CSR Cyber Security Raad

URGENTIEVERKLARING

7 augustus 2023

Extra inzet op cyberweerbaarheid noodzakelijk voor een digitaal veilige samenleving en het benutten van economische kansen

Dreigingen, incidenten en kwetsbaarheden zetten ons land onverminderd onder druk

Nederland heeft veel profijt van de hoge mate waarin onze samenleving gedigitaliseerd is. Technologische ontwikkelingen zoals (generatieve) artificiële intelligentie (AI) en kwantumtechnologie gaan razendsnel en brengen essentiële cyberweerbaarheidsvraagstukken met zich mee. Naast de vele kansen die dit brengt voor onze economie zorgt de hoge mate van digitalisering ook voor kwetsbaarheden en ongewenste afhankelijkheden, wanneer cybersecurity onvoldoende prioriteit krijgt. De verhoudingen in het digitale domein worden namelijk steeds complexer en de gevolgen voor onze vrijheid, veiligheid en economisch verdienmodel kunnen aanzienlijk zijn, zoals recente ransomware-aanvallen op vooraanstaande bedrijven en instellingen hebben aangetoond. Ook de veiligheid van industriële systemen komt steeds verder onder druk te staan en is er steeds meer aandacht nodig voor de bestrijding van allerlei vormen van cybercrime. Geopolitieke ontwikkelingen zorgen er eveneens voor dat onze digitale veiligheid en autonomie verder in gevaar komen. De Cyber Security Raad (hierna de raad) wil dat het aanstaande kabinet sterker inzet op cybersecurity en meer investeert hierin. De focus zou daarbij moeten liggen op meer regie op samenwerking, versterking van onze digitale autonomie en het behoud van onze kennispositie, alsook versterking van het onderwijs.

Het bovenstaande wordt bevestigd door het Cybersecuritybeeld Nederland (CSBN) 2023. Zo laat de oorlog in Europa tussen Rusland en Oekraïne eens te meer zien dat statelijke actoren cyberaanvallen inzetten om hun geopolitieke doelen te bereiken, waarbij ook de digitale dreigingen voor Nederlandse overheidsorganisaties, bedrijven en kennisinstituten onverminderd groot zijn. Een ander risico is dat een aantal statelijke actoren op grote schaal data probeert te vergaren van bedrijven en burgers om hier voordeel uit te halen. Het CSBN waarschuwt verder dat cybercriminaliteit een aantrekkelijk verdienmodel is met veel schade voor burgers en (overheids-)organisaties als gevolg. Nieuwe technologische ontwikkelingen, zoals generatieve AI, worden daarbij ook ingezet door allerlei kwaadwillenden.

In 2021 heeft de raad ten behoeve van de toenmalige kabinetsformatie het adviesrapport 'Integrale aanpak cyberweerbaarheid' aangeboden. In dit adviesrapport heeft de raad inzichtelijk gemaakt welke maatregelen voor Nederland nodig zijn om de cyberweerbaarheid op het noodzakelijke niveau te krijgen en te houden.

De geadviseerde investeringen telden op tot €833 miljoen over een periode van vier jaar, waarvan bijna €600 miljoen structureel en ongeveer €200 miljoen voor 2024. Slechts een deel van de adviezen van de raad is in het vorige coalitieakkoord overgenomen en het beschikbaar gestelde budget bleef flink achter; omgerekend is minder dan de helft van de door de raad voorgestelde investeringen structureel vrijgemaakt.

In de vorige kabinetsperiode is het besef in Nederland en Europa gegroeid dat cybersecurity een absolute randvoorwaarde is voor veilige verdere digitalisering, en dat beleid hierop het beste gevoerd kan worden vanuit een perspectief op onze publieke waarden als privacy, veiligheid en digitale autonomie. Zowel nationaal als op Europees vlak zijn goede initiatieven ontplooid die gaan zorgen voor aangescherpte verplichtingen, versterkt toezicht op (overheids-)organisaties, verbeterde informatiedeling en veiligere producten en diensten. De aandacht hiervoor mag echter nooit verslappen, want cyberweerbaarheid blijft een permanente zorg. Er zijn niet alleen nog altijd kwetsbaarheden die opgelost moeten worden, maar ook worden er continu nieuwe manieren bedacht om systemen binnen te komen. Het op peil brengen en houden van onze cyberweerbaarheid is dan ook geen gemakkelijke opgave en extra aandacht en investeringen tot op het eerder door de raad voorgestelde niveau zijn vereist. Met name de implementatie van de Europese wet- en regelgeving moet prioriteit krijgen. Dit zal gevolgen hebben voor bestuurslagen en organisaties van groot tot klein. Daarnaast is het sterker toerusten van uitvoeringsorganisaties in het cyberdomein met passende, robuuste wettelijke kaders essentieel.

De raad acht extra aandacht en investeringen vooral noodzakelijk voor de volgende onderwerpen:

1. Verstevigen regie op samenwerking

Uit het voorgaande blijkt dat de cyberweerbaarheid van Nederland op essentiële onderdelen nog steeds gevaar loopt. Dit kunnen we ons niet veroorloven. Voor veilige verdere digitalisering is ***een stevige domein-overstijgende regie op samenwerking*** nodig, waarbij cybersecurity, digitale autonomie en bestrijding van cybercrime als integrale onderdelen en noodzakelijke randvoorwaarden worden gezien. Dit begint met een nationale strategie, het tegengaan van departementale verkokering en het besef dat cyberweerbaarheid chefsache is: verantwoordelijkheden dienen belegd te worden op het hoogste politiek-bestuurlijke niveau. De Nederlandse Cybersecuritystrategie (NLCS) is (evenals de Strategie Digitale Economie en de Werkagenda Waardengedreven Digitaliseren) in het najaar van 2022 verschenen. De raad heeft aan de NLCS bijgedragen en kan zich in grote lijnen vinden in de geformuleerde doelstellingen en acties.

Een nieuw kabinet moet inzetten op regie op de gezamenlijke uitvoering hiervan, op het houden van focus en op het inspelen op nieuwe ontwikkelingen, vanuit publiek-private samenwerking. Deze gezamenlijke uitvoering is ook zeer relevant voor provincies, gemeenten en waterschappen die hun beleid eveneens baseren op nationale strategievorming. Op operationeel niveau zijn door het werken in ketens de afhankelijkheden tussen organisaties groot en zijn allerlei systemen met elkaar verknoopt. Daarbij dient de aandacht uit te gaan naar zowel onze ICT-infrastructuur als naar industriële systemen, zoals gebruikt in de energiesector en bij waterkeringen, bruggen en sluizen.

2. Versterken digitale autonomie

Gezien de toename in afhankelijkheden, ook ten opzichte van grote technologiebedrijven, moet het nemen van maatregelen voor het behoud van onze digitale autonomie ***centraal op het hoogste politieke en ambtelijke niveau*** worden belegd. Een voorbeeld hiervan is versterking van het nationale cloudbeleid. Europese samenwerking is daarbij randvoorwaardelijk, waarin Nederland een voortrekkersrol kan nemen. Dit dient gedaan te worden vanuit een integrale visie op digitalisering die ook een impuls geeft aan onze cyberweerbaarheid. Daarbij moet er vanuit het perspectief van digitale autonomie gericht geïnnoveerd worden door de overheid én het bedrijfsleven.

3. Behoud kennispositie en versterking onderwijs

Tot slot kunnen maatregelen voor het verhogen van onze cyberweerbaarheid alleen uitgevoerd worden wanneer over de volle breedte van onze maatschappij voldoende cybersecuritykennis aanwezig is. Daarbij hoort ook een gezond en goed toegerust onderzoeks- en innovatieklimaat, ***met extra publiek-private investeringsmogelijkheden***. Het tekort aan voldoende gekwalificeerde cybersecurityspecialisten wordt steeds nijpender en opleidingen blijven vooral in kwantitatieve zin achter. Daarnaast is voldoende cyberbewustzijn van burgers essentieel. Dit begint bij extra inzet op ***digitale geletterdheid*** (inclusief digitale veiligheid) in het basis- en voortgezet onderwijs, gegeven de verdergaande technologisering in dit domein en vooruitlopend op een algehele herziening van het curriculum.

Gezien de urgentie van het cyberweerbaarheidsvraagstuk roept de raad u op om in uw verkiezingsprogramma de noodzakelijke plannen, zoals hiervoor geschetst, op te nemen. Het eerder door de raad geadviseerde budget van structureel ongeveer €200 miljoen per jaar (vanaf 2024) is in de komende vier jaar voor de verschillende ministeries noodzakelijk om met publiek-private-wetenschappelijke samenwerking maatregelen te nemen voor veilige verdere digitalisering. Alleen zo kunnen onnodige incidenten worden voorkomen en houden we onze samenleving digitaal veilig.

Wij zijn uiteraard altijd bereid om een en ander nader toe te lichten.

De raadsleden van de Cyber Security Raad,

Private sector

Dhr. mr. Th.J. (Theo) Henrar
(waarnemend covoorzitter)
Voorzitter FME (ondernemersorganisatie voor de technologische industrie), lid van CSR namens FME

Mw. drs. C. (Claudia) de Andrade-de Wit
CIO, Directeur Digital & IT Haven Rotterdam,
lid van CSR namens het CIO Platform

Dhr. drs. J. (Joost) de Bruin
CEO Ordina Nederland,
lid van CSR namens NLdigital

Mw. mr. drs. S.C. (Sylvia) van Es
President Philips Nederland,
lid van CSR namens VNO-NCW

Dhr. mr. J. (Joost) Farwerck
CEO en voorzitter van de Raad van Bestuur bij KPN,
lid van CSR namens de vitale infrastructuur

Mw. T. (Tineke) Netelenbos
Voorzitter ECP, lid van CSR namens ECP, Platform voor de Informatiesamenleving

Dhr. S.J.A. (Steven) van Rijswijk
CEO bij ING en bestuurslid van de Nederlandse Vereniging van Banken, lid van CSR namens de financiële sector

Publieke sector

Dhr. P.J. (Pieter-Jaap) Aalbersberg EMPM
(covoorzitter)
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

Dhr. drs. E.S.M. (Erik) Akerboom MPM
Directeur-Generaal Algemene Inlichtingen en Veiligheidsdienst (AIVD)

Dhr. vice-admiraal B.G.F.M. (Boudewijn) Boots
Plaatsvervangend Commandant der Strijdkrachten bij het ministerie van Defensie

Dhr. mr. M.P. (Michiel) Boots
Directeur-Generaal Economie en Digitalisering bij het ministerie van Economische Zaken en Klimaat

Mw. E. (Eva) Heijblom MSc
Directeur-Generaal Digitalisering en Overheidsorganisatie bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Dhr. mr. H.P. (Henk) van Essen
Korpschef Politie

Dhr. Mr. A.R.E. (Guus) Schram
Procureur-generaal en plaatsvervangend voorzitter van het College van procureurs-generaal

Wetenschappelijke sector

Mw. prof. dr. B. (Bibi) van den Berg
Hoogleraar Cybersecurity Governance verbonden aan het Institute of Security and Global Affairs van Universiteit Leiden

Mw. prof. mr. E.M.L. (Lokke) Moerel
Senior Of Counsel Morrison & Foerster LLP,
Hoogleraar Universiteit Tilburg

CYBER SECURITY RAAD
p/a Nationaal Coördinator Terrorismebestrijding en Veiligheid
Turfmarkt 147 I 2511 DP I Den Haag
Postbus 20011 I 2500 EA I Den Haag

Telefoon: 070 751 5333 (secretariaat)
E-mail: info@cybersecurityraad.nl
www.cybersecurityraad.nl