Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Ons kenmerk
DGBI-DE / 19122822

Datum 20 juni 2019
Betreft Voortgang Roadmap Digitaal Veilige Hard- en Software

Geachte Voorzitter,

In een steeds meer verbonden samenleving is de digitale veiligheid van essentieel belang voor het vertrouwen in de digitale economie. De opkomst en ontwikkeling van het *Internet of Things* (IoT) leidt wereldwijd tot een versnelling van de digitalisering voor bedrijven en consumenten. Juist omdat de digitale wereld en de fysieke wereld steeds meer verweven raken, zijn de mogelijke gevolgen van digitale kwetsbaarheden ingrijpend. Het is belangrijk dat ICT-producten en -diensten digitaal veilig zijn: iedereen moet ze veilig en vertrouwd kunnen gebruiken. De digitale veiligheid van ICT-producten en -diensten komt niet vanzelf tot stand. Het kabinet heeft hiervoor met publieke en private partijen in 2018 de Roadmap Digitaal Veilige Hard- en Software (hierna: de roadmap) opgesteld. De roadmap is onderdeel van de Nederlandse Cyber Security Agenda (NCSA)[1].

In deze brief informeer ik u over de voortgang van de implementatie van de roadmap en de inzet voor de komende periode. Een schematisch overzicht is opgenomen in de bijlage. De maatregelen in de roadmap zijn in de eerste plaats erop gericht om de markt zo te prikkelen dat het algehele niveau van digitale veiligheid van hard- en software en IoT wordt verhoogd. Het afgelopen jaar zijn belangrijke stappen gezet en veel zaken zijn nog in wording. Wel is al duidelijk dat door de inzet van veel partijen op veel fronten de koers is ingezet naar grotere digitale veiligheid van hard- en software en IoT.

Wettelijke eisen, toezicht en aansprakelijkheid

Met het stellen van wettelijke minimum digitale veiligheidseisen kunnen onveilige IoT-apparaten van de markt worden gehaald en geweerd. Toezicht en handhaving geven aanbieders een prikkel om zich aan wet- en regelgeving te houden. Met een beroep op het aansprakelijkheidsrecht kunnen burgers en bedrijven schade door digitale onveiligheid verhalen. Dat biedt een financiële prikkel voor aanbieders om ICT-producten en -diensten veilig te houden.

Minimum digitale veiligheidseisen: de Radio Equipment Directive

Nederland maakt zich in de EU sterk voor het stellen van wettelijke minimum digitale veiligheidseisen aan IoT-apparaten via de Europese richtlijn voor radioapparatuur (de *Radio Equipment Directive*, RED). Op termijn gaan die gelden

[1] Over de voortgang van de NCSA u bent geïnformeerd door de minister van Justitie en Veiligheid op 12 juni jl.

voor alle IoT-apparaten in de Europese markt. Producten die niet aan de minimumeisen voldoen, kunnen dan van de markt worden geweerd en gehaald. Het Agentschap Telecom (AT) houdt hier in Nederland toezicht op. Op initiatief van Nederland wordt momenteel in EU-verband gekeken naar de invulling van de eisen. De Europese Commissie zal in 2019 een impact assessment uitvoeren. Nederland zal de komende periode een aanjagende rol blijven vervullen om ervoor te zorgen dat de minimum digitale veiligheidseisen in 2020 van kracht worden.

Veiligheidsupdates in het consumentenrecht
Op 15 april heeft de Europese Raad de richtlijn over overeenkomsten voor de levering van digitale inhoud en diensten (richtlijn digitale inhoud) en de richtlijn over overeenkomsten voor de verkoop van goederen (richtlijn verkoop van goederen) aangenomen. Ze introduceren nieuwe regels die de aan- en verkoop van goederen en digitale inhoud over de grenzen heen veiliger en gemakkelijker maken. Tijdens de onderhandelingen is gepleit voor maximumharmonisatie van de richtlijn verkoop van goederen, zodat in Europa overal dezelfde garantieregels gelden; deze inzet is conform de motie Van den Berg/Van der Lee[2]. Hiervoor was in de Europese Raad echter weinig steun. Resultaat van de onderhandelingen over de garantietermijn is dat de lidstaten een termijn van minimaal twee jaar moeten hanteren in hun nationale recht (minimumharmonisatie). Wat betreft cybersecurity is een verplicht updateregime voor digitale inhoud en tastbare goederen met een digitaal element onderdeel van beide richtlijnen. Consumenten hebben hiermee recht op (veiligheids-)updates zolang zij die redelijkerwijs mogen verwachten. Dit betekent dat in heel Europa een uniform beleid gaat gelden voor veiligheidsupdates bij consumentenaankopen. Deze norm gaat in de praktijk ingevuld worden.

Toezicht
Ik ben in gesprek met de Autoriteit Consument en Markt (ACM), de Autoriteit Persoonsgegevens (AP), de Nederlandse Voedsel- en Warenautoriteit (NVWA) en AT over hun rol bij het bevorderen van de digitale veiligheid van IoT-apparaten. Daarbij is vooral gesproken over de vraag of de toezichthouders de juiste bevoegdheden hebben om, in combinatie met het aangekondigde beleid, effectief op te treden. Het voorlopige beeld is dat de AP en de NVWA hiertoe voldoende bevoegdheden hebben. ACM en het AT zijn in afwachting van bevoegdheden die aan hen worden toegekend via de richtlijnen digitale inhoud en verkoop van goederen (ACM) en de RED (AT). Ik zet het gesprek met de toezichthouders voort om gezamenlijk naar synergie te blijven zoeken en aandacht te houden voor de digitale veiligheid van IoT-apparaten.

Aansprakelijkheid
In EU-verband wordt gesproken over het aansprakelijkheidsrecht in het licht van nieuwe technologieën. Nederland neemt deel aan een expertgroep over de richtlijn productaansprakelijkheid (85/374/EEG). De expertgroep is ingesteld door de Europese Commissie. Hieraan nemen lidstaten, private vertegenwoordigers en wetenschappers deel. De Europese Commissie verwacht voor de zomer met richtsnoeren te komen over de toepassing van de richtlijn

[2] Kamerstuk 21501-30, nr. 430

productaansprakelijkheid, als er sprake is van nieuwe technologieën. Hierin zal aandacht zijn voor software als onderdeel van een product. Aan de hand van de richtsnoeren van de Europese Commissie kan worden bezien welke vervolgstappen wenselijk zijn.

Standaarden en certificering
De digitale veiligheid van ICT-producten en -diensten (inclusief IoT) gedurende de hele productlevenscyclus kan verbeterd worden met veiligheidsstandaarden. Met certificering kan een ICT-leverancier duidelijk maken dat hij aan die standaarden voldoet. Deze transparantie in de markt stimuleert de vraag naar veilige ICT-producten en -diensten. Nederland maakt zich sterk voor effectieve standaarden. In de EU zet Nederland in op de bundeling en harmonisatie van bestaande initiatieven en voor de ontwikkeling van cybersecurity-certificering.

Cybersecurity-certificering in de EU: de Cyber Security Act
Eind 2018 hebben de Europese Raad en het Europees Parlement een akkoord bereikt over de Europese *Cyber security Act* (CSA). Deze verordening creëert een Europees stelsel van cybersecurity-certificering voor ICT-producten, -diensten en -processen. De verordening is op 7 juni jl. gepubliceerd. Er geldt een nationale implementatietermijn van twee jaar na publicatie voor het aanwijzen en inrichten van een nationale autoriteit die onder meer toezicht houdt op de naleving van de verordening. Na inwerkingtreding eind juni kan de Europese Commissie samen met de Lidstaten certificeringschema's voor ICT-producten, -diensten en -processen ontwikkelen. Certificering is voor ICT-leveranciers in de eerste instantie op basis van vrijwilligheid, maar de Europese Commissie zal voor eind 2023 aangeven welke schema's alsnog in de EU verplicht worden via aanvullende wetgeving. Nederland blijft, conform de motie Paternotte c.s.[3], pleiten voor verplichte cybersecurity certificering in de EU.

De ontwikkeling van Europese certificeringschema's zal naar verwachting dit jaar starten. Nederland zet zich de komende periode in op de voortvarende ontwikkeling en implementatie van cybersecurity-certificeringschema's, onder meer door Nederlandse initiatieven en expertise te koppelen aan Europese trajecten. Zo neemt Nederland actief deel aan een werkgroep gevormd door de Europese Commissie voor de ontwikkeling van een Europees cloud certificeringschema. Clouddiensten zijn een centraal element van ICT-producten en diensten. Samen met onder meer Duitsland en Oostenrijk heeft Nederland een aanbeveling opgesteld voor een Europees cloud certificatieschema met een reeks beveiligingsvereisten en de wijze waarop daarover verantwoording wordt afgelegd door een ICT-leverancier. Deze aanbeveling bouwt voort op het Nederlandse publiek-private raamwerk *Partnering Trust*[4] en het Duitse *Trusted Cloud*. Beide raamwerken zijn de afgelopen jaren in eigen land ontwikkeld en wederzijds erkend.

Standaardisatieorganisaties zoals het Nederlandse NEN en de Europese CEN/CENELEC spelen een belangrijke rol in de ontwikkeling van gedragen

[3] Kamerstuk 21501-30, nr. 422
[4] Met partners zoals NOREA, softwareleveranciers en de Belastingdienst is een gezamenlijk raamwerk ontwikkeld gericht op cybersecurity zekerheidsniveaus van ICT-producten en -diensten in de keten.

standaarden in de markt. Om een leidende rol te spelen in deze ontwikkelingen vervult Nederland de komende drie jaar het voorzitterschap en het secretariaat van de CEN/CENELEC werkgroep over digitale productveiligheid. De werkgroep is begin 2019 van start gegaan met onder meer een verkenning van IoT-standaarden. Dit om te bezien welke internationale standaarden, al dan niet na aanpassing, als Europese normen kunnen worden overgenomen en waar aanvullende Europese normen nodig zijn. Daarbij wordt ook gebruik gemaakt van Nederlandse kennis en expertise, zoals een handreiking voor de digitale veiligheid van IoT-apparaten ontwikkeld door het Centrum voor Informatiebeveiliging en Privacybescherming (CIP)[5]. Voor expertise buiten de EU zal via het *Global Forum on Cyber Expertise* (GFCE) de samenwerking worden gezocht met Singapore voor het uitwisselen van kennis en ervaringen.

Nationale ontwikkelingen
De ontwikkelingen in Nederland staan niet stil. In opdracht van mijn ministerie en het ministerie van Justitie en Veiligheid (JenV) ontwikkelt het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) in samenwerking met diverse private partijen 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.

Om de ontwikkeling van veilige software te stimuleren in de hele productlevenscyclus is het afgelopen jaar door de *Secure Software Alliance* (SSA) een kader gepubliceerd voor softwareontwikkelaars[6]. De komende periode zet de SSA in op pilots om de methodiek toe te passen bij bedrijven. Ook wordt de samenwerking gezocht met hogescholen en universiteiten om in ICT-opleidingen veilige softwareontwikkeling te stimuleren.

Inkoopbeleid van de overheid
De overheid kan met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en -diensten stimuleren. Zij is namelijk een belangrijke gebruiker. Door cybersecurity-criteria op te nemen in het inkoopbeleid moeten leveranciers van de overheid voldoen aan deze eisen. Hierdoor ontstaat een prikkel voor aanbieders om digitaal veilige producten en diensten op de markt te brengen. Ook geeft de overheid hiermee het goede voorbeeld. Zoals aangeven in de roadmap en in de brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (BZK) over het verhogen van informatieveiligheid bij de overheid[7], wordt onderzocht welke aanvullende cybersecurity inkoopeisen voor de overheid nodig zijn. Als onderdeel van het tweejarig ondersteuningsprogramma voor overheden van de implementatie van de Baseline Informatiebeveiliging Overheid (BIO) is begin dit jaar een expertgroep gestart om cybersecurity inkoopeisen te formuleren voor verschillende segmenten. Alle overheden (Rijk, provincies, gemeenten en waterschappen) dragen bij aan de inhoudelijke uitwerking van de betreffende inkoopsegmenten. Het eerste segment, veilige softwareontwikkeling, is voor de

[5] https://www.cip-overheid.nl/wp-content/uploads/2018/11/CIP-whitepaper-IoT-v1_0.pdf. CIP is een samenwerkingsverband van onder meer IBM, Philips, Centric, Lancom, DXC, Rijkswaterstaat, ECP en EZK.
[6] In oktober 2018 is het boek 'Agile Secure Software Lifecycle Management' gepubliceerd. SSA werkt samen met onder andere NOREA, ISACA ((inter)nationale beroepsvereniging van auditors) en PVIB (beroepsvereniging van informatiebeveiligers).
[7] Kamerstuk 26643, nr. 574

zomer gereed. Het gehele traject zal eind 2020 leiden tot een uitwerking van alle relevante ICT-inkoopsegmenten. De doelstelling is om deze cybersecurity inkoopeisen te gaan hanteren voor alle overheidslagen als onderdeel van BIO.

Cybersecurity onderzoek
Voor het veiliger maken van ICT-producten en -diensten is innovatie essentieel. Dcypher heeft in 2018 een nieuwe Nationale Cybersecurity Research Agenda (NCSRA III) gelanceerd. Deze agenda vormt een leidraad op het gebied van onderzoek en innovatie bij het realiseren van de ambities zoals beschreven in de NCSA. Er lopen momenteel verschillende tenders in de *research and development*-fase de SBIR cybersecurity. Een aantal van deze projecten heeft onder meer de beveiliging van hard- en software en IoT-apparaten tot doel en worden in 2019 afgerond. Het kabinet stimuleert open source encryptie met extra middelen in het kader van de NCSRA III. Het ministerie van JenV heeft hiervoor een bedrag van € 410.000 ter beschikking gesteld. Ook wordt via de Nationale Wetenschapsagenda ingezet op cybersecurity onderzoek. Zo is via de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO) een brede nationale cybersecurity onderzoeksoproep gepubliceerd van 5,5 miljoen euro, en wordt een oproep uitgewerkt in het kader van de Nationale Wetenschapsagenda (NWA) van 5,15 miljoen euro. Daarnaast is afgelopen jaar een verkenning gestart naar hoe de kennis en innovatie ambities van het kabinet zo goed mogelijk in publiek-private samenwerking kunnen worden vormgegeven. Ik ben daarover met vertegenwoordigers van uit de overheid, het cybersecurity bedrijfsleven en het kennisveld in gesprek. U zal hierover per brief nader over worden geïnformeerd. Tot slot wordt ook gewerkt aan een stevige verankering van cybersecurity binnen het missie gedreven innovatiebeleid.

Bewustwording
Gebruikers zijn zich vaak onvoldoende bewust van de risico's die ze lopen of ze overschatten hun veiligheid. Weten wat je kunt doen en laten zijn belangrijke bouwblokken voor burgers en (mkb-)bedrijven om hun eigen digitale veiligheid in handen te nemen. De overheid stimuleert bewustwording over cybersecurity en cybercrime door middel van campagnes. In 2019 wordt in samenwerking met het ministerie van JenV ingezet op het bieden van handelingsperspectieven gericht op gedragsverandering. Doordat de ministeries van JenV en Economische Zaken en Klimaat (EZK) hun campagnes in samenhang ontwikkelen wordt het gewenste effect vergroot. Daarbij wordt rekening gehouden met gedragswetenschappelijke inzichten. Eind mei is een grote publiekscampagne gestart met als thema *phishing*. Deze campagne maakt deel uit van de integrale aanpak cybercrime[8]. In oktober zal een vervolg aan deze campagne worden gegeven waarbij de focus zal liggen op de digitale veiligheid van IoT-apparaten zal liggen. In oktober zal eveneens de jaarlijkse Europese Cybersecurity Maand plaatsvinden waarin verschillende initiatieven zullen plaatsvinden, waaronder Alert Online.

Testen op digitale veiligheid

[8] Over de voortgang van de integrale aanpak cybercrime bent u geïnformeerd door mij en de minister van Justitie en Veiligheid op 12 juni jl.

Met de opmars van IoT is het van belang om inzicht te krijgen in het digitale veiligheidsniveau van producten die op de markt zijn. In dat kader heeft AT 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. De resultaten van het onderzoek worden binnenkort gepubliceerd. Daarnaast ontwikkelt en implementeert de Consumentenbond samen met een aantal internationale partnerorganisaties een testprogramma van verbonden apparaten. Het programma spitst zich toe op een aantal voor consumenten belangrijke aspecten rond digitale veiligheid en privacy. De eerste ervaringen worden nu opgedaan. Het is goed dat maatschappelijke organisaties dergelijke initiatieven nemen. Dit draagt bij aan transparantie in de markt rondom de digitale veiligheid van IoT-apparaten.

Monitor besmette IoT-apparaten en het opschonen van besmettingen bij gebruikers

Zoals ik eerder in de roadmap heb aangegeven, is honderd procent digitale veiligheid niet realiseerbaar. Het kan niet worden uitgesloten dat producten worden gecompromitteerd. Inzicht in gevallen van besmetting van IoT-apparaten stelt partijen in staat om maatregelen te treffen. Dit biedt fabrikanten bijvoorbeeld de mogelijkheid om een veiligheidsupdate uit te brengen. Verkopers kunnen overwegen om producten uit de schappen te nemen en gebruikers om producten te updaten of af te schakelen. Aanbieders van internettoegang kunnen een belangrijke rol spelen om consumenten te bereiken om maatregelen te nemen. Hiertoe is de afgelopen jaren een succesvolle werkwijze ontwikkeld door de vereniging *Abuse Information Exchange*[9]. Om aan het hierboven geschetste proces invulling te geven is een monitor voor besmette IoT-apparaten opgezet. Met subsidie van mijn ministerie zal de TU Delft de aankomende twee jaar metingen verrichten naar besmette IoT-apparaten in Nederland. Langs twee sporen wordt opvolging gegeven aan de resultaten. Het *Digital Trust Center* zal in gesprek gaan met fabrikanten en andere stakeholders over korte termijnmaatregelen die zij kunnen nemen om besmette apparaten veilig te maken. Door besmettingsinformatie over apparaten te delen met *Abuse Information Exchange* kunnen internetaanbieders hun klanten informeren zodat besmettingen worden opgeschoond. De monitor draagt met deze publiek-private werkwijze bij aan een schoner Nederlands internet en spreekt aanbieders aan op hun verantwoordelijkheid voor de digitale veiligheid van hun producten in aanloop naar Europese wettelijke maatregelen voor de langere termijn.

Tot slot

Het verhogen van de digitale veiligheid van hard- en software en IoT is een complex en grensoverschrijdend vraagstuk. Oplossingen voor de langere termijn vragen om een internationaal georiënteerde aanpak, in de eerste instantie in Europa. Het is van belang te bezien welke maatregelen Nederland alvast kan nemen en hoe we vanuit Nederlandse publieke en private expertise actief bijdragen aan internationale oplossingen voor de toekomst. Met het geheel aan maatregelen in de roadmap en de inzet van veel partijen zijn wij op de goede

[9] Een samenwerkingsverband van internetaanbieders

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Ons kenmerk
DGBI-DE / 19122822

weg. Ik blijf komend jaar inzetten op de realisatie van de maatregelen om het algehele niveau van digitale veiligheid in de markt van hard- en software en IoT te versterken.

Hoogachtend,

mr. drs. M.C.G. Keijzer
Staatssecretaris van Economische Zaken en Klimaat

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Ons kenmerk
DGBI-DE / 19122822

Bijlage: schematisch overzicht van Roadmap Digitaal Veilige Hard- en Software

Wettelijke eisen, toezicht en aansprakelijkheid	
Stand van zaken	Op initiatief van Nederland wordt momenteel in EU-verband gekeken naar de invulling van wettelijk minimum digitale veiligheidseisen voor IoT-apparaten onder de Radio Equipment Directive (RED). De Europese Commissie zal in 2019 een impact assessment uitvoeren.
	Op 15 april jl. heeft de Europese Raad de richtlijnen digitale inhoud en verkoop van goederen aangenomen. Consumenten krijgen hiermee recht op (veiligheids-)updates zolang zij die redelijkerwijs mogen verwachten.
	Dialoogsessies vinden plaats met toezichthouders AT, ACM, AP en NVWA over welke rol zij kunnen spelen op het gebied van IoT. AP en de NVWA hebben voldoende bevoegdheden. ACM en het AT zijn in afwachting van bevoegdheden via de richtlijnen digitale inhoud en verkoop van goederen (ACM) en de RED (AT).
Vooruitblik	Nederland zal de komende periode een aanjagende rol blijven vervullen om ervoor te zorgen dat de minimum digitale veiligheidseisen in 2020 van kracht worden onder de RED.
	Start van de implementatie van de richtlijnen digitale inhoud en verkoop van goederen.
	Voortzetting dialoogsessies met toezichthouders voor synergie.
	De Europese Commissie verwacht voor de zomer met richtsnoeren te komen over de toepassing van de richtlijn productaansprakelijkheid.

Standaarden en certificering	
Stand van zaken	De Europese *Cyber Security Act* is op 7 juni jl. gepubliceerd. Deze verordening creëert een Europees stelsel van cybersecuritycertificering voor ICT-producten, -diensten en -processen.
	Samen met onder meer Duitsland en Oostenrijk heeft Nederland een aanbeveling opgesteld voor een Europees cloud certificatieschema.
	Begin 2019 is onder Nederlands voorzitterschap en secretariaat een werkgroep gestart van CEN/CENELEC voor digitale productveiligheid.
	In opdracht van JenV en EZK ontwikkelt CCV 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.
	Door de Secure Software Alliance (SSA) is in 2018 een kader gepubliceerd voor veilige softwareontwikkeling.
	In 2018 is een handreiking voor de digitale veiligheid van IoT gepubliceerd door CIP waaraan onder meer IBM, Philips, Centric, Lancom, DXC, Rijkswaterstaat, ECP en EZK hebben bijgedragen.

Vooruitblik	De implementatie van de CSA zal starten. Er geldt een termijn van twee jaar voor het aanwijzen en inrichten van een nationale autoriteit die onder meer in Nederland toezicht gaat houden.
	De ontwikkeling van Europese certificeringschema's zal naar verwachting dit jaar starten. Nederland zet in op de voortvarende ontwikkeling en implementatie van cybersecurity certificeringschema's.
	De CEN/CENELEC werkgroep voor productveiligheid zal op basis van een verkenning van IoT-standaarden bezien welke Europese normen nodig zijn.
	SSA zet in op pilots voor veilige softwareontwikkeling bij bedrijven en samenwerking met kennisinstellingen om veilige softwareontwikkeling bij ICT-opleidingen te stimuleren.

Inkoopbeleid van de overheid

Stand van zaken	Begin 2019 is een expertgroep gestart om cybersecurity inkoopeisen te formuleren voor verschillende segmenten. Het eerste segment, veilige softwareontwikkeling, is voor de zomer gereed.
Vooruitblik	Het gehele traject zal eind 2020 leiden tot een uitwerking van alle relevante ICT-inkoopsegmenten. De doelstelling is om deze cybersecurity inkoopeisen te gaan hanteren voor alle overheidslagen als onderdeel van BIO.

Cybersecurity onderzoek

Stand van zaken	In 2018 is de derde Nationale Cybersecurity Research Agenda (NCSRA III) gepubliceerd.
	Er lopen verschillende tenders in de *research and development*-fase de SBIR cybersecurity.
	Het kabinet stimuleert open source encryptie met extra middelen in het kader van de NCSRA III. Het ministerie van JenV heeft hiervoor een bedrag van €410.000 ter beschikking gesteld.
	NWO heeft een brede nationale cybersecurity onderzoeksoproep gepubliceerd van 5,5 miljoen euro
	Er is verkenning gestart naar hoe de kennis en innovatie ambities van het kabinet zo goed mogelijk in publiek-private samenwerking kunnen worden vormgegeven.
Vooruitblik	In het kader van de Nationale Wetenschapsagenda (NWA) wordt een onderzoeksoproep uitgewerkt van 5,15 miljoen euro.
	Een stevige verankering van cybersecurity binnen het missie gedreven innovatiebeleid

Bewustwording

Stand van zaken	Bewustwordingscampagnes vinden plaats voor bedrijven en consumenten (JenV/EZK). Eind mei is een campagne gestart tegen *phishing*.

Vooruitblik	In oktober wordt een vervolg aan de campagne gegeven gericht op de digitale veiligheid van IoT-apparaten.

Testen op digitale veiligheid

Stand van zaken en vooruitblik	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. De resultaten van het onderzoek worden binnenkort gepubliceerd.
	De Consumentenbond ontwikkelt en implementeert samen met een aantal internationale partnerorganisaties een testprogramma van verbonden apparaten op digitale veiligheid en privacy.

Monitor besmette IoT-apparaten en het opschonen van besmettingen bij gebruikers

Stand van zaken en vooruitblik	Monitor besmette IoT-apparaten is opgezet in samenwerking met TU Delft, DTC en internetaanbieders via *Abuse Information Exchange*.