DİJİTAL SALDIRILAR, EMNİYET GÜÇLERİ AÇISINDAN ÖNEMİ VE KORUNMA YOLLARI

Digital Attacks, and its' Importance to Security Forces and Ways of Protection

Yusuf UZUNAY *

Özet

Gelişen bilişim teknolojilerine paralel olarak, veri iletişimi hayatımızın büyük bir bölümünü kapsayan önemli bir kavram haline gelmiştir. Veri iletişimini temel alan internetin icadı ise globalleşme adına büyük bir adım olmuş , bütün dünyayı tek bir tuş uzaklığına taşımıştır. Bu kadar büyük bir ortamda iletilen veriler üzerinde, çeşitli kötü niyetler de belirmiş ve özellikle emniyet birimleri açısından meydana getirdikleri riskler göz ardı edilemeyecek seviyeye gelmiştir. Veri iletişiminin güvenliğini sağlama konusu, dijital güvenlik kapsamına girmektedir.

Bu makalede ise dijital güvenlik kavramı üç değişik boyutta değerlendirilmiştir. Birinci bölümde dijital saldırılar ve oluşturdukları tehditler; ikinci bölümde bu saldırıların emniyet güçleri açısından önemi ve son olarak da bu tür tehditlerden korunmak için izlenmesi gereken yollar ele alınmıştır.

Anahtar Kelimeler: Dijital Güvenlik, Dijital Saldırı, Saldırı Tespiti

Abstract

In paralel with the devoloping information tecnologies, data transmission has become a significant concept covering a huge part of our life. The invention of internet which is based on data transmission has constituted a breakthrough for the part of globalization and rendered all parts of the world available through a single touch to the keyboard. There emerged ill-intentions concerning the data being transmitted through such a huge means and the risk created by them has reached especially for security forces up to a critical level that can not be ignored. The issue of realizing the security of data transmission falls into the domain of digital security.

In this article, digital security concept is being evaluated in three dimensions. In the first section digital attacks and the threat they create; in the second section the challenge of those attacks for security forces; and finally the ways that should be followed to be protected are being discussed.

Key Words: Digital Security, Digital Attack, Intrusion Detection

* Komiser Yardımcısı , Ankara Emniyet Müdürlüğü.

Giriş

Bilgisayarları birbirine bağlama fikri, ilk olarak 1957 ve 1962 yılları arasında askeri amaçlarla ortaya çıkmış ve müteakip yıllarda ilk ağ ARPA[1] (Advanced Research Project Agency) tasarlanmıştır. Temelde ABD tarafından bir saldırı durumunda, askeri üstlerin birbirleriyle kesintisiz iletişime devam etmesi amacıyla oluşturulan bu ağ, gelişen bilişim teknolojileri ve artan iletişim ihtiyacı ile giderek büyüyerek, 1975 yılında askeri ağ olmaktan çıkmış ve diğer kurumlarda da kullanılarak internetin temelini atmıştır (http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?ARPA:1).

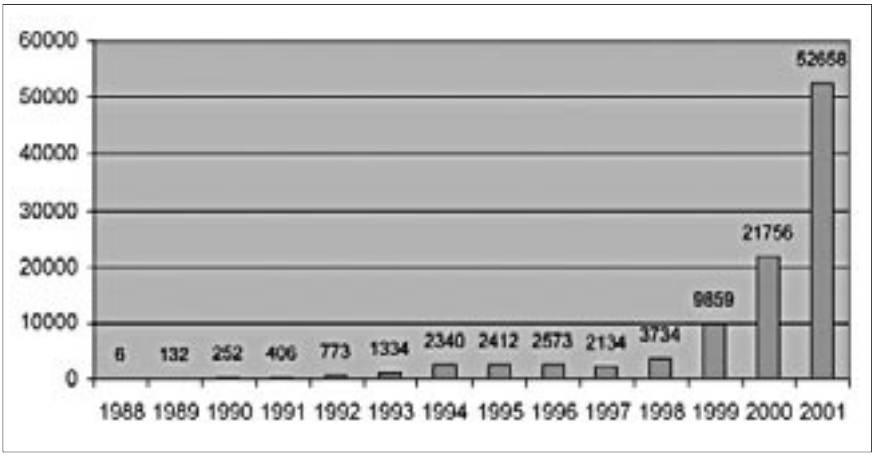
Gittikçe gelişen internet, günümüzde sadece iletişim değil, aynı zamanda büyük bir ekonomi ve reklam pazarı haline gelmiştir. Çok büyük bir kitleye hitap eden bu pazar, şirketler ve kamu kuruluşları başta olmak üzere, bireylere kadar uzanan geniş bir yelpazeyi içerisine almış ve dünyayı tek bir tuş uzaklığına taşımıştır.

İnternet kullanımının giderek artması, bir çok prosedürün dijital ortamda gerçekleşmesini sağlamış ve e-devlet, e-ticaret, e-bankacılık gibi kavramların oluşmasına sebebiyet vermiştir. Bu kavramlar bünyesinde insanların, oturdukları yerden bir çok işlerini yapabilmesi, yüksek derecede öneme sahip bilgilerin de internet ortamına aktarılması sonucunu doğurmuştur.

Bunca değerli bilginin bulunduğu bir ortamda, kısa sürede kötü niyetli kullanıcılar da boy göstermiş ve çeşitli amaçlarla diğer sistemlere karşı saldırılarda bulunmaya başlamışlardır. CERT/CC[2]

Tarafından yapılan istatistiklere göre, bu saldırıların miktarı gün geçtikçe artmaktadır (Şekil 1).

Şekil 1: CERT/CC Tarafından Bildirilen Yıllara Göre Rapor Edilen Saldırı Miktarı



[1] Askeri amaçlı yeni teknolojiler geliştirmekle sorumlu Amerika Savunma Birimi

[2] Computer Emergency Responce Team

Dijital Saldırılar

Kurum ve şahısların sahip oldukları tüm değer ve bilgilere izinsiz erişmek, zarar vermek, maddi/manevi kazanç sağlamak için bilişim sistemleri kullanılarak yapılan her türlü hareket dijital saldırı olarak nitelendirilebilir (http://www.siyahsapka.com / modules .php?name=News&file = article&sid=228). Dijital saldırılar pasif ve aktif saldırılar olmak üzere ikiye ayrılmaktadır.

Pasif Saldırılar

Pasif saldırılar iletişimi gizli olarak dinleme ve göstermeye dayanır. Amaç, aktarılan veriyi bir şekilde öğrenmektir. İki çeşit pasif saldırı tipi mevcuttur. Bunlar, paket içeriklerini görüntüleme ve trafik analizidir.

Paket içeriğini görüntüleme saldırısı, anlaşılması kolay bir saldırı şeklidir. İstenmeyen kişilerin, gönderdiğimiz paket içeriklerini görebilmesi anlamına gelir. Elektronik postada veya transfer edilen bir dosyada, hassas ve önemli bilgiler aktarılıyor olabilir. Bu tür iletişimlerin içeriklerinin başka biri tarafından öğrenilmeye karşı, korunması gerekir.

İkinci pasif saldırı şekli ise, trafik analizidir. Bu, biraz daha ustalık isteyen bir saldırı şeklidir.Şunu düşünelim; aktarılan verileri bir şekilde maskeliyoruz ve veriler hedefe ulaştığında açılamıyor(yani maskesi kaldırılamıyor). Bu tür bir maskeleme, bilişim sistemlerinde kapsülleme (encapsulation) ile sağlanır. Bir yerde kapsülleme kullanılsa bile, saldırganlar hala iletilen paketlerin kalıplarını gözlemleyebilir. Bu kalıptan saldırganın iletişim yapan kişileri, paketlerin frekans ve uzunluklarını tespit etmesi mümkündür. Bu bilgilerden faydalanılarak, mevcut iletişim yapısı hakkında çeşitli detaylar da tahmin edilebilir. Buna trafik analizi denir.

Pasif saldırılar, veriler üzerinde herhangi bir değişiklik yapmaz. Bu nedenle tespit edilmeleri de çok zordur. Fakat yinede bu saldırıların başarılı olması engellenebilir. Pasif saldırılar için yapılabilecek en iyi şey, tespit etmek yerine bu saldırılardan korunacak önlemler almaktır (Stallings, 2002:8).

Aktif Saldırılar

Saldırıların diğer bir çeşidi de aktif saldırılardır. Bu saldırıların özelliği, veri akışı üzerinde değişiklikler yapmaları veya yanlış veriler üretmeleridir. Dört kategoriye ayrılırlar.Bunlar maskeleme, tekrar oynatma, değiştirme ve hizmet aksatma saldırılarıdır.

Maskeleme, bir paketin sanki başka bir paketmiş gibi davranmasına denir. Örnek olarak iletilen bir paketin değiştirilerek, sistem üzerinde daha fazla ayrıcalık elde edilebilecek bir paket haline getirilmesi verilebilir.

Tekrar oynatma, verilerin ve o verilerle ilgili ardışık iletimlerin, yetkisiz etkiler üretmek için pasif olarak yakalanmasıdır. Paketlerin değiştirilmesi, basit olarak verilerin belirli bir bölümünün veya tamamının değiştirilmesi, paketlerin tekrar sıraya sokulması, geciktirilmesi gibi yetkisiz etki sağlamak için yapılan işlemler anlamına gelir. Örnek olarak "Ahmet'e gizli bilgileri okuması için izin ver" mesajının "Mehmet'e gizli bilgileri okuması için izin ver" şeklinde değiştirilmesini verebiliriz.

Hizmet aksatma, iletişim faaliyetlerinin normal kullanımını veya yönetimini engelleme veya kısıtlama anlamına gelir. Bu saldırılar, belirli bir hedefe yönelik yapılır. Örneğin x kurumuna yönelmiş bütün paketlerin önünü kesmek.

Hizmet aksatma saldırısının bir diğer çeşidi de, bütün ağı kesintiye uğratmaktır. Bu da ağın pasif hale getirilmesiyle veya ağ performansını olumsuz etkileyecek derecede çok paket gönderilmesiyle olur.

Aktif saldırılar, pasif saldırıların karakteristik olarak zıttıdır. Pasif saldırıları tespit etmek zor fakat engelleyecek önlemler almak olasıdır. Diğer taraftan aktif saldırılardan tamamıyla korunmak çok zordur.Bu, bütün iletişim faaliyetlerinin devamlı olarak korunmasını gerektirir. Bunun yerine amaç, saldırıları mümkün olduğunca kısa sürede tespit edip sebebiyet verecekleri zararlardan korunmaktır. Tespit etmenin, bu saldırılardan korunma anlamında da yıldırıcı bir etkisi olabilir (Stallings, 2002:8).

Riskler

Dijital saldırıyı gerçekleştiren kişiye ise *saldırgan* diyoruz. Saldırganların oluşturduğu tehdit ve riskleri iki grupta toplayabiliriz. Bunlar; Dahili Risk Unsurları ve Harici Risk Unsurlarıdır.

Dahili Risk Unsurları

Yapılan saldırı istatistiklerine göre inanılanın aksine, saldırıların %70'inin kurum içinden kaynaklandığı tespit edilmiştir. Kurum içindeki riskleri şu şekilde gruplayabiliriz;

a) Bilgisiz ve Bilinçsiz Kullanım: Kurum içindeki birinin herhangi bir art niyeti olmadan, sırf bilgisiz ve eğitilmemiş olmasından kaynaklanan risklerdir. Örnek olarak, internet devamlılığının hayati önem taşıdığı(e-ticaret) bir şirkette, temizlik işçisinin web sunucusunun fişini çekip elektrik süpürgesinin fişini takmasını verebiliriz. Böyle durumlara mahal vermemek için kurumda çalışan bütün işçilere olayın önemini idrak etmelerini sağlayacak konuşmalar yapılmalıdır. (http://www.siyahsapka.com / modules .php?name=News&file = article&sid=228)

b) Kötü Niyet (Bilgi sızdırma, İntikam isteği): İşte halen çalışmakta olan veya işten çıkarılmış kişilerin art niyet barındırmasıyla meydana gelebilecek tehlikeler bu gruba girer. Mesela başka firmayla yakınlığı olan bir işçi, direk kendi şirketinin sunucularına zarar verebilir, şifrelerinizi dışarıya çıkartabilir. Veya İşten çıkartılmış bir kullanıcı, eğer sistemde gerekli kullanıcı ayarları güncellenmediyse, sinirinden kendi hesabını kullanarak sisteme zarar verebilir veya kendi hesabı iptal edilse bile sistemin zaaflarını biliyorsa yine kurum açısından oldukça büyük bir risk taşır. (http://www.siyahsapka.com / modules .php?name=News&file = article&sid=228)

Harici Risk Unsurları

Kurum dışından gelebilecek saldırıların yarattığı tehlikeleri bu başlık altında inceleyeceğiz. Yine iki kısma ayırıyoruz;

a) Hedefe Yönelmiş Saldırılar (Hacker[3], Cracker[4]): Hedefi doğrudan bir yere, kurumdaki bir kişiye olan nefreti, kurumun ismi, kendi maddi menfaatleri gibi çeşitli nedenlerle saldırmak olan saldırganların oluşturduğu tehlikelerdir. Bu saldırganlar, işinde çok iyi olan bilgili hackerlar olabileceği gibi sadece bir kaç yerden öğrendiği bilgileri denemek için saldırı düzenleyen ergenlik çağındaki bir çocuk da olabilir. Birinci sırada söylediğimiz bilgili ve tecrübeli hackerlar, öncelikle sistem hakkında toplayabildikleri kadar bilgi toplar ve daha sonra bir plan dahilinde sisteme saldırırlar.

b) Hedef Gözetmeyen Saldırılar (Virus[5], Worm[6]): Bu saldırıların direk hedefi belli değildir. Sadece bu saldırılara maruz kalacak güvenlik açıklarını barındıran yerlere bulaşırlar. Bunlara en iyi örnek virüsler ve wormlardır.

Dijital Saldırıların Emniyet Açısından Önemi

Dijital Saldırıların emniyet açısından irdelendiği zaman şu zararları meydana getireceği görülür:

a) Kurumsal güven ve imaj kaybı

b) Maddi Zarar

c) Zaman ve emek kaybı

d) Kritik bilgilerin ele geçirilmesi

e) Üçüncü şahıslara yapılabilecek saldırıların mesuliyeti

f) İş ve Hizmet Kesintisi veya yavaşlaması

[3] Sınırlamaları aşmak için yollar keşfetmekten zevk alan kişi; her şeyi özellikle de görünüşte anlamsız detayları, onlardaki gizli tuhaflıkları, yeni özellikleri ve zayıflıkları keşfetmek için derinlemesine incelemeyi seven kimsedir.

[4] Bilgisayar sistemlerini kırarak, zarar vermekten zevk alan kişiler.

[5] Bir veya birden fazla programa kendini kopyalayarak eklenti yapabilen bir program içine gömülmüş kod parçasıdır.

[6] Kendi kendini çoğaltabilen, ağ bağlantısı sayesinde kopyalarını bir bilgisayardan başka bilgisayarlara gönderebilen bir programdır. Bu program gittiği yerde de aynı işlemleri gerçekleştirir ve ayrıca bunun yanında istenmeyen fonksiyonları da çalıştırabilir.

Kurumsal Güven ve İmaj Kaybı

Bir saldırının meydana getireceği zararlardan belki de en önemlisi, kurumsal güven ve imaj kaybıdır. Emniyet birimleri bünyesinde, çeşitli illerin ve başkanlıkların web sayfaları bulunmaktadır. E-devlet kavramının yoğun bir şekilde gündemde olduğu günümüzde, emniyet birimleri de vatandaşa yönelik bazı hizmetleri, internet ortamına taşımıştır. Örnek olarak Ankara Emniyet Müdürlüğü vatandaşlara kolaylık sağlaması açısından pasaport, ehliyet, plaka, ihbar, sanal masa, aranan şahıs gibi hizmetleri web sayfasından[7] online olarak sunmaktadır. Özellikle bu gibi online hizmetler sunan sayfalar, vatandaşlar tarafından oldukça sık ziyaret edilmektedir.

Güvenlik deyince insanların aklına, ilk başta Ordu ve Emniyet güçleri gelmektedir. Bu birimlerde hayati derecede öneme sahip bilgiler de bulunmaktadır. Vatandaşlar ise, bilgilerini bu kurumlara verirken, güvenlik yönünden hiçbir kaygı duymamaktadırlar çünkü bu kurumların temel felsefesi güvenliktir.

Bir taraftan güvenliğin emniyet birimlerinin işi olduğunu iddia ederken, diğer yandan bir gün emniyetteki herhangi bir web sitesinin adresi girildiğinde, yasa dışı bir örgütün propagandasıyla karşılaşılırsa, bu telafisi paralarla ifade edilemeyecek ve vatandaşın polise bakış açısını ve güvenini tamamen olumsuz bir yöne çevirecek büyük bir kayıp olacaktır.

Maddi Zarar

Ağımıza sızmış bir saldırgan veya gönderdiği zararlı kodlar oldukça yüksek miktarlarda maddi zararlara yol açabilmektedirler. Maddi zararları iki boyutta inceleyebiliriz. Bunlar: Doğrudan zararlar ve dolaylı zararlardır.

Doğrudan zararlar, saldırganın doğrudan, sızdığı sistem bileşenlerine verdiği zararlardır. Örnek olarak bios'u[8] yakma kabiliyetine sahip olan Çernobil virüsünü verebiliriz.

Dolaylı zararlar ise saldırganın hedef sistem faaliyetlerini durdurarak, hizmet verememesini sağlamasıyla meydana getirdiği zararlardır. Örneğin internet üzerinden e-ticaret yapan bir sitenin, bir saatliğine internetinin kesilmesi, o firmaya çok büyük miktarda maddi zararlar verebilmektedir.

Zaman ve Emek Kaybı

Saldırıların meydana getireceği bir diğer zarar da, zaman ve emek kaybıdır. Zaman ve emek, karşılığı maddi değerlerle ölçülemeyecek kavramlardır. Bir saldırıdan sonra sistemin eski haline dönmesi aylar, hatta bazen yıllar sürmektedir. Özellikle online hizmetlerin verildiği bir kurumda, internetin çok kısa süreliğine dahi kesilmesi, vatandaşa o kadar süre hizmet verememek anlamına gelir.

[7] www.ankaraemniyet.gov.tr

[8] Basic Input Output System

Kritik Bilgilerin Ele Geçirilmesi

Emniyetin özellikle istihbarat gibi birimlerinde, gizliliği oldukça hassas bilgiler tutulmaktadır. Bu gibi bilgilerin, bir saldırgan tarafından ele geçirildiği düşünülürse, ortaya çok tehlikeli sonuçlar çıkabilir.

Üçüncü Şahıslara Yapılabilecek Saldırıların Mesuliyeti

Yılların geçmesiyle dijital saldırılar ve karmaşıklıkları daha da artarak, günümüzde çok değişik varyasyonlarla karşımıza çıkmaktadırlar. Saldırı izlerinden saldırganlara ulaşmak da, bir o kadar zorlaşmaktadır. Çünkü günümüzde saldırganlar, hedefe doğrudan ulaşmak yerine birden fazla noktayı ele geçirip, oralardan dolaylı olarak saldırmaktadırlar. Bu da, arada hedefe ulaşmak için kurban olarak seçilen bilgisayarları, mesul duruma düşürmektedir. Sistemimizde bulunan güvenlik zafiyetlerinden kaynaklanacak böyle bir olaya maruz kalmak, bizim açımızdan hiç de iyi olmayacaktır. Eğer aksini ispatlayacak sistem kayıtlarını da tutmuyorsak , suçlu durumuna doğrudan kurumumuz düşecektir.

İş ve Hizmet Kesintisi veya Yavaşlaması

Sistemin çalışmasını engelleyecek nitelikte olan saldırılar sonucunda, gerek zarar gören sisteme bağlı yürütülen kurum içi işlemler, gerekirse halka, yine o sistemler kullanılarak sunulan hizmetler duracaktır veya yavaşlayacaktır. Örnek olarak pasaport müracaatlarının internet üzerinden alındığı bir online hizmeti düşünelim. Bilgilerin tutulduğu veritabanı hasar görürse, gerekli veri alınıp işlemler yapılamayacağından dolayı, müracaat eden vatandaşa da zamanında pasaport verilemeyecektir. Veya ağımıza sızan ve amacı internete çıkış bandımızın çoğunu kaplayıp hızımızı düşürmek olan bir kurtçuğu düşünürsek, yine internet hızı düşeceğinden buna bağlı olarak vatandaşın web sayfamızda halledeceği işlerin veya bizim kurum içinden yapacağımız işlemlerin hızı da düşecektir.

Korunma Yolları

Dijital saldırılardan korunma kavramının değişik boyutları vardır. Çünkü güvenlik kavramının sınırı yoktur. Güvenlikte yüzde kavramından söz edilemeyeceği gibi, tamamen güvenli bir sistem oluşturmak da imkansızdır. Bunun için önemli olan, kurumun amaçları ve çalışması doğrultusunda belirli kriterler ve güvenlik öncelikleri belirleyip, bu doğrultuda yapılacak sistematik ve planlı bir çalışmayla, mümkün olabilecek bütün güvenlik önlemlerini almaktır.

Güvenlikte unutulmaması gereken bir diğer husus da, güvenliğin tek bir noktada sınırlandırılmayarak birden fazla noktanın güvenliğinin göz önünde tutulmasıdır. İhmal edilen en ufak bir nokta, sistemi tamamen güvensiz kılabilir.

Şimdi saldırılardan korunmak amacıyla dijital güvenliğimizi nasıl sağlayacağımıza bir göz atalım;

Güvenliğin Boyutları

Güvenliği altı değişik boyutta inceleyebiliriz;

A) Fiziksel Güvenlik

B) Ağ Bazında Güvenlik

C) Bilgisayar Bazında Güvenlik

D) İletişim Bazında Güvenlik

E) Politika Bazında Güvenlik

F) Uzman Personel ve Eğitim

Fiziksel Güvenlik

Güvenliği sağlama yönünde çok çeşitli yöntemler ve düşünceler mevcuttur fakat unutulmaması gereken nokta, bu güvenlik önlemlerini alacağımız yapının temelinin sağlam olmasıdır. Fiziksel güvenlik, dijital güvenliğin en alt basamağında yer alan ve ilk olarak alınması gereken bir önlemdir. Çünkü sistemlere fiziksel olarak erişim çok rahat bir şekilde gerçekleşebiliyorsa, orada diğer güvenlik önlemlerinden söz etmeye gerek yoktur.

Fiziksel güvenlik, kurum için önem arz eden sistemlerin, kilitli bir odada tutulup bu odaya yalnız o sistemlerden sorumlu uzmanların girmesi anlamına gelmektedir. Çünkü bir sisteme fiziksel erişim mevcutsa, o sisteme zarar vermek için ileri düzey bir bilgisayar bilgisine ihtiyaç yoktur. Bir bardak suyu sistemin üzerine boşaltan biri, yapılabilecek saldırıların da en büyüğünü yapmış olur.

Fiziksel saldırılara maruz kalmamak için ağ yapısının da buna uygun olarak düzenli bir şekilde tasarlanmış olması gerekir. Sistemin işleyişini engelleyecek bütün unsurlar, mümkün olduğunca tek bir noktada toplanıp, bu noktaya erişimin devamlı olarak çizelgelerle kontrol edilmesi, ayrıca bu sistemlere erişim hakkına sahip olan kişilerin sorumluluk sınırları, kurumun güvenlik politikasında en ince ayrıntısına kadar belirtilmiş olması gerekir.

Ağ Bazında Güvenlik

Ağ bazında güvenlik, bir ağa yapılabilecek saldırılar göz önünde tutularak, alınabilecek güvenlik önlemlerini anlatmaktadır. Burada önem arz eden nokta, güvenlik olarak alacağımız bütün tedbirlerin birbiriyle tamamen ilişkili olduğudur. Ağ güvenliğini sağlarken, bilgisayar güvenliği konusunda değineceğimiz işletim sistemini düşünmemek çok yanlış olur. Şimdi öncelikle ağ bazında ne gibi önlemler alabiliriz bunlara bir göz atalım;

i. Erişim Denetimi (Güvenlik Duvarı)

ii. İçerik Denetimi (Saldırı Tespit, Virus Tespit, URL[9] Filtreleme)

iii. Ağ aktif cihazlarının güvenliği (Switch, Router)

iv. Güvenliğin Kontrolü (Zafiyet Tarama Sistemleri)

Erişim Denetimi

Erişim denetimi ağ paketlerinin geçişlerinin kontrol edilip, yetkisi olmayanların erişimlerinin engellenmesi anlamına gelir.

Bunu günümüzde en iyi sağlayan sistemler, Güvenlik Duvarı (Firewall) dediğimiz sistemlerdir. Güvenlik duvarı, bilişim literatüründeki anlamı ile iki yada daha fazla ağı birbirinden izole etmek için kullanılan sistem yada sistemler bütünüdür.

Bir güvenlik duvarı, parçalara böldüğü ağ üzerinde bir denetim noktasıdır. Denetim noktası üzerinden akan trafiği inceler ve belirlenen güvenlik politikasına aykırı trafiği durdurur. Ağ bölümleri arasında seçici geçirgenlik sağlar.

İçerik Denetimi

Erişim denetimi mekanizmaları, paketlerin veri olarak içeriklerini kapsamlı bir biçimde inceleyemezler. Bir ip (internet protocol) paketi incelendiğinde, başlık alanındaki bilgiler normal bir bağlantıyı işaret etse de, paketin veri alanı kısmında zararlı kodlar bulunabilmektedir. Bunu önlemek için erişim denetimine ek olarak içerik denetimi yapacak sistemlere de ihtiyaç duyarız.

İçerik denetimi, ip paketlerinin veri alanlarında detaylı incelemeler yapabilme anlamına gelir. Bunu yapan sistemlere örnek olarak Saldırı Tespit Sistemleri, Virüs Tespit Sistemleri ve URL Filtreleme Sistemleri'ni verebiliriz.

a) Saldırı Tespit Sistemleri : Saldırı tespit sistemleri bir bilgisayara veya bilgisayar ağına yapılan saldırıları gerçek zamanda tespit etmeye yarar. Ağ bazındaki saldırıları tespit eden sistemlere ***Ağ Tabanlı Saldırı Tespit Sistemleri (Network Based Intrusion Detection Systems - NIDS)***, tek bir bilgisayar sistemine yapılan saldırıları tespit eden sistemlere ise ***Bilgisayar Tabanlı Saldırı Tespit Sistemleri (Host Based Intrusion Systems - HIDS)*** denir (Dayıoğlu ve Özgit, 2002).

Saldırı tespit sistemleri çalışma mantığına göre ikiye ayrılır;

- Anormallik Tespiti
- Kötüye Kullanım Tespiti

Anormallik Tespiti Modeli: Anormallik tespiti modeline göre çalışan bir saldırı tespit sisteminde, saldırılar önceden sisteme tanıtılmamıştır. Normal ve anormal davranış mantığına göre çalışır. Öncelikle normal koşullar altında belirli bir süre çalıştırılması gerekir. Bu devre, saldırı tespit sisteminin normal davranış olarak tanımlanan kuralları oluşturup, hafızasına alma evresidir. Bu evreden sonra saldırı tespit sistemi normal olarak çalıştırıldığında, kendi hafızasına işlediği normal kavramı dışında bir iletişim gerçekleşirse, anormal bir davranış oldu diye alarm verecektir. Günümüzde bu model, çok sayıda yanlış alarm ürettiği ve normal davranış tanımlama evresinin çok zahmetli ve yeteri kadar saf olmaması gerekçesiyle fazla tercih edilmemektedir.

[9] Uniform Resource Locater

Kötüye Kulanım Tespiti Modeli: Bu modelde saldırılar önceden sisteme tanıtılmıştır. Kötüye kullanım tespiti modelinde çalışan bir saldırı tespit sistemi, devamlı olarak akan ip trafiğini dinler ve paketleri kendi elinde tanımlanmış saldırı kuralları ile karşılaştırır. Eğer aksi bir durum meydana gelirse alarm üretir. Tabiki saldırı kurallarının da devamlı olarak takip edilip güncellenmesi gerekir.

b) Virüs Tespit Sistemleri: Virüs tespit sistemleri de kötüye kullanım tespiti modelinde çalışan saldırı tespit sistemleriyle benzerlik gösterir. Çalıştırıldığı sistem üzerinde, kendine önceden tanıtılmış olan virüs imzalarını arar ve bulduğu zaman alarm verir. Yakalanan virüsü duruma göre temizleme, karantina altına alma gibi özellikleri mevcuttur.

c)URL filtreleme sistemleri: URL filtreleme sistemleri, genellikle lokal kullanıcıları kontrol altına almak için kullanılan sistemlerdir. Bağlanılacak URL'leri kontrol etmemizi sağlar. Bu sistemler sayesinde içerisinde belirli kelimeler geçen web sayfalarına, url adreslerine erişim kısıtlanabilir. Ayrıca kimin hangi saat ve dakikada nereye bağlandığı gibi bilgilerin kayıtları tutulabilir ve iç ağdan dışarıya karşı yapılacak herhangi bir saldırı durumunda bu kayıtlar adli delil olarak kullanılabilir.

Ağ Aktif Cihazlarının Güvenliği

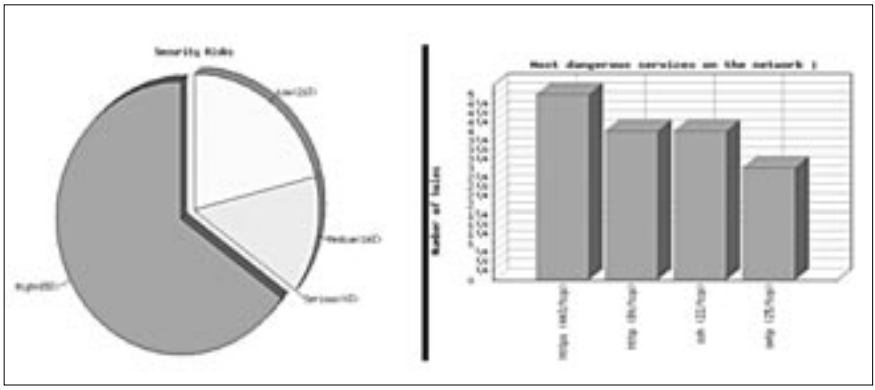
Güvenlik, sadece kullanılan sistemler ve bilgisayarlarla sınırlandırılmamalıdır. İletişim yolu üzerinde bulunan diğer switch, router gibi ağ aktif cihazlarının da güvenliği göz önünde tutulmalıdır. Örnek olarak kurumun web sayfasına giden yol üzerindeki bir routerda bulunan bir zafiyetten yararlanılarak, sayfanın istenmeyen adreslere yönlendirilmesi mümkündür. Bu da bizim açımızdan hoş olmayan sonuçlar doğurur.

Güvenliğin Kontrolü

Sadece belirli güvenlik önlemlerini alıp bununla yetinmek doğru bir güvenlik yaklaşımı olmaz. Kurulan güvenlik yapısı, belirli aralıklarla test edilmelidir. Çünkü her geçen gün yeni bir program ve yeni bir açık rapor edilmektedir. Bunların hepsini teker teker takip etmek, sistem yönetici için oldukça zor bir durumdur. Bunun için güvenlik testi işini sistem yöneticisi yerine yapabilecek sistemler kullanılabilir. Bu sistemlere ***Zafiyet Tarama Sistemleri (Vulnerability Analyzer Systems)*** adı veriyoruz.

Zafiyet Tarama Sistemlerini kendi ağınıza karşı çalıştırdığınız zaman, veritabanında kayıtlı olan saldırıları teker teker gerçekleştirerek, sisteminizin bu saldırılara karşı zaafları olup olmadığını tespit eder ve şekil 2'de de görüldüğü gibi sisteminizle ilgili çok detaylı ve grafiksel kayıtlar üretebilir. Siz de bu kayıtları inceleyerek sisteminizdeki güvenlik açıklarını kapatacak girişimlerde bulunabilirsiniz.

Şekil 2 : Güvenlik Açıklarını Gösteren Zafiyet Tarama Sistemi Kayıtları



Bilgisayar Bazında Güvenlik

Dijital güvenliğin başka bir basamağı da bilgisayarların kendi sistemlerinin güvenliğidir. Bunu değişik maddeler altında inceleyebiliriz;

- İşletim Sistemi Güvenliği
- Kod Güvenliği
- Erişim Şifreleri
- Yedekleme

İşletim Sistemi Güvenliği

Bilgisayar güvenliğinde ilk olarak incelenmesi gereken başlık, bilgisayar üzerinde çalışan işletim sisteminin güvenliğidir. İşletim sistemleri, kullanıcının bilgisayarla iletişim kurmasını sağlayan bir ara yüzdür. Çalıştıracağımız bütün programlar işletim sistemi üzerine inşa edilerek uygulanır. İşletim sisteminde meydana gelecek bir açık, diğer bütün uygulamaları da tehlikeye atar. İşletim sisteminin güvenliği için dikkat edilecek noktalar şu şekildedir;

• İşletim Sistemlerinin ve işletim sistemleri üzerinde çalışan programların en son yamaları, takip edilip zamanında güncelleştirilmelidir.

• İşletim sisteminin varsayılan kurulum ayarlarına dikkat edilmelidir. Her zaman için güvenlik ve kolay kullanılabilirlik birbirine zıt yönde ilerler. Varsayılan kurulumlarda ise kullanılabilirlik ön planda olduğu için işletim sistemi ilk defa kurulduğunda, gerekli ayar düzeltmeleri yapılmalıdır.

• İşletim sistemi üzerinde çalışan her program, açık olan her port yeni bir zafiyet tehlikesi anlamına gelmektedir. Bu yüzden gereksiz olan bütün programlar sonlandırılmalı, sadece işimizi gören portlar dışarıya açık olmalıdır.

Kod Güvenliği

Kod güvenliği, işletim sistemi ve üzerinde çalışan programların kodlarından kaynaklanabilecek zafiyetleri önleme adına alınan önlemlerdir.

Öncelikle işletim sisteminin kodları, güvenlik açısından oldukça hassas bir konudur. Güvenliğin son derece önem arz ettiği yerlerde kaynak kodu açık olan işletim sistemlerini kullanmakta fayda vardır. Çünkü böyle bir işletim sisteminin kodları arasında zararlı kodlar olup olmadığı kolayca tespit edilebilir.

İşletim sistemi üzerinde çalışan programların kodları, özenle incelenmeli veya güvenilir yerlerden imza ve bütünlük kontrolü yapılmalıdır. Eğer kendimiz bir program yazacaksak öncelikle programı, bütün güvenlik önlemlerini göz önünde bulundurarak çok iyi bir şekilde planlayıp daha sonra kod yazma aşamasına geçmeliyiz. Bunu yaparken sistem güvenlik uzmanı ile programcının ortak çalışması gerekmektedir.

Erişim şifreleri

Dikkat edilmesi gereken bir diğer nokta da, önemli makinelere erişmek için kullandığımız şifrelerin çok iyi seçilmesidir.

İyi bir şifrenin özellikleri şu şekilde olmalıdır;

• Sadece bir kişi tarafından bilinmelidir.

• Herhangi bir yere yazılı olmamalıdır.

• Birden fazla yere aynı şifre verilmemelidir.

• Ad, soyad, araba plakası, doğum tarihi gibi kolay tahmin edilebilecek kişiye özel şifreler verilmemelidir.

• Şifre anlamlı kelimelerden, sıralı harf veya sayılardan oluşmamalıdır.

Örnek: Emniyet, polis, 123456, qwerty

• Altı karakterden daha uzun ve içerisinde büyük-küçük harf, sayı ve özel karakterler olmalıdır.

• Şifreler devamlı sabit kalmamalı belirli aralıklarla değiştirilmelidir.

(http://consult.cern.ch/writeup/security/security_3.html)

Yedekleme

Herhangi bir saldırı veya fiziksel hasar anında, veri kaybetmeden sistemi en kısa sürede tekrar eski haline döndürmek için yedekleme mutlaka şarttır. Özellikle kritik bilgilerin tutulduğu sunucularda sistemin yedeğini devamlı olarak alacak yedekleme sistemlerinin kurulması gerekir.

Yedeklemede unutulmaması gereken en önemli nokta, zaman zaman sanki

sistem gerçekten çökmüş gibi yedeklerden geri dönüş tatbikatlarının yapılmasıdır. Bu genellikle göz ardı edilen ama oldukça önemli olan bir konudur.

İletişim Bazında Güvenlik

İletişim bazında güvenlikten kasıt, hatlar üzerinde gidip gelen verilerin güvenliğidir. Eğer veriler, herhangi bir işleme tabi tutulmadan direk düz metin (clear tex) olarak gönderilirse, yol üstündeki biri tarafından çok rahat bir şekilde dinlenilerek (sniff) ele geçirilebilir. Örnek olarak emniyette kritik bir birimde çalışan birinin mail kullanıcı adı ve şifresi hat dinlenilerek öğrenilebilir ve bundan sonra bu kişiye mail yoluyla gelen bütün bilgiler çok rahat bir biçimde okunabilir.

Bu şekilde bir saldırıya mahal vermemek için kritik öneme sahip bilgilerin, şifreli bir biçimde aktarılması gerekir. Bunu yapan değişik iletişim şifreleme teknikleri ve programları mevcuttur. Örnek olarak uzaktan erişimler için SSH (Secure Shell), sunuculara gelip giden trafiği şifrelemek için SSL (Secure Socket Layer), iki faklı ağın veya iki farklı noktanın birbiriyle güvenli iletişim için VPN (Virtual Private Network) sistemleri kullanılabilir.

Politika Bazında Güvenlik

Güvenlik açısından yapılması gereken işlem basamaklarından önemli olan bir tanesi de, güvenlik politikasının oluşturulmasıdır. Güvenlik politikası, kuruluşun yapısı göz önünde bulundurularak güvenlikle ilgili bütün riskler, önlemler, saldırı anında ve sonrasında yapılacak işlemlerin belirlenmesidir. Güvenlik politikası mutlaka ve mutlaka dökümente edilip, kuruluşun yönetiminde söz sahibi olan kişilere onaylatılmış bir biçimde herkesin görebileceği bir yere asılmalıdır.

İyi Bir Güvenlik Politikasının Özellikleri

• Güvenlik politikası öncelikle uygulanabilir olmalıdır. Politika kullanıcıların ve sistem yöneticilerinin eldeki olanaklarla uyabilecekleri kurallar ve ilkelerden oluşmalıdır.

• Politika yeteri düzey yaptırım gücüne sahip olmalıdır. Alınan güvenlik önlemleri ve politikayı uygulayan yetkililer yaptırımları uygulayabilecek güçle donatılmalıdır.

• Politika kapsamında herkesin sorumluluk ve yetkileri açıkça tanımlanmalıdır. Kullanıcıların sistem yöneticilerinin ve diğer ilgililerin, sisteme ilişkin sorumluluk ve yetkileri, kuşku ve çelişkilere yer bırakmayacak bir biçimde açıklanmalıdır. Gerekli durumlarda istisnalar ve alternatif uygulamalar açıklanmalıdır (Dayıoğlu ve Özgit, 2002).

Uzman Personel ve Eğitim

Sistemleri sadece kurup, o an için güvenlik önlemlerini almak tabiki yeterli değildir. Günümüzde her geçen gün yeni bir güvenlik açığı rapor edilmektedir. Bunun için unutulmaması gereken bir diğer husus da, bu sistemlerin güvenli bir şekilde devamlılığını sağlamaktır. Burada insan faktörü devreye girmektedir. Diyelim ki bir yerlerden uzman getirip bir seferliğine güvenli bir sistem kuruldu, eğer bu sistemden anlayan, güvenlik politikasını belirtilen sistematik ve düzende uygulayabilecek, sistemi devamlı kontrol altında tutup gerektiğinde ivedi müdahaleler yapabilecek uzman personel yoksa, sisteminizin güvenli bir şekilde işleyişine devam edebileceğini söylemek çok zor olacaktır.

Yapılabilecek en iyi şey, kurum içinden belirli sayıda personeli, sistem güvenliğini devamlı olarak takip edebilecek ve yönetebilecek seviyeye getirecek uzmanlık eğitimleri aldırıp, sırf güvenlik konusuyla ilgilenmelerinin sağlanmasıdır.

Ayrıca sadece teknik personeli değil, bu sistemlerden faydalanacak bütün personele de zaman zaman sistem güvenliği açısından dikkat edilmesi gereken hususlar konusunda, eğitimlerin verilmesi gerekir.

Sonuç

Bilişim güvenliği, çoğu zaman göz ardı edilen ama aslında gerçekleştirdiğimiz bütün bilgi aktarımına ve bu aktarım üzerinde oluşturduğumuz bütün uygulamalara temel teşkil eden çok önemli bir konudur.

Gelişen teknolojiyle birlikte, bilişim sistemlerine karşı yapılan saldırıların sayısı da gün geçtikçe artmaktadır. Dijital saldırıların meydana getireceği kayıplar özellikle emniyet güçleri gibi gizlilik ve güvenliğin üst düzeyde olduğu kuruluşlar için çok kritik ve hassas bir öneme sahiptir.

Bu konuda alınabilecek önlemler mevcuttur. Bu önlemler, dijital güvenlik kavramı kapsamına girer. Dijital güvenliğimizi sağlamak için bir çok metod vardır ama unutulmaması gereken bir diğer nokta hiçbir zaman yüzde yüz güvenliğin mümkün olmadığıdır. Önemli olan alınabilecek bütün güvenlik önlemlerini alıp, mevcut riskleri en aza indirgemektir.

Dijital güvenlik, süreklilik isteyen bir kavramdır. İhmal edilen küçük bir nokta veya güncellenmesi ertelenen bir program, telafisi mümkün olamayacak sorunlar yaratabilir. Bu yüzden gerekli politikaların belirlenip, planlı ve programlı bir şekilde uygulanması gerekir. Ayrıca bu politikaları uygulayacak yeterli bilgi düzeyine sahip, eğitimli personele ihtiyaç vardır.

Unutulmamalıdır ki; emniyet hizmetlerinin amacı, halkın refahını ve yaşam standartlarını korumaktır. Bu görevi muvaffakiyet ile sürdürmek için karşılıklı güvene ihtiyaç vardır. Bu güven ortamında, emniyet hizmetlerinin daha iyi görev yapması ve halka daha iyi hizmet götürüp toplum refahını sağlaması için tek muhtaç olduğu şey, başarıya götürecek her türlü yöntemi deneyip, günümüz teknolojisinden geri kalmamaktır. Teknolojiye, bilime ve eğitime yapılan yatırım geleceğe yapılan yatırımdır.

Kaynakça

Dayıoğlu, Burak. "İletişim Ağlarında Güvenlik", http://www.dikey8.com/modules.php?op=modload&name=NS-Documents&file=index.

Dayıoğlu, Burak ve Özgit, Atilla, (2002), Bilişim Güvenliği Kurs Notları, ODTU, Mart-Nisan.

İnternet'in Kısa Tarihi, http://www.romannet.net/tr/domain/history.htm.

Özavcı, Fatih, "Bilgi Güvenliği Sistemlerine Giriş", http://www.siyahsapka.com/modules.php?name=News&file=article&sid=228.

Stallings, William, (2002), Network Security Essentials 2/E, New Jersey: Prentice Hall.

http://consult.cern.ch/writeup/security/security_3.html

http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?ARPA

http://www.core.gen.tr/sunumlar/Senlik_1/hkrfsf/img8.html

STRESS ON POLICE OFFICER'S AND STRESS MANAGEMENT

Poliste Stres ve Stres Yönetimi

Mehtap YEŞİLORMAN*

Özet

Polislik mesleği, en stresli mesleklerden biri olarak kabul edilmektedir. Bu mesleğe mensup kimseler; iş yükünün fazlalığı, çalışma koşulları ve güvenlik tehlikesi faktörlerinin etkisiyle, yoğun stres altında çalışmaktadırlar. Polis stresi; işin tabiatından kaynaklanan faktörlerin dışında, çeşitli stres kaynaklarına sahiptir. Bu çalışmada poliste strese neden olan stres kaynakları; işin niteliğine, bireysel özelliklere, toplumsal çevre faktörlerine ve kullanılan araç ve gereçlerin niteliğine dayalı stres kaynakları olmak üzere dört grupta incelenmiştir. Çeşitli faktörlerin etkisiyle gelişen örgütsel stresin azaltılmasında yararlanılabilecek stratejiler, aynı şekilde bireysel, örgütsel ve toplumsal stratejiler biçiminde sınıflandırılmıştır. Son kısımda ise, polisler üzerindeki baskının azaltılması için danışmanlık hizmetlerine ilişkin birtakım öneriler sunulmuştur.

Anahtar Kelimeler: Stres, Örgütsel Stres, Polis Stresi, Poliste Stres Yönetimi.

Abstract

It is accepted that police profession is one of the most stressful profession. The people working in this profession are under stress because of overloaded responsibility of a duty, working conditions and security danger. The stress of police has not only natural effects but also several stress resources. In this contribution stress on police is categorised into four groups. These are qualification of the job, individual features, environmental social effects and means used. The strategies, which are able to used to reduce organisational stress as a result of several effects, are divided as individual, organisational and social strategies. Finally, several suggestions are presented about consultation services for reducing pressure on policeman.

Key Words: Stress, Organisational Stress, Police Stress, Coping with Stress on Police Officers.

* Yard. Doç. Dr., Fırat Üniversitesi Fen-Ede. Fak. Sosyoloji Böl.
e-mail: myesilorman@yahoo.com

ETNİK ÇATIŞMA SONRASI KURULAN POLİS BARIŞ MİSYONLARINI BEKLEYEN SORUNLAR

The Challenges Facing the Police Missions Established After Ethnic Conflict

Ali Dikici*

Özet

Günümüzde çokuluslu polis barış koruma misyonları başta eski Yugoslavya sınırları içinde kalan ülkelerde olmak üzere dünyanın her tarafına yayılmış durumdadır. Bu misyonların temel hedefi çatışmadan çıkan bu ülkelerde düzeni tekrar sağlamak, bu amaçla da siyasal kurumlara tekrar işlerlik kazandırmaktır. Etnik çatışmaların yaşandığı ülkelerdeki polis teşkilatlarının iyileştirilmesi, huzurlu ve üretken bir toplumun oluşturulmasında en önemli unsurlardan birini teşkil etmektedir. Bu makalede etnik çatışma sonrası polislik açısından dört önemli kavram tartışılmaktadır. -Polis kültürü, demokratik katılım, polisin görev yaptığı politik çevre ve son olarak da halkın güvenlik güçlerini algılama tarzı. Bu makalede ayrıca, istikrarlı ülkelerdeki mevcut polislik anlayışının, etnik olarak bölünmüş bu tip ülkelerde, güvenliği tehdit eden bazı unsurlarla mücadelede nasıl tatbik edilebileceği de ele alınmaktadır.

Anahtar Sözcükler: Polis, Polis-Halk İlişkileri, Etnik Çatışma, Etnik Gruplar, Çatışmanın Çözüme Kavuşturulması, Polis Reformcuları.

Abstract

Multilateral peace-keeping missions are pervasive in today's world, particularly in ex-Yugoslavian Republics. The goal of these missions is often to re-establish order, one way to accomplish this is to rebuild political institutions. Rehabilitating policing agencies within failed states is an essential component to establishing a peaceful and productive society. This paper discusses four issues that are important to policing after ethnic conflict. -Police culture, democratic participation, the political environment the police operate within, and the perceptions of the population about law enforcement. This paper also addresses the current perspectives on policing in stable states to some of the challenges facing creating law enforcement structures in unstable and often ethnically divided states.

Keywords: Police, Police-Public Relations, Ethnic Conflict, Ethnic Groups, Conflict Resolution, Police Reformers

* Emniyet Amiri, AGİT Makedonya Misyonu.