Memo

Van	Peter van der Els
Aan	Ministerie Justitie en Veiligheid
Datum	27 maart 2025
Referentie	-
Onderwerp	Internetconsultatie Cbb

L.s,

Dank voor het bieden van de mogelijkheid om bij te dragen aan de totstandkoming van deze belangrijke nieuwe wetgeving. Hierbij de reactie namens Fox-IT op de documenten van de internetconsultatie. Achtereenvolgens gaan wij in op het Cyberbeveiligingsbesluit, de Nota van toelichting en de (concept) Ministeriële regeling.

Wij zijn positief over de invoering van deze nieuwe wet- en regelgeving, omdat die bijdraagt aan een cyberveiliger Nederland, geheel in lijn met ons motto ‘For a more secure society’.

1 Cyberbeveiligingsbesluit

Artikel 4:
Dit artikel lijkt me van toepassing op Fox-IT en branchegenoten gezien punt g. Dit betekent dus ook dat een groot aantal artikelen van dit besluit niet van toepassing zijn – waar het deze diensten betreft. Hierdoor ontstaat mogelijk een complexe situatie, waardoor delen van ons bedrijf mogelijk onder de Cbb vallen en andere delen onder de Uitvoeringsverordening 2024/2690. Indien dit juist is, zien wij dit niet als een wenselijke situatie.

Artikel 16.2:
Deze classificatie dient ook te gelden voor de opgeslagen data (informatie); immers data of informatie is de asset die dient uiteindelijk beschermd te worden. Dit staat in 16.3 wel genoemd.

Artikel 20, 21,22, 23:
Hieruit blijkt impliciet dat de inhoud van de training rekening moet houden met de situatie in de eigen organisatie (de context in ISO termen). Dit mist echter in artikel 21 (eisen aan de training). Een trainier dient volgens artikel 22 gekwalificeerd te zijn, maar dit wordt niet concreet gemaakt. Overigens, zou het niet handiger zijn een bepaald kennisniveau voor bestuurders te eisen en vrij te laten hoe deze aan dit niveau komen? Bovendien laat de huidige formulering van artikel 23 geen ruimte voor bestuurders die al certificaten op het gebied van Informatieveiligheid hebben. Bijvoorbeeld, een geldige CISM certificatie voldoet niet aan de eisen van artikel 23. Deze artikelen zijn toch niet bedoeld om opleidingsinstanties mogelijkheden te geven tot extra omzet?

2 Nota van toelichting

Inleiding, **eerste alinea**
De tekst "... tot intrekking van Richtlijn (EU) 2016/1148.1 Die richtlijn wordt ook wel aangeduid als de NIS2-richtlijn." Is niet juist of tenminste verwarrend. Richtlijn 1148 wordt wel aangeduid als de NIS(1) richtlijn.

Gevolgen,
Eenmalige regeldruk
Gezien de beoogde risicogebaseerde aanpak vanuit NIS2 zou het logischer zijn dat het uitvoeren van een risicoanalyse een belangrijk onderdeel is. Een hiatenanalyse is een aanpak die meer uitgaat van het moeten voldoen aan een lijst.
Structurele regeldruk
Hoewel de wetgeving dit niet expliciet noemt, zijn kosten van (interne) audit en certificatie m.i. ook kosten die hieronder zouden kunnen vallen. Zie hiervoor artikel 6, waar ISO 27001 e.a. met name genoemd worden.

Artikelsgewijs

Artikel 6
Laatste alinea, het vierde lid: "Voorbeelden hiervan zijn een Information Security Management Systeem (ISMS) zoals de ISO 27000-reeks of het Cyber Security Management System (CSMS) op basis van EIC 62443."

Hier staat een referentie naar security management systemen uit ISO en IEC normen. Overigens staat IEC verkeerd gespeld als EIC. Het is goed dat deze standaarden worden aangehaald als voorbeelden van een managementsysteem (ISMS of CSMS) waarmee conformiteit aangetoond kan worden. Het zou dienstig zijn om bij de uitwerking van de zorgplicht per artikel te referen aan bijvoorbeeld de beheersmaatregelen van ISO 27001 en de uitwerking in ISO 27002. Of, makkelijker nog, de uitwerkingen te beperken en naar de relevante NEN/ISO/IEC normen te verwijzen. Tenslotte, waarom geen referentie naar NEN 7510 en ISO 22301?

3 Concept ministeriële regeling

Leeswijzer/Voor wie/Artikel 2
In de twee tabellen ontbreekt bij de sector *digitale infrastructuur* de subsector *Aanbieders van beheerde beveiligingsdiensten*.

Van wie
Eerste alinea: "In die ministeriële regelingen zullen daarnaast ook andere aspecten opgenomen worden, zoals de drempelwaarden voor significante incidenten, waarvoor de meldplicht geldt" Deze waarden zijn ook beschreven in de artikelen 5 t/m 14 van de Uitvoeringsverordening. Het is niet geheel duidelijk welke van toepassing zijn.

3.1 Paragraaf [PM]. Nadere invulling zorgplicht (verscheidene artikelen)
De volgende artikelen lezen als een soort samenvatting van o.a. de ISO 27002; ze beschrijven concrete maatregelen, die uit een specifieke context en risico-gebaseerde aanpak nodig zouden moeten blijken. Het voorschrijvend karakter van de artikelen lijkt strijdig met de beoogde risico-

gebaseerde aanpak. En qua inhoud, kan er niet beter verwezen worden naar geaccepteerde standaarden die specifieke aspecten nader uitwerken?

Artikel 6 (Beveiliging van toeleveringsketen - artikel 10 van het Cyberbeveiligingsbesluit)
“Onverwijld”: Dit graag nader uitwerken; het is niet altijd mogelijk om direct na het ontstaan van een incident iets te melden. Het zou beter zijn om een periode van een aantal (werk) uur na het ontdekken van het incident te benoemen, afhankelijk van de ernst van het incident. En waarom niet aansluiten met DORA?

Artikel 7.2 (Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen - artikel 11 van het Cyberbeveiligingsbesluit)
Punten “a. beveiligingspatches” en “c. technische kwetsbaarheden”. Ik zou hier punt c. Technische kwetsbaarheden als eerste benoemen in plaats van het huidige punt a. Immers, patches zijn een onderdeel van de remedie voor genoemde kwetsbaarheden. Management van technische kwetsbaarheden is het uitgangspunt. Indien er geen patch voorhanden is kan het nodig zijn een vervangende maatregel te nemen.

Artikel 10 (Beveiligingsaspecten ten aanzien van beheer van assets - artikel 16 van het Cyberbeveiligingsbesluit)
De assets zijn hier meer dan de systemen; het betreft allereerst de data/informatie uit processen die de systemen bevatten of verwerken. Die data/informatie dient geclassificeerd te worden en vervolgens conform die classificatie beschermd te worden. De eigenaar hiervan is hiervan verantwoordelijk; het is dus noodzakelijk dat de eigenaar geïdentificeerd wordt en bewust wordt gemaakt van zijn verantwoordelijkheid.

3.2 Artikelsgewijze toelichting

Artikel 4 – Beleid over risicomanagement
Dit stuk lijkt een samenvatting van wat er in ISO 27001 en 27005 staat.

Artikel 5 - Bedrijfscontinuiteit
Dit stuk lijkt een samenvatting van wat er in ISO 22301 staat.

De tweede alinea “Door te zorgen ... te laten vinden”: Dit is een concrete invulling van een maatregel, die uit een business impact analyse dan wel risicoanalyse nodig moet blijken.

Artikel 7 - Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk-en informatiesystemen
Pagina 14, derde alinea: “IT- en OT-systemen en deze zo mogelijk van elkaar te scheiden”. Men zou hier kunnen verwijzen naar de IEC 62443 waarin dit beschreven staat.

Artikel 10 - Beveiligingsaspecten ten aanzien van beheer van assets
In de tweede alinea staat “actuele inventaris te hebben van de assets”. Dus ook van data/informatie assets. Zoals in ISO 27002 genoemd. En voor een verdere uitwerking van asset management zou een verwijzing naar de ISO 55000 nuttig kunnen zijn.