Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Yöntemleri

Enis KARAARSLAN, Gökhan AKIN, Hüsnü DEMİR

ULAK-CSIRT
enis.karaarslan@ege.edu.tr, gokhan.akin@itu.edu.tr, hdemir@metu.edu.tr

Özet: Zararlı yazılımlar (trojan, virus, worm vb), makinelerde sorun yaratmaları dışında, büyük kurumsal ağlarda yarattıkları trafik ile ağ sistemlerinin yavaşlamasına ve hatta devre dışı kalmasına yol açabilmektedir. Bu bildiride, bu güvenlik sorunu ile savaşmak için gerekli önlemler anlatılacaktır. Bu önlemler alındığında, bilgi sistemleri daha tutarlı ve sağlam bir şekilde çalışacaktır.

Anahtar Kelimeler: Ağ Yönetimi, Kampüs Ağları, Güvenlik, Zararlı Yazılım, Çok Katmanlı Güvenlik.

Defense Against Malware On Enterprise Networks

Abstract: Malware (trojan, virus, worm, etc) causes problems on personal computers, but also causes slow down and break down on network systems in enterprise networks. In this paper, necessary precautions to fight with this security problem will be explained. The information systems will work more stable if these precautions are taken.

Keywords: Network Management, Campus Networks, Security, Malware, Multi Layer Security.

1. Giriş

İngilizce "malicious software" in kısaltılmış hali olan malware, yani zararlı yazılımlar çeşitli yollar ile bir bilgisayara bulaşıp, bulaştığı bilgisayar ve çevresine zarar vermesi için yazılmış programlardır. Zararlı yazılımlar (trojan/virus/worm gibi) bilgisayarlarda sorun yaratmaları dışında, kurumsal ağlarnda yarattıkları yoğun trafik ile bant genişliğin doldurulmasına ve ağ cihazlarının işlemci güçlerinin boşuna harcanmasına sebep olmaktadırlar. Bunlardan dolayı hattın devre dışı kalmasına bile yol açabilmektedirler.

Zararlı yazılımlar aşağıdaki zayıflıklardan yararlanarak sistemlere bulaşmaktadır:

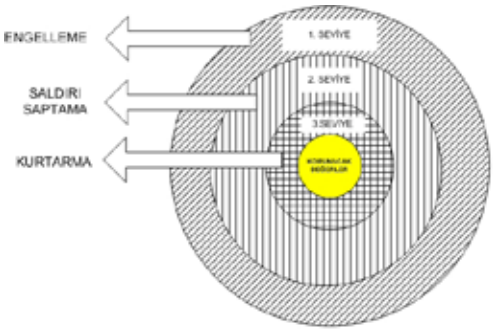
- İşletim sistemindeki veya işletim sistemi üzerinde çalıştırılan çeşitli yazılımlarda bulunan güvenlik açıkları,Kullanıcının bilgisayarına basit şifre ataması,
- Kullanıcının harici bir kaynaktan (eposta, sohbet yazılımları...vs) den gelen eklentileri /yazılımları kontrolsüz şekilde çalıştırması,
- USB ve benzeri ara birimlerden bağlanan hafıza ve sabit disk cihazlarında bulunan otomatik çalıştırma betiğine gizlenen kötü yazılımın, kullanıcının farkında olmadan çalışmasıdır.

Kampüs ağlarında, bu konuda ne tür önlemler alınabileceğini üç ana başlıkta incelememiz mümkündür:

- Kurumsal politika ve bilinçlendirme çalışmaları
- Makinelerde alınabilecek temel önlemler
- Ağda alınabilecek temel önlemler

Güvenlik için bu süreçleri tanımlarken, farklı ve birbirini tamamlayan işlevlere ait çok katmanlı güvenlik sistemlerinden söz edilmektedir. Katman yapısını, kurulacak güvenlik sistemlerinin özelliğine göre farklılaştırmak ve her katmanda alt katmanlar kullanmak mümkündür. Genel olarak üç katmandan oluşan bir yapıdan söz etmek mümkündür. Bu genel model Şekil 1'de gösterilmiştir. Katmanlar aşağıdaki gibidir [1], [2]:

- **İlk katman - Engelleme:** Zararlı yazılımların bulaşmasını ve yayılmasını engellemek.
- **İkinci katman - Saptama:** Bulaşmış bilgisayarları saptamak.
- **Üçüncü katman - Kurtarma:** Bulaşmış bilgisayardaki etkilerin temizlenmesi ve bu bilgisayarların aşkalarına bulaştırmasına ve ağa zarar vermesini engellemek



Şekil 1: Çok Katmanlı Güvenlik Modeli

2. Kurumsal Politika ve Bilinçlendirme Çalışmaları

Kurumsal kullanım politikaları tüm yerel ağlarda olmazsa olmaz bir gereksinimdir. Bu gereksinimi karşılayacak pek çok taslak İnternet'te bulunabilmektedir. ULAK-CSIRT Güvenlik Politikaları sayfası (http://csirt.ulakbim.gov.tr/politika/) buna örnek olarak verilebilir. Bu taslaklar yasalara ve kuruma uygun hale getirilerek uygulanabilir.

İşletim sistemi sayısının fazla olması ve hepsine kurum tarafından destek verilmesinin zor olmasında dolayı kurum politikası dahilinde; kullanıcılar kurumun belirlendiği işletim sistemlerinden birini kullanmaya yönlendirmelidir. Bu konuda bir alternatif olarak açık kaynak kodlu işletim sistemlerinin ele alınması yararlı olabilecektir. Bunlardan GNU/Linux başı çekmektedir. Pardus işletim sisteminin son yıllardaki başarıları da dikkate değerdir.

Bunun yanı sıra kurumlar, anti-virus yazılımı kullanımı, şifre belirlenmesi gibi başlıkları da politikaları dahilinde belirtmelidir. Belirlenen işletim sistemleri ve diğer politikalara göre kullanıcıların kötü yazılımlardan korunabilmeleri için gereken eğitimlerin hazırlanması önem arz etmektedir. Bu eğitimler, belli seviyelerde ve devamlı olmalıdır. Eğitimde devamlılığı sağlamanın ve maliyeti indirmenin en yeni yöntemlerinden biri de teknolojiyi devreye sokmaktır. Verilen eğitimlerin video kaydına alınması, demo koruma uygulamaları yapılması, çeşitli açık kaynak kodlu yazılımların kullanımlarının anlatılması gibi örnekler verilebilir.

Kullanıcı bağlantı sorunu yaşadığında danıştığı mekanizmalara zararlı yazılım bulma/koruma yöntemleri de eklenmelidir. Mesela; yavaşlıktan şikayet eden bir kullanıcıya virüs taraması yapması konusunda uyarı gönderilmesi genel bir uygulamadır. Ama bu uygulamayı nasıl

yapması gerektiği de ayrıntılı olarak kurumsal politikalarda belirtilmelidir.

Özel olarak hazırlanmış alan adı sunucusu kurularak kullanıcıların bu sunucuyu kullanmasını sağlaması önemli önlemlerden biridir. Karadelik DNS yapılandırması olarak da adlandırılan bu teknik yapılandırmanın en önemli kısmı kurumsal olarak bu politikayı dikte etmektir.

Farkındalık yaratmak için kullanıcıların İnternet'i ücretsiz kullanmadığını bilmesi gerekmektedir. Gereksiz indirdiği pek çok dosyanın esasen bir maliyeti olduğu kullanıcılara anlatılmalıdır. Çeşitli vesilelerle bu maliyetler kullanıcılara aktarılmalı ve ağın kurumun amaçlarına uygun kullanılması gerektiği hatırlatılmalıdır. Kampüs ağları örneğinde, amacın eğitim ve araştırmanın teşviği olduğu belirtilmelidir. Bu dosyalardan kaynaklanan zararlı yazılım sorunlarının; bilgi işlem birimlerine ve kendilerine kaybettirdiği zaman, mümkünse parasal olarak ifade edilebilmelidir.

Son olarak da kurumsal politikaların uygulanması ve bu uygulamanın denetlenmesi gereklidir. Bu denetleme, ağın büyüklüğüne ve personel sayısına göre değişmektedir. Kurumsal politikalara uyulmaması durumundaki yaptırımların da belirlenmesi gereklidir.

3. Makinelerde Alınabilecek Temel Önlemler

Makinelerde alınabilecek temel önlemler aşağıdaki gibidir:

- Güvenlik yamalarının sürekli uygulanması: Örneğin, Microsoft işletim sistemi ile çalışan bilgisayarın en son çıkmış "service pack" ile kurulması, (Şu an için XP işletim sistemi için son "service pack" SP2'dir.) Bunun dışında kalan güvenlik yamalarının güncelleme web sayfasından tamamlanması veya otomatik güncelleme ayarlarının her bilgisayarda yapılması. Açık kaynak kodlu işletim sistemlerinde yum, apt ve benzeri güncelleme yazılımları ile gereken güncellemelerin yapılması,

- Zararlı yazılımların mümkün olduğunca etkinliğini azaltmak için, kurumsal ağlarda bu yamaların merkezi bir makineye çekilmesi ve buradan diğer makinelere dağıtılmasını sağlayan yama yönetimi sistemleri de kullanılmalıdır.[5] Bu aynı zamanda hangi makinelerde yamaların geçildiğinin takibi açısından da önemlidir. Microsoft "Active directory" kullanılan ortamlarda, sistemlerin domain yöneticisi üzerinde kurulu SUS'dan (Smart Update Services) otomatik güncelleme alması sağlanabilir. "Active directory" olmayan ortamlarda, yine de bu tür bir hizmetin çalışmasını sağlayan çeşitli ücretli yazılımlar bulunmaktadır. Tabii ki bu tür sistemlerin çalışması için her makineye tek tek kurulmaları gerekecektir [5]. Kısıtlı haklarla kullanılabilmesi ve yönetilmesi kolay olan açık kaynak kodlu Linux, Unix, BSD benzeri sistemlerin tercih edilmesi,

- İşletim sistemlerinde gereksiz tüm servislerin kapalı olması, (Bazı açık kaynak kodlu işletim sistemleri bu şekilde gelmektedir.)

- Kurumun, kullanıcılarını antivirüs yazılımı bulundurmaya teşvik etmesi ve bunların güncel tutulması için gerekli mekanizmaları devreye alması. Bu konuda gereken bilgilendirmeyi yapması,

- Zararlı yazılımların bulaşma yöntemlerinden olan İnternet tarayıcısı seçimine göre, gereken güvenlik ayarlarının ve yamaların sürekli yapılması, (Kurumlar, çeşitli tarayıcıları takip ederek kullanıcılarına güvenli olduğunu düşündüğü tarayıcıyı önerebilir ve bu tarayıcının güvenlik ayarlarını ve gerekli güncellemelerini kullanıcılara ulaştırabilirler. Ayrıca kullanılan tarayıcıların üzerine eklenebilecek eklentiler sayesinde güvenlik arttırılabilmektedir. Mesela; "NoScript" yazılımı

bu konuda çok başarılı bir yazılımdır.)

- Kişisel güvenlik duvarı, IDS/IPS yazılımlarının kullanılmasının teşvik edilmesi. (Örneğin Windows Personal Firewall, Zonealarm, iptables, PF, vb.)

- Windows SP2 ile bir kullanıcının ve/veya IP adresinin ne kadar bağlantı oluşturabileceğinin denetlenmesi sağlanabilmektedir. Saniyedeki paket sayısını (PPS) düşürmek için her bağlantıdan en fazla ne kadar paket geçeceği şekillendirilebilir. Bu sayede, kullanıcıdan habersiz olarak zararlı yazılımların oluşturulan bağlantı sayısını yükseltmesi ve sınırı doldurması durumunda, kullanıcının erişiminin yavaşlaması ve durması söz konusudur. Kullanıcı bağlanamayıp ağ/güvenlik birimine başvurması durumunda sorunlu bilgisayar tespit edilmiş olur.

4. Ağda Alınabilecek Temel Önlemler

Ağda alınabilecek önlemler Tablo 1'de gösterilmiştir. Ağda alınabilecek önlemleri dört ana başlıkta sınıflamak mümkündür:

- L2 Cihazlar ile Alınabilecek Önlemler
- L3 Cihazlar ile Alınabilecek Önlemler
- Güvenlik Cihazları ile Alınabilecek Önlemler
- Diğer Sistemler ile Alınabilecek Önlemler

4.1. L2 Cihazlar ile Alınabilecek Önlemler

OSI'nin 2. katmanında çalışan yerel ağ cihazlarında alınabilecek önlemler aşağıdaki gibidir:

- MAC Adresi Bazında Güvenlik
- 802.1x Tabanlı Kimlik Tanımlama
- Broadcast/Multicast Sınırlandırması

4.1.1. MAC Adresi Bazında Güvenlik

Ağa kontrolsüz bilgisayar erişimini engelleyerek, kötü yazılım bulaşmış bir bilgisayarın tespiti daha kolaylaşmaktadır. Bu amaçla kullanılan tekniklerden bir tanesi port bazında MAC adresi güvenliğidir. Günümüzde zararlı yazılımlar bulaştıkları bilgisayarların tespitini zorlaştırmak için IP adreslerini ve MAC adreslerini bile değiştirebilmektedirler. Bu teknik ile MAC adreslerini değiştirmeleri durumunda ağ erişimleri duracak ve loglama sistemi ile yeri tespit edilebilecektir.

AĞDA ALINABİLECEK ÖNLEMLER	Birinci Katman *Bulaşmasını Engelleme*	Ikinci Katman *Bulaşmış Sistemi Saptama*	Üçüncü Katman *Kurtarma ve Etkileri Azaltma*	Kaynak No
4.1. L2 Cihazlar ile Alınabilecek Önlemler				
4.1.1. MAC Adresi Bazında Güvenlik		X	X	6
4.1.2. 802.1x Tabanlı Kimlik Tanımlama	X	X		7,8
4.1.3. Broadcast/Multicast Sınırlandırması		X	X	9
4.2. L3 Cihazlar ile Alınabilecek Önlemler				
4.2.1. VLAN Bazlı Güvenlik Çözümleri	X		X	10
4.2.2. Erisim Listeleri Alınabilecek Çözümler	X	X	X	11,12,13
4.2.3. QoS ile Bandgenişliği Sınırlaması			X	14,15
4.2.4. Yeni Nesil Güvenlik Çözümleri		X	X	16,17
4.3. Güvenlik Cihazları ile Alınabilecek Önlemler				
4.3.1. Firewall (Güvenlik Duvarları)	X	X	X	18
4.3.2. Antivirüs Geçitleri	X	X	X	19
4.3.3. IDS/IPS Sistemleri	X	X	X	20
4.4. Diğer Sistemler ile Alınabilecek Önlemler				
4.4.1. Saldırgan Tuzağı Ağları (Honeynet)		X		21,22
4.4.2. Merkezi Log Kontrolü		X		23,24,25
4.4.3. Trafik Analizi		X		4, 26
4.4.4. DNS Sunucu			X	13,27,28,29
4.4.5. Arp Saldırılarını Tespit Edebilen Uygulamalar		X		30

Tablo 1. Ağda Alınabilecek Önlemler

Yönetilebilir anahtarlama cihazları ile bu önlem alınabilmektedir. Aşağıda Cisco marka anahtar cihazları için örnek konfigürasyon bulunmaktadır. Ayrıntılı bilgi için bkz [6].

```
Interface <int adı> <int.no>
switchport port-security
switchport port-security maximum
<toplam PC sayısı>
switchport port-security violation
<protect | restrict | shutdown>
switchport port-security mac-address
<PC'nin MAC adresi>
```

4.1.2. 802.1x Tabanlı Kimlik Tanımlama

IEEE 802.1X, port tabanlı ağ erişim kontrol standardıdır. Kullanıcı bilgileri (kullanıcı adı, parola ve bazı özel durumlarda MAC adresi) yardımı ile ağa bağlanılmasına izin verilmesini sağlar. Kullanıcı doğrulama sırasında EAP (extensible authentication protocol-RFC2284) yöntemi kullanılır [7].

802.1x için ağ altyapısındaki yönetilebilir (switch, kablosuz ağ cihazı gibi) cihazlarda gerekli ayarlar yapılmalı ve kullanıcı bilgilerini denetleyip gerekli düzenlemeleri yapacak bir sunucu bulundurulmalıdır. Ayrıntılı bilgi için bkz [8].

Bu protokol sayesinde, sadece kurumun kullanıcıları izin verilen ağlara bağlanılacaktır. Güvenlik açısından, misafir bilgisayarların ayrı bir VLAN'a bağlanması ile yetkileri, ulaşabilecekleri ağlar ve kullanacakları iletişim kapıları kısıtlanabilecektir. Bu da zararlı yazılımların dağılmasını kısıtlayabilecektir.

Kullanıcının bu tür bir yöntemle sisteme bağlanması anında, kişisel antivirüs yazılımını ve imza güncelliğini denetleyen ticari sistemler de bulunmaktadır. Böylece kullanıcı, kurumun antivirüs yazılımını kurana ve/veya güncel imzaya sahip olana kadar, sistem tarafından ayrı bir sanal ağa alınacaktır. Ancak gerekli yüklemeler gerçekleştikten sonra kendi ağına bağlanabilecektir. Bu da, zararlı yazılımların etkin olmasını engelleyecek yöntemlerden birisidir.

4.1.3. Broadcast/Multicast Sınırlandırması

DoS veya DDoS saldırılarının bir kısmı broadcast (genel yayın) adresi üzerinden yapılmaktadır. Bu tür saldırıların etkisinin azaltılması için broadcast sınırlaması yapılmalıdır. Broadcast düşünülürken kullanılan protokol dikkate alınmalıdır. En yaygın olanları Ethernet ve IP'dir.

Broadcast/multicast/unicast trafiğinin 1 saniyede belirli bir yüzdeyi aşması durumuna, Broadcast/multicast/unicast fırtınası (storm) denilmektedir.

Ağ anahtarlama cihazları ile trafiğin arayüz bant genişliğinin belirli bir yüzdesinden çok olması durumunda aşan kısmının bloklanması ve hatta loglanması sağlanabilir. Aşağıda Cisco marka anahtar cihazları için örnek konfigürasyon bulunmaktadır. (Detaylı bilgi için bkz [9])

```
interface <int adı> <int.no>
storm-control multicast level <Yüzde.Küsüratı>
storm-control broadcast level <Yüzde.Küsüratı>
storm-control unicast level <Yüzde.Küsüratı>
storm-control action <shutdown | trap>
```

4.2. L3 Cihazlar ile Alınabilecek Önlemler

OSI'nin 3. katmanında çalışan cihazlarda alınabilecek önlemler aşağıdaki gibidir:

- Vlan Bazlı Güvenlik Çözümleri
- Erişim Listeleri ile Alınabilecek Çözümler
- QoS ile Kişi Başına Bant Genişliği Sınırlaması
- Yeni Nesil Güvenlik Çözümleri

4.2.1. VLAN Bazlı Güvenlik Çözümleri

Üçüncü katman ağ cihazlarında yapılacak ayarlamalar ile kötü amaçlı yazılımların ağ üzerindeki etkileri azaltılabilir. Aşağıda Cisco marka cihazlarda vlan bazında uygulanabilecek ayarlar bulunmaktadır. Konfigürasyon genel olarak kullanılması tavsiye edilen ayarları içermektedir, ancak kullanmadan önce uygulanacak ağın ihtiyaçları da göz önüne alınmalıdır [10].

```
int Vlan Vlan_Numarası
…i
p verify unicast source reachable-via rx
allowdefault
! VLAN altında belirtilmiş IP adresleri dışında
başka kaynak IP adresi ile o VLAN'den trafik
çıkmasını engeller.
no ip redirects
! ICMP redirect desteğini kapatır.
no ip unreachables
! ICMP unreachable paketlerinin geri yollanması
engeller. Bu özellik raslansal hedef IPler seçerek
DoS atağı yapmaya çalışan bir bilgisayara
ulaşılamadı mesajı geri gönderilmeyerek hem
yönlendirici üzerindeki yük azaltılır, hem de
atak yapan bilgisayarın time-out süresine kadar
beklemesine sebep olur.
no ip proxy-arp
! Ağ geçidi (gateway) tanımlamamış veya yanlış
tanımlamış bir istemcin yönlendirici tarafından
tespit edilerek o istemcilere ağ geçidi hizmetinin
otomatik verilmesi özelliğini kapatır.
```

4.2.2. Erişim Listeleri ile Alınabilecek Çözümler

Erişim listelerini kullanılıp yönlendiricilerde aşağıdaki önlemler alınarak kötü amaçlı yazılımların ağ üzerindeki yükü azaltılabileceği gibi kendilerini yaymaları da engellenebilir. Temel önlemler aşağıdaki gibi özetlenebilir:

- Yönlendiriciye gelen paketlerdeki kaynak IP adresleri kontrol edilmelidir. Dış ağdan iç ağa gelen paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne giriş (ingress) filtreleme denmektedir. İç ağdan dış ağa giden paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne çıkış (egress) filtreleme denmektedir. Bu filtrelemeler dahilinde RFC 3704'de [11] tarif edildiği gibi kaynağı olmayan 0.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 adresleri bloklanmalıdır. Ayrıca kurumun IP adresi aralığını, kaynak IP adresi olarak kullanarak yapılabilecek saldırıları engellemek için dışarıdan kurumun IP adresi kaynaklı trafik yasaklanmalıdır. Ayrıntılı bilgi için bkz [12,13].

- Güvenlik açıklarının kullandığı bilinen bazı portların kapatılması veya kısıtlanmasıdır. Bunlara örnek olarak şu portları belirtmek mümkündür: TCP 135, 137, 139, 445 UDP: 137, 138, 161, 162

- SMTP trafiğinin sadece iç mail sunucularına doğru açılmalı, diğer SMTP trafiğinin bloklanmalıdır.

- ICMP trafiğinde "packet-too-big", "time-exceeded", "echo-reply", "echo" ya izin vermek, geriye kalan ICMP türlerini bloklamaktır.

- Erişimi engellenen trafik loglanarak saldırgan bilgisayarın kimliği de tespit edilebilir. Ancak bunun çok sistem kaynağı tüketme riski de vardır.

Cisco marka yönlendiricilerde kullanılabilecek örnek erişim listesi aşağıda gösterilmiştir:

```
ip access-list Vlan_disardan
remark ******* icmp **********
permit icmp any any packet-too-big
permit icmp any any time-exceeded
permit icmp any any echo-reply
permit icmp any any echo
deny icmp any any
```

```
remark * bloklanacak portlar *
deny tcp any any eq 445 log
deny tcp any any range 135 139 log
deny udp any any range 135 139 log
deny udp any any range 161 162 log
remark * bloklanacak IPler *
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip <VLAN'in kendi IP adresi aralığı ve
wildcard maskesi> any
permit ip any any
```

Erişim listeleri ile istenmeyen trafik bloklanabileceği gibi kara delik oluşturmak amaçlı olarak, L3 cihazda policy-routing ile honeynet'lere veya IDS/IPS güvenlik sistemlerine de yönlendirilebilirler.

4.2.3. QoS ile Kişi Başına Bant Genişliği Sınırlaması

Birim kullanıcının dışarı veya içeri doğru kullanabileceği trafik miktarı QoS teknikleri ile kısıtlanabilir. Bu şekilde kötü bir yazılım bulaşmış bir bilgisayarın ağ kaynaklarını sömürmesi engellenir. Bu çözüm aynı zamanda P2P yazılımlarının da bant genişliğini tüketmesini engeller. Bunun için L3 bazlı anahtarlama cihazlarında yapılabilecek ayarlamalar kullanılabileceği gibi, açık kaynak kodlu ipfw gibi uygulamalarda kullanılabilir [14,15].

4.2.4. Yeni Nesil Güvenlik Çözümleri

Kötü amaçlı yazılımların IP adreslerini değiştirmelerini, DHCP ve ARP zehirleme saldırıları yapamalarını engellemek için L3 anahtarlama cihazlarında çeşitli çözümler bulunmaktadır. (Ayrıntılı bilgi için bkz [16,17]). Cisco marka anahtar cihazlarında bu amaçlarla DHCP Snooping, Dynamic ARP Inspection, IP Source Guard çözümleri vardır. Aşağıda bu çözümler için örnek konfigürasyon bulunmaktadır.

```
ip dhcp snooping
ip dhcp snooping vlan <vlan no>
ip arp inspection vlan <vlan no>
!i
nterface <int adı> <int.no>
description Istemci bilgisayar portu
ip verify source port-security
!i
nterface <int adı> <int.no>
description DHCP sunucusunun portu veya
Uplink portu
ip dhcp snooping trust
ip arp inspection trust
```

4.3. Güvenlik Cihazları ile Alınabilecek Önlemler

Ağ üzerinde güvenlik amaçlı kurulacak sistemlerle alınabilecek önlemler aşağıdaki gibidir:

- Güvenlik Duvarları (Firewall)
- Antivirüs Geçitleri
- IDS/IPS Sistemleri

4.3.1. Güvenlik Duvarları (Firewall)

Güvenlik duvarları, durum korumalı (statefull) çalıştıkları için, düzgün ayarlanmaları durumunda zararlı yazılım aktivitesi içeren birçok bağlantıyı engelleyebilecektir. Servis sağlayan sunucuların belirli portları hariç, bütün portlar kurum dışından içeri doğru erişime kapatılmalıdır. 4.2.2'de Erişim kural listeleri ile alınacak bütün çözümler güvenlik duvarlarında da alınmalıdır [19]. Güvenlik duvarının en basit kural tablosunun mantığı aşağıdaki gibi olmaldır.

```
# Kurum içinden dışarı trafik
Bilinen zararlı yazılım portlarını kapat
Bütün trafiğe izin ver
# Kurum dışından içeri
Sunuculara sunucu portlarından erişim izni
Geriye kalan bütün trafiği blokla
```

Güvenlik duvarı için ticari çözümler olduğu gibi, açık kaynak kodlu başarılı çözümler de

bulunmaktadır. Açık kaynak kodlu çözümler için destek veren firmalar da bulunmaktadır. Güvenlik duvarı çözümü seçmeden önce, [18] referansının incelenmesi önerilmektedir.

4.3.2. Antivirüs Geçitleri

Geçen trafiği zararlı içeriğe göre kontrol eden sistemlerdir. Özellikle büyük ağlarda sadece eposta trafiği için bu tür çözümler kullanılmaktadır. Kötü amaçlı yazılımların kendilerini bulaştırmak için en sık kullandığı tekniklerden biri eposta olduğundan, kullanılması ciddi bir fayda sağlamaktadır. Bunun için ticari çözümler kullanılabileceği gibi Clamav[19] gibi GPL lisansına sahip çözümler de kullanılabilir.

4.3.3. IDS/IPS Sistemleri

Günümüzde güvenlik duvarları bütünleşik olarak IDS/IPS mekanizmalarına sahip oldukları gibi, bu sistemler ayrı olarak da kurulabilmektedir. İyi yapılandırılmış bir IDS/IPS sistemi; ağı pek çok kötü yazılımdan izole edebileceği gibi, sorunun kaynağını tespitini de hızlandırmaktadır. Ancak bu sistemlerin iyi bir şekilde ayarlanmaması ve devamlı takip edilmemesi, yanlış tespitler sonucu sorununu da çıkarabilmektedir. Bu sistemler için, ticari çözümler kullanabileceği gibi Snort [20] gibi açık kaynak koduna sahip çözümler de kullanılabilir. Snort için http://www.bleedingsnort.com/ adresinde bulunan bleeding-malware.rules" dosyasındaki güncel zararlı yazılım imzaları kullanılmalı ve sistem sorumluları gözlemledikleri yeni saldırılara ait imzaları da kendileri eklemelidir.

4.4. Diğer Sistemler ile Alınabilecek Önlemler:

Alınabilecek önlemler aşağıdaki gibidir:

- Saldırgan Tuzağı Ağları (Honeynet)
- Merkezi Log Sunucu Sistemi
- Trafik Akış Analizi Sunucuları
- DNS Sunucu
- Arp Saldırılarını Tespit Edebilen Uygulamalar

4.4.1. Saldırgan Tuzağı Ağları (Honeynet)

Zararlı yazılım ve saldırganların saldırılarını saptamak için tuzak sistemleri (honeypot) kullanılabilir. Tuzak ağı (honeynet), tuzak sistemlerinden oluşan bir ağdır. Açık kaynak kodlu yazılımlarla bu tür sistemler kurmak ve yenilerini geliştirmek mümkündür.

Çeşitli bilinen zayıflıkları simüle eden, virüs ve worm etkinliğini yakalama amaçlı kurulan sistemlere örnek olarak "Nepenthes" ve "Amun" yazılımları verilebilir [21]. Bunun yanı sıra, "Honeyd" yazılımı ile bir makine üzerinde farklı işletim sistemlerini simüle eden sanal makineler, sanal yönlendiriciler ve sanal ağlar oluşturulabilir. Burada amaçlanan, bu makinelere saldırganların veya zararlı yazılımların erişimlerini takip etmektir. Ayrıca transparan olarak çalışan "Honeywall" yazılımı çalışan sistem, üzerinden geçen trafiği analiz etmekte, düzgün ayarlanması durumunda alt ağdaki tuzak sistem makinelerinin ele geçirilmesini ve buradan dışarı saldırı yapılmasını engelleyebilmektedir. ULAK-CSIRT Honeynet çalışma grubu bu konuda çalışmalarına devam etmektedir [22].

4.4.2. Merkezi Log Sunucu Sistemi

Ağ cihazlarında gelecek logları sürekli ve kesintisiz tutacak bir log sunucusu mutlaka bulundurulmalıdır. Bu sunucudaki kayıtlar incelenerek, kötü bir yazılım bulaşmış bilgisayarın yeri tespit edilebilir. 4.1.1, 4.1.3, 4.2.2, 4.2.4 ile 4.3.1 tarif edilen engelleme çözümleri, log sunucu sistemi ile kayıt altına alınmış olacaktır. Bu amaçla açık kaynak kodlu syslog veya syslog-ng uygulamaları kullanılabilir [23]. Log bilgisinin çok fazla olması durumunda ihtiyaca göre filtrelenip, gerekmesi durumunda da yöneticiyi eposta ile uyaran Swatch benzeri yazılımlarda karmaşayı azaltmak için kullanılabilir [24]. Ayrıca NAT ve DHCP gibi kaynak IP adresinin değişme ihtimali olan çözümler-

de, bulaşmış bir bilgisayarın tespiti için mutlaka log sunucuları yardımı ile kaynak adres takip altına alınmalıdır [25].

4.4.3. Trafik Akış Analizi Sunucuları
Ağ cihazları, üzerlerinden geçen trafik akış (flow) bilgisini, incelenmesi ve normal dışı davranışlar belirlenmesi için harici bir sunucuya yollayabilir. Bu şekilde fazla paket ve fazla trafik yaratan makineler takip edilebilir. Bu tür ağın çalışmasına zarar verebilecek makineler, 4.2.2'de belirtildiği şekilde akıllı yerel ağ cihazları üzerinden kapatılmalıdır. Bu akış bilgilerini analiz edebilen açık kaynak kodlu birden fazla yazılım vardır. [26] numaralı referanstan bu yazılımların listesi temin edilebilir.

Ayrıca yine ağ cihazlarının bize sağladığı monitor port özellikleri ile trafik bir bilgisayara yönlendirebilir ve trafik analiz edilebilir. Bu analiz için tcpdump, wireshark gibi yazılımlar kullanılabilir [4]. Aşağıda Cisco marka anahtarlama cihazlarında monitor özelliğini devreye almak için kullanılacak komutlar bulunmaktadır.

monitor session 2 source interface
<kaynak interface adı> <kaynak interface no>
monitor session 2 destination interface
<hedef interface adı> <hedef interface no>

4.4.4. DNS Sunucu
Zararlı yazılımların bir kısmı IRC kanalları ile yönetilmektedirler [27]. Yazılım önceden belirlenmiş domain adı ile belirli bir IRC sunucusuna bağlanır ve istenen komutları alır. İletişimi sağlayan IRC sunucusuna dinamik DNS adreslemesi ile ulaşmalarını engelleyerek, özellikle botnet türündeki kötü yazılımların etkinlikleri engellenebilir. Tabii ki bu önlemler de, muhtemelen bir sonraki nesil botnet'lerde geçersiz kalacaktır.

DNS sunucularını, zararlı yazılımlardan dolayı üzerlerine gelebilecek gereksiz trafik yükünü azaltmak için RFC 3704'de [11] tarif edildiği gibi kaynağı olmayan 0.0.0.0/8, 10.0.0.0/8, 192.168.0.0/16, 127.0.0.0/8 ve 169.254.0.0/16 adresleri bloklanmalıdır. [13,28]

Ayrıca DNS sunucularına saldırı gibi gelebilecek istekleri gözlemliye bilmek için "dnstop" gibi açık kaynak kodlu yazılımlar kullanılabilir. [29]

4.4.5. Arp Saldırılarını Tespit Edebilen Uygulamalar
Son dönemde arp zehirlemesi tekniği, kötü amaçlı yazılımlar tarafından da kullanılan bir teknik haline gelmiştir. Bu teknik ile aradaki adam saldırısı ile (man in the middle attack) hedef bilgisayarın bütün veri akışı dinlenebilmektedir. Arp tabanlı bu türden saldırılar için Arpwatch gibi uygulamalar bize yardımcı olabilecek açık kaynak kodlu yazılımlardır. Arpwatch ile ağdaki ARP aktiviteleri izlenerek loglanabilir.[30]

5. Sonuç

Bruce Schneier'in de belirtiği gibi "Güvenlik bir ürün değil, bir süreçtir." Kurumsal ağların ayakta tutulabilmesi için yapılması gerekenler bu bildiride özetlenmiştir. Ciddi yatırımlarla yapılabilecek önlemler var olduğu gibi; açık kaynak kodlu çözümler ve kurumsal bilinçlendirme ile birçok güvenlik ihlalinin önüne geçmek mümkündür.

Bu belgenin ayrıntılı bir rapor haline getirilme çalışmaları devam etmektedir ve ULAK-CSIRT belge sayfasında (http://csirt.ulakbim.gov.tr/dokumanlar/) yayınlanacaktır.

7. Kaynaklar

[1] Karaarslan E., 2008, Doktora Tezi

[2] Magiera J., Pawlak A., 2005, Security Frameworks for Virtual Organizations, In Virtual Organizations: Systems and Practices, Springer

[3] Deep Rants; CYA from botnets to phisherZ, Malware Acquisition postponed, http://isc.sans.org/diary.html?storyid=621

[4] Karaarslan E., Ağ Güvenlik Takibi(Network Security Monitoring) Süreçleri, http://blog.csirt.ulakbim.gov.tr/?p=38

[5] Karaarslan E., Yama Yönetimi, ULAKCSIRT, http://csirt.ulakbim.gov.tr/dokumanlar/Yama Yonetimi.pdf

[6] Akın G., Cisco Switchlerde MAC Adresi Güvenliği ile Kullanıcı Takibi http://blog.csirt.ulakbim.gov.tr/?p=59

[7] PPP Extensible Authentication Protocol (EAP), http://www.ietf.org/rfc/rfc 2284.txt

[8] Demir H., IEEE 802.1X ve Kurulumu http://blog.csirt.ulakbim.gov.tr/?p=52

[9] Akın G., Anahtarlama Cihazlarındaki Traffic Storm Control Özelliği http://blog.csirt.ulakbim.gov.tr/?p=55

[10] Akın G., Cisco Cihazlarda VLAN veya Fiziksel Interface Bazında Alınabilecek Güvenlik Önlemleri, http://blog.csirt.ulakbim.gov.tr/?p=69

[11] RFC3704, Ingress Filtering for Multihomed Networks, http://www.ietf.org/rfc/rfc3704.txt

[12] Kulduk S., Karaarslan E., Yönlendirici Güvenliği, Akademik Bilişim 2004, http://csirt.ulakbim.gov.tr/dokumanlar/Router Guvenligi.pdf

[13] Akın G., Marslılar Aramızda, http://blog.csirt.ulakbim.gov.tr/?p=53

[14] Karaarslan E., Cisco cihazlarda QOS uygulaması - UBRL, http://blog.csirt.ulakbim.gov.tr/?p=60

[15] Kırık Ö. , FreeBSD sistemlerde IPFIREWALL Kurulumu ve Konfigürasyonu, Akademik Bilişim 2003, http://ab.org.tr/ab03/tammetin/32.pdf

[16] Karaarslan E., OSI 2. Seviye Güvenliği, http://blog.csirt.ulakbim.gov.tr/?p=29 [17] Cisco arp çözümleri veye IP table dokumanı

[18] Karaarslan E., Ağ Güvenlik Duvarı Çözümü Olustururken Dikkat Edilmesi Gereken Hususlar, http://csirt.ulakbim.gov.tr/dokumanlar/Guven likDuvariCozumuOlusturmaSureci.pdf

[19] Linux Belgelendirme Çalışma Grubu, Posta Sunucuları için Spam Önleme Araçları Clamav Antivirus, http://belgeler.org/howto/antispamclamav. html

[20] Demirkol Ö. E., Snort 2.3 ve Acid Kurulumu, http://csirt.ulakbim.gov.tr/dokumanlar/Snort Kurulum.pdf

[21] Karaarslan E., Zararlı yazılımla (malware) mücadelede honeypot kullanımı, http://blog.csirt.ulakbim.gov.tr/?p=61 [22] Soysal M. , Bektaş O., HoneyWall Kurulumu, http://csirt.ulakbim.gov.tr/dokumanlar/Honey Wall.pdf

[23] Karaarslan E., Merkezi Loglama, http://blog.csirt.ulakbim.gov.tr/?p=68 [24] Karaarslan E., Swatch ile log dosyalarını takip etme, http://blog.csirt.ulakbim.gov.tr/?p=67

[25] Cisco cihazlarda nat loglaması [26] Demir H.Flow toplama gereçleri, http://blog.csirt.ulakbim.gov.tr/?p=50

[27] Akın G. , Güneş A., Bir Wormun Anatomisi, Akademik Bilişim 2007, http://csirt.ulakbim.gov.tr/dokumanlar/BirWo rmunAnatomisi.pdf

[28] Demir H. , BIND ile RFC 1918 IP Adresleri, http://blog.csirt.ulakbim.gov.tr/?p=51

[29] Demir H. , dnstop, http://blog.csirt.ulakbim.gov.tr/?p=66

[30] Demir H. , arpwatch, http://blog.csirt.