Rijksoverheid



CISO Cirkel CIP

Donderdag 26 oktober 2023

Kim Pfeifer

Coördinerend beleidsmedewerker toezicht informatieveiligheid

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De vraag van vandaag:

- Wat betekenen de zorgplicht en toezicht vanuit NIS2 voor mijn organisatie en bestuurder?
- Het antwoord is per organisatie verschillend....
- ....NIS2 biedt in ieder geval kansen voor verbetering!

Zorgplicht NIS2

- Risicoanalyse staat centraal
- Cyberbeveiligingsbewustzijn
- Cyber hygiëne beleid
- Evenredigheid en proportionaliteit

Toezicht NIS2

- Toezicht is verplicht
- Toezicht moet onafhankelijk zijn
- Toezicht kent 2 regimes: essentieel en belangrijk
- Verschil zit in: 1) ad hoc audits en 2) inzetten controlefunctionaris

Uitgangspunten Nederland zorgplicht en toezicht

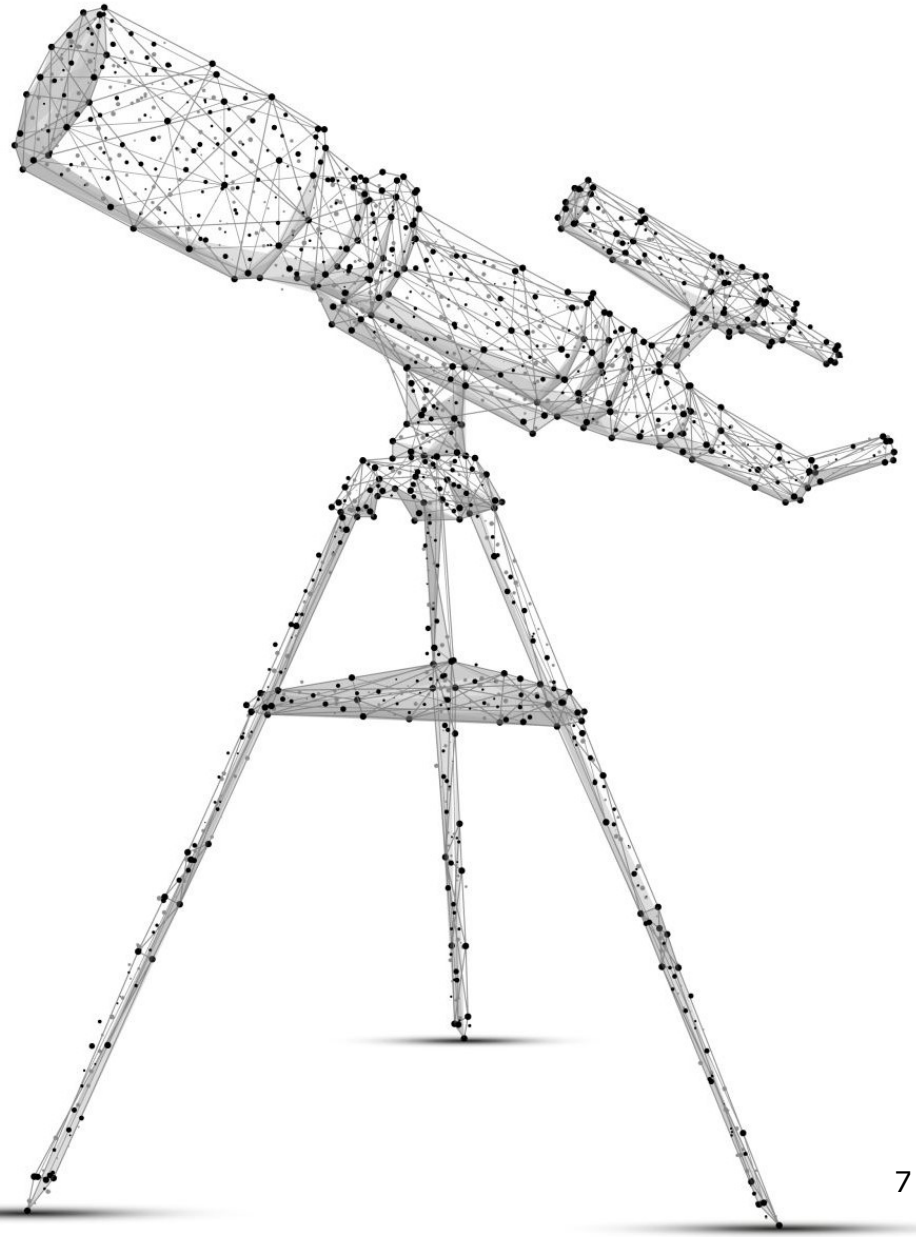
- Door de BIO 2.0 toe te passen, wordt invulling gegeven aan de zorgplicht (NB: VIR en VIR-BI worden ook meegenomen)
- Overheidsorganisaties zijn essentieel. Dus toezicht volgens artikel 32 NIS2
- Stelsel toezicht door Rijksinspectie Digitale Infrastructuur (RDI) op basis van bestaande verantwoordingen in bestuurslagen
- Herhaling: proportionaliteit en evenredigheid!!

Mapping NIS2/ISO/BIO

- **Incidentregistratie:** naast interne organisatie, ook sterk gericht op externe notificatie
- **Bedrijfscontinuiteit, crisis(beheer) en de (toeleverings)keten** heeft **meer aandacht in de NIS 2** dan de BIO. NIS2 vereist meer actieve rol van de organisatie
- **2FA**, **beveiligde spraak-/tekst- en videoverbindingen** en beveiligde **noodcommunicatiesystemen** moeten worden **ingezet wanneer gepast**

Uitwerking toezicht

- Interbestuurlijke werkgroep toezicht
- Per overheidslaag wordt bestaande verantwoording bekeken
- Op basis van bestaande situatie beeld krijgen wat nodig is om het toezicht robuust te maken



Stellingen

- Risicoanalyse geeft voldoende basis
- Het management/de bestuurder is betrokken en weet het grootste informatiebeveiligingsrisico
- De rapportage geeft voldoende basis voor toezicht
- De hele organisatie is betrokken en weet welke maatregelen genomen moeten worden
- De bestuurder maakt zich geen zorgen over aansprakelijkheid

Tot slot

- Webinar 12 oktober over NIS2 en de BIO terugkijken: www.weerbaredigitaleoverheid.nl

- Een volgend webinar, verzorgd door BZK en JenV, dinsdag 21 november van 15.00-16.00 uur als onderdeel van het Overheidsbreed Cyberprogramma