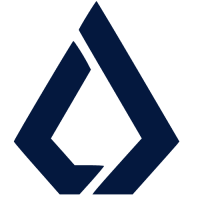
Case study: Security

Seven step approach



Project: Lisk Delegates

Project team: BBB-BC

Team: Joeri Berman (2834499)

Luc Urlings (3071081)

Stijn Baltessen (3064565)

Wouter Vandenboorn (3099571)

Floris Feddema (3188256)

Davy de Haas (3099695)

Opdrachtgever: Study case, Bartosz

Versie: 0.1

Versie datum: 3 april 2020

Status: Concept

# Document revisies

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Wijzigen** | **Auteur** | **Datum** |
| 0.1 | Opzet Document | Stijn Baltessen | 03-04-2020 |

# Inhoudsopgave

[**Document revisies**](#_bu2l4jqkimrr) **2**

[**Inhoudsopgave**](#_5pg2mng0n2po) **3**

[**Introductie**](#_8anxnj4hrgfu) **4**

[**Beschrijving case**](#_sdkb7p1qxmgj) **5**

[**Seven step approach**](#_djfvx4apkl6h) **6**

[**Discussie met de groep**](#_y9a4y0h6wipy) **7**

[**Identificeer de vragen**](#_49pivsptx4th) **8**

[**Brainstorm**](#_z6hvd6w1uz8j) **9**

[**Analyseer en structureer**](#_xew0oaz6sqtn) **9**

[**Formuleer leerdoelen**](#_35z77npcvh3l) **11**

[**Individuele studie**](#_10a2mcppftd0) **12**

[**Conclusie**](#_a5160cf0bvz2) **13**

[**Literatuurlijst**](#_y4hx91mbmk6z) **14**

# Introductie

Om de study case messaging op te lossen gaan we de seven step approach toepassen, in dit document zal elke stap worden uitgelegd. Uiteindelijke conclusie wordt op het einde opgeschreven.

Eerst wordt de study case uitgelegd en hierna de zeven stappen die genomen worden.

# Beschrijving case

Analyseer een van de 3 projecten smart power grid, predictive maintenance of manufacturing machines and IoT sensors for health centers.

Kijk hier naar de kwetsbaarheden en de best practices om security breaches te voorkomen.

Hoe kan je een aanval van TnTmix inzien zodra hij komt op het intranet van het bedrijf?

# Seven step approach

Hier staan de zeven stappen van de [seven step approach](https://portal.fhict.nl/Studentenplein/LMC/1920vj/Software%20engineering/Afstudeerfase/EnterpriseSoftware/CaseStudies/SevenStepsApproach.docx) methode die bij problem based learning voorkomt.

1. Discuss the case

2. Identificeer de vragen

3. brainstorm over potentiële bekende oplossingen

4. analyseer resultaat van brainstorm sessie

5. formulate learning objectives, wat moet er nog geleerd worden

6. individuele study om de kennis van 5 te krijgen

7. Discussieer de bevindingen van 6 hoe dit 5 en 2 beantwoord.

# Discussie met de groep

Hier wordt gediscussieerd wat de case study van ons vraag en of iedereen de opdracht snapt

We gaan bij het project IoT, bekijken wat hier de vulnerabilities van zijn. Hoe je TnTmix zou kunnen detecteren zodra hij op het bedrijfsnetwerk zit.

En wat de best practices zijn die je kan toepassen bij het uitvinden van IoT sensors.

# Identificeer de vragen

We hebben nu de probleemstelling, we gaan nu in dit hoofdstuk kijken welke vragen hierbij komen om het probleem op te lossen.

Per vraag zullen we onderbouwen waarom wij denken dat dit van belang is voor het oplossen van het probleem.

## Wat zijn de grootste security issues bij IoT?

Health centers gebruiken IoT sensoren, deze sensoren zijn verantwoordelijk voor vitale processen. Het is belangrijk om alle security issues te identificeren zodat je iemand met malicious intent voor kan zijn.

## Hoe identificeer je iemand die ongeautoriseerd toegang heeft op je netwerk (intranet)? Wat zijn de best practices hiervoor?

Security breaches tegen te gaan. In de tekst staat dat dit een van de dingen is waar Jack van de Aa tegenaan liep.

## Wat zijn de beste practices voor security for IoT?

Om bij het implementeren van deze sensoren de best practices toepast kan je al heel veel vulnerabilities voorkomen.

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

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

## Wat zijn veilige manieren om gevoelige data op te slaan?

# Brainstorm

Hier bespreken we wat de groep al weet en identificeren we de mogelijke oplossingen. Per mogelijke oplossing zeggen we ook waarom we denken dat een mogelijke oplossing is.

* Geen voorkennis van IoT, wel een grote IoT risk is dat het fysiek makkelijk te bereiken is. IoT is vaak een probleem omdat niet veel beleid is richting security tijdens het maken van het product.
* Netwerk Intrusion Detection System (NIDS) zoals SNORT. Honeypots. Netwerk verdelen in groepen (dmz groepen) zodat groepen alleen bij dingen kunnen waar de groep voor geautoriseerd is. Role based access.
* OWASP.
* Backups, snapshots, lokale backups, off-site backups, sandboxing.
* Secure verbinding. Devices updaten. Wachtwoorden niet op een plek zetten, op een veilige plek neerzetten. Betaalde password manager.
* anonimisering waar het kan, zo min mogelijk gevoelige data opslaan.

Analyseer en structureer

Binnen de groep is een kleine hoeveelheid kennis over dit onderwerp. Zo weten we nu dat IoT apparaten extra kwetsbaar zijn voor aanvallen. Dit komt omdat deze niet consequent geupdate worden en security geen hoge prioriteit is voor developers.

Een aantal manieren om ongeautoriseerde gebruikers binnen je netwerk te identificeren zijn:

* Het gebruik van honeypots
* Het gebruik van sniffers
* Role based access

In het geval van software zijn er een aantal regels waaraan de software developer moet voldoen om te garanderen dat de software veilig is. Denk aan:

* OWASP Top 10
* Data anonimiseren

Best practices voor veiligheid (binnen IoT):

* Lokale en niet lokale backups
* Snapshot
* Sandboxing
* Secure verbinding
* Software updaten
* Wachtwoorden niet op een plek zetten, op een veilige plek neerzetten.
* Betaalde password manager.

# Formuleer leerdoelen

Aan het einde van deze study case heeft de student veel kennis opgedaan, met deze kennis beheerst hij de volgende leerdoelen:

* De student weet wat IoT is.
* De student weet wat veilige manieren zijn om gevoelige data op te slaan.
* De student weet wat de best practises zijn voor security bij IoT devices.
* De student weet waar op gelet moet op het gebied van security bij het maken van een systeem.
* De student weet hoe hij iemand die ongeautoriseerde toegang heeft tot het netwerk kan detecteren.
* De student weet hoe je de impact van een hack op een health centre kan minimaliseren.
* De student weet wat de security by design principes zijn en hoe deze moeten worden toegepast.
* De student kan de gebreken in beveiliging van IoT devices identificeren.

# Individuele studie

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?

Wouter en Stijn.

Hoe identificeer je iemand die ongeautoriseerd toegang heeft op je netwerk (intranet)? Wat zijn de best practices hiervoor?

Wat zijn veilige manieren om gevoelige data op te slaan?

Floris en Luc.

Wat zijn de grootste security issues bij IoT?

Wat zijn de beste practices voor security for IoT?

Davy en Joeri.

## Hoe identificeer je iemand die ongeautoriseerd toegang heeft op je netwerk (intranet)?

Om erachter te komen of iemand ongeautoriseerd toegang heeft gekregen op het netwerk zijn er meerdere opties mogelijk.

* Er kunnen logs worden gemaakt die achteraf in te zien zijn
* Door middel van network monitoring kan er gekeken worden of gebruikers een abnormale hoeveelheid data versturen over het netwerk.
* Het gebruik van een intrusion prevention system.

Ook is het belangrijk om van te voren al zo veel mogelijk te doen om ongeautoriseerde toegang tegen te gaan. Hiervoor kunnen de volgende technieken ingezet worden.

* Er kunnen filters opgezet worden voor geolocatie of ip adressen.
* Er kunnen extra authenticatie lagen op het netwerk worden gezet
* Het gebruik van een intrusion detection system
* Een sandbox omgeving opzetten zodat mogelijke aanvallers hierin terecht komen.
* Verplicht technieken zoals 2 factor authenticatie inzetten
* Gevoelige informatie alleen over een VPN beschikbaar maken

Een intrusion detection system of een intrusion prevention system bestaan in twee verschillende vormen.

* Network intrustion detection system, dit analyseerd inkomend netwerk verkeer
* Host-Based intrusion detection system, houdt belangrijke bestanden op het systeem in de gaten.

### Wat zijn de best practices hiervoor?

1. Nooit standaard wachtwoorden houden als “password”, “root” of “admin”, dit zijn de eerste dingen die geprobeerd worden
2. Maak gebruik van en firewall, afhankelijk van de use case moet er gebruik gemaakt worden van een soft- / hardware firewall
3. Gebruik maken van TLS beveiligde verbindingen
4. Gebruik maken van een VPN voor bedrijfsnetwerken
5. Netwerken afschermen door middel van subnetwerken
6. Regelmatig al je software updaten
7. Gebruik maken van een password manager
8. Wachtwoorden niet herhaaldelijk gebruiken
9. 2-Factor Authentication gebruiken
10. Gebruik maken van virus scanners
11. Nooit links openen die in spam-mails staan
12. DMARC record opzetten
13. Gebruik maken van een geavanceerde browser als Google Chrome, Mozilla Firefox of Edge
14. IP Whitelisting, is dat alleen vooraf ingestelde IP adressen toegang krijgen tot het netwerk of gevoelige data
15. Rollen structuur opzetten binnen de organisatie. Gebruikers krijgen alleen toegang tot data waar ze bij mogen komen
16. Single Sign-On, hierbij worden alle rechten en mogelijkheden gelinkt aan 1 account
17. Monitoring van netwerken
18. Regelmatig een derde partij inhuren om de beveiliging te controleren.
19. Regelmatig je systeem backuppen op zowel online als offline backups
20. Maak gebruik van disk encryption

Ons leek het een leuk idee om voor iedereen binnen onze groep te noteren hoe zij voldoen aan het bovengenoemde lijstje. Daarom hebben we een matrix gemaakt en geven we alles een punt. 1 is het best, 2 is dat het deels gebruikt wordt en bij 3 wordt het niet toegepast.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Stijn | Davy | Joeri | Wouter | Floris | Luc |
| 1. | 2 | 1 | 1 | 2 | 1 | 1 |
| 2. | 2 | 2 | 1 | 3 | 2 | 3 |
| 3. | 1 | 1 | 2 | 2 | 1 | 2 |
| 4. | 3 | 2 | 2 | 3 | 2 | 3 |
| 5. | 3 | 3 | 3 | 3 | 3 | 3 |
| 6. | 2 | 1 | 1 | 2 | 1 | 1 |
| 7. | 2 | 1 | 1 | 2 | 1 | 1 |
| 8. | 2 | 1 | 2 | 2 | 1 | 2 |
| 9. | 2 | 1 | 2 | 1 | 2 | 2 |
| 10. | 3 | 1 | 1 | 3 | 1 | 3 |
| 11. | 1 | 1 | 1 | 1 | 1 | 1 |
| 12. | 1 | 1 | 1 | 1 | 1 | 1 |
| 13. | 1 | 1 | 1 | 1 | 1 | 1 |
| 14. | 3 | 2 | 2 | 3 | 2 | 3 |
| 15. | 2 | 1 | 1 | 1 | 1 | 1 |
| 16. | 1 | 1 | 1 | 1 | 1 | 1 |
| 17. | 3 | 3 | 3 | 3 | 3 | 3 |
| 18. | 3 | 3 | 3 | 3 | 3 | 3 |
| 19. | 3 | 1 | 1 | 3 | 1 | 2 |
| 20. | 3 | 1 | 3 | 3 | 1 | 3 |
| **Totaal** | 43 | 29 | 34 | 43 | 30 | 40 |
| ***AVG*** | 2.15 | 1.45 | 1.95 | 2.15 | 1.50 | 2.00 |

## Wat zijn veilige manieren om gevoelige data op te slaan?

Om gevoelige data op een veilige manier op te kunnen slaan zullen er met een aantal dingen rekening moeten worden gehouden.

* Wie/wat moet er toegang hebben tot de data
* Waar is deze data opgeslagen
* Welke data is echt nodig om op te slaan
* Welke data kan anoniem gemaakt worden
* Welke data moet gehashed worden
* Zijn de gebruikte technologieën veilig en up to date

Verder is ook belangrijk dat de data op een goede manier bij de opslaglocatie komt en er goed vanaf kan worden gehaald. Hierbij zijn de volgende punten heel belangrijk om rekening mee te houden:

* TLS beveiligde verbinding gebruiken (client to service en service to service)
* IP whitelisting voor data access
* Configuratiebestanden veilig opslaan in de CI/CD omgeving
* Data access service alleen open voor de services die het gebruiken
* Role based access zodat er alleen toegang is tot de data die nodig is
* Extreem gevoelige data mogelijk in een aparte data store met alleen referenties ernaar in de originele datastore
* De informatie flow goed in beeld brengen en mogelijke kwetsbaarheden signaleren
* Regelmatig security assessments doen (mogelijk ook door derden)
* Monitoring van de data infrastructuur

## Wat zijn de grootste security issues bij IoT?

### Insufficient Testing

De ontwikkelaars van IoT devices zijn meer gefocust op de snelheid van het leveren van nieuwe producten dan het beveiligen ervan. Veel IoT apparaten zijn daarom amper getest op kwetsbaarheden van de software en dit maakt het heel erg gemakkelijk om binnen te dringen in deze apparaten.

### Weak Passwords

Heel veel apparaten worden verstuurd met een standaard wachtwoord zonder enige instructie voor de gebruiker om dit wachtwoord zo snel mogelijk aan te passen. Hierdoor is het met behulp van DDoS aanvallen erg makkelijk om binnen te dringen in de apparaten. Het Mirai botnet is een van de beste voorbeelden die gebruikmaakt van deze kwetsbaarheden.

### IoT botnets

Een botnet zijn een aantal apparaten die zijn geïnfecteerd met malware en zijn onder de controle van een kwaadaardige actor. Elk apparaat wordt een bot genoemd en kan worden gebruikt voor allerhande dingen, zoals spamming, ransomware, DDoS attacks etc.

Er wordt vaak gebruikgemaakt van IoT apparaten omdat deze een slechte beveiliging hebben waardoor het installeren van malware gemakkelijker gedaan kan worden.

Veel botnets zorgen ervoor dat ze niet gedetecteerd worden door stiekem in de achtergrond te draaien zonder dat de gebruiker dit doorheeft en maar hele kleine aanvallen uitoefent op IoT apparaten. Dit zorgt ervoor dat er veel micro-breaches opkomen die allemaal een klein stukje data uitlekken in plaats van heel veel data tegelijk.

Enkele voorbeelden van tegenwoordig opgerolde botnets zijn Mirai (2016) en The Reaper (2017)

### Hijacked devices

Veel IoT devices hebben slechte of zelfs geen security wat het hacken van zo’n apparaat vrij gemakkelijk maakt. Omdat deze apparaten vaak verbonden zijn met een netwerk waar ook andere apparaten op aangesloten zijn is is de stap naar het hacken van andere apparaten op een netwerk zo gemaakt. Vaak gebeurd dit bij apparaten waarvan mensen zelf het niet eens van zouden verwachten zoals smart tv’s, printers of smart hubs.

### Lack of Updates

Veel van de IoT apparaten krijgen geen updates. Omdat de meeste apparaten vrij simpel en goedkoop zijn worden deze niet meegeleverd met de mogelijkheid om updates te krijgen. Of wanneer deze apparaten het wel hebben wordt dat veelal niet gedaan door de gebruikers. Dit kan leiden tot grote security issues binnen je netwerk.

Het gebeurd ook wel meer dan eens dat de fabrikanten maar voor korte duur firmware updates of security updates blijven uitbrengen.

### Onveilige communicatie

Beveiligde communicatie worden gedaan door de berichten te encrypten. Veel IoT apparaten doen dit niet. Dit zorgt ervoor dat andere apparaten de communicatie kunnen uitlezen. Vaak gebeurd dit zonder dat de gebruiker hier erg in heeft.

## Wat zijn de beste practices voor security for IoT?

### Beheren van apparaten in een netwerk

Het volgen en beheren van apparaten binnen je netwerk is belangrijk zodat je kunt weten welke apparaten zijn aangemeld en of dit van een vertrouwelijk iemand komt. Als dit niet het geval is kan dit meteen worden gezien en kunnen er passelijke maatregelen hiertegen worden getroffen.

### Apparaten afschermen

Door IoT apparaten op een eigen of een beschermd deel van een netwerk te laten draaien wordt er voorkomen dat andere apparaten toegang hebben tot (de communicatie van) deze apparaten.

### Updaten van IoT software

Het is belangrijk dat de IoT software zo snel mogelijk wordt geupdate waar mogelijk. Deze updates kunnen namelijk belangrijke beveiligingsupdates bevatten die essentieel zijn.

### Penetration Testing

Het uitoefenen van pen testen kan erg goed van toepassing komen om te zien of er zwakheden zijn in het systeem die beter nu kunnen worden gevonden dan iemand anders met een kwaadwillige gedachte. Door deze tests kun je meer zekerheid krijgen in de beveiliging binnen het apparaat.

### Strong Passwords

Zorg ervoor dat er nooit een standaard wachtwoord wordt gebruikt op een apparaat.

Hoe langer en complexer de wachtwoorden zijn, hoe moeilijker het wordt om deze met brute force te achterhalen.

Gebruik ook verschillende wachtwoorden voor elke applicatie zodat als er een wachtwoord is achterhaald deze niet kan worden gebruikt om binnen te dringen bij andere applicaties.

Het regelmatig veranderen van wachtwoord minimaliseer je de toegang tot de applicatie die dit wachtwoord gebruikt.

### Apparaten met security features kopen

De goedkopere kant van IoT apparaten hebben vaak geen of slechte beveiliging. Door daarop te letten bij de aankoop en te kiezen voor een iets duurder apparaat die wel goed beveiligd en getest is.

## 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 cyberaanvallen 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.

#### 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 hiertegen zijn:

* Server achter Firewall zetten
* Vergroot the grote van the connection queue en verminder the timeout tijd van open connecties.
* bepaalde poorten blokkeren
* 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 daarna 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 binnen 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-injection 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 creëren. 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.

# Conclusie

Voor IoT is er nog veel ontwikkeling nodig om het secure te maken. Er zijn wel veel punten waar de maker en de gebruiker op kan letten om risico te verkleinen.

## Doelstellingen

Hieronder nogmaals de doelstellingen van de case study op een rijtje:

* We gaan bij het project IoT, bekijken wat hier de vulnerabilities van zijn.
* Hoe je TnTmix zou kunnen detecteren zodra hij op het bedrijfsnetwerk zit.
* En wat de best practices zijn die je kan toepassen bij het maken van IoT sensors.

Deze punten zijn behandeld door de individuele studie. hierna is dit besproken waardoor iedereen ook deze kennis heeft opgedaan.

## Leerdoelen

Hieronder nogmaals de leerdoelen:

* *De student weet wat IoT is.*
* *De student weet wat veilige manieren zijn om gevoelige data op te slaan.*
* *De student weet wat de best practises zijn voor security bij IoT devices.*
* *De student weet waar op gelet moet op het gebied van security bij het maken van een systeem.*
* *De student weet hoe hij iemand die ongeautoriseerde toegang heeft tot het netwerk kan detecteren.*
* *De student weet hoe je de impact van een hack op een health centre kan minimaliseren.*
* *De student weet wat de security by design principes zijn en hoe deze moeten worden toegepast.*
* *De student kan de gebreken in beveiliging van IoT devices identificeren.*

Leerdoelen zijn behaald.

# 

# Literatuurlijst

<https://bitsensor.io/>

<https://www.snort.org/>