GÜVENLİK ÖNLEMİ ALINMAMIŞ KABLOSUZ YEREL ALAN AĞLARINDAN BAĞLANTI RİSKLERİ

Fatih Koç, BTYÖN Danışmanlık

Kablosuz Yerel Alan Ağlarının (WLAN) yaygınlığı, özellikle kablosuz ADSL modem ile ülkemizde ciddi bir artış göstermiştir. Son kullanıcılara hareket serbestliği sağlaması sebebiyle daha özgür ortamlar yaratan kablosuz ağlar, gerek kamuya açık alanlarda gerekse kullanıcıların ev ve iş yeri ortamlarında internet ve intranet erişimlerinde tercih edilmeye başlanmıştır. Özellikle halka açık internet ortamlarında (Hot Spot olarak da bilinir), kablosuz ağ kullanıcıları için kimlik doğrulama yapılması veya trafiğin şifrelenmesi beraberinde anahtar dağıtımı ve güncellenmesi gibi sorunları doğuracaktır. Bu sorunlar sebebiyle günlük hayatımızda sıkça bulunduğumuz kafeteryalarda, restoranlarda, ulaşım araçları gibi ortamlarda kullanılan kablosuz ağlarda güvenlik önlemleri ile karşılaşmamaktayız. Bu yazıda son kullanıcı bilgisayarlarından güvenlik önlemi alınmamış erişim noktaları kullanılmasının kullanıcı bilgisayarları için doğuracağı risklere değinilmiş ve bu risklerden kaçınılması için alınabilecek önlemler anlatılmıştır.

Kablosuz Yerel Alan Ağlarının (WLAN) yaygınlığı, özellikle kablosuz ADSL modem ile ülkemizde ciddi bir artış göstermiştir. Son kullanıcılara hareket serbestliği sağlaması sebebiyle daha özgür ortamlar yaratan kablosuz ağlar, gerek kamuya açık alanlarda gerekse kullanıcıların ev ve iş yeri ortamlarında internet ve intranet erişimlerinde tercih edilmeye başlanmıştır.

Kablosuz Ağların tarihçesinin daha eski olması ile birlikte, alınan güvenlik önlemlerinin tarihçesine bakılacak olursa, 1999 yılında kullanılmaya başlanan Wired Equivalent Privacy (WEP), ardından 2003'te geliştirilen Wi-Fi Protected Access (WPA) ve 2004 Haziranda 802.11i ile kablosuz yerel alan güvenliği için kullanılan kimlik doğrulama ve şifreleme önlemleri bugünkü halini almıştır.

Özellikle halka açık internet ortamlarında (Hot Spot olarak da bilinir), kablosuz ağ kullanıcıları için kimlik doğrulama yapılması veya trafiğin şifrelenmesi beraberinde anahtar dağıtımı ve güncellenmesi gibi sorunları doğuracaktır. Bu sorunlar sebebiyle günlük hayatımızda sıkça bulunduğumuz kafeteryalarda, restoranlarda, ulaşım araçları gibi ortamlarda kullanılan kablosuz ağlarda güvenlik önlemleri ile karşılaşmamaktayız. İnternete bağlanmak için kablosuz ağın ismini (Service Set Identifier – SSID) bilmemiz yeterlidir. SSID ise halka açık internet erişimi verilen yerlerin hemen hemen hepsinde yayınlanmaktadır.

Günümüzde sıklıkla karşılaşılmamakla beraber, kimi kurumsal ağlarda dahi güvenlik önlemi alınmamış kablosuz ağlarla karşılaşmaktayız. Bu kablosuz ağlar kimi zaman sadece internete erişim için tasarlanmış mimaride kullanılırken, kimi zaman da kurumsal amaçlarla iç ağa erişimde kullanılmaktadır.

Kullanıcı bilgisayarı açısından kablosuz ağ hakkında bilinen; ağın adı (SSID) ve güvenlik yapılandırmasıdır. Güvenlik önlemi alınmamış bir kablosuz ağ için güvenlik yapılandırması "Kimlik doğrulama yöntemi: Açık (Open), Şifreleme: Yok (Disabled)" olacaktır.

Güvenli olmayan kablosuz ağlardan yapılacak tüm erişimler şifresiz (kullanıcı tarafında kullanılabilecek VPN uygulamaları bu kapsamda değerlendirilmemiştir) olacağı için gerek diğer kullanıcılar gerekse Erişim Noktası için tüm trafik dinlenebilir niteliktedir.

Yaygın olarak kullanılan işletim sistemlerinde kullanıcılar, kablosuz bir ağa bağlandıklarında, bağlantı bilgileri (SSID ve güvenlik yapılandırması) tercih edilen ağ listesine (Preferred Network List – PNL) kaydedilir. Bağlantının kopması, kapsama alanı dışına çıkma ve ardından tekrar kapsama alanına girme durumunda otomatik olarak ağa bağlanma işi işletim sistemi (başka bir deyişle işletim sistemi

üzerinde çalışan bir servis) tarafından sağlanır. Kullanıcı tespit edilen bir kablosuz ağa (ağ ismine çift tıklayarak) bağlanmak istediğinde ve ağı tekrar gördüğünde işletim sistemi üzerinde çalışan bir servis tarafından otomatik olarak bağlanacak şekilde yapılandırılır. Bu yapılandırma kolay kullanım maksadı ile geliştirilmiştir.

Kablosuz ağlarda Şeytani İkiz (Evil Twin) olarak bilinen saldırı yönteminin kullandığı argüman yukarıda bahsedilen -güvenlik yapılandırması yapılmamış- ağlardır. Yani saldırı hedefi olan bilgisayarlar, daha önceden güvensiz bir ağa bağlanmış, PNL'de ilgili ağ bilgileri bulunan ve saldırı anında herhangi bir ağa bağlı olmayan bilgisayarlardır. Saldırgan güvenlik önlemi alınmamış ağı taklit ederek kullanıcıların oluşturulan bu sahte ağa bağlanmalarını sağlarlar. Bu saldırının gerçekleşmesi için kullanıcının herhangi bir kablosuz ağa bağlanmamış olması veya saldırgan tarafından bağlı olduğu ağdan koparılması gerekmektedir.

Microsoft Windows "Kablosuz Sıfır Konfigürasyon"(Wireless Zero Configuration-WZC) serisi çalışan bir bilgisayarda, kullanıcı kablosuz ağlara bağlandıkça "Tercih Edilen Ağ Listesi" (Preferred Network List - PNL) genişlemeye başlayacaktır. Yeni ağlara bağlandıkça, bağlanılan ağ bilgileri bu listeye eklenecektir. Kablosuz herhangi bir ağa bağlı olmayan kullanıcı, PNL'de bulunan ağlar için istek paketleri (Probe Request Packet) gönderecektir. İsteklerine cevap veren Erişim Noktaları'na PNL'de ki öncelik sırasına göre bağlanacaktır.

Kullanıcı bilgisayarı aynı SSID yayınını yapan iki erişim noktasından da (Access Point) sinyal alıyorsa bunlardan sinyali en güçlü olanı tercih edecek ve güçlü sinyal yayan erişim noktasına bağlanacaktır. Yani saldırgan, kurbana ne kadar yaklaşırsa veya ne kadar güçlü sinyalle yayın yaparsa, kurban kullanıcıyı kendi üzerine çekmesi de o kadar kuvvetle muhtemel olacaktır.

Kablosuz istemci bilgisayarı, işletim sistemi Microsoft Windows ise -WZC servisi ile kontrol edilen bir kablosuz adaptör ile- oturum açmadan, Mac OS da ise oturum açtıktan sonra bu saldırı için hedef bilgisayarlardır. Açık kaynak kodlu işletim sistemlerinde ise varsayılan yapılandırma değiştirilip "ilgili ağın gözlenmesi durumunda bağlan" gibi davranması sağlanmışsa aynı tehlikeler bu işletim sistemleri için de geçerlidir.

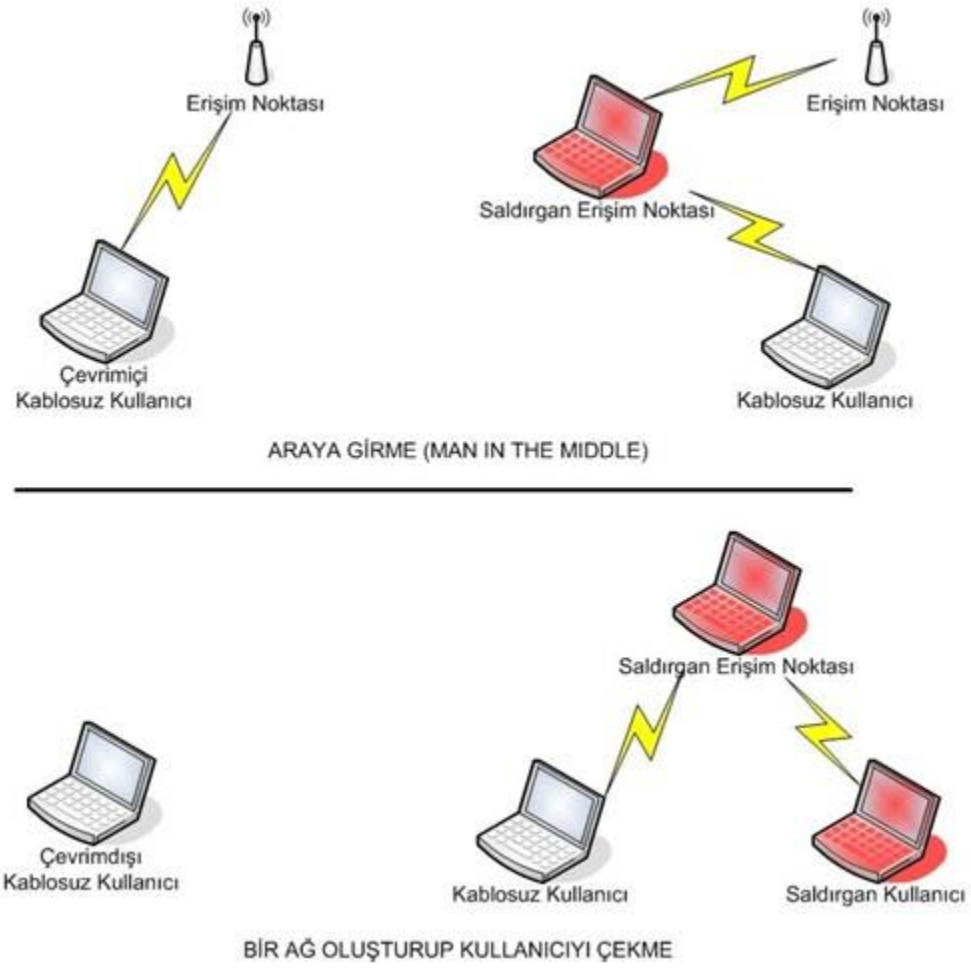
Peki, bu saldırı sonucunda kayıpların boyutu, kablosuz istemci bilgisayarları açısından veya bir adım öteye gidersek kurumsal bilgi güvenliği açısından ne seviyede olacaktır?

İşletim sisteminden bağımsız olarak, kablosuz istemcinin sahte bir ağa bağlanması, saldırgan ile istemci arasında HUB'a eşdeğer bir ağ kurulması anlamına gelir. Bu seviyeden sonra saldırgan çeşitli ağ tarama ve saldırı teknikleri ile istemci bilgisayarın dosya sistemine erişmeye çalışacaktır. Saldırganın kendi üzerinden internet hizmeti vermesi durumunda ise istemcinin tüm trafiği saldırgan üzerinden geçtiği için saldırgan açık trafiğin tamamına erişebilecektir. Saldırganın hedef bilgisayara erişip bir truva atı yerleştirmesi, daha sonra kullanılabilecek bir arka kapı yaratması anlamına gelmektedir. Saldırganın kurban bilgisayarında kablolu arayüzü ile kablosuz arayüzü arasında yönlendirme yapmayı başarması durumunda ise kablolu ağa kablosuz arayüz kullanılarak erişim söz konusu olabilir.

Kurumsal ağlar düşünüldüğünde, -ağ mimari yapılandırmasına bağlı olarak- böyle bir saldırı için kurumun sınır güvenlik önlemlerinin (internetten gelebilecek saldırılar için konumlandırılmış, Saldırı Tespit Sistemi(Intrusion Detection System-IDS), Saldırı Engelleme Sistemi (Intrusion Prevention System-IPS), Güvenlik Duvarı, İçerik Kontrolcüsü, vs.) pek bir önemi kalmamaktadır. Çünkü saldırı önlem alınmış kanallardan (kurumun internet çıkışı üzerinden) değil kullanıcı bilgisayarı üzerinden kurulmuş bir "yan kanal" dan gelmektedir.

Dikkat edilmesi gereken başka bir husus ta bir kurumsal ağda kablosuz ağ altyapısı kullanılmasa (başka bir deyişle bir tane dahi erişim noktası -access point- bulunmasa) dahi kullanıcıların kullandığı bilgisayarlarda bir kablosuz ağ kartı olması ve bu ağ kartının bir yerlerde kullanılması durumunda yukarıda anlatılan saldırı senaryosu geçerlidir.

Şekil 1'de araya girme ve kullanıcıyı kendi üzerine çekme yolu ile gerçeklenebilecek saldırı senaryoları bağlantı şemaları verilmiştir.



Şekil 1 Araya girme ve bir ağ oluşturup kablosuz kullanıcıyı çekme

Bu tipte bir saldırıya maruz kalınmaması için aşağıdaki önlemler alınabilir;

Kullanıcı bilgisayarları için:

Kullanılmıyorsa kablosuz arayüz kapatılmalıdır.
PNL'de güvensiz ağ profilleri bırakılmamalıdır.
İşletim sistemi ve kullanılan uygulama yazılımları güncel tutulmalı, özellikle güvenlik yamaları tam olmalıdır.
Dosya paylaşımı için gereğinden fazla yetkiler verilmemeli, gizli paylaşımlar kapatılmalıdır.
Halka açık internet erişimi kullanılırken hassas bilgi (e- posta, dosya vb.) transferinden kaçınılmalıdır.
Uyarı mesajlarına dikkat edilmeli, https bağlantılarında sertifika bilgileri kontrol edilmelidir.
Kişisel güvenlik duvarı açık olmalı, istisnai erişim ayarları gereksiz erişimler için açılmamalıdır.
Anti virüs yazılımları kullanılmalı, zararlı kod imzaları güncel tutulmalıdır.

Kurumsal ağlar için:

Bir etki alanı kullanılıyorsa grup politikası ile kullanıcıların kablosuz ağ yapılandırması için yapabilecekleri eylemler kısıtlanmalıdır.
Bir Ağ Erişim Kontrolcüsü (Network Access Controller - NAC) kullanılıyorsa bununla kullanıcıların yapılandırmasının güvenli olup olmadığı kontrol edildikten sonra kurumsal ağa alınmaları sağlanabilir.
Kablolu ve kablosuz ağların 24/7 izlenmesi ile saldırıların tespiti sağlanmalıdır.
Kurumsal ağda kablosuz ağ kullanılması durumunda WPA, WPA2 tercih edilmeli, kimlik doğrulama için PEAP veya sertifika tabanlı kimlik doğrulama yöntemleri kullanılmalıdır.

Referanslar:

[1] **http://searchsecurity.techtarget.com**

[2] **http://www.enterpriseitplanet.com**

[3] **http://www.techweb.com**

[4] **http://www.wi-fiplanet.com**

[5] **http://www.pcworld.com**

[6] **http://reviews.cnet.com**

[7] **http://www.ectnews.com**

[8] **http://www.blackalchemy.to**