Consultatie van het voorontwerp voor de

Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersecuritywet)

Reactie van KPN

KPN
Contactpersoon:
Postbus 30 000
2500 GA Den Haag

Kenmerk: RG/17/U/004

12 juli 2017

Inleiding en samenvatting

Cybersecurity is en blijft een grote uitdaging voor Nederland. Elke dag zijn er incidenten met hacks, spionage en (maatschappelijke) schade door cybercriminaliteit. KPN zet zich daarom ten volle in om onze diensten, producten en interne ICT te beschermen tegen cyberdreigingen.

De ontwikkelingen in het cyberdomein vragen om goede en realistische wetgeving om ondernemingen en vitale infrastructuren in Nederland te beschermen en grote schade door cybersecurityincidenten te voorkomen. KPN juicht het daarom toe dat de Europese Unie en de nationale overheid hier steeds meer aandacht voor hebben. De voorliggende implementatie van richtlijn (EU) 2016/1148 (de 'NIB-richtlijn') in de voorgestelde Cybersecuritywet is daar een voorbeeld van. KPN heeft op deze implementatie enkele op- en aanmerkingen die onderstaand zijn vertaald in concrete suggesties en verderop nader worden toegelicht.

Suggesties KPN:

- Gebruik dezelfde terminologie als in de NIB-richtlijn voor ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten aanbieden. Dit is nodig omdat de NIB-richtlijn deze ondernemingen expliciet uitzondert vanwege reeds bestaande Europese wetgeving, terwijl het voorontwerp door het gebruik van andere terminologie hier niet geheel duidelijk over is;
- Maak duidelijk welke gevolgen het overhevelen van de Wet gegevensverwerking en meldplicht cybersecurity naar de ontwerp Cybersecuritywet heeft voor aanbieders die door de NIB-richtlijn expliciet worden uitgezonderd;
- Hard- en softwarefabrikanten hebben een cruciale rol in de cybersecurityketen, terwijl er op dit moment niet voldoende waarborgen zijn voor de kwaliteit en veiligheid van hun producten. Hier is passende (Europese) wet- en regelgeving voor nodig, zodat kwetsbaarheden die een veiligheidsrisico vormen worden gemeld en gerepareerd;
- Zorg ervoor dat relevantie informatie over incidenten ook bij vitale aanbieders terecht komt, zodat zij mitigerende maatregelen kunnen nemen tegen vergelijkbare incidenten;
- Gebruik een eenduidige definitie voor 'inbreuken' en 'incidenten' of leg uit waarin een inbreuk zich onderscheidt van een incident.

Duidelijkheid nodig over positie telecomaanbieders in de Cybersecuritywet

Uit de NIB-richtlijn blijkt in overweging 7 dat "verplichtingen van aanbieders van essentiële diensten en digitaledienstverleners niet van toepassing [dienen] te zijn op ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten in de zin van Richtlijn 2002/21/EG (Kaderrichtlijn) aanbieden, welke onderworpen zijn aan de in die richtlijn specifieke veiligheids- en integriteitseisen, nog op verleners van vertrouwensdiensten in de zin van Verordening (EU) nr. 910/2014, dien onderworpen zijn aan de in die verordening vastgestelde veiligheidseisen."

In de Memorie van Toelichting (MvT) van het voorontwerp is opgenomen dat "de richtlijn niet van toepassing [is] op elektronische - communicatienetwerken en –diensten (telecomsector) en verleners van elektronische vertrouwensdiensten (zoals een certificaat voor een elektronische handtekening), omdat voor die sectoren al vergelijkbare EU-regels gelden". De MvT hanteert hiermee een iets andere bewoording dan de NIB-richtlijn (namelijk "elektronische - communicatienetwerken en –diensten (telecomsector)" en niet "ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten in de zin van Richtlijn 2002/21/EG (Kaderrichtlijn) aanbieden".

Hiermee lijkt hetzelfde doel te worden beoogd, namelijk dat de NIB-richtlijn (en dus ook de Nederlandse wet waarin de NIB-richtlijn wordt omgezet) niet moet gelden voor ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten aanbieden. Het is aan te raden – mede in verband met de afbakening tussen dit wetsvoorstel en de regels van de Telecommunicatiewet – de terminologie van de richtlijn aan te houden.

Het is daarbij onduidelijk hoe het overhevelen van de Wet gegevensverwerking en meldplicht cybersecurity naar de voorliggende conceptwetgeving zich verhoudt tot het uitzonderen van ondernemingen die openbare communicatienetwerken of openbare elektronische communicatiediensten aanbieden. In het eerder geconsulteerde Besluit meldplicht cybersecurity zijn elektronische communicatienetwerken of –diensten expliciet toegevoegd aan de lijst van vitale aanbieders en producten en diensten waarop de Wet gegevensverwerking en meldplicht cybersecurity van toepassing op is.[1] In de MvT wordt hier niet nader op ingegaan. Aan te raden is om duidelijkheid te geven over de gevolgen van de overheveling van de Wet gegevensverwerking en meldplicht cybersecurity voor ondernemingen die openbare communicatienetwerken of openbare communicatiediensten aanbieden.

Aansprakelijkheid van hard- en softwarefabrikanten

Kwetsbaarheden in hard- en software kunnen effect hebben op de veiligheid van netwerk- en informatiesystemen van digitaledienstverleners en vitale aanbieders. Veel bekende en minder bekende cybersecurityincidenten hebben een dergelijke kwetsbaarheid ten grondslag.

De fabrikanten van hard- en software zijn vaak wereldwijde spelers die hun eigen patch- en updatebeleid bepalen. Digitaledienstverleners en vitale aanbieders zijn van deze pat-

[1] KPN heeft uitgebreid gereageerd op de consultatie Besluit meldplicht cybersecurity: https://www.internetconsultatie.nl/besluitmeldplichtcyber/reactie/52aaa917-6365-4134-9c15-6db1d22519b0

ches en updates afhankelijk om hun ICT-infrastructuur te beveiligen. De praktijk leert echter dat hard- en softwarefabrikanten niet altijd even snel met een oplossing voor kwetsbaarheden komen waardoor hard- en/of software mogelijk kwetsbaar zijn voor cybersecurityincidenten. Deze afhankelijkheid van genoemde fabrikanten beperkt daarbij de mogelijkheden om passende en evenredige maatregelen te nemen om de risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen, zoals de conceptwet in artikel 7 verplicht stelt. Dit komt de beveiliging van genoemde infrastructuren niet ten goede.

Er bestaat geen honderd procent bescherming tegen cybersecurityincidenten, maar optimale veiligheid kan alleen worden bereikt wanneer in de gehele keten – van fabrikant tot eindgebruiker – voldoende (wettelijke) veiligheidsmaatregelen worden genomen. In deze keten zijn digitaledienstenleveranciers en vitale aanbieders belangrijk, maar evident niet de enigen, terwijl het zwaartepunt van cybersecurityregulering bij deze leveranciers wordt neergelegd. KPN begrijpt de complexiteit om passende regulering te maken voor hard- en softwarefabrikanten. Toch is het te betreuren dat er in de NIB-richtlijn geen nadere maatregelen zijn genomen om de verantwoordelijkheid van hard- en softwarefabrikant voor het leveren van degelijke producten en het onderhouden van hun producten te vergroten.

KPN pleit daarom voor een grotere verantwoordelijkheid voor fabrikanten van hard- en software voor de kwaliteit en veiligheid van hun producten. De ruimte die de NIB-richtlijn in overweging 58 geeft kan worden benut door hier passende nationale wet- en regelgeving voor te maken, bijvoorbeeld als onderdeel van de Cybersecuritywet. Een meldplicht is nodig om te zorgen dat kwetsbaarheden in hard- en software worden gemeld en waarmee deze fabrikanten zo nodig kunnen worden gedwongen om zo spoedig mogelijk kwetsbaarheden die een veiligheidsrisico vormen te repareren. Gezien de complexiteit en de schaal is voor dit onderwerp Europese wetgeving nodig, KPN roept daarom op om dit onderwerp zo spoedig mogelijk Europees te agenderen.

Delen van informatie en eenduidige definitie voor inbreuken en incidenten

Cybersecurityincidenten bij een digitaledienstverlener of vitale aanbieder zijn soms onderdeel van een grotere aanval of hebben het risico dat zij overslaan naar andere aanbieders. Het is daarom van belang dat relevante informatie over een incident, gemeld zoals omschreven in hoofdstukken drie en vier, wordt gedeeld met in ieder geval vitale aanbieders, waaronder degenen die openbare communicatienetwerken of openbare elektronische communicatiediensten aanbieden. Dit is nodig om te zorgen dat deze partijen bij een breder incident mitigerende maatregelen kunnen nemen wanneer dat nodig is. Op deze manier wordt zorggedragen dat vitale aanbieders niet worden verrast terwijl relevante informatie om een dergelijk incident te voorkomen al beschikbaar was, zo wordt voorkomen dat deze aanbieders geraakt worden door incidenten. In het geval van vitale aanbieders bevordert dit de nationale veiligheid.

Inbreuken en incidenten

In artikel 10 wordt onder 1 b gesproken over een inbreuk op de beveiliging van netwerken informatiesystemen die aanzienlijke gevolgen kan hebben voor de continuïteit van de door hem verleende dienst. Dit is de enige plek in de conceptwet waar wordt gesproken

over 'inbreuken', andere artikelen spreken over 'incidenten'. Ook de NIB-richtlijn spreekt enkel over 'incidenten'.

Het wordt echter niet toegelicht of er sprake is van een verschil in definities en of het zo kan zijn dat bij de beveiliging van netwerk- en informatiesystemen een incident kan plaatsvinden, terwijl er geen sprake is van een inbreuk. Om te voorkomen dat dit verschillend wordt uitgelegd is het aan te raden om een eenduidige definitie te gebruiken voor incidenten en inbreuken of om nader toe te lichten waarin een inbreuk zich precies onderscheidt van een incident.