TENDENZ IT
MAATWERK IN IT&CRM-OPLOSSINGEN

Voor MKB-bedrijven in Noord-Nederland

NIS2 en jouw bedrijf

Wat is het, wat moet je doen en hoe TendenZ IT je daarbij helpt.

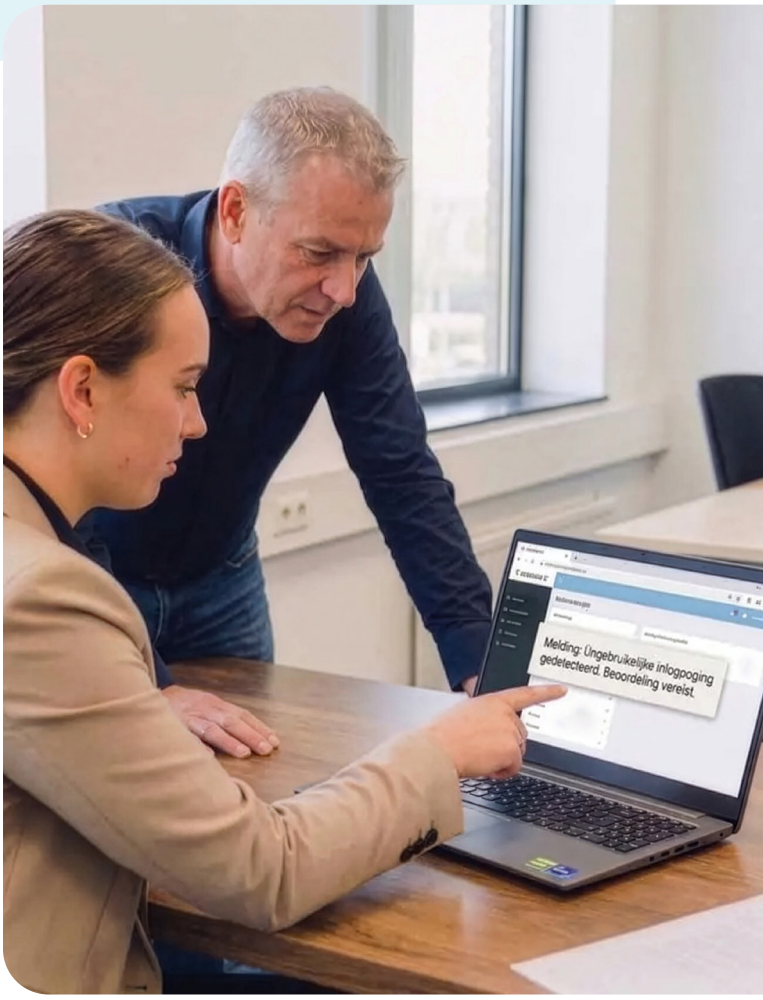
- Weten of jouw bedrijf eronder valt
- Begrijpen wat je moet regelen
- Rust, overzicht en grip

Herken je dit?

NIS2. Je hebt ervan gehoord, maar wat moet jij er precies mee?

Zo gaat het bij de meeste MKB-bedrijven.
En zo kan het anders.

Je krijgt mailtjes over NIS2, je leest iets op LinkedIn, een klant stelt vragen of je accountant noemt het. Maar of het ook echt voor jou geldt, wat je dan precies moet doen en wat het kost, dat blijft vaag. De wet zelf helpt ook niet mee. Termen als 'essentiële entiteiten', 'zorgplicht' en 'Cyberbeveiligingswet' zijn niet bepaald uitnodigend voor een drukke eigenaar of officemanager. Terwijl de deadline nadert: 1 juli 2026.



Klinkt dit bekend?

- Je weet niet zeker of jouw bedrijf onder de NIS2-wet valt
- Je levert aan grote opdrachtgevers die straks om bewijs van veiligheid vragen
- Je weet niet welke maatregelen je moet nemen of waar je moet beginnen
- Je hebt geen tijd of interne kennis om dit zelf goed uit te zoeken
- Je wilt gewoon weten: wat kost het, wat levert het op en wie helpt mij?

De kern van het probleem:
NIS2 raakt je ook als je er niet direct onder valt. Grote klanten zijn namelijk verplicht hun leveranciers te controleren op digitale veiligheid. Zonder aantoonbare beveiliging verlies je opdrachten, niet omdat je slecht werk levert, maar omdat je het niet kunt aantonen. **TendenZ IT** ziet dit nu al gebeuren bij bedrijven in Noord-Nederland.

Wat is NIS2?

De wet die cybersecurity verplicht maakt

Per 1 juli 2026 van kracht in Nederland onder de naam Cyberbeveiligingswet (Cbw).

NIS2 staat voor Network and Information Security 2. Het is een Europese richtlijn die in Nederland wordt ingevoerd via de Cyber-beveiligingswet. Het doel: bedrijven en organisaties die een belang-rijke maatschappelijke rol spelen, moeten hun digitale beveiliging structureel op orde hebben.

NIS2 is geen vrijblijvend advies. Het is wetgeving, met toezicht, handhaving en boetes. Bovendien is het bestuur van een organisatie persoonlijk aansprakelijk als de beveiliging niet op orde is. als je niet voldoet krijg je geen aansprakelijkheidsverzekering en/of keert hij niet uit Dat maakt het een boardroom-onderwerp, geen IT-feestje.

Val jij eronder?

NIS2 onderscheidt twee soorten organisaties:

Essentieel
Grote organisaties (250+ medewerkers of meer dan 50 mln omzet) in sectoren als energie, water, transport, gezondheids-zorg, banken, overheid en digitale infra-structuur.
Proactief gecontroleerd, elk moment.

Belangrijk
Middelgrote organisaties (50+ mede-werkers of meer dan 10 mln omzet) in dezelfde sectoren, plus maakindustrie, levensmiddelen, post & koeriersdiensten, chemie en onderzoek.
Gecontroleerd bij een incident.

En als je zelf niet NIS2-plichtig bent?

Dan ben je er nog niet. NIS2-plichtige organisaties zijn verplicht hun leveranciers te contro-leren. Als jij levert aan ziekenhuizen, gemeenten, energiebedrijven, transporteurs of grote productiebedrijven, kunnen zij straks eisen dat jij aantoont dat jouw beveiliging in orde is. Naar schatting moeten 50.000 tot 100.000 MKB-bedrijven in Nederland hieraan voldoen, ook zonder zelf direct NIS2-plichtig te zijn.

Wat zijn de boetes?
Essentieel: maximaal € 10 miljoen of 2% van de wereldwijde jaaromzet.
Belangrijk: maximaal € 7 miljoen of 1,4% van de wereldwijde jaaromzet.

Het bestuur is persoonlijk aansprakelijk.

Wat schrijft NIS2 voor?

Wat je minimaal op orde moet hebben

NIS2 schrijft geen specifieke software voor, maar wel concrete aandachtsgebieden.

De wet spreekt van 'passende en evenredige maatregelen'. Dat klinkt vaag, maar NIS2 geeft wel degelijk een concrete lijst van onderwerpen die je minimaal moet hebben geregeld. Hieronder de belangrijkste:

1 | Risicoanalyse en beleid

Breng je digitale risico's in kaart en werk met een actueel beveiligingsbeleid. Wat zijn de dreigingen voor jouw organisatie? Welke impact heeft een incident? Dat moet je kunnen beantwoorden en aantonen.

2 | Beveiliging van systemen en data

Toegangsbeheer, sterke wachtwoorden, multifactorauthenticatie (MFA) en encryptie van gevoelige data. Wie heeft toegang tot welke systemen? Dat moet je weten en kunnen controleren.

3 | Ketenveiligheid

Maak afspraken met je leveranciers over hun beveiliging. Cyberaanvallen lopen steeds vaker via de toeleveringsketen. Ook jouw klanten zijn verplicht dit van jou te vragen.

4 | Cyberhygiëne en awareness training

Medewerkers moeten weten wat de risico's zijn en hoe ze zich veilig gedragen. Reguliere awareness trainingen zijn verplicht, ook voor bestuurders die binnen twee jaar na inwerkingtreding een training moeten hebben gevolgd.

5 | Incidentrespons en continuïteit

Je moet een plan klaar hebben voor als het misgaat: wie doet wat, hoe herstel je en hoe ga je snel weer verder? Back-ups, crisisbeheer en een gedocumenteerd incident-responsplan zijn geen luxe, maar een wettelijke verplichting.

5 | Meldplicht

Bij een ernstig incident ben je verplicht dit te melden: binnen 24 uur als de dienst-verlening is verstoord, anders binnen 72 uur. Na een maand volgt een eindverslag bij de toezichthouder.

Niet een vinkje, maar een proces

NIS2-compliance is geen eenmalige exercitie. De wet vraagt om een structurele, aantoonbare aanpak die meegroeit met jouw organisatie en met de dreigingen die veranderen. Precies daarom helpt TendenZ IT niet alleen bij de start, maar blijft betrokken.

Zo werkt het

De TendenZ IT-aanpak

NIS2 als complete dienst.
Niet alleen advies, we regelen het met je. Van inzicht naar rust. In vier stappen.

TendenZ IT helpt MKB-bedrijven niet alleen begrijpen wat NIS2 inhoudt. We pakken het ook praktisch op: we brengen in kaart waar je staat, richten de beveiliging goed in en zorgen dat je structureel blijft voldoen.

We geloven dat cybersecurity geen technisch feestje is, maar een onderdeel van een gezond bedrijfsproces. Daarom richten we IT niet in vanuit standaarden, maar vanuit hoe mensen bij jou werken. Dat is hoe we rust, overzicht en grip realiseren.

1 | Inzicht in waar je staat

We beginnen met een nulmeting op maat. We brengen in kaart welke risico's er zijn, wat je al goed hebt geregeld en wat er nog ontbreekt. We maken 'impliciete kennis', dat wat alleen in hoofden zit, expliciet en zichtbaar. Zo weet je precies wat je te doen staat en wat het kost.

2 | Proces: maatregelen die bij jou passen

Op basis van de nulmeting implementeren we de juiste maatregelen. Geen overkill, geen generieke checklists. We passen het aan op jouw bedrijf, jouw systemen en jouw sector. Inclusief alle benodigde documentatie en beleidsstukken die je nodig hebt om aantoonbaar compliant te zijn.

3 | Oplossing: alles in orde en aantoonbaar

Op basis van het bezoek stellen we een oplossing voor die past bij de werkwijze. We kiezen de juiste modules, de juiste koppelingen en de juiste inrichting. We passen het systeem aan jouw processen aan.

4 | Rust: structureel compliant blijven

NIS2-compliance is geen eenmalige exercitie. Wij blijven betrokken. We monitoren, updaten en passen aan waar nodig. We komen minimaal vier keer per jaar langs om samen te kijken hoe IT optimaal blijft aansluiten op jouw processen. Zodat je ook volgend jaar nog voldoet en dat kunt aantonen.

Wij zijn geen externe leverancier

We zijn een verlengstuk van je team.
De klant bepaalt de prioriteit.
Wij zorgen dat IT daarop aansluit.
Dat is hoe we werken, bij NIS2 en bij alles wat we voor je doen.

Onze diensten voor NIS2

Wat TendenZ IT voor je regelt.

Een totaaloplossing die MKB-ondernemers ontzorgt bij de overgang naar NIS2.

TendenZ IT is een totaaloplosser. We leveren niet alleen de techniek, maar zorgen dat die aansluit op hoe mensen bij jou werken.
Hieronder de diensten die essentieel zijn voor NIS2-compliance:

Cybersecurity & back-ups

De technische fundering van NIS2. We beschermen systemen en data proactief tegen digitale dreigingen. We kijken verder dan een virus-scanner: betrouwbare back-ups zorgen dat bedrijfsprocessen direct kunnen doorgaan, ook bij een incident. Zodat jij niet stil staat als het misgaat.

IT-beheer & proactieve monitoring

NIS2 verplicht organisaties om hun systemen actief te monitoren. Wij verzorgen dagelijks beheer en signaleren problemen voordat ze impact hebben. Je kunt op ons rekenen voor snelle en effectieve ondersteuning. Rust in de organisatie, omdat professionals de vinger aan de pols houden.

Security awareness trainingen

De meeste cyberaanvallen beginnen bij mensen, niet bij systemen. We trainen je team om digitale risico's, zoals phishing of verdachte links, in de dagelijkse praktijk te herkennen. Praktisch, herkenbaar en afgestemd op hoe jullie werken. Inclusief training voor bestuurders, die NIS2 verplicht stelt.

Maatwerksoftware & koppelingen

Soms voldoet standaardsoftware niet aan je specifieke proces- of veiligheidseisen. Onze development-afdeling bouwt maatwerkoplossingen: portalen, koppelingen en integraties. Zodat informatie niet 'overal en nergens' staat, maar altijd op de juiste plek zit.

Cloudoplossingen & moderne werkplek

De wet eist controle over wie toegang heeft tot welke data. We richten omgevingen zoals Microsoft 365 zo in dat ze veilig, overzichtelijk en praktisch zijn. We kijken ook naar hoe en waar mensen werken: remote werken goed gefaciliteerd, zonder dat het ten koste gaat van de beveiliging.

Aanvullende dienst

Security awareness: jouw medewerkers als sterkste schakel.

Want de meeste cyberincidenten beginnen bij mensen, niet bij systemen.

Phishing, zwakke wachtwoorden, onbedoeld klikken op een verkeerde link. Bijna alle succesvolle cyberaanvallen beginnen bij menselijk gedrag. NIS2 verplicht organisaties dan ook expliciet om medewerkers bewust te maken van digitale risico's.

TendenZ IT biedt een security awareness platform waarmee medewerkers op een praktische en toegankelijke manier leren hoe ze veilig digitaal werken. Niet als eenmalige training, maar als doorlopend programma dat gedrag structureel verbetert.

Wat biedt het platform?

- Korte, praktische e-learningmodules die passen in de werkdag
- Gesimuleerde phishingaanvallen om gedrag te testen en te verbeteren
- Rapportages per afdeling en medewerker
- Certificaten als bewijs van deelname (NIS2-vereiste)
- Module voor bestuurders, verplicht binnen 2 jaar na inwerkingtreding
- Altijd actueel: inhoud wordt bijgewerkt op basis van actuele dreigingen

NIS2 verplicht dit expliciet
Organisaties die onder NIS2 vallen, zijn verplicht medewerkers regelmatig te trainen. Maar ook als je zelf niet direct NIS2-plichtig bent, is dit een slimme investering: een goed getraind team is de beste bescherming tegen cybercrime en een argument richting klanten die vragen stellen over jouw beveiliging.

Zo werkt het

Van eerste gesprek tot aantoonbaar veilig. Wij regelen het met jou.

Geen implementatie op afstand. Geen handleiding die je zelf uitzoekt.

TendenZ IT werkt anders dan de meeste IT-bedrijven. We sturen geen pakket op en verdwijnen. We komen bij je langs. We willen zien hoe jij werkt, wat er speelt en wat een oplossing moet kunnen. Dat is ook waarom onze klanten blijven.

1 | Vrijblijvend kennis-makingsgesprek

Je belt of mailt. We plannen een gesprek in zonder verplichtingen. We luisteren, stellen vragen en kijken of er een match is. Geen verkoop-praatje, gewoon een eerlijk gesprek.

2 | Bezoek op locatie en nulmeting

We bezoeken elke nieuwe klant op locatie. We brengen in kaart hoe je nu werkt, welke systemen je gebruikt en welke risico's er zijn. Op basis daarvan weet je precies wat je te doen staat.

3 | Aanpak op maat

Op basis van de nulmeting stellen we een aanpak voor die past bij jouw bedrijf, jouw sector en jouw tempo. We kiezen de juiste maatregelen en begeleiding.

4 | Implementatie en begeleiding

We richten het in en begeleiden het hele team bij de start. Inclusief documentatie, beleidsstukken en wat er verder nodig is. We zorgen dat iedereen er vanaf dag één mee uit de voeten kan.

5 | Altijd bereikbaar, altijd in ontwikkeling

Na de implementatie verdwijnen we niet. Je kunt ons altijd bellen. We denken mee als iets verandert. En we houden jouw beveiliging up-to-date, ook als de wet of het dreigings-landschap verandert.

Over TendenZ IT

Persoonlijk, betrokken en altijd op locatie.

TendenZ IT is meer dan een IT-bedrijf.
We zijn een partner.

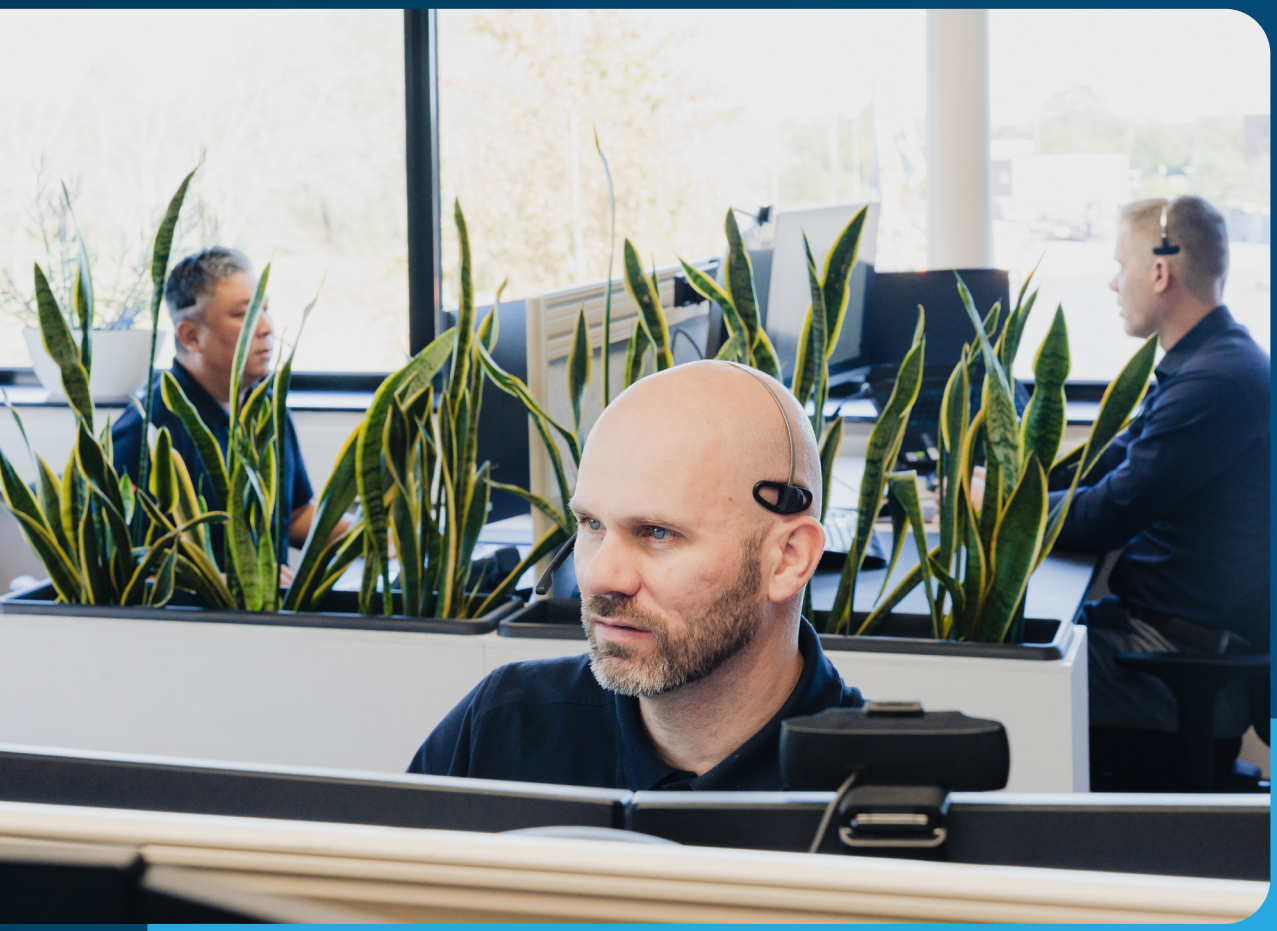
Al meer dan 27 jaar begeleiden wij MKB-bedrijven bij het inrichten van hun IT-omgeving. Vanuit Assen werken we voor klanten in heel Noord-Nederland. We kennen de regio, de branches en de uitdagingen van ondernemers die gewoon willen ondernemen, zonder IT-gedoe.

Onze filosofie is simpel: wij richten IT niet in vanuit techniek of standaarden, maar vanuit hoe mensen werken en hoe bedrijfsprocessen daadwerkelijk verlopen. Pas als we begrijpen hoe jij werkt, bepalen we welke IT daarbij past. Dat geldt ook voor NIS2.

Wat ons anders maakt:

- We komen altijd bij je langs: geen implementatie op afstand, elke nieuwe klant bezoeken we op locatie
- Maatwerk, geen confectie: we passen de oplossing aan jouw processen aan, niet andersom
- De klant heeft de regie: jij bepaalt de prioriteit, jij bepaalt wanneer een ticket is gesloten
- Alles onder één dak: van risicoanalyse tot awareness training tot doorlopend beheer
- Minimaal vier keer per jaar langs: structureel meekijken hoe IT optimaal blijft aansluiten
- Altijd bereikbaar: ook jaren na de implementatie, niet via een anoniem helpdesk callcenter

Klaar om NIS2 geregeld te hebben?



Plan een vrijblijvend kennismakingsgesprek.
We komen graag bij je langs.

tendenzit.nl/nis2

088 002 90 00

info@tendenz.nl

TendenZ IT is gevestigd in Assen en werkt voor klanten in heel Noord-Nederland.

De deadline voor NIS2-compliance is **1 juli 2026**.
Nu beginnen geeft je de tijd om het goed te doen.

TENDENZ IT
MAATWERK IN IT&CRM-OPLOSSINGEN