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.

HAZİRAN 2020

Asistanım Akıllı, Peki Güvenli Mi?

***DİJİTALLEŞMENİN** evlerimize ve ceplerimize kadar girmiş uzantısı akıllı asistanlar, ülkemizde yabancı ülkelerdeki kullanım oranlarına ulaşmasa da hızla gelişen ve gün geçtikçe daha çok hayatımızın içinde olacak bir pazar.*

Akıllı asistanlar 10 yıl öncesine kadar ütopyayken şu anda hemen hepimizin bir şekilde hayatındalar. 80'li yıllarda geçen çocukluğumun dizisi Kara Şimşek'in konuşan arabası "KITT" seviyesine henüz ulaşamamış olsa da oraya çok yakın olduğumuzu düşündüren bir hızda gelişiyoruz. Akıllı asistanlar, bilim kurgu eserlerin sıklıkla işlediği yapay zeka ve insansı robotların hayatımıza en sade hali ile entegre edildiği arayüzler aslında. Basit işleri sesli komutlarımız ile gerçekleştirip bizimle yine insan sesi aracılığıyla iletişime geçen küçük cihazlar.

Akıllı asistan diyerek illaki eve koyduğunuz bir kutudan bahsetmiyorum aslında. Hepimiz bir tanesini belki de bilmeden yanımızda taşıyor, o özelliklerini hiç kullanmadığımızı sanıyoruz. Ancak telefonlarımızın akıllı asistanları tahmin ettiğimizden çok daha sofistike ve **bizi sürekli dinliyor.** IOS ve Android işletim sistemli telefonlar, akıllı asistanları aktive edilmiş şekilde elimize geçiyor. Belki günlük hayatta her şeyi akıllı asistana sormuyoruz ama asistanı devreden çıkarmadığımız sürece akıllı asistan her an bir şey soracağımızı varsayarak bizi

dinliyor, isteklerimizi daha iyi anlayabilmek için söylediklerimizi yapay zeka süzgecinden geçiriyor ve bu verinin çok küçük bir kısmını da "false positive" yani yanlış alarmları önlemek adına insan süzgecine sokuyor.

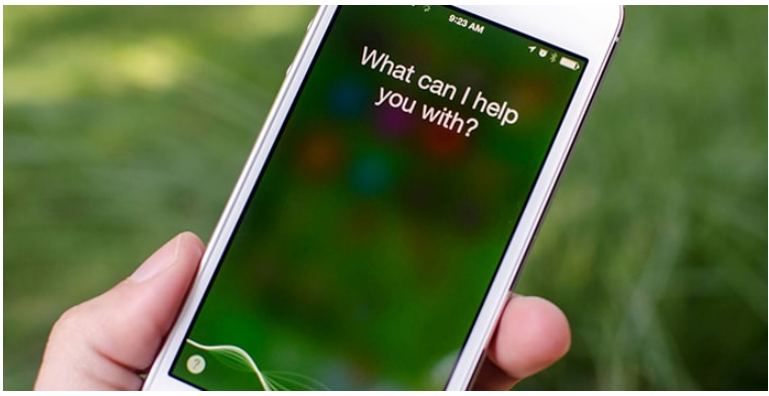
Telefonlarımız, asistan üzerinden dinleme haricinde **lokasyon bilgisini** de tuttuğu için asistanlar nerede, ne zaman, ne dediğimizi işleyen birer casus haline geliyor.

Cep telefonları haricinde özellikle **"akıllı ev"** konseptinin olmazsa olmazı ve belki de ilerleyen yıllarda hayatımızın vazgeçilmezi olacak ev tipi akıllı asistanlar ise konunun diğer bir boyutu. Çalışma mantığı bire bir aynı olsa da kullanım yaygınlığı ve güvenlik bilincinin telefonlar ile aynı seviyede olmaması sebebiyle ayrı bir risk grubu olarak ele almanın daha uygun olduğunu düşündüğüm cihazlar bu kutular.

Bu cihazlar ne mi yapıyor? En basitinden başlamak gerekirse istediğiniz müziği açıyor, hava durumunu söylüyor, en yakın nöbetçi eczane ya da açık market gibi sorularınızı yanıtlıyor. Bununla da sınırlı kalmıyor ve evinizdeki robot süpürge gibi akıllı cihazları kontrol edebildiği gibi bazı modellerde sizin hesabınızdan sipariş bile verebiliyor. Bunları yaparken de sizi 7/24 dinliyor.

Akıllı asistan üreticileri beni neden dinlesin diyeceksiniz, haklısınız, muhtemelen kişisel olarak sizi hedeflemiyorlar. Hatta sizi tanımak için bir akıllı asistana da ihtiyaçları yok. Çünkü sosyal medyadan internet kullanımınıza, alışverişlerinizden zevklerinize, her şey bir veri ve bu veriyi zaten kendi elinizle her gün güçlendiriyorsunuz.

Akıllı asistan üreticileri her konuşmanın kaydedilmediği konusunda güvence veriyorlar. "Anahtar Kelime"lerin kullanılmasını izleyen kısa zaman dilimlerini kaydettikleri, dolayısıyla konuşmaların bütününün kayıt altında olmadığı savunması kişisel verilerin korunması konusundaki kaygılar için verdikleri cevap. Ancak bu anahtar kelimeler duyulmadığı zamanlarda da dinleme yapıldığı gerçeğini değiştirmiyor.



Zaten herkesi sürekli kaydetmek disk alanı açısından büyük bir yatırım gerektiriyor, dolayısıyla anahtar kelimelerin süzülmesi mantıklı fakat anahtar kelimelerin neler olduğu ya da listesinin bir şekilde manüpüle edilip edilemeyeceği büyük bir soru işareti. Örneğin muhalif görüşe sahip insanları bu şekilde tespit eden devletler var mı? Ya da istihbarat örgütleri bu verilere ne ölçüde erişebiliyor? Üreticiler verdikleri güvencelerle süreç içerisinde kendi önlemlerini bize satmış oluyorlar, peki ürünler %100 güvenli mi?

Güvenlik işine ucundan kıyısından bulaşmış herkesin de rahatlıkla söyleyebileceği gibi %100 güvenlik diye bir şey yoktur, dolayısıyla akıllı asistanların da güvenlik açıkları olduğunu rahatlıkla söyleyebiliriz. Yapacağımız ufak tefek ayarlar ile bu cihazlara erişimi minimize ettiğimizde geriye üreticiye güvenmekten başka bir seçeneğimiz kalmıyor. Sık kullanılan akıllı asistanlar için bazı güvenlik önlemlerini aşağıdaki gibi listeleyebiliriz:

ALEXA/ECHO

- **Ses Kayıtları:** Periyodik olarak alexa ile olan ses kayıtlarınızı silin.
- **Güçlü Parolalar:** Güçlü parolalar tercih ederek iki faktörlü kimlik doğrulama kullanın.
- **Wifi:** Modem parolanızı güçlendirin.
- **Siparişler:** Pin kodu kullanın. Sipariş verme sık kullandığınız bir özellik değilse kapatın.

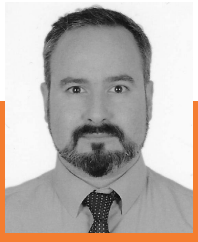
SİRİ

- **Ekran Kilidi:** Iphone kilitliyken Siri'ye erişimi engelleyerek Siri'ye erişim için parola kullanın.

GOOGLE HOME

- **Erişim:** Diğer cihazlara ve kişisel hesaplara erişimi sınırlandırın.
- **Ses Tanıma:** Ses tanıma özelliğini kullanarak kendi sesinizi tanımlayın.
- **Ses Kayıtları:** Ses kayıtlarınızı periyodik olarak silin.
- **Güçlü Parolalar:** Güçlü parolalar tercih ederek iki faktörlü kimlik doğrulama kullanın.
- **Mikrofon:** Kullanmadığınızda cihazın mikrofonununu kapatın.

Bunlara ek olarak güvenlik duvarı ile bir katman daha konabilir ama evde aldığınız önlemler sizi bir yere kadar korur. Bundan sonrası güvenlik hassasiyetinizin seviyesine göre akıllı asistanın veri trafiğinde anomali aramaya ya da akıllı asistan kullanmamaya doğru gidebilir. Ancak dünyanın dijitalleşme akışına ters gitmenin de gelecekte hayatımızı zorlaştırabileceği gerçeğini unutmamak gerekir.



YAZAR HAKKINDA

ERDEM AKSOY Budapeşte Teknik Üniversitesi Yazılım Mühendisliği bölümünden mezun olduktan sonra yurt içi ve dışında farklı firmalarda mühendislik, danışmanlık ve yöneticilik pozisyonlarında görev aldı. İş hayatına Çimtaş grup şirketlerinin IT Süreç ve Bilgi Güvenliği'nden sorumlu yöneticisi olarak devam etmektedir.

linkedin.com/aksoyerdem
erdemaksoy.org