Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2514 CV DEN HAAG

Directoraat-generaal
Economie en Digitalisering
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

Ons kenmerk
DGED-DE / 26175894

Uw kenmerk
172339.01U

Betreft Voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten (COM(2022)454)

Geachte Voorzitter,

De leden van de vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 15 november 2022 beraadslaagd over het door de Europese Commissie voorgestelde voorstel voor een verordening betreffende horizontale cyberbeveiligingsvereisten en het BNC-fiche van de regering. De leden van de fracties van GroenLinks, de PvdA, de SP en de PvdD gezamenlijk hebben naar aanleiding van het voorstel en het BNC-fiche enkele vragen. Ook de leden van de fracties van D66, de PVV en de OSF hebben vragen naar aanleiding van het voorstel en het BNC-fiche.

Hierbij treft u de beantwoording van de bij brief d.d. 6 december 2022 gestelde vragen de leden van de fracties van GroenLinks, de PvdA, de SP en de PvdD gezamenlijk en van de leden van de fracties van D66, de PVV en de OSF. De antwoorden zijn ingevoegd in de oorspronkelijke tekst van voornoemde brief.

M.A.M. Adriaansens
Minister van Economische Zaken en Klimaat

Directoraat-generaal Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 26175894

Vragen van de leden van de fracties van GroenLinks, de PvdA, de SP en de PvdD gezamenlijk

De leden van de fracties van GroenLinks, PvdA en de SP gezamenlijk hebben met interesse kennisgenomen van het voorstel. Zij ondersteunen het uitgangspunt dat er duidelijke algemene kaders moeten komen voor de veiligheid van digitale producten en diensten. De leden hebben wel een aantal vragen over onder andere de impact van de verordening op vrije en opensourcesoftware en over de effectieve handhaving van het voorstel.

Vrije en open source software

De leden zijn blij om te lezen dat open source software buiten handelsactiviteit is uitgezonderd van de werking van de verordening. Zij constateerden echter wel dat maar beperkt duidelijk is wat moet worden verstaan onder handelsactiviteit in het licht van deze verordening, zeker omdat de ontwikkeling van vrije- en open source software op een zeer grote verscheidenheid van manieren gebeurt, met vaak veel verschillende betrokken partijen.
Zou de regering bereid zijn om in de onderhandelingen in te zetten op een duidelijker kader voor opensourcesoftware-ontwikkelaars ten aanzien van de vraag wanneer zij wel en niet onder de reikwijdte van deze verordening vallen? Onderstreept de regering het belang van een gezonde en actieve opensourcesoftwaregemeenschap in Europa, zowel vanuit het perspectief om minder afhankelijk te zijn van software van buiten Europa, als vanuit het perspectief van digitale innovatie? Is de regering bereid om in de uitvoering van de verordening zo veel mogelijk duidelijkheid te scheppen omtrent de toepasbaarheid ervan voor de opensourcesoftwaregemeenschap?

Antwoord

Het kabinet onderstreept het belang van een gezonde en actieve open source gemeenschap, omdat deze belangrijk is voor innovatie en openheid een bijdrage kan leveren aan het veiliger maken van digitale producten. Het kabinet zet zich tijdens de onderhandelingen over het voorstel in voor meer duidelijkheid over de vraag wanneer open source software al dan niet onder de reikwijdte van de Cyber Resilience Act (hierna: CRA) valt. De beslissende factor daarbij ligt in de definitie van het 'op de markt aanbieden' van een product met digitale elementen. Alleen producten die 'op de markt' worden aangeboden vallen onder de CRA, hetgeen de daarin opgenomen cybersecurityverplichtingen voor fabrikanten en andere marktdeelnemers met zich meebrengt. De definitie van 'op de markt aanbieden' is: het "in het kader van een handelsactiviteit, al dan niet tegen betaling," verstrekken van een product met digitale elementen met het oog op distributie of gebruik op de markt van de Unie. Uit de voorwaarde dat het product met digitale elementen 'in het kader van een handelsactiviteit' moet zijn verstrekt om onder de CRA te vallen is af te leiden dat niet-commerciële software er niet onder valt. De bijbehorende overweging 10 gaat daarbij in op omstandigheden waaronder er bij open source sprake al dan niet is van een handelsactiviteit. Het kabinet hecht eraan dat deze omstandigheden verder wordt verduidelijkt.

De leden merken ook op dat veel vrije en open source software die gratis beschikbaar wordt gemaakt buiten handelsactiviteit vervolgens weer gebruikt wordt in commerciële producten door andere partijen. Veel software waar veel mensen (indirect) van afhankelijk zijn, wordt (grotendeels) ontwikkeld door vrijwilligers. Zou de regering willen pleiten voor het toevoegen van prikkels voor commerciële partijen om (semi-)vrijwillige upstream-opensourcesoftware-

ontwikkelaars te ondersteunen in het realiseren van de verplichtingen van de Cyber Resilience Act (CRA)?

Antwoord
Een product met digitale elementen waaronder ook losse software- of hardwarecomponenten worden verstaan) valt afhankelijk van de vraag of het in het kader van een handelsactiviteit is verstrekt, al dan niet onder de CRA. Een component dat niet in het kader van een handelsactiviteit is verstrekt (zoals niet-commercieel aangeboden open source software) valt niet onder de CRA. Zoals de regering het voorstel nu begrijpt, verplicht artikel 10, lid 4, de fabrikant om met het oog op de naleving van cybersecurity-eisen die in in artikel 10, lid 1, aan zijn product worden gesteld, om 'de nodige zorgvuldigheid te betrachten' (in het Engels: due diligence) bij de integratie van van derden afkomstige componenten in producten met digitale elementen. Zij zorgen ervoor dat dergelijke componenten de veiligheid van het product met digitale elementen dat zij aanbieden, niet in gevaar brengen. Het voorstel legt de eindverantwoordelijkheid voor de cybersecurity van een samengesteld product met andere woorden niet volledig bij de fabrikant van het samengestelde product. Artikel 11, lid 7, van het voorstel schrijft voor dat de fabrikant bij de vaststelling van een kwetsbaarheid in een component die in zijn product is geïntegreerd, deze kwetsbaarheid moet melden aan de persoon of entiteit die de component onderhoudt. De regering onderzoekt nog of en zo ja op welke manier er in de CRA een prikkel zouden moeten worden ingevoegd voor commerciële fabrikanten van digitale producten die niet-commerciële open source componenten gebruiken in hun product, om de ontwikkelaars van niet-commerciële componenten te ondersteunen in het veilig houden van deze componenten.

Handhaving
De leden constateren dat naast de CRA er ook een nieuwe productaansprakelijkheidsrichtlijn voorgesteld is. Is de regering van mening dat de CRA, in combinatie met de nieuwe productaansprakelijkheidsrichtlijn en andere wet- en regelgeving, voldoende mogelijkheden biedt voor eindgebruikers om nakoming van de verplichtingen uit de CRA af te dwingen? Welke onderdelen vindt de regering ver genoeg gaan, en welke kunnen nog verbeterd worden?

Antwoord
De verplichtingen waar producenten, importeurs en distributeurs aan moeten voldoen worden geregeld in de CRA zelf. Het vastleggen van duidelijke essentiële beveiligingseisen aan digitale producten en vereisten voor de respons op kwetsbaarheden in de CRA zal eindgebruikers, zowel consumenten als zakelijke gebruikers, veel beter in staat stellen om de nakoming hiervan af te dwingen. Ook wordt geregeld dat er effectief toezicht wordt gehouden op de naleving ervan, waarbij toezichthouders ook klachten van consumenten kunnen betrekken bij hun toezichtbeleid.
De huidige richtlijn productaansprakelijkheid ziet op aansprakelijkheid jegens consumenten, anders dan op basis van overeenkomst. De richtlijn regelt dat een producent aansprakelijk is voor schade die is veroorzaakt door een gebrek in zijn product. De richtlijn gaat over alle producten, waaronder medicijnen, auto's en producten met software. De richtlijn ziet kort gezegd op letsel- en overlijdensschade en schade aan producten die in de privésfeer worden gebruikt. Of er sprake is van een gebrek dient volgens de richtlijn te worden beoordeeld aan de hand van de omstandigheden van het geval. De richtlijn productaansprakelijkheid wordt op dit moment herzien, zoals de vraagstellers

terecht opmerken. In het voorstel daartoe wordt onder meer voorgesteld software als een product aan te merken. Ook wordt verduidelijkt dat bij de vraag of er sprake is van een gebrekkig product, "de productveiligheidsvoorschriften" in aanmerking moeten worden genomen, waaronder "de veiligheidsgerelateerde cyberbeveiligingsvoorschriften". Tijdens de onderhandelingen zal Nederland erop toezien dat de samenhang tussen de beide voorstellen zo goed mogelijk wordt gewaarborgd. Voor aansprakelijkheid op grond van overeenkomst tussen de consument en de verkoper kan overigens ook worden gewezen op de richtlijn verkoop goederen die ook ziet op goederen met digitale elementen. Deze richtlijn regelt dat bij niet-nakoming van de koopovereenkomst de consument de verkoper kan aanspreken die weer terecht kan bij zijn leverancier.

Levensduur
De leden zijn blij om te lezen dat de verordening een verplichting inhoudt om voor een bepaalde duur kwetsbaarheden op te lossen. Deze duur is echter beperkt tot de productlevenscyclus van vijf jaar, wat het kortste is. De leden merken op dat dit een ongelukkig gekozen termijn is, omdat dit mogelijk verspilling in de hand werkt. Veel fysieke producten zijn immers afhankelijk van veilige software en moet langer dan vijf jaar mee kunnen gaan. Een langere termijn zou kunnen zorgen voor meer ambitie en zo resulteren in veiligere én duurzamere producten. Is de regering het eens dat de termijn waarin updates moeten worden verstrekt voor fysieke producten beter niet begrenst kan worden om verspilling te voorkomen en hergebruik te stimuleren? In het BNC-fiche merkt de regering op dat zij van plan is om verheldering te vragen over de keuze voor de termijn om kwetsbaarheden op te lossen. De leden vragen wat de regering vindt van deze termijn en horen graag welke voor- en nadelen de regering ziet bij het hanteren van deze termijn. Als de regering geen voorstander is van de huidige termijn, bedoelt zij hier dan mee dat ze de maximering van de termijn het liefst geschrapt ziet worden? Is de regering het ermee eens dat een termijn die slechts gebaseerd is op de productlevenscyclus beter is, omdat dit beter aansluit op de bestaande regels over updateplichten tegenover consumenten, maar ook omdat dit beter aansluit bij de duurzaamheidsdoelen van Nederland en de EU?

Antwoord
Een argument voor het hanteren van een maximumtermijn kan zijn dat het voor producenten een lagere drempel geeft om nieuwe innovatieve producten op de markt te brengen omdat de hoeveelheid bijkomende verplichtingen dan voorspelbaar is en voor een beperkte duur is. Het kabinet hecht er echter aan om aan te sluiten bij de volledige levensduur van het product, en is geen voorstander van maximering van de ondersteuningstermijn. Een maximale beschermingstermijn van vijf jaar zou een ongewenste prikkel kunnen geven voor producenten om hun producten niet langer mee te laten gaan dan deze vijf jaar, hetgeen niet past bij de duurzaamheidsdoelen van Nederland en de EU. Daarnaast is een termijn van vijf jaar onvoldoende om bescherming voor alle categorieën van digitale producten te waarborgen, zoals producten in industriële toepassingen. Zoals terecht wordt opgemerkt geldt bovendien een verplichting voor verkopers voor het verstrekken van (beveiligings)updates voor goederen met digitale elementen, digitale inhoud en digitale diensten op grond van de richtlijn verkoop goederen (2019/771) en de richtlijn levering digitale inhoud (2019/770). Deze richtlijnen stellen dat updates geleverd moeten worden gedurende de periode die de consument redelijkerwijs kan verwachten, gezien de aard en het doel van goederen met digitale elementen, dan wel de digitale inhoud en diensten. Het betreft dus een open Europese norm. Als in de CRA een maximumtermijn voor

verplichte ondersteuning wordt gehanteerd en deze termijn korter is dan de periode waarin de verkoper op grond van de richtlijnen verkoop goederen en levering digitale inhoud verplicht is om updates te verstrekken, kan de verkoper lastiger aan die verplichting voldoen. Het kabinet pleit bij de onderhandelingen daarom voor een alternatief waarbij wordt aangesloten bij de verwachte productlevensduur. Daarbij wordt de periode waarin updateverplichtingen voor consumenten gelden ook meegenomen.

Daarnaast zullen gebruikers na het einde van deze wettelijke ondersteuningstermijn mogelijk gebruik willen blijven maken van het product met digitale elementen. Welke mogelijkheden biedt de CRA aan gebruikers om te zorgen dat ze ook na deze termijn veiligheidsupdates kunnen krijgen, eventueel van een andere partij dan de oorspronkelijke fabrikant?

Antwoord
In het voorstel voor de CRA zijn geen bepalingen opgenomen over veiligheidsupdates na afloop van de ondersteuningstermijn. Het staat gebruikers vrij om contractueel langere ondersteuningstermijnen overeen te komen met fabrikanten. Voor veel gebruikers is dit echter moeilijk af te dwingen als zij in een zwakkere onderhandelingspositie staan, daarom hecht het kabinet aan een ondersteuningstermijn die overeenkomt met wat de gebruiker redelijkerwijs van de productlevensduur mag verwachten. Het kabinet zal op dit punt om verheldering vragen en daarnaast inzetten op een verplichting voor fabrikanten om de door de fabrikant gegarandeerde ondersteuningstermijn duidelijk op de verpakking te vermelden zodat de gebruiker er zijn aanschaf van het product met digitale elementen mede op kan baseren. Dit kan voor fabrikanten een prikkel vormen om zich te onderscheiden met een langere ondersteuningstermijn.

Hoe kijkt de regering ernaar om een verplichting te stellen om broncode, inclusief voorbereidend materiaal zoals toolchains en compilatiegegevens, na een bepaalde termijn beschikbaar te moeten stellen als een fabrikant geen veiligheidsupdates meer wil leveren? De leden erkennen dat dit wellicht een onorthodox middel is, maar het zou wel innovatie kunnen promoten omdat door derden verder wordt gebouwd.

Antwoord
Het kabinet onderzoekt zoals gezegd mogelijkheden om tot een effectievere ondersteuningstermijn te komen zodat gedurende de hele levenscyclus van een product veiligheidsupdates beschikbaar worden gesteld. Dit zou in combinatie met de in het voorstel opgenomen bepalingen voor handhaving en sancties voldoende moeten zijn om digitale veiligheid van producten te garanderen. Bij een verplichting om broncode beschikbaar te stellen zou ook moeten worden meegewogen het belang bij bescherming van intellectueel eigendom dat fabrikanten hebben wanneer zij investeren in innovatie, en de nadelige gevolgen voor innovatie die een dergelijke verplichting aldus zou kunnen hebben. Tot slot zal het beschikbaar stellen van de broncode en voorbereidend materiaal niet per definitie leiden tot tijdige ontwikkeling van veiligheidsupdates door derden, en moet ook het risico op misbruik van dergelijke openbaarmaking door kwaadwillenden worden meegewogen.

Vragen van de leden van de fractie van D66
Met belangstelling hebben de leden van de D66-fractie kennisgenomen van het voorstel voor een verordening met betrekking tot horizontale

cyberbeveiligingsvereisten. Zij onderschrijven de grondgedachte, maar hebben hier in dit stadium al enkele vragen over.
De CRA heeft een tweeledige hoofddoelstelling. De vraag van de leden van de D66-fractie is in hoeverre bestaande Nederlandse wetgeving met betrekking tot digitale producten door de nieuwe normen uit de CRA wordt geraakt.
Meer in het bijzonder vragen de leden van de D66-fractie of er raakvlakken zijn met de Wet Digitale Overheid (WDO) en de CRA. Of valt hetgeen de WDO regelt onder de uitzondering "open source software, waar geen economische activiteit aan is gekoppeld"?

Antwoord
De bestaande Nederlandse wetgeving met betrekking tot digitale producten betreft geharmoniseerde Europese regelgeving. Het gaat dan bijvoorbeeld over de Uitvoeringswet Cyberbeveiligingsverordening, de implementatie van de Radioapparatenrichtlijn (ook wel Radio Equipment Directive of RED), en de implementatiewet richtlijnen verkoop goederen en levering digitale inhoud. Een goede aansluiting van de CRA op andere Europese regelgeving heeft de aandacht tijdens de onderhandelingen. Er zijn geen directe raakvlakken tussen de CRA en de WDO.

De CRA introduceert ex-post-verplichtingen. De fabrikant moet voor een periode van vijf jaar garanderen dat kwetsbaarheden van het product blijven voldoen aan de essentiële voorwaarden die in Annex I zijn vermeld. Wat de leden van de D66-fractie nog niet duidelijk is, is of de regeling van de CRA een eerbiedigende werking heeft. Met andere woorden: gelden de CRA-verplichtingen alleen voor digitale producten die na de inwerkingtreding van de nieuwe regels worden gefabriceerd en op de markt komen of gelden de verplichtingen ook voor producten van daarvoor, die al in gebruik zijn?

Antwoord
De CRA heeft inderdaad een eerbiedigende werking. De verplichtingen gelden op grond van artikel 55, tweede lid, van het voorstel voor producten met digitale elementen die na de inwerkingtredingsdatum in de handel zijn gebracht, maar ook voor reeds eerder in de handel gebrachte producten die na deze datum ingrijpend zijn gewijzigd met betrekking tot het ontwerp of het beoogde doel. Een uitzondering hierop is artikel 11 van het voorstel, waarin de meldplicht voor fabrikanten bij actief geëxploiteerde kwetsbaarheden is opgenomen. Deze geldt vanaf de inwerkingtredingsdatum voor alle producten met digitale elementen die binnen het toepassingsgebied van de CRA vallen, ongeacht wanneer ze in de handel zijn gebracht (zie artikel 55, derde lid, van het voorstel).

Het begrip 'producten met digitale elementen' is wat de leden van de D66-fractie betreft nogal diffuus. Hoe gaat de regering er zorg voor dragen dat hier meer duidelijkheid over komt?

Antwoord
Voor het kabinet is inmiddels door de Europese Commissie voldoende inzichtelijk gemaakt dat alle hard- en software onder de CRA valt, met uitzondering van software die als clouddienst wordt aangeboden (Saas), en niet-commercieel aangeboden producten met digitale elementen (zoals niet-commerciële open source software). Het kabinet is echter wel van mening dat teksten over deze uitzonderingen verdere verduidelijking behoeven, zodat ook in de sector voldoende juridische duidelijkheid wordt geboden. Het kabinet is hierover in

gesprek met de Europese Commissie, het voorzitterschap van de Raad van de EU en de digitale sector.

De regering schrijft dat zij opheldering gaat vragen over allerlei afbakeningskwesties met huidige wetgevingsvoorstellen. De leden van de D66-fractie zien dat de regering nog veel punten over de CRA opgehelderd wil krijgen en daar vragen over stelt. Zij wachten met belangstelling de antwoorden daarop af. Kan de regering een indicatie geven wanneer de inhoudelijke beantwoording van de vragen van de regering te verwachten is?

Antwoord
In het voorgaande antwoord is ingegaan op de afbakening van 'producten met digitale elementen'. Over andere afbakeningskwesties, zoals de verhouding met andere Europese wetgeving op het terrein van digitale veiligheid, verwacht het kabinet gedurende het Zweedse voorzitterschap van de Raad van de EU, dat tot en met juni 2023 duurt, helderheid te krijgen.

De leden van de D66-fractie constateren dat er door de verplichtingen van de CRA behoorlijk wat extra werk en kosten op het bord van het midden- en kleinbedrijf (MKB) terechtkomt. Is de regering niet bevreesd dat de positie van het MKB hierdoor verzwakt raakt, terwijl dat niet de bedoeling van de CRA is?

Antwoord
Het zo beperkt mogelijk houden van de regeldruk voor het mkb is een aandachtspunt voor het kabinet. De mogelijkheid tot zelfverklaring voor naar verwachting 90 procent van de digitale producten versus het uitvoeren van de conformiteitsbeoordeling door een derde partij draagt hieraan bij. Doordat ook digitale componenten onder de CRA vallen wordt het veilig houden van digitale productieketens ook gereguleerd. Daarmee draagt de CRA ook bij aan een sterkere positie voor het mkb als afnemer en gebruiker van producten met digitale elementen omdat hun toeleveranciers aan dezelfde verplichtingen moeten voldoen. Daarnaast draagt de CRA bij aan de concurrentiepositie van het mkb omdat een gelijk speelveld wordt gecreëerd voor alle producten met digitale elementen op de Europese interne markt.

De regering wil het toezicht en de handhaving van de regels in de CRA beleggen bij het Agentschap Telecom (AT). Nu het om een uitbreiding van de taken gaat, onderkent de regering dat er investeringen nodig zullen zijn in de capaciteit en expertise bij de AT om passend toezicht in te kunnen richten. Is hier bij de begroting voor de komende jaren rekening mee gehouden? Bij welk departement komt deze post te liggen?

Antwoord
Deze post komt te liggen bij het ministerie van EZK. Voor een gerichte schatting van de benodigde capaciteit voor de Rijksinspectie Digitale Infrastructuur (RDI, voorheen AT) is eerst meer helderheid nodig over de verplichtingen die uiteindelijk in de CRA worden vastgelegd. Het is nog vroeg in het onderhandelingsproces; over toezicht en handhaving moet binnen de Raad nog nadere discussie gevoerd worden. Na vaststelling van de wettekst gaat een implementatietermijn in. Die is in het voorstel vastgelegd op 24 maanden. Daarmee is nog voldoende tijd voor het begroten van de kosten.

De verordening heeft tot doel om de consument meer te informeren over cyberveiligheid van een product. De leden van de D66-fractie vragen de regering in hoeverre zij al een plan heeft om de informatiecampagne vorm te geven. Hoe probeert de regering dit in begrijpelijke taal voor consumenten te bewerkstelligen?

Antwoord
Het vergroten van het bewustzijn van cyberrisico's van burgers is een van de doelstellingen van de NLCS onder Pijler IV: Cybersecurity-arbeidsmarkt, onderwijs en de digitale weerbaarheid van burgers. Een belangrijk instrument dat het kabinet hiertoe inzet zijn verschillende doelgroep specifieke voorlichtingscampagneprogramma cyberveiligheid gericht op de cybersecurity basismaatregelen. Dit komt tot uiting in publiekcampagnes zoals 'Doe je updates', die zich richt op de veiligheid van slimme apparaten. Daarnaast biedt veiliginternetten.nl consumenten informatie en advies over wat zij kunnen doen en laten op het gebied van cybersecurity. Het is echter nog te vroeg in het onderhandelingsproces om te bezien of en wat voor informatiecampagnes er gewenst zouden zijn voor de CRA.

In hoeverre, zo vragen de leden van de D66-fractie, is de conformiteitstoets voldoende flexibel om mee te bewegen met de technologische ontwikkelingen? Kan er snel worden opgetreden tegen eventuele nieuwe gevaren door technologische ontwikkelen?

Antwoord
Bij de conformiteitsbeoordeling wordt getoetst of het product aan bepaalde essentiële eisen voldoet zoals opgenomen in productregelgeving. Voor de essentiële eisen wordt waar mogelijk gebruik gemaakt van terminologie die technologieonafhankelijk is, waarmee de toekomstbestendigheid van de conformiteitsbeoordeling in de CRA wordt bevorderd. In normen worden die essentiële eisen in technische bewoordingen uitgewerkt. Indien aan Europese geharmoniseerde normen wordt voldaan is er een vermoeden van conformiteit met de CRA. Geharmoniseerde normen komen tot stand in samenwerking met het bedrijfsleven in Europese standaardisatieorganisaties. Hiermee wordt geborgd dat de normen aansluiten bij de praktijk. Normen zijn relatief flexibel en worden met regelmaat herzien in het licht van technologische vooruitgang zonder de noodzaak om daarvoor regelgeving te wijzigen. Door deze flexibiliteit wordt de toekomstbestendigheid van de conformiteitstoets in de CRA geborgd en worden eventuele nieuwe toekomstige gevaren van technologische ontwikkelingen ondervangen.

Vragen van de leden van de fractie van de PVV
Kunt u een schatting geven van de totale kosten die het Nederlandse bedrijfsleven (op jaarbasis) door het voorstel voor haar kiezen krijgt, waarbij rekening wordt gehouden met de omvang van de bedrijven en de sectoren waarin zij opereert, alsmede aan welke ondersteunende maatregelen moet worden gedacht?

Antwoord
Zoals uiteengezet in het BNC-fiche maakt het impact assessment van de Commissie zowel de financiële consequenties en verhoogde regeldruk voor het bedrijfsleven inzichtelijk, als de baten voor de verschillende stakeholders en de samenleving als geheel. De totale nalevingskosten in de hele EU schat de Commissie in op ongeveer 29 miljard euro op een totale marktomzet van 1485

miljard euro per jaar, een inschattting voor specifiek het Nederlandse bedrijfsleven is niet beschikbaar. De nalevingskosten voor een bedrijf zullen variëren en zijn afhankelijk van de complexiteit en omvang van het product, de bestaande cybersecurity praktijk van een bedrijf, de omgeving (business-to-consumer of business-to-business) en de omvang van het bedrijf. Dit geldt voor zowel het mkb als grote bedrijven en is afhankelijk van hun rol in de digitale economie. De gemiddeld geschatte kosten van een zelfassessment zijn 18.400 euro en een conformiteitsbeoordeling door een derde partij zijn 25.000 euro. De Commissie verwacht dat het aantal cybersecurity-incidenten met producten met digitale elementen met bijkomende incidentresponskosten en reputatieschade met 33% vermindert. Voor de hele EU verwacht de Commissie een kostenbesparing als gevolg van incidenten van rond de 180 miljard per jaar tot 290 miljard euro per jaar. Het is aannemelijk dat bedrijven de verhoogde kosten zullen doorberekenen in hun prijs naar gebruikers (organisaties en consumenten). Dit moet worden afgewogen tegen de baten van gebruikers van verhoogde transparantie, dat producten met digitale elementen die zij afnemen standaard veiliger zijn en hun fundamentele rechten zoals privacy en bescherming van hun data ook beter zijn geborgd. Het kabinet heeft de Commissie om verduidelijking gevraagd omtrent mogelijke ondersteunende maatregelen voor met name het mkb.

Kunt u een specifieke opsomming geven van alle bevoegdheden die de Europese Commissie krijgt via gedelegeerde handelingen door voorliggend voorstel, alsmede hoe deze bevoegdheden eventueel weer kunnen worden teruggedraaid?

Antwoord
In onderdeel 6b van het BNC-fiche zijn deze bevoegdheden opgesomd. Specifiek met betrekking tot gedelegeerde handelingen bevat het voorstel de volgende bevoegdheden voor de Commissie:

- Het wijzigen van de verordening om producten met digitale elementen die onder andere EU-wetgeving met een gelijk beschermingsniveau uit te sluiten van de CRA (artikel 2, lid 4)
- Het actualiseren van de lijst van categorieën van kritieke producten met digitale elementen in Annex III en het specificeren van definities van deze producten (artikel 6, lid 2 en 3)
- Het identificeren van producten met digitale elementen waarvoor andere Unie wetgeving hetzelfde beschermingsniveau als de CRA garandeert, het vervolgens specificeren of een beperking of uitzondering van de reikwijdte van de verordening nodig is en, indien nodig, de reikwijdte van de beperking te bepalen (artikel 6, lid 5)
- De mogelijkheid om certificering te verplichten van bepaalde hoog kritieke producten met digitale elementen op basis van beoordelingscriteria die in de verordening staan (artikel 20, lid 5)
- Het specificeren van de minimale hoeveelheid informatie in de EU verklaring van conformiteit (artikel 20, lid 5)
- Het aanvullen van elementen die onderdeel moeten zijn van de technische documentatie (artikel 23, lid 5)

Het Europees Parlement of de Raad kan deze bevoegdheidsdelegatie te allen tijde intrekken en zo de delegatie van een bevoegdheid beëindigen. Het besluit laat de geldigheid van reeds van kracht zijnde gedelegeerde handelingen onverlet (artikel 50, lid 3).

Kunt u aangeven, kijkende naar de opmerking dat de meeste lidstaten het voorstel in de basis lijken te steunen, welke lidstaten het voorstel in de basis niet lijken te steunen en wat hun argumentatie is? Graag een gemotiveerd antwoord met zoveel mogelijk details.

Antwoord
Tot nu toe zijn er in de onderhandelingen voor de CRA nog geen lidstaten geweest die zich tegen de CRA hebben uitgesproken. Hiervoor verwijs ik graag naar het verslag van de Telecomraad van 6 december 2022 (TK 21501-33, nr. 1001).

Vragen van het lid van de fractie van de OSF
Het lid van de OSF heeft kennisgenomen van het voorstel om sectorbreed de digitale beveiliging te verhogen en daarmee de algehele ICT-infrastructuur minder kwetsbaar te maken. Hij ziet deze verordening als het toevoegen van het recht op cyberbeveiliging en stellen van een updateverplichting. In afwachting van de expertmeeting die de Tweede Kamer der Staten-Generaal organiseert, zijn er wel meerdere onduidelijkheden die voortkomen uit de verordening en de zienswijze van de regering verwoord in de BNC-fiche, welke het lid graag meer verhelderd zou willen zien.

Spoorboekje
De implementatie van de CRA zal nog vele stappen vergen totdat het gewenste niveau van horizontale cyberbeveiliging zal worden bereikt. Welke stappen zullen er moeten worden genomen? Welke voorstellen worden er aangekondigd? Welke criteria worden vast- en/of bijgesteld? En hoe wordt ook deze Kamer betrokken bij de realisatie en evaluatie?

Antwoord
Eerst zullen de Europese onderhandelingen voor de CRA moeten worden afgerond. Dat betekent dat er eerst een gezamenlijke positie op het voorstel geformuleerd moet worden door de Raad van de EU. Daarna gaan de Raad en het Europees Parlement met elkaar in onderhandeling over de tekst. Wanneer beide hebben ingestemd, gaat de in het voorstel opgenomen implementatietermijn lopen, zodat bedrijven en overheidsinstanties tijd hebben om zich voor te bereiden op uitvoering van de wet. In die periode zullen de geharmoniseerde normen worden uitgewerkt door de Europese standaardisatieorganisaties. Voor inhoud van de CRA verwijs ik graag naar het op 21 oktober 2022 verschenen BNC-fiche. Uw Kamer zal, samen met de Tweede Kamer, over de onderhandelingen worden geïnformeerd in aanloop naar en na afloop van de Telecomraad. Daarnaast wordt de Tweede Kamer geïnformeerd over de CRA bij de voortgangsrapportage van de Nederlandse Cybersecuritystrategie.

Aanvullend, welke route wordt geboden voor Nederlandse initiatieven om ook op Europese schaal uitvoerbaar te worden? Hierbij kunnen we bijvoorbeeld denken aan (aanvullende) richtlijnen, implementaties en ook (subsidie)regelingen.

Antwoord
Binnen het onderhandelingsproces voor de CRA heeft Nederland de ruimte om zelf voorstellen te doen voor invulling van de CRA. Het kabinet is positief over het voorstel voor de CRA, en heeft in 2021 en 2022 actief aandacht gevraagd voor het belang van horizontale wetgeving om de veiligheid van digitale producten te versterken. Naast de CRA bestaan er verschillende Europese subsidieregelingen waar de digitale sector gebruik van kan maken, zoals Horizon Europe en Digital

Europe. Vooralsnog zijn er geen aanvullende Nederlandse initiatieven voorzien die op Europese schaal uitvoerbaar gemaakt zouden moeten worden.

Voorziet de regering de wens en de mogelijkheid om een bredere procedure te doorlopen? Hierbij kan gedacht worden aan bijvoorbeeld meervoudige consultatie of installatie van een adviesorgaan vanuit de sector. Een bredere procedure, mogelijk zelfs cyclisch, zou kunnen bijdragen aan de (door)ontwikkeling van de criteria en de sectorbrede voorlichting van de standaard die wordt nagestreefd. Ook om, in de reikwijdte van de CRA, in afstemming te blijven/brengen met andere Unie wetgevingsinstrumenten.

Antwoord
Het kabinet ziet geen toegevoegde waarde in een nieuw adviesorgaan vanuit de sector. De bestaande Cyber Security Raad en informele rondetafels met de sector voorzien hier in voldoende mate in. Door de Europese Commissie is, voorafgaand aan de publicatie van de verordening, in 2022 een publieke consultatie georganiseerd waarop vanuit de sector is gereageerd.

Cyberbeveiliging betreft zeer specialistische kennis, terwijl volksvertegenwoordiging in veel gevallen een lekenbestuur is. Zeker op dit vakgebied. Op welke wijze wordt gewaarborgd dat de CRA als beleid ook uitvoerbaar zal zijn? Hoe wordt voorkomen dat deze verordening flopt?

Antwoord
In de consultatiefase voor de CRA heeft de Europese Commissie bedrijven uit verschillende sectoren de gelegenheid gegeven om mee te denken over de invulling van de wet. In Nederland zijn uitvoeringsinstanties als RDI en Nationaal Cyber Security Centrum (NCSC) betrokken bij de beoordeling van het voorstel. Het kabinet heeft onder meer door middel van informele rondetafels voeling met hoe het bedrijfsleven over de uitvoerbaarheid van de CRA denkt. De Europese Commissie zal regelmatig openbare evaluatieverslagen delen met de Raad en het Europees Parlement. Op basis hiervan of van andere signalen, kan de Europese Commissie indien nodig overgaan tot een herziening van de wet.

Er is veel geschaad vertrouwen als het gaat om overheden en haar ICT-projecten. Hoe wil de regering haar geloofwaardigheid herwinnen/bewijzen, zodat ze ook sectorbreed steun krijgt om met deze verordening de cyberbeveiliging daadwerkelijk naar een hoger niveau te tillen?

Antwoord
De CRA ziet niet op ICT-projecten van de overheid. Door goed contact te houden met de sector en uitvoerders, en door een actieve opstelling in de onderhandelingen, verwacht het kabinet bij te kunnen dragen aan een uitvoerbare CRA doe zorgt voor veiligere digitale producten en daarmee voor digitaal weerbaardere burgers en organisaties.

<u>Certificering en label</u>
Het lid van de OSF ziet deze verordening in het kader van een bewustwordingscampagne om te zorgen dat 'security-first' producten worden geleverd. Dit is een intrinsieke verplichting die de leverancier met liefde voor zijn product zou moeten realiseren. Hoe voorkomt de regering dat er met het certificaat een schijnveiligheid wordt gecreëerd dat de beveiliging op orde is?

Deelt de regering het standpunt dat voor een bewustwordingscampagne van de sector het afdoende kan zijn om certificering op vrijwillige basis te laten uitvoeren, zodat bedrijven de kosten waar nodig kunnen verrekenen door zo een hoogwaardiger digitaal product te leveren? Of: waarin zit de (proportionele) meerwaarde/noodzaak om de sector te verplichten te certificeren en te conformeren, met mogelijkheid van handhaving?

Antwoord
Het is essentieel dat eindgebruikers erop kunnen vertrouwen dat een product dat op de markt is geplaatst veilig is. Een hoger niveau van cybersecurity van producten met digitale elementen komt zonder regulering onvoldoende tot stand, zoals ook wordt onderstreept in het rapport van de Onderzoeksraad voor Veiligheid 'Kwetsbaar tot software'. De cybersecurity van producten met digitale elementen is nog grotendeels ongereguleerd, waardoor de verantwoordelijkheid in de praktijk vooral bij de gebruiker komt te liggen. In de Nederlandse Cybersecurity Strategie is een van de doelstellingen dat digitale producten en diensten veiliger moeten worden en stelt het kabinet dat herschikking van verantwoordelijkheden nodig is. De CRA is een belangrijk instrument om de verantwoordelijkheden van fabrikanten, importeurs en distributeurs vast te leggen en een gelijk speelveld te creëren voor aanbieders.
Conformiteitsbeoordelingen zijn in deze aanpak van groot belang. Producten met digitale elementen zullen onder de CRA worden voorzien van een CE-markering en gaan gepaard met een EU-conformiteitsverklaring. Hiermee geeft de fabrikant aan dat het product voldoet aan de essentiële cybersecurity-eisen van de CRA en op deze eisen is getest volgens de voorgeschreven conformiteitsbeoordeling. De verplichtingen zijn niet alleen bedoeld als bewustwordingscampagne voor fabrikanten, maar introduceren een kader dat de naleving van de cybersecurityvereisten en een goede procedure voor de respons op geconstateerde kwetsbaarheden afdwingbaar maakt. De markttoezichtautoriteiten zullen erop toezien dat de conformiteitsbeoordeling juist is verricht en dat geëxploiteerde kwetsbaarheden tijdig worden gemeld en opgelost. Hiermee wordt de veiligheid geborgd voor de eindgebruikers en schijnveiligheid voorkomen.
Voor de meeste producten kan de producent daarbij volstaan met een zelftoetsing, of op vrijwillige basis kiezen voor certificering door een derde partij, bijvoorbeeld als de afnemers van hun producten daar om vragen. Voor de kritieke producten met digitale elementen die worden opgesomd in Annex III van de CRA geldt dat niet met zelftoetsing kan worden volstaan. Voor deze producten doet een derde partij een onafhankelijke toetsing en moet een van de conformiteitsbeoordelingsprocedures in artikel 24, lid 3, van het voorstel worden gevolgd.

<u>Handhaving</u>
In het voorstel blijft onduidelijk hoe en met welke reikwijdte en daadkracht de CRA zal worden gehandhaafd. In het arsenaal van middelen die nodig zouden kunnen zijn, zou ook kunnen geworden gedacht aan handelingen die (momenteel) voorbehouden zijn tot het nationale recht. Kan de regering inzicht geven op de rechtsgevolgen die er kunnen voortkomen in de naleving van de CRA dan wel schenden van de CRA?

Antwoord
Artikel 53 van het voorstel bepaalt dat lidstaten in hun nationale recht moeten uitwerken welke bevoegdheden de nationale markttoezichthouder krijgt om de regels van de CRA te handhaven, met straffen die effectief, proportioneel en

afschrikwekkend moeten zijn. De wet ter uitvoering van de markttoezichtverordening ziet er op toe dat de markttoezichtautoriteiten de juiste bevoegdheden hebben om relevante documentatie over het product en de conformiteit van het product op te vragen bij marktdeelnemers, (onaangekondigd) documentencontroles en fysieke controles te houden en verdere onderzoeken in te stellen die benodigd zijn om conformiteit vast te stellen. Daarbij hebben de markttoezichtautoriteiten de bevoegdheid passende corrigerende maatregelen te nemen, zoals het aanbieden van een product op de markt te verbieden en het opleggen van sancties, waaronder geldboetes. De voorschriften voor de vaststelling van sancties valt onder het nationaal recht. De hoogte van de bestuursrechtelijke boetes die bij niet-naleving van de CRA kunnen worden opgelegd zijn ook in artikel 53 van het voorstel uitgewerkt, met maxima tot 15 miljoen euro of tot 2,5 procent van de totale wereldwijde jaarlijkse omzet.

Kijkende naar de implementatie van de Algemene Verordening Gegevensbescherming (AVG) is het heel belangrijk hoe voortvarend de handhaving wordt opgezet. Deelt de regering het standpunt dat er afdoende capaciteit dient te worden ingericht bij het toezichthoudende orgaan? Wat is afdoende? Welk budget dient begroot te worden en hoe groot zal de Europese bijdrage zijn?

Antwoord
Ja, het kabinet deelt het standpunt dat toezichthouders over voldoende capaciteit moeten beschikken. Aangezien het nog vroeg in het onderhandelingsproces is, is het nog niet goed mogelijk in te schatten wat afdoende capaciteit is voor een goede handhaving van de CRA. Implementatie van de CRA zal bekostigd worden uit de rijksbegroting.

Hoe wordt de grensoverschrijdende samenwerking vormgegeven? Hoe worden zogenaamde 'kastje-muur problemen' opgelost wanneer een gebruiker of melder zich in een ander land (dus onder een andere toezichthouder) bevindt dan het bedrijf dat het product of de dienst aanbiedt?

Antwoord
Markttoezichtautoriteiten werken veel grensoverschrijdend samen om non-conformiteit van producten tegen te gaan. Markttoezichtautoriteiten wisselen bijvoorbeeld voortdurend informatie met elkaar uit via het "Information and Communication System on Market Surveillance" en kunnen elkaar ondersteunen met onderzoeken. Markttoezichtautoriteiten hebben enkel bevoegdheden in hun eigen lidstaat. De markttoezichtautoriteit kan bij markttoezichtautoriteiten in andere lidstaten een informatieverzoek indienen om toegang tot informatie van de marktdeelnemer af te kunnen dwingen, en wanneer handhavingsmaatregelen in een andere lidstaat nodig zijn kan de markttoezichtautoriteit een gemotiveerd verzoek tot handhaving indienen bij een autoriteit in deze lidstaat. Artikel 48 en 49 van het voorstel voorzien tot slot in mogelijkheden om gezamenlijke activiteiten uit te voeren en zogenaamde bezemacties uit te voeren waarin gelijktijdige gecoördineerde controleacties plaatsvinden voor bepaalde digitale producten of categorieën digitale producten.

<u>Faillissementen en bedrijfsbeëindiging</u>
De verordening ziet op de actuele relatie van de aanbieder en de afnemer. Hierin zijn faillissementen en bedrijfsbeëindiging onbesproken factoren die de haalbaarheid van de doelstellingen van de verordening onder druk zetten. Op

welke wijze dienen de rechten voor gebruikers te worden voortgezet indien de aanbieder verdwijnt wegens faillissement of bedrijfsbeëindiging? Deelt de regering het standpunt dat kritieke infrastructuur moet worden voortgezet ook nadat de leverancier niet meer in beeld is? Welke definitie van 'kritiek' past ze toe? Hoe ziet de regering dat voor zich, vooral met het oog op zogenaamde 'proportairy software' en merken-/auteursrecht. Zou het wenselijk zijn dat binnen deze verordening de mogelijkheid wordt geboden dat — via de rechter en executeur van het faillissement — deze vervalt aan het publieke domein en voort kan bestaan als zogenaamde 'open source'? Of kan worden verkocht aan andere aanbieders? Welke continueringsverplichtingen zouden kunnen worden gesteld?

Antwoord
Artikel 10, lid 14, van het voorstel bepaalt dat in het geval een fabrikant (om welke reden dan ook) zijn activiteiten stopzet en daardoor niet in staat is aan de verplichtingen te voldoen, dit voordat het zover is moet melden aan de markttoezichtautoriteiten en, met alle beschikbare middelen en voor zover mogelijk, aan de gebruikers van de betrokken producten. Een soortgelijke verplichting is in artikel 13, lid 9, en artikel 14, lid 6, opgenomen voor de importeur repectievelijk distributeur van producten afkomstig van een fabrikant die zijn activiteiten stopzet. Het kabinet is nog aan het bestuderen of en op welke wijze en door wie vervolgens de cybersecurity van deze producten kan worden geborgd en wat hierover in de CRA zou moeten worden opgenomen. Hierover zal het kabinet in gesprek treden met de Commissie en het Voorzitterschap. Het is nog te vroeg om in te gaan op de hiervoor voorgestelde oplossingsrichtingen.

Startups en innovatie
De verordening verzoekt aanbieders om over te gaan tot certificering en het verkrijgen van een label. Zo ook voor startups en innovatie binnen de sectoren die onder deze verordening zullen vallen. Een zelfassessment van geschat 18.400 euro en/of een conformiteitsbeoordeling door een derde partij van geschat 25.000 euro kunnen worden gezien als aanzienlijke investeringen. Is de regering voornemens om hierin een subsidieregeling te voorzien? Of zijn er uitzonderingsregels of verminderde reikwijdte te verwachten om de administratieve lasten te verlichten?

Antwoord
De CRA zal zorgdragen voor security-by-design. Het kabinet zal bij de Europese Commissie vragen naar de mogelijkheden voor het mkb om aanspraak te maken op Europese subsidies, vanuit bijvoorbeeld het Digital Europe-programma. Een uitzondering op de CRA-eisen voor bijvoorbeeld startups wordt niet voorzien. Dit zou namelijk kunnen resulteren in minder vertrouwen van bedrijven en consumenten in producten van startups, aangezien die dan niet aan dezelfde digitale veiligheidseisen zouden hoeven te voldoen.

Daar waar Europese ontwikkelaars geconfronteerd worden met de CRA, is er een aannemelijke kans dat wereldwijd denkende spelers binnen de sector, innovatie buiten Europa gaan plaatsen. Is er bij de regering inzicht in hoe de CRA invloed zal gaan hebben op arbeidsmarkt van de sector en onze globale positie binnen de kenniseconomie?

Antwoord
Vooropgesteld wordt dat de verplichtingen in de CRA ook van toepassing zijn op producten die door bedrijven van buiten de EU op de interne markt worden

aangeboden. Het kabinet verwacht dat de CRA kan bijdragen aan het wereldwijde vertrouwen in de veiligheid van in de EU op de markt gebrachte producten. Geharmoniseerde standaarden en regulering over cybersecurity vergemakkelijken daarnaast handel binnen de EU. Daarmee versterkt de CRA het concurrentievermogen van Europese bedrijven op de wereldmarkt. Een inschatting van de invloed van de CRA op de arbeidsmarkt is moeilijk te geven. Aangezien Nederland sterk is gedigitaliseerd en de CRA horizontale regulering betreft, is de verwachting dat de vraag naar cybersecuritykennis toe zal nemen.

Eerlijke concurrentie
De nalevingskosten worden als 2% van de omzet geschat. Berekening: 29 miljard ten opzichte van 1485 miljard. Omdat een zelfassessment of conformiteitsbeoordeling geschat wordt op 18,4 tot 25 duizend euro, kan daarmee worden afgeleid dat voor dit specifieke certificaat er een omzet van boven de 1 miljoen euro als marktcomfort wordt ingeschaald. Deelt de regering het standpunt dat niche- en maatwerkoplossingen buitenproportioneel met administratieve lasten worden belast om te kunnen conformeren? Hoe wil de regering de markt positief reguleren en eerlijke concurrentie waarborgen? Heeft de regering toezichthouders op de markten om een zienswijze gevraagd?

Antwoord
Met betrekking tot niche- en maatwerkoplossingen beraadt het kabinet zich nog op een standpunt. De nalevingskosten zullen voor kleine en middelgrote producenten relatief zwaarder zijn dan voor grote producenten en dit zal voor niche- en maatwerkoplossingen ook relatief duurder zijn dan voor massaproductie. Met name voor het mkb, in het bijzonder kleine bedrijven, wordt bij de onderhandelingen door meerdere lidstaten waaronder Nederland aandacht gevraagd. Het kabinet staat daarbij open voor mogelijkheden om kleine en middelgrote producenten tegemoet te treden, op een manier die niet ten koste gaat van het niveau van cybersecurity van de betreffende digitale producten. Daarbij kan bijvoorbeeld worden gedacht aan ondersteuning en voorlichting over de wijze waarop zij aan de verplichtingen kunnen voldoen of de beschikbaarheid van subsidies vanuit bijvoorbeeld Digital Europe. Het kabinet gaat hierover nog in gesprek met toezichthouders en de sector.

Financiële consequenties
De regering gaat in op de financiële consequenties voor de rijksoverheid en/of medeoverheden, evenals de gevolgen van regeldruk voor bedrijfsleven en de burger. Hierbij worden miljardenbedragen genoemd. Zowel voor kosten als voor kostenbesparing. Zodra de gevolgen van de invoering van deze verordening duidelijk worden, is de regering voornemens om hiervoor een compensatieregeling in te richten? Zo ja, welke doelgroepen (zoals gemeenten of midden- en kleinbedrijf) en om welke redenen, zullen dan worden gecompenseerd? Op welke wijze zal dit in de begroting worden ingepast en/of hoe zal dit herleidbaar zijn?

Antwoord
Het kabinet voorziet geen compensatieregeling. Het kabinet zal de Europese Commissie bevragen op de mogelijkheden voor het mkb om een beroep doen op gelden uit Europese fondsen, zoals bijvoorbeeld Digital Europe. Voor mede-overheden zijn geen financiële consequenties voorzien.

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 26175894

Actieve rol voor de overheid
Aanvullend op een certificaat en een meldplicht bij incidenten, zou er ook een actieve rol voor de overheid kunnen worden belegd. Deelt de regering de mening dat bij cyberbeveiliging er digitale equivalenten van de hulpdiensten dienen te worden ingericht? Een soort van politie voor de opsporing, beveiliging en handhaving. Een soort brandweer die helpt met branden blussen en preventie. Een soort ambulance die jou bij trauma in leven probeert te houden en overdraagt aan hen die alle middelen hebben om je te helpen. Oftewel, deelt de regering de mening dat deze verordening meer nastreeft dan voorlichting en certificering? Of dat zou moeten nastreven?

Antwoord
Er bestaat momenteel nog geen horizontale cybersecuritywetgeving met verplichtingen voor alle marktspelers van digitale producten. Naast het zorgen voor transparantie over de mate van cybersecurity van dergelijke producten ten behoeve van de keuze van gebruikers (voorlichting) stelt de CRA-verordening horizontale robuuste cybersecurity voorwaarden aan alle producten met digitale elementen. De verordening vult daarmee een belangrijke lacune op in het cybersecuritylandschap.
Zowel op EU als op nationaal niveau bestaan er al wel veel initiatieven en relevante wetgeving op het gebied van cybersecurity ter bevordering van de digitale weerbaarheid. Zo wordt in de Nederlandse Cybersecuritystrategie 2022-2028 (NLCS) de visie op de digitale samenleving beschreven en de rol van overheid, bedrijven en burgers daarin. Bij de strategie hoort ook een actieplan met concrete acties om Nederland digitaal veiliger te maken. Op EU-niveau bestaat er, onder meer, sinds 2016 de Netwerk- en Informatiebeveiligingsrichtlijn die lidstaten onder meer verplicht om een nationale cyberstrategie, een Computer security incident response team (CSIRT) die ondersteuning en advies biedt bij incidenten, en toezichthouders te hebben. Als gevolg van de herziening van de Netwerk- en informatiebeveiligingsrichtlijn (NIB2), die uiterlijk in oktober 2024 moet zijn geïmplementeerd, krijgen veel meer sectoren en organisaties binnen de EU, te maken met wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen en daarmee ook het recht op de ondersteuning en advies van een CSIRT overeenkomstig de NIB2. Een CSIRT heeft bijvoorbeeld als taak om cyberdreigingen, kwetsbaarheden en incidenten te monitoren en te analyseren en om organisaties die onder de NIB2 vallen vroegtijdig te waarschuwen en informatie te delen over dreigingen, kwetsbaarheden en incidenten.
In Nederland hebben vitale aanbieders en onderdelen van het Rijk reeds recht op bijstand van het Nationaal Cyber Security Centrum (NCSC) en digitale dienstverleners (cloud, online marktplaatsen en zoekmachines) van het CSIRT voor digitale diensten. Daarbij kunnen publieke en private partijen via het Landelijk Dekkend Stelsel (LDS), een structuur van samenwerkingsverbanden op het gebied van cybersecurity, samenwerken om informatie en kennis uit te wisselen met als doel de slagkracht van die partijen te versterken en Nederland digitaal weerbaarder te maken. De Nederlandse Politie is verantwoordelijk voor opsporing en handhaving, ook in het digitale domein. Indien strafbare feiten worden of zijn gepleegd, kan de politie een opsporingsonderzoek uitvoeren. Gelet op (onder meer bovengenoemde) reeds bestaande organisaties, initiatieven en relevante wetgeving ter bevordering van de digitale weerbaarheid, is het kabinet niet voornemens een zogenoemde digitale brandweer of ambulance in te richten.

Phishing
Hoe moeten bedrijven en consumenten in het kader van deze verordening omgaan met phishing? Op dit moment gaan er al e-mails met een chanterende boodschap rond, met in de kern de illusie dat jouw e-mail/account/dienst/systeem is gehackt en overgenomen, en wordt losgeld in de vorm van bitcoins gevraagd. Zo'n 'melding' — ongeacht of de distributeur de juistheid al kan vaststellen — zou binnen 24 uur gemeld moeten worden. Deelt de regering het standpunt dat, met een aanvullende versterking van de rechtszekerheid (van bedrijven en gebruikers) en versterking van de 'digitale politie' en opsporingscapaciteit, deze verordening hierin zou moeten worden gewaarborgd?

Antwoord
De term phishing wordt veelal gebruikt om aan te duiden dat een crimineel moedwillig probeert een slachtoffer onder valse voorwendselen gegevens of geld te laten verstrekken, of op een bepaalde link en/of bijlage te laten klikken. De CRA beoogt de cybersecurity van digitale producten te verhogen, zodat de mogelijkheden voor criminelen om systemen te hacken of over te nemen worden verminderd. Phishing-acties die het hacken of overnemen van systemen beogen, kunnen daardoor minder succesvol worden. De CRA bevat echter geen bepalingen specifiek gericht op phishing. De meldplicht in artikel 11 betreft incidenten met, en kwetsbaarheden in de digitale producten zelf. Het enkele gebruik van een product of dienst voor criminele doeleinden is in beginsel geen aanleiding voor een melding op grond van artikel 11 van het voorstel.
Slachtoffers van phishing kunnen aangifte doen bij de politie. De politie werkt aan het mogelijk maken van digitale aangifte van meer criminaliteitsfenomenen. Van enkele vormen van phishing is dit inmiddels mogelijk. In de Veiligheidsagenda 2023-2026 zijn bovendien afspraken gemaakt over de ambities voor de landelijke prioriteiten van de opsporing. Cybercrime en online fraude zijn daarin als prioriteit benoemd en er zijn op deze onderwerpen ambities afgesproken voor het aantal onderzoeken.

Gijzeling van gegevens en systemen
In de laatste jaren worden ook overheden en publieke instellingen geconfronteerd met cyberbeveiligingsincidenten. Kan de regering aangeven hoe deze situaties (door de verordening) voorkomen hadden kunnen worden? Welke criteria worden gehanteerd, ook bij werkwijzen wanneer gegevens gegijzeld worden en systemen overgenomen?

Antwoord
Incidenten op informatieveiligheidsgebied zijn er in allerlei soorten en maten. Een aantal incidenten die recent het nieuws haalden, betrof een aanval met gijzelsoftware bij een tweetal gemeenten. Oorzaak van deze incidenten lag o.a. bij foutief wachtwoordgebruik, het niet goed toepassen van twee-factor authenticatie, het onvoldoende invulling geven aan leveranciersmanagement en onvoldoende continuïteitsbeheer. Door het naleven van de Baseline Informatiebeveiliging Overheid (BIO) wordt de kans op dit soort incidenten aanzienlijk beperkt. Als onverhoopt zo'n incident zich toch voordoet, helpen de maatregelen uit de BIO de gevolgen ervan te beperken. BIO bevat bepalingen die minimumeisen stellen aan bijvoorbeeld wachtwoordgebruik en twee-factor authenticatie. In de werkagenda Waardengedreven Digitaliseren alsmede in het Actieplan Nederlandse Cybersecuritystrategie is de actie opgenomen om de BIO in wetgeving te verankeren en toezicht op de naleving ervan te organiseren. De CRA zal het vooral

makkelijker maken voor overheden en publieke instellingen om veilige ICT-producten in te kopen omdat producten aan wettelijke cybersecurityeisen moeten voldoen om aangeboden te kunnen worden op de Europese markt. Daarnaast ondersteunen de Inkoopeisen Cybersecurity Overheid (ICO) overheidsorganisaties bij het stellen van eisen aan ICT-producten en diensten. Overheden en publieke instellingen zullen nog steeds zelf beveiligingsmaatregelen moeten treffen om incidenten te voorkomen of te mitigeren.

Actieve uitbating zwakheden door derden
Met de oorlog in Oekraïne is Europa wakker geschud dat er ook een digitaal front is. Hoe wil de regering deze verordening inzetten om zich te wapenen in de 'digitale oorlog'? Welke beperkingen en/of vrijheden van de nationale veiligheids- en inlichtingendiensten komen met de CRA in een ander daglicht te staan?

Antwoord
Het kabinet werkt aan een digitaal veilig Nederland, waarvoor de doelen worden beschreven in de Nederlandse Cybersecurity Strategie (NLCS). De NLCS beschrijft de cybersecurityaanpak voor de komende zes jaar om de Nederlandse samenleving
digitaal veilig te maken. Een belangrijke stap richting digitaal weerbare burgers en organisaties zijn veilige digitale producten, zoals beschreven in pijler II van de NLCS. De CRA is een integraal onderdeel van de acties bij deze doelstelling. Naast het creëren van cybersecurityvoorwaarden voor fabrikanten, leveranciers en importeurs van producten met digitale elementen, is de tweede hoofddoelstelling van de CRA het zorgen voor transparantie over de mate van cybersecurity van dergelijke producten ten behoeve van de keuze van gebruikers (consumenten en organisaties).
De regering voorziet niet dat de CRA van invloed zal zijn op de taken en verantwoordelijkheden van de Nederlandse inlichtingen- en veiligheidsdiensten, welke zijn vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2017. Inlichtingen- en veiligheidsdiensten hebben bijvoorbeeld een rol in de bescherming van bijzondere informatie zoals staatsgeheimen. Daartoe evalueert en ontwikkelt het Nationaal Bureau Verbindingsbeveiliging (dat onderdeel is van de AIVD) beveiligingsproducten voor gerubriceerde informatie. Hoewel de CRA eisen stelt aan producten met digitale elementen heeft de verordening geen effect op de verantwoordelijkheid die Nederlandse inlichtingen- en veiligheidsdiensten in dat kader hebben. Producten die exclusief zijn ontwikkeld voor de nationale veiligheid, militaire doeleinden of om gerubriceerde informatie te verwerken vallen namelijk buiten de reikwijdte van de CRA.

Bescherming van klokkenluiders en ethische hackers
Zwakten in systemen worden altijd door mensen ontdekt. Leveranciers hebben economische belangen bij het (ogenschijnlijk) ontbreken van zwakheden. Op welke wijze worden klokkenluiders en ethische hackers mede door deze verordening in bescherming genomen?

Antwoord
De verordening voorziet in toezicht door nationale markttoezichthouders. Personen die een kwetsbaarheid ontdekken zullen dit in eerste instantie bij de fabrikant kunnen melden, deze is immers het beste in staat (en op basis van de CRA bovendien verplicht) de kwetsbaarheid te verhelpen en te voorkomen dat de kwetsbaarheid wordt misbruikt met alle gevolgen van dien. De CRA bevat ook de eis dat fabrikanten beleid moeten hebben rondom *coordinated vulnerability*

Directoraat-generaal Economie en Digitalisering
Directie Digitale Economie

Ons kenmerk
DGED-DE / 26175894

disclosure. Als de kwetsbaarheid al actief is geëxploiteerd is de fabrikant volgens het voorstel verplicht om dit te melden bij ENISA, die dit vervolgens doorgeeft aan de nationale markttoezichthouders. Op het niet naleven van deze verplichting staat in het voorstel een boete van maximaal 15 miljoen euro of 2,5 procent van de totale wereldwijde jaarlijkse omzet als dat hoger is. Mocht de ontdekker van de kwetsbaarheid constateren dat de fabrikant de kwetsbaarheid niet verhelpt dan kan deze persoon uiteraard de nationale markttoezichthouder hiervan op de hoogte stellen. Op basis van dergelijke informatie kan de toezichthouder een onderzoek instellen.