De NIS2 komt eraan

Heeft deze nieuwe Europese richtlijn impact op jouw bedrijf?

- ICT beheer
- Cloud
- Security
- Hardware
- Telefonie

acf bentveld

ICT VOOR NU EN STRAKS

Wat is de NIS2?

De NIS2 is een Europese richtlijn die gericht is op het waarborgen van de veiligheid van netwerken en informatie, dus de veiligheid van ICT-netwerken en -omgevingen binnen bedrijven. Het is bedoeld om de cyberveiligheid binnen de Europese Unie te versterken en is van toepassing op verschillende branches.

Na de AVG (of GDPR), die met name gericht was op het waarborgen van de privacy en bescherming van de persoonsgegevens, dus weer een Europese richtlijn zich richt op de ICT, en dan met name de ICT-beveiliging van bedrijven.

Is zo'n wetgeving dan echt nodig?

Daarover kunnen we eigenlijk heel kort zijn. Wanneer alle bedrijven en organisaties in Europa hun ICT-beveiliging 100% op orde hadden en deze ook regelmatig verbeteren en aanpassen aan nieuwe bedreigingen dan was een dergelijke richtlijn niet nodig geweest. Dus juist omdat bij veel bedrijven en organisaties ICT-beveiliging onvoldoende prioriteit heeft is besloten hier een richtlijn voor samen te stellen die voor de gehele Europese Unie gaat gelden. Eind 2022 is deze wetgeving aangenomen en de lidstaten hebben tot **17 oktober 2024** de tijd om deze om te zetten in nationaal recht.

De NIS2 - voor wie geldt die nou?

De NIS2 is van toepassing op alle middelgrote en grotere ondernemingen uit de sectoren zoals die in de bijlagen I en II van de NIS2-richtlijn zijn opgenomen.

Zeer kritiek

Energie, vervoer, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, beheer van ICT-diensten (Business to Business), overheid en ruimtevaart. (bijlage I)

Kritiek

Post- en koeriersdiensten, afvalstoffenbeheer, chemische sector, levensmiddelensector, maaksector (specifieke takken daarbinnen), digitale aanbieders (zoals marktplaatsen), onderzoek. (bijlage II)

In bovenstaande verdeling zijn de termen Zeer kritiek en kritiek opgenomen waartussen, in het kader van de NIS2, onderscheid is gemaakt. Voor beide gaan dezelfde eisen voor cybersecurity en rapportage gelden maar de toezichts- en sanctieregelingen zullen verschillen. Voor de zeer kritieke sectoren geldt er een zwaarder toezichtsregime dan voor de kritieke sectoren.

Onderscheid in grootte van bedrijf

Om het allemaal nog wat makkelijker te maken (of toch eigenlijk niet) is er niet alleen een onderscheid in sectoren gemaakt maar richt de NIS2 zich vervolgens ook nog op organisaties die als groot of middelgroot worden aangeduid. **Bedrijven en organisaties met meer dan 50 medewerkers en een omzet hoger dan 10 miljoen euro per jaar en die worden aangeduid als zeer kritiek of kritiek vallen onder de NIS2.**

Op de volgende pagina is een schema terug te vinden waarmee kan worden bepaald of jouw bedrijf in het kader van de NIS2 een Essentieel of Belangrijk bedrijf is.

Hoe bepaal je nou wat voor jouw bedrijf gaat gelden?

Om te bepalen of voor jouw bedrijf / organisatie de NIS2 gaat gelden en of je dan onder kritiek of zeer kritiek valt doorloop je twee stappen die we onderstaand hebben uitgewerkt.

Allereerst doorlopen we onderstaande tabel. Valt jouw bedrijf / organisatie onder één van de genoemde sectoren dan is kritiek of zeer kritiek van toepassing.

Kritiek	Zeer kritiek
Afvalstoffenbeheer	Vervoer
Post- en koeriersdiensten	Banken
Digitale aanbieders	Gezondheidszorg
Productie, verwerken en distributie van levensmiddelen	Energie
Productie en distributie van chemische stoffen	Drink- en afvalwater
Onderzoek	Digitale infrastructuur
Vervaardiging	Beheer van ICT-diensten
	Overheid
	Financiële markt
	Ruimtevaart

Valt jouw bedrijf / organisatie in één van de genoemde sectoren en heb je bepaald of dit kritiek of zeer kritiek is. Dan doorloop je onderstaand schema om uiteindelijk te bepalen of je voor de NIS2 onder Essentieel of Belangrijk valt.

Zorg- en meldplicht

Voor zowel Belangrijke als Essentiele bedrijven gaat er een zorg- en meldplicht gelden. Daarnaast zullen beide groepen bedrijven maatregelen moeten nemen om beveiligingsrisico's beter te beheren en zichzelf hier beter tegen te beschermen.

Bedrijven die als belangrijk worden geclassificeerd zullen onder reactieve monitoring worden geplaatst terwijl Essentiele bedrijven proactief worden gemonitord. In de praktijk betekent dit dat belangrijke bedrijven pas zullen worden gecontroleerd nadat er een incident heeft plaatsgevonden. Essentiele bedrijven zullen proactief worden gecontroleerd of zij voldoende maatregelen hebben genomen om hun digitale infrastructuur voldoende te beschermen.

Informatiebeveiliging is net puzzelen De NIS2 vormt de basis om deze puzzel te kunnen leggen

Welke maatregelen moet je nemen?

De AVG kende nogal wat 'open' normen waaraan voldaan moest worden – het waren technische en organisatorische maatregelen en daar hield de omschrijving eigenlijk wel op. Voor veel organisaties was het dan ook totaal niet duidelijk wat er wel of niet moest gebeuren.

Ook in de NIS2 wordt er gesproken over passende en evenredige technische, operationele en organisatorische maatregelen. Dat klinkt net zo vaag als in de AVG werd omschreven maar gelukkig is er in de NIS2 een artikel opgenomen (artikel 21 lid 2) waarin maatregelen worden besproken waaraan minimaal zal moeten worden voldaan.

In het kort zijn dit de maatregelen waarover wordt gesproken:

- Beleid inzake risicoanalyse en de beveiliging van de informatiesystemen
- Back-up beheer en noodvoorzieningsplannen (zoals een incidentresponse plan en een recovery plan)
- De beveiliging van de toeleveringsketen (hierover later meer!)
- Basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging. Je dient dus de beveiliging van je ICT-omgeving goed voor elkaar te hebben en dient ook het team regelmatig training te geven over cybersecurity

Basismaatregelen

Wanneer we specifiek naar de basismaatregelen kijken hebben we het eigenlijk over ICT-maatregelen die ieder bedrijf al voor elkaar zou moeten hebben.
Voor de volledigheid zijn deze maatregelen, ook beschreven door het NCSC, hieronder nog eens genoemd.

	Zorg ervoor dat elke applicatie en elk systeem voldoende loginformatie genereert
	Pas multifactorauthenticatie toe waar nodig (of eigenlijk, waar mogelijk)
	Bepaal wie er toegang heeft tot (welke) data en (welke) diensten
	Segmenteer netwerken
	Versleutel opslagmedia met gevoelige (bedrijfs)informatie
	Controleer welke apparaten en diensten bereikbaar zijn vanaf het internet en bescherm deze
	Maak regelmatig back-ups van systemen en data en **test deze**
	Installeer software updates

Toeleveringsketen?

NIS2 richt zich op de gehele toeleveringsketen. Ook organisaties die zelf niet zijn te typeren als essentieel of belangrijk, maar wel zaken doen met dergelijke partijen, krijgen met de nieuwe richtlijn te maken. Ook kleine toeleveranciers in de MKB kunnen hierdoor te maken krijgen met de verplichtingen van de NIS2-richtlijn.

Rapportageverplichtingen van incidenten

De NIS2-richtlijn brengt rapportageverplichtingen met zich mee. Zo dient een incident binnen 24 uur te worden gemeld bij de toepasselijke autoriteiten (welke autoriteiten dat zijn is nog niet bekend), indien het incident de beschikbaarheid van de door haar aangeboden diensten heeft verstoord, en in elk geval binnen 72 uur in de andere genoemde gevallen in art. 24 van de richtlijn. Van alle incidenten zal er binnen een maand na de eerste melding een eindverslag ingediend moeten worden.

Toezicht, handhaving en audits binnen NIS2

NIS2 wordt gehandhaafd op proactief beleid waarbij controles steekproefsgewijs kunnen worden uitgevoerd en niet per se als reactie op een incident. Hierbij is er onderscheid gemaakt tussen essentiële- en belangrijke organisaties. Hierbij vallen de volgende twee verschillen op:
Essentiële organisaties zijn onderworpen aan inspecties ter plaatse en elders. Op verzoek moeten deze organisaties iedere vorm van informatie die nodig is om deze toezichttaken uit te voeren, aan de audit instantie overhandigen.
De belangrijke organisaties worden alleen aan dergelijke audits onderworpen wanneer er bewijzen of aanwijzingen zijn dat zij zich niet houden aan de voor hen vastgestelde NIS2-verplichtingen. In tegenstelling tot essentiële organisaties zijn belangrijke organisaties niet verplicht toegang te verlenen tot informatie voor controle doeleinden.

Kortom: Essentiële kunnen altijd worden gecontroleerd en dienen dan ook mee te werken aan audits en belangrijke organisaties gaan pas worden gecontroleerd als er iets mis is.

NIS2 tijdlijn

Het bedenken en uitwerken van Europese richtlijnen duurt vaak enkele jaren. Vervolgens zal de richtlijn nog voor iedere lidstaat moeten worden opgenomen in lokale wetgeving. Onderstaand hebben we de te verwachten globale tijdlijn van de NIS2 uitgewerkt.

2022

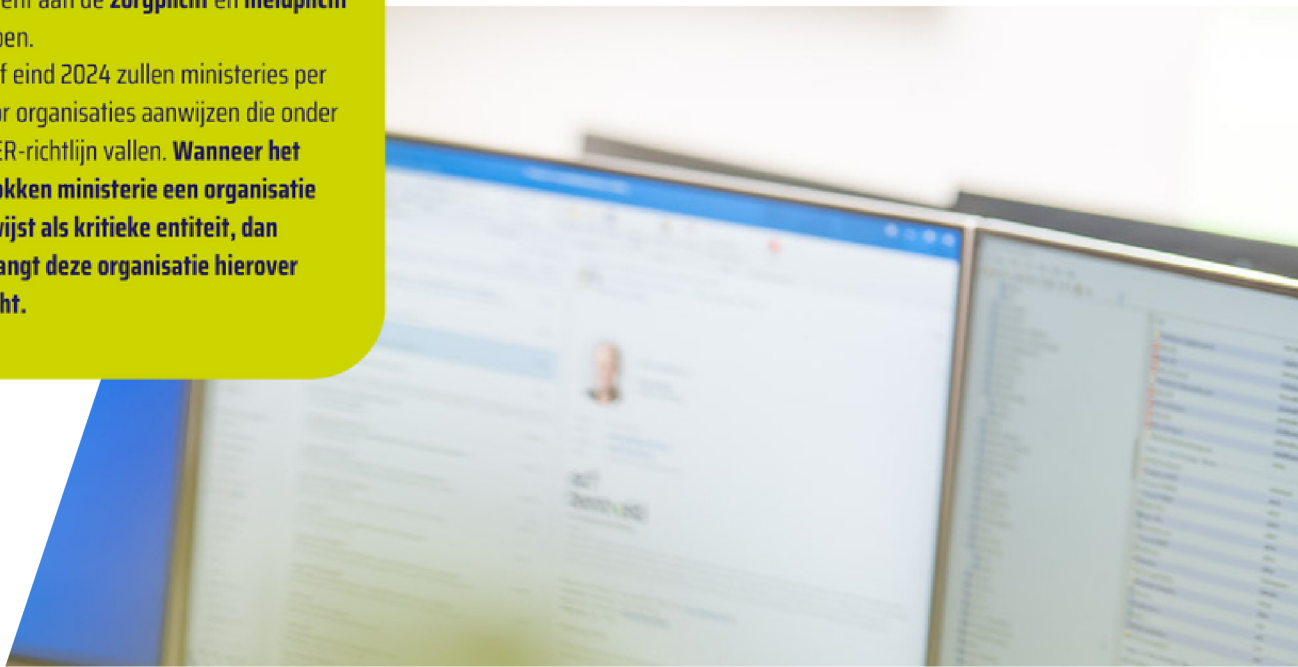
- Op **28 november 2022** is de NIS2-richtlijn vastgesteld door de Europese Raad. Op 9 december 2022 is de CER-richtlijn vastgesteld.
- Op **27 december 2022** zijn de NIS2- en CER-richtlijn gepubliceerd in de Official Journal van de Europese Unie.

2023

- In **januari 2023** is de implementatietermijn van **21 maanden** gestart, waarin de richtlijnen moeten worden opgenomen in nationale wetgeving.
- **Najaar 2023** start consultatieperiode. Gedurende 6 weken kunnen burgers en bedrijven nog verbetering/aanpassingen aanbrengen.

2024

- Naar verwachting zullen de wetten eind 2024 (Oktober) in werking treden, nadat deze door het parlement zijn behandeld. De organisaties die onder de NIS2-richtlijn vallen moeten vanaf dat moment aan de **zorgplicht** en **meldplicht** voldoen.
- Vanaf eind 2024 zullen ministeries per sector organisaties aanwijzen die onder de CER-richtlijn vallen. **Wanneer het betrokken ministerie een organisatie aanwijst als kritieke entiteit, dan ontvangt deze organisatie hierover bericht.**



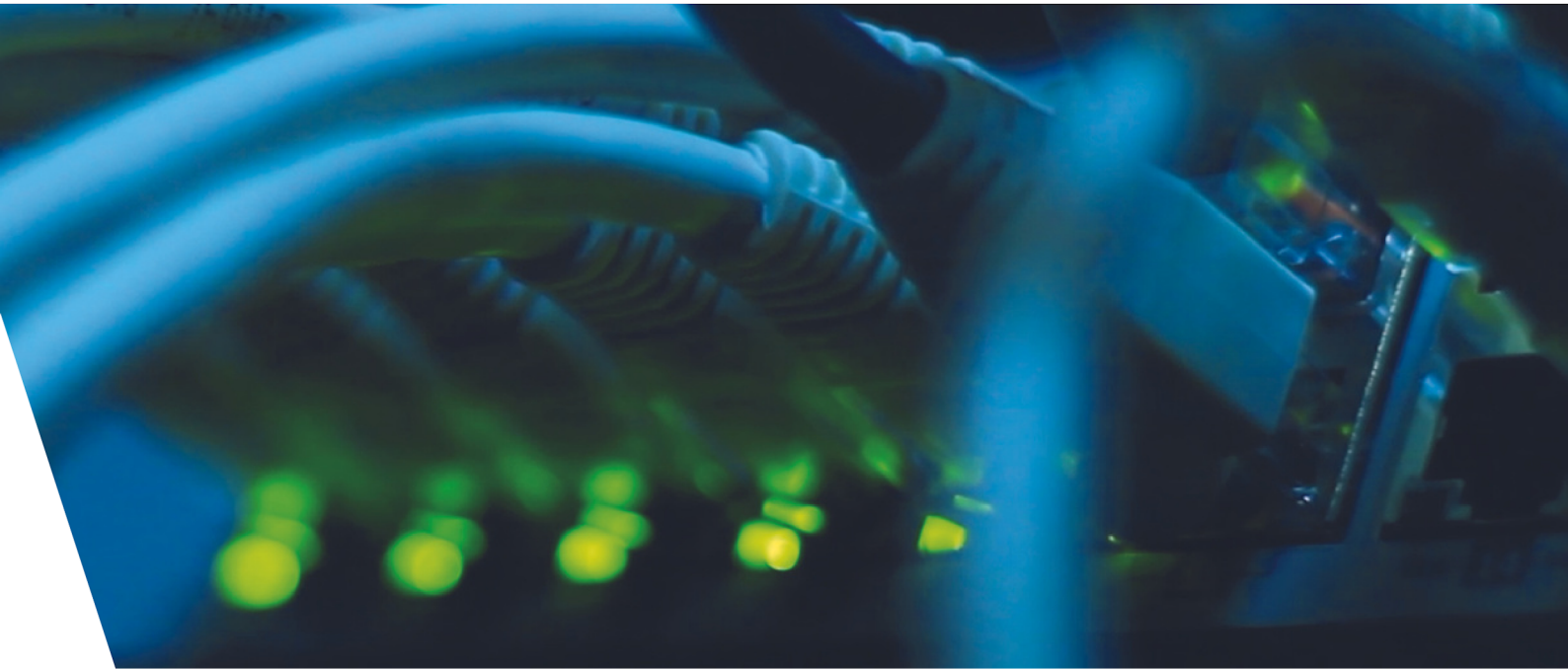
Boetes

Net als bij de AVG kunnen er bij de NIS2 boetes opgelegd worden indien niet aan de eisen en voorwaarden wordt voldaan. Er wordt hierbij gesproken over een percentage van de omzet of 7 miljoen (voor Belangrijke organisaties) of 10 miljoen (voor Essentiele organisaties) euro boete.
Daarnaast is er een bepaling opgenomen dat een bestuurder van een organisatie wettelijk bevoegd dient te zijn om security-maatregelen te nemen en dat deze bestuurder(s) aansprakelijk kunnen worden gesteld wanneer zij de NIS2 niet naleven.

Mijn bedrijf valt niet onder de Essentiele of Belangrijke sectoren. Dus ik hoef nu niets te doen?

Qua richtlijn hoef je in dit geval inderdaad niet te voldoen. Je kunt als bedrijf echter wel onderdeel zijn van een keten waardoor je wel zult moeten voldoen aan deze nieuwe richtlijn. Zie hiervoor ook het stukje over de Toeleveringsketen.

Natuurlijk heb je als ondernemer ook nog gewoon een verantwoordelijkheid naar je klanten, personeel en jezelf. Heb jij je ICT-beveiliging niet op orde dan kan dit zorgen voor langdurige uitval van je bedrijf of zelfs een faillissement. Door vaak eenvoudige stappen te nemen kun je je prima tegen cyberaanvallen beschermen.



Niets doen is geen optie! Ga met de cyberweerbaarheid van de je bedrijf en medewerkers aan de slag. Zorg ervoor dat je beveiliging op orde is en dat deze ook met regelmaat wordt nagelopen. Maak back-ups en informeer je medewerkers over cybersecurity en hoe zij dit kunnen herkennen.

Je hoeft uiteraard niet tot Oktober 2024 te wachten om te investeren in cyberbeveiliging. Cyberbeveiliging is niet iets dat je doet om aan een standaard te voldoen. Het is een essentieel onderdeel van de bescherming van je onderneming.

Conclusie

De NIS2 gaat er komen en uiteindelijk is wetgeving over dit onderwerp ook echt wel nodig. Er is in het bedrijfsleven helaas nog onvoldoende aandacht voor cybersecurity.

Het is wel helder dat de basismaatregelen beschreven in dit document en uitgegeven door het NCSC een hele grote stap in de goede richting zijn. Dus ga aan de slag!

Uiteraard kunnen wij je ondersteunen met die basismaatregelen en adviezen geven over meer geavanceerde maatregelen. Wil je hier hulp bij? Neem dan contact met ons op via 0527-858585 of info@acfbentveld.nl

Hulp nodig of heb je vragen?

Bel ons op 0527-858585, kom bij ons langs op Ecopark 63 in Emmeloord of stuur een e-mail naar info@acfbentveld.nl

Colofon

Dit is een uitgave van ACF Bentveld. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. ACF Bentveld kan daarvoor niet aansprakelijk worden gesteld. © ACF Bentveld. Niets uit deze uitgave mag worden hergebruikt zonder schriftelijke toestemming vooraf van ACF Bentveld.