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.

TEMMUZ 2017

Nesnelerin İnterneti ve Güvenlik

GÜNÜMÜZDE BİLGİSAYARLARIN YANI SIRA tabletler, cep telefonları, akıllı saatler, video kameralar, akıllı televizyonlar ve hatta lambalar, termostatlar, arabalar, drone'lar/İHA'lar (insansız hava araçları), sağlıklı yaşam için kullanılan cihazlar, tuvaletler – evet doğru okudunuz – internete bir biçimde "bağlı" durumda.

Bu sayede odasında uyumakta olan bebeklerin seslerini uzaktan duyabiliyor; dışarıdan evdeki bakıcının davranışlarını takip edebiliyor; favori programlarımızı daha sonra izlemek üzere kaydedebiliyor; odamızın sıcaklık ayarını yapıp, istediğimiz odanın ışığını açıp kapayabiliyoruz. Hatta gerekirse sifonu bile uzaktan çekebiliyoruz – bu son örnek ne kadar gerekli tabii ki tartışılabilir!

Gartner'a göre 2020 yılına kadar 20 milyar nesnenin internete bağlanması bekleniyor. Peki ama internete bağlı olan (veya bağlanacak) bu nesnelerin güvenliği ne durumda?

Açıkçası çoğu firmanın internete bağlı nesnelerde kullanım kolaylığını ön planda tutarak, güvenliği ikinci planda bıraktıkları gözleniyor.[1] Örneğin Şubat 2017'de, çok ünlü bir akıllı televizyon üreticisinin, kullanıcı televizyon izlerken elde edilen çeşitli bilgileri (kullanım saatleri, seyredilen kanallar, vb.) daha sonra reklam verenler ile paylaşmak üzere şirket merkezine gönderdiği ortaya çıktı. Başka bir akıllı televizyonda yer alan açık nedeniyle de, kötü niyetli kişilerin akıllı televizyon sahibinin Facebook hesabına girebildiği saptandı. Nisan 2017'de Dallas'ta, şehirdeki tüm sirenlerin çalışmasını sağlayan kötü niyetli kişiler,

şehirdekilerin ciddi bir saldırı altında olduklarını zannetmelerine yol açtı. Çin'de bazı öğrenciler, popüler bir arabayı "kırarak", uzaktan kapıların açılmasını, yağmur sileceklerinin çalışmasını sağladılar. Bu nedenle yüz binlerce araç üretici firma tarafından geri çağrıldı.

Örnekleri çoğaltmak mümkün, Amerika'da bebeklerin izlenmesi için kullanılan sesli/görüntülü cihazları kıran saldırganlar, gecenin bir yarısı bağırarak bebeklerin uyanmasına yol açtılar. Akıllı tuvaletleri hedefleyen bir grup araştırma görevlisi, bu cihazların kolaylıkla uzaktan "ele geçirilebileceğini", sürekli olarak uzaktan sifonun çalıştırılması nedeniyle su kullanımının çok yüksek düzeylere çıkarılabileceğini gösterdiler.

Henüz "ele geçirilerek" uzaktan kilitleri açılan kapıları, odaların/binaların değiştirilen sıcaklık düzeylerini konuşmaya başlamadık bile!

Peki kullanıcıların bu konudaki farkındalığı hakkında ne söyleyebiliriz? Bu bağlamda, 2016 yılında McAfee (Intel Security)[2] tarafından yapılan araştırma oldukça çarpıcı bilgiler içermekte:

- Kullanıcıların %79'u aldıkları internete bağlanabilen nesneyi hemen kullanmaya başlıyor,
- Bu kullanıcıların sadece %42'si nesneyi kullanmadan önce güvenlik önlemlerini aldığını düşünüyor.

Söz konusu nesnelerin güvenlik zafiyetlerine ilişkin kullanıcı farkındalığı ise hiç iç açıcı değil:

Sonuç olarak internete bağlı nesnelerin güvenliği için bir şeyler yapılması gerektiği açık bir şekilde görünüyor. Kuşkusuz bu noktada öncelikle internete bağlı nesneleri geliştiren firmalara, söz konusu nesnelerin kurulumunu, bakımını, yönetimini, işletimini gerçekleştiren kişilere ve firmalara önemli görevler düşüyor. Ancak acaba bu nesneleri kullanan bizler de güvenlik konusunda bir şeyler yapabilir miyiz?

Bu konuda farklı çalışma grupları[3] tarafından önerilen önlemleri bir kaç ana başlık altında özetleyebiliriz:

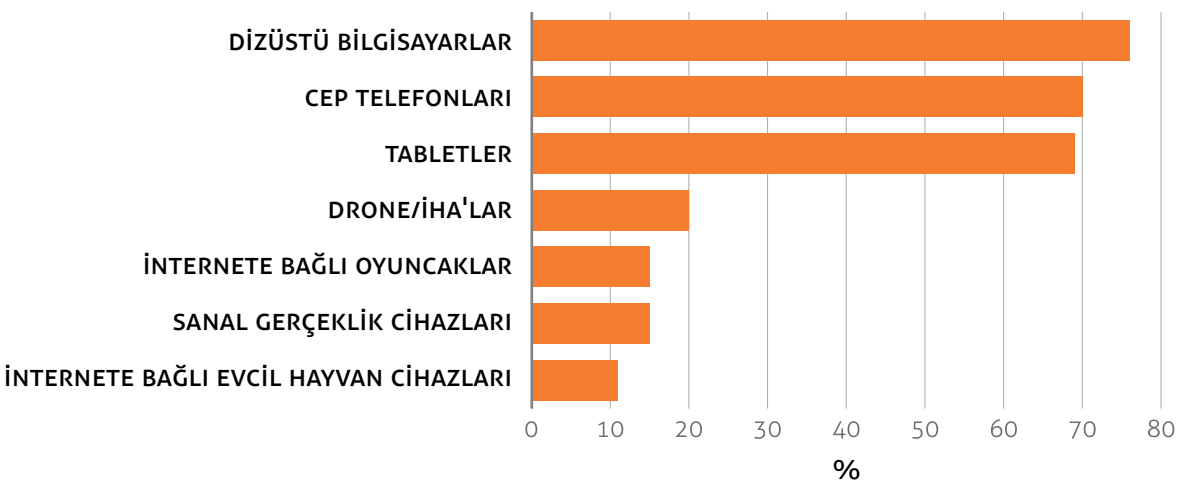
Mobil cihazlarınızı koruyun

İnternete bağlı nesneleri kontrol edebilmek için çoğu zaman cep telefonlarımıza ve tabletlerimize kurduğumuz uygulamaları kullanıyoruz. Gerek bu cihazlarda yer alan kişisel verilerimizi korumak, gerekse internete bağlı nesneleri yönetmek için yararlandığımız uygulamalara kötü niyetli kişilerin erişimini engellemek için, uzun, tahmin edilmesi zor ekran koruyucu parolalarla mobil cihazlarımızı güvenli hale getirmek, basit ama etkili bir çözümdür.

Veri iletişimini güvenli hale getirin

Veri iletişiminin herhangi bir şifreleme olmaksızın gerçekleştirilmesi durumunda, kötü niyetli kişiler kullandıkları çeşitli araçlarla iletilen veriyi rahatlıkla dinleyebilirler. Bu yüzden, veri iletişiminin güvenli bir protokol (Örneğin HTTPS) kullanılarak gerçekleştirilmesi oldukça önemlidir.

Kullanıcıların Güvenlik Zafiyeti Farkındalıkları



Ayarları değiştirin

İnternete bağlı nesneler, genellikle kullanım kolaylığı düşünülerek, çabukça kurulacak şekilde ayarlanmıştır (örneğin "fabrika ayarlarında" bilinen, hazır parolalar bulunabilir). Kullanmakta olduğunuz bütün nesneler üzerinde üretici tarafından önerilen güvenlik önlemlerinin gerçekleştirilmesi ve internete bağlı nesnelerin sadece sizin güvendiğiniz cihazlar ile haberleşmelerinin sağlanması yerinde olacaktır.

Güncellemeleri takip edin

Kullanılan mobil cihazların ve internete bağlı nesnelerin herhangi bir güvenlik zafiyetine sahip olup olmadıklarını kontrol etmek, gerekirse bu cihazlar ve nesneler tarafından kullanılmakta olunan yazılımların (işletim sistemi, vb.) güncellenmesini sağlamak, sizi daha güvenli hale getirecektir.

REFERANSLAR

1. IoT Security Foundation. "How Real are the IoT Security Concerns?". https://iotsecurityfoundation.org/how-real-are-the-iot-security-concerns/
2. "IoT Security and The Consumer: The Challenges and Education Question". https://www.i-scoop.eu/iot-security-consumer-education/
3. OWASP. "Consumer IoT Security Guidance". https://www.owasp.org/index.php/IoT_Security_Guidance#Consumer_IoT_wSecurity_Guidance

YAZAR HAKKINDA

Fırat Okay uzun yıllar BT altyapısı, sistem, ağ ve bilgi güvenliği konularında yurt içinde ve dışında eğitimler verdi, birçok projede görev aldı. BT Hizmet Yönetimi ve BT Yönetişimi konularında çalışmaya devam etmektedir. Kendisine firat@bir618.com adresinden ulaşabilirsiniz.

YASAL UYARI

Bu dokümanın tüm hakları Lostar Bilgi Güvenliği A.Ş.'ye aittir ve Creative Commons BY-NC-ND 4.0 (Attribution-NonCommercial-NoDerivatives 4.0 International - (CC BY-NC-ND 4.0) lisansı altında dağıtılır. Herhangi bir değişiklik yapmadan kaynak gösterilerek dağıtılabilir. Ticari olarak kullanılamaz.