The Trusted Third Party

Cyberbeveiligingswet (NIS2)

Op 17 oktober 2024 trad de NIS2-richtlijn in werking. Deze richtlijn verplicht Europese bedrijven in maatschappelijk kritieke en belangrijke sectoren om de weerbaarheid tegen cyberdreigingen te verhogen en de nodige cybersecurity maatregelen te treffen. Nederland moet deze richtlijn nog volledig omzetten in de nationale Cyberwet, die naar verwachting in het derde kwartaal van 2025 volledig van kracht wordt.

Cyberdreigingen nemen in frequentie en complexiteit toe, en daarmee de noodzaak voor robuuste cyberveiligheid. De NIS2-richtlijn is ontwikkeld om de weerbaarheid van kritieke sectoren in Europa te versterken. Wanneer een nieuwe regelgeving wordt geïntroduceerd, kan het een uitdaging zijn om deze te leren, te ontleden en te implementeren vóór de startdatum.

Werkt u in de IT-sector binnen de Europese Unie (EU)? Dan weet u waarschijnlijk al dat het ontrafelen van de details van de Network and Information Security Directive 2 (NIS2) op uw pad ligt.

We vonden het nuttig om u kort in te leiden in NIS2, zodat u uw implementatieproces kunt beginnen en een voorsprong behoudt op de regelgeving en op cyberaanvallers.

Inhoudsopgave

Wat is NIS2?

De NIS2-richtlijn is ontworpen om de cyberveiligheid te verbeteren in de EU-lidstaten en bij alle bedrijven die met hen zaken doen. Dit initiatief is een reactie op de groeiende risico's van digitalisering en het toenemende aantal cyberaanvallen en datalekken.

NIS2 breidt de oorspronkelijke NIS-richtlijn uit door meer sectoren en typen organisaties onder de regelgeving te brengen, inclusief die met een 'essentiële' en 'belangrijke' functie in de EU-markt. Het stelt strengere eisen, zoals uitgebreide incidentrapportage, risicobeheerprocedures, verantwoordelijkheids-maatregelen voor het management en strategieën voor continuïteit van de bedrijfsvoering. De NIS2-richtlijn legt niet alleen verplichtingen op, maar vereist dat organisaties aantoonbaar in control zijn over hun cybersecurity. Dit betekent dat zij niet alleen de juiste maatregelen moeten treffen, maar ook het beheer ervan op strategisch niveau moeten verankeren.

Wat houdt ‘in control’ zijn in?

In control zijn betekent dat organisaties volledige grip hebben op hun beveiligingsrisico's, zodat ze snel en effectief kunnen reageren op dreigingen en kwetsbaarheden. Dit gaat verder dan het implementeren van enkele technische oplossingen; het vraagt om een doorlopende risico-inventarisatie en -evaluatie (RI&E) en een sterk risicomanagementproces. Een strategische, integrale aanpak is hierbij essentieel: organisaties moeten precies weten waar hun kwetsbaarheden liggen en hoe ze deze kunnen beperken of wegnemen. In dit proces spelen security officers en chief information security officers (CISO’s) een cruciale rol door toezicht te houden op de juiste uitvoering en voortdurende evaluatie van de maatregelen.

CISO versus SO

Een belangrijk verschil tussen een CISO (Chief Information Security Officer) en een (information) security officer is hun rol en focus binnen de organisatie. Een CISO is meestal een strategische functie, gericht op het ontwikkelen en implementeren van het cybersecuritybeleid op hoog niveau. De CISO werkt aan de lange termijn visie en zorgt dat de organisatie brede cyber-securitystrategie aansluit bij de bedrijfsdoelen. De security officer, daarentegen, is meer operationeel gericht. Deze rol draait om de uitvoering en handhaving van de dagelijkse beveiligings-maatregelen, zoals het monitoren van systemen, het uitvoeren van risicoanalyses en het aanpakken van incidenten. Voor het werk dat moet worden gedaan om NIS2-compliant te worden, zijn vooral doeners nodig - mensen die zich praktisch bezighouden met implementatie en directe actie ondernemen. Security officers vervullen deze cruciale hands-on rol en vormen daarmee de kern van de operationele weerbaarheid die NIS2-vraagt, terwijl een CISO meer een overkoepelende ondersteunende rol speelt.

Risico's van niet-naleving

De NIS2-richtlijn introduceert forse boetes voor het niet naleven van de regels, evenals de mogelijkheid tot juridische procedures tegen organisaties en hun bestuurders. Hoewel de implementatie per lidstaat enigszins kan verschillen, is het cruciaal om goed voorbereid te zijn op de deadline voor nationale invoering. Voor Nederland wordt verwacht dat dit in het derde kwartaal van 2025 zal zijn.

Het is essentieel om de richtlijn actief te bestuderen, de impact op uw organisatie te evalueren en een strategie op te stellen om aan de vereisten te voldoen. U vraagt zich wellicht af: 'Wat betekent dit voor mij?' Maar het belangrijkste is eerst te bepalen of NIS2 van toepassing is op uw organisatie.

Heeft u hulp nog met bepalen of uw organisatie aan de nieuwe cyberbeveiligingswet (NIS2) moet voldoen? Stuur dan een e-mail met uw hulpvraag naar info@tt3p.nl

Verantwoordelijkheid voor cybersecurity in de keten: Verplichtingen voor NIS2-organisaties en hun leveranciers

Onder de NIS2-richtlijn rust er een duidelijke verantwoordelijkheid op 'essentiële' en 'belangrijke' organisaties om de cybersecurity binnen hun gehele toeleveringsketen te waarborgen. Dit betekent dat niet alleen de organisatie zelf, maar ook ketenpartners, zoals uitzendbureaus, verpakkingsbedrijven en andere leveranciers, compliant moeten werken volgens de vereisten van NIS2. In sommige gevallen moeten deze leveranciers zelf ook aan NIS2 voldoen, afhankelijk van hun impact op de continuïteit en veiligheid van de sector. De opdrachtgever heeft daarnaast de verantwoordelijkheid om risico's bij deze ketenpartners te identificeren en maatregelen te implementeren om deze risico's te beheersen. Dit kan inhouden dat contractuele eisen worden gesteld aan ketenpartners op het gebied van cybersecurity, of dat regelmatig audits en risico-assessments worden uitgevoerd om naleving te controleren. Zo zorgt de opdrachtgever ervoor dat zowel de organisatie als de toeleveringsketen voldoet aan de gestelde beveiligingsnormen, wat bijdraagt aan de algehele cyberweerbaarheid en continuïteit van de diensten binnen de sector.

Is mijn organisatie essentieel of belangrijk?

NIS2 deelt organisaties op basis van hun sector en impact in twee categorieën: ‘essentiële’ en ‘belangrijke’ entiteiten. Beide groepen vallen onder de NIS2-verplichtingen, maar de nalevingseisen en de bijbehorende risico’s verschillen per type entiteit:

Essentiële entiteiten

NIS2 wijst sectoren zoals transport, financiële diensten, gezondheidszorg en nutsbedrijven (inclusief energieleveranciers) aan als 'essentiële entiteiten' vanwege hun cruciale rol voor de samenleving en de economie. Dit verhoogt hun nalevingsverplichtingen, waaronder het verplicht melden van incidenten binnen 24 uur — een aanzienlijke verscherping ten opzichte van de eerdere richtlijn. Daarnaast introduceert NIS2 strenge boetes en zware consequenties bij niet-naleving, wat de verhoogde inzet en strengere regelgeving voor deze entiteiten benadrukt.

Een organisatie wordt als 'essentieel' aangemerkt als deze meer dan 250 werknemers heeft of een jaarlijkse omzet van € 50 miljoen of meer behaalt en behoort tot een van de volgende sectoren.

- Energie
- Transport
- Infrastructuur financiële markt
- Gezondheidszorg
- Watervoorziening (drinkwater & afvalwater)
- Digitale infrastructuur
- Overheidsdiensten
- Ruimtevaart
- Beheerders van ICT-diensten
- Bankwezen

Belangrijke entiteiten

NIS2 voegt een nieuwe groep toe voor 'belangrijke' entiteiten, waardoor de richtlijn wordt uitgebreid naar sectoren zoals postdiensten, afvalstoffenbeheer, de maakindustrie en voor het eerst de levensmiddelensector. Dit betekent dat deze sectoren hun cyberbeveiliging snel moeten herzien en verbeteren om te voldoen aan de eisen van NIS2. Hoewel de verplichtingen en boetes voor 'belangrijke' entiteiten minder streng zijn dan voor 'essentiële' entiteiten, blijft de uitdaging om binnen een korte tijd aan de eisen te voldoen aanzienlijk.

Uw organisatie wordt als 'belangrijk' beschouwd als deze meer dan 50 werknemers heeft of een jaarlijkse omzet van € 10 miljoen behaalt, en valt binnen een van deze categorieën (inclusief de categorieën die als essentieel worden aangemerkt):

- Digitale aanbieders
- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Levensmiddelen
- Chemische industrie
- Maakindustrie
- Onderzoek

De 10 essentiële cybersecurity risicobeheersmaatregelen

Een belangrijk onderdeel van de richtlijn is Artikel 21, waarin tien maatregelen voor het beheer van cyberrisico's worden uiteengezet. Lidstaten moeten erop toezien dat zowel 'essentiële' als 'belangrijke' entiteiten passende technische, operationele en organisatorische maatregelen treffen om risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. Deze maatregelen moeten incidenten voorkomen of de impact ervan op de ontvangers van diensten beperken. Hierbij dient rekening te worden gehouden met de nieuwste technologieën, relevante standaarden en kosten, en het beveiligingsniveau moet in verhouding staan tot het risico. Bij de beoordeling van de geschiktheid van de maatregelen moeten organisaties hun risicoblootstelling, grootte en de mogelijke gevolgen van incidenten overwegen, inclusief de ernst en kans op voorvallen en hun maatschappelijke en economische impact.

De NIS2-richtlijn introduceert tien essentiële maatregelen die organisaties moeten implementeren om hun cybersecurity op orde te brengen en te voldoen aan de vereisten. Deze maatregelen richten zich op het versterken van risicoanalyse, operationele continuïteit, ketenveiligheid en personeelsbeheer.

---

1. Beleid voor risicoanalyse en beveiliging van informatiesystemen
Ontwikkel een robuust beleid voor het identificeren en analyseren van potentiële risico's binnen informatiesystemen om tijdig kwetsbaarheden en dreigingen te herkennen.

2. Incidentrespons en beheer
Stel procedures op voor het effectief en snel reageren op beveiligingsincidenten om de impact ervan te beperken en toekomstige voorvallen te voorkomen.

3. Processen voor bedrijfscontinuïteit
Zorg voor processen zoals back-upbeheer, herstel na calamiteiten en crisisbeheer om de bedrijfsvoering veilig te stellen tijdens en na verstoringen.

4. Beveiliging van de toeleveringsketen
Voer veiligheidsmaatregelen door die de hele toeleveringsketen omvatten, inclusief de beveiliging van relaties met leveranciers en dienstverleners.

5. Beveiliging bij aanschaf, ontwikkeling en onderhoud van netwerken en informatiesystemen
Borg de veiligheid tijdens de volledige levenscyclus van systemen, van aanschaf tot ontwikkeling en onderhoud, inclusief kwetsbaarhedenbeheer en het tijdig melden van beveiligingsproblemen.

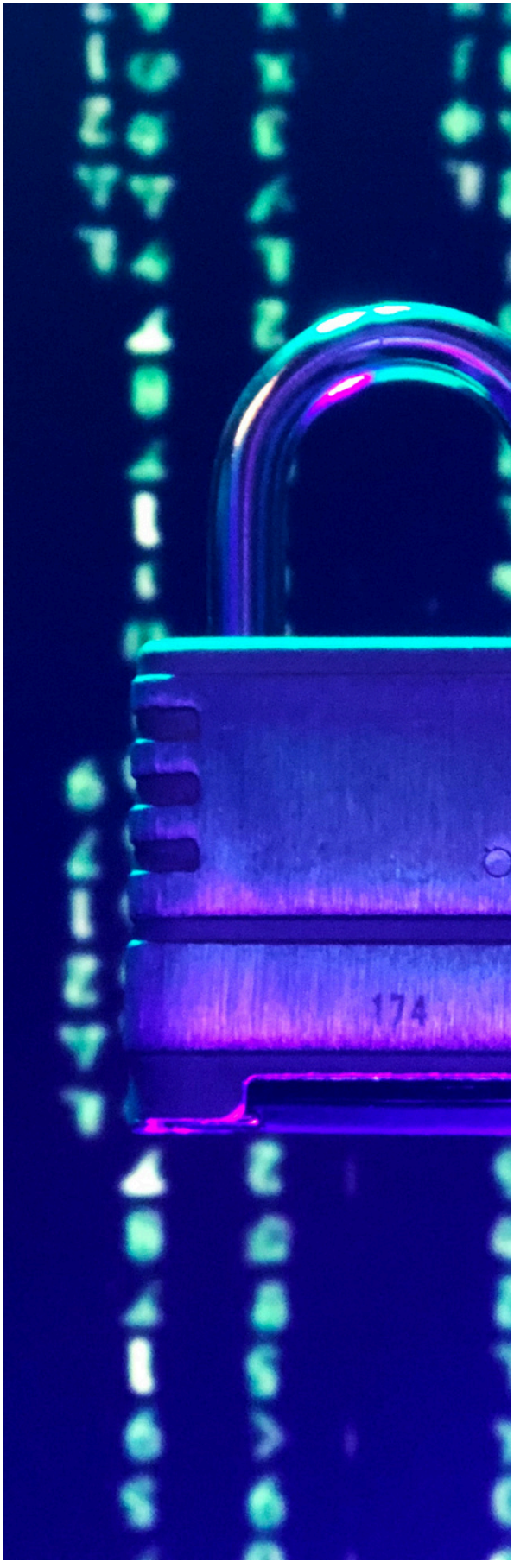
6. Evaluatie van risicobeheermaatregelen
Implementeer beleid en procedures om de effectiviteit van de genomen cyberbeveiligingsmaatregelen regelmatig te beoordelen en aan te passen waar nodig.

7. Basispraktijken voor cyberhygiëne en trainingen
Bevorder goede cyberhygiënische praktijken en zorg voor regelmatige cybersecuritytraining om medewerkers alert en vaardig te houden.

8. Cryptografie en encryptie
Stel beleid en procedures op voor het gebruik van cryptografie en versleuteling waar nodig, om gegevensintegriteit en vertrouwelijkheid te waarborgen.

9. Beveiliging van toegangsbeheer en rollen
Zorg voor een strikt toegangsbeheerbeleid waarbij alleen personen met een legitieme zakelijke noodzaak toegang krijgen tot systemen en gegevens. Dit minimaliseert het risico op ongeautoriseerde toegang en beschermt kritieke gegevens en systemen tegen misbruik.

10. Multifactor-authenticatie en beveiligde communicatiekanalen
Gebruik waar nodig multifactor-authenticatie, beveiligde communicatiekanalen (zoals voor stem, video en tekst) en noodcommunicatiesystemen om de veiligheid van interne en externe communicatie te waarborgen.



Rapportageplicht

Een terugkerend thema in de gehele NIS2-richtlijn is het belang van rapporteren. Zowel ‘essentiële’ als ‘belangrijke’ organisaties hebben een rapportageplicht, maar de eisen verschillen in striktheid en tijdlijnen. Essentiële entiteiten, zoals organisaties in cruciale sectoren (bijvoorbeeld gezondheidszorg en energie), moeten vaak striktere en snellere rapportagetijdlijnen volgen. Zij moeten bijvoorbeeld incidenten binnen 24 uur melden bij het Nationaal Cyber Security Centrum (NCSC). Belangrijke entiteiten hebben ook een verplichting om incidenten te rapporteren, maar de vereisten kunnen iets minder streng zijn afhankelijk van de nationale implementatie en het risiconiveau van de sector.

Bestuurdersaansprakelijkheid

NIS2 benadrukt ook het belang van bedrijfs-verantwoordelijkheid, waarbij wordt vereist dat het management actief betrokken is bij en inzicht heeft in de cybersecurity-inspanningen van het bedrijf. Managers in de organisatie kunnen gestraft worden voor beveiligingsinbreuken en kunnen zelfs aansprakelijkheden in privé en tijdelijke verboden op managementfuncties opgelegd krijgen.

Sancties

De nieuwe regels onder de NIS2-richtlijn zijn veel strenger dan voorheen en introduceren hogere of geheel nieuwe boetes in sommige gevallen. Lidstaten binnen de Unie kunnen echter besluiten nog hogere boetes op te leggen als zij dat willen. Bedrijven die als ‘essentieel’ worden beschouwd, moeten bereid zijn om boetes tot €10 miljoen of 2% van hun wereldwijde jaarlijkse omzet van het voorgaande jaar te betalen, afhankelijk van welk bedrag hoger is. Bedrijven die als ‘belangrijk’ worden beschouwd, kunnen boetes oplopen tot €7 miljoen of 1,4% van hun wereldwijde omzet van het vorige jaar, opnieuw afhankelijk van welk bedrag hoger is.

Waarom ook leveranciers NIS2 serieus moeten nemen

Leveranciers spelen een cruciale rol in de digitale keten en zijn vaak de verbindende schakels tussen NIS2-plichtige organisaties en hun eindgebruikers. Hoewel de directe verplichtingen van de NIS2-richtlijn primair gericht zijn op ‘essentiële’ en ‘belangrijke’ entiteiten, kunnen de risico’s van onvoldoende cyberbeveiliging in de keten ook voor leveranciers verstrekkende gevolgen hebben. Wanneer een leverancier het doelwit wordt van een cyberaanval, kan dit leiden tot verstoringen in de hele toeleveringsketen, met reputatieschade, boetes en verlies van klantenvertrouwen als mogelijke gevolgen.

Dit geldt in het bijzonder voor leveranciers zoals IT-dienstverleners, softwareontwikkelbedrijven, SaaS-platformen, clouddiensten, logistieke partners en zelfs producenten van verpakkings- of productiesystemen. Deze partijen beheren vaak kritieke infrastructuren of hebben toegang tot gevoelige data van NIS2-plichtige organisaties. Door proactief NIS2-principes te omarmen, tonen zij hun inzet voor veiligheid en betrouwbaarheid, wat hen een concurrentievoordeel biedt. Bovendien verkleinen ze de kans dat opdrachtgevers hen uitsluiten vanwege onvoldoende cyberveiligheid. Het naleven van de richtlijn is dus niet alleen een morele plicht, maar ook een strategische investering in de eigen toekomstbestendigheid.

Voordelen van de NIS2-naleving

Hoewel de NIS2-richtlijn organisaties verplicht om te investeren in cybersecuritymaatregelen, biedt naleving ook concrete voordelen die verder reiken dan alleen wetgevingsplicht:

Verhoogde cyberweerbaarheid
Door te voldoen aan de strenge eisen van NIS2, versterken organisaties hun weerbaarheid tegen cyber-dreigingen. Dit verkleint de kans op datalekken en operationele verstoringen, wat zorgt voor meer continuïteit en veiligheid binnen de organisatie.

Vertrouwen van klanten en partners
Organisaties die aantoonbaar voldoen aan de NIS2-normen laten aan klanten en partners zien dat hun gegevens en systemen goed beveiligd zijn. Dit kan een belangrijk concurrentievoordeel opleveren en vertrouwen opbouwen in zakelijke relaties.

Risicovermindering en lagere kosten op de lange termijn
Door proactief risico's te beheren, kunnen organisaties de impact van incidenten en daarmee samenhangende herstelkosten minimaliseren. De kosten van naleving wegen vaak op tegen de potentiële kosten van een groot beveiligingsincident.

Strategische voordelen
NIS2 vereist een integrale aanpak van cybersecurity, wat betekent dat organisaties hun beveiliging op strategisch niveau moeten verankeren. Dit helpt om security structureel te verbeteren, risico's te beheersen en goed voorbereid te zijn op toekomstige bedreigingen en regelgeving.

Door NIS2-naleving niet alleen als verplichting, maar ook als strategische investering te beschouwen, kunnen organisaties hun beveiliging naar een hoger niveau tillen en zich onderscheiden in een steeds competitievere markt.

Er is natuurlijk meer

Bovenstaande secties geven een breed overzicht van de verwachtingen binnen de NIS2-richtlijn; echter, dit is niet allesomvattend. We raden elke organisatie die binnen de Europese Unie opereert aan om de volledige richtlijn en haar vereisten met hun teams door te nemen en volledig te begrijpen wat de verwachtingen en gevolgen zijn van deze ingrijpende wetgeving.

Hoe kunnen wij u helpen?

Voor effectieve naleving van de NIS2-richtlijn moeten organisaties niet alleen inzicht hebben in hun beveiligingsrisico's, maar ook de juiste expertise beschikbaar hebben voor de uitvoering van hun beveiligingsbeleid. Wij bieden twee kernservices die u helpen om controle te krijgen en te behouden over uw cybersecurity: een diepgaande risico-inventarisatie & -evaluatie (RI&E) en de flexibele inzet van een remote security officer.

Cyber risico-inventarisatie & -evaluatie (RI&E)
Een diepgaand inzicht in de cybersecurityrisico's binnen uw organisatie.

Onze RI&E helpt uw organisatie om cybersecurity-risico's effectief in kaart te brengen en de zwakke punten binnen de terreinen van mens, organisatie en techniek te identificeren. We volgen hierbij het ISO 27001/2 raamwerk en voeren een grondige inventarisatie en evaluatie uit. Met een overzichtelijk rapport ontvangt u een helder beeld van de huidige status van uw beveiligingsmaatregelen, inclusief praktische aanbevelingen en een prioriteitenlijst. Dit stelt u in staat om op gestructureerde wijze te werken aan het verkleinen van uw risico's zodat uw organisatie 'in control' raakt van cybersecurity en voldoet aan de NIS2-richtlijn.

Remote Security Officer (RSO)
Flexibele expertise op afroep, ideaal voor organisaties zonder een vaste security officer.

Niet elke organisatie heeft de capaciteit of behoefte om een vaste security officer in dienst te nemen. Onze flexibele remote security officer biedt daarom precies de juiste ondersteuning, voor het aantal uren dat bij uw behoeften past. De RSO fungeert als uw vaste sparringpartner voor alle zaken rondom informatiebeveiliging. Hij ondersteunt bij de planning, implementatie en controle van beveiligings-maatregelen, coördineert bij incidenten en draagt bij aan het vergroten van de security-awareness binnen uw organisatie. U bepaalt zelf de intensiteit en de duur van de inzet, zodat u altijd de benodigde expertise beschikbaar heeft, zonder vast personeel. Met een RSO van TT3P kunt u direct werken aan NIS2-compliance.

Klaar om te beginnen?

Neem contact met ons op via info@tt3p.nl om te ontdekken hoe wij uw organisatie kunnen ondersteunen bij het behalen van de NIS2-vereisten en om een veilige, toekomstbestendige omgeving te creëren.