

A thin vertical black line is positioned on the left side of the page, extending from the top of the title area to the bottom.

DIGITALE HYGIENE NEDERLAND

JUNI 2018

Juni 2018

Report & Research: Dhr. V.Toms (GDI.Foundation)

Contact info: <https://www.linkedin.com/in/vincenttoms/>

Review: Dhr. R.Spoor (Surfnet) & Dhr. V.Gevers (GDI.Foundation)

Technical scans: Dhr. V.Gevers

Editing & review report: BenRi

Copyright



De tekst, tabellen en illustraties in dit rapport zijn samengesteld door GDI.Foundation en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Nederland. Meer informatie over deze licentie vindt u op <https://creativecommons.org/licenses/by/4.0/deed.nl>

MANAGEMENTSAMENVATTING

Digitalisering creëert over de hele wereld en dus ook binnen Nederland nieuwe kansen en mogelijkheden. Door de afhankelijkheid tussen de digitale wereld en onze reële wereld neemt ook de impact van digitale kwetsbaarheden voor ons dagelijks leven toe. Het afgelopen jaar is gebleken dat misbruik van deze kwetsbaarheden door cyber criminelen is toegenomen.

Maar wat is de status van de digitale hygiëne van Nederland? Hoe kwetsbaar zijn we en wat is de impact hiervan? Op verzoek van NCSC is een onderzoek verricht naar het Nederlandse digitale landschap, het Internet-of-Things (IoT) en de kwetsbaarheden in het Nederlandse digitale landschap.

HOOFDBEVINDINGEN

Het onderzoek geeft een beeld van het digitale landschap van Nederland en haar (toekomstige) kwetsbaarheden. Dit landschap is echter te complex en veelomvattend om deze in de beperkte onderzoeksperiode volledig in kaart te brengen, inclusief al haar kwetsbaarheden.

Uit het onderzoek is gebleken dat de connecties van het Nederlands digitale landschap met het internet divers is en het gebruik van internet groot is. Opvallend is dat bepaalde producten van leveranciers een groot marktaandeel hebben. Een eventuele kwetsbaarheid in één van deze producten en niet tijdig mitigeren van het risico, kan derhalve grote impact hebben voor onze samenleving.

Het verbinden van alles met iedereen d.m.v. IoT & IT gebeurt middels een breed scala aan protocollen en verbindingen. Met de introductie van IoT en de connectiviteit met internet, IT omgeving e/o andere netwerken, ontstaan er nieuwe kansen maar ook nieuwe bedreigingen¹. Denk hierbij bijvoorbeeld aan op internet aangesloten wasmachines, smart watches, smart cities en pacemakers². Alle verbindingen hebben in potentie een kwetsbaarheid die misbruikt kan worden. Daar IoT en IT in elkaars verlengde liggen zal de invloed van een kwetsbaarheid voor de andere keten toenemen³.

Lang niet alle IoT apparaten zijn vanaf het internet te detecteren. Het is dan ook zeer waarschijnlijk dat er nog volop onveilige apparaten zijn, alleen zijn deze niet rechtstreeks te benaderen vanaf het internet. Het aantal gedetecteerde (onveilige) IoT apparaten in Nederland is in relatie met de rest van de wereld nog beperkt. De ontwikkelingen en het gebruik van IoT staan nog in de kinderschoenen, de voordelen zijn groot en het gebruik neemt elke dag toe. De ontwikkelingen m.b.t. Big Data, Cloud en Artificial Intelligence (AI) worden steeds vaker gecombineerd met IoT-data en is grens/continent overstijgend.

Het kunnen steunen op een betrouwbare en secure verwerking in de volledige keten, van IoT data tot en met de cloud, is nog als pril te bestempelen. Industriestandaards, keurmerken en/of richtlijnen om een secure IoT te borgen zijn niet wettelijk verplicht, compliance controls & frameworks, richtlijnen en andere security eisen zijn onvoldoende aanwezig. Maar ook de governance inzake de IoT-data en wetgeving hieromtrent is nog onvoldoende uitgewerkt (GDPR).

Ten aanzien van de impact van kwetsbaarheden voor het digitale landschap en maatschappij kan geen antwoord worden gegeven. De impact bij misbruik is van buitenaf niet te bepalen en is voor

elke casus/gebruiker verschillend. Het aantal gedetecteerde kwetsbaarheden en tijdigheid in het mitigeren van de kwetsbaarheid, kan wel als indicator worden gehanteerd voor vervolgacties.

RISICO'S EN UITDAGINGEN

Grote zorgpunten zijn met name op het gebied van consument gerelateerde (IoT) apparaten. Denk hierbij aan de onduidelijkheid voor de koper in welke mate voldoende privacy en security maatregelen aanwezig zijn. Welke maatregelen moet de gebruiker zelf treffen? Weet de consument vooraf wat er met (persoonlijke) digitale data gebeurt? Een voorbeeld hiervan is het nog steeds aanwezig zijn van kwetsbare internetcamera's en de perikelen⁴ die er zijn geweest omtrent Facebook data.

De uitdagingen waar we met z'n allen voor staan om de digitale hygiëne op peil te houden zijn:

- **Structureel inzicht** verkrijgen in de ontwikkeling en gebruik van (onveilige) IoT & IT
- Het komen tot **keurmerken/ kwaliteitseisen** en **onafhankelijk toezicht** op veilige apparaten of minder veilige (IoT/IT) apparaten.
- **Aansprakelijkheid in de keten** bij het waarborgen van privacy & securitymaatregelen.
- De aanwezigheid van **industrie standaarden**, meetbare **hardeningguidelines & connectivity eisen** en **geautomatiseerde securityupdates** in de levenscyclus van een product of dienst en keten.
- **Een verantwoording van leveranciers** over de effectiviteit van de getroffen maatregelen

CONCLUSIE EN AANBEVELINGEN

Het voornaamste risico is het ontbreken van structureel inzicht over de toekomstige ontwikkelingen van IoT, nieuwe kwetsbaarheden die het met zich meebrengt en de combinatie met reeds bestaande IT-kwetsbaarheden.

De volgende punten vormen volgens ons een belangrijke meerwaarde om dreigingen en de impact hiervan te beheersen: het hebben van industrie standaarden, securityratings van leveranciers & producten, meetbare hardeningguidelines en connectiviteit-eisen en ook "Security by design" en "Privacy by design"⁵ in de levenscyclus van een product of dienst.

De Cyber Security Raad heeft eerder dit jaar gepleit⁶ voor ***"Een onafhankelijke monitor van gehackte en kwetsbare IoT-apparaten, zodat publieke informatie beschikbaar komt over welke fabrikanten en leveranciers hun apparaten onvoldoende beveiligen."***

GDI.Foundation steunt dit advies en hoopt dat dit op korte termijn concreet vorm krijgt.

INHOUDSOPGAVE

1	<u>INTRODUCTIE.....</u>	5
1.1	AANLEIDING ONDERZOEK.....	5
1.2	ONDERZOEKSVRAGEN	5
1.3	LEESWIJZER	5
1.4	ONDERZOEKSMETHODE.....	5
2	<u>HET NEDERLANDSE DIGITALE LANDSCHAP & INTERNET.....</u>	8
2.1	OMVANG EN DIVERSITEIT ICT-APPARATUUR EN SYSTEMEN	8
2.2	SUB CONCLUSIE	9
3	<u>HET NEDERLANDSE INTERNET-OF-THINGS.....</u>	10
3.1	DUIDING VAN HET INTERNET-OF-THINGS	10
3.2	TOEPASSINGEN IOT	11
3.3	KENMERKEN VAN IOT	12
3.4	NEDERLAND & IOT	17
3.5	SUB CONCLUSIE	20
4	<u>KWETSBAARHEID VAN DE NEDERLANDSE DIGITALE OMGEVING</u>	21
4.1	DUIDING VAN DIGITALE KWETSBAARHEDEN.....	21
4.2	OMVANG KWETSBARE SYSTEMEN IN NEDERLAND	21
4.3	GEMETEN DIGITALE KWETSBAARHEDEN.....	22
4.4	OVERIGE DIGITALE KWETSBAARHEDEN	26
4.5	SUB CONCLUSIE	29
5	<u>AANVULLENDE BEVINDINGEN.....</u>	30
5.1	HUIDIGE SITUATIE.....	30
5.2	LESSONS LEARNED & GEDRAG	30
5.3	HOE “SMART” IS ONZE TOEKOMST	31
6	<u>CONCLUSIE EN AANBEVELINGEN.....</u>	33
6.1	BELANGRIJKSTE BEVINDINGEN.....	33
6.2	MOGELIJKHEDEN OM RISICO'S TE MITIGEREN	34
6.3	AANBEVELINGEN	34
	<u>BRONVERMELDING.....</u>	35

1 INTRODUCTIE

1.1 AANLEIDING ONDERZOEK

Vanuit het Nationale Cyber Security Centrum (NCSC) is er de behoefte uitgesproken om beter zicht te krijgen op de op internet aangesloten apparatuur in Nederland en de potentiële kwetsbaarheid daarvan. In bijzonder is er op dit moment veel interesse in Internet-of-Things (IoT). Dit zijn apparaten die rechtstreeks verbonden zijn aan het internet zoals webcams, slimme thermostaten en dergelijke. Het vermoeden is dat de beveiliging van dergelijke apparaten achterloopt in vergelijking met de beveiliging van ‘traditionele’ ICT-apparatuur zoals laptops en servers omdat IoT-devices vaak niet beheerd worden. Dergelijke devices worden low-cost ontwikkeld en het (geautomatiseerd) beheer is daarbij veelal onvoorzien. Het NCSC heeft opdracht gegeven aan GDI.Foundation om d.m.v. big data-analyse van openbare bronnen een eerste analyse hierover uit te voeren. De resultaten van dit onderzoek worden gebruikt om het NCSC te helpen om de impact van “cyber” incidenten beter in te schatten en haar adviezen beter toe te spitsen.

1.2 ONDERZOEKSVRAGEN

In het kader van voorliggend onderzoek, heeft het NCSC de volgende specifieke onderzoeksvragen gesteld aan GDI.Foundation:

- ❑ *Hoe ziet het Nederlandse digitale landschap eruit in het algemeen?*
Hoeveel ICT-systemen zijn er in Nederland aan het internet gekoppeld? Wat voor systemen (smartphones, servers)? Wat draait er op (Windows, Android)? Welke diensten worden daarop aangeboden (www, dns, ssh, etc.)?
- ❑ *Hoe ziet het Nederlandse Internet-of-Things (IoT) eruit?*
Steeds meer ICT-systemen behoren tot het zogenaamde Internet-of-Things, zoals beveiligingscamera’s en slimme thermostaten. Hoe groot is het Nederlandse IoT? Hoeveel en welke type IoT-devices zijn bereikbaar vanaf het Nederlands internet?
- ❑ *Welk percentage van Nederlandse ICT is kwetsbaar?*
Nadat het Nederlandse digitale landschap (inclusief IoT) in kaart is gebracht, is het belangrijk om te weten welk deel hiervan kwetsbaar is. Welk deel draait op verouderde software of biedt een verouderde versie van een dienst aan? Welk deel van het IoT maakt bijvoorbeeld gebruik van een standaardwachtwoord?

1.3 LEESWIJZER

In hoofdstuk 2 wordt inzicht verstrekt op de deelvraag “*Hoe ziet het Nederlandse digitale landschap eruit in het algemeen?*”, hoofdstuk 3 gaat in op de deelvraag “*Hoe ziet het Nederlandse Internet-of-Things (IoT) eruit?*” en hoofdstuk 4 gaat in op de deelvraag “*Welk percentage van Nederlandse ICT is kwetsbaar?*” Het sluitstuk van het onderzoek, hoofdstuk 5 betreft een aantal *discussiepunten* op basis van de *huidige situatie* en “*Lessons Learned*”.

1.4 ONDERZOEKSMETHODE

Het onderzoek bestaat uit een deskresearch en field research. Onder field research wordt hier enerzijds verstaan het gebruiken van openbare brondata, zoals Shodan¹² en Censys¹³, en

anderzijds het daadwerkelijk meten van de digitale omgeving door middel van uitgevoerde vulnerability scans.

1.4.1 SCOPING EN AFBAKENING

De scope van het onderzoek betreft datgene wat vanaf het internet te detecteren/onderzoeken is over het digitale landschap van Nederland gebruik makend van openbare bronnen en aanvullende analyses. Eventuele nieuwe connecties van apparaten na de uitvoering van de field research vallen buiten de onderzoeksresultaten. Ook de fysieke en personele risico's vallen buiten scope van dit onderzoek. Volledigheidshalve merken we op dat het een zogenaamd "quick scan" onderzoek betreft en eventuele ervaringscijfers e/o vergelijkingsmateriaal ontbreekt.

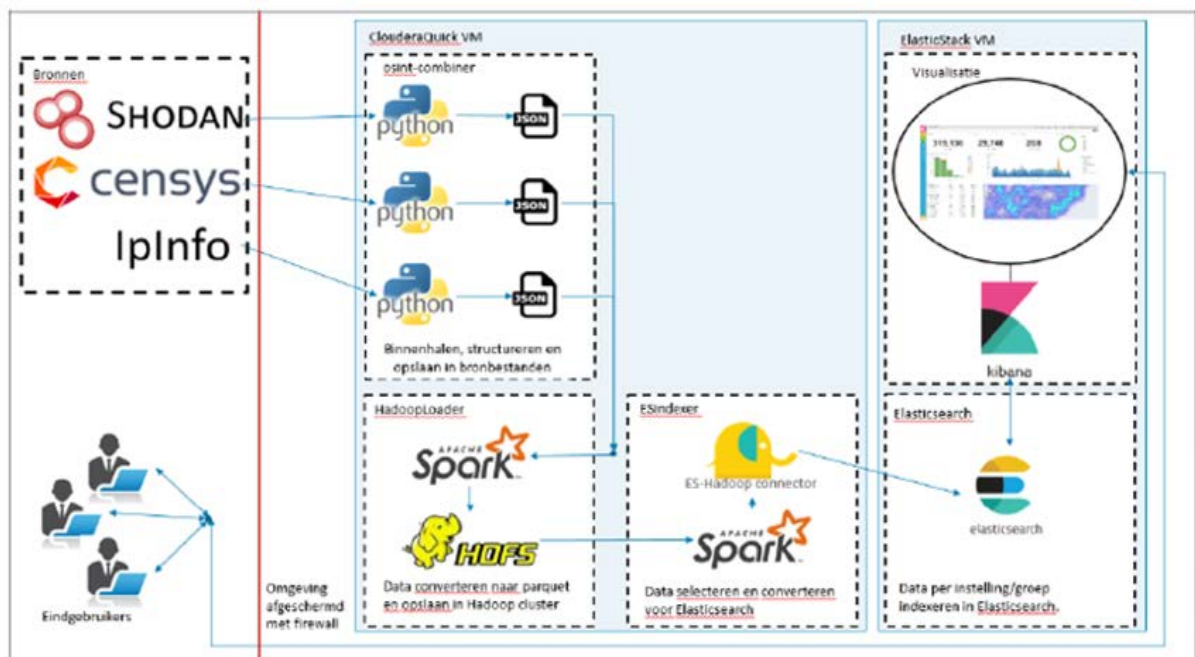
1.4.2 ONDERZOEKSPERIODE

Het onderzoek heeft plaatsgevonden in de periode oktober 2017 – mei 2018.

1.4.3 NADERE TOELICHTING FIELDRESEARCH

Bij dit onderzoek hebben we gebruik gemaakt van diverse openbare bronnen en scan methoden. Hieronder volgt een korte toelichting van de belangrijkste hiervan.

1.4.3.1 Dashboard "Internet & Cyber Security Health Check"



Figuur 1 - Technische inrichting tooling "Internet & Cyber Security Health Check (bron: V.E.Toms - GDI.Foundation)

Het onderzoek maakt gebruik van de ontwikkelde tool "Internet & Cyber Security Health Check" (ZIE FIGUUR 1). Deze tool gebruikt publiek beschikbare data en, indien benodigd, wordt dit aangevuld met extra scans (ZMap e/NMap). De code aangaande de tooling is openbaar op GitHub geplaatst en i.s.m. SURFnet tot stand gekomen. De technische omgeving staat bij SURFnet en wordt beheerd door SURFnet. De tool is onderdeel van het project "Internet & Cyber Security Health Check" dat gesponsord wordt door SIDN.Fonds⁷ i.s.m. SURFnet⁸.

Processtappen

1. Binnenhalen van open bron data op basis van selectie vooraf, met scripts
2. Verder verwerking van de ruwe data in Python en output zetten in JSON-files
3. Inlezen van output JSON files in Hadoop⁹

4. Klaarzetten geselecteerde data via Hadoop (Spark) voor Elasticsearch¹⁰
5. Inlezen van output in Elasticsearch
6. Report generator¹¹ e/o aanvullende queries/analyses in Elastic (Kibana)¹⁰

1.4.3.2 Shodan

Shodan¹² is een zoekmachine waarin men gericht kan zoeken voor specifieke op internet aangesloten apparaten. Dit kan op basis zijn van IP-adres, type apparaat (bijv. webcam of thermostaat) of protocol (bijv. MQTT of TR-069). In sommige gevallen is het op basis van de zoekresultaten ook af te leiden of de gevonden apparaten kwetsbaar zijn als die bijvoorbeeld gebruikmaakt van een standaardwachtwoord.

1.4.3.3 Censys

Censys¹³ is een zoekmachine die het hele internet dagelijks scant voor aangesloten ICT-apparatuur. Censys maakt gebruik van het netwerk scanning tool Zmap¹⁴ die in staat is om grootschalige netwerkscannen snel uit te voeren. Hierdoor is het mogelijk om de hele IPv4 space binnen 45 minuten te onderzoeken. Resultaten van dergelijke scans worden beschikbaar gesteld via hun publieke website.

1.4.3.4 IpInfo

IpInfo¹⁵ is een tool om aanvullende informatie op te vragen voor een gegeven IP-adres. Deze tool kan bijvoorbeeld worden gebruikt om te achterhalen in welk Autonoom Systeem (AS) een specifiek IP-adres zich bevindt. Ook kan hiermee worden gezien, met een redelijke zekerheid, waar op aarde het aangesloten ICT-systeem zich bevindt. Hiermee is het mogelijk om bijvoorbeeld resultaten uit andere bronnen te beperken tot systemen die zich in Nederland bevinden.

1.4.3.5 ZMAP/ NMAP

Het ZMap-project is een verzameling opensource hulpmiddelen waarmee onderzoekers grootschalige studies kunnen uitvoeren naar de hosts en services die het openbare internet vormen. In combinatie met ZGRAP kan snel een globaal inzicht worden verkregen in o.a. in type protocollen. NMAP¹⁶ is voor het verdere finetunen. Hiermee wordt aanvullende informatie verkregen over de versie van het besturingssysteem, port specificatie, type apparaat, etc..

1.4.3.6 Overige bronnen

Onder overige bronnen wordt verstaan alles wat openbaar beschikbaar is op het internet. Dit betreft onder andere social media, Google, SIDN, AMS-IX, tooling w.o. OWASP, OSINT¹⁷, beveiligingsadviezen van het NCSC¹⁸ en CVE informatie¹⁹.

2 HET NEDERLANDSE DIGITALE LANDSCHAP & INTERNET

In dit hoofdstuk wordt ingegaan op de deelvraag “Hoe ziet het Nederlandse digitale landschap eruit in het algemeen?” waarbij nader wordt ingegaan op vraagstukken als “Hoeveel ICT-systemen zijn er in Nederland aan het internet gekoppeld? Wat voor systemen (smartphones, servers)? Wat draait er op (Windows, Android)?”

Om een beeld te vormen van het Nederlandse digitale landschap is er onderzoek uitgevoerd naar onder meer het aantal IP-adressen binnen Nederland, aantal gebruikers, datagebruik, type aansluiting met het internet, aantal websites en IoT-devices.

2.1 OMVANG EN DIVERSITEIT ICT-APPARATUUR EN SYSTEMEN

2.1.1 AANTAL IP-ADRESSEN

Het Nederlandse internet bestaat uit bijna **55 miljoen IP-adressen**²⁰. Het percentage IPv6 adressen binnen Nederland is 12,6 % (6,5 milj.). Ten opzichte van bijvoorbeeld Duitsland (36, 3%) en België (49,86%) loopt Nederland ver achter bij het implementeren van IPv6.^{21 & 22}.

2.1.2 DATA GEBRUIK

Wederom is het **internet datagebruik** binnen Nederland gestegen²³ ten opzichte van de voorgaande jaren. Voor de beeldvorming: eind 2001 was de “traffic in 1.222TB²⁴” en eind 2017 “traffic in **1.200.961TB**²⁵”. M.a.w. een stijging van 1.000% in 16 jaar tijd ten aanzien van het downloaden van digitale informatie. Een verklaring hiervoor is de toename in de aanbidding en het gebruik van digitale entertainment als Netflix, Youtube, vlogs & blogs, etc. in combinatie met het aantal uren dat besteedt wordt op het internet. In de analyses van CBS²⁶ en SIDN²⁷ zijn aanvullende verklaringen te vinden over het waarom en de toename in het gebruik van internet.

2.1.3 AANTAL GEBRUIKERS VAN HET INTERNET

Het totaal aantal geregistreerde inwoners in Nederland is op d.d. 20 februari 2018 17.201.528. Het percentage gebruikers van het internet binnen Nederland, vanaf 12 jaar, is rond de **97%**²⁸. In 2017 had 98% van de Nederlandse huishoudens thuis toegang tot internet en behoort daarmee tot de best scorende Europese landen²⁹.

2.1.4 BROWSERS

De voornaamste browser die in Nederland gebruikt wordt betreft **Chrome (+/- 50%)** vervolgens Safari (25%) en overige browsers als FireFox, Internet Explorer en Edge³⁰.

2.1.5 DESKTOP V.S. MOBIEL

Op basis van geanalyseerde webstatistieken (168.084.969 bezoekers op bekende websites) blijkt dat er van de internetgebruikers **60,9% desktop gebruikers** zijn en **39,1% mobiele gebruikers** (smartphones, tablets en wearables).

2.1.6 TYPE MOBIEL

Het meest gebruikte mobiele besturingssysteem in Nederland bij mobiele communicatie is **Android (57%)**. Vervolgens **Apple (41%)**, Windows (0,74%), Samsung (0,15%), Blackberry (0,06%), Symbian, Linux, Nokia en overige³¹.

2.1.7 AANTAL DESKTOP / SERVERS (WINDOWS)

Windows is met 81% veruit het meest populaire besturingssysteem voor desktop computers in Nederland³². Tijdens het moment van onze scan waren er meer dan 70.000 Windows desktops e/o Windows servers aangesloten op het Internet.

2.1.8 WIFI CONNECTIES

Door heel Nederland zijn er meer dan **6.051.799 Wifi-netwerken**³³ in kaart gebracht. Daarvan hebben er 3.701.864 WPA2-beveiliging, 552.381 WPA-beveiliging en 636.214 WEP-beveiliging. Voor 648.844 is de beveiliging onbekend en 512.496 zijn open netwerken waarvan meer dan 3750 openbare HotSpots³⁴ van KPN op openbare locaties zoals vliegvelden en NS-stations.

2.1.9 ROUTERS/ MODEMS

Met betrekking tot de zakelijke markt van routers en modems is **CISCO** de absolute marktleider (76,4 %) en HPE/Aruba met 14,3% op een tweede plaats. Juniper is met 3 procent de enige andere partij die boven de 1 procent scoort³⁵. Ten aanzien van de consumentenmarkt is de relatie gemaakt tussen grootste internet dienstleveranciers (ISP) in Nederland en type routers die zij aanbieden. De grootste aanbieders zijn KPN en Ziggo. KPN³⁶ levert met name de **ExperiaBox** en **ZTE modems**. Bij Ziggo wordt momenteel een **Connectbox** verstrekt. Een volledige lijst van modems en routers die door Ziggo in de afgelopen jaren zijn geleverd is terug te vinden op hun site³⁷.

2.1.10 WEBSITES

Er zijn **5.806.624 websites**³⁸ met een **.NL-extensie** waarvan minimaal **4.346.708 websites worden gehost** door verschillende eigenaren. Deze hoeven **niet per se uit Nederland te komen** (outsourcing). De reden hiervoor is dat één webserver meerdere websites draait en deze in het buitenland ook gehost worden.

2.1.11 INTERNET OF THINGS (IOT)

Binnen Nederland zijn KPN en “The Things Network” de voornaamste en meest prominente speler bij het aanbieden van een IoT netwerk. Deze zijn beide geënt op de LoRa techniek. (Lora, ofwel Long Range Low Power, is een LP-WAN technologie die kleine pakketjes data kan uitwisselen tussen objecten en systemen). Een andere wereldwijde speler voor IoT netwerken betreft Zigbee³⁹. In hoofdstuk 3 wordt nader ingegaan op IoT en het gebruik hiervan in Nederland.

2.2 SUB CONCLUSIE

De connecties van het Nederlands digitale landschap met het internet is divers en het gebruik (“afhankelijkheid”) van internet is groot. Niet alleen qua data maar ook ten aanzien van het aantal gebruikers en type apparaat dat hiervoor gebruikt wordt. Zo kan op basis van het aantal IP-adressen en inwoners de logische gevolgtrekking worden gemaakt dat een persoon met één of meer apparaten een verbinding heeft met het internet zoals laptop, smartphone, tablet, Homepods etc. Opvallend is dat bepaalde producten van leveranciers een groot marktaandeel hebben, zoals CISCO, in de aansluiting met het internet. Een eventuele kwetsbaarheid in één van deze producten en niet tijdig mitigeren van het risico, kan derhalve grote impact hebben voor onze samenleving.

3 HET NEDERLANDSE INTERNET-OF-THINGS

In dit hoofdstuk wordt nader ingegaan op de deelvraag “Hoe ziet het Nederlandse IoT eruit?” Dit wordt gedaan door eerst te bezien wat onder IoT wordt verstaan, de toepassingen hiervan, welke connectiviteiten brengt dit met zich mee en hoeveel IoT gerelateerde devices vanaf het internet zijn te detecteren.

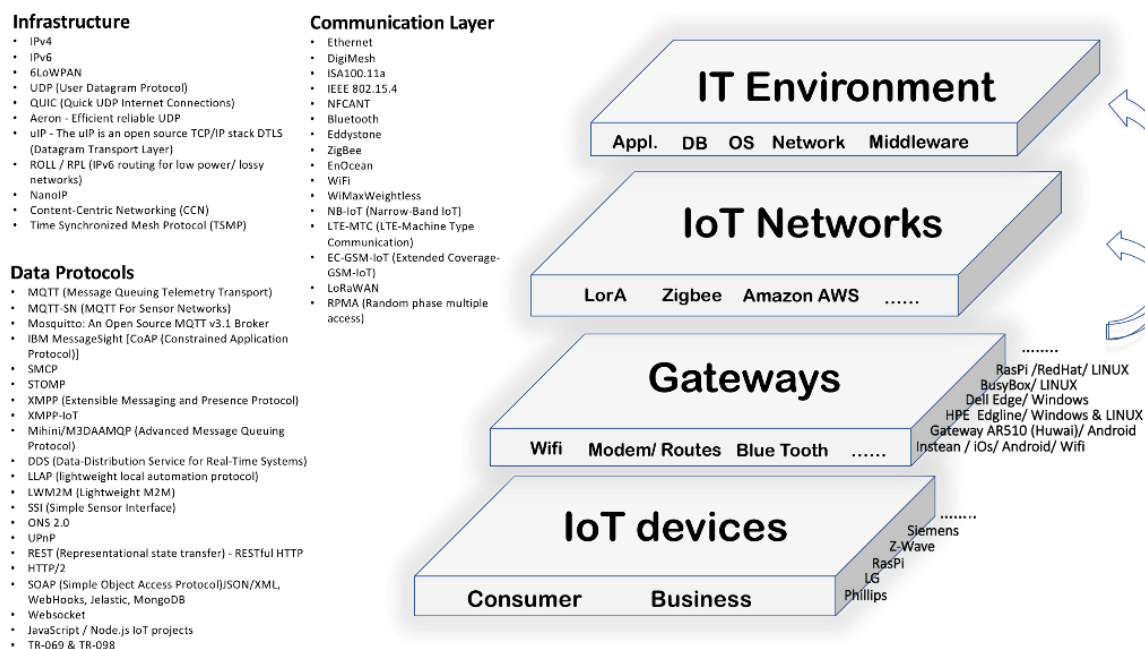
3.1 DUIDING VAN HET INTERNET-OF-THINGS

Wereldwijd worden verschillende definities gehanteerd voor IoT. Het begrip IoT is aan eind van de jaren '90⁴⁰ ontstaan en is opgebouwd uit technieken die al langer worden gebruikt. Het voornaamste verschil tussen het heden en verleden is de hoeveelheid apparaten en het beschikken over wereldwijd omvattende netwerk(en) waardoor connecties tussen dingen, mensen en processen mogelijk is.

In dit onderzoek wordt gebruikgemaakt van de definitie die door WODC¹ voor IoT wordt gehanteerd en tevens overeenkomt met die van ITU⁴¹ (ZIE OOK FIGUUR 2).

Definitie IoT:

“Een netwerk van objecten (vaak verbonden met het internet), die gegevens verzamelen over hun omgeving, deze kunnen uitwisselen en op basis daarvan (semi)autonome beslissingen nemen en/of acties uitvoeren die van invloed zijn op de omgeving”.



Figuur 2 – “Connectivities, protocols, layers and some IoT devices / suppliers” (bron: V.E.Toms - GDI.Foundation)

De fieldresearch heeft zich beperkt tot een aantal IoT-protocollen en apparaten. Reden hiervoor is de hoeveelheid aan informatie, doorlooptijd en het doel van het onderzoek (quick scan). De fieldresearch geeft derhalve ook geen volledig beeld/inzicht in de aanwezigheid van alle IoT in

Nederland. Dit verdient aanvullend onderzoek. In hoofdstuk 4 zijn de onderzochte protocollen en apparaten terug te vinden.

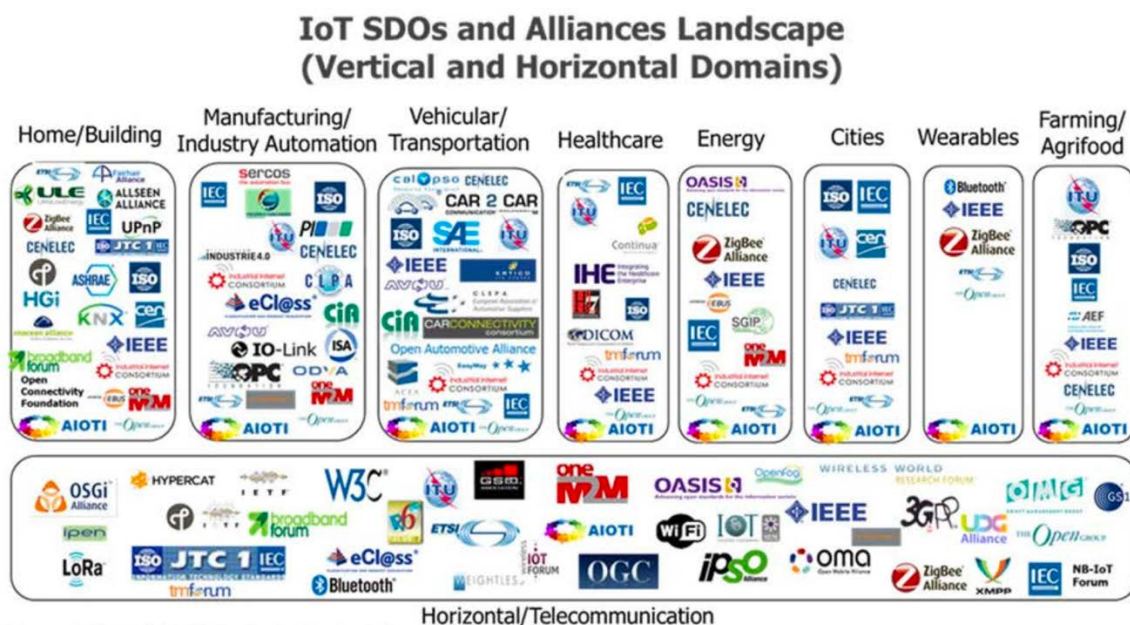
3.2 TOEPASSINGEN IoT

De combinatie van IT en IoT, en de koppeling met het internet, levert nieuwe inzichten, mogelijkheden en business. Dankzij de veelheid van apparaten in combinatie met sensoren kan een veel nauwkeuriger inzicht worden verkregen. Niet alleen over het gedrag van individuen maar ook over informatie voor bijvoorbeeld de agrarische sector, verzekeringsbranche, medische sector, politiek, Smart cities, etc.

3.2.1 DOELGROEP & BRANCHES

De doelgroep eindgebruikers van IoT is op hoofdlijnen te onderscheiden in een tweetal verschillende groepen en de combinaties hiertussen. Het primaire onderscheid is te maken tussen de consumer market (C) en business market (B). De combinaties die vervolgens te maken zijn betreft onder meer B2B, B2C, C2C, B2B2C.

Het gebruik en inzet van IoT is in elke branche/sector terug te vinden. Van SMART city/house tot aan de medische sector en personal health care. Een duiding per sector en de incorporatie van IoT in een primair e/o kritiek proces is niet transparant meetbaar. De inzet van IoT in auto's, wasmachines en agrarische sector⁴² zijn slechts enkele voorbeelden wat mogelijk is met IoT. Verdere uitwisseling van IoT data en connectiviteiten van IoT devices/diensten/netwerken tussen branches is zeer reëel zoals in **FIGUUR 3** wordt geïllustreerd.



Figuur 3 - SmartM2M: IoT Standards landscape and future evolutions (bron: ETSI)

3.2.2 TYPE APPARATEN EN DIENSTEN

Er zijn oneindig veel IoT-apparaten mogelijk zolang een apparaat bestaat en deze een signaal geeft (sensor). Het aanbod van IoT-apparaten wordt bepaald door de fabricage en vraag. De creativiteit van mens en organisaties is bijzonder hoog en leidt ook tot allerlei nieuwe diensten en combinaties van diensten. Van "Plek Checker", "Waar is mijn sleutel"⁴³, "Meting waterkwaliteit

om zwemmen in de binnenhaven mogelijk te maken⁴⁴ tot aan IoT in de medische sector⁴⁵ en zwaardere industrie⁴⁶.

3.2.3 POTENTIE VAN IOT

Internationaal is Internet of Things een van de belangrijkste economische ontwikkelingen op dit moment. Het biedt dan ook interessante nieuwe verdienmodellen voor Nederlandse ondernemers.⁴⁷ Het (ogenschijnlijk) gemak en de verkorting van de doorlooptijd voor het creëren van nieuwe digitale diensten en producten voor zowel business als consumenten, leidt nu al tot toename. Multinationals, nationale bedrijven, MKB en ook individuen over de hele wereld zijn in staat om een product of dienst te ontwikkelen en aan te bieden via het Internet waarbij de ontwikkelkosten bijzonder laag (kunnen) zijn. De potentie van IoT wordt ook onderkend door grote internationale instanties als bijvoorbeeld SIEMENS, KPN en PHILIPS en is terug te vinden in de investeringen die zij plegen op het terrein van IoT en in hun strategische visie.

De voorspelling van Gartner⁴⁸ dat rond 2020 meer dan 20 biljoen apparaten zijn aangesloten op het Internet, is dan ook wellicht ook te hoog ingeschat gezien huidige ontwikkelingen. De voordelen en kansen die het biedt voor meerdere partijen zijn echter groot. Een nadere analyse in de productie van IoT apparaten en inbedding van sensoren in het fabricageproces is niet onderzocht.

3.3 KENMERKEN VAN IOT

3.3.1 ONDERSCHIED ECOSYSTEEM IT & IOT

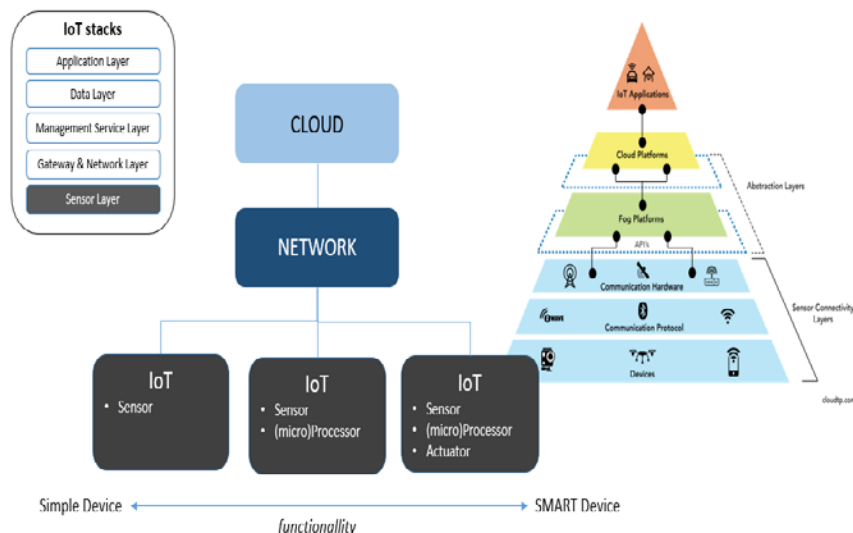
Een duidelijk onderscheidt in de ecosystemen tussen IT & IoT is lastig te maken. Behalve qua architectuur en netwerktypologie (gesloten-open) vertonen deze ecosystemen ook ten aanzien van internet gateways en op besturingssysteemniveau grote overeenkomsten.

Vanuit technische invalshoek is een beter onderscheid te maken. Dit heeft o.a. betrekking op functionaliteit van het apparaat, energieverbruik, rekenvermogen (CPU) en datatransmissie/transport (protocollen) die gehanteerd worden.

3.3.2 FUNCTIONALITEIT VAN TECHNISCHE COMPONENTEN IOT

Net als bij meerdere ICT-producten en diensten is te constateren dat een overlapping in functionaliteit van IoT plaatsvindt. Van een simpele sensor naar een apparaat wat beslissingen neemt met daaraan gekoppelde activiteiten (afhankelijk van doelbinding apparaat).

Het onderscheidend vermogen van IoT zit met name in het wel of niet hebben van een (micro)processor en actuatoren. Afhankelijk van het doel en efficiency, kunnen verschillende keuzes worden gemaakt inzake de procesmatige verwerking van de data, acties die hieruit voortvloeien en dataopslag. [ZIE FIGUUR 4](#)



Figuur 4 – “Functions of technical IoT components” (bron: V.E.Toms - GDI.Foundation)

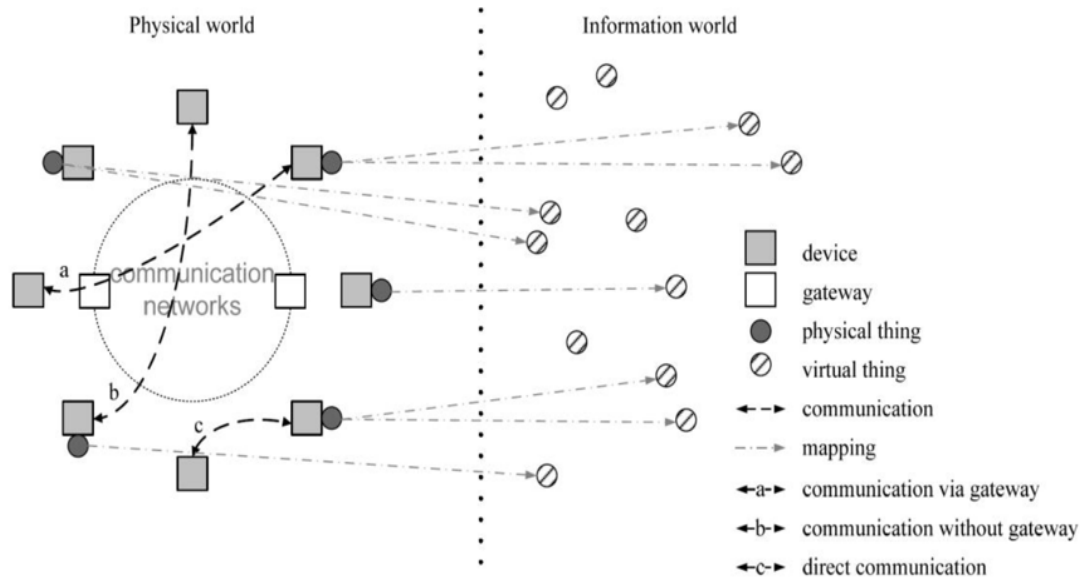
Een volledig IoT-systeem om iets te controleren en te reageren op waarnemingen bestaat uit de vier onderdelen⁴⁹.

1. Sensor: dit is de ingang van het systeem, er wordt hier door middel van een mechanisme een waarneming gedaan. Deze waarneming kan bijvoorbeeld de omgevingstemperatuur zijn. De uitgang van dit onderdeel kan een analoog of een digitaal signaal zijn.
2. Regelaar: veelal wordt dit gedaan door microprocessoren of digitale signaalprocessoren, die met digitale waarden werken.
3. Actuator: hier wordt de uiteindelijke beslissing analoog of digitaal uitgevoerd. Een actuator is een toestel dat invloed kan uitoefenen op zijn omgeving.
4. Internetconnectie.

Een voorbeeld van een IoT-apparaat waarin de vier elementen voorkomen is “*Toon de slimme thermostaat*” van Eneco⁵⁰. Een voorbeeld van een simpel apparaat is de hartslagmeter met GPS die vaker tijdens het sporten wordt gebruikt waar alleen een sensor in voorkomt.

3.3.3 CONNECTIVITEIT IOT APPARATEN

De connectiviteit van IoT apparaten verloopt op verschillende manieren. Het onderstaande schema (FIGUUR 5) geeft inzicht in welke types connectiviteit te onderkennen zijn m.b.t. IoT.



Figuur 5 – Technical overview of the Internet of Things as defined by ITU (bron: Dialogic i.o.v. Agentschap Telecom)

In het rapport van ITU⁴¹ en Stratix⁵¹ zijn diepgaander analyses terug te vinden over o.a. type netwerken, toepassing en connectiviteit van IoT.

3.3.4 TYPE IOT NETWORK

Net als in de IT-omgeving zijn er verschillende netwerken voor IoT te onderkennen. Het onderzoek heeft zich gericht op specifieke IoT-communicatie en laat hierbij glasvezel communicatie buiten beschouwing. In het rapport van Stratix⁵¹ wordt onderscheidt gemaakt tussen WAN, MAN, LAN en PAM. Hieronder zijn de definities opgenomen uit het rapport:

- ❑ **Wireless wide area ‘macro’ networks:** For communication using connectivity over larger areas (countries or larger), for example using macro networks like operator controlled mobile networks (or sometimes even satellite communication).
- ❑ **Metropolitan Area Networks:** Communication between devices on a more localized, metropolitan area (up to a couple of kilometers) in an area.
- ❑ **Wireless Local Area Networks:** Communication between devices in your home, office or workplace form a ‘Local Area Network’.
- ❑ **Personal Area Network (PAN):** Personal devices that you carry around and connect on a ‘personal scale’ form a Personal Area Network.

Specifiek voor Internet of Things en het gebruik hiervan in een MAN netwerk, worden Low-Power Wide-Area (LPWA) telecomnetwerken ontwikkeld op basis van onder andere de LoRa techniek. Zowel het commerciële LPWA-netwerk van KPN (LoRa) als het openbare netwerk van “The Things Network” is opgebouwd op basis van de LoRa techniek. Ook NB-IOT (Narrow Band IOT) is een LPWA-netwerk en wordt vooral ingezet door Vodafone en T-Mobile in Nederland⁵².

Dit wijkt af van bijvoorbeeld Machine to Machine (M2M) connectiviteit welke vaak op UMTS/2G/3G/4G is gebaseerd en zich kenmerkt door hoog verbruik in data en energie. Op dat gebied zijn er meerdere ontwikkelingen gaande, zoals LTE-M (Machine Type Communication

voor 4G netwerk) en connectiviteit met 5G. Ook GPRS en Bluetooth (zoals iBeacon) zijn netwerken welke voor IoT gebruikt worden.

Toelichting M2M

Met een M2M-connectiviteit, machine-tot-machine communicatie, kunnen bedrijfsmiddelen draadloos op lange afstand communiceren met andere bedrijfsmiddelen, mensen en IT-infrastructuur. Met een SIM-kaart van bijvoorbeeld KPN is een wereldwijde connectiviteit mogelijk. De verzamelnaam M2M geldt voor vier verschillende diensten⁵³:

1. **Machine to Machine (M2M)** Dit zijn toepassingen waarbij apparaten autonoom functioneren en automatisch met elkaar communiceren. *Voorbeelden*: slimme energiemeters, navigatiesystemen, dongels voor mobiel internet op laptops, e-readers en bloeddrukmeters.
2. **Machine to Human (M2H)** Dit zijn autonoom werkende apparaten. *Voorbeelden*: de beveiliging- of alarmsystemen die het beveiligingsbedrijf bellen en auto's die na een ongeluk het alarmnummer bellen.
3. **Human to Machine (H2M)** Dit zijn toepassingen waarbij een persoon een verbinding opzet met een autonoom functionerend apparaat. *Voorbeelden*: het instellen van een beveiligingscamera of een thermostaat.
4. **Human to Human (H2H)** Dit zijn toepassingen met geautomatiseerde spraakverbindingen tussen personen. Ondanks dat er hierbij mensen betrokken zijn, valt het onder de categorie M2M-diensten omdat een computer (semi-) zelfstandig de spraakverbinding tussen twee mensen tot stand brengt. *Voorbeelden*: de pechtelefoon in de auto, waarmee met één druk op de knop een verbinding met de hulpdienst automatisch wordt gestart voor een spraakverbinding tussen personen.

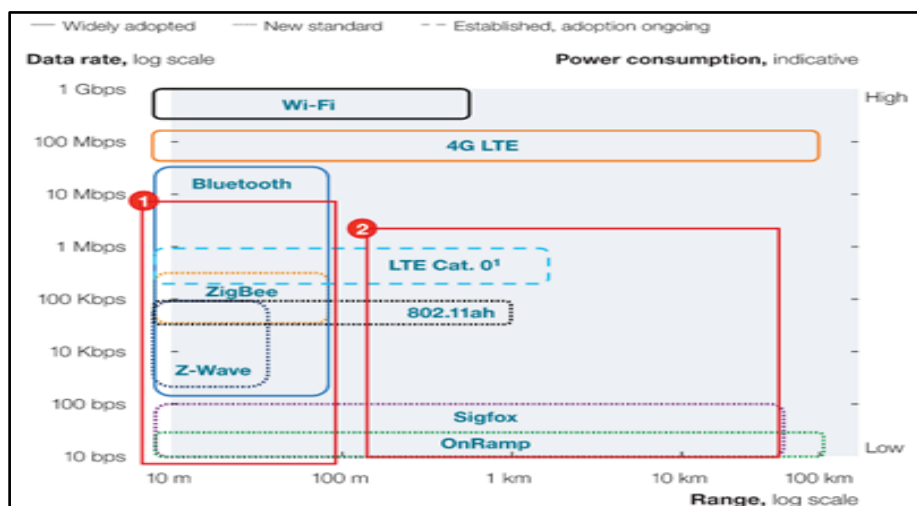
3.3.5 INTERNET GATEWAYS & BESTURINGSSYSTEEM

In de vorige paragraaf is eerder ingegaan op de types connectiviteit die te onderkennen zijn. Om IoT aan te sluiten met het internet is een gateway benodigd. Deze kan met een modem, router, satelliet, mobiel of SIM-kaart aangesloten worden waarmee een verbinding met het internet (IPv4 e/o IPv6 adressen) opgezet kan worden.

Uit productanalyse⁵⁴ & ⁵⁵ van IoT-internet gateways blijkt dat het besturingssysteem van de internet gateways voornamelijk gebaseerd is op Linux/Unix en Windows. Hierbij komt het ondersteunen van IoT voor meerder besturingssysteemplatformen (gateways) veelvuldig voor. M.a.w. een enkele aangeboden gateway voor IoT kan met meerdere besturingssystemen worden ondersteund.

3.3.6 PROTOCOLLEN, GATEWAYS EN AFSTAND

Volgens UDG Alliance⁵⁶ zijn een vijftigtal IoT-communicatieprotocollen onderkent. Afhankelijk van de hoeveelheid data en te overbruggen afstand maak je een keuze welk protocol / techniek het best past. Zoals te zien in onderstaand **FIGUUR 6**.










Figuur 6 - IoT protocols (bron: Postscapes)

3.3.7 PROTOCOLLEN, FREQUENTIE EN LICENTIE

Er is veel vraag naar frequenties voor draadloze technieken waaronder IoT. Draadloze communicatie is gebaseerd op elektromagnetische signalen en te vergelijken met geluid. Voor bepaalde geluidsfrequenties is een licentie vereist. Het Agentschap Telecom⁵⁷ is zowel uitvoerder als toezichthouder van wet- en regelgeving op gebied van telecommunicatie en bepaald voor welke frequenties⁵⁸ een licentie vereist is.

Op basis van het rapport “Onderzoek Dialogic over Internet of things” blijkt dat voor onder andere het LoRa techniek (KPN & The Things Network) geen licentie vereist is.

	SIGFOX	LoRa	clean slate	NB LTE-M Rel. 13	LTE-M Rel. 12/13	EC-GSM Rel. 13	5G (targets)
							
Range (outdoor) MCL	<13km 160 dB	<11km 157 dB	<15km 164 dB	<15km 164 dB	<11km 156 dB	<15km 164 dB	<15km 164 dB
Spectrum Bandwidth	Unlicensed 900MHz 100Hz	Unlicensed 900MHz <500kHz	Licensed 7-900MHz 200kHz or dedicated	Licensed 7-900MHz 200kHz or shared	Licensed 7-900MHz 1.4 MHz or shared	Licensed 8-900MHz 2.4 MHz or shared	Licensed 7-900MHz shared
Data rate	<100bps	<10 kbps	<50kbps	<150kbps	<1 Mbps	10kbps	<1 Mbps
Battery life	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years	>10 years
Availability	Today	Today	2016	2016	2016	2016	beyond 2020

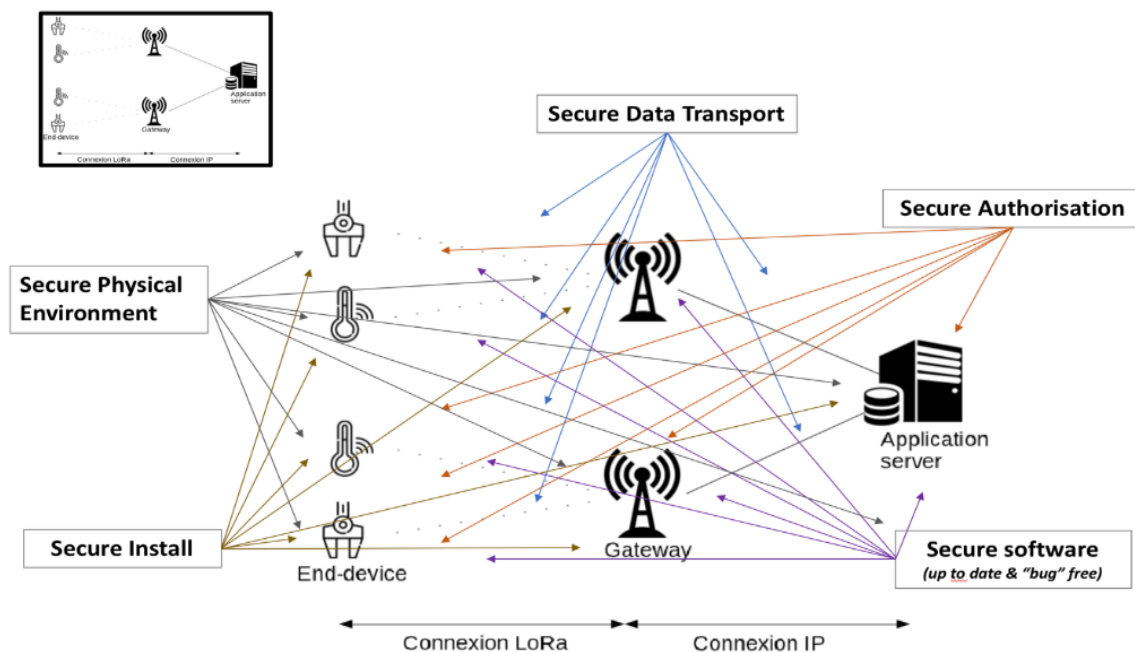
Figuur 7: Onderzoek dialogic over IoT (bron: agentschaptelecom)

3.3.8 BEVEILIGING & IOT: BELEID, RICHTLIJNEN EN NORMEN

Agentschap Telecom spreekt haar zorgen uit⁵⁹ over de beveiliging van IoT. Zo stellen zij dat “het aantal kwetsbare apparaten dat verbonden wordt met internet groeit. Van slimme thermostaten tot beveiligingscamera’s en van koelkasten tot smart-horloges en speelgoed: het ‘Internet of Things’ ontstaat. Door deze toename neemt ook de cyberdreiging toe.”

Het kunnen sturen en beheersen van de beveiliging vereist beleid, kaders, toetsbare richtlijnen en toezicht. Knelpunten om (tijdig) tot adequate maatregelen te komen zijn lastig. Zo is de dreiging en doelwit voor een criminele actor vooraf moeilijk te duiden, zijn de spelers in de keten divers zijn en komen de belangen niet altijd overeen. De voornaamste reden om (tijdig) tot adequate maatregelen wordt veroorzaakt door de snelheid van technologische ontwikkelingen, de dynamiek, hoeveelheid oplossingsmogelijkheden en toenemende complexiteit.⁶⁰

In het onderstaande figuur is zowel de complexiteit als de afhankelijkheid van beveiliging in de keten voor een kleine omgeving gevisualiseerd (4 IoT-apparaten, 2 gateway’s en 1 applicatie server).



Figuur 8 – Security Aspects, complexity and dependency (bron: V.E.Toms - GDI.Foundation)

Door meerdere partijen (zowel commerciële, stichtingen als overheid) wordt getracht om nadere invulling te geven aan de beveiliging van IoT. Een belangrijke partij hierin is NEN⁶¹. Zo is vanuit NEN een Nederlandse werkgroep 'IoT Security en Privacy'⁶² opgericht om invloed uit te oefenen op de internationale standaarden die momenteel ontwikkeld worden in verschillende standaardisatie groepen op Europees en mondiaal niveau. Ook vanuit OWASP⁶³, LoRa⁶⁴, KPN⁶⁵, Digital Trust Center (DTC)⁶⁶, NIST⁶⁷ & ⁶⁸ e.a. zijn initiatieven en adviezen te vinden over beveiliging.

Beleid, richtlijnen en normeringen voor het betrouwbaar gebruik kunnen maken van IoT ontbreken en is diffuus. Zowel een integrale benadering in de volledige keten, als ook uniformiteit in aanpak en adviezen en een centrale regie ontbreken.

3.4 NEDERLAND & IoT

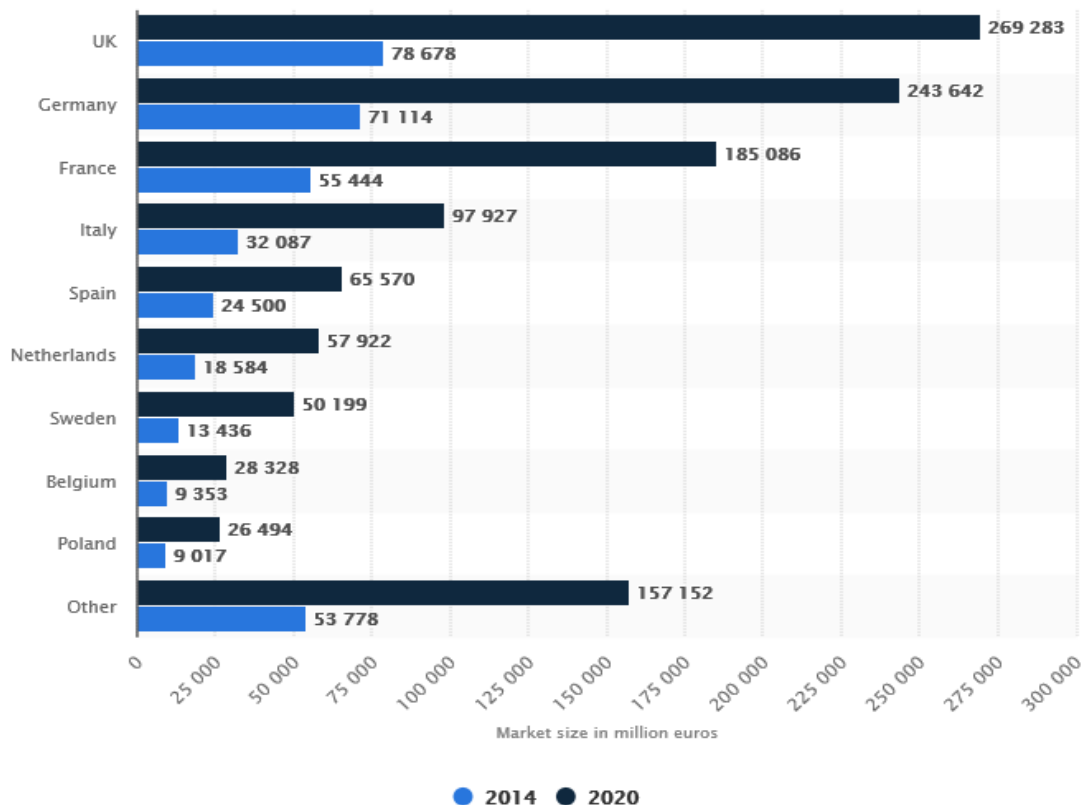
Voor dit onderzoek is er vanuit verschillende invalshoeken naar meerdere apparaten en protocollen analyse verricht om een beeld te krijgen van het gebruik van IoT in Nederland. Daarbij dient wel de kanttekening te worden geplaatst dat het resultaat niet uitputtend is. Namelijk, nieuwe IoT-apparatuur en nieuwe versies van bestaande apparaten worden dagelijks aangesloten op het internet.

Om specifiek inzicht te krijgen in de omvang van het aantal IoT-apparaten in Nederland, is er aan de hand van zogenaamde verkregen headers en attributen bepaald of een ICT-apparaat is aan te merken als een IoT-apparaat. Als een ICT-apparaat tijdens de scan (zie 1.4.3) bijvoorbeeld iets vermeldt over het merk/leverancier/protocol, dan wordt deze en andere data gebruikt om vast te kunnen stellen of het een IoT-apparaat betreft. Een voorbeeld hiervan is het merk Foscam, een grote leverancier van webcams. Een ander voorbeeld hiervan is het IoT apparaat Raspberry Pi, deze is te herkennen in Shodan aan de naamgeving "Raspi".

3.4.1 ADOPTIE VAN IOT IN NLD

In Nederland waren er tijdens het onderzoek 649 gateways en 50 communities aangesloten bij het Internet of Things Network⁶⁹. Wereldwijd zijn er 40.129 ontwikkelaars, 3.841 actieve gateways en 23.430 applicaties aangesloten aan het LoRaWan netwerk. Op basis van de Internet of things network (TTN) blijkt dat Noord West Europa met 2.184 gateways, voorop loopt met de adoptie/gebruik van IoT t.o.v. van andere landen⁷⁰ continenten.

Het onderstaande grafiek geeft de (voorspelde) marktgrootte weer van het Internet of Things (IoT) in Europa in 2014-2020, uitgesplitst naar land⁷¹.

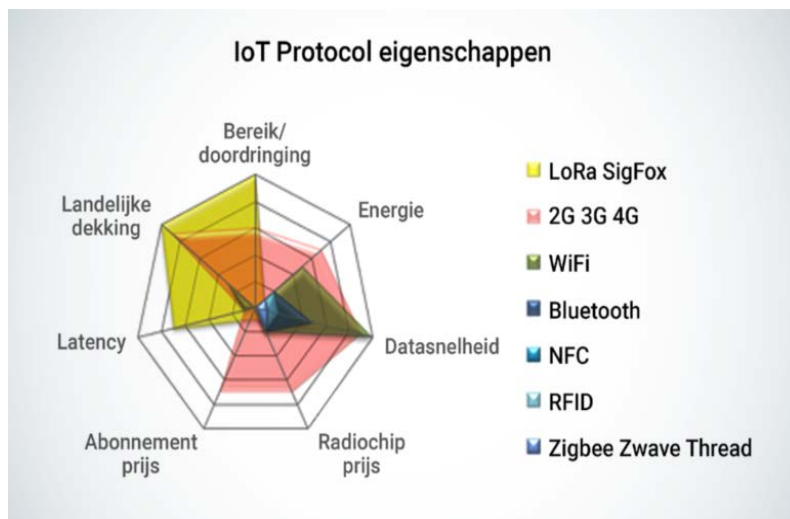


Figuur 9: (Voorspelde) marktgrootte IoT Europa (bron: Statista.com)

3.4.2 GROOTSTE NEDERLANDSE IOT NETWERK

KPN is de voornaamste en meest prominente commerciële speler met het aanbieden van een IoT-Netwerk in Nederland. Dit LoRa-netwerk dekt geheel Nederland af. De omzet van KPN met betrekking tot IoT is t.o.v. het vorige kwartaal met 40% gestegen^{72 & 73} en ook één van de strategische speerpunten van KPN⁷⁴. Een belangrijk onderdeel in deze omzetstijging is de verkoop van SIM-kaarten t.b.v. IoT M2M (MAN) netwerken. Ook ten aanzien van gelicenseerde frequenties voor het verbinden van ondermeer IoT aan het internet middels 2, 3, 4 en 5G blijkt dat KPN de grootste speler⁷⁵ is.

Een ander groot IoT-netwerk⁷⁶ in Nederland betreft het openbare "The Things Network". Ook deze is gebaseerd op de LoRa-techniek. Het onderstaande figuur is een weergave van een aantal protocollen en de dekking hiervan in Nederland.



Figuur 10: het verschil tussen de huidige LPWAN technieken en de andere protocollen: (bron:IoT-Academy)

3.4.3 TOENAME IOT (M2M)

In Q1 2018 was het totale klantenbestand (wereldwijd) van KPN met betrekking tot uitgifte van SIMs (M2M) **4,0 mln.** Ook het ACM⁷⁷ & ⁷⁸ signaleert een toename in gebruik van M2M nummers in Nederland t.b.v. IoT. Het M2M nummer (097) is bedoeld voor elektronische communicatiediensten waarbij het nummer normaal gesproken niet of automatisch wordt opgeroepen en veelal tot stand komt middels een SIM-kaart.

3.4.4 AANTAL GATEWAYS

Met de LoRa-techniek kunnen allerlei dingen met het internet praten zonder gebruik te hoeven maken van 3G of Wi-Fi. De gateways die gebruikt kunnen worden voor de aansluiting met het LoRa-netwerk, kan plaatsvinden met verschillende platformen w.o. Raspberry Pi (RasPi), OpenWRT en Cisco⁷⁹.

Tijdens de onderzoeksperiode waren er binnen Nederland ongeveer 650 gateways in Nederland aangesloten aan het openbare LoRa-Netwerk van TTN. Uit de scan zijn 9 RasPI's gedetecteerd, 4 Busyboxes, 7 INSTEON SmartLinc Home gateway's en 74 Dreambox (DVB) Digital TV/Radio in Nederland.

3.4.5 GEDETECTEERDE IOT PROTOCOLLEN

Bij de toegepaste methode is er vanaf het internet gescanned, waarbij alleen protocollen gedetecteerd kunnen worden van welke "de deur is opengezet". Om false positives te voorkomen is onderzoek gedaan naar verschillende types IoT-protocollen en vervolgens onderzocht welk protocol te detecteren is via een remote scan.

De scan heeft zich gericht op het protocol TR-069⁸⁰, MQTT⁸¹ en UPnP⁸² & ⁸³ in combinatie met de camera AVtech⁸⁴. Het gebruik van TR-069 protocol was tijdens de scan 4.800, voor MQTT 1.091 en het protocol UPnP i.r.m. AVtech Camera 817.

3.4.6 GEDETECTEERDE IOT APPARATEN

De focus van de scan heeft gelegen op een aantal IoT-apparaten die via het internet te detecteren waren. IoT-devices die achter NAT/firewall geplaatst zijn of die geen 'open deur' hebben kunnen niet worden gedetecteerd. In totaal zijn er 7.095 IoT apparaten tijdens de scan gedetecteerd. Opvallend is dat tijdens de scan de "Dahua" camera het meest voorkomt (zie tabel onder 4.3.7). Een analyse naar aantal verkochte IoT apparaten heeft niet plaatsgevonden gezien scope, doorlooptijd en doeleinde van het onderzoek.

3.5 SUB CONCLUSIE

Internationaal is Internet of Things een van de belangrijkste economische ontwikkelingen op dit moment. Het (ogenschijnlijk) gemak en de verkorting van de doorlooptijd voor het creëren van nieuwe digitale diensten en producten voor zowel business als consumenten, leidt tot een toename van nieuwe producten en diensten. Het gebruik en inzet van IoT is ook in elke branche/sector terug te vinden. Een nadere analyse van de inbedding van sensoren in het fabricageproces en het daadwerkelijk gebruik van IoT per sector is niet nader onderzocht.

Binnen Nederland zijn KPN (commercieel) en het gratis "The Things Network" de voornaamste en meest prominente spelers met het aanbieden van een IoT-MAN netwerk in Nederland.

Tijdens de onderzoeksperiode waren er binnen Nederland ongeveer 650 gateways in Nederland aangesloten aan IoT Netwerk van "The Things Network". Ten aanzien van aansluitingen van IoT middels M2M aan het IoT netwerk van KPN, is een verdere stijging geconstateerd door het ACM. Het totaal aantal gedetecteerde IoT apparaten en IoT protocollen (TR-069, MQTT) is 12.986.

Een duidelijk onderscheidt in de ecosystemen tussen IT & IoT is lastig te maken en liggen in elkaars verlengde (mede & hergebruik). Niet alleen qua architectuur en netwerktypologie (gesloten-open / peer to peer - matrix) maar ook ten aanzien van het besturingssysteem van Internet gateways vertonen deze grote overeenkomsten.

Met de introductie van IoT en de connectiviteit met internet, IT omgeving e/o andere IoT netwerken, ontstaan er meerdere en nieuwe connectiviteiten (kansen) en ook nieuwe bedreigingen¹. Het kunnen steunen op een betrouwbare en secure verwerking in de volledige keten, van sensor tot aan cloud, is essentieel bij het toepassen van IoT in (kritieke)processen.

Beleid, richtlijnen en normeringen voor het betrouwbaar gebruik kunnen maken van IoT in de keten ontbreken en is diffuus. Een integrale benadering in de volledige keten, uniformiteit en gemeenschappelijkheid in aanpak en adviezen, maar ook een centrale regie ontbreken. Het is onvoldoende transparant c.q. gecentraliseerd.

4 KWETSBAARHEID VAN DE NEDERLANDSE DIGITALE OMGEVING

In de vorige hoofdstukken is het Nederlandse digitale landschap inclusief IoT, in kaart gebracht. Dit hoofdstuk gaat in op de deelvraag “Welk percentage van Nederlandse ICT is kwetsbaar?” Hierbij wordt ingegaan op welk deel hiervan kwetsbaar is. Welk deel biedt een verouderde versie van een dienst aan? Welk deel van het IoT maakt bijvoorbeeld gebruik van een standaardwachtwoord? En/of heeft bekende kwetsbaarheden zoals ingebakken systeem wachtwoorden die niet uit te schakelen zijn (backdoor toegang).

4.1 DUIDING VAN DIGITALE KWETSBAARHEDEN

4.1.1 RISICO (KANS X IMPACT)

Het NCSC¹⁸ geeft adviezen naar aanleiding van een gevonden kwetsbaarheid of geconstateerde dreiging. Deze worden ingeschaald op de kans dat de kwetsbaarheid wordt misbruikt en de ernst van de schade die optreedt wanneer de kwetsbaarheid misbruikt wordt. (Kans x Impact).

In dit onderzoek ligt de focus op het in kaart brengen van digitale kwetsbaarheden die in potentie vanaf internet misbruikt kunnen worden om daarmee oneigenlijk toegang te verkrijgen tot devices. Via deze toegang ontstaan mogelijkheden om onheil aan te brengen. De impact hiervan kan “groot” zijn. Bijvoorbeeld als kwetsbare routers worden geïnfecteerd, zoals in de VPNfilter⁸⁵ acties, waarbij deze devices qua besturing overgenomen worden om daarmee bijvoorbeeld DDoS-aanvallen te kunnen uitvoeren.

4.1.2 BUITEN SCOPE: IMPACT

Een nadere analyse van de daadwerkelijke impact voor een ander bij het oneigenlijk verwerven van (hoge) rechten, ofwel andere mogelijkheden om bij een ander onheil aan te brengen, is buiten scope van dit onderzoek. Dit is niet vooraf te bepalen en zou per casus nader geanalyseerd moeten worden.

4.2 OMVANG KWETSBARE SYSTEMEN IN NEDERLAND

Het aantal kwetsbaarheden waar een zogenaamde CVE¹⁹ voor is opgesteld incl. security patch is rond de 94.000. Een CVE (Common Vulnerabilities and Exposure) is een registratie in een CVE databank van informatie over kwetsbaarheden in computersystemen en netwerken. Deze databank heeft als doel om het delen van deze informatie, volgens een bepaalde standaard, te vereenvoudigen. Echter niet voor alle potentiële kwetsbaarheden is een CVE beschikbaar zoals een onjuiste secure inrichting of standaardwachtwoorden. M.a.w. de potentiële mogelijkheden van een kwaadwillende actor strekt verder dan enkel de CVE's.

Nederland staat op nummer 7 op de wereldranglijst wat betreft onveilige blootstellingen via het internet⁸⁶ Met onveilige blootstellingen wordt bedoeld (a) een van nature niet-versleutelde service op het openbare internet, (b) het aanbieden van een “service” die niet geschikt is voor openbare toegang, of (c) verbindingsooze communicatie waarvan misbruik kan worden gemaakt.

Om inzicht te verkrijgen in de omvang van kwetsbare ICT-systemen en IoT-apparaten is door GDI.Foundation aanvullende onderzoek verricht waaronder het uitvoeren van scans (zie tevens paragraaf 1.4).

4.3 GEMETEN DIGITALE KWETSBAARHEDEN

4.3.1 IPV4 VERSUS IPV6

Het primair risico is dat door een tekort aan IPv4 adressen het internet gebruik en daaraan gerelateerde economie niet verder kan groeien. Er zijn te weinig IPv4 adressen beschikbaar om devices op het internet mee te adresseren. Nieuwe ontwikkelingen als IoT zullen stagneren en niet optimaal ingezet kunnen worden. Met IPv6 wordt dit probleem opgelost.

Een bijkomend voordeel van IPv6 is dat het verkrijgen van informatie over de digitale omgeving van het doelwit lastiger is. Denk hierbij aan open poorten, de versie van besturingssysteem, welke services via die poorten draaien en welke kwetsbaarheden deze hebben. De mogelijkheden om snel de kwetsbaarheden van een digitale omgeving in kaart te brengen (footprinting, fingerprinting) en een gerichte aanval w.o. DDoS⁸⁷ & ⁸⁸ uit te voeren, wordt hiermee gereduceerd.

Het gebruik van **IPv6** adressen is binnen Nederland **12,6 %**. Nederland loopt hiermee achter bij het gebruiken van IPv6²¹ ten opzichte van bijvoorbeeld onze buurlanden Duitsland (36, 3%) en België (49,86%).

Gebruik van Internet Protocol			NLD
Hard to footprint (reconnaissance)	IPv6		12,6 %
Easy to footprint (reconnaissance ⁸⁹)	IPv4		87,4%

Kans voor attacker (groot)

Afhankelijk van het motief, de middelen en kennis van de (criminele) actor is de effort om aan de benodigde informatie te komen over de digitale omgeving van de target o.b.v. Ipv4 “laag”. De IPv4-structuur geeft een goed inzicht om gericht een aanval te kunnen verrichten op basis van gebruik van deze structuur door een organisatie. De effort om aan de benodigde informatie te komen is laag.

NB. Het gebruik van IPv6 levert ook nieuwe beveiligingsuitdagingen⁹⁰ & ⁹¹ op waar rekening mee gehouden moet worden. Zo is o.a. het gebruik van IPSec bij IPv6 niet langer verplicht gesteld.⁹² IPv6 mag dus ook via onbeveiligde verbindingen zoals Telnet of ProFTP worden gebruikt.

4.3.2 BROWSERS

De voornaamste browser die in Nederland gebruikt wordt betreft Chrome (+/- 50%)⁹³ vervolgens Safari (25%) en overige browsers als FireFox, Internet Explorer en Edge. In 2017 waren er 202 kwetsbaarheden in de Microsoft Edge browser ontdekt en updates verstrekt. Safari volgt op een tweede plek met 178 beveiligingslekken, gevolgd door Chrome (153) en Internet Explorer (79)⁹⁴.

Chrome versie 65.0 komt binnen Nederland het meest voor en heeft 45 kwetsbaarheden waarvan 9 kwetsbaarheden de score “hoog” hebben. De risico's worden gemitigeerd door het verrichten van de laatste update⁹⁵.

Kans voor attacker (klein)

Om ervoor te zorgen dat de eindgebruiker beschikt over de nieuwste beveiligingsupdate, controleert o.a. Chrome regelmatig of de nieuwste versie wordt gebruikt. De updatecontrole zorgt ervoor dat de versie van Chrome automatisch wordt bijgewerkt met de nieuwste beveiligingsfuncties en bugfixes, zonder dat de eindgebruiker hier iets voor hoeft te doen.

Updates vinden op de achtergrond plaats wanneer de browser wordt gesloten en opnieuw geopend⁹⁶.

4.3.3 WIFI CONNECTIES

Draadloos werken biedt vele voordelen maar kent – zeker in vergelijking met een netwerk met vaste aansluitingen - ook ernstige en specifieke dreigingen, die de betrouwbaarheid van de informatievoorziening van een organisatie kunnen aantasten⁹⁷.

Het aantal WiFi-netwerken in Nederland is meer dan 6 miljoen³³. Daarvan zijn er meer dan 3,7 miljoen een veilige (beperkt veilige) verbinding (WPA2). In de onderstaande tabel zijn de meest onveilige WiFi-protocollen en aantallen opgenomen:

Kwetsbare WiFi connecties		NLD
Unsecure WiFi encryption	WEP (Wired Equivalent Privacy)	55.2381
	WPA (Wifi "Protected" Access)	648.844

Kans voor attacker (groot)

De mogelijkheden voor een attacker om misbruik te maken van WiFi is onder andere beschreven in de whitepaper *"De onderschatte schakel in netwerkbeveiliging"* en *"KRACK-aanvalstechniek: kwetsbaarheid in wifi-netwerken"*⁹⁸.

4.3.4 ROUTERS/ MODEMS

Met betrekking tot de zakelijke markt is CISCO de absolute marktleider (76,4 %) en HPE/Aruba met 14,3% op een tweede plaats. Juniper is met 3 procent de enige andere partij die boven de 1 procent scoort. De grootste internetaanbieders voor particulieren in Nederland zijn KPN en Ziggo. KPN⁹⁹ levert met name de ExperiaBox en ZTE modems. Bij Ziggo wordt momenteel een Connectbox verstrekt. Een volledige lijst van modems en routers die door Ziggo³⁷ in de afgelopen jaren zijn geleverd is terug te vinden op hun site.

Tijdens de scan zijn een aantal routers/ modems nader geanalyseerd op kwetsbaarheid waaronder de ZTE.

Kwetsbare Modems / Routers		Wereldwijd	NLD
Vulnerable Modem/ Router ¹⁰⁰	HUAWEI	28.9371	55
	ZTE	20.7246	3.054
	ZyXEL	714.448	622
	TP-Link	617.292	682
	D-Link devices in NL ^{101 & 102}	267.501	829
	Arris (ARRIS DOCSIS 1.1 / SIP 2.0 Touchstone Telephony Modem)	45	29
Devices with unsafe default credentials ¹⁰³	Password exposure in the banner [admin+1234]	8.563	73
	Default password in the banner ["default password"]	6.8786	430

Kans voor attacker (groot)

De mogelijkheid en kansen voor attackers is o.a. door de US-CERT nader beschreven in “*Cyber Actors Target Home and Office Routers and Networked Devices Worldwide*”¹⁰⁴ {mei 2018} en “*Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices*”¹⁰⁵ {april 2018}. Makkelijk te raden userid & wachtwoorden behoeven vanuit onze optiek geen nadere toelichting daar het risico zeer evident is.

4.3.5 WEBSITES

Wereldwijd zijn er meer dan 1.5 miljard websites op het internet¹⁰⁶. Hiervan hebben er 5,8 miljoen een .nl-extensie. 3,6 miljoen .nl-websites¹⁰⁷ staan met hun domeinnaam geregistreerd en waarvan er ruim 500.000 een SSL-certificaat (15,5%) hebben.

In Nederland zijn 6.065 websites¹⁰⁸ die volledig voldoen aan de moderne internetstandaarden. Een onderdeel om een 100% score te bereiken is het gebruik van DNSSEC, HTTPS en IPv6. Eerder was al vastgesteld dat het aantal IPv6-adressen 12,6% is binnen Nederland.

Tijdens de scan zijn een tweetal kwetsbaarheden van de “Top 10 grootste kwetsbaarheden” die een website met zich meebrengen nader onderzocht, waaronder het verkrijgen van het hoogste recht en de toegang tot de data.

Kwetsbare Websites		NLD
Access control ¹⁰⁹ (<i>Index site</i>)	in url:/sym/root/ intitle:index.of site:*.NL	28
Sensitive data exposure ¹¹⁰ (<i>Open Web DataBase</i>)	in text:"Index of /database" site:*.nl	1.293
	in text:"Index of /database" site:*.nl	3.390
	in text:"Index of /.git" site:*.NL ¹¹¹	37
Poor Encryption	not SSL (HTTPS)	> 3.000.00

Kans voor attacker (top 10 OWASP)

Gedetailleerde informatie over de kansen voor een attacker is terug te vinden op OWASP¹¹² met onder andere de “*Top 10 Most Critical Web Application Security Risks*”. Verder is door het NCSC de whitepaper “*ICT-Beveiligingsrichtlijnen voor Webapplicaties*”¹¹³ waarin informatie is te vinden over het waarom en hoe het risico te mitigeren.

4.3.6 AANTAL DESKTOP / SERVERS (WINDOWS)

Windows is veruit het meest populaire besturingssysteem voor desktopcomputers in Nederland (81%). Het aantal kwetsbaarheden van de verschillende versies van Windows is iets meer dan 8.900¹¹⁴ waarvan 2.033 een score hebben van hoger >9¹¹⁵.

Tijdens het moment van de uitgevoerde scan waren er meer dan 70.000 Windows desktops e/o Servers aangesloten op het Nederlandse internet. Hieronder is aangegeven hoeveel kwetsbare Windows versies er online waren. Er is geen nadere analyse verricht of de meest recente security patch geïnstalleerd is waarmee de kwetsbaarheid gemitigeerd is.

Kwetsbare Windows Desktop / servers (CVE >9 & q > 1.000)		NLD
End of Life & Extended support	Windows 5.0/ 5.1/ 6.1 Windows Server 2003 ¹¹⁶ Windows XP ¹¹⁶ / Windows 2000	2.540
CVE score > 9 & Aantal > 1.000	Windows 7 or 8 Windows Server 2008 R2 ¹¹⁶ Windows Server 2012 R2 Datacenter & Standard 9600	39.678

Kans voor attacker (klein)

Om ervoor te zorgen dat de gebruikers beschikken over de nieuwste beveiligingsupdate, voorziet Microsoft in een actief beveiligingsupdatebeleid voor de gebruikers.

4.3.7 INTERNET OF THINGS (IOT)

In hoofdstuk 3 is eerder ingegaan op IoT, gebruik, techniek en ecosysteem. Net als met andere nieuwe technieken en innovatie, ligt de focus van IoT niet primair op security gerelateerde aspecten.

Door de Cyber Security Raad (CSR) is een nadere analyse van de kansen en bedreigingen van IoT in een rapport¹¹⁷ beschreven waarin zij haar zorgen uit over de beheersbaarheid van het IoT als het om cybersecurity en privacy gaat. Voor het nader duiden van het type risico is mede gebruik gemaakt van de Top10 lijst van OWASP inzake IoT. Hieronder staan de door ons gevonden kwetsbare IoT op basis van de uitgevoerde scan.

Kwetsbare IoT		Wereldwijd	NLD
Devices with default credentials ^{103 & 118}	GPon Home gateway	710.809	73
	iOmega (network storage)	19.551	722
	AVTech (upnp) {webcam}	80.924	817
	Netcam {webcam}	8.900	161
	Dahua {webcam}	337.791	4.321
	Netatmo {webcam}	3.840	843
Insecure Installed Gateways	RasPi	3.823	9
	BusyBox	6.333	4
	INSTEON SmartLinc Home gateway	33	7
	Dreambox	2.787	74
Unencrypted Services ¹¹⁸	MQTT {port:1883}	36.554	1.091
	TR-069 {port:7547}	24.745.091	4.800

Kans voor attacker (groot)

De kans dat een kwetsbaarheid wordt gesignaleerd en gecorrigeerd door de eindgebruiker is niet groot. Verder ontbreekt er veelal een actief securityupdatebeleid, aanwezigheid van hardening en aansluit criteria in de volledige (IoT) keten en control mechanismen c.q. early alerts bij afwijking in de cybersecurity en eventuele schending van de privacy.

De meest **urgente bedreigingen** van het IoT worden gevormd door risico's op het **gebied van veiligheid en privacy**.

Veiligheidsrisico's liggen onder meer op het gebied van cybercriminaliteit, zoals het **inbreken in en overnemen van IoT** - apparaten en het **stelen van data**. Daarnaast kunnen *disfunctionerende IoT* - apparaten veiligheidsrisico's met zich meebrengen. Bedreigingen op het gebied van privacy zijn het risico op privacyschending, bijvoorbeeld door het gebruik van (gevoelige) gegevens voor andere doeleinden dan waarvoor ze verzameld zijn. Deze bedreigingen hangen sterk samen met veiligheidsrisico's.

Wanneer de beveiliging van IoT - toepassingen niet op orde is, wordt de kans dat kwaadwillende personen toegang krijgen tot persoonsgegevens groter. Ook bedreigingen op het gebied van andere waarden brengen veiligheidsrisico's met zich mee. **Hoe afhankelijker we bijvoorbeeld worden van technologie en grote (buitenlandse) bedrijven, des te groter de gevolgen kunnen zijn als er iets misgaat.**

Bron: "[\(Verkeerd\) verbonden in een slimme samenleving Het Internet of Things: kansen, bedreigingen en maatregelen](#)"

4.4 OVERIGE DIGITALE KWETSBAARHEDEN

4.4.1 "OPEN" BIG DATA

De toename in de vastlegging van data (big data) en uitwisseling van data e/o informatie creëert nieuwe mogelijkheden voor allerlei doeleinden. Maar dit creëert ook mogelijkheden voor kwaadwillende actoren. Denk hierbij aan verkoop van data, gebruiken van de verkregen data als creditcardgegevens en (toekomstige) afpersing van organisaties i.h.k.v. GDPR compliancy en boetes (4% van de omzet). Het afgelopen jaar is het lekken van grote hoeveelheden aan (kritieke) data ook regelmatig voorgevallen.

In de tabel hieronder zijn een aantal databases (DB) opgenomen die "open" staan voor eenieder met een internetconnectie. Deze DB's hebben een directe connectie met het internet.

"Open" Big Data (DB)		Wereldwijd	NLD
Sensitive data exposure (unsafe defaults)	MongoDB	58.323	2.105
	ElasticSearch	37.116	666
	Redis	21.107	667
	Memcached ¹¹⁹	91.184	2.517
	Cassandra	1.460	46
	CouchDB	5.318	354

Kans voor attacker (groot)

De data is voor eenieder kwaadwillende actor "zeer" gemakkelijk te verkrijgen. Ondanks wereldwijde waarschuwingen is de lek (unsecure install e/o verouderde versie) nog steeds aanwezig en neemt het aantal "open" DB's weer toe. Monitoring tooling, wat alleen gebruikt maakt van de CVE-kwetsbaarheden, detecteert geen kwetsbaarheden die veroorzaakt worden door een onveilige inrichting (configuratie).

4.4.2 INDUSTRIAL CONTROL SYSTEM

Veel organisaties zetten ICS/SCADA (Industrial Control Systems) in voor primaire procesbesturing; van het aansturen van apparaten bij olieraffinaderijen tot nucleaire installaties of waterzuivering. De dreiging van hackers op deze systemen neemt toe en daarmee ook de aandacht van security-onderzoekers voor de beveiliging van deze systemen¹²⁰.

Bij procesautomatisering is het belangrijk dat fabrieken kunnen blijven draaien, treinen kunnen blijven rijden, stoplichten blijven werken. Indien het systeem niet beschikbaar is vanwege uitvoering van een patch, kan dit veel geld kosten en zelfs tot maatschappelijke ontwrichting leiden.

Kwetsbare ICS		Wereldwijd	NLD
PLC	Siemens	2.788	45
	GE-SRTP	20.352	200
	PLC Works	788	83
	FINS)	115	71
	ProCroNos	180	0
SCADA	HART (port:5094 hart-ip)	121	30
	Red Lion (port:789 product:"Red Lion Controls")	1.088	0
DCS	Modbus	13.817	137
	DNP3	347	0
	Niageria Fox	49.766	1.399
	MELSEC-Q (mitsubishi)	114	1
RTU	BACnet (Achmea)	13.744	34
	EtherNET (port:44818)	28.656	706
	CODESYS (port:2455 operating system)	2.154	62

Kans voor attacker (hoog)

De mogelijkheid en kansen voor attackers om ICS systemen die via internet zijn te benaderen daadwerkelijk te misbruiken is groot. Vaak gaat het om oude systemen (legacy) die niet regelmatig vervangen worden. Het patchen van ICS systemen loopt dan ook niet synchroon met de huidige mogelijkheden en bekende kwetsbaarheden.

4.4.3 PROTOCOLLEN & SERVICES

Elke poort en onderliggende service heeft zijn risico's. Het risico is afkomstig van de versie van de service, of iemand deze correct heeft geconfigureerd en de mate van encryptie.

In principe is elk protocol waarbij de controle van authenticiteit, integriteit en vertrouwelijkheid niet plaatsvindt onveilig. Ook is het belangrijk om alle andere (overbodige) protocollen en services uit te schakelen zodat de kans op misbruik van deze protocollen/services wordt gemitigeerd.

Elke communicatie die gevoelige gegevens, w.o. password & userid, verzendt over het openbare netwerk, zou een gecodeerd kanaal moeten gebruiken zoals SSL/TLS of bijvoorbeeld IPSEC. De voorkeur gaat uit naar hoe kritieker de informatie is, des te sterker de cryptografie van het versleutelde protocol moet zijn. ^{121 & 122}

Kwetsbare remote protocollen		Wereldwijd	NLD
Lack of Transport Encryption/ Integrity	ProFTP	-	5.750
	Open SSH	7.747.342	202.684
Unsecure (network) Software	Dnsmasq ¹²³	1.393.329	1.538
	gSOAP ¹²⁴	187.721	431
Remote Control with default credentials	RDP (Remote Desktop)	434.750	38.240
	VNC	207.213	4.486

Kans voor attacker (hoog)

Het aantal bekende exploits en tooling om misbruik te maken van onveilige protocollen en services is groot^{121 & 125}. Dit vereist weinig kennis e/o kunde en is via google voor een ieder te vinden.

4.5 SUB CONCLUSIE

Nederland staat op nummer 7 op de wereldranglijst wat betreft *onveilige* blootstellingen via het internet op basis van verrichte portscan⁸⁶. Het door GDI.Foundation uitgevoerde onderzoek heeft vastgesteld dat er in Nederland bijna 1,5 miljoen kwetsbare apparaten/ protocollen waren tijdens de scan. Op basis van verder onderzoek blijkt dat hiervan 287.717 apparaten/ protocollen daadwerkelijk te misbruiken zijn. De scan heeft een beperkte scope en is op basis van de field research gebleken dat de mogelijkheden voor een kwaadwillende actor veel verder strekt.

Het aantal gedetecteerde onveilige IoT-apparaten in Nederland is in relatie met de rest van de wereld nog beperkt. Echter de ontwikkelingen en gebruik van IoT staat nog in de kinderschoenen, de voordelen zijn groot en het gebruik neemt elke dag toe

Het merendeel van de detecteerde kwetsbaarheden heeft betrekking op bekende kwetsbaarheden zoals het gebruiken van onveilige protocollen, onveilige inrichting van de IT en het nog steeds voorkomen van een standaardwachtwoord. Wij hebben geen aanvullende analyses uitgevoerd wat hier de impact van is. Het is voor ons ook niet zichtbaar of kwetsbaarheden onderdeel uitmaken van de voor Nederland vitale processen. Een voorbeeld hiervan zijn de gevonden kwetsbaarheden inzake ICS-systemen die een mogelijk cruciaal onderdeel kan uitmaken van het energienetwerk.

5 AANVULLENDE BEVINDINGEN

Op basis van de research en nadere analyses hebben wij enkele hoofdbevindingen en “lessons learned” geëxtraheerd.

5.1 HUIDIGE SITUATIE

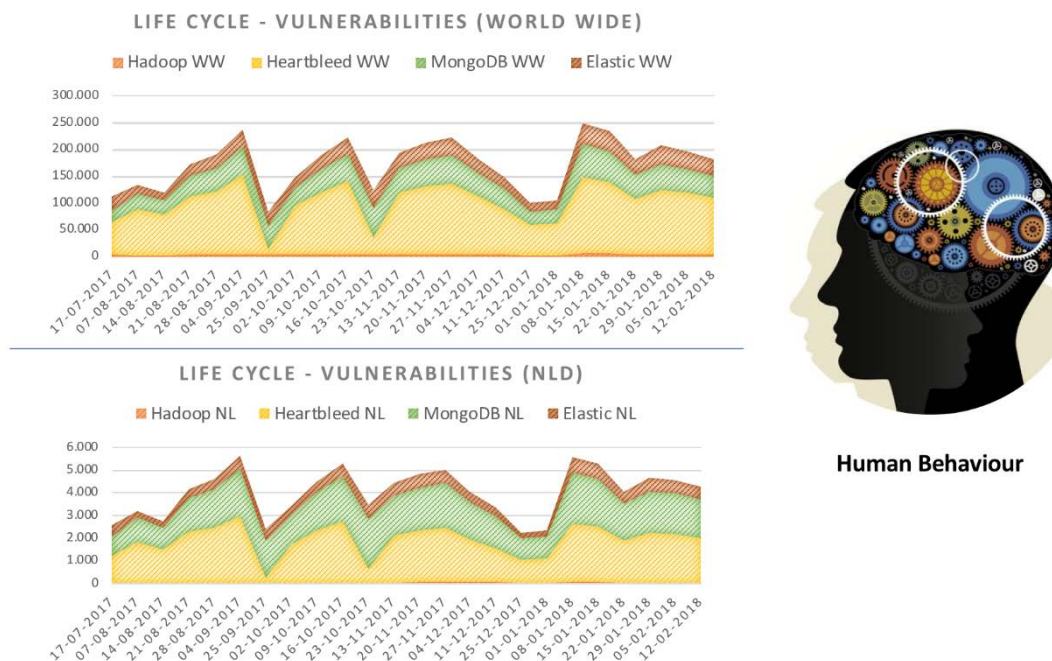
- **“Time to Market” v.s. “Security by Design”.** Het verlagend effect op de kostprijs, het (ogenschijnlijk) gemak en de verkorting van de doorlooptijd voor het creëren van nieuwe digitale diensten en producten voor zowel business als consumenten, leidt nu al tot toename^{126 & 127}. Eenieder over de wereld is in staat om een product of dienst te ontwikkelen en aan te bieden via het internet waarbij de ontwikkelkosten bijzonder laag (kunnen) zijn. Dit leidt tot vele nieuwe producten en diensten waarbij “security/ privacy by design” niet altijd gewaarborgd is.
- **Toename “intrusion paths” en potentiële security kwetsbaarheden.** Het verbinden van alles met iedereen gebeurt middels een breed scala aan protocollen en verbindingen. Al deze protocollen en verbindingen hebben in potentie kwetsbaarheden die misbruikt kunnen worden. IoT en IT liggen in elkaars verlengde waardoor het aantal connecties en dus ook de kwetsbaarheden toenemen.
- **(Mondiale) Data governance ontbreekt.** De signalen van IoT in combinatie met vergaren van andere databronnen (Big Data) zijn niet transparant, grensoverschrijdend en er ontbreekt governance hoe hier mee om moet worden gegaan. Een belangrijk vraagstuk is bijvoorbeeld of de signalen van IoT onder de GDPR (General Data Protection Regulation) vallen? Wie is eigenaar en wie zijn de verwerkers van de IoT signalen en is de eindgebruiker op de hoogte van wat met wie wordt gedeeld, met welk doel en wat er met die informatie gedaan wordt?
- **Industriestandaards, keurmerken en/of richtlijnen om een secure IoT te borgen zijn niet aanwezig.** Er zijn nog geen of onvoldoende standaarden ontwikkeld om IoT op een voldoende veilige manier te ontwikkelen. Daar waar er al standaarden zijn, worden deze nog onvoldoende afgedwongen e/o geëist voordat een IoT-product of -dienst in gebruik kan worden genomen. Voor afnemers is het op deze manier niet vast te stellen of de producten en diensten veilig te gebruiken zijn.
- **De kaders en controls inzake de cyber security van IoT is laag.** Kwetsbaarheden, onveilige verbindingen e/o ongeautoriseerde toegang (autorisaties) worden niet preventief voorkomen, gedetecteerd en/of gemonitord. Garanties (assurance) in welke mate de keten “secure” en privacy compliant is (van device tot aan opslag), is derhalve nog niet aanwezig. Controls, compliance control frameworks, richtlijnen en andere security eisen ontbreken t.a.v. IoT gebruik, data en beheer.

5.2 LESSONS LEARNED & GEDRAG

Uit het verleden is gebleken dat een groot aantal hacks hebben plaatsgevonden op basis van relatief eenvoudige kwetsbaarheden als het hebben van een standaardwachtwoord, onveilige verbindingen en/of onjuiste technische inrichting (software). Adequaat testen kost tijd en geld en conflicteert veelal met “time to market” en kostprijs.

In 2017 is in samenwerking met SURFnet, de lifecycle van een aantal kwetsbaarheden gevolgd. Het betreft onder andere een aantal databases waarvan met zekerheid gesteld kan worden dat deze te hacken zijn en zelfs dat deze gehackt zijn (o.a. MongoDB).

Ondanks de internationale aandacht en persberichten is een toename van deze kwetsbaarheden te constateren. Hierbij valt op dat Nederland eenzelfde trend beeld laat zien als in rest van de wereld.



Figuur 11 – Life Cycle Vulnerability: Trends and Human Behaviour (bron: V.E.Toms - GDI.Foundation)

In het vorige hoofdstuk is eerder gebleken dat het gebruik van onveilige protocollen en het gebruik van standaardwachtwoorden nog steeds voorkomen. Aspecten waarvan verwacht mag worden dat deze niet meer voorkomen.

5.3 HOE “SMART” IS ONZE TOEKOMST

We moeten ons bewust worden van de ontwikkelingen die er allemaal aan staan te komen, noem het de kansen, en we moeten ons ook bewust worden van de bedreigingen¹²⁸. Bewustwording van kwetsbare apparaten en verbindingen is alleen de eerste stap. Dit is nog onvoldoende om de situatie te verbeteren.

Het aantal gedetecteerde onveilige IoT-apparaten in Nederland is in relatie met de rest van de wereld nog beperkt. Echter de ontwikkelingen en het gebruik van IoT staan nog in de kinderschoenen, de voordelen zijn groot en het gebruik neemt elke dag toe. De ontwikkelingen m.b.t. Big Data, Cloud en Artificial Intelligence (AI) worden steeds vaker gecombineerd met IoT-data en is grens/continent overstijgend. “Time to market” en gebruiksgemak worden belangrijker gevonden dan “security/privacy by design” bij de ontwikkeling en productie van IoT-apparaten.

Vanuit privacy en security optiek levert met name de IoT-apparaten voor de consument, een groot risico op. De nu ogenschijnlijke beperkte impact van onveilige IoT zal gezien de explosie in gebruik (20.8 miljard in 2020¹) en door het ontbreken van toezicht op secure/privacy compliant apparaten, in de nabije toekomst grote invloed hebben op ons dagelijks leven, besluitvorming en privacy. Het moment van misbruik, op welke wijze (protocol, device, autorisatie, malware, etc.) en het doel (bijv. DDOS) is helaas niet of nauwelijks te voorspellen.

De Cyber Security Raad heeft in 2017 gepleit¹²⁸ voor *“Een onafhankelijke monitor van gehackte en kwetsbare IoT-apparaten, zodat publieke informatie beschikbaar komt over welke fabrikanten en leveranciers hun apparaten onvoldoende beveiligen.”*

GDI.Foundation steunt dit advies en is van mening dat nietsdoen geen optie is. Tijdigheid in het handelen is echter wel een belangrijke factor om de digitale hygiëne te borgen. Zeker gezien de snelheid van de huidige ontwikkelingen, mogelijkheden en belangen. Hierbij kunnen we ons afvragen wie er in staat is om er iets aan te doen. Is er überhaupt draagvlak of ruimte binnen de politieke en economische kaders om iets te verbeteren? Is dit een taak voor de overheid of hoort de commercie hier een oplossing voor te bieden. Of is er een mogelijke vorm van samenwerking te realiseren waar beide een rol in kunnen spelen?

GDI.Foundation is van mening dat we bij het maken van keuzes en maatregelen niet tegen de verandering moeten zijn. De verandering is niet te stoppen en biedt mooie mogelijkheden. Echter vroegtijdige detectie van toekomstige bedreigingen (bijv. IoT), tijdige bijsturing op negatieve effecten, het treffen van preventieve maatregelen en het proactief informeren van (potentiële) slachtoffers, zijn keuzes die gemaakt moeten worden en acties die uitgevoerd moeten worden om de digitale hygiëne van Nederland te bewaken.

6 CONCLUSIE EN AANBEVELINGEN

6.1 BELANGRIJKSTE BEVINDINGEN

Door GDI.Foundation is op verzoek van NCSC een onderzoek verricht naar het Nederlandse digitale landschap, IoT en de kwetsbaarheden in het Nederlandse digitale landschap.

Hieruit is gebleken dat de connecties van het Nederlandse digitale landschap met het internet divers is en het gebruik (“afhankelijkheid”) van internet groot is. Niet alleen qua data maar ook het aantal gebruikers en type apparaat dat hiervoor gebruikt wordt. Opvallend hierbij is dat bepaalde producten van leveranciers een groot marktaandeel hebben, zoals CISCO, in de aansluiting met het internet. Een eventuele kwetsbaarheid in één van deze producten en niet tijdig mitigeren van het risico, kan derhalve grote impact hebben voor onze samenleving.

Met de introductie van IoT en de connectiviteit met internet, de IT-omgeving e/o andere IoT netwerken, ontstaan er meerdere en nieuwe connectiviteiten. Binnen Nederland zijn KPN (commercieel) en TTN (gratis) de voornaamste en meest prominente spelers met het aanbieden van een IoT-netwerk in Nederland. Het (ogenschijnlijk) gemak en de verkorting van de doorlooptijd voor het creëren van nieuwe digitale diensten en producten voor zowel business als consumenten, leidt tot toename in het gebruik van IoT.

Met name consument gerelateerde (IoT) apparaten, de onduidelijkheid voor de koper in welke mate voldoende privacy en security gerelateerde maatregelen aanwezig zijn, welke maatregelen de gebruiker zelf moet treffen en ook het vooraf weten wat met (persoonlijke) digitale data gebeurt, is een groot zorgpunt. Tijdige signalering en proactieve informatiedeling (early warning system/ alerts) om te kunnen corrigeren ontbreekt in de keten richting de gebruiker.

Het onderzoek heeft vastgesteld dat er in Nederland bijna 1,5 miljoen kwetsbare apparaten/ protocollen waren tijdens de scan. Op basis van verder onderzoek blijkt dat hiervan 287.717 apparaten/ protocollen daadwerkelijk te misbruiken zijn. Een groot aantal de gedetecteerde kwetsbaarheden heeft betrekking op bekende kwetsbaarheden als standaardwachtwoord en het gebruik van onveilige protocollen. Dit beeld wordt bevestigd in het rapport en onderzoek van Rapid7. Nederland staat op nummer 7 op de wereldranglijst wat betreft *onveilige* blootstellingen via het internet op basis van verrichte portscan⁸⁶.

Ten aanzien van aantal gedetecteerde onveilige IoT-apparaten in Nederland is deze nog beperkt in relatie met de rest van de wereld. Echter de ontwikkelingen en gebruik van IoT staat nog in de kinderschoenen, de voordelen zijn groot en het gebruik neemt elke dag toe.

Het kunnen steunen op een betrouwbare en secure verwerking in de volledige keten, van IoT data tot en met de cloud, is nog als pril te bestempelen. Industriestandaards, keurmerken en/of richtlijnen om een secure IoT te borgen zijn niet wettelijk verplicht, compliance controls & frameworks, richtlijnen en andere security eisen zijn onvoldoende aanwezig. Maar ook de governance inzake de IoT-data en wetgeving hieromtrent is nog onvoldoende uitgewerkt (GDPR).

6.2 MOGELIJKHEDEN OM RISICO'S TE MITIGEREN

Gezien de ontwikkelingen en gebruik van IoT is de kans zeer aannemelijk dat het aantal kwetsbare apparaten en onveilige connecties toe zal nemen. Het hebben van industrie standaarden, securityratings van leveranciers & producten, meetbare hardeningsguidelines en connectiviteit eisen maar ook meetbaarheid & verantwoording door leveranciers over “Security by design” en “Privacy by design” in de levenscyclus van een product of dienst en toezicht hierop, vormen een belangrijke meerwaarde om de dreigingen en de impact hiervan beter te beheersen.

De voornaamste uitdagingen waar we met z'n allen voor staan om de digitale hygiëne op peil te houden zijn:

- **Structureel inzicht** verkrijgen in de ontwikkeling van IoT & IT zodat overheden e/o andere verantwoordelijke instanties, tijdig kunnen bijsturen op negatieve effecten van onveilige apparaten voor de maatschappij en burger.
- Het komen tot **keurmerken/ kwaliteitseisen** en **onafhankelijk toezicht** hierop, zodat de gebruiker onderscheid kan maken tussen veilige (IoT/IT) apparaten of minder veilige (IoT/IT) apparaten.
- **Aansprakelijkheid in de keten** bij het waarborgen van privacy & security gerelateerde aspecten in de grens overstijgende keten van dienstlevering en data.
- De aanwezigheid van **industrie standaarden**, meetbare **hardeningsguidelines & connectivity eisen** en **geautomatiseerde security updates** in de levenscyclus van een product of dienst en keten.
- **Toetsing en de verantwoording van leveranciers** over de getroffen maatregelen omtrent de adequaatheid in de bescherming van **gedrag (privacy) gerelateerde IoT-informatie**. Valt IoT gerelateerde data nu wel/niet in scope van de algemene verordening gegevensbescherming (AVG) en welke waarborgen heb je als consument/afnemer?

Met name het laatste punt is tot op heden onderbelicht en zal gezien de huidige ontwikkelingen (4^{de} industriële revolutie¹²⁹, data-economie en toename van IoT) in de nabije toekomst een groot zorgpunt worden wat nu de nodige aandacht behoeft.

6.3 AANBEVELINGEN

Behoudens de eerder vermelde uitdagingen is de voornaamste aanbeveling het z.s.m. in uitvoering brengen van het eerder uitgebrachte advies van CSR¹²⁸

- ❖ Het z.s.m. implementeren van **“Een onafhankelijke monitor van gehackte en kwetsbare IoT-apparaten, zodat publieke informatie beschikbaar komt over welke fabrikanten en leveranciers hun apparaten onvoldoende beveiligen”**.

Inzicht voor de eindgebruiker/afnemer is essentieel bij het kunnen maken van een keuze. Een onderdeel wat nu ontbreekt.

We moeten bij het maken van keuzes en maatregelen niet tegen de verandering zijn. Die verandering is niet te stoppen en biedt mooie mogelijkheden. Echter vroegtijdige detectie van toekomstige bedreigingen (bijv. IoT), tijdige bijsturing op negatieve effecten, het treffen van preventieve maatregelen en ook het proactief informeren van (potentiële) slachtoffers zijn keuzes en acties die gemaakt moeten worden om de digitale hygiëne van Nederland te bewaken.

BRONVERMELDING

- ¹ <https://www.wodc.nl/onderzoeksdatabase/2734-kansen-en-bedreigingen-internet-of-things.aspx>
- ² <https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update>
- ³ https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf
- ⁴ <https://www.ad.nl/digitaal/zijn-jouw-data-gelekt-via-facebook-vandaag-weet-je-het~a6f0f517/>
- ⁵ <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>
- ⁶ https://www.cybersecurityraad.nl/binaries/CSR_Advies_IoT_NED_tcm107-314537.pdf
- ⁷ <https://www.sidnfonds.nl/projecten/internet-en-cyber-security-health-check>
- ⁸ <https://www.surf.nl/persberichten/2016/02/surf-security-award-2016-voor-gdi-foundation.html>
- ⁹ <http://hadoop.apache.org/>
- ¹⁰ <https://www.elastic.co/products>
- ¹¹ <https://github.com/sbeyn/kibana-plugin-traffic-sg>
- ¹² <https://www.shodan.io/>
- ¹³ <https://censys.io/>
- ¹⁴ <https://zmap.io/>
- ¹⁵ <https://ipinfo.io/>
- ¹⁶ <https://nmap.org/>
- ¹⁷ <http://osintframework.com/>
- ¹⁸ <https://www.ncsc.nl/actueel/beveiligingsadviezen>
- ¹⁹ <https://cve.mitre.org/>
- ²⁰ <https://lite.ip2location.com/netherlands-ip-address-ranges>
- ²¹ <https://www.google.com/intl/nl/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption>
- ²² <https://ams-ix.net/technical/statistics/route-server-stats>
- ²³ <https://ams-ix.net/technical/statistics>
- ²⁴ <https://ams-ix.net/technical/statistics/historical-traffic-data?year=2001>
- ²⁵ <https://ams-ix.net/technical/statistics/historical-traffic-data?year=2017>
- ²⁶ <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/83429NED/table?ts=1528387112104>
- ²⁷ <https://www.sidn.nl/a/kennis/trends-in-internetgebruik>
- ²⁸ <http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83429NED&D1=0&D2=0,3-6&D3=0&D4=a&HDR=T&STB=G1,G2,G3&CHARTTYPE=1&VW=T>
- ²⁹ & <https://www.cbs.nl/nl-nl/nieuws/2018/05/nederland-koploper-in-europa-met-internettoegang>
- ³⁰ <http://gs.statcounter.com/browser-market-share/all/netherlands>
- ³¹ Google analytics, Statista.com, Statcounter.com
- ³² <http://gs.statcounter.com/os-market-share/desktop/netherlands#monthly-201708-201709-bar>
- ³³ <https://wicle.net/stats#geostats>
- ³⁴ <https://www.kpn.com/internet/wifi-hotspots.html>
- ³⁵ <https://www.computable.nl/artikel/nieuws/infrastructuur/6343323/250449/ciscos-aandeel-in-netwerkapparatuur-blijft-teruglopen.html>
- ³⁶ <https://www.kpn.com/search.htm?q=modem>
- ³⁷ <https://www.ziggo.nl/klantenservice/wifi/modem/>
- ³⁸ Shodan, port 80, 443 Country.nl
- ³⁹ <http://www.zigbee.org/>
- ⁴⁰ <https://www.postscapes.com/internet-of-things-history/>
- ⁴¹ <https://www.agentschaptetelecom.nl/documenten/rapporten/2017/december/6/onderzoek-dialogic-over-internet-of-things>
- ⁴² <http://www.ioti.com/agriculture> & <http://iotlineup.com/>
- ⁴³ https://www.bol.com/nl/p/proximo-fob-phone-and-key-finder-for-ip/9200000012124331/#product_specifications
- ⁴⁴ <http://waterbuoy.sensemakers.info/>
- ⁴⁵ <https://www.usa.philips.com/healthcare/innovation/about-health-suite>
- ⁴⁶ <https://siemens.mindsphere.io/>
- ⁴⁷ <https://www.kvk.nl/over-de-kvk/media-en-pers/nieuws-en-persberichten/internet-of-things-verdienmodel-van-de-toekomst/>
- ⁴⁸ https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

⁴⁹ <https://dzone.com/articles/iot-systems-sensors-and-actuators>

⁵⁰ <https://www.eneco.nl/energieproducten/toon-thermostaat/>

⁵¹ <https://www.stratix.nl/media/media/documents/rapport-internet-of-things-in-the-netherlands.pdf>

⁵² <https://internetofthingsnederland.nl/iot-netwerken/>

⁵³ https://www.acm.nl/sites/default/files/old_publication/publicaties/16001_097-en-06-nummers-informatie-voor-telecomaanbieders-20160701.pdf

⁵⁴ https://www.postscapes.com/internet-of-things-hardware/#iot-board-comparison/?view_218_search=Linux&view_218_page=1

⁵⁵ <http://iotlineup.com/>

⁵⁶ <http://www.devicegateway.com/main-iot-protocols>

⁵⁷ <https://www.agentschaptelecom.nl/over-agentschap-telecom/organisatie>

⁵⁸ <https://www.agentschaptelecom.nl/onderwerpen/nationaal-frequentieregister>

⁵⁹ <https://www.agentschaptelecom.nl/actueel/nieuws/2018/juni/04/onveilige-iot-apparatuur-risico-voor-samenleving>

⁶⁰ https://hcss.nl/sites/default/files/files/reports/HCSS_ICT_kwetsbaarheid_en_nationale_veiligheid.pdf

⁶¹ <https://www.nen.nl/Over-NEN/Onze-strategie.htm>

⁶² <https://www.nen.nl/NEN-Shop/Elektrotechniek-Nieuws/Werkgroep-Internet-of-Things-Security-IoTS-opgericht.htm>

⁶³ https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

⁶⁴ <https://www.itu.int/en/ITU-T/studygroups/com17/Pages/telesecurity.aspx>

⁶⁵ <https://communicatie.kpn.com/whitepaperiotsecurity>

⁶⁶ <https://www.digitaltrustcenter.nl/>

⁶⁷ <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>

⁶⁸ https://www.nist.gov/sites/default/files/documents/2018/04/13/iot_program_discussion_draft_april_2018.pdf

⁶⁹ <https://www.thethingsnetwork.org/country/the-netherlands/>

⁷⁰ <https://www.thethingsnetwork.org/map?gateway=32729>

⁷¹ <https://www.statista.com/statistics/686435/internet-of-things-iot-market-size-in-europe-by-country/>

⁷² https://overons.kpn/content/downloads/Infographic-Q1-2018_ENG.pdf

⁷³ <https://overons.kpn/nl/pers/kwartaalcijfers/publicatie-kpn-eerste-kwartaalcijfers-2018>

⁷⁴ https://annualreport2017.kpn/app/uploads/KPN_IR-2017_Single_navigation.pdf

⁷⁵ TNO (2015) Monitor Draadloze Technologie 2015. Trends en ontwikkelingen in de mobiele sector.

⁷⁶ <https://www.lora-alliance.org/>

⁷⁷ <https://www.acm.nl/sites/default/files/documents/telecommonitor-tweede-halfjaar-2017.pdf> &

⁷⁸ https://www.acm.nl/sites/default/files/old_publication/publicaties/17346_monitor-nummeruitgifte-2016-2017-06-19.pdf

⁷⁹ <https://loriot.io/lora-gateways.html>

⁸⁰ <https://www.security.nl/posting/494199/Grootschalige+aanval+op+dsl-routers+via+poort+7547>

⁸¹ [https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport?utm_medium=EM&asrc=EM_NLN_53091091&utm_campaign=20160204_Word%2520of%2520the%2520Day:%2520MQTT%2520\(MQ%2520Telemetry%2520Transport\)_kherbert&utm_source=NLN&track=NL-1823&ad=905763&src=905763](https://internetofthingsagenda.techtarget.com/definition/MQTT-MQ-Telemetry-Transport?utm_medium=EM&asrc=EM_NLN_53091091&utm_campaign=20160204_Word%2520of%2520the%2520Day:%2520MQTT%2520(MQ%2520Telemetry%2520Transport)_kherbert&utm_source=NLN&track=NL-1823&ad=905763&src=905763)

⁸² <https://nl.phhsnews.com/is-upnp-security-risk2635>

⁸³ <https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices>

⁸⁴ <http://avtech.nl/>

⁸⁵ <https://blog.talosintelligence.com/2018/05/VPNFilter.html>

⁸⁶ https://www.rapid7.com/globalassets/_pdfs/research/rapid7-national-exposure-index-2018.pdf

⁸⁷ <https://www.ncsc.nl/actueel/whitepapers/bescherming-tegen-ddos-aanvallen.html>

⁸⁸ <https://www.ncsc.nl/actueel/factsheets/factsheet-technische-maatregelen-voor-de-continuïteit-van-onlinediensten.html>

⁸⁹ https://pure.uva.nl/ws/files/2411235/157619_440188.pdf & <https://www.nlda-tw.nl/janmartin/vakken/TIOP/Cyber%20Warfare/Offensive%20cyber%20operaties%20versie%2014032011%20definitief%20DA%20Dreijer.pdf>

⁹⁰ <https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2014/rapport-ipv6-beveiliging.pdf>

⁹¹ <https://github.com/vanhauser-thc/thc-ipv6>

⁹² <https://tools.ietf.org/html/rfc6434#section-11>

⁹³ <https://netmarketshare.com>

⁹⁴ <https://www.cvedetails.com/browse-by-date.php>
⁹⁵ <https://chromereleases.googleblog.com/2018/03/stable-channel-update-for-desktop.html>
⁹⁶ <https://support.google.com/chrome/answer/95414?co=GENIE.Platform%3DDesktop&hl=nl>
⁹⁷ <https://www.ncsc.nl/actueel/whitepapers/whitepaper-wifi.html>
⁹⁸ <https://www.ncsc.nl/actueel/nieuwsberichten/krack-aanvalstechniek-kwetsbaarheid-in-wifi-netwerken.html>
⁹⁹ <https://www.kpn.com/service/internet/wifi-en-modems/handleidingen-experia-box.htm#!/devices/all/internet>
¹⁰⁰ zie bijv. <http://routerpwn.com/>
¹⁰¹ <https://www.quora.com/How-can-I-hack-a-d-link-routers-password>
¹⁰² <https://thehackernews.com/2016/09/hacking-d-link-wireless-router.html>
¹⁰³ zie bijv. <https://cirt.net/passwords>
¹⁰⁴ <https://www.us-cert.gov/ncas/alerts/TA18-145A>
¹⁰⁵ <https://www.us-cert.gov/ncas/alerts/TA18-106A>
¹⁰⁶ <http://www.internetlivestats.com/total-number-of-websites/>
¹⁰⁷ <https://www.sidn.nl/a/veilig-internet/ssl-anno-2018-onmisbaar-voor-elke-website-en-webshop>
¹⁰⁸ <https://internet.nl/halloffame/>
¹⁰⁹ https://www.owasp.org/index.php/Category:Access_Control
¹¹⁰ https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
¹¹¹ <https://en.internetwache.org/dont-publicly-expose-git-or-how-we-downloaded-your-websites-sourcecode-an-analysis-of-alexas-1m-28-07-2015/>
¹¹² https://www.owasp.org/index.php/Main_Page
¹¹³ <https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html>
¹¹⁴ https://www.cvedetails.com/product-list/product_type-o/vendor_id-26/firstchar-/Operating-Systems.html
¹¹⁵ <https://www.cvedetails.com/top-50-vendor-cvssscore-distribution.php>
¹¹⁶ <https://support.microsoft.com/en-us/lifecycle/search?alpha=Windows%20Server%202003>
¹¹⁷ https://www.cybersecurityraad.nl/010_Actueel/iot-toepassingen-vormen-bedreiging-voor-veiligheid-en-privacy.aspx
¹¹⁸ https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vulnerabilities
¹¹⁹ <https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-waarschuwt-voor-misbruik-publiek-beschikbare-memcached-systemen-bij-ddos-aanvallen.html>
¹²⁰ <https://www.ncsc.nl/actueel/nieuwsberichten/eerste-kennisevenement-ics-scada-van-het-ncsc.html>
¹²¹ <https://security.stackexchange.com/questions/71780/what-are-the-insecure-protocols-in-terms-of-pci-dss>
¹²² https://www.speedguide.net/ports_sg.php
¹²³ <https://www.security.nl/posting/533560/Google+vindt+kwetsbaarheden+in+dns-software+Dnsmasq>
¹²⁴ <https://krebsonsecurity.com/2017/07/experts-in-lather-over-gsoap-security-flaw/>
¹²⁵ https://www.speedguide.net/ports_sg.php
¹²⁶ <https://www.statista.com/topics/4123/internet-of-things-iot-in-europe/>
¹²⁷ <https://www.visioncritical.com/internet-of-things-stats/>
¹²⁸ https://www.cybersecurityraad.nl/binaries/CSR_Advies_IoT_NED_tcm107-314537.pdf
¹²⁹ <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond>

