> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Ministerie van Justitie en Veiligheid
Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
5477819

Bijlagen
1

Datum 23 mei 2024
Onderwerp Toekomstvisie Cyberweerbaarheidsnetwerk

Om de digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties te vergroten is publiek-private samenwerking van essentieel belang. Een belangrijke manier om dit te bereiken is het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden. In deze brief ga ik in op de toekomstvisie van publiek-private samenwerking voor cybersecurity. Hierin kijken we hoe de verschillende bestaande elementen van het Landelijk Dekkend Stelsel kunnen uitbreiden en versterken.
Deze toekomstvisie vormt het kader voor de doorontwikkeling van dit stelsel, waarna gestart kan worden met het opstellen van een bouwplan. In dit bouwplan wordt de inrichting van dit stelsel verder uitgewerkt. Het sluitstuk van deze visie is een nieuwe naam die beter aansluit bij deze doorontwikkeling. Het Landelijk Dekkend Stelsel wordt omgedoopt tot het *Cyberweerbaarheidsnetwerk*, waarin met meer eenduidigheid, intensiever en breder zal worden samengewerkt in publiek-privaat verband.

Aanleiding

In 2017 adviseerde de Cyber Security Raad om het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden in te richten.[1] Een stelsel met als doel om organisaties in staat te stellen hun slagkracht te verhogen door informatie over cybersecurity breed, efficiënt en effectief met elkaar te delen. De beoogde partners in het stelsel waren publieke en private schakelorganisaties met een breed bereik richting het gehele Nederlandse bedrijfsleven. In 2018 is het Landelijk Dekkend Stelsel van start gegaan. Sinds de oprichting van het Landelijk Dekkend Stelsel hebben diverse ontwikkelingen plaatsgevonden die positief bijdragen aan de door de Cyber Security Raad beoogde succesfactoren.

In de Nederlandse Cybersecuritystrategie 2022-2028 zijn de ambities en acties voor een digitaal veilige samenleving opgenomen.[2] Het kabinet beschrijft in een van de acties dat in samenwerking met private partners een bouwplan wordt opgesteld dat het kabinet in staat stelt om samen met het bedrijfsleven de digitale weerbaarheid te verhogen. Hiermee willigt het kabinet ook een grote behoefte van de private partners in. Onderdeel van dit bouwplan is een overzicht van de huidige staat van het Landelijk Dekkend Stelsel om inzicht te creëren in de initiatieven die reeds zijn ontwikkeld en de huidige leemtes in het Landelijk

[1] https://www.cybersecurityraad.nl/documenten/adviezen/2017/06/01/csr-advies-naar-een-landelijk-dekkend-stelsel-van-informatieknooppunten---csr-advies-2017-nr.-2.
[2] Kamerstukken II, 2022-23, 26643, nr. 925.

Dekkend Stelsel. Deze kabinetsvisie geeft richting zodat het bouwplan kan worden uitgewerkt

Informatiedeling en het Landelijk dekkend Stelsel
Op grond van de Wet beveiliging netwerk- en informatiesystemen, waarin ook de eerste Europese netwerk- en informatiebeveiligingsrichtlijn (NIS1-richtlijn) is geïmplementeerd, heeft het Nationaal Cyber Security Centrum de taak om dreigings- en incidentinformatie te verstrekken aan vitale aanbieders en rijksoverheidsorganisaties.

Daarnaast kan het Nationaal Cyber Security Centrum op grond van diezelfde wet dreigings- en incidentinformatie, die is verkregen in het kader van de bijstandstaak voor vitale aanbieders en rijksoverheidsorganisaties, verstrekken aan schakelorganisaties, als deze informatie relevant is voor andere aanbieders dan Rijk en vitaal.[3] Deze schakelorganisaties zijn bij ministeriële regeling en bij wet aangewezen en bedienen allen een specifieke doelgroep.
Sinds de wijziging van de Wet beveiliging netwerk- en informatiesystemen van december 2022 kan het Nationaal Cyber Security Centrum in nog ruimere zin dreigings- en incidentinformatie delen met eerdergenoemde schakelorganisaties. Ook kan het Nationaal Cyber Security Centrum hierdoor in uitzonderlijke gevallen rechtstreeks informatie delen met aanbieders die niet deel uitmaken van de Rijksoverheid of geen vitale aanbieder zijn. Er is sprake van een dergelijk uitzonderlijk geval wanneer een organisatie geen wettelijk aangewezen schakelorganisatie heeft én een dreiging of incident aanzienlijke gevolgen heeft of kan hebben voor de continuïteit van de dienstverlening van deze aanbieder.

Ook is als gevolg van het ontwikkelen van het Landelijk Dekkend Stelsel het sectoraal Computer Security Incident Response Team-overleg ontstaan en is het vertrouwen tussen de partners in het stelsel gegroeid. Het Landelijk Dekkend Stelsel is daarnaast gekoppeld aan diverse informatiebronnen, zoals het Nationaal Detectie Netwerk. Deze ruimere mogelijkheden om informatie te delen is van invloed op de uitwerking van het bouwplan.

Veranderend landschap
De kernfunctie van het Landelijk Dekkend Stelsel betreft op dit moment het delen van dreigingsinformatie. De wettelijke kaders voor het Nationaal Cyber Security Centrum en andere organisaties met taken op het terrein van cybersecurity in Nederland gaan opnieuw veranderen. De aankomende implementatie van de herziene EU-richtlijn netwerk- en informatiebeveiliging (de NIS2-richtlijn) en het wetsvoorstel bevordering digitale weerbaarheid bedrijven hebben grote invloed op de mogelijkheden om dreigings- en incidentinformatie te kunnen delen.
De implementatie van de NIS2-richtlijn betekent ook een forse uitbreiding van de doelgroep van het NCSC naar meer dan 7.000 organisaties, waaraan informatie en advies bij digitale dreigingen en incidenten moet worden gegeven.
De daarnaast voorgenomen integratie van het Nationaal Cyber Security Centrum, het Digital Trust Center en het Computer Security Incident Response Team voor digitale dienstverleners tot één organisatie zal ook een belangrijke verandering vormen.[4] Deze nationale cybersecurity organisatie zal organisaties in Nederland, groot of klein, publiek of privaat, vitaal- of niet-vitaal, onder meer van relevante informatie en kennis over dreigingen en incidenten voorzien en waar mogelijk ook verdere hulp bieden bij incidenten.

[3] Dit zijn bijvoorbeeld aangewezen computercrisisteams en OKTT's (organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot andere netwerk- en informatiesystemen).
[4] Kamerstukken II 2022/23, 26643, nr. 1058.

In de loop der tijd zijn aanvullende wensen ontstaan voor samenwerking die goed passen bij de doorontwikkeling van het Landelijk Dekkend Stelsel naar het Cyberweerbaarheidsnetwerk. Er is behoefte aan het verbinden van meer typen schakelorganisaties zodat het bereik nog verder wordt verbreed. Voorbeelden van nieuwe netwerkpartners zijn bijvoorbeeld leveranciers van ICT- en securitydiensten die een belangrijke rol spelen in het weerbaar maken van ondernemingen binnen het Koninkrijk der Nederlanden. Daarnaast is er behoefte aan het uitbreiden van de functies waarbij, naast informatiedeling, aandacht is voor onderwerpen zoals kennisuitwisseling en opleiden, trainen en oefenen. Tot slot zijn in de loop der jaren meerdere initiatieven en samenwerkingsverbanden ontstaan die belangrijk zijn voor de cyberweerbaarheid, denk hierbij bijvoorbeeld aan het Programma Cyclotron.[5] Om al deze activiteiten te stroomlijnen en naadloos op elkaar aan te laten sluiten is consolidatie wenselijk.

Doelstelling en visie
Gebaseerd op het veranderende speelveld en het actieplan van de Nederlandse Cybersecuritystrategie is de doelstelling van het Cyberweerbaarheidsnetwerk aangepast. De vernieuwde doelstelling luidt: 'Met een brede set (publieke en private) organisaties gecoördineerd samenwerken, die gezamenlijk de verantwoordelijkheid willen dragen voor het uitvoeren van benodigde decentrale functies om organisaties binnen het Koninkrijk der Nederlanden in staat te stellen om hun weerbaarheidsniveau en daarmee hun slagkracht te verhogen.'
Om deze doelstelling te bereiken is een toekomstvisie geschetst die als basis dient voor het verder uit te werken bouwplan voor de publiek-private samenwerking op het gebied van cybersecurity. Deze visie wordt hieronder kort samengevat aan de hand van zeven beleidskeuzes.

1. Naamgeving: van Landelijk Dekkend Stelsel naar Cyberweerbaarheidsnetwerk

De huidige naam van het 'Landelijk Dekkend Stelsel' blijkt onvoldoende recht te doen aan de bedoeling. Zo is gebleken uit de gesprekken die met partners hierover zijn gevoerd. De termen 'landelijk', 'dekkend' en 'stelsel' wekken verwachtingen die niet overeenkomen met de realiteit en het doel van deze samenwerking. Daarom wordt de naam Cyberweerbaarheidsnetwerk geïntroduceerd die de essentie van de publiek-private samenwerking beter dekt en recht doet aan de vernieuwde doelstelling.

2. Aantal schakelorganisaties

Op dit moment zijn er, naast het Nationaal Cyber Security Centrum, zeven schakelorganisaties onderdeel van het huidige Landelijk Dekkend Stelsel. Deze schakelorganisaties zijn in de Wet beveiliging netwerk- en informatiesystemen of bij ministeriële regeling aangewezen. Om zoveel mogelijk organisaties binnen het Koninkrijk digitaal weerbaarder te maken is het van belang dat het Cyberweerbaarheidsnetwerk een breder bereik krijgt met meer en verschillende typen schakelorganisaties. Daarbij dienen deze schakelorganisaties onderling samen te werken zodat zij hun specifieke doelgroep organisaties beter kunnen bedienen en hun weerbaarheid kunnen vergroten. Onderdeel van deze uitbreiding is het aanhaken van meer sectorale computercrisisteams, Information and Sharing and Analysis Centres (ISACs) en overige samenwerkingsverbanden, coalities en brancheorganisaties. Deze nieuwe schakelorganisaties zijn belangrijk voor het Cyberweerbaarheidsnetwerk, aangezien deze schakelorganisaties regionaal en/of sectoraal de weerbaarheid van bedrijven en andere organisaties kunnen vergroten. Daarnaast is het van belang dat ook leveranciers van IT-oplossingen aan het netwerk worden toegevoegd, zoals Internet Service Providers, Managed Service Providers en Managed Security Service Providers.

[5] Kamerstukken II 2022/23, 26643, nr. 925.

3. Inzet van het netwerk tijdens en na een incident

De publiek-private samenwerking binnen het huidige Landelijk Dekkend Stelsel is op dit moment voornamelijk gericht op het delen van informatie in de periode vóórdat een cyberincident plaatsvindt. Maar tijdens en na incidenten en crises vormt publiek-private samenwerking ook een belangrijke meerwaarde. Daarom wordt er binnen het Cyberweerbaarheidsnetwerk voortaan niet enkel gekeken naar de publiek-private samenwerking voordat incidenten en crises plaatsvinden, maar wordt ook ingezet op het verder ontwikkelen van de samenwerking tijdens en na incidenten en crises in samenhang met de nationale crisisstructuur.

4. Andere vormen van publiek-private samenwerking

De huidige publiek-private samenwerking binnen het Landelijk Dekkend Stelsel is primair gericht op informatiedeling. Zoals eerder aangegeven, zal het publiek-private samenwerkingslandschap veranderen als gevolg van de vernieuwde wetgeving en de integratie van het Nationaal Cyber Security Centrum, het Digital Trust Center en het Computer Security Incident Response Team voor digitale dienstverleners tot een nationale cybersecurityorganisatie. Doordat er een centraal knooppunt ontstaat voor het delen van informatie zal er op termijn ruimte zijn om andere vormen van publiek-private samenwerking te stimuleren. In de praktijk zijn er meer activiteiten die schakelorganisaties (kunnen) verrichten in het netwerk die van toegevoegde waarde zijn voor de weerbaarheid van organisaties binnen het Koninkrijk. De verschillende thema's waarlangs publiek-private samenwerking verder ontwikkeld wordt zijn: (1) informatiedeling; (2) doelwit- en slachtoffernotificatie; (3) incidentafhandeling; (4) kennisuitwisseling (5) en tot slot opleiden, trainen en oefenen.

5. Afspraken over publiek-private samenwerking

Op dit moment zijn de taken en verantwoordelijkheden binnen het huidige Landelijk Dekkend Stelsel onvoldoende duidelijk. Ook zijn er onvoldoende heldere afspraken gemaakt over de wijze van samenwerking. Om ervoor te zorgen dat schakelorganisaties en hun doelgroep organisaties beter weten hoe zij het Cyberweerbaarheidsnetwerk kunnen inzetten, moeten de randvoorwaarden voor en afspraken over deelname beter worden vastgelegd binnen het cyberweerbaarheidsnetwerk. Dit zal leiden tot heldere formele rollen binnen het netwerk. Dit geldt bijvoorbeeld ook voor de samenwerking van het Nationaal Cyber Security Centrum met de Dutch Institute for Vulnerability Disclosure (DIVD). Hiermee geef ik uitvoering aan de motie Rajkowski.[6]

De ambitie van het Cyberweerbaarheidsnetwerk is dat uiteindelijk alle organisaties in het Koninkrijk der Nederlanden bereikt kunnen worden. Dit betekent dat er actief moet worden gezocht naar een set partners die samen dit bereik hebben. Van samenwerkingspartners wordt verwacht dat zij (pro)actief deelnemen aan het verder ontwikkelen van de functies van het netwerk, en dat zij daarbij het 'quid pro quo' principe hanteren en dus niet alleen kennis en informatie komen halen, maar ook brengen. Op die manier ontstaat er vertrouwen in dat deelnemers aan samenwerkingsverbanden wederkerig profiteren, een belangrijke voorwaarde om succesvol te zijn. Om deze doelen te bereiken is het ontwikkelen van een duidelijke set van samenwerkingsafspraken essentieel.

[6] Motie van het lid Rajkowski over onderzoek naar een formelere rol voor het Dutch Institute for Vulnerability Disclosure 2022D37576.

6. Sturing op publiek-private samenwerking

Er is op dit moment nog beperkt regie op het huidige Landelijk Dekkend Stelsel. Met de uitbreiding van deelnemers aan het Cyberweerbaarheidsnetwerk en het inrichten van nieuwe functionaliteiten zijn heldere governance en inrichtingsprincipes nog belangrijker geworden voor de doorontwikkeling van de publiek-private samenwerking. Er is daarom besloten dat regie nodig is op het netwerk als geheel, maar ook op de uitvoering ervan. De Nationaal Coördinator Terrorismebestrijding en Veiligheid zal optreden als regiehouder op het netwerk. De visie, het beleid en de kaders zijn en worden in nauwe afstemming en samenwerking met de beleidsdepartementen, de uitvoeringscoördinator én de netwerkpartners opgesteld en onderhouden. Het Nationaal Cyber Security Centrum, gezamenlijk met het Digital Trust Center, treedt op als uitvoeringscoördinator binnen het netwerk. Op termijn wordt dit de organisatie die ontstaat uit de integratie van het Nationaal Cyber Security Center, het Digital Trust Center en het Computer Security Incident Response Team voor digitale dienstverleners. Ook voor de uitvoering geldt dat deze in nauwe afstemming en samenwerking plaatsvindt, in dit geval met de regiehouder, beleidsdepartementen en netwerkpartners.
Regelmatig wordt de werking van het netwerk geëvalueerd, zowel voor wat betreft resultaten, als wat betreft de wijze van uitvoering.

7. Behoefte voor consolidatie veranderingen

Er zijn door de tijd heen veel losse initiatieven ontstaan (publiek én privaat) die raakvlakken hebben met de publiek-private samenwerking in het kader van het huidige Landelijk Dekkend Stelsel. Uit gesprekken met schakelorganisaties is gebleken dat er behoefte is aan consolidatie waarbij initiatieven waar mogelijk worden samengevoegd onder de paraplu van het nieuwe Cyberweerbaarheidsnetwerk. Daarbij is het uitgangspunt dat het netwerk goed aansluit op reeds lopende publiek-private samenwerkings-trajecten, zodat hierin consolidatie optreedt.

Vervolg
Deze visie is tot stand gekomen in nauwe samenwerking met publieke en private partners. De hierboven toegelichte beleidskeuzes en visie zullen ertoe leiden dat het Nationaal Cyber Security Centrum, in samenwerking met het Digital Trust Center, een bouwplan opstelt in samenwerking met publieke en private partners om het Cyberweerbaarheidsnetwerk door te ontwikkelen. In dit bouwplan wordt het startpunt bepaald waarbij voortgebouwd wordt op wat al aanwezig is in het netwerk en worden de activiteiten om het netwerk te versterken geprioriteerd. Hierbij worden goed lopende onderdelen van het huidige Landelijk Dekkend Stelsel voortgezet in het Cyberweerbaarheidsnetwerk en waar nodig verder ontwikkeld en gestimuleerd. Voorbeelden hiervan zijn het Programma Cyclotron en de afspraken die gemaakt zijn in het Landelijk Crisis Plan Digitaal.
De voortgang wordt op regelmatige basis bewaakt, zowel wat betreft de rolverdeling, als de inhoudelijke resultaten. Per functie worden publiek-private netwerkpartners gevraagd om actief betrokken te zijn bij de ontwikkeling van het netwerk en het bewaken van voortgang. Over de ontwikkeling van het Cyberweerbaarheidsnetwerk wordt uw Kamer periodiek geïnformeerd met de voortgangsrapportage over de Nederlandse Cybersecuritystrategie.

De Minister van Justitie en Veiligheid,

D. Yeşilgöz-Zegerius