Internetconsultatie Cyberbeveiligingswet (NIS2) – reactie Cisco Nederland

Cisco Nederland verwelkomt de implementatiewet van de NIS2-Richtlijn. De snelle ontwikkelingen in het digitale landschap en de bijbehorende uitdagingen gecombineerd met een toenemende geopolitieke spanningen dwingt de Europese Unie om een stevig kader neer te zetten om cyberveiligheid te garanderen en de digitale weerbaarheid te verhogen. Als marktleider in veilige connectiviteit binnen vitale processen en de vitale infrastructuur van Nederland ziet Cisco de NIS2-Richtlijn als belangrijk raamwerk dat de juiste tools heeft om dit te borgen – veelal in samenspraak met de Aanpak Vitaal.

In deze internetconsultatie geeft Cisco graag haar reactie op de implementatiewet. Als Cisco dragen we grote verantwoordelijkheid om de cyberveiligheid van Nederland te verzekeren. Vanuit deze verantwoordelijkheid delen we graag onze expertise. In deze reactie leest u een aantal vragen, suggesties en andere opmerkingen waar wij zorg over dragen. We hebben ons best gedaan dit zo volledig mogelijk te noteren en staan er altijd voor open om dit nader toe te lichten.

1. **Gemaakte implementatiekeuzes**

Hoofdstuk 4 benoemt welke organisaties onder de NIS2-Richtlijn zullen vallen en welke niet. Vanuit Cisco begrijpen we dat er een afweging is gemaakt op basis van dreigingsniveau. We herkennen echter dat door het groeiende dreigingsniveau van cyberaanvallen de NIS2 het moment is om zoveel mogelijk organisaties mee te nemen.

In dit hoofdstuk staat dat de verantwoordelijkheid van de aanwijzing van essentiële entiteiten interdepartementaal wordt belegd, door meerdere bewindspersonen of uitvoeringsinstanties de autoriteit hierover te geven. Cisco herkent dat een complexe wetgeving als de NIS2 centrale aansturing behoeft, vooral als het gaat op de aanmerking van entiteiten als essentieel. Fragmentatie van verantwoordelijkheid kan leiden tot onnodige verwarring. Om dit te voorkomen ziet Cisco het als essentieel om één autoriteit te hebben die de entiteiten aanmerkt, zoals de Minister van Justitie en Veiligheid. Ministers van andere departementen kunnen als adviseur optreden. Door de gevoeligheid van de aard van de werkzaamheden is het verantwoordelijk om één autoriteit te hebben.

2. **Meldplicht**

Paragraaf 5.6 Informatiedeling stelt dat partijen voor wie het relevant is worden geïnformeerd en geadviseerd over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen. Cisco erkent het belang van een goede meldplicht en zorgplicht de basis vormt van de NIS2. Wel voegen we hieraan toe dat het belangrijk is dat er duidelijke richtlijnen zijn over het soort meldingen dat gedeeld moet worden. Het is niet praktisch of haalbaar en zelfs contraproductief als alle signalen die wij ontvangen doorgeven aan diensten. Vaak is het zo dat gedetecteerde signalen zijn opgelost, voordat we de kans zouden hebben om het te melden. Wij adviseren daarom dat er een richtlijn wordt opgesteld die stelt dat alleen significante incidenten gemeld worden. Dit voorkomt informatie-overload en zorgt ervoor dat de ontvangers alleen relevante en actiegerichte informatie ontvangen. Zo'n richtlijn kan gelden als basis. We zien ook het belang van ruimte voor individuele afspraken om de meldplicht strenger in te richten, namelijk al bij kleinere incidenten. We denken graag mee over de inrichting van een dergelijke richtlijn en het raamwerk dat bepaalt wanneer een melding van toepassing is.

3. **Financiële borging**

Organisaties door heel Nederland – klein en groot – lopen aan tegen het vraagstuk hoe ze de nieuwe maatregelen kunnen en moeten financieren. Deze zorg komt voort uit ervaringen van security specialisten die vaak nog onvoldoende draagvlak ervaren bij hun management. Enerzijds kan dit komen

door onvoldoende security kennis, anderzijds vereist het opschalen van cyberveiligheidsmaatregelen een flinke financiële inspanning. Niet elke organisatie kan die dragen.

Cisco stelt voor om naar Vlaams voorbeeld te onderzoeken wat de mogelijkheden zijn om organisaties subsidies te bieden voor cybersecurity verbetertrajecten. Het Vlaams Agentschap Innoveren & Ondernemen subsidieert bij mkb en maatwerkbedrijven 50% van de kosten wanneer externe begeleiding is ingekocht voor het duurzaam verbeteren van hun cyberveiligheid. Bij ondernemingen die niet voldoen aan de mkb-criteria maar wel onder de NIS2-richtlijn vallen bedraagt de tussenkomst van VLAIO 35% van de kostprijs. Een dergelijke subsidie kan veel Nederlandse mkb'ers ondersteunen in hun transitie naar een cyberweerbare organisatie die voldoet aan de NIS2-eisen. Wellicht kan zo'n subsidie gekoppeld worden aan de invulling van een mkb-keurmerk op cyberveiligheid aan de motie van het Lid Rajkowski.

4. **Toekomstbestendige wetgeving**

Bij de totstandkoming van de NIS2 was generatieve AI nog niet op de markt. Sindsdien is het gebruik van kunstmatige intelligentie wijdverspreid en is een AI-Verordening aangenomen. Hiermee heeft AI ook haar intreden gedaan in het offensieve en defensieve cyberdomein. Vanuit Cisco uiten we onze zorgen over de toekomstbestendigheid van de NIS2 en of deze Richtlijn de huidige ontwikkelingen omtrent AI kan meenemen in compliance trajecten. We zien dat het nodig is dat er een brug wordt geslagen tussen de AI Act en de NIS2, zowel op Europees niveau, als in de Nederlandse uitvoeringswet.

Over Cisco

Cisco is de wereldwijde technologieleider die veilige connectiviteit levert en cyberweerbaarheid garandeert. Cisco levert het meest uitgebreide platform voor beveiligingsoplossingen voor preventie, opsporing, onderzoek en de reactie op bedreigingen voor organisaties van elke omvang, waarbij gebruik wordt gemaakt van cloud-, netwerk- en endpointverkeer. Ons doel is om een inclusieve toekomst voor iedereen te realiseren door onze klanten te helpen hun toepassingen opnieuw te herdefiniëren, onderneming te beveiligen, infrastructuur te transformeren en hun duurzaamheidsdoelstellingen te behalen.

Om haar maatschappelijke betrokkenheid te verdiepen is Cisco in 2017 gestart met haar investeringsprogramma Digitale Versnelling Nederland (DVN). Inmiddels loopt de tweede termijn, waarbij er specifiek aandacht is voor vitale infrastructuur, cyberveiligheid en gezondheidszorg. DVN heeft de afgelopen jaren met verschillende maatschappelijke partners succesvolle projecten opgezet. Voorbeelden hiervan zijn publiek-private samenwerkingen met het UWV, het Havenbedrijf, het EOKM, onderwijsinstellingen en verschillende departementen. Kortom, met Digitale Versnelling Nederland werkt Cisco aan een solide fundament als randvoorwaarde voor een veilige, inclusieve en duurzame digitale samenleving.