Provincie Noord-Brabant

NIS2 WETGEVING

Wat betekend dit voor onze organisatie

NETWORK AND INFORMATION SECURITY DIRECTIVE

De NIS2 (Network and Information Security directive) is een nieuwe Europese richtlijn en vervangt de huidige NIS richtlijn. Het belangrijkste doel van de NIS2 is het vergroten van digitale weerbaarheid en het beperken van de gevolgen van cyberincidenten in de Europese Unie (EU).

NIS2 = Alle 27 lidstaten

In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de CBW (Cyberbeveiligingswet). Op het moment dat de CBW wordt aangenomen, vervangt deze de huidige Wbni (Wet beveiliging netwerk- en informatiesystemen)

NIS2 VERSUS NIS1

Richtlijn geldt voor meer sectoren
De NIS2 is van toepassing op zowel essentiële als grote bedrijven. Meer middelgrote en grote bedrijven moeten aan de richtlijn gaan voldoen.

Lijst van minimale basisbeveiliging
De richtlijn is concreter dankzij een lijst van minimale basisbeveiligingen die bedrijven moeten implementeren.

Indeling in essentiële en belangrijke sectoren
De nieuwe richtlijn verdeelt bedrijven in essentiële en belangrijke sectoren.

Beveiliging in de keten aanpakken
Bedrijven moeten beveiligingsrisico's in hun toeleveringsketen adresseren. Hieronder vallen ook risico's die ontstaan door relaties met leveranciers.

Strenger toezicht
Nationale autoriteiten moeten strenger toezicht houden en strenger handhaven.

ESSENTIELE SECTOREN

De NIS2 maakt een onderscheid tussen essentiële en belangrijke sectoren

Essentiele Sectoren

- Energie
- Afvalwater
- Banken
- Digitale infrastructuur
- Gezondheidszorg
- Drinkwater
- Vervoer
- Financiële markten
- Overheidsdiensten
- Ruimte

Belangrijke Sectoren

- Post en Koeriersdiensten
- Afvalverwerking
- Productiebedrijven
- Voedselindustrie
- Verwerking en distributie
- Digitale aanbieders
- Chemische industrie

ESSENTIEEL VERSUS BELANGRIJKE SECTOREN

Essentiele sectoren
Essentiele sectoren vallen onder de meldplicht en zorgplicht van de NIS2 dit houdt onder meer in:

- Dat de toezichthouder (Rijksdienst Digitale Infrastructuur) proactief toezicht houdt op de betreffende sectoren;

-Verplichting om de gehele “toeleveringsketen” in kaart te brengen en op een juiste wijze te beveiligen;

- Duidelijke communicatie bij eventuele cyberincidenten.

Belangrijke sectoren

- Dat de toezichthouder achteraf toezicht houdt op de betreffende sectoren (na incidenten);

VERPLICHTINGEN NIS2

Nieuwe verplichtingen
Om als organisatie te voldoen aan de verplichtingen vanuit de NIS2 moeten er diverse (nieuwe) activiteiten worden ondernomen. Het betreft hier de volgende verplichtingen:

- Zorgplicht
- Meldplicht
- Registratieplicht

ZORGPLICHT

Provincies moeten maatregelen treffen om hun netwerk- en informatiesystemen te beschermen tegen incidenten. Hieronder valt zowel kantoorautomatisering (KA) als operationele technologie (OT), zoals bruggen, sluizen en VRI's. Een voorbeeld van maatregelen zijn:

- Risicoanalyses en beveiliging informatiesystemen;
- Maatregelen op het gebied van bedrijfscontinuiteit;
- Beveiliging van de leverancierskеten;
- Beleid incident afhandelingen.

MELDPLICHT

De provincie wordt verplicht om bij significante incidenten binnen 24 uur een vroegtijdige waarschuwing en binnen 72 uur een melding met aanvullende informatie te maken bij het CSIRT en de toezichthouder (RDI).

- Er wordt beoogd om de melding aan het CSIRT technisch zo in te richten dat het verspreiden van de informatie maar één handeling vergt. Daarnaast zijn er verschillende rapportageverplichtingen (voortgangs- en/of eindverslag).

- Voor het maken van de meldingen richt het NCSC een meldportaal in, waar provincies op moeten aansluiten.

Provincie Noord-Brabant

REGISTRATIEPLICHT

Provincies moeten zich bij het NCSC Nationaal Cyber Security Center registreren als essentiële entiteit. Hierbij moeten enkele basisgegevens over de provincie aangeleverd worden, zoals adres- en contactgegevens. Deze gegevens worden vervolgens gedeeld met ENISA (het Agentschap van de Europese Unie voor Cyberbeveiliging).

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

TOEZICHTHOUDER

De RDI (Rijksdienst Digitale Infrastructuur) is aangewezen als toezichthouder voor provincies. De belangrijkste punten v.w.b. het toezicht zijn:

- De RDI gaat toezicht houden op het hele stelsel van informatieveiligheid voor de overheid op basis van systeemtoezicht.
- RDI maakt zoveel mogelijk gebruik van de bestaande verantwoordingsinformatie en vraagt bestuurslagen deze eenduidig/eenvormig aan te leveren.
- Er zijn nog veel onduidelijkheden over hoe RDI toezicht exact gaat inrichten.

NIS2 TOEZICHT EN AANSPRAKELIJKHEID

Toezicht de belangrijkste punten:

- Periodieke controle en aansprakelijkheid bij non-conformity op de richtlijnen.
- Boetebevoegdheid van 2% van wereldwijde omzet met maximum van 10Mio.
- Bij een incident: gerechtelijke persoonlijke aansprakelijkheid bij incidenten met schade.

Aansprakelijkheid:

De NIS2 brengt voor overheidsbestuurders geen nieuwe aansprakelijkheden met zich mee. Dit betekent dus niet dat er geen aansprakelijkheid binnen overheidsinstanties is. Immers ook nu kunnen bestuurders bij grove nalatigheid al aansprakelijk worden gesteld.

Provincie Noord-Brabant

NIS2 ONDERZOEK PBLQ

In opdracht van het Interprovinciaal Overleg (IPO) heeft PBLQ een impactanalyse uitgevoerd naar de eisen en verplichtingen die voortkomen uit de NIS2 richtlijnen en de bijbehorende Cyberbeveiligingswet (CBW) en BIO2. Hiermee is in kaart gebracht.

- Wat de huidige stand van zaken is bij de afzonderlijke provincies in relatie tot de zorgplicht, meldplicht en het toezicht;

- Welke additionele inspanning de twaalf provincies afzonderlijk moeten leveren om te voldoen aan de verplichtingen vanuit de NIS2, in termen van activiteiten, bemensing en benodigde financiële middelen.

NIS2 HOE STAAN WE ER VOOR

Uitkomst onderzoek PBLQ:

De uitkomst van het onderzoek is dat we als organisatie een laag risico hebben op de implementatie van de NIS 2. Onderwerpen die nog aandacht behoeven zijn:

- Opleidingen (bestuur en medewerkers)
- BCM inrichting
- Leveranciersmanagement
- Inrichten proces meldplicht