Naar een open, veilig en welvarend digitaal Nederland

Advies inzake de Nederlandse Cybersecurity Agenda (NCSA)

CSR
Cyber Security Council
Cyber Security Raad

‘Naar een open, veilig en welvarend digitaal Nederland’

Advies inzake de Nederlandse Cybersecurity Agenda (NCSA)

Gericht aan:

De minister van Justitie en Veiligheid

Kopie aan:

De minister van Onderwijs, Cultuur en Wetenschap
De staatssecretaris van Economische Zaken en Klimaat
Voorzitter VNO-NCW

CSR
Cyber Security Council
Cyber Security Raad

25 juni 2018

CSR-advies 2018, nr. 1

Excellentie,

Hierbij ontvangt u het advies van de Cyber Security Raad (CSR) ten aanzien van de Nederlandse Cybersecurity Agenda (NCSA) 'Nederland digitaal veilig'.

Inleiding

Nederland moet een veilige, open en welvarende samenleving zijn en blijven. De ontwikkelingen in het digitale domein bieden veel economische en maatschappelijke kansen die alleen kunnen worden verzilverd als Nederland digitaal veilig is. Nieuwe technologieën ontwikkelen zich razendsnel en zijn een belangrijke drijfveer voor innovatie en economische groei. De impact en snelheid waarmee technologie zich ontwikkelt vragen om een dynamische aanpak die aangepast moet kunnen worden aan veranderende dreigingen. Nederland heeft een goede uitgangspositie om de economische kansen van de digitale toekomst voluit te benutten en innovatie te bevorderen. Onlangs verscheen de Nederlandse Digitaliseringsstrategie[1] met 24 bijbehorende ambities waarmee het kabinet bijvoorbeeld het verdienvermogen van Nederland verder wil versterken en zorgen voor betere digitale vaardigheden en cyberveiligheid in de maatschappij. Het is daarom des te belangrijker dat de randvoorwaarden voor economisch succes goed worden geborgd: veiligheid, vertrouwen en betrouwbaarheid van de digitale infrastructuur. Dit is niet vanzelfsprekend gezien de constante toename van de cyberdreigingen en de groeiende (digitale) afhankelijkheid van technologische toepassingen. Cybersecurity is een cruciale randvoorwaarde om de kansen die digitalisering onze samenleving biedt te verzilveren, dreigingen het hoofd te bieden en fundamentele rechten en waarden te beschermen. Het Cybersecuritybeeld Nederland 2018 (CSBN)[2] laat zien dat de digitale dreiging omvangrijk en permanent is. De weerbaarheid staat onder druk door de complexiteit en connectiviteit van de digitale infrastructuur. Incidenten binnen Nederland en Europa hebben in de afgelopen jaren laten zien dat digitale aanvallen een grote impact op de samenleving kunnen hebben. Dit onderstreept de noodzaak om te blijven investeren in onze digitale veiligheid.
De NCSA is, in combinatie met de onlangs verschenen National Cyber Security Research Agenda (NCSRA III)[3] een belangrijk instrument om de komende jaren in publiek, privaat én wetenschappelijk verband de cybersecurity van Nederland aan te pakken.

Nederlandse Cybersecurity Agenda (NCSA)

Op vrijdag 20 april jl. heeft de minister van Justitie en Veiligheid de NCSA aangeboden aan de Tweede Kamer. De agenda is tot stand gekomen in nauwe samenwerking tussen diverse overheidspartijen, private organisaties, wetenschappelijke en maatschappelijke partners. De agenda valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling:

Nederland is in staat op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.

De zeven ambities zijn:

1. Nederland heeft zijn digitale slagkracht op orde
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software

[1] Nederlandse Digitaliseringsstrategie, Ministerie van Economische Zaken en Klimaat, 2018
[2] Cybersecuritybeeld Nederland 2018 (CSBN 2018), Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie, 's-Gravenhage
[3] National Cyber Security Research Agenda III (NCSRA III), dcypher, 2018

4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity

De NCSA bouwt voort op de effecten die zijn gerealiseerd bij de eerdere nationale cybersecurity-strategieën uit 2011 en 2013[4] en levert een belangrijke bijdrage aan de verhoging van de digitale weerbaarheid van ons land. De NCSA doet gestand aan het regeerakkoord 2017-2021.[5] De Roadmap Digitaal Veilige Hard- en Software ('Roadmap DVHS'), die onderdeel is van de agenda, beoogt de benodigde samenhangende aanpak te bieden om als Nederland voorop te lopen bij het bevorderen van de digitale veiligheid van hard- en software.

De NCSA richt zich op de uitdagingen die wij als land hebben om een veilige, open en welvarende samenleving te blijven. Niet alleen de digitale weerbaarheid staat onder druk. De transformatie die door de komst van de digitalisering geïnstigeerd is, vraagt dringend om duiding. Vooralsnog is cybersecurity gericht op de bescherming van systemen tegen internationale dreigingen met risicomanagement als belangrijkste methode. Maar zien we daarmee de volledige reikwijdte en impact van de cybersecurity-vraagstukken die op ons afkomen? [6] Het cybersecuritylandschap is weerbarstig en brengt ook nieuwe maatschappelijke, juridische en ethische vraagstukken met zich mee en is zodanig complex dat regie, sturing en heldere kaders noodzakelijk zijn. Om deze ambities te verwezenlijken zijn er naast visie, strategie en slagkracht ook investeringen nodig. Daarbij zijn toekomstgericht leiderschap en een actieve en samenwerkingsgerichte houding van de overheid, de private partijen en de wetenschap noodzakelijk.

De raad ondersteunt en omarmt de ambities en de doelstellingen van de NCSA en is positief over het feit dat cybersecurity als integraal onderdeel van de nationale veiligheid wordt gezien. De uitgangspunten en doelstellingen passen in de wens van de raad tot actieve samenwerking tussen de overheid, de private partijen en de wetenschap alsook meer samenhang in de aanpak en een vooraanstaande rol van Nederland in EU en NAVO-verband. De raad herkent de opvolging van zijn eerdere adviezen in de NCSA. De invoering van onder andere de Roadmap DVHS en het onlangs gelanceerde Digital Trust Center (DTC) ziet de raad als waardige opvolging van zijn adviezen.

[4] Nationale Cybersecurity Strategie 1 'Slagkracht door samenwerking' (2011) en Nationale Cybersecurity Strategie 2 'Van bewust naar bekwaam' (2013), Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie, 's-Gravenhage

[5] Regeerakkoord 2017 - 2021 'Vertrouwen in de toekomst'

[6] De Cyberrevolutie: pak me dan als je kan. Oratie uitgesproken door Prof. dr. B. van den Berg, Universiteit Leiden, 2018

ADVIES

Er staat in het nieuwe digitale tijdperk veel op het spel voor ons land. Nederland heeft de ambitie om de economische kansen te verzilveren, innovatie te bevorderen en onze digitale positie vast te houden; Nederland moet een veilige, open en welvarende samenleving zijn en blijven. *Dit gaat niet vanzelf.* De digitale ontwikkelingen gaan razend snel en spelen zich af in een complexe internationale omgeving waardoor de consequenties voor de nationale welvaart en de veiligheid niet altijd direct zichtbaar zijn. Het is hiervoor van belang dat fundamentele vraagstukken worden geadresseerd, zoals de gevolgen van onze groeiende (digitale) afhankelijkheid, de mate waarin we kunnen en willen beschikken over fall-backopties en onze soevereiniteit. *We moeten beschermen wat van ons is.* Daarom moet cybersecurity hoog op de nationale en Europese politieke agenda staan.

In dit advies geeft de raad aan waar de komende jaren de focus op moet liggen en welke onderwerpen uit de NCSA nadere aandacht verdienen.

1. **Inventarisatie en besluitvorming fundamentele vraagstukken**
2. **Slagvaardige en samenhangende implementatie van de NCSA**
3. **Structureel investeren in cybersecurity**

Ad 1. Inventarisatie en besluitvorming fundamentele vraagstukken

De verregaande digitalisering van de samenleving vraagt om een weerbare samenleving die ook de sociaal maatschappelijke en economische gevolgen van de groeiende (digitale) afhankelijkheid van de verregaande digitalisering overziet en begrijpt. Alleen dan kunnen er bewuste keuzes worden gemaakt en kan tijdig en effectief worden gereageerd op kansen en bedreigingen. De vraagstukken spelen zich af in een complex internationaal speelveld dat geen *level playing field is.* In het digitale domein is het lastig om een balans te vinden tussen de kernwaarden.
Nederland streeft naar een vrije, veilige en welvarende samenleving. Deze drie belangrijke kernwaarden komen om verschillende redenen steeds meer onder druk te staan. Door de digitale ontwikkelingen komen belangrijke publieke waarden en mensenrechten als privacy, gelijke behandeling, autonomie en menselijke waardigheid in het geding.[7]

[7] Cybersecuritybeeld Nederland 2018 (CSBN 2018), Nationaal Coördinator Terrorismebestrijding en Veiligheid, Ministerie van Veiligheid en Justitie, 's-Gravenhage

Fundamentele waarden, zoals transparantie, privacy en veiligheid en vrijheid van meningsuiting, staan soms met elkaar op gespannen voet. Het beschermen van fundamentele rechten en waarden vergt inzicht in de vraagstukken en een open dialoog tussen alle betrokken partijen.

Nederland moet op korte termijn beter voorbereid zijn op deze ontwikkelingen door de vraagstukken te adresseren en heldere standpunten in te nemen die passen binnen het gedachtegoed van onder meer de EU en NAVO. Internationale ontwikkelingen zijn van grote invloed op de soort en de mate waarin we bepaalde maatregelen kunnen treffen. Een belangrijke vraag is dan ook hoe ver we kunnen en willen gaan bij het naleven van de kernwaarden in het belang van een open, veilige en welvarende digitale samenleving. De hang naar economisch groei kan op gespannen voet komen te staan met de veiligheid van producten en diensten – marketing before security. Een voorbeeld van een fundamenteel vraagstuk is de wens om als land open te zijn en controle te houden over de eigen data. Dit staat haaks op het feit dat de Nederlandse digitale infrastructuur inmiddels afhankelijk is van veelal buitenlandse dienstverleners. Door de sterke marktpositie van deze bedrijven, beschikken zij over meer middelen om hun producten en diensten tegen cyberaanvallen te beschermen. Dit lijkt op het eerste gezicht vooral positief, omdat hierdoor onze data beter worden beschermd.

Het is echter noodzakelijk dat er beter zicht komt op welke strategische technologische assets Nederland op (middel)lange termijn nodig heeft om haar cyberveiligheid te waarborgen zonder afhankelijk te zijn van buitenlandse aanbieders. De afhankelijkheid van een groot aantal bedrijven van een klein aantal hoofdzakelijk buitenlandse aanbieders, heeft verder tot gevolg dat de maatschappelijke impact bij verstoringen groot kan zijn. De vraag is hoe afhankelijk ons land is of wil zijn van andere landen en/of organisaties met een monopoliepositie. Hoe wenselijk vinden wij dit? In hoeverre streven we naar digitale autonomie en zijn wij bereid te investeren in oplossingen? Dit zijn slechts enkele voorbeelden van fundamentele vraagstukken en daarmee niet uitputtend.

Overheid, bedrijfsleven en samenleving zijn nog niet adequaat uitgerust om met deze nieuwe vragen om te gaan. Inadequaat reageren op fundamentele vraagstukken kan grote gevolgen hebben. De raad is van mening dat er snel zicht moet komen in de vraagstukken die van invloed zijn op bovengenoemde kernwaarden. Het is belangrijk dat er door politiek en overheid duidelijke standpunten worden ingenomen over de meest fundamentele vraagtukken. De raad adviseert dat de verschillende aspecten van cybersecurity in samenhang worden besproken in de vaste Kamercommissies en ziet hier voor zichzelf een rol weggelegd om de onderwerpen te adresseren en adviserend op te treden.

- *De raad adviseert dat er op korte termijn een inventarisatie wordt gemaakt van de strategische en technische assets die Nederland nodig heeft om haar cybersecurity te waarborgen.*
- *De raad adviseert dat er een inventarisatie wordt gemaakt van de belangrijkste maatschappelijke, juridische en ethische vraagstukken in relatie tot cybersecurity. Op basis van de inventarisatie moeten belangenafwegingen worden gemaakt.*
- *De raad adviseert een maatschappelijk debat over de maatschappelijke, juridische en ethische vraagstukken in relatie tot cybersecurity en de vertaling daarvan naar visie, beleid, wet- en regelgeving.*
- *De raad adviseert dat de verschillende aspecten van cybersecurity in samenhang worden besproken in de Tweede Kamer.*
- *De raad vindt het belangrijk dat Nederland hierin een vooraanstaande rol speelt binnen de Europese Unie en in internationaal verband.*

Ad 2. Slagvaardige en samenhangende implementatie van de NCSA

De cybersecurityvraagstukken zullen nog complexer en omvangrijker worden en cybercrime blijft toenemen. De fysieke en digitale wereld raken steeds verder met elkaar vervlochten. Het zal effect hebben op onder andere werkgelegenheid, gezondheidszorg, mobiliteit en welvaart en dwingt ons om continu alert te blijven en voorbereid te zijn op alle mogelijke scenario's. Het is belangrijk dat we slagvaardig kunnen reageren op misstanden en/of cyberaanvallen. Overheid, bedrijfsleven en burgers ondernemen stappen om de weerbaarheid te vergroten, maar dit gaat niet snel genoeg. *Daarom mag de uitvoering van de van de NCSA geen vertraging oplopen*.
De raad constateert dat de ambitie van de NCSA hoog is en dat het succes in sterke mate afhangt van de inzet van een groot aantal verschillende stakeholders. Dit kan de uitvoering van de NCSA een langdurig proces maken. De raad adviseert dan ook een prioritering aan te brengen in de gestelde ambities, doelstellingen en maatregelen en zorg te dragen voor een strakke regie en alert optreden bij dreigende vertraging.
Voor een slagvaardige uitvoering is het nodig om naast prioritering een gezamenlijke koers uit te zetten en de benodigde samenwerking te stimuleren. Door een goede aansluiting op veelbelovende initiatieven die ons land rijk is kan er sneller resultaat worden bereikt. Daarnaast adviseert de raad met voorrang te investeren in kennisontwikkeling.

Gezamenlijke koers en stimulering samenwerking

Een succesvolle implementatie vraagt om een gezamenlijke koers en goede afstemming tussen de overheid, de private partijen, het maatschappelijk middenveld en de wetenschap. De NCSA zet in op een integrale cybersecurity-aanpak. Dit vraagt een gezamenlijke inzet van het bedrijfsleven, maatschappelijke organisaties en van verschillende overheidspartijen. Dit jaar is een aantal strategieën die (mede) in het teken staan van cybersecurity verschenen en staat er een aantal op het punt te verschijnen[8], De onderlinge samenhang van deze strategieën verdient de volle aandacht. De raad is van mening dat er veel aandacht is geweest voor onderlinge afstemming bij de totstandkoming van de strategieën en dat dit proces nog steeds gaande is. Echter, aandacht voor afstemming is ook nodig bij de uitvoering van de diverse plannen.
Niet alleen vanuit Nederland, maar ook vanuit de Europese Unie worden initiatieven genomen die om afstemming vragen, zoals de Wet beveiliging netwerk- en informatiesystemen (Wbni), die voortvloeit uit de Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn) en het voorstel voor de nieuwe Europese cyberbeveiligingsverordening van de Europese Unie.

Het afstemmen van zowel de *inhoud* als de *uitvoering* van de verschillende strategieën, wettelijke kaders en agenda's is randvoorwaardelijk om een integrale aanpak te kunnen ontwikkelen.

- *De raad adviseert om onderlinge afstemming van de verschillende cybersecurity-strategieën en waar mogelijk een gezamenlijke implementatie.*
- *De raad vraagt overheidsorganisaties om zorg te dragen voor voldoende aandacht voor cybersecurity en de aanpak van kwetsbaarheden in systemen in alle relevante (cyber- en digitaliserings)strategieën*.

[8] Naast de NCSA zijn dit jaar de Notitie 'Wereldwijd voor een veilig Nederland', Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022 van het ministerie van Buitenlandse Zaken (waarin cyberdiplomatie een prioriteit is), de Nationale Digitaliseringsstrategie van het ministerie van Economische Zaken en Klimaat (EZK) en de National Cyber Security Research Agenda III (NCSRA III) van dcypher verschenen. In 2017 kwam het ministerie van Buitenlandse Zaken ook uit met de internationale Cyberstrategie 'Digitaal bruggen slaan' en is tevens het adviesrapport 'Maak Waar' van het ministerie van Binnenlandse Zaken en koninkrijksrelaties (BZK) verschenen. Naar verwachting worden de volgende strategieën nog gepresenteerd: de Defensie Cyber Strategie van het ministerie van Defensie, de Agenda Digitale Overheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en de Integrale aanpak cybercrime van het ministerie van Justitie en Veiligheid.

De raad vindt dat er vanuit de verschillende verantwoordelijke partijen een samenhangend beroep moet worden gedaan op de inzet van de overheid, de private partijen, het maatschappelijk middenveld en de wetenschap. In dit kader omarmt de raad het voorstel voor de Cybersecurity Alliantie. De overheid staat wat de raad betreft aan de lat voor het vervullen van een krachtige regierol. De raad adviseert dat er vanuit de overheid wordt gekeken naar positieve stimulans om de benodigde samenwerking vorm te geven, zoals onder andere genoemd in het advies van de raad over informatie-uitwisseling.[9]

- *De raad adviseert dat er in samenhang een beroep moet worden gedaan op de inzet van de overheid, de private partijen, het maatschappelijk middenveld en de wetenschap als het gaat om cybersecurity. De raad adviseert dat ook de in de agenda genoemde Cybersecurity Alliantie dit als aandachtspunt meeneemt.*
- *De raad adviseert dat er ook gekeken wordt naar positieve stimulans om de benodigde samenwerking vorm te geven.*

Aansluiting op lopende initiatieven

Nederland is in beweging en dat is een goede zaak. De afgelopen jaren zijn door diverse nationale stakeholders initiatieven ontplooid op het gebied van cybersecurity. Deze initiatieven zijn van uiteenlopende aard. Ze variëren van het helpen om jonge hackers op het rechte pad te houden, het creëren van cybersecuritybewustzijn bij diverse doelgroepen tot het ontwikkelen van lesmateriaal voor basisscholen. Met andere woorden de uitvoering van de NCSA staat niet op zichzelf en zal nauw moeten aansluiten op lopende initiatieven. De raad constateert dat niet alle initiatieven in ons land en binnen de EU even goed bekend zijn.

- *De raad adviseert om bij de uitvoering van de NCSA veelbelovende initiatieven in kaart te brengen en daar zoveel mogelijk bij aan te sluiten.*

Aandacht voor kennisontwikkeling

De digitale toekomst van Nederland moet veilig worden gesteld. Dat kan door te zorgen voor voldoende cybersecurityprofessionals en door de Nederlandse jeugd voor te bereiden op de digitale toekomst. De Cyber Security Raad acht het van belang deze zaken voortvarend aan te pakken. In een eerder advies[10] drong de raad al aan op het ontwikkelen van digivaardigheden bij de jeugd en het vergroten van het aantal cyberexperts.
Het beschikken over voldoende cybersecurity-expertise en over cybersecurity-experts is een cruciale randvoorwaarde voor een succesvolle uitvoering van de NCSA. In 2016 is door de ministeries van Justitie en Veiligheid, Onderwijs, Cultuur en Wetenschap, Economische Zaken en Klimaat en NWO dcypher[11] opgericht. Naast een opdracht op het gebied van cybersecurity-onderzoek kreeg de instelling ook een opdracht voor cybersecurity in het hoger onderwijs mee. De raad adviseert dat de gemaakte vorderingen in kaart worden gebracht zodat er een recent beeld van de situatie ontstaat. Ook wetenschappelijk onderzoek op het vlak van cybersecurity levert een belangrijke bijdrage aan de kennispositie van Nederland. De aansluiting van wetenschappelijk onderzoek op de kennisbehoefte binnen de Nederlandse overheid en het bedrijfsleven verdient de aandacht.

[9] CSR Advies 2017, nr. 2 ‘Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime’, ’s-Gravenhage
[10] CSR Advies 2015, 'Advies aan de staatssecretarissen van Veiligheid en Justitie en Onderwijs, Cultuur en Wetenschap inzake cybersecurity in het onderwijs en het bedrijfsleven', ’s-Gravenhage
[11] dcypher verenigt onderzoekers, docenten, producenten, gebruikers en beleidsmakers in Nederland om kennis en kunde over cyberveiligheid te verbeteren, www.dcypher.nl/nl

Uit cijfers van verschillende wetenschappelijke onderzoekers blijkt dat het aantal investeringen in cybersecurity-onderzoek in de afgelopen jaren steeds verder is gedaald. Investeringen in de wetenschappelijke kennis is juist nu van belang gezien het feit dat de toenemende vraag en het dreigende tekort aan cybersecurityprofessionals een wereldwijd probleem is en steeds meer cybersecurityprofessionals in Nederland naar het buitenland vertrekken.[12] In het regeerakkoord[13] is extra geld vrijgemaakt voor cybersecurity. Dat is goed nieuws, maar de omliggende landen investeren veel meer. We moeten voorkomen dat topspecialisten in cybersecurity naar het buitenland vertrekken. Met de mogelijke oprichting van een cybersecurity-instituut en structureel meer geld voor wetenschappelijk onderzoek, maken we het academisch werk in Nederland op dit gebied aantrekkelijker. De raad adviseert dat er vaart moet worden gezet achter de oprichting van het instituut en dat er structureel geïnvesteerd wordt in wetenschappelijk cybersecurity-onderzoek.

- *De raad adviseert dat er vaart wordt gemaakt met de oprichting van een cybersecurity-instituut en dat er structureel geïnvesteerd wordt in wetenschappelijk cybersecurity-onderzoek.*
- *Het dreigende tekort aan cybersecurity-specialisten is nog steeds een belangrijk punt van aandacht voor de raad. Om die reden adviseert de raad dat er een recent beeld ontstaat van de laatste stand van zaken door de vorderingen van de opdrachten die dcypher heeft meegekregen in kaart te brengen.*

Ad 3. Structureel investeren in cybersecurity

Om onze digitale positie te behouden en te kunnen blijven concurreren met landen als het Verenigd Koninkrijk, Frankrijk, Duitsland en de Scandinavische landen is het van belang om meer te investeren in cybersecurity en de aanpak van cybercrime. Dit vormt ook een van de belangrijkste kernconclusies uit de Cyber Readiness Index (CRI) voor Nederland.[14] De raad adviseert het kabinet hierin structureel te blijven investeren.

Met de investering van 95 miljoen euro in cybersecurity[15] is hiermee een eerste belangrijke stap gezet. Daarmee zijn we er nog niet; er zullen meer stappen moeten worden gezet naar de toekomst toe om ons te kunnen wapenen tegen statelijke actoren en de toenemende georganiseerde misdaad. Alleen zo kunnen we in Nederland blijvend de kansen verzilveren en innovatie bevorderen en daar is meer geld voor nodig.

- *De raad adviseert het kabinet op basis van een langetermijnvisie structureel te investeren in cybersecurity en de aanpak van cybercrime.*

[12] Herbert Bos, Michel van Eeten, Bart Jacobs (november, 2017), 'De noodzaak tot Nederlandse zelfredzaamheid gebaseerd op de nationale behoefte aan eigen hoogwaardige expertise, via kennisontwikkeling en circulatie', www.dcypher.nl/files/downloads/documents/cybersecurity-behoud-versterking-v2.pdf
[13] Regeerakkoord 2017 – 2021: 'Vertrouwen in de toekomst'
[14] Potomac Institute for Policy Studies (2017), The Netherlands cyber readiness at a glance, Arlington
[15] Regeerakkoord 2017 – 2021: 'Vertrouwen in de toekomst'

GERICHTE ADVIEZEN

De adviezen zijn gericht op het kabinet, de overheid, het bedrijfsleven en de wetenschap. De raad benadrukt het belang van een integrale aanpak. De raad adviseert:

- De minister van Justitie en Veiligheid onderstaande onder de aandacht te brengen bij de leden van het kabinet:
    - Zet cybersecurity blijvend op de agenda en investeer de komende jaren substantieel en structureel in een open, veilig en welvarend digitaal Nederland en zorg ervoor dat de verschillende aspecten van cybersecurity in samenhang worden besproken in de Tweede Kamer.
    - Adresseer de maatschappelijke, juridische en ethische vraagstukken in relatie tot digitale ontwikkelingen en cybersecurity in het maatschappelijke debat, maak een gedegen belangenafweging en vertaal dit naar visie, beleid en wetgeving. Laat Nederland hierin een vooraanstaande rol spelen binnen de Europese Unie en in internationaal verband.
    - Draag er zorg voor dat er op korte termijn een inventarisatie wordt gemaakt van de strategische en technische assets die Nederland nodig heeft om haar cybersecurity te waarborgen.
    - Draag zorg voor voldoende aandacht voor cybersecurity en de aanpak van kwetsbaarheden in systemen in alle relevante (cyber- en digitaliserings)strategieën.
- De minister van Justitie en Veiligheid :
    - Breng prioritering aan in de gestelde ambities, doelstellingen en maatregelen van de NCSA en draag zorg voor een strakke regie op de NCSA en alert optreden bij vertraging.
    - Stimuleer structurele onderlinge afstemming met andere overheidsinstanties op het terrein van cybersecurity en kies waar mogelijk voor een gezamenlijke implementatie.
    - Draag zorg voor aansluiting bij veelbelovende initiatieven bij het uitvoeren van de NCSA.
    - Bevorder transparantie en efficiëntie door waar mogelijk een gezamenlijk beroep te doen op de inzet van de overheid, de private sector, het maatschappelijk middenveld en de wetenschap als het gaat om cybersecurity. Neem dit mee als aandachtspunt voor de Cybersecurity Alliantie.
    - Draag in gezamenlijkheid met de overige departementen zorg voor onderzoek naar de mogelijkheden voor de inzet van positieve stimulans om de benodigde samenwerking met de private sector vorm te geven en voer deze door.

- De minister van Justitie en Veiligheid onderstaande gezamenlijk op te pakken met de minister van Onderwijs, Cultuur en Wetenschap en de staatssecretaris van Economische Zaken en Klimaat:

    - Draag zorg voor een versnelde oprichting van een cybersecurity-instituut.
    - Draag zorg voor structurele investeringen in wetenschappelijk cybersecurity-onderzoek.
    - Draag zorg voor een goed beeld van de stand van zaken als het gaat om cybersecurityprofessionals in Nederland.

’s-Gravenhage,

Namens de Cyber Security Raad,

Jos Nijhuis
Covoorzitter CSR

Dick Schoof
Covoorzitter CSR