SAU Fen Bilimleri Enstitüsü Dergisi
6.Cilt, 3.Sayı (Eylül 2002)

BİLGİSAYAR AĞLARINDA GÜVENLİK DENETİMLERİ

Ümit ERSÖZ

Özet- **Bilişim sektöründeki gelişmeler kurumsal ve kişisel verilerin bilgisayar sistemleri üzerine taşınmasını sağladı. Bu gelişmeler başlangıçta güvenlik tedbirleri ve tehlikeleri dikkate alınmadan gerçekleştiği için şu an çoğu hizmet güvenlik açıklarına sahiptir. Büyük ölçekli bilgisayar ağlarının oluşturulması ve kötü niyetli saldırganların verdiği zararların izlenmesiyle güvenlik tedbirleri alanında gelişmeler gözlenmeye başladı. Sistem güvenliğini sağlamaya yönelik firewall yazılımları, saldırıları önceden sezmeye yönelik saldırı tespit sistemleri ve güvenlik açıklarını tespit amaçlı zayıflık tarama sistemleri bilişim sektöründe güvenlik politikaları olarak kendisini göstermektedir.**

Anahtar kelimeler **- Firewall, Proxy, Saldırı tespit sistemleri, Zayıflık tarama sistemleri.**

Abstract- **The developments of IT sector provide to be carried institutional and personal data on computer systems. Most of the services have security deficiencies because these developments were come true without to be paid attention security precautions and hazards. The developments on the field of security precautions were started to observed as being constructed big scaled computer systems and being observed the bad purposed attackers' hazards. The firewall software which obtain system security, network intrusion detection system which obtain sense of attacks beforehand and vulnerability scanner systems to determine security gaps are security policies on IT sector.**

Key words **– Firewall, Proxy, Network intrusion detection systems, Vulnerability scanner systems.**

U. Ersöz; SAÜ Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, Sakarya, uersoz@ihlas.com.tr

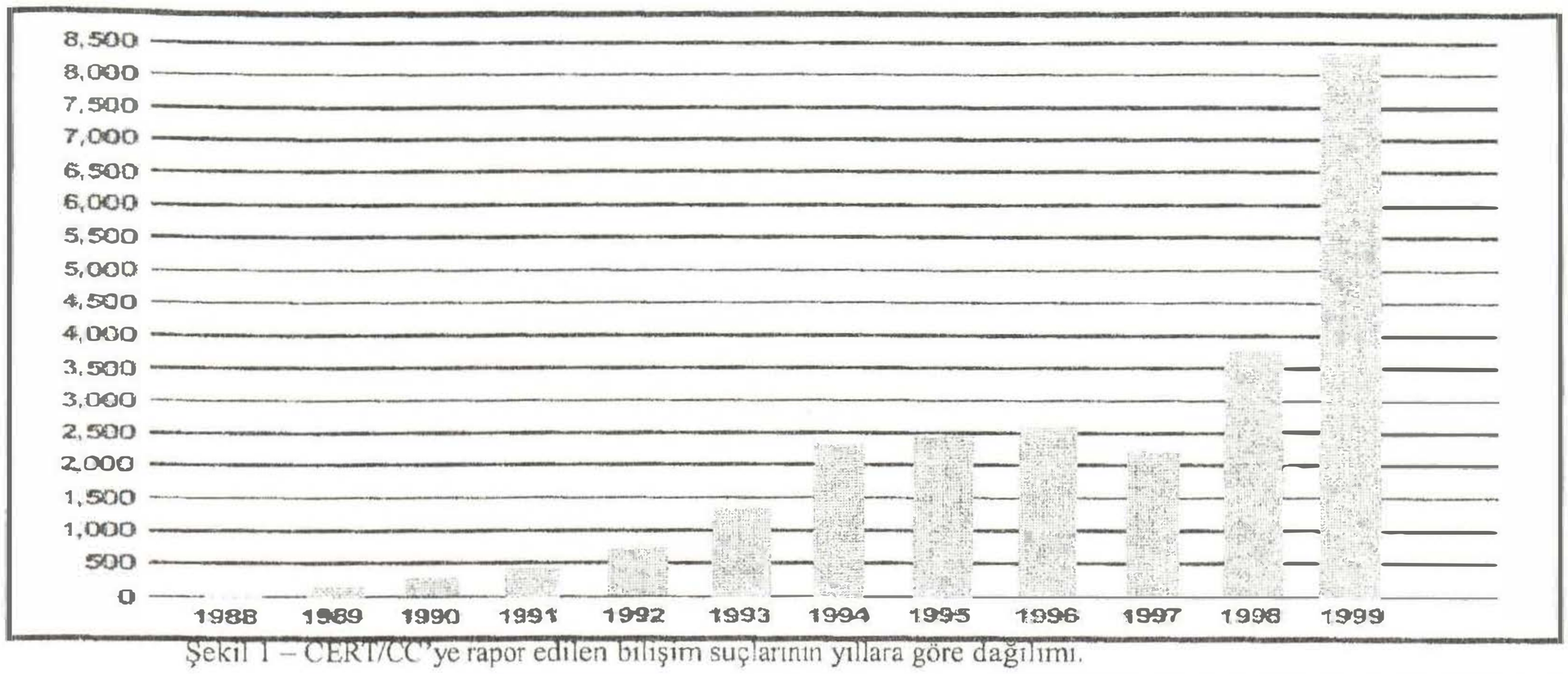
I. GİRİŞ

Günümüz, bilginin çok önem kazandığı, çok hızlı üretildiği ve kısa zamanda güncelliğini yitirdiği bir çağ olmuştur. Bilginin bu kadar önem kazanması, bilgi teknolojilerininde çok hızlı gelişmeler göstermesine sebep olmuştur. Her geçen gün daha modern iletişim teknolojileri ve daha hızlı bilgisayar ağ yapıları ortaya konulmaktadır. Bilgisayarlar bu gelişmelerin ışığında tek başına kullanılır olmaktan çıkmış, Internet ve kuruluşların Intranet'i gibi büyük ağ yapılarının birer parçası durumunu almıştır. Bilgi teknolojilerinin bu gelişimi yaşamımızın her alanında kendini göstermesine yol açmıştır; banka hesapları, sağlık kayıtları, alış-veriş vb. Hedeflenilen nokta ağ üzerindeki hizmetlerin her hangi bir zamanda herhangi bir yerdeki kullanıcılara ulaştırılabilmesidir.

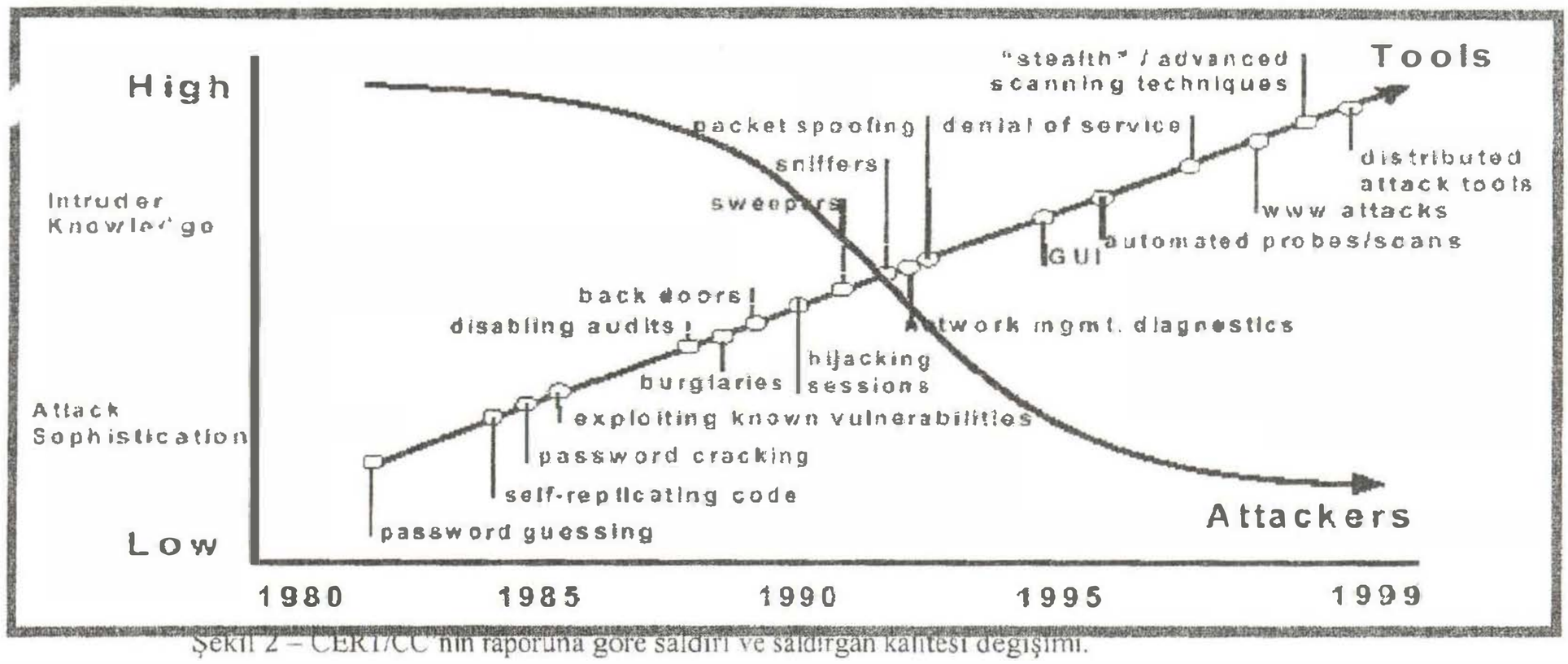
Bilgi teknolojilerinin bu denli farklı alanlarda hizmet vermesi çok kısa bir zaman zarfında gerçekleşmiştir. Bu kadar hızlı geçiş bazı konularda hazırlıksız yakalanılmasına, gerekli alt yapı çalışmalarının tamamlanmadan çözümlerin üretilmesine neden olmuştur. Bu konuların başında hizmetlerin güvenlik destekleri gelmektedir.

Ağ yapıları büyüdükçe, dağıtıklığı ve karmaşıklığı arttıkça bu sistemlerin doğruluğunu, eksiksizliğini denetlemek ve hizmetlerin sürekliliğini sağlamak zorlaşmaktadır. Sistemlerin işlerliğini koruyabilmek ve işlenen bilgilerin güvenliğini sağlamak artık çok önem kazanmış ve güvenlik politikaları oluşturulmasını zorunlu kılar duruma gelmiştir.[1]

Uluslar Arası Bilgisayar Acil Durum Müdehale Ekipleri Koordinasyon Merkezi (Computer Emergency Response Teams Coordination Center-CERT/CC) yaptığı istatistiklere göre 1997 ve 2000 yılları arasında rapor edilen bilişim suçlarının yıllara göre sayısı geometrik olarak artmaktadır.[2]



Şekil 1 – CERT/CC'ye rapor edilen bilişim suçlarının yıllara göre dağılımı.



Şekil 2 – CERT/CC'nin raporuna göre saldırı ve saldırgan kalitesi değişimi.

Günümüzde en büyük bilgisayar ağı durumunda olan Internet'in ilk yıllarında güvenlik konusu önemsiz olarak görülmüş ve gereken ciddi çalışmalar yapılınamıştır. Internet'in temelini oluşturan TCP/IP protokol ailesinin çoğu protokolündeki güvenlik açıkları bu yaklaşımı doğrulamaktadır. Bu ağa bağlı kurum sayısının her geçen gün daha da artması güvenliğin önemli bir problem olarak görülmesini sağlamıştır.

1988 yılında Morris Worm'unun Internet üzerinde çok sayıda bilgisayara bulaşması ve bu sistemleri çalışmaz duruma getirmesi, güvenlik konusuna dikkatleri çekmiş ve teknik önlemlerin alınması yolunda çalışmaların başlamasını sağlamıştır.[1]

II. GÜVENLİK TEDBİRLERİ İLE NELER KORUNMAKTADIR

Bir kuruluş Internet'e bağlanmakla güvenliğini riske atmış olmaktadır. Kurumun sahip olduğu veriler, kaynaklar ve saygınlığı saldırılara karşı tehdit altında bulunmaktadır.

Veriler : Veriler ile ilgili gizlilik, bütünlük, kullanıma hazırlık güvenlikle ilgili üç temel esastır.

Gizliliğe, kuruma ait ve üçüncü şahıslar tarafından erişilmesi istenmeyen; kurumun finansal bilgileri, yeni ürün tasarımları, organizasyon bilgileri ve faliyet gösterdiği alana ilişkin özel raporlar türündeki veriler için gereksinim duyulur. Bu bilgisayarların Internet ortamından ayrı olması düşünülebilir. Böylece gizli bilgilerin ayrılması ve Internet ortamından sadece gizli olmayan verilerin erişime açık olması sağlanalabilir.

Veriler gizli olmasa dahi onların yetkisiz kişilerce değiştirilmesi veya yok edilmesi istenmez. Bu tip saldırılara maruz kalınması maddi kayıpların doğmasına sebep olacaktır.

Verileri ihtiyaç halinde ulaşılabilir olması istenir. Verilerin zarar görmesi veya erişilebilirliğinin sınırlandırılması ileriye yönelik iyi bir planlama ile yapılmalıdır.

Kaynaklar : Internet'e bağlanılmakla sistem kaynaklarıda riske atılmış olunmaktadır. Gerekli güvenlik sağlanılamazsa veri depolama alanları, işlemci gücü, bellek kullanımı yetkisiz kişilerin müdehalesine maruz kalacaktır.

Saygınlık : Kurumun gizli verilerinin ortaya çıkması veya veri kayıplarının olduğunun anlaşılması maddi

zararlara neden olduğu gibi kurumsal kimliğine olan güveni zayıflatacaktır.

Kurumun sistemine olan bir sızma sistem kaynaklarının kötü amaçlar doğrultusunda kullanılmasına neden olabilir. Sızılan sistemlerin farklı kuruluşlara saldırı amaçlı kullanımı saldırıların sızılan sistem üzerinden geldiği görüntüsünü verecektir

Kurumun veya kişisel isim hakkı kullanılarak yanıltıcı bilgilerin yayılması düzeltilemeyecek kötü sonuçları ortaya çıkarabilir. Kuruma ait mail sisteminin bu amaçla kullanılması karşılaşılabilecek bir saldırı tipidir.

Kurumun sistemine olan sızma, kaynaklarının farklı saldırılar için aracı olarak kullanılması ve isim hakkının başkaları tarafından kullanılması kuruluşun imajı üzerinde düzeltilmesi zor yalnış anlaşılmaları doğuracaktır. [3]

III. SALDIRILARIN MEYDANA GELİŞ ŞEKİLLERİ

Saldırganların sistemler üzerine gerçekleştireceği saldırılar sistemin güvenliği ve saldırganın amaçı doğrultusunda farklı gruplara ayrılabilir.

Davetsiz misafir türündeki saldırılarda istenmeyen kişilerin sisteme girmesi şeklinde gerçekleşir. Bu saldırılar genellikle sistem üzerinde yetkili bir kullanıcının kullanıcı adı ve şifresi denenerek elde edilmesi sonucunda meydana gelmektedir. Böylece sistemde yetkili bir kullanıcı davranışını sergileyerek amaçlarına ulaşacaklardır.

Bir başka saldırı şekli olarak, servis kilitleme saldırıları izlenmektedir. Bu saldırı yöntemiyle sistemin yetkili kullanıcılar tarafından kullanılamaması sağlanmaktadır. Sistem üzerinde sürekli mesajlar ve istekler oluşturulması ile sistemin kaynaklarının zamanlarını boşa harcamak suretiyle servis verilemez duruma getirilir. Saldırıları engellemek adına alınmış bazı tedbirlerde saldırganlar tarafından kullanılmaktadır. Örneğin geçerli kullanıcı ve şifrenin erişim hakkını engellemek için yapılan başarısız teşebbüsler kullanıcının girişinin kilitlenmesine neden olacaktır.

Bazı saldırı şekillerinde saldırganlar kuruluşun sistemine doğrudan girmeden istedikleri bilgileri elde edebilirler. Bu saldırılar genellikle bilgi vermeye yönelik hazırlanmış hizmetlerin kullanılması ile olur. Bazı hizmetler ise yerel alan ağlarında kullanılmaya yönelik tasarlanmıştır ve Internet üzerinden kullanılması güvenli olmamaktadır. [4]

IV. SALDIRGAN TİPLERİ

Saldırganların amaçları farklı olsada sergiledikleri bazı genel tutumlar mevcuttur. Bir saldırgan asla yakalanmak istemeyecektir. Saldırganlar girmeyi başardığı bir sisteme sürekli erişebilmek için farklı ulaşım yolları oluşturmaya çalışırlar. Yakalansalar bile erişim yollarını gizli tutmaya çalışırlar. Bu genel özellikler dışında saldırganlar gruplanabilir:

Eğlence İçin Saldıranlar : Belirgin bir hedefi olmayan, girdikleri sistemlerin önemli bilgiler içerebileceğini düşünerek bunlara ulaşmaktan keyif alan, ama zarar vermeyen saldırgan tipleridir. Çok bilinen Internet sitelerine girmek onlar için başarıdır.

Zarar Vermek İçin Saldıranlar : Saldırdıkları sistemlere zarar veren saldırgan tipleridir. Girdikleri sistemleri tahrip edmeye ve yıkıcı zararlar vermeye çalışırlar.

Skor Tutucular : Ulaşabildikleri sistem sayısı ve çeşitliliğine göre puan topladıklarına inanan saldırgan tipleridir. Sistemlere zarar verme amacı içinde değildirler ama daha sonra erişebilmek için kendilerine yeni ulaşım yolları hazırlarlar. Çok bilinen veya iyi korunan sistemlere ulaşmak onlar için daha önemlidir.

Bilgi Hırsızlığı İçin Saldıranlar : Bu tip saldırganlar ulaşabildikleri sistemlerden paraya dönüştürülebilcek verileri alırlar. Bir çeşit casusluk olarakta nitelendirilebilecek saldırgan tipleridir. Ulaştıkları sistemlere zarar vermeden sadece istedikleri bilginin bir kopyasını alırlar. [3]

V. GÜVENLİĞİN SAĞLANMASI İÇİN YAPILABİLECEKLER

Güvenliğin sağlanmasında yapılabilcek en basit yöntem kullanılan ürünlerin sağladığı güvenlik tedbirlerine güvenmektir. Bu yaklaşımın tehlikeler düşünüldüğünde ve ürünlerin açıklarını kapatmak için çıkarılan yamalar görüldükçe pek uygun olmadığı anlaşılacaktır. Açıkların kapatılmasından önce uğranılan saldırlar sistem üzerinde çok ciddi zararların oluşmasına sebep olacaktır.

Diğer bir basit güvenlik tedbiri ise sistemin hiç kimse tarafından bilinmemesinden istifade etmektir. Ama bu yaklaşım nadiren uzun süre çalışır. Internet'te dahil olmak üzere bir ağda üzerinde hizmet sunabilmek ve alabilmek için sistem bilgilerinin bir merkezde kaydının bulunması gerekir. Saldırganlar bir hizmet sunulduğu veya alındığı taktirde yeni sistemlerin farkına varacaklar ve henüz güvenlik tedbirlerinin yetersiz olduğunu düşünerek bu sistemlere erişmeyi deneyeceklerdir. Dolayısıyla bu yaklaşım güvenli bir çalışma ortamı sağlamayacaktır.

Çok kullanılan bir güvenlik yaklaşımı ise konak bazında alınan güvenlik yaklaşımıdır. Bu yaklaşımda her bir konak makinanın güvenliği ayrı ayrı ele alınır. Konağın sunduğu hizmet veya alacağı hizmet doğrultusunda bilinen güvenlik problemlerini bertaraf etmek için gerekli tedbirler alınır. Konak güvenliği her makina ve her işletim sistemi için farklı tedbilerin alınmasını gerektireceği için çok sayıda makina bulunan ağlar için uygulanabilirliği düşüktür. Ama aynı ağ içerisinde daha yüksek güvenlik seviyesi gerektiren konaklar olduğunda uygulanması faydalı olacaktır.

Sistemlerin büyümesi ve sunulan hizmetlerin çoğalması durumunda konak bazında güvenlik yaklaşımından ağ güvenliği yaklaşımına geçmek daha akılcı olacaktır. Ağ güvenliği yaklaşımı ile ağdaki değişik konaklar ve onların sunduğu hizmetler üzerinde yoğunlaşılır.Bu yaklaşımda ağları korumak için firewall'lar, özel kullanıcı belirleme mekanizmaları, şifreleme teknikleri sıralanabilir. Ayrıca ağ güvenliğinden yeterince emin olabilmek ve gelebilecek saldırıları tespit etmek için saldırı tespit sistemleri ile güvenlik konusunda yardımcı olacaktır. Bunun yanında zayıflık tarama sistemleri ile sistemimizde almış olduğumuz önlemlerin bilinen saldırı teknikleri karşısındaki tutumu incelenerek, açıklar konusunda daha doğru çözümler üretilmesi sağlanalabilir.

V.1. Firewall'lar

Bir sistemin özel bölümlerinin, halka açık bölümlerinden ayrılmasını, hizmetlerden belirlenen erişim hakları doğrultusunda faydalanılmasını sağlayan, yetkisiz erişimleri engelleyen uygulamalardır.

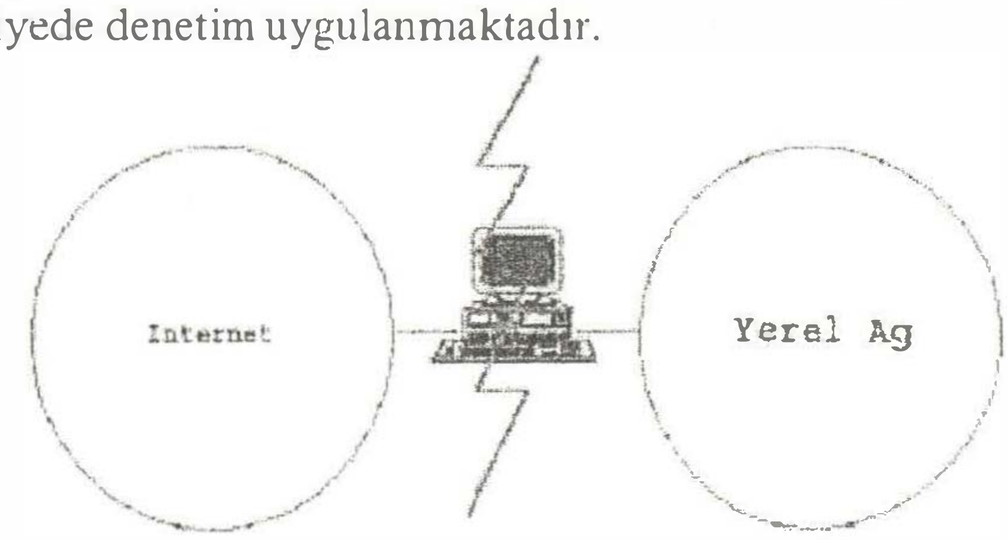
Firewall'lar kullanım kolaylığı ve güvenlik arasında bir uzlaşma olmaya yönelmektedir. Internet ağından erişilebilir yerel ağ, "risk bölgesi" olarak düşünülebilir. Bir koruma duvarı olmadan yerel ağımızın tümü bir risk bölgesi olur.

Bir güvenlik duvarı, Internet'in erişebildiği daha ufak bir alan tanımlayarak risk bölgemizi küçültür. Daha ufak bir risk bölgesi tanımlayarak, Internet'ten gelecek bir sızmayı tespit etmek için inceleyeceğimiz alanı küçültmüş oluruz. Güvenlik duvarlarının çeşitli bileşenler ve ayarlamalar kullanan birçok çeşiti vardır. [5]

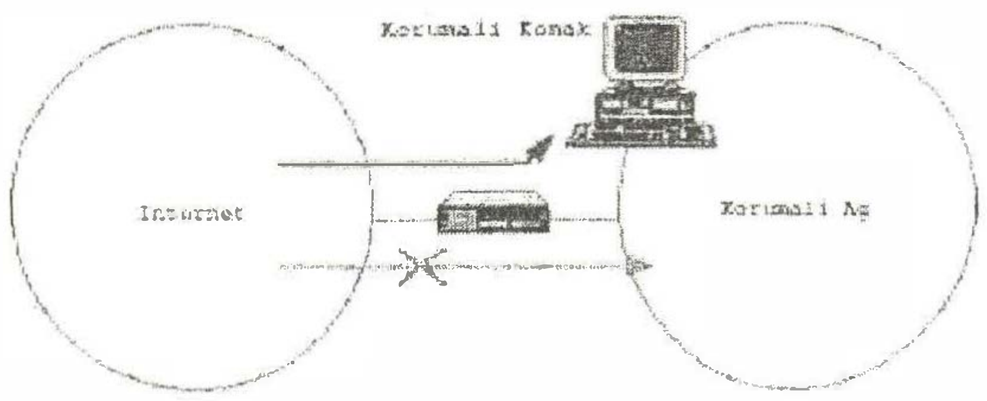
Firewall ile erişim denetiminde kullanılabilecek iki temel yaklaşım vardır. İlki, İnternet bağlantısından tam olarak izin verilmişlerin dışındaki hizmetleri engelleyen bir güvenlik duvarı planlamaktır. İkinci yaklaşım bunun tam tersidir. Tam olarak kısıtlanmış olmayanlara izin veren bir duvarın planlanmasını gerektirir. Buradaki fark, ilk durumda güvenlik duvarı herşeyi engellemek üzere tasarlanmıştır ve hizmetlere dikkatli bir değerlendirmeden sonra izin verilir. İkinci durumda, sistem yöneticisi güvenlikte zayıf noktaları belirlemeli ve açık bırakılmaları çok riskli olacak olan hizmetleri kapatmalıdır. Kullanıcılar genellikle ilk yaklaşımı daraltıcı görüyorlar ve koruma duvarına ürtkenliği engelleyici bakıyorlar. İkinci yaklaşım kullanıcılara Internet kaynaklarını kullanmaları için daha çok serbestlik sağlıyor ve güvenlik duvarımızda güvenlik delikleri açmak için de daha çok serbestlik tanıyor.
Temel olarak 3 çeşit firewall mimarisinden söz edilebilir. Bunlar :

- Çift Ağ Arayüzlü Konak Mimarisi
- Denetlenen Konak Mimarisi
- Denetlenen Alt Ağ Mimarisi

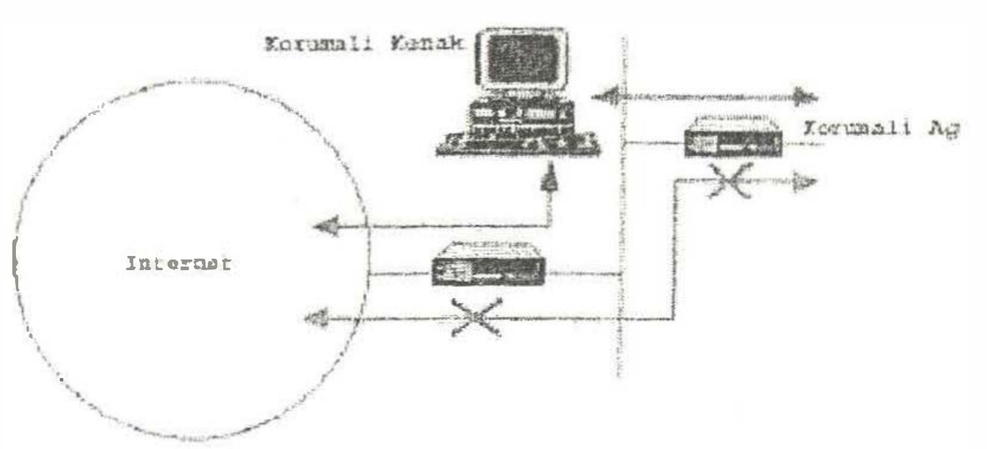
Çift ağ arayüzlü konak mimarisinin temelinde iki ağ arayüzüne sahip bir konak vardır ve bu konak üzerine inşa edilir. Bu konak iç ağ ile dış ağ arasında yönlendirici gibi işlev görür ama yönlendirme özelliği kullanılmaz, vekil sunucu görevini yerine getirir. Yerel ağ ile harici ağ doğrudan iletişim kurmaz ve bu iletişim işlevi çift ağ ara yüzlü konak tarafından kotarılır. Ağlar arasındaki IP trafiği tamamen bloke edilmiş durumdadır ve yüksek seviyede denetim uygulanmaktadır.



Şekil 3. Çift ağ arayüzlü konak mimarisi



Şekil 4. Denetlenen konak mimarisi



Şekil 5. Denetlenenen konak mimarisi

Denetlenen konak mimarisinde Internet hizmetleri yerel ağ dahilinde bulunan bir konak üzerinden sağlanır. Bu mimaride güvenlik kontrolu asıl olarak paket filtreleme

mekanizması üzerinden sağlanmaktadır. Korumalı konak, yerel ağ dahilinde yer alır. Paket filtreleme, dış yönlendirici üzerinde ve güvenlik politikasına uyan Internet hizmetlerinin sadece korumalı konağa erişebileceği şekilde kotarılır. Dışarıdan gelen servis istekleri sadece korumalı konağa yönlendirileceği için bu konağın üst düzeyde güvenliği sağlanmalıdır.

Korumalı konak mimarisinde bazı dezavanytajlar söz konusudur. Saldırgan korumalı konağa ulaştığı durumda, ağın geri kalan konaklarına ulaşması için engel kalmayacak. Denetlenen konak mimarisinde ise paket filtreleme yönlendiricisi her hangi bir sebeple aşılırsa yine ağın diğer konaklarına doğrudan erişim imkanı doğacaktır.
Denetlenen alt ağ mimarisinde: denetlenen konak mimarisine, dahili ağı Internet'ten ayıran bir çevre ağ eklenerek elde edilir. Eklenen çevre ağ güvenlik kademesi oluşturmak için yapılmıştır ve korumalı konağı barındırır.

Bu şekilde bir yapılanmanın çıkış nedeni hedef durumdaki korumalı konağı, dahili ağdan ayırmak ve her hangi bir güvenlik problemi karşısında saldırı ile dahili ağı yüz yüze bırakmamaktır. Dahili ağ ile çevre ağ arasında paket filtreleme yeteneği bulunan yönlendirici yer almaktadır. Bu yönlendirici üzerinde dahili ağ kullanıcılarının hem korumalı konağa hem harici sunuculara erişim yetkileri güvenlik politikaları göz önüne alınarak verilir. Dahili ağın dışında kurulan çevre ağın, dış dünya ile bağlantısı yine paket filtreleme yeteneğine sahip bir yönlendirici üzerinden kotarılır. Bu yönlendirici üzerinde hem dahili ağı hemde korumalı konağı korumaya yönelik bir güvenlik politikası izlenir. Korumalı konak aynı zamanda dahili ağın vekil sunuculuğunuda üstlenecek şekilde düzenlenebilir. Böylece dahili ağın yapacağı istekler korumalı konağa olmakta ve korumalı konakta onlar adına harici sunuculardan hizmet talep etmektedir. [3]

Firewall'ları sunduğu güvenlik seviyesi düzeyinde sınıflandırabiliriz. Bunlar:

- Paket filtreleme yapan firewall'lar
- Proxy firewall'lar
- Uygulama düzeyli firewall'lar

Paket filtreleyen firewall'lar bilgisayara girecek olan paketleri kontrol ederek, belirlenen kurallar çerçevesinde filtrelerinden geçirerek paketlerin akıbetine karar verir. Bu akıbet üç şekilde olur. Paket ya kabul edilir, ya kabul edilmediğine dair paketi gönderen sisteme bir cevap gider ya da hiçbir cevap verilmeden paket bloke edilir.
Proxy firewall'ların çalışma prensibi vekaleten iş yapmaktır. Bizim makinamız adına dışardaki herhangi bir sisteme hizmet isteği yapar ve ondan gelen cevapları da bizim makinamıza taşır.

Uygulama düzeyli firewall'lar OSI başvuru modeline göre uygulama katmanı düzeyinde, uygulama protokolleri üzerinde güvenlik denetimi sağlar.

V. 1.1. Paket Filtrelemeye Yönelik Firewall

Bilgisayar ağlarında verilerin iletimi için küçük parçalara ayrılması gerekir. Bu küçük parçalar TCP/IP protokolü kullanılan ağlarda IP paketi olarak adlandırılır. Verilerin paketler şeklinde iletimi ağın birçok sistem tarafından paylaşılmasına müsade eder. Paketlerin iletimi esnasında hedeflerine ulaşabilmesi, paketlerde yer alan IP başlık bilgilerinin yönlendirici adı verilen cihazlar tarafından okunup doğru yönde aktarılması ile mümkün olur. Yönlendirici bir donanım veya genel amaçlı bir işletim sistemi üzerinde çalışan bir yazılımda olabilir. Paket filtreleme ise bu yönlendiriciler üzerinde koşturulan filtereleme amaçlı yazılımlar ile gerçeklenir. [4]

Paket filtrelemeye yönelik firewall'lar ağdaki trafik akışını paket bazında çok sıkı bir denetimde tutan mekanizmalardır. Bu firewall'lar kendi üzerinden geçen trafiği kontrol altında tutarak bunlardan sadece kabul edilebilir olanların geçişine izin verirler. Kabul edilebilirlik sınırı ağdaki servisler ve güvenlik politikası doğrultusunda belirlenir. Mesela bir ağ üzerinden email hizmeti sunuluyor ise SMTP paketlerinin geçişi firewall politikasında izin verilecek şekilde belirlenmelidir.
Paket filterelemeye dayalı firewall kullanımında dikkat edilmesi gereken önemli nokta, tüm ağ trafiğinin sadece bu mekanizma üzerinden geçerek aktığından emin olmaktır. Başka çıkış noktaları olan bir ağda bu tip bir mekanizmayı kurmak güvenlik konusunda problemleri doğuracaktır. Çünkü saldırılar diğer bağlantı noktaları üzerinden geçebileceği için paket filtreleme mekanizmamız bir işe yaramayacaktır. Paket filtelemeye dayalı firewall ile;

- Yerel ağdan dış ağlara giden paket trafiği sınırlandırılabilir.
- Dış ağlardan yerel ağa gelen paket trafiği sınırlandırılabilir.
- Ağ trafiği hakkında bilgi edimek mümkün olur.

Bir paket filtereleme yazılımı IP katmanı seviyesinde kontrol gerçekleştirir ve IP başlığında yer alan aşağıdaki bilgilere göre davranış sergiler.

- Kaynak IP Adresi
- Hedef IP Adresi
- Protokol Tipi
- Kaynak Port
- Hedef Port
- Eğer ICMP mesajı ise mesaj tipi
- Paketin giriş yaptığı ağ arayüzü
- Paketin hangi ağ arayüzüne iletileceği

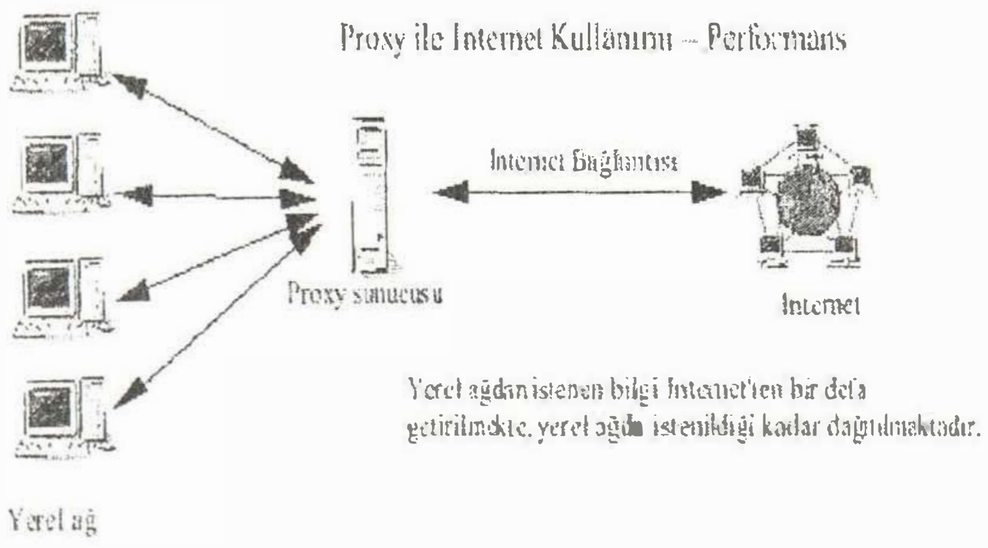
Son iki bilgi paket yönlendirme mekanizması tarafından sağlanırken diğer bilgiler IP paketi içinde saklıdır.

Paket filtreleme yazılımları paketin taşıdığı veri ile ilgilenmez ve dolayısıyla kullanıcı bazında denetim gerçekleştirmezler.

Bir firewall mimarisinde paket filtreleme istenilen aşamada yapılabilir. Sadece tek yönlendirici içeren mimarilerde paket filtrelemenin yapılacağı yer bu yönlendiricilerdir. Bunun yanısıra konak bazında da paket filtreleme yapılabilir.

V.1.2. Proxy Firewall'lar

Bir proxy, yerel ağ ile dış dünya arasında yer alan ve başta bilginin güvenli bir şekilde temini ve paketlerin depolanmasını sağlayan bir programdır. [6]
Proxy kavramı tüm konaklara erişim varmış gibi görünüyorken bir ya da birkaç tane konağa erişim sağlar. Özel bir protokol ya da protokol kümesi için bir proxy sunucu çift arayüzlü konak veya korumalı konak üzerinde çalışır. İstemci programı Internet üzerindeki gerçek sunucu yerine proxy sunucu ile bağlantı kurar. Proxy sunucu istenin izinli olup olmadığına baktıktan sonra eğer izin veriliyor ise gerçek sunucu ile bağlantı kurar ve haberleşme boyunca istemci ile sunucu arasında yer alır. Proxy, gerçeklemede özel bir donanım gerektirmez ancak birçok hizmet için özel yazılım gerektirir.
Proxy ön belleği yardımıyla yerel ağdaki istemci, dışarıdaki bir sunucuya doğrudan bağlanmadan yine yerel ağdaki sunucu üzerinden servis alır. Proxy sunucu bir istek aldığı anda eğer bu isteği kendi disk alanından karşılayabiliyorsa istemciye doğrudan gönderir, aksi taktirde asıl sunucuya bağlanır ve bu sunucudan aldığı bilgileri istemciye yollar. Bu sırada yolladığı paketleri, ileride gelebilecek istekleri karşılayabilmek amacıyla depolar.



Şekil 6. Proxy firewall

Böylelikle birkaç bilgisayarın aynı anda aynı bilgileri almak için mevcut band genişliğini kullanmaları önlenmiş olur. Ayrıca yerel ağdan daha hızlı bilgi transferi gerçekleştirilebilir.

İstatistikler, proxy kullanan ağlarda performans artışının %40'lara kadar ulaştığını göstermiştir. Özellikle kısıtlı band genişliğine sahip organizasyonlarda bir proxy sistemin kurulumu büyük önem taşır.

Proxy için bazı dezavantajlarda mevcuttur. Yaygın olarak kullanılan ve eski hizmetler için proxy yazılımları mevcuttur. Ancak yeni ya da yaygın kullanılmayan hizmetler için yazılım bulmak zordur. Diğer bir dezavantajı ise her protokol için ayrı proxy sunucu gerekmesidir. İstemci ve sunucu arasında proxy'nin saydam olması ve isteklerin filtrelenmesi için protokol bazında farklı proxy sunucular gerektirir. [4]

Proxy'nin çalışma şekli Internet hizmetleri arasında farklı şekilde gerçeklenir . Her hizmet proxy desteği ile dizayn edilmediği için sunucu ve istemci bazında farklı işlemler gerektirirler. İstemciler proxy sunucuyla temasa geçtiğini ve gerçek sunucuyu bildirmek zorunda olduğunu bilir, bu desteği vermeyen istemcilere yama yazılımlar üretilmiştir. İstemcinin proxy sunucuya bağlantı desteği yoksa kullanıcı başka bir prosedürü takip ederek proxy sunucuya gerçek sunucuyu bildirmek durumundadır. [4]

V.1.3 Uygulama Düzeyli Firewall'lar

Uygulama düzeyli firewall'lar en sıkı koruma sağlayan mimaridir. OSI başvuru modeline göre uygulama katmanı düzeyinde çalışır; uygulamaya yönelik tam denetim yapma imkanı sunar. Genel olarak güçlü bir iş istasyonu üzerine yüklenen yazılımla gerçekleştirilir. Bu tür firewall'lar proxy firewall'lara benzer ama oturum kurulduktan sonra bile paketlerin sınaması yapılır. Bu da beklenmedik saldırılardan korunmayı kuvvetlendirir. [7]

Bu yöntem, ağ yöneticisine, paket filtrelemeli ve proxy firewall'a göre daha güvenli, daha sıkı bir koruma imkanı verir. İstenen programların çalışmasına izin verilirken, yasak olanlar engellenir. Bu tür güvenlik duvarı kullanılması durumunda ağ yöneticisine büyük bir sorumluluk düşer; gerekli olan konfigürasyonu kendisi yapmalıdır.

Uygulama düzeyli firewall'da kabul edilecek veya kabul edilmeyecek kuralları içeren bir tablo oluşturulur. Bu tablo üzerindeki bir kurala uyan ve geçme hakkı elde eden paketler karşı tarafa geçirilir. Aksi durumda uygulama için gerekli paket geçişi engellenir.

V.2. Saldırı Tespit Sistemleri

Güvenlik politikasının yaptırımının sağlanması kadar, ihlallerin tespitide önem arz etmektedir. Saldırı tespit sistemleri, yerel ağdan veya bağlı bulunulan harici ağlardan gelebilecek ve ağımızdaki sistem kaynaklarına zarar verebilecek, çeşitli paket ve verilerden oluşabilen saldırıları tespit ederek kayıt tutmak ve uyarı mesajları yollama görevini üstlenmişlerdir.

Saldırganların bir kısmı bu iş için otomatize edilmiş araçlarla saldırırken, uzman seviyesindeki saldırganlar saldırdıkları hedefe göre değişebilen çeşitli yöntemler kullanırlar. Yerel ağı korumak amaçlı Firewall ve Anti-

virüs gibi sistemleri sadece ilk tip saldırganları engelleme imkanı sunmaktadırlar. Korunmak için kurulan bu sistemlerin aslında saldırganları yavaşlattığını ve bu yavaşlama aşaması sırasında onları tespit edip yakalama imkanı sunduğu kabul edilerek güvenlik yolunda ilk adımlar atılmış olabilir.

Eğer bu sistemler saldırganları yavaşlatma amaçlı olarak kurulduysa düzenli olarak saldırı kayıtlarının incelenmesi de gerekmektedir. Bu durumda pasif olan firewall ve anti-virüs sistemlerine ek olarak Saldırı Tespit Sistemleri de kurmak gereklidir. Böylece gerektiğinde aktif olabilecek bir savunma aracı da kazanılmış olur.

Saldırı Tespit Sistemleri ile ağa yapılabilecek tüm saldırıları belirleme ve gerektiği durumda engelleme imkanı kazanılır. Düzenli olarak tuttukları kayıtlar incelenerek saldırganların neler yaptıkları ve hangi gruba dahil oldukları anlaşılabilir. Gerektiğinde kötü niyetli görülen isteklerin ağa girmesine izin verilmeyebilir. [8]

V.2.1. Saldırı Tespit Sistemlerinin İçerik Olarak Çalışma Şekilleri

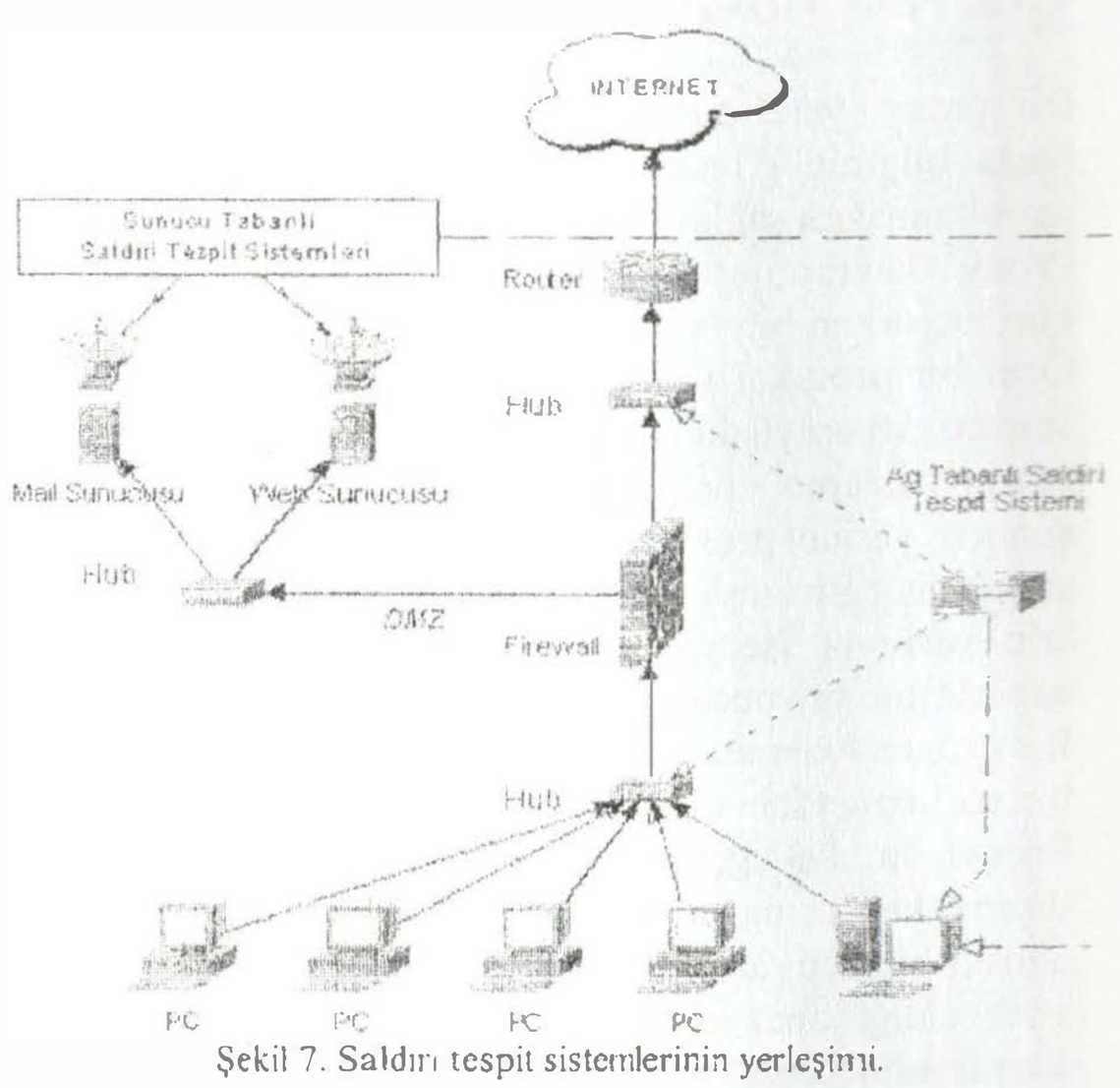
Saldırı tespit sistemleri içerik olarak iki ayrı prensipte çalışmaktadırlar, ilk yapıda anti-virüs sistemlerinde olduğu gibi oluşturulmuş çeşitli imzalar ile paketleri incelemek ve saldırıları saptamak hedeflenmektedir. İkinci yapıda ise sistemlerin ve ağın işleyişi belirli bir düzende yapılandırılmıştır, bu düzende olabilecek herhangi bir anormallik saldırının tanımlanmasını sağlamaktadır.

İlk tür saldırı tespit sistemleri günümüzde yaygın olarak kullanılmaktadırlar. Belirlenen çeşitli kurallar çerçevesinde ağ üzerinde yakalanan paketleri inceleme şeklinde çalıştıkları için her saldırının izlerinin tanımlanmış olması gereklidir. Genelde bu tür sistemlerde saldırıların çokluğu, her saldırı varyasyonu için ayrı kurallar koyma işini bir miktar zorlaştırmaktadır. Ancak ticari yazılımlarda otomatik olarak Internet'ten hergün yeni saldırı imzaları indirilebilmektedir.

İkinci tür saldırı tespit sistemlerinde ise durum bir miktar daha akla yatkındır. Ağda yada çeşitli sunucularda düzenli olarak yapılmakta olan işlemleri takip ederler ve farklı ya da olağandışı hareketler gördüklerinde ise rapor ederler. Bu tür sistemlerin normal olarak nitelendirilebilecek hareketleri öğrenmeleri oldukça fazla zaman almaktadır. Ayrıca bu hareketlerin zaman içerisinde değişebilirliği, kurulduğu sistemlerin yeniden yapılandırılması veya ağa yeni sistemler eklemek işi daha da zorlaştırmaktadır. [8]

V.2.2 Saldırı Tespit Sistemlerinin Yerleşim Olarak Çalışma Şekilleri

Saldırı tespit sistemleri yerel ağda çalıştıkları yere göre yine ikiye ayrılmaktadırlar. Ağ Tabanlı sistemler olarak tanımlanan grup, yerel ağdaki tüm bilgileri yakalayabilen bir sisteme kurulurlar ve ethernet kartının promiscuous moda geçirerek ağdaki tüm trafiği dinlerler, saldırıları rapor ederler ve gerektiğinde bir sunucuya açılmakta olan oturumu engellerler. İkinci grup ise Sunucu Tabanlı sistemler olarak anılmaktadır. Ağ Tabanlı sistemler gibi tüm ağı değilde sadece üzerinde kurulduğu sunucuya gelip gitmekte olan verileri ve o sunucunun kayıt dosyalarını, yürütülen süreçleri incelerler.



Şekil 7. Saldırı tespit sistemlerinin yerleşimi.

Ağ Tabanlı saldırı tespit sistemleri ağa yapılabilecek olası saldırıları raporlamak üzere tasarlanmıştır. Ağdaki yakalayabildiği tüm paketleri incelerler ve ağa giriş izni olup olmadığına karar verip, rapor tutar. Kuruldukları sistemde dinleyecekleri ağ sayısı kadar kaliteli ethernet kartı bulunmalıdır. Genel olarak posix tabanlı sistemlerde ya da kendi özel işletim sistemlerinde çalışmaktadırlar. Ciddi bir performans kaybı söz konusu olabildiği için Windows tabanlı sistemler tercih edilmemektedir. Ağ parçalarını dinlerken bazı saldırı tespit sistemleri tek bir sistem ile bu işlemi tamamlarlar, bazı sistemler ise her ağ parçasını kendisinden farklı her biri agent (yardımcı) olarak adlandırılan sistemler ile dinlemektedir. Böyle durumlarda örneğin 5 yardımcı lisansı ile gelmektedirler. Her yardımcı 1 veya 2 ağ parçasını dinleyebilir özelliğe sahiptir.

Sunucu Tabanlı saldırı tespit sistemleri ise çeşitli özel sunuculara yüklenerek, o sunucuya yönelik saldırıları tespit etmek veya önlemek şeklinde çalışırlar. Bulundukları sistemlerin konfigurasyon dosyalarını, sistem ile ilgili kayıtların tutulduğu dosyaları izlemeye almak, o sistemin bütünlüğünde meydana gelebilecek değişiklikleri incelemek ve sisteme yönelik kötü niyetli kullanımları engellemek görevlerinden başlıcalarıdır.

Kuruldukları sistemlere tanı olarak uyum sağlayabilmeleri konusunda zorlukları vardır. İşletim sistemlerinin doğası gereği birbirleriyle uyumluluk göstermeleri nadirdir ve bu durum saldırı tespit sistemlerinin o işletim sistemine özel yazılmış olması, o sistemin zayıflıklarına uygun yapılandırılmış olması gibi zorunlulukları ortaya çıkarmaktadır. Özel bir sunucu yazılımı için üretilmiş olanlarıda vardır. Örneğin : Snort for US. [8]

V.3. Zayıflık Tarama Sistemleri

Otomatik zayıflık tarama sistemleri bir ağ parçası içinde bulunan istemci, sunucu, yönlendirici, firewall gibi tüm ağ bileşenlerinin güvenlik zayıflıklarının bulunmasını, bulunan zayıflıkların kapatılma yöntemleriyle ilgili referans ve açıklamaların listelenmesini sağlayan yazılımlardır.

Ağ güvenliğindeki zayıflıklar, hatalı yapılan ağ tasarımından, sadece görselliği ön planda tutularak hazırlanmış kötü yazılımlardan, donanım, işletim sistemini ya da kullanılan protokoldeki güvenlik eksiklerinden kaynaklanır. Bunun sonucunda yetkisini aşan kötüye kullanımlara zemin hazırlayarak sistemin işlerliğini tehlikeye sokar. [9]

Zayıflık tarama sistemlerini üç grup altında toplamak mümkündür:

- Yerel Sistem Zayıflık Tarama Sistemleri
- Uzak Sistem Zayıflık Tarama Sistemleri
- Uygulamaya Özel Zayıflık Tarama Sistemleri

Zayıflık tarama sistemlerinin özellikleri :
Zayıflık tarama sistemleri daha önce yayınlanmış sistem zayıflıklarını bir veritabanı halinde bünyesinde bulundurur. Üretici firmalarca ya da gönüllü kişilerce yeni duyurulan zayıflıklar bu veritabanlarına eklenerek dağıtılır. Zayıflık tarama sistemleri, veritabanlarındaki bu zayıflık bilgilerinden istifade ederek hedef gösterilen sistemler üzerinde bu zayıflıkları test ederler.

Zayıflık tanımlama için kendilerine özel script dillerde içerirler. Böylece sistem yöneticilerine kendi zayıflık scriptlerini oluşturup hedef sistemlerini test imkanı sunarlar.

Yıllık olarak yayınlanan zayıflık bilgileri takip edilmesi zor rakamlara ulaştığı günümüzde düzenli takip imkanı sunar.

Bir saldırgan gibi sistemler üzerindeki zayıflıkları test eder, sonuçları çeşitli formatlar ve düzenler halinde raporlama imkanı sunar. Raporlarında tespit edilen zayıflıklar için çözüm yolları ve referans kaynaklarıda verebilirler.

Zayıflık tarama sistemlerinin eksiklikleri:

- Henüz yayınlanmamış güvenlik zayıflıklarını bulamazlar.
- Gerçek bir saldırgan gibi saldıramazlar. Ancak veritabanlarında tanımlandığı çerçevede saldırılar gerçekleştirirler.
- Paket kayıplarının yoğun olduğu ağlar üzerinde doğru sonuçlar üretemez ve yanıltıcı olabilirler.
- Uygulamaların açılış mesajları veya verilebilecek sahte yanıtlar zayıflık tarama sistemlerini yanıltabilirler.

VI. SONUÇ

Bilişim teknolojilerindeki hızlı gelişim ile bilginin çeşitli sayısal ortamlar üzerinden tüm dünyaya sunulması artık mümkün duruma gelmiştir. Ama bu gelişim yanında bir takım problemleride doğurmuştur. Bilginin ve bilgi sistemlerinin maruz kaldığı saldırılar her geçen gün artmaktadır. Artan bu güvenlik problemleri yeni yeni güvenlik çözümlerinin üretilmesini, var olanların geliştirilmesini gerekli kılmıştır. Saldırıları önlemeye yönelik ürünlerin kullanılması kaçınılmaz olmuştur. Bunun yanında saldırıları tespit eden ve saldırganlar gibi davranış gösteren ürünler sayesinde güvenlik açıkları için daha iyi çözümler üretilmesi mümkün duruma gelmektedir.

KAYNAKLAR

[1] DAYIOĞLU, B., ÖZGİT, A., "Internet'te Saldırı Tespit Teknolojileri", İletişim Teknolojileri 1. Ulusal Sempozyumu Ve Fuarı, 17-21 Ekim 2001, Ankara
[2] CERT/CC Web Sitesi, http://www.cert.org , CERT 2001
[3] KARAAHMETOGLU, O., "Internet Güvenliği Kavramları ve Teknolojileri", Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, 2001
[4] AY, Y., "Internet'te Firewall Güvenlik Kavramı", Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, 1996
[5] BARRON, B., ELLSWORTH, J. H., SAVETZ, K. M., "Internet Unleashed", p 135-148, 1997
[6] ÇETİN, G., ÇELİK, K. G., "Linux Ağ Yönetimi", p159, Ağustos 2000
[7] ÇÖLKESEN, R., ÖRENCİK, B., "Bilgisayar Haberleşmesi ve Ağ TEknolojileri", p 273, Ekim 2000
[8] ÖZAVCI, F., "Saldırı Tespit Sistemleri Giriş", http://www.siyahsapka.com, Kasım 2001
[9] ÖZAVCI, F., "NESSUS ve Zayıflık Tarama Sistemleri v.1", http://www.siyahsapka.com, Ocak 2002