İTÜ/NET Öğrenci Yurtları Ağ Altyapısı Tasarımı

Çağla Ayvazoğlu[1], Oğul Çeliksoydan[1], Gökhan Akın[1]

[1] İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, İstanbul

cagla.ayvazoglu@itu.edu.tr, ogul.celiksoydan@itu.edu.tr, gokhan.akin@itu.edu.tr

Özet: İTÜ/NET, İTÜ öğrencilerine, akademik personeline ve çalışanlarına hizmet vermek amacıyla kurulmuştur. İTÜ, Ulusal Akademik Ağ (ULAKNET) üzerinden sınırlı kaynaklarla İnternet hizmeti almaktadır ve bu kaynağın birincil kullanım amacı eğitim, bilimsel araştırma, sosyal hizmetler ve idari işlemlerdir. Makale dahilinde İTÜ/NET'in daha etkin, verimli ve amacına yönelik kullanılabilmesi için; İTÜ yurtlarında kalan tüm kullanıcıların hangi kurallara uymalıları gerektiği ve İTÜ yurt ağ güvenlik politikalarının[1] neler olduğundan bahsedilmiştir.

Anahtar Sözcükler: Tasarım, Politika, Güvenlik, İTÜ/NET, ULAKNET, LAN Design, Security, Dormitory Networks

1. Giriş

Kampüs ağları belirli bir yerleşimde çok sayıda aktif uç (dolayısıyla da kullanıcı) barındıran ağlardır. Kampüs ağlarının en yaygın örnekleri üniversitelerdir. İTÜ'de büyük kampüs ağlarına iyi örneklerinden biridir. Pek çok farklı kullanıcı profiline ev sahipliği yapan kampüs ağları, bu kullanıcılar için farklı politika uygulamalarını ve kullanıcı yerleşimlerine göre ağ cihazlarında farklı yapılandırmaları gerekli kılmaktadır. Bu süreç düzgün bir ağ alt yapısı tasarımı, politikanın belirlenmesi ve güvenlik de göz önüne alınarak gerekli yapılandırmaların uygulanması şeklindedir.

2. Ağ Alt Yapısı

Kampüs ağının kolay yönetilebilmesi ve kampüs kullanıcılarının iyi hizmet alabilmesi için en önemli ölçütlerden birisi ağ alt yapısıdır.

Ağ yapılandırmasında, altyapı ve kablolama işlemleri bir proje içerisinde öncelikli olarak tasarlanıp, analiz edildikten sonra uygulanmalıdır.

Alt yapının belirlenmesi aşamalarında tasarımın çok iyi yapılmış olması gerekir. Profesyonel bir çalışma yapılması hatta dışarıdan da destek alınması olumlu olacaktır.

Tasarımı yaparken, ağ cihazların konulacağı konum belirlenmeli, cihazlar kabinet içerisine yerleştirilmelidir. Kesinlikle kabinet kilit altına alınmalı ve serin bir ortamda tutulmalıdır. Cihazlar kabinet içerisine sabitlenmeli, kablolama gözle takip edilecek şekilde iyi tasarlanarak yapılmalıdır. Böylece kabloların dağınık durması engellenmiş olur ve olası bir sorunda kablonun takılı olduğu port kolayca bulunabilir. Şekil-1'de kötü tasarlanmış bir örnek görülmektedir. Çok bağlantının kabinette bulunması dağınık olmasına sebep olmamalıdır. Buna örnek aynı kabinetteki kablolamanın düzenlenmiş hali olarak Şekil-2'de görülmektedir.

Şekil 1. Kötü Yapılandırılmış Bir Kabinet

Şekil 2. İyileştirme Çalışması Sonucu

Kabinetin yanı sıra yurt kullanıcıları üniversite öğrencilerinin kullanımına açık olan ağlardır ve öğrenciler çoğu zaman kendi odalarında barınan prizlere pek iyi bakmamaktadırlar. Bu da çok sayıda priz sorununa yol açmaktatır. Bu sebepten mümkün oldukça kablo kanalı kullanılmamalı, kablolama ve prizler duvar içersine gömülü olarak tasarlanmalıdır.

3. Üniversite Ağı Erişim Hizmetleri Altyapısı

Üniversite ağının altyapısının bir omurga kablolaması bulunmalıdır. Günümüzde kampüs ağ omurgaları en az Gigabit Ethernet ile, kullanıcıların erişimleri ise 10/100 Mbps Ethernet teknolojisi ile yapılandırılmalıdır. Binalar arasında Single mode fiber optik kablolar, bina içlerinde ise maksimum 100m mesafe için Cat5e ve Cat6 kablolar kullanılabilir. Daha uzun mesafelerde yine fiber optik kablo kullanılmadır.

Ağın güvenliğini sağlamak amacı için güvenlik duvarı (firewall) mutlaka bulunmalıdır.

Kampüs içerisinde kablosuz ağ tasarlanabilir. Bunun için yaygın olarak 802.11g ve daha güncel olan 802.11n protokolleri kullanılabilir.

Kampüs ağının işletilmesi, bağlı olan kullanıcılara sorunsuz bir şekilde İnternet erişimin verilmesinin yanı sıra yerel ağda verilen hizmetlere de hızlı ve sorunsuz erişilmesini sağlamaktadır. Üniversitenin ana sayfası veya öğrenci işleri web sayfaları, kullanıcı dosya sunucuları, yazılımların barındığı ftp sunucuları, bu şekilde erişilebilecek yerel ağ hizmetlerinden sayılabilir.

4. Politikanın Belirlenmesi

Üniversite bilgisayar ağları, öğrencilere, akademik personele ve idari çalışanlara hizmet vermek amacıyla kurulurlar. Kaynağın kullanım önceliğinin, akademik amaçlı araştırma ve geliştirme faaliyetleri olduğu düşünülerek, daha etkin, verimli ve amacına yönelik kullanılabilmesi sağlanmalıdır. Bu amaçla kampüs ağından faydalanan tüm kullanıcılara uygun kullanım kuralları ve ağ güvenlik politikaları belirlenmeli, bu kurallara kullanıcıların uymalarının sağlanması gerekmektedir.

Kampüs ağları, yerel alan ağında çok sayıda bilgisayarın, yazıcının, sunucunun, yurtlardaki öğrenci bilgisayarlarının, dial-up kullanıcılarının ve VPN kullanıcılarının bağlandığı bir ağ olarak düşünülebilir. Kullanıcıların kurdukları ağ bağlantı-

ları İnternet kaynaklarına ulaşma imkanı sağlar; ama beraberinde mevcut imkanların diğer kullanıcılarla paylaşılmasını gerektirir. Bu kapsamda; kullanım politikaları, sistemin bütünlüğünü ve diğer kullanıcıların güvenliğini tehlikeye atmamak için ağa bağlanan tüm kullanıcıların sorumluluklarını anlamalarını sağlamak amacıyla hazırlanmalıdır. [4]

Ağa bağlanan kullanıcıların, bağlandıkları ve kullandıkları servise göre ayrı ayrı tanımlamış kullanım politikaları bulunmalıdır. Bu sebepten yurtlarda barınan kullanıcılar içinde ayrı politka yapılandırılmalıdır.

Yurtlarda barınan ve kampüs ağından faydalanan kullanıcılar için "Yurtlar Ağ Kullanım Poltikası"nın belirlenmesinin yanı sıra, sürekli kullanıcılarının değiştiği yurtlarda sorunsuz bir şekilde hizmet verebilmek ve kullanıcı tespitlerini kolaylaştırabilmek için yurt kullanıcılarına özel bir "kayıt prosedürü" de belirlenebilir.

Bu amaçla çok sayıda öğrenciyi barındıran yurtlarda her yıl, hatta mümkünse her dönem başında kullanıcıların takibi açısından kullanıcı bilgileri kayıt altında alınmalıdır. Bu kayıtlarda kullanıcıların iletişim bilgileri, IP ve/veya MAC adresleri, barındıkların yurt bilgileri (oda,priz) ayrıntılı olarak alınmalıdır.

Kayıt prosedürünün yanı sıra yurtlar ağ kullanım politikaları aşağıdaki bölümleri barındırmalıdır.

a) Verilen Hizmetin Tanımı

Politakın oluşturulmasında mutlaka son kullanıcıya verilen hizmetin hangi sınırlar dahilinde olduğu belirtilmeldir. Bu ilerde son kullanıcıdan gelecek verilen hizmet dışındaki talepleri engelleyecek ve kullanıcını bu hizmetler dışında istemlerinin karşılanmayacağının belirtilmesine yardımcı olacaktır. Hizmet tanımı dahilinde yurt ağı dahilinde ağ'dan hangi hizmetleri alabileceği ve hangi hizmetleri alamayacağı belirtilmeldir. Örnek olarak P2P yazılımlarının kullanılması üniversite dahilde izin verilmeyen bir servisse belirtilebilir. Bunun yanı sıra yine son kullanıcıya internet erişim hızları garanti edilip edilmediği, hangi sorunlara müdahale edilip hangilerine bilgi işlem birimince müdahale edilmeyeceği belirtilmelidir. İTÜ Yurtlar kullanım politikalarında bu amaçla "İTÜ/BİDB, İTÜ/NET'in servis sağlayıcıdan kaynaklı İnternet erişiminde yaşanabilecek sorunlardan sorumlu tutulamaz." [1] şeklinde bir ifade bulunmaktadır. Buna ifadeye rağmen bu gibi sorunlarda yinede bilgi işlem birimi sürekli aranmakta ve hizmet istenebilmektedir.

b) Ağ Kuralların Belirtilmesi

Kullanıcının verilen hizmetten hangi kurallar dâhilinde faydalanabileceği politikada açıkça belirtilmelidir. Kuralların esas amacı kullanıcının ağa ve kendisine verebileceği potansiyel zararların önüne geçmek, bant genişliğinin adil bir şekilde dağıtılmasını sağlamak ve kurumun İnternetinin kötü amaçlı kullanılmasını engellemek olmalıdır. Ayrıca kullanıcıya internet ortamında yaptığı her hareketten sorumlu olduğu ve yarattığı trafiğin tamamen izlenebileceği bilgisi verilmelidir. Bu kapsamda aşağıdaki konulara ilişkin kurallar konulması düşünülebilir:

- Kullanıcının hangi IP adresini kullanacağı
- Dosya paylaşımı
- Dosya indirme ve İnternete Yükleme (download, upload) kotası
- Kullanıcının verebileceği internet hizmetleri
- Kişisel cihazının güvenliğini sağlaması
- Cihazından bilerek veya bilmeyerek yapılan ağ saldırılarına ilişkin sorumluluğu
- Servis sağlayıcının politikalarına [2] ve T.C. yasalarına uyma sorumluluğu

c) Yaptırımların Belirtilmesi

Kurallara uyulmaması durumunda İnternet

bağlantısının belirli sürelerde veya süresiz olarak kesilmesi (ihlal edilen kurala bağlı olarak), daha ciddi ihlallerde ise üniversite bünyesindeki disiplin mekanizmasının harekete geçirilmesi söz konusu olabilir. Bunların detaylı bir şekilde poltikada belirtilmesi gerekmektedir.

5. Güvenlik Tasarımı

"Yurtlar Ağ Kullanım Politikası"nın belirlenip kullanıcıya imzalatılması tek başına ağ güvenliğinin sağlanması için yeterli olmayacaktır. Ağ güvenlik tasarımı ağ planlamasındaki en önemli faktörlerden biridir. Özellikle kampüs ağları güvenlik konusunda ciddi bir özen gerektirir. Binlerce aktif ucun bulunduğu bir iç ağda özellikle ikinci katman ataklarına karşı güvenlik önlemlerine önem verilmelidir.

Ayrıca kampüs ağlarında kullanıcı profili çeşitliliği söz konusudur. Farklı kullanıcı türlerine karşı farklı güvenlik politikaları uygulanması gerektiği aşikardır. Bu politikalar sistemin güvenliğini sağlamak, son kullanıcının bilinçli veya bilinçsiz olarak kendisine ya da bir başkasına zarar vermesini engellemek ve gerektiği durumlarda kullanıcının yerini kesin olarak tespit etmek amacındadır. Bu amaçla Istanbul Teknik Üniversite'si öğrenci yurtlarında uygulanmış olan ve halen uygulanan güvenlik çözümleri artıları ve eksileriyle şu şekildedir.

a. Kullanıcı takibinde uygulanmış olan güvenlik yöntemi:

En yaygın kullanılan güvenlik uygulamalarından biri olan port bazında MAC adresi sabitleme uygulaması İTÜ yurtlarında da uzun yıllar uygulanmıştır. Hatta üzerine otomatik çalışan bir uygulama bile geliştirilmiştir.[5]
Uygulama kullanıcının bağlandığı anahtarın portunda tek bir MAC'e izin verecek şekilde port-güvenliğinin (port-security) aktive edilmesi şeklinde çalışmaktadır. Bu uygulama ikinci katman ataklarına karşı güçlü bir savunma mekanizması oluşturur. Fakat uygulanmasında çeşitli güçlüklerle karşılaşılmıştır. Öncelikle her porta teker teker MAC sabitleme, bilgi işlem çalışanı tarafında oldukça zaman tüketen ve efor gerektiren bir uygulamadır. Yurt kullanıcıların 12 haneli onaltılık sistemdeki bir ifadeyi yanlış bildirmesi veya - sık karşılaşılan bir durum olarak - yanlışlıkla kablosuz ağ adaptörünün MAC adresini vermesi o kullanıcının internete çıkamaması anlamına gelmektedir. Ayrıca kullanıcının taşınması veya bilgisayarını değiştirmesi durumunuda yapılandırmanın değiştirilmesi gerekmektedir. Sonuç olarak bu çözüm uygulanması çok zor olduğu için terkedilmiştir.

b. Kullanıcı takibinde halen uygulanmakta olan güvenlik yöntemi

Port bazında IP sabitleme, her porta tek bir IP'ye izin veren erişim kural listesimin uygulanması ile çalışır. Port haritalaması sonucu her prizin hangi anahtarının hangi portuna bağlı olduğu belirlenir. O portta hangi IP'ye izin verilmişse kayıt sırasında verilen priz bilgisinden yararlanarak kullanıcıya statik olarak kullanılmak üzere o IP verilir. Böylece her priz bir IP ile eşleştirilmiş olur. MAC bazlı bir kısıtlama yoktur yani doğru IP'yi girmek koşuluyla bir porttan herkes internete çıkabilmektedir. Ancak tek bir IP'ye izin verildiği için aynı anda en fazla bir kullanıcı çıkabilir. Aynı zamanda kullanıcıların yer ve IP bilgileri tutulmakta olduğu için yerin tespit edilebilmesi de sağlanmaktadır.

Port bazında IP sabitleme başarılı bir güvenlik çözümü olsa da onun da eksik kaldığı noktalar vardır. En önemli eksikliği IP çakışmasını engelleyememesidir. IP çakışmasının tespiti ARP protokolüyle yapılmaktadır. ARP paketlerinde IP başlığı bulunmadığı için ve Erişim kural listeleride IP başlığına göre filtreleme yaptığı için bu paketleri süzememektedir. Çakışmaya neden olan kişi yanlış IP girdiği için İnternete çıkamasa da IP'nin gerçek sahibinin internet çıkamamasına da sebep olabilmektedir. Ayrıca son kullanıcın statik IP

yapılandırmasını bilmesi ve IP adres bilgilerini yanlış girmemesi gerekmektedir. Bu da teknik destek birimine fazladan yük bindirmektedir.

c. Halen güvenlik amaçlı uygulanan diğer yöntemleri

Kullanıcının kontrolü ve yerinin tespitinin yanı sıra ikinci katman ataklarına karşı alınan diğer güvenlik önlemleri aşağıdaki gibi sıralanabilir. [6]

- BPDU Guard: STP protokolüne karşı yapılanilecek bir ataktan sistemin korunması için kullanılan bir çözümdür. "BPDU Guard" kullanıcı porttan bir BPDU paketi alınması durumunda portu kapatır.
- CDP veya benzeri protokollerin kapatılması: Anahtar portundan son kullanıcıya cihaz hakkında detaylı bilgilendirme yapan bu protokollerin paket yollamasını engellemek için kullanılır.
- DHCP Snooping: Güvenilmeyen portlardan DHCP sunucusu hizmetinin verilmesi engeller.[7]
- DHCP Snooping Limit Rate: Saldırganın sahte DHCP istekleri yaparak IP havuzunu tüketmesini engellemek için saniyede belli bir değerin üstünde istek yollaması durumunda portun kapatılmasıdır.
- Max MAC 1: Bir porttan aynı anda en fazla bir MAC'in çıkmasına izin verir. Bu anahtar cihazlarının hub gibi çalışmasına yol açabilecek MAC sel ataklarına çözüm olduğu gibi, kullanıcın birden fazla bilgisayara ağa sokmasınıda engellemektedir.

d. Yakın zamanda devreye alınacak güvenlik yöntemleri

- Option 82
- IP Source Guard
- Dynamic ARP Inspection

DHCP sunucusunda ve anahtar cihazlarında option 82 desteği aktive edilecektir. Yani her anahtar DHCP isteğine kendi andını (hostname'ini) ve isteğin hangi porttan geldiği bilgisini ekleyecek ve sunucu buna göre IP verecektir. Bu sistemin avantajları şu şekilde sıralanabilir:

- Otomatik IP alınacağı için kullanıcıdan kaynaklı hatalar ortadan kalkacaktır.
- Option 82 sayesinde anahtar cihaz, hangi IP/MAC adresinin hangi portta barındığını bilecek ve bunun için bu bilgilerden "DHCP Source Binding Database" tablosu oluşturabilecektir. Bu sayede:
  - Her port için erişim kural listesi yazılmasına gerek kalmaya-caktır. "IP Source Guard" olarak isimledirilen anahtar güvenlik özelliği otomatik olarak bu listeyi oluşturup uygulayacaktır.
  - "IP Source Guard" portu açmadan önce DHCP haricinde hiç bir pakete izin vermeyeceği için IP çakışmasının da önüne geçilecektir.
  - Kullanıcılara ait MAC adresleri doğru bir şekilde elde edilmiş olduğundan ARP zehirleme ataklarını önlemek amacıyla "Dynamic ARP Inspection" isimli güvenlik çözümü uygulanabilecektir.

Özetle bu mimari kullanıcıyı takip edebilme ve tek IP'ye izin verme amaçlarını sağlamaya devam edeceği gibi, IP çakışması ve ARP zehirleme ataklağının da önüne geçecek ve bunu otomatik IP kullanarak yapacağı için kullanıcının da ağ çalışanlarının da işini kolaylaştıracaktır.

6. Sonuç

Günümüzde kampüs alan ağlarında ciddi port sayısına ulaşan üniversite yurt ağları var olan kampüs ağ yapısından ayrı olarak değerlendirilmeli ve ona göre tasarlanmaldır. Tasarımda bu konu uzman olanlardan profesyonel destek alınması faydalı olacaktır.

Tasarım aşaması sonrasında bütün ayrıntıların düşünüldüğü bir "Yurt Ağ Kullanım

Politikası" belirlenmelidir. Bu bütün yurt kullanıcıların ulaştırılmalı ve okuduklarına dair mümkün ise ıslak imzaları ile onaylatılmalıdır.

Son olarak kullanıcıların her şeye rağmen kural dışı kullanımının engellenmesi ve bu gibi durumlarda tespitlerinin sağlanabilmesi için güvenlik çözümleri de çok detaylı tasarlanıp uygulanmalıdır.

Kaynaklar

[1] İTÜ Öğrenci Yurtları Ağ Kullanım Politikaları V1.3, İstanbul Teknik Üniversitesi, Bilgi İşlem Daire Başkanlığı, 2007, http://bidb.itu.edu.tr/?i=12

[2] Akademik Ağ ve Bilgi Merkezi (ULAKBİM) ,ULAKBİM "Kabuledilebilir Kullanım Politikası, 2007, http://www.ulakbim.gov.tr/ulaknet/kullanim-politikasi 2007.pdf

[3] Campus Information Technology Security Policy, UC Berkley, 2007 https://security.berkeley.edu/IT.sec.policy.html

[4] Karaarslan,E., Akın G., "Kurumsal Ağlarda Zararlı Yazılımla Savaş", Akademik Bilişim 2008, Çanakkale

[5] Karaarslan,E., Akın G., "Kurumsal Ağlarda Zararlı Yazılımla Mücadele Kılavuzu", Ulaknet Çalıştayı 2008,

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

[7] Akın G., "DHCP Servisine Yeni Bir Bakış", www.gokhanakin.net, INET"TR 2008, Ankara