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.

ŞUBAT 2018

Akıllı TV'niz de Sizi İzliyor mu?

YERLİ SİNEMAMIZIN O GÜZEL "ZEKİ MÜREN DE BİZİ GÖRECEK Mİ?" REPLİĞİNE bu yazıda yer vermeyip, yaşanmış küçük bir anekdotu anlatmak istiyorum. Rahmetli babaannem bütün ömrünü köyde geçirmişti ve televizyonla ilk kez, esnaf olan kardeşinin ilçedeki evinde, 70'li yıllarda tanışmıştı.

Televizyon açılıp birden Bülent Ecevit'i karşısında görünce de hemen telaşlı bir şekilde örtüsünü başına alıvermişti. Kadıncağız yıllar sonra bile bizlere espri konusu olmaktan kurtulamamıştı.

O yıllardan bu yana köprülerin altından çok sular aktı. Yıllar geçerken cihazlar da akıllanıp yüzlercesi gündelik yaşamımıza girdi ve girmeye de devam edecek gibi görünüyor. Gün geçmiyor ki "bu da mı akıllandı" dediğimiz bir cihaz daha teknolojinin toz tutmayan raflarında yerini almasın. Ancak henüz hâlâ birçoğumuz evimizde akıllı tost makinesi ve akıllı yumurta pişirme cihazı kullanmadığımız için, telefonlarımızdan sonra en çok karşılaştığımız akıllı cihaz olan ve kendisinden gözlerimizi saatlerce alamadığımız akıllı TV'lerimizin güvenliği ile ilgili bir iki ufak ama önemli noktaya değinmek istiyorum. Hepimizin aklına ara sıra geliyordur: Biz güzel güzel akıllı TV'mizi izlerken acaba o da bizi izliyor mu?

Önce bilgisayarlarla hayatımıza giren zararlı yazılımlar, akıllı telefonlarımıza yönelik tehditlerle devam etti ve nesnelerin Internet'e bağlanmasıyla

(IOT) birlikte birçok cihazımız tehditlere açık hale geldi. Çoğumuzun evinde bulunan akıllı TV'ler de Internet'e bağlı diğer cihazlarımız gibi tehdit altında. Aslında cihazlarımızdan çok bizler tehdit altındayız. Tehditlerin amaçları farklı farklı; bazıları kullanıcı adı ve şifrelerini hedeflerken, bazıları kredi kartı bilgilerini ele geçirmeyi, bazıları da daha masum görünen kullanıcı alışkanlıklarını takip edip bu bilgileri reklam vs. şirketlerine satmayı hedefliyor. Ayrıca özel hayatın içine girilmesi gibi niyetler de olabilir ki en can sıkıcılarından biri bu olsa gerek.

Akıllı TV'lerin taşıdığı riskleri daha etkili yapan etkenlerden biri, bilgisayarlardan ve telefonlardan gelebilecek risklere karşı çoğumuzda farkındalık oluşmuş bulunmasına karşılık, bir bilgisayardan farkı olmayan akıllı TV'ler için gerekli duyarlılığın henüz oluşmamasıdır. Diğer bir etken de, akıllı TV'lerin bilgisayarlar gibi Internet'e bağlanıp işlem yapmamıza izin vermesine rağmen, bilgisayarlarda alışkın olduğumuz, bizi zararlı yazılımlara karşı koruyan antivirus/antimalware yazılımları ve firewall'ların daha düne kadar akıllı TV'ler için bulunmamasıdır. Üstelik bu önlemler hem yeni yeni uygulamaya alınmaktadır hem de hâlâ olgunlaşmaya açık yönleri vardır.

2015 yılında Samsung akıllı TV'nin ses tanıma fonksiyonunun, ortamdaki sesleri dinleyip metin haline getirerek, bu metinleri Internet üzerinden üçüncü parti firmalarla paylaştığı ortaya çıkmıştı. (Sonrasında Samsung bu paylaşımın sadece spesifik bir firma ile olduğunu belirtti ve güvenli bir platform oluşturmak için hangi önlemleri aldıklarını paylaştı.[1]) Normal şartlar altında ses fonksiyonu açıkken ekranda bir mikrofon işareti belirmekte ve sesli komutları şifreleyerek saklamakta ve yine bu bilgiyi şifreli olarak Internet üzerinden iletmektedir. Ancak, televizyonumuza bulaşan zararlı bir yazılım, bu ses tanıma fonksiyonunu kullanarak ortam dinlemesi yapar ve dinlediklerini Internet üzerinden kötü niyetli sahibine iletirse ne olacak?

Bu ve benzeri konular sadece Samsung'a özgü değildir. ABD'de yaygın olan Vizio adlı akıllı televizyon platformunun, kullanıcı izleme alışkanlıklarını program, saat, IP bilgisini içerecek şekilde kaydettiği ve bu bilgileri Internet reklam firmaları ile paylaştığı ortaya çıkmıştı. Bu nedenle, 2.2 milyon ABD doları ceza ödemek zorunda kalmıştı. Geçtiğimiz yıllarda LG'nin de akıllı reklam (Smart Ad) fonksiyonu tepki toplamıştı.

Akıllı TV üreticileri platformlarını güvenli hale getirmek için önlemlerini alıyorlar. Bu kapsamda akıllı TV'ler topladıkları kişisel verileri şifreli olarak depoluyor ve iletiyor olabilirler; ama akla gelen ilk soru, bu şifrelemenin ne kadar güvenli ve kırılamaz bir şifreleme olduğudur. Ayrıca, televizyona ulaşan kötü niyetli kişilerin veya programların, bu şifreli veriyi kullanmak yerine TV'deki fonksiyonu kullanıp, verileri doğrudan, şifrelenmeden önce televizyona giriş noktasından ele geçirme riski de söz konusudur. 2017'de dışarıya sızan bazı belgelere göre, CIA ve MI5'in akıllı TV'lerin birer dinleme cihazına dönüşmesi için ortak çalışma yürüttükleri (Weeping Angel), bu kapsamda geliştirdikleri yazılımlarla ortam dinlemesi yapabildikleri, televizyon üzerinden televizyonun bağlı olduğu ağa erişerek tüm ağ üzerinde akan veriyi dinleyebildikleri ve kamerası olan TV'lerle ortam izlemesi de yapabildikleri ortaya çıkmıştır.[2]

Peki akıllı TV'lerimizi daha güvenli hale getirmek için hangi temel önlemleri alabiliriz? Aşağıdaki adımlar %100 güvenliği garanti etmemekle birlikte, birçok tehdidin önlenmesine yardımcı olacaktır. Alınabilecek temel önlemler:

- **TV'nin Internet'e bağlı olması gerekmiyorsa,** yani sadece standart TV özellikleriyle kullanılıyorsa Internet bağlantısını gerçekleştirmeyin; kurulum sırasında bağlanmışsa da kapatın. Internet'e bağlı olması, saldırganlar için potansiyel bir açık kapı demektir. (Internet bağlantısını kapatınca artık bir akıllı TV'nizin olmadığını da belirtmem gerekir, standart TV'den bir tüp uzaktasınız :))
- **TV üzerindeki kamerayı** bir bantla kapatabilirsiniz. (Yıllar geçse de, cihazlar değişse de bu önlem değişmeyecek gibi...)
- **Mikrofonu da,** kullanmıyorsanız veya kullanmadığınız zamanlarda kapatabilirsiniz. Eğer uzaktan kumandanızda gömülü mikrofon varsa, onu da üçüncü bir firmanın mikrofonsuz olan bir kumandası ile değiştirilebilirsiniz.

- **TV üreticileri** güvenlik açıkları ortaya çıktıkça veya yeni geliştirmeler oldukça güvenlik güncellemeleri yayınlarlar. Bu tür güncelleştirmeleri can sıkıcı bulabilirsiniz, ama düzenli olarak yüklenmeleri gerektiğini unutmayın.
- **Ekrana gelen şüpheli mesajları**, özellikle de başka cihazlara bağlantının onaylanmasına yönelik mesajları onaylamayın.
- **TV'niz ilk defa kurulurken** "kolay kurulum", "hızlı kurulum" gibi seçenekleri seçerek değil, kişiselleştirme ve gizlilik özelliklerinin açılıp kapatılabildiği "özelleştir" (custom settings) modunda kurulum yapılmasını sağlayın.
- **Internet'e bağlı** bütün cihazlarınızda olduğu gibi, şüpheli görünen uygulamaları indirmeyin.
- **"Gizlilik Politikası"** vb. adları altındaki koşulları içeren dokümanları onaylamadan önce okuyun (ne kadar uygulanabilir, tartışılır :)) Üreticilerin kullanıcı alışkanlıklarına ilişkin bilgileri sadece kullanıcıların rızası ve onayı varsa tutması gerekmektedir. Ne var ki bu rıza ve onay genellikle ilk kurulum aşamasında sorulur ama sonradan değiştirilebilir.
- **Akıllı TV'nizden** bankacılık işlemi yapmayın.
- **Akıllı TV'nizin** web tarayıcısını kullanırken, bilgisayarınızda olduğu gibi ziyaret ettiğiniz sitelere dikkat edin, seçici olun.
- **Tereddütte kaldığınız** konularda TV üreticinize danışın.

Yapılabilecek temel düzenlemeleri Samsung akıllı TV için aşağıda bulabilirsiniz. Ancak, aynı markanın farklı modellerinde bile bu adımlar değiştiğinden, farklı markalarda tamamen farklı olacaktır. Burada sadece örnek olması ve fikir vermesi açısından yer verilmiştir:

Ses tanıma, kaydedip iletme fonksiyonlarını kapatmak için:

- Menü > Smart Özellikler > Hüküm ve Koşullar > Ses Tanıma Gizlilik İlkesi adımı altında "Onaylıyorum" seçeneğini kaldırın.
- Menü > Smart Özellikler > Hüküm ve Koşullar > Nuance Gizlilik Bildirimi adımı altında "Onaylıyorum" seçeneğini kaldırın.

Güncel yazılım versiyonlarını indirmek için:

- Menu > Destek > Yazılım Güncelleme adımından en son güncel yazılımı kontrol edip, TV'nize yükleyin. Tabii ki bunu yapabilmeniz için Internet'e bağlı olmanız gerekecektir.

Wi-fi bağlantısını kesmek için:

- Menu > Ağ > Ağ Ayarları altından bağlantıyı kapatabilirsiniz.

Sonuç olarak, bu yazı akıllı TV'lerde %100 güvenliğin sağlanmasını garanti etme iddiasıyla değil, farkındalığı artırmak ve alınabilecek basit ama önemli temel önlemleri dikkatlere sunmak için kaleme alınmıştır. Sitemizin güzel mottosu ile yazıyı bitirmek istiyorum, "Güvenli Günler".

REFERANSLAR

1. https://news.samsung.com/global/what-samsung-is-doing-to-keep-your-smart-tv-secure
2. http://www.zdnet.com/article/how-cia-mi5-hacked-your-smart-tv-to-spy-on-you/

YAZAR HAKKINDA

AYTEKİN GÜZELİŞ Yazılım Geliştirme, Network, IT Denetimi, IT Yönetişimi, IT Risk Yönetimi ve Bilgi Güvenliği alanlarında 16 yılı aşkın tecrübeye sahip. Ülkemizde mesleki gelişime katkıda bulunmak adına ISACA Istanbul Chapter'da Araştırma ve Yayın Direktörü olarak destek veren Aytekin; ulusal ve uluslararası birçok konferansta konuşmacı olarak da yer almaktadır. CISA, CRISC ve ITIL sertifikaları bulunmaktadır.