Artikelsgewijs commentaar

Artikel 7

Artikel 7 lid 1: De volgende zin is verwarrend en sluit andere behandelopties van risico's uit (verplaatsen, vermijden en accepteren): *"De entiteit neemt op basis van dit beleid maatregelen om op een structurele wijze tot een beveiligingsniveau te komen dat is afgestemd op de risico's."*

Advies om dit aan te passen naar:

"De entiteit komt op basis van dit beleid op een structurele manier tot een risico-overzicht en een behandeling van de risico's die in lijn is met dit beleid."

Artikel 7: Er ontbreekt in dit artikel het hebben van een risico-overzicht en het rapporteren over de status van de risico's naar de risico-eigenaar. Dit zijn essentiële aspecten voor het werken van risicomanagement en dus het nuttig laten zijn van dit proces. Zie hieronder aanvullingen *'inzicht en rapportage'*.

Artikel 7 lid 2: Er wordt gesproken over een risicobeleid waarin procedures moeten staan. Dit is verwarrend. Is het een beleid of een procedurebeschrijving? Ook is onduidelijk wat 'het vaststellen' betekent.

Advies om dit aan te passen naar:

"Het beleid, bedoeld in het eerste lid, omvat in ieder geval:

a. *Een vastgestelde risicomanagementmethodiek; en*
b. *Vastgestelde risicoacceptatiecriteria*
c. *Vastgestelde eisen voor procedures voor identificatie, analyse, beoordeling, evaluatie, inzicht, rapportage en behandeling van risico's."*

Ook is hierin het woord herbeoordeling vervangen voor evaluatie.

Artikel 8

Artikel 8: niet het woord beleid gebruiken, maar vastgelegd procedures. Beleid is hier een niet gangbare term. Procedures of gedocumenteerd processen is wel gangbaar en dekt hetgeen dat wordt bedoeld in artikel 8. Dan wordt 8.3 ook vrijwel geheel overbodig.

Artikel 8 lid 2: "incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden te detecteren, analyseren en classificeren." Hier wordt te breed gedefinieerd, waardoor de nadruk van goede incidentafhandeling wordt verminderd. Er lopen namelijk twee zaken door elkaar: incidenten of bijna incidenten en kwetsbare plekken. Monitoring en detectie kan nog worden genoemd (zoals in 8.4 wordt gedaan), maar kwetsbaarhedenscanning is een proces dat veel beter past bij onderhoud van assets. Wel kan gesteld worden dat er een aansluiting moet zijn van kwetsbaarhedenscanning naar monitoring en detectie naar incidentproces.

Artikel 9

Artikel 9 lid 1 Pleonasme: *"test en beoefent"* in de zin *"De entiteit legt dat plan schriftelijk vast, past dat plan toe in geval van een incident, en test en beoefent dit plan periodiek."*

Advies om dit aan te passen naar:

"De entiteit legt dat plan schriftelijk vast, past dat plan toe in geval van een incident, en test dit plan periodiek."

Artikel 9 lid 2: De term betrouwbaarheid wordt hier voor het eerst gebruikt en schept onduidelijkheid over de strekking hiervan. Daarnaast is het onderscheid van software en hardware nieuw in de Cbb. De zorgplicht van art. 21 van de wet gaat alleen in op: inclusief back-upbeheer.

Advies om dit aan te passen naar:

"De essentiële entiteit of belangrijke entiteit stelt procedures vast voor het maken, terugzetten en periodiek verifiëren van de beschikbaarheid en integriteit van back-ups van software en gegevens (inclusief het vervangen van hardware, indien dit van toepassing is)."

Artikel 9 lid 3: Samenvoegen met 1. Dit moeten geen separate plannen zijn, zeer onwenselijk om tijdens een crisis verschillende plannen te hebben.

Artikel 10

Artikel 10 lid 2: Zin is onduidelijk: *"Over de aan die rechtstreekse leveranciers en rechtstreekse dienstverleners te stellen cyberbeveiligingseisen en borgt dat deze afspraken worden nagekomen. De entiteit houdt de afspraken actueel."*

Advies om dit aan te passen naar:

"Over de te stellen cyberbeveiligingseisen aan die rechtstreekse leveranciers en rechtstreekse dienstverleners en borgt dat deze afspraken worden nagekomen. De entiteit houdt de afspraken actueel."

Artikel 10 lid 2: Toevoegen dat de entiteit controles uitvoert op de leveranciers: *"De entiteit houdt de afspraken actueel en controleert de leverancier op naleving van de afspraken."*

Artikel 11

Artikel 11 lid 1: Het eerste deel van de tekst voegt niets toe, behalve verwarring. Advies om de gehele tekst te verwijderen en een tekst op te nemen dat er eisen met betrekking tot beveiliging moeten worden gesteld aan een te verwerven systeem op basis van een risicoanalyse.

De risicoanalyse hier is anders dan nu beschreven in Artikel 7. Deze risicoanalyse is specifiek en die in artikel 7 generiek. Indien een specifieke risicoanalyse onderdeel moet zijn van de risicomanagementmethodiek en dus een eis is, dan ook in Artikel 7 dit duidelijk beschrijven!

Artikel 11 lid 2: De tekst in lid 2 is zeer globaal. Voor de Nederlandse weerbaarheid zou een meer verplichtend karakter voor het uitvoeren van technische controles, zoals pentesten, code review, red-teaming en scanning, zeer wenselijk zijn. Bijvoorbeeld:

"Indien van toepassing stelt de essentiële entiteit of belangrijke entiteit procedures op voor de veilige ontwikkeling van haar netwerk- en informatiesystemen. De entiteit legt deze procedures schriftelijk vast en past deze aantoonbaar toe. Deze procedures hebben betrekking op alle ontwikkelingsfasen van haar netwerk- en informatiesystemen en benoemen het (extern) laten testen van de beveiliging (bijvoorbeeld door pentesten)."

Artikel 11 lid 3: "Veranderingsbeheer" wijzigen in de gangbare term "wijzigingsbeheer".

Artikel 12

Artikel 12: 'Cyberhygiëne' is geen gangbare term. Daarnaast is er geen definitie bepaald van 'Cyberhygiëne' in zowel de Cbw als Cbb en moet dit teruggelezen worden in de preambule van de NIS2-richtlijn of MvT/Nota van Toelichting. Advies om de term bewustzijn en veilig gedrag te gebruiken.

Artikel 12 lid 1 sub b: Voegt niets toe t.o.v. sub a. Advies om te verwijderen of aan te passen naar *"a. bewust zijn van de risico's met betrekking tot de netwerk- en informatiesystemen van de entiteit en het belang kennen van de beveiliging hiervan"*

Artikel 12 lid 1 sub c: De tekst *"praktijken op het gebied van cyberhygiëne toepassen."* wijzigen naar: *"Veilig gedrag met betrekking tot .."*

Artikel 15

Artikel 15: Multi-factor authenticatie is specifiek benoemd in art. 21 lid 3 sub j Cbw, maar niet uitgewerkt in de Cbb of de Nota van Toelichting. Advies om een passage toe te voegen over het gebruik van multi-factor authenticatie.

Artikel 15: Er is geen uitwerking van procedures of een procesbeschrijving. Advies om dit toe te voegen. Een beleid stelt kaders en een procesbeschrijving legt vast hoe dit gebeurt.

Artikel 15: Er ontbreekt iets over beperking van rechten tot het noodzakelijke. Hierdoor kan een leemte ontstaan namelijk: Nu voldoet een organisatie die in dit beleid zet: iedereen mag overal bij, dat vinden we praktisch. Dit is fundamenteel voor informatiebeveiliging en mag dus scherper.

Artikel 15: Advies om Nota van Toelichting aan te vullen met een passage over hogere rechten (privileged access management).

Artikel 16

Artikel 16 lid 3: Het is onmogelijk om volledig & actueel te eisen. Dan voldoet elke organisatie per definitie niet aan de wet. Voorstel om "*volledige en actuele"* te verwijderen.

Artikel 18

Artikel 18: Toevoegen van de maatregelen die volgen uit de risicoanalyse: “De essentiële entiteit of belangrijke entiteit evalueert periodiek de doeltreffendheid van de maatregelen die zij heeft genomen op grond van artikel 21, eerste lid, van de wet ***en op basis van de risicobehandeling die volgt uit artikel 21 lid 3 sub b*** en de effecten ervan in de praktijk, en legt het resultaat daarvan schriftelijk vast. De entiteit past naar aanleiding van die evaluaties de maatregelen waar nodig aan.”

Pasquil is beschikbaar voor toelichting en denkt graag mee!

De reactie is geschreven door:
Arvid Landwaart
Lynley Vrolijk
Daniël Tjeerdsma