Notitie

Van Siebe Kok (skok@energie-nederland.nl)
Aan Ministerie van Justitie en Veiligheid
Datum 1 juli 2024
Onderwerp Reactie op de internetconsultatie van de Cyberbeveiligingswet

Reactie op de internetconsultatie van de Cyberbeveiligingswet

Met veel belangstelling heeft Vereniging Energie-Nederland* (hierna E-NL) kennisgenomen van de concept Cyberbeveiligingswet (Cbw). Met deze Cbw wordt de NIS2 richtlijn in Nederland geïmplementeerd. E-NL maakt graag gebruik van de mogelijkheid op deze conceptwet te reageren. Wij scharen ons grotendeels achter de reactie die vanuit VNO-NCW is ingediend, maar willen middels deze reactie ook van de mogelijkheid gebruik maken een aantal punten namens de energiesector in te brengen.

(* Zie pagina 6)

Algemeen

- E-NL is positief over de doelen uit de NIS2 richtlijn en de concept Cbw. Het verhogen van de digitale veiligheid en weerbaarheid is van groot belang, al helemaal voor de energiesector.

- We zijn verheugd dat de NIS2 richtlijn, welke in Nederland wordt geïmplementeerd middels de Cyberbeveiligingswet (Cbw), minimumeisen stelt aan de harmonisatie van cyberbeveiliging in de EU. E-NL is dan ook positief over de voorliggende Cyberbeveiligingswet. De belangen van goede cybersecurity en digitale weerbaarheid zijn de energiesector bekend. Ook het belang van een digitaal veilige energiesector hoeft niet te worden uitgelegd.

- Van belang hierin is een duidelijk afgebakende en heldere terminologie. Waar de Wet beveiliging netwerk- en informatiesystemen (Wnbi) sprak over vitale sectoren, wordt in de Cbw gerept over belangrijke en essentiële entiteiten uit de

sectoren in bijlagen 1 en 2. Daarnaast heeft de CER het over kritieke entiteiten, die vervolgens ook in artikel 8 van de Cbw voorkomen. E-NL roept op om zoveel als mogelijk een eenduidige terminologie te hanteren. We begrijpen dat dit niet altijd mogelijk is in verband met de terminologie die in de Europese richtlijnen wordt gebruikt. Daarom het verzoek, ten einde eventuele verwarring te voorkomen, om waar mogelijk een uitleg in de Memorie van Toelichting toe te voegen.

- Een verder punt van zorg in de concept Cbw is het feit dat er weinig details in worden beschreven. Veel punten worden volgens de concepttekst in de AMvB uitgewerkt. Dit terwijl veel bedrijven nu al graag meer duidelijkheid over de keuzes hadden gezien. We verzoeken u daarom ook met klem om werk te maken van deze punten en deze waar nodig ook in de Cbw mee te nemen. In het vervolg van deze reactie zullen we op een aantal voorbeelden ingaan.

- Omdat veel details worden pas in de AMvB worden uitgewerkt, wordt de tijdspanne om aan de eisen in de Cbw te gaan voldoen zeer krap. Wij pleiten er daarom voor dat de toezichthouders hier rekening mee houden, al dan niet via een overgangsregeling.

- Voor een aantal partijen is nog onduidelijk of zij wel of niet onder de Cbw gaan vallen. De zelfevaluatie biedt hiervoor ook geen soelaas. We zouden graag duidelijkere richtlijnen zien die aangeven welke partijen onder deze wet gaan vallen.

- We zouden graag meer duidelijkheid hebben over de reden van het registreren van domeinnamen voor een elektriciteitscentrale. De essentiële dienst is daar niet aanwezig en deze centrales hebben ook geen eigen domeinnamen, die zijn namelijk in handen van de IT-afdeling die geen koppelingen heeft met de essentiële dienst.

Opleidingsplicht

- Het bestuur van een essentiële of belangrijke entiteit wordt verplicht kennis en vaardigheden op het gebied van cybersecurity

op te doen en deze aantoonbaar actueel te houden. E-NL juicht toe dat het belang van cybersecurity op deze manier groter wordt. Echter, er zijn een aantal zaken hierover onduidelijk. Wie geldt, bijvoorbeeld, als bestuurder? Gaat dit enkel om de Raad van Bestuur zoals uitgelegd in het bestuursrecht? Of geldt dit ook voor de bestuurders/managers van bepaalde business units? Hoe zit dit in groepsmaatschappijen waarvan niet elke BV onder deze wet valt? Of voor het moederbedrijf waarvan een van de dochters onder deze wet valt? Het is belangrijk dat hier duidelijkheid over komt.

- Daarnaast zijn er zorgen over de opleidingscertificaten. Wie mag deze uitgeven? Op basis waarvan mogen deze worden uitgegeven? Gaat dit gereguleerd worden? Omdat veel bedrijven grensoverschrijdend handel doen, is het essentieel dat deze certificaten Europees erkend worden. Ook moet er worden opgepast voor 'cowboygedrag' rondom het uitgeven van deze certificaten.

Zorgplicht

- Het volledig uitsluiten van risico's is niet mogelijk. E-NL is blij dat dit ook wordt erkend. Bedrijven zijn zelf in staat hun risico's in kaart te brengen en invulling te geven aan de voorschriften uit de NIS2.

- Wat betreft de ketenzorgplicht is E-NL tevreden dat hier aandacht voor komt. Vooral omdat hiermee ook de aanbieders van digitale apparatuur/systemen aan essentiële of belangrijke entiteiten aan strenge eisen moeten gaan voldoen. Daarnaast zijn wij positief over het feit dat de ketenzorgplicht geldt voor de directe toeleveranciers.

- Veel bedrijven benaderen hun risicomanagement vanuit een *all-hazards approach*, waarbij de digitale risico's slechts een onderdeel zijn van alle risico's waar rekening mee moet worden gehouden. We willen daarom ook graag het belang benadrukken van een goede samenhang tussen de Cbw de Wet weerbaarheid kritieke Entiteiten (Wwke).

Meldplicht

- E-NL pleit voor meer duidelijkheid over de drempelwaarden rondom de meldplicht. Dan gaat het bijvoorbeeld over wat nu exact bedoeld wordt met een significante dreiging (artikel 37). Dit kan ook per AMvB worden uitgewerkt, maar het is belangrijk dat hier drempelwaarden worden vastgelegd. Er mag geen twijfel bestaan of significante incidenten al dan niet gemeld moeten worden. Bij het opstellen hiervan gaan wij graag met u in gesprek om hierover mee te denken. E-NL pleit ervoor geen strengere eisen te stellen dan in de NIS2 richtlijn staan voorgeschreven.

- Daarnaast is er onduidelijkheid over wat er gebeurd met de drempelwaardes van entiteiten die onder de huidige Wbni vallen. Worden deze aangepast of blijven ze behouden? Wij pleiten ervoor in het begin aan te sluiten bij de drempelwaarden uit de NIS1, bijvoorbeeld de grens van 100MW voor energiecentrales, en deze niet te verlagen. Na verloop van tijd zouden hier wanneer nodig aanvullingen op gedaan kunnen worden. Ook hierover gaan we als sector graag met u in gesprek.

- Het is voor energieproducenten lastig om vast te stellen wie de exacte ontvanger van de geleverde dienst is. Elektriciteit wordt op het net ingevoed. Via dit net kan het naar elke afnemer in Nederland of naar het buitenland getransporteerd worden. Wanneer er een productie-installatie uitvalt, zijn er mechanismes in plaats om dit op te vangen, zowel nationaal als internationaal. De leveringszekerheid voor de eindafnemer is dus geborgd. Het Europese net kan zelfs de uitval van meerdere elektriciteitscentrales opvangen. Wie zijn dan de "ontvangers van diensten" die leveranciers van elektriciteit moeten informeren in het geval van een significante dreiging?

- In artikel 38.3 wordt vermeld dat het CSIRT adviseert over het melden van significante incidenten met een criminele aard aan de rechtshandhavingsinstanties. Is het bij criminele aard niet altijd verstandig om aangifte te doen? Kan dit verder verduidelijkt worden?

- Heeft de entiteit nog invloed op of inzicht in wat er uiteindelijk met het centrale contactpunt of met derde landen wordt uitgewisseld? Is het bekend welke informatie er exact wordt uitgewisseld met het centrale contactpunt? Wordt aan de entiteit medegedeeld wat er met een melding wordt gedaan?

- De entiteit zou te allen tijde op de hoogte moeten worden gehouden van wat er wordt gedaan met de informatie uit de melding.

- Het door het CSIRT verplichten tot informeren van (rechts)personen over een dreiging (artikel 40 Cbw) is momenteel te vrijblijvend. Dit moet altijd in overleg met de entiteit gebeuren en hier moeten duidelijke voorwaarden aan worden gesteld om onnodige paniek te voorkomen. Het informeren van (rechts)personen heeft daarnaast vooral een educatieve waarde tijdens een dreiging. Bijvoorbeeld door het delen van concrete tips over wat te doen wanneer de elektriciteitsvoorziening wordt onderbroken. Dit geldt dan niet enkel voor de directe afnemers, maar voor iedereen op het (deel) van het elektriciteitsnet dat wordt geraakt.

Toezicht

- Er wordt gesproken over een beveiligingsscan. Is het een mogelijkheid om dit aan te kunnen tonen d.m.v. een certificaat van een onafhankelijke en gekwalificeerde deskundige? Of kan deze enkel en alleen worden uitgevoerd door de toezichthouder zelf?

- Artikel 77: Handhavingsmaatregelen – de maximale boete is 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar ***"van de onderneming waartoe de essentiële entiteit behoort".*** Wordt hier bedoeld de omzet van de Nederlandse overtredende onderneming, die ook de beslissingen neemt over de cyberbeveiligingsmaatregelen? Of zou ook de omzet van een eventuele Europese of niet-Europese moeder kunnen meetellen,

die niet betrokken is in het cyberbeveiligingsbeleid en zelf ook geen essentiële entiteit is in NL? Graag duidelijkheid op dit punt.

Over Vereniging Energie-Nederland

Vereniging Energie-Nederland (hierna E-NL) is de brancheverenigingvoor alle partijen die betrokken zijn bij het produceren, leveren en verhandelen van stroom, gas en warmte. Wij vertegenwoordigen vrijwel de volledige energiemarkt in Nederland. Onze ruim 80 leden – waaronder vele nieuwkomers – zijn actief in hernieuwbare en niet-hernieuwbare energie. Zij bieden diverse diensten aan en komen voortdurend met innovatieve en duurzame initiatieven.

Wij maken ons in Den Haag en Brussel sterk voor de belangen van onze leden op elk gebied van energievoorziening. Van het opwekken en verhandelen van energie tot aan de levering ervan aan consumenten en bedrijven. Daarnaast ondersteunen we de ontwikkeling van nieuwe dienstverlening van onze leden. Denk bijvoorbeeld aan hulp bij het verduurzamen van gebouwen.
Als brancheverenigingdragen wij bij aan een duurzame toekomst. Wij blijven ons inzetten voor een energiemarkt waarin duurzaamheid, betrouwbaarheid, leveringszekerheid en betaalbaarheid centraal staan.

Het is onze ambitie om een halvering van de CO2-uitstoot te bereiken in 2030. In 2050 moet de energievoorziening 100% CO2-neutraal zijn. Met het oog op de geplande uitrol van hernieuwbare energiebronnen, is Nederland op weg om koploper te worden in Europa.

Wij streven naar een optimale markt met laagdrempelige toe- en uittreding. Met ruimte voor nieuwe en innovatieve spelers en bedrijven. Energiebedrijven moeten voldoende prikkels krijgen om te investeren. Omdat onze energiemarkt Europees is, streven wij naar oplossingen en beleid op Europees niveau. Dit zorgt voor een gelijk speelveld om collectief en efficiënt te kunnen verduurzamen.