GÜVENLİ GÜNLER BÜLTENİ

Bilgisayar kullanıcılarına yönelik hazırlanır. Her ayın 15'i çıkar. Diğer sayılara erişmek ve sonraki mesajların direk posta kutunuza gelmesi için guvenligunler.com adresini ziyaret ediniz.

OCAK 2019

Ücretsiz Internet mi? Elbette...

***GÜNÜMÜZ DÜNYASINDA** bir anımızın bile bağlantısız geçmesini istemiyoruz; öyle bir duruma dayanamıyoruz, kendimizi eksik hissediyoruz. Evde, tatilde, yolda, arabada, uçakta, hatta abartıp araç kullanırken bile bağlantıda olanları maalesef görüyoruz.*

Bu yazıda, kullandığımız cihazların bağlantılarını ele almak yerine, bu cihazları kullanan bizlerin bağlantı alışkanlıklarından, aldığımız risklerden ve riskleri azaltmak için uygulayabileceğimiz çözüm önerilerinden bahsetmek istiyorum.

Bizi Hangi Riskler Bekliyor

Örneğin bir mekâna vardık, elimizde telefonumuz var, iç sesimizi dinleyip bedava internet var mıdır diye şöyle bir kontrol eder miyiz? İnternet hattımızın bakiyesine bağlı olarak cevabımız değişebilir. Ancak aynı soruyu yurtdışına çıkmış bir yurdum insanına sorsak kesinlikle cevabı "elbette" olacaktır.

Halka açık Wifi bağlantılar bir takım riskleri de beraberinde getirir

Bedava internet bağlantıları çoğunlukla şifresiz olarak kullanımımıza sunulur. Ancak bir şifresiz ağa bağlandığımızda cihazımız ile bağlantı

noktası arasında gidip gelen trafiğin arasına girilmesi (Man in the Middle Attack) mümkündür. Böylelikle cihazımızdaki bütün işlemlerimiz de izlenebilmektedir. En azından, cihazımızla ilgili pek çok bilgi paylaşılabilir, bu bağlantıyı kullanarak yaptığımız iletişim dinlenilebilir

Benzer bir durumda ise, ücretsiz bir ağa bağlandığınızı zannedip aslında kötü niyetli *hacker*'ların kendi sahte ağlarına bağlanmış olabilirsiniz. Bir örnekle anlatmaya çalışalım. Diyelim ki bir otel odasındasınız ve ücretsiz ağa bağlanmak için elinizdeki telefonla ücretsiz ağ arıyorsunuz. Hemen yakındaki bir *hacker* sizi kandırmak için halka açık Wifi sinyali süsü vererek kendi bağlantılarını size kullandırabilir. Otelin adına benzer bir adla yayın yapmakta olduğunu düşünelim. Haliyle bu sahte ağa bağlanırsanız *hacker*'ın eline düşmüş olursunuz. Bu andan itibaren de internet ile aranızda *hacker* vardır ve yaptığınız her işlemi görecektir.

Güzelce bağlanırsınız, bağlantıya devam etmek için size önerdikleri casus uygulamayı da kendi ellerinizle yüklersiniz, ondan sonra da her yaptığınız işlem ekran çıktıları ile birlikte siber suçluların kendi belirledikleri bir merkeze aktarılır ve cihazınızın içindeki en ince ayrıntı bile ele geçirilir.

Bitti mi? Aksine daha yeni başladı. Bir süre sonra aynı cihazla şirket ağına bağlanırsınız. Siber suçluların en istedikleri davranış budur. Böylece sizin bedava yapmış olduğunuz internet bağlantısı, şirketiniz için de bir riske dönüşmüş olur. Şirket ağından eriştiğiniz bütün bilgiler ise soluğu siber suçluların merkezinde alır.

Bedava internet sağlayana güvendik, şirketimizin bilgilerinin kötü niyetli kişilerin eline geçmesinde piyon olduk.

Güven, teknolojinin en zayıf bileşeni

Yukarıda anlattığımız senaryonun yanı sıra bazen gerçekten de güvensiz bir ağa bağlanmak zorunda kalabilirsiniz. Belki "denize düşen yılana sarılır" misali, zorunluluk sonucu başınıza her insanın karşılaşabileceği bir durum gelebilir. O nedenle, bu tür durumlarda almanız gereken önlemleri inceleyelim.

Alınabilecek Önlemler

Senaryodaki riskleri azaltmak hiç de sanıldığı kadar zor değildir. Diyelim ki bir bedava internet noktasına bağlandık. Bizi izleme ihtimali olan kötü amaçlı kişileri bizimle uğraştıklarına pişman etmek için çaba harcamalıyız. Çok genel ama bizi çoğu

tehlikeden koruyacak olan önlemlerin birkaçını listeleyelim :

1. Ücretsiz bir noktaya bağlandığınızda *online* alışveriş ya da finansal işlem yapmayın; hatta hassas bilgilerinizi vermeniz gereken hiçbir işlem yapmayın.
2. Şirket ağına bağlanırken mümkünse iki faktör doğrulama ile VPN bağlantısı kurun. Bu sizin iletişiminizi güvenli hale getirerek Wifi ile açtığınız kapıyı bir nebze de olsa kapatacaktır.
3. SSL bağlantısı ile siteleri kullanın. http:// ile başlayan siteler yerine https:// ile başlayan siteleri tercih edin. Böylelikle bağlantı kurduğunuz site ile cihazınız arasındaki bağ şifreli olarak gerçekleşecektir.
4. Mobil cihazınızın otomatik Wifi bağlantısı yapma özelliğini kapatın. Bu, kontrolünüz dışında bir bağlantıya engel olmanızı sağlar.
5. Kullanmadığınız zamanlarda Wifi bağlantısını kapatın. Örneğin bir doküman hazırlıyorsanız, internet ihtiyacınız yokken Wifi bağlantısını kapatmak, arka planda kurulma ihtimali olan güvenlik seviyesi düşük bağlantıları engelleyecektir.
6. Mobil cihazınızın Bluetooth bağlantısını izleyin, kontrol altında tutun. Veri transferine açık olmadığından emin olun.
7. Cihazınızı koruma altına alın. Virus ve Malware engelleyen yazılımların kurulu ve çalışır vaziyette olmasına dikkat edin. Bu koruma yollarını uygulamanın, daha önceden yani "yılana sarılmadan, denize düşmeden" alınması gereken bir önlem olduğunu bilin.

Özetle, "bedava sirke baldan tatlıdır" atasözünü internete bağlanma felsefeniz haline getirmeden önce, hem kendinizi hem de şirketinizi siber saldırganlar için kolay lokma haline getirebileceğinizi hatırlayın.

YAZAR HAKKINDA

Bülent Muşlu lisans ve yüksek lisans eğitimini İTÜ Bilgisayar Mühendisliği bölümünde tamamladıktan sonra 1991 yılından beri Bilgi Teknolojileri sektöründe kurumsal ve uluslararası şirketlerde görev yapmıştır. Uzun yıllar Unix konusunda uzmanlık yaptıktan sonra tecrübelerini eğitmen olarak sektöre aktarmış, ardından ITIL Expert sertifikası ile birlikte Service Management konusunda çalışmıştır. Çalışma hayatını BKM'de Bilgi Güvenliği, BT Uyum ve Hizmet Yönetimi Direktörü olarak devam ettiren Bülent Muşlu, ISO 22301LA, ISO27001LA, Certified Ethical Hacker sertifikalarına sahiptir.