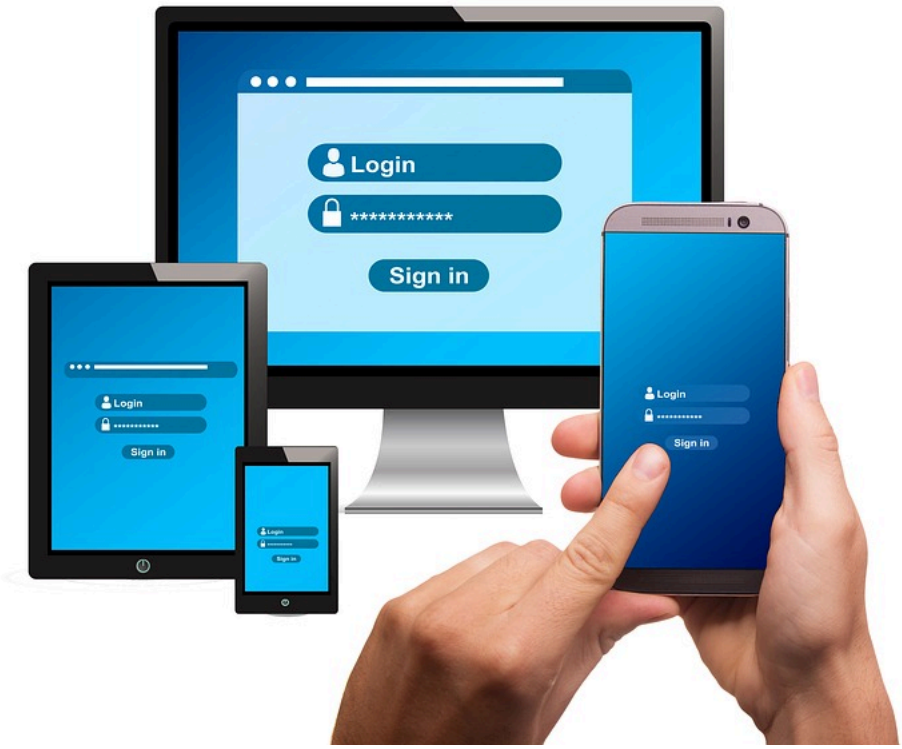
Kablosuz Ağ & Modem Güvenliği

Günümüz teknoloji çağında artık birçok ev ve işyerinde internet bağlantısı mevcuttur. Bilgisayarların, laptopların, tabletlerin, mobil aygıtların ve hatta televizyonların bile internete bağlanabildiği bir çağın içindeyiz.

“Benim başıma gelmez” şeklindeki düşünenler saldırganların sadece önemli olabilecek bilgileri almaya odaklandığını düşünmemelidir. Önemsiz gibi gözüken bazı bilgiler saldırgan için büyük öneme sahip olabilir. Bu gibi durumlarla mücadele etmek için her kullanıcının cihazının hassas bilgiler içerdiğini düşünmesi ve gerekli güvenlik önlemlerini alması gerekmektedir. İnternete, kablosuz erişim cihazı ile (bir dizüstü bilgisayar ya da tablet) halka açık bir erişim noktasından bağlanıldığında uzaktaki saldırganların olası ihlallerine açık hale gelinebilir. Aşağıdaki güvenlik önlemleri bu saldırganlara karşı korunmasının sağlanması açısından yardımcı olacaktır.

- Kablosuz cihazın sahibinin cihazını erişiminin uzağında başıboş bırakmaması gerekmektedir.
- Cihazın açılış şifresinin daima kolayca tahmin edilmeyecek bir şifre olmasına özen gösterilmelidir.
- Kablosuz özelliğinin, kullanılmadığı durumlarda kapalı bırakılması gerekmektedir. Öyle ki Wi-Fi Infrared ve Bluetooth cihazlar bu özellikleri açık olduğunda kendilerini ortama sürekli anons ederler. Bu durumda saldırganlar tarafından bulunması kolaylaşır.
- Kablosuz cihaz ağ donanımının güncel tutulması: Ağ cihazı donanımı aslında basit bir yazılım içerdiğinden diğer her yazılım gibi saldırılara açıktır. Bu cihazların sürücülerinin güncel tutulması son seviye güvenlik önlemi desteğinin de alınması anlamına gelir. Güncellenmeyen yazılımlar saldırılara açıktır.
  Kablosuz özellikli cihazın güncel virüs yazılımıyla korunması ve güvenlik duvarının sürekli aktif olduğundan emin olunması gerekmektedir. Böylece virüs ve casus yazılımlara karşı risk en aza indirilmiş olur.
- Hassas / Kişisel bilgilerin şifrelenmesi: Cihaz şifrelenmiş ise yetkisiz bir kişi cihaza erişse bile şifrelemeyle hassas bilgilerin çıkarcı ellere geçmesi engellenmiş olur.
- Kablosuz özelliği sağlayan donanımın kaynak paylaşım özelliğinin kapatılması: Dosyaların paylaşılması bu dosyaların değiştirilebileceği veya silinebileceği anlamına gelebilir.
- Halka açık kablosuz cihazların tercih edilen bağlantı noktaları listesinden silinmesi: Bazı işletim sistemleri kişiye özel tercih edilen kablosuz bağlantı noktaları listesi oluşturulmasına izin verir. Bu listeye sahip olan cihazlar ortamda öncelikle bu kablosuz ağları ararlar. Eğer saldırgan kendi cihazını bu cihazları taklit edecek şekilde ayarlarsa hedefteki cihaz saldırganın kablosuz cihazına otomatik olarak bağlanır ve bilgi göndermeye başlar.
- Kablosuz Ad-Hoc Modu özelliğinin kapatılması: “Ad-hoc” özelliği, cihazın diğer bilgisayarlarla kablosuz bir bağlantı üstünden minimum güvenlik gereksinimiyle doğrudan bağlanmasını sağlar. Saldırganların bilgilere ve kaynaklara erişimini engellemek için bu özellik kapatılmalıdır.
- Hem kablosuz hem de kablolu ağ bağlantısının aynı anda kullanılmaması gerekmektedir. Kablosuz ağ üstünden cihaza bağlanan saldırgan köprüleme modu (bridge mode) açıksa kablolu bağlantı arkasındaki cihazlara bağlanabilir.



- Kablosuz Ağ bağlantı sayfasının gerçek olduğuna dikkat edilmelidir: Kullanıcılar kablosuz ağ bağlantı sayfaları aracılığıyla istenen bilgileri girdikten sonra kablosuz ağa bağlanabilirler. Bu sayfalar saldırganlar için caydırıcıdır. Ancak saldırgan bu sayfanın sahtesini yaparak kullanıcıların bilgilerini

çalmayı amaçlar. Bu sebeple halka açık kablosuz ağları kullanmadan önce giriş yapılan sayfaların gerçek olup olmadığı sertifika bilgisinden kontrol edilmelidir.

- Hassas/Kişisel bilgilerin halka açık kablosuz ağlar üstünden gönderilmemesine dikkat edilmelidir: Halka açık kablosuz ağların genellikle güvensiz olduğu düşünülür. Belirli güvenlik önlemlerini almadan hassas bilgilerin kablosuz ağlar üstünden gönderilmesi önerilmez.
- Kablosuz ağlar üstünden kurumsal ağlara bağlanırken ilgili kurumun sunduğu şifrelenmiş özel ağın kullanılması gerekmektedir. Bu programlar bilgileri şifreleyerek göndereceğinden saldırganların bilgileri elde etmelerini engeller. Her özel şifrelenmiş ağ programına güvenilmemelidir.
- Modeme özel yönetim sayfasına girerek varsayılan erişim şifresinin değiştirilmesi gerekmektedir.

Modemin üstünde yazan kablosuz ağ şifresi genellikle karışıktır ve yeterince güvenlidir. Bu şifrenin kimseyle paylaşılmaması gerekmektedir.

- Modemin ara yüzünden MAC adresi filtrelemesi yapılması, WPA-WPA2 şifreleme algoritmalarının kullanılması önemli bir güvenlik önlemi alınması anlamına gelmektedir.
- Modeme bağlanmak için kullanılan SSID adının değiştirilmesi ve hatta gizlenmesi başka cihazların kablosuz ağı görmesini engeller.

Kablosuz ağ güvenliğiyle ilgili ayarların nasıl yapıldığını gösteren bir video aşağıdaki linkten izlenebilir.

- https://www.guvenliweb.org.tr/dokuman-detay/kablosuz-ag-modem-guvenligi
- https://www.infosec.gov.hk/english/yourself/wireless_3.html
- https://resources.infosecinstitute.com/10-crucial-end-user-security-tips/

ETİKETLER

#KablosuzAğ #Modem