Ministerie van
Justitie en Veiligheid

Samenwerking op het gebied van cybersecurity

Maak nadere samenwerkingsafspraken op basis van bestaande verantwoordelijkheden en bevoegdheden.
De digitale dreiging voor de nationale veiligheid houdt aan, aldus het Cyber Security Beeld 2020. Publiek-private samenwerking is dan ook essentieel. Hiervoor zijn de bestaande wettelijke kaders, met sectoraal toezicht en handhaving, én vertrouwen tussen partijen randvoorwaardelijk.
Het Nationaal Cyber Security Centrum (NCSC) is een kennisautoriteit op het gebied van dreigingsinformatie, die van groot belang is voor vitaal om de juiste (beveiligings-)maatregelen te treffen. De vitale sectoren zijn en blijven verantwoordelijk voor beveiliging en incidentrespons, met toezicht en handhaving door de sectorale toezichthouders.
Voor een optimale samenwerking zijn nadere werkafspraken tussen het NCSC, de vitale sectoren en toezichthouders noodzakelijk. Er dient in gezamenlijkheid een escalatiepad te worden opgesteld voor situaties waarin bij ernstige kwetsbaarheden beveiligingsadviezen niet of niet voldoende zouden worden opgevolgd door vitaal. De eerste stap is escalatie tussen NCSC en het vitale bedrijf, waarbij het bedrijf ingaat op de uitkomsten van de eigen risicoanalyse die leidend is voor te nemen maatregelen. In het uiterste geval kan de toezichthouder waar nodig maatregelen afdwingen, in geval van drinkwater de ILT. Structureel oefenen met elkaar is van belang om de werkafspraken te toetsen op effectiviteit, voor begrip voor elkaars positie en voor kennis van elkaars processen.

Nationaal Cyber Security Centrum
Sabine Gielens

Vertrouwelijke informatiedeling

Richt 'trusted channels' in tussen overheid en vitale sectoren.
Statelijke actoren zijn een steeds grotere bedreiging voor de belangen van de Nederlandse staat. Het schaden van deze belangen zou onder andere via verstoring van de vitale processen kunnen plaatsvinden. De overheid verwacht dat de vitale infrastructuur, waaronder de drinkwatersector, zich weerbaarder maakt tegen deze dreigingen. Hiervoor is tijdige informatievoorziening inclusief handelingsperspectief vanuit de overheid nodig om de juiste maatregelen te kunnen treffen en te rechtvaardigen.
Eén van de obstakels bij informatiedeling is dat hoog geclassificeerde dreigingsinformatie alleen onder strenge voorwaarden kan worden gedeeld. Het delen van dergelijke informatie kan alleen plaatsvinden als er onderling vertrouwen is tussen de overheid en vitale sectoren. Vewin pleit ervoor om naast de reguliere informatie-uitwisseling, 'trusted channels' te realiseren voor het delen van geclassificeerde (dreigings-)informatie door alle overheidsinstanties met vitale sectoren. Hiertoe zou per sector of vitaal bedrijf een Security Liaison Officer aangesteld kunnen worden.

Economische Veiligheid, Nederlandse Cybersecurity Agenda, Nationale Veiligheid Strategie
Sabine Gielens