Roadmap

Digitaal Veilige Hard- en Software

Roadmap

Digitaal Veilige Hard- en Software

Ministerie van Economische Zaken en Klimaat
Ministerie van Justitie en Veiligheid

Den Haag, april 2018


09:41
smart home
DEVICE
GROUP
SCENE
add new
preferences
speaker
lights
heating
power
doors
locks
OFFICE
LIGHT

Inhoud

Voorwoord

Een teddybeer, een wasmachine, een thermostaat en een bewegingssensor hebben op het eerste oog weinig met elkaar gemeen. Behalve dan dat je ze allemaal kunt aansluiten op het internet. Een teddybeer als middel om een taal te leren, een wasmachine die alleen draait als de windmolens draaien, en een thermostaat die leert wanneer hij een tikkie lager kan. En sensoren kunnen - afhankelijk van de apparaten en apps waarmee ze worden gecombineerd - je huis veilig houden, of de alarmcentrale bellen als iemand valt. Het internet der dingen staat in de kinderschoenen en het groeit razendsnel. Het maakt ons leven makkelijker en leuker. Het heeft zijn eigen mogelijkheden én problemen. Juist omdat de digitale wereld en de fysieke wereld hier met elkaar verweven raken, zijn de mogelijke gevolgen van digitale kwetsbaarheden ingrijpend. Kinderspeelgoed, dat zich ontpopt als spionage-apparatuur. Of slimme thermostaten in Nederland die worden ingezet voor DDOS-aanvallen elders in de wereld – en geen mens die er iets van merkt. Met deze Roadmap Digitaal Veilige Hard- en Software gaan we daar iets aan doen.

De digitale veiligheid van hard- en software vraagt om een aanpak die flexibel genoeg is om mee te bewegen met nieuwe ontwikkelingen en stevig genoeg om effectief te zijn. Een aanpak die helderheid schept over risico's en oplossingen, die richting geeft aan standaardisering en verplichte certificering, met campagnes die ons bewust maken van de risico's. Een aanpak die duidelijk maakt wat je er zelf als consument aan kunt doen. De aanpak beoogt dat aanbieders, gebruikers, en andere betrokkenen weten waar ze aan toe zijn, en draagt bij aan het vertrouwen in de digitalisering. Hiermee draagt de Roadmap dus niet alleen bij aan de digitale veiligheid, maar ook aan het realiseren van de kansen van de voortschrijdende digitalisering.

In deze Roadmap zijn maatregelen bijeengebracht die moeten leiden tot een aanzienlijke verbetering van de digitale veiligheid van hard- en software. Dat wil niet zeggen dat we alles al weten; daarvoor zijn de problemen te nieuw en te complex. Sommige trajecten bevinden zich nog in de verkenningsfase: daar willen we met alle betrokkenen - en dat zijn er nog al wat, bij digitale apparaten - uitwerken wat we gaan doen. Dat speelt bij het ontwikkelen van een veiligheidsmonitor en van innovatieve oplossingen voor het veilig houden of afvoeren van hard- en software. Het speelt ook bij vraagstukken rond aansprakelijkheid en toezicht. Deze Roadmap is een levend document. Zo nodig sturen we tussentijds bij en jaarlijks publiceren we een update, waarin we de vorderingen in kaart brengen.

Ik kijk er naar uit om met u op weg te gaan naar digitaal veilige hard- en software.

Mona Keijzer
Staatssecretaris van Economische Zaken en Klimaat


Station 2
Montagestation

Samenvatting

Door de digitalisering raken we steeds afhankelijker van ICT. Dit brengt vele voordelen met zich mee, maar maakt ons ook kwetsbaar, bijvoorbeeld voor gegevensdiefstal, sabotage van bedrijfsprocessen of afpersing. Doordat steeds meer apparaten met elkaar verbonden zijn, is digitale veiligheid niet alleen in het belang van het individu, maar ook van de samenleving als geheel. Veel partijen, waaronder de overheid, nemen op dit moment maatregelen om de veiligheid van digitale producten te bevorderen. Door gebrek aan samenhang en vanwege markt- en gedragsfalen missen deze maatregelen echter nog de nodige effectiviteit.

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. Dit kan bijvoorbeeld met sterke wachtwoorden, tijdige updates en verwijdering van gegevens aan het einde van de levenscyclus. Hierbij is ook de gezamenlijke verantwoordelijkheid van belang: niet alleen de aanbieders van een product, maar ook de gebruikers hebben een rol te spelen bij digitale veiligheid. De overheid zet verschillende instrumenten in om de veiligheid van hard- en software te stimuleren en ook andere partijen als brancheorganisaties en universiteiten leveren daaraan een bijdrage.

Steeds moet daarbij de juiste balans worden gevonden tussen veiligheid, vrijheid en economische groei. Een eenzijdige focus op veiligheid kan ten koste gaan van andere publieke waarden als mensenrechten en innovatie. Dit terwijl innovatieve producten op termijn de digitale veiligheid juist kunnen verbeteren. Deze roadmap is erop gericht dreigingen het hoofd te bieden, fundamentele rechten en waarden te beschermen en tegelijkertijd de kansen van digitalisering volop te benutten. De roadmap biedt ook ruimte voor aanvullende maatregelen in specifieke domeinen of sectoren. De risicoanalyses en daarbij passende maatregelen kunnen immers aanzienlijk verschillen per domein of sector.

In deze roadmap worden de volgende maatregelen voorgesteld:

Standaarden en certificering. Het gebruik van standaarden is belangrijk voor het terugdringen van kwetsbaarheden, zowel bij het ontwerp als bij het gebruik van een product. Bovendien kunnen standaarden de vraag naar veilige producten stimuleren. Er wordt met name gestuurd op het harmoniseren van uiteenlopende initiatieven voor het opstellen van standaarden om de (kosten)effectiviteit te behouden én op een actieve bijdrage aan Europese onderhandelingen op het gebied van standaarden en verplichte certificering.

Monitor digitale veiligheid van producten. Het opsporen en delen van informatie over kwetsbaarheden biedt de fabrikanten de mogelijkheid om onveilige producten aan te passen. Verkopers kunnen overwegen om producten uit de schappen te nemen en gebruikers om producten te patchen of af te schakelen. Het kabinet gaat met publieke en private partijen een monitor ontwikkelen met informatie over de digitale veiligheid van producten, met specifiek aandacht voor Internet-of-Things-apparaten. Hierbij betrekt het kabinet internationale ervaringen.

Opschonen besmette producten bij gebruikers. Aanbieders van internettoegang kunnen een belangrijke rol spelen bij het vergroten van de veiligheid van hard- en software. Het kabinet gaat in gesprek met de aanbieders van internettoegang over hoe zij – analoog aan de succesvolle aanpak van botnets - kunnen bijdragen aan de bestrijding van onveilige IoT-apparaten.

Testen op digitale veiligheid. Testen zijn nodig om kwetsbaarheden in verschillende fasen van de product-levenscyclus op te sporen. Om ervaring op te doen en kennis op te bouwen over wat een gedeeld testplatform kan bieden, komt er een pilot aan de hand van diverse sectorale use cases.

Cybersecurity-onderzoek. Voor het veiliger maken van hard- en software is innovatie essentieel. Daarom investeert Nederland in onderzoek naar innovatieve oplossingen om veiligheidsproblemen het hoofd te bieden.

Aansprakelijkheid. Met een beroep op het aansprakelijkheidsrecht kunnen gebruikers schade door digitale onveiligheid verhalen. Dat biedt een financiële prikkel voor aanbieders om hard- en software veilig te houden. Het kabinet is met stakeholders en wetenschappers in gesprek over aandachts- en verbeterpunten rond aansprakelijkheid bij digitaal onveilige hard- en software. Ook neemt Nederland actief deel aan de expertgroep over aansprakelijkheid en nieuwe technologieën. Nederland stelt in de onderhandelingen over het richtlijnvoorstel digitale inhoud en digitale diensten voor om in alle gevallen veiligheidsupdates te verplichten bij software die is geleverd aan een consument.

Wettelijke eisen, toezicht en handhaving. Met het stellen van minimumveiligheidseisen kunnen onveilige producten van de markt geweerd worden. Het kabinet onderzoekt welke miniale veiligheidseisen kunnen worden gesteld aan apparaten via de Europese Radio Equipment Directive.

Bewustwordingscampagnes en empowerment. Als onderdeel van de cybersecurity bewustwordings-campagnes van veiliginternetten.nl lanceert de overheid één of meer beleidsondersteunende publiekscampagnes voor digitaal veilige hard- en software. Bewustwordingscampagnes zullen waar nodig aansluiten op bovengenoemde maatregelen, om consumenten en het MKB bewust en weerbaar te maken.

Inkoopbeleid van de Rijksoverheid. De Rijksoverheid is een belangrijke gebruiker van hard- en software. Zij kan criteria voor digitale veiligheid in haar inkoopbeleid opnemen en daarmee zowel het goede voor-beeld geven als de vraagzijde van digitaal veilige producten stimuleren. Het kabinet gaat onderzoeken welke aanvullende maatregelen nodig en gewenst zijn bij inkoop binnen de Rijksoverheid voor de digitale veiligheid van hard- en software.

1. Inleiding

De voortgaande digitalisering en snelle ontwikkelingen op ICT-gebied bieden Nederland grote kansen voor economische groei en maatschappelijke ontwikkeling. Dankzij nieuwe technologieën zijn we in staat informatie en kennis te verspreiden op een schaal en met een snelheid die voorheen ondenkbaar waren. Naar verwachting neemt het belang van ICT in de toekomst alleen maar verder toe. Zo was de economische groei de afgelopen tien jaar voor een kwart toe te schrijven aan ICT. Veelal wordt deze beweging de digitale revolutie genoemd. En velen claimen dat we slechts aan het begin van deze revolutie staan.

We raken door de voortzettende digitalisering steeds afhankelijker van ICT. Het is daarom belangrijk dat iedereen zo veilig en vertrouwd mogelijk gebruik kan maken van digitale producten. Dit is niet alleen van belang voor de eigen digitale veiligheid, maar ook voor de samenleving in zijn geheel. Door kwetsbaarheden in hard- en software kunnen kwaadwillende partijen zich namelijk eenvoudig toegang verschaffen tot een apparaat, en via het apparaat tot het netwerk waar het deel van uitmaakt. Met alle gevolgen van dien. Denk bijvoorbeeld aan het inzetten van gehackte slimme thermostaten voor DDOS-aanvallen, de mogelijkheid om apparaten of hele productieprocessen te verstoren, en diefstal van informatie die op een apparaat is opgeslagen.

Beleidsuitdaging

Allerlei partijen, waaronder de overheid, nemen maatregelen om de digitale veiligheid van hard- en software op orde te brengen.[1] 100% digitale veiligheid is niet mogelijk. Het maatschappelijk optimale niveau van digitale veiligheid is echter nog niet bereikt. Dit komt ten dele doordat de samenhang tussen verschillende maatregelen ontbreekt.[2] Daarnaast is er sprake van zogenaamd markt- en gedragsfalen. Zo houdt het bedrijfsleven niet altijd rekening met de veiligheidsrisico's die digitale processen en producten met zich meebrengen. Ook kunnen consumenten moeilijk een goede inschatting maken van het veiligheidsniveau van een digitaal apparaat, en kunnen zij de langetermijneffecten van hun beslissing op het gebied van digitale veiligheid moeilijk overzien.

De opgave is om de juiste mix van maatregelen te formuleren voor dit complexe speelveld. Er zijn mogelijk nieuwe en andere (zwaardere) (beleids)maatregelen nodig om digitaal veilige hard- en software te stimuleren. Hierbij hebben verschillende partijen op verschillende niveaus (bijvoorbeeld nationaal, Europees en internationaal) een rol.

1 Zie TNO-onderzoek onderzoek 'Digitaal Veilige Hard- en Software' (2017) voor een groslijst (niet uitputtend) van diverse instrumenten die partijen al inzetten om de digitale veiligheid van hard- en software te bevorderen.
2 TNO-onderzoek (2017).

Het is belangrijk om een compleet beeld te geven van de keten, problemen, inzetbare instrumenten (zowel de huidige als mogelijk nieuwe) en oplossingen die ze bieden.

Roadmap Digitaal Veilige Hard- en Software

De Roadmap Digitaal Veilige Hard- en Software ('Roadmap DVHS') beoogt de benodigde samenhangende aanpak te bieden om als Nederland voorop te lopen bij het bevorderen van de digitale veiligheid van hard- en software.[3] De roadmap heeft een dynamisch karakter: hij is wendbaar genoeg om in te kunnen spelen op nieuwe ontwikkelingen en robuust genoeg om te kunnen investeren in langetermijn maatregelen.

De Roadmap DVHS geeft mede invulling aan de Nederlandse Cybersecurityagenda,[3] en benut inzichten en aanbevelingen uit het TNO-rapport 'Digitaal Veilige Hard- en Software'. Bij het opstellen van deze roadmap is bovendien rekening gehouden met Europese ontwikkelingen[4] en het advies van de Cyber Security Raad over dit onderwerp.[5]

Work in progress

De roadmap is en blijft 'work in progress'. De ministeries van Economische Zaken en Klimaat en Justitie en Veiligheid willen met publieke en private partijen deze roadmap blijven (door)ontwikkelen en uitvoeren. De hiervoor liggende roadmap biedt de eerste bouwstenen. Hierbij zijn algemene uitgangspunten geformuleerd en is getracht om tot een samenhangend set van maatregelen te komen om de digitale veiligheid op een gebalanceerde wijze te bevorderen, waarbij diverse partijen een verantwoordelijkheid hebben. Dit laat onverlet dat er aanvullende maatregelen nodig of al getroffen zijn, bijvoorbeeld voor specifieke sectoren en domeinen.

3 Nederlandse Cyber Security Agenda 'Nederland digitaal veilig', Ministerie van Justitie en Veiligheid (2018).
4 https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#usefullinks.
5 CSR2017, 'Naar een veilig verbonden digitale samenleving; Advies inzake de cybersecurity van het Internet of Things (IoT)'.

Internet of Things

Een belangrijke drijver van de digitale revolutie is het zogenaamde *Internet of Things* (IoT). Steeds meer producten raken verbonden met het internet. IoT is een groeiend paradigma met technische, sociale en economische betekenis. Het is een opkomend concept dat bestaat uit een breed ecosysteem van onderling verbonden diensten en apparaten, zoals slimme alledaagse huisobjecten, camera's, auto's en gezondheidsmonitoren. Kenmerkend voor deze technologie is het verzamelen, uitwisselen en verwerken van gegevens via het internet. In 2017 waren 8.4 miljard apparaten verbonden met het internet, een toename van 31 procent ten opzicht van 2016. In 2020 zal dat aantal naar verwachting zijn gestegen tot 20.4 miljard. Minstens 63 procent daarvan zullen consumentenapparaten zijn.[1] De overige 37 procent betreft apparaten die door bedrijven worden gebruikt.

Dreiging

De afgelopen jaren waarschuwden verschillende securityexperts over de toenemende dreiging vanuit het IoT. IoT-apparaten zijn over het algemeen slecht beveiligd. Dit komt onder andere door het gebruik van standaardwachtwoorden, het ontbreken van encryptie en van software-updates om kwetsbaarheden en basale ontwerpfouten te verhelpen. De afgelopen jaren zijn deze kwetsbaarheden meerdere malen misbruikt en zijn IoT-apparaten als middel ingezet voor het uitvoeren van aanvallen. Daarnaast zijn in apparaten misbruikt om gebruikers af te luisteren of hun omgeving te manipuleren.

IoT in Nederland

Meer dan 92 procent van de Nederlanders heeft meer dan één IoT-apparaat in huis. Deze apparaten zijn aantrekkelijk voor cybercriminelen. 82 procent van de Nederlanders erkent dat apparaten die verbonden zijn met het internet gehackt kunnen worden. Desondanks treft bijna driekwart (71%) geen maatregelen tegen cybercrime.[2] Dat leidt in toenemende mate tot problemen, ook voor derde partijen. Met Mirai-malware werden IoT-apparaten als slimme thermostaten en smart tv's gehackt en misbruikt om het Internet plat te leggen, met naar schatting $ 110 miljoen schade in Noord-Amerika en Europa als gevolg. Ook Nederlandse IoT-producten werden door deze malware geïnfecteerd.

1 https://www.gartner.com/newsroom/id/3598917.
2 BIT 2017, Internet Eigenwijs.

Begrippen

In deze roadmap worden verschillende begrippen gehanteerd, zoals hard- en software en digitale producten en diensten. In Figuur 1 worden deze begrippen geïllustreerd met het voorbeeld van een slimme wasmachine. Het verschil tussen **hard- en software** is op twee manieren uit te drukken:

1: Hardware is een verzamelterm voor de fysieke onderdelen in digitale apparaten en software de verzamelterm voor de niet-tastbare programmatuur die op digitale apparaten wordt uitgevoerd. Voor het goed functioneren van een digitaal apparaat is de dynamiek tussen hard- en software cruciaal. Zo heeft hardware een bepaalde prestatie-limiet. Als de software prestatie-eisen stelt die hoger zijn dan deze limiet, kan het apparaat niet goed functioneren.

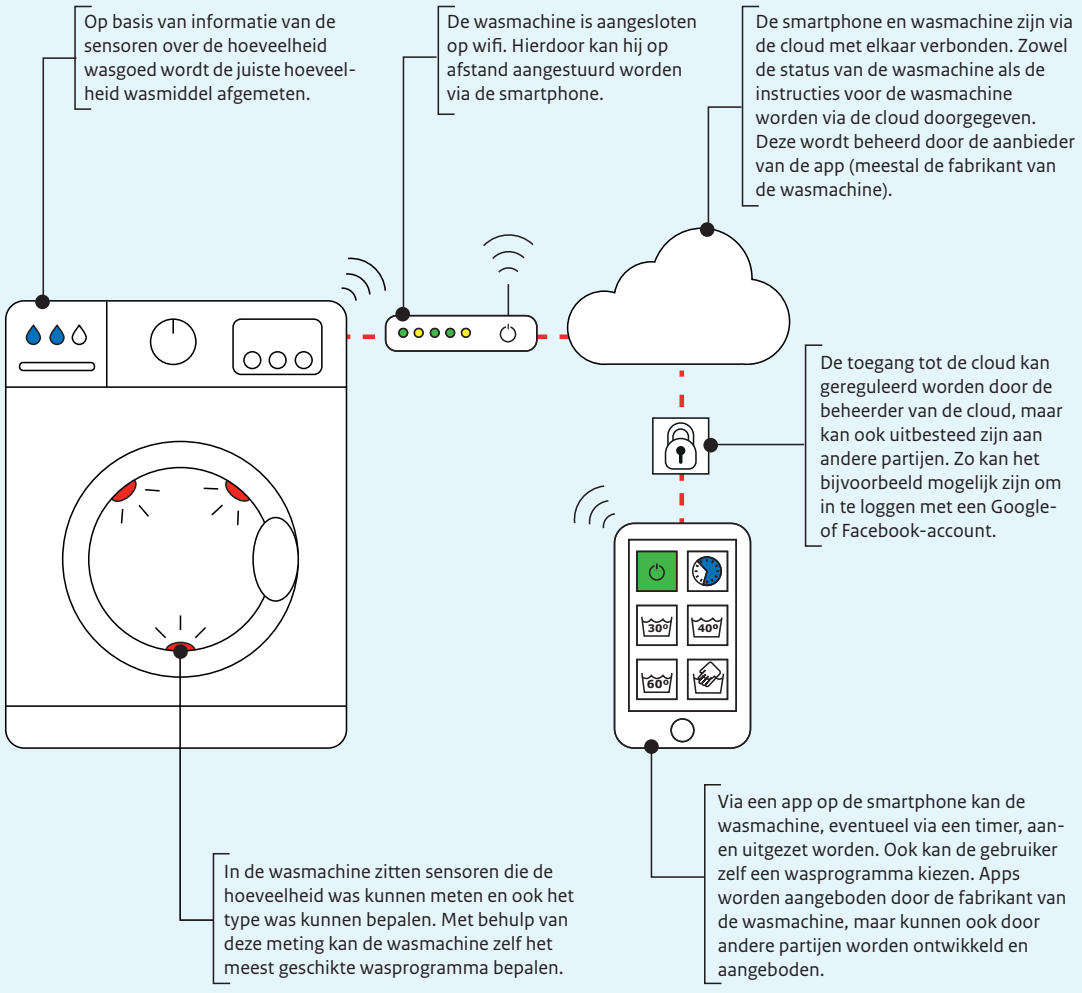
2: Het verschil tussen hard- en software kan ook uitgedrukt worden in de mate van bestendigheid. Hardware zou hierbij gezien kunnen worden als het deel van de digitale apparatuur met een vaste functionaliteit die niet veranderd kan worden en software als het deel dat makkelijker aangepast, vervangen of verwijderd kan worden. Dit onderscheid is echter gradueel. Bepaalde software is door de producent ingeprogrammeerd in de hardware en kan door de gebruiker moeilijk worden aangepast of verwijderd. Voorbeelden hiervan zijn firmware, die op een laag niveau controle uitvoert over de hardware, en ingebedde software, die specifiek voor een bepaalde hardware is ontworpen en vaak de enige software op het apparaat in kwestie is. Ook voor hardware geldt dat de functionaliteit van een component niet onveranderlijk is. Deze functionaliteit kan immers gestuurd worden door aanpassingen in de software. De fysieke eigenschappen van de hardware blijven daarbij echter wel hetzelfde.

Digitale producten zijn producten met een softwarecomponent. Deze producten kunnen ook hardwarecomponenten bevatten, maar dat is geen vereiste. Een **digitale dienst** is een dienst die langs elektronische weg wordt geleverd. Voorbeelden van dergelijke diensten zijn het updaten van software of uitlenen van een digitaal product.

Figuur 1 *De begrippen hard- en software en digitale producten en diensten kunnen geïllustreerd worden aan de hand van het voorbeeld van een slimme wasmachine. Deze wasmachine is in staat om op basis van sensoren in de wastrommel het juiste wasprogramma en de juiste hoeveelheid wasmiddel te kiezen. Ook kan de wasmachine aangesloten worden op wifi en daarmee verbinding maken met een smartphone. Via een app op de smartphone kan de wasmachine vanaf een afstand aangestuurd worden. De wasmachine en de smartphone communiceren met elkaar via een cloudservice.*

Alle mechanische en elektronische onderdelen van de wasmachine en de smartphone vallen onder hardware. Denk bijvoorbeeld aan de wastrommel en de sensoren en chips in de wasmachine en smartphone. Deze onderdelen worden, zowel in de wasmachine als in de smartphone, op laag niveau aangestuurd door firmware. Op hoger niveau worden de smartphone en wasmachine aangestuurd door specifieke software. Die is door de fabrikant in de wasmachine zelf ingeprogrammeerd (ingebedde software). Op de smartphone kan de software door de gebruiker gedownload worden in de vorm van een app.

De wasmachine is een digitaal product omdat hij een softwarecomponent bevat. Aan dit digitale product is een digitale dienst gekoppeld, namelijk de cloud service. Als de wasmachine niet gekocht maar gehuurd is, dan wordt de wasmachine zelf ook gezien als een digitale dienst.

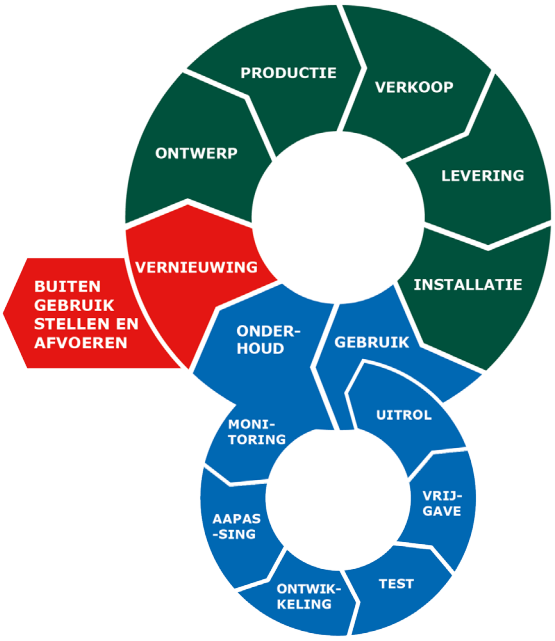


2. Uitgangspunten

De Roadmap DVHS hanteert vijf uitgangspunten voor de (door)ontwikkeling en uitvoering van een aanpak voor digitaal veilige hard- en software. Deze uitgangspunten staan hierna toegelicht.

2.1 Productlevenscyclus-benadering

Alle fasen van de productlevenscyclus zijn van belang voor het verhogen van de digitale veiligheid bij hard- en software. Grofweg zijn er drie fasen te onderscheiden: de fase vóór ingebruikname, de fase van gebruik en de fase van afstoting. Bij het veiliger maken van hard- en software wordt snel gedacht aan het stellen van eisen aan het ontwerp van een product. Bij digitale producten is de fase van gebruik echter minstens zo belangrijk. Dit omdat er bij digitale producten vaak een dienst geleverd wordt (vaak in de vorm van een cloudservice) die continu wordt bijgewerkt. Niet alleen de fabrikant, maar ook de gebruiker van het product is in deze fase verantwoordelijk voor het borgen van de digitale veiligheid, bijvoorbeeld door wachtwoorden te wijzigen of updates te installeren (zie uitgangspunt 2 'Gezamenlijke verantwoordelijkheid'). Op het moment dat de fabrikant besluit de software niet meer bij te werken, kan het zijn dat de gebruiker de software nog steeds blijft gebruiken. De fase van afstoting wordt daarom ook expliciet meegenomen in het maatregelenpakket.



***Figuur 2** Alle fasen van de productlevenscyclus zijn van belang voor het verhogen van de digitale veiligheid bij hard- en software. Er kan onderscheid worden gemaakt tussen de fase vóór ingebruikname (groen), de fase van gebruik (blauw) en de fase van buiten gebruik stellen en vernieuwen (rood).*

2.2 Gezamenlijke verantwoordelijkheid

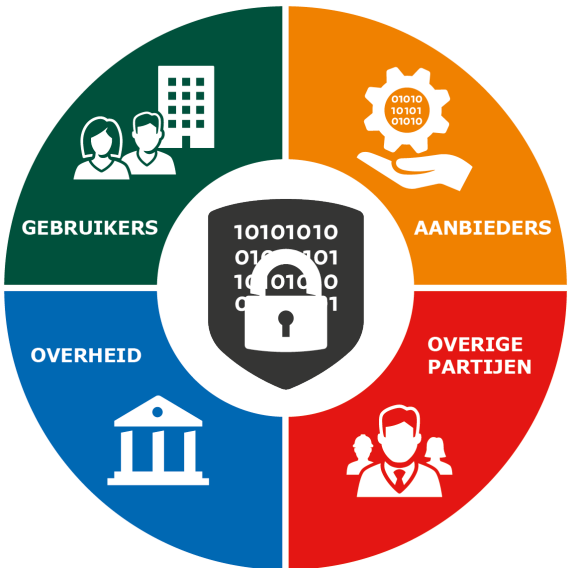
Er zijn verschillende verantwoordelijkheden en rollen voor de betrokken partijen, ervan uitgaande dat alle partijen nodig zijn om de digitale veiligheid van hard- en software te bevorderen. De betrokken partijen zijn echter erg divers: van consumenten, MKB en multinationals tot wetenschappers, belangenorganisaties en toezichthoudende instanties. Ieder heeft een eigen rol en eigen verantwoordelijkheid. Hierbij valt over het algemeen van grote professionele partijen meer te verwachten dan van bijvoorbeeld kleinere partijen. Op hoofdlijnen is de volgende verdeling te maken, waarbij onder meer de context (bijvoorbeeld business-to-business-relatie, consumer-to-business-relatie, consumer-to-consumer-relatie, vitale sector/niet-vitale sector) en het type speler (bijvoorbeeld professionele versus niet-professionele partij) bepalend is voor de precieze invulling.

Aanbieders (fabrikanten en verkopers): aanbieders zijn primair verantwoordelijk voor de digitale veiligheid van de door hen aangeboden hard- en software, en bijbehorende diensten. Zij vormen de eerste schakel voor het verankeren van digitale veiligheid bij het ontwerp, de productie en de verkoop van hard- en software.

Gebruikers (van consumenten en MKB tot multinationals): gebruikers kunnen de vraag naar digitaal veilige hard- en software stimuleren. Ook spelen zij een rol bij het onderhouden van hard- en software. Hierbij moet wel rekening worden gehouden met de beperkte rationaliteit van gebruikers: gebruikers kunnen moeilijk de impact van digitale veiligheidsrisico's inschatten, en zien bij een teveel aan informatie door de bomen het bos niet meer.

Overheid (incl. toezichthoudende instanties): de overheid is verantwoordelijk voor het borgen van publieke waarden. Dit kan de overheid doen met verschillende beleidsinstrumenten zoals stimuleringsmaatregelen, gedragsexperimenten en wetgeving. Ook kan de overheid als aanbestedende partij en gebruiker de vraag naar digitaal veilige hard- en software bevorderen.

Overige partijen (van brancheverenigingen, consumentenorganisaties en intermediaire bedrijven tot wetenschappers): naast de voornoemde partijen is er een diverse groep van andere partijen die kunnen bijdragen aan de digitale veiligheid van hard- en software. Het is belangrijk om ook deze partijen te betrekken bij de roadmap.



Figuur 3 Alle betrokken partijen zijn nodig om de digitale veiligheid van hard- en software te bevorderen.

2.3 Balans publieke waarden

Een dynamische balans tussen veiligheid, vrijheid en economische groei is nodig bij het bevorderen van de digitale veiligheid van hard- en software. Digitale veiligheid is een belangrijke voorwaarde om het economisch potentieel van digitalisering te benutten. Maar een eenzijdige focus op veiligheid kan ten koste gaan van andere publieke waarden als mensenrechten en innovatie. Ter illustratie: een set van maatregelen die geen rekening houdt met het innovatieklimaat kan afbreuk doen aan het innovatieve vermogen van Nederland. Dit is onwenselijk. Innovatieve producten kunnen immers juist bijdragen aan het versterken van de digitale veiligheid. Het kabinet zet zich daarom samen met zijn partners in voor een vrij, veilig en open cyberdomein, waarin de kansen van digitalisering volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.[1] Dit kan gerealiseerd worden door een constante open dialoog tussen alle stakeholders, zowel nationaal als internationaal.

2.4 Portfolio-benadering

Een breed palet aan instrumenten is nodig om de digitale veiligheid van hard- en software te bevorderen. Het ecosysteem van digitale producten is complex. In verschillende fasen van de productlevenscyclus kunnen, zoals

1 Zie onder meer de Nederlandse Cybersecurity Strategie 2 (2013) en Internationale Cyberstrategie 'Digitaal bruggen slaan' (2017).

Afwegen van publieke waarden

Het zoeken naar een juiste balans van publieke waarden is complex. Het conceptuele denkkader uit het rapport 'Balancing interests in developing cyber policy; A conceptual framework' dat PWC en Clingendael in opdracht van de ministeries van Economische Zaken en Klimaat, Jusititie en Veiligheid en Buitenlandse zaken hebben opgesteld illustreert dit. Achter economische groei, vrijheid en veiligheid gaan diverse dimensies schuil om deze publieke belangen te borgen. Denk bijvoorbeeld aan de keuzevrijheid van een gebruiker om een software-update te installeren. Moet de gebruiker deze beslissing te allen tijde zelf nemen, of zijn er situaties denkbaar waar de software-update automatisch geïnstalleerd moet worden? Het antwoord op deze vraag kan invloed hebben op andere publieke waarden. Zo kan het direct doorvoeren van een software-update positieve effecten hebben op de digitale veiligheid, maar een aantasting zijn van de individuele vrijheid.

Core public interests	Dimensions of intervention	Key policy dilemmas
Freedom	Ethical	• Paternalism vs. individual responsibility • Human vs. computer
	Economic	• Protective vs. reactive • Monopolies vs. competitive market
Prosperity	Legislative	• Transnational vs. national • Regulation vs. 'laissez faire'
	Administrative	• Centralized vs. decentralized • Private vs. public
	Diplomatic	• Transparency vs. secrecy • Digital sovereignty vs. international cooperation
Security	Protect & enforce	• Offensive vs. defensive • Known vs. unknown enemy

Figuur 4 Een conceptueel kader voor het afwegen van de publieke waarden vrijheid, veiligheid en welvaart in het cyberdomein. Uit: 'Balancing interest in developing cyber policy; A conceptual framework' (PWC en Clingendael, 2017).

hiervoor is toegelicht, kwetsbaarheden ontstaan. Ook kunnen in verschillende onderdelen van digitale producten veiligheidsrisico's ontstaan, met ieder hun eigen impact. Diverse partijen – zowel nationaal als internationaal – zijn betrokken bij deze fasen en bij de productie van de verschillende onderdelen. De risico's zijn dus niet te bestrijden met één instrument. Meerdere instrumenten zijn nodig om de digitale veiligheid van hard- en software op een gebalanceerde en dynamische wijze te bevorderen. Het is belangrijk om bij deze instrumentenmix te kijken naar hoe de instrumenten zich tot elkaar verhouden: waar ontstaan er mogelijk spanningsvelden en waar kunnen instrumenten elkaar juist versterken? De overheid heeft hierbij een regiefunctie om de publieke waarde 'digitale veiligheid' te borgen. Dit kan zij doen met 'zachtere' instrumenten als voorlichting en stimuleringsmaatregelen of 'hardere' instrumenten als wet- en regelgeving.

Preventie, detectie en mitigatie

De maatregelen van deze roadmap zijn onder te verdelen in drie categorieën: preventie, detectie en mitigatie (zie Figuur 5). Maatregelen uit de eerste categorie worden ingezet om veiligheidsrisico's in te perken, zoals het stellen van standaarden of het stimuleren van innovatie op het gebied van digitaal veilige hard- en software. Aangezien 100% digitale veiligheid niet haalbaar is, worden ook instrumenten ingezet om veiligheidsrisico's te detecteren, zoals het actief testen van digitale systemen. Tot slot worden er maatregelen genomen om de gevolgen van veiligheidsincidenten te mitigeren. Een belangrijk instrument hierbij is het aansprakelijkheidsrecht. Deze mix van instrumenten wordt in het volgende hoofdstuk verder toegelicht.

Figuur 5 Een breed palet aan instrumenten is nodig om de digitale veiligheid van hard- en software te bevorderen.

Basisbeginselen digitaal veilige hard- en software

Vanuit de regiefunctie van de overheid om de publieke waarde van digitale veiligheid te borgen is het relevant om te bezien in hoeverre hier een set van basisbeginselen voor digitaal veilige hard en software mogelijk is. Met deze basisbeginselen wordt een set van elementen en kenmerken bedoeld die het kabinet met publieke en private partijen wil waarborgen of uitsluiten als het gaat om digitaal veilige hard- en software. Denk hierbij aan non-default wachtwoorden, transparantie over datagebruik en doelen van algoritmen, en helderheid over de snelheid van beveiligingsupdates. Bij het ontwikkelen van een set van basisbeginselen wordt aangesloten op bestaande initiatieven. Het streven is om (vanuit gedeelde normen) dreigende versnippering van de aanpak tegen te gaan en harmonisatie te bevorderen. Deze set aan basisbeginselen kan ook dienen als de basis voor eventuele sectorspecifieke aanvullende maatregelen (zie uitgangspunt 5 hieronder) en voor een proactieve opstelling in Europa. Het streven is om met stakeholders tot een nationale gedeelde beschrijving van deze basisbeginselen te komen die effectief en efficiënt is.

2.5 Ruimte voor een aanvullende (gedifferentieerde) aanpak

De roadmap DVHS biedt een basis om als Nederland voorop te lopen in het bevorderen van de digitale veiligheid van hard- en software. In deze roadmap staan de eerste bouwstenen, waarbij is gezocht naar een gebalanceerde set van maatregelen die voldoet aan de hiervoor genoemde uitgangspunten. Dit laat echter onverlet dat er aanvullende maatregelen nodig zijn. Het maken van afgewogen risicobesluiten en het vinden van passende maatregelen blijft nodig binnen elk domein en elke sector. Bij een consumentenproduct speelt er bijvoorbeeld een andere afweging dan bij kritische infrastructuren of industriële processen. Ook zijn maatregelen in het ene domein niet altijd passend voor een ander domein. Binnen deze roadmap (en daarbuiten) blijft er daarom ruimte om domein- of sectorspecifieke maatregelen te treffen indien dat nodig of gewenst is.

3. Maatregelen

3.1 Standaarden en certificering

Standaarden en certificering kunnen bijdragen aan de digitale veiligheid van hard- en software gedurende de gehele levenscyclus: van ontwerp tot en met de afstotingsfase. In de ontwikkelfase dringen standaarden 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. Deze certificering door een onafhankelijke en deskundige instantie kan afnemers helpen om de juiste keuze te maken, en kan de vraag naar veilige producten stimuleren.[1] Standaarden en certificering kunnen ook worden gebruikt om een vermoeden van overeenstemming met wettelijke eisen aan te tonen (zie onderdeel 3.7).

Nederland zet in op het zo veel mogelijk harmoniseren van de verschillende standaardisatie- en certificerings-initiatieven. Er lopen nu namelijk veel initiatieven[2] waardoor bedrijven niet weten welke standaarden ze moeten gebruiken, en afnemers niet weten wat het gebruik van een standaard of certificaat inhoudt. Hierdoor neemt de effectiviteit van standaarden en certificering af. Ook leidt de versnippering van initiatieven ertoe dat partijen veel kosten moeten maken en tijd kwijt zijn aan hun standaardisatie. Vooral het MKB ondervindt hier hinder van: zij hebben vaak weinig middelen om standaarden te implementeren, en zijn (mede daardoor) vaak afhankelijk van de (uiteenlopende) eisen van dominante afnemers.

Om de beschikbaarheid en adoptiegraad van standaarden die bijdragen aan de digitale veiligheid te bevorderen, draagt Nederland actief bij aan standaarden en certificering die (Europees) breed worden geaccepteerd. Hierdoor wordt versnippering en verstoring van het level playing field tegengegaan. Door wederzijdse erkenning van standaarden en certificaten kunnen ook transactiekosten dalen, met als gevolg een betere betaalbaarheid van digitaal veilige IoT-apparaten.

Acties

» 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. Op korte termijn dringt het kabinet aan op het vaststellen van verplichte certificering voor specifieke productgroepen, d.w.z. voor producten waarvan het risico het grootst is of waarmee in de praktijk veel problemen zijn. Op de langere termijn moet door geleidelijke uitbreiding een verplichte certificering of het voldoen aan een CE-markering voor alle met internet verbonden

1 CPB Policy Brief 2018/1, Knelpunten op de markt voor cyberveiligheid.
2 O.a. TNO-onderzoek (2017).

EU Raamwerk Beveiligingscertificering ICT-producten en -diensten

Met het voorstel voor een Cybersecurity Act wil de Europese Commissie een geharmoniseerd kader tot stand brengen voor de cyberbeveiligingscertificering van ICT-producten en -diensten. Het ontbreken van wederzijds erkende standaarden en certificatiesystemen vormt een barrière voor een Europese markt voor cybersecurityproducten en –diensten en leidt tot te kleine schaal voor aanbieders en te weinig keuze en onzekerheid voor afnemers. Dat verandert als producten en diensten worden gecertificeerd volgens een Europees certificeringsschema dat aangeeft dat ze, op een omschreven beveiligingsniveau, weerbaar zijn tegen aantastingen van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van data of de aangeboden functionaliteiten en diensten. Met de Europese Cybersecurity Act wordt op Europees niveau de versnippering aangepakt en harmonisatie en wederzijdse erkenning van cybersecurity certificaten nagestreefd. Op het moment dat een Europees certificeringsschema wordt vastgesteld voor een product of dienst, vervallen de nationale overheidsschema's en mogen lidstaten daarvoor geen eigen certificering meer ontwikkelen.

Partnering Trust

Het doel van Partnering Trust is uniformering van de eisen aan (online) ICT-diensten, zodat aanbieders de veiligheid en betrouwbaarheid van hun aanbod helder kunnen specificeren en op uniforme wijze bewijs kunnen leveren van de kwaliteit van diensten (bijvoorbeeld voor audits en certificeringen). De partners Trusted-Cloud (in Duitsland), Labelcloud (in Frankrijk) en Zeker-Online (in Nederland) richten zich op online diensten, inclusief clouddiensten. Clouddiensten zijn essentieel voor de ondersteuning van nieuwe digitale diensten omdat ze voorzien in de benodigde gegevensopslag en computercapaciteit. Daarom heeft de Europese Commissie in haar mededeling over normalisatiepraktijken ook clouddiensten aangewezen als prioriteit. Binnen Partnering Trust werkt Nederland in samenwerking met o.a. Duitsland, Frankrijk en EC aan een goed werkbare invulling van deze prioriteit.

Secure Software Alliance

Deze alliantie beoogt het SSF-raamwerk (secure software framework) voor 'secure software development' verder te ontwikkelen en de kwaliteit ervan te borgen. In de kern gaat het om het zo vroeg mogelijk veilig maken van softwareproducten, door in elke fase van de productlevenscyclus de mogelijke kwetsbaarheden af te dekken. Daarnaast streeft de alliantie ernaar om opdrachtgevers/inkopers en opdrachtnemers van hard- en software dichter bij elkaar te brengen. Zeker bij maatwerk is de relatie tussen opdrachtgever en opdrachtnemer, en de onderlinge verantwoordelijkheidsverdeling, essentieel. Certificaten die toezien op proceskwaliteit zijn een belangrijk onderdeel daarvan. Met het SSD-raamwerk van CIP worden de opdrachtgever en de opdrachtnemer aangesproken waarbij uitgegaan wordt van een baseline normenkader dat de kwaliteit van het eindproduct borgt.

Smart Industry

Om de kansen van digitalisering voor de Nederlandse maakindustrie te benutten, is in 2018 het startschot gegeven voor het Standaardisatieplatform Smart Industry, als onderdeel van de bredere actieagenda standaardisatie Smart Industry.

producten gaan gelden (zie paragraaf 3.7 'Wettelijke eisen, toezicht en handhaving'). Dit zal het kabinet ook in de Europese Raad bepleiten.[3]

» Bevorderen standaarden/certificering: vooruitlopend op de CSA heeft Nederland op een aantal belangrijke terreinen het initiatief genomen tot het stimuleren van de toepassing van internationale standaarden en tot samenwerkingsverbanden en raamwerken, zoals Partnering Trust, Secure Software Alliance en het Standaardisatieplatform Smart Industry. Ten aanzien van reeds bestaande en mogelijk nieuwe initiatieven zal Nederland ter voorbereiding op de CSA actief de samenwerking met andere Europese landen opzoeken. Tevens wordt bezien hoe het toepassen van standaarden en certificering kan worden bevorderd door prikkels aan te brengen in de markt. Verzekeraars, maar ook het inkoopbeleid van de overheid, kunnen hier bijvoorbeeld een belangrijke rol spelen.
» Bundeling standaardisatie- en certificeringsinitiatieven: Nederland wil proactief op relevante Europese en mondiale standaardisatie- en certificatie-initiatieven aansluiten via het standaardisatieplatform NEN, dat een belangrijke rol kan spelen bij het stroomlijnen van de activiteiten vanuit Nederland in de diverse internationale standaardisatie-instellingen. Op die manier kan worden gezorgd dat Nederlandse belangen worden meegenomen en een breed draagvlak ontstaat voor internationale standaarden en certificatieschema's.
» Nederland gaat werk maken van multilaterale samenwerking rond IoT-standaardisatie, onder meer via het Global Forum on Cyber Expertise (GFCE). Mogelijke partners zijn landen uit de top 10 van de Global Competitiveness Index van het World Economic Forum, die toonaangevend zijn in de productie en 'early adoption' van hard- en software.

3.2 Monitor digitale veiligheid van producten

Zoals eerder aangegeven, is 100% digitale veiligheid niet realiseerbaar. Het kan altijd voorkomen dat een onveilig product op de markt komt, of dat een product tijdens de ontwikkelingsfase onveilig raakt of dat er voor dit product geen updates meer verschijnen. Zowel producenten, verkopers als gebruikers hebben belang bij transparantie over de kwaliteit en veiligheid van digitale producten. Een monitor met informatie over de veiligheid van digitale producten kan daarbij van groot belang zijn. Producenten kunnen bij geconstateerde kwetsbaarheden hun producten aanpassen, en er bij evidente onveiligheid voor kiezen het product eventueel van de markt halen. De informatie helpt hen bovendien om veilige producten te blijven ontwikkelen. Verkopers kunnen besluiten een product uit de schappen te nemen, en gebruikers kunnen besluiten voor hun veiligheid het product te (laten) patchen of af te schakelen.

Het is wenselijk daarbij zoveel mogelijk internationaal te opereren, gezien het bij uitstek internationale karakter van de markt voor digitale producten. Welke informatie relevant is en welke informatie voor wie beschikbaar moet komen voor deze monitor is onderwerp van verder onderzoek. Dit onderzoek betrekt ook internationale ervaringen met monitors.

Acties:

» Het kabinet gaat met publieke en private partijen een monitor met informatie over de digitale veiligheid van digitale producten ontwikkelen, met specifieke aandacht voor IoT-apparaten. Hierbij betrekt het kabinet internationale ervaringen.

3.3 Opschonen besmette producten bij gebruikers

Aanbieders van internettoegang kunnen een belangrijke rol spelen bij het terugdringen van digitale kwetsbaarheden. Vanuit hun beheerstaak voor de internetverbinding kunnen zij gebruikers er op attenderen dat onveilige apparaten op het internet zijn gesignaleerd. Dit kan bijdragen aan de digitale veiligheid tijdens de gebruiks- en afvoerfase van de productlevenscyclus.

Abuse Hub

De vereniging Abuse Information Exchange beheert een centrum (Abuse Hub) dat hun leden voorziet van reguliere rapporten over de met botnetmalware besmette computers bij hun eindgebruikers. De leden bestrijken meer dan 90% van de vaste breedbandinternetaansluitingen in Nederland; daar bevindt zich vermoedelijk ook het overgrote deel van de in huis of kleinzakelijke omgeving gebruikte IoT-apparaten. Abuse Hub heeft haar meerwaarde bewezen: het aandeel van besmette computers van de bij Abuse Hub aangesloten aanbieders is van 80% in 2010 gedaald tot 60% in 2016. Bij uitbreiding van de rapportage naar besmette IoT-apparaten zou een grote slag gemaakt kunnen worden. Abuse Information Exchange onderzoekt momenteel de haalbaarheid van de uitbreiding van de scope naar IoT-apparaten.

3 Deze actie geeft invulling aan de overgenomen motie van het lid Paternotte c.s. om in de Europese raaad te pleiten voor verplichte certificering van op internet aangesloten apparaten (Kamerstuk 21501-30, nr. 422).

In dialoog met aanbieders van internettoegang en de vereniging Abuse Information Exchange wordt bekeken hoe zij kunnen helpen om onveilige IoT-apparaten op het internet in te dammen. Daarbij wordt onderzocht of en hoe zij bij geconstateerde kwetsbaarheden of compromittering van een apparaat hun abonnees hierop kunnen wijzen en kunnen adviseren wat daaraan gedaan moet of kan worden. Dit kan een belangrijke bijdrage leveren aan het bestrijden van onveilige apparaten.

Acties:

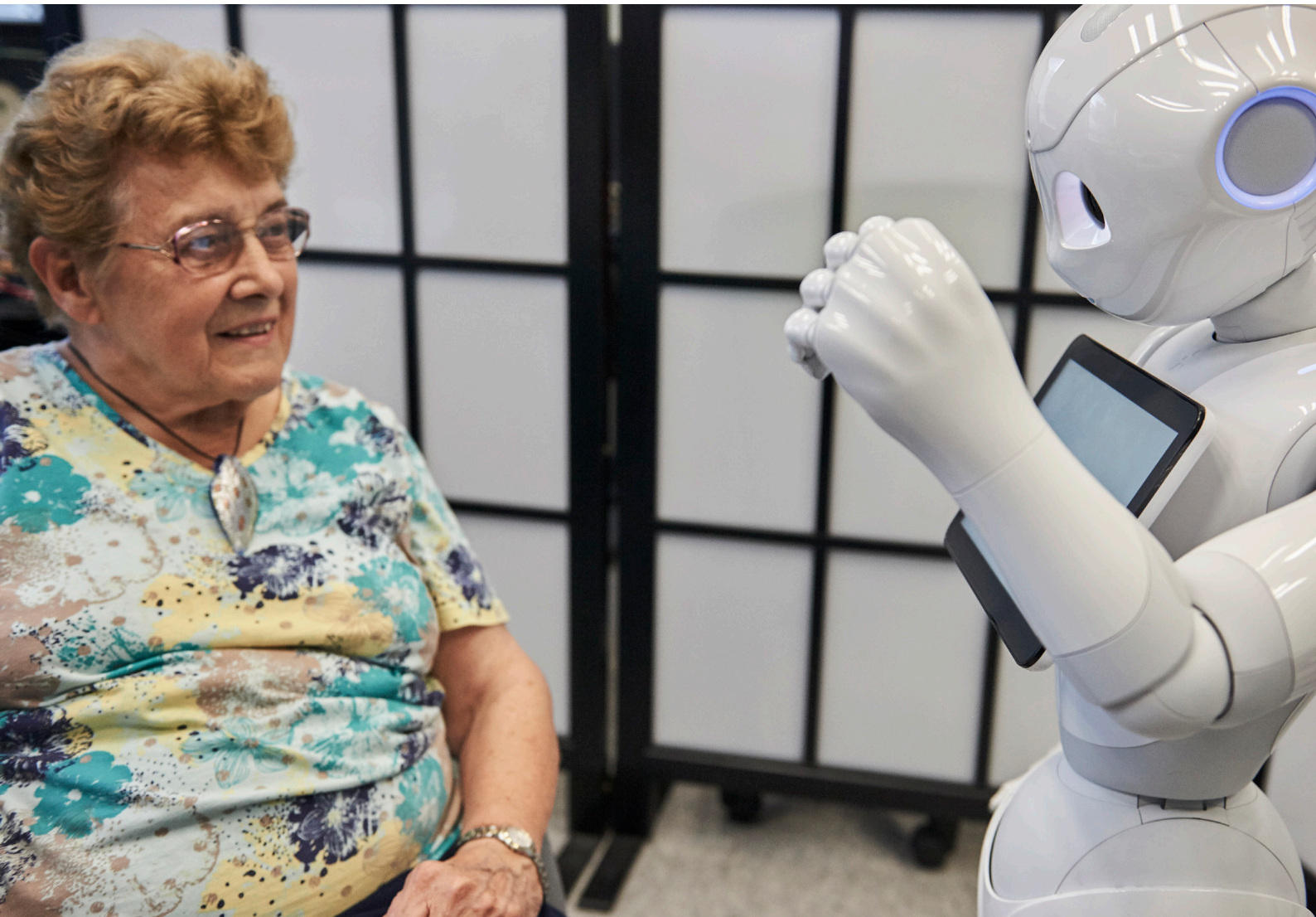
» Het kabinet gaat in gesprek met de aanbieders van internettoegang over hoe zij – analoog aan de succesvolle aanpak van botnets - gaan bijdragen aan de bestrijding van onveilige IoT-apparaten.

3.4 Testen op digitale veiligheid

Het testen van producten is cruciaal 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. Er zijn veel methoden om producten, diensten en systemen te testen op digitale veiligheid zoals cybersecurity scans, red-team-tests, pen(etratie)testen en ethische hacks (ten behoeve van responsible disclosure of coordinated vulnerability disclosure). Er ontstaat een cybersecurity-markt om tegemoet te komen aan de groeiende vraag naar testen, met een brede en gedifferentieerde vraag- en aanbodzijde. Die markt is ook dynamisch: cybercriminelen verzinnen steeds nieuwe manieren om producten en systemen aan te vallen en aanbieders moeten daarop anticiperen en reageren. De overheid wil samen met TNO en bedrijven in een pilot ervaring en kennis opdoen over de toegevoegde waarde van een gedeeld testplatform voor organisaties bij het testen van laagdrempeliger delen van de keten, of de gehele keten waar hun product deel van uitmaakt, en het uitwisselen van de opgedane kennis.

Acties:

» 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.



Cross Sector Cyber Testbed

Testen kan mogelijk laagdrempeliger worden en kennisuitwisseling effectiever als (onderdelen van) een testplatform kan worden gedeeld over meerdere sectoren heen (een 'Cross Sector Cyber Testbed' (CSCT)). Zo'n testbed moet bedrijven de mogelijkheid bieden om delen van de keten, of de gehele keten waar hun product deel van uitmaakt, te testen. Hierbij zijn meerdere partijen uit de betreffende keten betrokken. De mogelijkheid om 'over de keten' te testen is uniek en kan een belangrijke meerwaarde vormen voor aanbieders en gebruikers van ICT-producten en -diensten. De opgedane testinzichten zijn belangrijk voor al die partijen die zich bezighouden met het onderhouden van het gewenste digitale veiligheidsbeschermingsniveau. Ook kunnen deze inzichten dienen als input voor bestaande en nieuw te ontwikkelen standaarden en normen. Daarnaast bestaan er kansen om een koppeling te maken met de onderwijswereld, waarbij de testfaciliteiten gebruikt kunnen worden in opleidings- en onderzoeksprogramma's. Hiermee wordt niet alleen kennis opgebouwd, geborgd en gedisseminneerd, maar vindt ook een continu leren van elkaar plaats. Bovendien wordt bezien wat samenwerking met bestaande (internationale) testplatformen kan opleveren.

3.5 Cybersecurity-onderzoek

Het ontwikkelen en marktrijp maken van innovatieve oplossingen kan 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 (al dan niet technologische) oplossingen, maar ook om de onderzoek ten behoeve van gedragsbeïnvloeding (met name bij gebruikers) en om intensievere samenwerking ter versterking van de gehele kennisbasis

De ministeries van Onderwijs, Cultuur en Wetenschap, Justitie en Veiligheid, Defensie, en Economische Zaken en Klimaat gaan een sterkere regie voeren op de cybersecurity-kennisbasis.[4] Aanleiding is enerzijds de groeiende afhankelijkheid van buitenlandse leveranciers van cybersecurityproducten en -diensten en anderzijds een groeiende behoefte aan kennis en kunde op het gebied van digitale veiligheid. Cybersecurity en daarbinnen de ontwikkeling van de kennisbasis voor digitaal veilige hard- en software is één van de thema's die worden opgenomen in het programma Maatschappelijke Uitdaging Veilige Samenleving.[5] Daarbij gaat het om onderzoek naar veilige en betrouwbare systemen (inclusief vitale infrastructuren en communicatie); het beheer en de verdediging van systemen en (vitale) infrastructuren; het digitaal bewust en vaardig maken van burgers en organisaties; socio-economische factoren en ethiek van cybersecurity; privacy, identiteit en zeggenschap; en openbaar bestuur en rechtshandhaving.

Nederland zet daarnaast in op het ontwikkelen van cybersecurity-onderzoek en op de toepassing van het Small Business Innovation Research (SBIR) instrument, voor onderzoek dat bijdraagt aan nieuwe innovatieve, digitaal veilige hard- en software, en positieve externe effecten als kennisspilovers.

Ook stimuleert Nederland de ontwikkeling van encryptiesoftware die bijdraagt aan de digitale veiligheid van hard- en software. In bovengenoemde NCSRA III wordt een bedrag van € 410.000 extra vrijgemaakt om onderzoeksinitiatieven en projecten op het gebied van cybersecurity te stimuleren en encryptie daar als belangrijk onderwerp in terug te laten komen.

Om tot nieuwe innovatie oplossingen te komen voor de fase van afvoer van hard- en software gaat het kabinet dialoogsessies organiseren met betrokken partijen. Uit onderzoek blijkt dat instrumenten voor deze fase onderbelicht zijn. Het ontwikkelen van instrumenten voor deze fase biedt kansen voor aanbieders, gebruikers en de gehele samenleving. Denk bijvoorbeeld aan nieuwe businessmodellen als software-as-a-service. Hierbij kopen gebruikers geen product, maar betalen zij voor het gebruik daarvan. Dat biedt zowel aanbieder als gebruikers een aantal voordelen, waaronder een duidelijker belegde verantwoordelijkheid. De aanbieder heeft de zorg voor installatie, onderhoud, beheer, tijdige automatische updates en upgrades op afstand, en back-ups. Daarnaast draagt dit businessmodel bij aan een duurzaam gebruik van producten, en daarmee aan een duurzame samenleving.

4 Vergaderjaar 2017–2018 Aanhangsel van de Handelingen, 664.

5 Zie de maatschappelijke uitdaging veilige samenleving in Kennis- en Innovatieagenda 2018-2021; Maatschappelijke uitdagingen en Sleuteltechnologieën. https://www.topsectoren.nl/publicaties/publicaties/rapporten-2017/december/11-12-17/kia-2018-2021.

Nationale Cybersecurity Research Agenda III (NCSRA III)

Momenteel is de derde Nationale Cybersecurity Research Agenda (NCSRA III) in ontwikkeling. De NCSRA III biedt een kader voor het brede en multidisciplinaire cybersecurity onderzoek. In de uitvoering van die agenda is het doel om de onderzoeksinspanningen op het gebied van Cybersecurity in zowel de publieke als de private sector op elkaar af te stemmen. Een van de vijf pijlers van de agenda is 'beter ontwerp', waaronder alle activiteiten in de softwareontwikkeling in de fase voor ingebruikname worden verstaan.

Small Business Innovation Research (SBIR)

SBIR benut de creativiteit van ondernemers om maatschappelijke problemen op te lossen en daagt ondernemers uit om nieuwe producten te ontwikkelen en op de markt te brengen. De SBIR werkt in de vorm van een getrapte innovatiecompetitie, waarbij de ondernemingen met de beste offertes de opdracht krijgen voor een haalbaarheidsonderzoek. De ondernemingen met de meest kansrijke haalbaarheidsonderzoeken krijgen de opdracht om hun product verder te ontwikkelen; eerst in een proeftuin of pilot, vervolgens krijgen de oplossingen een goede kans in overheidsaanbestedingen.

Acties:

- Dcypher komt in Q2 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.
- Er lopen momenteel verschillende tenders in de research and development fase van de SBIR Cybersecurity. Deze projecten hebben beveiliging van IoT hard- en software tot doel en worden halverwege 2019 afgerond.
- Het kabinet stimuleert open source encryptie door extra middelen hiervoor vrij te maken in het kader van de NCSRA III.
- Het kabinet gaat dialoogsessies organiseren over innovatie oplossingen voor de fase van afvoer van hard- en software.

3.6 Aansprakelijkheid

Het aansprakelijkheidsrecht geeft niet alleen gebruikers handvatten om schade door digitale onveiligheid te verhalen, maar ook aanbieders prikkels 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.

Het kabinet bespreekt het aansprakelijkheidsregime met stakeholders en wetenschappers en vraagt hen mee te denken over het optimaliseren van de preventieve werking van het aansprakelijkheidsrecht. Daarbij staat de vraag centraal waar partijen in de praktijk mee te maken hebben. Welke schade wordt nu door welke partij geleden vanwege onveilige hard- en software? Zijn bedrijven en consumenten bekend met de mogelijkheden die het bestaande aansprakelijkheidsrecht, onder meer betreffende productaansprakelijkheid, biedt om schade te verhalen? Waar lopen zij mogelijk tegenaan als zij hun schade proberen te verhalen?

In de tot nu toe gevoerde gesprekken komt onder meer naar voren dat het aansprakelijkheidsrecht op zichzelf voldoende mogelijkheden lijkt te bieden om schade te verhalen. Wel is - volgens deze gesprekken - verbetering mogelijk door het nader definiëren van de begrippen 'fout' of 'gebrek': het is niet altijd duidelijk wanneer gezegd kan worden dat er een fout zit in software c.q. wanneer software gebrekkig is. En dus is niet altijd snel duidelijk of de aanbieder aansprakelijk is voor de fout of het gebrek. Dit kan buiten het aansprakelijkheidsrecht om, door het formuleren van product- en minimumeisen, die verduidelijken wanneer sprake is van een fout of gebrek in de software. Als software niet aan deze eisen voldoet, is het makkelijker om aan te tonen dat de software gebrekkig is en om de schade te verhalen (zie ook paragraaf 3.7). Sommigen verwachten dat de effectiviteit van deze eisen groter is dan van het uitbreiden van het aansprakelijkheidsrecht. Dat komt ook doordat negatieve externe effecten beter worden tegengegaan via product- en

Europese ontwikkelingen aansprakelijkheid

Digitaal veilige hard- en software is bij uitstek een grensoverschrijdend onderwerp. De Europese Commissie heeft in 2017 de EU-richtlijn over productaansprakelijkheid geëvalueerd. Naar verwachting stelt de Commissie in april 2018 de uitkomsten vast. Deze uitkomsten vormen een goede aanleiding om ook in EU-verband van gedachten te wisselen over de vraag of, en zo ja hoe, de regeling van productaansprakelijkheid aangepast zou moeten met het oog op technologieën zoals IoT-apparaten en software. In dit licht is van belang dat Nederland zal deelnemen aan de expertgroep van de Europese Commissie over aansprakelijkheid en nieuwe technologieën. Ook de richtlijn productaansprakelijkheid komt daarbij aan bod. In tot op heden gevoerde gesprekken op nationaal niveau en in de literatuur is al gesuggereerd om de regeling van productaansprakelijkheid ook op software toe te passen. Ook is hierin geopperd het schadebegrip uit te breiden met zogenoemde zuivere vermogensschade (nu is het schadebegrip bij productaansprakelijkheid kort gezegd beperkt tot schade door dood of letsel). Dit betrekt het kabinet bij de beoordeling van de uitkomsten van genoemde evaluatie en de deelname aan de expertgroep.

De volgende ontwikkeling is van belang voor de aansprakelijkheid van verkopers van digitale inhoud en digitale diensten (bijv. software, e-books, films, muziekstreaming) richting consumenten. Op dit moment wordt onderhandeld over een EU-richtlijnvoorstel 'betreffende bepaalde aspecten met betrekking tot de contracten voor de levering van digitale inhoud'. Dat regelt de rechten voor de koper en de verkoper, zoals contractuele eisen aan de te leveren digitale inhoud en rechtsmiddelen voor de consument als de verkoper de overeenkomst niet nakomt. Het voorstel waar de lidstaten onderling overeenstemming over hebben bereikt verplicht de verkoper – kort gezegd – om beveiligingsupdates te verstrekken. Deze verplichting geldt alleen niet als de consument er uitdrukkelijk op is gewezen dat geen updates worden verstrekt en hij hiermee uitdrukkelijk heeft ingestemd. Een vermelding in de algemene voorwaarden, bijvoorbeeld, volstaat dus niet. Nederland wil consumenten verdergaand verzekeren van beveiligingsupdates. Met deze updates is niet alleen de individuele consument gebaat, maar ook de maatschappij als geheel. Onveilige hard- of software bij één of meerdere consumenten, kan namelijk grote schade bij derden aanrichten. Daarom heeft Nederland in de onderhandelingen over het EU-richtlijnvoorstel voorgesteld om in alle gevallen veiligheidsupdates te verplichten. Voor dit voorstel probeert Nederland op dit moment steun te vergaren in Brussel. De onderhandelingen tussen de Raad en het Europees Parlement lopen nog.

minimumeisen: software die niet aan de eisen voldoet, komt de markt niet op. Daarmee wordt niet alleen schade bij individuele consumenten en bedrijven voorkomen, maar ook maatschappelijke schade die bijvoorbeeld door DDoS-aanvallen wordt veroorzaakt.

Acties:

- 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. Op basis hiervan stelt het kabinet samen met publieke en private partijen mogelijke vervolgstappen vast.
- Nederland neemt actief deel aan de expertgroep over aansprakelijkheid en nieuwe technologieën en betrekt daarbij de inbreng van Nederlandse stakeholders.
- 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.

3.7 Wettelijke eisen, toezicht en handhaving

Met het stellen van minimumveiligheidseisen kunnen onveilige producten van de markt geweerd worden. Op initiatief van Nederland wordt in EU-verband momenteel gekeken of het mogelijk is om via de richtlijn voor radiorandapparatuur (Radio Equipment Directive, hierna 'RED') voor apparaten die draadloos verbonden zijn met het internet – een significant en groeiend deel van het IoT – minimale digitale veiligheidseisen te stellen. Producten die niet aan deze eisen voldoen worden dan van de markt gehaald.

Toezicht en handhaving geven aanbieders een prikkel om zich aan wet- en regelgeving te houden. Afhankelijk van zijn mandaat kan de toezichthoudende instantie ingrijpen in bepaalde fasen van de productlevenscyclus. Om de handhaving te versterken gaat het kabinet (internationale) samenwerking tussen de verschillende toezichthoudende instanties stimuleren. Er zijn diverse toezichthoudende instanties met een deelverantwoordelijkheid voor de handhaving van de digitale veiligheid van hard- en software. Zo houdt de Autoriteit Consument en Markt toezicht op

een belangrijk deel van de consumentenbescherming en de Autoriteit Persoonsgegevens op privacyregelgeving. Daarnaast zijn er toezichthoudende instanties voor specifieke sectoren als de gezondheidszorg, vervoer en energie. Zij hebben vaak weer internationale counterparts.

Acties:

- Het kabinet onderzoekt welke minimale veiligheids-eisen kunnen worden gesteld aan apparaten via de Europese Radio Equipment Directive.
- 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.

3.8 Bewustwordingscampagnes en empowerment

Bewustwordingscampagnes en het stimuleren van empowerment kunnen gedurende de gehele productlevenscyclus ingezet worden. Zo kunnen ontwerpers bewuster worden gemaakt van het belang om security-by-design toe te passen, kunnen afnemers worden geattendeerd op (on)betrouwbare apparaten, en kunnen gebruikers gestimuleerd worden om hun producten digitaal veilig te houden.

Nederland zal bewustwordingscampagnes en empowerment op het gebied van digitaal veilige hard- en software vooral inzetten om de impact te vergroten van bestaande en nieuwe maatregelen. Doel van de bewustwordingscam-pagnes is vooral om consumenten en het MKB bewust te maken van de digitale veiligheidsrisico's van IoT-apparaten,

Radio Equipment Directive (RED)

De RED schrijft de eisen voor waar apparatuur aan moet voldoen om het Europese keurmerk CE te mogen dragen. Agentschap Telecom is hier toezichthouder op. De voorschriften gaan tot dusver over zaken als gebruiksveiligheid, voorkómen van interferentie en storingsgevoeligheid. De RED biedt echter ook een haakje om (na activering) minimaal veiligheidseisen te stellen aan de digitale veiligheid van apparaten die onder de RED vallen. Europees geharmoniseerde standaarden en certificering (paragraaf 3.1. van deze roadmap) kunnen ondersteuning bieden bij het voldoen aan deze wettelijke eisen.

van wat ze daar aan kunnen doen en welke overheidsmaatregelen hen daarbij helpen. Daarbij zullen inzichten uit de gedragswetenschappen en gedragsexperimenten worden ingezet om te zorgen dat de gebruikers ook weten wat ze moeten doen (welke handelingsperspectieven ze hebben) voor de juiste aankoopbeslissing en het juiste gebruik van hard- en software.

De campagnes sluiten aan op het digitale platform voor cybersecurity-informatie veiliginternetten.nl, dat ook voor andere cybersecuritycampagnes wordt ingezet. Ook wil Nederland de bewustwording en empowerment gedurende de ontwikkelingsfase van een product stuwen. Aanbieders kunnen dit binnen de eigen organisatie oppakken, en grote bedrijven kunnen kleine bedrijven daarbij helpen. Ook kunnen cyberessentials[6] bijdragen aan de digitale veiligheid van het eigen bedrijf.

Acties:

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

6 Cyber essentials zijn security richtlijnen die bedrijven helpen hun basis op orde te krijgen. Het Digital Trust Center i.o. zal er via haar digitale platform informatie en advies over verschaffen.

3.9 Inkoopbeleid van de Rijksoverheid

Het inkoopbeleid van de Rijksoverheid kan de digitale veiligheid van de gehele productlevenscyclus bevorderen. Door criteria hierover 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.

De Rijksoverheid kan met haar inkoopbeleid de vraagzijde van digitaal veilige producten stuwen. Zij is namelijk een belangrijke gebruiker. Hierdoor ontstaat een prikkel voor aanbieders om digitaal veilige producten op de markt te brengen. Ook geeft de Rijksoverheid hiermee het goede voorbeeld: kijk naar de digitale veiligheid van hard- en software voordat je die koopt. Daarnaast is het voor de Rijksoverheid uiteraard belangrijk dat zij met vertrouwen gebruik kan maken van de door haar ingekochte hard- en software. Het kabinet wil daarom verkennen welke aanvullende maatregelen nodig zijn op terrein.

Acties:

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

Dit rapport is een uitgave van:

Ministerie van Economische Zaken en Klimaat
Postbus 20401 | 2500 EK Den Haag

Ministerie van Justitie en Veiligheid
Postbus 20301 | 2500 EH Den Haag

www.rijksoverheid.nl

April 2018