SAKARYA
ÜNİVERSİTESİ

Sakarya universitesi bilgisayar muhendisligi

Ad-Soyad : Wajeeh Albasha

Ögrenci numarası : G181210552

Konu : IoT Security

İÇİNDEKİLER

IoT Security

Nesnelerin interneti güvenliği ınternet kullanan cihazların ve bu cihazların kullandığı ağın güvenliğini sağlama yöntemidir.

IoT güvenliği geniş ve aynı zamanda çok gerekli ve çokça ilgi gören bir konudur.

IoT, geniş ve sürekli büyüyen bir uygulama yelpazesine sahip olduğu kanıtlanmış belirli işlevlere sahip "nesnelere" veya cihazlara internet bağlantısı eklemeyi içerdiğinden, kendi içinde geniş bir alandır.

IoT çözümleri, yolların, arabaların ve evlerin güvenliğini artırmaktan ürünleri üretme ve tüketme şeklimizi temelden iyileştirmeye kadar, çalışma ve yaşama şeklimizi iyileştirecek değerli veriler ve içgörüler sağlar. Başarı, siber güvenlik risklerini azaltırken IoT çözümlerinin ve verilerinin bütünlüğünü ve gizliliğini sağlamaya bağlıdır.

Modern IoT ekosistemleri karmaşıktır. Hemen hemen her sektördeki makineler ve nesneler, hücresel ağlar üzerinden bulut uygulamalarına ve arka uçlara veri göndermek üzere bağlanabilir ve yapılandırılabilir. Dijital güvenlik riski, IoT yolculuğu boyunca her adımda mevcuttur ve bir sistemin güvenlik açığından yararlanacak bir grup bilgisayar korsanı vardır. Ne yazık ki, IoT cihazları arasındaki çeşitli veri türleri ve bilgi işlem gücü, herhangi bir IoT dağıtımını koruyabilecek 'herkese uyan tek bir' siber güvenlik çözümü olmadığı anlamına gelir. Herhangi bir IoT işi için ilk adım, cihazlar ve ağ sistemleri ile kullanıcı ve müşteri arka uç sistemlerindeki güvenlik açıklarını inceleyen kapsamlı bir güvenlik riski değerlendirmesinden geçmektir. Özellikle coğrafi olarak ölçeklenip genişledikçe, dağıtımın tüm IoT yaşam döngüsü boyunca risk azaltılmalıdır.

Aşağıdaki resimde ise bazı ınternet uygulamaları ve onların zaaflıkları yer almaktadır.


Web & Mobile Application
Cloud
Communications
Gateways / Smart Edge Devices
IoT Sensors / Actuators
Data Types
Closed / open platforms
Variable policies
High data volume handling
Public / private / hybrid cloud deployment
2G, 3G, LTE, 5G
DSL, Fibre, LPWAN
Wi-Fi, Bluetooth
MQTT, IP, ZigBee, Mesh RF, Wi-Fi etc
Variable communications protocols
Time-sensitive data analysis
Limited power
Low bandwidth
Constrained capabilities
Sensitive data: video, audio, location, personal information
Technical data: environmental measurement, uptime reports
Code
Lack of penetration testing
Weak User / Third Party Authentication
Code
Policy management
Insecure communications
Policy management
Denial-of-service
No / insecure updates
Poor hardware design
Design faults
Software / firmware implementation faults
Inability to update
Users
Policy management
Data storage

IoT güvenliğinin zorlukları

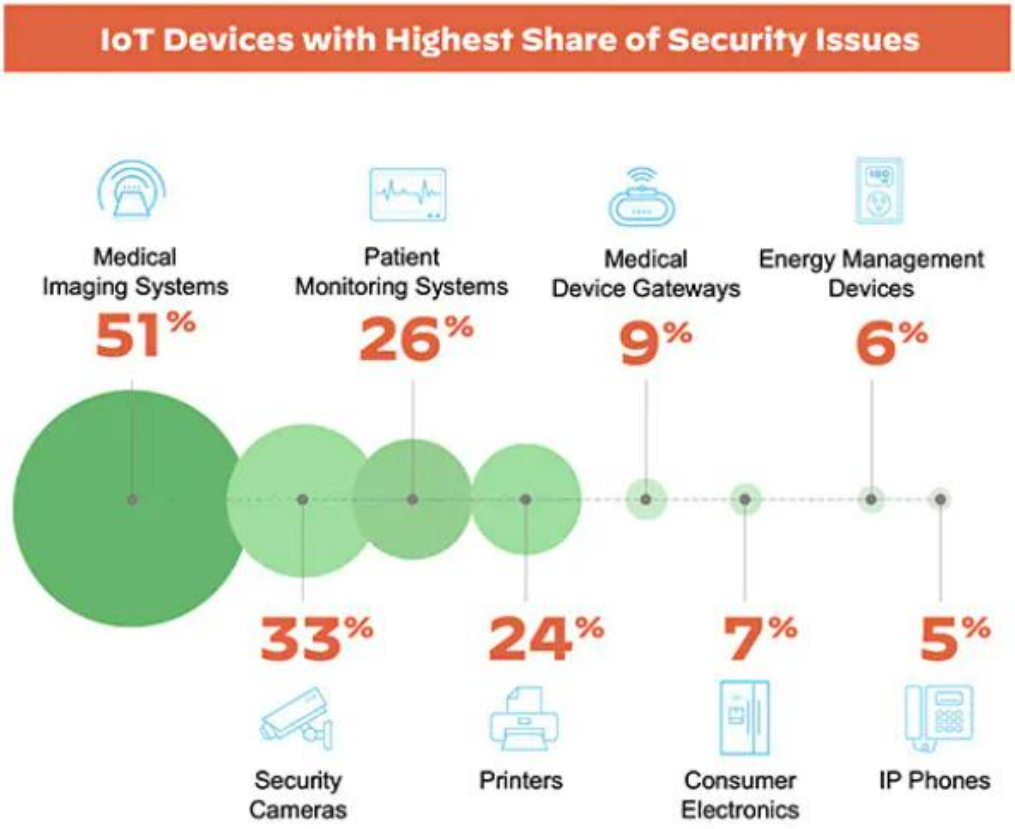
IoT güvenliği, özellikle ağa bağlı fiziksel IoT cihazlarını hedef alan siber saldırı olasılığına karşı koruma sağlayan bir siber güvenlik stratejisi ve koruma mekanizması olarak anlaşılabilir. Güçlü bir güvenlik olmadan, bağlı herhangi bir IoT cihazı, kötü bir aktör tarafından nihayetinde sızmak, kullanıcı verilerini çalmak ve sistemleri çökertmek için ihlal, uzlaşma ve kontrole karşı savunmasızdır.

IoT'de güvenlik için kapsayıcı zorluk, çok sayıda farklı IoT cihazının ağa bağlanmaya devam etmesiyle paralel olarak saldırı yüzeyinin dramatik bir şekilde genişlemesidir. Nihayetinde tüm ağ güvenliği duruşu, en az güvenli cihaza sunulan bütünlük ve koruma düzeyine indirilir.

Güvenlik ekipleri artık IoT güvenliğine özgü yeni ve giderek artan zorluklarla karşı karşıyadır, örneğin:

1. Envanter – ağda hangi IoT cihazlarının bulunduğu ve yeni cihazların nasıl güvenli bir şekilde yönetileceği konusunda net bir görünürlük ve bağlama sahip olmamak.
2. Tehditler – yama yapılması zor veya imkansız olan IoT cihaz işletim sistemlerine iyi yerleştirilmiş güvenlik eksikliği.
3. Veri hacmi – hem yönetilen hem de yönetilmeyen IoT cihazlarından üretilen büyük miktarda veriyi denetleme.
4. Mülkiyet – kuruluş içindeki farklı ekipler tarafından IoT cihazlarının yönetimiyle ilişkili yeni riskler.
5. Çeşitlilik – IoT cihazlarının sınırsız biçimleri ve işlevleri açısından tam çeşitliliği.
6. Operasyonlar – IoT cihazlarının temel operasyonlar için kritik olduğu, ancak BT'nin temel güvenlik duruşuna entegre edilmesinin zor olduğu birleştirme krizi.

Son olarak güvenlik sorunlarından en çok etkilenen cihazları belirten bir grafik . Bu da korumamız için en çok yoğunlaşmamız gereken cihazları gösterir



KAYNAKÇA

1. IoT Security - Definition (trendmicro.com)
2. IoT Security - A Safer Internet of Things (for 2022) (thalesgroup.com)
3. What is IoT Security? - Palo Alto Networks