databalance
managed IT solutions

it creation

sj solutions
datamanagement

NIS2 in één middag

Het concreet maken van de regelgeving

- Versie: 1.1
- Datum: 27 juni 2024
- Auteur: Sebastiaan Bakker
- Classificatie: Publiek

NIS2

Een greep uit de de belangrijkste zaken waar NIS2 voor staat:

- Meldplicht
  - Het inlichten van stakeholders als het fout gaat.
- Toezicht
  - Monitoren en controleren van de naleving door de bevoegde autoriteiten (RDI).
- Zorgplicht
  - Risicobeheersing op basis van passende technische en organisatorische maatregelen.

Niet complex

- Veel van de punten die in de wet zijn omschreven, zijn niet nieuw.
- Er bestaan al veel technische en organisatorische maatregelen om compliance te bewerkstelligen.
- Door voort te bouwen op de ISO27001/2 kunnen er al veel meters gemaakt worden.
  - Alle onderdelen vanuit de ISO-normen zijn ook terug te vinden in de NIS2.

Basisprincipes

De drie basisprincipes die indirect centraal staan in de ISO27001 norm:

1. **Beschikbaarheid**: systemen, platformen en applicaties dienen toegankelijk te zijn.
2. **Integriteit**: de data moet betrouwbaar zijn.
3. **Vertrouwelijkheid**: informatie dient alleen voor de juiste mensen toegankelijk te zijn.

Maatregelen

Risicomanagement

Datamanagement

Supply chain

Cybersecurity

Governance

Risicomanagement

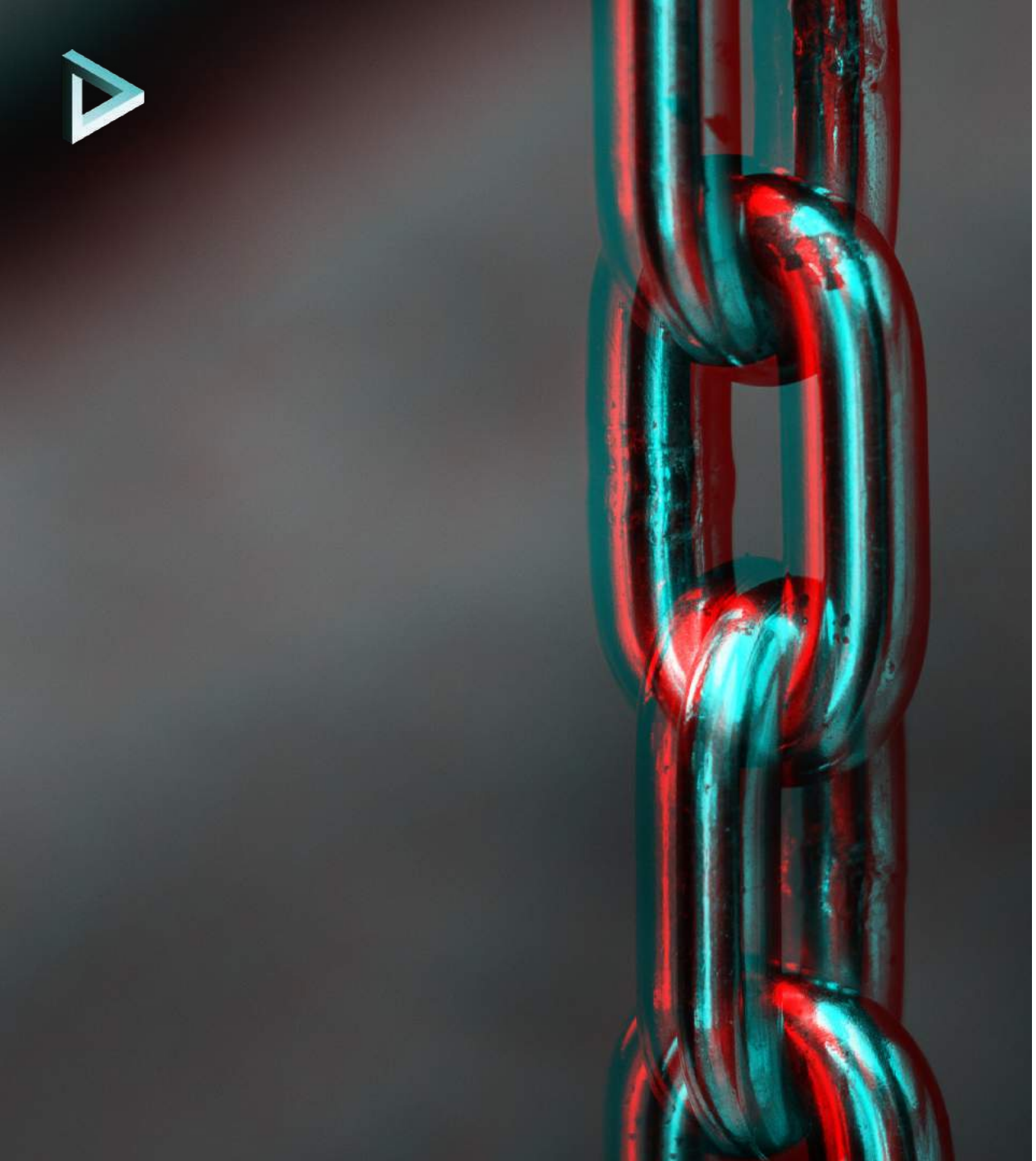
- Risicomanagement staat centraal bij iedere wet, norm en richtlijn die er bestaat.
- Om te weten wat er fout kan gaan en waar je op moet focussen moet je inzicht hebben.
- Risico’s inzichtelijk maken en concretiseren helpt bij het bepalen van prioriteiten en het vrijmaken van budgetten.
- Ook voor risicomanagement (in IT context) bestaan al standaard werkwijzen.

Governance

- Wie, wat doet en waar ligt de verantwoordelijkheid (zowel intern als extern)?
- Zorg ervoor dat er een eigenaar is binnen de organisatie voor cybersecurity.
- Definieer enkele doelstellingen die ervoor zorgen dat de organisatie veiliger te werk gaat.
- Weet welke externe organisaties en/of wetten en regels invloed hebben op het bedrijf.

Datamanagement

- Welke data wordt er verzameld en is dat echt nodig voor de bedrijfsvoering?
- Waar wordt de data opgeslagen en onder welke jurisdictie vallen deze regio’s/data?
- Breng in kaart of contractueel privacy is geborgd en of overal duidelijk is wat er gedaan dient te worden wanneer het misgaat.



Supply chain

- Eén van de aandachtspunten bij NIS2 is de focus op de digitale keten.
- Het is noodzakelijk om een overzicht te hebben van welke partners en leveranciers er betrokken zijn en welke rol zij vervullen.
- Om in-control te blijven is het noodzakelijk het gesprek met de partners aan te gaan.

Cybersecurity

- Het gaat om het geheel der maatregelen (“*lines of defence*”) en de samenhang daartussen.

- In de ISO27001:2022 norm zijn er vier verschillende domeinen:
  - Organisatie
  - Mensen
  - Fysiek
  - Technisch

- Niet alle maatregelen zijn altijd van toepassing. Context is key.

Aantoonbaarheid

- Opstellen van beleid en het inrichten van processen maakt voldoen aan NIS2 aantoonbaar.
  - En helpt ook bij aantoonbaar kunnen voldoen aan andere al bestaande wetten zoals AVG.
- ISO27001 is niet een verplichting, maar kan helpen.

databalance
managed IT solutions

it creation

sj solutions
datamanagement

Bedankt

Ga voor meer informatie naar:

- www.databalance.eu
- www.sj-solutions.nl
- www.itcreation.nl