Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5333 (secretariaat)
E info@cybersecurityraad.nl
Datum
30 januari 2024

Onderwerp
CSR Brief aan de informateur: Komend kabinet moet sterker inzetten op cybersecurity en meer investeren

Aan de informateur,
de heer R.H.A. Plasterk
t.a.v. Bureau Woordvoering Kabinetsformatie
Postbus 20018
2500 EA Den Haag

Geachte Heer Plasterk,

De Cyber Security Raad (hierna de raad) roept het nieuwe kabinet op om sterker in te zetten op onze digitale veiligheid. Cybersecurity is een absolute randvoorwaarde om Nederland draaiende te houden en onze economie te laten groeien. De veranderde geopolitieke situatie leidt tot fysieke én digitale dreigingen die onze nationale veiligheid raken en onze vrijheid, democratie en welvaart onder druk zetten. In deze brief geven we u eerst een advies op hoofdlijnen, gevolgd door een onderbouwing daarvan.

Advies op hoofdlijnen

Cybersecurity vraagt stevige centrale regie vanuit de overheid, gezamenlijk optrekken met het bedrijfsleven en de wetenschap, plus proactief beleid en tempo in de uitvoering. Hiertoe zijn in de afgelopen jaren veel goede stappen gezet met de Nederlandse Cybersecuritystrategie (NLCS) als belangrijke basis. Maar de implementatie gaat niet snel genoeg en investeringen zijn niet toereikend. Prioriteiten in de uitvoering zijn:

- Het implementeren en operationaliseren van EU wet- en regelgeving, om de cyberweerbaarheid van veel meer organisaties op orde te krijgen, inclusief het toezicht daarop.
- Het beter zicht krijgen op de groeiende digitale dreigingen, en vooral het tijdig en breed delen van informatie daarover, inclusief versterkte cybercrime bestrijding.
- Het verkleinen van de cyberweerbaarheidskloof tussen organisaties, van de vitale infrastructuur tot het midden- en kleinbedrijf. Daarbij dienen de meest volwassen en bepalende organisaties de zwaarste verantwoordelijkheid te dragen (groot helpt klein).

Daarnaast roept de raad op om in deze kabinetsperiode extra aandacht te besteden aan:

- Risico's in onze digitale infrastructuur en het opbouwen van eigen technische capaciteit om afhankelijkheden tegen te gaan. Dit geldt bijvoorbeeld voor het gebruik van cloudtechnologie.
- Het aanpakken van het groeiend tekort aan cybersecurityspecialisten en het waarborgen van onze kennispositie voor cybersecurity.
- De digitale veiligheid bij nieuwe technologische ontwikkelingen zoals artificiële intelligentie (AI).

Veel grote bedrijven hebben cybersecurity inmiddels in hun top 3 van prioriteiten opgenomen. Het is aan het komende kabinet om dit goede voorbeeld te volgen, en in het coalitieakkoord zowel te investeren in een versterkte NLCS uitvoering als in genoemde strategische thema´s. Geadviseerd wordt om €200 miljoen in 2024 op te nemen (in lijn met het advies van de raad uit 2021), oplopend tot €550 miljoen in 2028 en verder.

Achtergrond

Onze maatschappij is tot in de haarvaten afhankelijk van het internet en andere digitale netwerken, diensten en producten. Ontwikkelingen op het gebied van digitalisering gaan razendsnel en bieden veel kansen, maar brengen ook essentiële vraagstukken op het gebied van cyberweerbaarheid met zich mee. Adequate cybersecurity hoort voor organisaties bij een gezonde bedrijfsvoering, net als grip op hun financiële huishouding; het is een dragende factor die overal aanwezig én noodzakelijk is, anders komt de veiligheid en continuïteit in gevaar en stokt onze economie.

Ondanks alle getroffen maatregelen laten opeenvolgende edities van het Cybersecuritybeeld Nederland (CSBN) zien dat cyberrisico´s onverminderd toenemen, zowel door aanvallen van cybercriminelen als acties van statelijke actoren. Er zijn legio voorbeelden en recente incidenten drukken ons nog eens met de neus op de feiten: de ransomware-aanval bij de KNVB door de criminelen van Lockbit[1] en het datalek bij softwareleverancier Nebu, waardoor meer dan 100 Nederlandse bedrijven en organisaties (waaronder Heineken, VodafoneZiggo en de NS) werden getroffen[2]. In november jl. werden Australische havens platgelegd door een cyberaanval; het is voorstelbaar dat dit ook in Nederland zou kunnen gebeuren.

Uitvoering NLCS onder centrale overheidsregie

De Nederlandse Cybersecuritystrategie (NLCS) die in het najaar van 2022 verscheen, biedt een stevig fundament voor de toekomst. De raad heeft de visie en ambities die in de NLCS zijn opgenomen omarmd. Datzelfde geldt ook voor de andere strategieën op het gebied van (veilige) digitalisering, van verschillende departementen. Gezien de huidige cybersecurityrisico´s moet tempo gemaakt worden met de uitvoering van die strategieën. Daarvoor is intensieve publiek-privaat-wetenschappelijke samenwerking nodig.

De raad beveelt het nieuwe kabinet daarom sterk aan om niet opnieuw te beginnen met het maken van plannen voor cybersecurity, maar de NLCS als uitgangspunt te nemen voor de komende kabinetsperiode[3] en de cybersecurityaanpak van daaruit verder te versterken. Gezien de complexiteit en de grote hoeveelheid betrokken partijen, is een voorspelbare overheid van groot belang om tot een adequate uitvoering te komen. De volgende onderdelen van de NLCS zijn daarbij op nationaal niveau cruciaal:

- Het inrichten van technische én organisatorische mechanismen voor het tijdig en breed delen van informatie over dreigingen, kwetsbaarheden en incidenten over alle sectoren (overheid, bedrijven en maatschappelijke organisaties) heen, inclusief doelwit- en slachtoffernotificatie.
- Het bestrijden van cybercrime via versteviging van bestaande initiatieven, in de gehele keten van opsporing en vervolging.
- Beveiliging van operationele technologie (OT), waaronder de bundeling van expertise in de verschillende ketens. De procesindustrie, maar ook onze waterkeringen, de energiesector en ziekenhuizen maken hier gebruik van. Onderlinge afhankelijkheden zijn daarbij groot, omdat allerlei OT- en IT-systemen met elkaar zijn verknoopt.
- De cyberweerbaarheid van het midden- en kleinbedrijf (mkb); het is dringend noodzakelijk om de cyberweerbaarheidskloof tussen bedrijven te verkleinen. De keten is zo sterk als de zwakste schakel en elke organisatie dient de basisbeveiliging op orde te hebben[4].
- Het terugdringen van het tekort aan cybersecurityspecialisten, ter versterking van onze kennispositie.

[1] Zie Informatie cyberinbraak KNVB | KNVB
[2] Zie Datalek Nederlandse bedrijven steeds groter: zeker 2 miljoen klanten getroffen (nos.nl)
[3] Een voortvarende uitvoering is ook zeer relevant voor provincies, gemeenten en waterschappen, omdat zij hun beleid ook baseren op nationale strategievorming.
[4] De demissionair minister van Justitie en Veiligheid heeft de raad om advies gevraagd over verkleining van die cyberweerbaarheidskloof, hetgeen in het eerste kwartaal van 2024 beschikbaar zal komen.

De raad roept u daarbij op om tijdens de coalitieonderhandelingen te kiezen voor een stevige regierol van de overheid op het vlak van (veilige) digitalisering. Door die rol zoveel mogelijk centraal te beleggen kan ook departementale verkokering worden tegengegaan. De portefeuilleverdeling tussen de verschillende toekomstige bewindslieden moet op die centrale regierol aansluiten.

Internationale context en invoering EU regelgeving

Cybersecurity heeft een grensoverschrijdend karakter; inzet op internationale samenwerking is daarom een belangrijke randvoorwaarde om onze nationale belangen te beschermen. Dit wordt benadrukt in de recente Internationale Cyberstrategie[5] van het Ministerie van Buitenlandse Zaken. Deze strategie zet in op drie doelstellingen:

- Het tegengaan van de cyberdreiging van staten en criminelen.
- De versterking van democratische en mensenrechtelijke principes in de digitale ruimte.
- Het behoud van een wereldwijd open, vrij en veilig internet.

Een ander essentieel onderdeel van de NLCS is de implementatie van de Network and Information Security Directive (NIS2). Dit is een omvangrijke EU-richtlijn, die in de loop van 2024 operationeel wordt. Dit betreft onder andere de invoering van een zorgplicht en meldplicht bij een veel groter aantal (publieke en private) organisaties dan momenteel het geval is, inclusief versterkt toezicht daarop. Ook is binnen de EU zeer recent een akkoord bereikt over invoering van de Cyber Resilience Act (CRA) voor digitale producten in alle lidstaten. Implementatie van deze wet zal ook in de komende kabinetsperiode plaatsvinden.

Strategische thema's die extra aandacht vragen

De raad is van mening dat onderstaande drie thema´s extra aandacht vragen van het nieuwe kabinet, gegeven de verschillende strategieën op het gebied van (veilige) digitalisering die reeds gelanceerd zijn. Alleen dan kan de cyberweerbaarheid van Nederland in de nabije toekomst op het noodzakelijke niveau worden gebracht.

1. Verstevig onze digitale autonomie, ook in de context van cybersecurity

De technologieën die samen onze digitale infrastructuur vormen, bestaan uit vele verschillende componenten, bouwstenen en applicaties waarin kwetsbaarheden en risicovolle afhankelijkheden aanwezig kunnen zijn, en waarvoor tal van verschillende organisaties verantwoordelijk zijn. De robuustheid en betrouwbaarheid van deze systemen is een essentiële randvoorwaarde om onze economische kansen en innovatief vermogen te behouden.

Het overgrote deel van dergelijke technologieën komt van grote bedrijven uit landen buiten de EU. Daarmee neemt dus ook onze afhankelijkheid van deze bedrijven en landen toe. Dit is niet per definitie altijd en overal problematisch, want toegang tot deze hoogwaardige technologie draagt bij aan onze brede welvaart. Die afhankelijkheid kan echter ook diverse cybersecurityrisico's met zich meebrengen, hetgeen versterkt wordt door geopolitieke ontwikkelingen. Dit heeft ook zijn weerslag op onze nationale veiligheid, concurrentiekracht, fundamentele rechten en democratische rechtsstaat.

Het bovenstaande vraagt om het tijdig maken van afgewogen strategische beslissingen[6] over het mitigeren van dergelijke risicovolle afhankelijkheden en het opbouwen van eigen capaciteit op technisch gebied, zodat

[5] Internationale Cyberstrategie 2023-2028, Daadkrachtige Diplomatie in het Digitale Domein, ministerie van Buitenlandse Zaken, juni 2023. Zie Internationale Cyber Strategie 2023 - 2028 (overheid.nl)

[6] Het kan daarbij gaan om het besluiten over (nationaal of EU) beleid en bijbehorende regelgeving, maar ook om het nemen van bepaalde investeringsbeslissingen.

Nederland haar publieke waarden blijvend kan beschermen. Dit kan bijvoorbeeld door de industrie in Nederland of de EU te stimuleren, of door partnerschappen aan te gaan met gelijkgestemde landen. Besluiten daarover moeten genomen worden op het hoogste nationale politiek-bestuurlijke niveau, zowel in Nederland als binnen de EU.

De Agenda Digitale Open Strategische Autonomie[7] biedt een gewogen kader om toekomstig Nederlands beleid vorm te geven voor de meest cruciale digitale technologieën. Een belangrijk voorbeeld daarvan is cloudtechnologie, waarbij er een afhankelijkheid is van de dominante buitenlandse leveranciers. Deze systemen bieden veel voordelen in gebruikersgemak, functionaliteit, flexibiliteit en schaalbaarheid, evenals intrinsieke aandacht voor cybersecurity. Het is echter wel van belang om risicovolle afhankelijkheden terug te dringen of te vermijden. Hierover wordt op dit moment afgestemd in EU-verband, hetgeen moet gaan leiden tot toekomstige EU-richtlijnen op dit vlak.

2. Versterk het onderwijs en onderzoek om onze kennispositie te behouden

De raad dringt bij het nieuwe kabinet aan op gestructureerde en gecoördineerde actie voor de versterking van cybersecurityonderwijs en -onderzoek, conform de gestelde doelen in de NLCS. Daarvoor dienen bestaande publiek-privaat-wetenschappelijke initiatieven als basis. Het betreft de volgende drie thema´s:

- Tekort aan specialisten: cybersecurity is een multidisciplinair werkveld; naast technici zijn ook specialisten met een juridische, bestuurlijke, ethische en economische achtergrond nodig. Zoals eerder in deze brief genoemd, kunnen strategieën zoals de NLCS alleen worden uitgevoerd wanneer over de volle breedte voldoende kennis aanwezig is. Echter, het tekort aan gekwalificeerde specialisten en benodigde docenten wordt steeds nijpender. Hierdoor treedt nu al stagnatie op in meerdere sectoren en dreigen er extra beveiligingsrisico´s te ontstaan.
- Versterking van onderzoek: de raad constateert dat het huidige onderzoeks- en innovatieklimaat voor cybersecurity nog niet voldoende is toegerust. Er is weliswaar een breed scala aan mogelijke nationale en EU-financieringsinstrumenten, maar de samenhang in geselecteerde onderzoeksonderwerpen en goede afstemming van vraag en aanbod ontbreekt. Hierdoor staat onze kennispositie op de langere termijn onder druk, hetgeen ook gevolgen zal hebben voor onze nationale veiligheid.
- Meer digitale geletterdheid: er dient op korte termijn een extra impuls te worden gegeven aan de digitale geletterdheid in het basis- en voortgezet onderwijs, vooruitlopend op een algehele herziening van het curriculum. Dit draagt ook bij aan het cyberbewustzijn van burgers, als eindgebruikers van digitale apparaten en systemen.

3. Waarborg tijdig en adequaat de digitale veiligheid bij nieuwe technologische ontwikkelingen

Technologische ontwikkelingen op het gebied van digitalisering volgen elkaar in hoog tempo op en ze hebben grote impact op onze maatschappij. Overwegingen omtrent veiligheid komen daarbij vaak pas in een (te) laat stadium aan bod. *Thought leaders* waarschuwen hier herhaaldelijk voor. Cybercriminelen en statelijke actoren blijken daarentegen wel in staat om nieuwe technologieën snel te incorporeren in hun modi operandi.

Dergelijke innovaties kunnen echter ook van grote waarde zijn voor de verbetering van de cyberweerbaarheid. Illustratief zijn de kansen en risico´s van (generatieve) AI in de context van cybersecurity. Met goede waarborgen kunnen dit soort innovaties op een verantwoorde wijze grootschalig gebruikt worden, maar

[7] Agenda Digitale Open Strategische Autonomie, ministerie van Economische Zaken en Klimaat, oktober 2023. Zie Kamerbrief over kabinetsaanpak Strategische Afhankelijkheden | Kamerstuk | Rijksoverheid.nl en Kamerbrief over aanbieding Agenda Digitale Open Strategische Autonomie | Kamerstuk | Rijksoverheid.nl

daarvoor moeten ook tijdig de juiste (cybersecurity-)maatregelen worden genomen. Een ander voorbeeld is de komst van kwantumcomputers; dit biedt een breed spectrum aan nieuwe kansen, maar ook hier zullen de gevolgen voor onze digitale veiligheid groot zijn.

Extra investeringen zijn noodzakelijk

In 2021 adviseerde de raad voor de toenmalige kabinetsformatie een serie maatregelen[8] waarvoor de investeringen optelden tot €833 miljoen over vier jaar. Voor 2024 is destijds €194 miljoen structureel voorgesteld. Het beschikbare budget bleef in het vorige coalitieakkoord flink achter; voor 2024 is slechts €93 miljoen vrijgemaakt in de NLCS en als er niets extra´s wordt gedaan, zal dit bedrag vanaf nu tot 2027 niet verder stijgen.

De urgentie is sinds 2021 alleen maar verder toegenomen door de groeiende cyberdreigingen en nieuwe technologische ontwikkelingen. Dit leidt tot verhoogde complexiteit en steeds meer geavanceerde aanvallen, zowel door diverse statelijke actoren als cybercriminelen. Om dit te weerstaan zijn, naast intensieve samenwerking op de eerdergenoemde thema´s (zowel intern binnen de overheid als in de triple helix), aanvullende investeringen over de gehele linie noodzakelijk. Anders zal het niet mogelijk zijn om de NLCS en aanpalende strategieën in de benodigde versterkte vorm uit voeren.

De raad acht het daarom dringend noodzakelijk dat een nieuw kabinet het eerder geadviseerde budget van structureel ongeveer €200 miljoen voor 2024 opneemt in het nieuwe coalitieakkoord en dit laat oplopen naar €550 miljoen in 2028 en verder. Uit het voorgaande volgt dat de verschillende ministeries met name extra middelen nodig hebben voor:

- Het versterken van de NLCS op vier cruciale onderdelen:
  - Het inrichten van een adequate informatiedeling over alle sectoren heen.
  - Het effectief bestrijden van cybercrime.
  - Het verbeteren van de digitale beveiliging van operationele technologie (OT).
  - Het verkleinen van de cyberweerbaarheidskloof tussen bedrijven, met de focus op het mkb.
- Het implementeren en operationaliseren van aankomende EU wet- en regelgeving, ter verhoging van de cyberweerbaarheid van veel meer organisaties, inclusief het toezicht daarop (als onderdeel van de NLCS).
- Strategische thema´s die ook in de context van cybersecurity extra aandacht vragen:
  - Het opbouwen van eigen technische capaciteit ter versterking van onze digitale autonomie.
  - Het verstevigen van onderwijs en onderzoek.
  - Het benutten van kansen en het mitigeren van risico´s van nieuwe technologieën, zoals AI.

Internationale vergelijking

Uitgaande van de investeringen zoals nu opgenomen in de NLCS, is er voor de komende jaren sprake van stagnatie, terwijl juist ook in de EU de noodzaak van extra regulering en investeringen wordt onderkend. Als we de Nederlandse investeringen in een internationaal perspectief plaatsen, valt Nederland in negatieve zin op. Het blijkt dat veel andere landen (die vergelijkbaar zijn in de mate van digitalisering en in omvang van het BBP per capita) wel plannen hebben om hun cybersecurity-investeringen vanaf 2024 verder te verhogen, of daartoe al hebben besloten:

[8] CSR Adviesrapport 'Integrale aanpak cyberweerbaarheid' | Rapport | Cyber Security Raad

- Finland[9] voorziet in een verhoging van het overheidsbudget voor cybersecurity van 30% in 2024, in het bijzonder om AI-gerelateerde risico's aan te pakken. In 2024 komt het budget uit op 280 miljoen euro[10].
- Estland verhoogde het cybersecuritybudget van 2022 naar 2023 met 20% tot 156 miljoen euro en zal ook de komende vijf jaar het budget met zulke stappen verhogen.
- België lanceerde in 2021 een cybersecuritystrategie; ook zijn er plannen om een met 30% toenemend budget vrij te maken vanaf 2024, ter versterking van de aanpak op federaal niveau. Dit staat los van investeringen op regionaal niveau, waaronder bijvoorbeeld ook onderwijs en onderzoek valt.
- Dezelfde tendens geldt voor Zweden, waar ook structureel in onderzoek en innovatie wordt geïnvesteerd.
- Dit is eveneens het geval voor Australië waar vanaf 2022 doorlopend (voor 5 jaar) extra budget voor cybersecurity beschikbaar is, met een forse investering in het tegengaan van digitale dreigingen.

Tot slot

In de afgelopen kabinetsperiode zijn veel verschillende maatregelen genomen om onze cyberweerbaarheid op peil te brengen en te houden. Het vergt een continue inspanning om te beschermen wat ons dierbaar is. We moeten daarbij accepteren dat 100% cyberweerbaarheid niet bestaat, maar te vaak is nog sprake van onnodige incidenten en kwetsbaarheden, en ongewenste afhankelijkheden.

Het bovenstaande vraagt om strategische capaciteit, een stevige regie op de uitvoering, het tijdig nemen van adequate maatregelen, intensieve samenwerking én extra investeringen. De raad zal daarom ook tijdens de komende kabinetsperiode blijven adviseren over de uitvoering en uitwerking van de Nederlandse Cybersecuritystrategie. Het doel daarvan is steeds om het kabinet te helpen en daarbij vooruit te kijken, zodat onze samenleving digitaal veilig kan blijven.

Hoogachtend,
Namens de Cyber Security Raad,

Pieter-Jaap Aalbersberg
Covoorzitter CSR

Theo Henrar
Waarnemend covoorzitter CSR

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.

[9] Finland telt 5,2 miljoen inwoners en heeft een vergelijkbaar BBP per capita als Nederland.
[10] Zie: https://dig.watch/updates/finland-plans-30-increase-in-cybersecurity-spending-in-2024-to-counter-ai-based-cyber-threats