KAMPÜS AĞ YÖNETİMİ

Ar.Gör.Enis Karaarslan
Ege Üniversitesi
BİTAM Kampüs Network Yönetim Grubu
enis.karaarslan@ege.edu.tr

ÖZET
Kampüs ağı, sınırlı bir coğrafi alan içindeki farklı yerel ağları birbirine baglayan büyük bir bilgisayar ağıdır. Ağın büyüklüğü yönetilmesini zorlaştırmakta ve yönetim süreçlerinin standartlara uygun yapılmasını gerektirmektedir. Bu çalışmada, kampüs ağlarının düzgün çalışmasının sağlanması için yapılması gerekenler, Ege Üniversitesi kampüs ağından örneklerle anlatılmıştır.

ABSTRACT
Campus (area) network is a big computer network which connects different LANs within a limited geographical area. The size of the network is a handicap of management and this complex environment requires a standardized management process. In this study, management tasks that need to run campus networks properly are described with the examples of the Ege University Campus network.

Anahtar Kelimeler: Ağ yönetimi, kampüs ağları, ağ güvenliği, yama yönetimi, güvenlik politikası

1.GİRİŞ

Kampüs ağları, farklı binalara yayılmış farklı yerel ağları (LAN) birleştiren büyük ağlardır. Bu adı, birçok binadan oluşan üniversite kampüslerinden almıştır. Bu ağlarda, omurga (backbone) adı verilen, kampüsteki alt merkezleri ana merkeze bağlayan, bir fiber ağ bulunmaktadır. Bu ağlarda Gigabit Ethernet, ATM gibi gelişmiş teknolojiler kullanılmaktadır. Örneğin Ege Üniversitesi, sahip olduğu yedibinin üzerinde bilgisayar ile büyük bir kampüs ağıdır. Sahip olduğu binalar alt merkezlere, alt merkezler de ana merkeze fiber optik kablolarla bağlanmakta ve Gigabit Ethernet teknolojisi kullanılmaktadır. Bilgisayarların utp kablolarla aktif iletişim cihazlarına (hub, switch, router... vb) bağlanması, bu aktif cihazların da ana omurga cihazlarına utp veya fiber kablolarla bağlanması ile bu büyük ağın elemanları birbiri ile konuşmaktadır. Üniversite kampüsleri farklı coğrafi lokasyonlara da dağılmış olabilir, bu durumda çeşitli WAN protokolleri ve Wireless bağlantılar da söz konusu olmaktadır. Kampüs ağ yönetiminde yapılması gerekenler, aşağıdaki başlıklarla özetlenebilir:

- Fiziksel altyapının sağlıklı çalışmasının sağlanması
- Kampüs ağının tanımlanması
- Ağ yönetimi
- Ağ güvenliğinin sağlanması
- Ağ tabanlı servislerin yönetimi
- Kullanıcıların bilinçlendirilmesi

2.FİZİKSEL ALTYAPININ SAĞLIKLI ÇALIŞMASININ SAĞLANMASI

Öncelikle, aktif ağ elemanlarını besleyen elektrik alt yapısının sağlam ve sorunsuz olması sağlanmalıdır. Ağ cihazlarına ayrı ve adanmış sigortalardan hat çekilmeli, mümkünse UPS ile sistem desteklenmelidir. Sigortalı ve topraklı prizler kullanılmalıdır. Gelen elektrik hattının topraklama değerinin mümkün olduğunca sıfıra yakın olmasına önem verilmelidir. UPS'in kısa süreli bir çözüm olduğu unutulmamalı, kritik önem taşıyan yerler ve merkez bilgi işlem için UPS'in yanı sıra jeneratör sistemi kullanılmalıdır.

Data kablosu, sonlandırma ve aktarma işlemlerinde kullanılan bütün bileşenlerin (patch panel, data prizi, patch ve drop kabloların) EIA/TIA-568B yapısal kablolama standartlarına uygun olması sağlanmalıdır. Kaliteli malzeme için; kablo üreticilerinin ürünleri ISO 9000 standardına uygun olmalı, kablo üreticisi sadece kablo değil, bütün tamamlayıcı bileşenleri üretiyor olmalıdır. Data hattı çekilecek yerlerin keşifi, tasarım ve kurulum sürecinde dikkat edilmesi gereken birçok detay vardır. Bu detaylar için Ege Üniversitesi Yapısal Kablolama Yönetmeliği [1] incelenebilir.

Kampüs içinde ve binalar arasında dolaşan fiber optik (F/0) hattının zarar görmemesi çok önemlidir. Özellikle fare gibi haşerelerin fiber ağlarına zarar vermemesi için binalar arasında zırhlı ve sağlam ”outdoor” kabloları kullanılmalıdır. F/O güzergahlarinda yeterli ve standartlara uygun uyarı levhaları olmalıdır. Ayrıca mimari çizimlerin projelendirilmesinde Yapı İşleri ile BIM arasında ortak çalışma sağlanmalıdır. Yapı İşlerinin bu fiber ağının geçtiği yerlerde dikkatli olması, bu kablolara kepçe ve benzeri araçlarla zarar vermemesi sağlanmalıdır.
Elektrikle çalışan bütün cihazların en büyük düşmanı toz ve sıcakır. Aktif cihazların tozdan uzak tutulması için

kabinetlerde tutulması, kabinetlerin hava akımını sağlayacak yapıda (fanlı ve termostatlı) olmaları gerekmektedir.

Sistem odalarında yangın söndürme sistemlerinin ve fiziksel güvenlik önlemlerinin (şifreli kapı sistemleri, kamera takip sistemi) olması gerekmektedir. Detaylı bilgi için bkz. [2].

3. KAMPÜS AĞININ TANIMLANMASI

Kampüs ağları, çok sayıda bilgisayar ve çok sayıda iletişim cihazından oluşan kompleks ağlar olduğu için, trafik yönetimi küçük ağlara göre daha zor olmaktadır. Bilgisayar sayısının fazlalığından, trafik optimizasyonu için sanal ağlar (VLAN) kullanılmaktadır. Bu sanal ağların yönlendirilmesi tercihen OSI'nin 3. seviyesini destekleyen switch'ler, yani yönlendirici (router) özelliği olan cihazlar tarafından gerçekleştirilmektedir. Nerede hangi sanal ağların bulunacağı, her sanal ağda kaçar bilgisayarın olacağı, bu sanal ağlar arasındaki iletişimin kontrolünün sağlanma yöntemleri ve bu işlemleri hangi aktif cihazların yapacağı belirlenmelidir. Değişen ihtiyaçlara göre bu bilgilerin güncellenmesi mutlaka sağlanmalıdır. Bu süreçler için öncelikle ağ tanımlanmalıdır.

Ağın tanımlanması, ağ yönetimi ve aynı zamanda ağ güvenliği için çok kritik önem taşıyan bir çalışmadır. Bu çalışmada aşağıdaki bilgiler toplanmalıdır:

- Ağ Topolojisi: Ağı oluşturan cihazların birbirlerine nasıl bağlandığını ve nasıl iletişim kurulduğunu tanımlayan şemalar oluşturulmalı veya güncellenmelidir. Bu dökümanlar her an erişilebilir durumda olmalıdır.
- Alt ağlar (subnet): İç ağda kullanılan alt ağlar ve bunların nerede yönlendirildikleri veya yönlendirilecekleri (routing) belirlenmelidir. Büyük ağlarda, iç ağ omurgasında yönlendirmeler ve sanal ağ (VLAN) uygulamaları yapılıyorsa, bunlar açıkça tanımlanmalı ve ağ topolojisi olarak çizimleri sağlanmalıdır.
- Bilgisayar sayısı: Sistemdeki toplam bilgisayar sayısı önemli bir kriterdir. Aslında daha önemlisi birim zamanda aktif olan bilgisayar sayısının belirlenmesidir. Aynı zamanda, ağa eklenebilecek bilgisayarlar sayısı da göz önünde tutulmalıdır.
- Band genişliği (bandwith): Hattın ne yoğunlukta kullanıldığı ölçülmelidir. SNMP parametreleri tanımlanan her cihazın trafik kullanım istatistiksel değerleri toplanabilir. Bunun için ücretsiz bir yazılım olan Multi Router Traffic Grapher - MRTG http://people.ee.ethz.ch/~oetiker/webtools/mrtg) programı kullanılabilir.
- Bağlantı (connection) sayısı: Özellikle iç ağdan dış ağa yapılan ağ bağlantılarının sayısı hesaplanmalıdır. Günümüzdeki ağ güvenlik duvarları, kurulan bağlantılara ait bilgileri bağlantı süresince tutmaktadırlar. Seçilecek güvenlik çözümlerinin kararlaştırılmasında bu sayının bilinmesi kritiktir. Bu sayının ölçülmesi için, bir adet demo ağ güvenlik duvarının (içinde sadece "her şeye izin ver" kuralıyla) sistemin önüne kurulması ve ölçüm yapılması iyi bir çalışma olarak karşımıza çıkmaktadır. Bu aynı zamanda sistemde aktif olan bilgisayar sayısını da ortaya çıkarmakta kullanılabilir.
- Trafiğin cinsi: Ağın çeşitli noktaları hat dinleme (sniffer) programları, saldırı tespit sistemleri kurulu makinalar ile takip edilmeli ve netflow data'ları toplanarak ağ trafiği analizi yapılmalıdır. Bu çalışmayla istenmeyen trafik tespit edilmeli ve engellenmesi durumunda hat kullanımının nasıl değişeceği hesaplanmalıdır.
- Kampüs kaynaklarına erişim yöntemleri: Coğrafi yapı nedeniyle dağınık yerlerde bulunan kişilerin telekom hatları üzerinden birbirleriyle veya merkezle bağlantıları ve erişim yöntemleri tanımlanmalıdır. Mobil kullanıcıların kablosuz (wireless) yerel ağlardan veya şirket dışından erişimine hangi kurallar dahilinde izin verilip verilmediği de belirlenmelidir.

Servis sağlayan sunucu makineleri (server) hakkında detaylı bilgi toplanmalıdır. Kampüs ağlarında, sistem yönetiminin kontrolü altında bulunmayan sunucuların da olduğu unutulmamalıdır. Bu durumda, dışarıya hizmet vermek isteyen kişilerin, bu sunucular için ağ yönetimine başvurması sağlanmalıdır. Örnek bir başvuru form içeriği için bakınız (http://security.ege.edu.tr/dilekce.htm). Bu başvuruda en azından aşağıdaki bilgiler kullanıcıdan alınmalıdır:

- Makinanın alan (domain) adı
- İşletim sistemi ve sunucu yazılımları (web sunucu, mail sunucu yazılımları)
- Makineye ait MAC ve IP adresleri
- Dışarıya sunduğu hizmetler ve bu hizmetler için gerekli olan TCP/UDP portları
- Sunucu yöneticisi ile iletişim kurmakta kullanılabilecek telefon ve email adresleri

Sunucularda çalışan servislerin saptanması için, ücretsiz bir yazılım olan Nmap (http://www.insecure.org) programı kullanılarak bilgisayar ağındaki sunucuların portları taranabilir. Bu program ve Nessus gibi zafiyet tarayıcıları ile sistemdeki zayıflıklar da saptanabilir. Tabii ki bulunan portlar arkasında başka uygulamalar çalışıyor olabilir. Sistemdeki cihazlarda hangi portta hangi servisin çalıştığını öğrenmek için ücretsiz bir

yazılım olan AMAP (Application MAPper) programı (http://www.thc.org) kullanılabilir.

İç ağda iletişimi sağlayan cihazların oluşturduğu (switch/hub) yapısının topolojisi çıkarılmalı ve çizimleri yapılmalıdır. Switch'ler eğer yönetilebilir cihazlarsa, hangi portlarında hangi bilgisayarların olduğu (MAC ve IP adresleriyle) dökümante edilmelidir. Mümkünse bu bilgisayarların hangi işletim sistemine sahip oldukları, kullanıcıların hangi saatler içinde bu sistemleri kullandıkları da takip edilmelidir. Bu bilgisayarların bir etki alanına (domain controller) bağlı çalışıp çalışmadıkları, hangi bilgi sistemlerine bağlı oldukları da tespit edilmelidir.

Ayrıca ağ sistemini kullanan kullanıcılar hakkında da bilgi toplanmalıdır. Kullanıcı tipleri ve kullandıkları ağ tabanlı uygulamalar belirlenmelidir. Kullanıcıların hangi sistemlere, hangi saat dilimlerinde, hangi port'lardan eriştikleri de tespit edilmelidir. Böylelikle kullanıcı tabanlı çözümlerin sağlanması mümkün olabilecektir.

Internet üzerinden gelebilecek bilinen saldırı tipleri de göz önünde bulundurularak sistemde hangi servislerin kullanılmasına izin verileceği, hangilerine izin verilmeyeceği de belirlenmelidir. Bazı durumlarda da bu servislerin kullanılmasına ancak belirli kısıtlamalarla izin verilmesi gerekebilecektir.

Bu bilgilerin toplanması ve dökümante edilmesi kolay bir süreç değildir. Mümkün olduğunca çok bilgi toplanmasıyla ağ daha iyi yönetilebilecektir. Ağ çalıştığı sürece, aktif olarak bu bilgiler toplanmaya ve dökümante edilmeye devam edilmelidir. Bu süreçler için çeşitli ağ yönetim yazılımları kullanılması gerekebilecektir.

4.AĞ YÖNETİMİ

Büyük bir kampüs ağında yüzden fazla aktif ağ cihazı, yüze yakın VLAN olabilmektedir. Böyle bir ağdaki trafiğin izlenmesi, özellikle bir yavaşlama/çalışmama anında sorunun hangi VLAN'da ve o VLAN'a ait hangi switch'in hangi portundaki bilgisayarda olduğunun bilinmesi önem kazanmaktadır. Acil durum politikasında, aksaklıkların yaşanması durumunda yapılması gereken prosedürler belirlenmelidir. Sistem yöneticileri ile iletişimin kurulması için gerekli telefon numaraları gibi bilgiler güncel olarak bulundurulmalıdır. Ağ cihazları ve sunucularından gerekli bilgileri alabilmek için Simple Network Management Protokol (SNMP) kullanılmalıdır. SNMP, cihaz ve ağ yönetimi için vazgeçilmez bir protokoldür. Bu protokol sayesinde, trafik istatistiklerinden bellek ve işlemci kullanımına kadar bir cihaz ve üzerinden geçen veri trafiği hakkında çok detaylı bilgiler edinilebilmektedir.

Cihazlarda, SNMP protokolü kullanılarak erişimde kullanılacak Oku (Read only) ve Oku-Yaz (Read-Write) parametreleri tanımlanmaktadır. Ağda bu istatistikleri toplayacak bir veya birden fazla bilgisayar atanmalıdır. Bu bilgisayarlara Ağ Yönetim İstasyonu\Merkezi (AYM) denmektedir. AYM, üzerinde çalışan yazılımlarla belirli aralıklarla ağ cihazları ve sunuculardan bu istatistikleri toparlayacak (poll) şekilde ayarlanmalıdır. Aynı zamanda cihazlarda, sistem durumunda karakterististik değişiklik olduğunda AYM'ye uyarı gönderecek (snmp trap) şekilde ayar yapılmalıdır. Cihazda gözlenen CPU, bellek veya hat kullanımının fazla olması bir saldırı tespiti olabilmektedir. Toplanan verileri grafiksel olarak görüntüleyen Multi Router Traffic Grapher (MRTG)[1] veya PRTG[2] gibi programlar bulunmaktadır. Bu tür programlar ve yapılan eklentilerle ağ trafiği izlemenin en etkin nasıl yapılabileceğinin sorgulanması ve bu konuda ipuçlarının verildiği, "Ağ Trafiği İzleme Sürecinin İyileştirme Projesi" Ege Üniversitesi kampüs ağında uygulanmaktadır ve sistemin önemli bir kısmı tamamlanmıştır. Proje sayfasına http://bornova.ege.edu.tr/~enis/proje/agizleme adresinden ulaşılabilir. Detaylı bilgi için bkz [3].

Yerel ağdaki iletişim cihazları ve ağ yönetimi için ayrı bir VLAN kullanılmalı (management vlan – Vlan 1) ve bu ağa olan iletişimler kontrol altında tutulmalıdır.

Daha güçlü bir ağ için ağ yönetim sistemleri kullanılması gerekmektedir. Kampüs ağlarında yüzlerce aktif cihaz bulunmaktadır. Örneğin Cisco cihazlarını yönetmek için Ciscoworks yazılımı kullanılmaktadır. Bu tür sistemlerle cihazların uzaktan yönetiminde aşağıdaki işlemler yapılabilir:

- Bütün ağın topolojisinin çıkartılması,
- Yönetilebilir cihazların yazılım versiyonlarının tespiti ve güncellemesi,
- Konfigürasyon yönetimi,
- Log ve snmp bilgilerini takip ederek hangi cihazlarda sorun yaşandığının tespiti,
- Performans takibi.

Ağdaki bütün makinaları uzaktan yönetmek ve sorunlarını gidermek istenildiğinde; Hp Openview, Tivoli Netview, CA Unicenter gibi çeşitli ücretli ağ yönetim yazılımlarının kullanılması da gerekebilecektir.

5.AĞ GÜVENLİĞİNİN SAĞLANMASI

Ağ güvenliğinin sağlanması sürecinde öncelikle risk analizi çalışması yapılmalı ve güvenlik politikası

[1] MRTG, http://www.mrtg.org
[2] PRTG, http://www.paessler.com/prtg

oluşturulmalıdır. Hedeflenen güvenlik ışığında, güvenlik duvarı, saldırı tespit sistemleri, antivirüs sistemleri gibi güvenlik önlemleri alınmalıdır. Bu süreci üç ana aşamada toplamak mümkündür:

- Risk analizi çalışması
- Güvenlik ve kabul edilebilir kullanım politikasının oluşturulması
- Güvenlik önlemlerinin alınması

5.1.Risk Analizi Çalışması

Risk belirleme çalışması en önemli noktadır çünkü bu çalışma ile sağlanacak güvenlik seviyesi ve bütçe belirlenmektedir. Bu çalışmada kurum için maddi-manevi değer taşıyan sistemler belirlenir ve bu sistemlerin birim zaman için işlevlerini görememeleri durumunda yaşanacak kayıp hesaplanır. Birim zaman işlev görememelerine yol açacak durumun bir yıl içinde kaç defa oluşabileceği hesaplanır ve bu iki değer çarpılarak yıllık kayıp değeri bulunur. Sonra bu değer göz önünde bulundurularak tehditler için önlem projeleri hazırlanır. Bu projelerde hangi tür sistemlerin nasıl kurulacağı belirlenmektedir. Hangi sistem kurulacaksa kurulsun, öncelikle ağın tanımlanması gerektiği unutulmamalıdır.

5.2.Güvenlik ve Kabul Edilebilir Kullanım Politikasının Oluşturulması

Kurumların maddi ve manevi zararlardan korunması için, kurumun güvenlik stratejisini tanımlayan, güvenliğin nasıl ayarlanacağını ve yönetileceğini belirten güvenlik kurallarına güvenlik politikası denir. Güvenlik politikaları teknik kılavuzlar değildir, herkesin anlayacağı basit bir şekilde güvenlik hedeflerini belirlerler. Ağ güvenlik politikası, kısaca kurumun bilgisayar ağının güvenliğini ilgilendiren her türlü bileşenin yönetimi ile ilgili stratejinin resmi şekilde yazılı olarak ifade edilmesidir. Detaylı bilgi için bkz [4]. Kurumun bir güvenlik politikasına sahip olması, eğer sahip değilse de oluşturması gerekmektedir.

Kabul edilebilir kullanım politikasında (acceptable use policy), ağ ve bilgisayar olanakların kullanımı konusunda kullanıcıların hakları ve sorumlulukları belirtilir. Kullanıcıların ağ ile nasıl etkileşimde oldukları çok önemlidir. SANS Enstitüsü'nün oluşturduğu politika şablonu için bakınız [5]. Türkiye'de üniversitelerin İnternet bağlantısını sağlayan Ulakbim'in uyguladığı kullanım politikası için bakınız [6].

5.3.Güvenlik Önlemlerinin Alınması

Ağ yöneticisi, İnternet (web sayfaları, duyuru listeleri ..vb) imkanlarını kullanarak güncel güvenlik tehditlerini takip etmelidir. Bu süreçte kullanılabilecek adreslerin bir listesi için http://bornova.ege.edu.tr/~enis/guvenlik/ adresi incelenebilir.

Büyük kampüs ağlarında alınabilecek başlıca güvenlik önlemleri olarak aşağıdaki süreçleri belirtmek mümkündür:

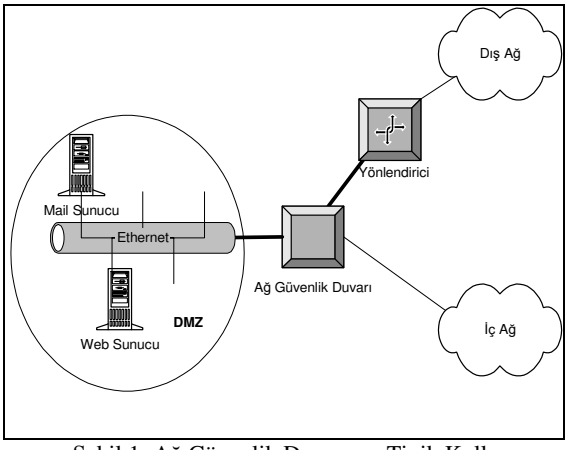
- Aktif Cihazların Güvenliği
- Ağ Güvenlik Duvarı
- Saldırı Tespit Sistemi
- Ağ Tabanlı Antivirüs Sistemleri
- VPN
- Yama Yönetimi

5.3.1.Aktif Cihazların Güvenliği

Aktif cihazların öncelikle fiziksel güvenliği sağlanmalıdır. Bu cihazlara TCP/IP protokolü üzerinden erişimde, bu protokolün zayıflıklarına karşı önlem alınmalıdır. Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Detaylı bilgi için bkz [7]. Yönlendirici cihazı üzerinde alınabilecek güvenlik önlemleri için bkz [8].

5.3.2.Ağ Güvenlik Duvarı

Ağ güvenlik duvarı, kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve internet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Ağ güvenlik duvarı, içeride birbirlerine güvenen, az korumalı makinaların olduğu kurum ağı ile dış ağlar (Internet) arasına yerleştirilir ve aradaki fiziksel bağlantı yalnızca güvenlik duvarı tarafından sağlanır. Ağ güvenlik duvarının tipik kullanımı Şekil 1'de gösterilmiştir. Güvenlik duvarlarının, çeşitli artıları olan "bridge mod"da "transparent" çalışma seçeneği de dikkate alınmalıdır.



Şekil 1: Ağ Güvenlik Duvarının Tipik Kullanımı

Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans arttırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar. Bu cihazın güvenlik politikasını uygulayacak şekilde ayarlanması ve değişen güvenlik koşullarına göre bu ayarlamaların

güncellenmesi gerekecektir. Güvenlik sorunlarını çözmek için, bir antivirüs sunucusu veya web adresi denetleyicisi sunucusu gibi çözümlerle ortak olarak çalışabilirler. Detaylı bilgi için bkz [9].

5.3.3.Saldırı Tespit /Engelleme Sistemleri

Günümüzün artan güvenlik sorunları sonucunda, ağ güvenlik duvarlarının yanı sıra, saldırıları tespit eden ve engelleyen daha detaylı sistemlere ihtiyaç duyulmaktadır:

- Saldırı Tespit Sistemleri (IDS): Bir ağ veya belirli bir sunucu üzerindeki veri trafiğini takip ederek saldırıları tespit eden ve sistem yöneticisini verdikleri alarm mesajlarıyla (e-posta, çağrı cihazı ..vb) uyaran sistemlerdir. Aynı zamanda, istenirse güvenlik duvarına veya yönlendiriciye kural yazıp gerekli engellemeleri de yapabilmektedirler.
- Saldırı Engelleme Sistemleri(IPS): Bir ağ veya sunucu üzerindeki veri trafiğini denetleyen, saldırı olduğu tespit edilen veya istenmeyen trafiği durdurabilen sistemlerdir. IPS'in gücünün, saldırı tespit algoritmasından geldiği unutulmamalıdır. IPS, IDS'in ihtiyaca göre fonksiyonları değiştirilmiş türevidir.

5.3.4.Antivirüs Sistemleri

HTTP, FTP ve SMTP gibi veri trafiklerini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen ağ tabanlı antivirüs sistemleri bulunmaktadır. Ne kadar iyi sistemler kurulsa da virüs taraması bir miktar yavaşlığa yol açacaktır. Büyük ağlarda, DNS ile entegre çalışan ve sadece mail (smtp) trafiğini tarayan sistemler tercih edilmelidir.

Bu tür ağ tabanlı sistemler kurulsa da, her kullanıcının makinasında bir antivirus yazılımı bulunmalıdır. Kullanıcıların kurumsal antivirüs çözümünü kullanması sağlanmalıdır. Kampüs ağında, kullanıcıların bir web sayfasına bağlanıp sadece bir link'e tıklayarak makinasına antivirüs kurması sağlanmalıdır. Kurulacak imza dağıtım sunucusu ile, kullanıcıdan bağımsız otomatik güncelleştirme yapılmalıdır.

5.3.5.VPN

Kampüs ağı dışından, ortak kullanıma açık veri ağları (public data network) üzerinden kurum ağına bağlantıların daha güvenilir olması ve iç ağın imkanlarından yararlanılabilmesi için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi esas olarak alınır. Public/Private anahtar kullanımı ile sağlanır.

5.3.6.Yama Yönetimi

Patch (yama), yazılım üreticisi şirketlerin, yazılımları güncellemek ve/veya hatalarından arındırmak için hazırladıkları paketlere verilen isimdir. Özellikle kurumsal ağ yönetiminde, ağ elemanlarının yazılımlarının takip edilmesi ve yama uygulanmasında bazı yöntemlerin kullanması gerekmektedir. Yama yönetimi methodları olarak aşağıdaki yöntemler sayılabilir:

- Otomatik Güncelleştirme: Kişisel sistemlerin (Windows, Linux ...vb) sık sık güncellenmesi gerekecektir. Kişisel sistemlerde, kritik yamaların otomatik alınması için ayar yapılabilmektedir. Windows makinalarda "auto update" ayarları yapılarak güncelleme otomatik hale getirilebilmektedir. Debian'da "apt-get update", "apt-get upgrade" komutlarıyla sistem güncel tutulabilmektedir. Bu komutlar cron ile çalıştırılarak otomatikleştirilebilir. Her makinanın tek tek yama almasının yaratabileceği sorunlar; Her makinada bu tür ayarların yapılmamış olma olasılığı, gereksiz yere bandgenişliği harcaması (Proxy sistemleri kullanılarak aşılabilir) ve yeterince hızlı olmamasıdır.
- Merkezi Dağıtım: Kurumsal ağlarda bu yamaların merkezi bir makinaya çekilmesi ve buradan diğer makinalara dağıtılması daha iyi bir çözüm olarak karşımıza çıkmaktadır. Bu aynı zamanda hangi makinalarda 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 öncelikle her makinaya tek tek kurulmaları gerekecektir.

6.AĞ TABANLI SERVİSLERİN YÖNETİMİ

DNS, DHCP, Web, Mail gibi ağ tabanlı servislerinin düzgün çalışması sağlanmalıdır. Örneğin DNS servisinin düzgün çalışıp çalışmadığı http://www.dnsreport.com ve http://www.dnsstuff.com/ gibi adreslerden kontrol edilmelidir. Aynı adreslerden mail sunucular da test edilebilir. Sunucularda düzenli ve sık olarak yedekleme yapılmalıdır.

Mail sunucuların relay'e açık olup olmadıkları test edilmelidir. Spam gönderen mail sunucular kara listeye alınmakta ve birçok mail sunucu artık bu sunuculardan gelen mailleri kabul etmemektedir. http://www.spamhaus.org gibi sitelerden mail sunucuların bu tür listelerde olup olmadığı kontrol edilmelidir. Ağ dışından da spam maillerin kullanıcıları rahatsız etmemesi için mail sunucularda spam

kontrolleri aktif edilmelidir.

7.KULLANICILARIN BİLİNÇLENDİRİLMESİ

Kullanıcıların kullandıkları sistemde neyi nasıl yapmaları gerektiği hakkında bilinçlendirilmesi gerekmektedir. Bu şüphesiz ki en çok emek gerektiren ve en zor süreçlerden biridir. Öncelikle kabul edilebilir kullanım ve güvenlik politikalarının kullanıcı tarafından bilinmesi gerekmektedir. Kullanıcıları politikalardan haberdar etmek için birçok yöntem kullanılabilir. Kullanıcıların bir web sayfası aracılığı ile her an güvenlik ve kullanım politikasına erişebilmeleri sağlanmalıdır. Örneğin Ege Üniversitesi'nde uygulanan güvenlik politikasına http://security.ege.edu.tr/gvpolitika.php adresinden ulaşılabilmekte ve duyuru düzenekleriyle değişiklikler kullanıcıya ulaştırılmaktadır. Politikalar okunması sıkıcı dökümanlardır. Kullanıcılara bu bilgileri ulaştırmak için güvenlik ipuçları ileten epostalar atmak, ufak bilgi yarışmaları düzenlemek gibi ilginç yöntemler kullanılabilir.

İnternet servisleri ve nasıl kullanılacağına dair bir portal oluşturulmalıdır. Örneğin Ege Üniversitesi'nde http://internet.ege.edu.tr adresinde böyle bir bilgilendirme portalı yıllardır etkin olarak kullanılmaktadır.

8.SORUNLAR VE ÇÖZÜMLER

Karşılaşılan başlıca sorunlar aşağıdaki gibidir:

- Elektriksel: Bu tür sorunların birçoğu elektrik altyapısına yeterince önem verilmemesinden veya elektrik yapısının artık o bölge için yetersiz kalmasından kaynaklanmaktadır. Bildiride belirttiğimiz standartlara uyulmadığı durumlarda aktif cihazların portları veya cihazın kendisi yanmakta ve bu da o yerel ağın bir süreliğine devre dışı kalması anlamına gelmektedir.
- Toz ve fiziksel erişim: Aktif cihazların kabinetlere alınmadığı alt ağlarda tozlardan kaynaklanan cihaz sorunları da yaşanabilmektedir. Bir başka karşılaşılan durum ise bazı kullanıcıların kablolarla oynaması ve bunun da yerel ağda sorunlara yol açmasıdır.
- Virüs: Kullanıcıların kendi makinalarına antivirüs çözümlerini kurmamaları sonucunda bütün iç ağa virüs yayan bir nokta haline gelmeleridir.
- İstenmeyen trafik: Dosya paylaşım programlarıyla film, müzik gibi yüksek boyutlu verilerin çekilmesiyle bandgenişliği amaç dışı harcanmakta ve internet erişimi yavaşlamaktadır.

Bütün bu sorunların çözümü, standartlara yani kurallara uygun ağ kullanımıdır. Bu konularda Ege Üniversitesi Network Yönetim Grubu tarafından birçok başarılı çalışmaya imza atılmıştır ama yapılacak daha birçok çalışmanın gerektiği aşikardır.

9. SONUÇLAR

Bu bildiride, kampüs ağ yönetiminde dikkat edilmesi gerekenler özetlenmiştir. Güvenlik ve ağ sorunları hep olacaktır, zaten ağ yöneticileri oluşan sorunları çözmek ve ağın düzgün olarak işlemesini sağlamak için vardır. Ağ yöneticisi artan güvenlik tehditleri yüzünden, güvenlik konusununda güncel bilgileri sürekli olarak takip etmeli ve sorunlar büyümeden gerekli önlemleri almalıdır.

Alınan tedbirlerin uygulanmasında idari mekanizmanın onayı ve desteği sağlanmalı, yapılan düzenlemeler kullanıcılara duyurulmalıdır. Ağ yönetiminde, standartlara uyulması durumunda kampüs ağları mümkün olan en az sorunla yönetilebilecektir. Diğer küçük ağlarda da benzer süreçler daha küçük çaplı olarak geçerlidir.

KAYNAKLAR

[1] Karaarslan, E., Baloğlu, C., Ege Üniversitesi Yapısal Kablolama Yönetmeliği, http://internet.ege.edu.tr/nyg_Kablo_Taslak25042004v3.pdf, 2004

[2] Sistem Odaları için İhtiyaç Tanımı, Hacettepe Üniversitesi Bilgi İşlem Dairesi Başkanlığı Ağ ve Sistem Destek Grubu, http://security.ege.edu.tr/dokumanlar.php

[3] Hazırol, U.M., Begit, F., Karaarslan, E., "Ağ Trafiği İzleme Temelleri", Akademik Bilişim 2005

[4] Karaarslan, E., Teke, A., Şengonca, H., "Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması", Iletişim Günleri 2003

[5] SANS Institute, Acceptable Use Policy Template, http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

[6] Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) "Kabul Edilebilir Kullanım Politikası" Sözleşmesi, http://www.ulakbim.gov.tr/dokumanlar/kullanimpolitika.uhtml

[7] Karaarslan, E., "Network Cihazlarının ve Sistemlerinin Güvenliği", inet-tr 2002

[8] Kulduk, S., Karaarslan, E., "Yönlendirici Güvenliği", Akademik Bilişim 2004

[9] Karaarslan, E., "Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar", Akademik Bilişim 2003