Vewin
Vereniging van waterbedrijven in Nederland

Position Paper

Cybersecuritywet

Met de Cybersecuritywet krijgen aanbieders van essentiële diensten - een subgroep van de vitale aanbieders, waaronder de tien Nederlandse drinkwaterbedrijven - een meldplicht voor ICT-inbreuken én een aantoonbare zorgplicht voor de beveiliging van netwerk- en informatiesysteem.

Gevolgen
Als (mogelijk) gevolg van de Cybersecuritywet beschikt de overheid over vertrouwelijke herleidbare informatie van aanbieders van essentiële diensten. Naast de melding van een ICT-inbreuk aan het Nationaal Cyber Security Centrum (NCSC) en het bevoegde gezag, moet ook informatie worden verstrekt over getroffen tegenmaatregelen en maatregelen om herhaling te voorkomen. In het kader van de zorgplicht moeten aanbieders van essentiële diensten passende technische en organisatorische maatregelen treffen om de risico's voor de beveiliging van hun netwerk- en informatiesysteem te beheersen. De bevoegde autoriteit kan aanbieders van essentiële diensten een auditplicht opleggen met als doel om vast te stellen of de aanbieder heeft voldaan aan de gestelde beveiligingseisen (zorgplicht). De resultaten van de audit moeten worden verstrekt aan de bevoegde autoriteit.

Borging vertrouwelijkheid van informatie
Aangezien het hier om vertrouwelijke informatie gaat, zoals (technische) cybersecurity-maatregelen en mogelijke kwetsbaarheden in netwerk- en informatiesystemen, die herleidbaar is naar aanbieders van essentiële diensten, moet worden voorkomen dat deze gegevens met een beroep op de Wet openbaarheid van bestuur (Wob) opvraagbaar zijn. Openbaarmaking van herleidbare gegevens maakt aanbieders van essentiële diensten kwetsbaar voor gerichte ICT-aanvallen. Hiermee zou de Cybersecuritywet een bedreiging voor hen en de maatschappij worden. Daarom is de Cybersecuritywet voorzien van een bijzondere openbaarheidsregeling. Vewin pleit voor behoud van deze regeling. Deze voorkomt namelijk dat vertrouwelijke gegevens die door aanbieders van essentiële diensten aan het NCSC en/of het bevoegde gezag zijn aangeleverd en herleidbaar zijn naar de betreffende aanbieder met een beroep op de Wob opgevraagd kunnen worden. Deze openbaarheidsregeling geldt ook voor vertrouwelijke herleidbare gegevens die zijn verkregen door onverplichte meldingen aan het NCSC. Hierdoor draagt de regeling bij aan de gewenste 'just culture' waarbij bedrijven vrijwillig informatie uitwisselen met het NCSC ter verbetering van de veiligheid van het gehele systeem.

- **Behoud in het kader van de nationale veiligheid de in de Cybersecuritywet opgenomen bijzondere openbaarheidsregeling.**
  Hiermee wordt voorkomen dat vertrouwelijke herleidbare gegevens van essentiële diensten op basis van de Wob bij het NCSC en/of bevoegde gezagen opgevraagd kunnen worden.

Den Haag, 12 maart 2018
Voor informatie Sabine Gielens, 070 349 08 83, gielens@vewin.nl

Vewin
Bezuidenhoutseweg 12
2594 AV Den Haag
T (070) 3490 850
info@vewin.nl
www.vewin.nl
Postbus 90611 • 2509 LP Den Haag