Cyberbezpieczeństwo dla produktów IoT

Wojciech Uzdrzychowski
www.smart-ce.eu
https://www.linkedin.com/in/wojciech-uzdrzychowski/

KONFERENCJA
R&D ELECTRONICS POLAND
B+R ELEKTRONIKI W POLSCE
5 ED. EMC FOR BUSINESS

Skąd taki temat?

- Rosnąca liczba urządzeń i ataków (rpi),
- Obowiązek wynikający z dyrektywy RED,
- Czas implementacji (przykład DL)

Co to jest cyberbezpieczeństwo?

Cyberbezpieczeństwo (ang. cybersecurity) – ogół **technik**, **procesów** i praktyk stosowanych w celu **ochrony sieci** informatycznych, **urządzeń**, **programów** i **danych** przed atakami, uszkodzeniami lub nieautoryzowanym dostępem. (...)

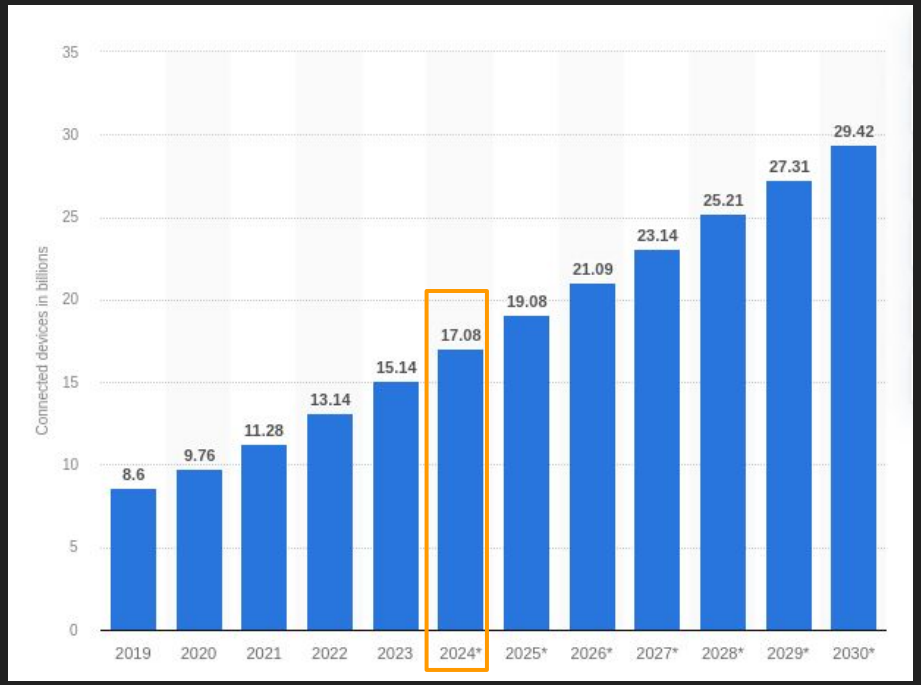
Cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

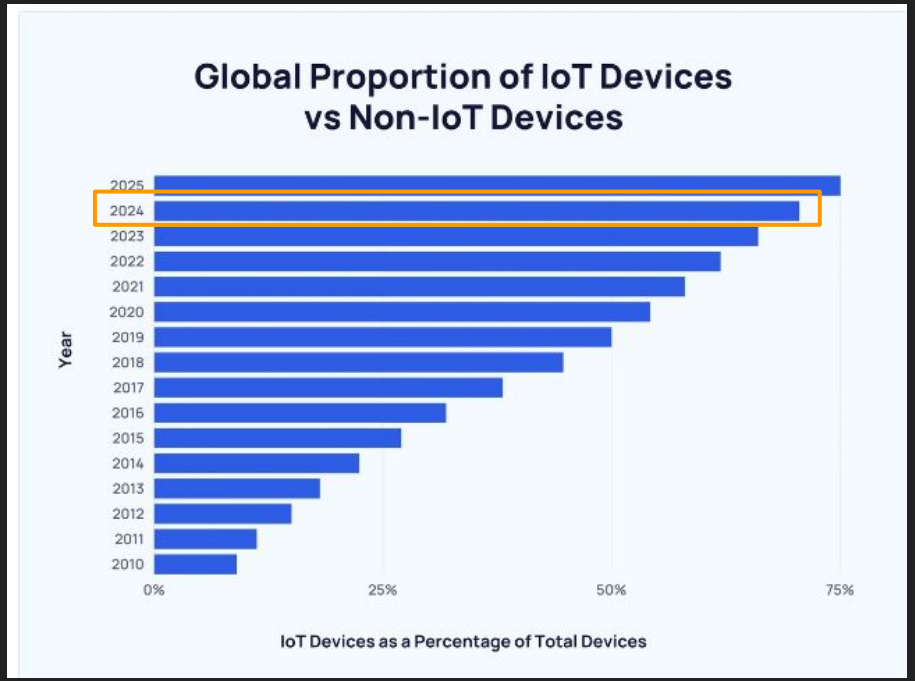
https://pl.wikipedia.org/wiki/Cyberbezpiecze%C5%84stwo

Co to jest urządzenie IoT?

- Urządzenie z dostępem do internetu
- Przetwarza, gromadzi lub przesyła dane
- Najczęściej tanie i o małej mocy obliczeniowej

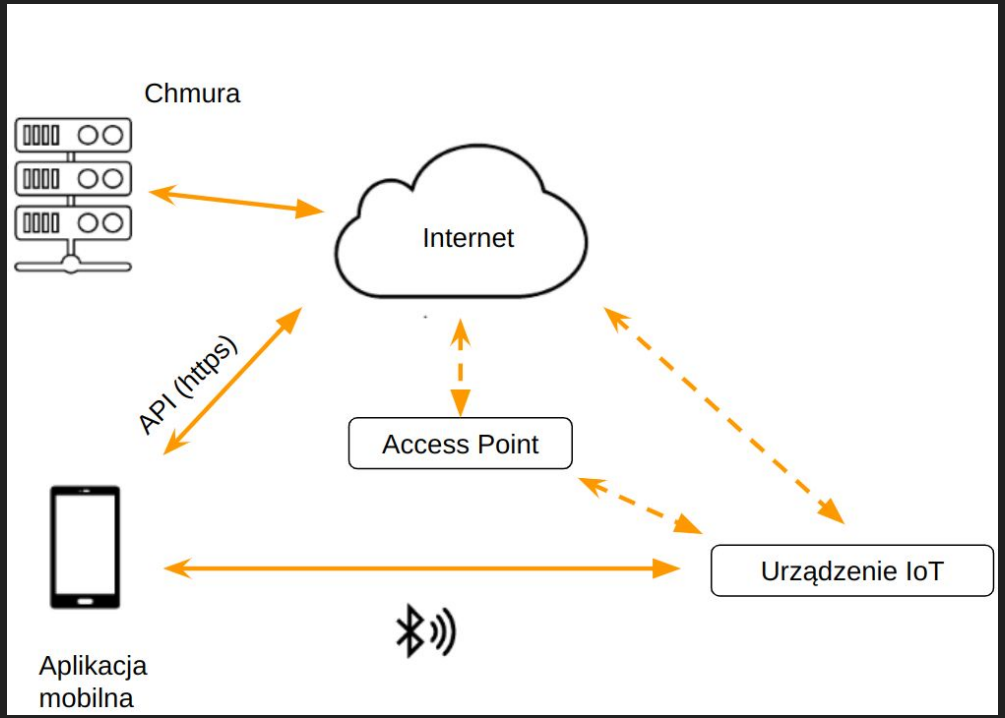
Jak dużo jest urządzeń IoT?





https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
https://transformainsights.com/research/forecast/highlights

Architektura systemu IoT



Statystyka ataków

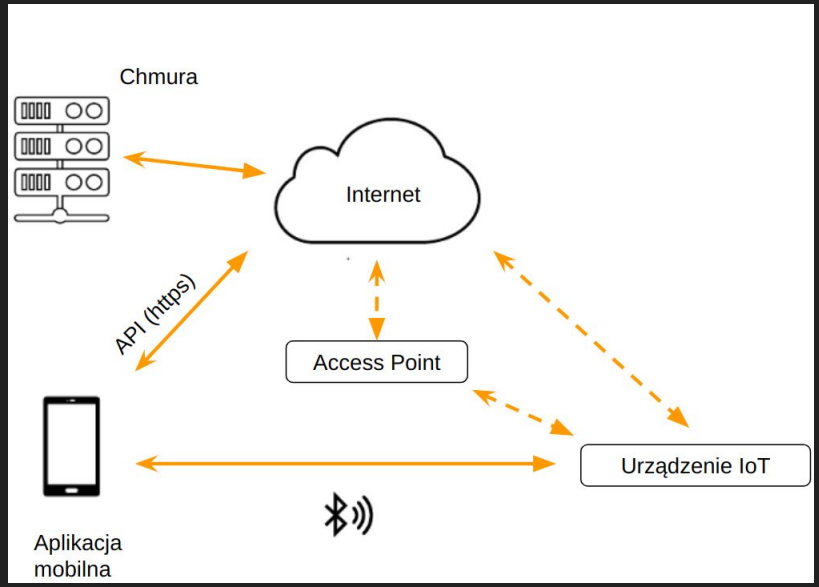
- W roku **2022** liczbę ataków szacuje się na ok **112** milionów (32 miliony w 2018)
- Wzrost rok do roku: **87%***
- **89%** organizacji, które używają urządzeń IoT został dotkniętych atakiem o średnim koszcie **$250k**
- W ciągu ostatnich **3 lat 69%** organizacji zauważyło **wzrost** liczby ataków na urządzenia IoT

*malware incidents

https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/
https://www.keyfactor.com/state-of-iot-security-report-2023/#keyfindings

Powody niskiego poziomu zabezpieczeń

- Brak perspektywy makro
- Brak świadomości wśród programistów
- Problemy bezpieczeństwa z łańcuchem dostaw
- Używanie niepewnych frameworków i bibliotek stron trzecich



Powody - top 10

1. Słabe, łatwe do odgadnięcia lub zakodowane na stałe hasła (hardcoded)
2. Niebezpieczne usługi sieciowe
3. Niebezpieczne interfejsy ekosystemu
4. Brak mechanizmu bezpiecznej aktualizacji
5. Używanie niebezpiecznych lub przestarzałych komponentów
6. Niewystarczająca ochrona prywatności
7. Niebezpieczny transfer i przechowywanie danych
8. Brak zarządzania urządzeniami
9. Niebezpieczne ustawienia domyślne
10. Brak bezpieczeństwa fizycznego

https://owasp.org/www-chapter-toronto/assets/slides/2019-12-11-OWASP-IoT-Top-10---Introduction-and-Root-Causes.pdf
https://arxiv.org/abs/1705.06805

Czego chcą atakujący?
I czy każdy atakujący to przestępca?

- Pieniędzy
- Kradzież danych osobowych (tożsamości) -> pieniądze
- Wykorzystanie do dalszych ataków
- Chęć poprawy bezpieczeństwa

[avast] https://www.avast.com/c-hacker-types

->10

Ryzyka i konsekwencje

Analiza ryzyka

Określenie **co tak naprawdę chcemy chronić** i na ile to wyceniamy

Perspektywa producenta

-czas/pieniądze
-koszt wprowadzenia poprawek w HW/SW

Życie i zdrowie - rozruszniki serca, pompy insulinowe

Konsekwencje

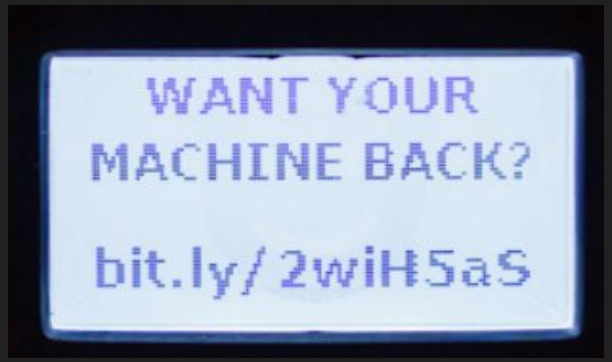
Konsekwencje
-reputacja, odejścia pracowników
-dane/prywatność klientów
-naprawienie szkód, odszkodowania

regulacje (RED) -> kary/wycofanie produktu z rynku

Realne przykłady

Ekspres do kawy żąda okupu

Dostanie się do sprzętu, urządzenie w trybie AP, nieszyfrowane połączenie do smartfona, aktualizacje bez szyfrowania, uwierzytelniania i podpisywania kodu, dostanie się do uP -> disassembler, alternatywne oprogramowanie udające, początkowo chciał kopać kryptowaluty



https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/

Realne przykłady

The Persirai botnet

Ponad 1000 różnych modeli kamer IP, połączenie przez otwarty port, ściągnięcie i zainstalowanie alternatywnego oprogramowania, ponad **122 000 zostało przejętych** i użytych do ataku DDoS

Pompa insulinowa

Cukrzyk sam zbadał pompę insulinową, nieszyfrowany tekst do komunikacji, przechwycenie, zmodyfikowanie dawki, odtworzenie wiadomości, atak zadziałał, pacjent nic nie wiedział -> poprawka po 5 miesiącach

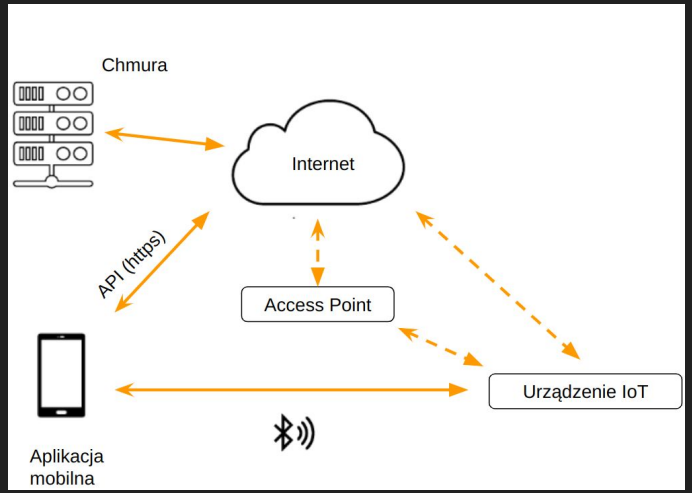
[pp] https://www.trendmicro.com/en_us/research/17/e/persirai-new-internet-things-iot-botnet-targets-ip-cameras.html

Jak się włamać do urządzenia IoT? Ustrukturyzowane podejście

IoT - Pentesting

- **Dostęp fizyczny/analiza HW**
- **Zdobycie Firmware’u**
- **Analiza Komunikacji / radio**
- Analiza aplikacji mobilnej/webowej

Celem jest zdobycie firmware’u



https://www.iotpentestingguide.com/

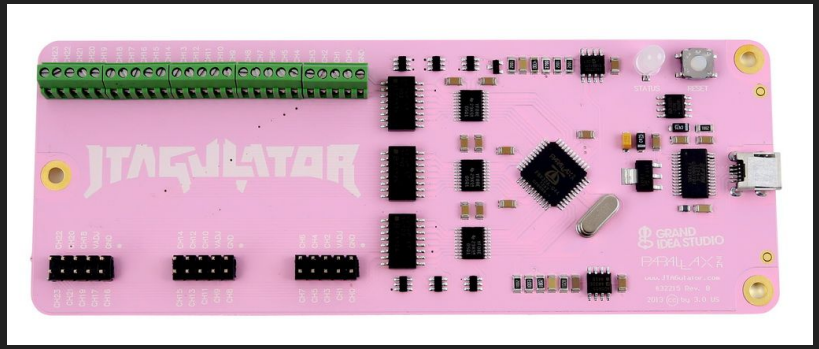
Analiza Hardware’u

- Bezpieczeństwo fizyczne
- Inspekcja zewnętrzna
- Dostępność portów
- Inspekcja wewnętrzna
  - Użyte układy scalone

SPI, I2C, USB, UART, I2C, JTAG, SWD

\+ Informacje dostępne on-line, raporty FCC

Analiza Hardware’u



[zdj] https://www.tarlogic.com/blog/owasp-fstm-obtaining-iot-device-firmware/

https://hackerwarehouse.com/product/jtagulator/

Komunikacja Radiowa

RFID
kopiowanie
domyślne klucze i niepewne mechanizmy szyfrowania
->brute force

BLE
przechwycenie, analiza, modyfikacja, retransmisja

WiFi
Ataki przez deasocjacje i asocjacje
802.11: ramki zarządzające nie są szyfrowane, pakiety można podsłuchać, zmodyfikować i odtworzyć

LoRa

Zigbee

Użycie **SDR** (ang. Software defined radio)

Identyfikacja częstotliwości
Identyfikacja modulacji
przechwycenie i zdekodowanie komunikacji
odtworzenie/modyfikacja i odtworzenie transmisji

Analiza Firmware’u

OWASP Firmware Security Testing Methodology

Etapy analizy:
1: Zbieranie informacji
2: Zdobycie firmware’u urządzenia IoT
3: Analiza firmware’u
4: Rozpakowanie systemu plików
5: Analiza zawartości systemu plików
6: Emulacja firmware’u
7: Analiza Dynamiczna
8: Debugowanie
9: Wykorzystanie plików wykonywalnych

Czego szukać:

1. Zakodowane na stałe hasła
2. Backdoor’y.
3. Adresy URL (aktualizacje).
4. Tokeny.
5. API i klucze szyfrujące.
6. Użyte algorytmy szyfrowania.
7. Lokalne ścieżki dostępu.
8. Szczegóły środowiska
9. Mechanizmy Autentykacji i Autoryzacji
10. Identyfikatory SSID
11. Podatne serwisy
12. Pliki konfiguracyjne
13. Pliki źródłowe
14. Oprogramowanie firm trzecich

https://www.tarlogic.com/cybersecurity-glossary/fstm/
https://github.com/scriptingxss/owasp-fstm

Jak się zabezpieczyć?

Mapowanie wektorów ataku

Kroki:

- Lista wszystkich komponentów
- Przygotowanie diagramu zależności i komunikacji
- Identyfikacja wektorów ataku dla każdego komponentu, kanału komunikacyjnego i protokołu
- Klasyfikacja zagrożeń ze względu na ich krytyczność

Mapowanie wektorów ataku

Mapowanie zagrożeń za pomocą metody **STRIDE,** która skupia się na identyfikacji słabych stron, a nie na wrażliwych zasobach lub potencjalnych atakujących.

Spoofing	(podszywanie się)
Tampering	(manipulacja)
Repudiation	(wyparcie się)
Information Disclosure	(ujawnienie informacji)
Denial of Service	(blokada usługi)
Elevation of Privilege	(zwiększenie uprawnień)

https://en.wikipedia.org/wiki/STRIDE_model

Mapowanie wektorów ataku

Klasyfikacja zagrożeń **DREAD**

Damage	jak dużą szkodę wyrządza
Reproducibility	jak łatwa jest do zreprodukowania
Exploitability	jak łatwa jest do wykorzystania
Affected Users	ile użytkowników to dotyczy
Discoverability	jak łatwo jest zidentyfikować zagrożenie

https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model)

Regulacje i normy

->25

Regulacje i normy

Dyrektywa RED 2014/53/EU -> Rozporządzenie **2022/30**

Artykuł 3

Zasadnicze wymagania

3. Urządzenia radiowe w obrębie określonych kategorii lub klas skonstruowane są w sposób gwarantujący spełnienie następujących zasadniczych wymagań:

d) urządzenia radiowe nie wywierają niepożądanego wpływu na sieć i jej funkcjonowanie ani też nie wykorzystują zasobów sieciowych w nieodpowiedni sposób, powodując tym samym niedopuszczalne obniżenie poziomu usług;

e) urządzenia radiowe mają wbudowane systemy zabezpieczające w celu zapewnienia ochrony danych osobowych i prywatności użytkownika i abonenta;

f) urządzenia radiowe wyposażone są w funkcje, które zapewniają ochronę przed oszustwami;

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053

Regulacje i normy

Dyrektywa RED 2014/53/EU -> Rozporządzenie **2022/30** -> Rozporządzenie **2023/2444**

Od **1 Sierpnia 2025**

Jakie urządzenia?

- Urządzenia przetwarzające dane osobowe, lokalizacyjne i związane z ruchem
- Urządzenia do opieki nad dziećmi,
- Zabawki,
- Urządzenia noszone (wearables), ubrania
- Urządzenia podłączone do internetu, które pozwalają na przekazanie środków pieniężnych w tym kryptowalut

Regulacje i normy

Dyrektywa RED 2014/53/EU -> Rozporządzenie 2022/30

2016/679 Rozporządzenie o ochronie danych

1) „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679

Regulacje i normy

Dyrektywa RED 2014/53/EU -> Rozporządzenie 2022/30

Ocena zgodności

- Bezpieczeństwa nie da się zmierzyć
- Normy jeszcze nie są zharmonizowane
- Podejście wysokiego poziomu
- Zalecane wprowadzenie od początku projektu

Regulacje i normy

Dyrektywa RED 2014/53/EU -> Rozporządzenie 2022/30

Normy, które najprawdopodobniej zostaną zharmonizowane:

ETSI EN 303 645 V2.1.1, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

prEN 18031-1:Common security requirements for radio equipment - Part 1: Internet connected radio equipment

prEN 18031-2: Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment

prEN 18031-3: Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value

Regulacje i normy

prEN 18031-1/2/3

[ACM] - Access control mechanism
[AUM] - Authentication mechanism
[SUM] - Secure update mechanism
[SSM] - Secure storage Mechanism
[SCM] - Secure communication mechanism
[RLM] - Resilience mechanism
[NMM] - Network monitoring mechanism
[TCM] - Traffic control mechanism
[CCK] - Confidential cryptographic keys
[GEC] - General equipment capabilities
[CRY] - Cryptography
[LGM] - Logging Mechanism.
[DLM] - Deletion mechanism
[UNM] - User notification mechanism

Każdy standard z rodziny **EN 18031** mapuje się do innego artykułu dyrektywy…

Document	Covers the essential requirements of	Addresses security assets and risks	Addresses network assets and risks	Addresses privacy assets and risks	Addresses financial assets and risks
prEN 18031-1 (JT013058)	3.3.(d)	✓	✓	×	×
prEN 18031-2 (JT013059)	3.3.(e)	✓	×	✓	×
prEN 18031-3 (JT013060)	3.3.(f)	✓	×	×	✓

…ale to producent, przez ocenę ryzyka, musi zadecydować czy do danego urządzenia stosuje się jeden czy kilka standardów.

Current Status of the Certification System in Europe MIC MRA International Workshop 2024 Tokyo 06 March 2024
https://www.tele.soumu.go.jp/resource/j/equ/mra/pdf/05/e/05.pdf

Regulacje i normy

ETSI EN 303 645 V2.1.1, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements

Zestaw 13 rekomendacji gdzie najważniejsze to:

- Brak domyślnego hasła,
- Polityka ujawniania podatności,
- Dbanie o aktualizację oprogramowania

- Charakteryzują się wysokim poziomem i są zorientowane na wyniki

Vulnerability Management and Communication:
Implement a means to manage reports of vulnerabilities,
Communicate securely.

Software and System Integrity:
Keep software updated
Ensure software integrity
Validate input data

Data Security and Privacy:
No universal default passwords
Securely store sensitive security parameters.
Ensure that personal data is secure.
Make it easy for users to delete user data.

System Resilience and Accessibility:
Minimize exposed attack surfaces.
Make systems resilient to outages.
Examine system telemetry data.
Make installation and maintenance of devices easy

Regulacje i normy

Implementation conformance statement (ICS) pro forma

Table B.1: Implementation of provisions for consumer IoT security

Clause number and title			
Reference	**Status**	**Support**	**Detail**
5.1 No universal default passwords			
Provision 5.1-1	M C (1)		
Provision 5.1-2	M C (2)		
Provision 5.1-3	M		
Provision 5.1-4	M C (8)		
Provision 5.1-5	M C (5)		

M	the provision is a mandatory requirement
R	the provision is a recommendation
M C	the provision is a mandatory requirement and conditional
R C	the provision is a recommendation and conditional

Regulacje i normy

ETSI TS 103 701

Określa metodologię oceny zgodności urządzeń IoT, ich związek z powiązanymi usługami

Zdefiniowane przypadki testowe i kryteria oceny dla każdego zalecenia.

Nie rozszerza normy ETSI 303 645

IXIT - (Implementation eXtra Information for Testing) wraz z ICS zawiera dodatkowe informacje o implementacji zabezpieczeń potrzebne przy ocenie zgodności (Gray-box testing)

Regulacje i normy

ETSI 303 645

Polityka ujawniania luk w zabezpieczeniach + Bug bounty

Dlaczego zachęcać do szukania luk?

Jak komunikować się ze zgłaszającym?

Nagrody?

Zagrożenia

ETSI TR 103 838 Coordinated Vulnerability Disclosure
ISO/IEC 29147 ISO/IEC 29147: "Information technology - Security techniques - Vulnerability Disclosure".
ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes

https://iotsecurityfoundation.org/manage-vulnerability-reports-webinar/
https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

->35

Normy, dokumentacje techniczne, raporty

ETSI TS 103 815 V1.1.1 (2024-01) CYBER; Cyber Security for Consumer Internet of Things; Requirements for Residential Smart Door Locking Devices
TS 103 848 - Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things

ETSI TR 103 621 V1.2.1 (2022-09)
Guide to Cyber Security for Consumer Internet of Things

ETSI TR 103 743 V1.1.1 (2021-07)
CYBER; Home Gateway Security Threat Analysis

ETSI TS 103 929 V1.2.1 (2023-05)
Cyber Security (CYBER); Mapping of specific requirements of standardisation request for RED articles 3(3)(d), 3(3)(e) and 3(3)(f) to IEC 62443-4-2 requirements and to ETSI EN 303 645 provisions

ETSI TR 103 838 Coordinated Vulnerability Disclosure

ETSI TR 103 331 V2.1.1 (2022-12)
Cyber Security (CYBER); Structured threat information sharing
ETSI TR 103 644 V1.2.1 (2020-09)
CYBER; Observations from the SUCCESS project regarding smart meter security

Normy, dokumentacje techniczne, raporty, linki

prEN 18031-1 Common security requirements for radio equipment - Part 1: Internet connected radio equipment
prEN 18031-2: Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment
prEN 18031-3: Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value

ETSI TS 103 701: CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements

ISO/IEC 27005: Information security, cybersecurity and privacy protection — Guidance on managing information security risks
EN IEC 62443-4-2: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej -- Część 4-2: Wymagania techniczne bezpieczeństwa dla komponentów IACS

https://github.com/V33RU/IoTSecurity101
https://www.youtube.com/@mattbrwn
https://yogeshojha.com/me/wp-content/uploads/2020/04/Yogesh-Ojha-SARCON-Getting-STarted-with-IoT.pdf

PRACTICAL IOT HACKING, The Definitive Guide to Attacking the Internet of Things, Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods, ISBN-13: 978-1-7185-0091-4 (ebook)

The IoT Hacker's Handbook A Practical Guide to Hacking the Internet of Things, Aditya Gupta, ISBN-13 (electronic): 78-1-4842-4300-8

EOF

Wojciech Uzdrzychowski
www.smart-ce.eu
https://www.linkedin.com/in/wojciech-uzdrzychowski/