

Cyberbeveiliging: dit moet je op orde hebben

Waarom krijg je hiermee te maken?

- Sinds 15 augustus 2026 geldt de Cyberbeveiligingswet (NIS2).
- De wet geldt voor grotere organisaties in vitale sectoren, zoals zorg, energie, vervoer, overheid en voeding.
- Het mkb valt er meestal zelf niet onder. Je klanten soms wel.
- Die klanten moeten van de wet ook hun leveranciers controleren. Jij bent zo'n leverancier.

Hoe merk je dat?

- Je krijgt een vragenlijst over je beveiliging.
- Er komen beveiligingseisen in contracten en aanbestedingen.
- Je klant vraagt om bewijs, zoals tweestapsverificatie, geteste back-ups en training van medewerkers.
- Soms vraagt een klant ook naar een pentest of een ISO 27001-certificaat.

Wat betekent dat voor jou?

- Val je er zelf niet onder, dan heb je geen wettelijke plichten zoals registreren of incidenten melden.
- Je klant wil wel zeker weten dat jouw beveiliging op orde is.
- Met de maatregelen op de volgende pagina kun je die vragen beantwoorden.
- Twijfel je of je zelf onder de Cyberbeveiligingswet valt? Doe de zelftest op regelhulpenvoorbedrijven.nl/NIS-2-NL.

Waar begin je?

- Loop de checklist op de volgende pagina langs en vink af wat al geregeld is.
- Begin bij wat klanten vaak vragen: tweestapsverificatie, back-ups, updates, medewerkers en een plan voor als het misgaat.
- Zorg dat je kunt laten zien wat je hebt geregeld.

Val jij onder de keten? Dan moet je dit op orde hebben

1. Risico's en beleid

- Weet welke systemen en gegevens het belangrijkst zijn en wat er mis kan gaan.
- Leg op papier vast hoe je met beveiliging omgaat. De directie keurt dit goed.
- Wijs één persoon aan die verantwoordelijk is voor cybersecurity.

2. Toegang en accounts

- Tweestapsverificatie (MFA) op alle accounts: Microsoft 365, je boekhoudsoftware en werken op afstand.
- Medewerkers hebben alleen toegang tot wat ze nodig hebben.
- Accounts van medewerkers die uit dienst gaan, worden direct afgesloten en laptops en telefoons ingeleverd.

3. Apparaten en systemen

- Houd een overzicht bij van alle apparaten, systemen en software.
- Installeer updates op tijd en vervang systemen die geen updates meer krijgen.
- Virusscanner en firewall staan aan, laptops en telefoons zijn versleuteld.
- Server en netwerkkapparatuur zitten achter slot en grendel.

4. Back-up en doorwerken

- Maak elke dag een back-up en bewaar een kopie los van je netwerk.
- Test regelmatig of terugzetten werkt en bewaar het testrapport.
- Zorg voor een plan om door te werken als systemen uitvallen.

5. Als het misgaat

- Zorg voor een incidentplan op één A4: wie bel je, wie beslist en wie informeert klanten?
- Weet wanneer en waar je een incident moet melden, zoals een datalek bij de Autoriteit Persoonsgegevens.
- Oefen het plan minstens één keer per jaar.

6. Medewerkers

- Iedereen krijgt training in veilig werken en het herkennen van phishing.
- Medewerkers weten hoe ze een verdachte mail of incident melden.
- Maak duidelijke afspraken over thuiswerken en het gebruik van eigen apparaten.

7. Leveranciers

- Weet welke leveranciers toegang hebben tot je systemen of gegevens.
- Leg afspraken over beveiliging met ze vast in het contract.
- Check of je belangrijkste leveranciers hun beveiliging op orde hebben.

8. Controleren en aantonen

- Controleer minstens één keer per jaar of je maatregelen werken, en verbeter wat beter kan.
- Bewaar bewijs: je beleid, de testrapporten van je back-ups, gevolgde trainingen en je incidentplan.
- Zo heb je het antwoord klaar als een klant of toezichthouder ernaar vraagt.