NIS2 in 2024

Jeroen Koster

Agenda

- Nieuws omtrent de NIS2
- Voorsorteren op de NIS2
  - Belangrijke aandachtspunten NIS2
  - Mapping NIS2 → BIO1.04
  - Risico gestuurd te werk gaan
- Resumé
- Vragen

Nieuws omtrent de NIS2

Eind januari maakte de minister van Justitie en Veiligheid bekend dat de Nederlandse uitwerking van de Europese NIS2-richtlijn vertraging heeft opgelopen.

De implementatie had op 17 oktober 2024klaar moeten zijn, maar dat wordt niet gehaald. Die beslissing brengt de volgende vragen met zich mee:

- Hoelang gaat de vertraging duren?
- Wat betekent dat voor jouw organisatie?
- Wanneer gaan de zorgplicht en de meldplicht in?
- Wanneer start het toezicht?

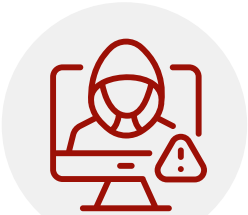
Feiten en vragen

NIS2 wordt niet in 2024 vertaald naar Nationale wetgeving.

Jaarbeeld Ransomware 2023 toont:

- 30% via kwetsbaarheden
- 28% onrechtmatig toegang

Wat zijn nu de juiste stappen zonder de NIS2?



Control frameworks zijn een middel, geen doel.

Hackers gaan gewoon door. Ook zonder NIS2.

.....?

Voorsorteren op de NIS2

Die in 2025 al komt

Belangrijkste aandachtpunten die blijken uit analyses

1. NIS2 gaat uit van een **risico gestuurde aanpak.**
2. De NIS2 maakt voor de maatregelen **geen onderscheid in (type) systeem**, maar gaat uit van een **entiteit**.
3. Reageren op **incidenten** is een essentieel onderdeel van het treffen van maatregelen.
4. Voor de **maatregelen** uit artikel 20 en 21 wordt **geen verschil gemaakt tussen essentiële en belangrijke entiteiten**.
5. De **(toeleverings)keten** komt duidelijk naar voren in de NIS2.
6. Bedrijfscontinuïteit is expliciet onderdeel van de maatregelen, met de voorbeelden **back-upbeheer, noodvoorzieningsplannen en crisisbeheer.**
7. **Cyberhygiëne** is beschreven op verschillende manieren in de NIS2 en vergt ook afweging van de organisatie zelf.
8. 10 miljoen euro **boete** en aansprakelijkheid **bestuur.**

Met de NIS2 zonnebril naar de BIO kijken

Wat moeten we in het achterhoofd houden richting de BIO 1.04

- ✓ **Incidentregistratie** kent aanvullende eisen ten opzichte van de BIO. De NIS is, **naast interne organisatie**, ook sterk gericht op **externe notificatie**.
- ✓ **Bedrijfscontinuïteit, crisis(beheer) en de (toeleverings)keten** heeft **meer aandacht in de NIS2** dan nu in de BIO staat. De NIS2 vereist een meer actieve rol van de organisatie.
- ✓ **2FA, beveiligde spraak-/tekst- en videoverbindingen** en beveiligde **noodcommunicatiesystemen** moeten worden **ingezet wanneer gepast**.
- ✓ **NIS maakt geen onderscheid in type systemen** en is daarmee allesomvattend, **inclusief OT/procesautomatisering**.

inergy

Mapping NIS2 artikelen → BIO controls

Waar hebben wij de mapping op gebaseerd?

- IBD: NIS2-mapping-op-handreiking-bio2-0-opmaat-v2-2-def
- IBD: 20231110-analyse-mapping-NIS2-en-ISO-27002-en-BIO
- IBD: 20221215-handreiking-indeling-bio-v104zv-aan-iso-iec-27002-2022-v11-def

Voorbeelden tussen NIS2 en BIO 1.04

BIO2 Control-nr.	Control-soort	BBN van control	Control-titel	Control	Doel	NIS2 artikel	Control-nr. BIO 1.0.4zv	Maatregelnr. BIO 1.0.4zv
					eigenaarschap toe te wijzen.			
5.10	Organisatorisch	1	Aanvaard gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen behoren te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Waarborgen dat informatie en andere gerelateerde bedrijfsmiddelen passend worden beschermd, gebruikt en behandeld.	21i	08.1.3	08.1.3.1

Control-nr.	Control-soort	BBN van control	Control-titel	Control	Doel	NIS2 artikel	Control-nr. BIO 1.0.4zv	Maatregelnr. BIO 1.0.4zv
				beheersen.				
5.15	Organisatorisch	1	Toegangsbeveiliging	Er behoren regels op basis van bedrijfs- en informatiebeveiligingseisen te worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Toegang voor bevoegden bewerkstelligen en toegang voor onbevoegden tot informatie en andere gerelateerde bedrijfsmiddelen voorkomen.	21g, 21i	09.1.2	09.1.2.1

ontrol-nr.	Control-soort	BBN van control	Control-titel	Control	Doel	NIS2 artikel	Control-nr. BIO 1.0.4zv	Maatregelnr BIO 1.0.4zv
				retourneren.				
14	Organisatorisch	1	Overdragen van informatie	Er behoren regels, procedures of overeenkomsten voor informatieoverdracht te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe belanghebbende.	24	13.2.3	13.2.3.1

Waar moet ik dan beginnen?

Risico gestuurd te werk

MAPGOOD

Mens
Apparatuur
Programmatuur
Gegevens
Organisatie
Omgeving
Diensten

Risicomatrix		Impact				
		Niet merkbaar	Klein	Gemiddeld	Groot	Desastreus
Kans	Dagelijks					
	Wekelijks					
	Maandelijks					
	Jaarlijks					
	< Jaarlijks					

Kwetsbaarheden omzetten naar acties

K2I4 Steeds meer kwetsbaarheden in software

- BIO 1.04 control 12.6.1 Beheer van technische kwetsbaarheden: Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
- BIO 1.04 control 12.6.2 Beperkingen voor het installeren van software: Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.

K3I5 Gevaren in ketens uit zicht

- BIO 1.04 control 15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert.
- BIO 1.04 control 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
  Control 15.2.1. enzovoort …

Capaciteit/geld loskrijgen met goed verhaal

Project X Mitigeren van K2I4: Steeds meer kwetsbaarheden in software.

- BIO 1.04 controls 12.6.1 en 12.6.2 verbeteren.

Project Y Mitigeren van K3I5: Gevaren in ketens uit zicht.

- BIO 1.04 controls 15.1.2, 15.1.3 en 15.2.1 verbeteren.

Wie gaat het doen?
Wat gaat het kosten?

College

Resumé

Stappen ter voorbereiding

1. Maak een risicoanalyse
2. Ga risico gebaseerd verbeteren op basis van BIO 1.04
3. Incident response plan maken + oefenen
4. Documenteer dit goed

Vragen?