OUCH! | Ağustos 2018

OUCH!

SANS SECURITY AWARENESS

Herkes İçin Aylık Güvenlik Farkındalığı Bülteni

Akıllı Ev Cihazları

Akıllı Ev Cihazları Nelerdir?

Eskiden sadece bilgisayarınız, akıllı telefonunuz veya oyun konsolunuz gibi birkaç cihazınız evinizden internete bağlanırdı. Ancak günümüzde ampülleriniz ve televizyonunuza bağlanan hoparlörlere, kapınızdaki hatta arabanızdaki kilite kadar giderek artan sayıda cihaz internete bağlanıyor. Çok yakın bir gelecekte neredeyse evinizdeki bütün cihazlar internete bağlanabilecek. Bu bağlı cihazlar nesnelerin interneti (IoT) veya Akıllı Ev Cihazları (Smart Home Devices) olarak isimlendirilmektedir. Tüm bu cihazlar hayatımıza büyük kolaylıklar getiridiği gibi, kendine özgü tehlikeleri de barındırmaktadır.

Problem Nedir?

Ev ağınıza bağlanan cihaz sayısı artıkça, yanlış gidebilecek şeyler de artar. Siber saldırganlar cihazlarınızı başkalarına saldırmak üzere kullanabilir, cihaz sağlayıcıları aktiviteleriniz ile ilgili kapsamlı bir bilgi toplayabilir veya cihazlarınıza bulaşan virüsler onları kullanmanızı engelleyebilir. Akıllı Ev Cihazları üreten pek çok şirketin siber güvenlik ile ilgili tecrübesi bulunmamakta ve güvenliği ek bir maliyet olarak görmektedir. Sonuç olarak satın almış olduğunuz pek çok cihazda çok az güvenlik önlemi vardır ya da neredeyse hiçbir güvenlik önlemi yoktur. Örneğin bazı cihazların oldukça bilinen varsayılan parolaları vardır ya da bu parolalar güncellenememekte veya konfigüre edilememektedir.

Kendimi Nasıl Koruyabilirim?

Peki, ne yapabilirsiniz? Akıllı ev cihazlarınızdan yararlanmanızı kesinlikle istiyoruz, ama güvenle. Bu cihazlar hayatınızı kolaylaştırmak için muhteşem özellikler sunmaktadır. Ek olarak teknolojinin gelişmesiyle birlikte akıllı cihazları kullanmak dışında bir seçeneğiniz de olmayabilir. Kendinizi koruyabilmeniz için uygulamanız gereken temel adımları sıralayalım:

Sadece İhtiyacınız Olan Cihazları Bağlayın: Güvende olmanın en basit yöntemi cihazınızı gerekmediği sürece internete bağlamamaktır. Eğer kullandığınız bir cihazın çevirimiçi olmasına ihtiyacınız yok ise onu Wi-Fi ağınıza bağlamayın. Tost makinanızın telefonunuza bilgilendirme göndermesine gerçekten ihtiyacınız var mı?

Neyi Bağladığınızı Bilin: Ev ağınıza hangi cihazlar bağlı? Emin değil misiniz ya da hatırlamıyor musunuz? Kablosuz ağınızı düğmesinden kapatın ve nelerin artık çalışmadığını görün. Herşeyi farkedemeyebilirsiniz fakat bağlı olduğu unuttuğunuz ne kadar çok cihaz olduğuna şaşıracaksınız.

Güncel tutun: Tıpkı bilgisayarınız ve mobil cihazlarınız gibi, sahip olduğunuz akıllı cihazlarınızın da güncel olması kritik derecede önemlidir. Eğer cihazınızın otomatik güncelleme yapma özelliği var ise, aktif hale getirin.

Parolalar: Cihazlarınızdaki parolaları sadece sizin bildiğiniz, benzersiz ve güçlü bir parola ile değiştirin. Büyük olasılıkla bunları sadece bir defa girmek zorunda kalacaksınız. Tüm parolalarınızı hatırlayamıyor musunuz? Endişelenmeyin, biz de hatırlayamıyoruz. Onları güvenli bir şekilde saklamak için bir parola yöneticisi kullanmayı düşünün.

Gizlilik Seçenekleri: Eğer cihazınız gizlilik seçeneklerini değiştirmenize izin veriyorsa, topladığı ya da paylaştığı bilgileri sınırlayın. Bir seçenek, basitçe bilgi paylaşım özelliklerini devre dışı bırakmak olabilir.

Cihaz Sağlayıcıları: Cihazlarınızı bildiğiniz ve güvendiğiniz sağlayıcılardan satın alın. Otomatik güncelleme, varsayılan parolaları ve gizlilik ayarlarını değiştirme gibi güvenlik desteği olan ürünleri tercih edin.

Her Zaman Dinleme: Eğer bir cihaz sizin sesli komutlarınızı anlıyorsa, ortamı sürekli olarak dinliyordur. Örneğin, Alexa ve Google Ev cihazlarınız hassas içerikli konuşmalarınızı kaydedebilir. Cihazlarınızı yerleştireceğiniz yeri belirleken bunu göz önünde bulundurun ve gizlilik seçeneklerini gözden geçirin.

Misafir Ağı: Akıllı Ev cihazlarınızı, bilgisayarlarınız ve mobil cihazlarınız için kullandığınız birincil Wi-Fi ağı yerine ayrı bir "Misafir" Wi-Fi ağına koymayı değerlendirin. Bu şekilde, herhangi bir Akıllı Cihaz enfekte olursa, birincil ağınızdaki bilgisayarlarınız veya mobil cihazlarınız güvende kalmaya devam edebilir.

Yeni teknolojilerden korkmak için hiçbir neden yoktur, ancak barındırdıkları riskleri anlamalısınız. Bu basit birkaç adımı uygulamak, çok daha güvenli bir Akıllı Ev oluşturmanıza yardımcı olacaktır.

Türkçe Çevirisi

Selma Süloğlu, ODTÜ Bilgisayar Mühendisliğinde doktorasını tamamlamış olup Hawaii Üniversitesinde yazılım mimarileri ve yazılım güvenliği üzerinde doktora sonrası araştırma yapmaktadır.

Sema Yüce, Türkiye'nin önde gelen kurumsal şirketlerinde ve özellikle bilişim, finans, telekomünikasyon, sigortacılık, sanayi, perakendecilik gibi sektörlerde; bilgi güvenliği, uyum, BT yönetişim/strateji, risk yönetimi, iş sürekliliği, hizmet yönetimi, altyapı hizmetleri, yazılım geliştirme ve program/proje yönetimi alanlarında yönetici ve danışman olarak 19 yılı aşkın süre görev yaptıktan sonra, Truth ISC (www.truth-isc.uk) adıyla kurduğu Türkiye ve İngiltere'de faaliyet gösteren danışmanlık şirketinde hizmet vermeye devam etmektedir.

Konuk Yazar

Robert M. Lee *(@RobertMLee) SANS Sertifikalı eğitmen ve FOR578 – Siber Tehdit İstihbaratı ve ICS515 - ICS Aktif Savunma ve Olaylara Yanıt kitaplarının yazarıdır. Robert aynı zamanda Dragos isimli endüstriyel siber güvenlik şirketinin kurucusu ve CEO'sudur.*

Kaynaklar

Parolalar:	https://www.sans.org/u/GEB
Parola Yöneticileri:	https://www.sans.org/u/GEG
Ev Ağınızı Güvenli Hale Getirmek:	https://www.sans.org/u/GEL