NIS2 CHECKLIST VOOR MKB – SUPPLY CHAIN COMPLIANCE

10 stappen naar *aantoonbare* cyberveiligheid.

Naar schatting **50.000 tot 100.000 MKB-bedrijven** krijgen indirect met NIS2 te maken — niet via de overheid, maar via hun klanten. Dit is uw praktische checklist. Geen IT-jargon. Wel bewijs op papier.

- 10 concrete stappen
- Geen IT-kennis vereist
- Klaar vóór 1 juli 2026

Deadline: 1 juli 2026 — Cyberbeveiligingswet Nederland van kracht. Gemiddeld traject: 3–5 maanden. Wie nu start, haalt het.

Pagina 1 van 2 →

VAL IK ONDER NIS2?

U VALT DIRECT ONDER DE WET ALS...

- **Werkzaam in 18 kritieke sectoren** (energie, zorg, transport, financieel, IT, overheid...)
- **Meer dan 50 medewerkers** of meer dan €10 mln omzet/balanstotaal

U VALT INDIRECT ONDER DE WET ALS...

- **U levert aan NIS2-plichtige organisaties** — ziekenhuizen, gemeenten, energiebedrijven, banken, logistiek
- **Uw klant eist het contractueel** — ook zonder officiële aanschrijving kunt u een vragenlijst ontvangen

DE 10-STAPPEN CHECKLIST

01 Stel vast of u onder de wet valt (of als leverancier)

Gebruik de **zelfevaluatietool** van het Digital Trust Center. Lever ik aan klanten die NIS2-plichtig zijn? De kans is groot dat u vóór 1 juli al een vragenlijst ontvangt.

URGENT

☐ GEREED?

02 Wijs een verantwoordelijke aan voor cybersecurity

Geen fulltime CISO nodig — maar er moet iemand zijn met de regie. **De directeur is eindverantwoordelijk.** Uw IT-leverancier kan dit niet voor u invullen.

URGENT

☐ GEREED?

03 Stel een informatiebeveiligingsbeleid op

Heeft u een document dat beschrijft hoe uw organisatie omgaat met data, toegang en beveiliging? **Dit is de basis van elke NIS2-toetsing.** Zonder dit document kunt u geen beleid aantonen.

URGENT

☐ GEREED?

04 Breng uw back-up en herstelplan op orde

Controleer: hoe oud is de laatste back-up? Is die **extern opgeslagen**? Is hij ook teruggezet als test? Een back-up die nooit getest is, is geen back-up.

URGENT

☐ GEREED?

05 Inventariseer apparaten en toegangsrechten

Weet u hoeveel laptops, telefoons en cloudaccounts toegang hebben tot uw bedrijfsdata? **Wie heeft beheerdersrechten?** Medewerkers mogen geen onnodige lokale beheerdersrechten hebben.

BELANGRIJK

☐ GEREED?

> *Wacht niet op het telefoontje van uw klant. Wanneer die belt, is het te laat om op tijd te zijn.*
>
> — Webinar Samen Digitaal Veilig & Schilteman, februari 2026

DAEMEN ICT | Lupasafe
076 – 596 1391
daemen-ict.nl · lupasafe.com

STAPPEN 6 T/M 10 + TIJDLIJN & CERTIFICERING

Compliant zijn is één ding. *Aantonen* is het andere.

CHECKLIST VERVOLG — STAPPEN 6 T/M 10

06 Zet meervoudige verificatie (MFA) aan op alle accounts

Microsoft 365, e-mail, VPN — overal. **MFA is de goedkoopste maatregel met de grootste impact.** Veel hacks worden voorkomen door simpelweg MFA in te schakelen. Basiseis in NIS2.

URGENT

☐ GEREED?

07 Bescherm thuiswerkers en remote verbindingen

Werken medewerkers thuis of op locatie? Verplicht gebruik van **VPN** en zorg voor **schijfversleuteling (encryptie)**. Geen lokale beheerdersrechten. Laptop gestolen zonder encryptie? Data weg.

BELANGRIJK

☐ GEREED?

08 Train uw medewerkers in cyberbewustzijn

De meeste cyberaanvallen beginnen met een medewerker die op een phishinglink klikt. **Jaarlijkse training en phishing-simulaties** zijn een NIS2-verplichting én de meest effectieve maatregel die u kunt nemen.

URGENT

☐ GEREED?

09 Zorg voor een incidentresponsplan

Wat doet u als u morgen gehackt wordt? Wie belt u? Wie informeert u? Bij NIS2 moet u significante incidenten **binnen 24 uur melden** bij de toezichthouder. Leg dit vast — ook al is het maar een A4.

BELANGRIJK

☐ GEREED?

10 Documenteer en maak het aantoonbaar

Compliance zonder bewijs bestaat niet. Uw klant en toezichthouder willen het **zien**, niet alleen horen. Gebruik een dashboard dat automatisch bijhoudt waar u staat — exporteerbaar voor audits en klantrapportages.

URGENT

☐ GEREED?

WELK CERTIFICERINGSNIVEAU HEEFT U NODIG?

SC 10 — MEEST MKB	SC 20 — SUBSTANTIAL	SC 30 — HIGH
BASIC	**SUBSTANTIAL**	**HIGH**
Voor MKB-toeleveranciers. 8 op de 10 bedrijven komen hiermee prima uit de voeten.	Voor bedrijven met hogere risicoprofielen of gevoeliger ketenposities.	Voor organisaties die zelf NIS2-plichtig zijn. ISO 27001 dekt een groot deel af.
17 controles	Uitgebreide set	Volledig NIS2
✓ AANBEVOLEN VOOR U		

TIJDLIJN — WANNEER MOET WAT GEREGELD ZIJN?

NU — Q1 2026	Q2 2026	1 JULI 2026	NA INGANGSDATUM
Start zelfevaluatie	**Klanten schrijven aan**	**Wet van kracht**	**Handhaving**
Breng de grootste gaten in kaart	Grote opdrachtgevers controleren hun keten	Cyberbeveiligingswet Nederland	Toezichthouder controleert actief

1 op 5	21 dg	3–5 mnd	100K+
MKB-bedrijven wordt jaarlijks slachtoffer van een cyberaanval	gemiddeld herstel na aanval voordat bedrijf weer operationeel is	gemiddeld traject voor SC 10 certificering voor MKB	MKB-bedrijven geraakt via ketenverantwoordelijkheid NIS2

DAEMEN ICT × LUPASAFE

Weet u binnen *30 minuten* waar u staat.

Daemen ICT koppelt het Lupasafe-platform in een uurtje aan uw Microsoft 365-omgeving. U krijgt direct uw score op alle 17 SC 10-controles — groen, oranje of rood. Geen IT-consultant nodig.

Gratis NIS2-scan →

076 – 596 1391
info@daemen-ict.nl

Daemen ICT
De Waterman 5, Rijsbergen · 076 – 596 1391 ·
info@daemen-ict.nl · daemen-ict.nl