“Mijn klant vraagt naar NIS2”: gids voor leveranciers

U valt niet onder NIS2, maar een klant stuurt u een beveiligingsvragenlijst of nieuwe contractclausules. Hier leest u waarom, en hoe u met vertrouwen antwoordt.

NIS2 Aware · nis2aware.eu · november 2026

Waarom uw klant vragen stelt

Organisaties die onder NIS2 vallen, moeten de beveiliging van hun **toeleveringsketen** beheren. Een groot deel van de incidenten begint bij een leverancier: een gehackte IT-dienstverlener, een gecompromitteerde software-update, het gestolen wachtwoord van een onderhoudsfirma. Uw klant moet dus de beveiliging beoordelen van de leveranciers waarvan hij afhangt, en u bent er een van.

Wat hij kan vragen

- Een **beveiligingsvragenlijst** (vaak 20 tot 100 vragen) over uw maatregelen.
- **Contractclausules**: minimale maatregelen, melding van incidenten binnen een korte termijn, auditrecht, vertrouwelijkheid.
- **Bewijzen**: een CyberFundamentals-zelfevaluatie of -verificatie, een ISO/IEC 27001-certificaat, een samenvatting van uw beveiligingsbeleid.
- Concrete maatregelen: **multifactorauthenticatie**, back-ups, tijdige updates, beperkte toegang tot zijn systemen.
- Een **contactpersoon voor beveiliging** op naam, bereikbaar bij een incident.

Hoe antwoordt u?

1. **Geen paniek, en beloof niet te veel.** Antwoord eerlijk: “in orde”, “in uitvoering (tegen een bepaalde datum)” of “niet van toepassing”. Een geloofwaardig plan is beter dan een loze ja.
2. **Lees de clausules aandachtig** voor u tekent: meldingstermijnen, aansprakelijkheid, auditrecht. Laat ze nakijken als dat nodig is.
3. **Bundel uw antwoorden op één plaats**, zodat u ze voor de volgende klant kunt hergebruiken.

4. **Maak er een troef van:** een leverancier die duidelijk en snel antwoordt, wekt vertrouwen en wint contracten.

Uw actieplan van 30 dagen

Week	Acties
1	Wijs een contactpersoon voor beveiliging aan. Schakel multifactorauthenticatie in op e-mail en toegang op afstand.
2	Controleer uw back-ups: minstens één kopie offline of onveranderbaar, en test een herstel. Schakel automatische updates in.
3	Verwijder overbodige beheerdersrechten. Controleer of elk toestel actuele antimalware heeft.
4	Schrijf een incidentprocedure van één pagina, inclusief hoe u uw klanten informeert. Maak uw personeel bewust van phishing.

Volgende stap: toon het aan

Het **CyberFundamentals**-kader van het CCB heeft een niveau **Basic** dat bij veel kleine bedrijven past. Een zelfevaluatie volgens CyFun Basic geeft u een gestructureerd antwoord op de meeste vragenlijsten. U vindt de tools op atwork.safeonweb.be.

> **Test uzelf eerst:** onze snelle maturiteitscheck toont uw lacunes in vijf minuten.

Algemene informatie over het Belgische NIS2-kader op datum van november 2026, geen juridisch advies. Raadpleeg altijd de meest recente informatie van het CCB (ccb.belgium.be en atwork.safeonweb.be).