Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD 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 30 november 2021
Betreft Voortgang Roadmap Digitaal Veilige Hard- en Software

Ons kenmerk
DGBI-DE / 21288826

Geachte Voorzitter,

Met deze brief informeer ik uw Kamer over de voortgang van de Roadmap Digitaal veilige Hard- en Software. Het afgelopen jaar heeft COVID-19 ons laten zien hoe afhankelijk we zijn van digitale diensten en producten: thuis werken, leren en ondernemen was voor velen de norm. Een meer hybride manier van werken dient zich aan waarbij Nederland als samenleving en economie permanent de voordelen wil blijven plukken van de voortschrijdende digitalisering. Daarbij is het des te belangrijker dat de ICT-producten en -diensten die dat mogelijk maken digitaal veilig zijn. Vanuit de Roadmap Digitaal Veilige Hard- en Software (DVHS) zet het kabinet een breed palet van maatregelen in om dat te bevorderen. De Roadmap DVHS maakt onderdeel uit van de Rijksbrede aanpak voor digitale veiligheid in de Nederlandse Cyber Security Agenda (NCSA) waarover uw Kamer op 28 juni jl. is geïnformeerd.[1]

De Roadmap DVHS bestaat uit een combinatie van Europese en nationale maatregelen. Het vaak grensoverschrijdende karakter van ICT-producten en -diensten vereist een Europese aanpak, die niet alleen voor een hoger digitaal beveiligingsniveau zorgt maar bovendien bijdraagt aan een gelijk speelveld en een beter concurrentievermogen van Nederlandse bedrijven in de EU. Deze Europese kaders komen tot stand op basis van Europese normen en waarden zoals digitale veiligheid, privacy en consumentenbescherming, en dragen bij aan de versterking van de digitale soevereiniteit van Europa op mondiaal niveau.

Wettelijke eisen, toezicht en aansprakelijkheid

Wettelijke digitale veiligheidseisen voor apparaten
Ten aanzien van Europese wettelijke digitale veiligheidseisen zijn er ontwikkelingen op het gebied van de *Radio Equipment Directive*, de *General Product Safety Regulation* en een aangekondigde *Cyber Resilience Act*.
Op 29 oktober jl. heeft de Europese Commissie bekend gemaakt dat wettelijke digitale veiligheidseisen gesteld zullen worden aan draadloos communicerende apparaten in het kader van de Europese richtlijn voor radioapparatuur (de *Radio Equipment Directive*, RED). Nederland heeft een leidende rol gespeeld in het

[1] Kamerstuk 26643, nr. 767

stellen van deze Europese eisen. De betreffende gedelegeerde handeling is verzonden aan de Europese Raad en het Europees Parlement. Mits er geen bezwaren volgen wordt dit besluit begin 2022 van kracht en volgt een overgangstermijn van dertig maanden om producten aan te passen die vanaf dan op de Europese markt komen. Consumenten kunnen er vervolgens op vertrouwen dat nieuw aangeschafte producten voldoen aan Europese normen, waarbij zij als gebruiker wel medeverantwoordelijk zijn deze producten veilig te blijven gebruiken. Producten die vanaf medio 2024 niet aan de cybersecurityeisen voldoen kunnen van de markt worden geweerd en gehaald door Agentschap Telecom (AT).

Parallel hieraan wordt al geruime tijd gewerkt aan normen voor de technische invulling van de veiligheidseisen, in voorbereiding op een opdracht van de Europese Commissie aan de Europese standaardisatieorganisaties CEN, CENELEC en ETSI om deze normen te ontwikkelen. Nederland speelt ook hierbij een leidende rol. Met subsidie van mijn ministerie ondersteunt het Nederlandse normalisatie instituut NEN het Nederlandse voorzitterschap van een Europese CEN/CENELEC werkgroep voor *Internet of Things* (IoT) -veiligheid. Nederlandse bedrijven leveren een constructieve bijdrage en ook vanuit AT, wordt deelgenomen aan dit standaardisatieproces.

Naast de ontwikkelingen op het gebied van de RED, wordt ook de *General Product Safety Directive* (GPSD) herzien. 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 ingeval er voor consumentenproducten geen specifieke geharmoniseerde veiligheidseisen bestaan. 30 juni jl. is een voorstel voor een verordening gedaan door de Commissie die de GPSD moet vervangen, de *General Product Safety Regulation (GPSR)*. Onderdeel van het voorstel, dat op algemene productveiligheid toeziet, is om nieuwe technologische ontwikkelingen, waaronder het verbonden zijn van producten en ook het bevatten van software componenten, expliciet op te nemen als te beoordelen veiligheidsaspect. Hierover is uw Kamer geïnformeerd via een BNC-fiche[2]. Voor Nederland is het opnemen van digitale veiligheidseisen in de GPSR een logische vervolgstap op het stellen van vergelijkbare eisen in de RED.

Ten aanzien van horizontale regulering heeft de Europese Commissie dit jaar een studie verricht naar de noodzaak voor mogelijke horizontale Europese regulering met betrekking tot de veiligheid van ICT-producten en diensten in brede zin. Dit mede naar aanleiding van Raadsconclusies over de cybersecurity van *Internet of Things* (IoT) apparaten van de Telecomraad op 7 december 2020.[3] De resultaten van deze studie zijn nog niet bekend, maar de voorzitter van de Europese Commissie Ursula von der Leyen heeft tijdens haar Staat van de Unie op 15 september jl. de Europese *Cyber Resilience Act* aangekondigd. Een wetsvoorstel daartoe wordt in 2022 verwacht. Nederland vindt dat Europese wettelijke digitale veiligheidseisen voor ICT-producten en diensten noodzakelijk zijn, en ziet een voorstel dan ook met interesse tegemoet. In de tussentijd zal

[2] Kamerstuk 22112 nr. 1589
[3] Kamerstuk 21501-31, nr. 598

Nederland actief het gesprek aangaan met de Europese Commissie over de mogelijke inhoud van een voorstel.

Veiligheidsupdates in het consumentenrecht
Op 16 februari 2021 is het Implementatiewetsvoorstel richtlijnen verkoop goederen en levering digitale inhoud bij de Tweede Kamer ingediend en deze is nog in behandeling.[4] Op 7 juli 2021 heeft de minister voor Rechtsbescherming de nota naar aanleiding van het verslag met de Kamer gedeeld.[5] Met dit wetsvoorstel worden twee Europese consumentenrichtlijnen (verkoop goederen en levering digitale inhoud)[6] geïmplementeerd, die met ingang van 1 januari 2022 van kracht zijn. De Autoriteit Consument en Markt (ACM) zal toezicht houden. Het wetsvoorstel introduceert nieuwe en verduidelijkt bestaande regels die de aan- en verkoop van goederen en digitale inhoud, ook over de grenzen heen, veiliger en gemakkelijker maken en het expliciteert onder meer een verplicht updateregime voor digitale inhoud en tastbare goederen met een digitaal element. Consumenten hebben hiermee recht op (veiligheids-) updates zolang zij die redelijkerwijs mogen verwachten. De verkoper/handelaar zal afspraken moeten maken met een derde, zoals de fabrikant of een softwareleverancier, die de updates kunnen leveren. 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.

De ACM bereidt op dit moment voorlichting over deze nieuwe regelgeving voor. De ACM zal deze voorlichting onder meer verstrekken via haar website en het consumentenvoorlichtingsportaal Consuwijzer.nl.

Toezicht
Zoals gezegd is de verwachting dat de gedelegeerde handeling van de RED eind dit jaar van kracht wordt, waarna een overgangstermijn volgt. Agentschap Telecom heeft ter voorbereiding van haar toezichthoudende taken een IoT testlaboratorium ingericht waarin diverse apparaten worden getest op cybersecurityaspecten. De ervaringen hierbij worden door AT gebruikt in gesprekken met de Europese Commissie en toezichthouders uit andere lidstaten, alsook in overleggen met de industrie.

De ACM gaat samen met AT onderzoek doen naar domotica-apparaten, slimme apparaten voor thuisgebruik. Deze apparaten worden gebruikt om de processen in een woning te automatiseren en kunnen (indirect) worden verbonden met het internet. In het onderzoek worden de apparaten onder meer beoordeeld op informatie voor en na de aankoop, op informatie over updates en de kwaliteit daarvan en andere cybersecurityaspecten. Binnen dit onderzoek is aandacht voor verplichtingen op grond van het huidige generieke consumentenrecht en de nieuwe verplichtingen op grond van de implementatiewet van de richtlijnen verkoop goederen en levering digitale inhoud. Dit onderzoek is tevens een

[4] Kamerstuk 35734, nr. 2
[5] Kamerstuk 35734, nr. 7
[6] 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.

voorbereiding van AT op de toezichthoudende taken op grond van de gedelegeerde handeling van de RED.

In vervolg op hun gesprekken vorig jaar met leveranciers zal de ACM naar verwachting voor eind dit jaar communiceren over een afgerond onderzoek naar precontractuele informatieverplichtingen bij de online verkoop van slimme apparaten.[7]

De Autoriteit Persoonsgegevens (AP) heeft in 2021 onder haar focus 'dataprotectie in een digitale samenleving' onder meer de volgende acties ondernomen in haar toezicht op persoonsgegevens in digitaal veilige hard- en software. Op Europees niveau hebben de AP en haar Europese evenknieën (verenigd in de *European Data Protection Board*, de EDPB) richtlijnen uitgebracht voor de ontwikkeling en inzet van spraakassistenten en *connected vehicles*.[8] Daarnaast neemt de AP deel aan de Stakeholders Cybersecurity Certification Group in het kader van de *Cybersecurity Act* (CSA, zie hierna) en de ontwikkeling van Europese certificeringschema's voor ICT-producten, diensten en processen.
Op nationaal niveau heeft de AP de automotivesector gewezen op de Algemene verordening gegevensbescherming (AVG) en de richtlijn *connected vehicles*. Daarnaast heeft AP samen met de Inspectie Gezondheidszorg en Jeugd een factsheet *E-Health* gepubliceerd voor de zorgsector[9], en een rapport over *smart cities* waarin (privacy)aanbevelingen worden gedaan om verantwoord verder te kunnen ontwikkelen.[10]

Aansprakelijkheid
Naar aanleiding van verkennend onderzoek door het *Centre for the Law and Economics of Cyber Security* van de Erasmus Universiteit Rotterdam naar de juridische en economische barrières voor bedrijven om schade te verhalen als gevolg van cybersecurity incidenten, heeft een aantal dialoogsessies plaats gevonden met stakeholders uit het veld. Op het gebied van aansprakelijkheid staat contractvrijheid tussen bedrijven onderling voorop, ook op het gebied van cybersecurity. Gegeven dit kader is het gesprek aangegaan om te bezien hoe de overheid kan bijdragen aan een situatie waarbij afnemers van ICT-diensten meer zekerheid hebben in hun onderlinge relaties met leveranciers. De stakeholders hadden een breed spectrum van invalshoeken, variërend van een nadruk op contractvrijheid en de daarmee samengaande eigen verantwoordelijkheid van partijen om bij contracten cybersecurity-gerelateerde aspecten mee te nemen, een mogelijke rol voor brancheorganisaties om aangesloten bedrijven te helpen met voorbeeld clausules, tot een grotere rol van de overheid bijvoorbeeld op het gebied van certificering. Met name dit laatste punt sluit aan op andere actielijnen uit deze Roadmap DVHS.

[7] https://www.acm.nl/nl/publicaties/consumenten-beter-geinformeerd-over-updates-bij-aankoop-slim-apparaat-na-actie-acm
[8] https://autoriteitpersoonsgegevens.nl/nl/nieuws/edpb-guidelines-voor-connected-cars-en-spraakassistenten
[9] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/factsheet_e-health.pdf
[10] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-publiceert-aanbevelingen-voor-smart-cities

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Digitale Economie

Ons kenmerk
DGBI-DE / 21288826

Standaarden en certificering

Cybersecurity certificering in de EU
Er wordt voortgang gemaakt met de implementatie van de Europese Cybersecurity Act (Cyberbeveiligingsverordening, CSA), zowel in Nederland als in de EU. De CSA creëert een Europees stelsel op het gebied van cybersecurity-certificering voor ICT-producten, diensten en processen. Het uitvoeringswetsvoorstel Cyberbeveiligingsverordening is in behandeling bij uw Kamer. Het wetsvoorstel gaat onder meer om het aanwijzen van een nationale cyberbeveiligingscertificeringsautoriteit, oftewel een toezichthouder. AT zal worden aangewezen als nationale toezichthoudende autoriteit. AT is vergevorderd in het treffen van voorbereidingen om de genoemde taken uit te kunnen oefenen.

Op Europees niveau wordt ondertussen onder de vlag van de CSA gewerkt aan de ontwikkeling van de eerste Europese cybersecurity-certificeringsschema's. Naar verwachting zal het cybersecurity-certificeringsschema voor beveiligingselementen van ICT-producten (*Common Criteria*) in de eerste helft van 2022 worden afgerond. Het certificeringsschema voor clouddiensten zal naar verwachting in de tweede helft van 2022 worden afgerond. Nederland draagt hier aan bij via de publiek-private Online Trust Coalitie (OTC). Daarnaast wordt door het Europese agentschap voor cybersecurity ENISA het proces gestart voor de ontwikkeling van een cybersecurity-certificeringschema voor 5G-netwerkapparatuur. In het werkprogramma van de Europese Commissie zijn ook cybersecurity-certificeringsschema's voor IoT-apparatuur en geautomatiseerde industriële controlesystemen aangekondigd als onderdeel van de CSA.

In de Nederlandse publiek-private *Online Trust Coalitie* (OTC) zijn het afgelopen jaar belangrijke stappen gezet met betrekking tot het vergroten van vertrouwen in clouddiensten.[11] Begin dit jaar is een witboek gepubliceerd waarin drie pijlers worden gepresenteerd als fundament voor vertrouwen in clouddiensten: intrinsieke betrouwbaarheid van clouddiensten op basis van geharmoniseerde standaarden, het bieden van zekerheid door middel van een onafhankelijk verstrekte *assurance*-verklaring en eenduidige en geharmoniseerde rapportage hierover. Deze pijlers worden meegenomen in de Nederlandse inbreng voor de ontwikkeling van het hierboven genoemde cybersecurity-certificeringsschema voor clouddiensten onder de CSA. Nederland speelt met deze publiek-private inbreng in de EU een grote rol bij de vormgeving van het cybersecurity-certificeringschema voor clouddiensten. Nederland werkt daarbij nauw samen met andere lidstaten zoals Duitsland. Dit komt de effectiviteit van het certificeringsschema ten goede en helpt om de uiteindelijke implementatie in Nederland optimaal te doen verlopen. Zo heeft Nederland ook een pilot uitgevoerd om de mogelijke werking van het concept-certificeringsschema voor clouddiensten te testen in samenwerking met Secura, Exact en AT.

Nationale ontwikkelingen
Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) heeft in opdracht van de ministeries van Economische Zaken en Klimaat (EZK) en Justitie en

[11] https://onlinetrustcoalitie.nl/

Veiligheid (JenV) in samenwerking met diverse private partijen een risicoklasseindeling Digitale Veiligheid ontwikkeld voor het midden- en kleinbedrijf (mkb). De risicoklasseindeling is beschikbaar via de website van het Digital Trust Center (DTC).[12] Deze tool maakt voor ondernemers inzichtelijk wat hun risicoprofiel is en welke maatregelen daarbij horen. Daarnaast heeft het CCV een certificeringsschema ontwikkeld voor pentesten. Dit schema is in april 2021 gepubliceerd.[13] Aanbieders van pentesten kunnen zich op basis hiervan laten certificeren. Dit verschaft duidelijkheid voor de afnemer over de kwaliteit van deze dienst.

Met betrekking tot veiligheid van software zijn ten behoeve van een effectieve implementatie van het *Framework Secure Software*[14] in organisaties geautomatiseerde controles ontwikkeld. Dit geeft organisaties meer inzicht in cybersecurity binnen het constante ontwikkelproces van complexe softwareproducten in samenwerking met hun toeleveranciers.

Cybersecurity inkoopeisen van de overheid
Op het gebied van cybersecurity ziet de overheid het als haar taak het goede voorbeeld te geven, haar rol als goed opdrachtgever op het gebied van eigen ICT-middelen te versterken en daarmee ook een algemene beweging in de markt te stimuleren naar het ontwikkelen en aanbieden van veilige ICT-producten en diensten voor de hele samenleving. Dat doet de overheid door slimmer en bewuster in te kopen, zodat ICT-aanbieders een economische prikkel krijgen om meer veilige producten te ontwikkelen.

Als onderdeel van de Roadmap DVHS, het programma NL DIGIbeter en het Rijksinkoopbeleid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is begin dit jaar het instrument Inkoopeisen Cybersecurity Overheid (ICO) opgeleverd. Met dit instrument kunnen (overheids)opdrachtgevers ten behoeve van ICT-inkopen en -aanbestedingen specifieke informatiebeveiligingseisen formuleren.[15] Deze eisen worden vervolgens meegestuurd bij een aanbesteding en kunnen later in een contract met een leverancier worden opgenomen. Door de open toegang via BIO-overheid.nl is het daarnaast mogelijk voor marktpartijen om gebruik te maken van de mogelijke eisen die de inkopende overheden hanteren. Sinds de start van de ontwikkeling hebben er pilots plaatsgevonden met de cybersecurity-inkoopeisen bij 35 inkooptrajecten binnen alle overheidslagen inclusief uitvoeringsinstanties.

ICO bestaat inmiddels uit tien inkoopsegmenten, waaronder clouddiensten en serverplatforms. Tegelijkertijd worden ook nieuwe invalshoeken toegevoegd. Zo zijn dit jaar de informatieveiligheidseisen aangevuld met privacy-eisen. Deze aanvulling wordt nu in de praktijk getest. Het beeld dat uit de pilots kwam is dat ICO door de informatiebeveiligingsfunctionarissen als een belangrijk inkoophulpmiddel wordt gezien. Daarmee verdient ICO een vaste plek in het inkoopproces van de overheid. Tegelijkertijd werd geconstateerd dat inkopers en

[12] https://www.digitaltrustcenter.nl/risicoklasse
[13] https://hetccv.nl/keurmerken/expert/keurmerk-pentesten
[14] https://securesoftwarealliance.org/framework-secure-software/
[15] https://www.bio-overheid.nl/ico-wizard/

opdrachtgevers het complex vinden om informatiebeveiligingseisen mee te nemen bij inkooptrajecten omdat ze moeite hebben om een programma van functionele eisen te vertalen naar specifieke ICT-gerelateerde beveiligingseisen. Betere samenwerking tussen ICT-specialisten, opdrachtgevers en inkopers kan dit vraagstuk helpen oplossen.

Er is een implementatiestrategie ontwikkeld gericht op de verbreding van het gebruik van deze cybersecurity-inkoopeisen en op het op gang krijgen van een betere interactie tussen de driehoek informatiebeveiliger, opdrachtgever en inkoper. Eind 2022 zal het gebruik van ICO worden geëvalueerd. Dan zal ook de vraag worden beantwoord of het gebruik van het instrument ICO bij inkoop verplicht moet worden voor alle overheidsorganisaties. Tot die tijd is de inzet gericht op het stimuleren van het gebruik, doorontwikkeling van ICO, en het opdoen van ervaringen met de ICT-leveranciers die zich moeten houden aan de gestelde beveiligingsvereisten.

Testen op digitale veiligheid
Het afgelopen jaar hebben diverse cybersecurity- en privacytests op slimme apparaten plaatsgevonden in het kader van het testprogramma *Connected products* van de Consumentenbond. De Consumentenbond werkt in dit programma internationaal samen met zusterorganisaties. De testresultaten zijn beschikbaar op de website van de Consumentenbond. Uit de verschillende onderzoeken komt het beeld naar voren dat meer bekende, gerenommeerde merken het meest aandacht hebben voor privacy en veiligheid. Daarnaast blijkt uit onderzoek van Belgische zusterorganisatie Testaankoop dat er een grotere kans is op tekortkomingen op het gebied van cybersecurity en privacy in producten van minder gerenommeerde merken die door consumenten gekocht worden via internationale handelsplatforms.[16] In reguliere vergelijkende test van de Consumentenbond ligt de nadruk op bekende merken, verkrijgbaar in Nederland. Ook worden sommige tests periodiek opnieuw uitgevoerd of aangevuld met nieuwe producten.

Er zijn tests uitgevoerd voor beveiligingscamera's, deurbelcamera's, babyfoons, robotstofzuigers, printers, wasmachines en drogers. Bij de in 2021 nieuw geteste beveiligingscamera's hadden 23 producten voldoende oog voor cybersecurity en privacy en was er één product onder de maat.[17] Bij de veertien geteste deurbelcamera's scoorden de geteste apparaten allemaal een voldoende.[18] Een positieve ontwikkeling is dat de vier extra geteste babyfoons met camera en een app voldoende scoorden in tegenstelling tot een jaar eerder.[19] De tien geteste robotstofzuigers met bediening via een app zijn allemaal op een veilige manier te gebruiken, maar daarvoor moet een consument bij de meeste wel zelf deze aspecten goed instellen. Bij drie modellen is het niet goed mogelijk om een persoonlijk account te wissen bij doorverkoop of weg doen.[20] Printers laten voor de Consumentenbond een zorgwekkender beeld zien, ook omdat printers

[16] https://www.consumentenbond.nl/smarthome/test-privacy-veiligheid-smart-home-producten
[17] https://www.consumentenbond.nl/beveiligingscamera/kopen
[18] https://www.consumentenbond.nl/beveiligingscamera/beste/beste-deurbel-met-camera
[19] https://www.consumentenbond.nl/babyfoon
[20] https://www.consumentenbond.nl/robotstofzuiger/kopen

technologisch een langere geschiedenis hebben dan andere verbonden apparaten. Over de hele linie van privacy en veiligheidsaspecten scoren printers matig.[21] Uit een test van twintig printers bleken vier modellen gevoelig voor misbruik via bekende printerkwetsbaarheden. De Consumentenbond gaat over deze testresultaten in gesprek met vertegenwoordigers van printerfabrikanten. Op merkniveau zijn de achterliggende app-platforms van zeven wasmachine en wasdroger merken getest. Hoewel geen grote kwetsbaarheden zijn gevonden, is er ruimte voor verbetering.[22]

Het testen van het 'smart'-deel van een consumentenproduct is aanvullend op de reguliere tests van de Consumentenbond. Met subsidie van mijn ministerie vergroot de Consumentenbond de eigen kennis en expertise, om daarmee de consument beter te kunnen voorlichten. Met deze testresultaten kunnen consumenten ook de digitale veiligheid en privacy van producten meewegen in hun aankoopkeuzes.

Meten en opschonen digitale apparaten
Met subsidie van mijn ministerie heeft de Technische Universiteit Delft (TU Delft) een monitor ontwikkeld die geautomatiseerd metingen doet om zicht te krijgen in het aantal besmette, met het internet verbonden, slimme apparaten in Nederlandse netwerken. Het project is afgelopen juni afgerond.[23] Overzichten van IP-adressen van gecompromitteerde apparaten worden maandelijks met de *Internet Service Providers* (ISPs) gedeeld via de *Abuse Information Exchange*. De desbetreffende ISPs kunnen vervolgens hun klanten benaderen om de apparaten op te schonen. Daarnaast creëert de monitor overzichten van betrokken fabrikanten welke gebruikt kunnen worden om met hen het gesprek aan te gaan. In de projectfase werd deze informatie gedeeld met het Digital Trust Center. De TU Delft heeft vastgesteld dat het aantal gemeten besmette apparaten in Nederland laag is ten opzichte van andere landen, met een gemiddelde van 109 apparaten per dag. IP camera's en op een netwerk aangesloten opslagruimten (NAS) zijn nog steeds de meest voorkomende categorieën. Met de afronding van de projectfase onderzoekt AT momenteel de mogelijkheden om de monitor van TU Delft op te nemen in hun IoT testlaboratorium ter ondersteuning in hun toekomstige toezichthoudende taak onder RED vanaf komend jaar. Om deze reden heb ik besloten om de TU Delft financieel te steunen zodat de monitor tot eind dit jaar operationeel blijft.

Cybersecurity onderzoek en innovatie
Om te kunnen beschikken over veilige ICT-producten en -diensten moet Nederland inzetten op een hoogwaardige en autonome kennisbasis op het gebied van cybersecurity. Cybersecurity is een van de onderwerpen in de Kennis- en innovatieagenda (KIA) veiligheid van het Missiegedreven topsectoren- en innovatiebeleid (MTIB). In deze context heeft het kabinet besloten tot de oprichting van een publiek-privaat samenwerkingsplatform voor cybersecurity-kennis en -innovatie, genaamd dcypher. Voortbouwend op het werk van haar voorganger moet dcypher de krachten op het terrein van onderzoek, innovatie en

[21] https://www.consumentenbond.nl/printer
[22] https://www.consumentenbond.nl/wasmachine
[23] https://weis2021.econinfosec.org/wp-content/uploads/sites/9/2021/06/weis21-rodriguez.pdf

onderwijs beter gaan bundelen om zo te komen tot een thematische aanpak in de hele innovatieketen.[24]

Eind 2020 is het bestuur van dcypher ingericht met vertegenwoordiging vanuit private organisaties, kennisinstellingen en de overheid. Ter ondersteuning van dcypher is bij de Rijksdienst voor Ondernemend Nederland (RVO) een platformbureau opgericht. Ook is een start gemaakt met de inhoudelijke agendering en programmering van kennis en innovatietrajecten door middel van een tweetal routekaarten op de thema's geautomatiseerd kwetsbaarheden onderzoek (*Automated Vulberability Research*) en cryptocommunicatie.[25] Naarmate de agenderings- en programmeringsprocessen vorderen zullen in de loop van volgend jaar nieuwe routekaarten worden opgezet.

Op Europees niveau wordt ingezet op cybersecurity kennis en innovatie via Nederlandse representatie in de *Governing Board* van het recentelijk opgerichte *European Cybersecurity, Industrial, Technology and Research Competence Centre* (ECCC). De nationale input richting het ECCC zal vormgegeven worden middels nog op te richten Nationale Coördinatie Centra (NCC). Om de nationale inzet op dit onderwerp zoveel mogelijk te stroomlijnen, wordt het Nederlandse NCC, net als dcypher, ondergebracht bij RVO. Medio volgend jaar wordt de Kamer opnieuw geïnformeerd over de ontwikkelingen op het gebied van cybersecurity kennis en innovatie.

Bewustwording
Bijna driekwart van de Nederlanders heeft een of meerdere slimme apparaten in huis. Het overgrote deel van deze groep is zich ervan bewust dat die apparaten gehackt kunnen worden en dat ze dus voorzien moeten worden van updates wanneer die beschikbaar zijn. Toch stelt meer dan de helft van de mensen het uitvoeren van updates uit, vergeet het, of vindt het teveel gedoe. Dit blijkt uit onderzoek uitgevoerd in opdracht van mijn ministerie.[26] Daarmee zijn Nederlanders kwetsbaar voor internetcriminelen. De schaalgrootte en de snelheid waarmee internetcriminelen hun aanpak aanpassen en perfectioneren maken het makkelijk voor criminelen om online hun slag te slaan. Daarom is mijn ministerie eind 2019 gestart met de publiekscampagne 'Doe je updates'. Het doel van deze campagne is om consumenten voor te lichten over de noodzaak van het regelmatig updaten van slimme apparaten zoals babyfoons, draadloze speakers, deurbellen en slimme lampen.

Er hebben inmiddels drie rondes van de campagne plaats gevonden, waarvan de laatste van eind november 2020 tot en met januari 2021. Bij de derde ronde lag de nadruk op het thuiswerken en de router als voordeur naar de slimme apparaten. Uit effectmetingen van de campagnerondes blijkt dat de campagne goed wordt ontvangen, maar dat de slag naar het gewenste gedrag nog gemaakt moet worden. Voor het einde van dit jaar zal een vierde campagneronde starten, waarbij de focus wordt verlegd van bewustwording naar het beïnvloeden van het

[24] Kamerstuk 26643, nr. 674
[25] De keuze voor deze thema's is gebaseerd op de missie cyberveiligheid van de Kennis- en Innovatie Agenda (KIA) Veiligheid en consultaties met het veld.
[26] https://www.campagnetoolkits.nl/documenten/publicaties/2020/01/31/flitspeiling-slimme-apparaten

gewenste gedrag. Het is belangrijk dat burgers worden gestimuleerd om software-updates te doen om hun online veiligheid te verhogen.
Daarnaast heeft in oktober de tiende editie van de jaarlijkse Europese cybersecuritymaand 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 is een breed vraagstuk en vraagt om de blijvende inzet vanuit het bedrijfsleven, wetenschap en overheid in Nederland en in Europa. De afgelopen kabinetsperiode zijn belangrijke stappen gezet. Om er voor te zorgen dat de beleidsaanpak via de Roadmap DVHS toekomstbestendig is, zal ik de Roadmap DVHS extern laten evalueren. Daarnaast heeft de Cyber Security Raad in haar rapport 'Integrale aanpak cyberweerbaarheid' uit april dit jaar[27] adviezen en aanbevelingen gedaan voor de inzet voor de komende kabinetsperiode en de bijbehorende investeringen die raken aan de Roadmap DVHS. Beide rapporten zullen input vormen voor het beleid van het volgende kabinet, gericht op een structureel hoger digitaal veiligheidsniveau van ICT-producten en diensten voor burgers en bedrijven.

Stef Blok
Minister van Economische Zaken en Klimaat

[27] https://www.cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid