CYBER WISE

Nesnelerin İnterneti (IoT) Güvenlik Referans Rehberi

BİZNET - SECURRENT - SECURRENT ME - PENETRA

Yasal Sorumluluklar

Cyberwise Research Task Force

- Fatih Kayran - fatihk@cyberwise.com.tr
- Rıdvan Ethem Canavar - ridvanc@cyberwise.com.tr

İçindekiler

Yönetici Özeti

Gelişen teknoloji ve iletişim altyapıları ile beraber, üretilen fiziksel teknolojik bileşenler internet veya bölgesel mesh vb. ağlar vasıtasıyla haberleşebilme yetenekleri kazanmaktadır. Literatürde "Nesnelerin İnternet (Internet of Things)" olarak adlandırılan bu kavramda nesne, herhangi bir fiziksel teknolojik bileşen (sensör, aktüatör, bilgisayar, akıllı araba vb.) olabilirken; internet, bu nesnelerin veri iletişimi yapabilme kabiliyetini belirtmektedir. Günlük hayatımızda kullandığımız akıllı telefondan, trafik sinyalizasyon sistemlerine kadar birçok sistem nesnelerin interneti kapsamında değerlendirilmektedir. Gartner, 2015 yılında 6 milyar IoT cihazı kullanıldığını belirtirken, 2025 yılında bu sayının 27 milyar cihaza ulaşmasını öngörmektedir[1]. Bulunduğumuz dönem **"Pre IoT Era"** olarak adlandırılırken, özellikle 5G ve IPv6 teknolojilerinin yaygınlaşmasıyla beraber IoT cihazlar hayatımızda daha büyük oranda yer kaplamaya başlayacaklardır.

Hayatımızın her alanında yer almaya başlayan IoT cihazlar, siber güvenlik kaygılarını da beraberinde getirmektedirler. İnternete bağlı bir kalp piline veya trafik sinyalizasyon altyapısına yapılabilecek bir siber saldırı ölümcül sonuçlara yol açabilmektedir. Her ne kadar siber güvenlik kaygıları, teknolojinin gelişimini takip etse de; teknolojinin gelişim hızı ve siber güvenlik olgunluğunun oluşum hızı arasında çoğu zaman farklılıklar olmaktadır. Siber güvenlik olgunluğunun gelişim hızı, teknolojinin gelişim hızından yavaş kalmakta ve IT sektörüne kıyasla, IoT siber güvenlik olgunluğu henüz emekleme çağında olarak yorumlanmaktadır.

Gartner, 2013'ten 2020 yılına kadar IoT siber güvenliğine yönelik harcamaların 188.05 milyar dolardan, 840.50 milyar dolara ulaşmasını öngörmektedir ve yıllık bazda ortalama %25 büyüme beklemektedir[2]. IoT siber güvenliğine yönelik artan harcamaların beraberinde, olgunluğu arttırma amacıyla da çeşitli regülasyonlar ve güvenlik referansları yayınlanmıştır. Bu yazı kapsamında enstitüler, uluslararası ve ulusal kuruluşlar tarafından yayınlanmış regülasyonlar ve güvenlik referans dökümanları derlenerek nesnelerin interneti (IoT) güvenlik referans rehberi haline getirilmiştir.

1. Nesnelerin İnterneti (IoT) Güvenlik Referans Rehberi

Uluslararası kuruluşlar ve ülkelere ait standardizasyon enstitülerinin yayınlamış olduğu nesnelerin interneti güvenlik referans dökümanlarını genel olarak incelediğimizde üretim sürecinde uygulanabilecek, cihaz seviyesinde birçok güvenlik gereksinimi olduğu gözümüze çarpmaktadır. Bu güvenlik gereksinimlerinin ortaya çıkması sürecinde IoT cihazlara yapılan saldırılar oldukça etkin rol oynamış ve IoT cihazlarda en çok yer alan 10 zafiyet OWASP (The Open Web Application Security Project) tarafından listelenmiştir.

1.1. OWASP Internet of Things Top 10 - 2018

OWASP tarafından 2014 yılında başlatılan OWASP Internet of Things Project'in bir çıktısı olan ve 2018 yılında yayınlanan IoT Top 10 dökümanında[3] yer alan zafiyetleri incelediğimizde;

1) Weak, Guessable, or Hardcoded Passwords
2) Insecure Network Services
3) Insecure Ecosystem Interfaces
4) Lack of Secure Update Mechanism
5) Use of Insecure or Outdated Components
6) Insufficient Privacy Protection
7) Insecure Data Transfer and Storage
8) Lack of Device Management
9) Insecure Default Settings
10) Lack of Physical Hardening

zafiyetlerinin yer aldığını görmekteyiz. Bu zafiyetlerden bazılarına göz attığımızda ilk sırada yer alan *"Weak, Guessable, or Hardcoded Passwords(1)"* zafiyetinde, birçok IoT cihazda varsayılan veya basit parola kullanımı sonucunda saldırganların bu cihazlara yetkisiz erişim yapabildiklerine vurgu yapılmıştır. IoT cihazlar kullanılarak 2016 yılında oluşturulan Mirai botnetinde, yaklaşık 600.000 adet cihaz yer almaktaydı. Özellikle internet erişimi olan ve varsayılan parolalara sahip IP kameralar, DVR cihazları Mirai botnetin belkemiğini oluşturmuştur. Mirai botnetinin kullandığı varsayılan kullanıcı adlarını ve parola bilgilerini, botnetin kaynak kodlarından[4] incelediğimizde, birçoğumuzun aşina olduğu kelime gruplarının mevcut olduğunu görmekteyiz.

Mirai botnetinde kullanılan kullanıcı isimleri : 666666, 888888, admin, admin1, Administrator, guest, mother, root, service, supervisor, support, tech, ubnt, user

[1] Gartner IoT Global Forecast and Analysis, 2015-2025 - ID: G00325939
[2] Gartner Forecast: IoT Security, Worldwide, 2016 - ID: G00302108
[3] OWASP IoT Top 10 - https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
[4] Mirai Botnet - https://github.com/jgamblin/Mirai-Source-Code

Mirai botnetinde kullanılan parolalar : 666666, 888888, admin, password, admin1234, smcadmin, 1111, 1111111, 1234, 12345, 54321, 123456, 7ujMko0admin, pass, meinsm, guest, fucker, xc3511, vizxv, xmhdipc, default, juantech, root, klv123, klv1234, Zte521, hi3518, jvbzd, anko, zlxx, 7ujMko0vizxv, system, ikwb, dreambox, user, realtek, 0, service, supervisor, support, tech, ubnt

Özellikle IoT cihaz üreticilerinin "Go To Market" stratejilerinde güvenliğin geri planda bırakılması ve düşük maliyetin amaçlanması sonucunda *"Insecure Network Services(2)", "Insecure Ecosystem Interfaces(3)", "Insufficient Privacy Protection(6)", "Insecure Data Transfer and Storage(7)", "Insecure Default Settings(9)"* ve *"Lack of Physical Hardening(10)"* zafiyetlerine oldukça sık karşılaşılmaktadır. IoT cihazların büyük bölümünde düşük işlem kapasitesi (dolayısıyla düşük maliyet) ve yüksek batarya ömrünün amaçlanmasından dolayı kriptografi gerektiren güvenlik önlemlerinin IoT cihazlarında uygulanabilmesi oldukça güç olabilmektedir. Şifreli bir iletişim için SSL / TLS kullanımı veya yerel depolamada bulunan kişisel verilerin şifrelenmesi, cihazın kaynaklarını büyük ölçüde tüketeceğinden dolayı, IoT cihaz üreticileri için maliyet ve güvenlik bir *"trade-off"* oluşturmaktadır.

IoT cihazların dağıtık yapısı ve merkezi bir noktadan yönetiminin getirdiği zorluklardan dolayı *"Lack of Secure Update Mechanism(4)", "Use of Insecure or Outdated Components(5)"* ve *"Lack of Device Management(8)"* başlıkları da OWASP IoT Top 10'de yer almıştır.

Yazının devam bölümlerinde ülkemizde ve dünyada bu alanda yapılmış çalışmalar ele alınacaktır.

1.2. Cumhurbaşkalığı Dijital Dönüşüm Ofisi - Bilgi ve İletişim Güvenliği Rehberi

Cumhurbaşkalığına bağlı Dijital Dönüşüm Ofisi tarafından Temmuz 2020'de yayınlanan Bilgi ve İletişim Güvenliği Rehberinde[5] nesnelerin internet güvenliği de yer almıştır. Dijital Dönüşüm Ofisi bu rehberde nesnelerin interneti güvenliğini beş ana başlık altında değerlendirmiştir. Bunlar;

1) Ağ Servisleri ve İletişimi
   - Ağ Portlarının Kısıtlanması
   - Ağ Servislerinin Güvenlik Kontrolleri
   - Güvenli Yapılandırma
   - Cihazın Güvenli İmhası veya Tekrar Kullanımı
   - Yetkisiz Cihazların Kurum Ağına Bağlanmasının Engellenmesi
   - Cihaz Güvenlik Duvarının Aktifleştirilmesi
   - Kablosuz Erişim Noktalarına Güvenli Bağlantı
   - Cihazların Merkezi Yönetimi
   - Ağ Üzerinden Gönderilen Verinin Şifrelenmesi
2) Dâhili Veri Depolama
   - Veri Yedekleme
   - Verilere Yetkili Erişim
   - Kullanılan Cihazlardan Kritik Verinin Temizlenmesi
   - Kimlik Doğrulama ve Yetkilendirme
   - Oturum Sonlandırma İşlemlerinin Aktifleştirilmesi
   - Kimlik Doğrulama Politikası
   - Kullanıcı Yetki Sınırlaması
   - Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi
   - Sıfırlama Mekanizmaları
3) API ve Bağlantı Güvenliği
   - Varsayılan Kimlik Doğrulama Bilgilerinin Değiştirilmesi
   - API ve Bağlantı Güvenliği
   - Web Uygulama Güvenlik Duvarı Kullanımı
   - Sistem API'lerinde Güvenli Haberleşme Protokolü Kullanımı
4) Diğer Güvenlik Tedbirleri
   - Güncellemelerin Kontrolü
   - Cihazlara Fiziksel Erişimin Kısıtlanması
   - Gömülü İşletim Sistemi İçin Kod Analiz Raporu Alınması
   - Elektromanyetik Sızıntılara Karşı Güvenlik Önlemlerinin Alınması
   - Tersine Mühendisliğe Karşı Koruma

şeklindedir. OWASP IoT Top 10'de bulunan zafiyetler ile bu maddelerde alınması gereken önlemlere baktığımızda, Bilgi ve İletişim

[5] Dijital Dönüşüm Ofisi Bilgi ve İletişim Güvenliği Rehberi - https://cbddo.gov.tr/bgrehber

Güvenliği Rehberinin kapsayıcı bir rehber olduğu gözümüze çarpmaktadır. Önlemlerin sadece fiziksel cihaz seviyesinde kalmayıp tüm IoT ekosistemini hedeflediği görülmektedir.

1.3. The C2 Consensus on CSDE - IoT Device Security Baseline Capabilities

The Council to Secure the Digital Economy (CSDE) tarafından yayınlanan IoT Device Security Baseline Capabilities[6] dökümanında IoT güvenlik gereksinimlerinin üretim sürecinde ve ürünün yaşam döngüsünde ele alınması gerektiğini belirtmiştir.

1) Secure Device Capabilities – Baseline
   - Device Identifiers
   - Secured Access
   - Data In Transit Is Protected
   - Data At Rest Is Protected
   - Industry Accepted Protocols are Used for Communications
   - Data Validation
   - Event Logging
   - Cryptography
   - Patchability
2) Product Lifecycle Management Capabilities - Baseline
   - Vulnerability Submission and Handling Process
   - EoL/EoS Updates and Disclosure
   - Device Intent Documentation

Ayrıca aynı dökümanda *"Secure Device Capabilities"* ve *"Product Lifecycle Management Capabilities"* başlıklarına ek olarak *"Regarding Future Secure Capabilities"* ve *"Additional IoT Device Security Capabilities and Practices"* adında iki tane daha ek başlık yer almaktadır.

1) Regarding Future Secure Capabilities – Phase in Over Time
   - Device Intent Signaling
   - Device Network Onboarding
2) Additional IoT Device Security Capabilities and Practices
   - Secure Development Lifecycle
   - Hardware Rooted Security
   - Time Distribution
   - System Resiliency
   - Secure Toolchains
   - Software Transparency and Bill of Materials
   - Least Functionality
   - Physical Access Control
   - Best Current Practices

1.4. European Telecommunications Standards Institute EN 303 645 - TS 103 645

European Telecommunications Standards Institute (ETSI) tarafından Haziran 2020 yılında yayınlanan EN 303 645[7] ve Şubat 2019 yılında yayınlanan TS 103 645[8] Cyber Security for Consumer Internet of Things dökümanlarını incelediğimizde, tüketiciği elektroniğine yönelik üretim sürecinde uygulanabilecek 13 güvenlik gereksiniminden bahsedilmiştir. Bu güvenlik gereksinimleri incelediğinde genel olarak cihaz seviyesi güvenliğinin hedeflendiği görülmektedir.

1) No universal default passwords
2) Implement a means to manage reports of vulnerabilities
3) Keep software updated
4) Securely store sensitive security parameters
5) Communicate securely
6) Minimize exposed attack surfaces
7) Ensure software integrity

[6] CSDE IoT Device Security Baseline Capabilities - https://securingdigitaleconomy.org/projects/c2-consensus/

[7] ETSI EN 303 645 - https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf

[8] ETSI TS 103 645 - https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

8) Ensure that personal data is secure
9) Make systems resilient to outages
10) Examine system telemetry data
11) Make it easy for users to delete user data
12) Make installation and maintenance of devices easy
13) Validate input data

1.5. NISTIR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers

National Institute of Standards and Technology tarafından Mayıs 2020 tarihinde yayınlamış IR 8259 - Foundational Cybersecurity Activities for IoT Device Manufacturers[9] dökümanında üreticilerin IoT cihazlarında uygulaması gereken temel aktiviteleri pre-market ve post-market safhaları olmak üzere ikiye ayırmıştır.

1) Manufacturer Activities Impacting the IoT Device Pre-Market Phase
   - Activity 1: Identify Expected Customers and Define Expected Use Cases
   - Activity 2: Research Customer Cybersecurity Needs and Goals
   - Activity 3: Determine How to Address Customer Needs and Goals
   - Activity 4: Plan for Adequate Support of Customer Needs and Goals
2) Manufacturer Activities Impacting the IoT Device Post-Market Phase
   - Activity 5: Define Approaches for Communicating to Customers
   - Activity 6: Decide What to Communicate to Customers and How to Communicate It
     - Cybersecurity Risk-Related Assumptions
     - Support and Lifespan Expectations
     - Device Composition and Capabilities
     - Software Updates
     - Device Retirement Options
     - Technical and Non-Technical Means

1.6. NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline

National Institute of Standards and Technology tarafından Mayıs 2020 tarihinde yayınlamış olduğu IR 8259 dökümanına ek olarak aynı tarihte IR 8259A IoT Device Cybersecurity Capability Core Baseline[10] dökümanını da yayınlamıştır. 8259A dökümanında ilk dökümandan farklı olarak IoT cihazların minimum siber güvenlik kabiliyetleri vurgulanmıştır.

1) **Device Identification :** The IoT device can be uniquely identified logically and physically.
2) **Device Configuration :** The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.
3) **Data Protection :** The IoT device can protect the data it stores and transmits from unauthorized access and modification.
4) **Logical Access to Interfaces :** The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
5) **Software Update :** The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.
6) **Cybersecurity State Awareness :** The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

1.7. NISTIR 8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

National Institute of Standards and Technology tarafından Haziran 2019 tarihinde yayınlanmış IR 8228 - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks[11] dökümanında siber güvenlik risklerine ek olarak privacy riskleri de ele alınmıştır. Yaygınlaşan IoT cihazların siber güvenlik kaygılarını doğurmasının en büyük faktörlerinden biri de mahremiyet riskleridir. Günlük hayatımızda vazgeçilmez hale gelmiş olan IoT cihazlar, kullanıcılarının kişisel verilerini işleyebilmekte ve depolayabilmektedir. 8228 dökümanı bir güvenlik referans dökümanı olmamasına rağmen, privacy risklerini konu aldığı için bu yazı içerisinde yer almıştır.

[9] NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers - https://csrc.nist.gov/publications/detail/nistir/8259/final
[10] NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline - https://csrc.nist.gov/publications/detail/nistir/8259a/final
[11] NISTIR 8228 Considerations for Managing Internet of Things Cybersecurity and Privacy Risks - https://csrc.nist.gov/publications/detail/nistir/8228/final

1.8. Department for Digital, Culture, Media and Sport - Code of Practice for Consumer IoT Security

DDCMS tarafından Ekim 2018 yılında yayınlanmış Code of Practice for Consumer IoT Security[12] dökümanı diğer referans dökümanlarına benzer olarak 13 başlık altında yayınlamış olduğu best-practice'lerin yanında, IoT ekosistemindeki paydaşları 4'e ayırmıştır. Bu paydaşlar aşağıdaki gibidir.

1) **Device Manufacturer :** The entity that creates an assembled final internet-connected product. A final product may contain the products of many other different manufacturers.
2) **IoT Service Providers :** Companies that provide services such as networks, cloud storage and data transfer which are packaged as part of IoT solutions. Internet-connected devices may be offered as part of the service.
3) **Mobile Application Developers :** Entities that develop and provide applications which run on mobile devices. These are often offered as a way of interacting with devices as part of an IoT solution.
4) **Retailers :** The sellers of internet-connected products and associated services to consumers.

13 başlık altında yayınlamış olduğu best-practice'ler aşağıdaki gibidir. Bu best-practice'ler ile ETSI 303-645 dökümanındaki başlıkların birbirlerine çok yakın olduğu dikkat çekmektedir.

1) No default passwords
2) Implement a vulnerability disclosure policy
3) Keep software updated
4) Securely store credentials and security-sensitive data
5) Communicate securely
6) Minimise exposed attack surfaces
7) Ensure software integrity
8) Ensure that personal data is protected
9) Make systems resilient to outages
10) Monitor system telemetry data
11) Make it easy for consumers to delete personal data
12) Make installation and maintenance of devices easy
13) Validate input data

2. Sonuç

Güvenlik referans dökümanlarının özellikle büyük bölümünün son 1 yıl içerisinde yayınlandığı görülmektedir. Bu açıdan baktığımızda IoT cihazlarının güvenlik probleminin enstitüler, ulusal ve uluslararası kuruluşların gündeminde olduğunu ve süreç içerisinde güvenlik olgunluğunun ileri bir seviyeye taşınacağını düşünmekteyiz. Önümüzdeki yıllarda, incelediğimiz güvenlik gereksinimlerinin bir referans olmaktan çıkıp regülasyon haline geleceği, üreticilerden ürünlerini bu regülasyonlara uygun bir şekilde üretmelerinin isteneceği ve common-criteria vb. test laboratuvarları ile ürünlere bu kabiliyetlerin kazandırılmış olma durumularının test edileceğini göreceğiz. Aynı zamanda ülkemizdeki kurumlar tarafından da bu konu takip edilmekte ve çalışmalar yapılmakta olup, bizler de bu çalışmaların bir paydaşı olarak görev almaktayız.

[12] Code of Practice for Consumer IoT Security - https://bit.ly/2RzeMij

Biznet Bilişim Sistemleri ve Danışmanlık Sanayi Tic. A.Ş.

Ticari Sicil No: 159433

İSTANBUL
Nida Kule Plaza,
Kozyatağı Mah.
Değirmen Sok. No:18
Kat:19 34742 Kozyatağı,
Kadıköy, İstanbul
+90 216 688 8182

ANKARA
ODTÜ Teknokent İkizler
Binası Üniversiteler Mah.
İhsan Doğramacı Bulvarı
No:35 B Blok Kat:106800
Çankaya / Ankara
+90 312 210 1177

DUBAI
SECURRENT ME FZ LLC
214, Building 12, DIC
502318, UAE - Dubai
+9 9714 390 16 46-49

LAHEY/ HOLLANDA
Penetra Cyber Security
Strawinskylaan 411
1077XX Amsterdam
The Netherlands
+31(0)70-2045180

CYBER WISE