Energeia

Netbeheerders gaan cyberaanvallen melden

Tijdo van der Zee
31 juli 2017

AMSTERDAM (Energeia) - De Wet gegevensverwerking en meldplicht cybersecurity, die deze maand door de Eerste Kamer werd goedgekeurd, is een nieuwe stap van de wetgever om het toenemende cybergevaar het hoofd te bieden. Ook de energiesector krijgt met de wet te maken. Jeroen Naves en Margot van Meeuwen-Verbaan van advocatenkantoor Pels Rijcken & Droogleever Fortuyn: "We moeten nu wel haast maken".

De wereldwijde cyberaanval die vorige maand een deel van de Rotterdamse haven platlegde, toont nog maar eens aan dat de samenleving kwetsbaar is geworden voor kwaadwillenden in het digitale domein. Het Nationaal Cyber Security Centrum (NCSC), een centrum dat valt onder het ministerie van Justitie en Veiligheid, waarschuwde dan ook: de digitale weerbaarheid van Nederland blijft achter op de groeiende dreiging.

De nieuwe wet schrijft voor dat bedrijven en overheidsorganisaties binnen 'vitale sectoren' digitale aanvallen verplicht melden bij het NCSC. "En dan gaat het niet alleen om aanvallen die daadwerkelijk schade hebben berokkend", zegt Naves, "maar ook aanvallen die afgeslagen zijn. Juist die, omdat je wil weten welke methoden cybercriminelen gebruikt hebben."

Een melding bij het NCSC bevat in ieder geval informatie over de aard en omvang van de aanval, het vermoedelijke tijdstip, de mogelijke gevolgen, de prognose van de hersteltijd en de getroffen of te nemen herstelmaatregelen, zegt Naves. "En dan wil het NCSC liever hebben dat je ze direct inlicht en later de melding aanvult. Directe melding geeft de mogelijkheid om snel te handelen."

Vitale sectoren

Maar wat zijn nu 'vitale' aanbieders? "Dat zijn bedrijven en organisaties waarvan de samenleving veel nadeel ondervindt als ze stil komen te liggen", zegt Van Meeuwen-Verbaan. "Dus dat betekent bijvoorbeeld dat Schiphol hier wel onder valt, maar de luchthaven in Rotterdam vooralsnog niet." Voor de energiesector gaat het om de gas- en elektriciteitsnetbeheerders, van zowel de regionale netten als van de transmissienetten. Eigenaren of exploitanten van grote energiecentrales zijn ervan gevrijwaard, behalve dan van de kerncentrale in Borssele, want voor de nucleaire sector geldt ook een

meldplicht.

"De wet loopt vooruit op een Europese richtlijn, de Richtlijn netwerk- en informatiebeveiliging [NIB-richtlijn, red.]", zegt Naves. "Maar de Nederlandse wetgever was al met de Wet gegevensverwerking en meldplicht cybersecurity aan de slag toen de richtlijn in de conceptfase zat, en dat heeft tot gevolg dat deze wet geen volledige uitwerking is van de richtlijn. De wetgever zal de wet voor die datum aanvullen."

Geen handen-in-het-haar-taferelen

Dat zijn bijvoorbeeld aanpassingen in de lijst van bedrijven en instellingen die incidenten zullen moeten melden, zegt Van Meeuwen-Verbaan. "Ziekenhuizen vallen er nu niet onder, maar gaan er wel onder vallen. De Amsterdamse haven zit er nu nog niet bij, maar dat gebeurt straks wel." Het NCSC verzamelt alle meldingen -"dat zullen er niet veel meer zijn dan een handvol per jaar"- en bekijkt per geval wat er moet gebeuren. Of bijvoorbeeld andere bedrijven en instellingen op de hoogte gebracht moeten worden, om de schade zo beperkt mogelijk te houden.

De Europese richtlijn ziet er op toe dat de verschillende nationale veiligheidscentra onderling contact houden en elkaar inlichten op het moment dat er in één van de landen een aanval gemeld wordt. Op deze manier, zo is de bedoeling, wordt de veiligheid in heel Europa vergroot. Het feit dat het aantal meldplichtigen in ieder geval redelijk beperkt blijft, zal er toe leiden dat er geen toestanden ontstaan zoals nu bij de Autoriteit Persoonsgegevens, die door de duizenden meldingen die binnenkomen in verband met de meldplicht datalekken met de handen in het haar zit.

Beveiligingsmaatregelen

Een tweede aanpassing is eigenlijk veel belangrijker. De NIB-richtlijn schrijft namelijk voor dat organisaties in de betreffende vitale sectoren passende beveiligingsmaatregelen nemen. "Het is nu nog niet duidelijk of dit een lijst van duidelijke eisen wordt, of dat dit minder concreet beschreven wordt zoals in de tekst van de NIB-richtlijn het geval is", zegt Naves. Deze eis uit de richtlijn zal waarschijnlijk een plek krijgen in de Wet gegevensverwerking en meldplicht cybersecurity, denkt Naves. "Daarover zal nu heel snel vergaderd moeten worden. Er is haast geboden, want ook dit onderdeel van de richtlijn moet uiterlijk 9 mei 2018 in Nederlandse wetgeving zijn geïmplementeerd."

Hoe zit het eigenlijk met handhaving? Een wet zonder handhaving is een tandeloze

tijger. Die zit nu niet in de wet -en dat is geheel volgens de wens van werkgeversorganisatie VNO-NCW. "Maar sancties zullen er straks wel inkomen", zegt Naves. De invulling van de sancties wordt door de NIB-richtlijn aan de lidstaten overgelaten, maar vaststaat dat deze doeltreffend, evenredig en afschrikwekkend moeten zijn. . Overigens hoeven bedrijven straks echt niet bang te zijn dat hun meldingen, met alle ins en outs publiek zullen worden gemaakt. De NCSC zal er prudent mee omgaan, verwacht Van Meeuwen-Verbaan. "De NCSC zal aan het eind van het jaar wellicht een lijst publiceren van het aantal meldingen per sector. Zoiets. Bedrijfsgevoelige informatie blijft vermoedelijk geheim."

© 2017 Energeia. Alle rechten voorbehouden.