— Het belang van samenwerking tussen NIS2 bedrijven/organisaties en Toeleveranciers

NIS2 en de impact op de keten

eye cyber security

Samen Digitaal Veilig

Iedereen:

“Samen veilig werken in de toeleveringsketen is prima, maar...”

NIS2 organisaties:

“...wij willen onze leveranciers niet kwijt.”

Bedrijven:

“...wij willen onze klanten niet kwijt.”

Brancheverenigingen:

“Gebruik dan gewoon NIS2 Quality Mark, de norm die bij allebei past.”

Samen Digitaal Veilig

Inhoudsopgave

NIS2 in het kort

Op 17 oktober 2024 moeten we allemaal klaar zijn met de nieuwe Europese NIS2 richtlijn.

> **“Europa eist dit omdat digitale netwerken en informatiesystemen beter beschermd moeten worden tegen toenemende cybercriminaliteit.”**

NIS2 staat voor Network- and Information Security en draait om het veilig houden van onze essentiële en belangrijke sectoren tegen cyberbedreigingen.

Organisaties en bedrijven in deze sectoren moeten hun eigen online beveiliging op orde hebben en hebben aanvullend zorgplicht voor de digitale veiligheid van hun leveranciers. Dit betekent dat die leveranciers, vaak mkb-bedrijven, actief moeten werken aan hun digitale veiligheid.

> **“Het is essentieel dat alle NIS2 organisaties en bedrijven in de keten samenwerken.”**

Het platform Samen Digitaal Veilig en Eye Security als kennispartner bieden een scala van hulpmiddelen en ondersteuning om deze samenwerking te faciliteren. Dit eBook is jouw gids voor NIS2. Ontdek wat het inhoudt en leer hoe je kunt samenwerken met klanten en leveranciers om aan deze wet te voldoen.

Het NIS2 Quality Mark is opgezet door cybersecurity-specialisten en juristen die hun sporen hebben verdiend bij ministeries, Rijkswaterstaat en grote bedrijven in samenwerking met brancheorganisaties en auditsinstellingen. Het is noodzakelijk om bedrijven een pad te bieden naar een steeds betere cybersecurity. Starten met ISO27001 of een andere gerenommeerde norm is voor velen te zwaar en niet direct noodzakelijk in deze situatie. Het is belangrijker dat bedrijven continu aandacht hebben voor cybersecurity. NIS2 Quality Mark heeft dat via een ingebouwde Plan Do Check Act-cyclus.

Digitale bescherming is essentieel voor onze samenleving

Europa zet zich met NIS2 in voor de digitale veiligheid van haar burgers. Dit is essentieel om problemen te voorkomen, zoals:

- Een patiënt die een dringende operatie mist door een ransomware-aanval op het ziekenhuissysteem.
- Een stad die geen toegang heeft tot schoon drinkwater als gevolg van een cyberaanval op een waterzuiveringsinstallatie.
- Patiënten die belangrijke medicijnen te laat bezorgd krijgen door een cyberaanval op een logistiek bedrijf.
- Mensen die geconfronteerd worden met lege schappen in de supermarkt.
- Studenten die geen examen kunnen doen door een cyberaanval.

> **“Een klein foutje kan grote gevolgen hebben.”**

Bovenstaande voorbeelden maken duidelijk dat niet alleen één bedrijf voorzorgsmaatregelen moet nemen. Denk aan de keten als een ketting; hij is het meest kwetsbaar op de zwakste plek.

En dat is precies waar cyberhackers naar zoeken. Zelfs een klein foutje bij een toeleverancier kan grote gevolgen hebben voor een bedrijf met een belangrijke functie in onze samenleving.

Kwetsbaarheden in de keten

Door toenemende digitalisering zijn er nieuwe kwetsbaarheden ontstaan die specifiek voortkomen in de keten, ook wel supply chain genoemd.
Dit zijn de meest voorkomende kwetsbaarheden binnen een supply chain:

Onveilige externe toegang

Wanneer derde partijen toegang krijgen tot systemen of gegevens binnen de supply chain, kan een gebrekkige beveiliging van externe toegangspunten een bedreiging vormen. Deze onbeveiligde toegang kan worden misbruikt door hackers.

Malware en kwaadaardige software

Malware en andere kwaadaardige software kan zich verspreiden via de supply chain. Hierdoor kunnen systemen en gegevens beschadigd raken of gecompromitteerd worden.

> **“Kwaadaardige software kan zich makkelijk verspreiden via de keten.”**

Cyberaanvallen op leveranciers

Leveranciers binnen de supply chain kunnen het doelwit worden van cyberaanvallen met als doel toegang te verkrijgen tot gevoelige data of systemen. Wanneer een leverancier gecompromitteerd raakt, kan dit leiden tot een reeks beveiligingsproblemen in de gehele keten.

Onvoldoende gegevens-beveiliging bij partners

Als partners in de supply chain onvoldoende gegevensbeveiliging implementeren, kunnen gevoelige gegevens worden blootgesteld aan ongeautoriseerde toegang.

Verstoring van leveringen

Cyberaanvallen kunnen ook gericht zijn op het verstoren van de logistieke processen binnen de supply chain. Dit kan leiden tot vertragingen, verstoorde voorraden en uiteindelijk impact hebben op de operationele efficiëntie.

Wat is NIS2 en waarom raakt het ons allemaal?

De NIS2 is aangekondigd, met wettelijke verplichtingen die in de Wbni komen te staan. Praktisch gezien: net als bij de AVG moet een flink aantal bedrijven verplicht maatregelen nemen op het vlak van cybersecurity. Dat heeft impact. De nieuwe NIS2 cybersecurity zorgplicht eist van een groot aantal bedrijven en organisaties dat zij de supply chain gaan beveiligen.

Kort gezegd: als NIS2 bedrijf* moet je zorgen dat jouw leveranciers digitaal veilig werken om cyberincidenten in de keten te voorkomen. En als leverancier dien je goede afspraken te maken met deze NIS2 bedrijven om je grote klanten te behouden. Dat heeft grote impact op heel veel bedrijven en organisaties in Nederland.

> **“Voldoen aan NIS2 is essentieel in de klant-leveranciersrelatie.”**

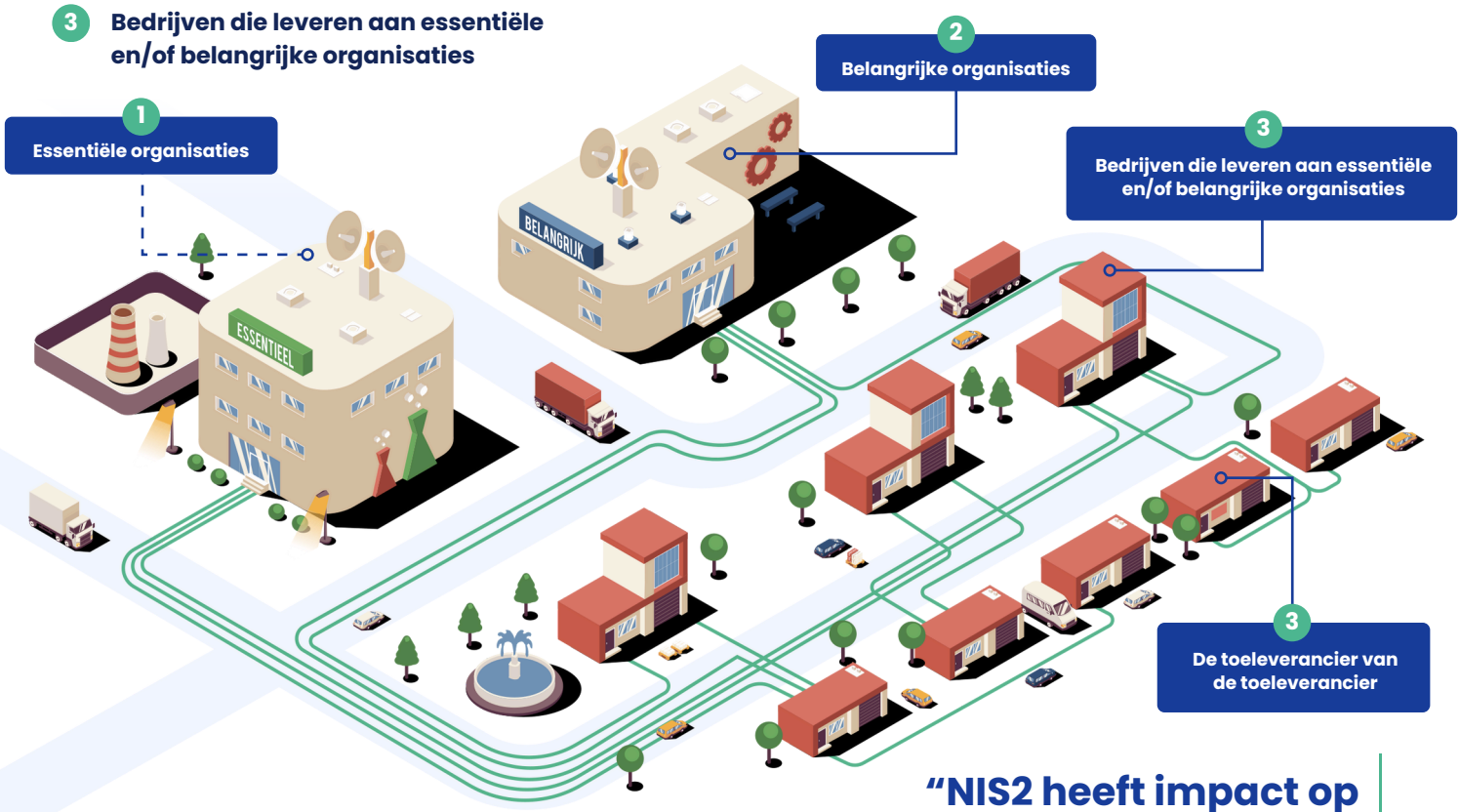
* NIS2 bedrijven: essentiële en belangrijke organisaties, zie volgende pagina.

Deze organisaties moeten voldoen aan NIS2

NIS2 is van toepassing op de volgende doelgroepen:

1. **Essentiële organisaties**
2. **Belangrijke organisaties**
3. **Bedrijven die leveren aan essentiële en/of belangrijke organisaties**

Daarnaast zijn er kleine bedrijven die vallen onder de uitzondering (strategische doelwitten) en apart aangewezen organisaties.



"NIS2 heeft impact op zowel grote als kleine bedrijven."

Essentiële organisaties

Organisaties met minimaal 250 werknemers of een jaaromzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro in de volgende sectoren*: Energie, Transport, Bankwezen, Infrastructuur financiële markt, Gezondheidszorg, Drinkwater, Digitale infrastructuur, Beheerders van ICT-diensten, Afvalwater, Overheidsdiensten en Ruimtevaart.

Belangrijke organisaties

Organisaties met minimaal 50 werknemers of een jaaromzet en balanstotaal van meer dan 10 miljoen euro in de bovengenoemde sectoren of in*: Digitale aanbieders, Post- en koeriersdiensten, Afvalstoffenbeheer, Levensmiddelen, Chemische stoffen, Onderzoek en Vervaardiging/Manufacturing.

* Check de details bij de overheid op https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

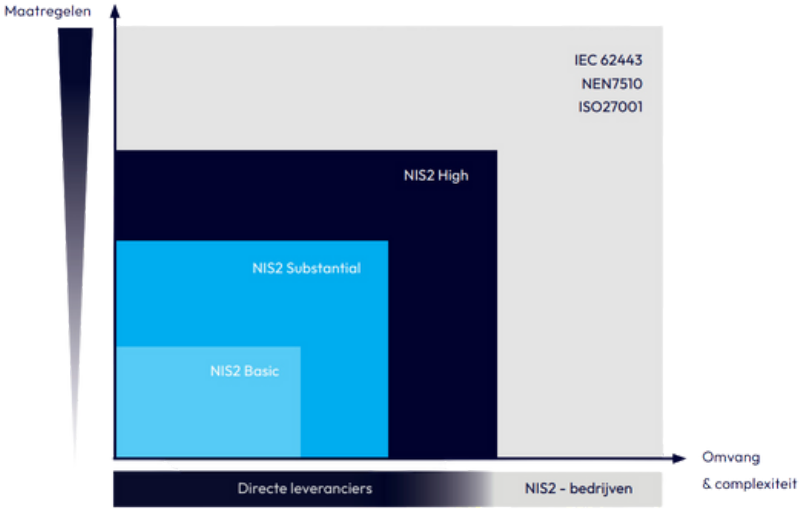
NIS2 Quality Mark: haalbare oplossing voor de toeleveringsketen

Het NIS2 wetsartikel 21.2d stelt dat alle NIS2 organisaties cybersecuritymaatregelen moeten opleggen aan hun directe leveranciers. De specifieke maatregelen variëren op basis van een risico-inventarisatie voor elke leverancier. Het uitvoeren van zo'n risico-inventarisatie is veel werk.

Uit de risico-inventarisatie komt een risicoprofiel. Dat bepaalt hoeveel risico er is en hoeveel maatregelen je zou moeten opleggen. Te hoge eisen aan je leverancier neigen naar normen zoals ISO27001 en NEN7510. Dat kan onnodige kosten met zich meebrengen.

Het NIS2 Quality Mark, als cybersecurity-normering, past beter bij mkb-bedrijven en hun risico's. Het naleven van haalbare cybersecuritynormen kan dan juist de zakelijke relaties versterken.

Optimale normen voor alle bedrijven



NIS2 Quality Mark Basic is het instapniveau voor basis cyberhygiëne

Basis cyberhygiëne is essentieel. NIS2 Quality Mark Basic is geschikt voor mkb-bedrijven. Ze kunnen daarmee laten zien dat hun cyberhygiëne op orde is. Hoger instappen via NIS2 Quality Mark Substantial of High kan ook. Vervolgens groeit men jaar na jaar door naar hogere cybersecuritynormen via de normeringsladder-systematiek.

NIS2 Quality Mark biedt haalbare normen

Het NIS2 Quality Mark vormt een belangrijke schakel tussen bedrijven die samen streven naar betere cyberveiligheid.

Voor veel toeleveranciers zijn (te) zware normen niet nodig.

Voor diverse veiligheidsniveaus is het gebruik van breed gedragen normen daarom aan te raden. Bij hoge risico's kan een ISO-cybersecuritynorm geschikt zijn, maar vaak is een norm die beter aansluit bij mkb-bedrijven veel effectiever.

Het NIS2 Quality Mark is ontworpen om op verschillende risiconiveaus met allerlei leveranciers passende afspraken te maken. Door dit Quality Mark in de inkoopvoorwaarden op te nemen, wordt het risico op verstoringen in de supply chain verminderd, terwijl aan de wettelijke vereisten wordt voldaan.

Toeleveringsketen beveiligen en passende maatregelen afspreken

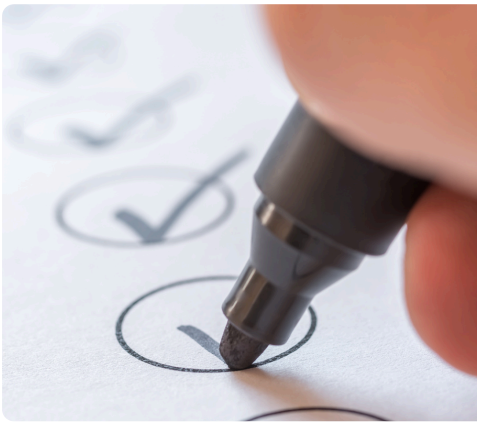
Maatregelen passend bij het risico

Het NIS2 Quality Mark groeipad met een haalbaar Basic cyberhygiëne instapniveau

Meer informatie op nis2qualitymark.eu/keurmerk

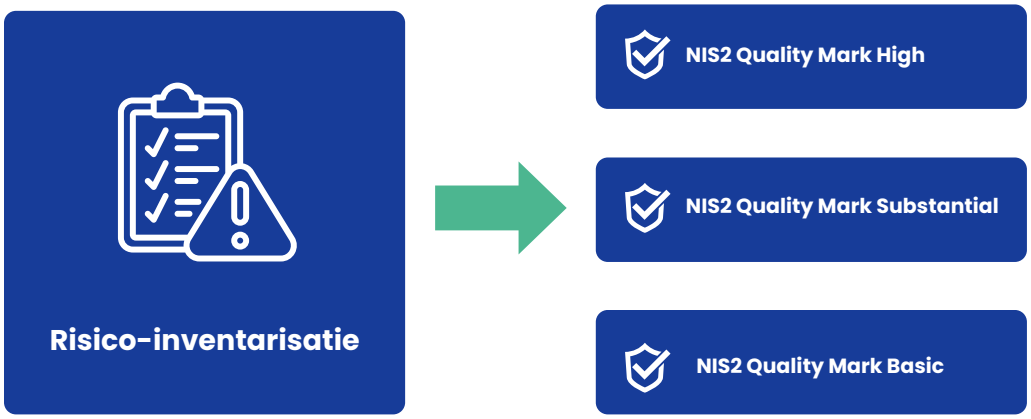
Wat moet je doen?

1. Risico-inventarisatie leveranciers maken (met cybersecurityspecialist)
2. Bepaal het risiconiveau.
3. Leg de passende cybersecuritystandaard op.
4. Zet de standaardvoorwaarden in de inkoopvoorwaarden/contracten.
5. Ontvang het bewijs van de audit dat de leverancier eraan voldoet.
6. Zorg voor een goede afstemming tussen inkoop en IT over de te bepalen norm. Voorkom hierdoor een mogelijk te zware norm die niet passend is bij het contract (incl. mogelijk maatwerk) voor je leverancier.



Stel risico-inventarisatievragen zoals...

- Is er e-mailverkeer met de leverancier door één of meerdere van je medewerkers en één of meerdere medewerkers van de leverancier?
- Gebruik je digitale systemen van deze leverancier binnen de bedrijfsvoering?
- Is deze leverancier een belangrijke schakel in de leveringsketen en kan een verstoring van zijn diensten of producten jouw vermogen om te produceren of leveren beïnvloeden?
- Hoe lang kun je zonder de producten en/of dienstverlening van deze leverancier zonder dat de bedrijfsvoering wordt verstoord?



Geen risico is natuurlijk ook een uitkomst

Volledige risico-inventarisatie op **www.samendigitaalveilig.nl**

Samen Digitaal Veilig: volledige ondersteuning bij NIS2

Risico-inventarisaties maken van alle toeleveranciers is een stevige klus. Essentiële en belangrijke bedrijven kunnen dit in samenwerking met hun cybersecurity-partner doen via de SDV portal. De Samen Digitaal Veilig portal is de oplossing voor de toeleveringsketen met onder andere de volgende mogelijkheden:

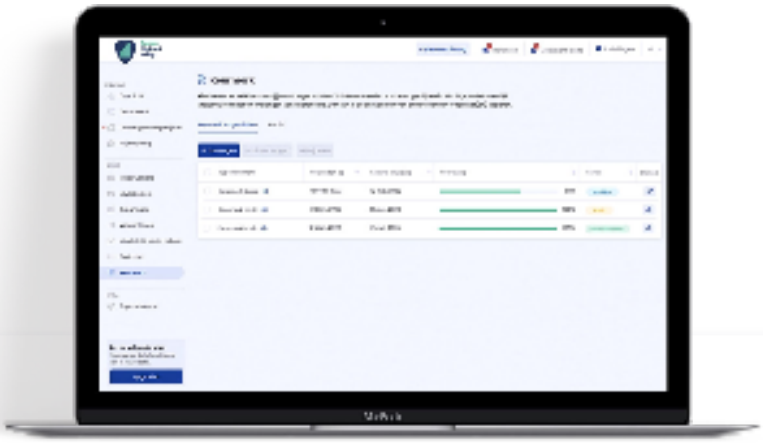
- Risico-inventarisaties
- NIS2 vragenlijsten oplopend in risico
- Ingebouwde PDCA-cyclus met reminders en checks
- Persoonlijke ondersteuning
- Begrijpelijke maatregelenlijsten
- Voorbeelddocumenten
- Supportdesk

"Samen Digitaal Veilig met het NIS2 Quality Mark."

Inkoopvoorwaarden NIS2 kosteloos beschikbaar

Om u als klant te ondersteunen is een set aan ondersteunend materiaal ontwikkeld. Belangrijk zijn de NIS2 Quality Mark normeringen en een document met NIS2 inkoopvoorwaarden waar de wet in is verwerkt zodat compliance makkelijker wordt.

- Alle onderdelen van de wet in een addendum
- Geschikt om toe te voegen aan je eigen inkoopvoorwaarden
- Gemaakt door juristen met verstand van cybersecurity
- Uitleg via webinars
- Downloadbaar



NIS2 QUALITY MARK

Het NIS2 Quality Mark is een kwaliteitskeurmerk voor cybersecurity. De inhoud is samengesteld door juristen, cybersecurityspecialisten én grote en kleine bedrijven. Meer informatie over het NIS2 Quality Mark vind je op:

nis2qualitymark.eu

Samen Digitaal Veilig is licentiehouder van het NIS2 Quality Mark, en biedt het online platform en de ondersteuning om bedrijven en organisaties te helpen het NIS2 Quality Mark te behalen.

Met 70 deelnemende branches bereiken we meer dan 125.000 bedrijven in Nederland

Over Samen Digitaal Veilig

Samen Digitaal Veilig (SDV) is een initiatief van branche- en beroepsorganisaties, MKB-Nederland en VNO-NCW. Enkele jaren geleden is SDV begonnen met hulp van het ministerie van Justitie en Veiligheid en het ministerie van Economische Zaken en Klimaat. Minister Grapperhaus gaf daarvoor het startschot. Dankzij deze overheidssteun kunnen alle bedrijven in Nederland de startversie van Samen Digitaal Veilig gratis gebruiken. Nu en in de toekomst.

De uitbreiding op het SDV-platform met NIS2 ondersteuning is door brancheorganisaties zelf georganiseerd en gefinancierd. Dit is gedaan omdat het belangrijk is dat de toeleveringsketen – voornamelijk bestaande uit mkb-bedrijven – op een goede en zorgvuldige manier geholpen wordt bij de invoering van de NIS2 wet in Nederland.

Over Eye Security

Eye Security is een toonaangevend Europees cybersecuritybedrijf dat een alles-in-één-beveiligingspakket biedt voor bedrijven van elke omvang. Dit pakket omvat 24-uursmonitoring en -detectie, snelle incidentrespons door experts, en optioneel een cyberverzekering. Onze gestroomlijnde aanpak biedt maximale beveiliging en voordelen voor onze klanten.

Wij geloven dat elk bedrijf topbeveiliging verdient. Met het toenemende aantal en de complexiteit van cyberaanvallen zijn organisaties in Europa kwetsbaarder dan ooit. Alleen in een veilige digitale wereld kunnen we floreren, innoveren en groeien.

Bij Eye Security helpen we organisaties echt hun cyberrisico's te verlagen. Samen met onze partners begeleiden we bedrijven om weerbaarder te worden tegen cyberaanvallen en NIS2-compliance te bereiken. Bezoek onze website voor een gratis adviesgesprek en ontdek hoe we jouw organisatie dag en nacht kunnen beveiligen.

We waarderen de no-nonsense en pragmatische aanpak van Samen Digitaal Veilig, die perfect aansluit bij onze filosofie. Deze samenwerking geeft ons de kans om niet alleen klanten te beveiligen, maar ook te helpen bij het voldoen aan belangrijke regelgeving zoals NIS2, versterkt door het NIS2 Quality Mark.

Samen Digitaal Veilig

samendigitaalveilig.nl