thinktech
STM Teknolojik Düşünce Merkezi

# IoT'ye Yapılan Siber Saldırılar Yüzde 600 Arttı

Nesnelerin interneti, her ne kadar hayatımızı kolaylaştırsa da dikkatli olunmazsa pek çok güvenlik açığını da beraberinde getiriyor. Bilgisayarımız hack'lendiğinde bile birçok veri tehlikeye girerken arabamızın, telefonumuzun veya evimizdeki güvenlik sisteminin, kameraların hack'lenebilme ihtimali "Güvenliği nasıl sağlayacağız?" sorusunu akıllara getiriyor.

2017 yılı itibariyle 8.4 milyar cihaz internete bağlanabiliyor. 2020 yılına kadar bu sayının 25 milyara ulaşması bekleniyor. Nesnelerin internetinin kullanım alanı genişledikçe tehlikeler de buna paralel olarak artıyor. 2020 yılına gelindiğinde siber atakların yüzde 25'inin internete bağlanan nesnelere yapılacağı öngörülüyor[1].

**2020'de Evlerde İnternete Bağlanan 15 Cihaz Olacak**

Uluslararası yazılım şirketi Symantec'in "2018 İnternet Güvenlik Tehditleri Raporu"na göre, 2016 ve 2017 yılları arasında IoT'ye yapılan saldırılar yüzde 600 arttı. Saldırganların bu ataklarının nedenleri arasında, türlü cihazlara ve bilgisayarlara kötü amaçlı kripto madenciliği uygulamaları yüklemek de var. Bu tür niş ataklar ise 2017'nin son çeyreğinde yüzde 8500 arttı[1].

İngiltere'de hükümet, internete bağlanabilen cihaz üreticilerine, siber güvenliklerini artırmalarını sağlamak için çeşitli tedbirler getirdi. Özellikle artan güvenlik ihlalleri, daha çok kullanıcının bilgilerinin çalınması, ülkedeki yönetimi yeni yasalar getirmeye zorladı. Örneğin IoT cihazlarda parolaların kolayca ele geçirildiği anlaşılınca bu tür cihazlara fabrika ayarlarına sıfırlanamayan parolalar gibi ek önlemler getiriliyor.

Ülkede son kullanıcıların, şirketlerin, büyük kuruluşların verilerini iyi koruyabilmeleri için hükümet üreticilerle bir araya gelerek "Tasarımda Güvenlik" ismi verilen bir düzenleme paketi oluşturdu. Buna göre cihaz üreticisi İngiltere'de kullanılacak IoT aygıtlarında uyulması gereken bazı güvenlik önlemlerini dikkate alacak. IoT cihazının kullanıldığı bir noktada güvenlik araştırması yapılmak istenirse anında rapor verebilmek için uygun özellikte olması gerekecek[2]. Son kullanıcı için cihaz güncellemelerinin otomatik yapılması, anlaşılır bir kullanım kılavuzunun kullanıcıya sunulması, kullanıcının isterse kişisel bilgilerini sistemden kolaylıkla silebilmesinin mümkün olması, kurulum ve bakım işlerinin son kullanıcının rahat anlayacağı biçimde yapılabilmesi pakette öngörülen konulardan bazıları.

Hükümet, yaptığı araştırmada İngiltere'de her evde internete bağlı en az 10 aygıt olduğunu belirtiyor. 2020 yılına kadar bu sayının en az 15 olacağı tahmin ediliyor. Tabii bu cihazlar için her eve girebilmenin artık daha fazla yolu var; akıllı televizyonları, klimaları, aydınlatma sistemlerini, medya oynatıcıları, buzdolaplarını, akıllı yıkama makinelerini, cep telefonlarını, tablet, bilgisayar ve giyilebilir teknolojileri düşününce bir ağa bağlı cihaz sayısındaki artışın süreceğini öngörmek zor değil[3].

---

1 https://newblogtrustlook.files.wordpress.com/2017/09/iot-security-survey-infographic-2017.pdf
2 https://www.gov.uk/government/news/new-measures-to-boost-cyber-security-in-millions-of-internet-connected-devices
3 https://www.information-age.com/iot-devices-improved-cyber-security-123471065/

**Her Organizasyonun Yaklaşımı Farklı**

Siber saldırı risklerine karşı büyük şirketlerin, organizasyonların yaklaşımları farklı oluyor. Bölgeye, ürün türüne, iş alanına göre farklılık gösteren tedbirleri şirketler kendi yaklaşımlarını geliştirerek alıyorlar. Ancak IoT, pek çok öncü teknoloji, medya ve iletişim şirketini merkeziyetsiz bir güvenlik çözümü arayışına itecek; zira IoT, işletmelerin operasyonlarını beklenmedik yollarla birleştiriyor. Farklı alanlarda yürütülen işleri birbirine bağlayan IoT aygıtları veri topluyor, izliyor, rapor ediyor ve cihazlar çalıştıkça ortaya iyi korunması gereken büyük bir potansiyel siber saldırı hedefi çıkıyor. İş dünyası liderleri bir siber risk paradigması geliştirip ön tehditten olay sonrasına kadar olan süreci seviyelere ayırıp ayrı ayrı öngörmek, beklemek, yeni tehditleri izlemek ve nötralize etmek zorunda. Yeni yaklaşımların da sonuç vermediği anlarda organizasyon tehditle karşı karşıya kalabilir, burada da şirket için hedef mümkün olan en kısa sürede normale dönmek olacaktır[4].

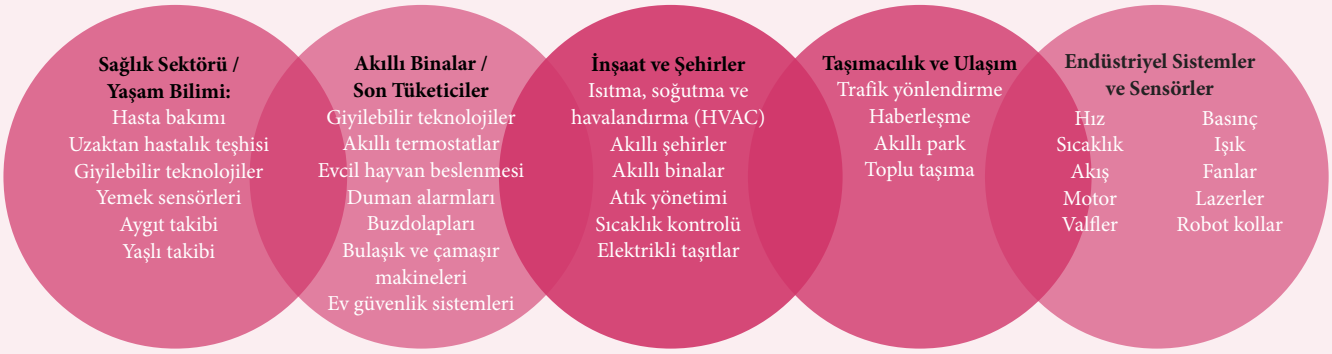
**Güvenliğinizi Nasıl Sağlarsınız?**

- İnternetin bağlı olduğu cihazınızda kullanıcı ismi/parola değişikliği görüyorsanız dikkat. Saldırıda bulunanların yapacağı ilk iş kullanıcı adı ve parolayı değiştirmek olacaktır.
- Cihazlarınızın güvenlik ve yazılım güncellemelerinin yapıldığından emin olun. Özellikle güvenlik yazılımlarınızın güncel olması cihazlarınızın ataklara karşı daha efektif korunmasını sağlar.
- Ağ depolama ve dosyalama işlerinizde mutlaka şifreleme kullanın. Cihazınıza girilse bile dosyalara erişim kolay olmasın.
- Şifrelerinizi birkaç ayda bir düzenli olarak değiştirin[5].
- Söz konusu nesneler olduğunda, bunları kullananlar insanlar olduğu için bilinçli kullanım da önemli hale geliyor. Örneğin şirketlerin, çalışanlarına bu tür cihazları kullanırken dikkat etmelerini hatırlatmaları gerekiyor. Bunun dışında her kullanıcının erişimi diğerininkinden farklı olabilir. Herkese tam erişim vermek yerine parçalamak daha yerinde bir davranış olacaktır[6].

**Siber Tehditlere Genel Bakış**[7]

Siber tehdit şemasına genel bir bakış atıldığında tehdidin aslında bitmek tükenmek bilmeyen boyutlarda olabileceğini söyleyebiliriz. Üstelik bu şema sürekli değişiyor. IoT'nin etkileyeceği yaşam alanları ve sektörleri özetlemeye çalışınca geniş bir yelpazede işlerin değişeceği, bununla birlikte kaygıların artacağı görülebiliyor.

**IoT'nin Etkileyeceği Alanlar**




4 https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html
5 https://www.informationsecuritybuzz.com/articles/how-to-protect-your-iot-devices/
6 https://www.csoonline.com/article/3244467/internet-of-things/2018-prediction-securing-iot-connected-devices-will-be-a-major-cybersecurity-challenge.html
7 Deloitte; Cyber risk in an Internet of Things world www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html