Wat is de NIS2-richtlijn?

In deze digitale tijd maken zowel individuen als organisaties zich steeds meer zorgen over cyberbeveiliging omdat cyberaanvallen steeds vaker voorkomen. In 2016 heeft de Europese Commissie de EU-richtlijn voor netwerk- en informatiebeveiliging (NIS) geïntroduceerd om de cyberveiligheid in de hele Europese Unie te verbeteren. Maar de richtlijn voldeed niet helemaal aan de verwachtingen voor verantwoording, dus heeft de Commissie besloten deze te vervangen door de uitgebreidere NIS2-richtlijn.

NIS2 verplicht bedrijven om belangrijke cyberbeveiligingsmaatregelen te nemen. Dit omvat het beveiligen van de toeleveringsketen, het gebruik van cryptografie en encryptie (artikel 18). Ook benadrukt artikel 89 het belang van het implementeren van basispraktijken voor cyberhygiëne. Hieronder vallen zero-trustprincipes, regelmatige software-updates, configuratie van apparaten, het opdelen van netwerken en het beheer van identiteiten en toegang voor essentiële en belangrijke entiteiten.

NIS vs. NIS2 - wat is er veranderd?

Er zijn een aantal belangrijke verschillen tussen de oude en de nieuwe richtlijn:

- In het nieuwe voorstel verdwijnt het onderscheid tussen Operators of Essential Services (OES) en Digital Service Providers (DSP). In plaats daarvan worden entiteiten als essentieel of belangrijk geclassificeerd.
- Het toepassingsgebied van de richtlijn wordt uitgebreid naar nieuwe sectoren op basis van hun cruciale rol voor de economie en de samenleving. Dit omvat nu alle middelgrote en grote bedrijven in deze sectoren. Lidstaten kunnen ook kleinere entiteiten met een hoog risicoprofiel identificeren.
- Er wordt voorgesteld om een Europees verbindingsnetwerk voor cybercrises (EU-CyCLONe) op te richten. Dit netwerk zou gezamenlijke snelle noodplannen voorbereiden en implementeren, bijvoorbeeld in het geval van een grootschalig cyberincident of -crisis.
- Meer samenwerking bij het vrijgeven van nieuwe beveiligingsproblemen die in de hele Unie zijn ontdekt. Er wordt een lijst met administratieve sancties opgesteld, vergelijkbaar met die van GDPR/AVG, waaronder boetes voor het niet naleven van de rapportage- en beheerverplichtingen van risico's op het gebied van cyberbeveiliging.
- NIS2 legt directe verplichtingen op aan het management om de naleving van de wetgeving door hun organisatie te implementeren en te controleren. Dit kan leiden tot boetes en een tijdelijk verbod op het uitvoeren van managementfuncties, ook op het C-suite niveau.

Daarnaast worden er meer specifieke eisen gesteld aan de procedure voor het melden van incidenten, de inhoud van de rapporten en de tijdlijnen (binnen 24 uur na ontdekking van het incident). Op Europees niveau versterkt het voorstel de cyberbeveiliging voor belangrijke informatie- en communicatietechnologieën. De lidstaten zullen in samenwerking met de Commissie en ENISA, het bureau voor cyberbeveiliging van de Europese Unie, risicoanalyses van cruciale toeleveringsketens moeten uitvoeren.

Op wie is de richtlijn van toepassing?

Onder de oude NIS-richtlijn moesten lidstaten beslissen welke bedrijven als essentiële dienstverleners werden beschouwd en dus onder de richtlijn vielen. Maar onder de nieuwe NIS2-richtlijn geldt er een soort limiet op de grootte van bedrijven, een zogenaamde „size-cap", die onder de regelgeving vallen. Dit betekent dat alle middelgrote en grote bedrijven die actief zijn in sectoren of diensten die onder de richtlijn vallen, erdoor worden beïnvloed.

Hieronder vindt u een classificatie per bedrijfsgrootte:

Essentiële entiteiten (EE) De drempelwaarde voor grootte kan verschillen per sector, maar is meestal ongeveer 250 werknemers, een jaaromzet van €50 miljoen of een balans van €43 miljoen	**Belangrijke Entiteiten (IE: "Important entities")** De drempelwaarden voor grootte kunnen verschillen afhankelijk van de sector, maar over het algemeen gaat het om ongeveer 50 werknemers, een jaaromzet van €10 miljoen of een balanstotaal van €10 miljoen
Energie	Postdiensten
Transport	Afvalbeheer
Financiën	Chemische industrie
Openbaar bestuur	Onderzoek
Gezondheidszorg	Voedselsector
Lucht- en ruimtevaart	Productie
Watervoorziening (drinkwater & afvalwater)	Digitale dienstverleners (bijv. sociale netwerken, zoekmachines, online marktplaatsen)
Digitale infrastructuur (bijv. cloud computing-dienstverleners en ICT-beheer)	

NIS2 heeft ook gevolgen voor overheidsinstanties op centraal en regionaal niveau, maar niet voor parlementen en centrale banken.

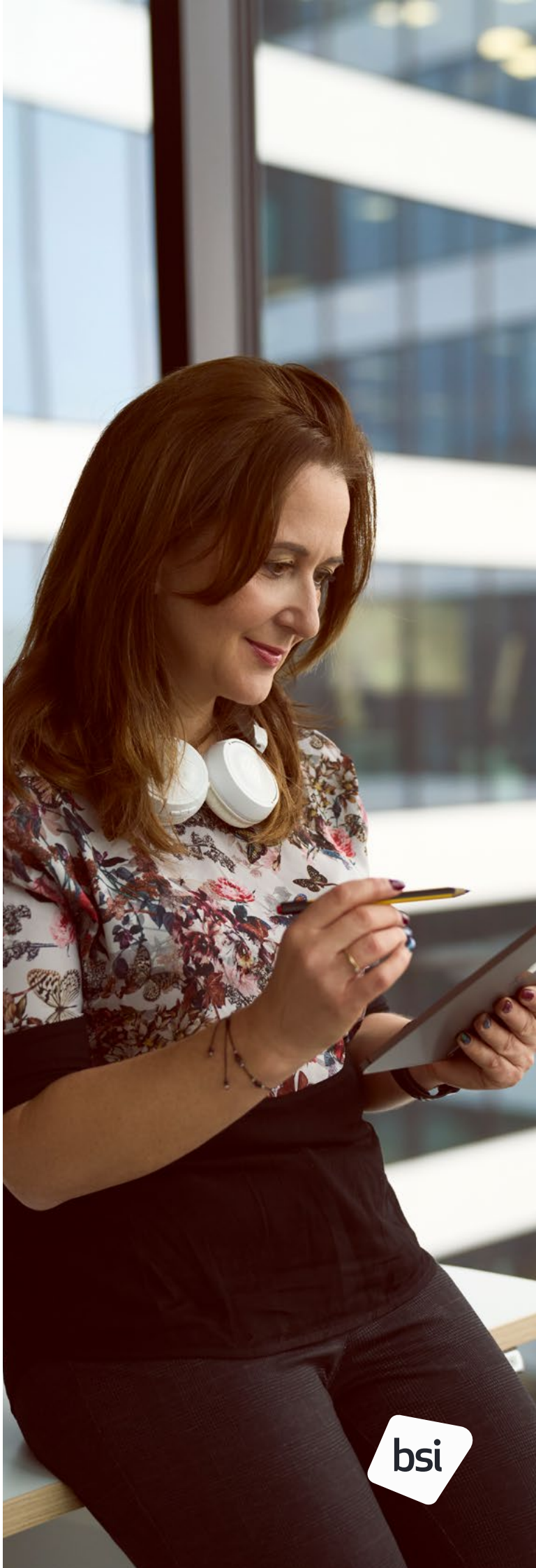
Wanneer wordt het ingevoerd?

Het nieuwe NIS2-kader moet vóór 17 oktober 2024 worden opgenomen in de nationale wetgeving van alle EU-lidstaten. Na de definitieve goedkeuring op 16 januari 2023 hebben de betrokken entiteiten een nalevingsperiode van 21 maanden gekregen zodra de richtlijn van kracht wordt. Hieronder volgt een overzicht van de belangrijkste datums in de ontwikkeling van NIS:

- **6 juli 2016:** NIS vastgesteld
- **9 mei 2018:** Deadline voor lidstaten om NIS om te zetten in nationale wetgeving
- **7 juli 2020:** Europese Commissie start overleg over hervorming NIS
- **16 december 2020:** Europese Commissie publiceert voorstel voor NIS2
- **22 november 2021:** Europees Parlement stelt onderhandelingspositie vast
- **3 december 2021:** Europese Raad stelt onderhandelingspositie vast
- **13 januari 2022:** Eerste ronde van trialoogonderhandelingen
- **16 februari 2022:** Tweede ronde van de trialoogonderhandelingen
- **13 mei 2022:** Politieke overeenstemming bereikt
- **10 november 2022:** Europees Parlement stemt voor goedkeuring van NIS2
- **28 november 2022:** NIS2 goedgekeurd door de Raad van de EU
- **27 december 2022:** NIS2 wordt gepubliceerd in het Publicatieblad en treedt 20 dagen later in werking, op 16 januari 2023
- **17 oktober 2024:** Deadline voor lidstaten om NIS2 om te zetten in nationale wetgeving

Hoe kunnen wij uw bedrijf helpen om aan NIS2 te voldoen?

Bij BSI hebben we een team van ervaren experts die u kunnen ondersteunen bij het voldoen aan alle beveiligingseisen die nodig zijn om te voldoen aan de NIS2-richtlijn. Met onze hulp kunnen organisaties mogelijke boetes vermijden en het vertrouwen van klanten vergroten. Van het identificeren van OES tot zelfevaluatie, risicobeoordeling en risicobeheer, onze ervaring in het werken met organisaties in alle sectoren kan u helpen om te voldoen aan de NIS2-richtlijn.



BSI biedt momenteel de volgende diensten met betrekking tot de NIS2-vereisten:

- Cyberstrategie/governance
- Beoordelingen van cybersecurityhouding/maturiteit tegen branche-standaard kaders
- Ontwikkeling van informatiebeveiligings-/cyberstrategie, presentaties voor het bestuur
- Gap-analyse en implementatieondersteuning (ISO 27001, SOC 2, NIST CSF/800-53)
- Bewustwordingstrainingen voor informatiebeveiliging en cyberveiligheid
- Bedrijfscontinuïteit (ISO 22301)

Crisisbeheer en reactie op incidenten

- Bedrijfscontinuïteit (ISO 22301)
  - Bedrijfsimpactanalyse (BIA)/Beleidsontwikkeling/Bedrijfscontinuïteitsplanning
- Disaster Recovery-ondersteuning, implementatie en periodieke tests
- Threat Led Penetration Testing (TLPT)
- Open Source Intelligence (OSINT)
- Fysieke beveiligingsbeoordelingen en aanval simulatie (Red/Blue/Purple Team)
- Planning en implementatie van Incident Response (ISO 27035)
- Dreigingsmodellering/bedreigingsbeoordelingen

Risicobeheer en rapportage

- Ontwikkeling en implementatie van IT-risicobeheerkader (ISO 27005)
  - Risicobeheer van derde partijen (ISO 27036-2)
  - Beoordeling van de huidige stand van zaken van het levenscyclusbeheer van derde partijen
  - Ontwikkeling van een end-to-end leveranciersbeheerkader
  - Implementatie van het risicobeheerkader voor derde partijen in combinatie met lopende ondersteuning voor risicobeheer
- BSI werkt samen met technologiepartners die tools hebben om het volledige levenscyclusbeheer van leveranciers te vergemakkelijken
  - Certificering Threat Intelligence/Computer Emergency Response Team (CERT)
  - Beoordelen van de huidige positie en bepalen van de toekomstige staat
  - Opzetten van een rapportagekader

Waarom zijn ISO 27001 en ISO 22301 essentieel voor NIS2-naleving?

De NIS-regelgeving adviseert bedrijven om prioriteit te geven aan "naleving van internationale normen" bij hun inspanningen voor naleving . Bovendien worden de technische richtlijnen van het Europees Agentschap voor Cyberbeveiliging (ENISA) gekoppeld aan best practice-normen, zoals ISO 27001.

Van alle diensten die BSI aan uw bedrijf kan leveren met betrekking tot NIS2, zijn er twee van belang: ISO 27001 en ISO 22301.

- Het implementeren van een Information Management System (ISMS) dat voldoet aan ISO 27001 stelt organisaties in staat om risico's en blootstelling aan beveiligingsdreigingen te minimaliseren. Dit omvat het identificeren van benodigde beleidslijnen, het inzetten van geschikte technologieën en het trainen van personeel om fouten te voorkomen. ISO 27001 vereist ook jaarlijkse risicobeoordelingen, waardoor organisaties proactief kunnen reageren op veranderende risico's.

- Deze certificering dient als bewijs voor leveranciers, stakeholders en regelgevende instanties dat de juiste technische en organisatorische maatregelen zijn genomen. Dit levert uw organisatie ook concurrentievoordeel op de markt.

- Voor organisaties die hun aapak willen verbeteren, wordt het toevoegen van ISO 22301 voor bedrijfscontinuïteitsmanagement aanbevolen. ISO 22301 helpt bij het implementeren, onderhouden en voortdurende verbetering van bedrijfscontinuïteitspraktijken. Hoewel ISO 27001 aspecten van het bedrijfscontinuïteitsmanagement (BCM) omvat, biedt ISO 22301 een duidelijk omschreven proces voor de implementatie van BCM. Certificering volgens ISO 22301 versterkt verder de naleving van NIS2.

De synergie tussen ISO 27001 en ISO 22301 stelt organisaties in staat om een geïntegreerd managementsysteem te ontwikkelen dat zowel een ISMS als een BCMS omvat. Deze holistische benadering helpt niet alleen bij de naleving, maar bevordert ook de ontwikkeling van weerbaarheid binnen cyberbeveiliging.

Waarom BSI kiezen?

Wij zijn experts op het gebied van cyberbeveiliging, risicobeheer en het beschermen van informatie. En we begrijpen goed hoe deze aspecten van invloed zijn op verschillende sectoren over de hele wereld.

Wat zijn uw volgende stappen?

- Controleer of de regelgeving van toepassing is op uw bedrijf
- Informeer het management of de raad van bestuur over de nieuwe regelgeving
- Neem contact met ons op voor hulp bij het voldoen aan de NIS2-richtlijnen via **info.nl@bsigroup.com**