

— Het belang van samenwerking tussen NIS2 bedrijven en toeleveranciers

NIS2 en de impact op de keten



**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.”**

— Brancheorganisaties:

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



**Samen
Digitaal
Veilig**

Inhoudsopgave

| | |
|------------------------------------------------------------------------|-----------|
| NIS2 in het kort | 4 |
| Digitale bescherming is essentieel voor onze samenleving | 5 |
| Kwetsbaarheden in de keten | 6 |
| Wat is NIS2 en waarom raakt het ons allemaal? | 7 |
| Deze organisaties moeten voldoen aan NIS2 | 8 |
| NIS2 Quality Mark: haalbare oplossing voor de toeleveringsketen | 9 |
| NIS2 Quality Mark biedt haalbare normen | 10 |
| Samen Digitaal Veilig: volledige ondersteuning bij NIS2 | 11 |

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 NIS2 Quality Mark en het platform van Samen Digitaal Veilig bieden alle benodigde 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 gegevensbeveiliging 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, verstoorte 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.”

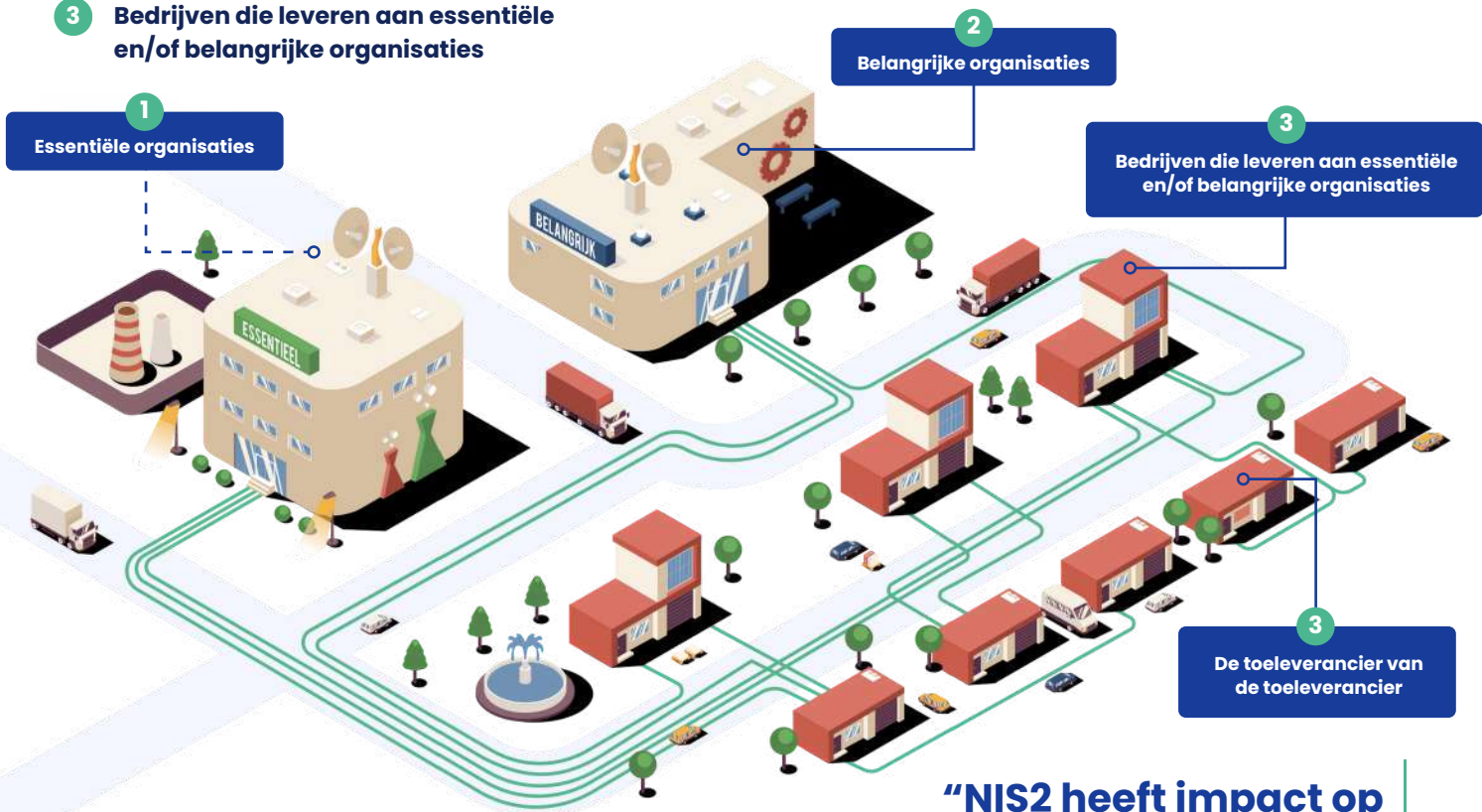
* NIS2 bedrijven: essentiële en belangrijke organisaties, zie volgende pagina.

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 jaarmzet 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 jaarmzet 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/>

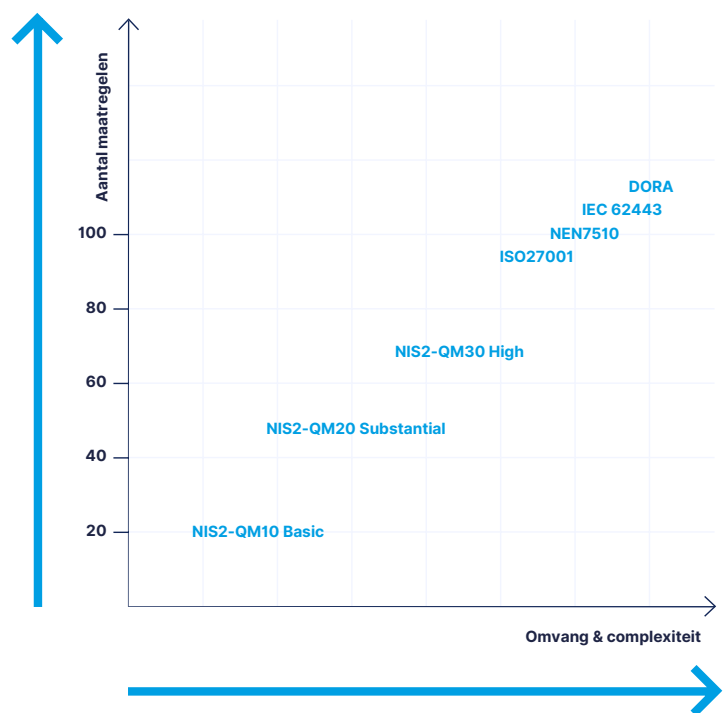
NIS2 Quality Mark: Haalbare oplossing voor de toeleveringsketen

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

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



Voor de risicoafdekking bij mkb-bedrijven past het NIS2 Quality Mark heel goed.



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 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 vermindert, terwijl aan de wettelijke vereisten wordt voldaan.

Maatregelen passend bij het risico



Het NIS2 Quality Mark groeppad met een haalbaar Basic instapniveau

Samen Digitaal Veilig: volledige ondersteuning bij NIS2

Risico-inventarisaties maken van alle toeleveranciers is een stevige klus. Essentiële en belangrijke bedrijven kunnen dit 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
- ✓ Toelichting, uitleg en voorbeelden bij alle vragen
- Management dashboards
- ✓ Reminders versturen en antwoorden controlleren
- ✓ Meldplicht functies via alerts
- ✓ Ingebouwde PDCA-cyclus met reminders en kwartaal- en jaarlijkse checks

Toeleveranciers die het NIS2 Quality Mark willen halen om aan de NIS2 eisen van hun klanten te voldoen gebruiken Samen Digitaal Veilig, een complete oplossing inclusief:

- ✓ Persoonlijke intake met NIS2 ondersteuner
- ✓ Begrijpelijke maatregelen lijsten
- ✓ Voorbeelddocumenten
- ✓ Invulwebinars
- ✓ Supportdesk
- ✓ Inclusief de NIS2 Quality Mark-norm

**“Samen Digitaal Veilig met
het 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 onze deelnemende 55 branches bereiken we meer dan 110.000 bedrijven in Nederland

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 ook in de komende jaren.

De uitbreiding op het Samen Digitaal Veilig platform met de NIS2 ondersteuning is door de 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.



**Samen
Digitaal
Veilig**

samendigitaalveilig.nl