IoT Security

Cyberboswachters

Tim Dams

IoT Security: alles komt samen

- We zagen al hoe Mirai (2016) aantoonde hoe krachtig een botnet van IoT-apparaten kan zijn
- IoT-netwerken beveiligen vereist **alles** wat we al leerden — én meer

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

Waarom is IoT moeilijker te beveiligen?

Beperking	Gevolg voor security
Low-power	Security protocols mogen geen extra batterij kosten
Lage bandbreedte	Zware encryptie of updates zijn vaak niet haalbaar
Beperkte hardware	Weinig CPU en opslag → minder beveiligingsmogelijkheden
Moeilijk te updaten	Patches uitrollen is omslachtig of fysiek vereist
Onbeschermde locaties	Fysieke toegang voor aanvallers is reëel

> **Opmerking**
>
> **Enterprise IoT** vs **consumer IoT**: een industriële sensor heeft vaak een doordachte update-strategie. Een slimme koelkast thuis vermoedelijk niet.

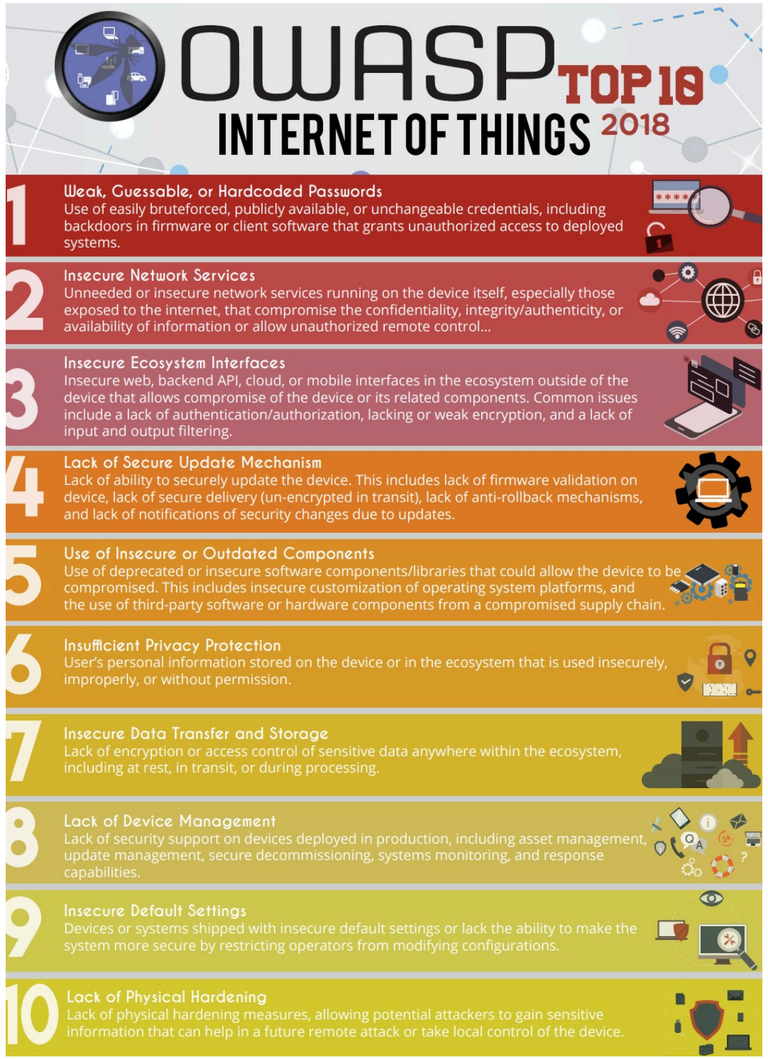
OWASP IoT Top 10

OWASP (*Open Web Application Security Project*) is een open-source platform voor cybersecurity kennis.

- Publiceert **Top 10** lijsten van meest voorkomende kwetsbaarheden
- Gerangschikt van meest voorkomend → minst voorkomend
- Praktische tools, best practices en gidsen beschikbaar

> **Tip**
>
> **IoTGoat** (github.com/OWASP/IoTGoat): een bewust onveilige firmware om de OWASP IoT Top 10 te leren kennen door ze zelf uit te buiten.
>
> Ook de Belgische OWASP-tak organiseert (gratis) workshops en events.

OWASP IoT Top 10: overzicht



OWASP IoT Top 10 — versie 2018 (Bron: owasp.org).

#1 — Zwakke of hardcoded wachtwoorden

- Default wachtwoorden zijn publiek bekend — aanvallers kennen ze
- Wachtwoord aanpassen is vaak **omslachtig** op IoT-apparaten
  - → Geen webinterface → via fysieke knoppen of vreemde tools
  - → Resultaat: gebruikers laten het default wachtwoord staan

⚠ Waarschuwing

"Wat kan een hacker nu met mijn digitale thermometer?"

Een cybercrimineel gebruikt de thermometer niet als doel — maar als **springplank** naar de rest van je netwerk.

Belangrijk

Mirai (2016) besmette honderdduizenden apparaten puur door default wachtwoorden te proberen. Het resulteerde in één van de grootste DDOS-aanvallen ooit.

#2 — Ongebruikte of onveilige netwerkservices

- IoT-apparaten draaien vaak **meerdere netwerkservices** waar de gebruiker niets van weet

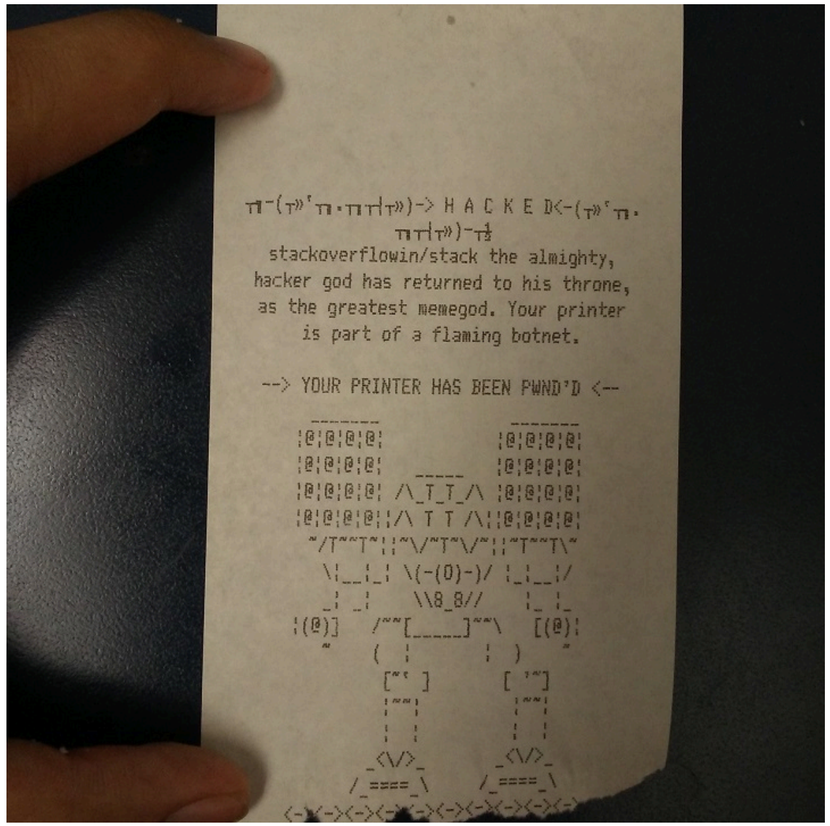
  → Printers, routers, camera's: vaak Telnet, FTP, SNMP, … actief

- Sommige services zijn **inherent onveilig**: bv. Telnet communiceert **onversleuteld**

> **Tip**
>
> Bekijk welke services actief zijn op je systemen: `services.msc` op Windows.

> **Opmerking**
>
> In 2017 bereikte een grayhat hacker **150.000 printers** in Nederland via poort 9100.
>
> Hij printte waarschuwingsbriefjes om gebruikers te wijzen op de onveiligheid van hun apparaat.

#2 — Printer hack (2017)



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

> ⚠ **Waarschuwing**
>
> Controleer altijd welke netwerkservices actief zijn op een nieuw apparaat — en zet onnodige services **uit**.

#3 — Onveilig ecosysteem

IoT-apparaten zijn zelden alleen — ze maken deel uit van een **ecosysteem**:

- Cloud-dashboards (fitbit.com, Google Nest, …)
- Smartphone-apps
- Third-party koppelingen (IFTTT, Alexa, …)

> ⚠ **Waarschuwing**
>
> De veiligheid van je apparaat is even sterk als de **zwakste schakel** in het hele ecosysteem.
>
> Als fitbit.com gehackt wordt → kans dat aanvallers ook bij jouw data of apparaten kunnen.

> **Tip**
>
> Gebruikers vergeten welke third-party diensten toegang hebben tot hun accounts.
>
> Controleer geregeld via je **Google** of **Apple** accountinstellingen welke apps en services gekoppeld zijn.

#4 — Geen of onveilig updatemechanisme

- Updates zijn cruciaal om beveiligingslekken te dichten
- Maar bij IoT is updaten vaak **niet vanzelfsprekend**:

- Apparaat heeft geen remote update-mogelijkheid → fysiek ter plaatse gaan
- Update mislukt → apparaat *gebrickt* → nog meer problemen
- Fabrikant brengt patches uit voor *x* jaar, daarna: niets meer
- Fabrikant bestaat niet meer → patches komen nooit meer
- Bug zit in een **externe chip** → wie is verantwoordelijk?

> **Tip**
>
> Abonneer je als cyberboswachter op **CVE-feeds** en RSS-feeds van fabrikanten om tijdig op de hoogte te zijn van nieuwe kwetsbaarheden.

#4 — BrakTooth (2021)

- Kritieke Bluetooth-kwetsbaarheid in **miljoenen** IoT-apparaten
- Bug zit in de **Bluetooth-chip**, niet in de software van de fabrikant
- Sommige chipfabrikanten: *“we patchen alleen als er genoeg vraag naar is”*

BrakTooth: de zoveelste Bluetooth-kwetsbaarheid.

Mogelijke aanvallen:

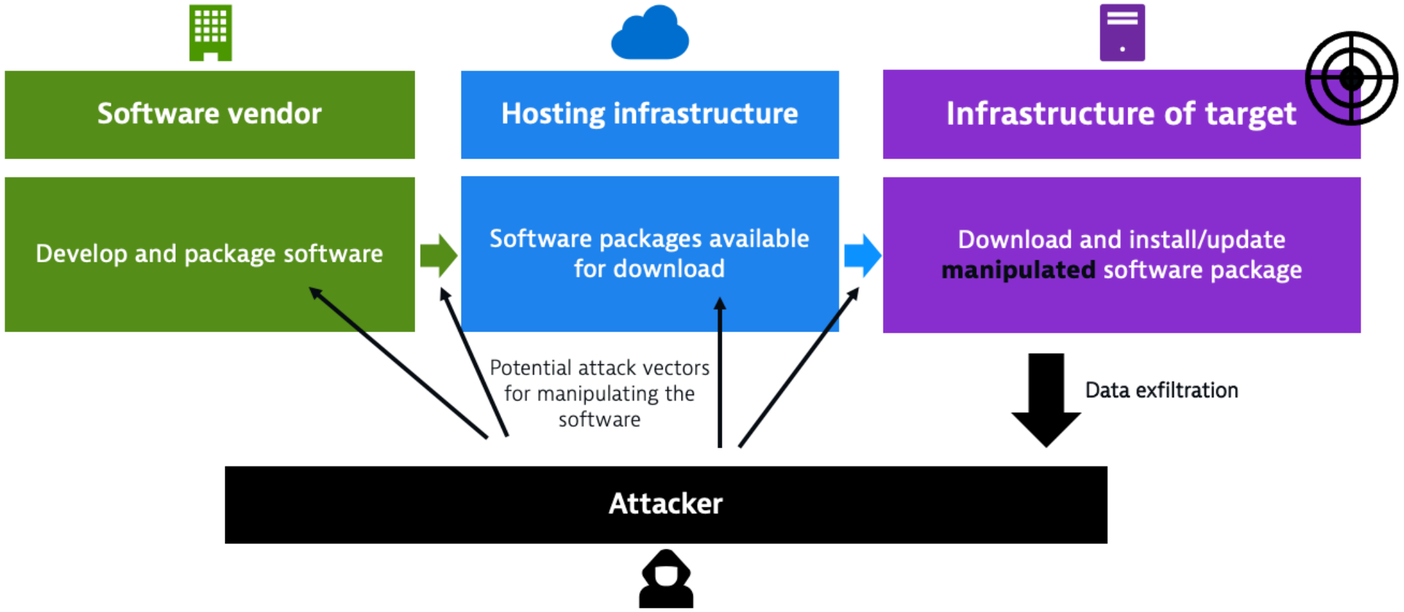
- **DoS**: apparaat crashen
- **ACE** (Arbitrary Code Execution): eigen code uitvoeren op het apparaat

#5 — Oude of onveilige componenten

- Een IoT-apparaat bevat **tientallen onderdelen** van verschillende fabrikanten
- Hardware: chips, radio-modules, sensoren
- Software: bibliotheken, protocollen, besturingssysteem

> ⚠ **Waarschuwing**
>
> Een bug in een gedeelde component (bv. een Bluetooth-chip of een open-source bibliotheek) treft **alles** wat die component gebruikt.
>
> **Log4J (2021)** en **Heartbleed (2014)**: kleine bugs in veel gebruikte bibliotheken met wereldwijde impact.

#5 — SolarWinds: de supply chain attack



Supply chain attack: de aanvaller richt zich op een zwakke schakel in de keten (Bron: dynatrace.com).

> **Opmerking**
>
> Hackers kraakten de FTP-server van SolarWinds (wachtwoord: *solarwinds123*).
>
> Ze voegden een backdoor toe aan de Orion-software-update → duizenden klanten, waaronder de Amerikaanse overheid, werden automatisch besmet.

#6 — Onvoldoende privacybescherming

- IoT-fabrikanten verzamelen vaak persoonlijke data van gebruikers
- **GDPR** verplicht een veilige omgang met die data
- Probleem: data staat beveiligd in de cloud, maar **onversleuteld op het apparaat zelf**

> ⚠ **Waarschuwing**
>
> Een ultra-beveiligde database bij de fabrikant helpt niets als diezelfde data als *plaintext* op het IoT-apparaat wordt bewaard.
>
> Denk aan: fitness-trackers, slimme luidsprekers, bewakingscamera's.

#7 — Onveilige datatransfer en opslag

Herinner je de **McCumber kubus**: C.I.A. moet gelden voor data in **alle** vormen:

Fase	Risico
Opslag	Data onversleuteld op het apparaat
Overdracht	Communicatie onversleuteld (Telnet, HTTP, …)
Verwerking	Data tijdelijk onbeveiligd in geheugen

Belangrijk

Encryptie enkel tijdens overdracht geeft een **vals gevoel van veiligheid**.

Als de data onversleuteld op het apparaat staat, is de encryptie tijdens verzending nutteloos.

#8 — Gebrek aan apparaatbeheer

In een enterprise IoT-omgeving: **honderden tot duizenden apparaten** beheren.

Waarom is robuust device management essentieel?

- Te veel apparaten om manueel te bedienen
- Apparaten bevinden zich op **moeilijk bereikbare of gevaarlijke plaatsen**
- **Alarmen** nodig bij storingen of afwijkende metingen
- Efficiënt gebruik van personeel
- Deel van **mission-critical systemen**: elke downtime = verlies of boetes

> ⚠ **Waarschuwing**
>
> Een goed device management systeem is duur — maar een gecompromitteerd IoT-netwerk is duurder.

#9 — Onveilige standaardinstellingen

- Apparaten komen *uit de doos* met **standaardinstellingen** die aanvallers kennen
- Niet alleen wachtwoorden — ook:
  - → Open poorten en services
  - → Onveilige protocollen ingeschakeld
  - → Debugmodus actief

Opmerking

Windows XP urban legend: computers die rechtstreeks aan het internet werden gehangen tijdens de installatie werden soms al besmet voordat de installatie klaar was.

Artikels bevestigen dat dit effectief mogelijk was.

Belangrijk

Gezonde gewoonte: controleer **alle instellingen** van een nieuw apparaat vóór je het in productie neemt. Zet alles uit wat je niet nodig hebt.

#10 — Gebrek aan fysieke hardening

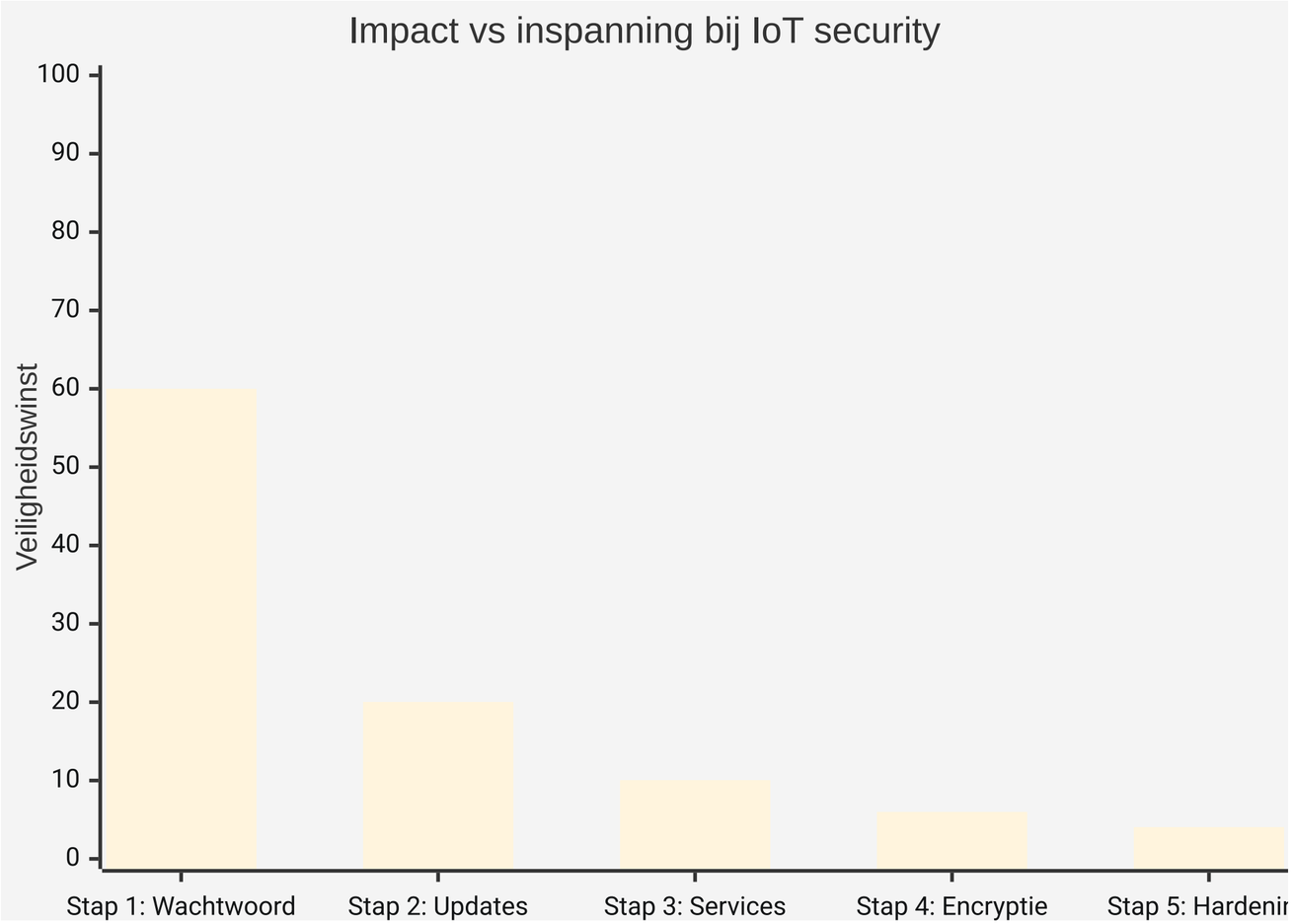
- IoT-apparaten staan op **publiek toegankelijke plaatsen**
- Werken weken/maanden zonder dat iemand er naar omkijkt
- Aanvallers kunnen rustig en ongezien knoeien (*tamperen*)

> **Tip**
>
> TPM-chips vinden steeds meer hun weg naar nieuwe IoT-apparaten.
>
> De kost valt in het niets bij de potentiële schade van een gecompromitteerd apparaat.

Risico's:

- **UART / debug-interfaces** toegankelijk → eigen firmware flashen
- **Geen Secure Boot** → ongeautoriseerde software laden
- **Geen TPM** → data uitlezen van het apparaat

Conclusie: de wet van diminishing returns



Conclusie

- **Basismaatregelen** leveren de grootste veiligheidswinst op:

  → Goede wachtwoorden, geen defaults, updates, onnodige services uitschakelen

- Elk volgend niveau is **belangrijk maar incrementeel**
- OWASP IoT Top 10 is een praktisch raamwerk om niets te vergeten

> **Tip**
>
> 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.

> **Belangrijk**
>
> Cybersecurity is geen eindbestemming — het is een voortdurend proces van **leren, aanpassen en verbeteren**.