Het belang van samenwerking tussen NIS2 bedrijven en leveranciers

NIS2 en de impact op de keten

IRISONE ICT

Inhoudsopgave

NIS2 in het kort

Op 17 oktober 2024 start de nieuwe Europese NIS2 richtlijn, In Nederland iets later, maar we moeten er wel aan beginnen.

> **“Nieuwe Europese richtlijn verplicht dat bedrijven hun cybersecurity op orde hebben.”**

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

De NIS is in Nederland opgenomen in de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Praktisch gezien moet een flink aantal bedrijven verplicht maatregelen nemen op het vlak van cybersecurity. Dat heeft impact.

NIS2-bedrijven* moeten hun digitale infrastructuur en systemen beveiligen, procedures opzetten voor het melden van incidenten en regelmatig beveiligings-protocollen evalueren en bijwerken.

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

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

De nieuwe NIS2 ketenzorgplicht eist van een groot aantal bedrijven en organisaties dat zij de supply chain gaan beveiligen. Het NIS2 wetsartikel 21.2d stelt dat alle NIS2 bedrijven risico’s in de keten, vanuit leveranciers, moeten vermijden. Dit betekent dat die leveranciers, vaak mkb-bedrijven, actief moeten werken aan hun digitale veiligheid.

Kort gezegd: als NIS2 bedrijf moet je zorgen dat jouw leveranciers digitaal veilig werken om cyberincidenten in de keten te voorkomen. Daarvoor moeten goede afspraken worden gemaakt. En als leverancier moet je aantoonbaar werken aan je cybersecurity volgens deze afspraken, anders raak je NIS2 bedrijven kwijt als klant. Dit heeft grote impact op veel bedrijven en organisaties in Nederland.

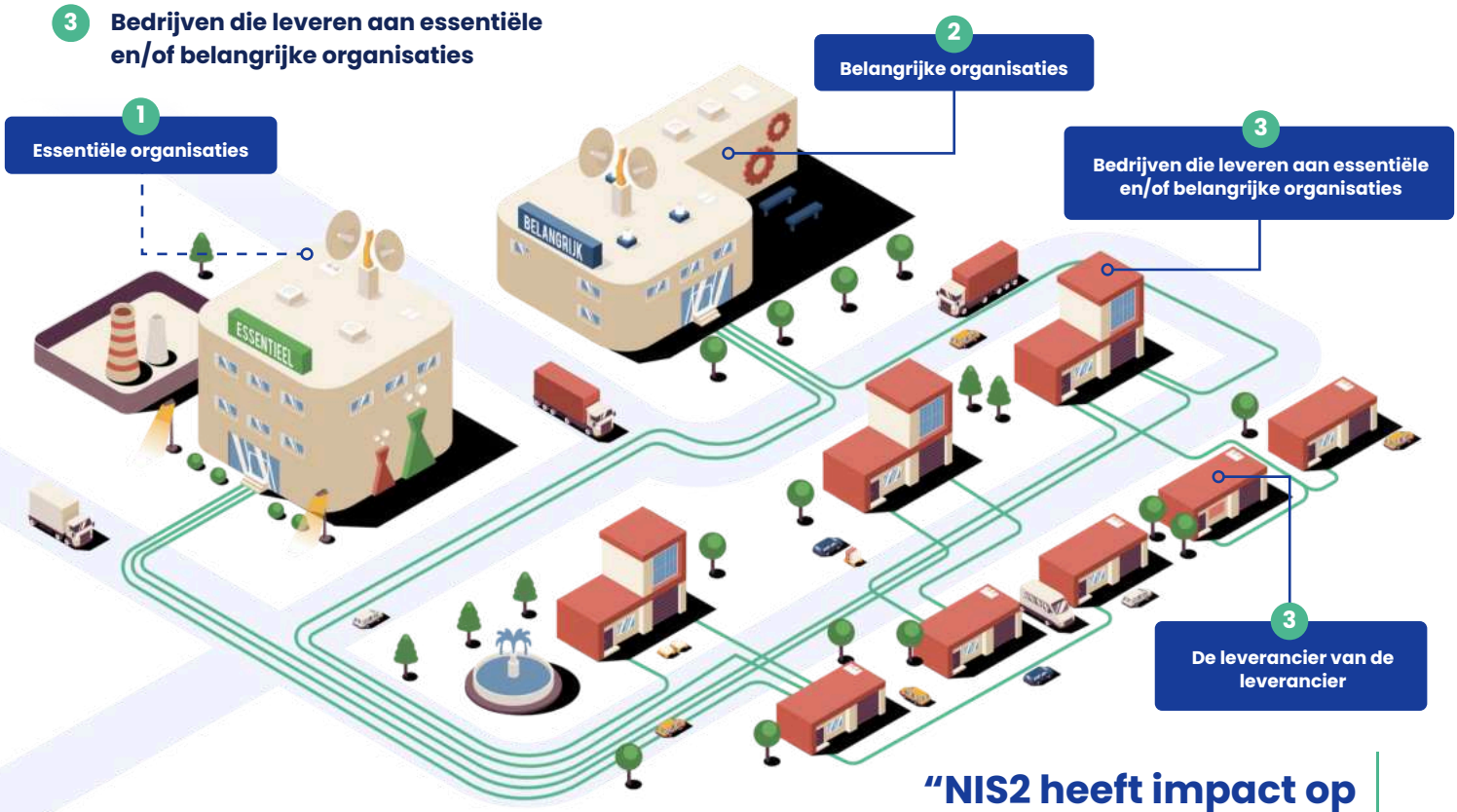
Belangrijke punten van de richtlijn zijn onder meer:

- **Strengere eisen**: Er worden strengere eisen gesteld aan de beveiliging van netwerk- en informatiesystemen.
- **Ketenzorgplicht**: Ondernemingen zijn verplicht om niet alleen hun eigen cybersecurity te waarborgen, maar ook actief bij te dragen aan de beveiliging van de gehele keten waar zij deel van uitmaken. Dit houdt in dat zij verantwoordelijkheden hebben ten aanzien van de digitale veiligheid van hun partners en leveranciers.
- **Meldplicht**: Er is een meldplicht voor incidenten. Dit betekent dat als er iets misgaat, je dit moet melden bij de relevante autoriteiten.
- **Toezicht en handhaving**: Er worden maatregelen ingevoerd om de naleving van de NIS2 richtlijn te verzekeren, inclusief financiële sancties voor niet-naleving.

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**



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

Essentiële en belangrijke organisaties

Essentiële bedrijven, zoals die in Energie, Transport, Bankwezen, Gezondheidszorg en Digitale infrastructuur, zijn cruciaal voor de stabiliteit van de samenleving. Belangrijke bedrijven, zoals Post- en koeriersdiensten, Levensmiddelen, Chemische stoffen en Manufacturing*, vervullen ook een belangrijke rol in economische activiteiten en dagelijkse behoeften.

Mkb-leveranciers

Mkb-leveranciers** die leveren aan essentiële en belangrijke bedrijven zullen te maken krijgen met de NIS2 vanwege de ketenzorgplicht. Dit betekent dat zij verantwoordelijk zijn voor het waarborgen van de cyberbeveiliging binnen hun eigen bedrijf en in hun leveranciersketen, om zo de digitale weerbaarheid van de hele sector te versterken.

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

** Lees meer op https://www.samendigitaalveilig.nl/nieuws/ketenzorgplicht-nis2-richtlijn-raakt-ruim-50-000-mkb-bedrijven/

Waarom raakt NIS2 ons allemaal?

Door toenemende digitalisering zijn er nieuwe kwetsbaarheden ontstaan die specifiek voorkomen in de keten, ook wel supply chain genoemd. NIS2 bedrijven zijn afhankelijk van de veiligheid in hun keten. Cyberincidenten mogen deze keten niet verstoren. Als leverancier ben je hier onderdeel van en is de NIS2 dus ook van toepassing voor jou.

> **"Elk cyberincident kan de keten verstoren."**

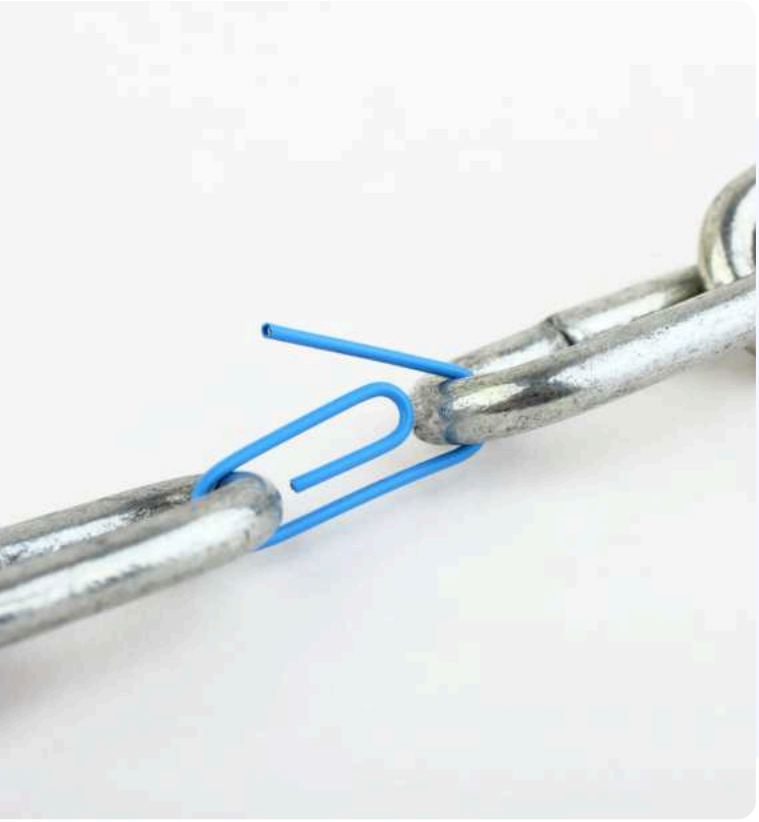
Veelvoorkomende kwetsbaarheden binnen een supply chain zijn:

- Onveilige toegang en zwakke databeveiliging: Als externe partners slecht beveiligd zijn, kunnen ze gemakkelijk doelwit zijn voor hackers.
- Malware: Dit kan zich door de keten verspreiden en systemen en informatie in gevaar brengen.
- Aanvallen op de logistiek: Dit zijn pogingen om de levering te ontregelen, wat leidt tot vertragingen en verstoringen in de voorraad.

Digitale bescherming is essentieel voor onze samenleving

Europa heeft de NIS2 verplicht gemaakt omdat ze haar burgers veilig wilt houden. 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 supply chain als een ketting; hij is het meest kwetsbaar op de zwakste plek.

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

Voldoen aan NIS2 met een haalbare norm

Als NIS2 bedrijf moet je zorgen dat je directe leveranciers goed beschermd zijn tegen cyber-aanvallen. Om te borgen dat alle leveranciers hun digitale veiligheid op orde hebben zal een algemeen geaccepteerde norm gebruikt moeten worden.

ISO27001 is een goede norm voor grote en complexe organisaties, maar voor mkb-bedrijven te zwaar. Er is een alternatief met een groeipad dat beter past voor deze wet.

Het NIS2 Quality Mark is de kwaliteitsnorm voor cybersecurity voor mkb-bedrijven. Het is zeer geschikt om stap voor stap de digitale veiligheid te verbeteren en risico's in de keten te verminderen.

Het naleven van een haalbare cybersecuritynorm kan hiermee de zakelijke relaties juist versterken, in plaats van verstoren.

Optimale normen voor alle bedrijven

NIS2 Quality Mark is de haalbare norm voor samenwerking in de keten

Door bij de basis te starten, worden mkb-bedrijven zich meer bewust van hun digitale veiligheid en kunnen ze aan hun klanten bewijzen dat ze de basis goed hebben geregeld. Daarna verbeteren ze elk jaar hun beveiliging verder door de stappen van de cybersecurityladder te volgen.

Iris One: volledige ondersteuning bij NIS2

Iris One stelt in samenwerking met Samen Digitaal Veilig een breed scala aan tools beschikbaar, speciaal voor het mkb. Ons hoofddoel? Zorgen dat iedereen die onder de NIS2 valt op een goede manier aan deze wet kan voldoen.

We bieden verschillende oplossingen aan en ondersteunen je in dit project.

- Risico-inventarisaties
- NIS2 vragenlijsten oplopend in risico
- Meldplicht functies via alerts
- Ingebouwde PDCA-cyclus met reminders en kwartaal- en jaarlijkse checks
- Begrijpelijke maatregelenlijsten
- Invulwebinars
- Supportdesk

“Iris One helpt je bij het NIS2 proof maken van je bedrijf”

IRIS ONE ICT

Iris One is dé ICT-specialist voor ondernemend Nederland. Vanuit onze locaties, elk met hun unieke identiteit en specialisme, bieden we gezamenlijk een complementair spectrum van diensten aan het mkb in Nederland.

Meer informatie?

Heb je vragen over NIS2 of het halen van het NIS2 Quality Mark?
Neem dan contact op via iris@iris-one.nl.

Over Iris One
Iris One is dé ICT-specialist voor ondernemend Nederland. Wij geloven in een complementaire aanpak, waar kennis & expertise hand in hand gaan. We zetten mensen centraal, stappen daadkrachtig naar voren en worden gedreven door een grenzeloze ambitie om de digitale toekomst vorm te geven.
In een wereld die digitaal continu in beweging is, wapenen we uw organisatie tegen dreigingen. Met de aandacht voor kwaliteit en klantgerichtheid waar Iris One om bekend staat.

Wij kennen onze rol als ICT-dienstverlener en wij weten dat ondernemers het druk genoeg hebben met het runnen van hun onderneming. We nemen daarom een aantal essentiële zaken uit handen, en dat gaat verder dan enkel het leveren van hard- en software. De NIS2 wetgeving is daar een mooi voorbeeld van. Wij helpen onze klanten en hun leveranciers te voldoen aan deze wetgeving, zowel op het vlak van beleid, bewustzijn van medewerkers als de techniek. Wij zien het als onze plicht om Nederland en Europa digitaal veiliger te maken.

In de samenwerkingen met Samen Digitaal Veilig en ThreadStone Cyber Security hebben we de perfecte partners gevonden om uw organisatie te ondersteunen aan de NIS2 wetgeving te voldoen. Een solide basis, duidelijke richting en de pragmatische aanpak vormen de formule voor succes.

IRIS ONE ICT