# Evaluatie Roadmap Digitaal Veilige Hard- en Software

Eindrapport

KWINK GROEP

# Evaluatie Roadmap Digitaal Veilige Hard- en Software

Eindrapport

Datum: 16 juni 2022
Auteurs: Pauline Modderman
Niek de Vreeze

KWINK GROEP

# Inhoud

# 1.Inleiding

## 1.1. De Roadmap Digitaal Veilige Hard- en Software

Digitalisering maakt ons steeds afhankelijker van ICT. Dit heeft voordelen, maar maakt ons ook kwetsbaar. Door een toenemende verbondenheid van apparaten is digitale veiligheid daarbij niet alleen een belang van het individu, maar ook van de samenleving als geheel. Daarom is samenhang in maatregelen en marktcoördinatie belangrijk om de nodige effectiviteit te bewerkstelligen. De Roadmap Digitaal Veilige Hard- en Software biedt 'een samenhangend pakket aan maatregelen om onveiligheden in hard- en software te voorkomen, kwetsbaarheden te detecteren, en om de gevolgen daarvan te mitigeren. Alle fasen van de productlevenscyclus worden daarbij betrokken; van het ontwerp en de productie, tot en met het gebruik en de afstoting van een product moet de digitale veiligheid bevorderd worden.'[1]

De Roadmap Digitaal Veilige Hard- en Software (Roadmap DVHS) is een product van de ministeries van Economische Zaken en Klimaat (EZK) en Justitie en Veiligheid (JenV) en is grotendeels parallel aan de Nederlandse Cybersecurity Agenda (NCSA) opgesteld. De Roadmap DVHS bevat bijna één-op-één dezelfde maatregelen als ambitie 3 ('Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software') van de NCSA, maar bevat meer toelichting en verdere uitwerking van deze maatregelen.[2]

**Doelstellingen en maatregelen**

De NCSA heeft onder de ambitie 'Nederland loopt voorop in het bevorderen van digitaal veilige hard en software' de volgende vier doelstellingen opgesteld:[3]

1. Nederland zet in op het voorkomen van digitale veiligheidsrisico's in hard- en software door het stimuleren van standaardisatie- en certificeringsinitiatieven en het versterken van toezicht en handhaving.
2. Nederland zet in op het detecteren van digitale veiligheidsrisico's, door het testen van digitale producten en het inzichtelijk maken van digitale veiligheidsrisico's.
3. Nederland zet in op het mitigeren van digitale veiligheidsrisico's door het aansprakelijkheidsregime, en het versterken van het bewustzijn en handelingsperspectief voor burgers en bedrijven.
4. Nederland zet in op het realiseren van een set van basisbeginselen om de digitale veiligheid van hard- en software te bevorderen.

Om aan deze vier doelstellingen te voldoen, is in 2018 de Roadmap DVHS opgesteld. In de Roadmap zijn maatregelen bijeengebracht die moeten leiden tot een aanzienlijke verbetering van de digitale veiligheid van hard- en software.[4]

In de Roadmap zijn negen maatregelen geformuleerd:

1. Standaarden en certificering
2. Monitor digitale veiligheid van producten
3. Opschonen besmette producten bij gebruikers
4. Testen op digitale veiligheid

[1] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 9.
[2] Dialogic (2021). Evaluatie van de opbouw en meetbaarheid van de Nederlandse Cybersecurity Agenda. P. 95.
[3] NCTV (2018). Nederlandse Cybersecurity Agenda. P. 27.
[4] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 7.

5. Cybersecurity-onderzoek
6. Aansprakelijkheid
7. Wettelijke eisen, toezicht en handhaving
8. Bewustwordingscampagnes en empowerment
9. Inkoopbeleid van de Rijksoverheid

In hoofdstuk 3 zetten we verder uiteen wat deze maatregelen inhouden en welke acties op deze maatregelen zijn ondernomen.

## 1.2. Doel en aard van de evaluatie

De evaluatie is in korte tijd uitgevoerd in de periode april – medio mei 2022. Het betreft geen klassieke evaluatie van doeltreffendheid en doelmatigheid. Het doel is om inzicht te geven in het effect en nut van de genomen acties en om aanbevelingen te geven ten aanzien van onderwerpen of acties die worden gemist en die overwogen kunnen worden om toe te voegen in de herijking van de Roadmap. De kern van de dataverzameling (en de belangrijkste basis voor de conclusies) betreft de percepties van betrokkenen.

De resultaten van deze evaluatie vormen de input voor herijking van de Roadmap DVHS als onderdeel van de nieuwe Nederlandse Cybersecurity Strategie.

## 1.3. Aanpak

Om tot conclusies en aanbevelingen te komen zijn eerst documenten bestudeerd, zoals de Roadmap zelf, de NCSA en de Kamerbrieven waarin is gerapporteerd over de voortgang op de maatregelen in de Roadmap. De resultaten van de documentenanalyse zijn voorgelegd aan en aangevuld door de directie Digitale Economie van het ministerie van EZK.

Vervolgens zijn dertien interviews gevoerd met stakeholders die op verschillende manieren betrokken zijn (geweest) bij de Roadmap. Bijlage 2 geeft een overzicht van de gesprekspartners. De samenstelling van gesprekspartners is in overeenstemming met de opdrachtgever tot stand gekomen.

De ‘eerste beelden’ van het onderzoek zijn in een clusteroverleg cybersecurity en privacy van het ministerie van EZK besproken. Daarnaast heeft de opdrachtgever de kans gehad om het conceptrapport in te zien.

## 1.4. Leeswijzer

Hoofdstuk 2 bevat de overkoepelende reflecties die voortkomen uit de evaluatie. De daaropvolgende hoofdstukken beschrijven de bevindingen waarop deze reflecties zijn gebaseerd. Hoofdstuk 3 beschrijft de maatregelen en acties in de Roadmap DVHS. Per maatregel is een samenvatting van gevoerde acties en resultaten opgenomen, en de percepties van de gesprekspartners over deze maatregel. Hoofdstuk 4 beschrijft op een hoger abstractieniveau de percepties van de gesprekspartners over de functie en de impact van de Roadmap DVHS. Hoofdstuk 5 bevat suggesties van gesprekspartners voor de herijking van de Roadmap.

# 2. Overkoepelende reflecties

De hoofdvragen van deze evaluatie zijn *"Breng de resultaten, de uitkomst en de impact van de in de Roadmap DVHS geformuleerde ambities en overkoepelende doelstellingen in kaart"* en *"Wat zijn ten opzichte van 2018 nieuwe nationale en internationale ontwikkelingen op het gebied van digitaal veilige hard- en software die relevant zijn voor de herijking van de Roadmap DVHS?".* In dit hoofdstuk beschrijven de overkoepelende reflecties die we op basis van de evaluatie (beschreven in hoofdstuk 3-5) willen meegeven.

### De inhoud van de Roadmap Digitaal Veilige Hard- en Software en de betrokkenheid van stakeholders

In de Roadmap DVHS zijn uiteenlopende maatregelen en activiteiten opgenomen. Sommige activiteiten zijn geïnitieerd vanuit de Roadmap en sommige activiteiten zijn aangejaagd of versneld dankzij de Roadmap. Er zijn ook activiteiten die zijn beschreven in de Roadmap (en in de voortgangsrapportages over de Roadmap), maar waarvoor geldt dat in de praktijk weinig of geen interactie is geweest tussen degenen die deze activiteit hebben uitgevoerd en de betrokkenen bij de Roadmap.

De Roadmap DVHS heeft ook tot doel om samenhang te bieden in beleid. Het tonen van wat er gaande is op het gebied van digitaal veilige hard- en software kan een goede reden zijn om activiteiten op te nemen die niet per se zijn gestart dankzij de Roadmap. Echter, de manier waarop in de Kamerbrieven over de voortgang is gerapporteerd kan wel de indruk wekken dat alle behaalde resultaten zijn toe te schrijven aan 'de Roadmap'. Dit wekt bij sommigen ergernis op.

Ook geven verschillende betrokkenen aan dat ze het waardevol zouden vinden om eens in de zoveel tijd met alle stakeholders die maatregelen uitvoeren die in de Roadmap staan contact te hebben.

We geven daarom ter overweging mee om te zoeken naar manieren om de stakeholders meer te betrekken, bijvoorbeeld door eens per jaar een bijeenkomst met alle stakeholders te organiseren, waarin de stakeholders delen welke activiteiten ze hebben uitgevoerd. Ook bevelen we aan om in de rapportages over de voortgang transparant te zijn over de rol en betrokkenheid van de verschillende stakeholders, waaronder het ministerie van EZK (ook in het geval er geen betrokkenheid van het ministerie van EZK is geweest).

### Rapporteren over de voortgang

Sinds de start van de Roadmap is er jaarlijks in een Kamerbrief over de voortgang gerapporteerd. Desalniettemin geven verschillende gesprekspartners aan geen zicht te hebben op de voortgang en resultaten van bepaalde activiteiten. We geven ter overweging mee om op een centrale plek (bijvoorbeeld een website) te rapporteren over de voortgang op de verschillende maatregelen. Daarbij kan het behulpzaam zijn om de maatregelen en de activiteiten en resultaten directer aan elkaar te verbinden, bijvoorbeeld door een tabel op te nemen waarin de voortgang is weergegeven (zie bijvoorbeeld de Kamerbrieven over het programma DTC).[5]

### Veiligere hard- en software

Het is niet mogelijk om exact vast te stellen of hard- en software veiliger is geworden (al dan niet dankzij de maatregelen uit de Roadmap). Veel van de gesproken stakeholders zijn wel van mening dat de maatregelen uit de Roadmap de juiste maatregelen zijn om bij te dragen aan veiligere hard- en software.

We bevelen het ministerie van EZK ten eerste aan om te zoeken naar informatie die een indicatie vormt voor de bijdrage van de Roadmap aan veiligere hard- en software. Bijvoorbeeld: als een handreiking is opgesteld kan

[5] Ministerie van Economische Zaken en Klimaat (2022) Kamerbrief 'Voortgangsbrief Digital Trust Center' (zie bijlage 1 voor de tabel).

bijgehouden worden hoe vaak de handreiking is gedownload en kunnen bedrijven bevraagd worden over de effecten die zij zien van het implementeren van de handreiking.

Ten tweede valt op dat de resultaten van maatregelen uit de Roadmap vaak zaken zijn als kaders, handreikingen, geautomatiseerde controles en rapporten. Voor deze producten geldt dat er in meer of mindere mate vervolgstappen nodig zijn om ervoor te zorgen dat de activiteiten uiteindelijk leiden tot een verhoogde veiligheid van hard- en software. We raden het ministerie van EZK daarom aan om de maatregelen uit de Roadmap DVHS te scannen en te bepalen voor welke activiteiten vervolgacties uitgevoerd kunnen worden die bijdragen aan de verhogen van de veiligheid. Bijvoorbeeld: als er een handreiking is opgeleverd, zou het zonde zijn als deze niet gebruikt wordt.

# 3. Maatregelen: activiteiten en resultaten

In dit hoofdstuk bespreken we de negen maatregelen uit de Roadmap DVHS. Per maatregel vatten we de genomen acties en (directe) resultaten daarvan samen en geven we de percepties van gesprekspartners weer. De uitgebreide beschrijving van alle acties en resultaten is te vinden in bijlage 1.

## 3.1. Standaarden en certificering

In de Roadmap staat beschreven dat standaarden en certificering bijdragen aan de digitale veiligheid van hard- en software gedurende de gehele levenscyclus: van ontwerp tot en met de afstotingsfase. Zo dringen standaarden in de ontwikkelfase de kwetsbaarheden terug, en in de gebruiksfase kunnen standaarden zien op het verhelpen van de kwetsbaarheden. Door een hard- en softwareapparaat of de aanbieder daarvan te certificeren, is het voor gebruikers duidelijk wat zij van een apparaat of aanbieder mogen verwachten.[6] De Roadmap beschrijft de volgende vier acties:

1. *Nederland dringt in de onderhandelingen in Brussel aan op snelle vaststelling van de Cybersecurity Act (CSA) en een voortvarende ontwikkeling van een Europees raamwerk Beveiligingscertificering voor ICT-producten en -diensten.*[7]
2. *Bevorderen standaarden/certificering.*
3. *Bundeling standaardisatie en certificeringsinitiatieven.*
4. *Inzetten op multilaterale samenwerking rond Internet of Things (IoT)-standaardisatie.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

Op de maatregel standaarden en certificering is een breed scala aan acties uitgevoerd.[8] De Kamerbrieven maken een onderscheid tussen acties op Europees en nationaal niveau:

1. **Cybersecurity certificering in de EU**
   Nederland heeft bijgedragen aan ontwikkelingen van standaarden en certificeringsschema's op Europees niveau. Voorbeelden hiervan zijn een bijdrage vanuit de publiek-private Online Trust Coalitie (OTC) aan de ontwikkelingen van certificeringsschema's en het starten van een werkgroep van CEN/CENELEC. Resultaten hiervan zijn onder andere een manifest, een whitepaper en adviezen gericht aan instanties / organisaties op EU niveau die zich met certificering bezighouden. Ook heeft Nederland invloed uitgeoefend op wetgeving die op Europees niveau is ontwikkeld (de Cybersecurity Act) en stappen gezet om deze wetgeving in Nederland te implementeren. Momenteel is Nederland betrokken bij de ontwikkeling van de Europese certificeringsschema's die binnen het kader van de Cybersecurity Act ontwikkeld worden.
   In samenwerking met nationale en Europese partners zijn meerdere standaarden en certificeringsschema's ontwikkeld. Bijvoorbeeld pentesten (penetratie testen) en het Framework

[6] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 19.
[7] Inmiddels is niet meer sprake van een 'Europees raamwerk Beveiligingscertificering voor ICT-producten en -diensten' maar van Europese certificeringsschema's voor ICT-producten, ICT-diensten en ICT-processen.
[8] Zie bijlage 1 voor een uitgebreid overzicht van alle acties en resultaten.

Secure Software. In Europees normalisatieverband heeft Nederland samen met NEN een leidende rol opgepakt in het bepalen van de in Europa geldende normen voor cyber security in producten.

2. **Nationale ontwikkelingen standaarden en certificering**
   De OTC is gelanceerd met als doel: 'Het beschikbaar maken van een eenduidige, efficiënte methode waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn. En die helpt bij het invulling geven aan de relevante wet- en regelgeving.'[9] In het kader van veilige software ontwikkeling zet de Secure Software Alliantie in op pilots om methodieken toe te passen in het bedrijfsleven. Resultaten hiervan zijn duidelijke, geautomatiseerde, eenduidige en efficiënte methoden die beschikbaar zijn om de kwaliteit van producten en diensten te toetsen. Daarnaast zijn stappen genomen om de standaarden en certificering in het onderwijs en bedrijfsleven te institutionaliseren.

**Percepties uit de interviews**

In de gesprekken is vaak genoemd dat de inzet op standaarden belangrijk is, zo geven meerdere gesprekspartners aan dat deze maatregel tot de kern van de Roadmap behoort. Specifiek zijn de pentesten meerdere keren als positief resultaat benoemd. Ook de Cyber Security Act[10] is in veel gesprekken genoemd als belangrijke wet, waarbij het dus ook van belang wordt geacht dat Nederland hier invloed op uitoefent.

Hoewel veel gesprekspartners dus het belang van deze maatregel benoemen, zijn meerdere gesprekspartners kritisch op de huidige stand van zaken rondom standaarden. Deze gesprekspartners zijn niet per se van mening dat vanuit de Roadmap meer had moeten gebeuren, maar ze geven wel aan dat het nog niet lukt om standaarden op Europees niveau te harmoniseren ("er zijn losse lijstjes") en dat het beïnvloeden van Europese standaarden zowel vanuit Nederland als vanuit andere landen tekort schiet. Er is ook een aantal gesprekspartners dat aangeeft geen zicht te hebben op hoe de inzet op standaarden en certificering vanuit de Roadmap verloopt.

## 3.2. Monitor digitale veiligheid van producten

In de Roadmap staat beschreven dat 100% digitale veiligheid niet realiseerbaar is. Het kan namelijk altijd zo zijn dat producten die op de markt komen onveilig zijn of dat voor producten geen updates meer beschikbaar komen. Het is voor de producent, verkopers en gebruikers daarom belangrijk dat transparantie bestaat over de kwaliteit en veiligheid van digitale producten. De Roadmap benoemt dat een monitor met informatie over de veiligheid van digitale producten daarbij van groot belang is.[11] De Roadmap beschrijft de volgende actie:

1. *Het kabinet gaat met publieke en private organisaties een monitor maken met informatie over digitale veiligheid van producten met specifieke aandacht voor IoT-apparaten.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

In de Kamerbrief van 2019 wordt deze maatregel separaat genoemd. In de Kamerbrieven van 2020 en 2021 is deze maatregel gecombineerd met de maatregel 'Opschonen besmette producten bij gebruikers'. Zodoende bespreken we de acties en resultaten gezamenlijk met de acties gezamenlijk met de volgende maatregel (paragraaf 3.3).

[9] Online Trust Coalition (2020). Manifest.
[10] Zie bijlage 3 voor een beschrijving van deze wet.
[11] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 21.

**Percepties uit de interviews**

Er zijn weinig gesprekspartners die een beeld hebben bij de maatregel monitor digitale veiligheid van producten. Een kritische noot die een gesprekspartner benoemt is dat een product niet veilig verklaard kan worden, want de toepassing en het gebruik van een product bepaalt voor het grootste deel hoe veilig het is. Anderzijds noemt deze gesprekspartner ook dat het wel goed is om in te zetten op het van de markt weren van de “grootste rotzooi”.

## 3.3. Opschonen besmette producten bij gebruikers

In de Roadmap staat beschreven dat aanbieders van internettoegang een belangrijke rol spelen bij het verminderen van digitale kwetsbaarheden bij gebruikers. De beheerstaak voor de internetverbinding van aanbieders, kunnen zij gebruiken om gebruikers erop te attenderen dat onveilige apparaten op het internet zijn gesignaleerd.[12] De Roadmap beschrijft de volgende actie:

1. *Het kabinet gaat in gesprek met de aanbieders van internettoegang over hoe zij gaan bijdragen aan de bestrijding van onveilige IoT-apparaten.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

De Technische Universiteit (TU) Delft heeft een monitor ontwikkeld die geautomatiseerde ontwikkelingen doet om zicht te krijgen op het aantal besmette apparaten. Het resultaat van deze monitor is dat is vastgesteld dat het aantal besmette apparaten in Nederland relatief laag is. Overzichten van IP-adressen van gecompromitteerde apparaten worden maandelijks gedeeld met de Internet Service Providers (IPSs). Zij kunnen vervolgens hun klanten benaderen om de apparaten op te schonen. Het Digital Trust Centre (DTC) heeft de bevindingen van de TU Delft vervolgens opgepakt. De conclusies waren dat één fabrikant ver uitstak boven de rest van de fabrikanten. DTC heeft email contact gezocht met deze fabrikant, maar dat heeft niet tot een gesprek geleid. Verder heeft DTC prioriteit gegeven aan het verspreiden van informatie over de kwetsbaarheden in, en van IoT producten.

**Percepties uit de interviews**

Een aantal gesprekspartners geeft aan het opschonen van besmette producten bij gebruikers een belangrijke maatregel te vinden, omdat het goed is dat inzichtelijk is gemaakt dat er relatief weinig besmette apparaten zijn in Nederland. Meerdere gesprekspartners benoemen dat ze de maatregel nuttig vinden, maar weinig of geen zicht hebben op welke activiteiten rondom deze maatregel zijn uitgevoerd.

Een gesprekspartner noemt dat de monitor een mooie tool is die interessante resultaten heeft opgeleverd, maar dat vervolgens niet genoeg is gedaan met de resultaten, wat volgens deze gesprekspartners een gemiste kans is (bijvoorbeeld: het aanspreken van de bedrijven waarover bekend werd dat er wel veel besmette producten aanwezig waren).

Meerdere gesprekspartners zijn van mening dat deze maatregel te veel gericht is op de verantwoordelijkheid van aanbieders en gebruikers, terwijl de fabrikanten verantwoordelijk zijn. Tot slot is er een gesprekspartner die van mening is dat deze maatregel geen taak van het ministerie van EZK zou moeten zijn, maar van het ministerie van JenV (want het gaat over digitale weerbaarheid: om besmette producten op te kunnen schonen moet je ze eerst vinden).

[12] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 21.

## 3.4. Testen op digitale veiligheid

In de Roadmap staat beschreven dat het testen van producten cruciaal is om zekerheid te verkrijgen over de digitale veiligheid daarvan. Aanbieders testen producten, bijvoorbeeld tijdens de ontwerpfase, en bedrijven en organisaties lichten de digitale veiligheid van hun interne ICT-omgeving (geregeld) door. Een cybersecuritymarkt ontstaat om tegemoet te komen aan de groeiende vraag naar testen. Die markt is dynamisch: doordat cybercriminelen steeds nieuwe manieren verzinnen om producten en systemen aan te vallen moeten aanbieders daarop anticiperen en reageren.[13] De Roadmap beschrijft de volgende actie:

1. *Er komt een pilot om aan de hand van diverse sectorale use cases ervaring en kennis op te doen met wat een gedeeld testplatform kan bieden.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

Sinds 2020 loopt het programma *Connected Products* van de Consumentenbond, waarin tests op slimme apparaten hebben plaatsgevonden. Uit deze tests kwam dat de gerenommeerde merken het meeste aandacht hebben voor privacy en veiligheid. Met deze resultaten kunnen consumenten de digitale veiligheid en privacy van producten meewegen in hun aankoopkeuzes. Daarnaast heeft Agentschap Telecom onderzoek laten uitvoeren naar de veiligheid van 22 apparaten. Dit heeft geresulteerd in twee rapporten over de digitale veiligheid van IoT apparatuur.

**Percepties uit de interviews**

Meerdere gesprekspartners geven aan dit een nuttige maatregel te vinden. Sommigen geven wel aan dat de maatregel verbreed zou moeten worden, door ook te focussen op de aanbodkant. Een gesprekspartner benoemt dat testen enerzijds zinvol is, maar dat anderzijds de vraag is of er echt iets wordt gedaan met testresultaten, omdat de laagste prijs voor consumenten vaak doorslaggevend is. Volgens een gesprekspartner zou ook deze maatregel (net als het opschonen van besmette producten) een taak moeten zijn van het ministerie JenV en niet van het ministerie EZK (want gaat om weerbaarheid: zorgen dat producten, diensten et cetera minder kwetsbaar zijn voor hacken).

## 3.5. Cybersecurity-onderzoek

In de Roadmap staat beschreven dat innovatieve oplossingen een belangrijke bijdrage leveren aan het digitaal veilig maken van hard- en software. De innovatieopgaven verschillen per fase in de productlevenscyclus. Voor de fase van afstoting zijn geheel nieuwe oplossingen nodig om de slag te maken naar het veilig uitschakelen en verwijderen van hard- en software. Bij ontwerp, productie en gebruik gaat het niet alleen om het ontwikkelen van nieuwe oplossingen, maar ook om onderzoek ten behoeve van gedragsbeïnvloeding, en tevens om intensievere samenwerking ter versterking van de gehele kennisbasis.[14] De Roadmap beschrijft de volgende acties:

1. *Dcypher[15] komt met een nieuwe Nationale Cybersecurity Research Agenda (NCSRA III) waarin de onderzoeksinspanningen rond (onder meer) het ontwerpen van veilige systemen en diensten op elkaar worden afgestemd.*

[13] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software.
[14] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 23.
[15] Bij deze actie uit de Roadmap van 2018 gaat het nog om de voorloper van het huidige dcypher. Het opstellen van een nieuwe NCSRA is bij het huidige dcypher geen doelstelling meer.

2. *Er lopen momenteel verschillende tenders in de research & development fase van de SBIR Cybersecurity. Deze projecten hebben beveiliging van IoT hard- en software tot doel en worden halverwege 2019 afgerond.*
3. *Het kabinet stimuleert open source encryptie door extra middelen hiervoor vrij te maken in het kader van de NCSRA III.*
4. *Het kabinet gaat dialoogsessies organiseren over innovatie oplossingen voor de fase van afvoer van hard- en software.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

Sinds het opstellen van de Roadmap zijn de volgende investeringen in onderzoek gedaan, waarover is gerapporteerd in de Kamerbrieven over de voortgang op de Roadmap en in de Kamerbrief 'Informatie- en communicatietechnologie (ICT)' uit 2020:

- In juni 2019 is vanuit de NWA €8 miljoen gehonoreerd aan het onderzoeksproject INTERSECT. Dit onderzoeksproject richt zich op de mogelijkheden van een veilig IoT door technisch onderzoek te combineren met juridische en criminologische benaderingen. In het INTERSECT-consortium doen 47 organisaties mee.[16]
- In december 2019 is een *call* geopend van circa €8 miljoen voor cybersecurity-, governance- en cryptologievraagstukken.[17]
- De Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) heeft eind 2019 ruim €4 miljoen gehonoreerd aan tien onderzoeksprojecten die binnen de *call* Cybersecurity - Digitale Veiligheid & Privacy zijn ingediend.[18]
- In 2021 heeft het ministerie van EZK twee SBIR rondes gefinancierd, waarbij ook het ministerie van Defensie financieel heeft bijgedragen. Tezamen hebben de SBIR's voor *Automated Vulnerability Research* en Cryptocommunicatie een budget van €1,5 miljoen.[19]
- Het ministerie van JenV heeft een bedrag van €385.000[20] ter beschikking gesteld voor het stimuleren van open source encryptie. Van deze investering is nog geen resultaat bekend.

In de periode vanaf 2020 is de opvolger van het dycpher platform; ('dcypher 2.0') opgericht.[21] Deze opvolger van het platform heeft een bestuur met vertegenwoordiging vanuit private organisaties, kennisinstellingen en de overheid. Dcypher (2.0) is ondergebracht bij Rijksdienst voor Ondernemend Nederland (RVO). Daarbij zijn twee routekaarten (op de thema's geautomatiseerd kwetsbaarheden onderzoek en cryptocommunicatie) opgesteld met de inhoudelijke agendering en programmering van kennis- en innovatietrajecten. Deze hebben een looptijd tot 2026 en de inhoudelijke resultaten van deze trajecten zijn dus nog niet bekend. Voor een routekaart is een basisfinanciering van ongeveer €2 miljoen beschikbaar in de opstartfase.

**Percepties uit de interviews**

Verschillende gesprekspartners hebben aangegeven dat ze cybersecurity-onderzoek zeer belangrijk vinden, en dat ze graag zouden zien dat (nog) meer ingezet zou worden op cybersecurity-onderzoek. Enkele gesprekspartners geven aan dat ze weten dat dcypher een rol speelt op dit gebied, maar zijn niet op de hoogte van wat de ontwikkelingen rondom dcypher precies zijn. Een gesprekspartner is uitgesproken kritisch. Deze gesprekspartner is van mening dat ten opzichte van het belang van deze maatregel en het belang dat de

[16] Zie: https://intersct.nl/consortium/.
[17] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Informatie- en communicatietechnologie (ICT)'.
[18] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Informatie- en communicatietechnologie (ICT)'.
[19] Zie: https://www.rvo.nl/subsidies-financiering/sbir/abc-sbir/cryptocommunicatie.
[20] De kamerbrief uit 2019 die rapporteert over de voortgang op de Roadmap stelt dat door JenV een bedrag van €410.000 ter beschikking is gesteld. Het ministerie van EZK heeft later naar de onderzoekers gecommuniceerd dat dit een bedrag van €385.000 betrof.
[21] De voorganger van het huidige dcypher richtte zich vooral op het onderzoeksveld en liep tot oktober 2020. Met name door de wens om het bedrijfsleven te betrekken bij het onderzoek en de resultaten te laten landen in het veld is besloten 'dcypher 2.0' op te richten. Zie: https://dcypher.nl/cms/view/b2bc77c2-abc1-423b-8e8d-2112cfc4db88/dcypher-history.

Rijksoverheid zegt hieraan te geven, veel te weinig op onderzoek is ingezet en te weinig middelen daarvoor beschikbaar zijn gesteld. Deze gesprekspartner benoemt ook dat het onderzoeksproject INTERSECT volledig buiten het ministerie van EZK is gelopen (en is ingediend in een open NWO competitie). Dit dient volgens deze gesprekspartner dus niet gezien te worden als uitkomst van de Roadmap.

## 3.6. Aansprakelijkheid

In de Roadmap staat beschreven dat het aansprakelijkheidsrecht gebruikers handvatten geeft om schade door digitale onveiligheid te verhalen en prikkels creëert om voorzorgsmaatregelen te nemen ter voorkoming of beperking van schade. Aansprakelijkheid vormt een belangrijke financiële prikkel voor aanbieders om hun hard- en software veilig te maken én te houden. Daardoor wegen aanbieders mogelijke negatieve externe effecten mee bij de ontwikkeling en het op de markt brengen van hard- en software. Hiermee draagt het aansprakelijkheidsrecht bij aan de digitale veiligheid van hard- en software gedurende de gehele productlevenscyclus.[22] De Roadmap beschrijft de volgende acties:

1. *Het kabinet is met stakeholders en wetenschappers in gesprek over aandachtspunten rond de aansprakelijkheid bij digitaal onveilige hard- en software, en mogelijke verbeterpunten en oplossingen, om vervolgstappen te bepalen.*
2. *Nederland neemt actief deel aan de expertgroep over aansprakelijkheid en nieuwe technologieën en betrekt daarbij de inbreng van Nederlandse stakeholders.*
3. *Nederland stelt in de onderhandelingen over het richtlijnvoorstel digitale inhoud en digitale diensten voor om in alle gevallen veiligheidsupdates te verplichten als het gaat om software die is geleverd aan een consument.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

De Kamerbrieven rapporteren over de maatregel 'Aansprakelijkheid' als sub-thema onder de maatregel 'Wettelijke eisen, toezicht en aansprakelijkheid'. Om de indeling van de Roadmap zo veel mogelijk te volgen bespreken we de acties en resultaten die in de Kamerbrieven specifiek onder het sub-thema 'Aansprakelijkheid' staan separaat. Door het Centre for the Law and Economics of Cyber Security van de Erasmus Universiteit Rotterdam is onderzoek uitgevoerd naar welke juridische en economische barrières er in de praktijk zouden zijn voor bedrijven onderling om schade te verhalen naar aanleiding van een cybersecurity incident. Uit dit onderzoek volgt dat juridische en economische barrières bestaan die het zeer complex maken voor bedrijven om geleden schade na een cybersecurity incident te verhalen. Op basis van dit onderzoek heeft een aantal dialoogsessies plaatsgevonden met stakeholders uit het veld. Uit deze dialoogsessies kwam naar voren dat de stakeholders verschillende invalshoeken hebben: variërend van een behoefte aan contractvrijheid en daarbij horende eigen verantwoordelijkheid, tot een behoefte aan een grotere rol van de overheid op bijvoorbeeld het gebied van certificering.

**Percepties uit de interviews**

Meerdere gesprekspartners benoemen het belang van deze maatregel. Volgens een gesprekspartner zou dit de kern van de Roadmap moeten zijn, omdat hier veel winst op te behalen valt. Deze gesprekspartner geeft aan dat op dit moment te veel afhankelijkheid is van leveranciers van software: als je eenmaal met bepaalde software werkt, stap je niet makkelijk over naar een andere producent. De marktwerking schiet dus volgens deze gesprekspartner tekort, waardoor leveranciers onvoldoende prikkel ervaren om hard aan de veiligheid van hun diensten te werken. Een andere gesprekspartner is juist van mening dat een gedeelde

[22] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 24.

verantwoordelijkheid bestaat voor leverancier en klant. Een klant neemt vaak namelijk producten en diensten af van meerdere leveranciers en combineert deze. Het is dan niet terecht om vervolgens één van de leveranciers aansprakelijk te maken voor de veiligheid.

Verschillende gesprekspartners uiten hun zorgen over de Implementatiewet verkoop goederen en levering digitale inhoud, waarin de verplichting om updates te verstrekken bij handelaren is gelegd.[23] Dit terwijl handelaren (verkopers) afhankelijk zijn van producenten.

## 3.7. Wettelijke eisen, toezicht en handhaving

In de Roadmap staat beschreven dat minimumveiligheidseisen onveilige producten van de markt kunnen weren. Op initiatief van Nederland zijn in EU-verband via de richtlijn voor radiorandapparatuur Radio Equipment Directive (hierna 'de RED'), minimale digitale veiligheidseisen gesteld voor apparaten die draadloos verbonden zijn met het internet. Dit stelt in staat om producten die niet aan de eisen voldoen van de markt te halen.[24] De Roadmap beschrijft de volgende acties:

1. *Het kabinet onderzoekt welke minimale veiligheidseisen kunnen worden gesteld aan apparaten via de Europese Radio Equipment Directive.*
2. *Het kabinet organiseert een nationale dialoogsessie voor toezichthoudende instanties, om te bezien welke rol zij de komende periode kunnen spelen om de digitale veiligheid van hard- en software te bevorderen, synergie te creëren tussen de verschillende acties van toezichthouders en te kijken hoe samenwerking tussen toezichthouders kan worden verbeterd.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

De Kamerbrieven rapporteren onder het kopje 'Wettelijke eisen, toezicht en aansprakelijkheid' in plaats van 'Wettelijke eisen, toezicht en handhaving' (zoals de maatregel in de Roadmap). De Kamerbrieven maken op deze maatregel een onderscheid op vier sub-thema's[25]:

1. **Wettelijke digitale veiligheidseisen voor apparaten**
   Nederland heeft zich hardgemaakt voor Europese wettelijke digitale veiligheidseisen aan alle slimme apparaten via de Europese richtlijn voor radioapparatuur (de Radio Equipment Directive, RED). Voorafgaand aan de totstandkoming van de RED heeft Agentschap Telecom (AT) onderzoek laten uitvoeren naar welke technische eisen onder de RED geschikt zouden zijn en heeft het Nederlandse normalisatie instituut (NEN) het voorzitterschap van een Europese werkgroep voor IoT-veiligheid ondersteund. Als resultaat van deze richtlijn kunnen consumenten erop vertrouwen dat nieuw aangeschafte producten voldoen aan Europese normen. Met deze richtlijn kan AT producten die vanaf half 2024 niet aan de eisen voldoen weren en van de markt halen.
2. **Veiligheidsupdates in het consumentenrecht**
   Het implementatiewetsvoorstel richtlijnen verkoop goederen en levering digitale inhoud is door de ministeries van EZK en JenV (Rechtsbescherming) voorbereid in 2021 en in april 2022 door de Eerste Kamer goedgekeurd. Op 27 april 2022 is de implementatie wet in werking getreden. Met deze Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud zijn twee Europese consumentenrichtlijnen (verkoop goederen en levering digitale inhoud) geïmplementeerd.

[23] Zie bijlage 3 voor een beschrijving van deze wet.
[24] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 25.
[25] In de Kamerbrieven van 2020 en 2021 staat ook 'Aansprakelijkheid' als thema besproken onder het thema 'Wettelijke eisen, toezicht en handhaving'. Aangezien dit hoofdstuk de opbouw van de Roadmap volgt bespreken we aansprakelijkheid in paragraaf 3.6.

De wet introduceert nieuwe en verduidelijkt bestaande regels die de aan- en verkoop van goederen en digitale inhoud, ook binnen de EU, veiliger en gemakkelijker maken en het expliciteert onder meer een verplicht updateregime voor digitale inhoud en tastbare goederen met een digitaal element. De ACM houdt toezicht op de naleving van de verplichtingen die uit de Implementatiewet voortvloeien.

3. **Toezicht**
   Overkoepelend zijn dialoogsessies gehouden met AT, de ACM, de Autoriteit Persoonsgegevens (AP) en de Nederlandse Voedsel en Waren Autoriteit (NVWA) over wie welke rol zou kunnen (moeten) spelen op het gebied van IoT. Hieruit kwam dat de AP en de NVWA voldoende bevoegdheden hadden. AT heeft inmiddels ook voldoende bevoegdheden (vanwege de RED-eisen). Daarnaast is AT inmiddels aangewezen als Nationale Cybersecurity Certificeringsautoriteit onder de Cyber Security Act. De ACM gaat toezichthouden op de naleving van de updateverplichting. Voor deze toezichthoudende functie krijgt de ACM extra handvatten.
   - AT heeft in het kader van haar toezichthoudende taken voortkomend uit de RED-eisen een IoT testlaboratorium ingericht waarin diverse apparaten worden getest op cybersecurityaspecten. De ervaringen uit het testlaboratorium worden door AT gebruikt in gesprekken met de Europese Commissie en toezichthouders uit andere lidstaten.
   - De ACM voert (samen met AT) onderzoeken uit naar domotica-apparaten en naar precontractuele informatieverplichtingen bij de online verkoop van slimme apparaten. Daarnaast heeft de ACM een aantal grote aanbieders van slimme apparaten aangesproken op informatieverplichtingen. Resultaten hiervan zijn dat op de website consuwijzer.nl is aangegeven welke informatie voorgaand aan de koop aan consumenten verstrekt moet worden. Drie aanbieders (bol.com, Coolblue en MediaMarkt) verstrekken deze informatie inmiddels.
   - De AP en AT nemen op Europees niveau deel aan de stakeholdersgroep Cybersecurity Certification Group in het kader van de ontwikkeling van de CSA.
   - Op Europees niveau hebben de AP en haar Europese evenknieën richtlijnen uitgebracht voor de ontwikkeling en inzet van spraakassistenten en *connected vehicles*. Op nationaal niveau heeft de AP meerdere aanbevelingen gedaan over slimme apparaten.
4. **Aansprakelijkheid**
   *Besproken in paragraaf 3.6.*

### Percepties uit de interviews

Veel gesprekspartners benoemen het belang van de RED. Een gesprekspartner noemt dat de ontwikkelingen rondom de RED liepen op het moment dat de Roadmap startte, en dat de Roadmap zodoende heeft geholpen om verdere stappen te zetten. Enkele gesprekspartners zijn inhoudelijk wel kritisch op de RED, omdat de scope te smal is (alleen gericht op draadloze apparaten).

Over de toezichthouders zijn verschillende gesprekspartners positief dat AT er taken bij heeft gekregen. Het samenbrengen van toezichthouders is volgens enkele gesprekspartners minder goed gelukt dan was gehoopt. Het gesprek tussen toezichthouders (zoals AT, de ACM, de Inspectie Gezondheidszorg en Jeugd (IGJ), de NVWA en de AP) zou volgens deze gesprekspartners geïntensiveerd moeten worden, omdat cybersecurity over alle domeinen heengaat.

## 3.8. Bewustwordingscampagnes en empowerment

In de Roadmap staat beschreven dat Nederland bewustwordingscampagnes en empowerment op het gebied van digitaal veilige hard- en software vooral zal inzetten om de impact te vergroten van bestaande en nieuwe maatregelen. Dit kan in de gehele productlevenscyclus. Zo kunnen ontwerpers bewuster worden gemaakt van het belang om *security-by-design* toe te passen, kunnen zakelijke afnemers worden geattendeerd op (on)betrouwbare apparaten, en kunnen consumenten gestimuleerd worden om hun producten digitaal veilig te houden.[26] De Roadmap beschrijft de volgende actie:

1. *Als onderdeel van de cybersecurity bewustwordingscampagnes van veiliginternetten.nl lanceert de overheid een of meer beleidsondersteunende publiekscampagnes voor digitaal veilige hard- en software.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

In opdracht van EZK is een onderzoek uitgevoerd waaruit blijkt dat meer dan de helft van de mensen het uitvoeren van updates uitstelt. Naar aanleiding van dit onderzoek is de publiekscampagne 'Doe je Updates' gestart. Deze beleidsondersteunende publiekscampagnes voor digitaal veilige hard- en software kennen een landingspagina op de publiek private website veiliginternetten.nl. Van deze campagne hebben inmiddels vier *flights* plaatsgevonden. Uit effectmetingen blijkt dat de campagne goed wordt ontvangen, maar dat de slag naar het gewenste gedrag nog gemaakt moet worden. Daarnaast heeft in 2021 de tiende editie van Alert Online plaatsgevonden. Hierbij hebben onder andere webinars plaatsgevonden over gedragsbeïnvloeding en ketenveiligheid.

**Percepties uit de interviews**

Veel gesprekspartners vinden ook dit een belangrijke maatregel: "je moet het doen". Wel noemen meerdere gesprekspartners dat de campagnes breder en meer integraal ingestoken moeten worden en dat er meer samenwerking zou kunnen zijn, omdat nu meerdere partijen bezig zijn met campagnes. Het zou volgens deze gesprekspartners goed zijn als het ministerie van EZK de samenwerking rondom voorlichting en communicatie initieert. Eén gesprekspartner is kritisch op de campagnes gericht op consumenten, omdat de verantwoordelijkheid voor digitaal veilige hard- en software niet bij consumenten neergelegd zou moeten worden.

## 3.9. Inkoopbeleid van de Rijksoverheid

In de Roadmap staat beschreven dat het inkoopbeleid van de Rijksoverheid de digitale veiligheid van de gehele productlevenscyclus kan bevorderen. Door criteria in het inkoopbeleid op te nemen moeten potentiële aanbieders van de Rijksoverheid voldoen aan deze eisen. Deze criteria kunnen zien op alle fasen van de cyclus.[27] De Roadmap beschrijft de volgende actie:

1. *Het kabinet gaat onderzoeken welke aanvullende maatregelen voor de digitale veiligheid van hard- en software bij inkoop binnen de Rijksoverheid nodig en gewenst zijn.*

**Samenvatting acties en resultaten op basis van Kamerbrieven en aanvullingen van het ministerie van EZK**

Middels het programma Inkoopeisen Cybersecurity is gekomen tot de 'ICO-Wizard'. Dit is een laagdrempelig instrument om gericht inkoopeisen mee samen te stellen voor aanbesteding/inkopen. Deze eisen worden

[26] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 26.
[27] Ministeries van EZK en JenV (2018). Roadmap Digitaal Veilige Hard- en Software. P. 27.

vervolgens meegestuurd bij een aanbesteding en kunnen later in een contract met een leverancier worden opgenomen. Door de open toegang via BIO-overheid.nl, waar het ICO op te vinden is, is het mogelijk voor marktpartijen om gebruik te maken van de mogelijke eisen die de inkopende overheden hanteren.

### Percepties uit de interviews

Veel gesprekspartners geven aan dat deze maatregel bij het ministerie van BZK ligt en dat zij er verder geen zicht op hebben. Enkele gesprekspartners benoemen dat het goed is dat deze maatregel er is, omdat de overheid (als grote inkopende partij) het goede voorbeeld kan geven en druk kan uitoefenen op leveranciers (om aan veiligheidseisen voor hard- en software te voldoen). Enkele andere gesprekspartners geven aan dat ze weten dat er een wizard ontwikkeld is, maar dat ze geen beeld hebben of die wizard ook wordt gebruikt.

# 4. Functie en impact Roadmap DVHS

De impact die met de Roadmap DVHS beoogd wordt is de benodigde samenhangende aanpak te bieden om als Nederland voorop te lopen bij het bevorderen van de digitale veiligheid van hard- en software. In dit hoofdstuk gaan we in op de vraag in hoeverre de Roadmap heeft bijgedragen aan deze overkoepelende ambities, die we samenvatten als: bijdragen aan veilige hard- en software en samenhang brengen in beleid.

Vooraf constateren we dat het niet mogelijk is om exact vast te stellen of genoemde ambities gehaald zijn en in hoeverre effecten zijn toe te schrijven aan de Roadmap DVHS. Er is bijvoorbeeld niet vastgelegd waaraan afgemeten kan worden of er nu meer samenhang in beleid is dan voor de Roadmap DVHS en er zijn geen indicatoren voorhanden waaraan afgemeten kan worden of hard- en software veiliger is geworden. Daarom verwijzen we in dit hoofdstuk naar de percepties uit de gesprekken, want als de brede groep van gesproken stakeholders van mening is dat de Roadmap DVHS heeft bijgedragen aan een de gestelde ambities (of juist niet), vormt dat ook een indicatie voor bereikte impact.[28] Voordat we ingaan om de bijdrage van de Roadmap aan de gestelde ambities, beschrijven we meer algemeen wat de gesprekspartners zien als de functie en het bereik van de Roadmap.

## 4.1. Bekendheid/ overkoepelend beeld van de functie van de Roadmap DVHS

De meeste gesprekspartners zijn betrokken bij een of enkele maatregelen van de Roadmap. Desondanks kennen veel gesprekspartners ook de andere maatregelen (waar ze niet direct bij betrokken zijn). Regelmatig noemen gesprekspartners dat ze niet precies weten welke activiteiten wel en niet onderdeel zijn van de Roadmap. Meerdere gesprekspartners zijn uitgesproken positief over het contact met de directie Digitale Economie van EZK, los van of het nou gaat om acties uit de Roadmap of niet. Genoemd is bijvoorbeeld dat het ministerie van EZK goed signalen ophaalt en die ook vertaalt op Europees niveau. Ook zijn veel gesprekspartners er positief over dat ze zien dat de focus van het ministerie van EZK ligt op (het beïnvloeden van) wet- en regelgeving op Europees niveau.

Meerdere gesprekspartners benoemen dat dat ze de Roadmap wel kennen, maar dat ze niet weten hoe het staat met de voortgang op de verschillende maatregelen. Een gesprekspartner zou graag zien dat er een internetpagina zou zijn waar de voortgang van de Roadmap op wordt bijgehouden. Sommige gesprekspartners benoemen dat ze input hebben geleverd toen de Roadmap is opgesteld, maar dat het de laatste twee/drie jaar vanuit hun perspectief ‘wat stil’ is geweest rondom de Roadmap.

Gesprekspartners hebben verschillende beelden over wat het nut van de Roadmap is (geweest). Volgens sommigen zijn de doelstellingen van de Roadmap gehaald door andere organisaties te stimuleren (bijvoorbeeld met financiële middelen). Volgens anderen zijn in de Roadmap vooral acties opgenomen die al liepen, en is er vervolgens door het ministerie van EZK beperkt extra inzet geleverd op die acties. De indruk van verschillende gesprekspartners is dat het ministerie van EZK capaciteit en middelen met name inzet op de beïnvloeding van

[28] Zie bijlage 2 voor het overzicht met gesprekspartners.

wet- en regelgeving op Europees niveau, en dat op de andere maatregelen in de Roadmap weinig of geen capaciteit en middelen zijn ingezet. Enkele gesprekspartners zijn zeer kritisch, omdat zij van mening zijn dat in de voortgangsbrieven over de Roadmap resultaten aan de Roadmap toegeschreven worden, terwijl die buiten de Roadmap om zijn behaald. Deze gesprekspartners zien hun eigen activiteiten of behaalde resultaten terug in de rapportages over de Roadmap, terwijl er geen interactie met de Roadmap is geweest. Enkele andere gesprekspartners geven aan dat in de Roadmap geen nieuwe acties zijn opgenomen, maar dat activiteiten dankzij de Roadmap wel zijn vastgelegd en extra impuls hebben gekregen.

## 4.2. Bijdrage Roadmap DVHS aan veilige hard- en software

Veel gesprekspartners zijn van mening dat de maatregelen die zijn opgenomen in de Roadmap de juiste maatregelen zijn om veiligere hard- en software te bewerkstelligen. De meeste gesprekspartners kunnen geen antwoord geven op de vraag of hard- en software sinds de start van de Roadmap al veiliger is geworden. Ze geven aan dat er veel ontwikkelingen lopen, maar dat de impact nog niet gemeten kan worden (bijvoorbeeld de impact van alle Europese regelgeving die in ontwikkeling is). Van degenen die de vraag wel beantwoorden denkt één gesprekspartner dat hard- en software (nog) niet veiliger is geworden, één gesprekspartner denkt juist van wel (want er is binnen bedrijven meer aandacht voor cybersecurity).

Een gesprekspartner is uitgesproken kritisch op de ambitie zelf, omdat volgens deze gesprekspartner ‘veilige hard- en software niet bestaat’. De toepassing van software bepaalt of iets veilig is. Andere gesprekspartners zijn het niet eens met deze kritiek, zij geven aan dat volledig veilige hard- en software niet bereikbaar is, maar dat het wel degelijk zin heeft om bijvoorbeeld te eisen dat softwareontwerpers aan bepaalde normen moeten voldoen.

## 4.3. Bijdrage Roadmap DVHS aan samenhang in beleid

Weinig gesprekspartners kunnen iets zeggen over of de Roadmap heeft bijgedragen aan samenhang in beleid. Enkele gesprekspartners zijn positief. Ze benoemen dat de Roadmap samenhang tussen verschillende elementen brengt, zorgt voor overzicht doordat over allerlei maatregelen en activiteiten op één plek wordt gerapporteerd, en dat je als stakeholder dankzij de Roadmap ook kan zien waar anderen mee bezig zijn.

Meerdere gesprekspartners geven aan dat er nog meer samenhang zou kunnen zijn, bijvoorbeeld tussen verschillende onderdelen van het ministerie van EZK (zoals het DTC ten opzichte van beleidsafdelingen) en tussen departementen. Ook is regelmatig genoemd dat het ministerie van EZK (nog) actiever zou kunnen sturen op het verbinden van verschillende partijen, bijvoorbeeld toezichthouders.

# 5. Herijking Roadmap DVHS

In het onderzoek zijn verschillende punten naar voren komen die belangrijk zijn voor de herijking van de Roadmap. In paragraaf 5.1. bespreken we eerst suggesties die gesprekspartners hebben gedaan voor de herijking van de Roadmap. Daarin maken we een onderscheid in suggesties voor het aanpassen van de focus van de Roadmap en suggesties voor toevoegingen aan de Roadmap. In paragraaf 5.2. bespreken we vervolgens contextuele ontwikkelingen die volgens gesprekspartners van belang zijn voor de herijking van de Roadmap.

## 5.1. Suggesties voor herijking van de Roadmap DVHS

Volgens veel gesprekspartners bevat de Roadmap de juiste maatregelen. Voor de herijking is het volgens deze gesprekspartners vooral van belang om op deze maatregelen actie te blijven ondernemen of meer actie te ondernemen. Overkoepelend is genoemd dat een analyse van beschikbare middelen en capaciteit gedaan zou moeten worden, aangezien het geen zin heeft maatregelen op te nemen zonder dat er middelen en capaciteit beschikbaar zijn. Een ander overkoepelend genoemd punt is om bij het bepalen van maatregelen en acties de focus niet te eenzijdig te leggen op het ministerie van EZK, DTC en de toezichthouders: belangrijk is ook goed te luisteren naar leveranciers en eindgebruikers.

Eerst bespreken we vijf suggesties voor het aanpassen van de focus van de Roadmap. Deze suggesties gaan dus niet over specifieke maatregelen, maar gaan over de rode draad die de Roadmap volgens gesprekspartners zou moeten hebben. De volgorde van deze suggesties hebben we min of meer gebaseerd op hoe vaak een suggestie terugkwam in de gesprekken. Daarna bespreken we vier suggesties die gesprekspartners hebben gedaan voor toevoegingen aan de Roadmap, waarbij de rode draad en de huidige maatregelen wel in stand blijven. Deze suggesties zijn in willekeurige volgorde opgenomen.

### Suggesties van gesprekspartners voor aanpassen focus van de Roadmap DVHS

1. **Meer aandacht voor ketens en ketenveiligheid**
   De Roadmap is te veel ingestoken vanuit het perspectief van IoT en individuele producten, en te weinig vanuit ketens en ketenveiligheid. Ketens zijn buitengewoon complexe en vertakte diensten van netwerken en software. Met name de delen ‘cloud’ en ‘diensten’ binnen de ketens zouden meer aan bod moeten komen in de Roadmap. De voornaamste ambitie zou moeten zijn om ketens zo veilig mogelijk te maken, om vervolgens van daaruit maatregelen te formuleren. Overigens zijn er ook gesprekspartners die van mening zijn dat een te brede ambitie (gericht op de gehele keten) zorgt voor verlies van focus.
2. **Meer aandacht voor verbinding tussen maatregelen, acties en betrokkenen partijen**
   Meer verbinding tussen maatregelen, acties en betrokken partijen is wenselijk. Een structureel overleg met betrokken partijen zou bijvoorbeeld waardevol kunnen zijn. Hierin kunnen betrokkenen verbinding met elkaar leggen en sparren over ontwikkelingen die eraan zitten te komen. Het ministerie van EZK zou meer de regie kunnen voeren op die verbindingen, bijvoorbeeld tussen toezichthouders. De rol van het DTC zou nog meer in de Roadmap naar voren kunnen komen en de verbondenheid met andere departementen in de Roadmap is nog onderbelicht.

3. **Prioritering van maatregelen**
   De juiste maatregelen staan in de Roadmap, maar een prioritering van maatregelen is wenselijk. De maatregelen zijn nu gepresenteerd alsof ze aan elkaar gelijk zijn, maar ze hebben een andere orde van grote. Voor sommige gesprekspartners geeft de Roadmap zodoende geen reëel beeld van de werkelijkheid. In hoofdstuk 3 is al beschreven hoe de gesprekpartners tegen de individuele maatregelen aankijken, en welke maatregelen wat hen betreft tot de kern van de Roadmap behoren.
4. **Meer aandacht voor participatie van het ministerie van EZK in Europa**
   Het Europees niveau is het schaalniveau waarop de aandacht zou moeten liggen. In de Roadmap is de inzet "in Europa" verdeeld over verschillende maatregelen, maar deze inzet zou binnen de Roadmap centraal moeten staan. Wanneer namelijk niet voldoende inzet wordt gepleegd op Europese ontwikkelingen loopt Nederland achter de feiten aan. Een gesprekspartner noemt daarbij dat de inzet op Europa een eigen maatregel ('bullet') zou moeten zijn.
5. **Aandacht alleen op fabrikanten en leveranciers en niet consumenten**
   De focus zou meer zou moeten komen te liggen op de verantwoordelijkheid van fabrikanten en leveranciers in plaats van op consumenten. Consumenten hebben namelijk weinig zicht op de veiligheid van hun hard- en software. Wanneer veel kwetsbaarheden bij gebruikers optreden is het ergens eerder al in de keten fout gegaan.

#### Suggesties van gesprekspartners voor toevoegingen aan de Roadmap DVHS

Maatregelen gericht op:

1. **Gegevensbescherming**: Belangrijk onderdeel van cybersecurity, dat nu buiten de scope van de Roadmap valt.
2. **Valorisatie**: Het omzetten van kennis naar (commerciële) producten.
3. **Privacywetgeving:** Waarbij verbinding gemaakt zou moeten worden met de Algemene verordening gegevensbescherming (AVG), Data Act, Data Governance Act en Digital Services Act.[29]
4. **Transparantie**: Laten zien hoe organisaties (bedrijven, publieke organisaties) het doen op het gebied van veilige hard- en software.

## 5.2. Contextuele ontwikkelingen

In deze paragraaf bespreken we contextuele ontwikkelingen waar volgens gesprekspartners rekening mee gehouden moet worden bij de herijking van de Roadmap DVHS.

#### Europese wet- en regelgeving

Veel gesprekspartners noemen Europese wet- en regelgeving als belangrijke ontwikkelingen voor de herijking van de Roadmap. Gesprekspartners geven niet aan *hoe,* maar wel *dat* (onder andere vanuit de Roadmap) de belangen en visie van Nederland meegenomen dienen te worden bij de totstandkoming van Europese wet- en regelgeving. Ook noemen gesprekspartners dat de Europese wet- en regelgeving invloed hebben op de maatregelen in de Roadmap. Daarbij is een aantal keer genoemd dat ook een discussie wordt gevoerd rondom Europese bevoegdheid en verplichtingen ten opzichte van nationale autonomie. Hieronder geven we een beknopt overzicht van de genoemde wet- en regelgeving. In Bijlage 3 geven we een uitgebreidere beschrijving van wat deze ontwikkelingen. Genoemd zijn (in willekeurige volgorde):

1. De Cybersecurity Act
2. Radio Equipment Directive

[29] Zie voor deze drie acts de beschrijving in bijlage 3.

3. De Cyber Resilience Act
4. Herziene richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS 2-richtlijn)
5. AI Act
6. Data Act
7. Data Governance Act
8. Digital Services Act

### Nationale publicaties

Op nationaal niveau zijn in de afgelopen periode een aantal rapporten en onderzoeken uitgekomen die volgens gesprekspartners belangrijk zijn om kennis van te nemen bij de herijking van de Roadmap. Ook hierbij geven gesprekspartners niet aan *hoe,* maar wel *dat* deze publicaties van belang zijn. Hieronder geven we een beknopt overzicht van deze publicaties. In Bijlage 3 geven we een uitgebreidere beschrijving.

1. Kingdom of the Netherlands (2022). Non-paper on the principles of a Cyber Resilience Act.
2. CBS (2021). Bijna drie kwart van de Nederlanders maakt gebruik van slimme apparaten.
3. WRR (2021). Opgave AI. De nieuwe systeemtechnologie.
4. CSR (2021). Adviesrapport Integrale aanpak cyberweerbaarheid.
5. OVV (2021). Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix.

### Contextuele/technologische ontwikkelingen

Ook hebben de gesprekspartners verschillende contextuele en technologische ontwikkelingen genoemd die wat hen betreft belangrijk zijn bij de herijking van de Roadmap:

1. Er is een toegenomen aandacht voor de **energietransitie.** Bij de energietransitie komen heel veel slimme toepassingen kijken. Apparaten met een slimme verbinding (IoT, bijvoorbeeld toegepast in warmtepompen en zonnepanelen) kunnen helpen bij het bereiken van klimaatdoelstellingen, maar brengen ook risico's met zich mee omtrent veilige hard- en software.
2. Een toegenomen aandacht voor **duurzaamheid** creëert nieuwe uitdagingen: een manier om apparaten duurzamer te maken is om ze langer te gebruiken. Hiervoor is het nodig dat fabrikanten updates blijven aanbieden. Zonder update is het apparaat na verloop van tijd niet meer (veilig) te gebruiken.
3. Toenemende **geopolitieke spanningen en dreigingen**, waaronder de huidige oorlog in Oekraïne.
4. Huidige **schaarste van goederen** vormt een risico voor onveilige producten. Door schaarste is de kans groter dat fabrikanten hun producten zo snel mogelijk willen aanbieden, waardoor er minder aandacht is voor de veiligheid, en consumenten ook minder kritisch zijn.
5. **Beperktere hoeveelheid aanbieders en leveranciers**. Steeds minder, maar grotere leveranciers en aanbieders.
6. Probleem met **capaciteit** door middel van een tekort aan cyber security expertise.
7. De **opkomst van AI in cybersecurity**. Dit zou een soort *silver bullet* moeten worden om veel problemen tegen te gaan.

# Bijlage 1: Overzicht activiteiten en resultaten

### Verantwoording

Deze bijlage bevat de activiteiten en resultaten daarvan die onder de Roadmap zijn uitgevoerd en tot stand gekomen. De primaire bronnen die hiervoor zijn gebruikt zijn de Kamerbrieven over de voortgang van de Roadmap, die jaarlijks rapporteren over de activiteiten en resultaten. Daarnaast is aanvullende informatie onderzocht (bijvoorbeeld informatie waarnaar de Kamerbrieven verwijzen). Nadat een conceptversie van dit overzicht was opgesteld, is dit overzicht met de opdrachtgever (ministerie van Economische Zaken en Klimaat, directie Digitale Economie) gedeeld. De informatie is vervolgens door hen aangevuld. Dit is in de voetnoten benoemd met '*Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat*.'

| **1. Standaarden en certificering** | |
|---|---|
| **Activiteiten** | **Resultaten** |
| **1a. Cybersecurity certificering in de EU** | |
| • Nederland implementeert de Europese Cyber Security Act (CSA) via het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening en wijst Agentschap Telecom aan als de nationale autoriteit.[30] | • De nationale implementatie is afgerond in de vorm van de uitvoeringswet. Er wordt nog wel gewerkt aan lagere regelgeving.[31] |
| • In de Nederlandse publiek private Online Trust Coalitie (OTC) zijn afgelopen jaar belangrijke stappen gezet met betrekking tot het vergroten van vertrouwen in de cloud diensten.[32] | • Op initiatief van de Europese Commissie heeft de European Cloud Service Provider Certification Working Group (CSPCert) in juni 2019 een advies aan het Europese Agentschap voor Netwerk- en informatiebeveiliging (ENISA) uitgebracht voor de invulling van het cybersecuritycertificeringsschema voor Cloud Service Providers (CSP). Namens Nederland hebben Zeker-OnLine, NOREA en de Erasmus Universiteit onder de vlag van Partnering Trust (de voorloper van de OTC) hierin geparticipeerd. In dat advies heeft de op *assurance* gebaseerde conformiteitsvaststelling een belangrijke plaats gekregen.[33]<br>• In 2020 heeft de OTC een Manifest gepresenteerd. Het Manifest gaat in op het doel van de Online Trust Coalitie, de deelnemers, de uitgangspunten en de vraagstukken.[34]<br>• Begin 2021 publiceerde de OTC het whitepaper Vertrouwen in de *cloud*. De kern van dit whitepaper, vertrouwen, leunt op 3 pijlers:<br>  ○ Geharmoniseerde *frameworks* en *governance* bij organisaties en *cloudservices* die zorgt voor betrouwbaarheid (criteria).<br>  ○ Onafhankelijk bewijs dat dat effectief is (*conformity assessment*).<br>  ○ De gestandaardiseerde informatie die over pijler 1 en 2 wordt verstrekt.[35]<br>• ENISA werkt in 2021 aan de totstandkoming van een certificeringsschema voor clouddiensten in het kader van de Europese Cybersecurity Act (CSA). Het conceptschema, waar door verschillende Nederlandse partijen en vertegenwoordigers aan is bijgedragen, is eind december 2020 voor een |

[30] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[31] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[32] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[33] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[34] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[35] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.

| | |
|---|---|
| | publieke consultatie gepubliceerd. Vanuit de OTC heeft EZK de Nederlandse bijdragen aan dit schema zoveel mogelijk gecoördineerd.[36]<br>• ENISA heeft aan de partijen die betrokken zijn bij de totstandkoming van dit schema gevraagd om *Proof of Concepts* (PoC) uit te voeren om een beeld te krijgen van de uitvoerbaarheid van het schema. Door OTC is in samenwerking met een aantal deelnemende organisaties een PoC uitgevoerd. De resultaten van deze PoC zijn aan ENISA gerapporteerd en geanonimiseerd verspreid.[37] |
| • Certificeringsschema's (CSA):<br>○ Nederland draagt bij aan de ontwikkeling van Europese schema's voor ICT-producten, clouddiensten en 5G-netwerkapparatuur.[38]<br>○ Nederland draagt met expertise vanuit de publiek private OTC bij aan de ontwikkeling van een certificeringschema voor clouddiensten.[39]<br>○ Nederland zal inzetten op de ontwikkeling van certificeringschema's voor industriële controlesystemen, Internet of Things (IoT) en veilige software ontwikkeling op basis van het raamwerk van de publiek-private Secure Software Alliance (SSA).[40]<br>○ Nederland heeft in het European Cloud Service Provider Certification Working Group (CSPCert) verband met onder meer Duitsland en Oostenrijk een aanbeveling opgesteld voor een Europees cloud certificatieschema.[41] | • Nederland heeft via de CSPCert in juni 2019 een advies aan ENISA en de Europese Commissie uitgebracht voor de invulling van het cybersecuritycertificeringsschema voor Cloud Service Providers (CSP).[42]<br>• De OTC heeft een werkgroep opgericht die een platform biedt aan alle partijen en deskundigen die vanuit Nederland betrokken zijn bij het opstellen van het certificeringsschema voor clouddiensten 'European Cybersecurity Certification Scheme for Cloud Services' (EUCS). Binnen dit platform worden ervaringen en ideeën uitgewisseld teneinde een consistente Nederlandse inbreng te realiseren.[43]<br>• Nederland heeft hierdoor een belangrijke inbreng gehad bij de ontwikkeling van de *meta-approach*, de *conformity assessment* die als onderdeel van het schema ontwikkeld is. Belangrijke uitgangspunten hierbij waren aansluiten op de voor de clouddienstverlening zeer relevante *assurance* standaarden van de International Auditing and Assurance Standards Board (IAASB) en het realiseren van een aanpak die door het Agentschap Telecom (AT) kan worden gehanteerd in haar nieuwe rol als National Cybersecurity Certification Authority (NCCA). In deze activiteit is nauw met Agentschap Telecom (AT) samengewerkt.[44]<br>• De certificeringsschema's voor 5G en voor de *common criteria* worden ontwikkeld, het certificeringsschema voor IoT is aangekondigd door de Europese Commissie.[45]<br>• De Nederlandse inzet op de ontwikkeling van certificeringschema's voor industriële controlesystemen, Internet of Things (IoT) en veilige softwareontwikkeling heeft zich vertaald in de prioritering van deze schema's door de Commissie in het *rolling work program*.[46] |
| • Onder Nederlands voorzitterschap en secretariaat is een werkgroep gestart van CEN/CENELEC voor digitale productveiligheid.[47] | |
| • Centrum voor Criminaliteitspreventie en Veiligheid (CCV) ontwikkelt een cybersecurity risicomodel voor (mkb-)bedrijven inclusief passende beschermingsmaatregelen, een certificeringsschema voor cybersecuritydiensten en een lijst met eisen die bedrijven kunnen stellen aan deze dienstverleners.[48] | • Het CCV heeft in samenwerking met diverse private partijen een risicoklasseindeling Digitale Veiligheid ontwikkeld voor het mkb. De risicoklasseindeling is beschikbaar via de website van het Digital Trust Center (DTC).[49] |
| | • Door de SSA is in 2018 een kader gepubliceerd voor veilige softwareontwikkeling.[50] |
| | • Er is een handreiking voor de digitale veiligheid van IoT gepubliceerd door Centrum Informatiebeveiliging en Privacybescherming (CIP) waaraan onder meer IBM, Philips, Centric, Lancom, DXC, Rijkswaterstaat, Electronic |

[36] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[37] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[38] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[39] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[40] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[41] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[42] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[43] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[44] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[45] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[46] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[47] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[48] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[49] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[50] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.

| | |
|---|---|
| | Commerce Platform (ECP) en het ministerie van Economische Zaken en Klimaat hebben bijgedragen.[51] |
| **1b. Nationale ontwikkelingen standaarden en certificering** | |
| • CCV heeft een certificeringsschema ontwikkeld voor pentesten. | • Het certificeringsschema voor pentesten is in april 2021 gepubliceerd. Aanbieders van pentesten kunnen zich op basis hiervan laten certificeren. Dit verschaft duidelijkheid voor de afnemer over de kwaliteit van deze dienst.[52] |
| • Ten behoeve van een effectieve implementatie van het Framework Secure Software in organisaties zijn geautomatiseerde controles ontwikkeld.[53] | • De geautomatiseerde controles geven organisaties meer inzicht in cybersecurity binnen het constante ontwikkelproces van complexe softwareproducten in samenwerking met hun toeleveranciers.[54] |
| • De OTC is gelanceerd met ruim dertig partijen vanuit het bedrijfsleven, wetenschap en overheid.[55] | • De OTC maakt een eenduidige, efficiënte methode beschikbaar waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn.[56] |
| • De SSA zet in op pilots om de methodiek toe te passen bij bedrijven. Ook is de samenwerking gezocht met hogescholen en universiteiten om in ICT-opleidingen veilige softwareontwikkeling te stimuleren.[57] | • Door de SSA is een kader gepubliceerd voor softwareontwikkelaars en de gebruikers/organisaties die software gebruiken met als doel de veiligheid van software meetbaar, beheersbaar en controleerbaar te maken.[58]<br>• Vervolgens is het raamwerk van de SSA aangescherpt en zijn verschillende aanvullende producten ontwikkeld:[59]<br>  ○ Een *awareness training* voor teams van softwareontwikkelaars, *productowners* (binnen bedrijven vaak juristen, verantwoordelijk voor een specifieke dienst die bij externen wordt ingehuurd) en bestuurders. Deze training is ontwikkeld en toegepast bij de Wageningen Universiteit (WUR) en International Creditcard Services (ICS).<br>  ○ Richtlijnen voor het toepassen van het raamwerk in organisaties met een volwassenheidsmodel en een meetinstrument om de effectiviteit van de verbetermaatregelen continu te monitoren.<br>  ○ Een governance dashboard met managementinformatie waarmee bestuurders de veiligheid van software gedurende de gehele levenscyclus kunnen monitoren.<br>• Het raamwerk is onderdeel geworden van het curriculum van NCOI en de Universiteit van Antwerpen, om vanaf de start van hun carrière veilige softwareontwikkeling mee te geven aan toekomstige ICT'ers, en in de postacademische opleidingen voor software engineers op de VU en Antwerpen. Diverse Hogescholen besteden in hun onderwijs aandacht aan het framework. De VEReniging van Software Engineers (VERSEN) is een belangrijke partner en is initiatiefnemer van een internationale (Frankrijk, Duitsland, Spanje) samenwerking om een Horizon programma in te dienen, waarbij het raamwerk onderdeel wordt van alle softwareontwikkeling die plaatsvindt onder de vlag van de Europese Commissie.<br>• Het raamwerk is volledig geïmplementeerd bij ICS en op de *controls* in het framework wordt gesteund door onder andere de toezichthouders bij ABNAMRO (moedermaatschappij van ICS), en De Nederlandsche Bank (DNB).<br>  ○ Het Framework Secure Software is geïmplementeerd bij de WUR en deels bij het Kadaster. Het Framework wordt nu geïmplementeerd bij Klaver Vier verzekeringen en bij Leaseplan. |

[51] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[52] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[53] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[54] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[55] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[56] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[57] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[58] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[59] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.

## 2. Monitor digitale veiligheid van producten

*De Kamerbrief van 2019 noemt deze maatregel nog separaat. In de Kamerbrieven van 2020 en 2021, na het ontwikkelen van de monitor, wordt de voortgang op deze maatregel gezamenlijk besproken met maatregel 3 (opschonen besmette producten bij gebruikers). Daarom bespreken we de activiteiten en resultaten van maatregel 2 als onderdeel van maatregel 3.*

## 3. Opschonen besmette producten bij gebruikers

| Activiteiten | Resultaten |
|---|---|
| • De Technische Universiteit (TU) Delft heeft een monitor ontwikkeld die geautomatiseerd metingen doet om zicht te krijgen in het aantal besmette, met het internet verbonden, slimme apparaten in Nederlandse netwerken.[60] | • TU Delft heeft vastgesteld dat het aantal gemeten besmette apparaten in Nederland laag is ten opzichte van andere landen, met een gemiddelde van 109 apparaten per dag. IP camera's en op een netwerk aangesloten opslagruimten (NAS) zijn nog steeds de meest voorkomende categorieën.[61]<br>• Overzichten van IP-adressen van gecompromitteerde apparaten worden maandelijks met de Internet Service Providers (ISPs) gedeeld via de Abuse Information Exchange (AIE). De desbetreffende ISPs kunnen vervolgens hun klanten benaderen om de apparaten op te schonen.[62] |
| • Door het DTC is intensief samengewerkt met de TU Delft om de data van de metingen om te zetten in bruikbare informatie.<br>• Het DTC is in gesprek gegaan met fabrikanten en andere stakeholders over korte termijnmaatregelen die zij kunnen nemen om besmette apparaten veilig te maken.[63] | • Uiteindelijke analyse door het DTC leverde hetzelfde beeld op als geschetst door de TU Delft: het aantal besmettingen van IoT producten in Nederland is laag. Uit de analyse kwam wel één fabrikant naar boven die in absolute getallen ver uitstak boven de rest. Het DTC heeft daarom eind 2020 en begin 2021 per e-mail contact gezocht met deze specifieke leverancier. Dit heeft niet geleid tot een gesprek.<br>• Naar aanleiding van de analyse heeft het DTC prioriteit gegeven aan het verspreiden van algemene en specifieke informatie over de kwetsbaarheden in en van IoT producten.[64] |

## 4. Testen op digitale veiligheid

| Activiteiten | Resultaten |
|---|---|
| • In 2020-2021 hebben diverse cybersecurity- en privacy tests op slimme apparaten plaatsgevonden in het kader van het testprogramma Connected Products van de Consumentenbond.[65] | • De testresultaten zijn beschikbaar op de website van de Consumentenbond. Uit de verschillende onderzoeken komt het beeld naar voren dat meer bekende, gerenommeerde merken het meest aandacht hebben voor privacy en veiligheid.[66] Met deze testresultaten kunnen consumenten ook de digitale veiligheid en privacy van producten meewegen in hun aankoopkeuzes.[67] |
| • AT heeft onderzoek uit laten voeren naar de digitale veiligheid van 22 apparaten in de categorieën slim speelgoed, IP-camera's, routers, slimme sloten, babymonitors en slimme thermostaten.[68] | • Twee rapporten als resultaten:<br>○ Rapport over digitale veiligheid van IoT-apparatuur: Agentschap Telecom (2019). Onderzoek veiligheid apparaten.[69]<br>○ Rapport over digitale veiligheidseisen van IoT-apparatuur: Qbit Cyber Security (2020). Essential requirements for securing IoT consumer devices.[70] |

[60] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[61] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[62] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[63] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[64] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[65] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[66] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[67] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[68] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[69] Zie: https://www.agentschaptelecom.nl/onderwerpen/slimme-apparaten/documenten/rapporten/2019/09/25/rapport-digitale-veiligheid-van-IoT-apparatuur.
[70] Zie: https://www.agentschaptelecom.nl/onderwerpen/slimme-apparaten/documenten/rapporten/2020/08/26/onderzoeksrapport-essential-requirements-for-securing-IoT-consumer-devices.

| 5. Cyber-security onderzoek | |
|---|---|
| **Activiteiten** | **Resultaten** |
| • Het kabinet heeft een publiek-privaat samenwerkingsplatform voor cybersecurity-kennis en -innovatie opgericht, genaamd dcypher.[71]<br>• Vijf kwartiermakers uit wetenschap, onderwijs, bedrijfsleven en overheid hebben een advies uitgebracht over de vormgeving van een nieuw platform als opvolger van dcypher. Op basis van de aanbevelingen uit dit advies wordt het nieuwe platform ingericht.[72] Er zullen concrete projecten worden ontwikkeld met als doel om valorisatie in het cybersecurity domein te stimuleren, meer cybersecurity personeel op te leiden en internationaal leidende cyber expertise te genereren.[73] | • Het bestuur van dcypher is ingericht met vertegenwoordiging vanuit private organisaties, kennisinstellingen en de overheid. Ter ondersteuning van dcypher is bij de Rijksdienst voor Ondernemend Nederland (RVO) een platformbureau opgericht. Ook zijn twee routekaarten opgesteld met de inhoudelijke agendering en programmering van kennis en innovatietrajecten (looptijd tot 2026) op de thema's geautomatiseerd kwetsbaarheden onderzoek (*Automated Vulberability Research*) en cryptocommunicatie.[74] |
| • Op Europees niveau wordt ingezet op cybersecurity kennis en innovatie via Nederlandse representatie in de Governing Board van het recentelijk opgerichte European Cybersecurity, Industrial, Technology and Research Competence Centre (ECCC). De nationale input richting het ECCC zal vormgegeven worden middels nog op te richten Nationale Coördinatie Centra (NCC).[75] Een kwartiermaker is aangesteld om het NCC op te zetten. De verwachting is dat in de tweede helft van 2022 al een aantal taken opgestart kan worden. De doelstelling is om begin 2023 volledig operationeel te zijn.[76] | |
| • Ruim €8 miljoen aan onderzoeksgeld is toegekend aan het achtjarig onderzoeksproject An Internet of Secure Things – INTERSECT met ruim 45 aangesloten onderzoeksinstellingen, bedrijven en maatschappelijke organisaties. Het onderzoeksproject wordt gecoördineerd door de TU Eindhoven.[77] | |
| • Dcypher (voorganger van de huidige dcypher) heeft een nieuwe Nationale Cybersecurity Research Agenda (NCSRA III) gelanceerd.[78] | • Deze agenda vormt een leidraad op het gebied van onderzoek en innovatie bij het realiseren van de ambities zoals beschreven in de Nederlandse Cybersecurity Agenda (NCSA).[79] |
| • Investeringen in onderzoek:<br>○ In juni 2019 is vanuit de NWA €8 miljoen gehonoreerd aan het onderzoeksproject INTERSECT. Dit onderzoeksproject richt zich op de mogelijkheden van een veilig IoT door technisch onderzoek te combineren met juridische en criminologische benaderingen. In het | |

[71] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[72] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[73] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[74] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[75] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[76] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[77] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[78] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[79] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.

| | |
|---|---|
| INTERSECT-consortium doen 47 organisaties mee.[80]<br>○ In december 2019 is een call geopend van circa €8 miljoen voor cybersecurity-, governance- en cryptologievraagstukken.[81]<br>○ De Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) heeft eind 2019 ruim €4 miljoen gehonoreerd aan tien onderzoeksprojecten die binnen de call Cybersecurity - Digitale Veiligheid & Privacy zijn ingediend.[82]<br>○ In 2021 heeft het ministerie van EZK twee SBIR rondes gefinancierd, waarbij ook het ministerie van Defensie financieel heeft bijgedragen. Tezamen hebben de SBIR's voor Automated Vulnerability Research en Cryptocommunicatie een budget van €1,5 miljoen.[83]<br>○ Het ministerie van JenV heeft een bedrag van €385.000[84] ter beschikking gesteld voor het stimuleren van open source encryptie. Van deze investering is nog geen resultaat bekend.[85] | |

| 6. Aansprakelijkheid | |
|---|---|
| • Door het Centre for the Law and Economics of Cyber Security van de Erasmus Universiteit Rotterdam is onderzoek uitgevoerd naar welke juridische en economische barrières er in de praktijk zouden zijn voor bedrijven onderling om schade te verhalen naar aanleiding van een cybersecurity incident.[86]<br>• Naar aanleiding van dit onderzoek heeft een aantal dialoogsessies plaatsgevonden met stakeholders uit het veld.[87] | • Uit het onderzoek komt naar voren dat de geleden schade varieert van financiële schade, verlies en/of verwijdering van data tot reputatieschade of productieverlies. Uit het onderzoek volgt dat er juridische en economische barrières zijn die het zeer complex maken voor bedrijven om geleden schade na een cybersecurity incident te verhalen.[88]<br>• Uit de dialoogsessies kwam naar voren dat de stakeholders een breed spectrum aan invalshoeken hadden, variërend van een nadruk op contractvrijheid en de daarmee samengaande eigen verantwoordelijkheid van partijen om bij contracten cybersecurity-gerelateerde aspecten mee te nemen, een mogelijke rol voor brancheorganisaties om aangesloten bedrijven te helpen met voorbeeld clausules, tot een grotere rol van de overheid bijvoorbeeld op het gebied van certificering.[89] |

| 7. Wettelijke eisen, toezicht en handhaving | |
|---|---|
| **Activiteiten** | **Resultaten** |
| **7a. Wettelijke digitale veiligheidseisen voor slimme apparaten** | |
| • Nederland maakt zich hard voor Europese wettelijke digitale veiligheidseisen aan alle slimme apparaten via de Europese richtlijn voor | • Op 29 oktober 2021 heeft de Europese Commissie bekend gemaakt dat wettelijke digitale veiligheidseisen gesteld zullen worden aan draadloos communicerende apparaten in het kader van de Europese richtlijn voor radioapparatuur (RED). Nederland heeft een leidende rol gespeeld in het |

[80] Zie: https://intersct.nl/consortium/.
[81] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Informatie- en communicatietechnologie (ICT)'.
[82] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Informatie- en communicatietechnologie (ICT)'.
[83] Zie: https://www.rvo.nl/subsidies-financiering/sbir/abc-sbir/cryptocommunicatie.
[84] De kamerbrief uit 2019 die rapporteert over de voortgang op de Roadmap stelt dat door JenV een bedrag van €410.000 ter beschikking is gesteld. Het ministerie van EZK heeft later naar de onderzoekers gecommuniceerd dat dit een bedrag van €385.000 betrof.
[85] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[86] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[87] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[88] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[89] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.

| | |
|---|---|
| radioapparatuur (de Radio Equipment Directive, RED).[90] | stellen van deze Europese eisen. De betreffende gedelegeerde handeling is verzonden aan de Europese Raad en het Europees Parlement. Wanneer deze handeling van kracht gaat kunnen consumenten er vervolgens op vertrouwen dat nieuw aangeschafte producten voldoen aan Europese normen, waarbij zij als gebruiker wel medeverantwoordelijk zijn deze producten veilig te blijven gebruiken. Producten die vanaf medio 2024 niet aan de cybersecurityeisen voldoen kunnen van de markt worden geweerd en gehaald door AT.[91]<br>• Daarnaast zet Nederland zich onder andere middels het uitbrengen van een non-paper in voor een Cyber Resilience Act (CRA) waarin duidelijke minimumeisen voor cybersecurity worden gesteld aan alle digitale producten, diensten en processen en die een zorgplicht oplegt aan de leveranciers en fabrikanten om gedurende de hele levenscyclus zorg te dragen voor de digitale beveiliging van deze producten, diensten en processen. Voor de CRA wordt in het najaar een voorstel van de Europese Commissie verwacht.[92] |
| • Het Nederlandse normalisatie instituut NEN ondersteunt het Nederlandse voorzitterschap van een Europese CEN/CENELEC werkgroep voor IoT-veiligheid. Nederlandse bedrijven en AT nemen deel aan dit proces.[93] | • Door het vervullen van het voorzitterschap en het secretariaat van de eerder werkgroep, pakt Nederland een leidende rol in het bepalen van de in Europa geldende normen voor cyber security in producten.[94] |
| • Vooruitlopend op het Europese standaardisatieproces heeft AT onderzoek uit laten voeren naar welke technische eisen onder de RED geschikt zouden kunnen zijn.[95] | • Het rapport is gepubliceerd. Uit het rapport blijkt dat een set van acht eisen zorgt voor een betere bescherming van consumenten tegen cyberaanvallen.[96] |
| **7b. Veiligheidsupdates in het consumentenrecht** | |
| • Op 27 april 2020 is de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud in werking getreden.<br>• De Autoriteit Consument & Markt (de ACM) bereidde in 2021 voorlichting over de richtlijnen verkoop goederen en levering digitale inhoud voor. De ACM verstrekt deze voorlichting onder meer via haar website en het consumentenvoorlichtingsportaal Consuwijzer.nl.[97] | • Met het Implementatiewetsvoorstel richtlijnen verkoop goederen en levering digitale inhoud zijn twee Europese consumentenrichtlijnen (verkoop goederen en levering digitale inhoud) geïmplementeerd.<br>• De ACM houdt toezicht op de regels die uit de Implementatiewet voortvloeien. De wet introduceert nieuwe regels en verduidelijkt bestaande regels die de aan- en verkoop van goederen en digitale inhoud, ook over de grenzen heen, veiliger en gemakkelijker maken en het expliciteert onder meer een verplicht updateregime voor digitale inhoud en tastbare goederen met een digitaal element. Consumenten hebben hiermee recht op (veiligheids-) updates zolang zij die redelijkerwijs mogen verwachten. De verkoper/handelaar zal afspraken moeten maken met een derde, zoals de fabrikant of een softwareleverancier, die de updates kunnen leveren.[98] |
| **7c. Toezicht** | |
| • Autoriteit persoonsgegevens:<br>○ AT heeft in het kader van haar toezichthoudende taken voortkomend uit de RED-eisen een IoT testlaboratorium ingericht waarin diverse apparaten worden getest op cybersecurityaspecten.[99]<br>○ Daarnaast is AT inmiddels aangewezen als Nationale Cybersecurity | • De ervaringen uit het testlaboratorium worden door AT gebruikt in gesprekken met de Europese Commissie en toezichthouders uit andere lidstaten, alsook in overleggen met de industrie.[102] |

[90] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[91] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[92] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[93] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[94] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[95] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[96] Zie: https://www.agentschaptelecom.nl/documenten/rapporten/2020/08/26/onderzoeksrapport-essential-requirements-for-securing-IoT-consumer-devices.
[97] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[98] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[99] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[102] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.

| | |
|---|---|
| Certificeringsautoriteit onder de Cyber Security Act.[100]<br>• AT neemt deel aan de Europese Stakeholders Cybersecurity Certification Group (ECCG) en is actief in ENISA werkgroepen voor ontwikkeling van schema's onder de Cyber Security Act.[101] | |
| • Acties van de Autoriteit Consument & Markt:<br>○ De ACM heeft samen met AT onderzoek gedaan naar domotica-apparaten, slimme apparaten voor thuisgebruik. Deze apparaten worden gebruikt om de processen in een woning te automatiseren en kunnen (indirect) worden verbonden met het internet.[103]<br>○ De ACM zal communiceren over een afgerond onderzoek naar precontractuele informatieverplichtingen bij de online verkoop van slimme apparaten.[104]<br>○ De ACM heeft een aantal grote online aanbieders van slimme apparaten aangesproken op de bestaande informatieverplichtingen bij hun aanbod van slimme apparaten aan consumenten.[105]<br>○ Naar één partij loopt nog onderzoek door de ACM. De ACM heeft hierover gepubliceerd en roept consumenten op meldingen te doen bij ConsuWijzer als zij voorafgaand aan een online aankoop van een slim apparaat niet goed zijn geïnformeerd. | • De ACM heeft op haar site consuwijzer.nl aangegeven welke informatie voorafgaand aan de koop aan consumenten moet worden verstrekt bij het online aanbod van slimme apparaten.[106]<br>• Drie van de aanbieders, Bol.com, Coolblue en MediaMarkt geven inmiddels meer informatie bij hun aanbod van slimme apparaten. Dit gaat onder andere om informatie over software-updates, wat het product doet, of je andere diensten nodig hebt om het apparaat te kunnen gebruiken, en welke eisen er gesteld worden aan de digitale omgeving van de consument.[107] |
| • Acties van de Autoriteit Persoonsgegevens (AP):<br>○ De AP neemt deel aan de ECCG in het kader van de CSA en de ontwikkeling van Europese certificeringschema's voor ICT-producten, diensten en processen.<br>○ Op nationaal niveau heeft de AP de *automotive* sector gewezen op de Algemene verordening gegevensbescherming (AVG) en de richtlijn *connected vehicles.* | • Op Europees niveau hebben de AP en haar Europese evenknieën richtlijnen uitgebracht voor de ontwikkeling en inzet van spraakassistenten en *connected vehicles*.<br>• De AP heeft samen met de Inspectie Gezondheidszorg en Jeugd (IGJ) een *factsheet* E-Health gepubliceerd voor de zorgsector, en een rapport over *smart cities* waarin (privacy)aanbevelingen worden gedaan om verantwoord verder te kunnen ontwikkelen.[108] De *factsheet* E-health is op de website van de IGJ vanaf januari 2021 tot en met mei 2022 318 maal bezocht en het document is 302 maal gedownload.[109] De *factsheet* E-Health heeft ook op de website van AP gestaan. Hoe vaak de *factsheet* daar is bekeken en gedownload is niet bekend. |
| • Dialoogsessies zijn gehouden met toezichthouders AT, de ACM, de AP en de Nederlandse Voedsel en Waren Autoriteit (NVWA) over welke rol zij kunnen spelen op het gebied van IoT.[110] | • Uit de dialoogsessies bleek dat de AP en de NVWA voldoende bevoegdheden hebben. De ACM en AT waren in afwachting van bevoegdheden.[111] AT heeft inmiddels bevoegdheden gekregen vanuit de RED-eisen (overgangsperiode tot 1 augustus 2014. Voor de ACM is de implementatieweg verkoop goederen en digitale inhoud in april 2020 door de Eerste Kamer goedgekeurd. |

[100] Zie: https://magazines.agentschaptelecom.nl/staatvandeether/2021/01/agentschap-telecom-als-nationale-cybersecurity-certificeringsautoriteit.
[101] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[103] Zie: https://www.acm.nl/nl/publicaties/acm-en-onderzoeken-veiligheid-en-juiste-informatie-bij-verkoop-slimme-apparaten.
[104] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[105] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[106] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[107] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[108] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[109] Informatie verstrekt door de Inspectie Gezondheidszorg en Jeugd.
[110] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[111] Ministerie van Economische Zaken en Klimaat (2019) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.

| 8. Bewustwordingscampagnes en empowerment | |
|---|---|
| **Activiteiten** | **Resultaten** |
| • In opdracht van EZK is een onderzoek[112] uitgevoerd waaruit blijkt dat meer dan de helft van de mensen het uitvoeren van updates uitstelt.[113]<br>• EZK is naar aanleiding van dit onderzoek gestart met de publiekscampagne 'Doe je updates'.[114] | • Er hebben inmiddels vier *flights* van de campagne plaats gevonden. Uit effectmetingen van de campagnerondes blijkt dat de campagne goed wordt ontvangen, maar dat de slag naar het gewenste gedrag nog gemaakt moet worden.[115] |
| • De tiende editie van Alert Online heeft in 2021 plaatsgevonden, waar onder de vlag van Alert Online worden verschillende bewustwordingsinitiatieven in de Europese cybersecuritymaand samen gebracht.[116] | Tijdens deze editie is georganiseerd:[117]<br>• Kick off met presentatie resultaten trendonderzoek veilig online.<br>• Webinar over gedragsbeïnvloeding.<br>• Webinar over ketenveiligheid. |

| 9. Inkoopbeleid van de Rijksoverheid | |
|---|---|
| **Activiteiten** | **Resultaten** |
| • Het programma Inkoopeisen Cybersecurity is gestart.[118]<br>• Een expertgroep met vertegenwoordigers vanuit het Rijk, de provincies, de gemeenten en de waterschappen heeft bijgedragen aan het formuleren van cybersecurity inkoopeisen voor de verschillende onderkende inkoopsegmenten zoals clouddiensten en serverplatformen.[119] | • Dit programma heeft de ICO-Wizard opgeleverd. Dit is een laagdrempelig instrument om gericht inkoopeisen mee samen te stellen voor aanbesteding/inkopen. Deze eisen worden vervolgens meegestuurd bij een aanbesteding en kunnen later in een contract met een leverancier worden opgenomen. Door de open toegang via BIO-overheid.nl, waar het ICO op te vinden is, is het mogelijk voor marktpartijen om gebruik te maken van de mogelijke eisen die de inkopende overheden hanteren.[120,121]<br>• Voor de Wizard zijn elf inkoopsegmenten uitgewerkt. Naast de 11 onderkende ICT-inkoopsegmenten is de ICO-Wizard aangevuld met Privacy-By-Design-eisen en het inkoopsegment Procesautomatisering (gebaseerd op CSIR).[122]<br>• Sinds de start van bovenstaande ontwikkelingen hebben er pilots plaatsgevonden met de cybersecurity-inkoopeisen bij 35 inkooptrajecten binnen alle overheidslagen inclusief uitvoeringsinstanties.[123] Inmiddels zijn er 50 bekende gebruikersorganisaties binnen de overheid die de uitkomsten uit ICO-Wizard gebruiken bij ICT-inkopen en –aanbestedingen.[124] |
| | • Er is een implementatiestrategie ontwikkeld gericht op de verbreding van het gebruik van de ICO en het op gang krijgen van een betere interactie tussen de driehoek informatiebeveiliger, opdrachtgever en inkoper.[125] Dit traject loopt door tot eind 2022. Doel van de implementatiestrategie is te komen tot met klem gebruiken door alle overheidsorganisaties. Onder deze implementatiestrategie zijn verschillende activiteiten uitgevoerd zoals een communiqué voor partnerpartijen, een presentatie voor bestuurders/beslissers is gemaakt, een standaard Demo is ontwikkeld en uitgerold om de Inkoop-driehoek te versterken en workshops zijn gegeven voor de Inkoop-driehoek. Daarnaast zijn er nog verschillende activiteiten die nog ontwikkeld of gestart moeten worden.[126] |

[112] Zie: https://www.campagnetoolkits.nl/documenten/publicaties/2020/01/31/flitspeiling-slimme-apparaten.
[113] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[114] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[115] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[116] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[117] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[118] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[119] Ministerie van Economische Zaken en Klimaat (2020) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[120] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[121] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[122] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[123] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[124] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.
[125] Ministerie van Economische Zaken en Klimaat (2021) Kamerbrief 'Voortgang Roadmap Digitaal Veilige Hard- en Software'.
[126] Informatie verstrekt via beleidsdirectie Digitale Economie van het Ministerie van Economische Zaken en Klimaat.

# Bijlage 2: Gesprekspartners

| Gesprekspartners (alfabetische volgorde) | |
|---|---|
| 1 | Agentschap Telecom |
| 2 | De Autoriteit Consument & Markt |
| 3 | CIO Platform Nederland |
| 4 | CIP-Overheid |
| 5 | Consumentenbond |
| 6 | dcypher |
| 7 | Digital Trust Centre |
| 8 | TU Delft |
| 9 | Ministerie van Economische Zaken en Klimaat |
| 10 | NLdigital |
| 11 | Online Trust Coalitie |
| 12 | Stichting Koninklijk Nederlands Normalisatie Instituut |
| 13 | VNO-NCW |

# Bijlage 3: Beschrijving van contextuele ontwikkelingen

**Beschrijving Europese wet- en regelgeving:**

1. **De Cybersecurity Act (CSA).** De Cybersecurity Act (CSA) is ingegaan in 2019 en betreft een verordening waarmee de EU grensoverschrijdende cyberaanvallen beter het hoofd kan bieden. De nieuwe regels geven Europa een kader voor de certificering van producten, processen en diensten op het gebied van cyberveiligheid en versterken het mandaat van het EU-agentschap voor cyberveiligheid, ENISA.[127]
2. **Richtlijn levering van digitale inhoud en digitale diensten.** In 2019 zijn twee nieuwe richtlijnen aangenomen die van groot belang zijn voor het consumentenrecht. De Richtlijn digitale inhoud voorziet in een thans bestaande lacune met betrekking tot overeenkomsten die zien op de levering van digitale inhoud en diensten. De nieuwe Richtlijn consumentenkoop vervangt de oude Richtlijn consumentenkoop uit 1999.[128]
3. **Radio Equipment Directive.** De RED zijn de Europese wettelijke digitale veiligheidseisen aan alle slimme apparaten via de Europese richtlijn voor radioapparatuur. De introductie van deze minimum veiligheidseisen in het kader van de RED vereist gedelegeerde handelingen[129] van de Europese Commissie. Deze handelingen, zijn ingegaan op 1 februari 2022 en worden verplicht op 1 augustus 2024.[130]
4. **De Cyber Resilience Act (CRA).** Een eerste voorstel voor de CRA wordt in het najaar van 2022 verwacht. Doel is om gestroomlijnde cyberbeveiligingsvereisten vast te stellen die een breed scala aan digitale producten en hun ondersteunende diensten bestrijken, waaronder tastbare digitale producten (draadloos en bedraad) en niet-ingebedde software, en zou hun hele levenscyclus bestrijken. De Cyber Resilience Act zou ook een aanvulling zijn op de gedelegeerde handelingen in het kader van de Radio Equipment Directive (zie hieronder).[131]
5. **Herziene richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS 2-richtlijn).** Voorstel van de Europese Commissie dat nu voorligt breidt het toepassingsgebied van de NIS richtlijn inzake netwerk- en informatiebeveiliging uit.[132]
6. **AI Act.** De AI Act is een voorgestelde Europese wet met betrekking tot kunstmatige intelligentie. De wet kent drie risicocategorieën toe aan AI toepassingen: 1) Een verbod op toepassingen en systemen die een onaanvaardbaar risico vormen, zoals een door de overheid gerund sociale score systeem zoals dat in China wordt gebruikt; 2) Specifieke wettelijke vereisten voor risicovolle toepassingen zoals tools die sollicitanten rangschikken; 3) Grotendeels ongereguleerd laten van toepassingen niet expliciet zijn verboden of als risicovol worden vermeld.[133]
7. **Data Act.** De Data Act is een voorstel voor een verordening die de regels voor eerlijke toegang tot en gebruik van gegevens harmoniseert. Het zal een sleutelrol spelen in het digitale decennium en helpen om de regels voor de digitale economie en de samenleving vorm te geven.[134]

[127] Zie: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.
[128] Zie: https://www.bjutijdschriften.nl/tijdschrift/tijdschrifteuropeesrecht/2019/9-10/NtER_1382-4120_2019_025_009_002/fullscreen#:~:text=2%20lid%205%20Richtlijn%20(EU,de%20verkoper%20of%20een%20derde.
[129] Gedelegeerde handelingen zijn door de Europese Commissie vastgestelde besluiten, die dienen als wijziging van, of aanvulling op de niet-essentiële elementen van wetgeving.
[130] Zie: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0030.
[131] Zie: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act.
[132] Zie: https://www.grantthornton.nl/insights/themas/cyberrisico/nieuwe-richtlijn-cyberbeveiliging-nis-2.0-voorgesteld/.
[133] Zie: https://artificialintelligenceact.eu/.
[134] Zie: https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet.

8. **Data Governance Act (DGA).** In december 2021 hebben de Europese Raad en het Europees parlement een voorlopig akkoord bereikt over de DGA. De DGA is het eerste wetgevingsinitiatief van de Europese datastrategie die tot doel heeft van de EU een leider te maken in een data gestuurde samenleving. De DGA zorgt ervoor dat gegevens vrij binnen de EU en tussen sectoren kunnen stromen. Dit heeft zowel een voordeel voor burgers als voor bedrijven en overheidsorganisaties.[135]
9. **Digital Services Act (DSA). 0**De Digital Services Act (DSA) vormt de toekomstige basis voor digitale diensten en verduidelijkt de verantwoordelijkheden van deze diensten qua activiteiten en informatie richting afnemers. De DSA verbetert onder meer de bestrijding van illegale inhoud online.[136]

**Nationale publicaties:**

1. **Kingdom of the Netherlands (2022). Non-paper on the principles of a Cyber Resilience Act.** Met deze non-paper wil Nederland bijdragen aan een brede beleidsdiscussie over cybersecurity in het algemeen en de Cyber Resilience Act in het bijzonder, waarin de noodzakelijke stappen worden geschetst om te zorgen voor een veilige Europese digitale interne markt.[137]
2. **CBS (2021). Bijna drie kwart van de Nederlanders maakt gebruik van slimme apparaten.** Dit rapport beschrijft dat bijna drie kwart van de Nederlanders van 12 jaar of ouder slimme apparaten bezit.[138]
3. **WRR (2021). Opgave AI. De nieuwe systeemtechnologie.** Dit rapport beschrijft dat kunstmatige intelligentie (AI) allerlei vormen en toepassingen kent: van gezichtsherkenning tot vertaalapps, van medische diagnoses tot anticiperen op criminaliteit, en van fraudebestrijding tot het beïnvloeden van wat we kopen, lezen en stemmen. En dat is nog maar het begin. Als Nederland zich op deze fundamentele verandering niet goed voorbereidt, is er niet alleen het risico dat kansen worden gemist, maar ook dat de samenleving opgescheept wordt met een technologie die onze belangen niet dient.[139]
4. **CSR (2021). Adviesrapport Integrale aanpak cyberweerbaarheid.** Dit rapport beschrijft dat de Nederlandse digitale veiligheid en digitale autonomie onder druk staan en daarmee het maatschappelijk en economisch welzijn. De cyberweerbaarheid van ons land moet chefsache zijn. Daarom verdient cyberweerbaarheid regie op het hoogste politieke- en ambtelijke niveau en een aanpak waarbij publiek, privaat en wetenschap elkaar versterken. Nederland moet de krachten bundelen en werken aan één cyberweerbaarheidsstrategie met een meerjarenprogramma zodat we onze ambities kunnen verwezenlijken, ons kunnen wapenen tegen cyberaanvallen en onze digitale autonomie kunnen verstevigen. Hiervoor is een investering nodig van €833 miljoen, boven op de huidige uitgaven en budgetten voor cyberweerbaarheid.[140]
5. **OVV (2021). Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix.** De Onderzoeksraad voor Veiligheid concludeert in het rapport 'Kwetsbaar door software' dat de Nederlandse aanpak van digitale veiligheid snel en fundamenteel moet veranderen om te voorkomen dat de maatschappij ontwricht raakt door cyberaanvallen. De Onderzoeksraad onderzocht hiervoor beveiligingslekken die ontstonden bij duizenden organisaties door kwetsbaarheden in software van Citrix.[141]

[135] Zie: https://data.overheid.nl/actueel/nieuws/data-governance-act.
[136] Zie: https://www.rijksoverheid.nl/actueel/nieuws/2021/11/24/eu-ministers-akkoord-met-regelgeving-digitale-diensten-en--markten.
[137] Zie: https://www.permanentrepresentations.nl/documents/publications/2022/01/12/non-paper-on-the-principles-of-a-cyber-resilience-act.
[138] Zie: https://www.cbs.nl/nl-nl/nieuws/2021/48/bijna-drie-kwart-van-de-nederlanders-maakt-gebruik-van-slimme-apparaten.
[139] Zie: https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie.
[140] Zie: https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid.
[141] Zie: https://www.onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software---lessen-naar-aanleiding-van.

**Nassaulaan 1**
**2514 JS Den Haag**

**+31 (0)70 359 6955**
**info@kwinkgroep.nl**
**www.kwinkgroep.nl**

KWINK GROEP