Nationaal Coördinator Terrorismebestrijding en Veiligheid Pieter-Jaap Aalbersberg

‘Oefenen, oefenen en nog eens oefenen!’

Als Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) bij het ministerie van Justitie en Veiligheid is Pieter-Jaap Aalbersberg sinds 1 februari 2019 verantwoordelijk voor onder andere cybersecurity. Omdat dit onderwerp hoog op de agenda staat bij de drinkwaterbedrijven, stellen wij hem enkele vragen over de weerbaarheid van de vitale sectoren en de toenemende digitale dreigingen voor de drinkwatersector. ‘Vooral oefenen is essentieel.’

Volgens de NCTV neemt de dreiging in het algemeen toe, met name op de aandachtsvelden cybercrime, statelijke actoren en samenhang ICT-systemen. Aalbersberg: 'Meer specifiek voor de drinkwatersector bestaat er een aanzienlijk risico op cybercriminaliteit en is er belangstelling vanuit statelijke actoren. Dit komt door het karakter van de drinkwatervoorziening als vitaal proces. Het is dus van groot belang om binnen je sector na te gaan of de bescherming tegen ongewenste zaken van buitenaf (nog) op orde is, zodat je niet achter de feiten aanloopt.'

'Jaarlijks brengen wij als NCTV met onze partners binnen de overheid, de wetenschap en het bedrijfsleven het Cybersecuritybeeld Nederland uit (het CSBN). Daarin duidt de Nationaal Coördinator de meest recente ontwikkelingen en dreigingen op de digitale veiligheid van Nederland. Uit het laatste dreigingsbeeld van juni dit jaar blijkt wederom dat de digitale dreiging van landen in de vorm van spionage en sabotage een permanente dreiging vormen voor onze nationale veiligheid.'

Dreiging neemt toe

Aalbersberg kijkt breder dan alleen het versterkingsprogramma vitale infrastructuur dat het kabinet medio 2019 aankondigde. Hij vertelt: 'In 2019 was de titel van het Cybersecuritybeeld nog 'Ontwrichting ligt op de loer'. Dit jaar was onze toon al wat alarmerender: 'Cyberincidenten kunnen de gehele Nederlandse maatschappij verlammen'.' De reden hiervoor is volgens Aalbersberg dat elk jaar de dreiging toeneemt en onze weerbaarheid achterblijft. Daarom benadrukt hij dat de weerbaarheid omhoog moet: 'Bij de rijksoverheid, de provincies en de gemeenten, bij de vitale aanbieders, maar ook bij het mkb en de grotere bedrijven… en de burgers zelf.'

Prioriteiten in versterkingsprogramma

Volgens Aalbersberg is het belangrijk prioriteiten te stellen. 'Ik zie nog te veel sectoren ICT-vernieuwingen doorvoeren zonder iets aan cybersecurity te doen. Bij veel bedrijven is er niet 24/7 een ICT-afdeling aanwezig. Maar je moet altijd meteen kunnen ingrijpen als er van buitenaf een datastroom binnenkomt die verstrekkende gevolgen kan hebben, zoals het stilleggen van je hele systeem. Dat is de realiteit in de wereld van nu en daarop moeten we voorbereid zijn.'

'Onder onze aanpak van cybersecurity hangt een versterkingsprogramma, inclusief een cybersecurity-agenda. Onze overheid, de regering en de minister zijn steeds bezig met het zetten van stappen om Nederland weerbaarder te maken. Ook hier is de grote uitdaging dat zaken niet meer op zichzelf staan, maar dat alles met elkaar samenhangt.'

Investeren in techniek en organisatie

Het versterkingsprogramma roept iedereen op om de boel op orde te hebben en dat houdt primair in dat sectoren zelf moeten investeren. 'Dat kan gebeuren met ondersteuning door het Nationaal Cyber Security Centrum (NCSC) in Den Haag. Om te kunnen vaststellen wat nu precies de dreiging is, moet je heel 'eenvoudig' weten waar alles zit. Dus niet alleen alle hoofdsystemen, maar ook alle kleine systemen. Tegenwoordig zit de kwetsbaarheid vaak niet in de grote, goed beveiligde computersystemen op het hoofdkantoor, maar in een kleine server met een router ergens ver weg. Dan gaat het om vragen zoals: is alle onderhoud up-to-date? Weet iedereen wat hij of zij moet doen? Zijn alle processen goed? Als het niet op orde is, investeer dan. Maar kijk ook verder. Zoals: heb je de juiste leveranciers? Dit betekent natuurlijk ook iets voor de drinkwatersector. Ik ben van mening dat de vitale sectoren, inclusief de drinkwaterbedrijven, al goed meedoen. Maar mijn boodschap is wel: blijf alert!'

Cyberweerbaarheid: trusted channels

De Cyber Security Raad heeft in een recent rapport over cyberweerbaarheid de ministers van Justitie en Veiligheid (JenV) en Binnenlandse Zaken en Koninkrijksrelaties (BZK) geadviseerd om binnen één jaar in samenwerking met de vitale sectoren zogeheten 'trusted channels' te realiseren. De drinkwatersector pleit hier al langere tijd voor. Met het oog op de toenemende digitale dreiging moet de overheid de vitale sectoren tijdig voorzien van inlichtingeninformatie inclusief handelingsperspectief om de juiste maatregelen te kunnen treffen en te rechtvaardigen. *Neemt u dit advies over?*

Aalbersberg: 'Het versterkingsprogramma vitale infrastructuur houdt in dat het NCSC informatie deelt met alle sectoren, zowel op het gebied van risico als van dreiging. Dat is een belangrijke rol van de overheid. De NCTV en het Veiligheidsloket voorzien het NCSC 24/7 van informatie, dat het vervolgens doorzet naar de vitale sectoren. Wij willen de vitale sectoren zo snel mogelijk waarschuwen, zodat iedere sector zelf maatregelen kan treffen bij risico's en dreigingen.'

'Op dit moment werken we intensief samen met de telecombedrijven aan de introductie van 5G, waarbij we ook kijken naar de actuele technische ontwikkelingen binnen de cybersecurity. Wat zijn de risicodreigingen? Daarbij maken we steeds de afweging: wat doen we juist wel en wat niet? Deze ontwikkeling is van belang voor hoe we dat straks met de overige vitale sectoren verder gaan aanpakken. Dit zit heel erg in de richting van 'trusted channels'. Daarbij wordt de supply chain ook steeds belangrijker. Samen met alle sectoren ontwikkelen we momenteel een versterkte aanpak ter bescherming van de vitale infrastructuur.'

Bevoegdheidsverdeling

Onderdeel van de versterkte aanpak is onderzoek naar bevoegdheden van de overheid om bij cybersecurity gerelateerde crises in te grijpen. *Tot waar reikt volgens u de verantwoordelijkheid van de vitale sector en waar start die van de overheid?*

Aalbersberg: 'Minister van JenV Grapperhaus heeft aangekondigd dat hij hiernaar wil kijken. Primair zijn de vitale sectoren zelf verantwoordelijk, dus ook de drinkwatersector is eerst zelf aan zet. Maar men kan daarin natuurlijk wel samenwerken met de overheid. Die staat daar ook positief tegenover.'

‘Mocht het echt nodig zijn, dan moet de overheid in het belang van de burgers wel middelen hebben om te kunnen ingrijpen. Stel dat er onvoldoende maatregelen worden genomen, dan is de vraag: is er een vorm van doorzettingsmacht nodig, als laatste redmiddel? We kijken momenteel naar hoe we deze doorzettingsmacht kunnen verankeren. Want onze samenleving moet voorbereid zijn op cyberbedreigingen. De doorzettingsmacht is niet gebaseerd op puur van bovenaf ‘ingrijpen’. Het gaat erom de sectoren het zelf te laten doen, ze erop aan te spreken, ze zo sterk mogelijk te laten zijn en daarop aan te sluiten.’

Governance van digitale veiligheid

De Onderzoeksraad voor Veiligheid (OVV) start een onderzoek naar de governance van digitale veiligheid in Nederland. *Hoe verhoudt dit zich tot uw onderzoek naar bevoegdheden van de overheid om bij cybersecurity gerelateerde crises in te grijpen?*

Aalbersberg: ‘De OVV heeft aangekondigd een onderzoek te doen naar de Citrix-casus van begin dit jaar. En daarin vooral te kijken naar de rol van de overheid: hoe heeft zij hierin gehandeld, hoe zijn de betrokken partijen ermee omgegaan? Dat is voor ons belangrijk, zo leren wij wat er beter kan. Maar het is vooral een onderzoek naar deze specifieke casus, geen breed onderzoek naar digitale veiligheid.’

‘Daarnaast zijn wij als NCTV bezig met een verkenning van de wettelijke bevoegdheid van het NCSC tot het delen van informatie met andere partijen zoals niet-vitale organisaties. Op deze manier werken we verder aan een landelijk dekkend stelsel, waarbij bedrijven en organisaties kunnen beschikken over de juiste informatie om hun eigen verantwoordelijkheid te kunnen nemen in het digitaal veilig maken van hun systemen.’

Dat zijn allemaal stappen die eraan bijdragen om ons land veilig te houden bij een digitale bedreiging. Juist naar aanleiding van de Citrix-casus is het belangrijk dat we externe onafhankelijke partijen onderzoek laten doen om daarvan te leren. Dit soort crises zijn niet eenmalig. Ze zullen vaker voorkomen en iedere crisis kan en moet belangrijke informatie opleveren voor verbetering.’

Belang van voorbereiding

In de kabinetsreactie op het rapport ‘Voorbereiden op digitale ontwrichting’ van de Wetenschappelijke Raad voor het Regeringsbeleid

staat dat oefenen één van de belangrijkste maatregelen is om ons voor te bereiden op incidenten. *Wat is de stand van zaken van het opzetten van een breed publiek-privaat oefenprogramma?*

Aalbersberg: 'Het onderwerp 'voorbereiding' moet prioriteit blijven houden bij de raden van commissarissen van de drinkwaterbedrijven. Daarnaast moet je een heel goed crisisplan hebben en tot slot is het adagium 'oefenen, oefenen en nog eens oefenen!'. Soms is dat alleen oefenen op het gebied van ICT. Maar stel dat alle bedieningen van pompstations opeens worden geblokkeerd. Krijg je het dan snel voor elkaar dat alles weer loopt zoals het moet? Weerbaar zijn betekent dat je je beveiligingsniveau op orde hebt, maar ook dat je een eventuele breuk of verstoring snel opmerkt en maatregelen voorhanden hebt om de continuïteit te borgen.'

'Je kunt nog zulke goede plannen hebben, maar tijdens een praktijkoefening zie je vaak dat niet iedereen alles even scherp op zijn netvlies heeft staan. Dan bedoel ik ook iedereen, op alle organisatieniveaus: van medewerkers op de werkvloer tot aan de raad van bestuur. Je test meteen of je crisisplan nog op orde is. Ook daarom is oefenen zo belangrijk.'

ISIDOOR-oefening

'Op rijksniveau kennen we de ISIDOOR-oefening, een driedaagse cross-sectorale oefening waaraan publieke en private partners meedoen. Het doel van de oefening is de gezamenlijke aanpak, samenwerking en coördinatie bij een cybercrisis testen.' Deelnemers zijn afkomstig uit verschillende sectoren zoals: drinkwater, energiedistributie, haven, nucleair, chemie en telecom. Ook verschillende ministeries oefenen mee met deze verschillende gesimuleerde cyberincidenten. 'Zo'n grote oefening, over sectoren heen, moet ook op Europees niveau gebeuren, omdat een grote internet- of energie-uitval zich vaak niet beperkt tot één land.'

'Vanwege de coronapandemie zijn verschillende geplande oefeningen tussen het Rijk en de vitale sector verschoven naar volgend jaar. De ISIDOOR-oefening, waarbij het Rijk en vitale organisaties samen oefenen, is daarvan de meest in het oog springende.'

'Voor wat betreft (stress)testen bevinden we ons op dit moment in een verkennende fase, waarbij eerst uitgevraagd en geïnventariseerd wordt wat op dit moment al daaraan raakt. Hierna kijken we naar de verdere behoeften en noodzaak voor security (stress)testing binnen het Rijk en de vitale sector.'

Toeleveranciers

In de versterkte aanpak is veel aandacht voor toeleveranciers van vitale sectoren. De drinkwatersector pleit voor certificering van IACS-systemen (Industrial Automation & Control Systems). Dit zijn meet- en regelsystemen die worden gebruikt voor de aansturing van primaire processen binnen de vitale infrastructuur zoals onder andere bij de drinkwatervoorziening. Hierbij zou gekeken moeten worden naar voorwaarden rondom het updaten van producten en de betrouwbaarheid van de leverancier zelf. Gezien het internationale karakter van de meeste leveranciers zou certificering op Europees niveau moeten plaatsvinden. *Hoe staat u hier tegenover?*

Aalbersberg: 'Het draait hier niet alleen om een certificering. In een klassiek productieproces kon je zelf veel sturen. Maar tegenwoordig

EPCIP-richtlijn (Europese richtlijn tot bescherming van de kritieke infrastructuur):

In 2019 is de EPCIP-richtlijn geëvalueerd. Hieruit kwam naar voren dat deze weinig zou hebben bijgedragen aan de bescherming van Europese kritieke infrastructuur. Eén van de oorzaken zou zijn dat de scope van de richtlijn te beperkt is, waardoor deze op slechts een aantal sectoren van toepassing is. In opdracht van de Europese Commissie wordt een haalbaarheidsstudie uitgevoerd naar mogelijke oplossingen voor het verder versterken van de bescherming van kritieke infra in de EU. Vewin houdt vast aan het eerdere standpunt, namelijk dat de Nederlandse drinkwatervoorziening geen onderdeel is of moet worden van de Europese kritieke infrastructuur. Uitval van drinkwater in Nederland heeft namelijk géén grensoverschrijdende impact. De huidige sectorale wetgeving en beleid, aangevuld met de Wet beveiliging netwerk- en informatiesystemen bni (afgeleid van de Europese NIS-richtlijn), bieden een volledig kader voor bescherming van de Nederlandse drinkwatervoorziening. Wel zou meer ingezet kunnen worden op uitwisseling van ervaringen tussen lidstaten en sectoren, en op onderzoek naar de afhankelijkheden van toeleveranciers.

Standpunt van Vewin is: Houd de Nederlandse drinkwatervoorziening buiten de Europese kritieke infrastructuur en de scope van de EPCIP-richtlijn.

NIS-richtlijn (Europese richtlijn voor netwerk- en informatiebeveiliging):

De NIS-richtlijn is in Nederland via de Wet beveiliging netwerk- en informatiesystemen (Wbni) geïmplementeerd. Hiermee hebben 'aanbieders van essentiële diensten' (AED's, waaronder de tien Nederlandse drinkwaterbedrijven) een meldplicht voor ICT-incidenten gekregen (een meldplicht aan de toezichthouder en het NCSC, het Nationaal Cyber Security Centrum van de NCTV), alsook een aantoonbare zorgplicht voor de beveiliging van hun netwerk- en informatiesystemen. De richtlijn wordt in opdracht van de Europese Commissie geëvalueerd. De lidstaten zouden de richtlijn op een té verschillende wijze hebben geïmplementeerd (lidstaten zouden verschillende methoden hebben voor de identificatie van AED's, voor het vaststellen van wanneer exact incidenten gemeld moeten worden, etc.).

Standpunt van Vewin is: Geen aanvullende wet- en regelgeving vanuit Europa; invulling van de meld- en zorgplicht is een nationale aangelegenheid, gebaseerd op het risicoprofiel en de impact van uitval van de vitale voorziening. Wel zouden met het oog op meer harmonisatie op Europees niveau uitgangspunten kunnen worden opgesteld voor de identificatie van AED's en voor de drempelwaarde van de meldplicht.

opereren veel organisaties in een geïntegreerde supply chain met leveranciers en subleveranciers. Dan moet je verder kijken dan je eigen bedrijf. Wees je ervan bewust dat je kritische schakels net zo goed in de supply chain kunnen zitten, denk bijvoorbeeld aan onderhoudsleveranciers. Als vitale sector ben je daar net zo verantwoordelijk voor, als voor je eigen gebouw.'

'Soms helpt certificering daarin, maar het draait om veel meer. Het gaat bijvoorbeeld ook om je oefenprogramma blijven controleren, oefenen met je supply chain en het blijven checken van de bedrijven in de supply chain. Hoort hij er nog bij of niet? Dit doe je samen met de overheid als partner. Het betekent ook kritisch blijven kijken naar de ontwikkelingen van de technologie. Hoe is het gesteld met cybersecurity? Dat is misschien wat wennen voor bepaalde sectoren, want daarmee kijk je ook kritisch naar de producten in de supply chain. Soms helpt certificering daarbij. Maar dit is maar één element en nooit het enige element. Want ook met certificering zul je scherp moeten blijven.'

Europese regelgeving

Ook op dit gebied is regelgeving vanuit Brussel belangrijk voor Nederland. *Met welke ontwikkelingen in Europa moet rekening worden gehouden? Wat is het Nederlandse standpunt ten aanzien van de reviews van de EPCIP- en NIS-richtlijnen?*

Aalbersberg: 'Voor de digitale weerbaarheid van onze vitale sectoren is het belangrijk om op Europees vlak samen te werken. Bijvoorbeeld op het gebied van ontwikkeling en innovatie, kennisdeling en gezamenlijk oefenen. Omdat cybersecurity niet ophoudt bij landsgrenzen, moeten we alert blijven op wat er elders in Europa gebeurt. Ook hier helpen Europese richtlijnen.'

'De NIS-richtlijn heeft ons echt wat gebracht qua prioritering en samenwerking op het gebied van cybersecurity. We zullen in ons land de boel goed op orde moeten hebben. Als eerste binnen de rijksoverheid en de vitale sectoren. Maar we moeten ook de standaards beter krijgen. Bij een review van de richtlijn kijken we hoe we de digitale weerbaarheid verder kunnen verhogen.'

'Op dit moment wordt gewerkt aan het in kaart brengen van de huidige wettelijke taken en bevoegdheden die het mogelijk maken informatie te delen of in het uiterste geval in te grijpen dan wel te sturen op de digitale veiligheid bij overheid, vitale en niet-vitale organisaties. Deze verkenning moet in januari 2021 af zijn en de uitkomsten zullen worden betrokken bij de wijziging van de Wbni.'

Waakzaam, maar optimistisch

Ondanks alle risico's en dreigingen die continu op de loer liggen, blijft Aalbersberg positief gestemd. 'Vergeleken met Europa zijn we in Nederland al heel ver op het gebied van technologie. Daarom willen hackers onze systemen ook wel eens 'uitproberen'. Dat heeft als positief gevolg dat wij nu best ver zijn op het gebied van cybersecurity. Wij zijn er toch om de vinger op de zere plek te leggen. Hoewel de dreiging toeneemt en de weerbaarheid in het algemeen binnen ons land wat achterblijft, lopen multinationals en vitale sectoren daarin weer wat voorop. Maar zo langzamerhand zijn we ook allemaal afhankelijk van de zwakste schakel ergens anders. Dus we hebben een collectieve verantwoordelijkheid om dit onderwerp hoog op de agenda te houden.'

Terminologie NCTV

Cybercrime; criminaliteit met als doelwit en middel ICT. Denk aan manipulatie van computerchips in bedrijfssystemen, bankpassen en mobiele telefonie. Op deze manier willen criminelen geld verdienen en kunnen dat internationaal heel makkelijk. Binnen cybercrime zijn geen grenzen.

Statelijke actoren; andere landen ontplooien offensieve activiteiten met als doel economische spionage of het veroorzaken van verstoringen. Waar het bij cybercrime om geld draait, zijn statelijke actoren er vooral in geïnteresseerd netwerken in handen te krijgen om deze te kunnen manipuleren.

Samenhang ICT-systemen; de meeste systemen zijn niet meer individueel of 'standalone', maar hangen nauw samen met andere componenten van een netwerk of organisatie. Daardoor kunnen hele bedrijven plat komen te liggen wanneer er zich een kleine storing in een deelsysteem voordoet. Door deze integratie en de grote mate van afhankelijkheid van ICT zijn bedrijven en sectoren steeds kwetsbaarder. Om deze reden is in het onlangs geschreven Cybersecuritybeeld de term 'ontwrichting' nu veranderd naar 'verlamming'.