Opvolging aanbevelingen *Kwetsbaar door software: Lessen naar aanleiding van beveiligingslekken door software van Citrix*

Publicatiedatum rapport: 16 december 2021

1. Over het rapport

De Onderzoekraad voor Veiligheid onderzocht beveiligingslekken die ontstonden door kwetsbaarheden in software van fabrikant Citrix. Op 17 december 2019 maakte Citrix een kwetsbaarheid in zijn software bekend en publiceerde het bedrijf tijdelijke maatregelen die organisaties die de software gebruiken konden nemen om de risico's te beperken. Zowel de fabrikant als vrijwillige beveiligingsonderzoekers vanuit onder meer het Dutch Institute for Vulnerability Disclosure (DIVD) zochten op internet welke Nederlandse organisaties nog kwetsbare software gebruikten en risico liepen aangevallen te worden. Deze informatie deelden zij met het Nationaal Cyber Security Centrum (NCSC). Het NCSC waarschuwde direct het deel van de Nederlandse gebruikers waarvoor zij zich verantwoordelijk achtte: overheidsdiensten en vitale organisaties. Andere organisaties werden door het NCSC niet gewaarschuwd.

Aanvallers konden op grote schaal digitale systemen binnendringen van organisaties die niet of niet op de juiste manier maatregelen hadden getrokken. Als zij in de tussentijd niet zijn opgemerkt hebben deze aanvallers tot op de dag van vandaag onbevoegd toegang tot systemen en data van deze organisaties die zij op elk moment kunnen activeren, met disruptieve effecten op bedrijfsprocessen, dienstverlening, privacy en veiligheid.

Uit het voorval blijkt dat Nederlandse overheidsorganisaties en bedrijven kwetsbaar zijn voor cyberaanvallen en dat er geen nationale structuur is waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd. Het onderzoek van de Onderzoeksraad voor Veiligheid laat zien dat kwetsbaarheden in software leiden tot onveiligheid voor organisaties die software gebruiken, en voor hen die van deze organisaties afhankelijk zijn. De kloof groeit tussen digitale afhankelijkheid en de dreigingsomvang enerzijds, en de weerbaarheid van de samenleving daartegen anderzijds. Snel en fundamenteel ingrijpen is nodig om te voorkomen dat de maatschappij ontwricht raakt.

Daarom doet de Onderzoeksraad in dit rapport zeven aanbevelingen. De eerste aanbeveling is erop gericht om op korte termijn de responscapaciteit te vergroten. De zes volgende aanbevelingen hebben als doel om op de langere termijn het publieke en private stelsel te versterken en prikkels te introduceren zodat er een systeem ontstaat waarbinnen fabrikanten en afnemers voortdurend werken aan het veiliger maken van software.

De Onderzoeksraad doet de aanbeveling om op Europees niveau kwaliteitseisen aan software te stellen om softwarefabrikanten te dwingen verantwoordelijkheid te nemen voor de veiligheid

van hun product. De Onderzoeksraad adviseert overheden en het bedrijfsleven hun krachten te bundelen. Door samen te werken kunnen ze hun positie richting softwarefabrikanten versterken en hun schaarse expertise beter benutten. Binnen de overheid kan de bewaking van de digitale veiligheid worden geregeld zoals de bewaking van het voeren van zorgvuldig begrotingsbeleid is vastgelegd in de Comptabiliteitswet. Ook beveelt de Raad aan dat grotere bedrijven en organisaties wettelijk worden verplicht om verantwoording af te leggen over de wijze waarop zij hun digitale veiligheid beheersen.

De volgende partijen hebben op de aanbevelingen gereageerd, op volgorde van ontvangst:

- Kamer van Koophandel (KVK), 21 maart 2022;
- Unie van Waterschappen (UvW), 14 april 2022;
- VNO-NCW, mede namens MKB-Nederland, 10 juni 2022;
- Business Software Alliance (BSA), 16 juni 2022;
- Citrix, 24 juni 2022;
- het kabinet, via de ministers van Justitie en Veiligheid (JenV) en Economische Zaken en Klimaat (EZK), en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (BZK), 10 oktober 2022.

De volledige reacties van de geadresseerde partijen zijn te vinden op de website van de Onderzoeksraad.[1]

Ondanks rappels hebben de volgende geadresseerde partijen geen reactie op de aan hen gerichte aanbevelingen gestuurd: de Eurocommissaris voor Interne Markt en de Eurocommissaris voor “een Europa dat klaar is voor het digitale tijdperk”, Vereniging Nederlandse Gemeenten, Land- en Tuinbouworganisatie LTO Nederland, Interprovinciaal Overleg; en softwarefabrikanten Ivanti, Fortinet, F5 en Palo Alto. Dat de partijen niet gereageerd hebben is een gemiste kans om te laten zien wat ze doen om digitale veiligheid te verbeteren.

Deze notitie bevat een algemene conclusie over de opvolging van aanbevelingen, gevolgd door een samenvatting van de ontvangen reactie per aanbeveling en een conclusie over de opvolging ervan.

[1] De Raad had een aantal partijen, waaronder de KVK, UvW en VNO-NCW, niet expliciet een aanbeveling gedaan, maar wel aangeschreven als zijnde binnen het stelstel relevante partijen.

2. Algemene conclusie over de opvolging

De maatschappij is vanwege de toenemende mate van afhankelijkheid van digitale systemen kwetsbaar voor cyberaanvallen. De potentiële gevolgen van deze aanvallen kunnen voor individuele organisaties – of zelfs voor de gehele nationale veiligheid – desastreus zijn. Organisaties hebben bij het gebruik van digitale systemen een verantwoordelijkheid om de veiligheid en beveiliging te waarborgen. Zij zijn daarbij mede afhankelijk van hoe fabrikanten hun verantwoordelijkheid voor veiligheid invullen. Dit vraagt ook een inspanning van overheden, toezichthouders en non-gouvernementele organisaties.

Om de veiligheid te vergroten heeft de Raad aanbevelingen gericht aan relevante betrokken partijen in binnen- en buitenland. Uit hun reacties blijkt dat de relevantie door de partijen wordt herkend. Het kabinet stelt in algemene zin dat cybersecurity een grensoverschrijdende maatschappelijke opgave is. Om dit het hoofd te bieden, heeft het kabinet de huidige Nederlandse Cybersecurity Strategie (NLCS) met bijbehorend Actieplan tot stand gebracht. Het vormt de strategie voor de komende zes jaar, tot 2028.[2] Het kabinet lijkt daarmee werk te maken van cybersecurity in Nederland. De kabinetsreactie laat echter zien dat het meerdere jaren gaat duren (tot 2026) tot alle randvoorwaarden zijn ingevuld om alle organisaties zo snel en doeltreffend te kunnen waarschuwen. Fabrikanten wijzen naar de verantwoordelijkheid van de afnemer en het ontbreken van een gelijk speelveld. Het is op dit moment nog niet duidelijk welk effect Europese horizontale regelgeving zal hebben op deze dynamiek.

De Raad vindt het hoopvol dat de partijen verschillende intenties uitspreken en acties benoemen die ze (gaan) ondernemen. De kloof tussen cyberdreiging en weerbaarheid wordt echter continu groter. De Raad roept de partijen dan ook op tot een voortdurende versnelling van het handelen om de digitale veiligheid te vergroten.

De Raad benadrukt verder dat veilige software allereerst de verantwoordelijkheid van de softwarefabrikanten is en dat het nodig is dat zij collectief actie ondernemen. Fabrikanten moeten meer investeren om de veiligheid van software voortdurend te verbeteren, zich aan deze voortdurende veiligheidsverbetering te committeren en afnemers inzicht bieden in de veiligheid van de software.

In deze notitie bespreekt de Raad de afzonderlijke reacties en spoort alle partijen nogmaals aan om snel en fundamenteel in te grijpen om te voorkomen dat de maatschappij ontwricht kan raken door cyberaanvallen.

3. Opvolging per aanbeveling

Aanbeveling 1

Aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken[3]

> 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.

Reactie kabinet

Het kabinet geeft in een uitgebreide beleidsreactie antwoord op de vraag hoe het met de aanbevelingen van de Onderzoeksraad omgaat. De reactie op aanbeveling 1 is thematisch geordend. Voor de overzichtelijkheid houdt de Raad die ordening hieronder aan.

Organisatie van cybersecurity informatiedeling

Het kabinet stelt dat binnen het zogenoemde Landelijk Dekkend Stelsel (hierna: LDS of het stelsel) *algemene informatie* over digitale veiligheid en specifieke risico's gedeeld kan worden. Doel van het stelsel is alle organisaties in Nederland, publiek en privaat, in staat te stellen hun weerbaarheidsniveau en hun slagkracht te verhogen via informatiedeling. Het kabinet noemt het stelsel "jong" (opgericht in kabinetsperiode 2017-20) en spreekt uit het stelsel de komende jaren te willen "doorontwikkelen" via de Nederlandse Cybersecuritystrategie (NLCS). Van belang daarbij noemt het kabinet om het stelsel "effectief en efficiënt in te richten met heldere aanspreekpunten", zonder de eigen verantwoordelijkheid uit het oog te verliezen.

Fragmentatie, zoals door de Onderzoeksraad gesignaleerd, moet volgens het kabinet "zoveel mogelijk voorkomen worden". Er is in 2022 een verkenning uitgevoerd om de betrokken

[3] Uit praktische overwegingen schrijft de Onderzoeksraad de overheid in zijn rol als afnemer aan via de staatssecretaris van Binnenlandse Zaken, het Interprovinciaal Overleg, de Vereniging van Nederlandse Gemeenten en de Unie van Waterschappen. De andere organisaties, waaronder zorg, onderwijs, vitale aanbieders en het overige bedrijfsleven schrijft de Raad aan via de bij de SER betrokken ondernemersorganisaties VNO-NCW, MKB Nederland en LTO Nederland.

diensten tot integratie te laten komen.[4] De diensten – het NCSC, DTC en CSIRT DSP[5] - hebben die intentie. De resultaten van de verkenning zijn volgens het kabinet positief, wat recent heeft geleid tot het verder uitwerken van de integratie in een zogenoemd programmaplan. Uit een separate Kamerbrief blijkt dat de volledige integratie van de genoemde diensten vorm moet krijgen tussen 2024 en 2026.[6] De NLCS en het bijbehorende actieplan bevatten handelingen die het kabinet aanvullend stelt te nemen om het stelsel verder te ontwikkelen.[7]

Een voor het kabinet belangrijk punt om te benoemen is dat in 2020 de zogenoemde Cyber Info/Intel Cel (CIIC) is opgericht. Dit betreft een samenwerkingsverband voor informatiedeling tussen AIVD, MIVD, NCSC en het Openbaar Ministerie. Dit verband ligt volgens het kabinet in lijn met de aanbeveling van de Raad om private en publieke responscapaciteit beter samen te brengen.[8] Het kabinet streeft er naar een samenwerkingsplatform op te richten waarin informatie kan worden gedeeld, geanalyseerd en gedistribueerd en heeft hiertoe onderzoek laten verrichten.[9]

Knelpunten bevoegdheden Rijksoverheid informatiedeling
Het kabinet stelt het eens te zijn met de aanbeveling van de Raad dat onwenselijke wettelijke obstakels rondom informatiedeling moeten worden weggenomen. In 2021 heeft het kabinet daartoe een inventarisatie verricht naar wettelijke bevoegdheden. De inventarisatie leidde ertoe dat het kabinet de Wet beveiliging netwerk- en informatiesystemen (Wbni) wil gaan wijzigen. Doel van de wetswijziging is “zo optimaal mogelijk” informatie-uitwisseling door het NCSC en andere organisaties mogelijk te maken. Het wetsvoorstel strekt ertoe het NCSC een ruimere bevoegdheid te geven om dreigings- en incidentinformatie (indien relevant) aan andere organisaties te kunnen verstrekken. Zo kunnen meer organisaties (direct of geschakeld) worden gewaarschuwd wanneer dat nodig is, aldus het kabinet. Het wetsvoorstel is op 4 oktober 2022 aangenomen in de Tweede Kamer en wordt dit jaar aangeboden aan de Eerste Kamer.

---

[4] Kamerbrief van de ministers van JenV en EZK, “Uitvoerder programmaplan sporen integratie CSIRT-DSP, DTC & NCSC”, kenmerk: 4196464, 13 september 2022. Hierin stellen de ministers: “De uitkomsten van deze verkenning dragen bij aan meer synergie en het tegengaan van versnippering binnen het overheidslandschap van cybersecurity en de wens tot nauwere samenwerking en integratie. De ambitie is om gezamenlijk een nieuwe organisatie te vormen die op het gebied van cybersecurity hét nationale expertisecentrum, informatieknooppunt én CSIRT is.”
[5] Resp. Nationaal Cyber Security Centrum, Digital Trust Center, Computer Security Incident Response Team voor digitale dienstverleners.
[6] Kamerbrief van de ministers van JenV en EZK, “Uitvoerder programmaplan sporen integratie CSIRT-DSP, DTC & NCSC”, kenmerk: 4196464, 13 september 2022.
[7] Zie met name hoofdstuk 3 van de NLCS, pp. 24-30.
[8] De Onderzoeksraad merkt op dat dit samenwerkingsverband momenteel alleen uit publieke organisaties bestaat.
[9] De uitkomsten staan in: P. Oldengarm en L. Mooy, “Cyclotron: Gezamenlijk sneller en gerichter delen van informatie rondom (dreigende) cyberincidenten in publiek-privaat verband”, 31 mei 2022.

Het kabinet noemt het Digital Trust Center. Het DTC informeert en adviseert ongeveer 2 miljoen niet-vitale bedrijven in Nederland hoe hun digitale weerbaarheid te verbeteren. Om taken en bevoegdheden van het DTC te verbeteren is onder andere het wetsvoorstel "bevordering digitale weerbaarheid bedrijven" opgesteld.[10] Volgens het kabinet worden niet-vitale bedrijven sinds de zomer van 2021 actief geïnformeerd over bij de overheid bekende ernstige digitale dreigingen en kwetsbaarheden.[11]

Het kabinet sluit zijn reactie op deze aanbeveling af met de constatering dat het nog niet in alle gevallen mogelijk is om potentiële slachtoffers te waarschuwen. Dit geldt bijvoorbeeld wanneer het gaat om persoonsgegevens (in het kader van onder meer de AVG). Daarom stelt het kabinet, onder coördinatie van JenV, een onderzoek in om vast te stellen "op welke manier doelwit- en slachtoffernotificatie uit niet-strafrechtelijke bron verder vormgegeven kan worden." Deze handelingen zijn ook opgenomen in het NLCS-actieplan.

Voor wat betreft voldoende wettelijke regeling van taken en bevoegdheden is, ten slotte, het thema "scannen" in relatie tot het NCSC van belang. Het NCSC heeft volgens het kabinet als wettelijke taak om technisch onderzoek te verrichten naar dreigingen en incidenten, en Rijksoverheid-gelieerde organisaties en vitale aanbieders daarover te informeren en adviseren. Voor die taakuitoefening scant het NCSC ook op kwetsbaarheden in digitale systemen van de genoemde organisaties, wanneer dat mogelijk is zonder de systemen van de organisaties binnen te dringen. Het NCSC beschikt echter niet over de wettelijke bevoegdheid te scannen zonder toestemming om dergelijke systemen binnen te dringen. De Europese NIB2-richtlijn (zie ook aanbeveling 2, 6 en 7 hieronder) leidt tot aanpassing van de scanbevoegdheden van het NCSC. Zo mag het NCSC scannen op kwetsbaarheden als organisaties daarvoor toestemming geven, of wanneer niet wordt binnengedrongen in de systemen van de organisatie.

Reactie Unie van Waterschappen (UvW)
De UvW stelt de aanbeveling te onderschrijven. De waterschappen – individueel en gezamenlijk – herkennen de toenemende digitale afhankelijkheid. Het onderwerp staat bij hen hoog op de bestuurlijke agenda, zo stelt de UvW. Sinds 2017 zijn de waterschappen aangesloten bij het CERT-WM[12]. Dat stelt hen in staat met andere partijen, waaronder

[10] De Raad van State heeft over dit wetsvoorstel positief advies uitgebracht. Het wordt dit najaar aangeboden aan de Tweede Kamer.
[11] De Onderzoeksraad heeft in zijn rapport gerefereerd aan de aankondiging van EZK op 13 september 2021 dat DTC een proef startte om bedrijven actief te informeren over digitale dreigingen. Het ging volgens dat bericht om 40 bedrijven In het vierde kwartaal van 2022 bestaat de pilot uit 57 bedrijven. https://www.digitaltrustcenter.nl/pilot-dtc-informatiedienst (Nederland kent 1,9 miljoen bedrijven waarvan ruim 400 duizend BV's, bron: CBS).
[12] Computer Emergency Response Team Watermanagement.

Rijkswaterstaat, samen te werken bij cyberaanvallen. Volgens de UvW heeft dit zijn meerwaarde bewezen bij recent ontdekte kwetsbaarheden, waaronder Apache Log4j.[13] De waterschappen onderzoeken de komende maanden de doorontwikkeling van het CERT-WM naar een centraler en proactiever orgaan. De UvW stelt dat de waterschappen hun digitale weerbaarheid regelmatig toetsen middels cyberoefeningen, en via audits door een gecertificeerd extern bureau. De UvW merkt echter ook op dat informatieveiligheid steeds meer geld en schaarse capaciteit kost. Daarom is de UvW verheugd met de aanbeveling van de Raad om het thema (inter)nationaal aan te pakken. Ook constateert de UvW dat samenwerking met andere overheden “nog heel versnipperd plaatsvindt”. Goede samenwerking met de betrokken ministeries van JenV, IenW, BZK en EZK kost de waterschappen veel tijd en energie, zo stelt de UvW. Het roept daarom op tot meer coördinatie op informatieveiligheid binnen de Nederlandse overheid.

Reactie VNO-NCW (mede namens MKB-Nederland)
VNO-NCW en MKB-Nederland stellen de aanbeveling toe te juichen. Informatiedeling is volgens de partijen cruciaal voor bedrijven om zich beter te kunnen wapenen tegen cyberaanvallen. De partijen vinden het een “zeer ongewenste situatie” dat het NCSC vooralsnog niet het mandaat heeft om incident- of dreigingsinformatie te delen met niet-vitale organisaties, en deze dus niet tijdig beschermingsmaatregelen kunnen nemen. VNO-NCW en MKB-Nederland noemen een aantal ontwikkelingen die hen “hoopvol stemmen”, waaronder met name aanpassingen van wet- en regelgeving in Nederland en de EU die informatiedeling verruimen en verkenningen voor meer en betere samenwerking.[14] VNO-NCW en MKB-Nederland geven aan hoopvol te zijn over deze ontwikkelingen, maar maken zich tegelijkertijd zorgen dat ze nog niet volledig zijn geëffectueerd. Dat baart VNO-NCW en MKB-Nederland zorgen: het ontvangen van informatie maakt de samenleving niet per definitie veiliger. Volgens de partijen moet er ook naar gehandeld worden. VNO-NCW en MKB-Nederland stellen dat ze bijdragen aan het opvolgen van de aanbeveling middels onder andere het voorlichten van hun leden, bijvoorbeeld het activeren van brancheorganisaties om digitale veiligheid actief onder te aandacht te brengen. Ze zijn een project getiteld “Samen Digitaal Veilig” gestart om met name kleinere bedrijven te helpen.

VNO-NCW en MKB-Nederland vinden nadere verkenning noodzakelijk om te bezien waar en hoe (respons)capaciteit effectief en efficiënt kan worden samengebracht. Volgens hen verschilt de respons namelijk per organisatie, afhankelijk van de rol en specifieke

[13] In december 2021 werd een ernstige kwetsbaarheid gevonden in open source component log4J, dat wereldwijd in talloze met name zakelijke softwarepakketten wordt gebruikt om dataverkeer te loggen. Dit leidde tot wat experts wel en cyberpandemie noemden, een onmetelijk aantal mogelijk door aanvallers binnengedrongen systemen.
[14] Genoemde voorbeelden betreffen: de aanpassing van de Wet Beveiliging Netwerk- en Informatiesystemen, zodat het NCSC breder mandaat krijgt om verruimd informatie te delen; de nieuwe meldplicht van de Telecomwet 11a.2 lid 4; de Richtlijn voor netwerk- en informatiebeveiliging.

dienstverlening binnen het “digitale ecosysteem”. De werkgeversorganisaties stellen dat de Onderzoeksraad in zijn rapport geen definitie heeft opgenomen van wat het verstaat onder ‘responscapaciteit’, maar gaat ervan uit dat het dit breed opvat.[15] Onder voorwaarden zijn de partijen voorstander van het dichter bij elkaar brengen van het NCSC en het DTC. De publiek-private samenwerking die plaatsvond tijdens de Log4j-perikelen zagen VNO-NCW en MKB-Nederland als een voor herhaling strekkend voorbeeld.

Conclusie over opvolging
De aanbeveling wordt niet op korte termijn opgevolgd. Het kabinet heeft de intentie uitgesproken om de aanbeveling op te zullen volgen, zoals blijkt uit de reactiebrief. Van belang is dat deze intenties op zo kort mogelijke termijn worden omgezet in concrete handelingen gericht op *alle* organisaties in Nederland.

Het kabinet beschrijft een aantal organisatorische maatregelen, zoals het integreren van organisaties en voorstellen die het breder delen van informatie mogelijk moeten maken. Uit het actieplan van het kabinet blijkt dat de acties die nodig zijn om alle potentiële slachtoffers zo snel en doeltreffend mogelijk te waarschuwen, jaren in beslag gaan nemen (tot 2026). Wel koppelt het kabinet het realiseren van de mogelijkheid om alle potentiële slachtoffers te waarschuwen los van bredere initiatieven (zoals genoemd in het *Cyclotron*-rapport). Dit wijst erop dat de rijksoverheid juist op het punt van deze eerste aanbeveling zo snel mogelijk resultaat wil boeken. Dat is een positief teken.

Ondanks de door het kabinet toegezegde voortdurende aandacht en doorontwikkeling van het systeem om organisaties tijdig te waarschuwen, wordt de kloof tussen cyberdreiging en weerbaarheid in de tussentijd continu groter. Dat een hoger tempo maatschappelijk noodzakelijk wordt gevonden, blijkt onder meer uit de stap die een aantal in Nederland actieve multinationals hebben genomen om zelf een organisatie op te richten om onderling informatie te delen over dreigende cyberaanvallen.[16] De rest van het Nederlandse bedrijfsleven moet wachten tot het kabinet en andere partijen in de komende jaren een aantal juridische en technische zaken regelen.

Ook uit de reactie van andere partijen, zoals werkgeversorganisaties VNO-NCW en MKB Nederland, blijkt dat zij het tempo waarmee de maatregelen voor verbetering van de cyberveiligheid van Nederland te laag vinden. In de tussentijd voorzien vrijwillige

[15] De Raad definieert “responscapaciteit” in het rapport, paragraaf 2.5 als: “incidentbestrijding (respons): dit zijn de activiteiten die plaatsvinden als het incident daadwerkelijk is opgetreden”.
[16] De stichting NL CCoT bestaat naast ASML uit ABN AMRO, Ahold Delhaize, Akzo Nobel, ING, KPN, Philips, Rabobank en Shell. De NS heeft aangegeven ook mee te willen doen. De stichting werkt daarbij nauw samen met het Nationaal Cyber Security Centrum (NCSC). Bron: https://fhi.nl/nieuws/nauwe-samenwerking-in-stichting-helpt-asml-en-andere-multinationals-cyberweerbaarheid-te-verhogen/.

beveiligingsonderzoekers via organisaties zoals het Security Meldpunt, DIVD en het Clean Networks Platform zo veel mogelijk organisaties te waarschuwen wanneer zij kwetsbare servers hebben: zo heeft DIVD in 2020 een kleine 60.000 waarschuwingen verstuurd en in 2022 tot dusver ruim 170.000 waarschuwingen.[17] Het kabinet noemt deze initiatieven niet in zijn reactie maar gaat in op de eigen rol. De Raad roept het kabinet op om dergelijke partijen beter en sneller te faciliteren.[18]

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.

Reactie Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:
Beide Eurocommissarissen hebben geen reactie op de aan hen gerichte aanbevelingen gestuurd naar de Onderzoeksraad. Rappels en contact met de Nederlandse permanente vertegenwoordiging en een aantal Nederlandse (voormalig) Europarlementariërs om een reactie te verkrijgen hebben geen effect gehad. Wel werd de Raad uitgenodigd om het rapport in te brengen in een Impact Assessment geïnitieerd door de Europese Commissie ten behoeve van de *Cyber Resilience Act*. De Onderzoeksraad heeft in openbare bronnen beleidsvoornemens en maatregelen aangetroffen en geanalyseerd, die gerelateerd kunnen worden aan onze aanbevelingen aan de Eurocommissarissen.

De Europese Commissie publiceerde in september 2022 een voorstel voor nieuwe horizontale wetgeving, de *Cyber Resilience Act*. Dit wetsvoorstel heeft betrekking op alle producten met digitale elementen, en reguleert daarmee zowel hardware als software. De voorgestelde wet is een zogenoemde EU-verordening en zal daarbij direct van toepassing zijn in alle lidstaten van de EU. De wet stelt eisen aan fabrikanten wat betreft digitale veiligheid in hun producten, zowel bij het ontwikkelen van deze producten[19], als wanneer er kwetsbaarheden worden gevonden. Het wetsvoorstel verplicht fabrikanten om gedurende de levensduur van een

[17] Bron: https://www.divd.nl/
[18] Zie ook de Slingelandtlezing van Michel van Eeten, hoogleraar cybersecurity aan de TU Delft. https://www.bestuurskunde.nl/2019/11/14/blussen-met-nullen-en-enen-cyber-rampen-cyber-exceptionalisme-en-de-rol-van-de-overheid/.
[19] Een aantal eisen ten aanzien van softwareontwikkeling is onder andere dat producten geleverd moeten worden zonder bekende kwetsbaarheden en met een ‘secure by default’-configuratie.

product (met een maximum van vijf jaar) kwetsbaarheden snel en effectief te verhelpen en afnemers hiervan op de hoogte te stellen. Daarnaast moeten producten een “verklaring van conformiteit” hebben, wat behelst dat ze aan de gestelde eisen moeten voldoen alvorens op de Europese market gebracht te mogen worden. Fabrikanten worden verplicht om informatie over de samenstelling van hun producten te delen met hun afnemers, en om begrijpelijke informatie aan afnemers te verstrekken over veilig gebruik en veilige configuratie van het product.

Reactie kabinet
Ondanks dat deze aanbeveling niet gericht was aan het Nederlandse kabinet, reageerde het er wel op. Het kabinet deed dit ook ten aanzien van aanbevelingen 3 en 4 (zie hieronder). Het kabinet stelt dat het deze de aanbevelingen van de Raad onder de aandacht van de Europese Commissie heeft gebracht. Het kabinet wil “een actieve en stimulerende rol vervullen” ten aanzien van de Europese Commissie en softwarefabrikanten om maatregelen te nemen grensoverschrijdende digitale veiligheid te vergroten. Concreet stelt het kabinet dit publiek-privaat te doen door het ontwikkelen en toepassen van cybersecurity certificeringsschema’s van ICT-gerelateerde producten, diensten en processen onder de Europese *Cyber Security Act* en *Cyber Resilience Act (CRA).* Het kabinet zet zich bij onderhandelingen over de CRA in voor “het duidelijker beleggen van een zorgplicht voor cybersecurity bij fabrikanten en leveranciers” om de positie van afnemers te versterken.

Conclusie over opvolging
De aanbeveling wordt gedeeltelijk opgevolgd. De Europese *Cyber Resilience Act* (vooralsnog een voorstel, dus nog niet geïmplementeerd) kan er in potentie voor zorgen dat het voor fabrikanten niet meer vrijblijvend is om te investeren in digitale veiligheid van hun producten als zij op de Europese markt willen opereren. Ook geeft het wetsvoorstel afnemers duidelijker inzicht in wat fabrikanten doen aan de veiligheid van producten, alsook waaruit de producten bestaan. De Europese Commissie legt in dit voorstel echter niet vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden. Uitgezonderd zijn zeer specifieke gevallen wanneer de gevolgen tot lichamelijk letsel hebben geleid. Een aantal andere in de toelichting op de aanbeveling genoemde aspecten komen niet voor in de CRA, namelijk: de al dan niet verplichte deelname aan zogenoemde *bug bounty* programma’s, het delen van lessen, en het organiseren van onafhankelijke audits. De Raad waardeert de inzet van het kabinet om de aanbevelingen onder de aandacht te (blijven) brengen bij de Europese Commissie. Aandacht voor het continu verbeteren van de veiligheid binnen en buiten Nederland en Europa zal hiermee ten goede komen.

Aanbeveling 3
Aan fabrikanten van software gezamenlijk[20]:

> Ontwikkel met andere fabrikanten good practices om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.

Reactie Citrix
In reactie op deze aanbeveling deelt Citrix een aantal *good practices* die het bedrijf naar aanleiding van het onderzochte voorval heeft ontwikkeld, zoals het verzamelen van contactgegevens van hun afnemers en een *call home* functie van de software. De fabrikant stelt daarnaast groot voorstander te zijn van cybersecuritystandaarden voor fabrikanten als het gaat om softwareontwikkeling, omdat brede toepassing standaarden effectiever maakt en cybersecurity in de breedte verbetert. Citrix maakt zelf gebruik van verschillende standaarden, waaronder NIST, ISO, Common Criteria en SOC2, maar is als individuele fabrikant slechts een schakel in een grotere keten.

Reactie Business Software Alliance (BSA)
BSA geeft in de reactie aan dat softwareontwikkeling “een ingewikkeld proces” is. Volgens de brancheorganisatie bevat software vaak talloze componenten met veel regels code, waardoor foutloze code weliswaar een doel moet zijn, maar niet realistisch is. BSA bevestigt daarmee de bevindingen van de Onderzoeksraad zoals vervat in zijn rapport. BSA geeft aan dat veel partijen een rol spelen in softwareveiligheid, dat het veilige gebruik van software vaak bij de afnemers van producten ligt, en dat de verantwoordelijkheid om de risico’s te beheersen ook daar neergelegd moeten worden. BSA stelt een zogenoemd *secure software framework* ontwikkeld te hebben voor stakeholders in de industrie - van fabrikanten tot afnemers – om veiligheid te evalueren en communiceren.

Conclusie over opvolging
De aanbeveling wordt niet opgevolgd. Citrix en BSA geven aan voorstander en volger te zijn van (bestaande) standaarden voor de ontwikkeling van veilige software. Citrix en BSA zeggen niet toe dat ze zich in overeenkomsten met hun afnemers zullen committeren aan het voldoen aan deze standaarden. Brancheorganisatie BSA legt de verantwoordelijkheid voor veilig gebruik van software hoofdzakelijk bij de afnemers. Ten slotte gaan de partijen niet in op het sector-breed ontwikkelen van *good practices*. De Onderzoeksraad benadrukt hierbij nogmaals dat veilige software allereerst de verantwoordelijkheid van de softwarefabrikanten is en dat het nodig is dat zij collectief actie ondernemen. De Raad stelt in het rapport dat fabrikanten

[20] Deze aanbeveling is gericht aan alle fabrikanten van software. Uit praktische overwegingen schrijft de Onderzoeksraad de fabrikanten aan die betrokken waren bij de voorvallen die dit onderzoek beschrijft, en de (leden van de) brancheorganisatie Business Software Alliance.

meer zouden moeten investeren om de veiligheid van software voortdurend te verbeteren en afnemers inzicht bieden in de veiligheid van de software.

Aanbeveling 4
Aan fabrikanten van software gezamenlijk[21]*:*

> 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.

Reactie Citrix
Citrix stelt "*security bulletins*" over kwetsbaarheden te publiceren. Het bedrijf geeft bepaalde afnemers daarnaast vooraankondigingen over kwetsbaarheden. Citrix geeft aan hun afnemers aan te moedigen om "security contact details" te verschaffen, maar dat het initiatief hiervoor bij de afnemer ligt.

Reactie Business Software Alliance
BSA geeft aan dat het zogenoemde *coordinated vulnerability disclosure* goed ontwikkeld is in de branche. De partij gaat in de reactie niet in op het waarschuwen van afnemers door fabrikanten.

Conclusie over opvolging
De aanbeveling wordt niet opgevolgd. Citrix is bereid klanten te waarschuwen die zich daarvoor bij hen aanmelden. De andere aangeschreven fabrikanten hebben niet op de aanbeveling gereageerd. Brancheorganisatie BSA gaat niet in op het waarschuwen van afnemers door fabrikanten nadat zij een kwetsbaarheid hebben gesignaleerd, in weerwil van de in het OVV-rapport geconstateerde gebreken.

[21] Ibid.

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)[22]

> 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.

Reactie kabinet (staatssecretaris van BZK en minister van EZK)

Het kabinet stelt de aanbeveling te omarmen. De aanbeveling sluit volgens het kabinet aan op al lopende en voorziene inzet vanuit de overheid. Het kabinet stelt dat de overheid het als haar taak ziet “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.” Het kabinet noemt de overheid “een belangrijke marktpartij”, omdat alle overheidsorganisaties gezamenlijk jaarlijks veel ICT-producten en -diensten inkopen. Om de in de aanbeveling genoemde doelstellingen te helpen verwezenlijken, levert het zogenoemde programma Inkoopeisen Cybersecurity Overheid (ICO) daartoe instrumenten, zoals sets van inkoopeisen en een basisprocesbeschrijving. Het overheidsbeleid is er volgens het kabinet op gericht ICO een vaste plek te geven in het overkoepelende inkoopproces van alle Nederlandse overheden. Op termijn worden de normensets verplicht en “doorvertaald” conform Europese wet- en regelgeving, in het bijzonder de Cyber Security Act, aldus het kabinet.

Voor wat betreft bescherming van consumenten memoreert het kabinet dat sinds april 2022 de Implementatiewet van kracht is, waardoor specifiek de Europese richtlijnen “verkoop goederen” en “levering digitale inhoud” in Nederland worden geïmplementeerd.[23] De wet- en regelgeving moet aan- en verkoop van goederen en digitale inhoud veiliger en gemakkelijker maken. Concreet noemt het kabinet het voorbeeld dat consumenten hiermee recht hebben op (veiligheids-)updates van software “zolang zij die redelijkerwijs mogen verwachten”. Op deze

[22] Vanwege de relevantie van veilige software voor eindgebruikers (inclusief consumenten) dient ook de Consumentenbond hierbij te worden betrokken. En de KVK voor ondersteuning aan organisaties.
[23] In de beleidsreactie stelt het kabinet hieromtrent: “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 mag verwachten, en de consument hiermee instemt.”

wet- en regelgeving zal de Autoriteit Consument en Markt (ACM) toezicht houden. In dit verband noemt het kabinet verder dat “draadloos verbonden apparaten” die vanaf augustus 2024 op de Europese markt komen, moeten voldoen aan wettelijke cybersecurityeisen. Doen de producten dit niet, dan kunnen ze van de markt worden gehaald en geweerd. Agentschap Telecom ziet hierop toe.

Het kabinet sluit zijn reactie aangaande deze aanbeveling af met de intentie om de positie van softwaregebruikers te versterken via verankering van veiligheidseisen aan fabrikanten in de Europese CRA. In overleg met brancheorganisaties verkent het ministerie van EZK, ten slotte, hoe het heldere contractuele afspraken tussen leveranciers en afnemers kan stimuleren.

Reactie Kamer van Koophandel
De KVK stelt de aanbeveling te onderkennen door te wijzen op het belang van informatievoorziening en advisering over digitalisering. De KVK stelt echter dat het “niet een logische partij” is om hierbij te ondersteunen. De KVK geeft als reden dat dit veel verder zou gaan dan de wettelijke rol die de KVK daadwerkelijk heeft. Brancheorganisaties zijn volgens de KVK de meest aangewezen organisaties om een voortrekkersrol te nemen in informatievoorziening en advisering.

Conclusie over opvolging
De aanbeveling wordt gedeeltelijk opgevolgd. Het kabinet werkt aan wettelijke eisen waaraan fabrikanten moeten voldoen. Voor wat betreft aan het internet verbonden consumentenproducten zal de ACM toezicht gaan houden en afdwingen dat fabrikanten zich aan de wettelijke eisen houden. Voor zakelijke software is dat nog niet geregeld, maar ziet het kabinet mogelijkheden om dat via de Europese *Cyber Resilience Act* te gaan regelen. De Raad vindt het door het kabinet genoemde punt over het recht van consumenten om software-updates te krijgen een terechte, maar benadrukt tegelijkertijd dat het zou moeten gaan om eisen aan de voorkant. Een update is immers een reparatie achteraf, de potentiële onveiligheid is dan al een feit. Voor wat betreft het programma ICO en het punt met de schaarse expertise acht de Onderzoeksraad dat dan nog steeds elke organisatie zelf moet beoordelen of de producten aan die inkoopeisen voldoen. Dus met alleen een set inkoopeisen ben je als bedrijf of kleine overheidsorganisatie nog niet geholpen. De vraag blijft, kortom, hoe het kabinet die eisen gezamenlijk gaat (laten) afdwingen. De rol die de overheid hier voor zichzelf ziet – als voortrekker en goed opdrachtgever – is een niet geringe ambitie.

De KVK ziet voor zichzelf geen rol om in dit proces organisaties te ondersteunen, omdat dit buiten hun wettelijke taak zou liggen en beter zou passen bij brancheorganisaties. De Onderzoeksraad ziet in de wet op de KVK ruimte om daarin wel een rol te vervullen.[24] De

[24] Wet op de KvK: Er is een Kamer van Koophandel die tot doel heeft het stimuleren van economische ontwikkeling door middel van het informeren en ondersteunen op het gebied van ondernemen en

Raad acht het noodzakelijk dat afnemers hun krachten bundelen zodat zij hun positie richting fabrikanten kunnen versterken en schaarse cybersecurity-expertise gezamenlijk zo doelmatig en effectief mogelijk inzetten.

Aanbeveling 6
Aan het Nederlandse kabinet:

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

Reactie kabinet
Volgens het kabinet is het ministerie van BZK stelselverantwoordelijk en daarmee normsteller voor het opstellen van (wettelijke) kaders door de overheid voor de digitale veiligheid van Nederland. Er komt een zorgplicht voor informatieveiligheid, alsook overheids-breed toezicht. Het kabinet regelt de aspecten van plicht en toezicht in de aanstaande Wet Digitale Overheid (WDO) en andere relevante regelgeving. Het kabinet noemt daarbij de NIB2-richtlijn, die verplicht lidstaten om centrale overheden onder de reikwijdte van de richtlijn te brengen. De nationale implementatie van de richtlijn voor de overheid wil het kabinet gelijk laten oplopen met het regelen van de genoemde zorgplicht en toezicht.

Het kabinet stelt “tot een eenduidig, eenvoudig en geharmoniseerd stelsel” te komen “waarin gepaste interbestuurlijke handhaving” een plaats krijgt. Om dit te concretiseren stelt het kabinet dat in de WDO een eis van een jaarlijks IT-verslag en –verklaring zal worden opgenomen, ter ondersteuning van het toezicht. Volgens het kabinet versterkt dit “het horizontale toezicht en vergemakkelijkt de verticale verantwoording.” Totdat de verplichte IT-verklaring in de WDO wordt opgenomen, zal BZK er in overleg met alle vier overheidslagen mee experimenteren. Het kabinet zegt dat het Europees en internationaal het initiatief zal nemen om de ontwikkelde producten de standaard te maken, indien de experimenten succesvol zijn.

Conclusie over opvolging
De aanbeveling wordt opgevolgd. Het kabinet gaat onder andere een zorgplicht voor informatieveiligheid en overheidsbreed toezicht regelen in de WDO en/of andere gepaste regelgeving.

---

innovatie van personen die een onderneming drijven of overwegen een onderneming op te richten. Op dit moment adviseert de KvK al over wat ondernemers kunnen doen om het risico op een cyberaanval te verlagen en welke wet- en regelgeving op dat gebied relevant voor hen is. De KvK werkt onder meer samen met het DTC.

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.[25]

Reactie kabinet
Het kabinet benoemt allereerst dat er grote verschillen bestaan tussen organisaties en sectoren, waardoor het afleggen van verantwoording proportioneel moet zijn aan het beheersen van digitale veiligheidsrisico's. Het kabinet implementeert de eerdergenoemde NIB2-richtlijn in nationale wetgeving. De richtlijn verplicht aanbieders onder andere om adequate beveiligingsmaatregelen te treffen en om incidenten te melden. Dergelijke zaken gelden specifiek voor sectoren "met een hoog maatschappelijk belang", zoals "aanbieders van essentiële en belangrijke entiteiten". Onder deze richtlijn vallen nu meer sectoren dan onder zijn voorganger, zoals de zorg. Het midden- en kleinbedrijf valt er niet onder, terwijl daar ook bedrijven bij zijn die een grote impact hebben op de digitale veiligheidsrisico's van hun klanten. Het kabinet erkent dat het voor *alle* organisaties van belang is om digitale risico's te beheersen. Daarover verantwoording afleggen kent volgens het kabinet parallellen met verantwoordingsaflegging van andersoortige risico's. Het kabinet acht het van belang om met het thema cybersecurity aan te laten sluiten bij bestaande structuren die er voor zijn ingericht.

Het kabinet ziet twee mogelijkheden voor de opvolging van deze aanbeveling: in het bestuursverslag via wettelijke verankering in het jaarrekeningenrecht, of door aanscherping van de zogenoemde *Corporate Governance Code* (CCG). Voor wat betreft het bestuursverslag acht het kabinet het niet opportuun dit wettelijk te verankeren, omdat dit voor slechts twee tot vier procent van het Nederlandse bedrijfsleven zou gelden. Niet-beursgenoteerde bedrijven, het overgrote deel van de Nederlandse ondernemingen, kennen deze plicht niet "vanwege de proportionaliteit van de daarmee gepaard gaande administratieve lasten." De CCG bevat principes en bepalingen voor het stimuleren van *good governance* bij beursgenoteerde vennootschappen. Volgens het kabinet passen veel andere organisaties de CCG vrijwillig toe. Daarom heeft het kabinet deze aanbeveling onder de aandacht gebracht bij de zogenoemde Monitoring Commissie CCG.

[25] Het ligt in de rede om aan te sluiten bij bestaande structuren en verplichtingen in de Comptabiliteitswet 2016 (van toepassing op overheden), Burgerlijk Wetboek (niet-beursgenoteerde rechtspersonen), nadere voorschriften controle- en overige standaarden (NV COS) vanuit de NBA en geharmoniseerde wetgeving voor naamloze vennootschappen vanuit de EU.

Conclusie over opvolging

Het kabinet onderschrijft hiermee de strekking van de aanbeveling, maar gaat uit van vrijwilligheid. De aanbeveling wordt daarom vooralsnog niet opgevolgd. De door het kabinet genoemde aspecten rondom proportionaliteit zijn gericht op aandeelhouders.[26] Bedrijven zonder aandeelhouders hebben qua informatiebeveiliging ook belangrijke verantwoordelijkheden richting andere bedrijven in de keten. Daarbij is de omvang van het risico dat zij voor anderen die zaken met hen doen veroorzaken niet perse evenredig met hun omvang, maar met de functie die zij vervullen in het proces van hun klant of zakenpartner. Denk daarbij bijvoorbeeld aan een kleine organisatie die een betaalsysteem levert of een digitaal platform voor een groep aangesloten organisaties beheert.

De tijd moet uitwijzen of het uiteindelijke doel (dat de meeste bedrijven via hun jaarverslag verantwoording afleggen over hoe zij hun digitale veiligheidsrisico's beheersen) met vrijwillige toepassing van de CCG wordt bereikt. De aanbeveling bevatte overigens meer aanknopingspunten voor hoe de beheersing en verantwoording kunnen worden vormgegeven, waaronder een eenduidig mandaat voor CISO's. Op de meeste genoemde aanknopingspunten gaat het kabinet niet in.

[26] De Raad hanteerde de term "eenduidig" in zijn aanbeveling. De term "proportioneel" had passender geweest, om bedacht te zijn op de grote verscheidenheid aan organisaties en sectoren en dito manieren van verantwoordingaflegging.