Netbeheer Nederland

Netbeheer Nederland
Anna van Buerenplein 43
2595 DA Den Haag

Postbus 90608
2509 LP Den Haag
070 205 50 00
secretariaat@netbeheernederland.nl
netbeheernederland.nl

Ministerie van Justitie en Veiligheid
T.a.v. de heer F.B.J. Grapperhaus
Postbus 20301
2500 EH DEN HAAG

Kenmerk
BR-2020-1712
Datum
6 maart 2020

Behandeld door
Carine van Ravesteijn
E-mail
cravesteijn@netbeheernederland.nl

Doorkiesnummer
070 205 50 00

Onderwerp
Consultatiereactie op de wijziging van het Besluit Beveiliging Netwerk- en Informatiesystemen

Hooggeachte heer Grapperhaus,

Met deze brief maakt de vereniging Netbeheer Nederland, namens alle energienetbeheerders in Nederland, graag gebruik van de mogelijkheid haar reactie te geven op de consulatie van de wijziging van het Besluit Beveiliging Netwerk- en Informatiesystemen (Hierna: Bbni).

Bbni versterkt een goede basis
De E.U.-richtlijn NIS en de daarop gebaseerde Nederlandse wet Wbni, geven een uitstekende basis om werk te maken van de zorg- en meldplicht voor cybersecurity. Met het Bbni wordt deze zorg- en meldplicht voor cybersecurity meer geconcretiseerd. Deze invulling is voor de netbeheerders heel herkenbaar, omdat het op hoofdlijnen de aanpak beschrijft waar netbeheerders al werk van maken sinds de digitalisering van de netten is ingezet. Begrijpelijk, want al deze stukken gaan terug op dezelfde internationale standaarden (ISO, IEC). Daarmee versterkt het Bbni verder de plicht om de zorg- en meldplicht voor cybersecurity goed in te vullen. Dat dient het algemene belang van leveringszekerheid van de energievoorziening. De gezamenlijke netbeheerders vinden dit een goede zaak.

Administratieve last wordt herkend
In de stukken van de consultatie wordt terecht de bewijslast benoemd als meerwerk. Ook al gaat de relevante passage over de energieproducenten, de opmerkingen zijn net zo relevant voor netbeheerders. Een structuur van toezichthouder en onder toezicht gestelde partij geeft nu eenmaal veel meer administratieve lasten, waaronder het vanwege controles aantoonbaar maken van de genomen maatregelen, per voorkeur door externe assurance.

Checks & balances zijn goed en graag zo houden
De netbeheerders vinden de checks & balances van wetgever (Ministerie van J&V en Ministerie van EZK), toezichthouder (Agentschap Telecom), kennisinstituut en CERT (NCSC) en uitvoerende

organisaties (waaronder netbeheerders) uitstekend. Belangrijk voor netbeheerders is dat ieder zich aan de eigen rol committeert. Dan is ieder in zijn eigen kracht, en dat versterkt het gehele systeem.

Voorkomen moet worden dat partijen 'op elkaars stoel gaan zitten'. Dat laatste is problematisch gebleken tijdens de 'Citrix-crisis' in januari jl., toen het Agentschap Telecom vragen stelde op het moment dat incident- en crisismanagement vol aan de gang was, tezamen met het NCSC. Hoewel de vragen van het Agentschap Telecom uiteraard heel begrijpelijk zijn, is het in het kader van incident- en crisismanagement beter als deze vragen gesteld worden als de crisis is opgelost. De gezamenlijke netbeheerders zouden graag zien dat de instanties van de overheid hun taken nader op elkaar afstemmen.

Het NCSC krijgt volgens het Bbni toezichthoudende taken. De netbeheerders vragen zich af of dit verstandig is vanuit het oogpunt van checks & balances. We streven naar een gelijkwaardige relatie tussen de vitale partijen en het NCSC. Enkel in een gelijkwaardige relatie kunnen we elkaar gaan helpen in het voorkomen en mitigeren van dreigingen en risico's. Het NCSC stelde zich eerder op het standpunt dat meldingen aan het NCSC niet zouden worden doorgezet aan het AT. Immers, meldingen aan het NSCS zijn in het kader van een CERT, waardoor ieder welwillend is om te melden, ook als het nog niet echt duidelijk is of er werkelijk moet worden gemeld. Meldingen aan het AT horen bij het toezicht, en dat geeft meldingen een meer formeel karakter. Terughoudendheid bij meldingen aan een CERT zoals NCSC moet worden voorkomen, en daarom zijn de netbeheerders van mening dat het NCSC geen toezichthoudende rol zou moeten krijgen.

Specifieke richtlijnen bij voorkeur via de Europese standaardisatie (EC/EU-DSO/ENTSO-E & ENCS)

Het Bbni maakt de zorg- en meldplicht voor cybersecurity concreter. Echter, het geeft geen specifieke richtlijnen hoe bijvoorbeeld het benoemde risicomanagement moet plaatsvinden. De aanstaande Network Code for Cybersecurity van de Europese Commissie gaat deze specifieke richtlijnen waarschijnlijk wel geven. Met deze code zullen de Europese Commissie en de officiële standaardisatie-organen van TSO's (ENTSO-E) en DSO's (EU-DSO entity in oprichting) middels een systeemaanpak, open normen en volwassenheidsmodel duiding geven voor de praktische invulling van de NIS (Wbni en Bbni).

De gezamenlijke netbeheerders achten een Europese invulling van NIS – Wbni – Bbni van belang om twee redenen. Ten eerste wordt daarmee voorkomen dat netbeheerders te maken gaan krijgen met zowel nationale als Europese kaders. Dit kan betekenen dat een netbeheerder te maken krijgt met twee kaders waarop kan worden ge-audit. Dit kan onnodige administratieve lasten geven. In Duitsland is dit helaas al gebeurd, met ook negatieve impact op innovaties bij de slimme meterinfrastructuur.

Ten tweede zijn nationale invullingen inhoudelijk ongepast, omdat netbeheerders werken met pan-Europese fabrikanten en service verleners (van installateurs netcomponenten tot providers cloud). Juist door pan-Europese richtlijnen op te stellen komt er betere security. De netbeheerders hebben bijvoorbeeld veel kunnen bereiken met de pan-Europese aanpak van het European Network for Cybersecurity (ENCS, waarin de Nederlandse netbeheerders actief participeren). ENCS producten worden als 'Europese' standaardisatie serieus opgepakt door fabrikanten, die soms wat betreft security de productontwikkeling direct baseren op deze stukken van het ENCS.

De netbeheerders stellen voor dat als de beveiligingseisen van de aanstaande Network Code for Cybersecurity ten minste gelijkwaardig zijn aan die van de NIB-richtlijn, zij bij een volgende wijziging van het Bbni worden toegevoegd aan artikel 4 Bbni, zodat voor hen de beveiligingseisen van de Wbni niet langer gelden. Overeenkomstig artikel 1, onderdeel D van de artikelsgewijze toelichting, waarin wordt beschreven dat als de beveiligingseisen van de verordening van het EASA ten minste gelijkwaardig zijn aan die van de NIB-richtlijn de betrokken luchtvaart-AED's worden toegevoegd aan artikel 4 Bbni. Europese wetgeving gaat altijd boven nationale wetgeving. Nationale wetgeving mag niet in strijd zijn met Europese. Door netbeheerders ook op deze lijst te zetten wordt dit voorkomen.

Ter afsluiting constateren de netbeheerders dat het Agentschap Telecom in haar jaarplan 2020 een vergelijkbare visie omschrijft. Het AT geeft daarin blijk van de noodzaak van systeemtoezicht, open normen en een Europese aanpak. De netbeheerders onderschrijven deze visie en hopen dat dit ook de verdere praktische invulling wordt van het Bbni.

De gezamenlijke netbeheerders zijn uiteraard graag bereid bovenstaande opmerkingen nader toe te lichten.

Met vriendelijke groet,

André Jurjus
directeur