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

Datum 14 december 2020
Betreft Voortgang Roadmap Digitaal Veilige Hard- en Software

Ons kenmerk
DGBI-DE / 20289637

Geachte Voorzitter,

Met het ondernemen, werken en leren vanuit huis heeft COVID-19 laten zien hoe belangrijk digitalisering is voor onze samenleving en economie. Het belang neemt toe dat ICT-producten en diensten digitaal veilig zijn. Vanuit de Roadmap Digitaal Veilige Hard- en Software (DVHS) zet het kabinet een breed palet van maatregelen in om de prikkels in de markt verleggen in het complexe speelveld. Gezamenlijk tellen de verschillende maatregelen en de inzet van veel partijen op tot een maatschappelijke beweging naar een hoger digitaal veiligheidsniveau van ICT-producten en diensten, inclusief het *Internet of Things* (IoT of slimme apparaten). De Roadmap DVHS maakt onderdeel uit van de Rijksbrede aanpak voor digitale veiligheid in de Nederlandse Cyber Security Agenda (NCSA)[1] en bestaat uit een combinatie van Europese en nationale maatregelen. Het ontwikkelen van Europese wet- en regelgeving voor de digitale veiligheid ICT-producten en diensten draagt bij aan een gelijk speelveld en het concurrentievermogen van Nederlandse bedrijven in de EU op een hoger digitaal veiligheidsniveau. Deze Europese kaders die tot stand komen op basis van Europese publieke normen en waarden, zoals digitale veiligheid, privacy en consumentenbescherming dragen ook bij aan de versterking van de digitale soevereiniteit van Europa op mondiaal niveau. Ik steun dan ook het initiatief van het Duits voorzitterschap om in de Europese Telecomraad het belang van de digitale veiligheid van verbonden apparaten te benadrukken door middel van raadsconclusies. U bent hierover geïnformeerd door middel van de geannoteerde agenda van de Telecomraad van 7 december op 23 november jl.[2] In deze brief informeer ik u over de voortgang van de Roadmap DVHS en de inzet voor de komende periode.

Wettelijke eisen, toezicht en aansprakelijkheid

Wettelijke digitale veiligheidseisen voor slimme apparaten
Nederland maakt zich al enige jaren hard voor Europese wettelijke digitale veiligheidseisen aan alle slimme apparaten via de Europese richtlijn voor radioapparatuur (de *Radio Equipment Directive*, RED). De introductie van deze minimum veiligheidseisen in het kader van de RED vereist gedelegeerde

[1] Over de voortgang van de NCSA u bent geïnformeerd door de minister van Justitie en Veiligheid op 29 juni jl., Kamerstuk 26643, nr. 695.
[2] Kamerstuk 2150133, nr. 838

handelingen van de Europese Commissie. Een eerste daarvoor noodzakelijke *impact assessment* is inmiddels uitgevoerd. Verwacht wordt dat de gedelegeerde handelingen in het voorjaar van 2021 door de Europese Commissie worden gepubliceerd. Na een overgangsperiode zullen producten die dan op de markt komen moeten voldoen aan de betreffende eisen. De lengte van het overgangsperiode is nog onderwerp van gesprek in de EU.

Normen zullen nodig zijn om de technische invulling aan de eisen te geven. De Europese Commissie zal kort na de adoptie van de gedelegeerde handelingen opdracht geven aan de Europese standaardisatieorganisaties CEN, CENELEC en ETSI om de benodigde normen te ontwikkelen. Nederland wil een leidende rol spelen in deze ontwikkelingen. Met subsidie van mijn ministerie ondersteunt het Nederlandse normalisatie instituut NEN het Nederlandse voorzitterschap van een Europese CEN/CENELEC werkgroep voor IoT-veiligheid. Vooruitlopend op het Europese standaardisatieproces heeft Agentschap Telecom onderzoek uit laten voeren naar welke technische eisen onder de RED geschikt zouden kunnen zijn. Het onderzoeksrapport is eind augustus gepubliceerd.[3] Agentschap Telecom staat in contact met het NEN om de onderzoeksresultaten in te brengen in het formele standaardisatieproces.

Naast de ontwikkelingen op het gebied van de RED, wordt de *General Product Safety Directive* (GPSD) herzien door de Europese Commissie. De GPSD maakt, net als de RED, deel uit van het Europese CE-systeem voor productrichtlijnen (het zogenaamde *New Legislative Framework*, NLF) en geldt als vangnet in het geval voor een specifieke categorie producten geen eisen bestaan. Ten behoeve van de herziening van de richtlijn is een Europese expert groep opgericht om de GPSD te bezien in het licht van IoT en Artificiële Intelligentie. De expertgroep zal dit jaar een advies uit brengen aan de Europese Commissie. Voor Nederland is het opnemen van digitale veiligheidseisen in de GPSD een logische vervolgstap op het stellen van vergelijkbare eisen in de RED. De verwachting is dat halverwege 2021 een conceptwetsvoorstel voor de GPSD wordt geïntroduceerd door de Europese Commissie.

Tot slot is de Europese Commissie een studie gestart naar mogelijke horizontale Europese regulering voor de veiligheid van ICT-producten en diensten. De resultaten van deze studie worden in de loop van 2021 verwacht. Nederland blijft zich sterk maken voor wettelijke digitale veiligheidseisen om onveilige slimme apparaten van de Europese markt te kunnen weren.

Veiligheidsupdates in het consumentenrecht
In 2019 zijn in Brussel de richtlijn over overeenkomsten voor de levering van digitale inhoud en diensten (richtlijn levering digitale inhoud) en de richtlijn over overeenkomsten voor de verkoop van goederen (richtlijn verkoop goederen) vastgesteld.[4] Ze introduceren nieuwe en verduidelijken bestaande regels die de

[3] https://www.agentschaptelecom.nl/documenten/rapporten/2020/08/26/onderzoeksrapport-essential-requirements-for-securing-iot-consumer-devices
[4] Richtlijn (EU) 2019/771 betreffende bepaalde aspecten van overeenkomsten voor de verkoop van goederen en richtlijn (EU) 2019/770 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten.

aan- en verkoop van goederen en digitale inhoud, ook over de grenzen heen, veiliger en gemakkelijker maken. Uiterlijk op 1 juli 2021 moeten de richtlijnen zijn omgezet in nationale wetgeving. Het wetsvoorstel richtlijnen verkoop goederen en levering digitale inhoud implementeert beide richtlijnen en wordt naar verwachting begin volgend jaar naar uw Kamer gestuurd. Dit wetsvoorstel 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. Uitzondering hierop is wanneer de handelaar bij de aankoop de consument er expliciet op wijst dat hij geen updates mag verwachten, en de consument hiermee instemt.

Toezicht
Naast de bovengenoemde inzet om op Europees niveau wettelijke verplichtingen te stellen aan slimme apparaten zijn er mogelijkheden voor toezichthouders om binnen de bestaande wettelijke kaders stappen te zetten. De Autoriteit Persoonsgegevens (AP) heeft in februari jl. een advies gepubliceerd voor gebruikers om hun privacy te beschermen bij de aankoop en het gebruik van slimme apparaten. Er wordt ook onderzoek gedaan naar de privacyaspecten in de ontwikkeling van Nederlandse *smart cities* en er wordt een kader gegeven voor een toekomstbestendige ontwikkeling van *smart cities*. Dit rapport zal op korte termijn verschijnen.[5] Daarnaast heeft de AP in maart jl. tips gegeven aan consumenten voor de bescherming van privacy bij *connected cars*.[6] Ter voorbereiding op hun toezichthoudende taken onder de RED zal AT in 2021 testfaciliteiten ontwikkelen voor slimme apparaten. Hiermee wordt het voor AT mogelijk om zelfstandig te toetsen of slimme apparaten voldoen aan de dan geldende eisen onder de RED.

Eind 2019 heeft de Autoriteit Consument en Markt (ACM) op haar site consuwijzer.nl aangegeven welke informatie voorafgaand aan de koop aan consumenten moet worden verstrekt bij het online aanbod van slimme apparaten.[7] Daarin heeft ACM verduidelijkt dat informatie over hoe zaken geregeld zijn met updates ook informatie is die consumenten moeten krijgen voor de aankoop binnen de bestaande wettelijke kaders. De ACM heeft hierover ook gepubliceerd op haar algemene site acm.nl en via haar nieuwsbrief om bij partijen te onderstrepen dat consumenten hierover geïnformeerd moeten worden.[8] In de hierboven genoemde toekomstige wet- en regelgeving voor de verkoop van goederen en van levering digitale inhoud zal bovenop deze huidige informatieverplichting ook het verplichte updateregime na de aankoop gaan gelden. De ACM heeft de afgelopen zomer een aantal grote online aanbieders van slimme apparaten aangesproken op de bestaande informatieverplichtingen bij hun aanbod van slimme apparaten aan consumenten. 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-

[5] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/internet-things
[6] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-tips-voor-privacy-bij-connected-cars
[7] https://www.consuwijzer.nl/kan-ik-van-de-overeenkomst-af/zit-ik-ergens-aan-vast/informatieplicht
[8] https://www.acm.nl/nl/publicaties/acm-consument-heeft-recht-op-informatie-voordat-hij-slim-apparaat-koopt.

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. Naar een andere partij loopt nog onderzoek. De ACM heeft op 13 oktober jl. 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.[9]

Aansprakelijkheid
In algemene zin geldt dat op basis van het civiele aansprakelijkheidsrecht gebruikers verhaal kunnen zoeken voor geleden schade bij de rechter. Dit geldt ook op het gebied van *cybersecurity*. Gebruikers kunnen degene die de schade heeft aangericht, bijvoorbeeld een hacker, aanspreken op grond van onrechtmatige daad. Dit zal doorgaans niet makkelijk zijn. Daarnaast kunnen zij hun schade mogelijk verhalen op de producent of verkoper van de software op basis van overeenkomst. Als een producent software heeft aangeboden die vervolgens niet voldoet aan de digitale veiligheidseisen, is hij mogelijk aansprakelijk op grond van wanprestatie. Het aansprakelijkheidsrecht vormt aldus een marktprikkel voor aanbieders om voorzorgsmaatregelen te nemen ter voorkoming of beperking van schade. Ik heb onderzoek uit laten voeren door het Centre for the Law and Economics of Cyber Security van de Erasmus Universiteit Rotterdam 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. [10] In 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. Bedrijven zijn zelf verantwoordelijk voor het maken van onderlinge afspraken over cybersecurity. Een belangrijk aanknopingspunt om de eerder genoemde barrières mogelijk te verlagen is dat bedrijven onderling contractueel afspraken rondom cybersecurity vastleggen. Hierbij geldt wel contractvrijheid als uitgangspunt. Ik ga met het veld in gesprek om te verkennen op welke manier vanuit de overheid een handvat kan worden geboden aan bedrijven.

Standaarden en certificering

Cybersecurity certificering in de EU
De Europese *Cybersecurity Act* (Cyberbeveiligingsverordening, CSA) creëert een Europees stelsel van cybersecurity certificering voor ICT-producten, -diensten en -processen. Certificering is voor ICT-leveranciers in principe vrijwillig, maar de Europese Commissie zal voor eind 2023 aangeven of bepaalde certificeringschema's alsnog in de EU verplicht worden via aanvullende wetgeving. Nederland blijft, conform de motie Paternotte c.s.[11], pleiten voor verplichte cybersecurity certificering op Europees niveau. Voor de CSA geldt een nationale

[9] https://www.acm.nl/nl/publicaties/consumenten-beter-geinformeerd-over-updates-bij-aankoop-slim-apparaat-na-actie-acm en https://www.consuwijzer.nl/nieuws/slim-apparaat-kopen-grote-winkels-geven-nu-duidelijkere-informatie
[10] https://www.rijksoverheid.nl/documenten/rapporten/2020/06/24/aansprakelijkheid-voor-digitale-onveiligheid-in-b2b-relaties
[11] Kamerstuk 21501-30, nr. 422

implementatietermijn tot halverwege 2021 voor het inrichten van het stelsel in Nederland en het aanwijzen en inrichten van een nationale autoriteit die onder meer toezicht houdt op de naleving van de verordening. Nederland implementeert de verordening via het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening en wijst Agentschap Telecom aan als de nationale autoriteit. De consultatie van het wetsvoorstel is inmiddels afgerond en het wetsvoorstel is aangeboden aan de Raad van State voor advies.

De eerste Europese cybersecurity certificeringschema's worden momenteel ontwikkeld. Nederland draagt met expertise vanuit de publiek-private Online Trust Coalitie bij aan de ontwikkeling van een certificeringschema voor clouddiensten. Ook wordt voor beveiligingsaspecten van ICT-producten het multilaterale *Common Criteria*-stelsel omgezet naar een Europees schema onder de CSA. Daarnaast heeft de Europese Commissie in haar aanbeveling over de cyberveiligheid van 5G-netwerken van 26 maart 2019 aangegeven een certificeringschema te willen ontwikkelen voor 5G-netwerkapparatuur. In het kader van de implementatie van de Europese 5G-toolbox worden op initiatief van Duitsland en Polen voorbereidende werkzaamheden verricht. De Nederlandse inzet is dat deze werkzaamheden de input vormen voor de ontwikkeling van een certificeringschema voor 5G-netwerkapparatuur onder de CSA. Tenslotte zal de Europese Commissie middels een meerjarig werkprogramma haar inzet voor de toekomstige certificeringschema's bekend maken. Dit werkprogramma wordt eind dit jaar verwacht. Nederland zal onder meer inzetten op de ontwikkeling van certificeringschema's voor 5G-netwerkapparatuur, industriële controlesystemen, IoT en veilige software ontwikkeling op basis van het raamwerk van de publiek-private *Secure Software Alliance*.

Nationale ontwikkelingen
Als doorontwikkeling van het publiek-private *Partnering Trust* is in september de Online Trust Coalitie gelanceerd met ruim dertig partijen vanuit het bedrijfsleven, wetenschap en overheid.[12] Het doel van de Online Trust Coalitie is het beschikbaar maken van een eenduidige, efficiënte methode waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn. Deze methode draagt bij aan de invulling van de relevante wet- en regelgeving zoals de Cyber Security Act. Zoals eerder genoemd wordt vanuit de coalitie bijgedragen aan de ontwikkeling van het Europese cybersecurity certificeringschema voor clouddiensten en is voornemens ook bij te dragen aan veiligheidsvraagstukken in het kader van Gaia-X. Daarnaast ontwikkelt de coalitie momenteel een whitepaper die begin volgend jaar zal worden gepubliceerd.

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) ontwikkelt in opdracht van de ministeries van EZK en Justitie en Veiligheid in samenwerking met diverse private partijen een cybersecurity risicomodel voor (mkb-)bedrijven een kwaliteitsregeling voor cybersecuritydiensten en een lijst met eisen die bedrijven kunnen stellen aan deze dienstverleners. Voor de kwaliteitsregeling voor

[12] De deelnemers zijn de Online Trust Coalitie, ECP-Platform voor de informatiesamenleving, Bureau ICT-toetsing, CIO Platform Nederland, Cyberveilig Nederland, DHPA, Erasmus universiteit, Exact, EY, Google, ISP Connect, KIWA, Mazars, Mendix, Microsoft, NCSC, NEN, NLDigital, NOREA, PvIB/GEU, TNO, Wolters Kluwer TAA NL, Zeker-Online, Secura, Trusted Cloud (DE) / Gaia-x, Agentschap Telecom, Ministerie van EZK.

cybersecuritydiensten vinden pilots plaats en worden verbeteringen doorgevoerd zodat in 2021 de vaststelling en publicatie plaats kan vinden. Het risicomodel is de afgelopen periode getest bij bedrijven en positief geëvalueerd. Het Digital Trust Center zal het cybersecurity risicomodel aanbieden aan bedrijven op haar website.

Om de veiligheid van software in de gehele levenscyclus te stimuleren wordt publiek-privaat samengewerkt in het kader van de *Secure Software Alliance*. Het doel van het *Secure Software Framework*[13] is om de veiligheid van software gedurende de gehele levenscyclus meetbaar, stuurbaar en controleerbaar te maken. Het raamwerk is dit jaar in zijn geheel geïmplementeerd bij International Card Services (ICS) en de Universiteit Wageningen. Op basis van de opgedane ervaringen is het raamwerk dit jaar aangescherpt en zijn verschillende aanvullende producten ontwikkeld. Er is een awareness training gepubliceerd voor teams van softwareontwikkelaars. Daarnaast is een richtlijnen opgesteld voor het toepassen van het raamwerk in organisaties met een volwassenheidsmodel en een meetinstrument om de effectiviteit van de verbetermaatregelen continu te monitoren. Om de bewustwording onder bestuurders te stimuleren is een governance dashboard ontwikkeld met managementinformatie waarmee bestuurders de veiligheid van software gedurende de gehele levenscyclus kunnen monitoren. Dit stelt hen in staat om beslissingen te nemen rondom de risico's van de veiligheid van software. Een belangrijk aandachtspunt is de afhankelijkheidsrelatie van grote partijen van kleinere softwareontwikkelaars uit het mkb. Er wordt gezamenlijk gewerkt aan het betrekken en trainen van mkb'ers in het gebruik van het raamwerk om de veiligheid van hun software te verbeteren. Ten aanzien van ICT-opleidingen is in 2020 is het raamwerk 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.

Voor komend jaar is de inzet om het raamwerk bij meer organisaties te implementeren, het raamwerk onderdeel te laten worden van meer relevante opleidingen en wordt de Europese samenwerking verder vormgegeven. Onder andere Rabobank en KPN zijn de implementatie van het raamwerk aan het verkennen. Beroepsverenigingen zoals ISACA, NOREA, PVIB[14] zijn nauw betrokken bij de ontwikkeling van het raamwerk met als doel de principes op te nemen in hun beroepspraktijk.

Cybersecurity inkoopeisen van de overheid
Als belangrijke ICT-gebruiker kan de overheid met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en diensten stimuleren. Het ontwikkelen en implementeren van cybersecurity inkoopeisen voor alle overheidsorganisaties is een gedeelde doelstelling van de Roadmap DVHS en het programma NL DIGIbeter van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).[15] In samenwerking met het ministerie van BZK is de afgelopen periode een pakket aan

[13] https://securesoftwarealliance.org/agile-secure-software-lifecycle-management-secure/
[14] NOREA is een Nederlandse beroepsvereniging van IT-auditors, ISACA is een internationale beroepsvereniging van IT-auditors, PvIB is een Nederlandse beroepsvereniging van informatiebeveiligers
[15] Vergaderjaar 2019-2020, 26643, nr. 700

cybersecurity eisen en een tool ontwikkeld die overheidsorganisaties ondersteunt bij de inkoop van ICT-producten en diensten. De tool is sinds maart dit jaar online beschikbaar als prototype.[16] Een expertgroep met vertegenwoordigers vanuit het Rijk, de provincies, de gemeenten en de waterschappen hebben bijgedragen aan het formuleren van cybersecurity inkoopeisen voor de verschillende onderkende inkoopsegmenten zoals clouddiensten en serverplatformen. Op dit moment zijn er negen segmenten uitgewerkt. Eind 2020 zullen alle elf onderkende ICT-inkoopsegmenten beschikbaar zijn. Op dit moment wordt in pilots de tool getest bij verschillende overheidsorganisaties waaronder bij ICTU en Logius. De pilots lopen door tot in 2021. Om een breed beeld te krijgen van de praktische uitwerking van de cybersecurity inkoopeisen wordt ingezet op het uitvoeren van pilots in alle overheidslagen. De doelstelling blijft om deze cybersecurity inkoopeisen te gaan hanteren voor alle overheidslagen als een uitwerking van de Baseline Informatiebeveiliging Overheid (BIO). Ze vormen nadrukkelijk onderdeel van het BIO-versnellingsprogramma dat het ministerie van BZK in 2021 uitvoert.

Testen op digitale veiligheid
Het testen van producten op digitale veiligheid en het informeren van de consument door middel van de resultaten draagt bij aan de kennis en het bewustzijn van de consument omtrent digitaal onveilige apparatuur. De Consumentenbond is daarom sinds eind 2019 officieel van start gegaan met hun testprogramma *Connected products* en publiceert regelmatig resultaten in de consumentengids en op haar website. In dit programma worden apparaten getest op de verschillende aspecten van digitale veiligheid en privacy. Uit de resultaten blijkt onder andere dat er binnen verschillende productcategorieën problemen worden gevonden en dat er ook goed scorende producten zijn. De test van slimme lampen laat bijvoorbeeld zien dat er binnen deze productcategorie stappen zijn gezet maar dat vijf van de acht producten net geen voldoende vanwege verschillende kwetsbaarheden die toch aanwezig zijn. Een productcategorie die over het algemeen goed scoort is slimme thermostaten, waarbij geen enkel product onvoldoende scoorde op de test. Desondanks de goede technische score kunnen fabrikanten meer informatie verstrekken aan consumenten over updates binnen deze productcategorie. De tests op digitale veiligheid worden uitgevoerd bovenop de reguliere tests van producten die de Consumentenbond al geruime tijd uitvoeren. Aangezien dit een transformatie vergt van de test- en werkwijze, zal met een subsidie van mijn ministerie de Consumentenbond de komende twee jaar hun kennis en expertise op het gebied van het testen op digitale veiligheid kunnen vergroten.

Meten en opschonen van besmette slimme apparaten
De TU Delft heeft met subsidie van mijn ministerie metingen ontwikkeld om zicht te krijgen op het aantal besmette slimme apparaten in Nederland. Waar bij slimme apparaten veelal wordt gesproken over kwetsbaarheden en risico's zijn de apparaten in dit onderzoek al besmet met virussen. De TU Delft heeft een meetopstelling ontwikkeld met een steekproef van slimme apparaten waaraan periodiek nieuwe apparaten worden toegevoegd. Het beeld dat uit het onderzoek van TU Delft naar voren komt is dat het aantal gemeten besmette apparaten in

[16] https://www.bio-overheid.nl/ico-wizard/

Nederland laag is ten opzichte van andere landen. In Nederland zijn gemiddeld 125 besmettingen per dag gemeten, ongeveer één procent van de Nederlandse internetgebruikers. In Duitsland ligt het gemiddelde op ruim 2500 besmettingen per dag. In Egypte zijn gemiddeld ruim 15.000 besmettingen per dag gemeten.[17] IP camera's en op een netwerk aangesloten opslagruimten (NAS) zijn de meest voorkomende categorieën. Het is positief dat uit de metingen van TU Delft naar voren komt dat het aantal besmettingen in Nederland meevalt ten opzichte van andere landen. Tegelijkertijd blijft een groot aantal apparaten kwetsbaar voor misbruik en kunnen de gevolgen van misbruik voor een individuele gebruiker groot zijn. De uitkomsten van de metingen worden gedeeld met internetaanbieders en met het Digital Trust Center. Internetaanbieders kunnen met deze informatie contact leggen met klanten zodat besmettingen kunnen worden opgeschoond. Op basis van de data gaat het Digital Trust Center in gesprek met fabrikanten en andere stakeholders over maatregelen die zij kunnen nemen, bijvoorbeeld het ontwikkelen van een veiligheidsupdate.

Cybersecurity onderzoek
Veilige ICT-producten en diensten vereisen een constante focus op nieuwe technologieën en ontwikkelingen op het gebied van cybersecurity. Hiervoor is een stevige basis nodig op het gebied van kennisontwikkeling en innovatie. Uit verkenningen door TNO, NWO en Cyberveilig NL blijkt dat samenwerking over de gehele cybersecurity innovatieketen versterkt moet worden.[18] Op basis van deze verkenningen is besloten vraag en aanbod van kennis beter aan elkaar te verbinden door het oprichten van een samenwerkingsplatform als opvolger van Dcypher.[19] Hier zullen relevante partijen, expertise, instrumenten en middelen uit het cybersecurity domein bij elkaar komen in een brede, ketengeoriënteerde aanpak. In vervolg op de hierboven genoemde verkenningen hebben in de zomer vijf kwartiermakers uit wetenschap, onderwijs, bedrijfsleven en overheid een advies uitgebracht over de vormgeving van het nieuwe platform. Op basis van de aanbevelingen uit dit advies wordt het nieuwe platform ingericht. 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. Op het gebied van IoT is op basis van de Nationale Wetenschapsagenda in de zomer van 2019 ruim €8 miljoen aan onderzoeksgeld 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.[20]

Bewustwording
Nederlanders zijn steeds meer afhankelijk van het internet voor hun werk en levensbehoeften, terwijl de online dreiging stijgt en veilig online gedrag onvoldoende is ontwikkeld. Het is daarom van belang om in te blijven zetten op

[17] https://www.tudelft.nl/tpm/cybersecurity/themes-and-projects/iot/monitor/
[18] Vergaderjaar 2019-2020, Kamerstuk 26643, nr. 674.
[19] Dutch Cybersecurity Platform Higher Education and Research
[20] Kamerstuk vergaderjaar 2018–2019, 29 338, nr. 2

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Ons kenmerk
DGBI-DE / 20289637

bewustwording bij burgers om hen in staat te stellen om zelf beschermingsmaatregelen te nemen op het gebied van digitale veiligheid. Daarom is eind vorig jaar en begin dit jaar, in samenwerking met het ministerie van Justitie en Veiligheid, de campagne 'Doe je updates' uitgevoerd. Het doel is om consumenten voor te lichten over de noodzaak van het regelmatig updaten van slimme apparaten zoals babyfoons, draadloze speakers, deurbellen en slimme lampen. Veel slimme apparaten zijn te beveiligen met het doen van updates. Deze worden echter niet altijd door het product zelf aangeboden en consumenten zijn hiervan maar beperkt op de hoogte. Het overbrengen van deze kennis is daarom van belang voor de digitale weerbaarheid van burgers. De campagne is via online kanalen, radiocommercials en muziekdiensten verspreid. Begin dit jaar heeft hierbij het Nederlandse publiek kennis gemaakt met Hobbyhacker Hans die voor de overheid de boodschap overbrengt. Uit de evaluatie van de eerste twee rondes komt naar voren dat de creatieve opzet van de campagne zeker goed werkt om de boodschap over te brengen, maar dat herhaling van de campagne nodig is om daadwerkelijk gedragsverandering te bewerkstelligen. Dit najaar zal er een derde ronde van de campagne plaatsvinden waarbij de focus op veilig thuiswerken zal liggen. In oktober heeft eveneens de jaarlijkse Europese cybersecurity maand plaatsgevonden waar onder de Nederlandse vlag van Alert Online verschillende bewustwordingsinitiatieven zijn samen gebracht.

Tot slot
Het verhogen van de digitale veiligheid van hard- en software en IoT is een breed vraagstuk en vraagt om de inzet vanuit het bedrijfsleven, wetenschap en overheid in Nederland en in Europa. Samen met de partners blijf ik mij vanuit de Roadmap DVHS inzetten voor de maatschappelijke beweging richting een hoger digitaal veiligheidsniveau van ICT-producten en diensten.

Hoogachtend,

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