CIP Whitepaper IoT

Een samenleving kan zich geen Internet of Things veroorloven zonder aandacht voor integrale beveiliging. De risico's voor de privacy van burgers, de bedrijfs-voering en onze economie zijn daarvoor te groot.

Amsterdam, 6 november 2018

Auteurs:

Marcel Koers (CIP), in samenwerking met de CIP IoT-werkgroep:
Ben van Lier, Centric; Bram Havers, IBM; Henk Schepers, Philips;
Jan Buis, LANCOM Systems; Jan van der Sluis, DXC; Jelle Attema, ECP;
Meine van Essen, RWS; Roman Volf, Min. EZK.

Opdrachtgever:
CIP

Versie:
1.0

Status:
Becommentarieerde Praktijk

Amsterdam, 6 november 2018

Inhoud

Managementsamenvatting

Tot voor kort gebruikten we het internet als een communicatiekanaal en transportmiddel voor het verplaatsen of delen van informatie. Relatief sporadisch werden daarmee ook apparaten op afstand bestuurd, door de stuurcommando's via internet door te geven en te laten omzetten in de bedoelde activiteit. De communicatie ging van mens naar mens of van mens naar machine of apparaat: het was een Internet van Mensen.

Dat is niet meer zo. Slimme software heeft inmiddels heel veel menselijk denkwerk vervat in algoritmes die idealiter doen wat mensen ook zouden doen in gegeven situaties. Ze doen dat consequenter en sneller, en autonoom: de mens hoeft zich er niet meer om te bekommeren. De mens kán zich er soms niet eens meer mee bemoeien, denk aan de wereld van de financiële transacties, waar microseconden het verschil kunnen maken tussen winst of verlies.

Steeds meer apparaten ('dingen') worden voorzien van autonoom werkende software, van oceaanschepen tot pacemakers. Het is 'automatisering' in de letterlijke zin van het woord. Een nieuwe dimensie is nu dat deze apparaten onderling gaan communiceren. Consequenter, sneller en ook autonoom. Denk aan zelfrijdende auto's die elkaar 'zien' en botsingen voorkomen. Het aantal met elkaar verbonden dingen neemt explosief en exponentieel toe: dit is het Internet van Dingen (Internet of Things - IoT).

Als binnen afzienbare tijd heel veel 'dingen' met elkaar in verbinding zullen staan en zelf beslissingen nemen voordat de mens kan ingrijpen, dan komen veel beslissingen over maatschappelijk relevante of zelfs kritische activiteiten en handelingen feitelijk te liggen bij de ontwerpers van de algoritmes en van de massa's apparaten en apparaatjes die door enorme aantallen leveranciers over de wereld worden verspreid. Wie zich nu zorgen maakt over de bescherming van zijn persoonlijke gegevens, e-mailtjes en appjes, of de kritische bedrijfsdata, moet zich realiseren dat het aankomende scenario beveiligingsrisico's van een compleet andere dimensie met zich meebrengt. Dit is precies de aanleiding voor dit document.

Veel van de kwetsbaarheden in de wereld van IoT kunnen worden beperkt door het hanteren van een op zich beperkt en overzichtelijk aantal basisprincipes, standaarden en best-practices op het gebied van informatiebeveiliging. De dagelijkse praktijk is echter dat veel producenten van IoT-apparaten deze principes en best-practices niet toepassen en veel apparaten zelfs de meest basale beveiligingsmaatregelen missen. Het is daarom absoluut noodzakelijk dat overheid en industrie snel gaan samenwerken om ervoor te zorgen dat het IoT-ecosysteem wordt gebouwd op een fundament dat betrouwbaar en veilig is. Het Europese bedrijfsleven is/wordt nauw betrokken bij deze certificering en is medeverantwoordelijk voor de productie van veilige IoT-apparaten.

Om misbruik van met het internet verbonden apparaten te voorkomen en te bestrijden, heeft EZK samen met JenV en andere publieke en private partijen een Roadmap Digitaal Veilige Hard- en Software opgesteld. Deze roadmap bevat een samenhangende set van maatregelen voor de bevordering van de digitale veiligheid van hard- en software op een gebalanceerde wijze. Het betreft preventieve maatregelen als verkenningen naar wettelijke minimumveiligheidseisen en certificering, detectiemaatregelen als digitale veiligheidstesten, en mitigerende maatregelen als inzet van het aansprakelijkheidsrecht zodat gebruikers schade kunnen verhalen.

Deze whitepaper geeft een uiteenzetting van de risico's van misbruik en een aanzet tot een set basisbeginselen en mitigerende basisprincipes voor digitaal veilige IoT. Daarnaast verschaft hij good practices voor het realiseren van een verantwoord beveiligingsniveau voor IoT-apparaten. Deze IoT handreiking sluit aan op de hierboven genoemde roadmap. De set basisbeginselen kan ook dienen als de basis voor eventuele sectorspecifieke aanvullende maatregelen en voor een proactieve opstelling in Europa.

Dit document biedt een aanpak om de risico's door misbruik van IoT-apparaten en zelfs van een heel IoT-ecosysteem te mitigeren. De aanpak wordt gebaseerd op zes mitigerende basisprincipes en aanbevolen best-practices die kunnen worden gebruikt voor het realiseren van een verantwoord beveiligingsniveau voor IoT-apparaten en IoT-ecosysemen.

In een 5 stappenplan wordt uiteengezet hoe bereikt kan worden dat:

> *IoT zó wordt ontworpen, geproduceerd, ingezet en beheerd, dat de veiligheid wordt gemaximaliseerd en de risico's voor de bedrijfsvoering en het dagelijks leven tot een minimum worden beperkt.*

Dit document is een aanmoediging voor producenten en afnemers om gesprekken aan te gaan over de beveiliging van IoT en het ontwerpen, produceren, inkopen, inzetten en beheren in te kaderen. De beveiliging heeft tot doel dat je op de inzet van IoT kan vertrouwen in technische en juridische zin (privacy, beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid). Dat is wat je als organisatie, ondernemer of consument van een apparaat verwacht. Dat is ook wat je als ontwerper of producent moet willen aanbieden. Want vroeg of laat wordt deze kwaliteit voor de potentiele afnemers een doorslaggevend argument voor aanschaf of gebruik.

Het document is opgesteld in een samenwerking tussen deskundigen uit overheid en bedrijfsleven die het belang zien van informatieveiligheid voor de overheid, het bedrijfsleven en samenleving als geheel. Een samenleving waarin de betekenis van IoT toeneemt en de beveiliging ervan achterblijft.

Over CIP

CIP is het Centrum voor informatiebeveiliging en privacybescherming van, voor en door overheidsorganisaties. Het heeft zich ontwikkeld tot een publiek-private netwerkorganisatie, waarin ook gespecialiseerde marktorganisaties als kennispartners deelnemen.

Het centrum is opgericht voor informatie-uitwisseling en kennisdeling ter verbetering van de informatieveiligheid van de overheidsdienstverlening. Inmiddels bestaat het CIP-netwerk uit een groot aantal overheidsorganisaties en (private) kennispartners. Kennis die in deze organisaties aanwezig is op het vlak van informatiebeveiliging en privacybescherming wordt binnen de samenwerking in CIP-verband op verschillende manieren gedeeld en toegankelijk gemaakt. Het produceren van themadocumenten met zoveel mogelijk inbreng vanuit het netwerk is er één van. Aangesloten organisaties leren van elkaars oplossingen en werkwijzen en kunnen samen komen tot afspraken daaromtrent. Door meer samen doen draagt het CIP ook bij aan het optimaal gebruik van overheidsmiddelen.

1 INTRODUCTIE

De kansen die de inzet van IoT bieden kunnen niet los gezien worden van de risico's van misbruik. Daarin verschilt IoT niet van andere IT-inzet. Maar IoT heeft ook een heel eigen problematiek en risicoprofiel.

1.1 Prioriteit geven aan IoT beveiliging

De 'Things' van Internet of Things (IoT) worden steeds meer onze elektronische vingertoppen. Deze met Internet verbonden apparaten maken naadloze verbindingen mogelijk tussen mensen, netwerken en fysieke services. Ze voorzien ons van vitale informatie over de onze omgeving en ons handelen en zijn een bron van kennis om ons handelen te kunnen beïnvloeden. De stap van kennis naar kunde is dank zij Artificial Intelligence (AI) tegenwoordig een kleine stap, maar met grote gevolgen voor ons handelen en ieders positie in de maatschappij en de maatschappij zelf. De mogelijkheden die IoT biedt lijken onbeperkt en de ontwikkeling gaat razendsnel en in alle mogelijke richtingen. De beveiliging ervan houdt het tempo van innovatie niet bij. Naarmate we steeds meer netwerkverbindingen integreren in de bedrijfsvoering en ons dagelijks leven, zijn belangrijke processen die ooit handmatig werden uitgevoerd (en dus een zekere mate van immuniteit genoten tegen kwaadwillende cyberactiviteit) nu kwetsbaar geworden. Want de kansen die de inzet van IoT bieden kunnen niet los gezien worden van de risico's van misbruik door kwaadwillende actoren die informatiestromen van, naar en tussen op het netwerk aangesloten apparaten manipuleren of met apparaten zelf knoeien. Dit kan leiden tot diefstal en verlies van (bedrijfs-)gevoelige gegevens en privacy, verstoringen en onderbreking van bedrijfsvoering of vertraging van de internetfunctionaliteit als gevolg van DDoS-aanvallen via IoT devices die in grote aantallen beschikbaar zijn.

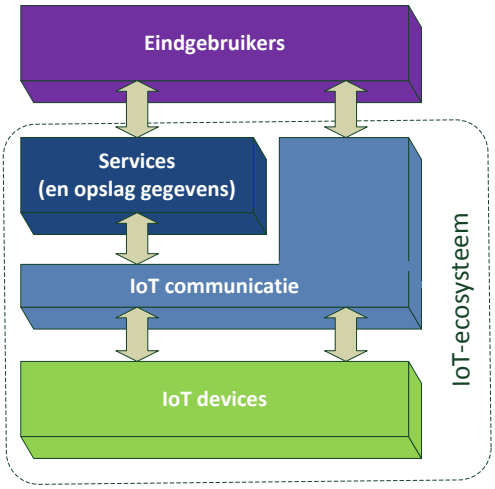
IoT heeft een heel eigen problematiek en risicoprofiel. Daarvoor zijn er twee belangrijke oorzaken:

1. IoT devices zijn verweven met de fysieke (ook letterlijk 'lijflijke') wereld. Veel meer dan informatieveiligheid is dan actieveiligheid in het geding. Dit geldt voor IoT-apparaten die de fysieke wereld beïnvloeden, denk daarbij aan pacemakers en insuline pompjes, maar ook voor de manipulatie van de intelligentie in sensoren, waardoor je bijvoorbeeld een autonome auto kunt beïnvloeden . Als binnenkort alle auto's in het verkeer met elkaar en met geleidesystemen verbonden zijn dan krijgt dat enkele risico een schrikbarende omvang.
2. IoT devices kenmerken zich door verbijsterend geringe resources als rekenkracht en powerbudget. Enigszins serieuze authenticatie- en integriteitscryptografie is dan meteen een probleem, maar ook ontbreekt vaak de (geheugen)ruimte voor een veilige softwaredownload. En dit gaat verder dan de techniek alleen: welke fabrikant kan zich de post-sales uitgaven voor beveiligingsupdates gedurende de levenscyclus van IoT-devices veroorloven?

1.2 Het IoT ecosysteem

Karakteristiek voor IoT-apparaten is dat ze zijn verbonden (onderling en met services) en toegankelijk zijn voor gebruikers (direct en via services). Deze gebruikers kunnen eindgebruikers en beheerders zijn. Het geheel van onderlinge verbondenheid vormt zich tot een systeem dat door zijn organische groei wordt aangeduid als IoT-ecosysteem.

In de praktijk zien we dat de IoT-apparaten niet alleen onder aansturing staan van de (organisaties met) eindgebruikers, maar ook aangestuurd, uitgelezen en doorgegeven kunnen worden door organisaties die de IoT-apparaten aanbieden. Denk bijvoorbeeld aan de leverancier van een 'connected' auto.
Iedere laag binnen het IoT-ecosysteem behoeft zijn eigen aandacht voor beveiliging. Zo kan de IoT communicatie beveiligd worden met gateways. Bedenk daarbij dat IoT-ecosystemen een breed scala aan verschijningsvormen kennen, die ieder om specifieke aandacht voor beveiliging vragen, zeker als de services in een 'cloud', en daardoor vaak over landsgrenzen heen worden aangeboden.



1.3 Doelstelling van deze whitepaper

Het is noodzakelijk dat overheid en industrie gaan samenwerken om ervoor te zorgen dat het IoT-ecosysteem wordt gebouwd op een fundament dat betrouwbaar en veilig is. Dit document legt de risico's van misbruik uit en biedt zicht op een aantal mitigerende basisprincipes en aanbevolen best-practices die kunnen worden gebruikt voor het realiseren van een verantwoord beveiligingsniveau voor de IoT-apparaten die bedrijven ontwerpen, produceren, inzetten en beheren. In een 5 stappenplan is beschreven hoe dit bereikt kan worden. De doelstelling van deze whitepaper is te bevorderen dat:

> *IoT zó wordt ontworpen, geproduceerd, ingezet en beheerd, dat de veiligheid wordt gemaximaliseerd en de risico's voor de bedrijfsvoering en het dagelijks leven tot een minimum worden beperkt.*

Deze whitepaper is een aanmoediging voor producenten en afnemers om gesprekken aan te gaan over de beveiliging van IoT en het ontwerpen, produceren, inkopen, inzetten en beheren in te kaderen. De beveiliging heeft tot doel dat bedrijven, overheden en burgers op de inzet van IoT kan vertrouwen in technische en juridische zin (privacy, beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid). Dat is wat organisaties, ondernemers of consumenten van een apparaat mogen verwachten.

Hoewel IoT een niet te miskennen dimensie toevoegt aan het privacyvraagstuk, kiezen we er in deze eerste versie van de whitepaper voor de basisprincipes te beperken tot die welke betrekking hebben op het autonoom opereren van (evoluerende) technologische toepassingen. 'Privacy' is een afgeleide kwaliteit, die zeker beïnvloed wordt door hoe het IoT ecosysteem en de daarin opererende devices ontworpen en toegepast worden. Maar om ook dat vraagstuk goed te kunnen doorgronden is het allereerst nodig dat er kennis komt van de technologie zelf en we grip krijgen en houden op de ontwikkelingen en innovaties die steeds meer ons leven - waaronder het aspect privacy - zullen bepalen.

1.4 De doelstelling in relatie tot de regiefunctie van de overheid

De overheid heeft, zoals die beschreven is in de Roadmap Digitaal Veilige Hard- en Software, een regiefunctie om de publieke waarde van digitale veiligheid te borgen. Vanuit die regiefunctie wordt bezien in hoeverre een set van basisbeginselen voor digitaal veilige hard- en software mogelijk en relevant is. Met deze basisbeginselen wordt een set van elementen en kenmerken bedoeld die het kabinet met publieke en private partijen wil waarborgen of uitsluiten als het gaat om digitaal veilige hard- en software.

Voor IoT biedt deze (met publieke en private partijen ontwikkelde) whitepaper basisprincipes en een aanpak om te komen tot een veilige inzet van die IoT en daarmee tot veilige IoT-ecosystemen. Dit met het doel de producten en afnemers aan te moedigen samen de veiligheid te waarborgen. Deze keuze voor een set van principes en het bieden van een aanpak kan ook dienen als de basis voor initiatieven voor sectorspecifieke aanvullende maatregelen en voor standaarden en certificeringen. Daarvoor zijn echter een grotere reikwijdte dan die van het CIP en een proactieve opstelling in Europa nodig.

1.5 Basisprincipes voor een veilige inzet van IoT

Veel van de kwetsbaarheden in IoT kunnen worden beperkt door het hanteren van basisprincipes en best-practices op het gebied van informatiebeveiliging. De dagelijkse praktijk is dat veel IoT-apparaten deze principes en best-practices niet toepassen en daardoor basale beveiligingsmaatregelen ontberen.

Er zijn echter veel factoren die bijdragen aan de beveiligingsproblemen. Het opstellen van beveiligingsmaatregelen op basis van (uitgebreide) security frameworks leidt tot lange lijsten van eisen met een in de tijd voortdurend evoluerende inhoud. Door te kiezen voor *basis*principes en best-practices blijft de omvang beperkt en worden de betrokkenen gewezen op het adequaat beveiligen en veilig houden tijdens alle fasen in de levenscyclus van de IoT-apparaten.

De volgende IoT-basisprincipes bieden samen met de daarbij behorende best-practices een gerichte focus op de beveiliging en het verbeteren van het vertrouwen dat aan het IoT-ecosysteem ten grondslag moet liggen:

Principe 1. Erkende methoden en technieken
Erkende en bewezen methoden en technieken voor ICT-beveiliging zijn benut voor de aanpak van risicomanagement en het nemen van de benodigde beveiligingsmaatregelen.

Principe 2. Risicoanalyses en het prioriteren van beveiligingsmaatregelen
Risicoanalyses zijn uitgevoerd, zodat de beveiligingsmaatregelen zijn geprioriteerd op basis van de gevolgen van de risico's op de werking van het IoT-ecosysteem en de bedrijfsvoering.

Principe 3. Security by Design en Security by Default
De beveiliging is integraal meegenomen in het ontwerp (Security by Design), waarna de noodzakelijke beveiligingsinstellingen standaard zijn geactiveerd (Security by Default).

Principe 4. Beveiligingsupdates en -patches
IoT-apparaten zijn up-to-date door het uitvoeren van beveiligingsupdates. Voor kwetsbaarheden zijn of worden patches uitgevoerd. Het IoT-apparaat is zo ontworpen dat dit (tijdens de vooraf gegarandeerde levensduur van het IoT-apparaat) geautomatiseerd en veilig gebeurt.

Principe 5. Bronnen en totstandkoming van de IoT-onderdelen en het IoT-ecosysteem
De voortbrengingsketen en de bronnen van het IoT-apparaat en het IoT-ecosysteem zijn bekend. Daar waar dit niet bekend is zijn passende beveiligingsmaatregelen getroffen of andere keuzes ter bescherming gemaakt.

Principe 6. Veilige netwerkconnectiviteit
Alleen die netwerkconnectiviteit, die noodzakelijk is voor het correct functioneren van het IoT-apparaat en het IoT-ecosysteem, is beschikbaar voor het IoT-apparaat. Deze connectiviteit is beveiligd.

1.6 Aanpak voor een veilige inzet van IoT

Het niet hanteren van de zes IoT-basisprincipes kan een significante impact hebben op de beveiliging van de IoT-apparaten en het IoT-ecosysteem. Om wel tot een veilige inzet van IoT in een gegeven context te komen kunnen (moeten), gebruikmakend van deze zes basisprincipes, de volgende vijf stappen worden doorlopen:

Stap 1. Organiseer
Benut de kennis in een multidisciplinaire aanpak, zodat iedereen betrokken is.

Stap 2. Inventariseer
Breng het ecosysteem van kansen en risico's in kaart, zodat iedereen daarmee bekend is.

Stap 3. Analiseer
Analiseer de beveiligingsrisico's van het ecosysteem, zodat iedereen zich van de risico's bewust is.

Stap 4. Beveilig
Voer standaard beveiligingsmaatregelen door in de delen van het ecosysteem, zodat deze beveiligd zijn.

Stap 5. Scherm af
Implementeer compenserende maatregelen voor de resterende zwakke plekken binnen het ecosysteem, zodat deze beschermd zijn in het IoT-ecosysteem.

1.7 Doelgroep van deze whitepaper

Het is een uitdaging om te bepalen wie verantwoordelijk is voor beslissingen over het realiseren van beveiligingseisen. Het zijn immers vaak verschillende bedrijven die een apparaat en bijbehorend operating systeem ontwerpen, samenstellen met onderdelen van soms dagelijks wisselende toeleveranciers, de software voor (delen van) het apparaat ontwikkelen, het netwerk ontwerpen, het apparaat inbedden in de informatievoorziening, gebruiken en beheren. Deze uitdaging wordt nog eens versterkt door een gebrek aan alomvattende, algemeen geaccepteerde internationale normen en standaarden voor IoT-beveiliging en de explosie van IoT apparaten.

Voor het toepassen van de principes is het van belang dat de betrokken partijen rekenschap afleggen over de veiligheid bij het ontwikkelen, produceren, implementeren of gebruiken van op het netwerk aangesloten apparaten. Concreet is deze whitepaper geschreven voor:

- IoT-ontwikkelaars: zij moeten rekening houden met beveiliging wanneer een apparaat, sensor, service of een onderdeel van het IoT wordt ontworpen en ontwikkeld;
- IoT-fabrikanten: zij moeten de beveiliging verbeteren van de IoT-apparaten die worden ingezet door organisaties en consumenten;
- Serviceproviders, die via IoT-apparaten services implementeren en aanbieden: zij moeten de beveiliging van de functies van de IoT-apparaten daarin meenemen, evenals de onderliggende beveiliging van de infrastructuur die deze services mogelijk maakt;
- Professionele gebruikers van IoT, zoals bedrijven en overheden, en specifiek CISO's en security-officers: zij moeten kunnen sturen op het nemen en laten nemen van beveiligingsmaatregelen voor een veilige inzet van IoT-apparaten;
- Overheid, bedrijven en consumentenorganisaties: zij moeten ondersteund worden bij het bieden van een coherente aanpak voor het beveiligen en veilig houden van IoT tijdens de gehele levenscyclus van het IoT-apparaat en het IoT-ecosysteem.

1.8 Ontstaan van dit document

Deze CIP IoT whitepaper is een product van de CIP-werkgroep IoT en is tot stand gekomen in een samenwerking tussen deskundigen uit overheid en bedrijfsleven die het belang zien van informatieveiligheid voor de overheid, het bedrijfsleven en samenleving als geheel. Een samenleving waarin de betekenis van IoT toeneemt en de beveiliging ervan lijkt achter te blijven. Een samenleving kan zich echter geen IoT-apparaten veroorloven die met onvoldoende aandacht voor veiligheid worden ingezet. De risico's voor de privacy van burgers, de bedrijfsvoering en onze economie zijn daarvoor te groot.

De werkgroep IoT heeft tot doel kennisdeling en krachtenbundeling een bijdrage tot stand te brengen aan een veiligere inzet van IoT-apparaten. De werkgroep hanteert daarbij het principe 'vóór allen, dóór allen', waarbij de samenwerking op 'Agile' wijze is ingericht, gericht op het bieden van toegevoegde waarde, waarbij de waarde creatie ontstaat door inbreng van ieder van de leden van de multidisciplinaire publiek-private werkgroep.

Het document heeft in 2018 zijn huidige vorm gekregen mede dankzij de bijdragen van de volgende groepsleden:
Ben van Lier, Centric; Bram Havers, IBM; Henk Schepers, Philips; Jan Buis, LANCOM Systems; Jan van der Sluis, DXC; Jelle Attema, ECP; Marcel Koers, CIP; Meine van Essen, RWS; Roman Volf, Min. EZK

2 BASISPRINCIPES VOOR EEN VEILIGE INZET VAN IoT

2.1 Erkende methoden en technieken

Veel bedreigingen, die voor IoT-apparaten en het IoT-ecosysteem nieuw zijn, kennen we al voor niet IoT-toepassingen. Veel methoden en technieken voor het veilig maken of houden van traditionele ICT, zoals een risicogebaseerde aanpak, zijn daardoor ook bruikbaar bij IoT. Door de kennis en ervaring uit de traditionele ICT te benutten ontstaat een steeds completer beeld van bedreigingen en te nemen maatregelen bij het veilig maken en houden van IoT.

Erkende methoden en technieken	
Basis principe	Erkende en bewezen methoden en technieken voor ICT-beveiliging zijn benut voor de aanpak van risicomanagement en het nemen van de benodigde beveiligingsmaatregelen.
Ratio	IoT security risico's zijn in de basis hetzelfde als andere IT en netwerkrisico's. Door niet gebruik te maken van de jarenlange ervaring die in deze raamwerken is verwerkt wordt het risico op veiligheidsproblemen groter. Daarom zijn bestaande IT security raamwerken een solide basis voor het beveiligingsbeleid. Deze generieke risicobeheer raamwerken kunnen worden aangevuld met specifieke IoT veiligheidsprincipes en maatregelen.
Best-practices	Start met de basis security en practices. Gebruik hiervoor een generiek security risk management framework om alle aspecten van de beveiliging in kaart te krijgen en risico mitigerende maatregelen op te stellen en leg dit vast in het beleid van de organisatie. Gebruik daarnaast (sector) specifieke security richtlijnen om het beleid en mitigerende maatregelen vast te stellen. ENISA heeft een basis uitgebracht voor IoT: • 'Basis Security Recommendations for IoT' [9]. en bases voor vier specifieke aandachtsgebieden: • Cyber Security and Resilience of smart cars [10]. • Security and Resilience of Smart Home Environments[11]. • Securing Smart Airports [12]. • Cyber security and resilience for Smart Hospitals [13]. NIST ontwikkelt een risicomanagement aanpak voor IoT: • Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks[20]. Risico's van IoT beperken zich niet tot het IoT apparaat alleen. Hanteer daarom een benadering waarin de context van het IoT apparaat wordt meegenomen. Benut bij de totstandkoming van het stelsel van maatregelen de gelaagdheid van het IoT-ecosysteem en onderliggende infrastructuur. Scherm de toegang tot het IoT-ecosysteem af voor niet-geautoriseerden, vooral wanneer er geen patches of updatemechanismen beschikbaar zijn of onvoldoende zijn om een specifieke (bekende) kwetsbaarheid aan te pakken. Neem deel aan platforms waarin bedrijfsleven en overheid kwetsbaarheden melden en bespreken, zodat belangrijke informatie over nieuwe dreigingen en kwetsbaarheden tijdig wordt ontvangen. Benut deze informatie ook voor het creëren van awareness bij de stakeholders, dus ook die bij de business die overweegt of besluit de IoT apparaten in te zetten. In Nederland bestaan er sectorspecifieke Information Sharing and Analysis Centres (ISAC's). Benut de kennis en ervaring van de traditionele ICT-afdelingen, CISO's, privacy- en security-officers en neem ze mee bij het beperken van de risico's en het nemen van beveiligingsmaatregelen. Bedenk dat IoT-apparaten, zoals smart TV's, ook door niet ICT-afdelingen worden ingekocht en ingezet.

2.2 Risicoanalyses en prioriteren beveiligingsmaatregelen

Bij het gebruik van IoT-apparaten kan de risico-acceptatie door gebruikers bij overheid, bedrijven en consumenten aanzienlijk verschillen, mede omdat de gevolgen van een beveiligingsincident voor de verschillende betrokkenen aanzienlijk kunnen verschillen. Deze verschillen zijn vaak van invloed op de inspanning die stakeholders willen leveren om de risico's helder te krijgen en mitigerende maatregelen te willen en kunnen nemen.

Risicoanalyses en prioriteren beveiligingsmaatregelen	
Basis principe	Risicoanalyses zijn uitgevoerd, zodat de beveiligingsmaatregelen zijn geprioriteerd op basis van de gevolgen van de risico's op de werking van het IoT-ecosysteem en de bedrijfsvoering.
Ratio	Als er zich een beveiligingsincident voordoet verschillen de gevolgen aanzienlijk per toepassing en daarmee de risico-acceptatie per partij en per stakeholder. Het prioriteren van de beveiligingsmaatregelen is nodig om te komen tot passende beveiligingsmaatregelen (dat wil zeggen: adequaat en niet te duur).
Best practices	Maak in een analyse duidelijk wat het beoogde gebruik van het IoT-apparaat is en in welk IoT-ecosysteem het wordt ingezet, zodat duidelijk is met wie informatie wordt gedeeld en waar die wordt opgeslagen. Neem hierbij de inzet nu en in de toekomst mee, kijk zo mogelijk ook naar de productstrategie van de leverancier, zodat duidelijk wordt wat de risico's zijn na updates. Bepaal de beveiligingsrisico's op basis van de resultaten van deze analyse en de dreigingen, inclusief het lekken van privacygevoelige informatie of bedrijfsgegevens, die zich bij het beoogde gebruik kunnen voordoen. Identificeer en authentiseer, zeker wanneer het IoT-ecosysteem omvangrijk is, de IoT apparaten die op het netwerk zijn aangesloten. Deze inventarisatie maakt helder welke IoT-apparaten in de prioritering moeten worden meegenomen. Neem de stakeholders mee in de resultaten van de analyse en de beveiligingsrisico's, zodat ook zij weten wat de potentiele risico's zijn en prioriteer de beveiligingsmaatregelen op basis van de mate waarin de risico's worden geaccepteerd door de stakeholders. Test de kwetsbaarheid van het IoT-apparaat en het IoT-ecosysteem door actief te proberen de beveiligingsmaatregelen te omzeilen[1]. Kijk hierbij naar alle lagen van het IoT-ecosysteem. Prioriteer op basis van de resultaten van de red-teaming-oefening waar en hoe aanvullende veiligheidsmaatregelen moeten worden genomen.

[1] Indien dit gebeurt bij een operationeel ecosysteem, dan spreekt men van een 'red-teaming'-oefening.

2.3 Security by Design en Security by Default

Beveiliging staat niet los van het IoT-apparaat en het IoT-ecosysteem. Door beveiliging integraal mee te nemen in het ontwerp ervan kunnen de voordelen van de beveiligingsmaatregelen worden benut, zonder dat deze naderhand als add-on niet meer of alleen tegen hoge kosten kunnen worden toegevoegd. Door beveiligingsmaatregelen initieel als 'fabrieksinstelling' in te schakelen voorkom je dat de maatregelen onbewust niet worden benut, doordat ze bij ingebruikname niet worden ingeschakeld.

Security by Design en Security by Default	
Basis principe	De beveiliging is integraal meegenomen in het ontwerp (Security by Design), waarna de noodzakelijke beveiligingsinstellingen standaard zijn geactiveerd (Security by Default).
Ratio	Door de beveiliging integraal onderdeel te laten zijn van het ontwerpproces voorkom je dat de beveiliging niet meer kan worden ingebouwd of alleen als een dure en complexe add-on kan worden ingebouwd, waardoor risico's niet worden gemitigeerd. Door de beveiliging standaard (by default) in te schakelen voorkom je risico's, doordat beveiligingsinstellingen onbewust onveilig zijn ingesteld.
Best practices	Bied als leverancier alleen IoT apparaten aan, waarvan de aanwezige beveiligingsmaatregelen standaard actief zijn en waarborg dat de gebruiker er vervolgens doelbewust voor moet kiezen de beveiliging (zelf) anders in te stellen. Zo moeten - bijvoorbeeld - bij oplevering van het IoT-complex de wachtwoorden van IoT-apparaten niet standaard, niet herleidbaar en sterk zijn zodat ze moeilijk te kraken zijn. Zorg er als ontwikkelaar voor dat de gebruiker een melding krijgt, wanneer hij de beveiliging lager dan default instelt. Bouw het IoT-apparaat op het meest recente besturingssysteem dat technisch en economisch haalbaar is. Dat garandeert dat bekende kwetsbaarheden geen onderdeel uitmaken van het gebruikte besturingssysteem. Hierbij hoort ook een langdurige updateverplichting, waarover verderop meer (principe 4). Zet als ontwikkelaar hardware in die is voorzien van beveiligingsfuncties om de bescherming en integriteit van het apparaat te verbeteren, bijvoorbeeld door computerchips te gebruiken met ingebouwde beveiliging en door te zorgen voor versleutelde data-opslag als het apparaat toegankelijk is of in handen kan komen van niet-geautoriseerden. Houd in het ontwerp rekening met de gevolgen van tijdelijke of langdurige uitval of falen van (delen van) het IoT, het netwerk en de services, waarmee het IoT apparaat is verbonden, zodat het IoT en het ecosysteem na een uitval of falen weer correct werken. Wanneer IoT-systemen worden gekoppeld met de eigen bedrijfsvoering en systemen, neem dan die context mee in Security by Design (Business Impact Analyse). Ken daartoe de keten, inclusief de verantwoordelijkheden, waarin de IoT-apparaten en de data ervan worden toegepast.

2.4 Beveiligingsupdates en -patches

Zelfs wanneer beveiliging wordt meegenomen in de ontwerpfase, kunnen na de implementatie kwetsbaarheden in producten worden ontdekt. Die kunnen worden voorkomen of hersteld door het uitvoeren van beveiligingsupdates en (wanneer zich kwetsbaarheden voordoen) patches. Het IoT-apparaat moet zo zijn ontworpen dat dit mogelijk is. Omdat IoT-apparaten niet voor onbepaalde tijd kunnen worden aangepast en bijgewerkt heeft een IoT-apparaat een end-of-life. Het voorkomen van onduidelijkheid over de end-of-life van een apparaat vraagt vooraf om duidelijkheid over de end-of-life strategie naar afnemers toe.

Beveiligingsupdates en -patches	
Basis principe	IoT-apparaten zijn up-to-date door het uitvoeren van beveiligingsupdates. Voor kwetsbaarheden zijn of worden patches uitgevoerd. Het IoT-apparaat is zo ontworpen dat dit (tijdens de vooraf gegarandeerde levensduur van het IoT-apparaat) geautomatiseerd en veilig gebeurt.
Ratio	Als updates en patches niet mogelijk zijn wordt een apparaat vroeg of laat onvermijdelijk onveilig. Dat is slecht voor de cyber- en businesssecurity, de gebruiker, de producent (reputatie) en de maatschappij.
Best practices	Verbind het IoT-apparaat met update- en patchservices, zodat updates en patches worden uitgevoerd. Waarborg de integriteit van de updates en patches enerzijds door deze vooraf te (laten) testen en anderzijds door de authenticiteit cryptografisch te waarborgen. Voer automatisch updates en patches uit, zodat deze snel (bij voorkeur near realtime) kunnen worden doorgevoerd. Deze snelheid kan verder worden verhoogd door de beslissing om over te gaan tot patchen te automatiseren op basis van kwetsbaarheidsrapporten afkomstig van de onderzoeks- en hackergemeenschappen. Inventariseer de kwetsbaarheden van IoT-apparaten. Doe dit in een samenwerkingsverband, waaraan beveiligingsexperts van alle partijen samenwerken, bijvoorbeeld gecoördineerd door een Computer Emergency Readiness Team (CERT). Een dergelijke inventarisatie stelt ontwikkelaars in staat om kwetsbaarheden in het softwareontwerp aan te pakken en te reageren wanneer dat van toepassing is, zodat de IoT-apparaten alle benodigde updates en patches krijgen. Bied een gegarandeerde minimaal te halen end-of-life datum en maak bekend wat de potentiele risico's zijn van gebruik van een apparaat na deze datum, zodat de organisaties een end-of-life strategie voor ieder IoT-apparaat kunnen ontwikkelen en consumenten weten hoe lang zij veilig gebruik kunnen maken van het apparaat.

2.5 Bronnen en totstandkoming van de IoT-onderdelen en het IoT-ecosysteem

De ontwikkeling van IoT-apparaten en het IoT-ecosysteem kunnen worden versneld door gebruik te maken van hardware en software (inclusief codebibliotheken), waarvan de bron buiten de organisatie van de ontwikkelaar ligt. Grondige kennis van de herkomst van de bronnen en hun eigenschappen is dan essentieel. Ontwikkelaars en fabrikanten moeten hun bronnen en voortbrenging kennen, zodat zij weten of er gerelateerde kwetsbaarheden zijn in de software- en hardwarecomponenten die door leveranciers buiten hun organisatie worden geleverd. De afnemers moeten zich bewust zijn van deze risico's, zodat ze beveiligingsmaatregelen kunnen (laten) toepassen of andere leveranciers kunnen zoeken. Ook na productie en ingebruikname is deze informatie essentieel om bedreigingen en kwetsbaarheden zo snel mogelijk te kunnen patchen, de IoT-apparaten en het IoT-ecosysteem terug te halen of consumentenadviezen uit te brengen over of en hoe een veilige inzet mogelijk is.

Bronnen en totstandkoming van de IoT-onderdelen en het IoT-ecosysteem	
Basis principe	De voortbrengingsketen en de bronnen van het IoT-apparaat en het IoT-ecosysteem zijn bekend. Daar waar dit niet bekend is zijn passende beveiligingsmaatregelen getroffen of andere keuzes ter bescherming gemaakt.
Ratio	De gebruikte hardware en software in een IoT-apparaat en het IoT-ecosysteem kan voor een aanvaller bekende zwakheden bevatten die kunnen worden gebruikt voor een aanval.
Best practices	De leveranciers van de IoT-apparaten en het IoT-ecosysteem voeren, waar mogelijk over de voortbrengingsketen heen, end-to-end risicoanalyses uit, waarbij zij de risico's afkomstig van zowel interne als externe leveranciersrisico's meenemen. Waar dit niet mogelijk is worden de risico's van de onbekendheid met de bronnen en de voorbrengingsketen ingeschat. De ontwikkelaars en leveranciers van de IoT-apparaten en het IoT-ecosysteem betrekken de toeleverende leveranciers bij het proces van risicobeoordeling en het bieden van transparantie over potentiële kwetsbaarheden. Toeleverende leveranciers worden in staat gesteld zich bewust te worden van de risico's van onveilige IoT-apparaten en het belang (ook commercieel) van bevordering van vertrouwen en transparantie. De leveranciers van de IoT-apparaten en het IoT-ecosysteem werken bij wijziging van de voortbrengingsketen de risicobepalingen en de benodigde beveiligingsmaatregelen bij. De leveranciers van de IoT-apparaten en het IoT-ecosysteem zorgen voor een actuele lijst van hardware en software om het onderlinge vertrouwen te kunnen vergroten, risico's van onbekende toeleveranciers beter te begrijpen en te beheersen en om eventuele kwetsbaarheden onmiddellijk na een incident op te kunnen sporen. De afnemers verkrijgen de bovenstaande informatie van de leveranciers of gaan na of er een certificering bestaat ten aanzien van de veiligheid die de voortbrengingsketen biedt bestaat. Indien die niet bestaat is extra aandacht nodig voor basisprincipe 6.

2.6 Veilige netwerkconnectiviteit

Het verbinden van IoT-apparaten met zowel een intern netwerk als het Internet maakt het mogelijk de grenzen van een IoT-ecosysteem te verleggen. Dit biedt nieuwe mogelijkheden en kansen, maar ook nieuwe dreigingen. Zeker wanneer een partij geen of weinig invloed heeft op het operationaliseren van de andere vijf basisprincipes is alertheid op dit punt gewenst. Soms is het mogelijk de netwerkconnectiviteit te beveiligen. Dit is met name aanbevolen wanneer daardoor de primaire functie van het IoT-apparaat niet wordt beperkt.

Veilige netwerkconnectiviteit	
Basis principe	Alleen die netwerkconnectiviteit, die noodzakelijk is voor het correct functioneren van het IoT-apparaat en het IoT-ecosysteem, is beschikbaar voor het IoT-apparaat. Deze connectiviteit is beveiligd.
Ratio	Door het beperken van de netwerkconnectiviteit wordt de toegang tot zwakheden en daarmee de kans op misbruik van zwakheden beperkt.
Best practices	Wanneer je geen of een beperkte invloed hebt op het ontwerp, bijvoorbeeld omdat gebruik gemaakt wordt van commerciële IoT componenten of omdat een ouder apparaat niet meer te patchen is, zorg dan voor netwerkbeveiligingsmaatregelen in de toegang tot het Internet. Dit kan bijvoorbeeld door de IoT apparaten achter een gateway in de vorm van een firewall te plaatsen. Maak een analyse van de netwerkconnectiviteit die noodzakelijk en veilig is om de benodigde primaire functionaliteit te bieden. Informatie over de aard en het doel van verbindingen vormt hier de basis voor. Bied alleen directe internetverbindingen aan die nodig zijn om kritieke functies van een IoT-apparaat te bedienen. Maak die keuzes bewust en op basis van de analyse van de netwerkconnectiviteit die noodzakelijk is en wees alert op mogelijkheden voor 'sluipverkeer' (covert channels). Beperk de risico's van connectiviteit door het aantal toegangen te beperken, de inzet van bewezen veilige standaarden, de inzet van detectievoorzieningen en het bieden van een veilige connectiviteit door de inzet van beveiligde zones, bijvoorbeeld met een VPN of een firewall. Stel als ontwikkelaar de beheerders in organisaties en de consumenten in staat netwerkverbindingen of specifieke poorten uit te schakelen wanneer nodig of gewenst om selectieve connectiviteit mogelijk te maken door de hiervoor benodigde besturingselementen in te bouwen. Informeer als leverancier de beheerders en de consumenten over waarom, wanneer en hoe zij die netwerkverbindingen of specifieke poorten in kunnen stellen.

3 AANPAK VOOR EEN VEILIGE INZET VAN IoT

De inzet van IoT kenmerkt zich door een grote mate van verbondenheid. Deze verbondenheid is er onderling technisch via netwerken, maar vooral ook organisatorisch, doordat er bij de realisatie vaak meerdere partijen betrokken zijn. Op het interne technische ontwerp van het IoT-apparaat heeft de partij die het IoT-apparaat inzet veelal geen of slechts beperkte invloed (gehad) en daarmee ook op de reeds genomen beveiligingsmaatregelen. Het veilig inzetten van IoT-apparaten vraagt daarom om een aanpak, waarbinnen technische en organisatorische maatregelen worden genomen die de oorzaken van de onzekerheden én de gevolgen (de risico's) van de onzekerheden beperken.

Door het toepassen van de basisprincipes worden de onzekerheden en de gevolgen beperkt. Hieronder volgt een aanpak die helpt invulling te geven aan deze principes. De aanpak biedt zo voor een organisatie, die IoT wil (gaan) inzetten, een aanpak om actief tot een veilige inzet van IoT te komen. De veiligheid neemt toe als meer stappen met een positief resultaat worden doorlopen. Indien geen van de stappen met een positief resultaat kunnen worden doorlopen is inzet van IoT niet veilig en wordt dan ook afgeraden. Een stapsgewijze aanpak voor de inzet van IoT-apparaten:

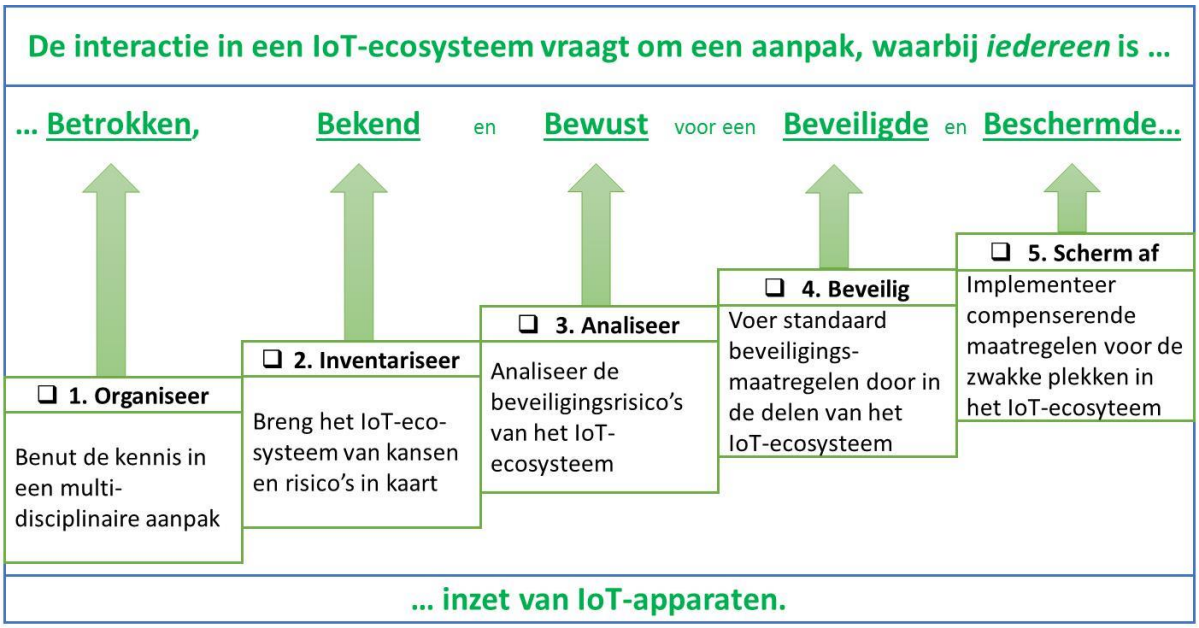
Stap 1. Organiseer
Benut de kennis in een multidisciplinaire aanpak, zodat iedereen betrokken is.

Stap 2. Inventariseer
Breng het ecosysteem van kansen en risico's in kaart, zodat iedereen daarmee bekend is.

Stap 3. Analiseer
Analiseer de beveiligingsrisico's van het ecosysteem, zodat iedereen zich van de risico's bewust is.

Stap 4. Beveilig
Voer standaard beveiligingsmaatregelen door in de delen van het ecosysteem, zodat deze beveiligd zijn.

Stap 5. Scherm af
Implementeer compenserende maatregelen voor de resterende zwakke plekken binnen het ecosysteem, zodat deze beschermd zijn in het IoT-ecosysteem.



3.1 Organiseer

Om een uitspraak te kunnen doen over de risico's en om een risicomanagement aanpak te hanteren zijn mensen nodig die de inhoudelijke kennis hebben van risicomanagement methoden en van de gebruikte technieken. Een multidisciplinaire aanpak vergroot daarbij het inzicht in de reden van de inzet en biedt toegang tot een netwerk van organisaties, waarin kennis over kwetsbaarheden wordt gedeeld. Bedenk daarbij dat de gebruikte software gebaseerd is op bestaande oplossingen en internetstandaarden, terwijl een IoT als apparaat vaak nieuw of relatief nieuw is. In de beveiligingsorganisaties en de ICT-afdelingen is hierover kennis voorhanden. Het organiseren en benutten van deze kennis, samen met diegenen die verantwoordelijk zijn voor de keuze en het gebruik, vergroot het bewustzijn. Communicatie over risico's en oplossingen is een belangrijke voorwaarde om dit bewustzijn te bereiken.

Een multidisciplinaire aanpak helpt bij:

- Het begrijpen van wie betrokken zijn bij de inzet en hun motieven en inzichten.
- Het collectief benutten van de in dit document beschreven basisprincipes en best practices.
- Het benutten van de gelaagdheid van het IoT-apparaat en het IoT-ecosysteem.
- Het begrijpen en doorgronden van (sector)specifieke securitybases en de richtlijnen.
- Het inzetten van methodieken voor risicoanalyses en risicomanagement, zoals ISO 27005.
- Het beleggen bij en laten nemen van verantwoordelijkheden door de betrokken partijen.

Stap 1: Benut de kennis in een multidisciplinaire aanpak.
Kies een aanpak waarbij de disciplines vanuit hun kennis en kunde worden meegenomen en betrokken zijn, zodat zij als stakeholder medeverantwoordelijk worden gemaakt voor een veilige inzet van IoT.

3.2 Inventariseer

Een IoT apparaat en een IoT ecosysteem komen tot stand door samenwerking tussen verschillende partijen. Iedere partij draagt bij in het netwerk van afhankelijkheden. Ieder schakel daarin biedt kansen, maar ook risico's: een ketting is zo sterk als de zwakste schakel. Om die kansen en risico's te kunnen inschatten is een beeld van het netwerk van afhankelijkheden een vereiste. Het in beeld hebben van de onderdelen en de onderlinge gegevensuitwisseling binnen het betreffende IoT ecosysteem mag daarbij als minimumvereiste gezien worden. De mate van fijnmazigheid van het beeld wordt bepaald door de mate waarin de partijen bereid zijn tot het verstrekken van informatie. Hoe fijnmaziger de informatie, hoe nauwkeuriger er in een volgende stap een inventarisatie van risico's voor de informatieveiligheid gemaakt kan worden. Deze fijnmazigheid kan bijvoorbeeld beperkt zijn doordat informatie over het voortbrengingsproces van het IoT-apparaat ontbreekt. Risicomanagement voor deze voortbrengingsketen en dit deel van het IoT ecosysteem is dan niet mogelijk.

Stap 2: Breng het ecosysteem van kansen en risico's in kaart.
Breng het IoT ecosysteem in kaart. Streef daarbij naar een fijnmazigheid die aansluit bij de mate waarin u invloed heeft op betrokken partijen.

3.3 Analiseer

Een veilige inzet van IoT vraagt om het nemen van de juiste beveiligingsmaatregelen. Of een maatregel nodig is wordt bepaald in een risicoanalyse. Het risico ontstaat door de kans dat een gebeurtenis zich voordoet en de negatieve gevolgen van de gebeurtenis wanneer zij zich voordoet, oftewel:
risico = kans x impact. Het uitvoeren van de risicoanalyse heeft tot doel de gevolgen te analyseren van bedreigingen, waaraan een IoT-ecosysteem, een bedrijfsproces en de informatie worden blootgesteld, deze bewust te onderkennen en op grond hiervan een passend beveiligingsniveau te bepalen en de beveiligingsmaatregelen te prioriteren. Kijk hierbij niet alleen naar het IoT-apparaat, maar juist ook naar het gehele IoT-ecosysteem en probeer te achterhalen waar de resterende zwakke plekken zich bevinden.

Stap 3: Analiseer de beveiligingsrisico's van het ecosysteem.
Voer een risicoanalyse uit. Kijk hierbij naar de zwakheden van het IoT-apparaat én het IoT-ecosysteem. Betrek hierbij (zie stap 1) partijen die de resterende zwakke plekken bij de inzet van de IoT apparaten kennen of kunnen achterhalen. Prioriteer de te nemen maatregelen op basis van kans x impact.

3.4 Beveilig

Een aanval op een IoT apparaat of een IoT ecosysteem als geheel is in veel gevallen een aanval die primair is gericht op bekende zwakheden. Pas wanneer er een aanval plaatsvindt die specifiek is gericht op uw IoT ecosysteem en de bekende zwakheden niet benut kunnen worden, zoeken aanvallers verder naar zwakheden. Dit betekent dat het doorvoeren van een standaardpakket van beveiligingshygiëne-maatregelen vaak een eerste aanval afslaat. De basisprincipes 3 en 4 beschrijven een belangrijk deel van de die standaard beveiligingshygiëne-maatregelen om het IoT-apparaat en het IoT-ecosysteem te beveiligen. In aanvulling daarop kan gekeken worden naar best-practices die zich, naast de IoT-apparaten, vooral richten op de rest van het IoT ecosysteem:

- Voor het sturen op de beveiliging van de IoT-communicatie en de services binnen het Ecosysteem kan de opdrachtgever gebruik maken van de SSD normen voor applicaties van het CIP.
- Voor het sturen op de beveiliging van apps op mobiele apparaten van eindgebruikers kan de opdrachtgever gebruik maken van de SSDm normen voor mobile apps van het CIP.
- Voor de ontwikkeling van veilige software kan door de ontwikkelaar gebruik malen van Secure Software Framework van Secure Software Alliance.

Stap 4: Voer standaard beveiligingsmaatregelen door in de delen van het ecosysteem.
Voer standaard beveiligingshygiëne-maatregelen door. Kijk daarbij naar de basisprincipes en best-practices en focus daarbij op die delen van het IoT ecosysteem, waarop u invloed heeft.

3.5 Scherm af

In stap 2 is gesteld dat het netwerk in de praktijk soms slechts ten dele is te inventariseren wanneer de mate van fijnmazigheid beperkt is. Ook is de invloed op de (keten van) leveranciers in de praktijk beperkt. Dit betekent dat niet altijd de toepasselijke maatregelen genomen en zeker niet bewaakt kunnen worden om een veilige inzet van IoT mogelijk te maken. Dit vraagt, in aanvulling op stappen 1 t/m 4, om compenserende maatregelen op een andere plaats dan daar waar de oorsprong van het risico zich bevindt. Een bekende en effectieve maatregel is het beschermen op netwerkniveau, door de netwerkconnectiviteit (basisprincipe 6) te beperken en in aanvulling daarop netwerksegmentering toe te passen. Het resultaat is een afscherming op netwerkniveau, zoals die ook met een DMZ (gedemilitariseerde zone) bereikt wordt in meer conventionele contexten: de toegang tot de zone is beperkt en indien de beveiliging binnen de zone wordt doorbroken worden de gevolgen beperkt gehouden door de segmentering.

Stap 5: Implementeer compenserende maatregelen voor de resterende zwakke plekken binnen het ecosysteem.
Beperk de toegang tot de IoT apparaten door deze op netwerkniveau af te schermen en plaats de IoT apparaten en de services die beperkt te beveiligen zijn in een of meer separate netwerkzones.

4 NUTTIGE BRONNEN

Nederland: CIP

[1]. Beveiligingseisen voor applicaties; 5 oktober 2014; https://www.cip-overheid.nl/category/producten/secure-software#grip-op-ssd-de-normen

[2]. Beveiligingseisen voor mobile apps; 25 februari 2016; https://cip-overheid.nl/category/producten/secure-software#grip-op-ssd-de-normen-voor-mobiele-apps

Nederland: Ministeries

[3]. Roadmap Digitaal Veilige Hard- en Software; 2 april 2018; https://www.rijksoverheid.nl/documenten/rapporten/2018/04/02/roadmap-digitaal-veilige-hard-en-software

[4]. Het Internet of Things: kansen, bedreigingen en maatregelen; Ministerie van Veiligheid en Justitie: WODC

[5]. Een verkenning naar de kansen en bedreigingen van het Internet of Things; 24 oktober 2016; Ministerie van Veiligheid en Justitie

- (Verkeerd) verbonden in een slimme samenleving; 12 juni 2017; Ministerie van Veiligheid en Justitie: WODC
- 'Naar een veilig verbonden digitale samenleving' , Advies inzake de cybersecurity van het Internet of Things (IoT) , CSR-advies 2017 (https://www.cybersecurityraad.nl/binaries/CSR%20Advies%20IoT%20digitale%20versie%20DEF%20NED_tcm56-298518.pdf)

Nederland: andere openbare bronnen

[6]. TNO; TNO 2016 R11648; Veilig omgaan met het Internet of Things: Een handreiking voor informatiebeveiligers; 8 december 2016; Ir. A.C.M. Smulders, L. Oosterheert MSc, R.H. ten Hove MSc, Drs. J. Adriaanse

[7]. SIDN: SPIN: a User-centric Security Extension for In-home Networks; SIDN Labs Technical Report SIDN-TR-2017-002; 30 juni 2017; Cristian Hesselman, Jelte Jansen, Marco Davids, and Ricardo de O. Schmidt

[8]. SSA: Agile Secure Software Lifecycle Management, Secure by Agile Design; Dr. lec. Barry Derksen MMC MSc CISA CGEIT, Monique Neggers CISA CISM CGEIT CRISK, Drs. Ing. Danny Onwezen CISA CISM, Stef Zelen RE

Europa: Enisa (de nummers verwijzen naar de nummers bij basisprincipe 1):

[9]. Basis Security Recommendations for IoT; 20 november 20 2017 https://www.enisa.europa.eu/publications/basis-security-recommendations-for-iot

[10]. Cyber Security and Resilience of smart cars; 13 januari 2017 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[11]. Security and Resilience of Smart Home Environments; 1 december 2015 https://www.enisa.europa.eu/publications/security-resilience-good-practices

[12]. Securing Smart Airports; 16 december 2016; https://www.enisa.europa.eu/publications/securing-smart-airports

[13]. Cyber security and resilience for Smart Hospitals; 24 november 2016; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

USA: Department of Homeland Security

[14]. STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS; versie 1.0; 15 november 2016

[15]. https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf

[16]. https://www.dhs.gov/publication/security-tenets-lces

[17]. https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

USA: Andere overheidsorganisaties

[18]. National Security Telecommunications Advisory Committee: Final NSTAC Internet of Things Report
[19]. NTIA
- Notice and Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
- Green Paper – Cybersecurity, Innovation and the Internet Economy, 2011
- New Insights into the Emerging Internet of Things
- Remarks of Deputy Assistant Secretary Simpson at Fostering the Advancement of the Internet of Things Workshop, 9/9/2016
- Internet Policy Task Force resource/review/cataloging of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things.

[20]. NIST
- Het National Institute of Standards and Technology (NIST) heeft een raamwerk voor cybersecurity risicomanagement gepubliceerd. Het raamwerk biedt, hoewel niet specifiek voor IoT, een risicokader voor het bepalen van risico's en de bijbehorende best-practices: https://www.nist.gov/cyberframework
- NISTIR 8228 (DRAFT) - Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks; https://doi.org/10.6028/NIST.IR.8228-draft
- Cyber-Physical Systems (CPS) Program: CPS Public Working Group (PWG) draft Cyber-Physical Systems (CPS) Framework Release 1.0
- International Technical Working Group on IoT-Enabled Smart City Framework
- NIST Special Publication (SP) 800-183, Network of Things, 7/28/2016

[21]. Federal Trade Commission
- FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World", January 2015

[22]. United States Congress
- Senate Committee on Commerce, Science, and Transportation committee hearing, "The Connected World: Examining the Internet of Things."
- Senate unanimously bipartisan resolution (S. Res. 110) calling for a national strategy to guide the development of the Internet of Things
- House Energy and Commerce Committee's "The Internet of Things: Exploring the Next Technology Frontier"

[23]. Government Accounting Office
- GAO engagement with DHS: GAO is currently engaged with DHS on IoT, code 100435, Status/entry in the most recent, June 3, 2016 List of Active GAO Engagements Related to DHS

Andere openbare bronnen:

[24]. Atlantic Council: Smart Homes and the Internet of Things – http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
[25]. I Am The Cavalry
- Five Star Automotive Cyber Safety Framework – https://iamthecavalry.org/5star
- Hippocratic Oath for Connected Medical Devices – https://iamthecavalry.org/oath

[26]. Online Trust Alliance:
- Consumer Best-Practices
- IoT Trust Framework v2.0 - Released Jan 5, 2017

[27]. Industrial Internet Consortium: http://www.iiconsortium.org/IISF.htm
- Open Web Application Security Project (OWASP)
- Internet of Things Project https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- Internet of Things Security Guidance https://www.owasp.org/index.php/IoT_Security_Guidance

[28]. Safecode.org relevant industry best-practices www.safecode.org

[29]. AT&T: Exploring IoT Security
[30]. IoT Security Foundation: IoT Security Compliance Framework, Release 1.1, December 2017
[31]. Symantec: An Internet of Things Reference Architecture
[32]. Gartner: Top 10 IoT Technologies for 2017 and 2018; 22 January 2016; Nick Jones
[33]. https://krebsonsecurity.com/2017/08/new-bill-seeks-basic-iot-security-standards/
[34]. IEEE:
- Proposed Embedded Security Framework for Internet of Things (IoT) ; https://ieeexplore.ieee.org/document/5940923/
- Security and Privacy Challenges in Industrial Internet of Things; https://ieeexplore.ieee.org/document/7167238/

Ook veel actuele informatie is te vinden bij:

[35]. **NCSC**
Het NCSC draagt bij aan het gezamenlijk vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving door het leveren van inzicht en het bieden van handelingsperspectief
https://www.ncsc.nl/ .

[36]. **Cyber Security Raad**
De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen
https://www.cybersecurityraad.nl/ .