Welke security by design principles zijn er? Welke zijn relevant voor IoT?

# Stel dat een IoT systeem voor een healthcenter gehackt wordt, hoe minimaliseer je deze schade?

Het is belangrijk om een goede beveiliging te hebben om cyber aanvallen tegen te gaan. Echter kan het zelfs met een goede beveiliging soms fout gaan en kan er op een of andere manier alsnog een aanval succesvol worden uitgevoerd.

In dit geval is het dan heel erg belangrijk dat de schade die ontstaat tijdens deze aanval zo veel mogelijk wordt beperkt. In dit hoofdstuk gaan we dieper in op mogelijkheden en technieken die ons kunnen helpen met het beperken van de schade in een dergelijk geval.

## Identificeren van de aanval

Er zijn veel verschillende manieren waarop een cyber aanval gedaan kan worden.

De impact van elke soort aanval is anders en vereist een andere aanpak. In het geval van een cyberaanval is het allereerst belangrijk om te identificeren wat voor een aanval het is.

### Welke veelgebruikte soorten aanvallen zijn er en hoe kunnen we dit identificeren?

Hier staat een korte lijst met meest voorkomende aanvallen en per aanval wordt uitgelegd wat het en de belangrijkste punten zijn om deze schade te beperken.

<https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Drive-by%20attack>

#### Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

DDoS/DoS is het overweldigen van de systeems resources zodat het niet zijn functie met acceptabel snelheid kan uitvoeren.

Acties die je kan ondernemen hier tegen zijn:

* Server achter Firewall zetten
* Vergroot the grote van the connection queue en verminder the timeout tijd van open connceties.
* bepaalde porten blocken
* incoming packets checken
* filtering

#### Man-in-the-middle (MitM) attack

Een MitM gebeurt wanneer de communicatie van een client naar een server niet direct is en wanneer de client dit niet weet, de “man in the middle” krijgt alle informatie van de client en stuurt het hierna pas door naar de server.

Preventie is het gebruik van juiste protocollen.

#### Phishing and spear phishing attacks

Valse berichten naar iemand sturen en deze legitiem over laten komen om deze mensen te bedriegen. Zodat deze mensen gegevens vrij geven.  
  
Preventie is om de mensen binnnen je bedrijf omgeving hier zo aware mogelijk van te maken. En aan te geven welke informatie via e-mail nooit zal worden gevraagd.

#### Drive-by attack

wanneer je op een site files kan downloaden en dit niet via een juist protocol doet kan iemand hier een andere download opzetten. Hiermee valt hij de gebruikers aan die bestanden van jouw site af downloaden.  
  
Preventie Probeer protocollen up to date te houden, voor gebruikers die downloaden is het van belang dat ze hun browsers en os up to date houden en probeer het bij https sites te houden.

#### Password attack

Er zijn programma’s die gemaakt zijn om wachtwoorden te kraken. Als iemand zich kan authenticeren terwijl zij helemaal niet die persoon is kan dit heel veel schade opleveren.  
  
Algemene preventie is om werknemers het belang van wachtwoord wijzigen laten inzien. En logs bijhouden van waar mensen inloggen en zodra dit niet het geval is hier een melding over geven.

#### SQL injection attack

SQL-injectie aanvallen zijn veel voorkomend binnen database georiënteerde websites en applicaties. De aanval maakt gebruik van onbeveiligde invulvelden die code niet wegfilteren uit de velden, hierdoor is het mogelijk voor een aanvaller om deze code uit te voeren in de database. Hierdoor wordt er veel mogelijk voor de aanvaller, hij kan bijvoorbeeld data ophalen vanuit de database maar data kan ook worden aangepast, toegevoegd of zelfs worden verwijderd.

De impact van een aanval zoals dit kan enorm zijn, aangezien het een enorm datalek kan zijn maar het kan er ook voor zorgen dat de applicatie onbruikbaar wordt gemaakt voor bepaalde tijd in het geval van het verwijderen van benodigde data.

Er zijn verschillende manieren om bescherming te creëren tegen SQL een paar voorbeelden hiervan zijn:

* Role based access naar de Database
* Filteren van data die ingevoerd kan worden door de gebruiker (parameterized queries)
* Maak gebruik van stored procedures binnen de Database.
* Creëer een white list van valide data die kan worden ingevoerd.

#### Cross-site scripting (XSS) attack

**“Cross-site scripting** (**XSS**) is de naam van een fout in de beveiliging van een [webapplicatie](https://nl.wikipedia.org/wiki/Webapplicatie). Het probleem wordt veroorzaakt doordat de invoer die de webapplicatie ontvangt (zoals [cookie](https://nl.wikipedia.org/wiki/Cookie_(internet)), [url](https://nl.wikipedia.org/wiki/Url), request parameters) niet juist wordt verwerkt en hierdoor in de uitvoer terechtkomt naar de eindgebruiker. Via deze bug in de website kan er kwaadaardige code ([JavaScript](https://nl.wikipedia.org/wiki/JavaScript), [VBScript](https://nl.wikipedia.org/wiki/VBScript), [ActiveX](https://nl.wikipedia.org/wiki/ActiveX), [HTML](https://nl.wikipedia.org/wiki/HTML), [Flash](https://nl.wikipedia.org/wiki/Adobe_Flash) etc.) geïnjecteerd worden. Hiermee kunnen onder meer sessiecookies worden bekeken, sessie van een gebruiker worden overgenomen, functionaliteit van een website worden verrijkt of onbedoelde acties voor een gebruiker worden uitgevoerd.” [[Wikipedia](https://nl.wikipedia.org/wiki/Cross-site_scripting)]

Om XSS aanvallen tegen te gaan zijn er een aantal stappen die ondernomen kunnen worden:

* Gegevens ingestuurd door gebruikers “schoonmaken”, valideren dat data bruikbaar is en valide.
* Speciale karakters zoals ?, /, < etc. niet toestaan, of encoderen naar plain-tekst.

#### Eavesdropping attack

Tijdens een afluister aanval wordt netwerkdata onderschept door de aanvaller. Er zijn twee verschillende afluister aanvallen:

Passief afluisteren: Een aanvaller onderschept netwerkverkeer en haalt informatie uit de netwerkdata.

Actief afluisteren: Een aanvaller vermomt zich als een gebruiker of service en stuurt queries of aanvragen naar applicaties of services om zo informatie hieruit te halen.

Het passief afluisteren is veel meer voorkomend dan actief afluisteren aangezien er voor het actieve afluisteren een vergaande kennis van het netwerk nodig is.

Een manier om dit tegen te gaan is door data te encrypten voordat het over het netwerk verstuurd wordt, hierdoor wordt het moeilijker voor een aanvaller om bruikbare data te kunnen onderscheppen.

#### Birthday attack

Om de integriteit van een bericht te kunnen verifiëren wordt er vaak gebruik gemaakt van een unieke hash. Deze hash identificeert het bericht vervolgens als uniek en geverifieerd. Bij een birthday attack probeert een aanvaller deze hash na te maken. Hierdoor denkt het systeem dat het bericht klopt en van een geverifieerde bron komt. De kans dat dit lukt is natuurlijk enorm klein vandaar ook de naam van de aanval birthday attack.

Een mogelijke preventie techniek die toegepast kan worden is het verbeteren van de has van deze verificatie functie. Hoe langer en moeilijker de hash is, hoe kleiner de kans is dat een aanvaller deze has succesvol kan repliceren.

#### Malware attack

Malware of kwaadaardige software is een veelvoorkomend probleem op zowel netwerken als computersystemen in het algemeen. Door middel van het gebruik van malware kunnen aanvallers enorm veel mogelijkheden voor zichzelf creeren. Denk hierbij aan bijvoorbeeld toegang tot een netwerk, het uitlezen van gebruikersgegevens, het onderscheppen van inloggegevens, het gijzelen van systemen en nog enorm veel andere dingen.

Een paar bekende voorbeelden van malware zijn:

* Trojans
* Worms
* Ransomware
* Droppers
* Polymorphic viruses
* Adware
* Spyware

Preventieve stappen die genomen kunnen worden om de infectie van malware tegen te gaan zijn:

* Antivirus software
* Firewalls
* Houd alle systemen op het netwerk up to date
* Gebruik sterke wachtwoorden
* Geef gebruikers onderwijs over het gebruik van netwerk en de mogelijke gevaren.

# Security by Design

Het principe van aan security denken tijdens het developen van een application. Het is relevant voor IoT om dit principe toe te passen.

## Wat zijn barrières voor effectieve IoT beveiliging

Als je de barrières inziet kan je ook bedenken wat je hiertegen kan doen en wat voor streven je hiervoor kan aanhouden.

### Apparatuur Levensduur

Oudere apparatuur wordt langzaam en onveilig, het kan zijn dat het apparaat niet meer ondersteund wordt of dat het niet meer compatibel is met moderne beveiligingsmaatregelingen. Je bent dan genoodzaakt om deze apparaten te vervangen, en dat gebeurt vaak. Denk maar aan de levensduur van een laptop of zelfs een telefoon, hiervoor is het niet vreemd om deze elke 2 jaar te vervangen met een nieuwer model. Dit nieuwe model geniet dan weer van alle nieuwe beveiligingsmaatregelen en software.

In het geval van IoT is de duratie van de levensduur van apparaten over het algemeen net iets anders. Veel IoT apparaten zijn ergens geplaatst om er voor een langere tijd gebruik van te kunnen maken. Het kan dan zijn dat organisaties niet de benodigde stappen ondernemen om ervoor te zorgen dat deze apparaten up to date blijven, en ook worden ze vaak niet snel genoeg vervangen. Hierdoor kunnen er mogelijk beveiligingslekken ontstaan via deze onveilige verouderde IoT apparaten die binnen het netwerk geplaatst zijn.

### Kwetsbaarheids management

Voor traditionele apparaten beschikken de meeste organisaties over vaste processen om besturingssystemen en applicaties regelmatig bij te werken.

IoT-producten vallen niet onder dergelijke normen, wat ertoe leidt dat kwetsbaarheden lange tijd - of zelfs voor altijd - onontdekt en niet-gepatcht blijven.

Als zij het streven hebben om hier wel aan te werken.

### Beveiligingsmaatregelingen

De meeste IoT implementaties missen nog de benodigde beveiligingsmaatregelen die horen bij internetveiligheid. De meeste producten van IoT werden nog niet in combinatie met internet gebruikt en dus zijn er nooit over deze veiligheidsrisico's nagedacht.

Daarnaast kan er ook door gebrek aan kennis of zelfs door gemakzucht niet een toereikend niveau van beveiliging op IoT devices. Het is belangrijk voor organisaties om ervoor te zorgen dat er op deze apparaten een voldoende beveiliging is ingesteld zodat hier geen veiligheidslekken in kunnen ontstaan.