Patricia Zorko, directeur Cyber Security, ministerie van VenJ

# ‘Samenwerking bij cyber-security van vitaal belang’

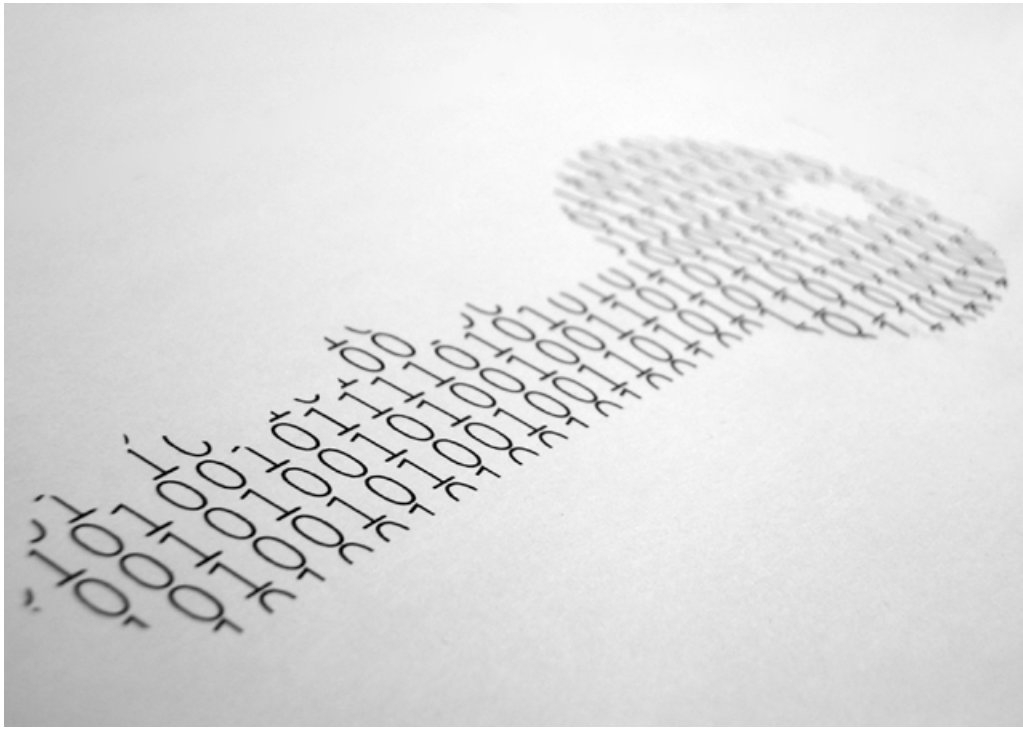
Afgelopen september is het Cybersecuritybeeld Nederland 2016 verschenen. Deze rapportage geeft inzicht in de belangen, dreigingen en ontwikkelingen op het gebied van cybersecurity. Als onderdeel van de vitale infrastructuur moet ook de drinkwatersector alert zijn op dreigingen op dit vlak. Directeur Cyber Security Patricia Zorko van het ministerie van Veiligheid en Justitie (VenJ) over enkele actuele veiligheidsdossiers. ‘Diensten en processen die belangrijk zijn voor ons dagelijks functioneren, worden verstoord en gesaboteerd.’

Beroepscriminelen organiseren zich steeds beter en maken gebruik van geavanceerde digitale aanvalsmethoden. Het afgelopen jaar vonden verschillende grootschalige aanvallen plaats met een hoge organisatiegraad, gericht op diefstal van geld en kostbare informatie. Naast de overheid waren bedrijven en burgers hiervan in toenemende mate het slachtoffer. Beroepscriminelen vormen daarmee een steeds grotere bedreiging voor de digitale veiligheid in Nederland.

Dat blijkt uit het Cybersecuritybeeld Nederland 2016 (CSBN 2016), gepubliceerd door het Nationaal Cyber Security Centrum van het ministerie van VenJ. Dit rapport wordt samengesteld in nauwe samenwerking met publieke en private partijen. Het bevat een feitelijke beschrijving op basis van inzicht en expertise vanuit overheidsdiensten, vitale sectoren en wetenschap. Voordat Patricia Zorko plaatsvervangend Nationaal Coördinator Terrorismebestrijding en Veiligheid en directeur Cyber Security werd, werkte ze onder andere bij de politie als kwartiermaker en als politiechef van de Landelijke Eenheid. In haar streven naar meer veiligheid in Nederland en in internationaal verband heeft zij zich vooral de laatste jaren verdiept in vraagstukken rond cybersecurity en gewelddadig jihadisme, precies de vraagstukken waarvoor zij in haar huidige functie verantwoordelijk is.

*Kunt u aangeven wat momenteel de grootste dreigingen voor de vitale sectoren in Nederland zijn?*
Zorko: 'Het rapport schetst een zorgelijk beeld van de veiligheidssituatie in het digitale domein. Er is sprake van toenemende en reële cyberdreigingen. Daarbij gaat het niet alleen om het ontvreemden van geld en kostbare commerciële informatie door cybercriminelen die steeds gewiekster opereren. Ook diensten en processen die belangrijk zijn voor ons dagelijks functioneren, worden verstoord en gesaboteerd. Er is sprake van spionage door andere landen, wat het verdienmodel van de Nederlandse economie kan ondermijnen.'

*Welke acties onderneemt de NCTV hierop, al dan niet samen met vitale sectoren?*
Zorko: 'Gelukkig hebben zowel de overheid als de bedrijven uit de vitale infrastructuur de afgelopen jaren niet stilgezeten. Met de acties uit de tweede Nationale Cyber Security Strategie hebben we veel bereikt. We hebben de BV Nederland de kennis, kunde en capaciteiten gegeven om op dit moment nog in de digitale voorhoede te blijven opereren.'



'Maar we kunnen het ons niet permitteren om stil te zitten. We moeten de komende jaren blijven investeren en ons blijven ontwikkelen. Juist in de samenwerking met de vitale infrastructuur zie ik daarin mooie voorbeelden. Denk bijvoorbeeld aan de opbouw en uitbouw van het Nationaal Detectie Netwerk, of publiek-private pilots om het cyber-ecosysteem in onze mainports Schiphol en Rotterdam te versterken, maar zeker ook het recent in de Tweede Kamer aangenomen wetsvoorstel gegevensverwerking en meldplicht cybersecurity om de samenwerking te versterken.'

## Wettelijke meldplicht ICT-inbreuken

Op 27 oktober jl. is het Wetsvoorstel gegevensverwerking en meldplicht cybersecurity door de Tweede Kamer aangenomen. De drinkwaterbedrijven, als zijnde vitale aanbieder, krijgen hiermee een wettelijk verplichte meldplicht voor ICT-inbreuken die (mogelijk) een grote impact hebben op de continuïteit van de vitale dienst. Melding vindt plaats bij het NCSC. *Kunt u aangeven wat de achtergrond van het wetsvoorstel is?*
Zorko: 'Laat ik vooropstellen dat het door de Tweede Kamer aangenomen wetsvoorstel breder is dan alleen een meldplicht. Wat mij betreft draait het veel meer om publiek-private samenwerking en biedt het daarvoor ook de randvoorwaarden. Bij het opstellen van dit wetsvoorstel hebben we veel en constructief contact gehad met vertegenwoordigers uit de vitale infrastructuur en dat heeft ons enorm geholpen. Ik ben Vewin en de drinkwaterbedrijven daar dan ook zeer erkentelijk voor.'

*Hoe zal worden omgegaan met vertrouwelijke gegevens die vitale aanbieders verstrekken aan de overheid (NCSC)?*
Zorko: 'Het wetsvoorstel schept de kaders voor informatie-uitwisseling, maar biedt ook belangrijke spelregels rondom vertrouwelijkheid. Gevoelige informatie die herleidbaar is tot een aanbieder, blijft met het wetsvoorstel ook vertrouwelijk. Op die manier willen we schroom om incidenten te melden wegnemen om zo ook de lessen

'MISDAAD VERSCHUIFT STEEDS MEER VAN OFFLINE NAAR ONLINE'

**Richtlijn voor Netwerk- en Informatiebeveiliging (NIB-richtlijn)**
Op 6 juli jl. heeft het Europees Parlement ingestemd met de Europese NIB-richtlijn, die gericht is op het creëren van een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen Europa. Lidstaten hebben 21 maanden om de richtlijn om te zetten in nationale wetgeving.

Het is al bekend dat de richtlijn voor de Nederlandse drinkwaterbedrijven gaat gelden. Hiermee krijgen de drinkwaterbedrijven een meldplicht voor ICT-inbreuken die een significante impact hebben op de continuïteit van de dienstverlening. Daarnaast krijgen ze een zorgplicht. Bedrijven moeten passende technische en organisatorische maatregelen treffen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen en om de gevolgen van incidenten te voorkomen of te minimaliseren. De zorgplicht moet ook aangetoond worden richting de toezichthouder, door bijvoorbeeld verstrekking van de resultaten van een beveiligingsaudit.

Inzet van Vewin is dat de NIB-richtlijn wordt geïmplementeerd via aanpassing van de drinkwaterregelgeving. In de Drinkwaterwet en het Drinkwaterbesluit is al veel geregeld rondom de voorbereiding en respons op verstoringen inclusief het toezicht hierop, uitgevoerd door de ILT. Door aan te sluiten bij de drinkwaterregelgeving blijven de verantwoordelijkheden helder en eenduidig; versnippering in wetgeving moet worden voorkomen.

Een ander belangrijk argument is dat in de Drinkwaterwet al is geregeld dat informatie die betrekking heeft op de voorbereiding of respons op verstoringen, niet opvraagbaar is op basis van de Wet openbaarheid van bestuur (Wob). Dit is van groot belang met het oog op de beveiligingsaudits die bedrijven straks aan de ILT moeten overleggen en de gevoeligheid van deze informatie. Tot slot pleit Vewin ervoor dat de afbakening van de meldplicht uit de NIB-richtlijn overeenkomt met de meldplicht uit het Wetsvoorstel gegevensverwerking en meldplicht cybersecurity.

die te trekken zijn uit een incident bij aanbieder A te gebruiken om de veiligheid van aanbieder B of C te verhogen. Zo maken we Nederland digitaal samen veilig.'

## Europese richtlijn

In juli jl. heeft het Europees Parlement de richtlijn voor Netwerk- en Informatiebeveiliging (NIB) aangenomen. Deze moet in mei 2018 in Nederlandse wetgeving zijn geïmplementeerd. De NIB-richtlijn omvat een meldplicht en zorgplicht voor vitale aanbieders, waaronder de drinkwaterbedrijven. Inzet van Vewin is dat de meldplicht aansluit bij bovenstaande meldplicht en dat toezicht en handhaving bij de sectorale toezichthouder, de ILT, blijft. *Hoe beziet u dit vraagstuk?*

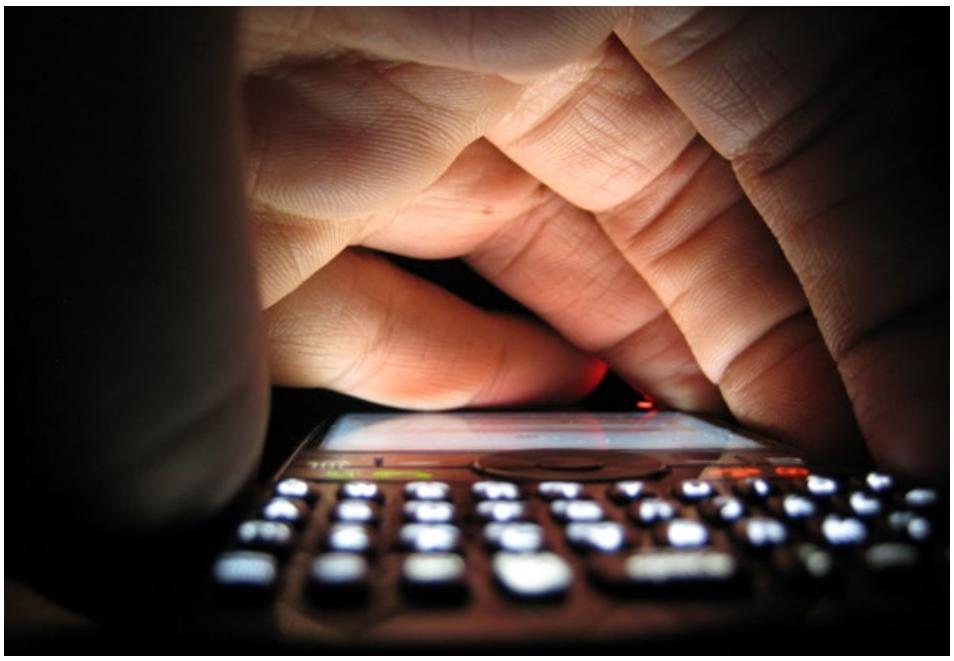
Zorko: 'Cybersecurity is van nature grensoverschrijdend, dus daarbij is het zeker van belang dat er op Europees niveau wordt gewerkt aan het verhogen van de digitale veiligheid. De afgelopen jaren hebben we dan ook veel tijd en energie gestoken in de onderhandelingen over deze richtlijn. Nu de richtlijn is aangenomen, moeten we samen met de vakdepartementen gaan bezien hoe we deze richtlijn in Nederland kunnen implementeren.'

*Wat zou dit vergen van (sectorale) toezichthouders?*
Zorko: 'Dat is nog geen eenvoudige opgave, aangezien er aanzienlijke verschillen zijn tussen de lidstaten en omdat de sectoren die in de richtlijn genoemd worden, verschillende juridische kaders kennen. Immers, de wetgeving die van toepassing is op de drinkwatersector, is niet dezelfde als die voor bijvoorbeeld de energiebedrijven. Wat mij betreft moeten we dus gaan zoeken naar een implementatievorm die past bij de vitale infrastructuur zoals we die kennen. Ook mogen de administratieve lasten niet onnodig hoog worden. Daarbij is het van belang dat toezicht op cybersecurity-verplichtingen aansluit bij bestaande fysieke verplichtingen. Cybersecurity moet in mijn ogen 'mainstream' worden. Dat vraagt niet alleen iets van toezichthouders, maar eigenlijk van iedereen.'

## Zorgplicht

Op basis van de NIB-richtlijn moeten bedrijven passende maatregelen nemen om de risico's voor de beveiliging van hun netwerken informatiesystemen te beheersen. Deze zogenoemde zorgplicht moeten ze ook aantoonbaar kunnen maken, door bijvoorbeeld het overleggen van auditrapportages.

*Hoe gaan VenJ en de overheid als geheel ervoor zorgen dat deze informatie niet openbaar wordt op basis van de Wob, gezien het feit dat het hier*



*om vertrouwelijke en gevoelige informatie gaat?*
Zorko: 'De implementatie van de NIB-richtlijn is nog 'work in progress'. De komende maanden werken we aan een wetsvoorstel dat in consultatie zal worden gebracht. In de uitwerking daarvan moeten we naar dit soort onderwerpen kijken. Ook hierbij geldt voor mij, dat we moeten zoeken naar een evenwicht tussen veiligheid en administratieve lasten. Ik wil daarbij zeker voortbouwen op het fundament dat we hebben gelegd met het wetsvoorstel Gegevensverwerking en meldplicht cybersecurity, en de randvoorwaarden voor vertrouwelijkheid en publiek-private samenwerking die dit biedt.'

## Kwetsbaarheid in kaart

De toenemende afhankelijkheid van ICT maakt onze samenleving steeds kwetsbaarder voor misbruik en uitval. De cybersecurity van ketens van vitale processen is essentieel voor de continuïteit van deze processen. Om de weerbaarheid ervan te verhogen, is Vewin ervan overtuigd dat allereerst de essentiële ICT-knooppunten in de vitale ketens en de afhankelijkheden daarbij van derden in kaart moeten worden gebracht. Aangezien het hier om een breed onderzoek over de verschillende vitale sectoren gaat, ziet Vewin graag dat het NCSC dit traject faciliteert.

*Onderschrijft u de noodzaak van een onderzoek naar intersectorale afhankelijkheden en ketenafhankelijkheden op het gebied van kritische cyberprocessen?*
Zorko: 'Het cybersecurity-veld kenmerkt zich door enorme ambitie. Enerzijds gebeurt er al veel en anderzijds zijn er nog zoveel zaken die onze aandacht behoeven. De ketenafhankelijkheid en de verbondenheid tussen sectoren is daar een voorbeeld van. Enerzijds hebben we de afgelopen jaren al een aantal best practices ontwikkeld, anderzijds moeten we hier de komende jaren in investeren. Vorig jaar hebben Shell en TenneT over dit onderwerp het rapport 'Cyber security supply chain risicoanalyse' geschreven. Wat mij betreft een stevig privaat initiatief. Uiteraard staat onze deur altijd open om over dit soort initiatieven te praten.'

## Nationaal Detectie Netwerk

De drinkwatersector heeft afgesproken dat zij vóór volgend jaar zomer is aangesloten op het Nationaal Detectie Netwerk, een samenwerkingsverband waarbinnen het rijk en vitale sectoren real-time informatie uitwisselen over digitale dreigingen en aanvallen. Hiermee kunnen partijen op basis van de eigen verantwoordelijkheid tijdig maatregelen treffen om mogelijke schade of uitval te beperken of te voorkomen. Eén van de kritiekpunten is dat er, met name aan de zijde van de overheid, nog te weinig informatie wordt gedeeld via het NDN.

*Welke verbeterstappen neemt u of gaat u nemen om dit te verbeteren?*
Zorko: 'In de eerste plaats wil ik de drinkwatersector complimenteren met de bereidheid om zo snel stappen te zetten. Natuurlijk moet het Nationaal Detectie Netwerk een stap verder ontwikkeld worden. Vaak zijn dit ook processen waar we al doende leren. Het is een gezamenlijke zoektocht om vraag en aanbod van informatie op elkaar te laten aansluiten. Daar wil ik dus samen met de drinkwatersector op inzetten. Laten we vooral ook openstaan voor kritiek om zo samen het NDN sterker te maken.'

'Detectie is wat mij betreft een topprioriteit waar ik mij samen met de vitale infrastructuur hard voor wil maken. Dat doen we dus ook in de vorm van investeringen. Staatssecretaris Dijkhoff heeft hier in de begroting voor het komende jaar dan ook ruimte voor gevonden. Omdat misdaad steeds meer verschuift van offline naar online, is volgend jaar al 5 miljoen euro en vanaf 2018 structureel 14 miljoen euro beschikbaar voor cybersecurity en de aanpak van cybercriminaliteit. Een belangrijk onderdeel van deze versterkingen, zullen versterkingen op het gebied van detectie zijn. Immers, het is van cruciaal belang om te zien wat er gebeurt om daar ook juist op te kunnen handelen.'

### Wetsvoorstel gegevensverwerking en meldplicht cybersecurity

Op 27 oktober jl. is het Wetsvoorstel gegevensverwerking en meldplicht cybersecurity in de Tweede Kamer aangenomen.

Hiermee krijgen vitale aanbieders, waaronder de drinkwaterbedrijven, een meldplicht voor ICT-inbreuken die (mogelijk) een grote impact hebben op de continuïteit van de vitale dienst. De melding vindt plaats bij het Nationaal Cyber Security Centrum (NCSC) van het ministerie van VenJ. Het doel van het wetsvoorstel is dat het NCSC tijdig hulp en bijstand verleent aan de getroffen vitale aanbieder(s) om de effecten van een ernstige ICT-inbreuk zoveel als mogelijk te beperken én om andere vitale aanbieders te waarschuwen. Hulp en bijstand staan dus voorop. Het wetsvoorstel voorziet niet in een handhavende rol voor het NCSC, noch in sancties.

Bij de melding moet de getroffen vitale aanbieder ook informatie verstrekken over de inrichting van haar ICT-systemen en netwerken. Die informatie heeft het NCSC nodig om de aanbieder te helpen én om de risico's voor andere vitale aanbieders in te kunnen schatten. Omdat het hier om gevoelige informatie gaat, bevat het wetsvoorstel een bijzondere openbaarheidsregeling. Hiermee is geborgd dat vertrouwelijke gegevens die herleid kunnen worden naar een vitale aanbieder, niet openbaar kunnen worden op basis van de Wet openbaarheid van bestuur (Wob).

De openbaarheidsregeling geldt overigens ook voor vertrouwelijke gegevens die zijn verkregen door onverplichte meldingen. Hierdoor draagt de regeling bij aan de gewenste just culture waarbij bedrijven vrijwillig informatie uitwisselen met het NCSC met als doel het verbeteren van de veiligheid van het gehele systeem.

Het wetsvoorstel is conform de inzet van Vewin, namelijk, focus op ICT-inbreuken met (mogelijk) een grote impact, geen toezicht en handhaving door het NCSC, en opname van een bijzondere openbaarheidsregeling.

Aanleiding van het wetsvoorstel is de zaak DigiNotar. Naar verwachting treedt de wet per 1 juni 2017 in werking.