Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

Visie Microsoft op het voorstel voor een Cybersecuritywet ter implementatie van de NIB-richtlijn van de Europese Unie (richtlijn 2016/1148)

Bewustwording over de risico's van cyberaanvallen en de noodzaak tot bescherming van netwerk- en informatiesystemen zijn van groot strategisch belang geworden, zowel in Nederland als op Europees en internationaal niveau. Microsoft geeft grote prioriteit aan de beveiliging van netwerk- en informatiesystemen, omdat de bescherming van onze klanten bij het gebruik van onze diensten en systemen cruciaal is voor hun vertrouwen in onze technologie. We geven hier invulling aan door IT-infrastructuur te beschermen, technologie te ontwerpen om cyberaanvallen te voorkomen en ons ertegen te wapenen, en door in dialoog te gaan met instituties en organisaties op landelijk, Europees en wereldwijd niveau.

De implementatie van de NIB-richtlijn in de Cybersecuritywet biedt Nederland een uitgelezen kans om een efficiënt regelgevend raamwerk te creeëren in nauwe harmonie met andere EU-lidstaten op basis van Europese regelgeving. Doelstelling moet zijn om eventuele hiaten te vullen en zo veel als mogelijk op bestaand cybersecurity-beleid door te bouwen, zoals in Nederland op het werk van het Nationaal Cybersecurity Centrum (NCSC) en de Nationale Cybersecurity Strategie (NCSS).

Microsoft verwelkomt de adoptie van de NIB-richtlijn, die in het licht van de groeiende noodzaak voor een algemeen hoger niveau van netwerk- en informatiebeveiliging zowel in Europa als wereldwijd de kaders biedt voor EU Lidstaten om mee aan de slag te gaan. Microsoft is verheugd via deze internetconsultatie haar visie te kunnen geven op het belang van een geharmoniseerde, heldere en efficiënte implementatie van de Richtlijn in Nederland.

Regulering van digitale diensten

Gegeven de specifieke eigenschappen van digitale diensten die in meerdere EU-lidstaten tegelijkertijd actief zijn, is een geharmoniseerd regelgevend raamwerk essentieel voor deze diensten om succesvol over grenzen heen te kunnen opereren. Verschillende soorten digitale diensten – clouddiensten (en dan vooral publieke clouddiensten), online zoekmachines en online marktplaatsen – vertegenwoordigen drie verschillende onderdelen van de digitale economie met drie verschillende niveaus van criticaliteit. Verplichtingen voor digitale diensten (zoals beveiligingseisen en de meldplicht van incidenten) moeten daarom worden gedifferentieerd per categorie en de daarbij behorende criticaliteit.

De definitie van een clouddienst in de NIB-richtlijn is wat Microsoft betreft te breed en maakt niet het noodzakelijke onderscheid tussen de verschillende niveaus van criticaliteit tussen verschillende soorten diensten. Een manier om wel de grootst mogelijke helderheid te verschaffen voor de criticaliteit van een clouddienst is door de definities te hanteren van de ISO17788 : 2014-standaard, zoals het type cloud (applicatie, platform of infrastructuur) en het model cloud (privaat, gemeenschap, hybride of publiek).

Clouddiensten gebaseerd op het type infrastructuur, ook wel Infrastructure-as-a-Service (Iaas) genaamd, hebben significante impact bij de overweging van criticaliteit in bepaalde omstandigheden. Zoals uitgelegd in sectie 10.2.1 (*"Service capabilities functional component")* van ISO 17789 : 2014-standaard kan een applicatie (i.e. Software-as-a-Service or SaaS) worden geïmplementeerd door het gebruik van een platform (i.e. Platform-as-a-Service or PaaS), welke op

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

haar beurt weer kan worden geïmplementeerd door het gebruik van infrastructuur (IaaS). De raakvlakken tussen deze opeenvolgende lagen die nodig zijn om clouddiensten te beheren betekenen dat een IaaS incident wellicht een grotere criticaliteit kan hebben dan een Paas of Saas incident. Daarnaast zijn publieke clouddiensten potentieel beschikbaar voor elk soort gebruiker. Publieke clouddiensten zouden daarom een hogere criticaliteit kunnen hebben dan private clouddiensten, zoals uitgelegd in sectie 8.5.12.4 ("*Implications of cloud deployment models*") van ISO-standaard 17789 : 2014. Dientengevolge zouden, binnen de doelstellingen van de NIB-richtlijn, de verplichtingen voor clouddiensten alleen toepasbaar moeten zijn op publieke IaaS clouddiensten.

De beveiligingsvereisten en meldplicht van incidenten moeten daarom implicaties van de criticaliteit van zowel IaaS- als publieke clouddiensten in overweging nemen zodat Nederland haar cybercapaciteit zo efficiënt en effectief mogelijk kan richten op het addresseren van de risico's van clouddiensten in de breedte.

Operators of Essential Services (OESs)

De Cybersecuritywet zou in operationele cybersecurity-maatregelen moeten voorzien op basis van, zoals in de NIB-richtlijn voorzien, een risico-gebaseerde en uitkomstgerichte benadering. Capaciteitsopbouw op het gebied van cybersecurity kan daarmee zo consequent mogelijk worden uitgerold in de gehele EU. Effectieve zogenoemde *security baselines* zijn een kritieke component van een robuust raamwerk voor het management van cyber-risico´s, zowel in de publieke als private sector. In deze context beveelt Microsoft aanbieders van kritieke diensten (*operators of essential services OESs*) aan om standaardprocessen van risicobeheer en de monitoring daarvan te ontwikkelen. Ook moeten daarbij bestaande internationale *best practices* in overweging worden genomen, zoals het *NIST Framework for Improving Critical Infrastructure Cybersecurity*.

Harmonisatie is ook van belang bij het definïeren van essentiele diensten, zoals dat door de Nederlandse regering is gedaan voor bijvoorbeeld waterkeringen. Bij de vertaling naar de Cybersecuritywet van welke kritieke infrastructuur onder essentiële diensten valt is het van belang dat de *OES* categoriën uit de NIB-richtlijn worden gehanteerd. Daarmee wordt de strekking van harmonisatie zoals in de Richtlijn opgenomen gerespecteerd en wordt bovendien de nu beschikbare capaciteit in de Lidstaten beter ingezet voor de bescherming van strategische infrastructuur. Om overlap tussen de Lidstaten te voorkomen vereist effectieve implementatie van de NIB-richtlijn het gebruik van *Security Baselines Harmonization* in de gehele EU.

Harmonisatie tussen EU-Lidstaten en publiek-private samenwerking

Het verbeteren van cybersecurity-samenwerking en het delen van informatie tussen EU Lidstaten is van groot belang om cyberweerbaarheid in de gehele EU te versterken. Microsoft suggereert daarom dat de daarvoor nationaal verantwoordelijke autoriteiten nauwer samenwerken met hun tegenhangers in andere Lidstaten, net als met relevante partijen in de private sector. Cybersecurity is een onderwerp met veel raakvlakken, en de technologie-sector is zowel doelwit als eerste respondent bij cyberdreigingen.

Vrijwillige samenwerking en informatiedeling tussen de nationale autoriteiten moet worden aangemoedigd en versterkt. Tegelijkertijd hebben dialogen en wederzijds vertrouwen geen invloed op het principe van territoriale verantwoordelijkheid jegens digitale diensten. Ofwel: alleen de nationaal verantwoordelijke autoriteit van een Lidstaat waarin de hoofdvestiging van een digitale

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

dienst zich bevindt heeft daadwerkelijk territoriale verantwoordelijkheid. Een meldplicht van incidenten moet daarom niet verward worden met vrijwillige samenwerking en informatiedeling.

Conclusie

Vanwege haar significante strategische belang is de NIB-richtlijn een belangrijke manier om het algehele niveau van netwerk- en informatiebeveiliging te verhogen, zowel in Nederland als in de hele EU. Een helder en geharmoniseerde implementatie van de NIS-richtlijn naar de Cybersecuritywet is een fundamentele stap naar een helder kader van regelgeving.

Jochem K.A. de Groot
Directeur Corporate Affairs
Microsoft Nederland