thinktech
STM Teknolojik Düşünce Merkezi

Yaşam Alanımız "Hack'lenme" Tehdidi Altında!

2019 yılında geçen sıradan bir günde, evde bakıcısıyla bıraktığınız bebeğinizi an be an akıllı cep telefonunuzdan izleyebilirsiniz. Kolunuzdaki akıllı saat sayesinde nabız ve EKG ölçümünüzü yapıp saniyeler içinde doktorunuzun bilgisayarına gönderebilirsiniz. Aracınız ya da eviniz hırsızların hedefi oldu diyelim. Akıllı güvenlik sisteminin polise ve telefonunuza saniyeler içinde gönderdiği sinyaller sayesinde hırsızları, parmağınızı bile oynatmadan adalete teslim edebilirsiniz. İşten çıkarken evinizin ısısını akıllı telefonunuzdaki uygulama aracılığıyla ayarlayabilir, hatta eve gitmeden fırınınızdaki yemeği pişirmeye başlayabilirsiniz. Bu imkânların olmadığı dönemlerle karşılaştırılınca bugün yaşadığımız çok konforlu bir hayat, değil mi? Üstelik nesnelerin internetinin bize sundukları, bunlarla sınırlı değil. Bugün, bir "akıllı çatal", yemeğinizi fazla hızlı yediğinizde sizi uyarabiliyor veya "akıllı top" o serbest vuruşu saatte kaç kilometre hızla kullandığınızı söyleyebiliyor.

Bu Kez Tehlike O Kadar Uzak Değil!

Basitçe internete erişimi olan her nesnenin, yani akıllı teknolojik aletin birbiriyle iletişim halinde olması olarak açıklanan nesnelerin interneti, insanlığa bir zamanlar hayal bile edemeyeceği konforu ve hatta akıllı top gibi -belki de şimdilik- "olmazsa olmaz" olarak tanımlayamayacağımız ancak hayatımıza şüphesiz keyif katan özellikler sağlıyor. Peki, "Bana lükslerimi verin, gereksinimlerim olmadan da yaşarım" diyen Oscar Wilde'ın favori teknolojisi olabilecek nesnelerin internetinde her şey toz pembe mi? Tıpkı yapay zekânın bir gün Superintelligence'a, yani makinenin insan zekâsını açık ara geçtiği bilinç ve zekâ seviyesine ulaşarak insan ırkını yok edebileceği teoremi gibi, nesnelerin interneti için de pek çok olumsuz senaryo mevcut. Ancak bu kez tehlike, o kadar da uzak olmayabilir.

Amazon ve Apple Bile "Hack'lendi"

Nesnelerin interneti ile birbirine bağlanan cihaz sayısı arttıkça; evinize giriş şifrenizden sipariş ettiğiniz son yemeğe, akıllı buzdolabınızdan akıllı cep telefonunuza dek etrafınızdaki akıllı eşyaların kontrolünün başkalarının eline geçme riski de artıyor. Bugün kullandığımız pek çok elektronik ürün, başka bir ülkede tasarlanmış ya da birleştirilmiş olsa da Çin'de üretiliyor. Aynı şekilde büyük şirketlerin sunucu bileşenlerinin çoğu da Çin'den tedarik ediliyor. *Bloomberg Newsweek*'in yayımladığı 4 Ekim 2018 tarihli, "Büyük Hack Dalgası: Çin Ufacık Çipleri ABD Merkezli Şirketlere Sızmak İçin Nasıl Kullandı?" başlıklı haberde Çin ajanlarının, aralarında Amazon ve Apple'ın da bulunduğu ABD merkezli yaklaşık 30 şirkete çip yoluyla sızdığı ifade ediliyor. Haberde, Amazon'un startup'ı olan Elemental Technologies'in sunucularının Çin merkezli Supermicro şirketinden tedarik edilmiş anakartlarında, asıl dizaynda yer verilmeyen ve bir pirinç tanesinden büyük olmayan mikroçipler bulduğu ve Elemental'ın bu anakartları kullanan yüzlerce müşteriden biri olduğu ifade ediliyor. Apple da, 2015 yılına dek Supermicro'nun müşterisiydi ancak şirket üç yıl önce Supermicro ile ticari ilişkisini, sebep göstermeksizin sonlandırmıştı[1].

1 https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Peki bu tip bir saldırı sonucunda ne elde edilebilir? Yazılım kaynaklı saldırılarla elde edilebilecek veri sınırlıyken, doğrudan anakarta yerleştirilmiş bir çiple şirketin hemen hemen her verisine erişim sağlanabilir. Saptanması çok daha zor olan "hardware hack" yöntemi olan çiplerle bir şirketin gizli bilgileri uzun yıllar takip edilebilir. Bu bilgiler için rakiplerinin kaç milyon dolar ödemeye razı geleceğini ise söylememize gerek yok.

Daha dünyanın önde gelen şirketleri kendilerini bu tip saldırılardan koruyamıyorken, bizler ne yapabiliriz? Bugün dünya üzerindeki cep telefonlarının yüzde 75'i ve bilgisayarların yüzde 90'ı Çin'de üretiliyorken belirli ülkelere yönelik yaptırım uygulanması ya da bireysel olarak Çin'de üretilmiş bir telefonu almamak makul ya da mantıklı bir çözüm gibi görünmüyor. Ayrıca 19 Ekim 2018 tarihli "Hacklenmiş Geleceğimiz" başlıklı *Washington Post* haberinde, Çin'in yanı sıra Rusya gibi başka ülkelerin de bu tip "sızma" girişimlerinin olduğu ifade ediliyor[2].

Crysler Jeep'in Kontrolü Ele Geçirildi

"Hack'lenme tehdidi hep vardı, nesnelerin interneti neyi değiştirdi ki?" diyenlerdenseniz, tekrar düşünün. Eskiden hack'lendiğinizde bilgileriniz ve bazen paranız çalınırken; bugün hack'lendiğinizde evinizdeki konuşmalarınız, görüntünüz kaydediliyor, şifresi ele geçirilen eviniz hırsızlara açık hale gelebiliyor. 2018'in Temmuz ayında akıllı süpürgelerin hack'lenerek ev sahiplerinin gizlice dinlenip, kameraya alınmasının mümkün olduğu ortaya çıkmıştı[3]. 2018'in başında Hancock Health isimli hastanenin IT sistemi hack'lenmiş, hastanenin tüm e-postalarını, hasta kayıtlarını, işletim sistemini ele geçiren ve 1.400 hastanın kaydının ismini "Üzgünüm" olarak değiştiren hacker'lar Bitcoin ile fidye talep etmişti. Hastane hacker'lara tam 55 bin dolar ödemek zorunda kalmıştı[4]. 2018'in Mart ayında ise FBI, akıllı otomobillerin hack'lenmeye açık kablosuz parçalarının bir listesini yayınlamıştı. 2018 içinde araştırmacılar, bir Crysler Jeep Cherokee'nin kontrolünü uzaktan ele geçirmeyi başarmıştı[5]. Yani hack tehdidi, paranız ve bilgilerinizden öte, hayatınızı dahi tehlikeye atabilir.

Ya Derinizin Altındaki Bilgisayar Hack'lenirse?

Nesnelerin interneti teknolojisiyle yaşam alanlarımıza yayılan hack tehlikesi, geleceğin teknolojileriyle daha da büyüyor. Gelecekte derimizin altına dahi konabilecek incelikte bilgisayarlar geliştirilmesi bekleniyor. Peki Amazon ve Apple gibi şirketleri avlayan çip yöntemi ya da yazılımsal tekniklerle, vücudumuzun içindeki bir bilgisayarın hack'lenmesi nasıl sonuçlar doğurabilir? Vücudumuzun içine yerleştirilecek bir bilgisayar, nesnelerin interneti aracılığıyla başka pek çok akıllı araç ile iletişim içinde olacak. Bağlı cihaz sayısı arttıkça, tehlike de artıyor. Aslında benzer bir teknoloji, bugün kullanımda. Vücuttaki glukoz seviyesini ölçen özel kontakt lensler ya da vücudu devamlı kontrol eden elektronik haplar gibi teknolojiler bugün sağlık sisteminin birer parçası[6]. Nesnelerin internetine atıfla "Bedenlerin İnterneti" adı verilen teknolojinin ürünü bu cihazların hack'lenmesi durumunda, sağlığınıza dair bilgilerin hacker'ların eline geçmesi ve hatta onların bu bilgileri değiştirmesi bile söz konusu olabilir.

Peki çözüm ne olabilir? *New York Times*'taki 11 Ekim 2018 tarihli makalesinde Bruce Schneiner, bu güvenlik probleminin şirketlerin çözeceği bir sorun olmadığını, artık hükümetlerin devreye girmesi gerektiğini ifade ediyor[7]. Çin şirketinin Amazon ve Apple'a sızdığı haberi üzerine kaleme alınan makalede, internetin bugünkü karmaşık yapısı sebebiyle hack'lenmeye müsait bir açığın saptanmasının çok zorlaştığı ve yeni yasaların devreye girmesi gerektiği vurgulanıyor. Yani küresel hack tehdidi karşısında bizim de, şirketlerin de yapabilecekleri son derece sınırlı. Üstelik, teknoloji şirketlerinin kaynaklarının büyük bir kısmını bu tehdit karşısında savunmaya harcaması, pek çok teknolojinin gelişimini sekteye de uğratıyor. Artık pek çok ülkenin işbirliği neticesinde atılacak ciddi adımlar bekleniyor. Bir gün uyanıp evinizdeki tüm akıllı cihazların başkasının kontrolü altına girdiğini görmeden; tost makineniz fotoğraflarınızı çekip başkalarıyla paylaşmadan, buzdolabınız hacker'lara fidyeyi ödemediğiniz müddetçe çalışmayı reddetmeden, bir şeyler yapılması gerektiği aşikâr...

2 https://www.washingtonpost.com/news/theworldpost/wp/2018/10/19/hacking/?noredirect=on&utm_term=.9e4d253b8416
3 https://gizmodo.com/hack-can-turn-robotic-vacuum-into-creepy-rolling-survei-1827726378
4 https://www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/
5 https://www.zdnet.com/article/fbi-to-drivers-watch-out-for-these-malware-attacks-on-your-car/
6 https://motherboard.vice.com/en_us/article/gvyqgm/the-internet-of-bodies-is-coming-and-you-could-get-hacked
7 https://www.nytimes.com/2018/10/11/opinion/internet-hacking-cybersecurity-iot.html