NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Reactie op consultatie CBB

Datum : 30 maart 2025

---

1) In de Cbw wordt in artikel 21 lid 3f gesteld, dat beleid en procedures moeten bestaan voor het beoordelen van de effectiviteit van maatregelen die cyberbeveiligingsrisico's beheersen:

    a. Dit lid wordt niet verder uitgewerkt in de Cbb. Hierdoor blijft het onduidelijk welke eisen gesteld worden aan dit 'beoordelen'. Deze onduidelijk is onwenselijk, omdat dit qua implementatie in de markt twee uiterste situaties in de hand kan werken. Deze twee uitersten zijn testwerkzaamheden op alle maatregelen, ook waar de organisatie zelf niet nut-en-noodzaak ziet maar wel tests uitvoert om zeker te stellen dat ze aan de wet voldoen. Anderzijds kunnen organisaties geen adequate invulling geven, aangezien zij geen concrete minimale verwachting zien.
    Ten aanzien van de minimale verwachting merken wij op dat bijvoorbeeld de ISO 27001 het organisaties toestaat om te selecteren welke maatregelen wel en niet beoordeeld moeten worden. Het zou daarom goed zijn een onderscheid aan te brengen in maatregelen en 'belangrijke maatregelen' (key controls).

    b. Cbb artikel 18 beschrijft wel een 'evaluatie' op 'doeltreffendheid'. Het valt op dat met deze termen wordt afgeweken van 'beoordeling' en 'effectiviteit'. Het gebruik van deze afwijkende termen lijkt te suggereren, dat hier een ander type evaluatie wordt bedoeld dat de beoordeling van maatregelen. Dit zou bijvoorbeeld kunnen gaan om een directiebeoordeling of managementsysteem beoordeling op het niveau van de doelstellingen van de onderneming. Het zou goed zijn de verwachting voor deze evaluatie beter uit te schrijven bijvoorbeeld met een verwijzing naar instrumenten zoals risico-indicatoren (KRI). Mocht met deze evaluatie toch de beoordeling van de effectiviteit van de maatregelen bedoeld worden, dan dient het Cbb aangepast te worden naar de definities en terminologie van de bovenliggende regelgeving.

2) In Cbw artikel 21 lid 3j wordt beschreven dat "wanneer gepast" er gebruik gemaakt moet worden van multi-factor authenticatie. In de Cbb is geen nadere uitwerking van wanneer dit gepast of niet gepast is. Ook indien de wetgever geen verplichtingen wil stellen aan deze overweging, is het naar onze mening wenselijk dat dit expliciet wordt uitgeschreven. Van “gepast gebruik”’ is sprake bij authenticatie tot een account met geprivilegieerde rechten. Dit zou geregeld kunnen worden in een nieuw artikel of door het huidige artikel 15 Cbb verder uit te breiden.

3) In Cbb artikel 16 wordt op dit moment de term 'asset' gebruikt. Wij stellen voor de term “activa” te gebruiken. Omdat dit artikel 16 een nadere uitwerking is van art. 21 lid 3 onder i Cbw en daar ook de term “activa” wordt gebruikt. En dit wijzigingsvoorstel geldt ook voor art. 10 van de Ministeriële Regeling.

Telefoon: + 31 (0)88 4960380
Mobiel: + 31 (0)6 20015632
E-mail: norea@norea.nl

Mercuriusplein 3,
Postbus 242,
2130 AE Hoofddorp

Web: www.norea.nl