Reactie Mr. Drs. J. Maas (persoonlijke titel) op consultatie Cyberbeveiligingsbesluit
Datum: 28-02-2025

- Cyberbeveiligingsbesluit

Art 7 – Beleid voor risicomanagement

Hoewel begrijpelijk dat de wettekst abstract en algemeen omschreven is, is risicomanagement de kern van NIS2 (en dus van de Cbw). Een aanvullend artikellid (art. 7 lid 3) zou toegevoegd moeten worden zodat entiteiten beter begrip krijgen van de elementen uit NIS2 binnen de risico gebaseerde aanpak, als onderdeel van het beleid voor risicomanagement, moeten vallen. Tevens wordt hierbij rekening worden gehouden met de overwegingen van andere lidstaten zodat een EU-brede en uniforme implementatie plaatsvindt. Hierdoor wordt voldaan aan de risico gebaseerde aanpak zoals verwoord in art. 21 lid 1 NIS2. De risico gebaseerde aanpak bevat een hoog detailniveau en kan bestaan uit een combinatie van meerdere risico gebaseerde aanpakken.

Elementen die in deze aanvullende art. 7 lid 3 toegevoegd zou moeten worden zijn:

a. de risico gebaseerde aanpak proactief is opgezet in het bestrijden van cyberdreigingen;
b. de belangrijke of essentiële entiteit blijft op de hoogte van nieuwe dreigingen en kwetsbaarheden om tijdig ingrijpen;
c. De maatschappelijke en economische gevolgen worden expliciet aan de risico gebaseerde aanpak toegevoegd;
d. de risico's rondom terroristische dreigingen worden aan de risico gebaseerde aanpak toegevoegd;
e. de risico's van de door mensen veroorzaakte dreigingen, technologische dreigingen en natuurrampen worden aan de risico gebaseerde aanpak toegevoegd;
f. de risico's met een lage waarschijnlijkheid, met mogelijke grote economische en maatschappelijke gevolgen, worden aan de risico gebaseerde aanpak toegevoegd;
g. De authenticiteit van de gegevens of aangeboden diensten wordt, naast de beschikbaarheid, integriteit en vertrouwelijkheid, aan de risico gebaseerde aanpak toegevoegd;
h. de risico's over het verkrijgen van toegang door derde partijen op de eigen netwerk- en informatiesystemen wordt aan de risico gebaseerde aanpak toegevoegd;
i. de evenredigheid van de genomen maatregelen wordt aan de risico gebaseerde aanpak toegevoegd;
j. de strategische veiligheidsrisico's rondom leveranciers en hun afhankelijkheid wordt aan de risico gebaseerde aanpak toegevoegd;
k. de risico gebaseerde aanpak omvat de mate waarin de entiteit afhankelijk is van netwerk- en informatiesystemen;
l. de risico gebaseerde aanpak omvat de risico's over het onderhoud van de netwerk- en informatiesystemen dat intern door eigen personeel wordt uitgevoerd of aan een externe partij is uitbesteed;
m. de risico gebaseerde aanpak omvat alle opgeslagen, verzonden, verwerkte gegevens of aangeboden diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen;
n. de risico gebaseerde aanpak wordt per netwerk- en informatiesysteem en de aangeboden dienst toegepast;
o. het beleid voor risicomanagement bevat het bevorderen en neerzetten van een cultuur van risicobeheer en het nemen van verantwoordelijkheid over de risicobeoordelingen en de maatregelen om cyberbeveiligingsrisico's te beheren;
p. het beleid voor risicomanagement bevat het onafhankelijk en periodiek auditen van de risico gebaseerde aanpak en het beleid voor risicomanagement;
q. het beleid voor risicomanagement bevat de integratie van andere belanghebbenden wanneer de interacties en relaties met hen binnen het toepassingsgebied van de wet vallen.

Om ook invulling te geven aan voortschrijdende inzichten en aanvullingen vanuit andere lidstaten zou aanvullen art. 7 lid 4 toegevoegd moeten worden dat periodiek dit beleid voor risicomanagement zoals verwoord in lid 1 en 2 wordt geëvalueerd en aangepast zodat dit beleid voor risicomanagement blijft voldoen aan de gestelde eisen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt, te blijven beheersen.

Art. 10 Beveiliging van de toeleveringsketen

Art. 10 lid 2: Verwijder '… waar mogelijk … ' in de eerste regel. Het is moeilijk te borgen dat de afspraken worden nagekomen wanneer er geen schriftelijke afspraken zijn. De keten is van wezenlijk belang en in die zin zouden de afspraken over de cyberbeveiligingseisen best een bepaalde vormvereiste mogen hebben. In dit geval een schriftelijke overeenkomst of addendum op de hoofdovereenkomst.

Art 11 Beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen

Art. 11 lid 2: Voeg aan het einde toe dat deze procedures, via schriftelijke afspraken, ook op dienstverleners van toepassing zijn aan wie de entiteit een of meer ontwikkelingsfasen heeft uitbesteed.