3rdRisk Solutions B.V.
Herengracht 124-128
1015 BT Amsterdam

Amsterdam, 28 juni 2024.

Betreft: Reactie 3rdRisk op de Cyberbeveiligingswet (Cbw).

Allereerst danken wij voor de mogelijkheid om via deze consultatie feedback te kunnen geven op de Cyberbeveiligingswet (vanaf nu Cbw). Graag maken wij van deze gelegenheid gebruik.

De Cbw implementeert de Europese Network and Information Security 2-richtlijn. De NIS2 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. Een doelstelling die wij ten zeerste ondersteunen.

Onze feedback op de concept wettekst en de memorie van toelichting beperkt zich tot ons expertisegebied, namelijk de beheersing van (informatiebeveiligings)risico's die ontstaan door de samenwerking met derde partijen, zoals verkopers, dienstverleners en partners.

Wij doen 3 observaties:

1. Geen expliciete aandacht voor de toeleveringsketen in de concept wettekst
2. Zorgplicht 'beveiliging van toeleveringsketen' mist concreetheid
3. Proactieve monitoring ontbreekt als onderdeel van de zorgplicht

Deze observaties zullen we hieronder uitwerken.

<u>Observatie 1: Geen expliciete aandacht voor de toeleveringsketen in de concept wettekst</u>

Hoofdstuk 7 in de concept wettekst gaat over de zorgplicht. In artikel 23 lid 1 en 2 staan de maatregelen beschreven die in lijn moeten zijn met de risico's.

De eerste observatie is dat de 'toeleveringsketen' of 'derde partijen' als zodanig niet terug te vinden zijn in dit hoofdstuk, laat staan de rest van de concept wettekst.

Dit is opmerkelijk gezien de toenemende trend waarbij organisaties steeds meer activiteiten en kritieke processen uitbesteden aan derde partijen. Het gevolg hiervan is dat de afhankelijkheid van derde partijen groeit en organisaties steeds kwetsbaarder worden voor incidenten bij derde partijen. Ons advies zou daarom zijn om in de wettekst zelf ook nadrukkelijk het belang van de toeleveringsketen te benadrukken.

Observatie 2: Zorgplicht 'beveiliging van toeleveringsketen' mist concreetheid

In de memorie van toelichting worden in paragraaf 5.3.4 de technische, operationele en organisatorische maatregelen uitgewerkt. Hier wordt geheel in lijn met de NIS2 richtlijn de beveiliging van de toeleveringsketen genoemd.

De memorie van toelichting stelt op bladzijde 21:

> *In artikel 21, tweede lid, NIS2-richtlijn is bepaald dat de door essentiële entiteiten en belangrijke entiteiten te nemen maatregelen ten minste het volgende moeten omvatten: […] d. beveiliging van de toeleveringsketen;*

Vervolgens wordt dit aspect twee paragrafen eronder als volgt uitgewerkt:

> *"Ten aanzien van de beveiliging van de toeleveringsketen [punt d] wordt in artikel 21, tweede lid, onderdeel d, en derde lid, NIS2-richtlijn aangegeven dat dit met inbegrip is van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Wanneer essentiële entiteiten en belangrijke entiteiten overwegen welke maatregelen in dit verband passend zijn, moeten zij rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures…"*

Wij volgen deze uitwerking. Echter blijft 'beveiliging van de toeleveringsketen' voor ons een abstract begrip dat concreetheid mist. Beter zou het volgens ons zijn om te spreken van 'beheersen van cyberrisico's in de toeleveringsketen'. Hiervoor hebben we de volgende redenen:

- Deze terminologie sluit beter aan bij vergelijkbare Europese initiatieven op andere risicodomeinen, zoals de CSRD and CSDDD op het gebied van duurzaamheid, waarin ook een zorgplicht wordt uitgewerkt om risico's en misstanden in de keten proactief op te sporen, te beoordelen en, indien onacceptabel, te beperken.
- In tegenstelling tot het begrip beveiliging is het bij ketenrisicobeheersing duidelijker welke concrete activiteiten het omvat, namelijk het inventariseren, analyseren, evalueren, behandelen en monitoren van cyberrisico's die voortkomen uit de keten.

Observatie 3: Proactieve monitoring ontbreekt als onderdeel van de zorgplicht

Tot slot valt het ons op dat de zorgplicht met name lijkt te bestaan uit reactieve maatregelen. Het cyberdreigingslandschap is echter dynamisch en vergt daarom continue monitoring van dreigingen en andere signalen. Dit geldt zeker ook voor de toeleveringsketen. Goede screening en certificering van ketenpartners zijn belangrijk, maar tegelijkertijd van relatieve waarde in een wereld waarin zowel de organisatie als haar buitenwereld razendsnel verandert. Daarom zouden wij willen adviseren om in de zorgplicht een vorm van proactieve monitoring op te nemen.

Bram Ketting [bram@3rdrisk.com], Rick Sollet [rick@3rdrisk.com], en Jelle Groenendaal [jelle@3rdrisk.com] zijn oprichters van 3rdRisk, een Nederlandse start-up dat een cloud platform heeft ontwikkeld om de beheersing van ketenrisico's gemakkelijker en efficiënter te maken. Voor meer informatie over onze visie en het platform: www.3rdrisk.com.