KABLOSUZ AĞLAR YOLGEÇEN HANI MI?

Çerez kutusundan yapılma antenlerle kablosuz ağ avına çıkan hackerlere karşı, şirket ve kurumların kablosuz ağ sistemlerinin güvenliğine özellikle dikkat etmesi gerekiyor.

Günümüzde bilgisayar ve çevre teknolojilerindeki gelişmeler sayesinde neredeyse her şeyin kablosuz olduğu bir dünyaya doğru hızla yol alıyoruz. Kablosuz bir yaşam kullanıcılara daha geniş bir hareket alanı, dolayısıyla daha fazla özgürlük sunuyor. Bunun en açık faydalarından birini de son yıllarda hızla yayılan bilgisayarlararası kablosuz iletişim ağları oluşturuyor. Bilgisayarları bir nevi radyo alıcısı gibi kullanarak şirketin kablosuz ağ yayının mevcut olduğu herhangi bir yerden ağ üzerindeki diğer sistemlere ulaşabilmek, kullanıcılara geniş bir hareket alanı ve daha serbest bir çalışma ortamı sağlıyor. Bu tarz ağlara dair farklı uygulamalara birçok yerde rastlamak mümkün. Kapıdan içeri girildiği anda çalışanlara ağ erişim imkanının sunulduğu işletmeler, müşterilerine kablosuz Internet bağlantısı sağlayan kafeler, havaalanları ve oteller bunlardan bazıları.

Ancak kablosuz ağların faydaları her ne kadar saymakla bitmeyecekmiş gibi görünüyor olsa da, özellikle kontrol altında tutulması gereken verilere ev sahipliği yapan şirket ve kurumlara ait kablosuz ağ uygulamalarının dikkatsiz bir biçimde gerçekleştirilmesi, bir takım güvenlik sorunlarına yol açabiliyor. Örneğin kablolu ağ sistemlerinde bina içi ağ kablolama sisteminizi bir şekilde fiziksel olarak koruyabilir ve bu yolla dışarıdan gelebilecek izinsiz girişleri engelleyebilirsiniz. Fakat iyi planlanmamış kablosuz ağ uygulamalarının, ağ sinyallerinin dışarıya taşması gibi yan etkisi mevcut. Bu durumun da dışarıdan geçen herhangi birine pencereden bir ağ kablosu uzatarak sisteminize bağlanmasını teşvik etmekten pek bir farkı yok.

Yukarıdaki disket düzeneği gibi basit bir biçimde tasarlanan antenler, kablosuz ağ avcılarının gözde malzemeleri arasında yer alıyor.

Basit Yapılı Antenlerin Marifetleri

İşte bu nedenle kablosuz ağlar, veri iletişiminde WEP (Wired Equivalent Privacy-Kablolu Eşdeğerinde Gizlilik) adı verilen bir şifreleme yöntemi kullanarak iletişim için kablolu ağlara benzer ölçüde bir güvenlik sağlamaya çalışıyorlar. Ancak WEP şifrelemesi, ister 40 bit olsun ister 128 bit, kablosuz ağlara dışarıdan müdahale gerçekleştirmek isteyen birinin biraz bilgili olması koşuluyla kablosuz ağların WEP anahtarı kolayca deşifre edilebiliyor. Üstelik işin bu derece kolay hale gelmesinden daha şaşırtıcı olan şey, birçok kablosuz ağda WEP şifrelemesinin bile kullanılmıyor oluşu. Windows.NET Magazine dergisinin Aralık 2002 sayısında yayınlanan bir makaleye göre Washington DC'de yapılan bir deneme sırasında sokakta kablosuz ağ sinyalleri aramak için dolaşan editörler, sadece 20 dakika içinde çoğu WEP şifreleme yöntemiyle bile korunmayan 40 farklı kablosuz ağ yayınına ulaşmayı başarmışlar. Yine BBC'de yayınlanan bir habere göre 2001'de Londra'da yapılan bir denemede isec adlı bir ağ güvenlik şirketi, yarım saatlik bir şehir turu sırasında 60 farklı kurumun kablosuz ağ yayınına ait sinyalleri yakalamayı başarmış. Bu yayınlara bir şekilde dahil olmak, kablosuz ağ yayını yapan erişim noktalarının devre dışı bırakılmasından şirketler için önemli verilerin çalınmasına kadar birçok dezavantajı beraberinde getirebiliyor. Hatta bu durum Wi-Fi ağlarının yoğun olarak kullanıldığı ülkelerde hackerler için ilginç bir hobiyi gündeme getirmiş: Kablosuz ağ sinyallerini daha iyi yakalayabilmek için basit malzemelerle güçlü ve taşınabilir antenler oluşturmak. Hatta bu amaçla marketlerde satılan bir çeşit patates cipsi olan Pringles kutularından (http://me.jeremiahwhite.com/pringles.html) veya disket ve ataçlardan oluşturulmuş basit antenlerden bile faydalanmayı ihmal etmiyorlar (http://www.wifi-montauban.net/communaute/index.php/DisquettAntenna)

Ne Yapmalı?

Neyse ki son zamanlarda bu tarz zayıflıkların gündeme gelmesi, kablosuz ağ cihazı üreticilerinin bu konuyu dikkate alması sonucunu doğurdu. Aslında WEP şifreleme sisteminin zayıf yönü genellikle kullanıcının başta belirlenen sabit bir anahtarı kullanması ve bu sabit anahtarın havada akan paketler içinden kolayca elde edilebilmesi nedeniyle ortaya çıkıyor. Bu durumu göz önüne alan çoğu üretici de paket anahtarlarını sürekli değiştirerek geçerli anahtarın bulunmasını zorlaştıran ve sisteme istemsiz girişleri engelleyen yeni WEP sistemlerini firmware güncellemesi olarak kullanıcılara sunmaya başladı. Dolayısıyla bu cihazların firmware güncellemelerini yapmak ve iletişim sırasında WEP şifrelemesini açık tutmak, veri güvenliğinin sağlanması açısından alınabilecek önlemlerin başında geliyor. Ayrıca kablosuz ağ kurulumu sırasında dışarı çıkan ağ sinyallerini minimuma indirecek bir düzenin göz önüne alınması ve ağ erişimi için kullanıcı kimliği doğrulama sistemlerinin kullanılması da, veri güvenliğinin sağlanmasına katkıda bulunabilecek bir diğer önemli unsur.

Levent Daşkıran

Mini Terimler Sözlüğü

802.11: 1997 yılında ortaya çıkan 802.11 kavramı, IEEE (Institute of Electrical and Electronics Engineers-Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından kablosuz ağ teknolojilerine dair koyulmuş iletişim özelliklerini belirler. 802.11 kablosuz ağ teknolojilerinin 802.11a, 802.11b ve 802.11g gibi çeşitleri bulunur ve bu çeşitler çalıştıkları frekans bandı ve sundukları hızlarla birbirlerinden ayrılırlar. Bu standartlar hakkında daha ayrıntılı bilgiyi http://www.webopedia.com/TERM/8/802_11.html adresinde bulabilirsiniz.

Wi-Fi: Wireless Fidelity kelimesinin kısaltmasıdır ve hangi standarda dahil olursa olsun bütün 802.11 ağlarını kapsayan bir terimdir (802.11a, 802.11b vs). Önceleri sadece 802.11b için kullanılan bu terimin içeriği, giderek daha farklı çeşitleri ortaya çıkan 802.11 sınıfı kablosuz ağ teknolojilerinin oluşturduğu karmaşayı ortadan kaldırmak üzere tüm bu kablosuz ağ standartlarını içine alacak biçimde genişletilmiştir.

WEP: Açılımı Wired Equivalent Privacy (Kablolu Eşdeğeri nde Gizlilik) olan WEP, kablosuz ağların kablolu ağlara oranla saldırılara daha açık oluşundan ileri gelen dezavantajları kapatmak üzere ortaya koyulan bir şifreleme sistemidir. WEP, radyo dalgalarıyla gönderilecek olan verilerin şifrelenerek paketlenmesini sağlar ve bu paketlerin şifrelerini alıcı tarafında çözülerek veriye ulaşılır.

Firmware: Çeşitli donanımların içeriğindeki bulunan ve donanımın nasıl çalışması gerektiğine dair yönergeler içeren programları depolamak üzere tasarlanmış olan yongalara ve bu yongalarda saklanmakta olan donanıma özgü programlara verilen isimdir.

Kaynaklar
http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm
http://www.usethesource.com/articles/01/08/10/1517228.shtml
http://www.cypherspace.org/~adam/rsa/rc4.html
http://www.eetimes.com/story/OEG20010803S0082
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf
http://www.webopedia.com