Auteurs: Gerard Doeswijk werkt bij SkyKick Seattle in de functie van Vice President Cybersecurity & Data Protection met als aandachtsgebieden softwareontwikkeling op basis van agile, data protection by design en default principes. Daarnaast houdt hij zich bezig met certificering- en assurancetrajecten van de back-up, cloud management en security SAAS/PAAS-producten. Hij is ingenieur in de informatica, gecertificeerd in agile methodieken, gecertificeerd lead auditor voor ISO 27001, ISO 22301 en CISA. Hij is bereikbaar via https://www.linkedin.com/in/gdoeswijk/

NIS2 en de regie op orde in de (cloud-)keten

IT-supply chain, compliance, incident management, cloud- en business-continuity. Om maar even met de deur in huis te vallen met een paar prachtige 'Dunglish' krachttermen die vandaag de dag (weer) op de agenda (zouden moeten) staan van de bestuurders c.q. board die druk bezig zijn met de volgende (IT-)governance uitdaging.

Nu we eindelijk een beetje grip gekregen op de Algemene Verordening Gegevensbescherming – in de volksmond vaak GDPR genoemd – moeten we met zijn allen alweer vol aan de bak met de Network Information and Security 2 (NIS2)-richtlijn. En? Weet u al wat die NIS2-richtlijn in concrete zin voor uw organisatie moet gaan betekenen? Of bent u, net als ik, druk in gesprek met consultants, advocaten en leest u ook de summiere toelichting bij de richtlijn op de website van het Nationaal Cyber Security Centrum?

Van uitstel komt geen afstel

Gelukkig hebben we in Nederland een beetje respijt gekregen. Het is natuurlijk niet duidelijk of de val van het kabinet in 2023

hier iets mee te maken heeft gehad. Maar wat zou het. Wat we wel weten is dat het Ministerie van Justitie en Veiligheid heeft geconstateerd dat zij de deadline van 17 oktober 2024 niet zullen halen.

Net als met de AVG blijft natuurlijk de Europese deadline hetzelfde, en van uitstel komt zeker geen afstel. Dus als u nog niet bent begonnen met de voorbereiding dan… Nou ja, vult u zelf maar in of u meer van paniekvoetbal of een rustig potje schaken houdt.

Concreet zijn er wel al een paar zaken. Zo kunt u in ieder geval al (laten) vaststellen of uw organisatie zich moet registreren en of u dat als een essentiële of belangrijke NIS2-entiteit (1) moet doen. En dan is er de zorgplicht (2), een mooi eufemisme voor vereisten of gebruiken we tegenwoordig liever de term requirements? Want dat is toch vaak iets dwingender, zeker als het in een contract is opgenomen.

Want u zult een risicoanalyse doen, en beleid en procedures voor incidentenbehandeling hebben. Om nog maar niet te spreken van noodvoorzieningenplannen (een mooie voor het spel galgje), een back-up en nog meer van dat soort kostbare zaken.

De pijn verzachten

Maar de essentie zit hem, net als bij de AVG, toch weer in de keten. U zult, en ik kan dit niet hard genoeg benadrukken, móéten weten hoe de informatiebeveiliging van álle toeleveranciers in uw IT-supply chain is geregeld én of deze dan ook voldoet aan de vereisten van de NIS2-richtlijn. En hier zit natuurlijk de crux en de pijn. Want u leest het al, het is een richtlijn en de vereisten moeten nog worden vastgelegd in (nationale) wetten en regelgeving. En die zijn nu juist nog even uitgesteld!

Rollen de questionnaires, de zogenaamde secondparty-audits, en de eerste NIS2-overeenkomsten alweer gestaag bij uw IT- en juridische afdeling binnen? Of heeft u proactief uw inkoopafdeling op pad gestuurd om de pijn voor uw eigen organisatie iets te verzachten? Nu kunnen we natuurlijk, lekker nationalistisch gaan roepen dat deze onzin-EU-regelgeving nou weleens mag stoppen. En wellicht dat er een nieuwe minister Digitale Zaken komt die dat in Brussel kan gaan verkondigen of ook hier een 'opt-out' voor vragen. Maar dat zou toch een beetje gek staan in dit verregaand gedigitaliseerde land.

Haast

Dus wat nu? Toch maar 'een beetje voorbereiden' en al die cloudpartijen op hun verantwoordelijkheden gaan wijzen met een questionnaire? Of bent u nog één van de weinige organisaties in Nederland die alles zelf in beheer heeft in uw datacenter in de kelder? Wij houden het bij onze organisatie op de oude, vertrouwde ISO 27001 (cybersecurity), ISO 27701 (dataprotection), ISO 22301 (business-continuity) en ISO 20000 (servicemanagement). De certificering op de eerste twee heeft ons al de nodige inzichten gegeven in onze risico's en de delta tussen wat we hebben kunnen opmaken uit de richtlijn en die twee standaarden.

Afgezet tegen de Infosheet NIS2-verplichtingen is er nog wat werk te doen. En gelukkig maar, want een ISO-gecertificeerd managementsysteem brengt nu eenmaal de vereiste om aan continue verbetering te werken. En dat is en blijft natuurlijk hard nodig als het gaat om cybersecurity. Of wacht u liever op de certificering onder de Cybersecurity Act (EU Verordening 2019/881)? Eén daarvan is de European Cybersecurity Certification Scheme for Cloud Services (EUCS). Die is de in 'de ontwikkelingsfase', volgens de informatie op de website van de Cybersecuritycertificeringsautoriteit (3) (nóg eentje voor galgje!). Gezien de haast waarmee het certificeringsschema voor artikel 42 van de AVG is opgepakt, en dat dit kandidaat-certiferingsschema alweer van juli 2020 is, is het wellicht raadzaam om uw energie en middelen anders en wijzer te besteden.

Let wel, als bestuurder krijgt u ook nog eens te maken met persoonlijke aansprakelijkheid bij het niet naleven van de NIS2. Dus neemt u dat alstublieft mee in de risicoanalyse, dan is die paar ton voor een cybersecurityprogramma wellicht wat minder misselijk. En als er dan toch ergens een opt-out kan worden gezocht, is het te hopen dat de nieuwe ministersploeg de wedstrijd in Den Haag begint, voordat er naar Brussel wordt getogen.

Referenties

(1) Infosheet NIS2 verplichtingen: Registratieplicht Publicatie Nationaal Cyber Security Centrum www.ncsc.nl
(2) Infosheet NIS2 verplichtingen: Zorgplicht Publicatie Nationaal Cyber Security Centrum www.ncsc.nl
(3) Certificeringsschema's Cybersecurity certificering (NCCA) Rijksinspectie Digitale Infrastructuur (RDI)