

Kablosuz Ağ Güvenliği (1)



ÇETİN KAYA
KOÇ

Kablosuz ve mobil ağlar için en büyük güvenlik tehditleri nelerdir?

Küçük, orta ve büyük binlerce şirket için kablosuz Internet ve intranet erişimi artık çok sıradan bir uygulama haline geldi, ancak bu durum cevapsız soruların kalmadığı anlamına gelmiyor. Cevabı veya çözümünü zor gözüken bazı soruları sorup, bunların içerik ve kapsamlarını anlamak için bu yazı köşemizi bir kaç hafta meşgul edeceğiz. Tabii bu köşe BThaber'in "de facto" güvenlik köşesi ve bu konu da yazarın uzmanlık alanı olduğu için güvenlik soru ve cevaplarına ağırlık vermemizde yarar olacaktır.

Bir soru ile başlayalım: Kablosuz ve mobil ağlar için en büyük güvenlik tehditleri nelerdir? Üç tane tehdit dikkat çekiyor: 1) İşletim sistemi çekirdeğindeki açıkların akıllı saldırganlar tarafından istismarı, 2) Dikkatsiz kullanıcıların güvenlik uyarılarını hiçe sayarak denize atlanmış gibi kablosuz ağ kullanması, 3) Denial-of-service saldırıları.

Bu tehditlerden birincisinin varlık nedeni, saldırganların gerçekten de çok bilgili, tecrübeli ve de akıllı olmaları. Geçtiğimiz yılda keşfedilen bu açıkların kaynağında sürücü yazılımı yönetimin

fonksiyonlardaki frame'lar üzerinde "buffer overflow" yöntemi ile kötü niyetli bir yazılımı "payload" üzerinden işletim sistemine aktarmak yatıyor. Böyle açıklar keşfedildiği ve çok iyi bilindiği halde, hala saldırıların olmasının nedeni sürücü yazılımların değiştirilmemiş olması. Peki niye değiştirilemiyor? Çünkü değiştirmenin metodu "ad hoc" yani birer birer yapmak gerekiyor. Windows update yapsanız bile, üçüncü parti sürücü yazılımlar değiştirilmediği için eski sürücüler varlıklarını korumaya ve açıklar var olmaya devam ediyor. Bazen IDS/IPS uygulamalarında bir fayda vermiyor, çünkü saldırganlar, söylediğim gibi biraz fazla akıllılar. Sürekli olarak saldırı şeklini değiştirip bu uygulamaları bypass ediyorlar. Çözümler: 1) Sürücülerin sürümlerini takip edip, gerektiğinde değiştirmemiz lazım, 2) Daha akıllı IDS/IPS uygulamaları saldırıları bertaraf edebilir ama bu konu henüz araştırma seviyesinde, beklemekten başka çaremiz yok.

Diğer kablosuz ağ tehditlerini daha sonra işleyeceğiz. İyi haftalar.

koc@cryptocode.net