databalance
managed IT solutions

it creation

sj solutions
datamanagement

NIS2 hoeft niet complex te zijn

Een inventaris van de maatregelen

- Versie: 1.1
- Datum: 24 september 2024
- Auteur: Sebastiaan Bakker
- Classificatie: Public

Vandaag

- Waar bestaat NIS2 uit?
  - Registratieplicht
  - Meldplicht
  - Zorgplicht
- Datamanagement
- Data (juist) in de cloud

Waar bestaat NIS2 uit?

- Registratieplicht
- Meldplicht
- Zorgplicht

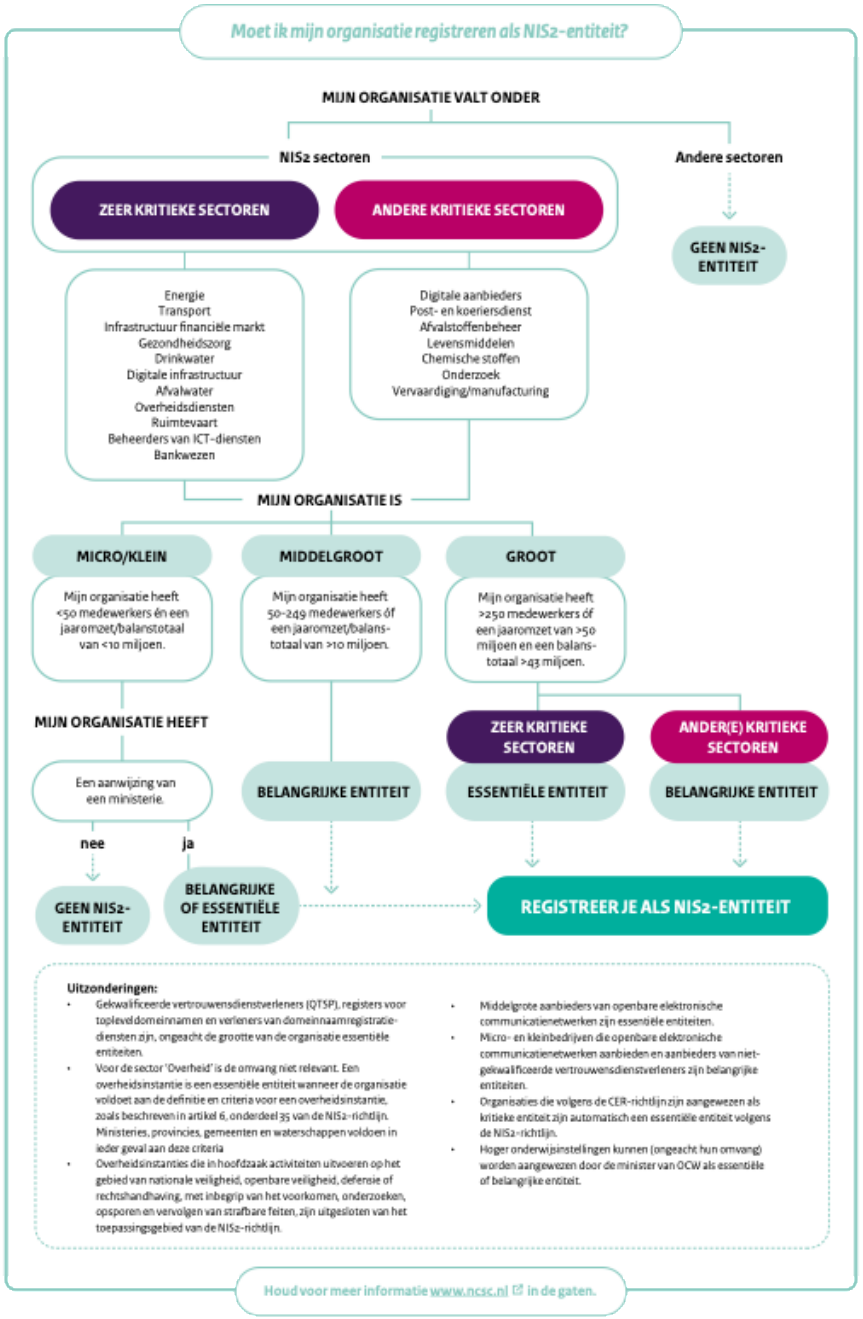
Registratieplicht

- Organisaties die **in-scope vallen van NIS2** dienen zichzelf te registreren in het entiteitenregister.

- **Het register** biedt duidelijkheid aan organisaties in hoeverre ze moeten voldoen aan de NIS2 en biedt een handvat voor regelgevende instanties en toezichthouders om een beeld te krijgen van de NIS2-entiteiten.

- Om de scope keuze te maken heeft het NCSC **referentiematerialen** (rechts) opgesteld.

- Wanneer een organisatie moet voldoen, moet er aan de slag worden gegaan met **de invulling van de maatregelen** uit de zorgplicht.



Meldplicht

- Organisaties in **kritieke sectoren** moeten ernstige cybersecurity-incidenten melden bij de nationale toezichthouder. In Nederland gaat de Rijksdienst voor Digitale Infrastructuur (RDI) toezicht houden op NIS2.

- Incidenten moeten **zo snel mogelijk** worden gemeld, in drie fasen:
  - Eerste melding binnen 24 uur na het ontdekken van het incident.
  - Uitgebreidere informatie dient binnen 72 uur te worden aangeleverd.
  - Een eindrapportage over de impact en de genomen maatregelen binnen een maand.

- De meldplicht geldt alleen voor incidenten die een **significante impact** hebben op de dienstverlening, zoals dataverlies, of een schending van de vertrouwelijkheid van gegevens.

- Niet voldoen aan de meldplicht **kan leiden tot boetes**, afhankelijk van de ernst van de overtreding en de sector. De wijze waarop deze boetes opgelegd kunnen worden, gaat met de overgang naar NIS2 veranderen.

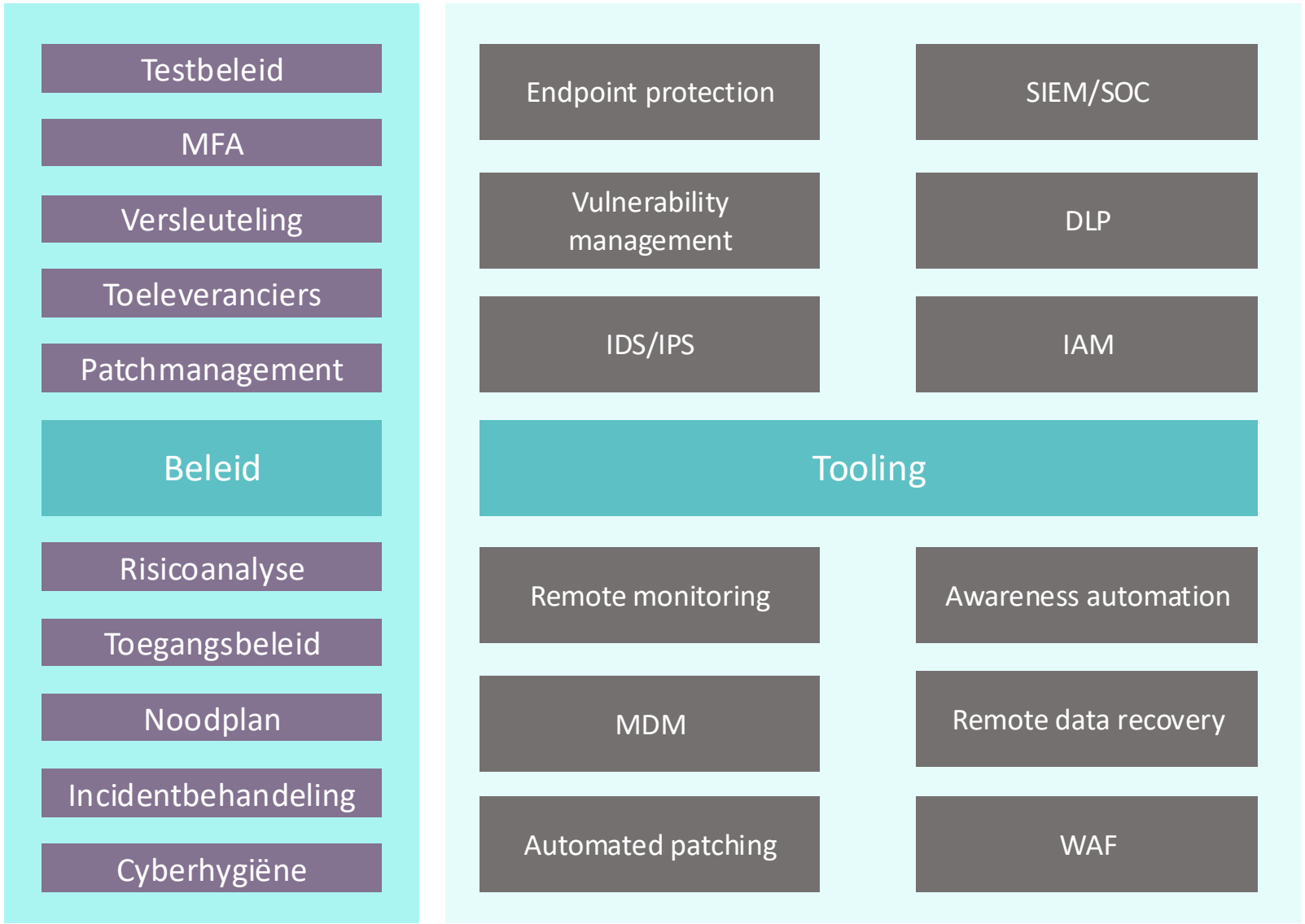
Zorgplicht

- Organisaties in kritieke sectoren moeten **proactieve maatregelen** nemen om cybersecurity te kunnen waarborgen en zo de kans op incidenten te kunnen verkleinen.

- De mate waarop invulling wordt gegeven aan de maatregelen en de diepgang van de maatregelen hangt af van de **context waarin een organisatie acteert**. Een effectieve invulling vereist risicoanalyses.

- Naast de basis van risicoanalyses zijn de volgende aspecten onmisbaar:
  - Eigenaarschap, verantwoording en rapportages,
  - Personeelsopleiding en bewustwording (awareness),
  - Technische en organisatorische maatregelen,
  - Incidentrespons en recovery,
  - Leveranciersmanagement,
  - Datamanagement.

Zorgplicht


Testbeleid
MFA
Versleuteling
Toeleveranciers
Patchmanagement
Beleid
Risicoanalyse
Toegangsbeleid
Noodplan
Incidentbehandeling
Cyberhygiëne
Endpoint protection
SIEM/SOC
Vulnerability management
DLP
IDS/IPS
IAM
Tooling
Remote monitoring
Awareness automation
MDM
Remote data recovery
Automated patching
WAF

Tooling

- **Vulnerability management**: gebruik tools zoals om zwakke punten in de infrastructuur te identificeren en te patchen, zodat je proactief kwetsbaarheden kunt verhelpen.
- **Intrusion Detection and Prevention Systems**: implementeren van IDS/IPS-oplossingen om verdachte activiteiten en inbraakpogingen op netwerken te detecteren en te blokkeren.
- **SIEM (Security Information and Event Management)**: gebruik van SIEM-platforms om real-time monitoring, detectie en rapportage van beveiligingsincidenten te automatiseren.
- **Endpoint Detection and Response (EDR)**: inzet van EDR-tools om endpoints (zoals werkstations en servers) te monitoren en te beschermen tegen malware en geavanceerde bedreigingen.
- **Data Loss Prevention (DLP)**: implementeer DLP-oplossingen om te voorkomen dat gevoelige data onbedoeld wordt gedeeld, gelekt of gestolen.
- **Identity and Access Management (IAM)**: beheer van toegangsrechten en identiteiten om ongeautoriseerde toegang tot systemen te voorkomen.

Tooling

- **Security awareness platforms**: train medewerkers met platforms om hen bewust te maken van cyberdreigingen en phishing-aanvallen te herkennen.
- **Penetratietesting en red team tools**: maak gebruik van third party pentesters of tools voor regelmatige penetratietesten om de beveiliging van je netwerk en systemen te evalueren en te versterken.
- **Web Application Firewalls (WAF)**: Gebruik van WAF-oplossingen om webapplicaties te beschermen tegen veelvoorkomende aanvallen zoals SQL-injectie of cross-site scripting (XSS).
- **Patch Management**: automatiseren van patchbeheer om ervoor te zorgen dat systemen up-to-date blijven en beveiligingslekken worden verholpen.
- **Mobile Device Management (MDM)**: oplossingen voor het beheren en beveiligen van mobiele apparaten binnen de organisatie, inclusief BYOD (Bring Your Own Device).
- **Back-up en disaster recovery tools**: gebruik van back-up- en hersteloplossingen om te zorgen dat je snel kunt herstellen van een cyberincident en dat gegevens veilig zijn.

Datamanagement

- **Digitaal verwerkte data** speelt een centrale rol in de NIS2-richtlijn en andere (cyber) frameworks, omdat het de ruggengraat vormt van elke moderne organisatie.

- Data is een van de **meest waardevolle activa** voor organisaties, en daarom is het vaak het primaire doelwit van cyberaanvallen zoals ransomware, DDoS-aanvallen, en datalekken.

- Regelgeving (waaronder NIS2) vereist daarom dat organisaties voldoen aan strikte normen voor databeveiliging. Voor de invulling van de strikte normen zijn onderstaande zaken van belang:
  - Data classificatie,
  - Data lifecycle management,
  - Encryptie van gevoelige data,
  - Geautomatiseerde gegevensarchivering,
  - Multi-cloud back-up oplossingen,
  - eDiscovery-functionaliteiten,
  - Ransomwarebescherming.

Data juist in de cloud

- Een hybride datamanagementoplossing, waarbij een deel van de data on-premise (eigen datacenter of private cloud) en een deel bij een derde partij in de public cloud wordt beheerd, biedt voordelen, met name in termen van flexibiliteit, kostenoptimalisatie en NIS2-compliance.

- **Hybride oplossingen** bieden het beste van twee werelden, de controle en beveiliging van on-premise opslag, gecombineerd met de flexibiliteit en schaalbaarheid van de cloud.

- Een hybride omgeving biedt **betere gegevensbeschikbaarheid** en zorgt voor **disaster recovery** met geografische diversificatie van data. Door kritieke back-ups zowel on-premise als in de cloud te bewaren, kan een organisatie sneller herstellen van incidenten.

- Door **replicatie van data** naar de cloud, kunnen organisaties snel data herstellen vanaf een externe locatie als de primaire systemen uitvallen. Dit minimaliseert downtime optimaal en zorgt ervoor dat kritieke gegevens en systemen zeer snel weer operationeel zijn.

Bedankt!

PDF van de presentatie? => sebastiaan@databalance.eu