya kadar başarılı olunabilir.

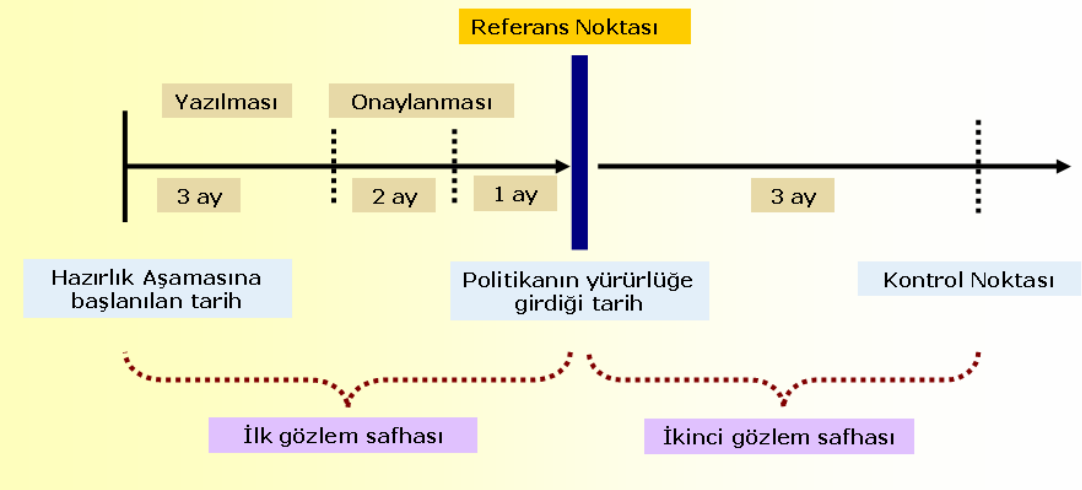
Güvenlik politikasının yürürlüğe girdiği tarih, yöneticiler, akademisyenler, öğrenciler ve çalışanlar, kısacası kurumun tüm kullanıcıları için, çalışma hayatlarında bir dönüm noktası olacaktır. Güvenliğin sağlanabilmesi için uyulması gereken tüm kurallar ve talimatlar yazılı hale getirildiğinden, kimsenin insiyatif kullanmasına ve karar verme aşamasında tereddüde düşmesine gerek kalmayacaktır. Bu sürecin istenildiği düzeyde verimli, kurumsal güvenlik adına faydalı olabilmesinin ve sürekliliğinin sağlanabilmesi için de, politika hazırlama ekibinin çalışmalarına en ufak bir yavaşlama olmadan devam etmeleri gerekir. Bu çalışmalar içerisinde, kullanıcılardan gelen taleplerin değerlendirilmesi, politikanın gözden geçirilmesi, politikaya uyumun sağlanması ve takibi yer almaktadır.

7.3.1. Taleplerin değerlendirilmesi ve gözden geçirme

Kullanıcıların fikirleri ve önerileri, kişisel tecrübelerine dayanarak verdikleri geri bildirimler, politikanın güncelliğinin, etkinliğinin ve sürekliliğinin sağlanması açısından çok faydalı olacaktır. Bu yönde elde edilen verilerle ve belli periyotlarla, güvenlik politikası gözden geçirilmelidir. Politikanın hazırlanan yeni sürümün getirdiği yenilikler ve bir önceki sürüm arasındaki farklar, nedenleriyle kullanıcılara aynı hassasiyetle duyurulmalıdır.

7.3.2. Uyumun sağlanması ve takibi

Güvenlik politikasının ele aldığı anahtar konuların etkin bir biçimde uygulanıp uygulanmadığını ve politikanın başarı seviyesini ölçmek amacıyla belli aralıklarla gözlemler yapılması gerekir. Başlangıç olarak, bu konuda bir gözlem süreci ortaya koyulabilir. Bu süreçte, güvenlik politikasının hazırlık aşamasının başlangıç tarihi ve yürürlüğe girdiği tarih arasında geçen süre (ortalama altı ay), ilk gözlem safhasını oluşturabilir. Burada referans noktası, politikanın yürürlüğe girdiği tarihtir. (Şekil 7.3.2.1)



Şekil 7.3.2.1 : Gözlem süreci

Bu ilk gözlem safhasında, daha sonra birbirleriyle karşılaştırmak üzere, belirlenen konularda bulgular toplanabilir. Daha sonra bu bulgular, ikinci gözlem safhası olan, referans noktası ile kontrol noktası arasında geçen sürede (ortalama üç ay) toplanan bulgularla karşılaştırılabilir. Bulguların elde edilebilmesi için mercek altına alınacak

konular ve izlenecek hususlara ait örneklerin yer aldığı, Tablo 7.3.2.1'dekine benzer bir tablo hazırlanabilir.

Tablo 7.3.2.1 : Veri kaynakları ve takip edilecek konular

Veri kaynakları	Takip edilecek konular
Güvenlik duvarı bilgi, hata ve uyarı mesajları	Hem içeriden dışarı hem de dışarıdan içeri doğru olan port bazında aktivitelerin ve internet kullanımının gözlemlenmesi
IDS/IPS sistemlerine ait bilgi, hata ve uyarı mesajları	Hem iç hem de dış yönde akan trafiğin, uygulama seviyesinde analizi ve dosya download/upload miktarının ölçümü
E-postalar	Gelen ve gönderilen virüslü e-posta oranı, Gelen ve gönderilen spam postaların oranı ve Toplam gönderilen e-posta miktarının ölçülmesi
İçerik Süzme	Politikada erişimi yasaklanmış olan sitelere girme girişimleri ve Politikada yapılması yasaklanmış olan oyun ve benzeri uygulamaların, toplam trafiğe oranları
Kullanıcı bilgisayarları	Gelen donanım ve yazılım problemleri, Ağın taranarak; antivirüs kullanmayan, yama ve güncellemeleri yapmamış olan kullanıcı bilgisayarlarını tespiti, Güçlü parola kullanım oranının tespiti, Uygun bilgisayar kullanımı ve yerleşiminin kontrolü
Fiziksel güvenlik	İzinsiz olarak kurulmuş olan hub, kablosuz erişim noktaları (access point) ve çekilmiş olan internet hatlarının tespiti

Örnekleri Tablo 7.3.2.1 de görülen konulardan elde edilen veriler ve bulgular, yapılan bu çalışmanın başarı oranının rakamsal bir göstergesi olacaktır. Sonuçların çok daha istikrarlı ve kapsamlı elde edilebilmesi için, oluşturulacak tablo veya kontrol listesi mümkün olduğunca geniş tutulmalıdır. Hatta her konuda, ayrı bir kontrol listesi hazırlanabilir.

7.4. POLİTİKA ÖRNEKLERİ

Kabul edilebilir kullanım politikası: Kabul edilebilir kullanım politikası, kurumun ağının, ağ cihazları ve hizmetlerinin kabul edilebilir kullanımı, kullanıcıların hakları, sorumlulukları ve kurumun tüzel kaynaklarını ve sahip olduğu bilgilerinin korunması için alınması gerekli önlemleri tanımlar.

Bilgisayar kullanım politikası: Bilgisayar kullanım politikası, kurumun sahip olduğu ve kurumsal görevlerini yerine getirmesinde yardımcı olmak üzere çalışanlarının kullanımına sunduğu bilgisayarlar ve kişilerin kendi sahip oldukları bilgisayarların,

amacına uygun olarak kullanılabilmesi için uyulması gereken kurallar ve talimatnameleri içerir.

Antivirüs politikası: Antivirüs politikası, kurumun internet ağ ve bilgisayarlarını, kötü amaçlı program kodlarının (virüs, solucan, Truva atı ve arka kapılar vb.) yarattığı tehditlerle, etkin bir şekilde mücadele edebilme ve büyük ölçüde olumsuz etkilerini azaltabilmek amaçlı hazırlanmış kurallar ve talimatnameleri tanımlar.

E-posta kullanım politikası: E-posta kullanım politikası, kurumsal kaynakların en verimli, etkin ve güvenli bir şekilde kullanılabilmeleri için, e-posta gönderme ve alma işlemi ile ilgili olarak uyulması gereken kurallar ve talimatnameleri içerir.

Öğrenci laboratuarları kullanım politikası: Öğrenci laboratuarları kullanım politikası; öğrencilerin ders, ödev ve akademik araştırma yapmaları amacıyla hizmete sunulmuş olan öğrenci laboratuarlarının, amacına uygun olarak kullanılabilmesi için uyulması gereken kurallar ve talimatnameleri içerir.

Öğrenci yurtları ağ kullanım politikası: Öğrenci yurtları ağ kullanım politikası, öğrenci yurtlarında öğrencilerin, eğitim ve araştırma amaçlı çalışmalarını internet destekli olarak yürütebilmeleri ve diğer kullanıcıların birincil ağ erişim gereksinimlerini (akademik, idari, eğitim, araştırma) yerine getirmelerine engel olmaması amacıyla, ağ kaynaklarının kullanımında uyulması gereken kurallar ve yasaklanmış faaliyetleri tanımlar.

İnternet kullanım politikası: İnternet kullanım politikası; kurumun akademik, idari, eğitim ve araştırma amacıyla çalışanlarının hizmetine sunduğu internet ağının, bu amaçlar doğrultusunda etkin, verimli ve güvenli olarak kullanımında uyulması gereken kurallar ve yasaklanmış faaliyetleri tanımlar.

Güvenlik duvarı kullanım politikası: Güvenlik duvarı, kurumun internet çıkışında bir geçit vazifesi görerek giren ve çıkan trafiği kurumun çalışma amaçları doğrultusunda, IP ve port bazında kontrol eder, izin verir veya engeller. Bu nedenle güvenlik duvarı kullanım politikası; kurumun internet ağının, akademik, idari, eğitim ve araştırma

amacıyla etkin, verimli ve güvenli bir şekilde kullanımını sağlayabilecek ayarların ve yapılandırmaların tanımlarını içerir.

Parola kullanım politikası: Parola kullanımı bilgisayar ve ağ güvenliği için önemli bir özellik olup kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir parola ağ ve bilgisayar güvenliğini tümüyle riske sokabilir. Bu nedenle parola kullanım politikası, güçlü parolalar oluşturulması, oluşturulan parolanın korunması ve bu parolaların değiştirilme sıklığı hakkında uyulması gereken kuralları ve talimatları tanımlar.

Uzaktan erişim politikası: Uzaktan erişim politikası, kurum kaynaklarının yetkisiz kullanımından dolayı kuruma gelebilecek potansiyel zararları asgari düzeye indirebilmesi için, kurum internet ağı dışındaki herhangi bir yerden kurumun yerel ağına erişilmesi ile ilgili uyulması gereken kuralları ve talimatları içerir.

Ağ cihazları güvenlik politikası: Ağ cihazları kullanım politikası, kurumun internet ağını oluşturan; yönlendirici (router), anahtar (switch), hub ve benzeri cihazların, azami düzeyde güvenliğinin sağlanabilmesi için gerekli konfigürasyon tanımlarını içerir.

Sunucu güvenlik politikası: Sunucu güvenlik politikası, kurumun bilgi kaynaklarına ve kullanmış olduğu uygulamalara, yetkisiz erişimleri ve gelebilecek potansiyel zararları asgari düzeye indirebilmek amacıyla, sahip olduğu sunucularının azami düzeyde güvenliğinin sağlanabilmesi için yapılması gereken konfigürasyon tanımlarını içerir.

VPN kullanım politikası: Sanal Özel Ağ (VPN) kullanım politikası, kurumun internet ağına, kurum dışından güvenli erişimin sağlanabilmesi ve kullanıcıların akademik ve eğitim amaçlı hizmetlerden faydalanabilmesi için uyulması gereken kuralları ve talimatları içerir.

Kablosuz iletişim (Wireless) kullanım politikası: Kablosuz iletişim (Wireless) kullanım politikası, kurum bünyesinde kullanılabilecek bütün kablosuz haberleşme cihazlarının (mobil bilgisayarlar, kablosuz erişim noktaları (access point), kablosuz modem, cep telefonları, PDA vb.) gerekli güvenlik tedbirleri alınmaksızın kurumun

bilgisayar ağına erişimini engellemek amacıyla uyulması gereken kuralları ve talimatları içerir.

Sunucu yedekleme politikası: Sunucu yedekleme politikası, sunucular üzerinde oluşabilecek hatalar ve olası saldırılar karşısında, sistemlerin kesinti sürelerini, olası bilgi kayıplarını, harcanabilecek insan emeğini ve işgücünü en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi amacıyla uyulması gereken kuralları ve talimatları içerir.

Fiziksel güvenlik politikası: Fiziksel güvenlik politikası, kurum bilgisayar ağına ait cihazların ve kritik kurumsal bilgilerinin korunması amacıyla sistem odasına, kurumsal bilgilerin bulundurulduğu sistemlerin yer aldığı tüm çalışma alanlarına ve kurum binalarına yetkisiz girişlerin yapılmasını önlemek amacıyla uyulması gereken kuralları ve talimatları içerir.

8. UYGULAMA: İSTANBUL ÜNİVERSİTESİ POLİTİKA ŞABLONU

Güvenlik politikası geliştirilmesinin işlendiği 7. Bölümde, bu alanda köklü ve kapsamlı projeler geliştirmiş olan üniversitelerin çalışmaları ve bu yönde hazırlanmış olan uluslararası standartlar esas alınarak, bir süreç ortaya konulmaya çalışılmıştır. Bu süreci meydana getiren adımlar; ayrıntıları ve örnekleriyle açıklanmıştır. Ortaya konulan süreç takip edilerek, İstanbul Üniversitesi'nde uygulanacak güvenlik politikasının hazırlık çalışmalarına başlanmıştır. Elde edilen bilgiler, örnekler ve belirlenen sistematik doğrultusunda aşağıda görülen, İstanbul Üniversitesi güvenlik politikası şablonu hazırlanmıştır.

	T.C. **İSTANBUL ÜNİVERSİTESİ REKTÖRLÜĞÜ** **BİLGİ TEKNOLOJİLERİ OFİSİ**	

POLİTİKA 1.0.0.
Sayı:
Bölüm:
Yayımlayan Birim:
Sorumlu Birim:
Sorumlu Yönetici:
Yürürlüğe Girdiği Tarih:
Revizyon Tarihi:

İçindekiler

Amaç

Kapsam

Sorumluluklar

Tanımlar

Terim: Tanımı

Genel İlkeler

Hariç Durumlar

Özel Durumlar

Uyum ve Yaptırımlar

Ekler

Geçmiş

Değiştirilme Tarihi:
Değiştirilen hususlar:
Yerini aldığı sürüm:

Sıkça Sorulan Sorular

İrtibat

Konu İlgili Personel Telefon e-posta

Dizin

8.1. İstanbul Üniversitesi Güvenlik Politikaları

Bir önceki bölümde hazırlanmış olan şablon; bilgisayar, internet, e-posta, parola, antivirüs, öğrenci laboratuvar ve yurt kullanımları örnek olmak üzere, ihtiyaç duyulan her konuda politika hazırlama hususunda kullanılabilir.

8.1.1. İstanbul Üniversitesi Ağ Kullanım Politikası

İstanbul Üniversitesi Ağ Kullanım Politikası, politikanın amacında belirtildiği üzere; kurumun ağının, ağ cihazları ve hizmetlerinin kabul edilebilir kullanımı, kullanıcıların hakları ve sorumlulukları, kurumun tüzel kaynaklarını ve sahip olduğu bilgilerinin korunması için alınması gerekli önlemleri ve uyulması gerekli kuralları tanımlamak amacıyla hazırlanmıştır.

T.C.
İSTANBUL ÜNİVERSİTESİ REKTÖRLÜĞÜ
BİLGİ TEKNOLOJİLERİ OFİSİ

İstanbul Üniversitesi Ağ Kullanım Politikası

POLİTİKA 1.0.0.

Sayı:	1
Bölüm:	1
Yayımlayan Birim:	İstanbul Üniversitesi Rektörlüğü Bilgi Teknolojileri Ofisi
Sorumlu Birim:	Ağ Sistemleri Güvenlik Birimi
Sorumlu Yönetici:	Hakan Aysal
Yürürlüğe Girdiği Tarih:	15.01.2007
Revizyon Tarihi:	En son sürümdür

İçindekiler

Amaç

İstanbul Üniversitesi Ağ Kullanım Politikası, kurumun ağının, ağ cihazları ve hizmetlerinin kabul edilebilir kullanımı, kullanıcıların hakları ve sorumlulukları, kurumun tüzel kaynaklarını ve sahip olduğu bilgilerinin korunması için alınması gerekli önlemleri ve uyulması gerekli kuralları tanımlamak amacıyla hazırlanmıştır.

Kapsam

Bu Kullanım Politikası, üniversitemizin öğrencileri, öğretim üyeleri, araştırmacıları, araştırma kuruluşlarındaki ve diğer birimlerdeki çalışanları olmak üzere tüm İstanbul Üniversitesi İnternet Ağı kullanıcılarını kapsamaktadır.

Sorumluluklar

İÜ/NET, kullanıcıların haberleşme gereksinimlerinin TCP/IP protokolü ile çalışan bir ağ üzerinden karşılandığı İstanbul Üniversitesinin sahip olduğu tüm servis ve altyapıya verilen isimdir. İÜ/NET Ağı; eğitim, bilimsel araştırma, teknik gelişme, teknoloji transferi, bilimsel, teknik ve kültürel bilginin yayılması gibi amaçlar için kurulmuştur. İÜ/NET, Türkiye Bilimsel ve Teknik Araştırma Kurumu'nun (TÜBİTAK) bir enstitüsü olan ULAKBİM tarafından, TÜBİTAK yönetmeliklerine uygun olarak işletilen "ULAKNET" üzerinden servis verir.

İstanbul Üniversitesi Bilgi Teknolojileri Ofisi, kurumsal güvenlik politikalarının hazırlanması, uygulanması, güncellenmesi, duyurulmasını sağlama ve takibinden sorumlu, İstanbul Üniversitesi Rektörlüğü'ne bağlı olarak çalışan merkezdir. Sistem ve ağ güvenliğinin ihlal edilmesi yasaktır, cezai ve hukuki mesuliyetle sonuçlanabilir. Bilgi Teknolojileri Ofisi bu tür ihlallerin söz konusu olduğu durumları inceler ve eğer bir suç oluştuğundan şüphe duyulursa yasa uygulayıcı ile işbirliği yapar.

Genel İlkeler

1. Genel kullanım ve mülkiyet:

1.1 Bilgi Teknolojileri Ofisi, kullanıcılara makul bir seviyede kişisel gizlilik sağlasa da, kullanıcılar, kuruma ait sistemler üzerinde yaratmış oldukları verilerin İstanbul Üniversitesi'nin mülkiyeti altında olduğunu bilmelidirler. İstanbul Üniversitesi internet ağının olası tehdit ve saldırılara karşı güvenliğini sağlayabilme gereksiniminden dolayı yönetim, kuruma ait sistemler üzerinde tutulan bilgilerin mahremiyetini garanti edemez.

1.2 Kurum çalışanları, kuruma ait bilgi sistemlerinin kişisel kullanımını makul seviyelerde tutmaktan sorumludurlar. Her bir birim kendi bilgi sistemlerinin kişisel kullanımı için gerekli kural ve talimatları oluşturmalıdır. Birimler böyle bir kural veya talimat oluşturmamışlar ve ortada bir belirsizlik durumu var ise kurumun koyduğu genel güvenlik politikaları geçerlidir.

1.3 Kullanıcılar önemli gördükleri ve paylaşıma açık olarak kullandıkları bilgileri mutlaka parolalar ile korumalıdırlar.

Güçlü parolalar oluşturma konusunda talimatlar için "Parola Kullanım Politikası"ndan faydalanılabilir.

1.4 Güvenliğin sağlanması ve ağın sağlıklı bir şekilde çalışmasının temini amacıyla, bu konuda İstanbul Üniversitesi'nde yetkili birim olan Bilgi Teknolojileri Ofisi, cihazları, sistemleri ve ağ trafiğini "Ağ Denetim Politikası" çerçevesi dahilinde istediği zaman gözlemleyebilir.

1.5 İstanbul Üniversitesi, "Ağ Denetim Politikası"na uyumun sağlanması amacıyla ağları ve sistemleri periyodik olarak denetleme hakkına sahiptir.

2. Güvenlik ve kişisel bilgiler:

2.1. Kurum çalışanları, gizli olsun veya olmasın kuruma ait bilgi sistemleri üzerinde yer alan tüm özel bilgilerin, yetkisiz kişiler tarafından erişimini önlemek için gerekli tüm adımları atmakla sorumludurlar.

2.2. Parolalar gizli tutulmalı ve hesaplar başkalarıyla paylaşılmamalıdır. Sahip oldukları sistemin yetkili kullanıcıları, parolaların ve hesapların güvenliğinden sorumludurlar. Sistem düzeyinde olan parolalar ayda bir, kullanıcı düzeyinde olan parolalar üç ayda bir düzenli olarak değiştirilmelidir. Bu konu ile ilgili uyulması gereken kurallar ve talimatlar "Parola Kullanım Politikası"nda belirtilmiştir.

2.3. Bütün masaüstü ve mobil bilgisayarlar, gözetim altında olmadıkları zamanlarda, on dakika veya daha az süre içerisinde otomatik devreye giren, parola korumalı bir ekran koruyucu ile veya kullanıcı oturumunu kapatarak (control + alt + delete veya Windows tuşu + L tuş kombinasyonları vasıtasıyla) güvenlik altına alınmalıdırlar. Bu konu ile ilgili uyulması gereken kurallar ve talimatlar "Bilgisayar Kullanım Politikası"nda belirtilmiştir.

2.4. Güçlü parolalar oluşturma konusunda talimatlara uymak için "Parola Kullanım Politikası" kullanılmalıdır.

2.5. Taşınabilir bilgisayarlar üzerinde tutulan bilgilerin özellikle saldırıya açık konumda olmaları sebebiyle, bunların güvenliğine özel ihtimam gösterilmelidir. BIOS ve işletim sistemi parolaları aktif hale getirilmelidir. Sadece gerekli olan bilgiler bu cihazlar üzerinde saklanmalıdır. Bu konu ile ilgili uyulması gereken kurallar ve talimatlar "Bilgisayar Kullanım Politikası"nda belirtilmiştir.

2.6. Kullanıcılar tarafından haber gruplarına İstanbul Üniversitesi e-posta adresi (…@istanbul.edu.tr, …@ogr.iu.edu.tr) kullanılarak gönderilen postalarda şöyle bir açıklama olmalıdır:

"Bu e-posta iş için gönderilenler hariç sadece yukarıda isimleri belirtilen kişiler arasında özel haberleşme amacını taşımaktadır. Size yanlışlıkla ulaşmışsa lütfen gönderen kişiyi bilgilendiriniz ve mesajı sisteminizden siliniz. İstanbul Üniversitesi bu mesajın içeriği ile ilgili olarak hiçbir hukuksal sorumluluğu kabul etmez.

This e-mail communication, except for business usage, is intended for the private use of the people named above. If you received this message in error, please immediately notify the sender and delete it from your system. Istanbul University does not accept legal responsibility for the contents of this message."

Bu konu ile ilgili uyulması gereken kurallar ve talimatlar "E-posta Kullanım Politikası"nda belirtilmiştir.

2.7. Bütün kullanıcılar bilgisayarlarında güncel bir tarama ve tespit yazılımı bulundurmak zorundadırlar. Bu konu ile ilgili uyulması gereken kurallar ve talimatlar "Antivirüs Kullanım Politikası"nda belirtilmiştir.

2.8. Kullanıcılar tanımadıkları kişilerden gelen ve virüs, solucan, Truva atı ve benzeri kötü amaçlı program kodları içerebilecek, e-posta eklerini açarken çok dikkatli olmalıdırlar. Bu konu ile ilgili ayrıntılı bilgiler, uyulması gereken kurallar ve talimatlar "E-posta Kullanım Politikası"nda belirtilmiştir.

2.9. "Bilgisayar Kullanım Politikası"nda belirtildiği üzere, bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek kuruma veya kişiye yönelik saldırılardan (spam gönderilmesi, phishing, elektronik bankacılık dolandırıcılıkları vb.) sistemin sahibi sorumludur.

3. Uygunsuz Kullanım:

Genel olarak aşağıdaki eylemler yasaklanmıştır. Herhangi bir kullanıcı kurumun kaynaklarını kullanarak hiçbir şart altında, Rektörlüğümüzün imzalamış olduğu "Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) Kullanım Politikası Sözleşmesi"ne aykırı ve herhangi bir yasadışı faaliyette bulunamaz.

Aşağıdaki faaliyetler hiçbir istisna olmadan kesinlikle yasaklanmıştır.

3.1. Ticari reklamlar ve haber duyuruları gibi istenmeyen mesajlar (spam iletiler) göndermek,

3.2. Başka bir kullanıcının posta sunucusunu veya posta adresini, o kullanıcının açık izni olmadan mesaj gönderme amacıyla kullanmak,

3.3. İÜ/NET üzerindeki hizmet kalitesini etkileyecek, bozacak, karışıklık yaratacak trafik düzenlemeleri oluşturmak,

3.4. İÜ/NET ağının kullanım amaçlarına uygunsuz, müstehcen, rahatsız edici materyalin üretilmesi ve dağıtımı

3.5. Gerçek dışı, sıkıntı, rahatsızlık verici, gereksiz korku yaratacak materyalin üretimi ve dağıtımı,
3.6. İftira ve karalama mahiyetinde materyalin üretimi ve dağıtımı,
3.7. Başkalarının fikri haklarını (copyright) ihlal edici mahiyetteki materyallerin, (yazı, makale, kitap, film, müzik eserleri dahil ancak bunlarla sınırlı kalmamak üzere) izinsiz kopyalanması, dijital hale dönüştürülmesi, lisanssız kullanımı ve dağıtımı,
3.8. Bir kullanıcının yetkisi olmadığı halde sunuculara erişmeye çalışarak ağ güvenliğini ihlal etmesi veya çeşitli yöntemlerle (ağ veya port tarama, paket sniffing, IP spoofing, ping seli ve hizmet durdurma dahil ancak bunlarla sınırlı kalmamak üzere) ağ iletişimini bozmaya çalışması,
3.9. İÜ/NET üzerinden ulusal veya uluslararası hizmetlerin (veritabanları, elektronik dergiler vb.) kasıtlı olarak yetkisiz kullanımı,
3.10. Kasıtlı olarak başkalarının verilerini veya çalışmalarını bozmak veya tahrip etmek,
3.11. İÜ/NET üzerinde, başkalarına kullanım olanağı vermeyecek oranda trafik yaratmak (film, müzik ve lisanssız yazılımları download veya upload etmek, internet üzerinden oyun oynamak vb.)
3.12. İÜ/NET'in çalışmasını engellediği, gereksiz trafik yarattığı ve ağın hizmet amacı dışında kullanımına sebep olduğu için, Bilgi Teknolojileri Ofisi tarafından ilan edilerek kullanımı yasaklanan dosya paylaşım (Torrent ve türevleri, edonkey, emule, Direct Connect, Kazaa, Limeware, BearShare, RapidShare dahil ancak bunlarla sınırlı kalmamak üzere) yazılımlarını ısrarla kullanmak,

Hariç Durumlar

Ağ ve sistem yöneticileri; yaptıkları işin gerektirdiği sorumluluklar neticesinde, ağ ve sistemlerin çalışmasını kesintiye uğratacak, engelleyecek veya zarar verecek bir faaliyetin tespiti sonrasında ağı tarayabilir, bu zararı veren kullanıcının ağa olan erişimini kesebilir, şüpheli gördüğü kullanıcının e-posta ve internet trafiğini inceleme altına alabilir. Ağ ve sistem yöneticileri gerçekleştirdikleri bu uygulamaların raporlarını, bağlı oldukları bir üst mevkiye bildirmek zorundadırlar.

Özel Durumlar

Müstehcen, rahatsız edici materyalin üretilmesi ve dağıtılmasının yasak olduğu durumlarda, akademik çalışma ve araştırma amaçlı olanlar hariç tutulur.

Uyum ve Yaptırımlar

1. İÜ/NET'in yukarıda belirtilmiş olan "Genel İlkelere" aykırı faaliyetler dahilinde kullanılması durumunda İstanbul Üniversitesi makamları gerçekleştirilen eylemin; yoğunluğuna, kaynaklara veya kişi / kurumlara verilen zararın boyutuna ve tekrarına göre aşağıdaki işlemlerin bir ya da birden fazla maddesini, sıra ile ya da sırasız uygulayabilir;

1.1. Kullanıcı sözlü ve/veya yazılı olarak uyarılır,
1.2. Kullanıcıya tahsis edilmiş İÜ/NET kaynakları, sınırlı veya sınırsız süre ile kapatılabilir,
1.3. Üniversite bünyesindeki akademik/idari soruşturma mekanizmaları harekete geçirilebilir,
1.4. Adli yargı mekanizmaları harekete geçirilebilir.

2. Kullanıcı, İstanbul Üniversitesi Bilgi Teknolojileri Ofisi'nin, sektörde meydana gelebilecek yasal gelişmeleri göz önünde tutarak bu Kullanım Politikası'nı değiştirebileceğinden haberdardır ve bunu açıkça kabul eder.
3. İstanbul Üniversitesi Bilgi Teknolojileri Ofisi, "Ağ Kullanım Politikası"nı istediği zaman değiştirme hakkına sahip olup, bu değişikliklerle beraber politikanın son halinin duyurulmasını sağlamakla sorumludur.
4. "Uygunsuz Kullanım" başlığı altında geçen çeşitli fiilleri gerçekleştiren kullanıcılar ayrıca; 5846 sayılı Fikir ve Sanat Eserleri Kanunu, Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlıklı bölümü ve Türk Ticaret Kanunu'nun ilgili maddeleri uyarınca, yasalar karşısında suçlu duruma düşebileceklerdir.

Tanımlar

BIOS (Basic Input Output System): İşlemci tarafından ilk çalıştırılan yazılım olan BIOS, işlemciyi anakart üzerinde bulunan diğer temel bileşenlerle tanıştırır ve BIOS kodunun işi bittiğinde işlemcinin hangi yazılımı çalıştıracağını söyler. Temel bir kural olarak BIOS, açılış aygıtı (bu aygıt disket, CD-ROM, DVD veya sabit disk olabilir) üzerindeki açılış bölümüne (boot sector) erişir. Açılış bölümü üzerinde bulunan bir çeşit açılış yöneticisi çalışır ve bilgisayarın temel işletim sistemini (Windows veya Linux gibi) yüklemeye başlar.
Virüs: Virüsler**,** başka programların içine kendisini kopyalayarak bulaşan bilgisayar programlarıdır.
Solucan: Solucanlar, virüslerle benzerlik taşısa da bir program veya taşıyıcıya ihtiyaçları olmayan, kendi kendilerini kopyalayabilme kabiliyetine sahip olan ve yayılmak için bilgisayarlar arasındaki bağlantıları kullanan programlardır.
Truva atı: Truva atları, zararsız ve gerekli gibi görünen fakat çalıştırıldığında kullanıcının haberi olmadan saldırganların sisteme uzaktan erişim sağlamasına, sisteme arka kapı yerleştirmesine, klavye hareketlerinin kayıt edilmesini, hizmet durdurma saldırılarına ve antivirüs veya yazılım güvenlik duvarlarının devre dışı kalmasını sağlayabilen programlardır. Virüs veya solucanların aksine Truva atları kendi başlarına yayılamazlar.
Spam: Spam, istenmeyen, reklam veya ticari amaçlı e-postalardır.
Phishing: Phishing, içeriği alıcıyı yanlış ve ilgi çekici ibarelerle saldırganın sitesine yönlendirme amaçlı, e-postalar vasıtasıyla yürütülen bir saldırı şeklidir.
Paket sniffing: Ağ üzerinde gidip gelen tüm veri paketlerinin, çeşitli araçlar yardımıyla toplanması işlemine denir.
IP Spoofing: Ağ üzerinde iletilen verileri çalmak için bilgisayarlar ve ağ cihazları üzerinde çeşitli işlemler yapılıp, veri paketlerini yanlış hedeflere gönderilmesini sağlamak amacıyla İnternet Protokolünde değerlerin olduğundan farklı olarak gösterilmesi demektir.

Ping Seli: Hedef sisteme büyük boyutta ve sıklıkta ping paketleri göndererek tampon belleğini doldurup sonrasında sistemin cevap veremez hale gelmesine ve çökmesine sebep olan saldırı türüdür.

Hizmet Durdurma (Denial of Service): Ağ ve sistemlerin normal işlemlerini ve normal iletişimini, bant genişliğini tüketmek, kaynaklarını sömürmek ve programlardaki kusurları kullanmak suretiyle kesintiye uğratmak için yapılan saldırılardır.
Download: Download, uzak bir sistemden dosyaların lokalde bulunan sisteme indirilmesi işlemine denir.
Upload: Upload, dosyaların lokalde bulunan bir sistemden uzaktaki bir sisteme gönderilmesi işlemine denir.

Ekler

Geçmiş

Değiştirilme Tarihi:	15.01.2007
Değiştirilen hususlar:	Değişiklik mevcut değildir.
Yerini aldığı sürüm:	En son sürümdür.

Sıkça Sorulan Sorular

İrtibat

Konu	İlgili Personel	Telefon	e-posta
Ağ sistemleri	Hakan Aysal	10058	haysal@iu.edu.tr
Sunucu Sistemleri	Levent İldeniz	14044	leventildeniz@iu.edu.tr
Kablosuz İletişim	Kürşat Gezginci	11562	kgezginci@iu.edu.tr

Dizin

9. TARTIŞMA VE SONUÇ

Bu tez çalışmasında, güvenlik politikalarının uygulanabileceği ve kullanılabileceği fiziksel çalışma ortamlarını incelemek amacıyla, kurumsal ağ altyapılarına en iyi örnek teşkil eden üniversite altyapıları ele alınmıştır. Burada yerel ve geniş alan ağ altyapıları genel tanımları ile beraber, kullanılan teknolojiler ve cihazlar çok fazla ayrıntıya girmeden incelenmiştir.

Güvenlik kavramı ve bileşenleri ortaya konulmuş ve yazılı kurallar olmadan tam bir güvenlik anlayışının oturtulamayacağı ve etkinliğini koruyamayacağı fikri ile bir sonraki adımlara geçilmiştir. Tehditlerin belirlenmesi, bunlara karşı önlem alabilmek adına geliştirilmiş güvenlik araçlarının öğrenilmesi ve bu güvenlik araçlarının politikalarla desteklenmesi olarak üç aşama ile belirtilen adımlar takip edilmiştir.

Güvenlik konusunda karşılaşılabilecek riskleri en aza indirmek adına, tehditler her yönüyle ve örnekleriyle tanımlanmıştır. Tehditlerin, gelişen teknolojiyle ve değişen uygulamalar ile geldiği nokta belirtilmiştir. Güvenlik politikaları oluştururken bu değişimin göz ardı edilmemesi gereği vurgulanmıştır.

Bu değişen ve gelişen tehditlere karşı alınabilecek önlemler ve sektörün geliştirdiği hem ticari hem de açık kaynak kodlu güvenlik araçları ve teknolojiler tanımları ve örnekleriyle incelenmiştir. Daha sonra güvenlik araçlarının geçirdiği evrim ve sektörün bu yöndeki geleceğe dönük eğilimleri ve politikalarla olan ilişkisi ortaya konulmuştur.

Tüm bu anlatılan ihtiyaçlar ve bunların giderilmesine yönelik teknik çözümler belli bir yere kadar güvenliği sağlayabilecektir. Bu nedenle her kurum için olduğu gibi, üniversiteler için de büyük öneme sahip kurallar dizisi olan güvenlik politikaları oluşturmak ve bunu bir standarda oturtarak genele yaymak, ideal olan uygulamadır. Bu çalışmada, bir Yüksek öğretim kurumunda politika oluşturma konusunda bir sistematik

belirlemek için hem ulusal hem de uluslararası birçok yaklaşım ve kaynak referans alınmıştır.

Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM), Türkiye'deki üniversiteler için referans oluşturması amacıyla, bir "Kullanım Politikası Sözleşmesi" hazırlamıştır. Ayrıca, Ege Üniversitesi, ODTÜ, Hacettepe Üniversitesi, Bilkent Üniversitesi ve İTÜ, kurumsal güvenlik politikaları ve bunlara destek olacak kullanım talimatlarını içeren belgelerini başarıyla ortaya koymuşlardır.

Dünya geneline baktığımızda da güvenlik politikaları ile uygulanmasının düzenli yapıldığını görmekteyiz. Örneğin; Cornell Üniversitesi "Politikaların kaleme alınması ve yayınlanması" başlıklı bir politika geliştirme yöntemi tanımlamıştır. Minnesota Üniversitesi, politika geliştirme, dağıtma ve takip süreci hakkında bilgiler içeren bir "Politika Yazma Rehberi" hazırlamıştır. Üniversite ve Yüksekokul Politika Yöneticileri Birliği (Association of College and University Policy Administrators: ACUPA) bir "en iyi uygulamalar ile politika oluşturma yöntemi" geliştirmişlerdir. SANS (SysAdmin, Audit, Network, Security) Enstitüsü ve Carnegie Mellon Üniversitesi güvenlik ve güvenlik politikaları konusunda kapsamlı çalışmalar ve yayınlar hazırlamışlardır.

TS ISO/IEC 17799 ve TS ISO/IEC 27001 standartları, kurumsal düzeyde bilgi güvenliğini başlatan, gerçekleştiren ve sürekliliğini sağlayan bilgi teknolojileri uzmanlarının kullanımı için, bilgi güvenlik yönetimi ile ilgili tavsiyeleri kapsamaktadır. ISO17799 da genel olarak, en düşük veya temel güvenlik gereksinimlerini ve risklere karşı dayanma gücünü anlayabilmek için idari ve teknik ortama ait bir risk değerlendirme işlemi kullanılır. Bu risk analizi, tehditlerin ve bunlara karşı alınabilecek tedbirlerin tanımlanması ve sonrasında kendine özel hazırlanmış politika ifadelerinin oluşturulmasını mümkün kılar.

Tüm bu öneriler ve rehber çalışmaların ışığında ve bunları kapsayacak şekilde bir politika oluşturma, geliştirme ve uygulama süreci ortaya konulmuştur.

Bu süreç aşağıdaki adımlardan meydana gelmiştir:

- **Hazırlık**

    - Kurum değer ve varlıklarının belirlenmesi
        1. Yazılım ve donanım
        2. Yazılı kaynaklar
        3. İnsan kaynakları
    - Ekibin belirlenmesi
    - Veri akış analizi çalışması
    - Tehditler ve karşı tedbirlerin ortaya konulması
- **Oluşturma**
    - Ortak bir biçim ortaya konulması
    - Taslak oluşturulması
    - Duyurulması ve dağıtımı
    - Güvenlik bilinçlendirme programı
- **Bakım**
    - Taleplerin değerlendirilmesi ve gözden geçirme
    - Uyumun sağlanması ve takibi

Bu süreci meydana getiren adımlar, ayrıntıları ve örnekleriyle açıklanmıştır. Ortaya konulan süreç takip edilerek, İstanbul Üniversitesi'nde uygulanacak güvenlik politikasının hazırlık çalışmalarına başlanmıştır. Elde edilen bilgiler, örnekler ve belirlenen sistematik doğrultusunda, İstanbul Üniversitesi güvenlik politikası şablonu hazırlanmıştır. Hazırlanan şablon daha sonra, "İstanbul Üniversitesi Ağ Kullanım Politikası" örneğiyle daha belirgin bir hale getirilmiştir.

Bundan sonra, bilgisayar, internet, parola, antivirüs, öğrenci laboratuvar ve yurt kullanımları örnek olmak üzere, ihtiyaç duyulan her konuda politika hazırlama hususunda bu şablon kullanılabilecektir.

Bu çalışmada eksik görülebilecek bir nokta; hazırlanan güvenlik politikasının onaylanıp yürürlüğe konamamasından ötürü, etkinliğinin ve takibinin ölçülememiş olmasıdır. Şekil 7.3.2.1. de ortaya konulan gözlem süreci, tezin hazırlanması döneminde daha önce belirtilen sebeple ele alınamamış ve rakamsal sonuçlar elde edilememiştir. Bu çalışmanın devamında belirlenecek bir zaman aralığında, kurumsal güvenlik politikası, buna destek olacak diğer politikalar ve talimatnamelerin kurum üzerindeki etkisi,

kullanıcılara düzenlenecek anketler ve güvenlik araçlarından elde edilecek bulgularla, çok daha verimli bir şekilde takip edilebilecektir.

Ortaya çıkarılan bu çalışmanın canlılığını ve etkinliğini koruyabilmesi için, İstanbul Üniversitesi Ağ Kullanım Politikası, yönetimin de desteğiyle teknolojideki gelişmeler ve kurumun ihtiyaçları doğrultusunda belli zamanlarda güncellenmelidir.

KAYNAKLAR

1. Tanenbaum Andrew S., 2003, *Computer Networks 4th Ed.*, Prentice Hall, New Jersey, s.8, 978-0130661029
2. Uçan Osman N. ve diğ., 2003, *Bilgisayar Ağları ve Haberleşme Teknikleri*, İstanbul Üniversitesi, İstanbul, s.5, 975-404-965-6
3. Slone John P., 1998, *Handbook of Local Area Networks*, CRC Press, Indianapolis, 0849399483
4. International Organization for Standardization (ISO), *Open Systems Interconnection -- Basic Reference Model: The Basic Model*, http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip
5. Türk Standartları Enstitüsü, *Bilgi Teknolojisi-Açık Sistemler Ara Bağlantısı-Temel Referans Model-Bölüm 1:Temel Model*, [çevrimiçi], https://www.tse.org.tr/turkish/abone/StandardDetay.asp?STDNO=31984&sira=0 , [Ziyaret Tarihi: 9 Ağustos 2006]
6. Postel J. ve Reynolds J., 1985, Network Working Group Request for Comments: 959, *File Transfer Protocol (FTP)*, http://www.ietf.org/rfc/rfc0959.txt
7. Klensin J., 2001, Network Working Group Request for Comments: 2821, *Simple Mail Transfer Protocol (SMTP)*, http://www.ietf.org/rfc/rfc2821.txt
8. Fielding R. ve diğ., 1999, Network Working Group Request for Comments: 2616, *Hypertext Transfer Protocol -- HTTP/1.1*, http://www.ietf.org/rfc/rfc2616.txt
9. Postel J. ve Reynolds J., 1983, Network Working Group Request for Comments: 854, *Telnet Protocol Specification,* http://www.ietf.org/rfc/rfc0854.txt
10. Sollins K., 1992, Network Working Group Request for Comments: 1350, *The TFTP Protocol (Revision 2)*, http://www.ietf.org/rfc/rfc1350.txt
11. *ASCII Table and Description*, [çevrimiçi], http://www.asciitable.com/, [Ziyaret Tarihi: 9 Ağustos 2006]
12. *The Reference Website for MPEG*, [çevrimiçi], http://www.mpeg.org/MPEG/index.html, [Ziyaret Tarihi: 9 Ağustos 2006]
13. *JPEG Homepage*, [çevrimiçi], http://www.jpeg.org/jpeg/index.html, [Ziyaret Tarihi: 9 Ağustos 2006]
14. Comer D., 2000, *Internetworking TCP/IP Vol I: Principles, Protocols and Architecture Fourth Edition*, Prentice Hall Publishing, New Jersey, s.183, 0-13-018380-6
15. Mockapetris P., 1987, Network Working Group Request for Comments: 1035, *Domain Names - Implementation And Specification*, http://www.ietf.org/rfc/rfc1035.txt
16. Yeong W. ve diğ., 1995, Network Working Group Request for Comments:1777, *Lightweight Directory Access Protocol (LDAP)*, http://www.ietf.org/rfc/rfc1777.txt

17. Mir Nader F., 2006, *Computer and Communication Networks*, Chapter 8.1. Transport Layer, Prentice Hall Publishing, New Jersey, 978-0-13-174799-9
18. Defense Advanced Research Projects Agency (DARPA), 1981, Transmission *Control Protocol Specification*, http://www.ietf.org/rfc/rfc0793.txt
19. Postel J., 1980, Network Working Group Request for Comments: 768, *User Datagram Protocol*, http://www.ietf.org/rfc/rfc0768.txt
20. Prasad K.V., 2003, *Principles of Digital Communication Systems and Computer Networks*, Chapter 16: ISO/OSI Protocol Architecture, Charles River Media, Massachusetts, 1584503297
21. Naugle M., 1998, *Illustrated TCP/IP*, Chapter 20: IP Overview, John Wiley & Sons, 978-0471196563
22. Defense Advanced Research Projects Agency (DARPA), 1981, *Internet Protocol*, http://www.ietf.org/rfc/rfc0791.txt
23. Zacker C., 2002, *Microsoft Windows 2000 Network Infrastructure Administration: Second Edition,* Chapter 4. NetWare Networking with Windows 2000, Microsoft Pres, Washington, 1-57231-904-6
24. Barnes D. ve Sakandar B., 2004, *Cisco LAN Switching Fundamentals*, Chapter I: LAN Switching Foundation Technologies, Cisco Press, Indianapolis, 1-58705-089-7
25. Goleniewski L. ve Jarrett Kitty W., 2006, *Telecommunications Essentials, Second Edition: The Complete Global Source*, Pearson Education, Boston, 0-321-42761-8
26. Institute of Electrical and Electronics Engineers, *IEEE 802.3 CSMA/CD (ETHERNET)*, http://grouper.ieee.org/groups/802/3/, [Ziyaret Tarihi: 10 Ağustos 2006]
27. Norris M., 2003, *Gigabit Ethernet: Technology and Applications*, Chapter 2: Ethernet-The Story So Far, Artech House, Norwood, 1580535054
28. Castelli Matthew J., 2004, *LAN Switching first-step*, Chapter 3. Local-Area Networking Introduction, Cisco Press, Indianapolis, 1-58720-100-3
29. Casad J., 2004, *Sams Teach Yourself TCP/IP in 24 Hours, Third Edition*, *Part III: Networking with TCP/IP*, Hour 9. Network Hardware, Sams Publishing, Indianapolis, 0-672-32565-9
30. Null L. ve Lobur J., 2003, *The Essentials of Computer Organization and Architecture,* Chapter 11: Network Organization and Architecture, Jones and Bartlett Publishers, London, 0-7637-2649-4
31. Axelson J., 2003, *Embedded Ethernet and Internet Complete*, Lakeview Research, Madison, s.89-90, 978-1931448000
32. Çevirenler: Çakır Ali Y. ve diğ., 2005, *Bilişim Teknolojilerinin Temelleri I: PC Donanım ve Yazılım Yardımcı Kitabı*, Sistem Yayıncılık, İstanbul, s.603, 975-322-364-1
33. Cisco Systems, Inc., 2004, *Internetworking Technologies Handbook, Fourth Edition*, Cisco Press, Indianapolis, 1-58705-119-2
34. Alwayn V., 2004*, Optical Network Design and Implementation*, Chapter 2. Time-Division Multiplexing, Cisco Press, Indianapolis, 1-58705-105-2
35. International Engineering Consortium, *Synchronous Digital Hierarchy (SDH)*, http://www.iec.org/online/tutorials/acrobat/sdh.pdf,
36. Oppenheimer P., 2004, *Top-Down Network Design, Second Edition*, Chapter 11. Selecting Technologies and Devices for Enterprise Networks, Cisco Press, Indianapolis, 1-58705-152-4

37. Türk Telekom, *Frame Relay*, [çevrimiçi], http://www.turktelekom.com.tr/webtech/default.asp?sayfa_id=63, [Ziyaret Tarihi: 13 Ağustos 2006]
38. Bass M. ve Stryland Eric W. Van, 2002, *Fiber Optics Handbook, Fiber, Devices, and Systems for Optical Communications*, McGraw-Hill, New York, 0-07-138623-8
39. Güncel Türkçe Sözlük, [çevrimiçi], www.tdk.gov.tr, [Ziyaret Tarihi: 13 Ağustos 2006]
40. Guel Michele D., 2001, *A Short Primer For Developing Security Policies*, The SANS Institute, http://www.sans.org/resources/policies/Policy_Primer.pdf [Ziyaret Tarihi: 14 Ağustos 2006]
41. Schneier B., 2000, *Computer Security: Will We Ever Learn?, Crypto-Gram Newsletter*, http://www.schneier.com/crypto-gram-0005.html, [Ziyaret Tarihi: 18 Ağustos 2006]
42. Bejtlich R., 2004, *The Tao of Network Security Monitoring Beyond Intrusion Detection*, Addison Wesley, Boston, Chapter 1. The Security Process: What is Risk?, 0-321-24677-2,
43. Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003, *Bilişim Güvenliği v1.1,* http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf [Ziyaret Tarihi: 20 Ağustos 2006]
44. Stoneburner G. ve Goguen A., 2001, *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Gaithersburg, s.8, 800-30
45. Karabacak B., 2006, *Bilgi Güvenliği Risk Yönetimi*, http://www.uekae.tubitak.gov.tr/sunum/2_Bilgi_Guvenligi_Risk_Yonetimi.pdf [Ziyaret Tarihi: 25 Ağustos 2006]
46. Filiz, A., 2005, OHSAS 18001 İş Sağlığı ve Güvenliği Yönetim Sistemlerinde Risk Analizleri Eğitim Notları, *Maltepe Üniv. e-KOBİ Dönüşüm Uzmanlık Sertifika Programı*
47. Bilişim Teknolojilerinde Risk Yönetimi, *TBD Kamu-BİB Kamu Bilişim Platformu VIII*, 27 Mart 2006, http://www.kamubib.tbd.org.tr/dokumanlar/cg2a2.doc [Ziyaret Tarihi: 25 Ağustos 2006]
48. Tipton H. ve Krause M., 1998, *Handbook of Information Security Management*, CRC Pres LLC, Florida, Chapter 3.1.1, 0849399475
49. Cole E. ve Krutz R., 2005, *Network Security Bible*, Wiley Publishing, Indianapolis, s. 35-40, 0-7645-7397-7
50. TBD Kamu-BİB, 2006, *Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0*, Türkiye Bilişim Derneği Yayınları, http://www.kamubib.tbd.org.tr/dokumanlar/BG2S.doc [Ziyaret Tarihi: 25 Ağustos 2006]
51. İnce F., 2006, Bilgi Güvenliği*, Türkiye Bilişim Ansiklopedisi*, Papatya Yayınları, İstanbul, s.162, 975-6797-38-X
52. Çağlayan M. Ufuk, 2003, Bilgi Güvenliği: Dünyadaki Eğilimler, *ULAKNET Sistem Yönetimi Konferansı-Güvenlik,* 3-4 Ekim 2003 Ankara, http://www.e-imza.gen.tr/templates/resimler/File/sunumlar/Bilgi_Guvenligi_3_Ekim_2003_Ufuk_Caglayan.ppt [Ziyaret Tarihi: 20 Ağustos 2006]

53. ISO/IEC FDIS 17799: 2005-02-11, *Information techniques, Security techniques, Code of practice for information security management (2nd edition)*, 2005-02-11, s.9
54. Eren Ş., 2006, Yazılımda Güvenilirlik, *Türkiye Bilişim Ansiklopedisi*, Papatya Yayıncılık, İstanbul, s.992, 975-6797-38-X
55. Labris Teknoloji, *Yazılım Güvenliği Yaklaşımı*, http://www.labristeknoloji.com/dosyalar/yazilim guvenlik denetimi ve risk analizi.doc, [Ziyaret Tarihi: 28 Ağustos 2006]
56. Hendrickx M., 2003, *XSS: Cross site scripting, detection and prevention*, Scanit Middle East, s.2, https://www.securinfos.info/english/security-whitepapers-hacking-tutorials/xss.pdf
57. Endler D., 2002, *The Cross Site Scripting (XSS) FAQ*, [çevrimiçi] http://www.cgisecurity.com/articles/xss-faq.shtml [Ziyaret Tarihi: 29 Ağustos 2006]
58. Balaban M., 2001, *Buffer Overflow`lar hakkında,* [çevrimiçi] http://www.olympos.org/article/articleview/183/1/10/buffer_overflowlar_hakkinda [Ziyaret Tarihi: 29 Ağustos 2006]
59. Ristick I., 2005, *Apache Security*, O'Reilly, Sebastopol, Section 10.6., 0-596-00724-8
60. Secunia Research, 08.12.2004, *Multiple Browsers Window Injection Vulnerability*, [çevrimiçi], http://secunia.com/secunia_research/2004-13/advisory/ [Ziyaret Tarihi: 27 Ağustos 2006]
61. Infosecure, 2005, *Türkiye'de En Sık Karşılaşılan Güvenlik Açıkları*, http://www.infosecurenet.com/10_guvenlik_acigi_2004.pdf [Ziyaret Tarihi: 29 Ağustos 2006]
62. SecuriTeam, 26 May 2002, *SQL Injection Walkthrough*, [çevrimiçi], http://www.securiteam.com/securityreviews/5DP0N1P76E.html [Ziyaret Tarihi: 30 Ağustos 2006]
63. Kevin Lam K. ve LeBlanc D., 2004, *Assessing Network Security*, Microsoft Press, Washington, s.296, 0-7356-2033-4
64. The Open Web Application Security Project (OWASP), 2004, *Improper Error Handling*, [çevrimiçi], http://www.owasp.org/index.php/Improper_Error_Handling [Ziyaret Tarihi: 30 Ağustos 2006]
65. The Open Web Application Security Project (OWASP), 2004, *The Ten Most Critical Web Application Security Vulnerabilities*, [çevrimiçi], http://www.owasp.org/images/c/ce/OWASP_Top_Ten_2004.doc
66. Levi A., 2006, *Ağ Güvenliği*, *Türkiye Bilişim Ansiklopedisi*, Papatya Yayınları, İstanbul, s.44, 975-6797-38-X
67. Allen J., 2001, CERT System and Network Security Practices, *In Proceedings of the 5th National Colloquium for Information Systems Security Education (NCISSE)*, Fairfax, VA, 2001
68. *Common Vulnerabilities and Exposures (CVE)*, [çevrimiçi], http://cve.mitre.org/, [Ziyaret Tarihi: 30 Ekim 2006]
69. United States Computer Emergency Readiness Team (US-CERT), *Vulnerability Notes Database*, [çevrimiçi], http://www.kb.cert.org/vuls, [Ziyaret Tarihi: 30 Ağustos 2006]
70. Dayıoğlu B., 2002, Ağ ve İşletim Sistemi Güvenliği, *TBD BIMY-9 Bildiriler Kitabı*

71. Internet Usage Statistics - *The Big Picture*, [çevrimiçi], http://www.internetworldstats.com/stats.htm [Ziyaret Tarihi: 30 Ağustos 2006]
72. Devlet İstatistik Enstitüsü, 2005, *Hanehalkı Bilişim Teknolojileri Kullanımı Araştırması Sonuçları*, DIE Haber Bülteni, 16 Kasım 2005, Sayı 179.
73. Tzu S., 2005, *Savaş Sanatı*, Anahtar Kitaplar, İstanbul, 975-7787-03-5
74. Maiwald E., 2001, *Network Security: A Beginner's Guide*, Osborne/McGraw-Hill, New York, 0072133244, s.81
75. E-Crime Watch Survey – Survey Results, Carnegie Mellon University Software Engineering Institute's CERT® Coordination Center, 2004, 2005, 2006
76. SearchSecurity.com Definitions, *Insider Threat*, [çevrimiçi], http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci1117699,00.html, [Ziyaret Tarihi: 30 Ağustos 2006]
77. Bastien G. ve Degu Christian A., 2004, *CCSP SECUR Exam Certification Guide*, Cisco Press, Indianapolis, s.31, 1-58720-072-4
78. Gregg M., 2006, *Certified Ethical Exam Prep*, Que Publishing, Indianapolis, 0-7897-3531-8
79. Whitaker A. ve Newman Daniel P., 2005, *Penetration Testing and Cisco Network Defense*, Cisco Press, Indianapolis, 1587052083
80. Dirican Can O., 2005, *TCP/IP ve Güvenliği*, Açık Akademi Yayınları, İstanbul, s.422, 975-98099-1-5
81. Nmap Reference Guide (Man Page), *Network exploration tool and security / port scanner*, [çevrimiçi], http://insecure.org/nmap/man/, [Ziyaret Tarihi: 1 Eylül 2006]
82. Imperva, Application Defense Center, *Brute Force Attack*, [çevrimiçi], http://www.imperva.com/application_defense_center/glossary/brute_force.html [Ziyaret Tarihi: 1 Eylül 2006]
83. Web Application Security Consortium, *Threat Classification, Brute Force*, [çevrimiçi], http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.tr.doc [Ziyaret Tarihi: 1 Eylül 2006]
84. Openwall Project, *John the Ripper Pro password cracker*, [çevrimiçi], http://www.openwall.com/john/pro/, [Ziyaret Tarihi: 2 Eylül 2006]
85. Cisco Network Academy Program, 2006, *Fundementals of Network Security v1.2*, Access Attack Examples, Module 1
86. VulnWatch, Vulnerability Disclosure Mailing List, *Netcat*, [çevrimiçi], http://www.vulnwatch.org/netcat/, [Ziyaret Tarihi: 1 Eylül 2006]
87. Bruno A., 2004, *CCDA Self-Study CCDA Exam Certification Guide Second Edition*, Cisco Press, Indianapolis, s.387, 1-58720-076-7
88. Efe A., 2006, *Yeni Nesil İnternet Protokolü'ne (Ipv6) Geçişle Birlikte İnternet Saldırılarının Geleceğine Yönelik Beklentiler*, Akademik Bilişim'06, 9-11 Şubat 2006, Pamukkale Üniversitesi, Denizli
89. Öztürkci H., 12.11.2004, *Windows 2000'de IPSec*, [çevrimiçi], http://www.turkmcse.com/makale/makale.php?id=1&makale_id=53 , [Ziyaret Tarihi: 7 Eylül 2006]
90. Mitnick Kevin D., 2002, *The Art Of Deception, Controlling the Human Element of Security*, John Wiley & Sons, Indianapolis, 0471237124
91. Klevinsky T.J.ve Laliberte S., 2002, *Hack I.T.: Security Through Penetration Testing*, Addison Wesley, Boston, Chapter 21.3, 0-201-71956-8

92. Atabey O., 2006, Temel Saldırı Teknikleri, [çevrimiçi], http://www.tcpsecurity.com/doc/genel/temelsaldiriteknikleri.html , [Ziyaret Tarihi: 11 Eylül 2006]
93. Mirkovic J.ve Dietrich S., 2004, *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall PTR, New Jersey, Chapter 4, 0-13-147573-8
94. The WildList Organization International, [çevrimiçi], www.wildlist.org, [Ziyaret Tarihi: 12 Eylül 2006]
95. Erbschloe M., 2005, *Trojans, Worms, and Spyware, A Computer Security Professional's Guide to Malicious Code*, Elsevier Butterworth–Heinemann, Oxford, s.17-18, 0-7506-7848-8
96. Cohen F., 1985, *Computer Viruses*, PhD thesis, University of Southern California
97. Szor P., 2005, *The Art of Computer Virus Research and Defense*, Addison Wesley Professional, NewJersey, Chapter 3. Malicious Code Environments, 0-321-30454-3
98. Ludwig Mark A., 1996, *The Little Black Book of Computer Viruses*, American Eagle, Arizona, s.16, 0-929408-02-0
99. Grimes Roger A., 2001, *Malicious Mobile Code: Virus Protection for Windows*, O'Reilly, Sebastapol, Chapter 5.3.1. Word Macros, 1-56592-682-X
100. Networks Associates Technology, Inc., *Virus Hoax Listings*, [çevrimiçi], http://vil.mcafee.com/hoax.asp, [Ziyaret Tarihi: 12 Eylül 2006]
101. Trend Micro, *Scams and Hoaxes*, [çevrimiçi], http://www.trendmicro.com/vinfo/hoaxes/hoax.asp, [Ziyaret Tarihi: 12 Eylül 2006]
102. *Trojan/Backdoors List*, ONCTek LLC, [çevrimiçi], http://www.onctek.com/trojanports.html, [Ziyaret Tarihi: 12 Eylül 2006]
103. Oldfield P., 2004, *Viruses and Spam*, Sophos Plc., s.7, 0-9538336-1-5
104. Skoudis E. ve Zeltser L., 2003, *Malware: Fighting Malicious Code*, Prentice Hall PTR, NewJersey, Chapter 3. Worms, 0-13-101405-6
105. Wang W., 2003, *Steal This Computer Book 3: What They Won't Tell You About the Internet*, No Starch Press, San Francisco,Chapter 7: Viruses and Worms, 1593270003
106. Stephenson P., 1999, *Investigating Computer-Related Crime, A Handbook For Corporate Investigators*, CRC Press, Florida, s.52, 0-8493-2218-9
107. Koltuksuz A., 2006, Virüsler, *Türkiye Bilişim Ansiklopedisi*, Papatya Yayınları, İstanbul, s.912, 975-6797-38-X,
108. Spyware List, [çevrimiçi], http://home.earthlink.net/~doniteli/index73.htm#list, [Ziyaret Tarihi: 13 Eylül 2006]
109. Walker A., 2005, *Absolute Beginner's Guide To: Security, Spam, Spyware & Viruses*, Que Publishing, Indianapolis, Chapter 2. Spyware, 0-7897-3459-1
110. SpywareGuide, Spyware List, [çevrimiçi], http://www.spywareguide.com/product_list_category.php?category_id=5, [Ziyaret Tarihi: 13 Eylül 2006]
111. Adware List, [çevrimiçi], http://securityresponse.symantec.com/avcenter/venc/auto/index/indexA.html, [Ziyaret Tarihi: 13 Eylül 2006]

112. AfterDawn Ltd., 30 September 2002, *Kazaa, BearShare, Morpheus and LimeWire are stealing from websites*, [çevrimiçi], http://www.afterdawn.com/news/archive/3390.cfm [Ziyaret Tarihi: 13 Eylül 2006]
113. Spyware Watch (UK), *What is stealware*, [çevrimiçi], http://www.spyware.co.uk/stealware.shtml [Ziyaret Tarihi: 13 Eylül 2006]
114. Karadeniz T., 15.02.2005, *Türkiye' de Phishing*, Olympos Security Güvenlik Portalı, [çevrimiçi], http://www.olympos.org/article/articleview/1403/l/2/ [Ziyaret Tarihi: 13 Eylül 2006]
115. Gralla P., 2006, *How Personal & Internet Security Work*, Que Publishing, Indianapolis, Chapter 6. How "Phishing" Attacks Can Steal Your Identity and How to Protect Against Them, 978-0-7897-3553-9
116. Önal H., *Açık Kaynak Kodlu Güvenlik Projeleri*, http://www.enderunix.org/docs/acikkod_guvenlik.pdf [Ziyaret Tarihi: 14 Eylül 2006]
117. Zwicky Elizabeth D. ve diğ., 2000, *Building Internet Firewalls*, O'Reilly Publishing, Sebastabol, s.19, 1-56592-871-7
118. Shirey R., 2000, *Internet Security Glossary*, Network Working Group, Request for Comments: 2828, s.73, http://www.ietf.org/rfc/rfc2828.txt
119. Çölkesen R., 2001, *Network TCP/IP Unix*, Papatya Yayıncılık, İstanbul, s.33, 975-679-702-9
120. Srisuresh P. ve Egevang K., 2001, Network Working Group Request for Comments: 3022, *Traditional IP Network Address Translator (Traditional NAT)*, http://www.ietf.org/rfc/rfc3022.txt
121. Srisuresh P. ve Holdrege M., 1999, Network Working Group Request for Comments: 2663, IP Network Address Translator (NAT) Terminology and Considerations, http://www.ietf.org/rfc/rfc2663.txt
122. Kivinen T. ve diğ., 2005, Network Working Group Request for Comments: 3947, *Negotiation of NAT-Traversal in the IKE*, http://www.ietf.org/rfc/rfc3947.txt
123. Albanese J. ve Sonnenreich W., 2004, *Network Security Illustrated*, McGraw-Hill, New York, s.230-232, 0-07-141504-1
124. Rekhter Y. ve diğ., 1996, Network Working Group Request for Comments: 1918, *Address Allocation for Private Internets*, http://www.ietf.org/rfc/rfc1918.txt
125. *Using nat, global, static, conduit, and access-list Commands and Port Redirection(Forwarding),* PIX, Document ID: 12496, [çevrimiçi], http://www.cisco.com/warp/public/707/28.html [Ziyaret Tarihi: 15 Eylül 2006]
126. *Güvenlik Duvarı Kavramları*, [çevrimiçi], http://www.belgeler.org/howto/proxy-fw_concepts.html , [Ziyaret Tarihi: 15 Eylül 2006]
127. Shimonski Robert J. ve diğ., 2003, *The Best Damn Firewall Book Period*, Syngress Publishing, Rockland, Chapter 3: DMZ Concepts, Layout, and Conceptual Design, 1931836906
128. Northcutt S. ve diğ., 2005, *Inside Network Perimeter Security*, Sams Publishing, Indianapolis, Chapter 7. Virtual Private Networks, 0-672-32737-6

129. *Secure Socket Layer*, [çevrimiçi], http://www.windowsecurity.com/articles/Secure_Socket_Layer.html, [Ziyaret Tarihi: 17 Eylül 2006]
130. *Stunnel - Universal SSL Wrapper*, [çevrimiçi], www.stunnel.org, [Ziyaret Tarihi: 17 Eylül 2006]
131. Lau J. ve diğ., 2005, *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*, Network Working Group Request for Comments: 3931, http://www.ietf.org/rfc/rfc3931.txt
132. Newman Daniel P., 2003, *CSPFA Exam Cram 2 (Exam 642-521)*, 2003, Que Publishing, Indianapolis, Chapter 3. Basics of the PIX Firewall, 978-0-7897-3023-7
133. Noonan W. ve Dubrawsky I., 2006, *Firewall Fundamentals*, Cisco Press, Indianapolis, Chapter 2. Firewall Basics, 1-58705-221-0
134. Check Point Software Technologies, *Stateful Inspection Technology*, http://www.checkpoint.com/products/downloads/Stateful_Inspection.pdf
135. Suehring S. ve Ziegler R., 2005, *Linux Firewalls, Third Edition*, Sams Publishing, Indianapolis, Chapter 3. iptables: The Linux Firewall Administration Program, 0-672-32771-6
136. *PF: The OpenBSD Packet Fitler*, [çevrimiçi], http://www.openbsd.org/faq/pf/index.html, [Ziyaret Tarihi: 17 Eylül 2006]
137. Check Point FireWall-1, [çevrimiçi], http://www.checkpoint.com/products/firewall-1/index.html, [Ziyaret Tarihi: 20 Eylül 2006]
138. Microsoft Internet Security and Acceleration (ISA) Server, [çevrimiçi], http://www.microsoft.com/isaserver/default.mspx, [Ziyaret Tarihi: 20 Eylül 2006]
139. Karaarslan E., *Ağ Güvenlik Duvarı Çözümü Oluştururken Dikkat Edilmesi Gereken Hususlar*, http://csirt.ulakbim.gov.tr/dokumanlar/GuvenlikDuvariCozumuOlusturmaSureci.pdf [Ziyaret Tarihi: 20 Eylül 2006]
140. *Juniper Networks Firewall / IPSec VPN*, [çevrimiçi], http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/, [Ziyaret Tarihi: 21 Eylül 2006]
141. *Cisco ASA 5500 Series Adaptive Security Appliances*, [çevrimiçi], www.cisco.com/go/asa, [Ziyaret Tarihi: 23 Eylül 2006]
142. *WatchGuard Security Appliances*, [çevrimiçi], http://www.watchguard.com/products/appliances.asp, [Ziyaret Tarihi: 23 Eylül 2006]
143. *Secure Computing CyberGuard TSP Firewall/VPN*, [çevrimiçi], http://www.securecomputing.com/index.cfm?skey=1578, [Ziyaret Tarihi: 23 Eylül 2006]
144. Endorf C., ve diğ., 2004, *Intrusion Detection & Prevention*, McGraw-Hill, New York, Chapter 6: IDS and IPS Architecture, 0072229543
145. Lockhart A., 2006, *Ağ Güvenliği İpuçları*, Açık Akademi Yayınları, İstanbul, s.255, 975-98099-2-3
146. Babbin J. ve Biles S., 2005, *Snort Cookbook*, O'Reilly Publishing, Sebastopol, Recipe 1.16. Capturing and Viewing Packets, 0-596-00791-4
147. *Analysis Console for Intrusion Databases*, [çevrimiçi], http://www.cert.org/kb/acid/, [Ziyaret Tarihi: 25 Eylül 2006]

148. Rehman R., 2003, *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID*, Prentice Hall PTR, New Jersey, 0-13-140733-3
149. Carter E.ve Hogue J., 2006, *Intrusion Prevention Fundamentals*, Cisco Press, Indianapolis, 1-58705-239-3
150. Rash M.ve Orebaugh A., 2005, *Intrusion Prevention and Active Response : Deploying Network and Host IPS*, Syngress Publishing, Rockland, s.194-195, 1-932266-47-X
151. *Intrusion Prevention Systems (IPS),* January 2004, NSS Group Ltd., [çevrimiçi], http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm, [Ziyaret Tarihi: 27 Eylül 2006]
152. Spitzner L., 2002, *Honeypots: Tracking Hackers*, Addison Wesley, Boston, 0-321-10895-7
153. Grimes Roger A., 2005, *Honeypots for Windows*, Apress, New York, s.303, 1590593359
154. NFR Security, *Back Officer Friendly*, [çevrimiçi], www.nfr.com/resource/backOfficer.php, [Ziyaret Tarihi: 30 Eylül 2006]
155. Kreibich C., *Honeycomb: Automated IDS Signature Creation using Honeypots*, University of Cambridge, [çevrimiçi], http://www.cl.cam.ac.uk/~cpk25/honeycomb/, [Ziyaret Tarihi: 1 Ekim 2006]
156. *Developments of the Honeyd Virtual Honeypot*, [çevrimiçi], http://www.honeyd.org/, [Ziyaret Tarihi: 1 Ekim 2006]
157. *KFSensor Advanced Windows Honeypot Server*, [çevrimiçi], www.keyfocus.net/kfsensor/index.php, [Ziyaret Tarihi: 1 Ekim 2006]
158. *HoneyBow sensor v0.1.0*, [çevrimiçi], www.mwcollect.org/, [Ziyaret Tarihi: 1 Ekim 2006]
159. *PatriotBox (Honey-Pot Server)*, [çevrimiçi], http://www.alkasis.com/, [Ziyaret Tarihi: 1 Ekim 2006]
160. *Specter, Intrusion Detection System*, [çevrimiçi], www.specter.com, [Ziyaret Tarihi: 2 Ekim 2006]
161. *Bubblegum Proxypot*, [çevrimiçi], www.proxypot.org, [Ziyaret Tarihi: 2 Ekim 2006]
162. *HOACD*, [çevrimiçi], www.honeynet.org.br/tools/, [Ziyaret Tarihi: 2 Ekim 2006]
163. *LaBrea: "Sticky" Honeypot and IDS*, [çevrimiçi], http://labrea.sourceforge.net/labrea-info.html, [Ziyaret Tarihi: 2 Ekim 2006]
164. *Tiny Honeypot*, [çevrimiçi], http://freshmeat.net/projects/thp/, [Ziyaret Tarihi: 2 Ekim 2006]
165. The Honeynet Project, *Sebek*, [çevrimiçi], http://project.honeynet.org/tools/sebek/, [Ziyaret Tarihi: 3 Ekim 2006]
166. The Honeynet Project, *Honeywall CDROM*, [çevrimiçi], http://www.honeynet.org/tools/cdrom/, [Ziyaret Tarihi: 4 Ekim 2006]
167. Kuehl K., *Honeynets: Detecting Insider Threats*, http://winfingerprint.sourceforge.net/presentations/honeynet-insider-threat-2004.ppt
168. UK Honeynet Project, *HoneyStick*, [çevrimiçi], http://www.ukhoneynet.org/honeystick.htm, [Ziyaret Tarihi: 4 Ekim 2006]

169. Chuvakin A. ve Peikari C., 2004, *Security Warrior*, O'Reilly Publishing, Sebastopol, Chapter 20. Honeypots, 0-596-00545-8
170. Stallings W., 2005, *Cryptography and Network Security Principles and Practices, Fourth Edition*, Prentice Hall, New Jersey, 0-13-187316-4
171. Clam AntiVirus, [çevrimiçi], www.clamav.net, [Ziyaret Tarihi: 5 Ekim 2006]
172. Symantec Mail Security for SMTP, http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-mail_security_for_smtp_5.0_04-2006.en-us.pdf
173. Mao W., 2003, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, New Jersey, Chapter 11.2 Authentication and Refined Notions, 0-13-066943-1
174. Burnett M. ve Kleiman D., 2006, *Perfect Passwords: Selection, Protection, Authentication*, Syngress Publishing, Rockland, s. 131-134, 1-59749-041-5
175. Schinder D.L., 2002, *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Rockland, s.420, 1-931836-65-5
176. Han Vinck A.J., 2005, Authentication Persons, University of Duisburg/Essen, http://www.exp-math.uni-essen.de/~vinck/crypto/add-to-5.pdf
177. DansGuardian, True Web Content Filtering for All, [çevrimiçi], http://dansguardian.org/, [Ziyaret Tarihi: 6 Ekim 2006]
178. Platform for Internet Content Selection (PICS), [çevrimiçi], http://www.w3.org/PICS/, [Ziyaret Tarihi: 6 Ekim 2006]
179. *What is Spam?*, [çevrimiçi], http://wiki.apache.org/spamassassin/Spam, [Ziyaret Tarihi: 7 Ekim 2006]
180. *Symantec Internet Security Threat Report, Trends for January 06–June 06*, Volume X, September 25, 2006, http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf
181. *Symantec Brightmail AntiSpam*, http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_brightmail_antispam_6.0_08-2004.en-us.pdf
182. *Kaspersky Antispam 3.0*., http://www.kaspersky.com/downloads/pdf/whitepaper_kas_3_en.pdf
183. The Apache SpamAssassin Project, [çevrimiçi], http://spamassassin.apache.org/, [Ziyaret Tarihi: 8 Ekim 2006]
184. *CERT/CC Statistics 1988-2006*, [çevrimiçi], http://www.cert.org/stats/, [Ziyaret Tarihi: 12 Ekim 2006]
185. Qualys, 2006, *On-Demand Security Audits and Vulnerability Management, A Proactive Approach to Network Security,* [çevrimiçi], http://securityguide.computerworld.com, [Ziyaret Tarihi: 10 Ekim 2006]
186. *Squid Web Proxy Cache*, [çevrimiçi], http://www.squid-cache.org/, [Ziyaret Tarihi: 14 Ekim 2006]
187. Özgit, A., 2003, Bilişim Güvenliğinden Ne Anlıyoruz?, *TBD BIMY-10 Bildiriler Kitabı*, 10-13 Nisan, Antalya
188. Fraser B., 1997, Network Working Group Request for Comments: 2196, *Site Security Handbook*, http://www.ietf.org/rfc/rfc2196.txt

189. Brennan Linda L. Ve Johnson Victoria E., 2004, *Social, Ethical and Policy Implications of Information Technology*, Idea Group, London, 1591402883
190. Laet G. ve Schauwers G., 2004, *Network Security Fundamentals*, Cisco Press, Indianapolis, 1-58705-167-2
191. SANS Institute GIAC (Global Information Assurance Certification) Basic Security Policy Ver. 1.4 February 27, 2001
192. Bishop M., 2002, *Computer Security: Art and Science*, Addison Wesley, Sebastopol, Chapter 4: Security Policies, 0-201-44099-7
193. Adalet Bakanlığı Bilgi Sistemlerinin İnternet Üzerinden Gelecek Tehlikelerden Korunması Ve Veri Güvenliğinin Sağlanmasında Uyulacak Usul ve Esaslar Hakkında Yönetmelik, [çevrimiçi], http://www.mevzuat.adalet.gov.tr/html/23057.html, [Ziyaret Tarihi: 17 Ekim 2006]
194. Çalışma ve Sosyal Güvenlik Bakanlığı, Ulusal Çalışma ve Sosyal Politikalar Kamu Araştırma Programı, [çevrimiçi], http://www.calisma.gov.tr/projeler/program.pdf, [Ziyaret Tarihi: 17 Ekim 2006]
195. Sağlık Bakanlığı, Bilgi Güvenliği Politikası, Kurumsal Bilgi Güvenliği Yönetim Politikası Bildirimi, http://istanbulsaglik.gov.tr/w/sb/bisi/belge/SB_bilgi_guvenligi.pdf
196. TBD Kamu-BİB Kamu Bilişim Platformu VIII, 25-28 Mayıs 2006, *Sonuç Raporları*, http://www.kamubib.tbd.org.tr/dokumanlar/CG1S.doc, http://www.kamubib.tbd.org.tr/dokumanlar/CG5S.doc, [Ziyaret Tarihi: 20 Ekim 2006]
197. *Kamu Bilgi ve İletişim Teknolojisi Projeleri Hazırlama Kılavuzu*, Devlet Planlama Teşkilatı Müsteşarlığı, Bilgi Toplumu Dairesi Başkanlığı, Temmuz 2006, http://www.bilgitoplumu.gov.tr/yatirim/2007_KamuBITKilavuzu_v3.doc
198. Türk Standartları Enstitüsü, 2006, Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, www.tse.org.tr
199. Türk Standartları Enstitüsü, 2006, Bilgi teknolojisi, Güvenlik teknikleri, Bilgi güvenliği yönetim sistemleri-Gereksinimler, www.tse.org.tr
200. Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM), *Kullanım Politikası Sözleşmesi - Acceptable User Policy (AUP)*, [çevrimiçi], http://csirt.ulakbim.gov.tr/politika/kullanimpolitika.uhtml, [Ziyaret Tarihi: 23 Ekim 2006]
201. Devlet Planlama Teşkilatı, 2005, *Kalkınma Planlamasında Bilgi Yönetimi Ve Devlet Planlama Teşkilatı İçin Kurumsal Bilgi Politikası Modeli*, Yayın No: DPT 2687
202. *E-Dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi, Sürüm 1.0*, Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi, Ağustos 2005, http://www.bilgitoplumu.gov.tr/yayin/2005BirlikteCal%C4%B1sabilirlikRehberi.pdf
203. Peltier Thomas R., 1999, *Information Security Policies and Procedures : A Practitioner's Reference*, CRC Auerbach Pres, Florida, s.53, 0-8493-9996-3
204. Riggs C., 2004, *Network Perimeter Security: Building Defense In-Depth*, Auerbach Publications, London, 0849316286
205. Morimoto R. ve diğ., 2006, *Microsoft Windows Server 2003 Unleashed, R2 Edition*, Sams Publishing, Indianapolis, 978-0-672-32898-5

206. Sullivan C., 2006, *Advanced Host Intrusion Prevention with CSA*, Cisco Press, Indianapolis, 978-1-58705-252-1
207. Cornell University, *Policy Development Process*, 2006, [çevrimiçi], http://www.policy.cornell.edu/preview/policy_process.cfm [Ziyaret Tarihi: 25 Ekim 2006]
208. University of Minnesota, Policy and Process Development Office, *Guide to Writing University Policy*, [çevrimiçi] http://www.fpd.finop.umn.edu/groups/ppd/documents/information/Guide_to_Writing.cfm, [Ziyaret Tarihi: 11 Ekim 2006]
209. Luker Mark A. ve Petersen R., 2003, *Educause Leadership Strategies, Volume 8, Computer and Network Security in Higher Education*, Jossey-Bass, 978-0-7879-6666-9
210. The Association of College & University Policy Administrators (ACUPA), [çevrimiçi], http://www.acupa.org/ , [Ziyaret Tarihi: 29 Ekim 2006]
211. Barman S., 2001, *Writing Information Security Policies*, New Riders Publishing, Indianapolis, s.19, 1-57870-264-X
212. The Fog Index, [çevrimiçi], http://www.sharedlearning.org.uk/fog_index.htm, [Ziyaret Tarihi: 7 Kasım 2006]
213. Sönmez V., *Metinlerin Eğitselliğini Saptamada Matematiksel Bir Yaklaşım (Sönmez Modeli)*, Mart 2003, Eğitim Araştırmaları Dergisi, Sayı:10
214. Karaarslan E. ve diğ., *Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması*, [çevrimiçi] http://csirt.ulakbim.gov.tr/dokumanlar/BilgisayarAglarindaGuvenlikPolitikalarininUygulanmasi.pdf, [Ziyaret Tarihi: 30 Ekim 2006]
215. California Berkeley University, Residential Computing, 2005, *Be Secure on the residence hall network*, http://www.rescomp.berkeley.edu/infosheets/besecure.pdf

ÖZGEÇMİŞ

1 Ocak 1972 tarihinde İstanbul'da doğan Hakan Aysal, 1989 yılında girmiş olduğu Yıldız Teknik Üniversitesi Mühendislik Fakültesi Elektrik bölümünden 1994 yılında mezun oldu. Aksaz Deniz Üs Komutanlığı Elektrik Sistemleri Grup Amirliği'nde yapmış olduğu askerlik hizmetinden sonra, 1998 yılına kadar hizmet sektöründe yöneticilik yapmıştır. 1998 yılında göreve başladığı İstanbul Üniversitesi'nde Bilgi Teknolojileri Ofisi'nde Bilişim Birimi sorumlusu olarak çalışmaktadır. Aynı zamanda 2003 yılında Enformatik Bölümü'nde başladığı Yüksek Lisans eğitimine devam etmektedir.