

IoT Security

Cyberboswachters

Tim Dams

Deze cursus werd gemaakt met hulp van AI-assistentie. Sommige afbeeldingen zijn door AI gegenereerd.





AI GENERATED

Wat leer je in dit hoofdstuk?

Na dit hoofdstuk kan je:

- ✓ de **specifieke uitdagingen van IoT-security** benoemen (low-power, long-life, firmware, defaults)
- ✓ met **Mirai** illustreren waarom zwakke IoT een systemisch risico vormt
- ✓ de rol van **TPM** en andere hardware-mitigaties situeren
- ✓ de **McCumber-kubus** toepassen op een IoT-case (rust / transport / verwerking)
- ✓ de **wet van diminishing returns** gebruiken bij security-prioritering

IOT SECURITY: ALLES KOMT SAMEN

Ieder IoT-apparaat in je netwerk is een potentiële **toegangspoort** tot de rest van je infrastructuur.

Mirai (2016) toonde al hoe krachtig een botnet van IoT-apparaten kan zijn. IoT beveiligen vraagt **alles** wat we al leerden, en meer.

Waarom is IoT moeilijker te beveiligen?



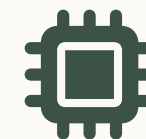
Low-power

Security protocols mogen geen grote hap uit de batterij nemen.



Lage bandbreedte

Honderden sensoren op hoge bandbreedte? Dat trekt geen enkel netwerk.



Beperkte hardware

Weinig CPU en opslag, dus minder beveiligingsmogelijkheden.



Moeilijk te updaten

Patches uitrollen is omslachtig, soms moet je fysiek ter plaatse.



Onbeschermdde locaties

Aanvallers kunnen ongezien met het apparaat knoeien.

Enterprise of thuis?

IoT is niet overal hetzelfde:

Enterprise IoT

- Een industriële sensor heeft vaak een **doordachte update-strategie**

vs

Consumer IoT

- Je slimme koelkast thuis vermoedelijk **niet**

OPEN WEB APPLICATION SECURITY PROJECT

OWASP IoT Top 10

Gerangschikt van meest voorkomend naar minst voorkomend.

OWASP

Een open-source platform voor **cybersecuritykennis**.



Top 10-lijsten

De meest voorkomende kwetsbaarheden, van meest naar minst voorkomend.



Tools en gidsen

Praktische tools, best practices en gidsen.



IoTGoat

Bewust onveilige firmware: leer de IoT Top 10 kennen door ze zelf uit te buiten.

IoTGoat: github.com/OWASP/iotgoat

De Belgische OWASP-tak organiseert (gratis) workshops en events.

OWASP IoT Top 10: overzicht

OWASP IoT Top 10

versie 2018, gerangschikt van meest naar minst voorkomend

1	Paswoorden zwak, raadbaar of hardgecodeerd
2	Ongebruikte of onveilige netwerkservices diensten die openstaan zonder dat het moet
3	Onveilig ecosysteem de app, de cloud en de webinterface errond
4	Geen of onveilig updatemechanisme firmware die je niet veilig kan bijwerken
5	Oude of onveilige componenten verouderde libraries en chips van derden
6	Onvoldoende privacy bescherming persoonlijke data die slordig bewaard wordt
	Onveilige datatransfer en opslag

Zwakke of hardcoded wachtwoorden

1

Default wachtwoorden zijn
publiek bekend



2

Aanpassen is **omslachtig**:
geen webinterface, wel
fysieke knoppen of vreemde
tools



3

Gebruikers laten het **default
wachtwoord** staan

Mirai (2016) besmette zo honderdduizenden apparaten, puur door default wachtwoorden te proberen. Het resultaat: een DDoS op Dyn die grote delen van het Internet platlegde.

"WAT KAN EEN HACKER NU MET MIJN DIGITALE THERMOMETER?"

Een cybercrimineel gebruikt je thermometer als **springplank** naar de rest van je netwerk.

Stroopers zoeken altijd de **weakest link**.

Zet je IoT in quarantaine

Eén gepwnd IoT-toestel mag niet de **toegangspoort** tot de rest van je netwerk worden: **netwerksegmentatie**.

Thuis

IoT-toestellen op het **gastnetwerk** van je router: de slimme stekker kan aan het Internet, niet aan je laptop of NAS.

vs

In een bedrijf

Aparte segmenten (bv. **VLANs**) voor camera's, printers, productiemachines en kantoor-pc's.

Layering en limiting in de praktijk. Hoe je dit opzet, zie je in **Network Security**.

Ongebruikte of onveilige netwerkservices

Printers bijvoorbeeld: er draaien vaak **meerdere netwerkservices** waar de gebruiker niets van weet.

Telnet

...

Sommige zijn **inherent onveilig**: Telnet communiceert **onversleuteld**.

Kijk zelf eens welke services op je Windows-pc draaien: `services.msc`.

2017

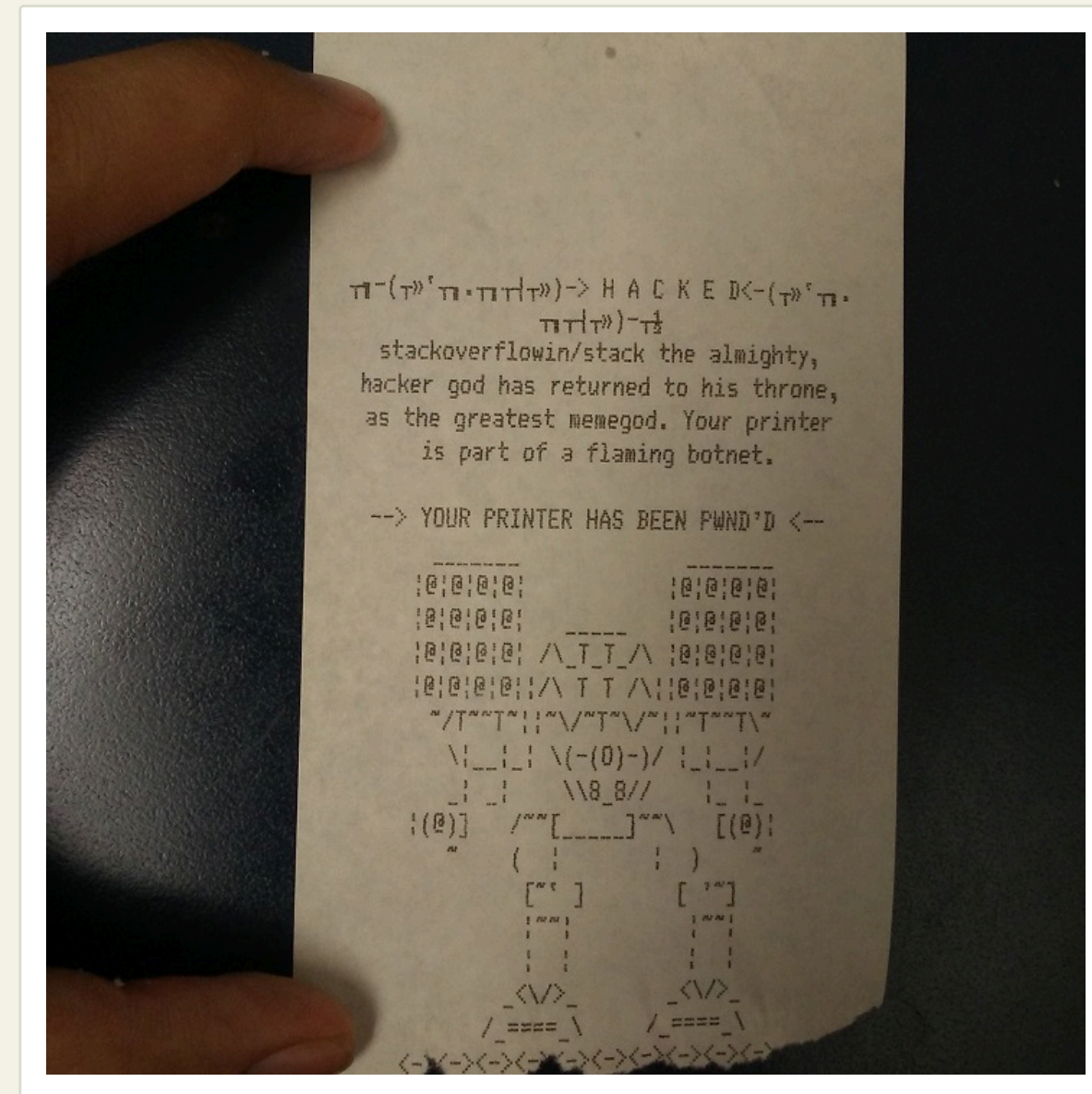
Printer hack

150.000

printers in Nederland (vermoedelijk) bereikbaar via
poort 9100

Een grayhat hacker printte er
waarschuwingbriefjes op.

Nieuw apparaat? Kijk welke netwerkservices
actief zijn en zet de onnodige **uit**.



150.000 printers bereikbaar via het open internet
(Bron: inktweb.nl).

Onveilig ecosysteem

Een IoT-apparaat staat zelden alleen:



Cloud-dashboards

fitbit.com, Google Nest, ...



Smartphone-apps



Third-party koppelingen

IFTTT, ...

Je apparaat is zo sterk als de **zwakste schakel**. Wordt fitbit.com gehackt, dan kunnen aanvallers mogelijk ook aan jouw data of apparaten.

Gebruikers vergeten welke diensten toegang hebben. Kijk geregeld in je **Google-** of **Facebook/Meta**-accountinstellingen wat er gekoppeld is.

Geen of onveilig updatemechanisme

Updates dichten lekken. Maar bij IoT is updaten **niet vanzelfsprekend**:

- ✗ Geen remote update → **fysiek ter plaatse** gaan
- ✗ Update mislukt → apparaat *gebrickt*
- ✗ Patches voor x jaar, daarna niets meer
- ✗ Fabrikant bestaat niet meer → **nooit** nog patches
- ✗ Bug in een **externe chip** → wie is verantwoordelijk?

Abonneer je als cyberboswachter op **CVE-feeds** en RSS-feeds van fabrikanten.

In Europa verplicht de **Cyber Resilience Act** fabrikanten tot beveiligingsupdates tijdens de verwachte levensduur (in principe minstens vijf jaar, vanaf december 2027).

Vlot tien jaar aan het net, amper drie jaar ondersteund



De ondersteuning stopt lang voor het toestel dat doet.

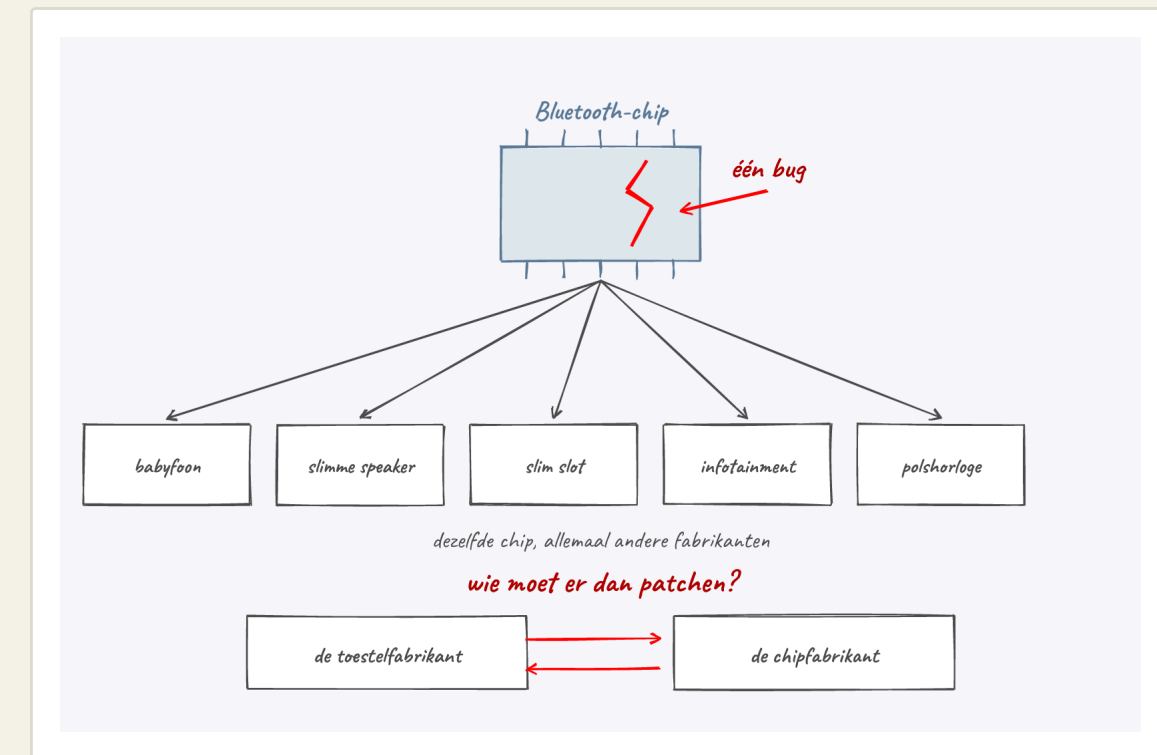
2021

BrakTooth

Kritieke Bluetooth-kwetsbaarheid in **miljoenen** IoT-apparaten.

De bug zit in de **Bluetooth-chip**, niet in de software van de fabrikant.

Sommige chipfabrikanten: “*we patchen alleen als er genoeg vraag naar is*”.



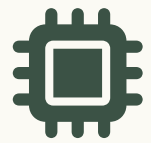
Eén bug in één chip, in toestellen van tientallen fabrikanten.

Mogelijke aanvallen: DoS: apparaat crashen

ACE: eigen code uitvoeren (Arbitrary Code Execution)

Oude of onveilige componenten

Een IoT-apparaat bevat **tientallen onderdelen** van verschillende fabrikanten.



Hardware

Chips, radio-modules, sensoren.



Software

Bibliotheken, protocollen, besturingssysteem.

Een bug in een gedeelde component treft **alles** wat die component gebruikt.

Log4J (2021)

Heartbleed (2014)

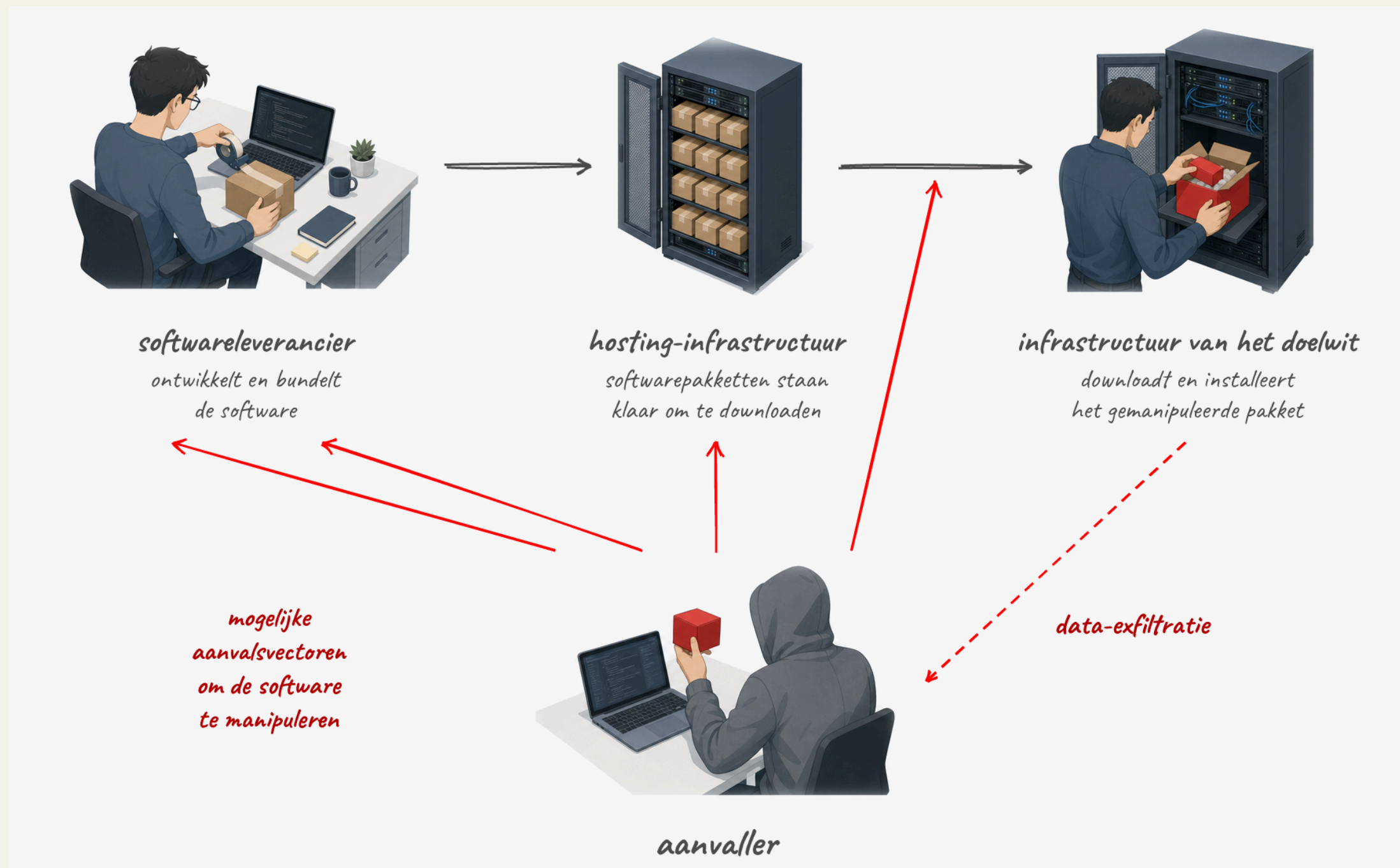
SolarWinds: een supply chain attack



De aanvallers richten zich op de **zwakste schakel** in de keten, om zo bij de klant achteraan te geraken.

Apart voorval, zelfde slordigheid: het wachtwoord van een update-server (*solarwinds123*) stond publiek op GitHub.

Supply chain attack: hoe werkt het?



Onvoldoende privacybescherming

IoT-fabrikanten verzamelen persoonlijke data. **GDPR** verplicht een veilige omgang ermee.

In de cloud

- Ultra-beveiligde database bij de fabrikant

vs

Op het apparaat

- Dezelfde data als **plaintext**

Onveilige datatransfer en opslag

De **McCumber-kubus**: C.I.A. moet gelden voor data in **alle** vormen.



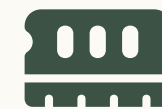
Opslag

Data onversleuteld op het apparaat.



Overdracht

Onversleutelde communicatie.



Verwerking

Data tijdelijk onbeveiligd in het geheugen.

Encryptie **enkel tijdens overdracht** geeft een vals gevoel van veiligheid. Staat de data onversleuteld op het apparaat, dan is die encryptie niet nutteloos, maar wel **onvoldoende**.

Gebrek aan apparaatbeheer



Aantallen

Honderden tot duizenden
apparaten: te veel om
manueel te bedienen.



Locatie

Moeilijk bereikbare of
gevaarlijke plaatsen.



Alarmen

Bij storingen of afwijkende
metingen.



Personeel

Enkel ter plaatse als het echt
nodig is.



Mission-critical

Elke downtime = winstverlies
of boetes.



Zelf ook veilig

Moet zelf robuust zijn, en is
zelden goedkoop.

Onveilige standaardinstellingen

Uit de doos komen apparaten met **standaardinstellingen** die aanvallers kennen.

Niet enkel wachtwoorden:

- ✗ Open poorten en services
- ✗ Onveilige protocollen ingeschakeld
- ✓ Gezonde gewoonte: controleer **alle instellingen** van een nieuw apparaat vóór je het in productie neemt, en zet uit wat je niet nodig hebt

WINDOWS XP: GEEN URBAN LEGEND

Een pc die tijdens de installatie aan het internet hing, was soms al **besmet** voor de installatie klaar was.

In 2004 overleefde een ongepatchte pc gemiddeld zo'n **20 minuten** op het Internet (zie **wormen** in H2).

Gebrek aan fysieke hardening

IoT-apparaten staan op **publiek toegankelijke plaatsen**, weken of maanden zonder dat iemand omkijkt. Aanvallers kunnen er rustig mee knoeien (*tamperen*).



UART / debug

Een seriële poort (vaak enkele pinnetjes op de print)
→ eigen firmware flashen.



Geen Secure Boot

Ongeautoriseerde software laden.



Geen TPM

Data uitlezen van het apparaat.

TPM

TPM-chips vinden steeds meer hun weg naar **nieuwe IoT-apparaten.**

De kost valt in het niets bij de schade van een gecompromitteerd apparaat.

Bewaar data ook **versleuteld** op het apparaat, voor als het fysiek gestolen of gemanipuleerd wordt.

TOT SLOT

Conclusie

We bespraken nog maar het tipje van de ijsberg.

De wet van diminishing returns

De **eerste**, eenvoudige stappen leveren de **grootste** winst op. Elke volgende stap voorkomt een steeds kleiner stuk van de problemen.

Basismaatregelen leveren de grootste veiligheidswinst op:

- ✓ Goede wachtwoorden
- ✓ Geen defaults
- ✓ **KISS**: elke extra feature is extra attack surface
- ✓ Updates

Elk volgend niveau is **belangrijk maar incrementeel**.

TOT SLOT

Wees veilig en verspreid het woord! ;)

Als we er samen in slagen de basis correct toe te passen én aan anderen te leren, maken we het digitale stropers al een pak moeilijker.

