Q&A NIS2 Cyberbeveiligingswet

Wanneer gaat de NIS2 Cyberbeveiligingswet in?

De NIS2 Cyberbeveiligingswet zal in Nederland naar alle waarschijnlijkheid in werking treden per 1 juli 2026. De reden daarvoor is de Europese verplichting om dit te doen. In de meeste andere Europese landen is de wet al van kracht. In Nederland zal de wet dus hoe dan ook dit jaar ingaan.

Hoe weet ik of ik NIS2-plichtig ben of niet?

Bedrijven en organisaties zijn zelf verantwoordelijk om uit te vinden of ze NIS2-plichtig zijn of niet. Er zijn 19 sectoren benoemd door de overheid die essentieel en/of belangrijk zijn. De supportdesk van Samen Digitaal Veilig helpt kosteloos als je er zelf niet uitkomt. Als je je gegevens invult sturen we een mail met de uitkomst.

SDV Supportdesk: www.samendigitaalveilig.nl/supportdesk

De 19 sectoren zijn:

- Energie
- Vervoer
- Bankwezen
- Infrastructuur voor financiële markten
- Gezondheidszorg
- Drinkwater
- Afvalwater
- Digitale infrastructuur
- ICT-dienstbeheer
- Overheidsdiensten
- Ruimtevaart
- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Chemische stoffen
- Levensmiddelen
- Vervaardiging/ industrie
- Digitale aanbieders
- Onderzoek
- Overige digitale diensten

Op de site van het NSCS staan alle criteria vermeld, zie:
https://www.ncsc.nl/cyberbeveiligingswet-nis2/over-de-cbw.

Hier staat ook de link naar de zelfevaluatietool die bedrijven kunnen invullen:
https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

Kom je er niet uit? Mail de SDV supportdesk je vraag,
https://samendigitaalveilig.nl/supportdesk/

Vallen kleine bedrijven ook onder de NIS2 wet?

Ja, kleine bedrijven kunnen ook te maken krijgen met de NIS2. Dat werkt indirect omdat er in wet verplichting staan voor grotere organisaties die er wel onder vallen.

De meeste MKB-bedrijven krijgen dus indirect via hun klanten met de wet te maken. Als die er direct of indirect eronder vallen, kan het zijn dat jij er ook mee te maken krijgt. Heb je als klein bedrijf bijvoorbeeld een grote klant die aan de NIS2 moet voldoen en ben jij een leveranciers waarin jouw klanten een potentieel risico zit? Dan heeft dit ook gevolgen voor jou.

Hoe kan ik controleren of mijn bedrijf cyberveilig is?

Doe nu de check met: https://samendigitaalveilig.nl/nis2cyberscore.
Invullen duurt 15 minuten en je krijgt direct een gratis rapport met een overzicht van je status en zelfs van wat je nog zou moeten doen

Moeten alle mkb-bedrijven aan de NIS2 voldoen?

Nee, niet alle mkb-bedrijven zijn verplicht om aan de NIS2 wet te voldoen.

Echter, MKB-bedrijven die leverancier zijn van grote ‘NIS2 bedrijven’ of als ze leveren aan een bedrijf dat zelf ook de verplichting hebben wel de verplichting om mee te werken aan de beveiliging van de toeleveringsketen. Veel bedrijven halen daarom een makkelijk te behalen norm. De meest populaire is NIS2-SC10, deze bevat 17 maatregelen waarvan veel bedrijven er al 7-8 in orde hebben. Die norm is voldoende. Je kunt ook kiezen voor zeer zware certificering door ISO27001 te halen. Die heeft 93 te behalen maatregelen.

Meer informatie over de NIS2 certificering staat op
www.samendigitaalveilig.nl/deelnemen
En ook op www.nis2supplychain.eu

Wat staat over het beveiligen van de toeleveringsketen in de wet?

Een belangrijk onderdeel van de NIS2 Cyberbeveiligingswet is het beveiligen van de toeleveringsketen. In de Nederlandse wet teksten Artikel 21 lid 3 onderdeel d Cbw.

(Artikel 21.2D van de Europese NIS2 teksten.) Dit betekent dat je niet alleen je eigen cyberbeveiliging moet versterken, maar als NIS2 entiteit ook verantwoordelijkheid draagt voor de digitale veiligheid binnen je toeleveringsketen. Met andere woorden, NIS2 organisaties zijn ook verantwoordelijk voor de beveiliging van hun klant. Daarom moeten mkb-bedrijven hun NIS2 klanten laten zien dat ze veilig werken. Het beste is via certificering

Veel mkb-bedrijven halen daarom NIS2-SC10 certificering. Deze bevat 17 maatregelen waarvan veel bedrijven er al 7-8 in orde hebben. Die norm is voldoende. Je kunt ook kiezen voor zeer zware certificering door ISO27001 te halen. Die heeft 93 te behalen maatregelen. Meer informatie over de NIS2 certificering staat op
www.samendigitaalveilig.nl/deelnemen
En ook op www.nis2supplychain.eu

Wat moet ik doen als mijn grote klant ISO27001 of NEN7510-norm eist van mij als toeleverancier?

Daar moet je niet zomaar in meegaan, tenzij je er zelf de voordelen ook van inziet. Het NIS2 Supply Chain certificaat is speciaal voor de toeleveringsketen. Is minder werk en wel een zeer acceptabel en goed bruikbaar alternatief. Je moet daar zeker met je klant over praten. NIS2-certificering wordt door meer dan 50 gerenommeerde auditpartijen geauditeerd dus is heel waardevol als bewijs.

Veel mkb-bedrijven halen daarom NIS2-SC10 certificering. Deze bevat 17 maatregelen waarvan veel bedrijven er al 7-8 in orde hebben. Die norm is voldoende. Je kunt ook kiezen voor zeer zware certificering door ISO27001 te halen. Die heeft 93 te behalen maatregelen. Meer informatie over de NIS2 certificering staat op
www.samendigitaalveilig.nl/deelnemen
En ook op www.nis2supplychain.eu

Moet ik als NIS2 bedrijf met al mijn leveranciers samenwerken?

Je moet voor elke leverancier een risico-inventarisatie maken. Niet al je leveranciers zijn risico leveranciers. Kijk voor meer informatie over risico leveranciers op https://samendigitaalveilig.nl/50000mkb/ of naar je te beschermen belangen, zodat je weet welke type leveranciers mogelijk hiervoor in aanmerking komen, zie: https://samendigitaalveilig.nl/te-beschermen-belangen/

Wat zijn de boetes voor NIS2 bedrijven die niet meedoen?

Om de wet te borgen zijn er stevige boetes aangekondigd. Maximaal 10 miljoen of 2% van de wereldwijde omzet voor essentiële bedrijven en maximaal 7 miljoen voor belangrijke bedrijven of 1,4% van de wereldwijde omzet. Toezichthouders kunnen deze boetes opleggen.
Er zijn ook andere boetes tot maximaal 1 miljoen voor:

Niet registreren kan een boete tot 1 miljoen

- niet registreren,
- niet voldoen aan administratieve verplichtingen,
- niet verstrekken van gevraagde informatie aan de toezichthouder,

Waarom zijn te hoge eisen gevaarlijk voor relatie tussen grote 'NIS2 bedrijven' en hun kleinere toeleveranciers?

Te hoge eisen van grote 'NIS2-bedrijven' aan hun kleinere toeleveranciers kunnen ervoor zorgen dat de samenwerking niet soepel verloopt. Het kan lastig zijn voor kleinere bedrijven om aan die strenge normen te voldoen, omdat ze misschien niet genoeg middelen hebben. Dit kan problemen veroorzaken in de toeleveringsketen. Ook kan het ervoor zorgen dat er minder variatie is in de keten, waardoor die minder goed bestand is tegen problemen. Als de eisen te hoog zijn, kan dit ook de algemene online veiligheid van de toeleveringsketen in gevaar brengen. Het is belangrijk om samen te werken op een manier die voor iedereen werkt en rekening houdt met wat ieder bedrijf kan doen. Het NIS2 Supply Chain certificaat ondersteunt hierin.

Ik heb al ISO27001 of NEN7510, moet ik dan nog steeds iets doen met betrekking tot NIS2?

Ja. Met ISO27001 of NEN7510 ben je al een heel eind op weg, echter er zit een zogenaamde GAP tussen genoemde normeringen en NIS2. Ten aanzien van de ontbrekende maatregelen zul je dus nog actie moeten ondernemen (o.a. Je moet meer toeleveringsketen zaken met je leveranciers afspreken, dat is du een zwaardere verplichting dan onder ISO27001 of NEN7510. Verder zijn er Operationele Technology (indien van toepassing) zaken en inrichten van wettelijke verplichtingen als registratieplicht, meldplicht etc.)

Waarom zouden we deze wet serieus nemen? Andere wetten werden ook beperkt gecontroleerd.

NIS2 Cyberbeveiligingswetgeving verschilt sterk van eerdere wetgeving zoals de AVG.

Bij NIS2 zijn toezichthouders expliciet aangewezen om ook proactief toezicht en inspecties uit te voeren. Toezichthouders hebben al aangekondigd dat ze zelf kiezen welke bedrijven ze gaan controleren.

Sectoren waar bedrijven inspecties zullen krijgen:

- Energiesector
- Digitale infrastructuur
- ICT-dienstbeheer (MSP's en MSSP's)
- Overheidsdiensten (met uitzondering van waterschappen)
- Ruimtevaart

Daarnaast draait NIS2 sterk om zorgplicht en aantoonbaarheid.

Belangrijk verschil:

- bij de AVG wordt vooral achteraf gehandhaafd;
- bij NIS2 worden bedrijven proactief bezocht door inspecteurs van de verschillende toezichthouders. Er is dus actieve controle waarbij inspecteurs bedrijven op eigen initiatief bezoeken. Daarnaast is er uiteraard controle nadat een incident is gemeld.

Daarnaast zien we dat grote organisaties, overheden, zorginstellingen en vitale sectoren hun leveranciers steeds vaker actief gaan uitvragen op cybersecurity.

Voor veel bedrijven komt de eerste druk daarom direct vanuit de overheid, maar dus ook vanuit klanten en ketenpartners.

Wij horen nog niets van klanten of leveranciers

Veel organisaties zitten momenteel in een afwachtende fase. De wet in meerdere keren uitgesteld en dat veroorzaakt onduidelijkheid en dan is er weinig reden om te gaan bewegen. Dat is logisch. Dat zien we breed in de markt.
Tegelijkertijd zien we dat:

- steeds meer grote organisaties voorbereidingen treffen;
- Inkoopafdelingen voorwaarden aanpassen;
- leveranciers actief worden beoordeeld;
- het onderwerp nu langzaam toch echt begint te spelen.

Gezien deze situatie is het verstandig om op tijd te beginnen, want in de praktijk duurt voorbereiding vaak meerdere maanden. Organisaties die wachten tot de eerste klantvraag komt of totdat er controle plaatsvindt, lopen het risico dat zij onder tijdsdruk moeten handelen.
Veel bedrijven kiezen er daarom voor om nu alvast basismaatregelen en aantoonbaarheid op orde te brengen.

Wij zijn niet direct NIS2 plichtig

Veel organisaties vallen inderdaad niet rechtstreeks onder de wet.
Maar NIS2 raakt ook leveranciers van NIS2-organisaties. Juist daarom ontstaat er steeds meer aandacht voor aantoonbare cyberhygiëne binnen de keten.

Bedrijven krijgen nu al vragen zoals:

- hebben jullie certificering?
- kunnen jullie bewijzen dat beveiligingsmaatregelen zijn getoetst?
- hebben jullie zelf jullie leveranciers gecontroleerd?

Ook niet-direct-plichtige organisaties krijgen daardoor steeds vaker met NIS2 te maken via klanten of contractvoorwaarden.

Kunnen we wachten eerst totdat de wet officieel ingaat?
Veel organisaties bereiden zich juist nu al voor omdat implementatie tijd kost. Zodra de wet is gepubliceerd in het Staatsblad is deze in werking en zijn alle onderdelen van toepassingen. Dus je moet opstarten voordat de wet ingaat anders ben je te laat. De overheid communiceert hierover via ons en via vele andere kanalen.

In de praktijk zien we trajecten van meerdere maanden voor:

- inventarisatie;
- leveranciersanalyse;
- beleidsvorming;
- technische verbeteringen;
- bewustwording;
- documentatie;
- auditvoorbereiding.

Wanneer klanten of toezichthouders actief gaan uitvragen ben je te laat. Wellicht krijg je van hen dan nog even tijd maar je loopt een risico.

Bij DORA wordt niet actief gecontroleerd en de CSRD werd deels teruggedraaid.

DORA, CSRD en NIS2 Cyberbeveiligingswet zijn echt verschillende wetten met een andere context.

- NIS2 Cyberbeveiligingswet krijgt veel aandacht en gaat gepaard met actief toezicht en inspecties.
- CSRD werd in een veel vroegere fase aangepast. Voor NIS2 Cyberbeveiligingswet ligt dat anders, omdat deze wet al in veel Europese landen actief is. Dus gaat deze ook in Nederland vanzelf in werking. Er is daar geen keuze.
- De vergelijking tussen deze wetten gaat daarom niet op.

De NIS2 Cyberbeveiligingswet gaat een grote impact hebben op organisaties en hun leveranciersketens.

NIS2 Supply Chain certificaat

Is het NIS2 Supply Chain certificaat eigendom van Samen Digitaal Veilig?

Nee, het NIS2 Supply Chain certificaat is geen eigendom van Samen Digitaal Veilig, maar een gezamenlijk initiatief van een tiental brancheorganisaties.

In Nederland is er vrij marktwerking p normen en keurmerken. NIS2 Supply Chain is een keurmerk dat algemeen door de markt wordt geaccepteerd als bewijs voor genomen cybersecuritymaatregelen. Er zijn meer dan 50 gerenommeerde auditorganisaties die in staan voor de kwaliteit van de audits. Er is een keurmerkcommissie die ondersteund wordt door cybersecurityspecialisten, communicatiespecialisten, juristen, auditors en testgroepen. Meer informatie vind je op de volgende website: https://nis2supplychain.eu/

Waarom moet ik het NIS2 Supply Chain certificaat halen?

De belangrijkste reden om het NIS2 Supply Chain certificaat te halen, is je eigen veiligheid en dat jouw grote klant dit van je kan eisen. Verder zullen ook banken, accountants en andere organisaties steeds vaker kijken of een bedrijf wel veilig werkt. Met het NIS2 Supply Chain certificaat laat je aan je klanten, en alle andere organisaties waar je mee werkt, zien dat je veilige werkmethodes hanteert en voldoet aan de gestelde voorwaarden.

We zien dat aanbestedingen nu al worden voorzien van specifieke cyberbeveiligingseisen zoals certificering. Bijvoorbeeld de KVK eist dit van leveranciers. In grote aanbestedingen voor bouw zien we hetzelfde gebeuren.

Wat gebeurt er als ik het NIS2 Supply Chain certificaat niet haal?

Als je het NIS2 Supply Chain certificaat niet behaalt, loop je het risico dat jouw bedrijf niet kan voldoen aan de specifieke eisen en normen die je klanten verwachten. Dit kan leiden tot het verlies van zakelijke kansen en mogelijk zelfs klanten.

Welke voordelen heeft het NIS2 Supply Chain certificaat?

Het NIS2 Supply Chain certificaat is een hulpmiddel zodat je geaudit kunt worden op de NIS2 Supply Chain normen. Het NIS2 Supply Chain certificaat kun je aan je grote klanten laten zien. Het vergroot het vertrouwen van klanten en partners en helpt bij het verminderen van cyberrisico's. Meer over het NIS2 supply Chain certificaat: https://nis2supplychain.eu/

Waarom zou ik kiezen voor het NIS2 Supply Chain certificaat?

Het NIS2 Supply Chain certificaat is speciaal ontwikkeld voor jou als leverancier van grote 'NIS2 bedrijven' of als je klant erom vraagt als die zelf onderdeel is van de toeleveringsketen aan grote bedrijven. Je kunt hiermee aantonen dat je voldoet aan de gestelde eisen en ontvangt hiervan ook een erkend keurmerk certificaat.

Kan ik het NIS2 Supply Chain certificaatabonnement op proef proberen?

Dit is niet mogelijk. Je kunt wel een oriëntatie webinar volgen. Dan krijg je het platform te zien en kun je al je vragen stellen. Kijk hier voor meer info: https://samendigitaalveilig.nl/webinars

Waarom is de prijs per jaar?

De reden dat je een abonnement per jaar hebt, is dat de wet zegt dat je continu moet aantonen dat je actief met cybersecurity bezig bent. Dit is dus niet eenmalig. Het NIS2 Supply Chain certificaat is drie jaar geldig, hierna volgt een nieuwe audit. Elke drie maanden krijg je een systeemmelding, zodat je niet vergeet om NIS2 verplichtingen mee te nemen als er dingen veranderen in je organisatie (denk aan nieuwe medewerkers of systemen).

In het Samen Digitaal Veilig platform zit alles wat nodig is om je certificaat te behouden, zoals geautomatiseerde kwartaalchecks, de verplichte nieuwe maatregelen, juridisch vereiste aanpassingen etc.

Wij hebben al ISO27001 en/of NEN7510

ISO27001 en NEN7510 zijn sterke normen en kunnen veel overlap hebben met NIS2. Toch zien veel organisaties aanvullend behoefte aan:

- praktische ketenaantoonbaarheid; ISO en NEN hebben vaak geen betrekking op alle leveranciers, terwijl NIS2 SC dat wel heeft;
- leverancierscommunicatie;
- proportionele supply chain-eisen in plaats van zware normen die veel tijd en geld kosten;
- specifieke NIS2-focus op zorgplicht richting leveranciers.

Daarom wordt in de praktijk vaak gekeken hoe bestaande normen kunnen worden gebruikt als basis of groeipad, zonder dubbel werk te veroorzaken.
NIS2 Supply Chain-certificering is daarbij vooral bedoeld als praktische en proportionele invulling richting ketenpartijen.

Het is geen officiële overheidscertificering

Klopt. Die bestaat ook niet! Er is geen enkele norm waarmee je aan de wet kunt voldoen. De NIS2 Cyberbeveiligingswet schrijft geen verplichte nationale certificering voor. Er is dus geen door de overheid verplichte norm vastgesteld.

Er zijn wel frameworks en diverse cybersecuritynormen. Die zijn geschikt omdat je dan lijstjes krijgt en gestructureerd kunt werken aan cybersecurity.

Wel bestaat er een specifieke NIS2-norm die speciaal voor deze wetgeving is ontwikkeld. Dat is NOS2 Supply Chain certificering.

Voor veel organisaties is het belangrijkste dat zij aantoonbaar kunnen maken dat passende maatregelen zijn genomen. NIS2 Supply Chain Certificering die is inbegrepen in het Samen Digitaal Veilig abonnement biedt hiervoor een praktische en snelle route.

Wat is de daadwerkelijke waarde van deze certificering?
Wanneer een organisatie succesvol is geaudit door een erkende auditorganisatie, geeft dat vertrouwen richting de markt.

De waarde zit vooral in aantoonbaarheid richting:

- klanten;
- verzekeraars;
- banken;
- toezichthouders.

Voor veel organisaties wordt cybersecurity steeds meer een voorwaarde om zaken te kunnen blijven doen. Wanneer je niet kunt aantonen dat je digitaal veilig werkt, kan dat uiteindelijk commerciële gevolgen hebben.

Daarnaast helpt een praktisch certificeringstraject organisaties om:

- structuur aan te brengen;
- risico's te verminderen;
- leveranciersbeheer te verbeteren;
- interne verantwoordelijkheden duidelijk te maken.

Samen Digitaal Veilig platform

Wat is de achtergrond van Samen Digitaal Veilig?

Samen Digitaal Veilig is opgezet door brancheorganisaties voor hun leden. Zie: https://samendigitaalveilig.nl/over-ons

Of bekijk onze partners: https://samendigitaalveilig.nl/partners/

Welke branches doen mee?

https://samendigitaalveilig.nl/partners/

Waarom doen deze branches mee?

Om hun leden te ondersteunen met digitale veiligheid en de voorbereiding op NIS2. Deze wet heeft grote impact op bedrijven en kan marktverstorend werken. Daarom is er behoefte aan een niet-commercieel platform waar je als bedrijf de juiste informatie krijgt en vooral niet meer gaat doen dan nodig is.

Er zijn heel veel aspecten die je kunt overwegen als je cybersecuritymaatregelen wilt nemen. Er zijn zeer veel zaken die je kut doen. Maar niet alles is nodig voor elke organisatie. Vandaar dat passend advies en ondersteuning wordt gecommuniceerd door brancheorganisaties aan hun leden. Hun advies is om Samen Digitaal Veilig te gebruiken.

Hoe werken de invul webinars?

Wekelijks kun je uitleg- en invul webinars volgen. Je wordt aan de hand genomen, en krijgt stap voor stap uitleg. Zo weet je precies wat je moet doen. Meld je direct aan: https://samendigitaalveilig.nl/webinars

Voor welke webinars kan ik me aanmelden?

We bieden diverse soorten webinars aan, zowel voor deelnemers als ter oriëntatie voor niet-deelnemers. Bekijk alle geplande webinars en reserveer je plek: https://samendigitaalveilig.nl/webinars

Zijn de webinars kosteloos?

De oriëntatie webinars zijn kosteloos te volgen.

De invul- en ondersteuning webinars zijn voor deelnemers met een betaald abonnement.

Hoe krijg ik Inzicht in leveranciersrisico's voor NIS2?

Hiervoor is de ERI ontwikkeld. De Estimated Risk Index (ERI) geeft organisaties direct inzicht in het digitale risicoprofiel van leveranciers.

Op basis van data van ongeveer 170.000 Nederlandse bedrijven helpt de ERI om je leveranciers te beoordelen op risico's en invulling te geven aan de NIS2 ketenzorgplicht.

Meer weten? Kijk op: https://samendigitaalveilig.nl/estimated-risk-index-eri/

Met ERI bespaar je heel veel tijd en kun je snel je leveranciers activeren.

Waarom moet de SDV-licentie doorlopen nadat de audit is behaald
Cybersecurity vereist veel aandacht en is geen eenmalige actie.

1. **NIS2-certificering vraagt continue opvolging**
   Cybersecurity is geen eenmalige audit, maar een doorlopende verplichting. Techniek moet elke dag werken, nieuwe medewerkers moeten worden getraind. Nieuwe leveranciers moeten worden gescreend. En er zijn nog meer zaken die je moet bijhouden.
   Daarom zijn kwartaalchecks en periodieke updates noodzakelijk om aantoonbaar compliant te blijven. In SDV is hiervan een groot deel geautomatiseerd zodat het je zelf weinig tijd kost.
2. **De certificering vereist herhaald bewijs van maatregelen**
   Het is niet voldoende om maatregelen één keer in te richten. Organisaties moeten periodiek opnieuw aantonen dat maatregelen nog actief, getest en actueel zijn.
3. **Wijzigingen binnen organisaties hebben directe impact**
   Nieuwe medewerkers, leveranciers, software of IT-wijzigingen kunnen invloed hebben op compliance en moeten daarom structureel worden bijgehouden.
4. **Back-ups, procedures en toegangsrechten moeten aantoonbaar gecontroleerd blijven**
   Toezichthouders, klanten en auditors verwachten continu bewijs dat processen daadwerkelijk blijven werken.

5. **Leveranciersrisico's blijven veranderen**
   NIS2 richt zich sterk op supply chain-risico's. Daarom moeten organisaties hun leveranciers periodiek blijven beoordelen en opvolgen.
6. **Klanten vragen steeds vaker actuele aantoonbaarheid**
   Niet alleen een certificaatdatum, maar ook bewijs dat cybersecurity actief wordt onderhouden.
7. **Cyberdreigingen veranderen continu**
   Nieuwe phishing methodes, AI-aanvallen en kwetsbaarheden maken structurele updates en awareness noodzakelijk.
8. **Een certificaat zonder opvolging verliest zijn waarde**
   Wanneer kwartaalcontroles, updates en opvolging stoppen, ontstaat het risico dat certificering of aantoonbaarheid vervalt.
9. **NIS2 gaat verder dan techniek alleen**
   Ook beleid, awareness, managementverantwoordelijkheid en documentatie moeten actueel blijven.
10. **SDV ondersteunt organisaties continu bij deze verplichtingen**
    Met kwartaalchecks, reminders, opvolging, documentatie en centrale aantoonbaarheid richting klanten en auditors.

Vergelijk het met BHV of brandveiligheid: ook dat regel je niet één keer voor altijd.

Het klinkt commercieel

Dat begrijpen we goed. De markt rondom NIS2 groeit snel en daardoor ontstaat ook veel commerciële communicatie.

Het SDV-initiatief is echter vanuit brancheorganisaties opgezet en niet vanuit commerciële partijen. Daarbij liggen de kosten aanzienlijk lager dan bij traditionele trajecten.

Belangrijk om te realiseren:

- klanten gaan bewijs vragen, dus aantoonbaarheid wordt noodzakelijk;
- supply chain risico's nemen toe;
- toezichthouders bereiden actief toezicht voor;
- cyberverzekeraars stellen strengere eisen;
- bestuurders worden nadrukkelijker verantwoordelijk gehouden.

Veel organisaties kiezen daarom voor een pragmatische aanpak: niet over investeren, maar wel zorgen dat basismaatregelen en aantoonbaarheid op orde zijn.

Onze IT-partner regelt dit toch al?

Veel organisaties verwachten dat hun IT-partner dit automatisch oppakt.

Dat is echter onmogelijk voor hen omdat de wet zegt dat je zelf een aantal zaken moet regelen. De NIS2 Cyberbeveiligingswet bevat meerdere elementen die niet bij de techniek horen en dus door de organisatie zelf moeten worden geregeld. In de praktijk zien we dat NIS2 dus aanzienlijk verder gaat dan alleen techniek of IT-beheer.

Zaken die niet technisch zijn, maar wel geregeld moeten worden:

- directie actief betrekken in verband met hoofdelijke aansprakelijkheid en verantwoordelijkheid voor het plan en interne communicatie;
- leveranciersrisico's beperken door contractuele afspraken te maken met leveranciers;
- bewustwording en training van medewerkers;
- incidentprocedures opstellen en testen;
- aantoonbaarheid van genomen cybersecuritymaatregelen via certificering richting klanten en toezichthouders.

Je MSP of IT-leveranciers kan technisch veel regelen, maar uiteindelijk moet een organisatie ook zelf een aantal zaken organiseren. Daarom starten veel bedrijven nu samen met hun MSP een praktisch NIS2-traject.

Ook zien we dat bedrijven iets meer technische zaken moeten afnemen dan nu het geval is. Spreek daarover met je leverancier.