Naar een landelijk dekkend stelsel van informatieknooppunten

Advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime

CSR
Cyber Security Council
Cyber Security Raad

Naar een landelijk dekkend stelsel van informatieknooppunten

Advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime

Gericht aan:
de minister van Economische Zaken
de staatssecretaris van Veiligheid en Justitie
de Korpschef Nationale Politie
het College van procureurs-generaal

de voorzitter van VNO-NCW
de voorzitter van MKB-Nederland
de voorzitter van Nederland ICT
de voorzitter van het CIO Platform Nederland
de voorzitter van de Raad van Bestuur van de Kamer van Koophandel (KvK)

CSR
Cyber Security Council
Cyber Security Raad

CSR-advies 2017, nr. 2

Excellenties, voorzitters,

Digitalisering brengt grote economische en maatschappelijke kansen met zich mee. Om die kansen te kunnen blijven benutten, is het noodzakelijk dat we vertrouwen hebben in de digitale wereld en ons er veilig in kunnen bewegen. Naast kansen brengt digitalisering ook dreigingen met zich mee onder andere op het gebied van spionage en sabotage.[1] Om bedreigingen tegen te gaan en ervoor te zorgen dat Nederland digitaal veilig is, is informatie-uitwisseling en samenwerking tussen overheidspartijen onderling en publieke en private partijen essentieel. Herna Verhagen pleit in haar rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten'[2] voor het verbeteren van de informatie-uitwisseling onder andere door uitbreiding van de Information Sharing and Analysis Centres (ISAC's) en het Nationaal Detectie Netwerk (NDN). Uit het onlangs verschenen rapport 'The Netherlands Cyber Readiness at a Glance'[3] blijkt dat de informatie-uitwisseling voor ons land een belangrijk punt van aandacht is, het scoorde het laagst op de *readiness index*. De urgentie van dit onderwerp is hoog: het tijdig beschikken over de juiste informatie is van groot belang voor de digitale weerbaarheid van organisaties in zowel publieke als private sectoren. Digitale weerbaarheid is één van de pijlers van een welvarend Nederland.

Informatiepositie bedrijfsleven

De raad constateert dat de informatie-uitwisseling met betrekking tot dreigingsinformatie en handelingsperspectieven met het Nederlandse bedrijfsleven dat niet als vitaal is aangemerkt in hoge mate tekort schiet. De huidige informatie-uitwisseling is hoofdzakelijk gericht op de Rijksoverheid en organisaties in de vitale infrastructuur. Het niet als vitaal aangemerkte deel van het bedrijfsleven heeft bewust of onbewust een informatietekort, omdat zij onvoldoende of niet zijn aangesloten op de structuur waarbinnen cybersecurity gerelateerde informatie wordt gedeeld. Er bestaat een aantal publiek-private samenwerkingsverbanden waarbij dreigingsinformatie en handelingsperspectieven worden gedeeld met het niet als vitaal aangemerkte deel van het bedrijfsleven, maar dit vormt geen dekkend geheel. Verder geldt dat vitale sectoren in grote mate afhankelijk zijn van toeleveranciers uit het niet als vitaal aangemerkte deel van het bedrijfsleven. Deze partijen zijn dus ook van invloed op de digitale veiligheid van de gehele keten. Het besef dat samengewerkt moet worden in digitale ketens is inmiddels wel tot diverse partijen doorgedrongen, maar moet voor een belangrijk deel nog worden vormgegeven.

Randvoorwaarden onvoldoende op orde

Om actuele, betrouwbare en toegankelijke informatie te kunnen uitwisselen moet aan bepaalde randvoorwaarden worden voldaan. Alle betrokken partijen moeten zich bewust zijn van het belang van wederzijdse informatie-uitwisseling. Ook moeten bedrijven voldoende in staat zijn de beschikbare informatie te verwerken en de handelingsperspectieven snel op te volgen. Op dit moment is er bij een deel van het bedrijfsleven nog relatieve onbekendheid met de digitale dreigingen en het belang van informatie-uitwisseling om deze dreigingen te kunnen beheersen. Ieder bedrijf is verantwoordelijk voor zijn eigen digitale veiligheid. Midden- en kleinbedrijven (mkb) hebben hier vaak geen budget voor, terwijl dit anno 2017 een management verantwoordelijkheid is en een essentieel onderdeel van de bedrijfsvoering. Herna Verhagen adviseert in haar rapport om 10 procent van het IT-budget als maatstaf te nemen.

[1] Cyber Security Beeld Nederland 2017

[2] 'De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten', Herna Verhagen, september 2016

[3] 'The Netherlands Cyber Readiness at a Glance', Melissa Hathaway & Francesca Spidalieri, Potomac Institute for Policy Studies, mei 2017

Het niet als vitaal aangemerkte deel van het bedrijfsleven heeft behoefte aan heldere contactpunten, maar is nu aangewezen op (het niet dekkende geheel van) publiek-private samenwerkingsverbanden en ICT dienstverleners. Niet alleen het delen van informatie met betrekking tot dreigingen is belangrijk, ook het kunnen analyseren van informatie en het stellen van prioriteiten in de aanpak op basis van informatie is belangrijk.

Gebrek aan inzicht in cybercrime

Cybercriminaliteit neemt in omvang toe en vormt een steeds grotere bedreiging.[4] De groeiende dreiging voor de cybersecurity van Nederland wordt vooral veroorzaakt door beroepscriminelen en statelijke actoren.[5] Door het gebrek aan meldingen/aangiftes is er een incompleet beeld van cybercrime in Nederland. Inzicht in cybercrime is noodzakelijk om effectiever erop in te kunnen spelen. De oorzaak van het lage aantal meldingen ligt onder andere in de complexiteit van het doen van aangifte. En als wel aangifte wordt gedaan, is er vaak onvoldoende zichtbare opvolging van de aangifte en vindt nauwelijks terugkoppeling plaats over wat er met de aangifte is gedaan. De kans op imagoschade voor het betreffende bedrijf is ook een belangrijke factor in het niet doen van aangifte.

Geconcludeerd kan worden dat op dit moment een groot deel van het bedrijfsleven een zwakke informatiepositie heeft en dus een makkelijk doelwit is voor cybercriminelen. Ook ontbreekt het aan goed inzicht in de cybercrime die ons land treft, waardoor het effectief hierop inspelen wordt bemoeilijkt. De informatie-uitwisseling binnen Nederland moet worden verbeterd, zodat we in de toekomst op dit punt zichtbaar stijgen op de *readiness index.*

Advies

Het delen en analyseren van informatie maakt het mogelijk om de cybersecurity van organisaties te vergroten en organisaties weerbaarder te maken tegen cyberincidenten en/of de schade ervan te beperken. Dit is van belang voor *alle* organisaties in Nederland. De raad vindt dat er snel maatregelen moeten worden getroffen om de informatie-uitwisseling in ons land op het gewenste peil te brengen, zodat Nederland ook digitaal een safe-place- to-do business is en blijft. Dit vereist het zoveel mogelijk wegnemen van barrières bij het delen van informatie en het stimuleren van het meldings- en aangifteproces en de opvolging ervan.

Het doel van dit advies is het verbeteren van de informatie-uitwisseling in Nederland door (1) de invoering van een landelijk dekkend stelsel van informatieknooppunten, (2) het scheppen van de randvoorwaarden voor succesvolle informatie-uitwisseling via de informatieknooppunten en (3) het vergroten van het inzicht in cybercrime door het stimuleren van het doen van meldingen en het versterken van de publiek-private samenwerking op dit terrein.

De raad onderscheidt de volgende belangrijke succesfactoren:

- *Een landelijk dekkend stelsel van informatieknooppunten[6] voor informatie-uitwisseling dat het hele Nederlandse bedrijfsleven bestrijkt;*
- *Het bedrijfsleven is in staat snel opvolging te geven aan dreigingsinformatie en handelingsperspectieven;*
- *Leveranciers van internetproducten en -diensten hebben een actieve houding ten aanzien van de*

[4] Nationaal dreigingsbeeld 2017, Georganiseerde criminaliteit, Politie, mei 2017
[5] Cyber Security Beeld Nederland 2017
[6] Onder informatieknooppunten wordt verstaan: bestaande organisaties, schakelorganisaties, instrumenten en initiatieven die de informatie-uitwisseling bevorderen.

invulling van de zorgplichten, zodat de producten en diensten intrinsiek veilig zijn;
- *Het eenvoudig kunnen melden/aangifte doen van cyberincidenten bij de politie.*

De raad onderscheidt de volgende handelingsperspectieven:
- *Nederland ontwikkelt een landelijk dekkend stelsel van informatieknooppunten;*
- *Nederland zorgt dat randvoorwaarden voor een succesvolle informatie-uitwisseling via de informatieknooppunten op orde zijn;*
- *Nederland zorgt ervoor dat cybercrime beter inzichtelijk wordt en versterkt de publiek-private aanpak op dit terrein.*

Ad. 1 Nederland ontwikkelt een landelijk dekkend stelsel van informatieknooppunten.

Landelijk dekkend stelsel

De raad adviseert de overheid om in samenwerking met de private sector op korte termijn te komen tot de invoering van een landelijk dekkend stelsel van informatieknooppunten. Het landelijk dekkend stelsel moet ervoor zorgen dat de informatie-uitwisseling het hele Nederlandse bedrijfsleven bestrijkt. Op dit moment is dat nog niet het geval en moet het stelsel worden uitgebreid. Bij de ontwikkeling van het landelijk dekkend stelsel wordt zoveel mogelijk gebruikgemaakt van reeds bestaande (schakel) organisaties, instrumenten en initiatieven op dit terrein. Het wetsvoorstel gegevensverwerking en meldplicht cybersecurity (WGMC) geeft het NCSC ruimere mogelijkheden om informatie te delen. Dit vindt de raad een goede ontwikkeling. Het is van belang dat het bedrijfsleven al dan niet met behulp van schakelorganisaties in voldoende mate in staat is dreigingsinformatie te verwerken en de handelingsperspectieven snel uit te voeren. Een inventarisatie van de stand van zaken vormt het vertrekpunt voor op- en uitbouw van het huidige stelsel. Ook acht de raad het van belang dat de verschillende rollen, taken en verantwoordelijkheden van de deelnemende organisaties onderling goed worden afgestemd en vastgelegd. De versnippering moet worden teruggebracht en de ontbrekende schakels in het stelsel moeten worden ingevuld.

De raad adviseert dat de ontwikkeling van een landelijk dekkend stelsel onder regie van de ministeries van Veiligheid en Justitie en Economische Zaken plaatsvindt in nauwe samenwerking met onder andere VNO-NCW, MKB-Nederland, CIO Platform Nederland en Nederland ICT.

Aandachtspunten ten aanzien van het landelijk dekkend stelsel zitten op de volgende onderdelen: Digital Trust Centre (DTC), Nationaal Detectie Netwerk (NDN) en Information Sharing and Analysis Centres (ISAC's) en regionale en sectorale initiatieven en leveranciers.

DTC

De raad onderschrijft het belang van de op 13 juni jl. aangenomen motie van de leden Hijink (SP) en Tellegen (VVD) over het oprichten en vormgeven van een DTC voor het niet als vitaal aangemerkte deel van het bedrijfsleven. De raad vindt dat een DTC in het kader van het bovengenoemde landelijk dekkend stelsel op juiste wijze moet worden gepositioneerd ten opzichte van de reeds bestaande informatieknooppunten. Een DTC moet actuele, betrouwbare en toegankelijke informatie beschikbaar stellen aan het bedrijfsleven. Het bedrijfsleven moet op zijn beurt een actieve houding aannemen in het opvolgen van adviezen en bereid zijn om zelf ook informatie te leveren aan een DTC.

NDN

De raad dringt aan op een versnelde uitrol van het Nationaal Detectie Netwerk (NDN). Eventuele obstakels moeten hierbij uit de weg worden genomen. De informatie uit het NDN moet ook kunnen

worden doorgezet naar het niet als vitaal aangemerkte deel van het bedrijfsleven via de Information Sharing and Analysis Centres (ISAC's) en een DTC.

ISAC's

De raad is van mening dat ISAC's een rol van betekenis spelen bij het delen van kennis en informatie binnen sectoren. De raad vraagt wel meer aandacht voor een cross sectorale en ketengerichte aanpak bij de ISAC's. De raad ondersteunt het voorstel van het ministerie van Economische Zaken over de oprichting van ISAC's voor de topsectoren. Dit draagt bij aan een betere cybersecurity van bedrijven die deel uitmaken van de topsectoren, omdat dit kennisintensieve bedrijven zijn die kwetsbaar zijn voor cybercrime. Dit van groot belang voor het toekomstige verdienvermogen van ons land.

Regionale en sectorale initiatieven

De raad vindt het van belang dat er regionale en sectorale initiatieven worden ontplooid waarbij de overheid, de vitale sectoren en het niet als vitaal aangemerkte deel van het bedrijfsleven, van mkb tot multinationals, zijn aangesloten. Grote bedrijven beschikken over meer mogelijkheden (mensen en middelen) om te investeren in cybersecurity. Vanwege ketenafhankelijkheden is het van groot belang dat alle ketenpartners aandacht hebben voor cybersecurity. Er zijn verschillende initiatieven gestart bijvoorbeeld bij Schiphol en de Rotterdamse haven, waarbij ketenpartners samenwerken om hun cybersecurity op orde te krijgen. De raad onderschrijft het belang van dergelijke initiatieven.

Leveranciers

Leveranciers van internetproducten en -diensten spelen een essentiële rol in het veilig maken en houden van organisaties. Zij dienen een goede invulling te geven aan hun zorgplichten en zij dienen hun klanten te ontzorgen door het leveren van relevante en toegankelijke informatie bij het veilig houden van hun digitale infrastructuur.

Ad. 2 Nederland zorgt dat randvoorwaarden voor een succesvolle informatie-uitwisseling op orde zijn.

Ondersteunende rol VNO-NCW, brancheorganisaties en Kamer van Koophandel (KvK)

Alle bedrijven, vitale bedrijven en niet als vitaal aangemerkte bedrijven, van mkb tot multinationals, moeten zich bewust zijn van de risico's die zij lopen en de grote rol die informatie-uitwisseling kan spelen bij het nemen van de juiste beveiligingsmaatregelen. De raad ziet voor brancheorganisaties een belangrijke functie weggelegd op het terrein van cybersecurity richting het bedrijfsleven. Hierbij gaat het om het informeren over en het wegwijs maken in het informatielandschap en om het verspreiden van doelgerichte dreigingsinformatie en handelingsperspectieven. Brancheverenigingen kunnen hun leden ook stimuleren om melding te doen van incidenten en/of aangifte te doen bij de politie. VNO-NCW kan de brancheorganisaties ondersteunen bij hun functie richting het bedrijfsleven. Ook ziet de raad een belangrijke rol voor de KvK bij het cyber-bewustmaken van het bedrijfsleven.

Financiële stimulans

Het 'maturity-level' van brancheorganisaties verschilt, daarom kunnen zij hulp gebruiken om de gewenste rol op het terrein van cybersecurity naar behoren te kunnen uitvoeren. De Rijksoverheid moet een financiële stimulans voor brancheorganisaties mogelijk maken, zodat brancheorganisaties hun functie op het terrein van cybersecurity richting het bedrijfsleven kunnen vervullen.

Ad. 3 Nederland zorgt ervoor dat cybercrime beter inzichtelijk wordt en versterkt de publiek-private aanpak op dit terrein

Doen van melding en aangifte

De Nationale Politie moet kunnen anticiperen op de ontwikkelingen op het gebied van cybercrime. Als cybercrime wordt gemeld, ontstaat er een beter beeld van de stand van zaken op het gebied van cybercrime. Het moet daarom voor burgers en het bedrijfsleven laagdrempeliger en toegankelijker worden om melding en/of aangifte van cybercrime te doen door bijvoorbeeld het mogelijk te maken om digitaal melding te maken van cybercrime. Hierbij geldt het principe ‘melden is belangrijker dan aangifte doen’, Met behulp van de toename van meldingen kunnen trends beter worden gesignaleerd en prioriteiten in de aanpak worden gesteld. VNO-NCW, MKB-Nederland, brancheverenigingen, KvK, Nederland ICT en het CIO Platform Nederland kunnen bedrijven stimuleren om actiever te zijn in het doen van melding en aangifte. De raad vraagt aandacht voor een goede terugkoppeling aan de melders door de politie zodat men op de lange duur gemotiveerd blijft om meldingen te doen.

Publiek-private samenwerking cybercrime

De raad vindt het van belang dat in het kader van het verbeteren van de informatiepositie op het gebied van cybercrime extra wordt geïnvesteerd in de publiek- private samenwerking. Deze samenwerking blijkt in veel gevallen van meerwaarde te zijn. Dat betekent dat de politie en het OM samenwerken met bijvoorbeeld de bancaire sector, de ICT-branche en andere relevante private partners aan een digitaal weerbaar en veilig Nederland.

GERICHTE ADVIEZEN

De adviezen zijn gericht op de overheid en het bedrijfsleven. Alleen als de verbetering van informatie-uitwisseling op het terrein van cybersecurity en cybercrime in gezamenlijkheid wordt opgepakt gaat het werken. De raad adviseert:

De minister van Economische Zaken en de staatssecretaris van Veiligheid en Justitie gezamenlijk:

1. Voer in samenwerking met de private sector een zoveel mogelijk op bestaande structuren gebaseerd landelijke dekkend stelsel van informatieknooppunten in. Versnel in dit kader de invoering van een Digital Trust Centre voor het bedrijfsleven dat geen deel uitmaakt van de vitale infrastructuur.

De minister van Economische Zaken

2. Maak een financiële stimulans mogelijk voor brancheorganisaties, zodat zij hun functie op het terrein van cybersecurity richting het bedrijfsleven kunnen vervullen.

De staatssecretaris van Veiligheid en Justitie:

3. Versnel de uitrol van het Nationaal Detectie Netwerk (NDN) en maak het mogelijk informatie uit het NDN breed te delen met het bedrijfsleven.

De minister van Economische Zaken, de voorzitter van VNO-NCW, de voorzitter van MKB-Nederland de voorzitter van Nederland ICT, de voorzitter van het CIO Platform Nederland, de voorzitter van de Kamer van Koophandel en voorzitters van brancheverenigingen gezamenlijk:

4. Maak het bedrijfsleven cyberbewust en motiveer hen een actieve rol in het delen van dreigingsinformatie en opvolgen van handelingsperspectieven op zich te nemen in het kader van het landelijk dekkend stelsel.
5. Stimuleer bedrijven om melding en/of aangifte van cybercrime te doen.
6. Zorg voor een cross sectorale aanpak van ISAC's waarbij de ketengedachte centraal staat. De initiatieven die Schiphol en de Rotterdamse Haven met hun ketenpartners hebben ontwikkeld zijn daar goede voorbeelden van.

De Korpschef Nationale Politie

7. Maak het doen van melding en/of aangifte van cybercrime door slachtoffers laagdrempeliger en zorg voor een goede terugkoppeling over de opvolging ervan.

De Korpschef Nationale Politie en het College van procureurs-generaal gezamenlijk:

8. Intensiveer en structureer de publiek-private samenwerking om de informatiepositie met betrekking tot cybercrime te versterken.

's-Gravenhage, juni 2017

Namens de Cyber Security Raad,

Eelco Blok Dick Schoof