Eurocommissaris Digitale Agenda, Neelie Kroes

‘Europese richtlijn voor netwerk- en informatiebeveiliging sluit aan bij Nederlandse wetgeving’

Sinds februari 2010 is Neelie Kroes (1941) als lid en vicevoorzitter van de Europese Commissie belast met de digitale agenda. In de zes jaar daarvóór was zij als eurocommissaris verantwoordelijk voor de portefeuille mededinging. Digitale veiligheid heeft op dit moment binnen de EU de allerhoogste prioriteit. Voor de drinkwatersector is dit een uiterst relevant onderwerp, omdat drinkwater voor de maatschappij van cruciaal belang is.

Onlangs bleek dat, net als bij veel andere bedrijfstakken, sommige systemen in de drinkwatersector waren geïnfecteerd met het Citadel botnet-virus, waardoor ze kwetsbaar werden voor hackers. Herhaling van een dergelijk probleem is ongewenst en we hebben Eurocommissaris Kroes daarom gevraagd ons meer te vertellen over de huidige status van de digitale agenda en de invoering ervan. Bovendien past de Nederlandse drinkwatersector een zeer innovatief elektronisch sensorsysteem toe, dat de kwaliteit van het drinkwater binnen de infrastructuren meet. Dit sluit aan bij het digitale programma van Kroes.

Voorgestelde richtlijn voor netwerk- en informatiebeveiliging

De Europese Commissie heeft onlangs een strategie voor cyberbeveiliging gepubliceerd, tegelijk met een voorgestelde richtlijn voor netwerk- en informatiebeveiliging (NIS). Een van de bepalingen van deze richtlijn zal zijn dat exploitanten van onontbeerlijke infrastructuren (financiële dienstverlening, transport, energie, gezondheidszorg), leveranciers van informatiediensten en overheidsinstanties maatregelen voor risicobeheer moeten nemen en ernstige ICT-incidenten met betrekking tot hun kernactiviteiten moeten rapporteren.

Meldingsplicht

In Nederland wordt een wettelijke meldingsplicht voorbereid die belangrijke industrieën (energie, drinkwater, telecommunicatie, controle en beheer van oppervlaktewater, transport en financiën) zal verplichten grote ICT-inbreuken te melden aan het ministerie van Veiligheid en Justitie (en specifiek aan het Nationaal Cyber Security Centrum (NCSC)), zodat er snel hulp kan worden geboden. Aanleiding voor deze meldingsplicht was de DigiNotar-zaak.

Hoe past de meldingsplicht in Nederland binnen het Europese voorstel?

Kroes: 'Laat ik op de eerste plaats zeggen dat beide initiatieven hetzelfde doel voor ogen hebben: we willen dat ernstige incidenten rondom cyberbeveiliging gemeld worden, zodat alle belanghebbenden adequaat kunnen reageren. De grootscheepse DDoS-aanvallen op Nederlandse banken eerder dit jaar onderstrepen de noodzaak van deze maatregelen. Een dergelijke informatiestroom is een essentieel onderdeel van de cultuur op het gebied van risicomanagement, waarvoor zowel de voorgestelde richtlijn als de Nederlandse wetgeving pleiten. De voorgestelde richtlijn heeft betrekking op essentiële informatie-infrastructuren, zoals vervoer, energie, het bankwezen en financiële instellingen, overheidsinstellingen en de belangrijkste verschaffers van toegang tot het internet. De richtlijn is niet identiek aan de Nederlandse wetgeving, maar sluit wel heel erg hierbij aan.'

Zal de Europese richtlijn ook van toepassing zijn op de drinkwatersector, die momenteel niet in het voorstel wordt genoemd?

Kroes: 'De voorgestelde richtlijn is gericht op de goede werking van de interne markt en is gebaseerd op artikel 114 van het EU-verdrag. Het voorstel heeft betrekking op kritieke informatie-infrastructuur, die een sterke invloed op de werking van de interne markt kan hebben. De drinkwatersector is hierin niet expliciet opgenomen, maar het voorstel zou tijdens de dialogen met de lidstaten aangepast kunnen worden. Het voorstel betreft in elk geval een richtlijn van minimumharmonisatie en zal niet voorkomen dat Nederland voorschriften moet hanteren voor sectoren die niet specifiek genoemd worden, zoals de watersector.'

Twee toezichthouders ongewenst

De voorgestelde EU-richtlijn bepaalt dat elke lidstaat een bevoegde nationale autoriteit moet aanstellen waaraan de desbetreffende bedrijven ICT-incidenten moeten rapporteren. Daarnaast zal deze autoriteit onder andere toezicht houden op de implementatie van de richtlijn, de mogelijkheid krijgen om opdracht te geven voor sectoraudits, de beveiliging van netwerken beoordelen en bindende instructies uitvaardigen.

Zo'n autoriteit met een toezichthoudende rol bestaat momenteel niet in Nederland. Het NCSC is geen toezichthoudende instantie, maar biedt eigenlijk meer ondersteuning en hulp. Met deze benadering zal de Europese Commissie de publiek-private benadering belemmeren die in Nederland de voorkeur geniet. Sterker nog, Nederland heeft al sectorvoorschriften voor vitale sectoren, waaronder eisen met betrekking tot bedrijfscontinuïteit. We moeten voorkomen dat er een situatie ontstaat waarbij tegelijkertijd twee regelingen van toepassing zijn. *Wat is uw visie op dit vraagstuk?*

Kroes: 'De richtlijn is expres bijzonder flexibel ten aanzien van de structuur en de nauwkeurige bevoegdheden van de verantwoordelijke autoriteiten. Het beoogde doel is dat bestaande structuren binnen de lidstaten dit oppakken als ze de middelen daartoe hebben. In die geest wil ik ons voorstel bespreken met lidstaten die moeilijkheden verwachten bij het zorgen voor samenhang met hun bestaande institutionele kader. Het is desalniettemin belangrijk om een enkelvoudig richtpunt te houden, om te garanderen dat verschillende activiteiten met betrekking tot cyberbeveiliging binnen een lidstaat gecoördineerd worden, naast effectieve samenwerking binnen het netwerk voor samenwerking op het gebied van informatiebeveiliging.'

Cultuur van risicomanagement

'In mijn optiek is zowel publiek-privaat partnerschap als privaat initiatief essentieel. Daarom gaat de richtlijn over het creëren van een cultuur van risicomanagement en informatiestromen, zonder kwaliteitsnormen op te stellen of nauwkeurige veiligheidsmaatregelen voor te schrijven. Dit is onderdeel van een cyberbeveiligingsstrategie, die initiatieven bevat die gericht zijn op de private sector. Op 17 juni 2013 heeft de Commissie een vrijwillig publiek-privaat platform opgestart om de huidige beste praktijken te bespreken.'

'De bevoegde autoriteiten moeten garanderen dat elke sector profiteert van de ontvangen informatie en dat de informatiestromen bilateraal blijven. In het voorstel moet elke lidstaat mechanismes vaststellen om te zorgen voor een efficiënte samenwerking tussen de publieke en de private sectoren.'

Vertrouwelijkheid garanderen

De richtlijn stelt dat de bevoegde nationale autoriteiten met elkaar en met de Europese Commissie informatie moeten uitwisselen over incidenten. Dit roept vragen op over de privacy en de risico's van openbaarmaking en de negatieve gevolgen hiervan. *Hoe kunt u de vertrouwelijkheid van de informatie garanderen?*

Kroes: 'Persoonsgegevens worden in veel gevallen in gevaar gebracht door incidenten rondom cyberbeveiliging. Ik begrijp

volledig dat mensen zich hier ongemakkelijk bij voelen. De voorgestelde richtlijn stemt echter volledig overeen met eerdere Europese richtlijnen ten aanzien van privacy. De regels rond gegevensbescherming zijn daarom volledig van toepassing en er wordt in het voorstel verwezen naar de erkenning ervan door het Handvest van de grondrechten van de Europese Unie.'

'Ik vind het belangrijk om ervoor te zorgen dat alle informatie die in dit verband nodig is, werkelijk relevant is voor ons doel, het bestrijden van inbreuken op cyberbeveiliging. De richtlijn benadrukt daarom dat, wanneer informatie volgens de Unie en de nationale regelgeving als vertrouwelijk wordt beschouwd, deze vertrouwelijkheid gegarandeerd moet worden bij de uitvoer van de activiteiten en de verwezenlijking van de doelstellingen zoals bepaald door de richtlijn. Er wordt ook gezegd dat informatie die als vertrouwelijk beschouwd wordt door een bevoegde instantie, uitsluitend uitgewisseld zou mogen worden met de Commissie en andere bevoegde instanties als deze uitwisseling absoluut noodzakelijk is voor de toepassing van de richtlijn. De uitgewisselde informatie moet beperkt worden tot wat relevant en proportioneel is voor het doel van uitwisseling.'

Evenwicht tussen openbaar en privébelang

'Er bestaat altijd nog de mogelijkheid voor een bevoegde autoriteit om bijzonder significante incidenten openbaar te maken, maar de richtlijn bepaalt dat de autoriteit in zo'n geval een evenwicht moet zoeken tussen het openbare en het private belang. De richtlijn zegt tevens dat bevoegde autoriteiten bijzondere aandacht moeten schenken aan de behoefte om informatie over productkwetsbaarheden bijzonder vertrouwelijk te behandelen, voorafgaand aan vrijgave van de desbetreffende beveiligingsupdates.'

Welke incidenten?

De richtlijn geeft geen duidelijke beschrijving van de ICT-incidenten die gerapporteerd moeten worden, maar vermeldt slechts: '…incidenten met een aanzienlijke impact op de beveiliging van de door hen verleende kerndiensten aan de bevoegde autoriteiten…'. Vewin is het eens met het beperken van de meldingsplicht tot grotere incidenten

die een bedreiging vormen voor de nationale veiligheid of die kunnen leiden tot sociale onrust. *Welke afbakening heeft u in gedachten?*

Kroes: 'De meldingsplicht is gemodelleerd op het juridische kader dat geldt voor de telecomsector, volgens de Europese kaderrichtlijn voor elektronische communicatienetwerken en -diensten. Het is van het grootste belang dat de openbare autoriteiten geïnformeerd worden over alle 'incidenten met een aanzienlijke impact op de beveiliging van de door hen verleende kerndiensten', zodat zij op de juiste manier preventieve en afwerende maatregelen kunnen ontwerpen, indien nodig kunnen reageren op een incident en relevante informatie kunnen verspreiden naar de private sectoren. De voorgestelde richtlijn verwijst expres naar een 'aanzienlijke' impact en 'kerndiensten', om zo de nadruk te leggen op de meer relevante incidenten. Onze ervaring met de kaderrichtlijn telecom toont aan dat op basis van zo'n definitie het aantal meldingen binnen zeer redelijke perken kan blijven.'

Regelgeving voor kostenverlaging voor elektronische communicatie

Op dit moment wordt een EU-verordening voorbereid om de kosten voor implementatie van de infrastructuur voor telecommunicatie te verlagen. Belangrijk element is de verplichting voor netwerkexploitanten om collega-exploitanten hun infrastructuur te laten gebruiken. Concreet gezegd betekent dit dat telecommunicatiekabels door drinkwaterbuizen zullen lopen.

Er is een belangrijk verband tussen drinkwater en de volksgezondheid. *In hoeverre is het gezamenlijke gebruik van de drinkwaterinfrastructuur te rijmen met de plicht van de waterbedrijven om de kwaliteit van hun drinkwater te garanderen?*

Telecomkabels in waterleidingen?

Kroes: 'De plicht tot de levering van gezond en schoon drinkwater wordt vastgelegd in de drinkwaterrichtlijn, die leidend zal zijn voor de implementering van regelgeving. De kwaliteit van het drinkwater moet dientengevolge altijd gegarandeerd worden. Als een deel van de waterinfrastructuur daarom gebruikt zou worden voor de plaatsing van telecommunicatiekabels, mag dit het veilig en betrouwbaar gebruik of de kwaliteit van het water op geen enkele manier hinderen.'

'Tegelijkertijd bestaat er een aanzienlijke potentiële synergie bij het gezamenlijk gebruik van water- en ICT-infrastructuur, zoals het aanbieden van verbeterde levering en betere waterkwaliteit. Denk bijvoorbeeld maar eens aan een efficiëntere

waterverdeling, mogelijk gemaakt door een betere controle, rechtstreekse kwaliteitsbewaking, betere lekdetectie en het mondiger maken van burgers voor een bewuster waterverbruik.'

In welke mate zullen drinkwaterbedrijven kunnen beslissen dat het gezamenlijk gebruik van hun leidingen ongewenst is?

Kroes: 'Het gezamenlijk gebruik van infrastructuur gaat over kansen om beter zaken te kunnen doen. Dit geldt voor bedrijven en voor de consument. Waterleidingbedrijven zijn spelers die gericht moeten blijven op het garanderen van één van de meest waardevolle grondstoffen die we ter beschikking hebben: schoon water. Maar hierbij zien ze mogelijk ook een kans om met minder inspanning betere dienstverlening te kunnen bieden. Daarom hoeven we volgens mij niet bang te zijn dat ze het voorstel niet steunen.'

Commerciële exploitatie van bestaande openbare infrastructuur

'Het voorstel van de Commissie is gericht op netwerkbeheerders, waaronder nutsbedrijven, om het mogelijk te maken om bestaande fysieke infrastructuur commercieel te exploiteren, door de infrastructuur bijvoorbeeld toegankelijk te maken voor telecombedrijven voor de aanleg van snel internet. Dit is niet evident, omdat in enkele lidstaten nutsbedrijven niet in bedrijfssectoren mogen werken die niet tot hun kerntaken behoren. Aan de andere kant is er al een aantal succesvolle lopende initiatieven, onder andere de aanleg van telecomnetwerken in riolen in Parijs, Wenen en Schotland.'

'Vanaf het begin heeft veiligheid in het wetsvoorstel centraal gestaan. Waterbedrijven moeten handelen in overeenstemming met de wetten die hun functioneren regelen in hun eigen landen, evenals de eerder genoemde drinkwaterrichtlijn. De veiligheid en de integriteit van de basisdienst mogen niet in gevaar komen, of dit nu gaat over water, energievoorziening of transport. Als er een mogelijk negatief effect op de basisinfrastructuur is, moet toegang tot deze infrastructuur geweigerd kunnen worden. Er is daarom geen enkele reden waarom de kwaliteit van het drinkwater negatief beïnvloed zou kunnen worden door mogelijk gezamenlijk gebruik.'

Versterken van de ICT-concurrentiepositie van de EU

De Nederlandse drinkwatersector gebruikt een zeer innovatief digitaal sensorsysteem, dat de kwaliteit van het drinkwater binnen het 118.000 kilometer lange drinkwaternet meet. Zelfs geringe plaatselijke vervuiling kan worden opgespoord en verwijderd. *Hoe kan dit de concurrentiepositie van de Europese ICT-sector ondersteunen?*

Kroes: 'Innovatie komt naar boven drijven als we durven vragen: 'Wat als?' Europa is altijd sterk geweest in het stellen van deze vragen. Uw innovatieve sensoren zijn een uitstekend voorbeeld van het antwoord dat gegeven kan worden als deze vragen gesteld worden. Schoon drinkwater is een goed dat overal ter wereld nodig is en de Nederlandse vakkennis op dit gebied is daarom een fantastische bron voor export en Europees leiderschap, door middel van het gebruik van ICT voor het faciliteren van vitale goederen.'

EIP on Water

'Het recentelijk gelanceerde European Innovation Partnership (EIP) on Water heeft deze koppeling erkend als een belangrijke kans op de markt, met een groeipotentieel van ongeveer 30% per jaar. Relevante sectoren, zoals de ICT-sector die ook in de bestuursstructuur van de EIP is vertegenwoordigd, zullen zich ongetwijfeld richten op deze kans waarmee duizenden banen gecreëerd worden. De resultaten gaan nog een stuk verder: snelle breedbandnetwerken vormen de ruggengraat van de eengemaakte markt. De voorgestelde regelgeving is gericht op een belangrijke kostenreductie voor de uitrol van deze netwerken, wat zal leiden tot een betere concurrentiepositie voor alle Europese bedrijven, naast de overduidelijke voordelen voor de burgers.'

Hoe kan de EU dergelijke innovaties in de drinkwatersector ondersteunen ter versterking van de Europese concurrentiepositie van de ICT-sector?
Kroes: 'De EIP on Water richt zich op het faciliteren van de ontwikkeling en inzet van innovatieve oplossingen voor wateruitdagingen en daarmee steunt het de concurrentiepositie van de Europese watersector. Slimme technologieën worden erkend als een belangrijke factor die het succes van de prioriteiten in het strategische implementatieplan van de EIP mogelijk maakt. Activiteiten zijn onder andere de identificatie en uitbanning van innovatiebarrières, het uitlijnen van de strategische prioriteiten met de verschillende Europese financieringsmechanismes om een maximaal hefboomeffect in de Opleiding & Ontwikkeling (O&O) van de watersector te bereiken en het opzetten van proefprojecten waarin waterkwaliteit aan digitale informatiesystemen gekoppeld wordt.'

Pionierprojecten FP7

'Het zevende kaderprogramma van de Europese Gemeenschap voor activiteiten op het gebied van onderzoek, technologische ontwikkeling en demonstratie (FP7) is al begonnen met pionierprojecten op het gebied van O&O-onderwerpen binnen het gebied, bijvoorbeeld: geavanceerd meten en voorspellen van consumptiepatronen, gecombineerde energie- en waterbeheerprogramma's of geavanceerd vraagmanagement met aangepaste prijsstelling. De EU zal deze steun voortzetten gedurende het volgende meerjarige kaderprogramma, voortbouwend op de bestaande samenwerking met lidstaatautoriteiten en partners uit de sector in de EIP 'Slimme steden en gemeenten' en de EIP's 'Water'. Ten slotte worden activiteiten in lijn gebracht die bijdragen aan de Digitale Agenda en de beleidsdoelstellingen Europa 2020, om de concurrentiepositie van Europa verder te versterken.'

Drs. N. (Neelie) Kroes is een dochter van een Rotterdamse vervoersondernemer en werd in 1971 Tweede Kamerlid voor de VVD. In het eerste kabinet-Van Agt (1977-1981) was zij staatssecretaris van vervoerszaken en PTT-zaken. Daarna was Kroes van 1982 tot 1989 minister van Verkeer en Waterstaat in de kabinetten Lubbers I en II. Na haar ministerschap vervulde ze diverse functies in het bedrijfsleven en was ze onder meer president van Universiteit Nyenrode. Vanaf 2004 is ze lid van de Europese Commissie, eerst met mededinging in haar portefeuille, sinds 2010 met ICT en telecom.