Hoe voldoe je als industrieel bedrijf aan NIS2?

In een wereld waar industriële bedrijven steeds afhankelijker worden van digitale processen, is databescherming cruciaal. De Europese NIS2-richtlijn stelt eisen aan bedrijven om cybersecurity en databeveiliging te verbeteren. Een betrouwbare back-upstrategie is een essentieel onderdeel van compliance met NIS2, met name Artikel 21.

IMMUTEC DATA PROTECTION & CYBERSECURITY

IMMUTEC B.V.
Poststraat 1, 6135 KR Sittard NL, T +31(0)85 301 97 70
info@immutec.eu, www.immutec.eu

WP V202401-NL

Dit lees je in deze whitepaper

- NIS2: wanneer en voor wie
- Achtergrond en totstandkoming van NIS2
- De uitdagingen voor de industrie rondom NIS2
- Misvattingen en vragen over back-ups
- Wat is een back-up ook alweer?
- Welke rol heeft de back-up binnen NIS2?
- Wanneer voldoet een back-up systeem aan de NIS2?
- Procedure om tot een toereikende strategie te komen
- Het 3-2-1-1-0 back-up systeem als absoluut minimum
- Aan de slag met de back-up

Wat is NIS2 en waarom is het relevant?

De NIS2-richtlijn (Richtlijn (EU) 2022/2555) is sinds 2024 van kracht en heeft als doel de cyberweerbaarheid van bedrijven te versterken door strengere eisen te stellen aan de bescherming van netwerk- en informatiesystemen. De richtlijn is gericht op zowel essentiële als belangrijke entiteiten binnen de industrie, waaronder productiebedrijven, logistieke operators, en andere organisaties die een cruciale rol spelen in de Europese economie.

NIS2 bouwt voort op de oorspronkelijke NIS-richtlijn en streeft naar een uniforme aanpak van cybersecurity binnen de EU. Deze nieuwe versie legt een sterkere nadruk op samenwerking tussen lidstaten en dwingt bedrijven om proactief te handelen op het gebied van risicobeheer en incidentrespons. Dit betekent dat organisaties verplicht zijn om robuuste technische en organisatorische maatregelen te implementeren die dataverlies voorkomen, herstel garanderen en cyberdreigingen effectief mitigeren.

Met deze richtlijn wil de EU niet alleen de digitale veiligheid verbeteren, maar ook de continuïteit van essentiële diensten waarborgen en het vertrouwen in de Europese digitale economie versterken. Voor industriële bedrijven is het voldoen aan NIS2 daarom niet alleen een wettelijke vereiste, maar ook een strategische noodzaak om operationele en reputatierisico's te minimaliseren.

De uitdagingen voor de industrie rondom NIS2

Om aan de cybersecurity- en dataprotectie-eisen van de NIS2-richtlijn te voldoen, is er nog veel werk te verrichten binnen de industrie. Bedrijven worden vaak geconfronteerd met vergelijkbare uitdagingen. De NIS2-voorschriften zijn complex en vereisen diepgaand onderzoek, specifieke kennis en aanzienlijke tijdsinvesteringen. Deze complexiteit wordt deels veroorzaakt doordat:

- De regelgeving soms vaag is en niet SMART geformuleerd. Dit maakt het lastig om concrete stappen te definiëren.
- De vereisten variëren per organisatie. Er is geen universele standaard die voor elke industriële sector direct toepasbaar is.
- IT-teams al overbelast zijn. Naast hun reguliere taken moeten zij ook de complexe eisen van NIS2 implementeren.
- Veel bedrijven niet weten waar te beginnen. Het ontbreken van een gestructureerde aanpak leidt tot uitstel en risico's.

Om organisaties hierin te ondersteunen, leggen we de focus op een van de meest cruciale aspecten: een robuuste en NIS2-conforme back-upstrategie.

In deze whitepaper behandelen we:

- Waarom een goede back-upstrategie essentieel is.
- Hoe back-ups bijdragen aan naleving van de NIS2-richtlijn.
- Welke elementen overwogen moeten worden.
- Aan welke exacte eisen een back-upstrategie moet voldoen.

Met deze inzichten bieden we bedrijven een praktisch kader om direct aan de slag te gaan en compliance te realiseren.

Misvattingen over back-ups

‘Onze cloudleverancier maakt automatisch een back-up.’

Risico: Veel cloudleveranciers bieden hoge betrouwbaarheid en redundantie, maar dit is geen vervanging voor een onafhankelijke back-up. Cloudservices beschermen doorgaans niet tegen onbedoeld verwijderen, wijzigingen door medewerkers, of specifieke aanvallen zoals ransomware.

Incident: Zonder een eigen back-upstrategie kan gegevensverlies door menselijke fout of kwaadwillende toegang permanent zijn, omdat de synchronisatie van wijzigingen ook de originele gegevens kan overschrijven.

‘Ransomware zal ons niet treffen, we zijn geen groot bedrijf.’

Risico: Cybercriminelen richten zich vaak juist op kleinere bedrijven omdat deze doorgaans minder geavanceerde beveiligingsmaatregelen hebben en sneller losgeld betalen om toegang te herstellen.

Incident: Een ransomware-aanval kan alle bestanden versleutelen, inclusief back-ups die niet goed geïsoleerd zijn. Zonder immutable storage of air-gapped back-ups kan zelfs een kleinere aanval verwoestend zijn.

‘Een enkele kopie van onze data is voldoende.’

Risico: Eén kopie biedt geen bescherming tegen hardwarestoringen, fysieke rampen (zoals brand of overstroming), of menselijke fouten. Als de primaire kopie beschadigd raakt, is er geen herstelmogelijkheid.

Incident: Industriële bedrijven die afhankelijk zijn van operationele processen kunnen aanzienlijke downtime en productieverlies ervaren als gegevens niet beschikbaar zijn.

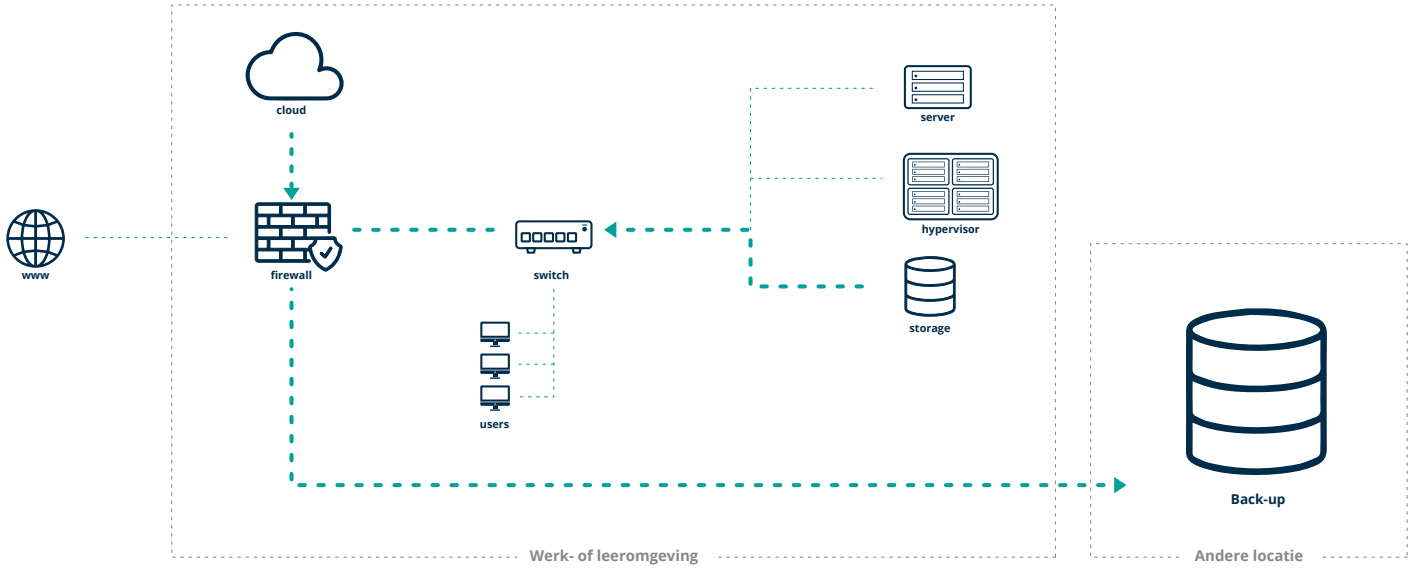
Deze aannames negeren de noodzaak van een robuuste, redundante back-upstrategie. Het niet implementeren van een solide back-upbeleid vergroot het risico op gegevensverlies, productie-uitval, reputatieschade en niet-naleving van regelgeving zoals NIS2.

Wat is een back-up ook alweer?

Een back-up is een veilige kopie van belangrijke gegevens, die je bewaard op een aparte plek. Als er iets fout gaat met de originele gegevens, zoals bij een virusaanval, storing of menselijke fout, kan de back-up deze gegevens herstellen.

Dit zorgt ervoor dat werk en processen snel weer kunnen doorgaan. Een cruciaal onderdeel van risicobeheer.

Met een back-up herstel je de data en waarborg je de continuïteit van jouw bedrijf.



Welke rol heeft de back-up binnen NIS2?

Artikel 21 van NIS2 benadrukt het belang van databeveiliging en continuïteit. Back-ups zijn essentieel om te voldoen aan de richtlijnen voor risicobeheer en incidentrespons.

Wanneer voldoet een back-up systeem aan de NIS2?
Een back-up systeem voldoet aan NIS2 als het:

- Redundant is (meerdere kopieën).
- Beveiligd is tegen manipulatie (immutable).
- Regelmatig getest wordt.
- Data op een externe locatie bewaart.

Procedure om tot een toereikende strategie te komen

1. Inventariseer kritieke systemen en data

- **Waarom is dit belangrijk**
  Het is essentieel om te weten welke systemen en data cruciaal zijn voor je bedrijfsvoering. Zonder een helder beeld van welke gegevens beschermd moeten worden, kunnen back-ups onvolledig of ineffectief zijn.

- **Hoe kun je dit aanpakken**
  - Identificeer systemen die essentieel zijn voor productie, logistiek, en bedrijfscontinuïteit.
  - Breng de data in kaart die wordt verwerkt, inclusief financiële, operationele en klantgegevens.
  - Gebruik de BIV-classificatie (Beschikbaarheid, Integriteit, Vertrouwelijkheid) om prioriteiten te bepalen.
  - Werk samen met IT- en operationele teams om een compleet overzicht te krijgen.

2. Voer een risicoanalyse uit

- **Waarom is dit belangrijk**
  Een risicoanalyse geeft inzicht in potentiële bedreigingen en kwetsbaarheden die je systemen en data kunnen treffen. Dit vormt de basis voor een gerichte back-upstrategie.
- **Hoe kun je dit aanpakken**
  - Identificeer risico's zoals ransomware, hardwarestoringen, en fysieke calamiteiten.
  - Analyseer de impact van gegevensverlies op bedrijfsprocessen.
  - Gebruik tools zoals een Data Protection Impact Assessment (DPIA) om privacyrisico's te evalueren.
  - Documenteer de bevindingen en prioriteer risico's op basis van waarschijnlijkheid en impact.

3. Stel een back-upstrategie op

- **Waarom is dit belangrijk**
  Een goed doordachte strategie biedt een gestructureerde aanpak om data te beschermen en snel te herstellen in geval van incidenten. Zonder strategie is de kans op hiaten in de back-updekking groot.
- **Hoe kun je dit aanpakken**
  - Definieer doelen zoals maximale toegestane dataverlies (RPO) en hersteltijd (RTO).
  - Bepaal hoe vaak back-ups moeten worden gemaakt en waar deze worden opgeslagen (on-site, off-site, cloud).
  - Plan voor incrementele en volledige back-ups op basis van de frequentie van gegevenswijzigingen.
  - Stel toegangsbeperkingen en versleuteling in voor back-ups.

4. Implementeer het 3-2-1-1-0 model

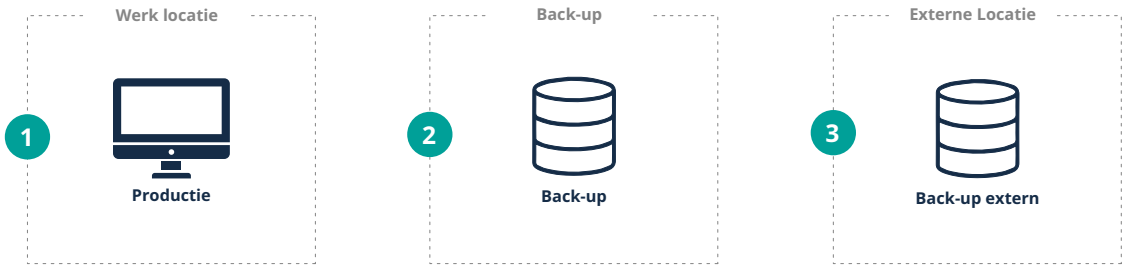
- **Waarom is dit belangrijk**
  Het model biedt een bewezen structuur die gegevensverlies minimaliseert en herstel garandeert. Het is afgestemd op de eisen van NIS2 en best practices in databeheer.
- **Hoe kun je dit aanpakken**
  - 3 kopieën: Maak een hoofdkopie, een lokale back-up en een off-site back-up.
  - 2 verschillende media: Gebruik bijvoorbeeld een lokale NAS (Network Attached Storage) en cloudopslag.
  - 1 externe kopie: Sla een kopie op een fysiek gescheiden locatie op om rampen op de primaire locatie te overleven.
  - 1 immutable kopie: Gebruik opslagoplossingen met write-once-read-many (WORM) mogelijkheden voor ransomwarebescherming.
  - 0 fouten: Stel automatische tests en monitoring in om de integriteit van back-ups te waarborgen.

3-2-1-1-0 back-up systeem als absoluut minimum

3-2-1-0-0 back-up systeem als absoluut minimum

Hoewel elke organisatie een ander back-up systeem nodig heeft om aan NIS2 criteria te voldoen, is er één methode dat elk bedrijf als absoluut minimum moet aanhouden: het 3-2-1-1-0 back-up systeem. Op de volgende bladzijden lees je meer over de inhoud van dit systeem en hoe dit zich verhoudt tot de NIS2.

3 Verschillende versies



Wat houdt het in?
Zorg voor minstens 3 versies van je data.

Gegevens heb je dan drie keer tot je beschikking. De kans dat er iets misgaat met alle drie de versies is een stuk kleiner dan wanneer je er slechts 1 of 2 hebt.

Waarom is dit essentieel
Redundantie is de sleutel tot het minimaliseren van het risico op gegevensverlies. Door drie kopieën te maken, is de kans dat alle kopieën tegelijkertijd verloren gaan aanzienlijk kleiner.

Voldoe aan NIS2
Dit sluit aan bij de risicomanagementvereisten van Artikel 21, waarin redundantie wordt genoemd als een basismaatregel om de impact van incidenten te minimaliseren. Meerdere kopieën dragen bij aan de beschikbaarheid van gegevens, een kernprincipe van de NIS2.

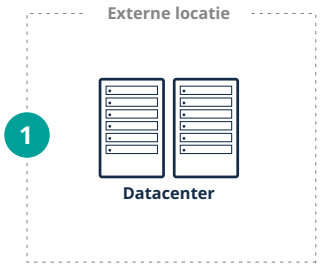
2 Soorten media

Wat houdt het in?
Bewaar nooit twee kopieën van jouw back-up op hetzelfde type opslagmedium. Zorg er bijvoorbeeld voor dat je data op een fysieke storage (NAS) staat, in de cloud of een private cloud.

Waarom is dit essentieel
Het gebruik van verschillende opslagmedia, zoals lokale servers en cloudopslag, biedt bescherming tegen specifieke risico's die verbonden zijn aan één type medium, zoals hardwarestoringen of aanvallen gericht op een enkel opslagplatform.

Voldoe aan NIS2
Dit beantwoordt aan de eis om fysieke en logische scheiding toe te passen, waardoor de kans op grootschalig verlies wordt beperkt. Het ondersteunt ook continuïteitsbeheer en gegevensintegriteit.

1 Offsite locatie

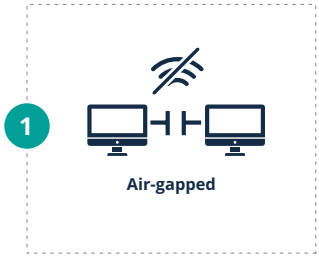


Wat houdt het in?
Het is ten zeerste aanbevolen om minstens één kopie van de back-up weg te houden van fysieke locatie waar de primaire data staat. Het is geen goed idee om die 2e kopie op dezelfde fysieke locatie te bewaren.

Waarom is dit essentieel
Door een kopie op een externe locatie te bewaren, worden data beschermd tegen fysieke calamiteiten zoals brand, overstromingen of diefstal op de primaire locatie.

Voldoe aan NIS2
Artikel 21 benadrukt de noodzaak van veerkracht in de infrastructuur. Het bewaren van een off-site back-up zorgt voor herstelmogelijkheden in het geval van een groot incident, waarmee bedrijven voldoen aan de eisen voor continuïteitsbeheer en incidentherstel.

1 Air-gapped kopie

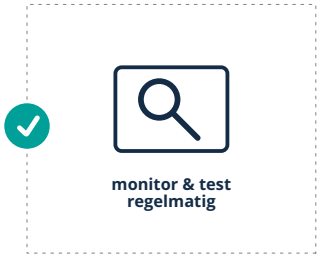


Wat houdt het in?
Air-gapped betekend dat er geen directe verbinding is tussen jouw IT-infrastructuur en het back-up platform. Voor kwaadwillenden is het vrijwel onmogelijk om hier bij te komen.

Waarom essentieel
Een air-gapped kopie is volledig fysiek en virtueel gescheiden van het netwerk, waardoor het onmogelijk wordt voor aanvallers om via een online verbinding toegang te krijgen tot deze back-up. Dit biedt robuuste bescherming tegen ransomware-aanvallen en andere cyberdreigingen die gericht zijn op het vernietigen of versleutelen van data. Omdat de air-gapped kopie niet toegankelijk is vanaf het primaire netwerk, blijft deze ongeschonden bij aanvallen op de overige systemen.

Voldoen aan NIS2
Deze aanpak sluit aan bij de vereisten voor gegevensbeschikbaarheid en integriteit, zoals vastgelegd in Artikel 21 van de NIS2-richtlijn. Door een air-gapped kopie te implementeren, voldoen organisaties aan de eisen voor incidentrespons en risicobeheer. Het biedt een bewezen strategie om gegevens te beschermen tegen ransomware en om continuïteit te waarborgen in geval van een aanval.

0 Backup fouten



Wat houdt het in?
Zorg ervoor dat je geverifieerde back-ups zonder fouten hebt. Controleer je back-up dagelijks. Voer op regelmatige tijdstippen hersteltest uit.

Waarom is dit essentieel
Het testen van back-ups zorgt ervoor dat de gegevens niet alleen correct worden opgeslagen, maar ook probleemloos kunnen worden hersteld. Zonder testen kunnen bedrijven valse zekerheden hebben over hun back-ups.

Voldoe aan NIS2
Regelmatige tests zijn in lijn met de verplichting om risicobeheersmaatregelen continu te evalueren en te verbeteren. Dit helpt bij het identificeren van zwakke punten in het back-up- en herstelproces en draagt bij aan het waarborgen van de beschikbaarheid van gegevens.

Aan de slag met de back-up

Hopelijk biedt dit whitepaper meer inzicht en een duidelijk startpunt om aan de NIS2-richtlijnen te voldoen. Het implementeren van een effectieve back-upstrategie blijft een complex proces dat tijd, expertise en investeringen vraagt. Tegelijkertijd zijn de risico's groot, zoals dataverlies, stilstand van productieprocessen en niet-naleving van regelgeving, wat kan leiden tot hoge boetes en reputatieschade. Veel bedrijven kiezen daarom voor de ondersteuning van specialisten zoals IMMUTEC, die kunnen helpen bij het ontwikkelen en uitvoeren van een NIS2-conform back-upbeleid.

Wat IMMUTEC voor je doet:

- ✔ **Samen het beleid bepalen:**
  Gebaseerd op alle voorgaande stappen, zoals BIV-classificatie en risicoanalyse, wordt een op maat gemaakt beleid ontwikkeld.
- ✔ **Inrichting van het beleid:**
  Het technisch en organisatorisch implementeren van de strategie.
- ✔ **Uitvoering van het beleid:**
  Zorgdragen voor dagelijkse operationele processen en back-upbeheer.
- ✔ **Beheer van de externe back-up:**
  Waarborgen dat back-ups veilig zijn opgeslagen en voldoen aan de NIS2-vereisten.
- ✔ **Periodieke checks:**
  Regelmatige evaluaties en tests om de effectiviteit en naleving te waarborgen.

Voordelen:

- ✔ **Geen eigen kennis, hardware of software nodig**
- ✔ **Geen opstartkosten dus geen afbreukrisico**
- ✔ **Lage TCO (total cost of ownership)**
- ✔ **Continuïteit geborgt**
- ✔ **Extra gemoedsrust**
- ✔ **Minder uren nodig van jouw IT'ers**
  minder druk, geen tijd kwijt aan updates en onderhoud