Internetconsultatie Cyberbeveiligingswet (NIS2) – reactie SURF

SURF is de ICT-coöperatie van onderwijs en onderzoek. Binnen SURF werken universiteiten, hogescholen, mbo-instellingen, umc's en onderzoeksinstellingen samen om de best mogelijke digitale diensten in te kopen of te ontwikkelen en om kennisdeling te stimuleren door steeds te blijven innoveren. Momenteel biedt SURF ruim vijftig diensten aan de leden, waaronder ICT-beveiligingsdiensten. Eén van de diensten betreft SURFcert, welke de CERT-functie voor de sector vervult. SURFcert biedt al meer dan dertig jaar ondersteuning en advies aan de leden bij cyberincidenten en kijkt continu of er bedreigingen zijn op het netwerk dat SURF voor leden beheert. Vanuit deze ervaring heeft SURF gekeken naar de werkbaarheid van de voorgestelde wet en onderstaande reactie geformuleerd.

De Cyberbeveiligingswet (Cbw) implementeert de Europese NIS2-richtlijn. De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. SURF onderschrijft het belang van een hoog gemeenschappelijk niveau van digitale weerbaarheid. Naar aanleiding van het wetsvoorstel worden de volgende punten onder de aandacht gebracht:

1. **Versterk samenwerking**

Goede informatiedeling is van cruciaal belang voor het versterken van de digitale weerbaarheid. De Cbw zou het cybersecuritystelsel daarom moeten verbeteren door samenwerking te versterken, ongeacht of organisaties wel of niet onder NIS2 vallen. Voor beide groepen organisaties is de behoefte aan juiste informatie en ondersteuning vanuit een CSIRT namelijk evident. Paragraaf 5.6.5 van de MvT besteedt aandacht aan de toewijzing van zogeheten schakelorganisaties. Volgens SURF is het wenselijk hier explicieter uit te werken op welke wijze organisaties die niet onder NIS2/Cbw vallen worden ondersteund en toegang krijgen tot (dreigings)informatie en ondersteuning bij (grote) incidenten. Dit onderstreept tevens het belang van het optimaal borgen van de positie van sectorale CSIRTs, waarbij zoveel mogelijk gelijkwaardigheid wordt nagestreefd, ongeacht of de betreffende sectoren wel of niet (geheel) onder NIS2/Cbw vallen.

2. **Waarborg rolvastheid bij incidenten**

In overeenstemming met artikel 29 en 30 van het wetsvoorstel moet een essentiële of belangrijke entiteit in het geval van een incident melding maken bij haar CSIRT en de bevoegde autoriteit. Bovendien dient een essentiële of belangrijke entiteit op verzoek van haar CSIRT of de bevoegde autoriteit tussentijds verslag uit te brengen over relevante ontwikkelingen. SURF pleit voor grote terughoudendheid met de verplichting voor een entiteit om op verzoek van haar CSIRT of de bevoegde autoriteit tussentijdse verslagen uit te brengen. Wij hechten grote waarde aan rolvastheid van alle betrokken partijen gedurende een incident. Bovendien is het van belang om met

name in de warme fase van een incident onnodige regeldruk te vermijden. Het is daarom wenselijk dat de bevoegde autoriteit of CSIRT gepaste afstand houdt gedurende de warme fase van de incidentafhandeling, zodat de essentiële of belangrijke entiteit zo effectief mogelijk kan handelen in overeenstemming met de primaire verantwoordelijkheden.

3. Beperk administratieve lasten

De wetgever voorziet met voorliggend wetsvoorstel een toename in regeldruk, onder andere in de vorm van administratieve lasten. SURF is van mening dat deze regeldruk tot een minimum moet worden beperkt. Zeker met betrekking tot de dubbele meldplicht (artikel 29.1) dient beter uitgewerkt te worden op welke manier extra regeldruk wordt voorkomen. Daarbij zou het voorkomen van dubbele administratie van incidentmeldingen (MvT 8.1.3) verder moeten gaan dan enkel een inspanningsverplichting voor de overheid.

Daarnaast valt artikel 45 op, waarin onder andere is opgenomen dat IP-bereiken via een daarvoor opgezet mechanisme aangeleverd dienen te worden, met aanvullend de verplichting om wijzigingen door te geven. Voor organisaties die grote aantallen reeksen IP-adressen beheren kan dit een behoorlijke last zijn. Bovendien merken wij op dat het gevoelige data betreft die niet in verkeerde handen dient te vallen. Uitgangspunt in deze dient data bij de bron te zijn. Dat verhoogt de accuraatheid van de gegevens en vermindert de kans dat de gegevens gecompromitteerd worden. Dit zou uitgangspunt moeten zijn bij de uitwerking in een algemene maatregel van bestuur zoals bedoeld in artikel 45.3.

4. Bescherm vertrouwelijkheid

In paragraaf 9.3 is onder meer uitgewerkt op welke wijze informatie van meldingen gedeeld kan worden met andere organisaties. Bepaalde meldingen zijn daarentegen voorzien van TLP-coderingen waarin staat aangegeven op welke wijze de informatie al dan niet gedeeld kan worden. Het wetsvoorstel lijkt hieraan voorbij te gaan. Het functioneren van het cybersecuritystelsel is ten dele gestoeld op de vertrouwensrelatie tussen CSIRT en haar melders. Wanneer deze relatie wordt ondermijnd doordat vertrouwelijkheid niet kan worden gegarandeerd, schaadt dit het functioneren. Graag benadrukken we daarom het belang van de vertrouwelijkheid en roepen op om de mogelijkheid tot het in stand houden van de vertrouwelijkheid ook in het wetsvoorstel te erkennen en borgen.