INFORMATIE BEVEILIGINGS DIENST

VNG Realisatie

Handreiking

IoT beveiliging

Een operationeel kennisproduct ter ondersteuning van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)

IT Building B.V. hanteert dit document als leidraad voor het advies, implementatie en beheer van gebouwautomatisering en online toegangscontrole en alle toepasbare diensten.

it Building control services

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Handreiking IoT beveiliging

Versienummer

1.2

Versiedatum

Februari 2020

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Rechten en vrijwaring

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie

Versie	Datum	Wijziging / Actie
0.7	16-04-2018	Initiële opzet
0.8	17-04-2018	Interne review
0.9	07-05-2018	Voor externe review
1.0	23-08-2018	Publicatie
1.1	20-11-2019	BIO aanpassing
1.2	05-02-2020	BIO 1.04 aanpassingen (in groen)

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD ondersteunt gemeenten bij hun inspanningen op het gebied van informatiebeveiliging en privacy / gegevensbescherming en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruikmaken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

VNG Realisatie

INFORMATIE
BEVEILIGINGS
DIENST

Leeswijzer

Dit product is een nadere uitwerking voor gemeenten van de Baseline Informatiebeveiliging Overheid (BIO). De BIO is eind 2018 bestuurlijk vastgesteld als gezamenlijke norm voor informatiebeveiliging voor alle Nederlandse overheden.

Doel

Het doel van dit document is om inzicht te verschaffen in risico's en beveiliging aandachtspunten van IoT toepassingen.

Doelgroep

Dit document is van belang voor de CISO, de systemeigenaren, applicatiebeheerders en de ICT-afdeling.

Relatie met overige producten

- Baseline Informatiebeveiliging Overheid (BIO)
- Informatiebeveiligingsbeleid van de gemeente
- Factsheet penetratietesten
- Procedure nieuwe ICT-voorzieningen
- Procedure afvoer ICT middelen
- Procedure mobiele gegevensdragers

Eigenlijk zijn op IoT dezelfde beveiligingseisen van toepassing als voor ICT, de belangrijkste raakvlakken met de Baseline Informatiebeveiliging voor de Overheid (BIO) zijn:

8.1.1 Inventariseren van bedrijfsmiddelen
8.3.1 Verwijderen van media
9.4.1 Beperking toegang tot informatie
9.4.2 Beveiligde inlogprocedures
11.2 Apparatuur
12 Beveiliging bedrijfsvoering
13.2 Informatietransport
14.1 Beveiligingseisen voor informatiesystemen
16.1.3 Coordinated Vulnerability Disclosure

Wat is er veranderd ten opzichte van de BIG?

Er is weinig veranderd ten opzichte van de BIG, de IoT uitdagingen voor gemeenten zijn niet gewijzigd, het document is aangepast aan de BIO.

Inhoudsopgave

1. Inleiding

Internet of Things (IoT) ofwel Internet der dingen is niet meer weg te denken uit de samenleving. Ook gemeenten hebben te maken met IoT. Er zijn gemeenten actief bezig met IoT, en de kans bestaat dat IoT al aanwezig is binnen de gemeente zonder dat men zich daarvan bewust is.

Eerst een afbakening, wat is nou IoT? Wikipedia zegt er dit over:

Het Internet der dingen (Engels: Internet of Things) refereert aan de situatie dat door mensen bediende computers (desktops, laptops, tablets, smartphones) in de minderheid zullen zijn op het internet. De meerderheid van de internetgebruikers zal in deze visie bestaan uit semi-intelligente apparaten, zogenaamde ingebouwde systemen (embedded systems). Alledaagse voorwerpen worden hierdoor een entiteit op het Internet, die kunnen communiceren met personen en met andere objecten, en die op grond hiervan autonome beslissingen kunnen nemen.

Denk bij die objecten aan alles waar een computer en Internet (communicatie) functionaliteit in gestopt kan worden, de mogelijkheden zijn wat dat betreft onbegrensd. IoT heeft naast een verbinding met Internet ook een besturingsinterface. Het IoT apparaat kan hiermee worden uitgelezen en bediend, bijvoorbeeld via een ingebouwde webserver of door middel van een app op een smartphone. Vaak is er dan ook nog een connectie met een systeem in de Cloud waar de leverancier van het IoT apparaat alle info en besturing van het apparaat regelt voor alle klanten.

Kenmerkend(er) voor IoT is dat, in plaats van geïsoleerde regelsystemen (de traditionele ‘thermostaat’ met één regelsysteem, één input en één output) er een web ontstaat van gekoppelde sensoren (input), actuatoren (output) en verwerkingssystemen (inderdaad veelal in de Cloud). Die onderlinge afhankelijkheden hebben grote implicaties als het gaat om beveiliging. In het sterk vereenvoudigde onderstaande schema wordt dit duidelijk, de IoT apparaten zijn verbonden via het Internet met een centrale Cloud omgeving waar vervolgens de gegevens of besturing met een App, een website of een andere interface kan worden gedaan.

Wat zijn mogelijkheden van IoT:

Sensor

IoT kan een sensor zijn die informatie levert ten behoeve van andere systemen, waarbij gebruik gemaakt wordt van het netwerk. Bijvoorbeeld een temperatuursensor, verkeersteller, luchtkwaliteit-meetinstrument. De gegevens van de sensor worden doorgaans opgeslagen in een systeem, bijvoorbeeld in de eerdergenoemde Cloud opslag, Daarnaast kunnen deze gegevens ook weer beschikbaar gesteld worden als (open) data waar anderen functionaliteit op kunnen aanbieden. De gegevens die door een IoT apparaat worden verzameld en opgeslagen kunnen ook persoonsgegevens zijn.

Besturing

IoT kan ook gebruikt worden voor besturing van apparatuur. Bijvoorbeeld een CV-ketel die wordt aangestuurd door een thermostaat. Denk hierbij ook aan slimme lampen in huis die bestuurd worden door een apparaat waartegen men kan spreken. De spraak wordt over het Internet naar een systeem gezonden die vervolgens die spraak kan omzetten naar een commando voor de lamp. Feitelijk wordt dus continue geluisterd naar wat gezegd wordt om een commando te kunnen herkennen, als het device actief is (en de app in de achtergrond draait) en de verbinding met het Internet actief is.

Samenvattend:

IoT heeft een aantal specifieke kenmerken, deze zijn volgens IoT Nederland :

1. Er zijn dingen (Things) als sensor of apparaat die iets registreren of meten;
2. Er wordt data verzameld door deze dingen;
3. Er is communicatie, er wordt data verzonden tussen apparaten of naar opslag;
4. Die data wordt (al of niet) geaggregeerd en betekenisvol gemaakt tot informatie (smart analytics);
5. Op basis van de geaggregeerde informatie worden beslissingen genomen of acties geautomatiseerd;
6. Er is een ecosysteem: community, context en Internet of Everything (IoE);
7. Er is connectiviteit: netwerk/Internet..

1.1. Scope, aanwijzing voor gebruik

Dit document is geschreven met als scope dat IoT fysiek deel kan uitmaken van de gemeentelijke infrastructuur. Daarmee wordt IoT een aandachtspunt van de CISO en I&A afdeling. Als IoT geen deel uitmaakt van de gemeentelijke IT betreft het aandachtsgebied de data die gegenereerd wordt door de IoT systemen, die mogelijk interessant kan zijn voor de gemeente.
De scope strekt zich ook uit over toeleveranciers als de IoT data afkomstig van sensoren/devices door een gemeente als dienst wordt afgenomen. Dan dient de gemeente zich ervan te vergewissen dat die leverende partij zich houdt aan de beveiligings- en privacy eisen, komend uit het beleid, van de gemeente (BIG en AVG).

1.2. Relatie IoT, ICT en SCADA

Deze paragraaf lijkt een vreemde eend in de bijt, echter IoT en SCADA hebben iets gemeenschappelijks. Wat is dan SCADA?

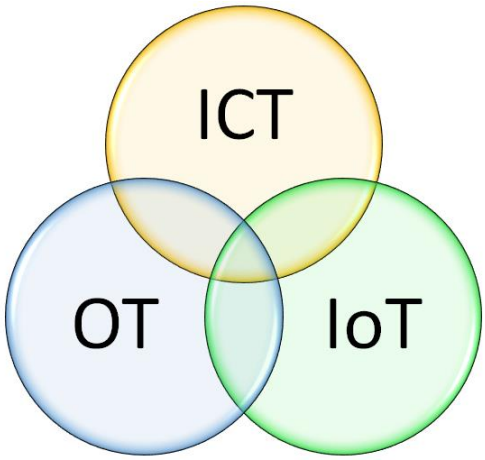
Voor het elektronisch aansturen van mechanische en/of industriële objecten in de openbare- of privéruimte worden vaak ICS/ SCADA standaard/systemen gebruikt. SCADA staat voor “Supervisory Control And Data Acquisition” en ICS voor “Industrial Control Systems”.

Deze systemen, verzamelen, versturen, verwerken en visualiseren meet- en regelsignalen van allerlei (industriële) objecten. Zij krijgen deze gegevens door van de verschillende onderdelen van zo’n object, zo’n onderdeel heet een PLC (Programmable Logic Controller). SCADA wordt vaak OT - Operationele Technologie genoemd. ICS/ SCADA aangestuurde objecten zijn vaak over grote afstanden verspreid en worden centraal aangestuurd en gemonitord door middel van een centraal aansturings- en monitoringssysteem.

Traditioneel loopt SCADA-verkeer niet via TCP/IP, dat wil zeggen dat SCADA-systemen geen IP-adres hebben en daarmee niet via internet benaderbaar zijn. Er zijn al wel meldingen van het toevoegen van IP gebaseerde connectiviteit aan SCADA-systemen waarmee deze wel aan Internet gekoppeld kunnen worden. Daarnaast is IoT zelf vaak al een sensor, met Cloud connectiviteit voor opslag en besturing. De stap naar het combineren van ICT, IoT en SCADA tot een complex geheel, is dan niet meer zo groot. Er is onderzoek gedaan naar dit verschijnsel waaruit blijkt dat er een toename is van SCADA-systemen die aan Internet gekoppeld worden.

Dit brengt nieuwe risico's met zich mee voor deze SCADA-systemen. Door het koppelen van IoT-systemen en mogelijk ook kantoorautomatisering wordt een complexe en in potentie zeer risicovolle situatie geschapen. De zwakheden van de vaak oudere SCADA-systemen en de vaak onveilige (want niet vanuit het oogpunt van veiligheid ontworpen) IoT apparaten vormen dan een aanvalsmogelijkheid naar de kantoorautomatisering en gemeentelijke systemen. Overigens geldt dit ook voor oudere sensoren die volgens de definitie niet IoT en SCADA-apparaten zijn.

Onderstaande afbeelding maakt duidelijk hoe de systemen zich verhouden tot elkaar. SCADA en IoT systemen kunnen via IT worden gekoppeld. In een SCADA-systeem kunnen ook IoT componenten zitten.



Bovenstaande maakt ook direct duidelijk dat de koppeling tussen verschillende systemen of omgevingen, ICT, OT (Operationele Technologie ofwel SCADA) en IoT, een risico met zich kan brengen. Een incident ten gevolge van een zwakheid binnen een van deze omgevingen zal ook de andere omgevingen kunnen beïnvloeden. Bijvoorbeeld: een beveiligingscamera wordt gehackt en door die camera worden de mogelijk gekoppelde ICT-systemen voor de opslag en de verwerking van de beelden aangevallen (en mogelijk ook gewone kantoor ICT-systemen). Het feit dat IoT of OT systemen niet direct deel uitmaken van de gemeentelijke kantoorautomatisering maakt dat deze systemen “vergeten” kunnen worden.
ICS/SCADA-systemen worden niet alleen door de gemeente gebruikt, deze systemen worden regionaal en landelijk ook op grote schaal ingezet door het Rijk, Provincies en Waterschappen voor waterbeheer, wegbeheer enzovoort. Voor ICS/SCADA-systemen is er bij Rijkswaterstaat samen met de Waterschappen in 2016 een CERT-WM (CERT-Water Management) opgericht, deze CERT draait binnen het Security Operations Center (SOC) van Rijkswaterstaat voor het verlenen van preventieve, reactieve en adviserende diensten aan haar deelnemers met betrekking tot cybersecurity van de OT in bijvoorbeeld bruggen, sluizen en waterkeringen.

2. Waar wordt gemeentelijke IoT gebruikt?

Het gebruik van IoT groeit hard en de voorspellingen zijn dat er tegen 2020 tegen de 30 miljard en in 2025 75 miljard IoT objecten in gebruik zijn[1]. Van intelligente armbanden, keukenapparatuur, speelgoed tot medische apparatuur, aardbevingssensoren en elektronica in auto's en vliegtuigen. Ook binnen gemeenten is IoT in gebruik. Enkele voorbeelden zijn:

- Rioolgemaal
- Bergbezinkbassin
- Verkeersregelinstallatie (VRI)[2]
- Camerasysteem raadzaal
- Camerasysteem voetgangerstunnel
- Camerasysteem invalswegen gemeente
- Camerasysteem gemeentewerf
- Bluswaternetwerk
- Openbare straatverlichting
- Diverse elektronische toegangspoorten en hekwerken
- Zwembad, waterkwaliteit filterinstallatie
- Noodaggregaat
- UPS (uninterruptible power supply)
- Matrix reclameborden toegangswegen
- Gebouwmanagementsysteem
- Luchtbehandeling
- Elektronisch toegangscontrolesysteem
- Brandmeldcentrales
- Inbraakdetectie systemen
- Liften
- Omroepinstallatie
- Ontruimingsinstallatie
- Warmtekrachtinstallatie
- Verkeerstellers

Binnen gemeentelijke gebouwen

Denk hierbij aan IoT systemen voor gebouwbeheersing, klimaatbeheersing, energie beheersing en verlichting. Hoewel dat soort systemen ook soms als SCADA gezien kunnen worden is die grens meer en meer aan het vervagen. Ook IoT gerelateerd aan fysieke veiligheid wordt meer en meer verbonden met het Internet. Dit geldt voor toegangssystemen en bewaking systemen met camera's en sensoren. Een ander voorbeeld is keukenapparatuur, koffieautomaten en liften die zelf doorgeven dat onderhoud nodig is, dit wordt gesignaleerd op basis van gebruiksgegevens. IoT kan ook worden meegebracht door gemeenteambtenaren (in de vorm van smart watches bijvoorbeeld) en zo ongezien gekoppeld worden aan het gemeentelijke netwerk. Daarnaast zijn er nog Tv-schermen (smart tv met Internet en spraakherkenning), webcast systemen en bijvoorbeeld slimme thermostaten.

1 De verwachting bestaat dat IoT toepassingen van een 5G variant gebruik gaan maken, wat ook voor een boost gaat zorgen.

2 Zie voor meer info over VRI: https://www.ivera.nl/

In de regio

Binnen de gemeentelijke regio kan IoT voor vele toepassingen worden ingezet, denk hier aan IoT die gebruikt wordt voor smart city - slimme steden-concepten. IoT kan worden ingezet om steden leefbaarder, veiliger, duurzamer en beter bereikbaar te maken. Deze initiatieven zijn veelal nog experimenteel en kleinschalig. Het is een kwestie van tijd tot verschillende IoT toepassingen hun intrede doen in de stedelijke omgeving. Er zijn vele mogelijkheden, denk aan slimme verlichting, beveiligingssystemen, crowdcontrol, bediening van bruggen en sluizen, omgevingssensoren, afval beheersing, smart parking, ouderenzorg en bijvoorbeeld verschillende verkeerssensoren. Er zijn gemeenten met stadspassen voor hun burgers die voor verschillende functies gebruikt kunnen worden, zoals toegang tot diensten of het betalen van goederen. Ook hier kunnen, door middel van het inzetten van IoT, de mogelijkheden worden uitgebreid. De vervolg stap is niet zo groot als informatie verzameld door de slimme stad gebruikt wordt voor open dataprojecten. Daarnaast zijn er ook andere ontwikkelingen waarbij IoT naar de gemeente toekomt, bijvoorbeeld in de vorm van zelfrijdende vervoersmiddelen. Zelfrijdende auto’s

Buiten de gemeente regio / landelijk

Verdere uitbreiding van snel Internet via mobiele netwerken en glasvezel maken dat alle IoT apparaten nog makkelijker connectie kunnen maken met het Internet en backend systemen. Denk hierbij aan het koppelen van regionale IoT tot een landelijk systeem. Maar ook energievoorziening (smart grid), klimaat en verkeerbeheersing zijn toepassingen waar IoT een rol speelt op steeds grotere schaal.

3. Wat zijn de risico's?

Met de toename van IoT objecten nemen de risico's ook toe. Maar ook de afhankelijkheid van goed werkende en betrouwbare IoT toepassingen neemt toe. Daarnaast neemt ook het belang toe van juiste en tijdige IoT data die al of niet voor andere processen gebruikt kan worden.

Traditioneel is IT-beveiliging gericht op de interne kantoorautomatisering van de organisatie. De laatste jaren wordt meer en meer duidelijk dat ook de "buitenkant" een bedreiging vormt. Daarmee werd het woord Cybersecurity geboren. Met IoT zal een deel van de gemeentelijke informatie verwerkende processen zich verplaatsen of verschuiven naar andere gebieden. Een connected smart city biedt nieuwe mogelijkheden, bijvoorbeeld door infrastructuur naar auto communicatie. Dit brengt vanzelfsprekend ook nieuwe risico's mee. Daarnaast is de kans groot dat IoT gekoppeld wordt aan de gemeentelijke IT-infrastructuur en daarmee worden IoT zwakheden ook een bedreiging voor de gemeentelijke informatie verwerkende processen.

De ICS-CERT van de Amerikaanse overheid geeft een rapport uit waarin zij de trends analyseren van de top 6 aan zwakheden in industriële automatisering omgevingen , deze top 6 is:

- Gebrek aan afscherming en segmentatie, ongeautoriseerde toegang tot IoT systemen en zwakheden in de afscherming tussen IT en OT-omgevingen;
- Functionaliteit minimalisatie / hardening: toename van mogelijkheden voor toegang door kwaadwillenden van buiten de omgeving maar ook ongeautoriseerde toegang van binnen de organisatie;
- Identificatie en authenticatie: gebrek aan tracability en accountability van gebruikers handelingen als een account wordt misbruikt/gehackt. Daarnaast het steeds moeilijker om functiewisselingen van gebruikers met speciale bevoegdheden bij te houden en aan te passen;
- Fysieke toegangsbeheersing: ongeautoriseerde fysieke toegang tot IoT/ICS/SCADA-apparatuur en locaties met als gevolg dat er een toename is van: kwaadaardige software en aanpassingen of kopiëren van software. Toegang tot het besturingsnetwerk. Diefstal of vernieling van apparatuur. Toevoegen van ongeautoriseerde (Shadow IT) om netwerkverkeer te onderscheppen en herzenden;
- Audit, analyse en rapporten: zonder een geformaliseerde geautoriseerde audit of review van logging van het systeem blijven ongeautoriseerde gebruikers en applicaties onzichtbaar;
- Toegangsbeheer: gecompromitteerde en onveilige communicatie van toegangsgegevens waardoor ongeautoriseerde toegang wordt verkregen.

Een ander niet te onderschatten aandachtpunt voor gemeenten is dat er waarschijnlijk al IoT aanwezig is binnen de infrastructuur maar dat men dit nog niet weet. Het is zaak om IoT-assets net als IT-assets te onderkennen en te registreren, inclusief eigenaarschap.

3.1. IoT Kenmerken en zwakheden

IoT apparaten zijn divers, van groot tot klein, van consumenten IoT tot geavanceerde systemen. IoT systemen vragen een andere aanpak dan standaard ICT-componenten in de infrastructuur van de gemeente. De IoT systemen worden gemaakt voor specifieke taken. Vaak zit er een speciaal operating systeem in, en omdat het een gespecialiseerd operating systemen is, zijn ze vaak moeilijk te updaten. Iets dat zeker niet kan met de standaard kantoorautomatisering tools.

IoT systemen hebben vaak geen ingebouwde firewall of andere beveiligingsfuncties die ze beschermt tegen aanvallers. Hier onder de belangrijkste kenmerken en bijbehorende zwakheden van IoT systemen.

Massaproductie en eigendomssoftware (propriëtair OS)

Als er een zwakheid gevonden wordt in een IoT apparaat dan zijn alle vergelijkbare IoT apparaten kwetsbaar. Vaak zijn patches en updates moeilijk te vinden of technisch helemaal niet mogelijk. Het risico hiervan is wel afhankelijk van het soort IoT en de inzet ervan.

Security by obscurity

Security by obscurity betekent hier dat men een (IoT) apparaat maakt waarbij vooraf geen openheid is over ontwikkelingsmethode en de broncode. De gesloten ontwikkeling en gesloten testen (als die al plaatsvinden) maken controle onmogelijk. Het gevolg is dat ingebouwde fouten en achterdeurtjes pas ontdekt worden nadat het systeem in productie is.

Geen hardening

Hoewel hier apart genoemd is het niet “hardenen” van het IoT systeem een security by design fout. Er worden onnodig systeemfuncties en poorten actief gelaten. Dit wordt niet opgemerkt bij testen, of dit wordt voor het testen opengezet en daarna niet gesloten. Hierdoor nemen de aanvalsmogelijkheden toe. Onder hardening valt ook het tegengaan van gebruik van standaard wachtwoorden en het sluiten van soms aanwezige achterdeurtjes. Bovendien draaien processen doorgaans met te veel rechten. Het afvangen hiervan valt ook onder hardening.

Zeer lang (operationeel) gebruik

IoT systemen die nu gebouwd worden kunnen als apparaat zeer lang in gebruik zijn. Een gevolg hiervan is dat het aantal gevonden zwakheden in de oude software toeneemt, en de reparatie mogelijkheid neemt af omdat het onderhoud op het oude systeem duurder wordt. Daarnaast mag ook fysiek onderhoud aan IoT systemen niet vergeten worden om die lange levensduur ook te garanderen.

Eigen protocollen

IoT apparaten communiceren middels een veelheid aan kanalen en protocollen. Dit betekent ook een toename in aanvalsmogelijkheden waarbij zwakheden worden uitgebuit. Dit kunnen ook zwakheden zijn in gestandaardiseerde protocollen waar gebruik van gemaakt wordt.

Toegang tot devices

De locatie is niet direct een eigenschap van IoT apparaten zelf, maar inzet buiten gecontroleerde infrastructuur betekent dat de (fysieke) toegangsbeveiliging doorgaans minder goed te regelen is.

Ontbreken van security by design

Een vooraf ingebouwde onveiligheid kan worden veroorzaakt door het niet toepassen van security by design. Beveiliging wordt niet vanaf de ontwerpfase meegenomen door de fabrikant. Voorbeelden hiervan zijn:

- Processen draaien met te veel of te hoge rechten, het laagste privilege principe wordt niet toegepast. Het gevolg van een simpele hack is dan ook dat de hacker direct hoge toegangsrechten krijgt. Vaak wordt dan ook nog de user "root" toegestaan.
- Het gebruiken van verouderde bibliotheken of verouderde hardware waardoor zwakheden ingebouwd worden zoals: software zoals Wi-Fi bibliotheken met gebreken en onveilige functies, geen beveiligde opslag van sleutelmateriaal en wachtwoorden. Gebruiken van verouderde chip ontwerpen omdat die nou eenmaal goedkoop en makkelijk te krijgen zijn.
- Geen ontwikkelstandaarden gebruiken en nauwelijks of helemaal niet testen; software niet tekenen en dit ook niet controleren, hierdoor kan een aanvaller eigen software ervoor in de plaats zetten. Kijk hiervoor bijvoorbeeld naar Grip op SSD [3]
- Het niet hanteren van PKI standaarden zoals het controleren of certificaten nog wel vertrouwd zijn. Het niet valideren van SSL certificaten waardoor MITM aanvallen mogelijk worden.

3 https://www.cip-overheid.nl/category/producten/secure-software

- Beveiligingsmaatregelen moeten ook geïsoleerd blijven werken. Het zou kunnen gebeuren dat een IoT-apparaat door uitval van connectie en/of bepaalde componenten, geïsoleerd raakt. Veiligheidsmaatregelen moeten blijven werken (nooit falen als de connectiviteit verbroken is.

Het ontbreken van privacy by design

Privacy by design wil zeggen dat al bij het ontwerp van informatiesystemen privacy verhogende maatregelen worden toegepast. Er zijn voldoende voorbeelden te geven van het feit dat dit niet standaard gebeurt (zie onder IoT als afluisterapparaat). Het IoT device zelf veroorzaakt dan een privacy probleem. Daarnaast is het zo dat IoT op veel manieren kan worden ingezet, denk bijvoorbeeld aan draadloze en draagbare IoT (wearables) die weer verbonden kan worden met transport zoals auto's en ook infrastructuur. Denk hier ook aan thermostaten, lampen, smart-Tv's en allerlei andere IoT apparaten. Hierdoor ontstaat een privacygevoelig beeld van mensen dat ontstaat uit wat men doet en wanneer. Op basis van de verzamelde informatie wordt profiling mogelijk. Tel daarbij op dat dit soort informatie ergens in "Clouds" verstopt zit waarvan de eindgebruiker geen idee heeft en waarvan ook niet bekend is hoe het beveiligd is. Het is te verwachten dat deze vorm van privacy gevoeligheid en bijbehorende risico's alleen maar zal toenemen met de toename van IoT in onze maatschappij. Het ontbreken van privacy by design levert risico's op voor de eindgebruiker maar ook voor de leveranciers. Zodra de verzamelde gegevens van IoT persoonsgegevens zijn (bijvoorbeeld kentekenregistratie), is ook de AVG van toepassing.

Geen updates meer

De leverancier kan besluiten geen updates meer uit te brengen, daarmee wordt op termijn het IoT systeem kwetsbaar als er zwakheden gevonden worden.

3.2. Wat kunnen hackers en wat gebeurt er nu al?

Met de toename van de IoT nemen ook IoT bedreigingen toe. De IoT bedreigingen van de apparaten zelf kunnen er toe leiden dat IoT iets anders gaat doen dan dat waarvoor de IoT is bedacht. Daarnaast kunnen er ook bedreigingen zijn waarbij IoT datgene doet waarvoor het is bedacht alleen gebeurt het op een manier die niet zo bedoeld was. Hieronder staan enkele voorbeelden van waargenomen incidenten die zijn opgetreden, die bovenstaande nog duidelijker maken.

Misbruik van de IoT actuatoren of de regelsoftware

IoT actuatoren kunnen zo gemanipuleerd worden dat ze onjuiste waarden als juist weergeven, of dat de waarden door de aansturingssoftware te wijzigen worden. Hierdoor wordt de sabotage niet opgemerkt en kan een systeem buiten de limieten gaan draaien en kapot gaan. Stuxnet[4] is hier een voorbeeld van.

4 https://nl.wikipedia.org/wiki/Stuxnet

IoT en botnets

Eind 2016 is er een omvangrijk botnet gevonden dat bestaat uit IP beveiligingscamera's die geïnfecteerd worden door zwakheden in de besturing van de camera's. Na infectie gaan ze deel gaan uitmaken van het botnet[5]. De malware gaat zelf op zoek op Internet en gevonden apparatuur die kwetsbaar is wordt besmet. Er ontstaat zo een groot netwerk waarmee bijvoorbeeld DDOS aanvallen worden uitgevoerd. Deze botnets worden in een nieuwe variant ook gebruikt voor het minen van crypto currency.

IoT als afluisterapparaat

IoT apparaten zijn/bevatten sensoren. Ook microfoons en camera's zijn sensoren. Deze microfoons zijn vaak bedoeld om opdrachten aan te nemen. Denk hierbij aan bijvoorbeeld smart Tv's of microfoons in kinderspeelgoed (luisterende en sprekende poppen). IoT-apparaten hebben niet veel rekenkracht dus verzamelde input moet ergens anders worden verwerkt tot opdrachten voor het apparaat of de eindgebruiker. IoT devices slaan vaak informatie op in de Cloud. Als dat niet de bedoeling is en de informatie is gevoelig dan is dat een lek. Een ander voorbeeld zijn trackingsystemen waar locatiegegevens (persoonsgegevens) en andere informatie naar de Cloud van de leverancier ergens buiten de EU/EER worden verzonden, die voor derden toegankelijk zijn.[6]

IoT ransomware

IoT ransomware is een scenario waar al wel over wordt gesproken (het is zeker mogelijk), maar waar nog geen bewijs voor is. IoT kan op verschillende manieren onderdeel worden van ransomware. Ten eerste kan de toegang ontzegd worden door de gijzeling van het IoT apparaat zelf. Ook kan via IoT apparaten de data die weggeschreven wordt ontoegankelijk worden gemaakt door de ransomware. Doordat er veel IoT apparaten in de omgeving zijn, is herbesmetting snel gebeurd. Hiermee wordt het IoT landschap voor een deel onbruikbaar en dit raakt dit diensten die er afhankelijk van zijn.

3.3. Privacy en data

Ook voor het privacyrisico dat ontstaat in relatie tot IoT wordt gewaarschuwd. Het afluisteren van de omgeving of het hacken van camera's zijn eerder genoemde voorbeelden hier van. Daarnaast hebben de meeste IoT toepassingen een vorm van Cloud opslag waarvan niet helemaal duidelijk is waar de opslag van de gegevens zich bevindt, wie erbij kan en wat er verder mee gedaan wordt. Met de toename van IoT wordt ook de kans groter dat IoT data die verzameld is voor een bepaald doel door een aanbieder wordt doorverkocht zonder dat de gebruiker dit weet. De opslag van IoT data in backend big-data systemen zorgt voor nieuwe uitdagingen waar gebruikers en beheerders zich van bewust moeten zijn. Met IoT kan op grote schaal privacy gevoelige data worden verzameld die ook passend beveiligd moet worden. Daarnaast moet deze persoonsgegevens verzameling ook geregistreerd worden in het register van verwerkingen van de gemeente.

5 https://en.wikipedia.org/wiki/Mirai_(malware)

6 https://www.security.nl/posting/544632/Kwetsbaarheden+in+online+diensten+voor+gps-trackers

4. IoT Beveiliging

IoT devices en de benodigde infrastructuur hebben specifieke aandachtspunten waar rekening mee gehouden moet worden. In het vorige hoofdstuk zijn de kenmerken en zwakheden uiteengezet. In dit hoofdstuk worden de beveiligingsprincipes uiteengezet. Deze principes zijn voor een deel afkomstig uit de baseline security recommendations van ENISA.[7] Gemeenten die een smart city willen zijn moeten zich bewust zijn van de uitdagingen die IoT met zich meebrengt en hier al in een vroeg stadium over nadenken. Dit kan lastig zijn omdat initiatieven zich veelal buiten het zicht van de CISO of de FG afspelen. Achteraf inbouwen van beveiliging is lastig. Daarnaast willen collega's waarschijnlijk liever niet horen dat een lopend experiment toch nog wat beveiligings- en privacy aandachtspuntjes heeft. Wat ook een rol speelt is de snelheid van ontwikkelen en de veranderingen in de technologie die dat met zich meebrengt. Tel daarbij op dat ontwikkelaars en bedrijven snel naar de markt willen met hun product of dienst. Daardoor staan het inbouwen van beveiliging en het testen en de privacy onder druk.

De BIG bevat in de basis ook aandachtpunten voor IoT beveiliging. De BIG is toepasbaar op de ICT van de gemeente maar ook toepasbaar op IoT en OT (SCADA). De basis voor de BIG is immers gebaseerd op de NEN/ISO 27002 norm welke omgeving en organisatie neutraal is. Er is ook een beveiligingsnorm voor industriële automatisering de EIC 62443.[8] Daarnaast zijn er specifieke IoT beveiligingsaandachtpunten in ontwikkeling van onder andere de OWASP.[9]

4.1. Basisbeveiligingsprincipes voor IoT

De basis op orde
Gemeenten die met IoT aan de slag gaan moeten de volgende basis beveiligings- en beheerprocessen op orde hebben om goed met IoT te kunnen omgaan[10], deze processen zijn:

- Patchmanagement
- Incidentmanagement
- Configuratiemanagement
- Changemanagement

Passende beveiliging
IoT moet afhankelijk van de context waarin het gebruikt wordt passend beveiligd worden. Risico is immers ook context afhankelijk. Bepaal de beveiligingseisen op basis van de context en scenario's met betrekking tot het gebruik van de IoT. Dit geldt zowel voor de IoT devices, de aansturing en de infrastructuur.

Eigenaarschap
Ieder IoT systeem heeft één of meerdere eigenaren die verantwoordelijk zijn voor de veiligheid en privacy en werking van het systeem. Sensoren, actuatoren en regelsystemen kunnen binnen een IoT systeem in eigendom zijn van andere partijen, dit maakt IoT beveiligen complex.

Isolatie
IoT en ook de eerder genoemde SCADA moeten in principe als onveilig worden beschouwd, in de afgelopen jaren is dit door incidenten al meermaals duidelijk geworden. IoT en kantoor automatisering behoren niet gemixt te worden, dat levert risico's op voor de gemeentelijke informatievoorziening. Dat betekent dat alle IoT en OT geïsoleerd moet worden van de gemeentelijke ICT en omgekeerd.

7 Zie ook de IoT baseline van ENISA: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

8 Zie link: https://www.nen.nl/NEN-Shop/Nieuwsberichten-Security/Industrieel-Platform-Cyber-Security-belangrijke-aanvulling-op-IEC-62443.htm

9 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

10 Zie ook: www.informatiebeveiligingsdienst/vdw

Geteste IoT
IoT moet worden getest. Bij voorkeur wordt gecertificeerde IoT apparatuur gebruikt. Dit laatste is nog niet mogelijk. Er is al enige tijd een discussie gaande over de rol van de overheid in het veilig krijgen van IoT en het verlagen van de risico's en wat de rol van de industrie hierin is[11]. Daarnaast gaan de IoT ontwikkelingen zo snel dat het lijkt alsof men hier achter de feiten aan blijft lopen.[12] Overigens wil niet zeggen dat gecertificeerde IoT betekent dat het voor altijd veilig is, IoT systemen kunnen ook gedurende de levensduur kwetsbaar worden als gevolg van nieuw ontdekte kwetsbaarheden. Laat een netwerk- en penetratietest uitvoeren.

Patchen
Voor kantoor automatisering komen regelmatig leveranciers patches uit om zwakheden te verhelpen, dit is niet direct gemeengoed voor IoT (en ook SCADA). Maar IoT systemen hebben ook werkstations en servers nodig die dan wel geïsoleerd zijn in het IoT netwerk, ze dienen ook geüpdatet te worden. De eigenaar en beheerder van de IoT moeten zich ervan bewust zijn dat patchen van de kantoorautomatisering ook betekent dat bijvoorbeeld Windows Pc's en netwerkapparatuur in andere omgevingen updates nodig hebben.

Monitoring
IoT moet net als ICT worden gemonitord om zicht te krijgen en te houden op de beveiligingsstatus van de IoT. Dit monitoren kan het beste gebeuren door monitoring van het netwerkverkeer.

Sabotage detectie
Sabotagedetectie is het vermogen van een apparaat om te detecteren dat een actieve poging wordt ondernomen (of aan de gang is) om de integriteit van het apparaat, of de met het apparaat verbonden gegevens, in gevaar te brengen, Sabotage detectie kan het mogelijk maken dat gepaste maatregelen genomen kunnen worden om de dreiging tegen te gaan. IoT apparaten moeten gedurende hun levenscyclus integer blijven om er van verzekerd te zijn dat men kan blijven vertrouwen op de werking van het apparaat en dat de juiste informatie wordt verkregen. Sabotage detectie kan worden toegepast op hard- en software.

Onderhoud en beheer
IoT apparatuur moet beheerd en onderhouden worden. Vanuit beheer moet er ook aandacht zijn voor wachtwoord management en updates. Bedenk ook dat als er door onderhoud of updates IoT systemen allemaal tegelijkertijd weer online komen dat het hele IoT ecosysteem hier wel tegen moet kunnen en dat niet een vorm van DDoS wordt veroorzaakt.

Beveiligingsmogelijkheden gedurende gehele levenscyclus
IoT-systeemontwerpers moeten eisen stellen aan de IoT-apparaten m.b.t. beveiligingsmogelijkheden gedurende de gehele levensduur, zoals bijvoorbeeld voorwaartse compatibele beveiligingsfuncties. IoT-systemen moeten in staat zijn om (als ze ouder te worden) nog steeds aan te passen aan meest recente veiligheidsproblemen. Nieuwe versleuteling, vooruitgang in protocollen, nieuwe aanvalstechnieken moeten kunnen worden weerstaan en dat vereist dat IoT-systemen jarenlang na de implementatie in staat zijn om opkomende veiligheidsproblemen aan te pakken.

Hardening
Zorg ervoor dat IoT-componenten worden beperkt tot de strikt benodigde functionaliteit (minimale levensvatbare functie) is om kwetsbaarheden / aanvallen te verminderen. Ongebruikte poorten en protocollen moeten worden uitgeschakeld en onnodige ondersteunende software moet worden verwijderd of uitgeschakeld. Zorg ervoor dat u onderdelen van derden bijhoudt en zo mogelijk laat verwijderen.

11 https://www.tweedekamer.nl/downloads/document?id=901b45ee-4073-4c90-8f29-0325399cfb31&title=Motie%20van%20het%20lid%20Paternotte%20c.s.%20over%20certificering%20van%20op%20internet%20aangesloten%20apparaten.pdf

12 https://www.cybersecurityraad.nl/010_Actueel/iot-toepassingen-vormen-bedreiging-voor-veiligheid-en-privacy.aspx

1:1 Authenticatie
Realiseer dat IoT niet een traditioneel één op één authenticatie model van gebruikers naar applicaties volgt. Elk onderdeel kan meer dan één gebruiker hebben en een gebruiker kan met meerdere componenten werken. Verschillende gebruikers kunnen toegang hebben tot verschillende gegevens of mogelijkheden op een enkel apparaat, en één gebruiker kan verschillende rechten op meerdere apparaten hebben. Meerdere apparaten kunnen machtigingen voor gebruikers met één gebruikersaccount, enzovoort. Zorg ervoor dat het IoT-systeem complexe trust- (vertrouwens-) en authenticatie schema's kan verwerken.

Datalek overdracht bij IoT component
IoT componenten kunnen worden verkocht of overgebracht naar derden tijdens hun levensduur. Neem dit mee in het beveiligingsplan en zorg dat IoT-systemen op dat moment de gegevens afschermen, vooraf verwijderd worden of gegevens isoleren om een veilige eigendomsoverdracht mogelijk te maken, zelfs als een onderdeel wordt verkocht of overgedragen.

Uniform gegevens beschermen
Besteed aandacht aan de volledige beveiliging van de dataketen end-to-end om ervoor te zorgen dat encryptie uniform en adequaat wordt toegepast om de beveiliging te waarborgen Gegevenscodering beschermt alleen versleuteld dataverkeer. Gegevens die over een gecodeerde link worden verzonden, kunnen nog steeds blootgesteld worden aan gevaar (bijvoorbeeld een cyberaanval) op elk punt dat niet ongecodeerd is, zoals bijvoorbeeld het moment voorafgaand aan versleuteling, na decryptie, en alle andere communicatiewegen die de codering niet afdwingen. Encryptie is niet totaal in de dataketen aanwezig. Wees er ook van bewust dat metadata over gecodeerde gegevens waardevolle informatie kan geven aan aanvallers, bescherm ook metadata.

Maak gebruik van open standaarden voor IoT

- Token methodiek gebaseerd op Security Assertion Markup Language (SAML) en eXtensible Access Control Markup Language (XACML) standaarden
- OpenIoT support role-based authentication and authorization
- OAuth2.0 (Open Authorisation)
- OpenID

4.2. IoT Beleid

De gemeente moet aanvullend IoT (beveiligings) beleid ontwikkeld en uitgedragen hebben waarin duidelijk de uitgangspunten staan voor het gebruik van IoT binnen de gemeente. Dit beleid moet ervoor zorgen dat voor IoT initiatieven de juiste dingen gedaan worden om te voorkomen dat beveiliging of privacy in het geding komt.

Security by design regels

De volgende beleidsuitspraken zijn van belang bij het gebruik van IoT.

Het hele IoT systeem wordt passend beveiligd gedurende alle fases van het systeem: ontwikkeling, bouw, inkoop/verwerving, beheer en afvoer. Hiervoor wordt minimaal een baselinetoets en indien nodig een risicoanalyse uitgevoerd. Die passende beveiliging bestaat uit een samenhangende set van organisatorische, procedurele en technische maatregelen.

- Beveiliging moet dusdanig worden gebruikt dat de veiligheid (safety) niet in gevaar komt.
- Stroombesparingsmaatregelen mogen niet zorgen voor lagere veiligheid en minder beveiliging en toename van risico.
- IoT wordt uitsluitend geïsoleerd ingezet van het ICT netwerk en verschillende IoT systemen worden geïsoleerd van elkaar.
- Er wordt uitsluitend geteste IoT gebruikt en de leverancier zorgt ervoor dat de IoT testbaar is.
- Voor IoT systemen worden zwakheden scans, netwerk en penetratietesten uitgevoerd en periodiek of bij grote wijzigingen herhaald.
- IoT systemen worden gemonitord.

Privacy

IoT systemen kunnen ook persoonsgegevens verzamelen en doorzenden, denk aan identificerende gegevens, biometrie, audio en video en resultaten van verwerkingen. Voor ieder IoT systeem wordt een pre-PIA scan uitgevoerd en zo nodig een DPIA uitgevoerd. De privacy maatregelen worden ingevoerd voordat het IoT systeem in gebruik genomen wordt.

Beheersing / Inkoop / verwerving

Maak inkoop/verwerving bewust van de noodzaak voor het stellen van informatiebeveiligingseisen in ieder aanschaftraject van IoT, functies met embedded ICT. Het is momenteel praktijk dat IoT vooral binnenkomt buiten de formeel geregelde aanbestedingstrajecten om!

4.3. Organisatie en proces

End of life

- IoT zal net als ICT ook een einde van de gebruiksfase kennen. Er moet een plan zijn om hier goed mee om te gaan. Daarnaast is het belangrijk om goed bij te houden waar IoT allemaal is, van ieder device moet men weten waar het is.
- Monitor de performance van de IoT apparaten zodat afwijkingen kunnen worden onderkend.
- Schoon betreffende apparaten van gevoelige informatie bij het uit gebruik nemen voor het afvoeren.

Bewezen technologie

Gebruik alleen bewezen technologie, dus bekende protocollen en versleutelingsalgoritmen, vermijd het gebruik van propriëtaire oplossingen[13] van de leverancier. De hoeveelheid aan keuzes van technologie is divers en afhankelijk van de soort IoT, het doel dat men wil bereiken en de vereiste connectiviteit. Het is niet eenvoudig om hier een eenduidig antwoord op te geven. [14] Kijk in ieder geval naar open standaarden.

Vulnerability management en incidentmanagement

- Zorg voor een ingericht incident management proces, en als dat er al is zorg er dan voor dat dit proces ook ingericht is voor IoT incidenten.
- Zorg voor een ingericht Asset en Configuratiemanagement.
- Ken de componenten van het IoT device / landschap. Veelal worden diverse libraries van derden gebruikt waar ook kwetsbaarheidsmeldingen voor bestaan. Dus ontleed het tot op component niveau (chips, besturingssysteem, software, protocollen).
- Zorg ervoor dat de IoT ook opgenomen wordt in informatie die de IBD van de gemeente krijgt zoals hardware en software die in gebruik zijn en externe IP-adressen (stap 3 en 4 van het aansluitproces). Op die manier kan de gemeente ook gericht informatie krijgen bij meldingen die anderen doen over de gebruikte IoT.
- Richt een Coordinated Vulnerability Disclosure procedure in voor het melden van IoT zwakheden en als er al een Coordinated Vulnerability Disclosure proces is, laat dan de IoT hier ook onder vallen.
- Deel gevonden zwakheden met de IBD.

Awareness en training

- Zorg voor goed opgeleid personeel op het gebied van informatieveiligheid en privacy.
- Geef op maat gemaakte bewustwordingstrainingen en geef aandacht aan specifieke aandachtspunten met betrekking tot IoT risico's en maatregelen.

13 https://nl.wikipedia.org/wiki/Propri%C3%ABtaire_software

14 https://www.postscapes.com/internet-of-things-protocols/

Derden

- Als er derden betrokken zijn bij het IoT systeem, maak dan afspraken over de beschermingsmaatregelen voor het verwerken van gegevens .
- Als persoonsgegevens in het geding zijn, zorg dan voor toestemming van de betrokkenen en sluit een verwerkersovereenkomst af.[15]
- Maak alleen gebruik van IoT hardware en software als de ontwikkelaars en leveranciers kunnen aantonen dat security is meegenomen in hun productieproces.

4.4. Overige en technische maatregelen

De overige en technische maatregelen voor IoT devices en systemen zijn belangrijk om te voorkomen dat zwakheden kunnen ontstaan of worden uitgebuit. Veel van de hier genoemde maatregelen zijn voor de bescherming van IoT apparaten zelf en zijn niet door gemeenten te realiseren maar dienen meegenomen te worden in de eisen naar leveranciers die IoT systemen en diensten leveren.

Hardware beveiliging

- Maak gebruik van IoT hardware waar beveiliging is ingebakken in de hardware, bijvoorbeeld door gebruik te maken van speciale beveiligingsfeatures in chips, processors en HSM (Hardware security module). Hierdoor kan er een vertrouwde opslag en transport plaatsvinden van sleutelmateriaal en apparaat instellingen. Dit zorgt er voor dat onbevoegde toegang zeer moeilijk is tot dat materiaal en instellingen door derden.

integriteits management en vertrouwen

- IoT systemen moeten vanaf het bootproces veiligheid garanderen voordat het laden van software kan plaatsvinden, dit vereist wel hardware ondersteuning.
- Software/code moet digitaal zijn ondertekend zodat de integriteit gewaarborgd blijft en manipulatie kan worden ontdekt voor, tijdens en na het starten van de software.
- Gebruik alleen toegestane vertrouwde en geteste software.
- Zorg ervoor dat een IoT systeem kan herstarten naar een vooraf vastgestelde beveiligde bekende configuratie als er wordt gepoogd binnen te dringen of als een upgrade niet geslaagd is.
- Bij voorkeur zijn IoT devices ‘stateless’ (dus zelf geen opslag/state hebben) ze kunnen dan volledig worden gereset.

Sterke basisbeveiliging en privacy

- Alle mogelijke beveiligingssettings moeten standaard aan staan, en het IoT apparaat/systeem moet standaard gehardened zijn zodat ongebruikte functies niet beschikbaar zijn voor kwaadwillenden.
- Probeer ieder device van een eigen sterk wachtwoord te voorzien, het mag niet mogelijk zijn meerdere IoT devices te benaderen met hetzelfde wachtwoord.

Data bescherming en compliancy

- Voldoe bij iedere verwerking van persoonsgegevens aan de AVG.
- Zorg ervoor dat persoonlijke gegevens worden gebruikt voor de gespecificeerde doelen waarvoor ze zijn verzameld, en dat verdere verwerking van persoonlijke gegevens passend is bij die doelen en dat de betrokkenen goed op de hoogte zijn.
- Minimaliseer de verzamelde en bewaarde gegevens.
- Gebruikers van IoT producten en diensten moeten hun rechten op informatie, toegang, verwijdering, rectificatie, gegevensportabiliteit, beperking van verwerking, bezwaren tegen verwerking en hun recht om niet te worden geëvalueerd kunnen uitoefenen op basis van geautomatiseerde verwerking.

15 https://www.informatiebeveiligingsdienst.nl/product/factsheet-verwerkersovereenkomsten/

Systeem beveiliging

- Ontwerp en implementeer IoT met in gedachten dat er grootschalige uitval, andere onbeschikbaarheid of compromittering, al dan niet door kwaadwillenden, zou kunnen optreden waardoor onacceptabel risico zou kunnen ontstaan voor de omgeving en mensen.
- Implementeer mechanismes voor zelf-diagnose en automatisch herstel (zoals de eerder genoemde reboot naar een beveiligde status (secure state) om het mogelijk te maken dat er hersteld kan worden van een fout of compromittering).
- Ontwerp en implementeer IoT dusdanig dat essentiële functionaliteit blijft werken, ook als het netwerk even niet beschikbaar is en doe dit ook voor centrale op Cloud gebaseerde systemen. Uitval van een deel mag niet leiden tot uitval van het hele systeem.
- Stel vast wat bewaartermijnen van de bewaarde gegevens zijn.

Secure software en firmware updates

- IoT bevat software en dat geldt natuurlijk voor het hele IoT systeem. Zorg ervoor dat het systeem vanaf een beveiligde server over een beveiligde verbinding veilige software updates of patches kan ontvangen. Met veilige software wordt bedoeld dat de software is gesigned en het geen achterdeurtjes of hardcoded account gegevens en wachtwoorden bevat. Het IoT apparaat moet in staat zijn te verifiëren dat de update klopt door het controleren van de digitale handtekening, certificaten en de certificaat keten voordat de update start. Gebruik bij voorkeur geen IoT devices die niet kunnen worden geüpdatet.
- Maak waar mogelijk gebruik van een automatische firmware update functie. Zorg er wel voor dat updates eerst worden getest om te voorkomen dat een systeem onbeschikbaar wordt.
- Firmware updates mogen geen gebruikers configuraties en data overschrijven, niet de security aantasten of een inbreuk op de privacy veroorzaken zonder notificatie aan de eindgebruiker.

Authenticatie

- Autorisatie en authenticatie moet worden ontworpen en toegepast op basis van het systeem risico, dit is afhankelijk van het gebruik en de soort IoT. Voer eventueel een risicoanalyse uit om het belang van het systeem vooraf vast te stellen.
- Bij installatie moeten standaard wachtwoorden en gebruikersidentiteiten aangepast worden en er moet een mechanisme zijn dat de sterkte van de gekozen wachtwoorden valideert.
- Authenticatie voor toegang moet gebruik maken van sterke wachtwoorden of een PIN en indien mogelijk gebruik maken van 2-factor authenticatie.
- Authenticatie gegevens moeten worden geïmplementeerd volgens geldende best practices, denk hier aan het hashen en salten en type versleuteling.
- Foutieve inlogpogingen worden gelogd, en het aantal inlogpogingen wordt beperkt.
- Wachtwoord en account herstel en reset mechanismes mogen niet aan een aanvaller verraden wat voor account info nodig is en of iets een bestaand account is.

Autorisatie

- Beperk de acties die voor een bepaald systeem zijn toegestaan door het implementeren van fijnmazige autorisatiemechanismen en het gebruik van het Principle of Least Privilege (POLP): applicaties moeten werken op het laagst mogelijke niveau.
- Apparaat firmware moet zijn ontworpen om bevoorrechte code, processen en gegevens te isoleren van delen van de firmware die geen toegang tot deze firmware nodig hebben. Apparaat hardware moet isolatieconcepten bieden om te voorkomen dat onbevoegden toegang krijgen tot beveiligingsgevoelige code.

Access control en fysieke veiligheid

- Gegevensintegriteit en vertrouwelijkheid moeten worden afgedwongen door toegangscontroles. Wanneer het onderwerp dat toegang vraagt geautoriseerd is om toegang te krijgen tot bepaalde processen, is het noodzakelijk om het gedefinieerde beveiligingsbeleid af te dwingen.
- Zorg voor een op context gebaseerde beveiliging en privacy die verschillende niveaus van belangrijkheid weerspiegelt.
- Maatregelen voor sabotagebeveiliging en detectie. Detectie en reactie op hardware matige sabotage mogen niet afhankelijk zijn van netwerkconnectiviteit.
- Zorg ervoor dat het apparaat niet gemakkelijk kan worden gedemonteerd en dat het gegevensopslagmedium in rust is gecodeerd en niet eenvoudig kan worden verwijderd.
- Zorg ervoor dat apparaten alleen de essentiële fysieke externe poorten (zoals USB en / of voeding) bevatten die nodig zijn voor hun werking en dat de test / debug-modi veilig ontworpen en gebouwd zijn, zodat ze niet kunnen worden gebruikt om kwaadwillig toegang te krijgen tot de apparaten. Vergrendel in het algemeen fysieke poorten naar alleen vertrouwde verbindingen.

Versleuteling

- Zorg voor een correct en effectief gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van gegevens en informatie (inclusief controleboodschappen), onderweg en in rust in opslag te beschermen.
- Zorg voor de juiste selectie van standaard en sterke versleutelingsalgoritmen en sterke sleutels en schakel onveilige protocollen uit. Controleer de robuustheid van de implementatie.
- Richt sleutelbeheer in voor het beheren van cryptografisch materiaal.
- Bouw apparaten om compatibel te zijn met lichtgewicht codering en beveiligingstechnieken.

Veilige en vertrouwde verbindingen

- Garandeer de verschillende veiligheidsaspecten - vertrouwelijkheid (privacy), integriteit, beschikbaarheid en authenticiteit - van de doorgestuurde informatie op de netwerken of opgeslagen in de IoT-toepassing of in de Cloud.
- Zorg ervoor dat de communicatiebeveiliging wordt geboden met behulp van geavanceerde, gestandaardiseerde (open) beveiligingsprotocollen, zoals TLS voor codering.
- Zorg ervoor dat inloggegevens niet onbeschermd worden getransporteerd in intern of extern netwerkverkeer.
- Waarborg de authenticiteit van gegevens om betrouwbare uitwisselingen van gegevens verzending en gegevensontvangst mogelijk te maken. Gegevens moeten altijd worden ondertekend waar en wanneer het wordt vastgelegd en opgeslagen.
- Vertrouw de ontvangen gegevens niet en verifieer altijd alle connecties. Ontdek, identificeer en verifieer / authentiseer de apparaten die op het netwerk zijn aangesloten voordat het vertrouwen kan worden gevestigd en bewaar hun integriteit voor betrouwbare oplossingen en services.
- IoT-apparaten moeten eerder beperkend dan toegeeflijk zijn in communicatie.
- Maak opzettelijke en bedoelde verbindingen. Voorkom ongeautoriseerde verbindingen met het apparaat of andere apparaten waarmee het IoT device is verbonden, op alle niveaus van de protocollen.
- Schakel specifieke poorten en/of netwerkverbindingen uit voor selectieve connectiviteit.
- Snelheidsbeperking: controleer en beheers het netwerkverkeer om het risico van geautomatiseerde aanvallen te verminderen.

Veilige koppelvlakken en netwerkdiensten

- Risicosegmentatie van netwerken: splits netwerkelementen in afzonderlijke componenten en/of segmenten om beveiligingsinbreuken te isoleren en het totale risico te minimaliseren.
- Protocollen moeten zo worden ontworpen dat, als een enkel apparaat is aangetast, dit niet van invloed is op de hele set.
- Vermijd de gebruik en levering van dezelfde geheime sleutel in een volledige IoT productfamilie, omdat het compromitteren van een enkel IoT apparaat voldoende is om de rest van de IoT productfamilie kwetsbaar te maken.
- Zorg ervoor dat alleen de echt benodigde netwerk poorten zichtbaar en beschikbaar zijn.
- Implementeer een DDoS-resistente en Load Balanced-infrastructuur.
- Zorg ervoor dat web interfaces de gebruikerssessie volledig versleutelen, van het apparaat naar de backend- en Cloud services, en dat ze niet gevoelig zijn voor aanvallen zoals genoemd in de OWASP top 10[16].

Veilige invoer en uitvoer

Maak gebruik van data invoer validatie en output controle.

Logging

Implementeer een loggingsysteem dat gebeurtenissen registreert met betrekking tot gebruikersauthenticatie, beheer van accounts en toegangsrechten, wijzigingen in beveiligingsregels en de werking van het systeem. Logboeken moeten worden bewaard op duurzame opslag en kunnen worden opgehaald via geverifieerde geauthentiseerde verbindingen.

Monitoring en auditing

Implementeer standaard systeem logging en monitoring om het gedrag van het apparaat te verifiëren, om malware te detecteren en integriteitsfouten te ontdekken. Neem waar mogelijk IoT systemen op in logmonitoring systemen of een SIEM (Security information & event management).

Voer periodieke audits uit en evalueer deze beveiligingscontroles om ervoor te zorgen dat de controles effectief zijn.

Voer minstens jaarlijks penetratietests uit of doe dit bij grote wijzigingen.

[16] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Bijlage 1 Stappenplan voor de gemeentelijke CISO

De kans is groot dat de CISO binnen de gemeente al te maken heeft met IoT (en SCADA) alleen is men zich hier nog niet bewust van. Dit wordt bijvoorbeeld veroorzaakt door het feit dat IoT-achtige projecten de gemeente binnenkomen via (vak) afdelingen en buiten I&A en buiten de CISO om.

De belangrijkste stappen om IoT (en SCADA) in kaart te brengen op een rijtje:

- Laat IoT en SCADA systemen ook onder de BIG vallen.
- Inventariseer waar IoT en SCADA systemen al voorkomen binnen de gemeente en vergeet niet om te vragen bij de afdeling facilitaire zaken en afdeling ruimtelijke ontwikkeling of vergelijkbaar. (gebouwbeheersing en verkeerslichten).
- IoT systemen moeten worden geregistreerd in een vorm van CMDB en een eigenaar hebben binnen de gemeente.
- Bepaal welke systemen verbonden moeten zijn met het internet.
- Doe voor verbonden IoT en SCADA systemen aanvullende risicoanalyses om maatregelen te bepalen, en doe dat altijd voor een aanbesteding.
- Richt netwerkmonitoring in waarbij ook aandacht moet zijn voor het onderkennen van Shadow IT door middel van een automatische scan.
- Identificeer IoT waar privacyaspecten aan de orde zijn en tref ook hier indien nodig ook aanvullende maatregelen voor.
- Isoleer IoT en SCADA systemen en waar mogelijk de besturing altijd van de kantoorautomatisering.
- Wijs verantwoordelijken aan voor de systemen zelf en de beveiliging ervan.
- Ben ervan als CISO, hiermee wordt bedoeld dat er niet een aparte gemeentelijke IoT CISO moet komen (niet te verwarren met de verantwoordelijkheden van de eigenaar van het systeem). Risico eigenaar is de eigenaar van het IoT ecosysteem, beveiliging is uiteindelijk verantwoordelijkheid van het college en daarmee heeft de CISO het mandaat om IB van deze systemen in beleid af te dwingen.
- Maak en publiceer aanvullend IoT en SCADA beveiligingsbeleid voor de gemeente. Zie hoofdstuk 6 voor een voorbeeld beleid.

INFORMATIE
BEVEILIGINGS
DIENST

it Building
control services

Bijlage 2 Voorbeeld IoT beveiligingsbeleid

Beleidsuitgangspunten IoT-beveiligingsbeleid van gemeente <naam gemeente>

Ten behoeve van een veilige toepassing van IoT binnen de gemeente zijn de volgende beleidsuitgangspunten van belang. Het doel van dit beleid is er voor te zorgen dat IoT toepassingen binnen de gemeente gebruikt kunnen worden en daarbij voldoende waarborgen in te bouwen dat dit op een verantwoorde wijze kan.
De gemeente <naam gemeente> hanteert de volgende beleidsuitgangspunten voor IoT.

Organisatorische uitgangspunten:

1. De gemeente draagt zorg voor het vaststellen van het eigenaarschap van de IoT toepassing, een IoT toepassing zonder eigenaar is niet toegestaan.
2. De eigenaar van de IoT toepassing is verantwoordelijk voor passende technische en organisatorische maatregelen om de risico's te verlagen welke gemoeid zijn met de IoT toepassing door:
    a. Als een IoT toepassing wordt overwogen wordt de CISO in het voortraject ingeschakeld om een eerste inschatting van de risico's te maken.
    b. Als een IoT toepassing wordt overwogen wordt in het voortraject de FG ingeschakeld om vast te stellen of privacy bevorderende maatregelen nodig zijn en of er een DPIA noodzakelijk is.
    c. Voor alle IoT toepassingen wordt een architectuur gemaakt.
3. IoT toepassingen worden niet in gebruik genomen voordat er een risico en indien nodig een privacy assessment is uitgevoerd en de bijbehorende risico verlagende maatregelen zijn geïmplementeerd.
4. De gemeente heeft een actuele registratie van alle IoT toepassingen waar de gemeente verantwoordelijk voor is.
5. IoT toepassingen worden net als ICT-systemen beheerd.
6. Zorg voor ingericht Asset en configuratiemanagement, ook voor IoT.
7. Voordat de IoT toepassing in gebruik wordt genomen is vastgesteld en vastgelegd wat met de data van de IoT toepassing gedaan mag worden en wat niet.
8. Zorg ervoor dat de IoT ook opgenomen wordt in informatie die de IBD van de gemeente krijgt zoals de IP-nummers en hard- en software die in gebruik is. Op die manier kan de gemeente ook gericht informatie krijgen bij meldingen die anderen doen over de gebruikte IoT.

Technische uitgangspunten

1. IoT toepassingen (hard- en software) worden passend beveiligd
2. IoT toepassingen zijn minimaal logisch gescheiden van gemeentelijke ICT-systemen
3. IoT toepassingen worden technisch gemonitord
4. Van IoT die de gemeente gebruikt is bekend uit welke componenten deze bestaat
5. IoT toepassingen worden voor ingebruikname afdiende getest
6. Voor IoT toepassingen worden jaarlijks vulnerabilityscans uitgevoerd

Aldus vastgesteld door burgemeester en wethouders van [gemeente] op [datum],

[Naam. Functie] [Naam. Functie]

_____ _____

Kijk voor meer informatie op:
www.informatiebeveiligingsdienst.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl