

Bilgisayar Ağ Sistemleri Güvenliği

Öğr.Gör Erhan Kahya

Trakya Üniv.Tekirdağ Meslek Y.O.Bilgisayar Prog.
ekahya@trakya.edu.tr

Özet: Günümüzün vazgeçilmez bir parçası olan bilgi işlemde bilginin gizliliği , özgünlüğü ve bütünlüğü devamlı bir saldırı altındadır.Bilgisayar korsanları (Hacker) tarafından devamlı bu sistemler saldırıya uğramakta ve bilgiler ele geçilmeye çalışılmaktadır. Bu nedenle büyük firmalar ve kişisel kullanıcılar saldırılara karşı çok büyük yatırımlar yapmaktadır. Yatırımlardan dolayı ülke ekonomisi büyük kayıplar yaşamaktadır.Ülkemizde bu saldırılara karşı yeni yeni yasal işlemler yapılması biraz olsun bu saldırıları azaltmıştır.

Anahtar Kelimeler:Bilgisayar ağı, hacker, saldırı

Abstract: The secrecy, originality and integrity of information processing which can not be given up in today's life is under a continuous attack. These systems are always being attacked by hackers and they are trying to get the stored information. Therefore big firms and personal users make big investments against these attacks. Because of the big investments ,the economy of the country is in danger of great losses.Taking some legal actions against attacks has decreased the number of attacks to some extent.

Keywords: Computer network, hacker, attack

1.Giriş

Günümüzde bilişim alanındaki en büyük sorunlardan biri ağ güvenliğidir.Büyük şirketler kurmuş oldukları ağ sistemlerinin saldırılara karşı korunması için yaşamsal bir savaş vermektedirler.Bundan dolayı çok büyük yatırımlar yapmakta ve büyük paralar harcanmaktadır. Ticari anlamda firmalar büyük zarar görmektedirler.Diğer taraftan bu tür sistemleri üreten ve yazılım geliştiren firmalar büyük bir para kazanmaktadırlar.Saldırı çeşitleri arttığı sürece her gün yeni bir ağ güvenliği programı ve sistemi ortaya çıkmaktadır.Tabii olarak bu gelişme yüzünden büyük bir pazar oluşmaktadır.

Burada sadece büyük firmalar değil kişisel bazdaki kullanıcılarda bilgi saklama ve korunması için çeşitli programlar ve sistemler almaktadır.Dünya çapında büyük bir pazar haline gelen bu güvenlik sistemleri dünya ülkelerinde olduğu gibi ülkemiz ekonomisine büyük zararlar vermektedir.

Yapılan araştırmalar dünya genelinde şirkete yapılan atakların % 70 ila % 90 arasında şirket çalışanları tarafından yapıldığını ortaya koymaktadır. Bu bilgi hırsızlığından tutun bilerek yada bilmeyerek sistemlere verilen zararları kapsamaktadır. Genelde işinden kötü şekilde ayrılan şirket çalışanları sistemlere ait bilgilerini başkalarına verebilmekte yada özellikle sistemleri sabote edebilmektedirler. Kendi bilgisayarlarına kurdukları “sniffer”(paket dinleyici) lar sayesinde başka kişilerin maillerini yada gizli bilgilerini elde edebilmektedirler. Yada her türlü önleminizi dışarıdan gelebilecek saldırılara karşı almışken içeriden birisi kolaylıkla önemli sistemlere erişebilir kritik bilgileri silip değiştirebilir yada rakip bir firmaya verebilir. Yada meraklı bir kullanıcı yeni öğrendiği hacker araçlarını sizin firmanız üzerinden başka firmalara girmek için kullanabilirler.(1)

Güvenlik için yapılan her yatırıma karşı bu saldırılar sürmektedir.Hatta Amerika'da dünyanın

en iyi korunan , girilmesi imkansız olan Savunma Bakanlığı bilgisayarlarına girilmiş ve bilgilere ulaşılmıştır. Amerika'da bu tür saldırılara ağır cezalar uygulanırken Türkiye'de bir yasal boşluktan dolayı yakalananlar elini kolunu sallayarak hapisten çıkmaktadır. Bundan dolayı ülkemizde en kısa sürede bu yasal boşluğun kapatılması gerekmektedir.

2. Ağ Güvenliği Sağlama Yöntemleri

Ağ güvenliği sağlanırken sadece güvenlik duvarı (firewall) tek başına düşünülmemelidir. Güvenlikte esas olan süreklilik, kullanılan cihazların ve yazılımların bir bütün halinde kurulması ve işletilmesidir. Ağ ortamındaki tüm elemanların bu sistem içine alınması gerekir. Fiziksel koruma yapılırken merkezi birim olduğu yer bir kontrol noktası haline getirilmelidir. Bu kontrol noktası ayrı bir odada olmalı ve sadece belli kişilerin girmesi sağlanmalıdır. Sistem içinde bir kabinet var ise bu kabinet her zaman kilit altında tutulmalıdır. Şu unutulmamalıdır ağ üzerinde saldırılar sadece dışardan değil en fazla içerdeki personelden gelmektedir.

Ağ cihazlarının ayarlanması, yönetimi ve kontrolünde kullanılan HTTP, Telnet, SSH, SNMP, TFTP ve FTP; TCP/IP protokolünün alt elemanları olduklarından, bu protokolün zayıflıklarına karşı önlem alınması gerekmektedir. Bu türden erişimlerde denetim, bu cihazların ve dolayısıyla ağ trafiğinin güvenliği için çok gereklidir. Cihazlarda kurulum sırasında oluşan varsayılan (default) ayarların, kullanıcı tarafından aktif edilen bazı ayarların iptal edilmesi veya düzgün olarak tekrar ayarlanması gerekebilmektedir. (2)

Ağ güvenliği tam olarak aşağıdaki güvenlik kavramlarını bir bütün olarak ele alınmasıyla sağlanabilir.(3)

- İnternet bağlantı güvenliği
- Saldırı ve Saldırı tespit sistemleri
- Veri güvenliği
- Virüslerden koruma
- Şifreleme

- Log analizi
- VPN Güvenliği

2.1. İnternet Bağlantı Güvenliği

İnternet'in genişlemesi ile beraber ağ uygulaması da beklenmedik şekilde genişlemiştir. Bu gelişmeyle birlikte ağ kurulup işletmeye alındıktan sonra ağ yönetimi ve ağ güvenliği büyük önem kazanmıştır. Çünkü internete bağlı ağ sistemleri arasında dolaşan hiçbir veri gerekli önlemler alınmadığı takdirde güvenli değildir. Ağın güvenilir biçimde çalıştırılması anahtar sözcük konumuna gelmiştir. Çünkü ağın günümüz teknolojisi ile kurulup çalıştırılmasıyla iş bitmemekte esas iş ağ performansının ve güvenilirliğinin sağlanmasında bitmektedir.

Firmanın bilgisayar sistemini kullanan personel genelde kişisel bilgilerini bilgisayarlarında depolarlar. Bu kişiler bilgisayarları İnternet'e bağlandığında kişisel bilgilerinin ekstra koruma gerektirdiğini bilmeliler. Ağlar bilgisayarlar ve veritabanları gibi değerli kaynakları birbirine bağlar ve firma için gerekli olan servisleri sağlarlar. Bir sunucunun sağladığı özellikler çoğaldıkça güvenlik açıkları içerme riski de o oranda artar. Bunun sebebi İnternet protokol ve standartlarının dizayn edilirken güvenliğin düşünülmemesidir.

Kullanıcıların genelde işlerini yeterlilikle yapabilmeleri ağ servislerine bağlıdır. Eğer kullanıcıların bu servislere erişimi engellenirse daha az üretken olurlar ve bu da firma için mali kayıp demektir.(4)

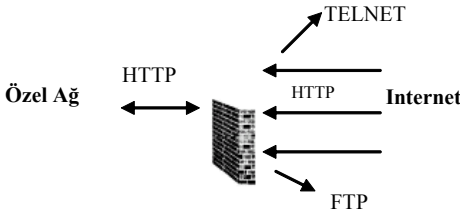
2003 yılında birçok kereler rastladığımız yaygın kullanılan işletim sistemi ve uygulamalarda bulunan açıkları kullanarak dağıtılan solucanlara (örn: Sql slammer, nachi bv.) karşı yine tedbirli olmak gerektiğini belirten uzmanlar, yeterli güvenlik önlemi alınmadan 24 saat İnternet'e açık bırakılan sistemlerin hacker'lar tarafından kötü amaçlı olarak servis kesintisi atakları için kullanılabileceğini söylüyorlar. Spam konusunda da 2004 yılında artış olacağını söyleyen uzmanlar bunun

için kurumların ek güvenlik çözümlerine gereksinimi olacağını belirtiyorlar.(5)

Uzmanlar kurumsal Internet güvenliği için şirket içi eğitimlerin olması gerektiğini, çalışanlara Internet bağlantısında dikkat etmeleri gerekli noktaların, e-posta alışverişinde göz önüne alınması gereken hususların ve her bir çalışanın kendi masaüstü koruma yazılımı ile sistemini periyodik olarak virüslere karşı taramasını öneriyorlar.(5)

Servis kullanımı engelleme (DoS) Internet'teki istemci ve sunucular için en ciddi tehditlerden biridir. Aynı zamanda engellenmesi en zor güvenlik tehdididir. Bir servis kullanımı engelleme saldırısı kurbanın normalde erişebildiği bir servise erişebilmesini engelleyen kötü amaçlı bir saldırdır. Bir saldırganın bunu gerçekleştirebilmesi için pek çok farklı yol vardır.

Bunun için özel ağ ile Internet arasında bir Firewall konulması gerekmektedir.Bu sistem ile ağ güvenliği tam olarak sağlanır ve erişim hakları düzenlenir.Bu sistem kurulurken şu noktalara dikkat edilmelidir.Kurulmadan önce ne tür bilgilerin korunacağı, ne derecede bir güvenlik uygulanacağı ve kullanılacak güvenlik algoritmaları önceden belirlenmelidir.Firewall'ın sistem üzerinde etkili kullanılması için ağ ortamı ile internet arasındaki tüm trafiğin Firewall üzerinden geçilmelidir.



Şekil 1.Tipik bir firewall(6)

2.1.1.Firewall türleri

-Packet-filtering firewall

Bu yöntem Firewall oluşturmanın en kolay yoludur.Paketlerin başlık alanı içindeki bilgi-

lere bakılarak istenmeyen paketler karşı tarafa geçmez.OSI modelinde 3 katman olan network katmanında çalışır.

-Circuit – level gateway

OSI modelinde 4 katmanı olan session katmanı düzeyinde çalışır.Bu sistemde oturum bir kez kabul edilip kurulduktan sonra ,her paket için denetim yapılmaz.Paketler kurulan sanal devre üzerinden geçer.

-Application – level gateway

En sık koruma yapan Firewall tekniğidir.OSI modelinde uygulama katmanı düzeyinde çalışır.Bu nedenle tam denetim yapma imkanı sunar.Bu tür düzenlemede oturum kurulduktan sonra bile paketlerin sınaması yapılmaktadır. Bundan dolayı beklenmedik saldırılara karşı korumayı güçlendirir.

2.2.Saldırı ve Saldırı Tespit Sistemleri

2.2.1. Saldırı Türleri

Birkaç tip saldırı türü vardır. Bunları DoS (nuke), Remote Exploits ve Trojanlar olarak ayırabiliriz.(7)

NUKE: Nuke, sisteminizi kilitleyen, geçerten, Internet erişimini kesen ve bu gibi zararlar veren saldırılara Nuke (nükleer bombanın kısaltması gibi) adı verilir. (7)

Nuke siz internete bağlıyken ISS nizce size verilen bir ip numarası yardımı ile bir başka kişinin özel programlar yardımı ile bilgisayarınıza paketler gönderilmesi ve bu paketlerin bilgisayarınıza zarar vermesidir.(8)

OOB Nuke: (Out of band Nuke) Sadece Windows NT ve 95'de bir bug olan OOB nuke, işletim sistemi Windows olan bir makinanın 139. portuna (Netbios session port) MSG_OOB tipi bir bağlantı (connection) yapılmasıyla gerçekleşir. Eğer 95 kullanıyorsanız sisteminizin mavi ekran vererek Internet bağlantısının kopmasına, NT kullanıyorsanız sistemin durmasına yol açar. ((7)

Land: Bilgisayarı kendi kendine senkronize ettirerek, arka planda Internet meselelerini yürüten Winsock adlı programın sonsuz döngüye girmesini sağlar. Böylece farenizi bile hareket ettiremezsiniz. Kaynak IP (Source), Kaynak Port ve Hedef IP (Destination IP) IP, Hedef Port'un aynı olduğu bir IP paketi, Land saldırısının gerçekleşmesini sağlar. (7)

Teardrop, Boink, Nestate: Internet üzerinde gelen giden veri, parçalar halinde taşınır, daha sonra işletim sistemi tarafından birleştirilen paket parçacıkları veriyi oluşturur (fragmentation). Çoğu sistemin duyarlı olduğu bu saldırı tipleri, bilgisayarınızın bozuk olarak bölünmüş 2 paketi birleştirmeye çalışması ile gerçekleşir. Boink, teardrop saldırısının ters olarak çalışan halidir. Nestate, teardrop saldırısının küçük değişimlere uğramış halidir ve teardrop ve boink saldırılarına karşı patch edilmiş Linux sistemlerinde etkilidir. (7)

Brkill: Eğer Windows yüklü bir bilgisayara, bağlantının sonlanması ile oluşan PSHACK tipi bir TCP paketi gönderirseniz Windows size o anki son bağlantı seri numarasını gönderir. Buradan yola çıkarak hedef makinedeki herhangi bir bağlantıyı zorla kesmeniz mümkün olur.

ICMP Nuke: Bilgisayarlar çoğu zaman aralarındaki bağlantının sağlamlığını birbirlerine ICMP paketleri göndererek anlarlar. Bu saldırı varolan bir bağlantının arasına sanki hata varmış gibi ICMP_UNREACH paketi göndererek oluşur. (7)

Jolt/SSPing: Windows 95 ve NT'nin yüksek boyuttaki bölünmüş ICMP paketlerini tekrar birleştirememesinden kaynaklanan bir saldırı tipidir. 65535+5 byte'lık bir ICMP paketi göndermek bu saldırıyı gerçekleştirir. (7)

SMURF: Networkler'de "broadcast address" olarak tanımlanan ve kendine gelen mesajları bütün network'e yönlendiren makineler vardır. Eğer birisi başka biri adına o makineye ping çekerse, ağ üzerindeki bütün çalışan makineler

hedef olarak belirlenen makineye ping çeker. Smurf, bu işlemi yüzlerce broadcast makineye tek bir kaynak IP adresinden ping çekerek saldırı haline çevirir. Bir anda bilgisayarlarınıza on binlerce bilgisayarın ping çektiğini düşünürsek değil sizin şirketinizin bağlantısı, maalesef Turnet (Türkiye Internet omurgası) çıkış gücü bile buna cevap vermeye yetmez ve bağlantılarınız kopar. (7)

Suffer: Suffer saldırısı bilgisayarınıza sanki binlerce farklı bilgisayardan bağlantı isteği geliyormuş gibi SYN paketleri gönderir. Bu saldırının sonunda Windows yeni bağlantılar için yeterli hafıza ayıramaz ve kalan hafızayı da bitirir. Bazı firewall türleri de böyle bir durum karşısında binlerce soru kutucuğu açarak makinenin kilitlenmesine sebep olur. (7)

Exploit'ler: Exploit'in kelime anlamı "kötüye kullanma, sömürme" demek. Yani sisteminizin normal bir özelliğinin bir açığını yakalayıp, bunu kötüye kullanabilir, sisteminizdeki, bilgilere ulaşabilirler. Exploitler genelde sistem tabanlı olarak çalışırlar yani Unix'e ait bir exploit Windows için çalışmaz. Bu güne kadar bulunan yaklaşık olarak 1000'in üzerinde exploit var. Ve bunların hepsinin nasıl çalıştığını anlatmamız güvenlik sebeplerinden dolayı mümkün değil. Aşağıda çok popüler olan bir kaç taneinden bahsedilecektir. (7)

Windows Null Session Exploit: Windows işletim sistemi, dışarıdaki kullanıcılara network üzerinde hiç bir hakka sahip olmadan oturum, kullanıcı ve paylaşım bilgilerini (session, user ve share) verir. Ve ne kadar ilginçtir ki, bu exploit, Windows Network API'sinde belgelenmiş ve feature (özellik) olarak gösterilmiştir. Kötü niyetli birisi bu exploit'i kullanarak sistem hakkında çok kritik bilgiler sahibi olabilir. (7)

PHF Exploit: Bu exploit oldukça eski olmasına rağmen halen karşılaşılabileceğiniz bir güvenlik açığıdır. Phf cgi yardımı ile sistemdeki dosyalara admin olarak erişebilirsiniz.

Yukarıdaki örnek Unix işletim sistemi ya da türevini kullanan bir makineden kullanıcı bilgilerinin ve şifrelerinin bulunduğu passwd dosyasını görmenizi sağlar. (7)

ASP Exploit: Active server page (ASP) özelliği kullanan Web sunucularda URL'nin sonuna bir nokta (.) yada ::\$DATA yazarak ASP'nin içeriğini (source code) görebilirsiniz. Eğer ASP'nin içerisinde her hangi bir şifre varsa bu exploit çok tehlikeli olabilir. (7)

http://www.aspkuullananserver.com/default.asp.
ya da
http://www.aspkuullananserver.com/
default.asp::\$DATA

Sendmail Exploit: Eski "send mail" sürümlerinde bir kaç basit hile ile sistemin şifrelerinin tutulduğu dosyayı çekmeniz mümkün. Ayrıca sistem kullanıcıları hakkında bilgi almak (EXPN) ya da bir kullanıcı isminin o sunucuda olup olmadığını da öğrenmek mümkün (VRFY). (7)

telnet mail.server.com:25

ICQ Tabanlı Exploitler: Son derece zayıf bir mimariye sahip olan ICQ sistemi, kolayca taklit edilebilen hatta gerçek "spoofing" bile yapmanıza gerek kalmayan bir sistemdir. ICQ kullanıcıları kolayca mesaj bombasına tutulabilir, şifreleri değiştirilebilir, onaya gerek kalmadan listenize alabilir, IP'si kullanıcı istemese bile görülebilir ya da ICQ chat yaparken mesaj taşması (flooding) yapılabilir. (7)

2.2.2.Saldırı Tespit Sistemleri

Saldırı tespiti ile ilgili yaklaşımı ikiye ayırırız.(9)

-Kalıp Eşleştirme (Signature) Sistemleri: Önceden tespit edilmiş saldırıların eş zamanlı olarak işleyici tarafından karşılaştırılmasını esas alır.

Ör:\ Snort vb.

-Anormallik Tespiti:Sistemi önce öğrenen, istatistiksel olarak normal çalışma yapısını çıkaran sistemlerdir. Buna göre anormal davranışları yakalarlar.

Ör:\ Cylant Secure, NFR(Network Flight Recorder) vb.

2.2.3.Saldırı Tespit Sisteminin Faydaları (10)

- Ağdaki saldırıları bulmada ve engellemede en büyük yardımcılarıdır.
- Bazen sunuculara, bazen ağa, bazen de her ikisine birden koruma sağlarlar.
- Güvenlik duvarları ve yönlendiriciler gibi pasif güvenlik cihazları değildirler. Aktif olarak raporlama, engelleme ve öğrenme gibi işlevleri yerine getirirler.
- Saldırı davranışlarından güvenlik zaafları bulunabilmektedir.
- Hangi noktaların güçlendirilmesi gerektiği bulunabilir.

2.2.4.Saldırı Tespit Sisteminin Problemleri

Saldırı tespit sistemleri birçok avantaja sahip olmakla birlikte bazı problemleri de bulunmaktadır. (10)

- Kötüye kullanım tespiti tabanlı yaklaşımda saldırı örüntüleri elle kodlanmak zorundadır ve ilk kez yapılan saldırılar (novel attacks) tanınmamaktadır.
- Anormallik tespiti tabanlı yaklaşımda ise olaylar arasında ilişki kurmak mümkün olamamaktadır.
- Saldırı tespit sistemleri önemli ölçüde yanlış alarm üretmektedirler (false alarm) .
- Üzerinde veri madenciliği yapılacak saldırı verisi fazla olduğunda sistem etkin olarak çalışmamaktadır.
- Veri madenciliği yaklaşımli saldırı tespitinin false positive (aslında saldırı meydana gelmediği halde STS tarafından sanki bir saldırı varmış gibi alarm verilmesi) oranı daha yüksektir ve bu tip tespit, eğitim ile değerlendirme aşamalarında etkin olmama eğilimindedir. Ayrıca daha karmaşıktır.

- Kural tabanlı saldırı tespit sistemleri uzman bilgilerine dayalı olarak kodlandıkları için değiştirilmeleri oldukça pahalı ve yavaştır.
- Sunucu günlüklerine dayalı saldırı tespiti her zaman mümkün olmayacağından büyük bir problemdir. Bunun yerine görsel-leştirme benzeri teknikler kullanılabilir.
- Sunucu günlükleri kimi zaman güvenli olmadığını sunucu günlüklerine dayalı saldırı tespiti de yanlış sonuçlar verebilmektedir (sunucu günlükleri tehdit altında bulunabilir, birileri kanıtları ortadan kaldırmak isteyebilir).

2.3. Veri Güvenliği

Kurumların internet veya özel iletişim hatları üzerinden akan verilerinin güvenliğinin sağlanması amacıyla kullanılacak teknolojiler şunlardır. (11)

Fiziksel Güvenlik: Bilgisayarların fiziksel güvenliğinin gerek şifre gibi unsurlarla gerekse akıllı kart türü araçlarla sağlanması.

- Kullanıcı Doğrulaması (Authentication) yöntemleri: Akıllı kart, tek kullanımlı parola, token ve Public Key Certificate gibi araçlar ve RADIUS gibi merkezi kullanıcı doğrulama sunucularının kullanılması.
- Şifreleme: Güvensiz ağlar üzerinden geçen verilerin güvenliği için Virtual Private Network veya şifreleme yapan donanımların kullanılması. Ayrıca web tabanlı güvenli veri transferi için SSL ve Public Key şifrelemenin kullanılması. Donanım tabanlı şifreleme çözümleri de mümkündür.
- İnkâr edilemezlik ve mesaj bütünlüğü: Sayısal imza teknolojisi kullanılarak bunlar sağlanabilir.

2.4. Virüslerden Koruma

Bilgisayar sistemlerinin arızalanmasına ve hatta çökmesine yol açan virüslerden korunmanın yolu oldukça basittir. Arızaların ve virüslerin sebebi de genellikle internet kaynaklıdır. Aslında, yapılan araştırmalar gösteriyor ki, sistemlerinin

arızalanmasının sebebi genellikle kullanıcı hatasından kaynaklanıyor. Ancak internette sörf yaparken bilgisayar gereksizce yüklenen programlar bilgisayar sistemlerinin arızalanmasına ve sistemin çökmesine yol açmaktadır.(12) İnternette içeriğin zenginleşmesi ve sörf yapan sayısının artmasının ardından kullanıcıların bilgisayarlarında yaşadığı sorunlar da artmaya başlamıştır. Ancak pek çok araştırmaya göre, bilgisayarda yaşanan sorunların çoğu kullanım hatasından veya gerekli programların sistemde yüklü olmamasından kaynaklanmaktadır. Virüslerden Koruma yöntemlerini şu şekilde sıralayabiliriz.

2.4.1. Antivirüs Programı Yüklenmesi

Korumasız olan bilgisayar ağlarına ve bilgisayar sistemlerine en büyük zararı, virüsler vermektedir. Bu yüzden gerek kurumsal gerekse bireysel kullanıcılar, sistemlerin en azından bir antivirüs programıyla koruma yolunu seçmelidir. Bilgisayar dünyasında çok çeşitli amaçlara yönelik antivirüs programları yer almaktadır. Norton Antivirüs (www.antivirüs.com), TrendMicro PC-cilin (www.trendmicro.com), McAfee Viruscan (www.mcafee.com) gibi bilinen markaların yanı sıra, www.free-av.com adresinden de farklı antivirüs programları bulunmaktadır.

2.4.2. Güvenlik Duvarı Örümesi

Bilgisayar sistemlerinin çökmesinde internet kaynaklı programlardan gelen virüslerin önemli rol oynadığı kesindir. Bu yüzden sisteminizi korumak ve İnternette güvenli sörf yapmak için firewall adı verilen güvenlik duvarını bilgisayarlara yüklemekte fayda vardır. Bu güvenlik sistemi aynı zamanda başka kullanıcıların bilgisayarınıza sızmasını da önlemekte önemli rol oynayacaktır. Bu yükleme işlemi için bilinen markalar Norton ve McAfee'nin sistemleri kullanılabilirliği gibi, BlackICE PC Protection 3.5 veya Zone Alarm 4.0 de kullanılabilir.

2.4.3. Yamaları Düzenli Yüklenmesi

Bilgisayar sistemlerinin yüzde 95'inde kullanılan Microsoft tabanlı Windows işletim sistemlerinde çoğu zaman kaynağı belirsiz olan açıklar ortaya çıkmaktadır. Microsoft firması da açığa

çıkın bu açıkları kapatmak için düzenli olarak, internet sitesi aracılığıyla yamaları yayınlamaktadır. Açıkları kapatmak ve sistemi korumak için gerekli yamaları <http://v4.windowsupdate.microsoft.com/tr/default.asp> adresi kullanılarak, kontrol edilebilir, sistemle karşılaştırılıp gerekli yamaları yüklenir.

2.4.4. Kullanım Hatlarının Düzeltilmesi

Sistemlerin arızalanmaması için, kullanıcının dikkat etmesi gereken önemli unsurlar vardır. Örneğin bilgisayara program yüklerken, kesinlikle art arda gelen kutuları okumadan 'evet' tuşuna basmamak gibi. Size servis veren veya ziyaret ettiğiniz internet sitelerinin hızlı kullanım tuşlarının yer aldığı yazılımları bilgisayarınıza yüklemeyin. Kullandığımız yazılım ve programların hangi şirket tarafından sertifika altına alındığını kontrol edin. e-postaların eklerini açarken uzantılarına dikkat edin.

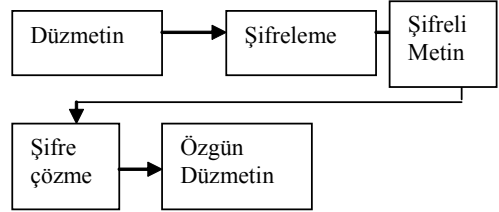
2.5. Şifreleme

Bilgisayar ağlarında bir kullanıcı başka bir kullanıcıya gönderdiği ileti üçüncü bir kullanıcı tarafından dinlenme ve değiştirilme olasılığı altındadır. Bu nedenle bilgilerin alıcı dışında başka kullanıcılar tarafından okunmaması ve değiştirilmemesi için kodlanması gerekmektedir. Yapılan bu işleme şifreleme denir. Metin şifrelendiğinde artık şifreli metin oluşmuştur. Şifreleme ve şifreyi çözmek için bir matematiksel algoritma ve anahtar gereklidir.

Burada anahtar şifreleme ve deşifrelemek için kullanılan sayısal karakter anlamına gelmektedir. Sistematik anahtar algoritmasında şifre ve deşifre de aynı anahtar kullanılır. Açık anahtar algoritmasında ise şifrelemek için açık, deşifre yapmak için gizli anahtar kullanılmaktadır. Dijital imzalar açık anahtar algoritmasıyla yapılır. Dijital imza imzanın sahibinin gizli anahtar kullanılarak oluşturulmaktadır. Alıcı ise imzayı sahibinin açık anahtarını kullanarak kontrol eder. (13)

Şifreleme yapılırken gruplar kendisine ait bir grup şifresi kullanılmalıdır. Her kullanıcı kendisine ait bir şifreleme kullanılmalıdır. Yazılım ve

donanım ürünlerindeki hazır şifreleme teknikleri kullanılmamalıdır. Nedeni üçüncü bir şahıs aynı yazılım ve donanım ürününe sahip olarak bu grup içine girebilir. Bu da verilerin üçüncü şahıslar tarafından ulaşılmasına sebep olur.



Şekil 2. Şifreleme ve şifreyi çözme işlemi (13)

Tüm bu şifreleme sistemi yapılandırmasında en önemli noktalardan biri de şifrelerin iyi seçilmesidir. Burada dikkat edilecek noktalar;

- Şifre içinde büyük ve küçük harf olmalıdır,
- Şifre içinde özel karakterler olmalıdır,
- Şifre içinde rakamlar olmalıdır,
- Kişiyi özel değerler olmamalıdır (doğum tarihi, çocuğunun adı gibi),
- Şifre karakter sayısı en az 7 veya 8 karakter olmalıdır.
- Şifre kolay ve hızlı yazılabilir olmalıdır. Etraftaki kişiler bunu görmesi zorlaşır.
- Şifreler her kesin ulaşabileceği bir yere not edilmemelidir.

Günümüz kriptografisindeki bu sorunu bir anahtar ile çözümlenmektedir. Anahtarın değeri çok değişik algoritmalara sahiptir. Ayrıca şifreleme algoritmaları artık gizli değildir. Sebabi anahtarın farklı uzunluk ve yapılarında algoritmaya sahip olmasıdır. Anahtar ile şifrelenmiş bir bilgi kullanılan algoritma yapısına bağlı olarak ilgili anahtar ile çözülebilir.



Şekil 3. Bir mesajın dinlenmesini önlemek için anahtar kullanımı (13)

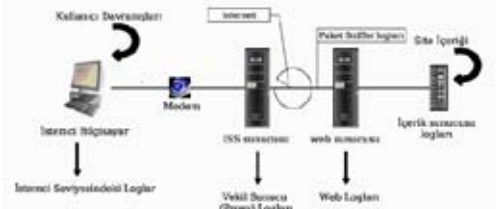
Kullanıcı 1 'in gönderdiği mesaj bir anahtar ile şifreler ve açık ortama gönderir.Kullanıcı 2 anahtar sayesinde şifreyi çözüp iletiyi görür. Bu sistemde anahtarlar aynı sistematik yapıya sahip olmamalıdır.Açık ortamdaki üçüncü kişiler aynı sistematik anahtar kullanarak bilgiye ulaşabilir.Bunu önlemek için Kullanıcı 2'nin kullandığı anahtar gizli olması gerekir.Çünkü Anahtar 1'i kullanarak Kullanıcı 2'ye ulaşmak mümkün olmayacaktır.Bu yapıya public key system denir.Açık anahtarı sistemde açık anahtarın başkaları tarafından bilinmesinde bir sakınca yoktur.Ama saklı anahtarın başkaları tarafından bilinmemesi gerekir.

Dijital anahtarlar açık anahtarlama sistemi üzerine kurulmuştur.Bu sistemde açık - gizli anahtar çifti bir sayı çiftinden oluşur.Gizli anahtarı sadece kullanıcı veya kurum bilir ve dijital imzayı oluşturmak için kullanır.Açık olan anahtar ise dijital imzayı doğrulamasında kullanılır.Bu da doğrulama sonucunda mesajın geldiği kişinin kimliğinin belirlenmesini ve doğrulanmasını sağlar.

2.6. Log Analizi

Bilgisayar ağlarında kullanılan ağ cihazları eventler hakkında kayıt yapma özelliğine sahiptirler.Bu kayıtlar sayesinde ağ üzerinde güvenlik olaylarının belirlenmesi ve önlem alınması sağlanmaktadır. Buna Log Analizi denilmektedir.(14)

Log analizi sayesinde sisteme girmeye çalışan kişilerin adres bilgilerine ulaşılmaktadır. Ayrıca sistem içinde bulunan kullanıcıların yaptıkları (dosya kaydetme , yazıcıdan çıktı alma gibi) işler kontrol edilmesi mümkün olmaktadır.



Şekil 4.Log Analizi(15)

Büyük firmalarda ise internet ortamında kullanıcıların hangi siteye girdikleri , hangi aşamada terk ettikleri , hangi sayfada daha çok / az zaman harcadıkları gibi bilgilere kolaylıkla ulaşmaları sağlanır.

Kamu kuruluşlarında ise kullanıcıların yapmış oldukları tüm işler kontrol edildiğinden dolayı tam bir güvenlik sağlanmış olur.

Cihazlarda kayıtların;

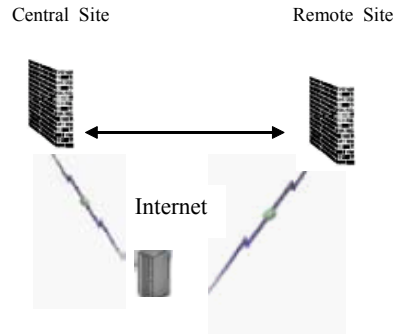
- SMMP Trap Logging
- Log saving

Şeklinde yapılıır.

SMMP'de sistem durumunda karakteristik değişiklikler ağ yöneticisine uyarı gönderir.Log Saving de sistem konfigürasyonuna bağlı olarak eventler hakkında kayıtlar saklanır.(16)

2.7. Vpn Güvenliği

Şirketlerin acente veya bölge müdürlükleri gibi temsilcilikleri arasında veri akışını özel bir güvenlik tüneli ile sağlanmasına VPN (Virtual Private Network) denir.VPN sayesinde firmalar bir operatöre ait mevcut alt yapıyı kullanarak verilerini güvenli ve hızlı bir şekilde gönderirler.



Şekil-5.VPN sistemi(9)

Ayrıca bu tür firmalar yüksek yatırım gerektiren özel network 'e sahip olmalarına gerek yoktur. Bu da maliyetler de önemli bir azalmaya sebep olacaktır.Diğer taraftan güvenlik ve hız gibi çok büyük bir avantajı sahip olacaklardır.

Sistem genel telekomünikasyon alt yapısını kullanmaktadır.VPN'i bir şirket tarafından sahiplenmiş veya kiralanmış özel bir hat olarak düşünülebilir.VPN 'nin amacı bir firmaya özel bir hat tahsis edilmesi yerine firmanın aynı hizmeti daha düşük fiyata herkes tarafından paylaşılan altyapıdan temin etmesidir.VPN ağında güvenli ortak paylaşım , data transferinin gerçekleştirilmesine izin vermektedir.(17)

Sanal özel ağ teknolojisinde datanın herkese açık hatlar üzerinden gönderilmeden önce şifrelenir.Verinin ulaşması istenen yerde ise deşifre edilir.Bunun yanında sadece iletilen data değil , gönderenin ve alanın network adresleri şifrelendiğinden extra bir güvenlik sağlanır.VPN yazılımlarını Windows NT gibi işletim sistemleri desteklemektedir ve firewall'un bir parçası olarak kurulum servisi vermektedir.

Bu sistemde kullanılan şifre doğrulama protokolleri PAP (Password Authentication Protocol) , CHAP (Challenge Handshake Authentication Protocol) ve SPAP (Shiva Password Authentication Protocol) dür.Daha sonra güvenli şifreleme çözümlerinde senkronize edilmiş anahtarlar ve dijital sertifika gibi teknolojiler gelişmiştir.

Bu sistem ücretlendirilmesi servisi sağlayıcı firmanın kullanmakta olduğu VPN donanımı ve bunların bakım ücretlerine göre değişmektedir. Maliyet ise şehirlerarası ve milletlerarası telefon bağlantılarına son vereceğinde kendini amorti etmektedir.(18)

3. Sonuç

Ağ güvenliği sağlanırken ister kurumsal ister kişisel baz da olsun ilk önce saldırı tespiti yapılmalıdır.Daha sonra bu tespite göre uygun program ve donanım seçilmelidir.Bilgisayar içindeki bilgiler kişiler için çok önemli olduğundan bunlardan gelebilecek bir saldırı sonucunda bilgilerin yok olması,istenmeyen kişileri eline geçmesi mümkün olacak.Bu da kişi ya da kuruluşların büyük zararlara uğramasına sebep olacaktır. Bu

yüzden ağ güvenliği sağlanırken yukarıda açıklanmış olan ağ güvenliği sağlama yöntemleri eksiksiz bir biçimde uygulanmalıdır.

Kaynaklar

[1] “Kurumsal Bilişim Güvenliği: Güvenlik Politikası, Teknolojileri ve Standartları Alanında En İyi Uygulamalar” seminer notları,web adresi: <http://support.infonet.com.tr/tr/presales/konsept.htm>2003

[2] **Karaaslan,E.,” Ağ Cihazlarının Yönetimi ve Güvenliği”**, Web adresi: <http://www.izmir.emo.org.tr/dergi/temmuz2003/network.htm>,07.2003 bülteni

[3] http://www.asistbilisim.com/Ağ_Guvenligi.htm

[4] Kurt,E. ,” Internet Güvenliği”, Web adresi: <http://www.olympus.org/index.php/article/articleview/128/1/2/>, 24.02.2002

[5] “Internet güvenliği: Virüs tehditleri artıyor”, Web adresi: http://www.turkpoint.com/e-guvenlik/int_guv_vir_teh_art.asp,2004

[6] Dr.Çölkesen,R. , Prof.Dr.Örencik,B. , “Bilgisayar Haberleşmesi ve Ağ Teknolojileri” ,ISBN:975-6797-00-2 , 2002

[7] <http://hackersitesi.sitemynet.com/Lamer/hacker.htm>

[8] ” Virüsler”, Web adresi: <http://www.bilgisayardershanesi.com/guvenlikvirusler.htm>,2004

[9] **Karaaslan,E.,”Network Güvenliği Te-melleri”**, Web adresi: <http://bornova.ege.edu.tr/~enis/bildiri/sunum/NetworkGuvenligiTe-melleri.ppt>,2004

[10] Takcı,H.,”Veri madenciliği ile Saldırı Tespiti”, Web adresi: <http://www.teknoturk.org/docking/yazilar/tt000117-yazi.htm>,2004

[11] <http://www.bilisimsurasi.org.tr/e-turkiye/docs/guvenlik07042004.doc>,2002

[12] "Virüslerden korunmanın kolay yolları", Web adresi: http://www.turkpoint.com/e-guvenlik/vir_uzak_durun.asp,2004

[13] Arş.Gör.Kodaz, H. , "RSA Şifreleme Algoritmasının Uygulanması" , Bilgisayar Mühendisliği Bölümü,Selçuk University , 2003

[14] "Web Teknolojileri", Web adresi: <http://www.projem.com/hizmetlerimiz/webteknolojileri.php>,2002

[15] "Bilgi Güvenliği Temel Kavramları" seminer notları, Web adresi: <http://seminer.linux.org.tr/seminer-notlari.php>,2004

[16] Arş.Gör. Karaaslan, E. , "Ağ Cihazlarının Güvenliğinin Sağlanma Yöntemleri " , Ege University Network Grubu , 2002

[17] Azaphan,G. , "Virtual Private Network" , Gaziantep University , 2002 , Web adres: http://www1.gantep.edu.tr/~c_dikici/b6.htm(2002)

[18] Yüктаşır,F. , "VPN (Virtual Private Network)" , 26 June 2002 , Web adres: <http://www.mutasyon.net>(26.06.2002)