Son, 11 juni 2024

Reactie Aschwin Geisler op de Cyberbeveiligingswet (Cbw).

Goed dat de overheid (cyber)veiligheid serieus neemt en de NIS 2 directive omzet in nationale wetgeving.

Een heel aantal opmerkingen over de concept wettekst zijn al door andere respondenten gemaakt. Naar mijn mening ontbreken nog de volgende drie:

1. In artikel 23 lid 1 wordt aangegeven “Ook neemt zij deze maatregelen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van haar diensten en voor andere diensten te beperken.”. Maar wat als de afnemer afziet van het afnemen van de dienstverlening (denk aan monitoring, kwetsbaarheidsbeheer, operationeel beheer) die incidenten kan signaleren of voorkomen? De volgende toevoeging (of tekst in die strekking) aan dat wetsartikel lost dat op: “voor zover de afnemer de hiervoor benodigde dienstverlening bij de entiteit heeft afgenomen.”.
   Het gaat er om dat als een afnemer onvoldoende beheerdienstverlening afneemt de dienstverlenende entiteit niet aansprakelijk kan worden gehouden voor de cyberkwetsbaarheid van de afnemer. Merk op dat sommige afnemers verplicht zijn hun beheerkavels bij verschillende entiteiten te moeten onderbrengen waardoor het in die gevallen onontkoombaar is dat het beheer bij een entiteit niet compleet cq onvolledig is..
2. In artikel 70 en 70a wordt de gerichte beveiligingsaudit beschreven. Is het billijk om de kosten voor deze audit bij de entiteit neer te leggen? Besef dat de entiteit ook al kosten moet maken om de audit te begeleiden en voor interviews (onderdeel van de audit) mensen zal moeten vrijmaken.
   Zeker als de entiteit al qua cyberveiligheid gecertificeerd is (ISO/IEC 27001, NEN 7510, BIO) en/of assurance verklaringen heeft (ISAE 3402, SOC 2), waarbij feitelijk de maatregelen uit artikel 21 van de NIS2 Directive worden getoetst. In zulke gevallen is de audit dubbelop en is het in rekening brengen van de kosten voor de audit naar de entiteit lastig te rechtvaardigen.
3. In artikel 71 wordt gesteld dat de bevoegde autoriteit de entiteit kan verplichten een overtreding openbaar te maken. Hier zal zeer terughouden mee moeten worden omgegaan, zeker om eventuele (reputatie) schade door openbaring voor bijvoorbeeld leveranciers of afnemers van een entiteit te beperken of voorkomen. Mijns inziens kan een stuk extra tekst “mits door de openbaring geen schade veroorzaakt wordt” hier goede hulp bieden.

Met vriendelijke groet,

Aschwin Geisler