Ministerie van Justitie en Veiligheid

> Retouradres Postbus 16950 2500 BZ Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Datum 10 oktober 2022
Onderwerp Beleidsreactie OVV Rapport 'Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix

Geachte voorzitter,

De Onderzoeksraad voor Veiligheid (OVV) heeft op 16 december 2021 het rapport "Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix" gepubliceerd. Via deze brief ontvangt u de beleidsreactie van het kabinet.

Aanleiding
De beveiligingslekken in de software van Citrix - als aanleiding voor de OVV voor het starten van onderzoek - werden in december 2019 bekend. Specifiek ging het om de kwetsbaarheid in de Citrix producten ADC en Citrix Gatewayservers. Deze producten worden onder andere gebruikt om externe toegang tot een netwerk mogelijk te maken, bijvoorbeeld voor thuiswerken en in sommige gevallen primaire processen. De potentiële impact van de kwetsbaarheid kon groot zijn omdat (1) veel organisaties gebruik maakten, en maken, van deze systemen, (2) de kwetsbaarheid breed bekend werd en (3) Citrix niet direct een sluitende oplossing kon bieden.[1] Deze problematiek heeft breed zichtbaar gemaakt hoe afhankelijk we als samenleving zijn van digitale systemen en hoe uitval kan leiden tot maatschappelijke ontwrichting. De impact van dit incident zou, tijdens de COVID-19 pandemie waarin we massaal thuis zijn gaan werken, nog veel groter zijn geweest. Bovendien maakte de problematiek duidelijk dat een probleem in software van een enkele leverancier in Nederland en wereldwijd voor grote problemen kan zorgen bij vele organisaties die hier direct maar ook indirect van afhankelijk zijn. Het rapport van de OVV is dan ook zeer nuttig voor de verdere versterking van onze digitale weerbaarheid. In deze brief wordt nader ingegaan op welke wijze het kabinet invulling zal geven aan de aanbevelingen die door uw organisatie aan het kabinet zijn gedaan om onze digitale veiligheid te versterken.

Leeswijzer
Deze brief geeft allereerst een overzicht van de zeven aanbevelingen die uw organisatie heeft geformuleerd. Vervolgens wordt ingegaan op de aanbevelingen van uw organisatie en in hoeverre het kabinet hierop acteert en hoe deze past

[1] Zie voor meer achtergrond Kamerstukken II, 2019-20, 26 643, nr. 658 en Kamerstukken II, 2019-20, 26 643, nr. 660

binnen het beleid van dit kabinet als onderdeel van de nieuwe Cybersecuritystrategie (NLCS).

Aanbevelingen van de OVV:
De OVV geeft aan dat het onderzoek laat zien dat kwetsbaarheden in software kunnen leiden tot onveiligheid voor organisaties die software gebruiken, en voor hen die van deze organisaties afhankelijk zijn. De OVV signaleert dat de kloof groeit tussen digitale afhankelijkheid en de dreigingsomvang enerzijds, en de weerbaarheid van de samenleving anderzijds. De OVV stelt dat snel en fundamenteel ingrijpen nodig is om te voorkomen dat de maatschappij ontwricht raakt. Daarom doet de OVV zeven aanbevelingen, waarvan er vier gericht zijn aan het kabinet of leden van het kabinet in het bijzonder.

Aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken:

1. Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend - gevraagd en ongevraagd - worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid. Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.

Aan de Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:

2. Zorg dat uw initiatieven om te komen tot wetgeving voor veiligere software leiden tot een Europese verordening die de verantwoordelijkheid van fabrikanten vastlegt en afnemers inzicht geeft in hoe fabrikanten die verantwoordelijkheid invullen. Leg vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden.

Aan fabrikanten van software gezamenlijk:

3. Ontwikkel met andere fabrikanten *good practices* om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.
4. Waarschuw en help al uw afnemers zo snel en doeltreffend mogelijk wanneer kwetsbaarheden in software gesignaleerd worden. Schep de randvoorwaarden die noodzakelijk zijn om uw afnemers te kunnen waarschuwen.

Aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Economische Zaken en Klimaat (ten behoeve van alle organisaties en consumenten in Nederland):

5. Bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk.

Aan het Nederlandse kabinet:

6. Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.
7. Verplicht alle organisaties om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.

Nederlandse cybersecurityaanpak

Cybersecurity is een brede en grensoverschrijdende maatschappelijke opgave voor onze samenleving. Om deze opgave het hoofd te bieden is onder coördinatie van de minister van Justitie en Veiligheid de NLCS met bijbehorend actieplan tot stand gekomen. Via deze strategie wil het kabinet de digitale veiligheid in Nederland, Europa en wereldwijd verder versterken. Ik hecht er waarde aan om in deze beleidsreactie de strategie te benoemen, omdat de aanbevelingen van de OVV belangrijke input vormden voor het formuleren van de strategische doelen en de uitwerking daarvan. De NLCS wordt daarom in een gezamenlijk pakket, met deze brief, aan de Tweede Kamer verzonden.

Beleidsreactie op de aanbevelingen

Op volgorde zal in deze brief op de verschillende aanbevelingen worden ingegaan.

Aanbeveling 1 *aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken:*

- *Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend - gevraagd en ongevraagd - worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid. Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.*

In de reactie op deze aanbeveling zal allereerst worden ingegaan op hoe het stelsel van cybersecurity informatiedeling is georganiseerd, hoe het kabinet deze in het kader van de nieuwe strategie wil doorontwikkelen en hoe daarin private en publieke responscapaciteit efficiënter kan samenwerken. Ten tweede wordt ingegaan op de bevoegdheden van de Rijksoverheid in het kader van informatiedeling met het oog op het oplossen van de door de OVV genoemde knelpunten. Ten derde wordt ingegaan op het scannen op kwetsbaarheden, zoals door de OVV in haar toelichting op de bovenstaande aanbeveling is genoemd.

Het stelsel van cybersecurity informatiedeling
Binnen het Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden kan algemene informatie over digitale veiligheid en specifieke dreigings- en risico-informatie gedeeld worden. Het doel van het LDS is om (publieke en private) organisaties in staat te stellen hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen door informatie over cybersecurity breed, efficiënt en effectief met elkaar te delen. Het is essentieel dat deze informatie-uitwisseling via schakelorganisaties leidt tot handelingsperspectief waarmee organisaties hun weerbaarheid kunnen verbeteren. Het LDS is een jong stelsel ingericht onder het vorige kabinet. Ten tijde van de Citrixproblematiek verliep parallel de aanwijzing krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) van een aantal computercrisisteams, die ook onderdeel zijn van het LDS, waardoor met hen specifieke dreigingsinformatie door het NCSC gedeeld kan worden.[2] Ook zijn er inmiddels krachtens de Wbni een aantal andere schakelorganisaties aangewezen (OKTT's), waarmee het NCSC hierdoor specifieke informatie kan delen.[3] De komende jaren wil het kabinet via de Nederlandse Cybersecuritystrategie – waar de minister van Justitie en Veiligheid regie over voert - inzetten op de doorontwikkeling van dit stelsel.

Het is daarbij van belang om het Landelijk Dekkend Stelsel effectief en efficiënt in te richten met heldere aanspreekpunten zodat organisaties geholpen zijn bij het treffen van maatregelen, waarbij zij zelf verantwoordelijk blijven. Daarbij dient de door de OVV gesignaleerde fragmentatie zoveel mogelijk voorkomen te worden. Het NCSC, het Digital Trust Center (DTC) en het CSIRT voor digitale diensten (CSIRT DSP) hebben de intentie om te komen tot integratie. [4] Hiertoe is een verkenning uitgevoerd, waarvan de resultaten op 7 september jl. aan de Tweede Kamer zijn aangeboden.[5] Deze verkenning heeft een positief beeld van de mogelijkheden gegeven. Deze integratie wordt nu verder uitgewerkt in een programmaplan.

De Rijksoverheid streeft ernaar om ook daarbuiten meer samenhang te creëren tussen bestaande schakelorganisaties en integratie waar nuttig te stimuleren. Voor alle bestaande sectorale computercrisisteams (CERT's) wordt daarom door de Rijksoverheid verkend in hoeverre meer samenwerking, samenhang of mogelijke samenvoeging met het NCSC toegevoegde waarde heeft.[6] Het blijft daarbij zaak om in het oog te houden waar expertise het best kan worden georganiseerd. Enerzijds is sectorspecifieke kennis nodig om maatregelen te treffen en handelingsperspectief te formuleren. Anderzijds kan fragmentatie van kennis juist nadelig zijn vanwege schaarse cybersecurity expertise en vertraging in de snelheid van informatiedeling. Nieuwe CERT's ontstaan in principe alleen daar waar dit toegevoegde waarde heeft. Sectoren en organisaties kunnen bovendien gebruik maken van bijvoorbeeld de openbaar toegankelijke algemene adviezen van het NCSC. In de NLCS en het bijbehorende actieplan van het kabinet wordt uitvoerig ingegaan op welke acties

[2] Regeling aanwijzing computercrisisteams.
[3] Dit betreffen organisaties die objectief kenbaar tot taak (OKTT) hebben andere organisaties of het publiek te informeren over dreigingen en incidenten.
[4] CSIRT-DSP staat voor Computer Security Incident Response Team voor digitale dienstverleners
[5] Kamerstukken II 2022-23 nr. 2022Z16336.
[6] De bestaande aangewezen CERT's zijn de Informatiebeveiligingsdienst (IBD), Zorg-CERT (Z-CERT), SURF en CERT Watermanagement (CERT-WM).

aanvullend worden genomen om het stelsel van cybersecurity informatiedeling verder door te ontwikkelen. [7]

Daarnaast is het in het kader van de OVV-aanbeveling van belang om te benoemen dat - in het kader van de uitvoering van de Nederlandse Cybersecurity Agenda uit 2018 - in 2020 de Cyber Info/Intel Cel (CIIC) is ingesteld. Daarbinnen brengen AIVD, MIVD, NCSC, OM en politie dreigingsinformatie bijeen. Medewerkers van deze organisaties werken fysiek samen en beoordelen hierin de informatie over cyberdreigingen.[8] Zo kan sneller een beeld worden gevormd van nieuwe dreigingen en kunnen organisaties sneller van handelingsperspectief worden voorzien. Naast deze succesvolle publiek-publieke samenwerking is een verkenning uitgevoerd naar het gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband. In lijn met de aanbeveling van de OVV om private en publieke responscapaciteit beter samen te brengen is het van belang dat de overheid en bedrijven effectief en efficiënt dreigingsinformatie en handelingsperspectief uitwisselen, passend bij de kennis en kunde van de ontvanger. Zoals opgenomen in de actieplannen bij de NLCS - en in lijn met de aanbeveling van de OVV - streeft het kabinet er daarom naar om een publiek-privaat samenwerkingsplatform op te richten waarin informatie snel kan worden gedeeld, gezamenlijk kan worden geanalyseerd, en kan worden gedistribueerd. Over het resultaat van de verkenning informeer ik u bij de aanbieding van de NLCS, waar het rapport met de resultaten van deze verkenning is bijgevoegd.

Bevoegdheden van de Rijksoverheid in het kader van informatiedeling
In lijn met de OVV-aanbeveling is het kabinet van mening dat onwenselijke wettelijke obstakels - bij informatiedeling door de overheid (zoals door het NCSC) - weggenomen moeten worden. Dat begint bij het inventariseren van wettelijke bevoegdheden om zodoende zicht te krijgen op obstakels. Om zicht daarop te krijgen heeft het vorige kabinet bestaande mogelijkheden rondom het delen van informatie in het kader van onze digitale weerbaarheid geïnventariseerd in 2021 en deze zijn reeds met de Tweede Kamer gedeeld.[9] Naar aanleiding van deze inventarisatie heeft het kabinet besloten om de Wet beveiliging netwerk- en informatiesystemen (Wbni) te wijzigen om zo optimaal mogelijk informatie uitwisseling door het NCSC met andere organisaties mogelijk te maken. Op 20 april jl. is het voorstel tot wijziging van de Wbni bij de Tweede Kamer ingediend. Dit wetsvoorstel strekt ertoe het NCSC een ruimere bevoegdheid te geven om dreigings- en incidentinformatie, die relevant is voor andere aanbieders dan vitale aanbieders of rijksoverheidsorganisaties, aan die andere aanbieders of hun schakelorganisaties te verstrekken. Het komt erop neer dat hierdoor meer organisaties, direct of via een schakelorganisatie, kunnen worden gewaarschuwd, zodat zij maatregelen kunnen treffen om te voorkomen dat zij slachtoffer worden van kwaadwillenden, zoals cybercriminelen. Voor een nadere toelichting op het wetsvoorstel verwijs ik u naar de memorie van toelichting.[10] Met dit wetsvoorstel wordt mede invulling gegeven aan de aanbeveling van de OVV voor voldoende mandaat, door het regelen van een verruiming van de wettelijke bevoegdheid om informatie te delen vanuit het NCSC. Op 4 oktober jl. is het wetsvoorstel aangenomen door de Tweede Kamer en binnenkort wordt het ingediend bij de

[7] Zie in bijzonder de acties onder pijler één 'Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties20' van de Nederlandse Cybersecuritystrategie.
[8] Te vinden via: https://zoek.officielebekendmakingen.nl/stcrt-2020-30702.html
[9] Kamerstukken II 2020-21, 26 643, nr. 738
[10] Kamerstukken II 2021-22, 36 084, nr. 5

Eerste Kamer. Ook zullen de taken als gevolg van de herziening van de Netwerk– en informatiebeveiligingsrichtlijn (NIB2-richtlijn) van organisaties zoals het NCSC en de sectorale toezichthouders door de implementatie van deze richtlijn flink worden uitgebreid.[11] Naar verwachting zal er dit najaar een definitief akkoord worden bereikt over de NIB2-richtlijn binnen de EU. Lidstaten hebben vervolgens 21 maanden om deze richtlijn om te zetten in hun nationale wetgeving. Bij verdere doorontwikkeling van het stelsel is het uiteraard van belang om telkens de passende wettelijke taak en -bevoegdheid in het oog te blijven houden om informatie te delen vanuit het NCSC. Overheidsorganisaties zoals het NCSC zijn bij de uitoefening van bevoegdheden tot het verstrekken van informatie uiteraard gehouden de daarvoor geldende wettelijke kaders (zoals de AVG) in acht te nemen.

Voor het niet-vitale bedrijfsleven is in 2018 het Digital Trust Center opgericht. Het Digital Trust Center informeert en adviseert circa 2 miljoen niet-vitale bedrijven in Nederland hoe zij hun digitale weerbaarheid kunnen verbeteren en jaagt de ontwikkeling van publiek-private samenwerkingsverbanden aan. Om de taken en bevoegdheden van het DTC, zoals het ontvangen, verwerken en versturen van specifieke dreigingsinformatie, wettelijk te borgen is het wetsvoorstel bevordering digitale weerbaarheid bedrijven (Wbdwb) opgesteld. Afgelopen zomer heeft de Raad van State haar advies over dit wetsvoorstel uitgebracht en het wetsvoorstel wordt dit najaar aan de Tweede Kamer aangeboden. Vooruitlopend op de Wbdwb is het Digital Trust Center in juni 2021 gestart met de informatiedienst, nadat zij de zogenaamde OKTT-status van het ministerie van JenV heeft ontvangen. Met deze OKTT-status kan het Digital Trust Center dreigingsinformatie ten behoeve van de doelgroepen van het DTC ontvangen van het NCSC. Hierover is de Tweede Kamer geïnformeerd. [12] Sinds de zomer van 2021 worden individuele niet-vitale bedrijven actief geïnformeerd over bij de overheid bekende ernstige digitale dreigingen en kwetsbaarheden (hoge kans, hoge impact).

Via bovenstaande initiatieven worden belangrijke stappen gezet voor de effectievere uitwisseling van informatie binnen het Nederlandse stelsel. Tegelijkertijd constateren we dat het nog niet in alle gevallen mogelijk is om (potentiele) slachtoffers te waarschuwen. Informatie over (potentiele) slachtoffers kan zowel uit strafrechtelijke als niet-strafrechtelijke bron komen, waarbij verschillende juridische regimes gelden om deze informatie te verwerken. Omdat het hierbij om persoonsgegevens gaat moet ook de organisatie die de slachtoffernotificatie doet over een passende grondslag beschikken om de (potentiele) slachtoffers te kunnen waarschuwen. Dit vergt uitgebreider onderzoek naar de wettelijke kaders en de passende uitvoering van deze taak. Daarom zal onder coördinatie van de minister van Justitie en Veiligheid een onderzoek worden uitgevoerd om vast te stellen op welke manier doelwit- en slachtoffernotificatie uit niet-strafrechtelijke bron verder vormgegeven kan worden. Daarnaast zullen de politie en het OM verkennen op wat voor manier het notificeren van slachtoffers die blijken uit strafrechtelijke onderzoeken verder vorm kan krijgen. Deze acties heb ik ook opgenomen in het actieplan bij de NLCS. Ik zal de Kamer informeren over de resultaten van deze verkenningen en de bijbehorende vervolgstappen zodra deze beschikbaar zijn.

[11] Als gevolg van de NIB2-richtlijn krijgen veel meer sectoren en organisaties binnen de EU te maken met wettelijke verplichtingen voor de beveiliging van hun netwerk- en informatiesystemen. Dit zijn bedrijven maar ook overheden. Deze organisaties dienen in het kader van een zorgplicht te voldoen aan een hoog niveau van cybersecurity. Incidenten met een aanzienlijke impact zullen ook tijdig gemeld moeten worden.
[12] Kamerstukken II 2020-21, 26643 nr. 760. en Kamerstukken II, 2021-22, 26643 nr. 817.

Het scannen op kwetsbaarheden
In het kader van voldoende wettelijke regeling van taken en bevoegdheden benoemt de OVV eveneens het thema scannen in relatie tot de bevoegdheden van het NCSC. Het NCSC heeft onder meer als wettelijke taak het verrichten van technisch onderzoek naar dreigingen en incidenten, ten behoeve van de taak om organisaties die deel uitmaken van de rijksoverheid en vitale aanbieders hierover te informeren en adviseren. In het kader van deze taakuitoefening scant het NCSC ook op kwetsbaarheden in netwerk- en informatiesystemen van deze organisaties, voor zover dit mogelijk is zonder daarbij die systemen van organisaties binnen te dringen. Voor zover scannen naar kwetsbaarheden het zonder toestemming binnendringen van een netwerk- of informatiesystemen inhoudt, beschikt het NCSC niet over de daartoe benodigde wettelijke bevoegdheid.[13] Als gevolg van de NIB2-richtlijn zullen de bevoegdheden van CSIRTs[14] (zoals het NCSC) om te scannen worden aangepast. De NIB2-richtlijn bevat voor CSIRTs de bevoegdheid om op kwetsbaarheden te scannen als daarvoor toestemming van een organisatie is verkregen of als hierbij niet in systemen van een organisatie wordt binnengedrongen.

Aanbeveling 2 *aan de Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:*

- *Zorg dat uw initiatieven om te komen tot wetgeving voor veiligere software leiden tot een Europese verordening die de verantwoordelijkheid van fabrikanten vastlegt en afnemers inzicht geeft in hoe fabrikanten die verantwoordelijkheid invullen. Leg vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden.*

Aanbeveling 3 en 4 *aan fabrikanten van software gezamenlijk:*

- *Ontwikkel met andere fabrikanten good practices om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.*
- *Waarschuw en help al uw afnemers zo snel en doeltreffend mogelijk wanneer kwetsbaarheden in software gesignaleerd worden. Schep de randvoorwaarden die noodzakelijk zijn om uw afnemers te kunnen waarschuwen.*

De aanbevelingen 2, 3 en 4 zijn gericht aan de Europese Commissie en aan fabrikanten van software gezamenlijk. In contacten met de Europese Commissie heeft het kabinet deze aanbevelingen onder de aandacht gebracht. Deze partijen zijn primair aan zet om opvolging te geven aan deze aanbevelingen. Het kabinet kan hierin verder een actieve en stimulerende rol vervullen op basis van de doelstelling in de tweede pijler van de NLCS om digitale producten en diensten veiliger te maken. Vanwege het grensoverschrijdende karakter van de markt voor ICT-producten en – diensten ligt het in algemene zin voor de hand om maatregelen te nemen in Europees verband.

Het kabinet zet zich publiek-privaat actief in voor de ontwikkeling en toepassing van cybersecurity certificeringschema's van ICT-producten, diensten en processen onder *de Cyber Security Act*. Binnen dat raamwerk is het ook de ambitie van Nederland om een certificeringschema te ontwikkelen voor de cybersecurity van software naast onderwerpen die al onderdeel zijn van het werkprogramma van de Europese

[13] Zie ook: Kamervragen (Aanhangsel) 2021-2022, nr. 460.
[14] CSIRT is de afkorting voor Computer Security Incident Response Team.

Commissie zoals clouddiensten, 5G-netwerkapparatuur en industriële controlesystemen. Ook voert Nederland actief het gesprek met de Europese Commissie en andere lidstaten over de ontwikkeling van horizontale regulering voor de cybersecurity van ICT-producten en diensten via de *Cyber Resilience Act*. Deze regelgeving biedt de uitgelezen kans om de verantwoordelijkheid voor de cybersecurity van ICT-producten en diensten steviger bij de fabrikanten en leveranciers van ICT-producten en diensten te beleggen. Nederland zet hierbij in op een wettelijke cybersecurity zorgplicht voor fabrikanten en leveranciers van alle ICT-producten en diensten (inclusief software) gedurende de hele productlevenscyclus ongeacht of een ICT-product of dienst wordt geleverd aan consumenten of organisaties. Het non-paper waarin dit standpunt is uitgewerkt is op 14 december 2021 door de minister van Economische Zaken en Klimaat aangeboden aan de Kamer. Het wetsvoorstel voor de Cyber Resilience Act is op 15 september jl. gepresenteerd door de Europese Commissie.

Ten aanzien van aansprakelijkheid geldt overigens in algemene zin dat op basis van het Europese wettelijk kader voor civiele aansprakelijkheid gebruikers verhaal kunnen zoeken voor geleden schade bij de rechter. Dit geldt ook op het gebied van cybersecurity. Zij kunnen hun schade mogelijk verhalen op de aanbieder van softwareproducten en diensten op basis van een overeenkomst. Als een softwareaanbieder een product of dienst heeft aangeboden die vervolgens niet voldoet aan afgesproken digitale veiligheidseisen, dan is de aanbieder mogelijk aansprakelijk op grond van wanprestatie. Contractvrijheid is in het civiele aansprakelijkheidsrecht het uitgangspunt. Daarbij geldt dat organisaties onderling contractuele afspraken moeten maken over de cybersecurity van softwareproducten- en diensten. Dat gezegd hebbende zoals hiervoor aangegeven zet Nederland zich bij de onderhandelingen over de Cyber Resilience Act in voor het duidelijker beleggen van een zorgplicht voor cybersecurity bij fabrikanten en leveranciers om de positie van afnemers bij het maken van deze afspraken te versterken.

Europese wettelijke cybersecurityvereisten zoals die zullen worden opgenomen in de aankomende Cyber Resilience Act, of door gebruikers gevraagde certificering zoals ontwikkeld onder de Cyber Security Act, kunnen behulpzaam zijn bij een toets door de rechter. Ook al is een gang naar de rechter op het gebied van het aansprakelijkheidsrecht alleen aan de orde nadat schade is geleden door een gebruiker, het is daarmee één van de mogelijke marktprikkels (bovenop eventuele toekomstige wettelijke verplichtingen) voor aanbieders om voorzorgsmaatregelen te nemen ter voorkoming of beperking van schade.

Aanbeveling 5 *aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Economische Zaken en Klimaat (ten behoeve van alle organisaties en consumenten in Nederland):*

- *Bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk.*

Het kabinet omarmt deze aanbeveling, die aansluit op reeds lopende, en voorziene inzet vanuit de overheid. De overheid ziet het als haar taak het goede voorbeeld te geven middels een voortrekkersrol, haar rol als goed opdrachtgever te versterken en daarmee ook een algemene beweging in de markt te stimuleren naar het

ontwikkelen en aanbieden van veilige ICT-producten en diensten. Alle overheidsorganisaties gezamenlijk kopen jaarlijks veel ICT-producten en -diensten in en dat maakt de overheid tot een belangrijke marktpartij. Het programma Inkoopeisen Cybersecurity Overheid (ICO) levert instrumenten om deze doelstellingen te helpen verwezenlijken: sets van inkoopeisen, een basisprocesbeschrijving en een 'wizard' waarmee voor specifieke inkopen en aanbestedingen relevante eisen op simpele wijze kunnen worden geselecteerd. De ICO-wizard is de afgelopen jaren opgezet en wordt doorontwikkeld. De inkoopsegmenten zijn eind vorig jaar aangevuld met privacy-eisen. Dit jaar wordt verder gewerkt aan de uitbreiding van nieuwe segmenten, invalshoeken en beveiligingseisen. Het beleid is erop gericht ICO een vaste plek te geven in het inkoopproces van de gehele overheid. Op termijn worden de normensets voor het veilig inkopen verplicht gesteld. In lijn met Europese ontwikkelingen zoals het opstellen van certificeringsschema's onder de Cyber Security Act zullen deze Europese schema's worden doorvertaald naar de al, voor de overheid verplichte, toegepaste normensets voor inkoopeisen. Het toepassen verloopt conform BIO altijd via risicomanagement, zodat deze door opdrachtgevers op de lokale situatie toegespitst kunnen worden. Hierdoor wordt invulling gegeven aan de aanbeveling van de OVV om als overheid een voortrekkersrol te vervullen ten aanzien van veiligheidseisen van hardware en software.

Door de open toegang van de cybersecurity inkoopeisen via de website BIO-overheid.nl kunnen ook leveranciers gebruik maken van de ICO-wizard en op voorhand bepalen met welke beveiligingseisen de inkopende overheden rekening moeten houden. Doordat de overheid transparant is over haar beveiligingseisen kunnen ICT-leveranciers producten en diensten ontwikkelen die daar bij voorbaat al aan voldoen.

Binnen het inkoopstelsel van de rijksoverheid zorgt het rijksbrede categoriemanagement en strategisch leveranciersmanagement, ten aanzien van de inkoop van generieke ICT, voor de verwerking in contracten van nieuwe aanvullende wettelijke verplichtingen en beleid. Daarnaast wordt als onderdeel van de I-strategie Rijk 2021-2025 gewerkt aan de kwaliteitscriteria van software en inkoopvoorwaarden. Dit moet bijdragen aan de inkoop van veilige en privacy verantwoorde software door de Rijksoverheid.

Op het gebied van consumentenbescherming is sinds april jl. de Implementatiewet richtlijnen verkoop goederen en levering digitale inhoud van kracht.[15] Met deze wet zijn twee Europese consumentenrichtlijnen (verkoop goederen en levering digitale inhoud)[16] geïmplementeerd. Deze wet 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

[15] Kamerstuk 35734, nr. 2.

[16] 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.

mag verwachten, en de consument hiermee instemt. De Autoriteit Consument en Markt (ACM) zal toezicht houden.

Daarnaast moeten draadloos verbonden apparaten die vanaf 1 augustus 2024 op de Europese markt komen voldoen aan wettelijke cybersecurityeisen onder de *Radio Equipment Directive*. Deze richtlijn is onderdeel van het Europese systeem van de CE-markering. Producten die niet aan de eisen voldoen kunnen van de markt worden geweerd en gehaald. Agentschap Telecom zal toezicht houden. Zowel organisaties als consumenten hebben baat bij deze Europese markttoegangseisen.

Voor verdere maatregelen die bijdragen aan deze aanbeveling zet het kabinet zoals hierboven genoemd in op versterking van de positie van gebruikers door te pleiten voor wettelijke eisen ten aanzien van de cybersecurity van digitale producten, diensten en processen en het introduceren van een zorgplicht voor fabrikanten en leveranciers in de *Cyber Resilience Act.* Daarnaast zal door het ministerie van EZK in overleg met brancheorganisaties worden verkend hoe het maken van heldere contractuele afspraken tussen leveranciers en afnemers kan worden gestimuleerd.

Aanbeveling 6 *aan het Nederlandse kabinet:*

- Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.

Het ministerie van BZK is, in de rol van stelselverantwoordelijke voor de overheid, normsteller voor het opstellen van de (wettelijke) kaders voor digitale veiligheid van de overheid, zoals het Besluit CIO-stelsel Rijksdienst 2021. Deze (wettelijke) kaders komen tot stand in nauw overleg met alle overheidslagen, waarbij wordt gestreefd naar breed draagvlak om zodoende samen tot resultaten te komen. In het licht van de gesignaleerde cyberdreiging, geldt echter ook voor de overheid in den brede de strategische keuze zoals geformuleerd in de NLCS, dat de regelgeving voldoende robuust moet zijn en dat we de vrijblijvendheid voorbij gaan. Dat betekent dat er overheidsbreed een zorgplicht voor informatieveiligheid komt en dat er overheidsbreed toezicht komt, beide te regelen in de Wet Digitale Overheid (WDO) en/of andere gepaste regelgeving.

De NIB2-richtlijn verplicht lidstaten om centrale overheden onder de reikwijdte van de richtlijn te brengen. Medeoverheden kunnen onder de reikwijdte van de richtlijn worden gebracht na een nationale risicobeoordeling. Ongeacht die uitkomst zetten we erop in om de nationale implementatie van de NIB2 voor de overheid gelijk op te laten lopen met het regelen van de zorgplicht en toezicht voor de overheid. Dat betekent dat dit wetstraject ook moet zijn afgerond binnen de implementatieperiode van de NIB2-richtlijn. Er zal ook steeds worden gekeken naar de analogie met de Comptabiliteitswet, waar toepasselijk. We komen hiermee tot een eenduidig, eenvoudig en geharmoniseerd stelsel, waarin gepaste interbestuurlijke handhaving een plaats zal krijgen.

In de WDO zal ter ondersteuning van het toezicht de eis van een jaarlijks IT-verslag en IT-verklaring van een onafhankelijke deskundige over de IT-veiligheid en continuïteit worden opgenomen. Dit versterkt het horizontale toezicht en vergemakkelijkt de verticale verantwoording. Door het opnemen van deze eis in de WDO neemt de feitelijke veiligheid toe en kan de auditlast die de meer dan 60 (Rijks)stelselhouders aan de lagere overheden opleggen, aanzienlijk afnemen. Deze IT-verklaring zal tevens worden betrokken bij het toezicht op de IT-veiligheid dat

op grond van de NIB2-richtlijn onder verantwoordelijkheid van BZK zal worden uitgeoefend op alle overheidsorganisaties.

In afwachting van de opname van de verplichte IT-verklaring in de WDO zal BZK (in nauw overleg met het ministerie van Financiën voor wat betreft het Rijk) binnen de vier overheidslagen Rijk, provincies, gemeenten en waterschappen, experimenteren met het IT-verslag en de IT-verklaring. Indien deze experimenten succesvol zijn zal BZK het initiatief nemen om de ontwikkelde producten Europees en internationaal de standaard te maken.

Aanbeveling 7 *aan het Nederlandse kabinet:*

- Verplicht alle organisaties om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.

Gezien de grote verschillen tussen organisaties en sectoren dient het afleggen van verantwoording proportioneel te zijn aan de digitale veiligheidsrisico's. Het type eisen hangt af van de aard van een organisatie. Nederland zal de eerdergenoemde NIB2-richtlijn, waarin onder meer de verplichtingen voor aanbieders om adequate beveiligingsmaatregelen te treffen én incidenten met aanzienlijke gevolgen voor de dienstverlening te melden, implementeren in nationale wetgeving. De regels gelden specifiek voor sectoren met een hoog maatschappelijk belang (aanbieders van essentiële en belangrijke entiteiten). Met het oog op meer harmonisatie binnen de EU voorziet de NIB2-richtlijn verder in een ten opzichte van de huidige NIB-richtlijn uitgebreidere regeling van toezicht en handhaving en harmonisatie van sanctieregelingen en rapportageverplichtingen in de lidstaten.

Het OVV-rapport, en eveneens het Cybersecuritybeeld Nederland 2022, maken echter duidelijk dat het van belang is voor alle organisaties om digitale risico's te beheersen. Verantwoording afleggen over digitale risico's kent parallellen met het afleggen van verantwoording over alle risico's voor een organisatie, bijvoorbeeld in het bestuursverslag. Daarbij is het van belang om met het thema cybersecurity aan te sluiten bij de bestaande structuren die hiervoor zijn ingericht. De realisatie van de genoemde aanbeveling kan geschieden door wettelijke verankering in jaarrekeningrecht of door aanscherping van de Corporate Governance Code. In de volgende alinea zal op beide opties worden ingegaan.

In het bestuursverslag, legt het bestuur onder andere verantwoording af over het beleid dat in het betreffende jaar is gevoerd. Hiertoe zijn wettelijke vereisten gesteld die zijn vastgelegd in het Nederlandse jaarrekeningrecht en die gebaseerd zijn op de Europese kaders daarvoor. De verplichting om een bestuursverslag op te stellen geldt alleen voor beursgenoteerde bedrijven en voor alle middelgrote en grote bedrijven (2-4 % van Nederlands bedrijfsleven). Voor het grootste deel van de Nederlandse ondernemingen is die verplichting niet van toepassing, vanwege de proportionaliteit van de daarmee gepaard gaande administratieve lasten. Voor de ondernemingen waarvoor wel een verplichting geldt om een bestuursverslag op te stellen, acht het kabinet het wettelijk verankeren van een verplichting om daarin te rapporteren over cybersecurity-risico's, op dit moment niet opportuun, omdat de Europese Commissie de prioriteit heeft gelegd bij de verplichting om een duurzaamheidsrapportage op te stellen.

In de Corporate Governance Code (hierna: de Code) zijn principes en best practice bepalingen opgenomen die zich richten op het stimuleren van goede governance bij beursgenoteerde vennootschappen. De Code is een product van zelfregulering van

marktpartijen en regelt de verhoudingen tussen het bestuur, de raad van commissarissen en de (algemene vergadering van) aandeelhouders. De Code is wettelijk verankerd, wat betekent dat beursvennootschappen verantwoording afleggen over de naleving van de Code in het bestuursverslag. Daarnaast is de Code voor vele andere ondernemingen en instellingen een inspiratiebron en kiezen zij ervoor de Code vrijwillig toe te passen.

Voor een goede corporate governance zijn adequate interne risicobeheersings- en controlesystemen van belang. Risico's op het gebied van cybersecurity zijn hier een belangrijk onderdeel van. Daarom heb ik de aanbeveling uit het OVV-rapport ook onder de aandacht gebracht van de Monitoring Commissie Corporate Governance Code. Wij hopen samen in gesprek te gaan over dit onderwerp om te bespreken in hoeverre de Corporate Governance Code aansluit bij de aanbevelingen van de OVV en de, in ontwikkeling zijnde, Nederlandse Cybersecurity Strategie om de komende jaren om de digitale veiligheid van de Nederlandse samenleving en economie te versterken.

Tot slot
De Nederlandse Cybersecurity aanpak zal zich de komende jaren verder ontwikkelen. Ik blijf de voortgang van de Nederlandse Cybersecuritystrategie daarom nauw monitoren en ik zal de Tweede Kamer hierover periodiek informeren. Daarbij zal ik de OVV aanbevelingen in het oog houden. Tot slot dank ik de OVV voor het onderzoeksrapport en de daarin opgenomen aanbevelingen ter bevordering van de digitale veiligheid van Nederland. Het is van belang dat we van incidenten blijven leren en lessen blijven meenemen in de versterking van onze digitale veiligheid.

De minister van Justitie en Veiligheid,

D. Yesilgöz-Zegerius

De minister van Economische Zaken en Klimaat,

M.A.M. Adriaansens

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
Koninkrijksrelaties en Digitalisering

A.C. van Huffelen