CSR Cyber Security Raad

Bezoekadres
Korte Voorhout 7
2511 CW Den Haag

Postadres
Postbus 20301
2500 EH Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl

Aan de informateur,
Mw. prof. dr. R.M. Letschert
t.a.v. Bureau Woordvoering Kabinetsformatie
Postbus 20018
2500 EA Den Haag

Datum
12 januari 2025

Onderwerp
CSR Brief aan de informateur: Komend kabinet moet sterker inzetten op digitale weerbaarheid, inclusief de benodigde investeringen

Geachte mevrouw Letschert,

Nederland investeert structureel te weinig in haar digitale veiligheid en weerbaarheid. De Cyber Security Raad (hierna de raad) vraagt daarom in deze brief aan het komende kabinet om €690 miljoen oplopend te investeren in de digitale weerbaarheid van onze samenleving.
Digitalisering is de ruggengraat van onze samenleving en economie: daarmee is cybersecurity een absolute randvoorwaarde voor onze nationale veiligheid, democratie en welvaart. Er zijn veel goede stappen gezet met als basis de Nederlandse Cybersecuritystrategie (NLCS) en de Nederlandse Digitaliseringstrategie (NDS), maar de implementatie moet sneller en er zijn grotere investeringen nodig.

De raad ziet vier prioriteiten voor beleid die de extra investeringen noodzakelijk maken:

1. **Versterk de digitale weerbaarheid van (rijks)overheid, vitale infrastructuur en bedrijfsleven**
   Onder invloed van het woelige geopolitieke tij nemen de digitale aanvallen op de vitale infrastructuur sterk toe. Ook over de weerbaarheid van de (rijks)overheid zelf nemen de zorgen toe. Vergroot daarom de weerbaarheid van de vitale infrastructuur, met name die van de telecom- en energiesector, die zijn het centrale zenuwstelsel van alle andere processen. Investeer bovendien niet alleen in preventie, maar ook in fysieke en digitale fallback scenario's. De raad bepleit verder het robuuster maken van ketenafhankelijkheden, meer deling van dreigingsinformatie, meer training op geopolitieke scenario's, krachtiger samenwerking tussen publieke en private partijen bij incidenten en dreigingen, en het dichten van de weerbaarheidskloof voor het mkb.
2. **Investeer in digitale autonomie**
   Onze toenemende afhankelijkheid van de grote digitale spelers buiten de EU brengt ernstige strategische risico's met zich mee voor onze nationale veiligheid en bescherming van gebruikersdata. Investeer daarom in digitale autonomie door het creëren van concurrerende Europese alternatieven op het gebied van onder meer cloud en artificiële intelligentie (AI). Dwing bij providers af dat dataopslag en beheer binnen de EU plaatsvinden en maak eindgebruikers bewust van de keuzes die er zijn. Investeer in een soevereine Rijkscloud. Vervul een aanjaagfunctie door de Europese markt te stimuleren met publieke aanbestedingen gericht op Europese bedrijven en geef de CIO Rijk een stevig mandaat voor strategisch leveranciersmanagement.
3. **Bereid Nederland voor op AI als katalysator van dreigingen**
   AI verandert de snelheid en schaal van cyberaanvallen fundamenteel. Volgens experts is er een reële kans dat Nederland binnen vijf jaar wordt overspoeld door steeds geraffineerdere, generiek toepasbare cyberaanvallen met AI. Nederland is daar niet op voorbereid. Investeer met Europese partners in

kennisopbouw en nieuwe defensieve oplossingen en respons om met AI gefaciliteerde aanvallen tijdig te herkennen en te pareren en daarmee de weerbaarheid te vergroten.

4. **Bescherm burgers beter tegen cybercrime**
   Ondanks campagnes om de Nederlander bewuster en zelfverantwoordelijker te maken neemt cybercrime alleen maar toe, met meer ransomware, botnets, phishing, malwareverspreiding en identiteitsfraude. Cybercrime kan tot maatschappelijke ontwrichting leiden, waarschuwde de politie onlangs in de media. Nederland loopt achter vergeleken met andere landen. De burger moet daarom meer aandacht krijgen in de cybercrime-aanpak en beter worden beschermd; die moet zich bewuster worden van de risico's, beter weten welke maatregelen te nemen zijn en waar hulp kan worden gevraagd. Verbeter de digitale kennis en vaardigheden vanaf het primaire onderwijs. Politie en OM moeten cybercrime intensiever gaan bestrijden en de drempel om aangifte te doen moet worden verlaagd. Dit kan bijvoorbeeld door één centraal loket voor het doen van meldingen en voor advies over maatregelen en het herstel van een cyberaanval.

Verder bepleit de raad het aanpakken van het groeiend tekort aan cybersecurityspecialisten, het waarborgen van onze kennispositie middels cybersecurity-onderzoek en het investeren in voortvarende uitvoering van wet- en regelgeving die momenteel wordt geïmplementeerd door overheid en het bedrijfsleven gezamenlijk, inclusief voldoende mankracht en middelen en aandacht voor toezicht.

Deze prioriteiten in beleid lichten we hierna nader toe.

1. Versterk de digitale weerbaarheid van overheid, vitale infrastructuur en bedrijfsleven

Het woelige geopolitieke tij zorgt ervoor dat digitale aanvallen op de vitale infrastructuur toenemen. Dit geldt ook voor de (rijks)overheid. Zichtbare incidenten met grote impact, zoals bij het Openbaar Ministerie, onderstrepen dit. Het recente Cybersecuritybeeld Nederland (CSBN) 2025 bevestigt dit beeld en de zorgen nemen toe, ook aan de bestuurstafels. Ook het mkb is steeds vaker doelwit van cybercriminelen en vormt een zwakke schakel in de toeleverancierskeketen van grote organisaties.

Cyberaanvallen kunnen directe maatschappelijke ontwrichting veroorzaken. Het is aan de overheid om de teugels in handen te nemen en de verschillende sectoren in staat te stellen passende maatregelen te treffen. Hierbij kan gedacht worden aan het robuust maken van (keten)afhankelijkheden, het delen van dreigings- en incidentinformatie, als ook structureel oefenen en trainen.

Nederland heeft een digitale infrastructuur van wereldklasse en deze komt steeds verder onder druk te staan. Of het nu gaat om het aansturen van bruggen en sluizen, gebruik van gps, industriële systemen voor onze energievoorziening, gebruik van internet in onderwijs en onderzoek, de opslag van data (al dan niet in de cloud) of sociaal communicatieverkeer tussen Nederlanders onderling: we rekenen op een digitale infrastructuur die snel, betrouwbaar en veilig is. Extra aandacht voor de weerbaarheid van de digitale infrastructuur is noodzakelijk.

<u>Aanbevelingen</u>

- Investeer in fysieke en digitale fallback scenario's om de impact bij verstoring te verkleinen. Zet in op een macro-risicobeeld over sectoren heen om afhankelijkheden en kwetsbaarheden in kaart te brengen en te mitigeren. De raad adviseert eveneens om de overheidsvraag voor vitale diensten in het veiligheidsdomein te bundelen.
- Maak afhankelijkheden in ketens robuuster, en zorg voor meer regie op, en intensivering van het (structureel) delen van inlichtingen- en dreigingsinformatie (ook over leveranciers uit risicolanden en informatie over incidenten), zoals in het programma Cyclotron. Zet in op meer oefenen en trainen op geopolitieke scenario's (ook op kleine schaal).

- De groeiende en veranderende dreiging vraagt om het versterken van de mogelijkheid voor publieke en private partijen om gezamenlijk krachtig te reageren op incidenten en dreigingen. Bijvoorbeeld in de vorm van een House of Cyber, een fysieke samenwerking tussen publieke en private partijen.
- De weerbaarheid van de (rijks)overheid staat onder druk. Bestuurlijke aandacht voor de noodzakelijke maatregelen en continue investeringen om de weerbaarheid te vergroten is nodig. Daarnaast is binnen het rijk centrale sturing en doorzettingsmacht door het CIO-stelsel Rijk noodzakelijk.
- Dicht de cyberweerbaarheidskloof voor het midden- en kleinbedrijf. Dit kan door in te zetten op het vergroten van de collectieve weerbaarheid (via leveranciers) van het mkb door publiek-private samenwerking, zoals binnen het Cyberweerbaarheidsnetwerk, en door meer focus op adviezen en informatie vanuit het vernieuwde Nationaal Cyber Security Centrum (NCSC) voor het mkb.

2. Investeer in digitale autonomie

Onze digitale infrastructuur leunt zwaar op technologie van grote spelers van buiten de Europese Unie. Hoewel Amerikaanse *hyperscalers* voordelen bieden in schaalbaarheid en gebruiksgemak, brengt deze eenzijdige afhankelijkheid grote strategische risico's met zich mee voor onze nationale veiligheid en de bescherming van gebruikersdata. Omdat de geopolitieke verhoudingen steeds verder onder druk komen te staan, is het noodzakelijk om gerichte keuzes te maken over welke 'Big Tech'-producten in te wisselen voor Europese alternatieven ten gunste van onze digitale autonomie.

Aanbevelingen

- Vervul een aanjaagfunctie: Stimuleer de Europese markt door publieke aanbestedingen actief te richten op Europese bedrijven.
- Voer een tweesporenbeleid voor de cloud:
    - Investeer in de ontwikkeling van een soevereine Rijkscloud met volledige controle op de cloud-omgeving door het Rijk, en in 'domestic cloud'-oplossingen, vergelijkbaar met huidige trajecten bij Defensie.
    - Dwing bij huidige buitenlandse providers verdergaande digitale soevereiniteit, zoals lokale opslag van data, af voor private clouds, waardoor afhankelijkheden ten gevolge van sanctiemaatregelen door de Amerikaanse overheid worden voorkomen, en maak eindgebruikers, die zelf kunnen kiezen waar hun data worden opgeslagen, bewust van de keuzen die er zijn.
- Versterk de regie binnen de Rijksoverheid: Geef de CIO Rijk een stevig mandaat voor strategisch leveranciersmanagement over alle ministeries heen. Centrale regie, inclusief het mandaat om besluiten door te voeren, is essentieel om als overheid een vuist te maken tegenover grote tech-partijen.
- Intensiveer Europese samenwerking: Benut het European Digital Infrastructure Consortium (EDIC) Digitale Gemeenschapsgoederen van Frankrijk, Duitsland, Italië en Nederland om de Europese digitale soevereiniteit te versterken door het faciliteren en stimuleren van sterke, concurrerende alternatieven uit Europa op het gebied van met name AI en cloud.

3. Bereid Nederland voor op AI als katalysator voor dreigingen

AI zorgt voor een fundamentele verandering in onze samenleving én in het digitale dreigingslandschap. Er zijn zorgwekkende ontwikkelingen betreffende de inzet van AI als wapen bij cyberaanvallen. Dergelijke aanvallen met AI zijn sneller en grootschaliger dan ‘normale’ cyberaanvallen en worden nu al autonoom ingezet door kwaadwillende (veelal statelijke) actoren; de intensiteit hiervan gaat in de nabije toekomst naar verwachting sterk toenemen. Hier zijn onze verdedigingsplannen niet op voorbereid, aangezien de raad een tekort aan expertise constateert in Nederland en de EU over deze AI-gestuurde cyberaanvallen. Om toekomstige schade te voorkomen, is het namelijk van groot belang dat Nederland sterker gaat inzetten op toepassingen voor het tegengaan van dergelijke aanvallen. Extra kennisopbouw hierover is onontbeerlijk om sneller stappen te kunnen zetten in de ontwikkeling van innovatieve producten hiervoor.

Aanbeveling

- Nederland moet met Europese partners een leidende rol nemen in de weerbaarheid tegen huidige en toekomstige AI-gefaciliteerde cyberaanvallen. Investeer in kennisopbouw en nieuwe producten om dergelijke aanvallen tijdig te herkennen en te pareren.

4. Bescherm burgers beter tegen cybercrime

Politiecijfers[1] en het jaarlijkse Internet Organised Crime Threat Assessment[2] laten al jaren een gestage toename zien van onder meer ransomware, botnets, phishing, malwareverspreiding en identiteitsfraude. Uit onderzoek blijkt eveneens dat een groot deel van deze incidenten onzichtbaar blijft: het zogenaamde *dark number*[3] is hoog. Veel EU-landen, zoals Estland en Groot-Brittannië, zijn verder in het vergroten van de digitale weerbaarheid van burgers. Belangrijk is eveneens de implementatie (over twee jaar) van de Europese Cyber Resilience Act (CRA) in Nederland, die over de volle breedte moet zorgen voor standaard goed beveiligde digitale producten.

Cybercriminaliteit kan in de nabije toekomst tot serieuze maatschappelijke ontwrichting leiden, zo waarschuwde het hoofd Operatiën Cyber van de Landelijke Politie onlangs in de media. De risico's zijn breed van overheidsdiensten tot kritieke infrastructuur en van telecomdiensten tot toeleveringsketens. Dit raakt ook de burger. De Nederlandse digitale infrastructuur wordt veel door statelijke actoren en cybercriminelen gebruikt voor digitale aanvallen. Actie is nodig om dit zo onaantrekkelijk mogelijk te maken.

Aanbevelingen

- Geef burgers meer aandacht in de cybersecurity-aanpak. Nederlanders moeten zich beter bewustworden van risico's, het nemen van basale maatregelen en weten waar hulp kan worden gevraagd. Zet in op het verbeteren van digitale kennis en vaardigheden vanaf het primair onderwijs.
- Maak middelen vrij voor de versterking van cybercrime opsporing en preventie bij politie en OM.
- Maak werk van de aanpak van bad hosting en malafide resellers[4]. Dit door onder andere in te zetten op Europese samenwerking in lijn met de *Kamerbrief over de voortgang integrale aanpak cybercrime juni 2025 (d.d. 27 juni 2025).*
- De raad komt in de loop van dit jaar met concrete adviezen om de weerbaarheid van burgers te vergroten. Te denken valt aan het creëren van een centraal loket waar Nederlanders niet alleen meldingen kunnen doen, maar bijvoorbeeld ook adviezen kunnen vinden over het nemen van basismaatregelen en het herstellen van een cyberaanval. Ons advies aan u is om voor de uitvoering hiervan reeds middelen vrij te maken.

Randvoorwaardelijke aanbevelingen

Voldoende cybersecurityspecialisten, kennis en innovatie

De raad roept op om in deze kabinetsperiode extra aandacht te besteden aan het aanpakken van het groeiend tekort aan cybersecurityspecialisten en het waarborgen van onze kennispositie voor cybersecurity middels cybersecurity-onderzoek[5]. Het tekort aan cybersecuritytalent is niet alleen een veiligheidsrisico, maar remt ook

[1] Cybercrimebeeld Nederland 2024, Politie / Openbaar Ministerie
https://www.om.nl/binaries/om/documenten/publicaties/cybercrime/2024/ccbn/samenvatting-ccbn-nederlands/Cybercrimebeeld%2BNederland%2B2024_Samenvatting.pdf Europol+2Europol+2

[2] Europol – Internet Organised Crime Threat Assessment (IOCTA) 2023
https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf Europol+9Europol+9Europol+9.

[3] Veiligheidsmonitor 2023, Centraal Bureau voor de Statistiek (CBS), maart 2024
https://www.cbs.nl/nl-nl/publicatie/2024/09/veiligheidsmonitor-2023

[4] Bad hosters en malafide resellers zijn aanbieders van digitale infrastructuur die bewust infrastructuur ter beschikking stellen aan criminele of andere kwaadwillende actoren.

[5] Zie ook 'Aanbiedingsbrief bij onderzoeksresultaten kwalitatieve en kwantitatieve tekorten cybersecurity professionals', 15 mei 2024
https://www.rijksoverheid.nl/documenten/kamerstukken/2024/05/15/kamerbrief-human-capital-cybersecurity

de innovatiekracht en de economische groei van Nederland. Over dit onderwerp heeft de raad in verschillende stadia geadviseerd, vanaf 2013. In de zomer van 2024 is er een signaalbrief[6] naar de toenmalige minister van Economische Zaken gestuurd over het groeiende (kwalitatieve en kwantitatieve) tekort aan cybersecurityspecialisten. De raad benadrukt daarin het belang van een gecoördineerde aanpak. Oplossingen vragen om centrale regie, betere afstemming tussen programma's en inzet op curriculumontwikkeling, zij-instroom en een leven lang leren. De huidige acties vanuit de overheid zijn nog niet toereikend en ook extra financiële middelen dienen hiervoor te worden vrijgemaakt.

Investeer voldoende in de implementatie van wetgeving
We staan aan de vooravond van de implementatie van verschillende EU wet- en regelgeving, zoals de aanstaande Cyberbeveiligingswet (Cbw) en de Cyber Resilience Act (CRA). De raad verzoekt het kabinet dan ook voldoende te investeren in het implementeren en operationaliseren van deze wet- en regelgeving, inclusief het toezicht daarop. De raad roept het aanstaande kabinet tevens op om de nationale implementatie van EU wet- en regelgeving uit te voeren met simplificatie in het achterhoofd. Vanuit de Europese Commissie is hiertoe onlangs de digitale omnibus gepubliceerd die ook oproept om regeldruk te verminderen. Ook de raad vindt het belangrijk dat bedrijven de ruimte krijgen om de geplande wetgeving te implementeren en ze niet op korte termijn te onderwerpen aan nieuwe aanvullende wetgeving. Dit zorgt ervoor dat bedrijven kunnen blijven ondernemen en innoveren.

Noodzakelijke middelen

Voor de uitvoering van de Nederlandse Cybersecurity Strategie (NLCS) en de noodzakelijke maatregelen om de weerbaarheid te vergroten is tot op heden te weinig geïnvesteerd. De raad acht het daarom dringend noodzakelijk dat een nieuw kabinet €690 miljoen structurele middelen voor de digitale veiligheid van Nederland in het nieuwe coalitieakkoord opneemt, in lijn met de nieuwe NAVO-norm van 1,5%. In de onderstaande tabel is per prioriteit indicatie gegeven van de structureel benodigde middelen van genoemde en andere noodzakelijke maatregelen.

	Structurele benodigde investering
Digitale weerbaarheid overheid, vitale infrastructuur en bedrijfsleven	€513 miljoen
Digitale autonomie	€40 miljoen
AI als katalysator voor dreigingen	€25 miljoen
Bescherming burgers tegen cybercrime	€60 miljoen
Cybersecurityspecialisten, kennis en innovatie	€35 miljoen
Wetgeving (implementatie en toezicht)	€17 miljoen
Totaalbedrag	**€690 miljoen**

[6] CSR Signaalbrief cybersecurity arbeidsmarkt, 4 juli 2024
https://www.cybersecurityraad.nl/documenten/2024/07/04/csr-signaalbrief-cybersecurity-arbeidsmarkt

Tot slot

In de afgelopen jaren zijn goede stappen gezet met de NLCS en de NDS als belangrijke basis. Het is nu tijd voor versnelling en meer investering in de toekomst. Een digitaal weerbare samenleving en economie vraagt om stevige en continue centrale beleidsregie vanuit de overheid, gezamenlijk optrekken met het bedrijfsleven, de wetenschap en het maatschappelijk middenveld, plus proactief beleid en tempo in de uitvoering. Cybersecurity vergt een multistakeholderbenadering, wat verder gaat dan bedrijfsleven en wetenschap. Ook relevante maatschappelijke organisaties moeten worden betrokken. Veel grote bedrijven hebben cybersecurity inmiddels in hun top 3 van prioriteiten opgenomen. Het is aan het komende kabinet om dit voorbeeld te volgen, en in het coalitieakkoord zowel te investeren in een versterkte uitvoering van de NLCS als in de overige genoemde strategische thema´s.

De raad zal ook tijdens de komende kabinetsperiode blijven adviseren over de uitvoering en uitwerking van de NLCS. Het doel daarvan is steeds om het kabinet te helpen en daarbij vooruit te kijken, zodat onze samenleving digitaal veilig kan blijven. De raad is te allen tijde bereid om met u en de onderhandelaars in gesprek te gaan over de inhoud van deze brief.

Hoogachtend,
Namens de Cyber Security Raad,

Marc Kuipers
Covoorzitter CSR namens de publieke sector

Sylvia van Es
Covoorzitter CSR namens de private sector

Over de Cyber Security Raad

De Cyber Security Raad is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De raad zet zich op strategisch niveau in om de cyberweerbaarheid in Nederland te verhogen. Door de unieke samenstelling van de raad (publiek-privaat-wetenschap) is het mogelijk om prioriteiten, knelpunten en incidenten vanuit diverse invalshoeken strategisch te benaderen en een integrale visie op kansen en bedreigingen te ontwikkelen.