VAN OERS
it advies

VAN OERS IT ADVIES
HOE WORD JE NIS2-PROOF?

De Network and Information Security directive, of NIS2-richtlijn, is de opvolger van de NIS-richtlijn. Deze is vastgesteld door de Europese Unie en richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. De komst van de richtlijn moet bijdragen aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties.

De NIS2-richtlijn richt zich naast sectoren die al onder de eerste NIS-richtlijn viellen ook op een aantal nieuwe sectoren. Het aantal publieke en private organisaties dat onder de richtlijn valt wordt dus groter. Een belangrijk verschil met de eerste NIS-richtlijn is dat organisaties automatisch onder de NIS2-richtlijn vallen als zij actief zijn in een van de onderstaande sectoren en volgens de onderstaande criteria gekenmerkt kunnen worden als 'essentiële' of 'belangrijke' entiteit.

GROEP A	GROEP B
Energie	Digitale aanbieders
Transport	Post- en koeriersdiensten
Bankwezen	Afvalstoffenbeheer
Infrastructuur financiële markt	Levensmiddelen
Gezondheidszorg	Chemische stoffen
Drinkwater	Onderzoek
Digitale infrastructuur	Vervaardiging/manufacturing
Beheerders van ICT-diensten	
Afvalwater	
Overheidsdiensten	
Ruimtevaart	

Essentiële entiteiten: dit betreffen grote organisaties die actief zijn in een sector uit groep A in de tabel.

Een organisatie is groot op basis van de volgende criteria:

- minimaal 250 werknemers of;
- een jaaromzet van meer dan € 50 miljoen en een balanstotaal van meer dan € 43 miljoen.

Belangrijke entiteiten: dit betreffen middelgrote organisaties die actief zijn in een sector uit groep A en middelgrote en grote organisaties die actief zijn in een sector uit groep B.

Een organisatie is middelgroot op basis van de volgende criteria:

- minimaal 50 werknemers of;
- een jaaromzet en balanstotaal van meer dan 10 miljoen euro.

Van essentiële entiteiten wordt over het algemeen aangenomen dat de uitval van hun diensten veel meer ontwrichtende impact heeft op de economie en samenleving, dan uitval bij belangrijke entiteiten. Essentiële entiteiten vallen onder een intensiever regime van toezicht, waar zowel voor- als achteraf toezicht wordt gehouden op de naleving van de verplichtingen. Voor belangrijke entiteiten geldt een lichtere vorm van toezicht. Hier wordt alleen achteraf toezicht gehouden, bijvoorbeeld als er aanwijzingen voor niet-naleving van de wet zijn of als er een incident heeft plaatsgevonden.

Micro- en kleine bedrijven vallen in principe niet onder de NIS2-richtlijn. De minister die verantwoordelijk is voor een bepaalde sector kan er echter wel voor kiezen om een micro- of klein bedrijf alsnog aan te wijzen op basis van een risicobeoordeling, bijvoorbeeld als blijkt dat hun dienstverlening van cruciaal belang is voor de Nederlandse economie of maatschappij. In dat geval worden deze bedrijven hierover geïnformeerd door het desbetreffende ministerie. Daarnaast zijn er nog micro- en kleine bedrijven die wel onder de NIS2-richtlijn vallen.

Het gaat dan om bedrijven die actief zijn in:

- Aanbieder van vertrouwensdiensten
- Register voor topleveldomeinnamen
- Verleners van domeinnaamregistratiediensten
- Aanbieder van openbare elektronische-communicatienetwerken
- Aanbieder van openbare elektronische-communicatiediensten

Overheidsinstanties uit de bovenstaande sectoren vallen ook automatisch onder NIS2-richtlijn. Daarnaast is het van belang dat organisaties zich ook bewust zijn van een ketenverantwoordelijkheid en hun klanten en of leveranciers de eis kunnen neerleggen dat zijn NIS2-compliance bereiken.

WELKE VERPLICHTINGEN SCHRIJFT NIS2 VOOR?

De NIS2-richtlijn schrijft een zorg- en meldplicht voor.
Tevens wordt er toezicht gehouden op de betreffende organisaties.

Zorgplicht

De richtlijn bevat een zorgplicht die entiteiten verplicht om zelf een risicobeoordeling te doen. Op basis daarvan nemen zij passende maatregelen om hun diensten zoveel mogelijk te waarborgen en de gebruikte informatie te beschermen.

Meldplicht

De richtlijn schrijft voor dat entiteiten incidenten binnen 24 uur bij de toezichthouder moeten melden. Het gaat om incidenten die de verlening van de dienst sterk (kunnen) verstoren. Een cyberincident moet ook bij het Computer Security Incident Response Team (CSIRT) gemeld worden. Dit team kan vervolgens hulp- en bijstand leveren. Factoren die een incident meldingswaardig maken, zijn bijvoorbeeld het aantal personen dat door de verstoring is geraakt, de tijdsduur van een verstoring en de mogelijke financiële verliezen.

Toezicht

Organisaties die onder de richtlijn vallen, komen ook onder toezicht te staan op naleving. Let op:

- Essentiële sector: voor- en achteraf toezicht;
- Belangrijke sector: achteraf toezicht.

Tijdsindicatie

Momenteel wordt de onderstaande planning gevolgd in het vertalen van de NIS2-richtlijn naar nationale wetgeving.
Dit is een indicatieve planning, die nog kan wijzigen.

WAT KAN MINIMAAL AL WORDEN GEDAAN?

Helaas kan op dit moment de vraag nog niet geheel concreet worden beantwoord, simpelweg omdat de concrete vertaling naar Nederlandse wetgeving pas net gestart is. In het najaar van 2023 start een consulatie-periode waarin burgers, bedrijven en overheidsinstellingen feedback kunnen geven op wet- en regelgeving die in voorbereiding is. Op dat moment kan ook meer duidelijkheid geboden worden over de concrete vertaling van de richtlijn naar nationale wetgeving, zodat organisaties zich beter kunnen voorbereiden. Hoewel veel vragen nu nog niet beantwoord kunnen worden, kan er wel al een basis worden gecreëerd om te voldoen aan de zorgplicht:

- Inventariseren en analyseren van risico's & maatregelen: nulmeting ofwel een cybersecurity assessment;
- Bewustwording van personeel van risico's en te nemen maatregelen zoals awareness trainingen en campagnes;
- Opstellen van bedrijfscontinuïteitplannen;
- Security monitoring & detectie;
- Protocollen voor crisisbeheersing definiëren: cybersecurity incident procedures;
- Basis hygiëne cybersecurity: logische toegangsbeveiliging, back-up en continuïteitprocedures, patchmanagement/ update beleid, versleuteling van data, logging, en andere;

Tevens bestaan er een aantal kaders van informatiebeveiliging welke de NIS2-compliance versterken. Dit betreffen de ISO standaard voor informatiebeveiliging (ISO 270001), de norm die betrekking heeft op informatiebeveiliging in de gezondheidszorg (NEN 7510) en het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (BIO).

Daarnaast is het verstandig om benodigd budget en capaciteit alvast te reserveren.

Organisaties kunnen zich ook al voorbereiden op de meldplicht en het toezicht door een intern proces te implementeren inclusief het beleggen van de taken en verantwoordelijkheid binnen de organisatie en deze duidelijk te communiceren. Tevens is het aan te bevelen om de aantoonbaarheid van bestaande cybersecurity-maatregelen concreet te maken. Denk daarbij aan de rapportage van het cybersecurity assessment, resultaten van awareness trainen en testrapportages van bedrijfscontinuïteitenplannen.

VAN OERS it advies

WAT KAN VERWACHT WORDEN VAN DE OVERHEID

Vanuit de overheid kunnen organisaties verwachten dat ze ondersteund worden door een Computer Security Incident Response Teams (CSIRT) die de volgende taken op zich zal nemen:

- Reageren op incidenten die vrijwillig of verplicht worden gemeld;
- Incidenten op nationaal niveau monitoren, aanbieders vroegtijdig waarschuwen en informatie over risico's en incidenten verspreiden;
- Deelnemen aan het internationale netwerk van CSIRT's;
- Op samenwerking gerichte contacten onderhouden met de particuliere sector.

De ondersteuning vanuit de overheid kan verder bestaan uit informatie-uitwisseling, richtlijnen en weerbaarheid verhogende instrumenten, bijvoorbeeld voor het uitvoeren van een risico-beoordeling.

WAT LEVERT HET OP

Wanneer organisaties hun beveiligingseisen niet op orde hebben zal dit waarschijnlijk resulteren in meer en hogere boetes. De boetes kunnen oplopen tot ten minste 10 miljoen euro of 2% van de totale wereldwijde omzet. De EU-lidstaten zijn echter vrij om te bepalen hoe hoog de boetes zijn, waardoor waarschijnlijk differentiatie van boetebedragenzal. De hoogte zal afhankelijk zijn van de aard van de inbreuk. Het is belangrijk om als organisatie ook te beseffen dat het voldoen aan de NIS2-richtlijn ook zeker wat gaat opleveren:

- **Verbeterde cybersecurity:**
  NIS2 is ontworpen om de algehele cybersecurity te verbeteren door organisaties aan te moedigen beveiligingsmaatregelen te implementeren en beveiligingsincidenten te melden. Dit draagt bij aan een verhoogde weerbaarheid tegen cyberaanvallen en potentiële gegevensinbreuken.
- **Vermindering van risico's:**
  Door te voldoen aan de beveiligingseisen en het implementeren van beste praktijken zoals vastgesteld in NIS2, kunnen organisaties hun blootstelling aan cybersecurityrisico's verminderen. Dit kan op lange termijn schade aan de reputatie en financiële verliezen voorkomen.
- **Vertrouwen van belanghebbenden:**
  Het voldoen aan NIS2-normen en het melden van beveiligings-incidenten kan het vertrouwen van klanten, partners en belanghebbenden vergroten. Het laat zien dat een organisatie toegewijd is aan het waarborgen van de beveiliging van gegevens en digitale diensten.
- **Samenwerking en informatie-uitwisseling:**
  NIS2 bevordert samenwerking tussen lidstaten en organisaties. Het faciliteert ook de uitwisseling van informatie over bedreigingen en incidenten, wat kan bijdragen aan een gecoördineerde reactie op grootschalige cyberaanvallen.
- **Verbeterde operationele efficiëntie:**
  Door te voldoen aan de beveiligingsnormen van NIS2 kunnen organisaties hun eigen beveiligingspraktijken verbeteren en zo efficiënter en veerkrachtiger worden.

Wilt u meer weten over hoe u NIS2 compliant kan worden of kunt u ondersteuning gebruiken op dit gebied?
Onze specialisten helpen u graag verder!

Brechtje Brugman-Dekkers
Manager IT advies
E. B.Brugman@vanoers.nl
T. +31 (0)6 820 464 65