GOV19

Cybersecurity: De dreiging neemt exponentieel toe

Pieter-Jaap Aalbersberg (NCTV)
Cyberincidenten zijn onderdeel van geopolitiek

Nathalie Jaarsma (Speciaal Gezant Cyber en Veiligheid ministerie van BZ)
We hebben een verantwoordelijkheid om het domein veilig te houden

Jan Swillens (MIVD)
Vaak lastig om vast te stellen wie achter een aanval zit

Erik Akerboom (AIVD)
Het is echt een nieuwe wereld waarin we zitten

de inhoud openen

Atos

JAARGANG 12 • NUMMER 19 • VOORJAAR 2022

INHOUD

En verder

VOORWOORD

Versterken digitale weerbaarheid: belangen kwetsbaar, dreiging complex

Cybersecurity is een essentiële randvoorwaarde voor de Nederlandse digitale economie en de samenleving, zo staat te lezen in de brief van 7 februari jl. van de minister van Economische Zaken en Klimaat aan de Tweede Kamer. Het impliceert, schrijft bewindsvrouw Micky Adriaansens, dat het aanbod van ICT-producten en diensten veiliger moet worden. Dat cybersecurity kennisontwikkeling en -innovatie gestimuleerd moeten worden. Dat consumenten en bedrijven zich meer bewust worden van digitale dreigingen en risico's, en hun weerbaarheid vergroten.

Diezelfde maand veranderde de Russische president Poetin de geschiedenis van Europa door Oekraïne met geweld binnen te vallen. Nadat vorig jaar de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) het nieuws haalde met het oprollen van een Russisch cyberspionagenetwerk, werd met de actie van Poetin nog duidelijker dat nationale veiligheidsbelangen kwetsbaar zijn, substantieel worden bedreigd en mogelijk aangetast door statelijke actoren.

Pieter-Jaap Aalbersberg, de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) spreekt over 'hybride' dreigingen, waarbij naast inzet van traditionele militaire middelen sprake is van het *hacken* van vitale infrastructuur of communicatiesystemen. Ook propaganda en nepnieuws worden gebruikt om de (lokale) bevolking op een verkeerd been te zetten. In dezelfde lijn maakte Jan Swillens, directeur van de Militaire Inlichtingen en Veiligheidsdienst (MIVD), het nieuws bekend van een *hack* op routers van willekeurige Nederlandse particulieren en bedrijven door een onderdeel van de Russische militaire inlichtingendienst GROe met als mogelijke inzet spionage, beïnvloeding en sabotage; bedreigend voor internationale vrede en veiligheid.

Juist als het gaat om onze democratische rechtsorde, of digitale integriteit en soevereiniteit, wil je in het kader van dreiging door statelijke actoren kunnen beschikken over een goede inlichtingenpositie en daar je eigen beveiliging op kunnen inrichten, is de toon van de gesprekken die we voor deze editie van GOV magazine voerden.

Maar de kloof tussen dreiging en weerbaarheid is de afgelopen jaren juist toegenomen. In de driehoek 'te beschermen belang', 'digitale dreiging' en 'weerbaarheidsmaatregelen' is een goede samenwerking, nationaal en internationaal, daarom noodzaak. Bijvoorbeeld als het gaat om sneller en gemakkelijker informatie te kunnen delen over digitale kwetsbaarheden en dreigingen.

Uiteindelijk zitten wij hier in Nederland op een enorm internetknooppunt. Wij zijn vergaand gedigitaliseerd en wij plukken economisch de vruchten van het internet. Dus wij hebben daarmee ook een verantwoordelijkheid om het domein veilig te houden.

Ik wens u véél leesplezier en inspiratie toe!

Met vriendelijke groet,

Willem Beelen
Hoofdredacteur GOV magazine en lid van de Atos Expert Community

ECCC: focus op ontwikkelen cybersecuritycapaciteit

Europa heeft een nieuwe organisatie om innovatie en industriebeleid op het gebied van cybersecurity te ondersteunen. Op 28 juni 2021 is daartoe de Verordening tot oprichting van het European Cybersecurity Competence Centre and Network (ECCC) gepubliceerd. Het ECCC vormt samen met het netwerk van nationale coördinatiecentra (NCC's) een ecosysteem dat de capaciteit van de cyberbeveiligingstechnologiegemeenschap in Europa moet gaan versterken. Miguel González-Sancho is deze nieuwe ECCC-organisatie aan het inrichten.

Het ECCC gaat in samenwerking met de EU-lidstaten een gemeenschappelijke agenda opstellen voor onderzoek, innovatie en ontwikkeling op het gebied van cyberbeveiligingstechnologie en dan gericht op de brede toepassing ervan binnen het openbaar bestuur en het bedrijfsleven. Cybersecurity is een van de hoogste prioriteiten van de Europese Commissie, met name om de Europese democratie en de integriteit van de 'digital single market' te beveiligen en te handhaven.
"Als alles met elkaar is verbonden, kan alles worden gehackt", zei voorzitter van de Europese Commissie Ursula von der Leyen afgelopen september bij de aankondiging van een Europese *Cyber Resilience Act*. Doel van dit wetsvoorstel is om gemeenschappelijke beveiligingsregels vast te stellen voor digitale producten en diensten die binnen de Europese Unie op de markt komen.

Het ECCC richt zich op het beheer van 1) onderzoek naar geavanceerde oplossingen voor IT-beveiliging (waarbij door de EU gefinancierde onderzoeksresultaten standaard open zijn); en 2) cybersecurityonderdelen van het programma Digitaal Europa (DIGITAL). Dit laatste programma richt zich op de operationele capaciteit van Europa's meest essentiële digitale componenten, zoals kunstmatige intelligentie (AI), supercomputers, geavanceerde digitale vaardigheden en cybersecurity.

Met betrekking tot dit laatste licht González-Sancho toe: "De Europese Commissie is al vele jaren actief door het financieren van ondersteunend onderzoek op het gebied van cybersecurity, en nu komt het DIGITAL-programma daar nog bij. En daar komt het ECCC in beeld, als het echt gaat om het aspect cybersecurity capaciteitsopbouw. De focus ligt daarbij op het anticiperen op cyberweerbaarheid. Voor alle duidelijkheid: het ECCC is niet in het leven geroepen om snel te reageren bij incidenten. Onze belangrijkste missie is het opbouwen van cyberweerbaarheidsvermogen."
"En belangrijk om te benadrukken: meer cyberweerbaarheidsvermogen is niet alleen bedoeld om beter voorbereid te zijn op cyberdreigingen, maar impliceert ook het verder ontwikkelen van een markt. Er zijn een aantal belangrijke strategische gebieden voor de Europese soevereiniteit in het digitale domein. Kunstmatige intelligentie (AI) is er een van, cybersecurity een andere. Veel EU-lidstaten zijn actief met de opbouw van cybersecuritycapaciteit, hetzelfde geldt voor de industrie. Het doel van het ECCC is om een structuur te bedenken die deze activiteiten en initiatieven op cybergebied onder één dak brengt."

Strategische prioriteiten

Het ECCC gaat de financiering beheren van de cybersecurityfondsen voor zowel het programma Digitaal Europa als dat van Horizon Europa en conform de lange-termijnbegroting van de EU voor 2021-2027. Daarnaast zullen ook de EU-lidstaten hieraan gaan bijdragen. Sinds de vaststelling van de Verordening tot oprichting, vertelt González-Sancho, is de raad van bestuur officieel aangesteld. Elke lidstaat en ook de Europese Commissie hebben vertegenwoordigers benoemd en de eerste officiële vergaderingen hebben plaatsgevonden om de strategische prioriteiten te bespreken.
"Er is nog veel administratief werk te doen, juist ook omdat de ECCC niet in Brussel of Luxemburg is gevestigd, waar de Europese Commissie is gezeteld. Het is in feite de eerste keer dat Roemenië gastheer is van een Europees organisatie. De Europese Commissie zal het kenniscentrum voor cybersecurity onder beheer houden,

Miguel González-Sancho Bodero is interim CEO van het European Cybersecurity Competence Centre and Network (ECCC) dat de Europese Unie ondersteunt bij het ontwikkelen van technologische en operationele cybersecuritycapaciteit. Het hoofdkantoor van ECCC is gevestigd in Boekarest. González-Sancho is sinds juli 2018 hoofd van de eenheid voor cyberbeveiligingstechnologie en capaciteitsopbouw bij de Europese Commissie, directoraat-generaal Communicatienetwerken, inhoud en technologie (DG Connect). Hij werkt inmiddels meer dan 20 jaar voor de Europese Commissie, met name aan beleidsdossiers en onderzoeks- en innovatieprogramma's, gericht op de sociale en economische impact van digitale technologie. González-Sancho was ook lid van het kabinet van de toenmalige vicevoorzitter van de Europese Commissie voor de Digitale Agenda, Neelie Kroes.

totdat het ECCC financieel en operationeel onafhankelijk kan functioneren. Als laatste zal het ECCC moeten worden aangesloten op de nationale coördinatiecentra van de verschillende EU-lidstaten en dat vereist ook nog enige afstemming."

'Incident response' is niet een van de taken van het ECCC. Maar gezien de toename van het aantal dreigingen en incidenten – zoals bijvoorbeeld Log4j – ligt het dan voor de hand om ook dergelijke incidenten proactief af te handelen?
"Een van de uitdagingen bij onderzoek naar cybersecurity is dat IT voortdurend verandert, en beveiliging loopt er altijd achteraan. Om uw vraag te beantwoorden: ja, in de toekomst zal het ECCC zijn verantwoordelijkheid nemen en de volledige keten aan benodigde cybersecuritycapaciteit afdekken. Van fundamenteel (basis)onderzoek tot en met de inzet van cyberbeveiligingsoplossingen. Daarom evalueert de Europese Commissie ook de aanvragen voor toepassingsprojecten ter ondersteuning van onderwerpen als AI en cybersecurity. Binnen Europa is zeer veel en goede cybersecurityonderzoekscapaciteit bij bedrijven en universiteiten beschikbaar. Maar als we naar de markt kijken, in concreto: wat er wordt gebruikt en ingezet, dan zijn dat voornamelijk oplossingen van buiten de EU. Vraag is dan ook: hoe kunnen we die kloof overbruggen? Dat geldt overigens niet alleen voor cybersecurity, dat geldt ook voor allerlei thema's op technologisch gebied. Een van de dingen waaraan het ECCC-bestuur werkt, is een strategische agenda met prioriteiten om dat soort ontwikkelingen in de toekomst goed te kunnen ondersteunen en te faciliteren."

Niettemin, als gevolg van de snelle ontwikkelingen in cyberdreigingen, heb je als het gaat om onderzoek, ontwikkeling en innovatie, enige stabiliteit nodig in termen van financieringsondersteuning, betoogt González-Sancho. "We hebben immers te maken met geld van de belastingbetaler en dat vereist transparante processen en plannen om de steun te verkrijgen van de *stakeholders*, in plaats van korte-termijnreacties op incidenten, wat feitelijk de taak van anderen is."
Hij vertelt dat het ontwikkelen van veilige software en dito oplossingen voor digitale weerbaarheid voorbeelden zijn van onderwerpen die in dit kader worden overwogen. "Hoe kunnen we dit soort beveiligingsoverwegingen naar de markt brengen als de markt eigenlijk heel snel software ontwikkelt?" Dat vraagt wellicht om wettelijke eisen, verplichtingen van sommige marktpartijen en 'zachte', maar sturende afstemming tussen de verschillende autoriteiten, zegt hij. "Maar je hebt een combinatie van dat alles nodig om succesvol te zijn.
De verschillende onderdelen moeten elkaar feilloos aanvullen. Waar we nu op inzetten zijn de instrumenten van de technologische toekomst."

Komt er een soort bibliotheek? Hoe komen we te weten over onderzoeksresultaten of beschikbare software?
"We zijn gebonden aan de regels van de programma's Digital Europe en Horizon Europe als het gaat om het publiek maken van de resultaten van EU-projecten. Nogmaals, dit is het geld van de belastingbetaler, dus daarvoor geldt standaard een open publicatie met betrekking tot wetenschapsbeleid. Echter, we hebben het hier over cybersecurity op bepaalde onderzoeks- en ontwikkelingsgebieden en dan kunnen er publicatiebeperkingen gelden. In sommige gevallen kan men ervan uitgaan dat informatie van gevoelige of strategische aard is en dan niet openbaar mag worden gemaakt, dat kan."

Korte termijn

De ECCC concentreert zich nu op de uitvoering van de begroting 2021-2022, terwijl er ondertussen ook wordt gewerkt aan de prioriteiten voor de latere begroting, zegt González-Sancho. "Er is een belangrijk element binnen de ECCC-structuur dat ik niet ongenoemd wil laten en dat is flexibiliteit. Het komt erop neer dat de EU-lidstaten zelf kunnen beslissen over de bijdragen die zij willen gaan leveren. Zo kunnen ze ook besluiten om hun gezamenlijke inspanningen via het ECCC uit te voeren."
"Een grote uitdaging wordt het nog om de beschikbare fondsen verder te vergroten. En direct daaraan gerelateerd is er de uitdaging voor de ECCC om met de strategische agenda te komen en de prioriteiten te gaan bepalen. Toch zou ik willen zeggen dat het de grootste uitdaging is om ervoor te zorgen dat alle betrokken partijen, dat wil zeggen alle EU-lidstaten en het ECCC, gaan samenwerken. *The proof of the pudding* voor de nabije toekomst is gelegen in het aantal projecten dat via samenwerking wordt gerealiseerd en dat cybersecuritycapaciteit, financiering en ondersteunende instrumenten voor digitale weerbaarheid worden gemobiliseerd."

Het is gerechtvaardigd om te concluderen dat er verschillen zijn tussen de EU-lidstaten voor wat betreft de mate van digitalisering. Sommige zijn verder dan andere. Voorziet u problemen?
"Daar hebben we in Europa in het algemeen al de hele tijd mee te maken. Het is duidelijk dat er, zonder namen te noemen, grote verschillen zijn op het gebied van cybercapaciteit. We zitten gezamenlijk in datzelfde schuitje, dus moeten we ook proberen niemand achter te stellen als het gaat om financiële steun en de verschillende cybersecurityprogramma's. We staan voor iedereen open en combineren dat in strategische samenwerkingen."
Kijkend naar de Europese samenwerking op het gebied van cybersecurity over de afgelopen vijf, zes jaar is González-Sancho vol vertrouwen. "Er is veel gebeurd wat voorheen niet denkbaar was. Er is een sterke trend om meer dingen samen te doen binnen de EU. En ja, het is zeker een uitdaging, ik bedoel, cybersecurity is al ingewikkeld op nationaal niveau. Maar over één ding is iedereen het eens: we moeten meer aan cybersecurity gaan doen, en een manier vinden om het gezamenlijk aan te pakken. We hebben te maken met een cyberbeveiligingspandemie en daar moeten we onze verantwoordelijkheid in nemen."

NCTV: digitale snelweg loopt dwars door samenleving heen

Nederland heeft een inhaalslag te maken waar het gaat om cybersecurity. De kloof tussen dreiging en weerbaarheid is groot, zelfs toegenomen de afgelopen jaren. Dat blijkt uit het 'Cybersecuritybeeld Nederland 2021', het jaarlijkse rapport van de NCTV. "Cyberaanvallen kunnen het zenuwstelsel van onze maatschappij raken en daarmee de maatschappij ontwrichten", zei Pieter-Jaap Aalbersberg bij de presentatie van het rapport. De digitalisering van de Nederlandse economie, en daarmee het effectief integreren van *supply chains*, legt ons geen windeieren, zegt Aalbersberg, "maar we zien ook dat juist door die samenhang de samenleving kwetsbaar is voor dreiging door criminelen en statelijke actoren."

De vraag is dan ook: wat moet er gebeuren om invulling te kunnen geven aan het beschermen van digitaal Nederland? Daartoe worden in de Nederlandse Cybersecurity Agenda (NCSA) de kaders gesteld. De agenda spreekt van zeven ambities:
1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software.
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur.
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime.
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling.
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

Via de Cybersecurity Alliantie geven publieke en private partijen maatregelen uit de agenda vorm. Ook wordt het Landelijk Dekkend Stelsel (LDS) verder doorontwikkeld om informatie over cybersecurity breder, efficiënter en effectiever te delen met publieke en private partijen. Het Nationaal Cybersecurity Centrum (NCSC) en het Digital Trust Center (DTC) zijn belangrijke schakels in het LDS. Het doel van deze kennisuitwisseling is ontwrichting te voorkomen en Nederland meer cyberweerbaar te maken.

Integraal vraagstuk

Cybersecurity is al lang niet meer iets dat met een computersysteem te maken heeft, stelt Aalbersberg. "De digitale snelweg maakt een steeds groter deel uit van de infrastructuur van ons land. We hadden asfalt, rail, water en lucht, daar is digitaal bijgekomen. Wij werken via de digitale snelweg, kopen via de digitale snelweg, we leren via de digitale snelweg, we socializen en communiceren met elkaar. De digitale snelweg loopt dwars door de samenleving heen. Dat betekent ook dat we de verdere ontwikkeling van de digitale infrastructuur niet als een los cyberinstrument moeten zien maar als een integraal vraagstuk. We worden steeds meer afhankelijk van die digitale infrastructuur en dat vraagt om investeringen die meer van gelijk niveau zijn met de andere delen van de infrastructuur in ons land. Een klassiek voorbeeld: als we in Nederland tien kilometer snelweg aanleggen dan omvat dat alle componenten: de vangrail, de verlichting, de kabels, alles zit erin. Zo ver zijn we nog niet in cybersecurity. Het is ook complex want in het ontwerpen van digitale snelwegen kun je niet eventjes zeggen 'we zetten er een hek omheen'. Het is een wedloop waar leveranciers van hardware en software, bedrijven, burgers en overheid voortdurend in beweging moeten blijven om te zorgen dat de *gap* tussen dreiging en weerbaarheid zo klein mogelijk wordt. Dat is een continu proces."
Aalbersberg stelt dat 'veiligheid' vaak nog wordt gezien als een sluitstuk. "In de klassieke veiligheid van een organisatie is dat ook logisch: een hek, een slagboom, een portier. Maar als het gaat om cybersecurity: dat is niet een sluitstuk, dat is onderdeel van je verdienvermogen. Je moet het belang ervan veel meer vooraan in de lijn meewegen, dus als onderdeel van je investeringen. In die golf zitten we nu en ook de Cyber Security Raad[1] (CSR) drukt op die integraliteit. We zullen als samenleving meer moeten investeren om ervoor te zorgen dat een van onze belangrijkste infrastructuren veilig is en veilig blijft."

Nederland heeft net een nieuw kabinet. Hebben bewindsleden hiervan kennisgenomen?
"Ik ben heel enthousiast over de tekst van het Regeerakkoord. Er is zelfs een staatssecretaris voor Digitale Zaken benoemd. Er is veel aandacht voor cybersecurity en ik lees een oproep aan departementen en andere partijen om te blijven investeren. Natuurlijk, vanuit mijn perspectief had er veel meer geld bij gemogen maar het kabinet doet nog steeds een forse investering. Cybersecurity is een groot thema in onze samenleving dat steeds hoog op de agenda moet blijven staan."
"Niet alleen bij de NCTV die kijkt hoe vitale processen te kunnen

Pieter-Jaap Aalbersberg is sinds 1 februari 2019 de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV richt zich naast contraterrorisme en statelijke actoren ook op de derde maatschappelijke opgave om Nederland digitaal veilig te maken. Aalbersberg was eerder korpschef van de politie-eenheid Amsterdam Amstelland. Ten tijde van de ramp met vlucht MH17, in 2014, leidde hij de repatriëringsmissie in de Oekraïne. Aalbersberg was lid van verschillende commissies van de Europese Unie tegen de aanpak van georganiseerde criminaliteit en maakte ook deel uit van het Executive Committee van Interpol.

"Cyberincidenten zijn onderdeel van geopolitiek"

beschermen. Het gaat ook om de grote bedrijven, het mkb, de burgers. Dit vraagt van ons allemaal wat. De NCTV is niet de baas, de NCTV is coördinerend en werkt onder de politieke verantwoordelijkheid van de minister van Justitie en Veiligheid. De cybersecurity agenda is niet van de NCTV maar is van het kabinet. Het is eigenlijk het spoorboekje van de Rijksoverheid samen met partners. Daarom vragen we ook advies aan de CSR en anderen omtrent wat we willen bereiken de komende jaren. De Tweede Kamer moet ook kunnen controleren wat de ambities zijn en wat de plannen opleveren. Er is nu ook een commissie Digitale Zaken in de Tweede Kamer die over inhoudelijke kennis beschikt."
Een belangrijk advies van de CSR is om meer te investeren in het onderwijs. In de woorden van Aalbersberg: "Er gewoon voor zorgen dat onze nieuwe burgers, onze toekomstige bestuurders, al vanaf de basisschool meer in de cyberwereld thuis zijn. Stellen wij onze samenleving in staat om de toekomst aan te kunnen? Dat klinkt heel groot, dat weet ik, maar het is veelomvattend. Vandaar dat we het hebben opgeknipt in zeven ambities, anders komt er geen beweging. Vandaar ook die hoge bedragen door alle partijen genoemd, want op alle vlakken moet je wat doen. Het gaat om onze nieuwe infrastructuur."

U zegt: de NCTV is coördinator, geen baas. Maar: zou er niet een baas moeten zijn? Is eindverantwoordelijkheid in deze aanpak voldoende gewaarborgd?
"We doen dit juist niet alleen maar samen met verschillende departementen. Het ministerie van Justitie en Veiligheid heeft een coördinerende rol op dit thema maar het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is bijvoorbeeld verantwoordelijk voor de digitale overheid. Ministeries als Economische Zaken en Klimaat en Infrastructuur en Waterstaat, met grote domeinen, doen volop in deze discussie mee en daar ben ik blij om. Er moet iemand zijn die kan duiden en er is een minister die zegt: 'Dit is wat we hebben afgesproken'. Zo zit ons land in elkaar en daar ben ik voorstander van. Het gaat erom dat we met elkaar verantwoordelijkheid nemen. Dat betekent ook dat je elkaar moeten kunnen aanspreken. Natuurlijk moet je als overheid op die processen regisseren en sturen. Of je ook moet kunnen ingrijpen en opleggen, daarop hebben we nog geen antwoord, dat zijn vragen voor de toekomst. Dat zijn echt zaken die je met elkaar moet bespreken. Alles op één punt neerleggen, daarvoor is het te groot. Maar de overheid moet wel regie voeren."

Publiek-privaat

Waarbij aangetekend: "Wat je vandaag opschrijft, is over drie maanden verouderd. De technologische innovaties en de werkelijkheid gaan sneller dan een overheid die dat probeert te reguleren. Zoals we leren als overheid dat dreiging een continu proces is geworden. Dialogen daarover vinden dus ook voortdurend plaats en we zijn ons er zeer van bewust dat de nieuwe agenda leidend is voor het beleid van dit kabinet. Het vaststellen van die agenda gebeurt altijd in samenhang. De kracht van Nederland is echt die publiek-private samenwerking. Er zijn weinig landen met zo'n samenwerkingsverband tussen wetenschap, privaat en publiek."

De overheid heeft een enorme *wake-up call* gekregen door de Citrix[2] affaire, zegt Aalbersberg. "Er zijn gelukkig grote stappen gemaakt; de aanpak van Citrix toen en meer recent van Log4j[3], dat is een wereld van verschil." Dat laatste is mede te danken aan het NCSC, dat een centrale rol is toebedacht in de operatie rondom dergelijke incidenten en de communicatie met partijen in het veld. "De overheid is meer dan de Rijksoverheid. Lokale overheden, waterschappen en provincies maken ook daarvan deel uit. Als ik kijk naar het bedrijfsleven dan denk ik dat het mkb nog voor grote uitdagingen staat. Individuele winkels kunnen die zelf niet aan, men zal in de collectiviteit stappen moeten zetten. En: we hebben ook de zorg voor zeventien miljoen burgers. Daar zien we ook kwetsbaarheden. Want als je praat over digitale infrastructuur, dan praat je ook over componenten als je smartphone of je laptop. Hoe slagen we erin als overheid om ook die kwetsbaarheden te beschermen?"
België kent een heel pragmatische oplossing: Itsme® waarbij bijvoorbeeld authenticatie wordt gekoppeld aan je smartphone. Er maken zo'n zes miljoen Belgen gebruik van. Het Centrum voor Cybersecurity België is bovendien centraal coördinatiepunt voor cyberveiligheid in België en bedient bevolking, bedrijven, overheidsdiensten en organisaties van vitaal belang via een één-loket aanpak. Is dat iets wat voor Nederland ook zou kunnen helpen?
"Je moet ervoor oppassen dat je een oplossing kiest die niet over *promise and under deliver* is. Als je al je inwoners als rechtstreekse klant ziet, dan moet je de dienstverlening wel kunnen garanderen in een zuiver overheidsproces. In Nederland is cybersecurity een gedeelde verantwoordelijkheid. Daarnaast is het kwetsbaar om van bedrijven afhankelijk te worden. Dat zijn elementen die voor ons meespelen in zo'n afweging. Andere landen maken andere keuzes."

"Wat ik wel belangrijk vind: hoe beschermen we de burger tegen verkeerde informatie, tegen misbruik van foto's, tegen manipulatie? Dat zijn grote vragen. De komst van sociale media is een *gamechanger* in de samenleving, ook als we kijken naar contraterrorisme en radicalisering."
De Europese Commissie werkt aan wetgevend kader door middel van de TOI-verordening die vanaf 7 juni 2022 van toepassing is op alle aanbieders van hostingdiensten die actief zijn in de EU. "In dat licht verwacht ik dat op korte termijn een wetsvoorstel naar de Tweede Kamer gaat wat het mogelijk moet maken om in te grijpen en berichtgeving over terrorisme en kindermisbruik *offline* te halen. Dat gebeurt in open bronnen, maar het is een eerste stap. Nederland probeert ook heel veel sectoren aan het werk te zetten."

Grote uitdagingen

"We staan voor grote uitdagingen. We zullen grote incidenten krijgen. Dat kan niet anders. We zullen ons erop moeten prepareren. En we zullen van elke situatie weer moeten leren. Ik zie wel dat wij ten opzichte van andere landen grote stappen maken en dat 'publiek' en 'privaat' met elkaar in verbinding zijn. Maar het is ook vallen en weer opstaan. Vanuit mijn rol voor nationale veiligheid moet ik ervoor zorgen dat we in ieder geval geprepareerd zijn op grote calamiteiten in de vitale sectoren. Dat moeten we samen doen.
Ik ben een optimist als ik kijk naar die vormen van samenwerking en ik ben een realist dat de dreiging groot is. Cyberincidenten zijn een onderdeel van geopolitiek."

[1] In 2011 heeft de toenmalige minister van Veiligheid en Justitie de Cyber Security Raad (CSR) geïnstalleerd. De CSR is een onafhankelijk adviesorgaan en heeft als taak de regering, publieke en private partijen gevraagd en ongevraagd te adviseren over relevante ontwikkelingen op het gebied van cybersecurity

[2] Door een beveiligingslek in de software van Citrix slaagden hackers erin om toegang te krijgen tot systemen van honderden Nederlandse bedrijven, overheden, ziekenhuizen en onderwijsinstellingen. Dit gebeurde in december 2019.

[3] December 2021 werd een kritieke kwetsbaarheid aangetroffen in Apache Log4j en dat impliceerde een groot beveiligingsrisico voor een breed scala aan organisaties omdat de software onderdeel is van webapplicaties en allerlei andere systemen.

Uw bedrijfskritische data beschermen

Iedere dag worden bedrijven, instellingen of particulieren geraakt door ransomware of malware. Het is vandaag de dag helaas niet meer de vraag of je gehackt wordt maar eerder wanneer; het gebeurt al vaak zonder dat we het door hebben. Uit een rapport van het Nationaal Cyber Security Centrum bleek dat er wereldwijd 1800 bedrijven zijn getroffen door gijzelsoftware. Een aantal daarvan ook in Nederland.

Hebben we het over ransomware dan wordt er vaak relatief weinig 'losgeld' gevraagd. Daarmee is dit dan ook slechts een klein deel van de werkelijke totale kosten van zo'n aanval. Zonder data geen bedrijfsvoering; de gevolgen van zo'n incident kunnen echter wel desastreus zijn voor uw organisatie. Denk hierbij aan verlies van data, omzet en mogelijke reputatieschade wat weer kan leiden tot een vertrouwensbreuk met uw klanten. Ook wordt veelal na het betalen van het losgeld niet de benodigde decryptie software gegeven en is de kans groot dat na verloop van tijd er een tweede aanval zal worden gedaan. De aanvaller weet immers dat er hoogstwaarschijnlijk weer zal worden betaald...

Het beschermen tegen cyber attacks ofwel uw cyber resilience kent verschillende lagen. Van goed naar beter naar best. Het is goed om data veilig te stellen met een back-up op disk of tape en herhaaldelijk het herstel te testen. Maar kwaadwillenden hebben steeds vaker het doel om naast primaire data ook back-up data te vernietigen of te versleutelen. De beste en ook veiligste oplossing is een onveranderbare kopie van back-up data en catalogus in een onzichtbare kluis te stoppen. Deze onzichtbare kluis, ook wel een cyber recovery vault genoemd, is zowel fysiek, als qua productie netwerk connectiviteit afgesloten van de productie omgeving. Het verbergen van data in een kluis is de juiste aanpak, maar niet de oplossing voor alles. Anders zou een tape ook voldoen. De opgeslagen data moet ook continu geanalyseerd worden op verdachte veranderingen die duiden op malware of ransomware. Want wanneer weet u dat data geïnfecteerd is?

Hiervoor wordt met cyber recovery software de data in de kluis automatisch geanalyseerd op verdachte veranderingen zoals aangepaste file extensies, bestandsgrootte, corrupte file structuur, corrupte file content of deels versleutelde bestandsinhoud. Vervolgens wordt hier direct over gerapporteerd. Met deze aanpak kan nog niet eerder geïdentificeerde malware of ransomware worden gedetecteerd. Het is mogelijk om binnen de kluis in een zogenaamde 'clean-room' de data te controleren zonder invloed van buiten en daarna getroffen productiesystemen te herstellen. Onze teams en onze specialisten gaan vanzelfsprekend graag met u in gesprek over onze oplossingen die bijdragen aan uw cyber resilience.

Jean Jacques Kroesbergen
Director Public & Connected Sustainable Society by **Dell Technologies Nederland**.

U kunt mij bereiken via mail
Jean_Jacques_Kroesbe@Dell.com
of bel naar **+31615629320**

DELL Technologies

CCB: evolutie vraagt tijd

Een tweetal strofes uit de Cybersecuritystrategie 2.0 van België: 'De evolutie van de cyberdreiging van financieel gedreven naar geopolitiek gemotiveerd is uiterst zorgwekkend. Westerse landen worden geconfronteerd met een dreiging in cyberspace die het gevaar van fysieke aanvallen overstijgt (...) Cybersecurity is niet enkel de verantwoordelijkheid van de overheid. Het is een gezamenlijke inspanning, waar alle betrokken stakeholders aan kunnen bijdragen: bevolking, bedrijven, overheidsdiensten en organisaties van vitaal belang'.

Het CCB geldt als centraal coördinatiepunt voor cyberveiligheid in België en bedient derhalve al die betrokken stakeholders. Een één-loket aanpak die voordelen biedt, stelt De Bruycker. Hij vertelt dat het CCB is gestart met het zich een beeld vormen van die betrokken partijen en de aan hen te leveren services. Die zijn vervolgens in een catalogus gegroepeerd.
"Het internet wordt vaak als een *public space* gezien maar ik denk dat er sprake is van een *private space* om eerlijk te zijn. Neem deze virtuele ontmoeting: ik ben verbonden met een privénetwerk van een internet serviceprovider, ik ga over die lijnen naar een andere internet serviceprovider om dan uiteindelijk in uw privéomgeving terecht te komen. Dat geldt voor 99 procent van alle internetverkeer. Het is niet zo dat ik hier naar buiten stap zoals ik uit mijn huis stap en de straat opga. In de fysieke publieke ruimte kunnen we als overheid relatief gemakkelijk camera's plaatsen vanuit veiligheidsoverwegingen, maar als overheid kun je niet zomaar een detectiesysteem plaatsen bij een internet serviceprovider. Echter, de cyberdreiging neemt toe en naar de bevolking is onze belangrijkste taak om ze daarvan bewust te maken. Sinds 2017 voeren we in de maand oktober campagne."
"De tweede groep zijn bedrijven en hen willen we vooral tools aanreiken. We hebben een cybersecurity *reference guide* gemaakt met daarin opgenomen een 160-tal checkpunten, opgesplitst naar *basic* en *advanced*, waarmee ze dreigingsniveau en risicoanalyse kunnen meten."
De derde groep zijn overheidsdiensten. België heeft een complexe overheidsstructuur wat een gecoördineerd cyberveiligheidsbeleid voor overheidsdiensten niet eenvoudig maakt. Daar ligt een uitdaging, erkent De Bruycker, "omdat overheidsdiensten in België zeer onafhankelijk werken en niet graag, laten we zeggen, beïnvloed worden of gestuurd worden of gecontroleerd worden door anderen. Dus dat was een beetje een moeilijke groep om mee van start te gaan, maar we hebben daarvoor toch een vorm gevonden vorig jaar en dat loopt nu ook."
De vierde groep kenmerkt hij als de belangrijkste: organisaties van vitaal belang. "Dat zijn de aanbieders van essentiële diensten en de operatoren van kritieke infrastructuur. Daarvoor hebben we bijvoorbeeld een *early warning* systeem gebouwd, een centrale hub waarop we alle informatie binnentrekken en vervolgens delen met die organisaties van vitaal belang en met de inlichtingen- en veiligheidsdiensten."

Evenwichtsoefening

"We hebben het CCB opgestart met als idee: wij gaan de leiding nemen. Maar cybersecurity is zeker niet enkel materie voor ons. Iedereen heeft zijn verantwoordelijkheid en wij willen iedereen respecteren in zijn verantwoordelijkheid. Dus ja, wij zijn de nationale autoriteit, maar we staan open voor alle voorstellen en voor alle ideeën. Feit is dat een dergelijke evolutie tijd vraagt. En zoals met alle evoluties in de wereld en in de geschiedenis, als je te snel wilt dan krijg je weerstand. Dat is een beetje de evenwichtsoefening die denk ik elk land meemaakt. Op een bepaald moment brengt iemand iets in beweging en dan komt er een reactie en zo ontstaat een wisselwerking. Defensie heeft aangegeven veel meer capaciteit te gaan opbouwen, misschien zelfs een offensieve capaciteit te gaan oprichten. Dat is nu een beweging in België die we proberen te kaderen. Wat betekent dit? Wat is het politiek draagvlak daarvoor? Eind vorig jaar hebben de Verenigde Staten besloten meer offensieve capaciteit in te zetten tegen de *ransomware* dreiging. Ik ben zeer benieuwd naar wat het effect daarvan zal zijn."

In uw Cybersecuritystrategie 2.0 waarin taken en doelstellingen voor de periode 2021-2025 worden geschetst, is het doel geformuleerd dat tegen 2025 België in het cyberdomein één van de minst kwetsbare landen van Europa moet zijn. Dat is een duidelijke ambitie. Hoe benchmarkt zich dat nu en wat is er dan nog nodig?
"Die benchmarking blijft een waanzinnige uitdaging. Wij gebruiken daarvoor momenteel een aantal indexen die meer strategisch van aard zijn, zoals bijvoorbeeld de National Cyber Security Index, die beheerd wordt door Estland. Daarnaast maken we gebruik van het BITSIGHT platform, dat is een meer technisch platform dat ons zicht geeft op onze kwetsbaarheden. Wij kunnen daar permanent volgen wat de ranking is van ons land ten opzichte van de andere EU-landen."
"Die kwetsbaarheid kent in onze visie twee richtingen: enerzijds de menselijke kwetsbaarheid en anderzijds de

Miguel De Bruycker is sinds 17 augustus 2015 directeur van het Centrum voor Cybersecurity België (CCB), de nationale autoriteit voor cyberveiligheid in België. In 2020 werd zijn mandaat aan het hoofd van het CCB verlengd met een tweede termijn van vijf jaar. De Bruycker studeerde aan de Koninklijke Militaire School en aan de Vrije Universiteit Brussel. In 2005 werd hij binnen de Algemene Dienst Inlichting en Veiligheid verantwoordelijk voor de veiligheid van geclassificeerde netwerken en voor het oprichten van de eerste Cyber Security capaciteit van Defensie. De Bruycker was een drijvende kracht achter de oprichting van het CCB in 2014.

"Cybersecurity is niet enkel de verantwoordelijkheid van de overheid"

technische kwetsbaarheid. De menselijke kwetsbaarheid, die komt er eigenlijk op neer: je kunt over de meest veilige wagen beschikken en het beste wegensysteem en de beste veiligheidsmaatregelen, maar daar past ook een zeker gedrag en bewustzijn van de chauffeur bij. Op het internet komt veel *spoofing* voor, dat is je voordoen als iemand anders, en het is zaak dat gebruikers zich daarvan bewust zijn en zich naar gedragen. Sinds 2017 kennen we hier in België in de maand oktober een grote nationale awareness campagne. De meest recente campagne was 'Wees slimmer dan een *phisher*'. We hebben sinds de start burgers ook gevraagd dat als ze iets verdachts opmerken dit via e-mail aan ons te melden. Dat kunnen ze doen op safeonweb.be, dat is ons nationaal portaal voor de bevolking. Op vier jaar tijd zijn we erin geslaagd om het aantal meldingen te laten stijgen naar bijna 13.000 per dag! Dat geeft ons een ongelooflijk zicht op wat er allemaal gebeurt en wij sturen die *malicious* links door naar bijvoorbeeld Microsoft en Google."
In dit verband, vertelt De Bruycker, wordt ook gebruikt gemaakt van het Belgian Anti-Phishing Shield (BAPS), een systeem waarbij in samenwerking met een aantal grote internet serviceproviders wordt gewaarschuwd voor onechte webpagina's. "Wij sturen per dag gemiddeld 10 tot 30 duizend keer een waarschuwing uit, wat betekent dat er even zo vaak door iemand op een link wordt geklikt naar een kwaadaardige webpagina."

Zijn er bepaalde trends uit af te leiden, komen die mails uit bepaalde landen of kringen?
"Nee, die analyses kunnen we niet zomaar maken. Feit is wel: het wordt alsmaar moeilijker om *phishing* mails te herkennen. Ze volgen de actualiteit, het is vaak ook perfect Nederlands en Frans. Ze worden beter en dus het is dringend tijd dat wij ook beter worden anders gaat het fout lopen."

Is er samenwerking met andere landen binnen Europa overigens in dit kader, de trends en de risico- en dreigingsactoren lijken min of meer gelijk?
"De dreigingen die wij zien zijn inderdaad voor de meeste EU-landen gelijkwaardig. Er komt op verschillende onderwerpen samenwerking op gang, vaak nog *case by case*, maar dat is een fantastische evolutie."
De Bruycker refereert onder meer aan *FluBot malware* die in mei 2021 opdook en waarmee criminelen zich via een app toegang verschaffen tot Android smartphones. Hij voegt eraan toe dat de Cybersecuritystrategie 2.0 van België ook aan een internationale context raakt, aan initiatieven van de Europese Unie om de cyberweerbaarheid binnen de EU te promoten en te verbeteren, met als basis de Cybersecurity Act van 2019.

Al in 2005 publiceerde u een visiedocument over cyberdefensie. U was er vroeg bij?
"Ja, blijkbaar wel. Ik zat als stafofficier bij de informaticadienst van Defensie en had directe contacten met stafofficieren van de dienst strategie. Die werkten aan een toekomstvisie voor Defensie en ik ben dan gevraagd om een hoofdstuk te schrijven over cyberdefence. Ik had al interesse in de initiatieven van de Amerikaanse luchtmacht op dat gebied en een toevallige ontmoeting met een vroegere studiegenoot gaf me ook veel inzicht. Ik vond dat toen al een heel boeiende materie omdat wij vanuit ICT-oogpunt ook geconfronteerd werden met de uitdaging om de netwerken van Defensie te beveiligen."

Strategische visie

"Mijn strategische visie voor de toekomst is dat je niet alleen de mensen moet klaarmaken voor het internet, maar dat we ook het internet zullen moeten klaarmaken voor de mens. En dat betekent dat we een extra laag zullen moeten bouwen bovenop het internet die veel meer gebaseerd is op digitale identiteit. Sta me toe een voorbeeld te geven: wanneer je op het internet een website opzet, dan komt daar een certificaat op, dat is een slotje dat je ziet in de URL-balk. Als je kijkt naar de fysieke wereld, althans in België is het al meer dan 100 jaar zo voor drukwerk, dan ben je wettelijk verplicht als je een flyer verspreidt of een affiche uithangt om erop te zetten wie verantwoordelijk is voor die boodschap. Maar dat is niet zo voor websites."
"Ik vind dat wij als overheid ook een rol spelen als het gaat over het wettelijk kader van het internet en dat betreft ook de identiteit. Stel je voor dat we allemaal rondrijden op de snelweg in een wagen zonder nummerplaat, wie houdt zich dan nog aan regels?" De Bruycker spreekt in dit verband over het concept van *trusted publisher* waarbij wordt uitgegaan van een aantal validatieniveaus waarvoor certificaten kunnen worden afgegeven.
"Het hoogste niveau is *extended validation* wat wil zeggen dat zowel de organisatie als de identiteit van de aanvrager worden gecontroleerd. Dat zie je als je bij je bank inlogt."
Hij vertelt dat er een prototype browser plug-in is ontwikkeld waardoor aan internet gebruikers via kleuren (groen, geel, oranje) zichtbaar wordt gemaakt hoe (on)veilig de bezochte website is. "Het doel is als ik een mail krijg van mijn bank met een link en ik klik op die link en ik kom terecht op een website die lijkt op de website van mijn bank, maar het niet is, dan kleurt de plug-in oranje."

Omgekeerd praat De Bruycker ook over het concept van *trusted sender* waarbij de identiteit van degene die een boodschap verstuurt kan worden gevalideerd. Daarbij zou gebruik gemaakt kunnen worden van Itsme® een app voor de smartphone waarmee mensen zich online kunnen identificeren. De app is een initiatief van enkele telco's en banken in België, is door de overheid geadopteerd en kent inmiddels bijna zes miljoen gebruikers. Een mobiele oplossing met als basis een door de overheid gevalideerde identiteit.
De Bruycker: "Waarom zou ik met die app niet aanloggen op mijn e-mail, op mijn Messenger of mijn WhatsApp? Dan krijg ik bijvoorbeeld een DID, een *Decentralized ID* token, met een bepaalde geldigheidsduur en om de zoveel tijd moet ik opnieuw via Itsme® bevestigen dat ik het ben en dan krijg ik een nieuw *token* en als ik een bericht ontvang van iemand – dat kan een sms zijn, een e-mail of een WhatsApp - dan kan ik controleren of daar een digitale identiteit aan gekoppeld is ja of nee."
Hij vertelt dat er in Estland en Griekenland vergelijkbare systemen bestaan, gekoppeld aan de smartphone. "Of dergelijke systemen onfeilbaar zijn, daarop heb ik geen antwoord, maar Itsme® is naar mijn weten nog nooit gekraakt."
De Bruycker plaatst wel een kanttekening. "Dergelijke toepassingen en ideeën ondervinden vaak weerstand omdat ze afbreuk zouden doen aan het concept van een open en *free* - lees bijna anoniem – internet. Dat biedt mensen wereldwijd de mogelijkheid om zich te laten horen, om ideeën te verkondigen, zonder schrik te moeten hebben voor vervolging. Dat is een belangrijk principe. Met die extra laag moeten we geen afbreuk doen aan de mogelijkheid anoniem te willen publiceren. Die twee moeten dus naast elkaar kunnen bestaan."

AIVD: digitale dreiging neemt exponentieel toe

'We' zijn ons in Nederland onvoldoende bewust van de continue cyberdreiging waaraan overheden, (kennis) instellingen, bedrijven en burgers bloot staan. 'We' moeten daarom zorgen dat onze verdediging veel beter wordt. Dat is in een notendop de boodschap van Erik Akerboom. Hij stelt dat cybersecurity een 'hoofdzaak van de leiding' moet zijn, ergo: hoog op de bestuurlijke agenda moet staan, juist op het thema digitale weerbaarheid. Akerboom pleit bovendien voor aangepaste wet- en regelgeving die het de AIVD mogelijk maakt sneller te kunnen handelen en nationale belangen beter te beschermen. "De digitale wereld is nu eenmaal fluïde, beweegt snel over grenzen heen."

Akerboom was tussen 1998 en 2003 al directeur Democratische Rechtsorde bij de AIVD. Om maar direct met de deur in huis te vallen: wat is er in die kleine twintig jaar veranderd? Cyberdreiging heeft een enorme vlucht genomen, nietwaar? De AIVD-topman knikt bevestigend: "Het regent incidenten. Er is een permanente stroom aan digitale aanvallen op burgers, op bedrijven, op ministeries, op ambassades. Het is voortdurend zoeken naar wie ons aanvalt. Het is echt een nieuwe wereld waarin we zitten, kijk ook naar de recente ontwikkelingen in Oekraïne. Onze teams zijn daar vanzelfsprekend druk mee bezig. Ontwikkelingen houden we scherp in de gaten en waar nodig acteren we. Het is vooralsnog vooral een fysieke oorlog om grondgebied, maar dat laat onverlet dat zich ook cyberdreigingen kunnen voordoen. Daar zijn we als dienst zeer alert op. Tegelijkertijd vind ik het belangrijk om rust en overzicht te bewaren. Rust is in situaties als deze een goede raadgever en vergeet niet: we hebben als dienst ook te maken met andere langer lopende cyberdreigingen om ons heen. Het is dus van belang om ook daar zicht op te hebben en niet alle aandacht alleen op de situatie rond Oekraïne te vestigen."

Digitale dreiging

De landen van waaruit de meeste digitale dreigingen komen zijn Rusland en China, gevolgd door Noord-Korea en Iran. Rusland is op vele terreinen actief. De AIVD haalde eerder het nieuws met het oprollen van een Russisch spionagenetwerk waarbij twee inlichtingenofficieren non grata werden verklaard. Akerboom vertelt dat het om een groot netwerk ging, toegespitst op technologie en wetenschap. De aanname was dat onderzoek in het netwerk onder betrokkenen zeer waarschijnlijk niet onder de radar zou blijven en dus koos de AIVD er zelf voor om 'in the lead' te zijn en het nieuws naar buiten te brengen. Ook om de Russen duidelijk te maken dat zulke activiteiten hier niet worden getolereerd.
Het is ook geen hogere wiskunde om te stellen dat de aanvaller in het voordeel is, weet Akerboom. "Daarom moeten we zorgen dat onze verdediging beter wordt. We moeten niet met z'n allen in het doel gaan staan, want dan win je ook geen wedstrijd. Maar we moeten écht onze verdediging beter op orde brengen en daarnaast ook heel snel kunnen reageren op dreigingen – en zeker digitale dreigingen – die op ons afkomen. De situatie in Nederland is dat onze digitale infrastructuur wordt misbruikt door andere landen om weer andere landen aan te vallen. Dat is een schending van onze soevereiniteit."
Dat onderzoek richt zich altijd op een viertal vragen: 1. wie is de aanvallende partij? 2. op wie zijn ze gericht? 3. welke methode gebruiken ze? en 4. wat kan eraan gedaan worden? "Wat mij opvalt in vergelijking met twintig jaar geleden is dat die digitale dreiging als een rode draad door alle veiligheidsonderwerpen heen is gaan lopen. Waar vroeger mensen een rol hadden in spioneren, inbreken of angst aanjagen, gebeurt dit tegenwoordig vrijwel allemaal digitaal", aldus Akerboom.
Hij stelt dat digitaal veiligheidsbeleid onderdeel moet worden van de normale bedrijfsvoering. "Je moet als CEO op de hoogte zijn van de risico's die je loopt, wat de belangrijkste parels zijn van de organisatie om te beschermen, dat je weet welke medewerker bij welke informatie kan, dat je je afvraagt waar je data staan en wanneer de laatste update is gedaan."
"Dat is echt geen *rocket science* maar heel basaal. Er is een kans dat je data ergens in de cloud in China staan, of ergens in de VS. Het is belangrijk dat bestuurders zich dat realiseren en maatregelen nemen: niet alleen als onderdeel van de normale bedrijfsvoering om je deuren dicht te doen, maar ook door de digitale deuren dicht te doen."

Economische spionage

Met de interventie bij het Russische spionagenetwerk gaf de AIVD daarom een belangrijk signaal uit: economische spionage is een realiteit. Nederland is een aantrekkelijk doelwit voor statelijke actoren die kennis en technologie willen stelen, stelt Akerboom. "We zien nog te vaak dat bedrijven die hoogtechnologisch zijn, vaak niet zijn ingericht op het beschermen van hun *intellectual property*, en dat raakt hun verdienvermogen. Voor landen die zijn geïnteresseerd in kennis en technologie zijn onze top tien sectoren een *shopping* list. Wij zijn heel goed in halfgeleiders, in de agricultuur, ons land

Erik Akerboom is sinds mei 2020 directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), een Nederlandse geheime dienst die ressorteert onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De AIVD legt zich toe op de binnenlandse veiligheid en verzamelt daarnaast inlichtingen, op civiel gebied, uit het buitenland. Akerboom was eerder Korpschef van de Nationale Politie (maart 2016-april 2020), secretaris-generaal bij het ministerie van Defensie (2012-2016) alsmede Nationaal Coördinator Terrorismebestrijding en Veiligheid (2009-2012) bij het toenmalige ministerie van Veiligheid en Justitie.

"Het is echt een nieuwe wereld waarin we zitten"

is op maritiem gebied toonaangevend... In al die sectoren beschikken wij over hoogwaardige en unieke kennis. China wil de machtigste economie worden en bouwt daar heel gestructureerd aan, via zowel de achter- als de voordeur zullen we maar zeggen. Het afgelopen jaar zijn er een aantal grote incidenten geweest. Op zichzelf niet een 'digitale 9/11' maar wel met een potentiële impact op de stabiliteit van Nederland. We zien dat veel aanvallen niet meer rechtstreeks zijn gericht op bijvoorbeeld energiecentrales maar op de *supply chain*. Het is dus belangrijk dat bedrijven ook op hun toeleveranciers letten. En ook dat softwarebedrijven kritisch naar de kwaliteit van hun eigen software kijken. "

Akerboom geeft aan dat er wat de AIVD betreft snel een slag gemaakt moet worden. In dit verband wordt door onder andere de AIVD ook gepleit voor het aanpassen van de Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv).

"Een onafhankelijke evaluatiecommissie heeft geconstateerd dat de wet voor een belangrijk deel goed werkt, maar voor een substantieel deel niet aansluit bij de praktijk van ons. En die praktijk is vooral: snel kunnen inspelen op iets wat we zien."

Akerboom geeft een voorbeeld: "Als we vaststellen dat een server is misbruikt, dan moet je meteen kunnen terugslaan en uitzoeken wie erachter zit. Daarvoor heb je soms maar een uur de tijd. Dat lukt niet als je allerlei protocollen moet volgen en rapportages moet maken, dat ga je gewoon niet redden. Dat is door die commissie vastgesteld en de Algemene Rekenkamer heeft daarop nog aanvullend onderzoek gedaan en geconcludeerd dat onze slagvaardigheid onder druk staat vanwege die wettelijke beperking. Dus het is echt hoog tijd dat die wet wordt aangepast, liever vandaag dan morgen."

Hebben jullie daarop zelf invloed?

"Onze invloed is aankaarten waar we tegenaan lopen en de wetsvoorstellen te toetsen op uitvoerbaarheid. Dus in die zin zijn we betrokken bij die wet. Hier tekent zich voor een geheime dienst als de onze natuurlijk ook een dilemma af. Want je kunt niet aan iedereen vertellen wat je doet en dus gebeuren er twee dingen: sommige mensen denken 'wat doen die diensten allemaal?' en andere mensen denken 'we hopen dat ze toch wel alles goed controleren'. Die twee gaan tegelijkertijd op. En dus moet je ruimte krijgen, maar ook goed gecontroleerd worden. Wij hebben een belangrijke beschermende taak naar de samenleving, zeker als het gaat om cyberdreiging. En bij die taak kunnen burgers erop rekenen dat wij niet alleen heel goed worden gecontroleerd, maar dat wij ook medewerkers hebben die heel duidelijk weten wat ze doen. We hebben heel goede hackers en die hacken terug als we worden aangevallen. We hebben heel goede analisten; gewetensvolle mensen die echt goed nadenken voordat ze iets doen. Maar ook assertief zijn als het gaat om het beschermen van ons intellectueel eigendom of onze staatsgeheimen."

Grote urgentie

En daarin schuilt zijn grote urgentie, benadrukt Akerboom: "De digitale dreiging neemt exponentieel toe. De wet is in die zin gedateerd dat ze uitgaat van statische momenten. Dus we schrijven een rapport en dan krijgen we toestemming. Maar de cyberwereld is iteratief. Een aanvaller hopt van server naar server om steeds zijn sporen uit te wissen. Dat tempo en die dynamiek volgen, daar moet de wetswijziging op gericht zijn. Ik ben niet voor minder toezicht, maar voor dynamischer toezicht, noem het '*real-time*'. Dat is in het belang van de Nederlandse veiligheid. Ik leg verantwoording af voor wat we kunnen doen en moeten doen. Dat is ook het wezen van een veiligheidsdienst in deze tijd. Die heeft niet alleen te maken met terrorisme en met spionage en met sabotage, maar heeft ook te maken met cyberaanvallen die onze economie, onze veiligheid en onze privacy permanent onder druk zetten. En het is aan ons dat we doorhebben wie dat doet en dat we ook de juiste instanties inlichten, op basis waarvan zij kunnen handelen. Ik pleit voor een breed front; dus niet alleen de AIVD, de MIVD en de NCTV, maar dat juist ook burgers, bedrijven, overheden, kennisinstellingen, dat wij allemaal een stap maken naar verhoogde alertheid en weerbaarheid en die nieuwe *mindset*. Ik zei al: het is echt een nieuwe wereld waarin we zitten."

Het is de taak van de AIVD om de Nederlandse overheid van onafhankelijke informatie te voorzien over internationale politieke ontwikkelingen en mogelijke intenties van andere naties. "Waarvoor we beducht zijn, is dat buitenlandse diensten zich bemoeien met onze politieke situatie door informatie op een bepaalde manier in te brengen of verkiezingen te beïnvloeden", zegt Akerboom. Hij geeft aan dat op dit terrein intensief wordt samengewerkt met de MIVD. "Vaak zit je in een grijze zone. Dan is er geen sprake van oorlog of vrede, maar een soort tussengebied waarin landen vijandelijke dingen aan het doen zijn en daar moet je dus ook samen op reageren. Dan brengen we mensen en middelen bij elkaar. We kunnen vaststellen dat we op een aantal terreinen écht verbeteringen en slagkracht ontwikkelen."

Onder water

Waar in de fysieke wereld vijandelijke stellingname over het algemeen goed traceerbaar is ("Je ziet bijvoorbeeld dat er wapens worden gekocht en er bewegingen of incidenten langs de grens plaatsvinden") gebeuren in het digitale domein "veel zaken onder water en zijn dus niet publiek zichtbaar. Naast spioneren willen vijandelijke staten ook malware plaatsen in vitale infrastructuur, zoals luchthavens en energiecentrales. Dat geldt ook voor bedrijven die economisch vitaal zijn. Elektriciteit, water, betaalverkeer, de bevoorrading van supermarkten, het is allemaal verweven in digitale processen. Niet altijd om direct te saboteren, maar vooral om een sterke positie te creëren, een onderhandelingsvoordeel."

"Wij zijn primair ingericht op het voorkomen van aanvallen. Wij zitten in de wereld van *leads*, zoals dat heet, van tips en signalen die we onderzoeken. Dat gebeurt op basis van vermoedens en aanwijzingen. Daarvoor hebben wij de inlichtingenmix, die ons bij wet is gegeven. We willen graag meer snelheid en slagkracht ontwikkelen om die inlichtingenmix ook volledig te kunnen uitnutten. Sporen van mogelijke aanvallers bevinden zich op verschillende media. Soms zitten die op social media, soms op forums, soms op de kabel, soms in de satellietwereld en soms ook 'gewoon' bij mensen die van bepaalde dingen weet hebben. Het is niet één ding. Het slim combineren van die bronnen dat is het echte inlichtingenwerk."

Aan dat intensieve speurwerk zou Akerboom via wetsaanpassing graag meer assertiviteit toevoegen. "Ik zie, ook in deze tijd, de grote waarde van inlichtingen. Soms kunnen we een burger of bedrijf beschermen, soms spionage of ICT sabotage voorkomen, soms kunnen we levens redden. Dat maakt het inlichtingenwerk zo bijzonder."

MIVD: veiligheid begint met een goede inlichtingenpositie

De oorlog in Oekraïne onderstreept het belang van de werkzaamheden van de MIVD: zicht houden op dreigingen tegen Nederland, de krijgsmacht en bondgenoten. Het is belangrijker dan ooit om met actuele en betrouwbare inlichtingen nationale besluitvorming en uitgezonden eenheden van de krijgsmacht te ondersteunen en in te grijpen als dat nodig is, door vijandelijke operaties tegen Nederlandse belangen te verstoren.

"Met de Russische inval in Oekraïne op 24 februari 2022 is de wereld ingrijpend veranderd. We zien vlakbij, in Europa, pal aan de grenzen van het NAVO-grondgebied, grootschalige conventionele oorlogvoering met grote hoeveelheden tanks, pantser voertuigen, granaten en kruisvluchtwapens. We zien een verhoging in het aantal cyberaanvallen op Oekraïne. En we zien desinformatie," aldus generaal Swillens.
Hij vervolgt: "De Russische Federatie investeert volop in militaire wapensystemen als onderdeel van de jaren geleden ingezette modernisering van hun krijgsmacht. De meest in het oog springende ontwikkelingen binnen de militaire techniek en wapensystemen vinden plaats op het gebied van hypersone wapens en ballistische raketten, onderzeeboten, nucleaire wapens, antisatellietwapens en modernisering van tanks en pantservoertuigen. Een deel van deze wapensystemen dient onder meer om anderen de toegang tot gebieden te ontzeggen. De inval in Oekraïne laat zien dat je rekening moet houden met onvoorstelbare scenario's. Dat is ook echt een onderdeel van inlichtingenwerk. Net als dat je nooit naïef mag zijn waar het op je eigen veiligheid aankomt."

De MIVD kijkt niet alleen naar militaire conflicten, technologische ontwikkelingen en de opbouw van buitenlandse krijgsmachten, maar is ook 24/7 bezig met het beschermen van wat digitaal belangrijk is voor de veiligheid van Nederland en onze bondgenoten. "Dit doen we in nauwe samenwerking met de AIVD. Maar ook werken we samen met andere veiligheidspartners zoals het Nationaal Cyber Security Centrum en het Defensie Cyber Security Centrum."
De capaciteiten bij de tegenstanders nemen toe, worden geavanceerder en tegenstanders worden ook steeds beter in het verhullen van hun activiteiten, constateert de directeur van de MIVD. "Als geopolitieke spanningen oplopen, en militaire eenheden worden ontplooid, wordt ook cybercapaciteit ingezet. Dit hebben we al eerder gezien, bij de grensconflicten in Georgië en nu ook in Oekraïne. In de offensieve cyberprogramma's wordt dan gerichter digitaal gespioneerd, er wordt desinformatie en propaganda verspreid om de publieke opinie te beïnvloeden en soms worden ook destructievere middelen ingezet. Hierdoor kunnen digitale netwerken onbruikbaar raken. Om hier als MIVD en ook als AIVD op in te kunnen spelen, is snelheid van handelen essentieel."

Vergaande samenwerking

De oorlog in Oekraïne onderstreept het belang van internationale samenwerking. Maar ook dichter bij huis is samenwerking van groot belang. Samenwerking tussen overheid, inlichtingendiensten, kennisinstituten en bedrijfsleven zijn een voorwaarde om Nederland veilig te houden in een wereld waarin vijandige cyberactiviteit snel evolueert, stelt Swillens. "Het gaat niet alleen om veiligheid in het traditionele domein maar ook om kennisveiligheid en economische veiligheid. Daarover moet je in gezamenlijkheid nadenken. Nederland is een kenniseconomie. Kennis delen is de kern van wetenschap en daar ben ik voor, maar je moet wel je maatregelen nemen tegen partijen die zich die kennis oneigenlijk willen toe-eigenen."

Samenwerking tussen de MIVD en AIVD is een gegeven. "Waar we op hebben ingezet is: hoe zorgen we dat we als diensten op het gebied van informatiedeling het optimale eruit halen? We hebben niet de luxe om allerlei 'tuinhekdiscussies' te voeren. Er zijn dwarsverbanden en als je informatie op een verstandige manier met elkaar deelt, dan levert dat veel meer inzicht op. Wat je wilt bereiken is dat de juiste informatie op het juiste tijdstip bij de juiste mensen met het juiste advies terechtkomt, zodat goede besluiten kunnen worden genomen", aldus Swillens.
"Het is prettig dat we één wet hebben waar we als beide diensten onder vallen. We hebben één toezichtregime, dus de uniformiteit van het indienen van bijzondere bevoegdheden loopt voor de AIVD en de MIVD via hetzelfde traject. De geïntegreerde aanwijzing is één richtinggevend document voor beide diensten. Wij hebben één opdracht; ook heel belangrijk, er zijn heel weinig landen die dit hebben. Wij mogen alleen bijzondere

Generaal-majoor Jan Swillens is sinds juni 2019 directeur van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). De taken van de MIVD zijn vastgelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en de Wet veiligheidsonderzoeken (Wvo). Swillens is sinds 1985 werkzaam bij het ministerie van Defensie en vervulde eerder de functie van commandant van het Korps Commandotroepen.

"Het is vaak heel lastig om vast te stellen wie achter een aanval zit"

bevoegdheden inzetten als dit is terug te voeren op een onderzoeksopdracht zoals geformuleerd in de geïntegreerde aanwijzing."

Een gezamenlijk onderdeel van de AIVD en de MIVD is de Joint Sigint Cyber Unit (JSCU). Deze eenheid is in 2014 operationeel geworden en richt zich op het afluisteren van radio- en satellietverkeer plus het verkrijgen van inlichtingen via cyberoperaties. "Dat is echt een eenheid die zich in de afgelopen zeven jaar ontzettend goed heeft ontwikkeld. Alles wat met ethercommunicatie te maken heeft, kunnen we daar binnenhalen. Dat combineren we met cyberinlichtingen en die combinatie is buitengewoon waardevol. Daarin zijn we in de wereld vrij uniek, dat dit niet een aparte entiteit is, maar in allebei de inlichtingen- en veiligheidsdiensten is geïntegreerd."

Grenzen vervagen

Veiligheid begint met een goede inlichtingenpositie, vindt Swillens. "Als je wordt aangevallen in het cyberdomein wil je natuurlijk weten door wie. Het is vaak heel lastig om vast te stellen wie achter een aanval zit: is het een crimineel of een hobbyist, of een statelijke actor? En dat is de inlichtingenpositie die je wil hebben: dat je ziet wat de identiteit van de aanvaller is. Als je een goede positie hebt, dan kun je ook je beveiliging daarop inrichten. Bij het vinden van oplossingen moeten we nauw samenwerken. De grenzen tussen publiek en privaat, tussen bedrijfsleven, kennisinstellingen en overheid, tussen criminelen en niet criminelen, tussen staten en niet staten, vervagen."
Swillens stelt vast dat binnen het cyberdomein, zeker waar het landen als Rusland en China betreft, sprake is van een offensieve cyberstrategie gericht op Nederland. Hij plaatst om die reden een waarschuwing bij bedrijven die, bijvoorbeeld in China, louter exportkansen zien. Ze zijn kwetsbaar, het besef dat er voortdurend aanvallen worden geplaatst lijkt nog niet alom aanwezig.

Het door de veiligheidsorganisaties AIVD, MIVD en NCTV gezamenlijk gepubliceerde rapport 'Dreigingsbeeld statelijke actoren', over buitenlandse spionage in Nederland, werd door de media amper opgepikt. Organisaties die inmiddels een aanval met *ransomware* hebben doorstaan hoef je niets meer te vertellen, zegt Swillens, maar dat jezelf wapenen tegen cybercrime goed functionerende inlichtingen- en veiligheidsdiensten vereist, dat besef is nog niet overal doorgedrongen. "Het beeld dat mensen hebben dat inlichtingendiensten bezig zijn met persoonsgegevens van willekeurige Nederlanders is hardnekkig. Maar daar zijn wij niet in geïnteresseerd. Veel internetbedrijven zoals Bol.com of Zalando weten meer over de mensen dan wij."

Dynamiek van de praktijk

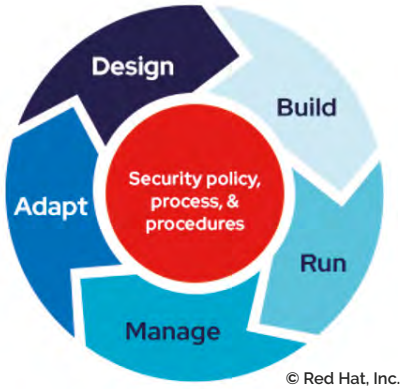
Evenals de AIVD pleit de MIVD voor – snelle - aanpassing van de bestaande Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv) om die beter te laten aansluiten op de operationele praktijk. "Optreden in dat cyberdomein gaat echt met een hoge snelheid gepaard. De tegenstander verhult zich. Die probeert een mistgordijn op te trekken en gaat razendsnel de hele wereld over, zoekt ergens een internet opgang en wisselt telkens van serviceprovider. De dynamiek van de praktijk, ergo: het snel kunnen volgen ván en het zicht houden óp een tegenstander in het cyberdomein, verhoudt zich heel lastig met een gedetailleerde toets aan de voorkant. Heel vaak weet je van tevoren niet hoe je precies gaat bewegen door dat domein. Wat we vaststellen is dat daar een meer effectieve waarborgsystematiek bij past. Dat kan door het toezicht meer te concentreren op de uitvoering en daar de *checks and balances* in te bouwen. En dat is eigenlijk waar we naar op zoek zijn: hoe kunnen we dat nu vastleggen in de wet op een manier dat dat werkbaar is voor ons en dat er geen waarborgen worden afgebouwd?"

"We leven – gelukkig - in een land waarin de diensten volledig onder toezicht staan en we alles binnen de wettelijke kaders doen, maar aan de andere kant stellen we vast dat we leven in een wereld die vereist dat we goed functionerende diensten hebben. Nederland is een kenniseconomie. Als je denkt aan zaken als hoogwaardige technologie, kwantumcomputing, nanotechnologie, intellectual property..., dat maakt ons interessant.
"Wat mij is opgevallen in de tijd dat ik deze functie bekleed, is dat veiligheid niet meer alleen het ministerie van Defensie en het ministerie van Justitie en Veiligheid raakt. Inmiddels zitten we regelmatig ook met Economische Zaken, Infrastructuur en Waterstaat en Onderwijs om tafel. Zij melden zich steeds vaker met vragen over inlichtingen en veiligheid. Wij hebben al eerder uitgesproken dat samenwerking tussen overheid, bedrijfsleven, kennisinstituten en inlichtingendiensten belangrijk is om Nederland veilig te houden. Daarin moeten we de komende jaren stappen zetten en dan met name op het gebied van kennisveiligheid en economische veiligheid."

Red Hat biedt integrale cybersecurity-aanpak voor hybride cloud

Hoe goed is uw hybride cloudomgeving beveiligd? Voldoet die aan de BIO-richtlijnen en kan hij eenvoudig worden geaudit? En is de infrastructuur in staat zichzelf volautomatisch te herstellen bij calamiteiten?

Red Hat levert een volledige enterprise open source technologie-stack voor het veilig implementeren en beheren van applicaties in een gedistribueerde hybride cloud. Daarbij kan Red Hat helpen om security te integreren in alle relevante bedrijfsonderdelen, de mensen, de techniek en de processen.

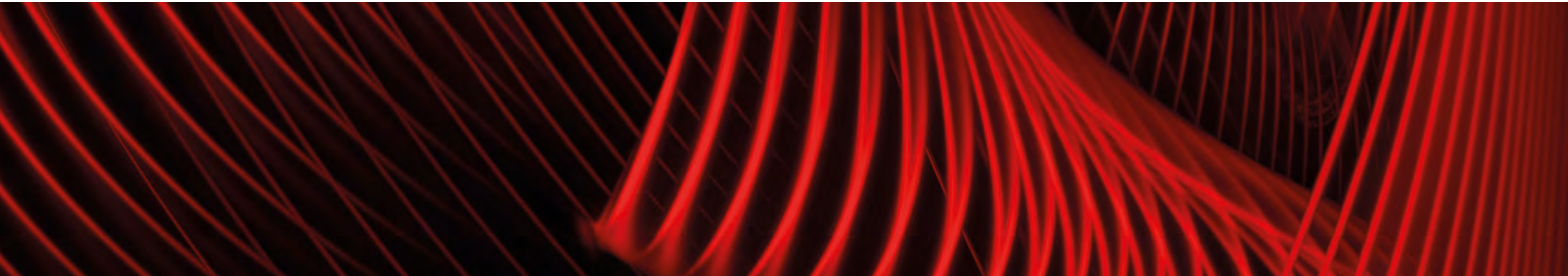


Beveiliging is daardoor geborgd in de volledige infrastructuur en gedurende de gehele levenscyclus van systemen en applicaties.

Zero Trust Networking heeft daarbij de voorkeur boven traditionele, op locatie gebaseerde beveiligingsstrategieën. Door de focus te leggen op microsegmentatie en een continue autorisatie tussen mensen en systemen en tussen systemen onderling is een hybride cloudomgeving altijd optimaal beveiligd.

Meer weten? Download hier het e-book: https://red.ht/3JLWLWW

Red Hat



NCSC: begrijpen, verbinden, voorkomen

Hans de Vries ontvangt GOV magazine daags nadat 'zijn' NCSC een waarschuwing heeft afgegeven over kwetsbaarheden in software (Log4j) die veel gebruikt wordt in webapplicaties en andere systemen. Dit deed een alarmbel afgaan bij talrijke organisaties in allerlei sectoren in Nederland. Een aantal zag zich zelfs genoodzaakt uit voorzorg ICT-systemen af te koppelen om een *ransomware* aanval te voorkomen. Het was, onbedoeld, een lakmoesproef voor het NCSC in de rol van nationaal Computer Emergency Response Team (CERT).

Want de mogelijke impact van de geconstateerde kwetsbaarheden was weliswaar nog niet te overzien maar aannemelijk groot en dus schakelden De Vries cum suis tien op de schaal van crisismanagement. Er was overleg met leveranciers van cybersecurity producten en -diensten, circa 80 in totaal, en vervolgens een sessie met vertegenwoordigers ("270 man aan de lijn") van organisaties in de vitale sectoren en het bedrijfsleven. "Dat is de slagkracht die je als NCSC moet kunnen tonen en dat is goed gelukt", merkt De Vries op. "De maatregel is op zo'n moment nog van een andere orde, maar je maakt een koppeling met organisaties om iedereen wakker te maken: dit is een ernstig vraagstuk!"

"We hebben de afgelopen jaren een trits van vraagstukken gehad", zegt De Vries, refererend aan eerdere incidenten rond Citrix, MS Exchange en SolarWinds. "Maar vervelend aan Log4j is dat het gaat om een bouwsteentje in heel veel software. Dat kan veel verschillende problemen veroorzaken en er is niet één eenvoudige manier om het te detecteren, repareren of uit te schakelen. Deze kwetsbaarheid zit al zeven jaar in die software alleen komt het nu pas boven water. Programmatuur zonder programmeerfouten bestaat niet, dus het is een *accident about to happen* en dan is het de vraag wanneer het op tafel komt en hersteld kan worden."
De Vries legt uit dat vaker kwetsbaarheden worden geconstateerd en dat daarvoor voor Nederland de leidraad 'Coordinated Vulnerability Disclosure' is opgesteld. Het doel hiervan is om kennis over kwetsbaarheden in ICT-systemen te delen zodat deze verholpen kunnen worden vóórdat deze actief misbruikt kunnen worden door derden. "Het NCSC speelt daar vaak een rol in om op die manier foutjes hersteld te krijgen, maar om in dit specifieke geval de patch in één keer ter tafel te krijgen..., een ingewikkeld vraagstuk."

Levensader

Het Log4j incident toont weer aan hoe diep doorgedrongen technologie is in onze dagelijkse omgeving, stelt De Vries. "Digitalisering is een levensader van de Nederlandse samenleving. De verwevenheid van technologie in de basisinfrastructuur voor dienstverlening is zo massaal dat er eigenlijk geen weg terug is. De bewustwording daarvan is nog niet overal ingezakt."
En die digitale infrastructuur is van levensbelang: voor het betalingsverkeer, schoon water uit de kraan en om de voeten droog te houden. De rol van de NCSC daarin: het identificeren en duiden van risico's en trends en het delen van informatie en kennis.
'Als overheidsorganisatie zijn we de verbindende schakel in een netwerk van nationale en internationale partners', leest het profiel op de website van het NCSC. Er wordt gewerkt mét en vóór de Rijksoverheid, organisaties in de vitale infrastructuur en een groeiend Landelijk Dekkend Stelsel (LDS). Dit laatste is een structuur waarin het NCSC en het Digital Trust Center (DTC) samenwerken met publieke- en private organisaties om informatie en kennis uit te wisselen. Het doel hiervan is digitale ontwrichting te voorkomen en Nederland 'cyber weerbaarder' te maken. Brancheorganisatie Cyberveilig Nederland, opgericht om de jonge sector van cybersecurity bedrijven een stem te geven, is ook belangrijk onderdeel van het LDS.

De Vries: "Het NCSC is opgericht om Nederland cyberweerbaarder te maken, maar dat wil niet zeggen dat we dat alleen kunnen doen." Dat is ook inherent aan het poldermodel, vindt hij, "de koppeling die we hebben met de verschillende sectoren werkt uitstekend. Het NCSC is er klaar voor om ook in die nationale setting een operationeel coördinerende rol te gaan vervullen, zoals we nu laten zien. De samenwerking in Nederland tussen de inlichtingen- en veiligheidsdiensten, het Openbaar Ministerie, Nationale Politie, de NCTV, die is prima. Het kan altijd beter, natuurlijk, maar het is gewoon goed."

Hans de Vries is sinds 1 januari 2019 directeur van het Nationaal Cyber Security Centrum (NCSC) dat ressorteert onder het ministerie van Justitie en Veiligheid. Eerder was De Vries al plaatsvervangend directeur Cyber Security bij de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Het NCSC is het nationaal informatieknooppunt voor de Rijksoverheid en organisaties uit de vitale sectoren, die bij wet zijn verplicht om ernstige digitale veiligheidsincidenten te melden. Het NCSC fungeert ook als nationaal contactpunt namens Nederland voor de EU-lidstaten.

"Cybersecurity is een internationaal vraagstuk"

Waarbij aangetekend: "Cybersecurity is een internationaal vraagstuk, dus als je het hebt over Nederlandse grenzen beschermen..., die zijn er eigenlijk niet. De Nederlandse Gasunie doet de dienstverlening in Duitsland voor de energie en in Nederland zijn wij enorm afhankelijk van bijvoorbeeld Microsoft software voor de Cloud. Het is zo verweven over de landsgrenzen heen, een hek eromheen zetten heeft geen zin. Dat vraagt dus internationale samenwerking en het vraagt ook coördinatie om dit vraagstuk op te pakken. Ook daarvoor is het NCSC opgericht."

Autoriteit

Daarbij past ook het beeld van 'autoriteit' waar het gaat om waarheidsvinding. "Je hoort zoveel in de wandelgangen, maar wat is nu waar en niet waar? Wat is er werkelijk aan de hand? Wij proberen dat te achterhalen en we doen dat ook in samenwerking met alle cybersecurity bedrijven in Nederland. Wij coördineren dat proces en dat verloopt eigenlijk heel soepel omdat iedereen dit ook wil. Die bedrijven zeggen allemaal: 'Lees het bericht en volg het NCSC'. Dat doen ze omdat ze het belangrijk vinden dat wij in gezamenlijkheid proberen 'de waarheid' te vertellen. Dat doen we niet alleen in Nederland, we hebben daarover ook binnen Europa afspraken gemaakt. We krijgen ook informatie uit België, Duitsland en andere landen en die delen wij weer. Uiteindelijk probeer je één waarheid te creëren. Zonder dat wordt het lastig opereren."

Dat is al moeilijk genoeg?

"Ja. Maar wat wij doen, maakt in ieder geval inzichtelijk waar het probleem zit en ook waar het probleem niet zit. Je hoort zoveel *hear say*, is deze applicatie gevaarlijk ja of nee? De een zegt 'ja' de ander zegt 'nee', maar wat is het nou echt? Wij proberen daar meer inzicht in te geven, maar we sturen ook oplossingsrichtingen de wereld in; welke methode van detectie kun je gebruiken, welke IP-nummers zijn kwetsbaar of welke moet je juist blokkeren? Die operationele coördinerende rol, daar ben ik blij mee. We tonen aan dat we dat ook kunnen."

"We hebben geen alziend oog in Nederland dat ziet waar de kwetsbaarheid zit. Er is een nationaal detectie netwerk maar dat is op dit moment feitelijk beperkt tot de Rijksoverheid en organisaties in de vitale sectoren. We hebben nu geen bevoegdheden om daarbuiten zelf te monitoren, we zijn afhankelijk van bedrijven die ons – vrijwillig – informeren. Op basis daarvan kunnen wij onderzoek doen, eventueel in gezamenlijkheid met de politie als er aangifte is gedaan."

Focus

De focus van het NCSC in drie woorden: begrijpen, verbinden en voorkomen. "Doordat wij begrijpen wat het vraagstuk is, en de juiste partijen aan elkaar verbinden met de juiste informatie, kunnen we helpen problemen te voorkomen", zegt De Vries. Hij voegt eraan toe, het laatste incident in het achterhoofd: "Wij hebben niet de bevoegdheid om in Nederland af te dwingen dat alle organisaties patches draaien. Zo werkt dat niet in ons land. Waar wij wel voor zijn, is ervoor zorgen dat de juiste informatie wordt aangeboden met de juiste prioritering, zodat bedrijven hun eigen verantwoordelijkheid beter kunnen dragen. Dat verhoogt de digitale weerbaarheid van Nederland."
Informatie vergaren, daardoor inzicht krijgen, en in actie komen, dat is kort samengevat de *modus operandi* van het NCSC. "Mijn basishouding is altijd: het meest efficiënte proces verzorgen zodat de snelheid is gewaarborgd. Snelheid – tijd – is cruciaal. Wachten is geen optie", zegt De Vries. Behalve het Digital Trust Center is ook Cyberveilig Nederland een belangrijke partner hierin, "want die zitten letterlijk aan de knoppen van de infrastructuur. Die verantwoordelijkheid hebben wij niet, advies geven over hoe zaken te signaleren of te detecteren en te verbeteren, dat is wat wij doen en kunnen. De verbetering of de update aanbrengen, dat is aan de IT-leverancier of aan de organisatie zelf, wij kunnen alleen advies geven."

De Cyber Security Raad (CSR) zegt in haar adviesrapport 'Integrale aanpak cyberweerbaarheid' aan het kabinet dat er 833 miljoen euro nodig is om cybersecurity in Nederland écht naar een hoger niveau te tillen. En ook dat de regie steviger kan.
"Ik vind het een afgewogen rapport en vind ook goed dat er een aantal fases zijn gedefinieerd, denk aan onderzoek en onderwijs. Het is natuurlijk goed dat wij proberen problemen op te lossen, maar kinderen leren om met deze IT-vraagstukken om te gaan is heel belangrijk. Ook belangrijk is om leveranciers te leren om *security by design* toe te passen bij productontwikkeling. Dus steek daar tijd en energie in, doe onderzoek naar hoe je dat het beste kunt organiseren."
De conclusie van de CSR dat de regie steviger kan, daarin herkent De Vries zich. Hoe meer er in gezamenlijkheid wordt opgetreden, hoe beter het is voor Nederland, vindt hij. "Met elkaar kunnen we ervoor zorgen dat écht begrepen wordt dat digitalisering je levensader is."
Dat de nieuwe Tweede Kamer een vaste commissie voor Digitale Zaken heeft geïnstalleerd noemt hij een belangrijke verbetering in de controle op cybersecurity vanuit het parlement. "Ik ben ook blij dat in het advies nadrukkelijk staat dat het NCSC versterkt moet worden. Dat deel ik, want je moet wel een goede uitgangspositie hebben – in mensen, in middelen - om die taken en die rol te kunnen vervullen. Er is echt wat voor nodig om dat op een constant niveau georganiseerd te krijgen, maar als we daarin slagen dan gaat Nederland daar goed bij varen."

Nabericht

De wereld is de laatste maanden sterk aan het veranderen door de Oekraïne-crisis. Ook op het digitale vlak heeft dit grote impact. Het NCSC heeft de afgelopen periode, vanuit haar taak en rol, de situatie nauwgezet in de gaten gehouden en overheid en bedrijfsleven op de hoogte gehouden van de stand van zaken.

Cyberdiplomatie voor regels en normen

Tussen periodes van lockdown door toog Nathalie Jaarsma december vorig jaar naar New York. Als lid van een nieuwe werkgroep van de Verenigde Naties sprak zij met collegae van over de hele wereld over normen en regels in cyberspace. Die zijn nodig, want wat mag je van elkaar verwachten en hoe spreek je elkaar aan als staten in geval van dreiging? "Dan is de vraag: welke regels gelden eigenlijk?"

Internationaal cyberbeleid staat al langer op de agenda van BZ. Het is mede vormgegeven door bijvoorbeeld een affaire als die van DigiNotar[1] in 2011 en het WRR-rapport 94 'De publieke kern van het internet. Naar een buitenlands internetbeleid' van 2015. Jaarsma: "Ik leidde in die periode het team veiligheid- en defensiebeleid binnen de Directie Veiligheidsbeleid en dat was ook de tijd dat 'cyber' als thema begon te spelen binnen de Verenigde Naties (VN), de NAVO en de Organisatie voor Veiligheid en Samenwerking in Europa (OVSE). De conclusie van het WRR-rapport was dat als de backbone van het internet in Nederland geraakt zou worden, dat dan de rapen gaar zouden zijn. De vraag die zich aandiende: moeten we ons daar niet beter op gaan equiperen, niet alleen iets doen aan onze eigen verdediging, maar ook een meer actieve rol nemen in het internationale domein?"

BZ zette daartoe een cybertaskforce op die het initiatief nam voor een internationale conferentie, de Global Conference on Cyberspace (GCCS). De toenmalige minister Uri Rosenthal was daar namens ons land als 'special envoy cyber' bij betrokken. Die conferentie resulteerde in een tweetal nieuwe initiatieven: het Global Forum on Cyber Expertise (GFCE) en de Global Commission on the Stability of Cyberspace (GCSC).
Focus van het GFCE ligt bij capaciteitsopbouw. "Want Nederland en andere gedigitaliseerde landen kunnen hun zaken wel op orde hebben, maar hoe gaat het in andere landen qua weerbaarheid en qua rechtsgang? De wereld draait door en ook die andere landen moeten mee in de vaart der volkeren van cybersecurity. Het GFCE is een soort marktplaats waar vraag en aanbod voor cyberassistentie bij elkaar komt. Dat kan zijn, traditioneel, tussen ontwikkelingslanden en Westerse landen, maar het kan ook zijn kennis uitwisselen op basis van een gelijkwaardig niveau van digitalisering."
De GCSC is in het leven geroepen, legt Jaarsma uit, "rond de vraag welke normen we met elkaar moeten afspreken in cyberspace. Daarover was al een discussie gaande binnen de VN, maar die had nog meer diepgang nodig. Wij wilden ons daar ook beter op positioneren en zagen het belang van een groep multi stakeholder actoren - het internet is uiteindelijk niet iets van overheden - die hierover zouden gaan nadenken."

Internationaal recht

Dat normatieve kader behoort, evenals de capaciteitsopbouw en de diplomatieke respons, tot het primaire aandachtsveld van Jaarsma. Over het normatieve kader: "Wij zien dat er staten zijn die offensieve cybercapaciteit hebben opgebouwd en die inzetten op een manier die bedreigend is voor internationale vrede en veiligheid. Dan is de vraag: welke regels gelden eigenlijk? Binnen de VN is een aantal trajecten gestart die inmiddels ook hebben geleid tot consensusafpraken over verantwoord statelijk gedrag in het digitale domein. Kort gezegd komt het erop neer dat bestaand internationaal recht in z'n geheel toepasbaar is in cyberspace. Daarnaast gelden er op dit moment elf gedragsnormen, weliswaar niet juridisch bindend, maar het betekent wel dat het normen zijn. Sommigen noemen dat vrijwillige normen en ja: zo kun je ze noemen, maar ze zijn niet vrijblijvend."

De inspanningen van de VN zijn erop gericht om "verkeersregels in cyber" op te stellen voor overheden, aldus Jaarsma. Dat was belegd bij een tweetal werkgroepen: de Group of Governmental Experts (GGE) en de Open Ended Working Group (OEWG). Vervolgens heeft de Algemene Vergadering van de Verenigde Naties Staten bij consensus opgeroepen om zich te houden aan de consensusrapporten van deze werkgroepen. Recent is een nieuwe OEWG gestart waar Jaarsma zelf deel van is. "Afgelopen december was ik in New York voor de eerste sessie van die werkgroep die voor vijf jaar is geïnstalleerd. Wat ons betreft moet het nu veel meer gaan over implementatie en ook: hoe spreek je elkaar aan als staten? Daarnaast is de uitdaging hoe we ervoor zorgen dat mensenrechten goed zijn geborgd. Want als gaat over internationaal recht in de breedte, dan staan mensenrechten erg onder druk. Hoe krijgen we dat beter verankerd? De implementatie van afspraken houdt natuurlijk verband met de diplomatieke respons, want op het moment dat je ziet dat staten zich niet houden aan de regels die je hebt afgesproken, dan moet je ze gaan aanspreken."
Daarin is ook een grote rol voor Jaarsma weggelegd, "om dat soort dialogen aan te gaan", zoals ze het zelf formuleert. Je

Nathalie Jaarsma bekleedt sinds september 2020 de functie van speciaal gezant cyber en veiligheid bij het ministerie van Buitenlandse Zaken (BZ). In die rol beijvert Jaarsma zich via diplomatieke weg voor een vrij, open en veilig cyberspace waarbij internationaal recht is gewaarborgd. Zij is in 2001 in dienst getreden bij voornoemd ministerie en was onder meer werkzaam als hoofd veiligheid- en defensiebeleid (2012-2016) en ambassadeur te Nicosia, Cyprus (2016-2020).

"Het internet is niet iets van overheden"

bent diplomaat of niet natuurlijk. Die gesprekken, licht ze toe, verlopen binnen de context van de afspraken over 'verantwoord statelijk gedrag' en de signalering van gedrag dat niet als zodanig wordt beschouwd, resulterend in de vraag of daarop door het betreffende land actie kan worden genomen. Jaarsma geeft een voorbeeld: "Er is gewoon een verplichting in internationaal recht, het *due diligence* principe, en die is ook vastgelegd in een niet-bindende norm. Die verplichting zegt dat op het moment dat een aanval vanuit een land effect heeft op een ander land, dan moet het land waar die aanval vandaan komt - en die overheid weet ervan – binnen de kaders van zijn nationale wetgeving al het mogelijke doen om die aanval te stoppen. Dat geldt ook voor Nederland. Dus de internationale afspraken over verantwoord statelijk gedrag is het kader van de diplomatieke respons en daarover hebben we ook in de EU afspraken gemaakt. Bijvoorbeeld over wat voor soort tools we kunnen inzetten als landen die afspraken schenden, met sancties als ultimo."

Diplomatieke responsgroep

Jaarsma spreekt in dit verband van een samenspel met de inlichtingen- en veiligheidsdiensten. "Voor de analyse – wat is er nu precies gebeurd en wie zit erachter, en waarom? – daarvoor heb je die diensten nodig. Je hebt je informatie uit het Intel-domein maar ook uit forensisch onderzoek, dat komt uit verschillende bronnen en dat moet ergens worden samengebracht. We hebben een diplomatieke responsgroep opgezet. Dat is een interdepartementale groep bestaande uit de verschillende spelers, dus zowel de diensten als de NCTV, Nationale Politie, Defensie en Algemene Zaken. Alle relevante spelers zitten daar om tafel om in eerste instantie de vraag te beantwoorden: wat is hier nu precies aan de hand? En vervolgens de vraag te beantwoorden: moeten wij hier diplomatieke actie op ondernemen en zo ja: hoe dan? Want je wilt effectief zijn, uiteindelijk is het doel om die foute gedragingen van staten te keren. Dan heb je dus ook te maken met verschillende soorten staten die gevoelig zijn voor verschillende soorten interventies."

Dan refereert u aan de 'usual suspects' te weten Rusland, China, Noord-Korea en Iran?
"Ik kan hier natuurlijk geen inlichtingen zitten delen, maar wat er in de jaarverslagen van de diensten staat neem ik ook gewoon als uitgangspunt."

Hoe verloopt 'grosso modo' die dialoog?
"Dat is een goede. Dan bedoel je waarschijnlijk met dit soort staten, niet met Duitsland?"

Inderdaad. Neem het oprollen van een Russisch spionagenetwerk door de AIVD waarbij twee inlichtingenofficieren ons land werden uitgezet.
"Ik was daar niet bij betrokken, ik was nog niet in functie toen. Wat er sowieso gebeurt op het moment dat je acties overweegt richting een ander land, of het nu gaat om een goed gesprek, het uitzetten van diplomaten of het opleggen van sancties, je gaat als overheid altijd te rade bij je experts die gaan over het betreffende land. Dus in het voorbeeld van Rusland: dan hebben we contact met onze landendeskundigen en met de post in Moskou en kijken we naar wat de bredere dossiers zijn die spelen. Er zijn hier mensen de hele dag bezig met Rusland, die hebben al die dossiers op hun vizier. Voor diplomatieke respons in reactie op onverantwoord statelijk gedrag in cyber nemen we het normatief kader als uitgangspunt; we bezien de impact op Nederland of op bondgenoten, hoe zeker we zijn over de schuldvraag en wat de beste manier is om een specifiek land aan te spreken cq hun gedrag te beïnvloeden. Die afwegingen worden heel zorgvuldig en in samenhang gemaakt."
"Om op de eerste vraag terug te komen: hoe dat soort cyberdialogen gaan, dat is wisselend. Een dialoog heeft vaak een heleboel verschillende onderwerpen in zich. We hebben recent een interdepartementale dialoog gehad met Rusland, waarbij verschillende delen van de Rijksoverheid aan tafel zaten en ook van de Russische overheid. Dan gaat het over een breed pallet aan onderwerpen, waaraan je ook recht wilt doen. Dat kan gaan over een bepaalde samenwerking die er is tot worstelingen met hoe je moet omgaan met kunstmatige intelligentie en hoe men daarover denkt. Met wat voor wetgeving zijn wij bezig, en met wat voor wetgeving zijn zij bezig? Daar speelt ook een beetje subtiele beïnvloeding bij, want je bent je eigen overwegingen aan het ventileren waarvan zij ook kunnen denken: daar kunnen we wellicht iets mee. Net zoals ze zouden kunnen denken dat ze ons ergens een hak mee kunnen zetten."
Dit soort dialogen is vaak ook het platform om cyberdreigingen te bespreken, zegt Jaarsma. "Je praat over wat je ziet gebeuren en kunt dat dan ook adresseren. 'We zien dat dit of dat bij u vandaan komt, daarover maken wij ons zorgen, wat gaat u eraan doen?' Dat kan dan gaan over wat wij zelf waarnemen, maar het kan ook gaan over wat Europa vindt. China bijvoorbeeld daar zitten we als EU op één lijn met betrekking tot onze zorgen over het stelen van intellectueel eigendom langs cyberweg. Dan ben ik de eerste die zich daarover uitspreekt en dat doen mijn Franse collega, mijn Duitse collega, mijn Zweedse collega bijvoorbeeld ook in de dialogen die zij hebben. Waarbij je ook probeert om A) te achterhalen wat de motieven zijn en B) te kijken naar mogelijkheden om dit soort landen beter in dat normatieve kader te krijgen."

Nieuw initiatief

In de Boedapest conventie van november 2001 zijn maatregelen vastgelegd voor het bestrijden van strafbare feiten via elektronische netwerken. Het verdrag is toen niet door alle landen ondertekend en hoewel een aantal landen dat later alsnog heeft gedaan, stelt Jaarsma nuchter vast: "Het is een illusie om te verwachten dat de hele wereld op een gegeven moment Boedapest gaat tekenen."
Om die reden heeft de VN een nieuw initiatief gelanceerd en dat is de 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes'. Die commissie is belast met een onderhandelingstraject dat moet resulteren in een nieuw internationaal verdrag ter bestrijding van cybercriminaliteit. "Dat moet een verdrag worden waarachter de hele VN zich gaat scharen. Dat zal waarschijnlijk een mindere standaard zijn dan de Boedapest conventie, maar dan heb je in ieder geval ook met andere landen een basis waarmee die uitwisseling soepeler kan gaan lopen."

Jaarsma refereert nog even aan een uitspraak van voormalig minister Stef Blok over de rol van Nederland in het cyberdomein: 'We zijn het aan onze stand verplicht'. "Uiteindelijk zitten wij hier in Nederland op een enorm internetknooppunt. Wij zijn vergaand gedigitaliseerd en wij plukken economisch de vruchten van het internet. Dus wij hebben daarmee ook een verantwoordelijkheid om het domein veilig te houden. Ik merk zoals onlangs in New York, waar we dan als Nederland met drie mensen zitten plus nog iemand van de permanente vertegenwoordiging, dat we invloed hebben. In onze grondwet staat expliciet vermeld - en daar zijn we voor zover ik weet uniek in - dat wij de internationale rechtsorde willen versterken en bevorderen. Het ontwikkelen van een normatief kader en spelregels voor verantwoord statelijk gedrag in cyber sluit daar naadloos op aan. Net als het aanspreken van landen die zich niet verantwoordelijk gedragen. Het is gewoon een opdracht aan onszelf."

Het interview met Nathalie Jaarsma vond plaats voorafgaand aan de inval in Oekraïne.

CFCS: volwaardige steun van regering en parlement

Al zes jaar op rij meldt het Deense Centrum voor Cybersecurity (CFCS) in zijn jaarverslag dat de dreigingsniveaus van cybercriminaliteit en cyberspionage 'zeer hoog' zijn. Dat specifieke dreigingsniveau, 'zeer hoog', geeft aan dat actoren in staat en bereid zijn om continu te proberen Denemarken aan te vallen, zo luidt de beoordeling in 'De cyberdreiging tegen Denemarken 2021'. Dit rapport stelt dat zowel cybercriminelen als statelijke actoren zich systematisch en aanhoudend richten op het maken van slachtoffers in Denemarken.

"We krijgen elk jaar veel media-aandacht als we met dit rapport naar buiten komen.
Niet omdat het *breaking news* is – het dreigingsniveau blijft min of meer hetzelfde, de voorbeelden verschillen – maar hoe meer bewustwording we kunnen creëren, hoe meer we kunnen hopen dat mensen dit serieus nemen."
Als oprichter en directeur van de CFCS kan Thomas Lund-Sørensen worden gezien als een senior professional in de wereld op het gebied van cyberbeveiligingscentra. "Ik denk dat het voor mij het juiste moment is om het stokje over te dragen en mij te gaan richten op andere dingen. Ik werk inmiddels meer dan twintig jaar in de buitenlandse dienst, waarvan tien jaar in het cybersecuritydomein en nu ben ik van plan om die twee te gaan combineren. Ik ga lesgeven, dat heb ik al eerder gedaan, maar deze keer ga ik met universiteiten in Denemarken werken aan cybersecurity intelligence kwesties. Daar kijk ik erg naar uit. Ook zal ik als niet-uitvoerend bestuurder betrokken zijn bij enkele kleine Deense startups en ben ik als partner gestart bij een exclusief maar wereldwijd georiënteerd consultancybedrijf in het Verenigd Koninkrijk, Macro Advisory Partners, waarbij ik mij richt op geopolitiek en cyberbeveiliging."

In het recente rapport 'Government Trends 2021' van het Deloitte Center for Government Insights prijst Deloitte het CFCS voor zijn gecentraliseerde aanpak. Lund-Sørensen daarover: "Het model dat we in 2012 voor de CFCS kozen, was eigenlijk vrij uniek in de westerse wereld. We hadden een regeringswisseling in 2011 en het nieuw aangetreden kabinet gaf hoge prioriteit aan de aanpak van cyberbeveiliging alsook aan de beveiliging van de Deense vitale infrastructuur, in het bijzonder de telecominfrastructuur. Er was in die tijd een agentschap dat verantwoordelijk was voor de telecommunicatiesector en haar beveiliging, maar de regering zag op basis van de cybersecuritydreigingen dat dit agentschap moest opschalen naar een centraal meldpunt. Dat dan tevens zou worden geïnformeerd door de nationale inlichtingendienst, juist ook vanwege haar kennis in het domein van cybersecurity."

Kritieke massa

"Dus dat was de eerste reden voor een centrale aanpak, de andere was dat we een klein land zijn en we niet echt de middelen hebben om onze bevoegdheden over verschillende instellingen te spreiden. Onze nationale politie, onze buitenlandse inlichtingendienst, onze veiligheidsdienst, ons leger, ze hadden allemaal tot op zekere hoogte kennis van cybersecurity. Het was simpelweg te kostbaar en tegelijkertijd ook moeilijk om voldoende, kritische massa aan competenties te creëren om het steeds belangrijker wordende cybersecurity vraagstuk daadwerkelijk aan te pakken."
Rond die tijd had Denemarken te maken met een van de eerste ("Althans in het openbaar erkende" zegt Lund-Sørensen) cyberaanvallen uit het buitenland, waarbij de ministeries van Handel en Scheepvaart werden getroffen.
"We hadden te maken met een *burning platform* en dat vroeg om een gecentraliseerde aanpak met één cybersecurity centrum waarin alle competenties konden worden gebundeld en dat zich zou kunnen bewegen binnen zowel de publieke als de geheime omgeving."

"Het was overigens destijds behoorlijk controversieel, niet zozeer in Denemarken maar in het algemeen, dat een organisatie met binnenlandse verantwoordelijkheid werd gecombineerd met de buitenlandse inlichtingendienst. De kennis binnen de buitenlandse inlichtingendienst over statelijke actoren, de kennis over de geavanceerde cybertechnieken en aanvallen en de ervaring vanuit de offensieve kant gaven echter de doorslag voor de regering en het parlement om het zo in te richten. Daarbij moesten we er wel voor zorgen dat we onze *checks and balances* onder controle hadden. Data van bijvoorbeeld burgers en binnenlandse aangelegenheden mochten niet door het inlichtingendomein heengaan en vice versa. Een raad van toezicht ziet daar op toe en ook dat alles volgens vastgestelde procedures verloopt."

In oktober 2015 nam het Verenigd Koninkrijk in grote lijnen het Deense cyberbeveiligingsmodel over met hun National Cyber Security Centre (NCSC) als onderdeel van het Government Communications Headquarters (GCHQ) - het Britse inlichtingen- en cyberagentschap. De jaren daarna kozen het Canadian Centre for Cyber Security, het New Zealand National Cyber Security Centre en het Australian Cyber Security Centre voor een zelfde structuur.

"We hebben 't over cybercriminaliteit op industriële schaal"

Thomas Lund-Sørensen was vanaf de start in 2012 tot 1 november 2021 directeur van het Deense Centrum voor Cyberbeveiliging (CFCS), onderdeel van de Deense Defensie-inlichtingendienst. Voordat hij bij de CFCS kwam, had Lund-Sørensen een lange en indrukwekkende carrière binnen de buitenlandse dienst, als speciale vertegenwoordiger voor Libië tijdens de opstand in 2011 en als ambassadeur in Jordanië. Hij heeft een master in politieke wetenschappen van de Universiteit van Kopenhagen en een diploma van de École Nationale d'Administration in Parijs.

Tamelijk trots

"Op dat moment hadden we onze zaken behoorlijk op de rit en begon het ook impact te hebben op de Deense samenleving. Er is toen besloten dat we, ondanks dat we deel uitmaken van een geheime inlichtingendienst, een onafhankelijke, open en naar de buitenwereld gerichte houding moesten hebben. Dat hield in dat velen van ons, en ik als oprichter en directeur in het bijzonder, naar buiten traden om ons nader te presenteren, door bijvoorbeeld in het openbaar te spreken en commentaar te geven op actuele kwesties. Deze verschillende PR-acties waren er met name voor bedoeld om een beeld te creëren en onze naam te vestigen als nationale cybersecurity autoriteit. Eentje met de beste kennis, competenties en praktijkervaring. Als ik nu terugkijk, denk ik dat we dat in tien jaar hebben opgebouwd en daar ben ik tamelijk trots op."

Lund-Sørensen zegt dat het CFCS de volwaardige steun krijgt vanuit zowel het Deense parlement als de regering. "Gedurende de verschillende coalities de afgelopen jaren, waarbij cybersecuritydreigingen steeds actueler werden, waren en zijn politici het er allemaal over eens dat cybersecurity de hoogste prioriteit heeft ('Dit is iets dat belangrijk is voor de Deense samenleving, cyberbeveiliging moet serieus worden genomen', zeggen ze) en zij ondersteunen ons werk met een solide wettelijk kader en substantiële financiële ondersteuning, maar ook door meer proactief te werken aan de verdere digitalisering van de Deense overheid."

Hij vertelt dat het Deense parlement in 2018 besloot dat vanwege snelle ontwikkelingen op het gebied van cyberbeveiliging er een aanzienlijk bedrag moest worden gereserveerd dat in 2020 zou worden gebudgetteerd en geformaliseerd. "Uiteindelijk werd het 2021 voordat hierover definitieve beslissingen werden genomen", glimlacht Lund-Sørensen. Het is een goed voorbeeld van hoe Deense politici prioriteit geven aan cybersecurity, vindt hij. "Het parlement zei in 2018 voor het eerst: 'Oké we weten niet precies wat we straks gaan doen, maar we gaan geld reserveren om iets te kunnen doen, als het moment daar is en we beter zijn geïnformeerd'. En ik denk dat dat een heel, heel volwassen beslissing was. Kortom: er is al die tijd een extreem sterke politieke steun geweest voor cyberbeveiliging in dit land."

Uw dreigingsanalyse voor 2021 gaat in op het feit dat de coronapandemie, waardoor meer mensen thuis kwamen te werken, een uitdaging vormde voor de beveiliging van de infrastructuur. Kunt u dat toelichten?
"Wat interessant is om te vertellen, is dat twee dagen nadat onze premier de aankondiging deed over de lockdown van het land, op 11 maart 2020, iedereen vanuit huis werkte. En dat zorgde natuurlijk voor een geheel nieuwe beveiligingsomgeving. Veel van mijn mensen in het CFCS werkten ook vanuit huis. Die snelle omschakeling naar op afstand werken is volgens mij een goed voorbeeld van hoe ver we zijn gekomen met betrekking tot de digitalisering van de Deense samenleving. Tegelijkertijd is het onze taak ervoor te zorgen dat in die nieuwe werkomgeving op afstand ook voor een juiste beveiliging wordt gezorgd."

Was er een toename van cyberaanvallen tijdens de pandemie?
"Nee, wat ons in ieder geval in het begin opviel, was dat we niet de enigen waren die naar huis werden gestuurd om te werken, ik denk dat veel cybercriminelen hetzelfde hebben meegemaakt. Maar de impact wereldwijd zorgde natuurlijk wel voor een cyberbeveiligingsprobleem. We weten dat criminelen zich zeer snel kunnen herorganiseren. Ik denk dat het heel belangrijk is om ons te realiseren dat we het niet hebben over de eenzame hacker, maar over cybercriminaliteit op industriële schaal. Georganiseerde misdaad dus."

Kunt u een voorspelling doen met betrekking tot toekomstige cyberdreigingen?
"Ik verwacht dat er voor veel meer sectoren cyberdreigingen actueel worden in onze maatschappij. Op dit moment hebben we zes kritieke sectoren, maar ik denk dat dat de komende jaren zal groeien naar tien, misschien zelfs vijftien. Ik ben er zeker van dat we in de loop van de tijd nieuwe eisen zullen stellen aan wat er moet worden gedaan om er in ieder geval voor te zorgen dat er een adequaat cyberbeveiliging niveau wordt behaald. We ondernemen daartoe veel verschillende initiatieven op het gebied van technische ondersteuning, op het gebied van cyberbeveiligingstraining en -onderwijs en op het delen van kennis tussen de verschillende entiteiten. Ik denk dat dit overigens geldt voor de meeste cyberbeveiligingsstrategieën in de westerse wereld. De ontwikkeling daarvan is sterk geïnspireerd door *best practices*. Onze strategie is in de eerste plaats gericht op de publieke sector, de overheid. Voor de private sector, en dan heb ik het over die bedrijven die geen deel uitmaken van de vitale infrastructuur, zoals kleine en middelgrote bedrijven, geldt nu nog een andere prioriteit. Ook daarvoor moeten er initiatieven ontwikkeld worden binnen die cyberbeveiligingsstrategie. Maar de primaire focus ligt nu op overheidsinstanties en organisaties met een verantwoordelijkheid voor onze nationale vitale infrastructuur."

Cybercriminaliteit stopt niet bij de grens. Hoe is de samenwerking met bijvoorbeeld de aangrenzende Scandinavische landen of andere landen in Europa?
"Het is een feit dat 99 procent van de cyberaanslagen uit het buitenland komt en niet uit Nederland, en ook niet uit de noordelijke landen. In onze publicaties verwijzen we naar Rusland, naar China, naar Noord-Korea en naar Iran als degenen met de meeste capaciteit op dit gebied. Dus ja, samenwerking is enorm belangrijk. Ik werk nauw samen met mijn collega's Hans de Vries in Nederland en Miguel De Bruycker in België als het gaat om het delen van kennis. Onze collega's van de buitenlandse veiligheidsdiensten zijn ook aan het intensiveren, feitelijk besteden we behoorlijk veel tijd aan het versterken van onze internationale positie met vergelijkbare entiteiten, en dan in het bijzonder in Europa."

Meer focus

Terugkijkend op 10 jaar CFCS en de ontwikkelingen met betrekking tot cybersecurity, is Lund-Sørensen over het algemeen tevreden met wat er is bereikt. Waarbij aangetekend: "We hebben nog steeds substantiële problemen op te lossen. Ik heb een langere lijst, maar een van de belangrijkste prioriteiten is dat er meer focus moet komen voor cybersecurity op bestuurdersniveau. Managers van overheidsinstanties, raden van bestuur, CEO's, ze hebben nog steeds moeite om cyberbeveiligingskwesties te doorgronden. En het is niet dat ik vind dat ze experts moeten zijn en alles over technologie moeten weten, maar zij zijn degenen die de toon moeten zetten in hun organisaties. Het is nu nog veelal onduidelijk of ze volledig inzicht hebben op de impact van de digitale transformatie van hun organisaties en de bijbehorende risico's."

Kan dit gebrek aan focus worden gezien als een gebrek aan kennis op bestuurdersniveau?
"Ik zou niet direct willen zeggen gebrek aan kennis. Laat me je een voorbeeld geven. Als iemand in de echte wereld, de analoge wereld, zou proberen om explosieven op zendmasten te plaatsen, wat zouden we dan doen? Natuurlijk laten we dat niet gebeuren en zorgen we voor bescherming van onze infrastructuur en jagen we de daders na. Maar als mensen in het cyberdomein digitale bommen zouden plaatsen... wat gebeurt er dan? Nog niet zo veel ben ik bang. Dus ik denk dat de intellectuele discrepantie tussen de fysieke, analoge, normale wereld en de digitale wereld nog steeds enorm is en die moet worden geslecht."

COLUMN

Duurzame cyberweerbaarheid vereist meer aandacht voor nieuwe technologie

Back-ups in orde, alle medewerkers doordrongen van veilig digitaal werken en zelfs multifactor authenticatie geïmplementeerd? Dan voelt het vast alsof je organisatie is opgewassen tegen digitale dreigingen. Dit soort basismaatregelen zijn echter pas het begin. Nieuwe technologieën die een nieuw soort dreigingen creëren, komen er in rap tempo aan. Deze innovaties zijn dus niet alleen kansen, maar bittere noodzaak om de weerbaarheid op peil te houden.

Op verzoek van de Cybersecurity Raad bracht het Rathenau Instituut in kaart welke technologische ontwikkelingen op de middellange termijn (2-8 jaar) van grote betekenis zullen zijn voor de cyberweerbaarheid van Nederland. Hieruit bleek dat er nu al actie ondernomen moet worden om de samenleving voor te bereiden op technologieën die nog maar in de kinderschoenen staan. Het stimuleren van innovatie blijkt niet alleen een economische, maar vooral ook een veiligheidskwestie.

Neem de kwantumcomputer. In theorie is zo'n machine in staat om de bestaande versleutelingsmethoden te doorbreken. Bedrijfsgeheimen, medische gegevens en de aansturing van allerlei industriële systemen zouden dan in één klap hun bescherming verliezen. De inschattingen lopen uiteen over hoe lang het nog duurt tot wetenschappers er in slagen om de daarvoor benodigde doorbraken te bewerkstelligen. Maar zelfs als dit nog decennia op zich laat wachten, geeft dat nu al reden tot zorg. Veel organisaties gaan er nu namelijk ten onrechte vanuit dat, zolang ze gegevens maar versleutelen, ze beschermd zijn en blijven. Het maakt ze niet uit waar hun gegevens staan opgeslagen, worden gekopieerd of wie de versleutelde gegevens voorbij ziet komen wanneer deze worden verzonden.

Als het van belang is om die gegevens ook over decennia nog geheim te houden, dan doen organisaties er goed aan om nu al te investeren in post-kwantumcryptografie. Aanbieders van vitale diensten, financiële dienstverleners en zorginstellingen moeten dus aan de slag met dit soort versleutelingsmethoden die kwantumcomputers kunnen weerstaan.

Kwantumcomputers zijn slechts een voorbeeld van een nieuwe technologie die de cyberweerbaarheid op de proef zal stellen. De volgende generatie mobiele telefonie (6G), satellietcommunicatie en toepassingen van machine learning bieden zich in rap tempo aan. Bestuurders moeten erop letten dat risicoanalyses die hen worden voorgelegd, ook die middellange termijn in ogenschouw nemen. Dus ook de vraag stellen: welke "kroonjuwelen" moeten er over tien of twintig jaar nog beschermd blijven?

De overheid kan hierin een stimulerende rol spelen: door middel van wetgeving, certificering en standaardisering leveranciers stimuleren om betere producten op de markt te brengen. Denk hierbij aan afspraken over technologische maatregelen zoals encryptie en vereisten als dataportabiliteit en interoperabiliteit, maar ook organisatorische normen over toezicht, het melden van incidenten en respons. In standaarden kunnen ook publieke waarden worden beschermd. Het 6G protocol zal bijvoorbeeld ook de mate waarin surveillance van gebruikers kan plaatsvinden bepalen, of bepalen waarop toezicht kan worden gehouden, wat consequenties heeft voor privacy. Standaarden komen nu vaak tot stand door inbreng van de technologie ontwikkelaars. Het zou getuigen van weinig lerend vermogen als we bij 6G pas weer aan het einde van het standaardisatieproces gaan bediscussiëren welke leveranciers vertrouwd kunnen worden.

Het ligt nu in de lijn der verwachtingen dat de belangwekkende nieuwe technologieën voor cyberweerbaarheid opnieuw door buitenlandse ondernemingen zullen worden ontwikkeld. De ruim zestig geconsulteerde experts en belanghebbenden voor het onderzoek van het Rathenau Instituut uitten daar vaak hun zorgen over. Zij ervaren zulke sterke afhankelijkheden van leveranciers, dat het kiezen voor een alternatief niet langer als haalbare optie zien (vendor-lockin). Met het Strategisch Kompas van de Europese Commissie (EC) staat sterkere digitale autonomie in elk geval wel volop op de politieke agenda.

Voor een deel wil de Europese Commissie de ontwikkeling van Europese alternatieven van buitenlandse producten en diensten bevorderen. Denk bijvoorbeeld op de Gaia-X data infrastructuur als antwoord op de dominantie van Amazone of zelfs de "secure connectivity" internetsatellietinfrastructuur als alternatief voor Starlink of OneWeb. Aangezien het van de grond af opbouwen van succesvolle alternatieven lang niet altijd haalbaar zal zijn, zien we ook hier dat de Europese Commissie gebruik maakt van de kracht van regulering en standaardisatie. Het gaat niet zozeer om het weren van buitenlandse producten of diensten, maar het garanderen van veiligheid en zeggenschap.

De uitdaging is om daarbij met nieuwe technologie de cyberweerbaarheid te verhogen en tegelijkertijd Europese waarden te beschermen. Om dat doel te bereiken is het van belang dat de overheid nog nadrukkelijker werk maakt van open standaarden, om zo ongewenste vendor-lockin te voorkomen. Een tweede praktische manier om die standaarden te realiseren is het aanscherpen van inkoopvoorwaarden. Grote organisaties, zoals de overheid en aanbieders van vitale diensten, kunnen hierin het voortouw nemen. Ten slotte zijn verbeteringen in het innovatieklimaat noodzakelijk, zodat bedrijven diensten en producten aanbieden die bijvoorbeeld privacy en autonomie centraal stellen.

Dit is niet alleen een kwestie van investeren in kennisontwikkeling. Het behouden van experts verdient daarnaast meer aandacht. Internationaal is er een chronisch tekort aan experts in cyberweerbaarheid, en dat geldt eens te meer als het gaat om experts met kennis van de nieuwste technologieën. Als het bijvoorbeeld gaat om kwantumtechnologie, machine learning of satellieten, wordt in Nederland technologie op wereldklasse ontwikkeld. Het stimuleren van bedrijvigheid is nodig om de talenten die in deze sectoren werkzaam zijn te behouden en economische kansen te benutten.

Deze technologische ontwikkelingen zullen niet alleen verbeteringen met zich meebrengen. Nieuwe technologieën creëren op hun beurt weer nieuwe kwetsbaarheden. Machine learning kan bijvoorbeeld zowel gebruikt worden om automatisch kwetsbaarheden te misbruiken als te herstellen. Vernieuwing brengt dus niet vanzelfsprekend vooruitgang. Vooruitgang wordt pas geboekt als het hele stelsel aan randvoorwaarden ervoor zorgt, dat de kansen op duurzame cyberweerbaarheid worden benut, en publieke waarden zoals autonomie en privacy worden geborgd.

Pieter van Boheemen is onderzoeker Digitale Samenleving bij het Rathenau Instituut. Hij houdt zich vooral bezig met de maatschappelijke impact van digitalisering op veiligheid, democratie en media. Zo onderzocht hij recent, op verzoek van het Europees Parlement, synthetische media. Ook droeg hij, op verzoek van de WODC (het Wetenschappelijk Onderzoek- en Documentatiecentrum, het kennisinstituut voor het ministerie van Justitie en Veiligheid) bij aan een studie naar schadelijk gedrag op het internet. Van Boheemen studeerde Life Science & Technologie aan de TU Delft en Universiteit Leiden.

DTC: samenwerken stimuleren

In totaal 361 bedrijven in Nederland kregen in 2021 een waarschuwing voor cyberdreiging. Afzender: het Digital Trust Center (DTC). Michel Verhagen licht toe: "We zijn in de zomer gestart met het ongevraagd delen van specifieke dreigingsinformatie met individuele niet-vitale bedrijven. Er zijn in 2021 vijftien aanleidingen geweest om dergelijke bedrijven te notificeren. Daarnaast hebben we een pilot 'gevraagd notificeren' met 57 bedrijven gestart. We gaan nu kijken of we dat proces kunnen automatiseren - zodat we veel grotere aantallen bedrijven kunnen waarschuwen."

Dat is nodig ook want het aantal aanvallen met ransomware was in 2021 wereldwijd bijna tweemaal zo hoog als in 2020. Vooral de industriesector was een populair doelwit. "We verwachten dus dat het aantal waarschuwingen flink gaat stijgen en pas dan kun je ook zeggen of deze nieuwe dienst het verschil maakt", aldus Verhagen. "Je kunt niet 100 procent voorkomen dat je ooit geraakt wordt. Maar 'weerbaar' betekent ook, dat als het dan tóch gebeurt, ondanks alle voorzorgsmaatregelen, dat je dan weet hoe te handelen. Dat je je back-ups op zo'n manier hebt gedaan dat je er ook daadwerkelijk bij kunt. Dat je je gegevens zodanig hebt beschermd dat in ieder geval de hele gevoelige data niet in verkeerde handen kunnen komen. Dat je ook een herstelplan hebt, zodat je relatief snel weer in productie kunt."

Twee miljoen bedrijven

Het DTC dankt zijn oorsprong aan een motie van de Tweede Kamer waarin werd gepleit om analoog aan het Nationaal Cyber Security Centrum (NCSC) voor de Rijksoverheid en vitale organisaties een vergelijkbare voorziening in het leven te roepen voor het brede bedrijfsleven in Nederland. Die werd in 2018 een feit. "Je praat over een kleine twee miljoen bedrijven – van zzp'ers tot multinationals - die heel erg variëren in bewustzijn, van onbewust onbekwaam tot bewust bekwaam. Onze rol daarin verschilt, maar als ik het generiek formuleer dan hebben we als taak om bedrijven van alles aan te reiken zodat zij maatregelen kunnen nemen die passen bij de risico's die ze lopen. Wat we niet doen is, wanneer bedrijven worden getroffen door een cyberincident, hen ook daadwerkelijk bij de hand nemen en *incident response* bieden."
Daarvoor is het aantal bedrijven te omvangrijk, daarvoor heeft het DTC niet de mensen en de middelen én is *incident response* bieden in deze context ook niet een primaire verantwoordelijkheid van de overheid, stelt Verhagen. "Die verantwoordelijkheid geldt uiteraard wel voor de Rijksoverheid zelf en organisaties die we als vitaal beschouwen", voegt hij eraan toe. Die specifieke taak is belegd bij het Nationaal Cyber Security Centrum (NCSC).

Informeren en adviseren ziet Verhagen als een primaire taak van het DTC. Hij noemt als voorbeeld het incident, december 2021, rond de Log4j software. "Dan proberen we wel meteen te duiden: wat is er nou precies aan de hand, wat kun je doen als bedrijf om te ontdekken of het ook jou heeft getroffen? Hoe kun je het eventueel gerepareerd krijgen en hoe kom je aan de juiste patch? Dus op actuele dreigingsinformatie reageren we direct. We zetten zo snel mogelijk een bericht op onze website en delen dat via onze social media kanalen. We gebruiken Twitter, we gebruiken LinkedIn, en sinds een aantal maanden hebben we ook een DTC Community die flink aan het doorgroeien is en waar nu meer dan 1.000 bedrijven deel van uit maken. Wat we zien is dat die bedrijven behalve dat ze over actuele informatie willen beschikken ook kennis met elkaar willen delen en elkaar willen helpen."

Samenwerking stimuleren

Dergelijke samenwerking stimuleren ziet Verhagen ook als taak van het DTC. "Cybersecurity is een *hot issue* op dit moment. Helaas is er nog heel veel werk te doen om een grote groep bedrijven die nog onvoldoende bewust zijn, of misschien al wel bewust maar nog eigenlijk onbekwaam zijn, om die op het juiste niveau te krijgen." "Aanvallers worden ook steeds geraffineerder. Als je kijkt naar *phishing* aanvallen van vijf jaar geleden, daar kon

Michel Verhagen is sinds januari 2018 manager van het Digital Trust Center (DTC). Daaraan voorafgaand was hij, april 2017, al aangesteld als kwartiermaker. Het DTC is onderdeel van het ministerie van Economische Zaken en Klimaat (EZK) en heeft als missie om 2 miljoen Nederlandse bedrijven (van zzp'er tot grootbedrijf in niet-vitale sectoren) weerbaarder te maken tegen cyberdreigingen. Verhagen werkt al sinds 1985 voor voornoemd ministerie, onder andere als plaatsvervangend directeur ICT & Toepassing en als plaatsvervangend directeur van Agentschap Telecom .

"De intensiteit en de omvang van cyberaanvallen nemen toe"

je nog om gniffelen vanwege bijvoorbeeld het slechte Engels. Maar bij *ransomware* aanvallen van nu wordt door aanvallers écht gekeken naar manieren waarop ze het meest kunnen verdienen. De intensiteit en de omvang van cyberaanvallen nemen toe. Het vereist ook dat je steeds meer alert bent en voorzorgsmaatregelen treft. Dat is een vraagstuk dat je vaak niet in je eentje helemaal ingeregeld krijgt en daarom stimuleren wij ook samenwerking. Je ziet ook steeds meer aanvallen in ketens dus je moet hierin samen optrekken als bedrijven, maar ook als overheid en bedrijven."

"Wij kennen op dit moment 42 samenwerkingsverbanden van bedrijven. Dat zien we lokaal zoals bij Brainport Eindhoven en in de havens van Rotterdam en Amsterdam. Dat zien we regionaal, bijvoorbeeld in Noord-Nederland waarin ook het mkb een rol speelt. Hetzelfde gebeurt in Zuid-Nederland. En ook steeds vaker sectorgericht want brancheorganisaties zien dat leden meer aandacht krijgen voor het onderwerp cyber."

De doelstelling voor 50 samenwerkingsverbanden eind 2023 lijkt goed haalbaar. Hiermee draagt het DTC ook bij aan de vorming van een Landelijk Dekkend Stelsel (LDS) van cybersecurity samenwerkingsverbanden zoals opgenomen in de Nederlandse Cybersecurity Agenda (NCSA).

Het DTC staat ook in contact met koepelorganisaties als NL.Digital, ECP | Platform voor de InformatieSamenleving, Kamer van Koophandel, VNO-NCW en MKB-Nederland en het CIO-platform. Via twee webinars zijn het afgelopen jaar beschikbare kennis, diensten en oplossingen van het DTC toegelicht aan sub-doelgroepen van beide ondernemersorganisaties. "Deze partijen kunnen hun achterban makkelijk bereiken. Wij zorgen ervoor dat de communicatie met hen goed is afgestemd. Ook het NCSC deelt informatie met ons die relevant is voor de doelgroep van het DTC."

Vijf basisprincipes

Het DTC hanteert vijf basisprincipes voor veilig digitaal ondernemen: 1. Inventariseer kwetsbaarheden; 2. Kies veilige instellingen; 3. Voer updates uit; 4. Beperk toegang; 5. Voorkom virussen en andere malware. "Op basis daarvan hebben we een aantal tools ontwikkeld en een heel belangrijke is de Basisscan Cyberweerbaarheid. Deze scan kun je in vijf minuten uitvoeren en dat biedt je als bedrijf de mogelijkheid om inzicht te krijgen in waar je staat. Is de basis op orde? Waar is extra inspanning nodig? Want we hebben wel back-ups maar geen offline back-up, ik noem maar even wat; we hebben wel een beleid voor wachtwoorden, maar dat is niet meer van deze tijd. Dat komt allemaal voort uit die vijf basisprincipes."

"Die hebben we opgesteld in overleg met verschillende IT-specialisten maar ook met bedrijven die graag hun ervaringen delen en willen meedenken hoe we pragmatisch andere bedrijven kunnen helpen. Want dat is nog wel eens lastig: een groot deel van de bedrijven die tot onze doelgroep behoren hebben niet veel IT-kennis. Dan heb ik het niet specifiek over het mkb, we zien ook grotere productiebedrijven die druk bezig zijn met automatisering maar zich niet altijd bewust zijn van de kwetsbaarheid van geautomatiseerde productiesystemen."

Hiervoor is door DTC in samenwerking met het bedrijfsleven de Security Check Procesautomatisering ontwikkeld. "Ook in de keten wordt gezocht naar de zwakste schakel. Dus we moeten ervoor zorgen dat de hele keten op een hoger niveau terechtkomt. Voor een deel kan dat gebeuren doordat een partij eisen stelt aan de leveranciers in die keten, maar voor een deel is dat ook ervoor zorgen dat kleine bedrijven hun verantwoordelijkheid pakken. Want ook de bakkerij die aan AH levert, kan getroffen worden en dan zijn de schappen leeg."

Integraal onderdeel

"Wat wij nastreven is dat in de operatie heel veel wordt samengewerkt. Ik vind het belangrijk dat we, als onderdeel van EZK, onze verantwoordelijkheid nemen hierin voor het bedrijfsleven. Cybersecurity moet een integraal onderdeel zijn van de manier waarop we met de diverse sectoren omgaan. Elke sector heeft zo z'n eigenaardigheden, de zorgsector is weer anders dan de onderwijssector, dus wij moeten wel weet hebben van wat er speelt om het goede advies te kunnen geven. Punt is: we vragen aandacht voor de kansen van digitalisering maar in onze benadering moeten we ook aangeven dat je die kansen alleen kunt verzilveren als je veiligheid meeneemt in de manier waarop je het organiseert. Steeds meer experts zeggen: 'Het is niet meer de vraag of het je gebeurt, het is meer de vraag wanneer het je gebeurt'."

Verhagen vindt dat er stappen worden gezet waar het gaat om het vergroten van de weerbaarheid van Nederland in cyberspace. "Ik denk dat we een heel eind zijn opgeschoten, samenwerking komt steeds meer van de grond. Tussen publieke organisaties maar ook tussen publieke en private organisaties. Wij worden als overheid ook beter in het optrekken van de verdediging en slagen er ook beter in om proactief te zijn. Dat is ook de uitdaging, om het samen naar een hoger niveau te brengen. Wij leggen als DTC de lat voor onszelf ook steeds hoger. Ik ben heel blij met wat we kunnen betekenen op dit moment als DTC. Het aantal bezoekers aan onze website is in een jaar verdubbeld van 100.000 naar ruim 200.000. Er zijn 10.000 scans ingevuld. We hebben 5.000 volgers op LinkedIn. Het is heel dankbaar werk dat we doen."

Tenslotte: in een brief aan de Tweede Kamer gedateerd 7 februari 2022 waarin deze wordt geïnformeerd over de voortgang van het DTC, schrijft minister Adriaansens: "Het DTC ligt op koers. Ook de komende jaren zal het ministerie van Economische Zaken en Klimaat blijven investeren in de cyberweerbaarheid van niet-vitale bedrijven om daarmee bij te dragen aan het verdienvermogen van ondernemend Nederland en de economische kansen van digitalisering daadwerkelijk te kunnen benutten."

CISO Rijk: versterken digitale weerbaarheid

Digitale weerbaarheid is in de definitie van Aart Jochem 'het duurzaam kunnen weerstaan en detecteren van, het reageren op en het herstellen van verstoring en misbruik van ICT door dreigingen'. Hij tekent daarbij aan dat "een betrouwbaar Rijks-ICT landschap als onderdeel van de basisinfrastructuur van Nederland een zekerheid moet zijn en geen variabele."

Zijn werkzaamheden voor pensioenuitvoerder PGGM en het NCSC – hij was in de periode 2012-2016 directieteamlid en hoofd *monitoring and response* – hebben Aart Jochem doen inzien dat "ervoor zorgen dat je op lange termijn duurzaam veilig bent", de essentie is van digitale weerbaarheid. "Niet alleen de patch van vanmorgen, maar dat je alles gewoon goed hebt ingeregeld in processen en dat je dat ook kan aantonen, want dat is van belang voor de afnemers of burgers en moet van de toezichthouder. En natuurlijk gaat het dan wel eens een keer fout, maar dat komt dan niet doordat je het systeem verkeerd hebt ingericht."

In 2019 is door toenmalig minister Ollongren de functie van CISO Rijk aangekondigd om zo de coördinatie op informatiebeveiliging binnen de Rijksoverheid structureel te verbeteren. Jochem is de eerste in die functie en maakt deel uit van de directie CIO Rijk waar Lourens Visser aan het hoofd staat. De CISO Rijk wordt ondersteund door een afdeling Informatiebeveiliging & Privacy, is ook voorzitter van de interdepartementale CISO-raad binnen de Rijksoverheid en werkt nauw samen met de directie Digitale Samenleving, de Rijksbeveiligingsambtenaar (BVA Rijk), het Nationaal Cyber Security Centrum (NCSC), de veiligheidsdiensten en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Samenwerken

Die coördinerende en verbindende rol ligt Jochem wel en hij onderschrijft ook de noodzaak ervan. "Ook binnen de departementen is iedereen wel doordrongen van het belang van samenwerking en gemeenschappelijke afspraken. De cyberdreiging neemt zo rap toe, je kunt het gewoon niet meer alleen, je moet echt samenwerken."
Jochem maakte een rondje langs de departementen, sprak met de diverse secretarissen-generaal (SG's) en inventariseerde: hoe staan we ervoor? Dat heeft er onder meer toe geleid dat in de I-strategie Rijk 2021-2025 concreet aandacht is voor beter sturen op informatiebeveiliging. Daarnaast is het bestaande CIO-stelsel versterkt met die rol van CISO, met bijbehorende taken en bevoegdheden.
Eén van Jochem's mandaten is "dat ik mijn leidinggevende mag passeren en direct richting de ambtelijke top mag gaan met advies – uiteraard wel met medeweten van. Normaal gaat bij de overheid alles keurig netjes via het stippellijntje, maar als het moet ga ik rechtstreeks naar de SG. Ook kan de CISO Rijk aanwijzingen geven namens de SG."
Anders gezegd: in acuut geval bij een groot incident heeft de CISO Rijk na afstemming de bevoegdheid om, bijvoorbeeld, systemen los te koppelen van het internet.

Jochem benadrukt dat alle departementale CIO's zich hebben gecommitteerd aan de I-strategie Rijk 2021-2025. Hij zegt: "In deze strategie is 'i' niet alleen iets van CIO Rijk maar staat centraal in de aanpak van de departementen. Ieder thema wordt door een van de CIO's getrokken en dat brede draagvlak gaat in de uitvoering zeker helpen."
Naast het ontwikkelen van een Rijksbrede Digitale Infrastructuur (RDI) behoort 'digitale weerbaarheid' tot de speerpunten van het beleid. 'Werken aan veiligheid is nooit af' staat te lezen in het omvangrijke (128 pagina's) strategiedocument.
De speerpunten van het thema 'Versterken digitale weerbaarheid' zijn:
1. Governance – beter sturen op risico's;
2. Werken aan feitelijke veiligheid;
3. Weerbare medewerkers.

Urgent en alarmerend

"Hoe meer je digitaliseert als samenleving hoe meer afhankelijk je wordt van technologie. Dus moeten we onze infrastructuur goed beveiligen en ook de privacy goed waarborgen. Als we afgaan op de berichten van de Cyber Security Raad en ook wat we uit andere bronnen en de media vernemen, is het dreigingsbeeld dusdanig dat we nu moeten acteren en geen plannen kunnen

Aart Jochem is sinds 1 november 2020 Chief Information Security Officer (CISO) Rijk bij de directie CIO Rijk van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Van december 2016 tot en met oktober 2020 had hij een vergelijkbare functie bij pensioenuitvoerder PGGM. Eerder was Jochem al voor de Rijksoverheid werkzaam bij het Nationaal Cyber en Security Center (NCSC) en de voorganger daarvan GOVCERT.nl. De CISO Rijk heeft onder meer als taak 'Versterken digitale weerbaarheid' zoals benoemd in de I-strategie Rijk 2021-2025. Ook impliceert de functie een belangrijke rol in contacten buiten het Rijk (ergo: met andere overheden en het bedrijfsleven) en de samenwerking met Rijksorganisaties.

"Onderzoeken laten zien dat de Rijksoverheid achterloopt in beveiliging, dat moet je niet negeren"

maken om het over vijf jaar op orde te hebben. Het is urgent en alarmerend en tegelijkertijd weten we ook dat de Rijksoverheid achterloopt in beveiliging. Dat zegt de Algemene Rekenkamer, dat zegt Cybersecuritybeeld Nederland, dat geeft wel aan: we moeten écht wat doen."

Hij zegt uit ervaring te weten dat je nooit op alle niveaus het hoogst kunt scoren. "Als je dat als ambitie neerzet weet je dat je gewoon heel veel moet investeren en dat het echt in de haarvaten van je organisatie moet zitten. Dat is maar voor weinig organisaties weggelegd. Een voldoende niveau halen is al verdraaid moeilijk, en als je dat op een bepaald moment hebt bereikt moet je er ook aan blijven werken om dat niveau te behouden. Wat dat betreft is het een beetje als topsport: je houdt best wel een poosje je conditie op niveau, maar als je niet blijft investeren en verbeteren dan zakt het vanzelf gewoon weer weg."
"Gelukkig – en dat wil ik onderstrepen – gebeurt er al heel veel op het gebied van informatiebeveiliging en zeker de bescherming van staatsgeheimen. Daar is een complete *governance* omheen gecreëerd, daar is goed beleid voor met allerlei accreditaties, de AIVD heeft een belangrijke rol daarin. Maar ik denk dat we zeker nog wel kunnen groeien als het gaat over continuïteit, beschikbaarheid en integriteit. Als je het hebt over data en je gaat je besluitvorming doen op basis van algoritmes, dan is ook de betrouwbaarheid en de integriteit van die data en die algoritmes belangrijk. Daar hebben we nog wel een aantal stappen te zetten."

Kroonjuwelen

Jochem geeft aan dat zijn ronde langs de SG's hem hielp een eerste beeld van de aanpak van de departementen te krijgen. Hij schetst een beeld van bestuurders die het belang onderkennen en beveiligers die aangeven wat nodig is. "Je moet met elkaar heel goed nadenken wat je wil beschermen. Wat zijn je kroonjuwelen? Welke risico's en beheerdoelen heb je en hoe kunnen we daaraan bijdragen om dat veilig te doen? De beweging naar de cloud is er eentje die bij het Rijk nu ook echt wel momentum gaat krijgen. Hoe beveilig je dat?"
Honderd procent veilig is een illusie, dat weet hij wel. "We sturen op het versterken van die digitale weerbaarheid. Dus weten waar je kroonjuwelen zijn, ervoor zorgen dat je signalen niet negeert, dat je op een goede manier reageert op wat er gebeurt en ook weer snel kunt herstellen."
"Het basisniveau is overal hetzelfde, maar departementen verschillen ook van elkaar, ook omdat ze ieder andere doelstellingen hebben. Wat je wel ziet is dat er heel veel bereidwilligheid is om *good practices* te delen en van elkaar te leren, bijvoorbeeld over *security awareness* of risicomanagement."
In die zin is ook het samenwerken en uitwisselen van ervaringen tijdens het incident met Log4j software in december 2021, waarbij een kwetsbaarheid in allerlei computersystemen werd aangetoond, een positieve indicatie voor het functioneren van de keten in geval van crisis. "Mijn directeur-generaal heeft ook een verantwoordelijkheid voor de andere overheidslagen, de gemeentes en waterschappen en de provincies, en dan proberen we één beeld te maken van hoe het ervoor staat. Het is niet zo dat ik één dashboard heb waar ik precies zie waar alle systemen staan en welke softwareversies er op draaien, maar ik weet wel dat iedere partij aan het werk is en ook bereid is zijn informatie te delen."

Natuurlijk probeer je in zo'n situatie ook handelingsperspectief te creëren en een inschatting te maken van de mogelijke impact van de aangetroffen kwetsbaarheid in de software, stelt Jochem. "De mensen van de Shared Service Centra, van DUO, de Belastingdienst, en de anderen, die zijn op zo'n moment heel hard bezig om te onderzoeken waar het zit en welke andere maatregelen ze kunnen nemen dan alleen *patchen*. Ik moet zeggen: het NCSC heeft voortreffelijk werk gedaan rond deze kwetsbaarheid, is in alle netwerken actief geweest, ook internationaal, die hebben echt de *lead* gepakt. Wij moeten dan zorgen als CISO's dat wij die *efforts* coördineren, dat we over de volle breedte aandacht krijgen, en dat we ervoor zorgen dat de kroonjuwelen beschermd blijven."

U noemt nu een paar keer het woord 'kroonjuwelen'.. heeft ieder departement helder wat die zijn?
"Ja, dat beeld is er wel. In elk geval heeft ieder departement zicht op zijn kritische systemen en te beschermen belangen, wat randvoorwaardelijk is om gewoon je dienstverlening te kunnen doen. Ze hebben daar ook risicoanalyses voor gedaan en doen steeds meer pentesten,."
Hij zegt dat dreigingsincidenten - zoals dus recent Log4j en eerder Citrix - bijdragen aan aandacht hiervoor. Dergelijke voorvallen impliceren ook telkens nieuwe analyses, rapportages en *lessons learned*, stelt Jochem vast, "dus de I-strategie is niet in beton gegoten, we zullen evalueren en aanpassen wanneer en waar dat nodig is en dat vind ik alleen maar heel gezond."
Met een glimlach: "We hebben in die I-strategie ook aandacht gevraagd voor *red teaming*. Dan huur je een ethische hacker in om een realistische hackaanval uit te voeren om te zien of je kroonjuwelen beschemd zijn. Beter op eigen initiatief een vertrouwde partij dit te laten doen dan door een cybercrimineel op je kwetsbare plek gewezen te worden."

Hoe staat het met internationale contacten?
"Ik heb binnenkort een overleg met mijn collega in België, Miguel De Bruycker. Een groot internationaal netwerk is er nog niet voor de CISO's in Europa. Ik ben wel van plan, zo gauw ik er zicht op heb, om dat te organiseren. Via het NCSC zijn er contacten met Europese CERTs en er is overleg geweest met een aantal landen rond bepaalde kwesties, maar dat is echt iets dat zich nog verder moet ontwikkelen. De situaties zijn ook anders: een NCSC in Nederland versus het NCSC in het Verenigd Koninkrijk of in Finland, ze hebben dezelfde naam maar voor de rest zijn de opzet en het mandaat gewoon heel verschillend."
Waar op dit moment meer oog voor is, geeft Jochem aan, "is wat er binnen Nederland buiten de overheid gebeurt. Wij willen aanhaken bij CIO- en CISO-netwerken binnen de financiële sector en de *retail* die al veel ervaring hebben met bijvoorbeeld de cloud transitie. Wij lopen daar als overheid achteraan. Dus om bij dat soort sectoren langs te gaan en te vragen 'Wat vinden jullie van ons plan?', dat is gewoon heel nuttig."

VISIE

Strategie voor cyberweerbaarheid: *assume breach*

Cyberaanvallers treffen steeds vaker doel. Zo blijkt uit het tweede Microsoft Digital Defense Report dat de effectiviteit van aanvallen in een jaar tijd is gestegen van 21 naar 32 procent.[1] Zijn de pijlen gericht op een organisatie, dan is in bijna de helft van de gevallen de overheidssector het doelwit. Hoe verhogen we de weerbaarheid tegen cyberaanvallen?

Eind 2021 was het 'code rood' bij veel IT-afdelingen. Ze namen het in een race tegen de klok op tegen cybercriminelen die lucht hadden gekregen van een lek in Apache Log4j, een Java-logtool die wordt gebruikt om 'logs' bij te houden van webservers. Die cybercriminelen kunnen via dit Log4Shell-lek bijvoorbeeld *ransomware* installeren op kwetsbare systemen, of deze systemen misbruiken voor het delven van cryptomunten.[2]

Het dringende advies aan organisaties met kwetsbare systemen was om de beschikbare patch zo snel mogelijk te installeren. Op het moment dat de kwetsbaarheid bekend werd, krioelde het op internet namelijk al van de bots waarmee cybercriminelen kunnen testen of organisaties en bedrijven het Log4Shell-lek al hebben gedicht. De kwetsbare Log4j-code zit in meer dan duizend bekende applicaties van leveranciers zoals SAP en Oracle maar ook in consumententoepassingen zoals Netflix en Minecraft. Iedere seconde telde dus.

Vertrouwen is cruciaal

Het maakt wel duidelijk dat organisaties nauwelijks de tijd hebben om te reageren op het moment dat een kwetsbaarheid in systemen of software aan het licht komt. Terwijl te laat reageren ernstige gevolgen kan hebben, zoals de versleuteling van gevoelige gegevens door ransomware. Niet voor niets dat onder andere de gemeenten Almere en Hof van Twente en de Kamer van Koophandel systemen preventief offline haalden toen het lek aan het licht kwam.[3]

Een te late reactie kan ook het vertrouwen schaden dat burgers en ondernemers hebben in de communicatie met de overheid. Of in de administratie van de overheid. Stel dat de administratie van de CoronaCheck-app niet goed functioneert. Dat heeft direct gevolgen voor het vertrouwen tussen de overheid en de burger die onterecht de toegang wordt ontzegd tot een pretpark of restaurant.

Digitale weerbaarheid

Voldoende weerbaarheid tegen een cyberaanval is cruciaal voor onze samenleving. Denk aan communicatie tussen burger en overheid; maar ook aan de betrouwbaarheid van de IT rondom de vitale processen zoals drinkwater en elektriciteit. Cybercriminelen weten dat. Zij doen er alles aan om dat vertrouwen te schaden door voor eigen gewin misbruik te maken van de IT van de overheid en aanvallen uit te voeren die de maatschappij op steeds grotere schaal ontwrichten.

Digitale weerbaarheid tegen cyberaanvallen is dan ook een belangrijk onderwerp, onder andere in de Nederlandse Cybersecurity Agenda.[4] 'Weerbare digitale processen en een robuuste infrastructuur' vormen een van de zeven ambities die hierin staan omschreven. Maar wat is er nodig voor die '*cyber resilience*'? Onder andere deze vijf punten zijn daarvoor belangrijk:

1. Beter samenwerken aan cyberveiligheid

Aanvallen vinden bijna nooit geïsoleerd plaats. Een aanval op 'organisatie a' is vaak een voorbode van aanvallen op soortgelijke organisaties, en heeft doorgaans ook gevolgen voor partijen waarmee wordt samengewerkt. Door lokaal, nationaal en zelfs internationaal samen te werken en actief informatie te delen, kan iedereen zich beter voorbereiden op wat komen gaat.

Deze samenwerking wordt ook benoemd in het regeerakkoord waarmee Rutte IV aan de slag is gegaan. "We beschermen onze bedrijven, vitale infrastructuur en

1. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report?rtc=1&SilentAuth=1&wa=wsignin1.0
2. https://www.ncsc.nl/onderwerpen/log4j
3. https://tweakers.net/nieuws/190688/gemeentes-almere-en-hof-van-twente-zetten-systemen-preventief-offline-door-log4j.html
4. https://www.ncsc.nl/onderwerpen/nederlandse-cyber-security-agenda

Aksel Dorèl is Head of Digital Security Nederland bij Atos.

economisch kapitaal beter door centraal gecoördineerde structurele samenwerking tussen onder andere het Nationaal Cyber Security Centrum (NCSC), het Digital Trust Center (DTC), overheden, bedrijven en wetenschappers. Zij kunnen sneller en makkelijker informatie delen over digitale kwetsbaarheden en 'hacks'."[5]

Een mooi voorbeeld van samenwerking is de manier waarop onder andere spoorwegbedrijven zich in Europees verband hebben verenigd in een Information Sharing and Analysis Center (ISAC).[6] Hier wordt sectorspecifieke informatie over incidenten, bedreigingen en risico's op een internationaal niveau met elkaar gedeeld. Die internationale benadering is belangrijk, omdat cybercriminaliteit ook internationaal is georganiseerd.

Het hebben van een samenwerkingsverband opent ook weer deuren. Zo is het de ambitie van het NCSC en het DTC om samenwerkingsverbanden met dezelfde uitdaging met elkaar te verbinden. Op die manier kan relevante informatie uit de ene sector snel en efficiënt worden gedeeld met de andere sector.

2. Meer aandacht voor detectie

Cybercriminelen slagen er na een digitale inbraak in om soms maanden onder de radar te blijven. Tijd genoeg om het netwerk in kaart te brengen en de waardevolle data naar buiten te sluizen. Of om in alle rust malware te installeren. Zo is de vrees dat we de komende maanden nog de gevolgen gaan zien van het Log4Shell-lek, op het moment dat indringers na een verkenningsperiode tot actie overgaan.

Een vroegtijdige detectie van een digitale inbraak is cruciaal, zodat hierop kan worden gereageerd met tegenmaatregelen. Managed Detection and Response (MDR) kan hier bijvoorbeeld bij helpen. Maar een snelle detectie kan alleen als er een goed beeld is van de aanwezige assets en de kwetsbaarheden daarin. Als je niet weet wat je hebt, weet je ook niet wat je moet beschermen. Voor een effectieve detectie zijn asset management en vulnerability management onmisbaar.

Detectie gaat bovendien verder dan het vroegtijdig signaleren van een initiële digitale inbraak. De focus moet ook liggen op het signaleren van door- en uitbraken. Een crimineel – eenmaal binnen – zal pogen onder de radar van de monitoring te blijven en tegelijkertijd door te breken door hoge privileges op het netwerk of systeem te verkrijgen. Detectie moet daarom nog fijnmaziger worden ingeregeld, met focus op doorbraak.

3. Security automatiseren

De dreiging van cybercriminelen neemt toe. Dat komt onder andere door het groeiende aanvalsoppervlak. Steeds meer zaken worden digitaal afgehandeld, waardoor cybercriminelen meer mogelijkheden krijgen om een organisatie aan te vallen. Maar ze krijgen daarbij ook de hulp van kunstmatige intelligentie (AI) en machine learning. Cybercriminelen hebben niet alleen onbeperkt de tijd en geld, maar scannen nu ook met 'zelflerende' tools het internet zonder dat ze daarbij zelf fouten kunnen maken.

Om niet achterop te raken, zal ook de verdediging de stap moeten zetten naar AI en machine learning. Bijvoorbeeld door het in kaart brengen van de assets en het signaleren van kwetsbaarheden op bekende assets volledig te automatiseren. Maar denk ook aan het signaleren en automatisch afslaan van verdachte situaties. De onderschepping van een phishingmail leidt dan automatisch tot het verwijderen van dezelfde mail uit alle mailboxen en een update van de firewallregels, en dat het liefst voor meerdere organisaties tegelijk. En dat allemaal 'onzichtbaar' voor de gebruikers. Security Orchestration, Automation & Response (SOAR)-tooling is een stap in die richting.

4. Focus op herstel

In een beveiligingsbeleid gaat meestal veel aandacht uit naar het voorkomen en detecteren van beveiligingsincidenten, en naar incident-respons. Doorgaans is er minder aandacht voor het herstel na een incident, zoals een gijzeling van data door *ransomware*. Terwijl iedere organisatie vroeg of laat slachtoffer zal zijn van een cyberaanval.

Hoeveel beschermende maatregelen een organisatie ook treft, het gaat een keer mis. '*Assume breach*.' Accepteer dat hackers altijd toe kunnen slaan, en zorg dat de organisatie in staat is om snel van een aanval te herstellen. Want ook dan telt iedere seconde.

In een herstelplan moet onder andere aandacht zijn voor het maken en regelmatig testen van de back-ups en het snel kunnen terugzetten van de data, voor de (telefonische) bereikbaarheid tijdens een aanval en voor de verdeling van de taken. Wie neemt contact op met leveranciers, wie zet de back-ups terug en wie staat klanten te woord? En hoe lang duurt het voordat een systeem weer up and running is? En welke systemen krijgen prioriteit? Het zijn slecht enkele punten die naar voren moeten komen in een Business Continuity Plan. Zorg er ook voor dat dat plan is in te zien als de IT niet beschikbaar is. Een ouderwets en tijdig gemaakt printje kan dan uitkomst bieden.

5. Urgentie creëren

Security is niet vrijblijvend. Zo stelt de Baseline Informatiebeveiliging Overheid (BIO) het maken van back-ups, bescherming tegen *malware* en het patchen van kwetsbaarheden verplicht. In het geval van als kritiek gekwalificeerde kwetsbaarheden worden patches 'zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd'. "In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen", zo staat in de BIO.[7]

Amerikaanse (federale) overheidsinstanties hebben te maken met een vergelijkbare verplichting. In november 2021 vaardigde het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) een 'verplichte instructie' uit, de 'Binding Operational Directive (BOD) 22-01, Reducing the Significant Risk of Known Exploited Vulnerabilities'. Volgens deze richtlijn moeten federale overheidsinstanties ernstige kwetsbaarheden binnen twee weken patchen. CISA houdt als onderdeel van de directive een catalogus bij met bekende kwetsbaarheden.[8]

Op de naleving van geldende verplichtingen mag best enige druk worden uitgeoefend. Zoals de Amerikaanse toezichthouder *Federal Trade Commission (FTC)* onlangs deed op bedrijven die onvoldoende haast maken met het dichten van de Log4j-kwetsbaarheid. De bijna agressieve waarschuwing van de Federal Trade Commision (FTC) was duidelijk: "The FTC intends to use its full legal authority to pursue companies that fail to take reasonable steps to protect consumer data from exposure as a result of Log4j, or similar known vulnerabilities in the future."[9]

5. https://www.kabinetsformatie2021.nl/documenten/publicaties/2021/12/15/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst
6. https://www.isacs.eu/european-isacs
7. https://www.bio-overheid.nl/media/1572/bio-versie-104zv_def.pdf
8. https://www.cisa.gov/news/2021/11/03/cisa-releases-directive-reducing-significant-risk-known-exploited-vulnerabilities
9. https://www.ftc.gov/news-events/blogs/techftc/2022/01/ftc-warns-companies-remediate-log4j-security-vulnerability

Het nieuwe potentieel van virtuele dimensies

Ontdek onze visie in Journey 2026

We denken dat we de wereld waarin we leven goed begrijpen. Maar de realiteit is dat een groot deel van de wereld nog onontdekt is. Zoals de ruimte, 90% van onze hersenen of 80% van de gegevens die we produceren.

De Atos Scientific Community stelt in hun nieuwe research en thought leadership dat "het ontsluiten van virtuele dimensies" potentieel biedt om de vele mogelijkheden van deze oneindige wereld te blijven realiseren.

Daarbij is het van essentieel belang om de overbrugging van de fysieke/digitale kloof veilig te beheren. Met name door de opkomst van autonome AI-cyberaanvallen.

Verken deze nieuwe publicatie
Journey 2026 – Unlocking virtual dimensions
(engelse publicatie)

GOV19
Atos