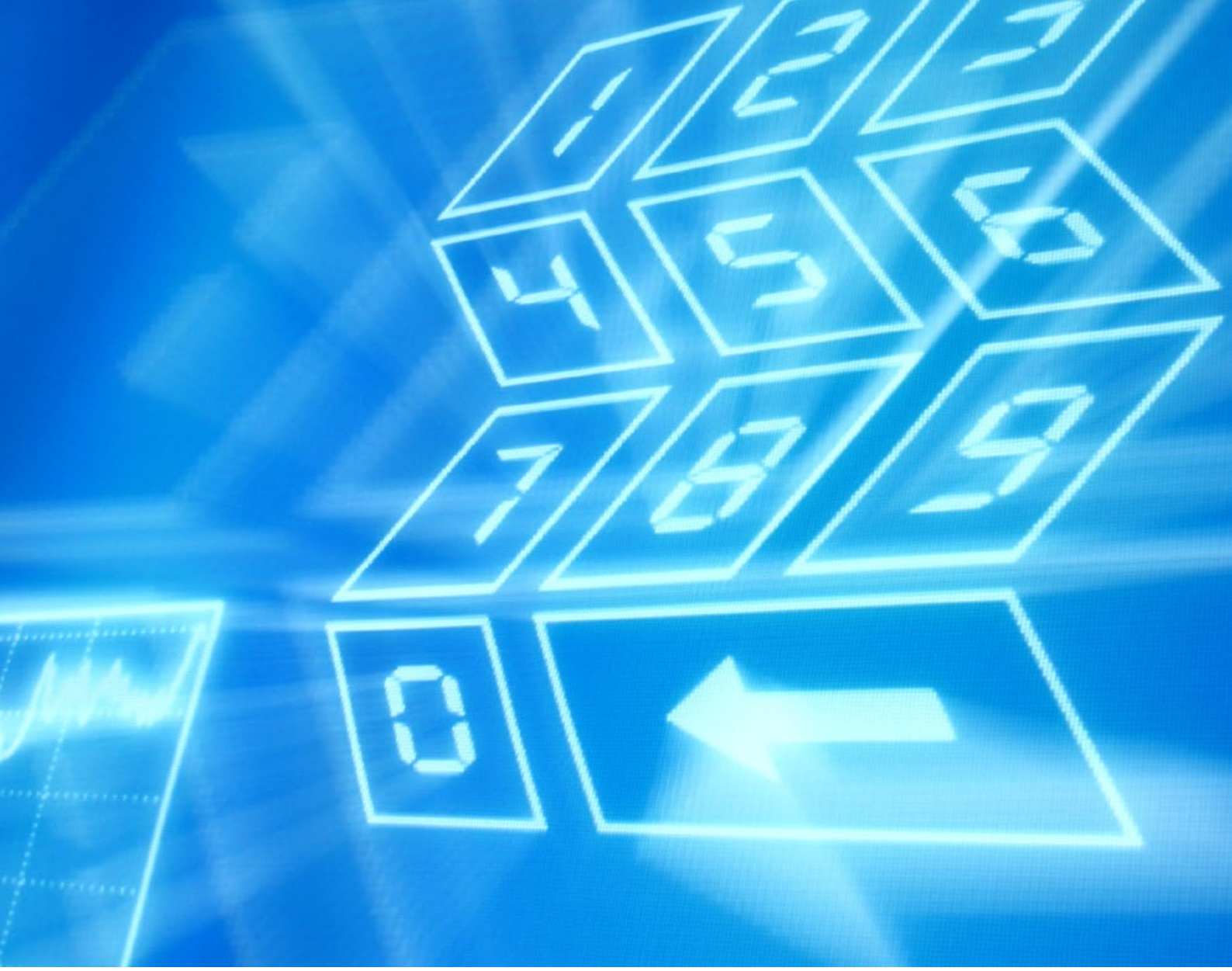

Consultatieronde van start

De Cybersecuritywet komt eraan

Vanaf medio 2018 krijgt Nederland één overkoepelende Cybersecuritywet. Bedrijven in de vitale infrastructuur, waaronder de tien Nederlandse drinkwaterbedrijven, krijgen hiermee onder meer een zorgplicht voor de beveiliging van hun netwerk- en informatiesysteem.

Afgelopen juni is de consultatieronde begonnen voor de Cybersecuritywet. Hiermee wordt uitvoering gegeven aan de Europese richtlijn voor netwerk- en informatiebeveiliging (NIB-richtlijn), die het Europees Parlement vorig jaar juli heeft aangenomen. Het doel van de NIB-richtlijn is om eenheid en samenhang te brengen in het Europese beleid voor netwerk- en informatiebeveiliging door de digitale paraatheid te vergroten en door de gevolgen van cyberincidenten te verkleinen.

Overlap met Wgmc

De Cybersecuritywet bevat niet alleen de bepalingen uit bovengenoemde NIB-richtlijn, maar ook uit het Wetsvoorstel gegevens-

‘INBREUKEN KUNNEN AANZIENLIJKE GEVOLGEN HEBBEN VOOR DE CONTINUÏTEIT VAN DE VITALE DIENST’

verwerking en meldplicht cybersecurity (Wgmc). Dit wetsvoorstel is in juli jl. door de Eerste Kamer aangenomen. Vanwege de inhoudelijke samenhang en overlap tussen dit wetsvoorstel en de NIB-richtlijn, is besloten dat er één overkoepelende Cybersecuritywet komt. Zodra de Cybersecuritywet in werking treedt, wordt het Wgmc ingetrokken.

Meld- en zorgplicht

Met de komst van de Cybersecuritywet krijgen bedrijven in de vitale infrastructuur (zoals drinkwaterbedrijven, energiebedrijven, banken, enzovoort) een meldplicht voor ICT-inbreuken. Hierbij gaat het om inbreuken die aanzienlijke gevolgen (kunnen) hebben voor de continuïteit van de vitale dienst.

Daarnaast krijgen bedrijven een zorgplicht voor de beveiliging van hun netwerk- en informatiesysteem. Dit wil zeggen dat bedrijven passende technische en organisatorische maatregelen moeten treffen om de risico’s voor de beveiliging van hun netwerk- en informatiesysteem te beheersen. Ook moeten ze maatregelen treffen om de gevolgen van eventuele incidenten te minimaliseren. Het doel is de continuïteit van vitale diensten, waaronder de drinkwatervoorziening, zoveel mogelijk te borgen. Toezicht en handhaving op zowel de zorg- als meldplicht liggen bij de sectorale toezichthouders.

ICT-inbreuken

De melding van ICT-inbreuken met daadwerkelijk aanzienlijke gevolgen voor de continuïteit moet plaatsvinden bij zowel het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Veiligheid en Justitie, als bij de sectorale toezichthouder. ICT-inbreuken die aanzienlijke gevolgen kúnnen hebben – ofwel de ‘bijna-ongelukken’ – hoeven alleen bij het NCSC gemeld te worden en niet bij de sectorale toezichthouder.

Een gewaarschuwd mens…

Het doel van melding bij het NCSC is dat het in staat wordt gesteld om hulp en bijstand te verlenen aan het betrokken bedrijf om de continuïteit van de vitale dienst te borgen of zo snel mogelijk te herstellen. Daarnaast kan het NCSC op basis van de melding een inschatting maken of ook andere vitale bedrijven gewaarschuwd moeten worden. Immers, een incident bij de één is een waarschuwing voor de ander. Bedrijven moeten dan melding van de inbreuk zelf doen én van de aard en de omvang ervan, de gevolgen, de getroffen maatregelen en overige gegevens die nodig zijn voor hulp, bijstand en risicoschatting. Hierbij kan het ook gaan om informatie over de inrichting van ICT-systemen en netwerken.

Openbaarheidsregeling

Tot slot bevat de Cybersecuritywet een zogenoemde bijzondere openbaarheidsregeling. Deze regeling voorkomt dat vertrouwelijke gegevens die herleidbaar zijn naar vitale aanbieders, bij het NCSC kunnen worden opgevraagd via een beroep op de Wet openbaarheid van bestuur (Wob). Het kan daarbij bijvoorbeeld gaan om gegevens die vitale bedrijven in het kader van de meldplicht aan het NCSC hebben verstrekt. 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 vitale bedrijven vrijwillig informatie uitwisselen met het NCSC. Doel is het verbeteren van de veiligheid van het gehele systeem.

Inzet Vewin

Namens de drinkwatersector heeft Vewin bij de internetconsultatie voor de Cybersecuritywet gepleit voor:

- Verruiming van de bijzondere openbaarheidsregeling voor vertrouwelijke herleidbare gegevens naar de sectorale toezichthouders. Zij beschikken straks ook over meldingen van ICT-inbreuken inclusief achterliggende informatie, zoals over ICT-systemen. Daarnaast biedt de wet de mogelijkheid dat vitale bedrijven een beveiligingsaudit krijgen opgelegd om naleving van hun zorgplicht aan te tonen. De resultaten van de audit moeten worden verstrekt aan de toezichthouder. Hierbij gaat het om vertrouwelijke en gevoelige informatie (over bijvoorbeeld kwetsbaarheden) die niet openbaar mag worden. Voorkomen moet worden dat de Cybersecuritywet een bedreiging wordt voor vitale bedrijven en daarmee voor de nationale veiligheid.

- Vasthouden aan het uitgangspunt dat de Cybersecuritywet alleen algemene bepalingen en normen bevat. De uitwerking van eisen, van bijvoorbeeld de zorgplicht, vindt, waar nodig, plaats in sectorspecifieke AMvB’s en/of richtsnoeren. Hierdoor kan worden aangesloten bij bestaande sectorspecifieke werkwijzen en planvorming.

‘CYBERSECURITYWET: CONTINUÏTEIT VAN VITALE DIENSTEN ZOVEEL MOGELIJK WAARBORGEN’