KABLOSUZ AĞ GÜVENLİĞİ NASIL SAĞLANIR?

Kablosuz ağlar, kablolu ağ iletişimine alternatif olarak çeşitli frekans aralıklarını kullanan ağ iletişim biçimidir. Günümüzde artan mobil ve taşınabilir cihaz sayısının artışı, kurulum maliyetinin düşüklüğü ve kolaylığı kablosuz ağ kullanımını arttırmıştır. Kablosuz ağ kullanımı artışına paralel olarak kablosuz ağ tehditleri ve kablosuz ağ güvenliğinin önemi de artmıştır. Kablosuz ağ güvenliği için alınabilecek bir dizi önlem vardır. Fakat unutulmamalıdır ki kablosuz ağlar, kablolu ağlar ile karşılaştırıldığında daha güvensizdir.

Kablosuz Ağ Güvenliği için Alınabilecek Bazı Önlemler:

Kablosuz Ağ Adı (SSID) ve Şifresini Değiştirme

Pek çok kullanıcı kablosuz ağ adını ve şifresini default yani varsayılan değerlerde kullanıyor. Bu durum saldırganlar ve kötü niyetli kişilerin modeminizin markasını ve modelini bulmasını kolaylaştırıyor. Marka ve model tespiti sayesinde saldırganlar internet üzerinden cihazımıza özel açıklıkları tespit edebilir ve ağımıza sızabilirler. Aynı şekilde modem şifremizi de mutlaka değiştirmemiz gerekiyor çünkü cihaz şifreleri de üretici firma tarafından atandığı için bu durum hackerların şifremizi kolay bir şekilde bulamalarına yol açabilir.

SSID Gizleme (Kablosuz Ağ Adı- Service Set Identifier)

Kablosuz ağ adı gizleme de ağın güvenliğini arttıracak işlemlerden bir tanesidir fakat tek başına elbette yeterli değildir. SSID gizleme son kullanıcının işini bir tık zorlaştıracaktır.

Kablosuz Ağ Şifresi

Yukarıda bahsettiğimiz gibi modemimizin şifresini değiştirmeliyiz, peki şifremiz nasıl olmalı? Kullanacağımız şifre uzun, tahmin edilmesi zor, sık kullanılmayan ve de başka bir yerde kullanmayacağımız bir şifre olmalı. Aynı şekilde harf, rakam ve sembollerden oluşmalı ki brute force saldırıları ile kolayca elde edilemesin. Bunun yanında tüm bu kriterlere uysa dahi şifremizi düzenli aralıklarla değiştirmemiz gerekli.

Şifreleme Protokolü

Kablosuz ağda veri iletişimi herkese açık bir ortamda gerçekleştirildiği için araya kötü niyetli üçüncü şahıslar girebilir. Bu sebeple verilerimizi karşı tarafa iletirken şifrelemeye ihtiyaç duyarız. Şifreleme protokolleri kablosuz ağ içinde veri iletişiminin güvenliğini sağlayan bir dizi kurallar bütünüdür. Veri bir taraftan diğer tarafa iletilirken uyulması gereken kuralların genel çerçevesini çizer. Bu sayede mesajın şifrelenmesi sağlanabilir. Günümüzde mevcut birçok şifreleme protokolü vardır fakat bunlardan bazıları gerçekten eski ve korumasızdır. Bu sebepler kablosuz ağımıza şifreleme protokolü seçerken güncel ve sağlam şifreleme protokolleri seçmemiz gerekmektedir. Örneğin, WEP eski ve zayıf protokollerden bir tanesidir. Bu sebepler kablosuz ağınız için bu sistemi kullanmaktan kaçınmalısınız. Bunun yerine WPA2 ve WPA3 gibi güncel ve güçlü protokoller kullanabilirsiniz.

Şifreleme Algoritmaları

Şifreleme algoritmaları ise şifreleme protokolü ile uyumlu olarak çalışan verileri şifreleyen ve şifrelenmiş veriyi geri çözen bir dizi matematiksel işlemler zinciridir. Şifreleme algoritmalarının bir çalışma sırası vardır ve işlemlerini bu sıraya göre yapar. Şifreleme protokolleri mevcut tüm şifreleme algoritmalar ile çalışamaz. Her birinin uyumlu olduğu şifreleme algoritmaları vardır. Mevcut şifreleme algoritmalarının da güçlü ve zayıf olanları vardır. Bu sebeple şifreleme algoritmasının da seçimine dikkat etmeniz gerekmektedir. Örnek olarak, WPA2 ve WPA 3, AES şifreleme algoritmasını destekler. AES geniş kullanım aralığına sahip ve mevcut bir zayıflığı bulunmayan bir şifreleme algoritmasıdır.

Mac Adresi Filtreleme

Bir diğer önemli güvenlik önlemi de mac adresi filtrelemedir. Mac adresi her cihaz için benzersiz (uniq) bir değerdir bu sebeple yer yüzünde aynı mac adresine sahip iki cihaz olamaz. Mac adresi filtrelemesi yaparak sadece izin verdiğimiz aygıtların sisteme erişimin sağlayabiliriz. Böylece, sisteme izin cihaz erişimini engellemiş oluruz. WPA3 için daha güçlü bir şifreleme algoritması olan SAE da kullanılabilir.

Vpn

Özellikle büyük organizasyonlarda, şirketlerde ve kurumlarda vpn kullanımı yaygındır. Vpn ile şirket çalışanları evden kurumun iç ağına güvenli bir şekilde bağlanabilir. Vpn iki network arasında bir tünelleme yaparak bir uçtaki cihazı bir diğer uca bağlanmasına olanak sağlamaktadır. Vpn'nin tek avantajı kişiyi evden kurum ağına bağlaması değildir. Aynı zamanda güvenli veri iletişimi de sağlar. Buna ek olarak Vpn, kurum ağına bağlanna cihazın kimlik ve veri kontrolü yapılmasını da mümkün hale getirmektedir.

Ağ Üzerinde Kimlik Tanıma İşlemi

Kablosuz ağa bağlanmak isteyen kişilerin kimliklerini kontrol ederek kablosuz ağa dahil etme işlemidir. Söz konusu işlem kurumsal kablosuz ağlarda uygulanır ve kimlik doğrulama sunucusu, radius sunucusu yada AAA (Authentication, Authorization, Accounting) sunucu ile gerçekleştirilebilir.Bazen hepsi bir arada da kullanılabilir. Bu ağın büyüklüğü ve karmaşıklığı ile ilgilidir. Ayrıca söz konusu işlemleri gerçekleştirmek için kimlik doğrulama protokolleri de kullanılır.

Misafir Ağ

Hem ev hem de kurumlarda konuklar (normalde çalışan olmayan harici kullanıcılar) için ayrı bir kablosuz ağ oluşturulmasına misafir ağ adı verilir. Misafir ağ kablosuz ağ güvenliği için çok önemli konulardan bir tanesidir. Öncelikle şifre ve parolanın dışarı sızmasını engeller çünkü misafir için ayrı bir ağ adı ve şifresi oluşturulur. Ayrıca bu ağ diğer ağdan yalıtılmıştır, bu sebeple misafir kullanıcının ağ içi cihazlara erişimi sınırlıdır. Son olarak izlemeyi kolaylaştırır. Misafir kullanıcının ağ içinde yaptığı aktiviteleri izlenmesini daha kolay hale getirir. Misafir ağ günümüzde pek çok cihaz tarafından desteklenen yazılımsal bir fonksiyondur. Default olarak kapalıdır ve router arayüzünden aktif hale getirilebilir.Örnek olarak, EAPkullanılabilir. (Extensible Authentication Protocol)

Firewall

Firewall ile kablosuz ağdaki paketleri filtreleyebilir ve güvenlik riski oluşturan portları erişime kapatabiliriz. Firewall ayrıca vpn bağlantılarına izin verebilir ve gelen vpn bağlantılarını denetleyebilir. Ayrıca gelişmiş firewall donanımları ve bunların yazılımları ile ağ içinde trafiği izleme ve kontrol işlemleri kolaylaştırılabilir. Bu tarz firewaller kurumsal kablosuz ağlar için tercih edilir ve dışarıdan gelen tehditleri algılayarak buna göre davranışlarda bulunabilir. Bu tarz sistemlere yazılım tabanlı IDS/IPS sistemleri de denir. Ayrıca next genaretion firewaller;URL filtreleme, antivirüs taraması, güvenlik duvarı çapında veri şifrelemesi gibi ileri düzey güvenlik önlemleri de içerebilir.

Yazılım Güncelleme

Pek çok kullanıcı tarafından önemsenmeyen fakat hayati öneme sahip bir husustur yazılım güncelleme. Özellikle kablosuz ağlar gibi dış kullanıcıların saldırısına her an açık olan ağdaki donanımların yazılımları her daim güncel olmak zorundadır. Pek çok firma donanımlarına uzun dönem yazılım desteği sağlayarak özellikle kurumsal taraftaki müşterilerini kendilerinde tutmak istemektedir. Bu sebeple, firewall, router ve accesspoint gibi kablosuz ağdaki yazılımlar daima en güncel sürümleri ile kullanılmalı ki ortaya çıkan zafiyetler yazılımsal olarak bertaraf edilebilsin. Aksi durumda hackerler tarafından bu zafiyetler sömürülebilir ve kablosuz ağınıza sızılabilir.

Sinyal Düşürücü Malzemeler

RF Kalkanlı boya ve film gibi malzemeler ile kablosuz ağ sinyalleri bulunduğunuz konumun dışarısına gitmesini engellemek ya da sinyal gücünü düşürmek için kullanılabilir. Bu sayede kablosuz ağ sinyalleri belli bir bölge ile sınırlı kalır ve network dış tehditlerden önemli ölçüde korunmuş olur.

Kablosuz ağlara en çok uygulanan saldırılar ve korunma yöntemleri:

Yukarıda kablosuz ağları korumak için uygulanabilecek güvenlik önlemlerinden bahsettik. Şimdi biraz da kablosuz ağlara uygulanan saldırı yöntemlerinden bahsedelim. Kısaca hangi korunma yöntemleri bu saldırıları engelleyebilir belirtelim.

DoS (Denial of Service) Saldırısı

Kablosuz ağın hizmet vermesini engellemek veya durdurmak için yoğun trafik yaratan saldırı türü.

Önlem: Firewall kullanımı, doğru konfigrasyonu ve düzenli güncellenmesi.

Trafik filtreleme ve sınırlama yapmak. Bant genişliğini düzenlemek.

Man-in-the-Middle (MitM) Saldırısı

Saldırganın iletişimde araya girerek iletişimi dinlemesi ve çeşitli bilgileri ele geçirmesini tanımlayan saldırı türüdür.

Önlem: Güçlü şifreleme protokolleri kullanmak. Vpn kullanmak.

Evil Twin Saldırısı

Saldırgan varolan bir kablosuz ağın adını kullanarak ağı taklit etmeye çalışır. Bu sayede ağa bağlanmaya çalıian kişilerin verilerini çalabilir yada söz konusu ağın şifresini elegeçirebilir.

Önlem: SSID gizleme, doğru ağ bağlantısı için setifikasyonları kontrol etme ve otomatik ağa bağlanmayı iptal etmek olabilir.

Rogue AP (Sahte Erişim Noktası) Saldırısı

Saldırgan sahte erişim noktaları yaratarak ağ üzerinden verileri çalmaya çalıştığı yöntemdir.

Önlem: Ağ erişim noktalarını sıklıkla kontrol etmek, izinsiz açılanları hemen sistemden atmak. WPA2 ve WPA3 gibi güncel şifreleme protokolleri kullanmak. Ağdaki ilgili yazılımların güncellemelerini düzenli olarak güncellemek.

Kaynakça

https://tldp.org/HOWTO/Secure-Programs-HOWTO/crypto.html

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri

https://www.researchgate.net/publication/320531569_Kablosuz_Ag_Teknolojileri_ve_Sifreleme

https://medium.com/kodx-platform/kablosuz-a%C4%9F-g%C3%BCvenli%CC%87%C4%9Fi%CC%87-%C5%9Fi%CC%87freleme-algori%CC%87tmalari-ve-wpa-3-protokol%C3%BC-1cb2cac366b4

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri

https://ahmetemindilben.com.tr/evil-twin-saldirisi-nedir-nasil-yapilir/
https://www.beyaz.net/tr/guvenlik/makaleler/ortadaki_adam_mitm_saldirisi_nedir.html

https://medium.com/swlh/5-effective-ways-to-tackle-your-wireless-security-f5f0cb41d1f1

https://medium.com/technology-hits/5-methods-for-improving-your-wireless-security-b5e5f2f32c79

https://aws.amazon.com/tr/what-is/vpn/

Ömer Kızılgedik

omerkizilgedik@gmail.com