NIS2-checklist

Val je onder de Cyberbeveiligingswet — en wat moet je nu doen?

Wet actief sinds 15 augustus 2026 | **Geen overgangsperiode**

OFFICIEEL BEKRACHTIGD

"Het voorstel is op 7 juli 2026 na stemming bij zitten en opstaan aangenomen door de Eerste Kamer" — met nagenoeg unanieme steun (op één fractie na).

Bron: Eerste Kamer der Staten-Generaal, wetsvoorstel Cyberbeveiligingswet, Kamerstuk 36.764 — implementatie van EU-richtlijn 2022/2555 (NIS2)

Wat er op het spel staat als je dit mist

- **Boetes tot €10 miljoen**
  of 2% van je wereldwijde jaaromzet voor essentiële entiteiten; tot €7 mln of 1,4% voor belangrijke entiteiten — wat hoger uitpakt, geldt.
- **Geen overgangstermijn**
  De wet geldt sinds 15 augustus 2026 direct. Handhaving kan vanaf dag één, zonder gewenningsperiode.
- **Bestuurders persoonlijk aansprakelijk**
  Geen aantoonbare stappen gezet om te beoordelen of je onder de wet valt? Dat kan al persoonlijke aansprakelijkheid opleveren, los van de onderneming.
- **Klanten eisen het van jou**
  Opdrachtgevers die zelf onder de wet vallen, stellen beveiliging steeds vaker als contracteis. Geen antwoord kunnen geven kost je de opdracht.

Ruim **8.000 organisaties** in 18 sectoren hebben sinds 15 augustus 2026 nieuwe wettelijke verplichtingen. Deze checklist laat in drie stappen zien waar jij staat — en wat een logische volgende stap is.

1 Val je rechtstreeks onder de wet?

Je valt (waarschijnlijk) onder de Cyberbeveiligingswet als je **allebei** onderstaande vakjes kunt aanvinken.

A. Sector — vink aan wat op jou van toepassing is

- ☐ Energie (elektriciteit, gas, olie, waterstof)
- ☐ Digitale infrastructuur (hosting, cloud, datacenters)
- ☐ ICT-dienstverlening (managed services, IT-beheer)
- ☐ Drinkwater / afvalwater
- ☐ Gezondheidszorg
- ☐ Transport (weg, spoor, lucht, water)
- ☐ Digitale aanbieders (marktplaatsen, zoekmachines, social platforms)
- ☐ Overheid (rijk, provincie, gemeente)
- ☐ Post- en koeriersdiensten
- ☐ Afvalbeheer
- ☐ Chemische productie/distributie
- ☐ Voedselproductie/-distributie
- ☐ Maakindustrie (kritieke producten: medisch, elektronica, machines, auto's)
- ☐ Ruimtevaart
- ☐ Financiële sector (banken, infrastructuur)
- ☐ Onderzoeksinstellingen

B. Omvang — vink aan wat op jou van toepassing is

- ☐ 50 of meer medewerkers
- ☐ Meer dan €10 miljoen jaaromzet én meer dan €10 miljoen balanstotaal

- [ ] Ik ben klein, maar wel: enige aanbieder in mijn sector, DNS-partij, certificaatverstrekker, of gemeente

Beide aangevinkt? Dan val je zeer waarschijnlijk onder de wet — als *essentiële* entiteit (grootste/kritiekste spelers, proactief toezicht, boete tot €10 mln) of als *belangrijke* entiteit (reactief toezicht, boete tot €7 mln).

2 Niet direct verplicht? Check deze 3 signalen

Veel MKB-bedrijven vallen niet rechtstreeks onder de wet, maar krijgen de eisen via via toch op hun bord.

- [ ] **Ketenaansprakelijkheid:** een klant die zelf onder NIS2 valt, stelt eisen aan zijn leveranciers — ook aan jou.
- [ ] **Groeiambitie:** je verwacht binnen 1–2 jaar door de grens van 50 medewerkers of €10 mln omzet te groeien.
- [ ] **Aanbesteding/inkoop:** grotere opdrachtgevers vragen steeds vaker om aantoonbare basisbeveiliging als eis in een offertetraject.

Eén van deze drie herkenbaar? Dan is nu voorsorteren goedkoper dan straks onder tijdsdruk inhalen.

3 Basis-cyberhygiëne — voor iedereen relevant

Of je nu wel of niet onder de wet valt: dit is het fundament dat elke toezichthouder, verzekeraar en grote klant tegenwoordig verwacht.

- [ ] Multi-factor-authenticatie (MFA) overal actief
- [ ] Back-ups: automatisch, getest, offline/immutable
- [ ] Patchmanagement: updates binnen vaste termijn
- [ ] Wachtwoordbeleid + wachtwoordmanager
- [ ] E-mailbeveiliging: SPF, DKIM, DMARC ingesteld
- [ ] Incidentresponsplan: wie doet wat bij een aanval
- [ ] Risicoanalyse van leveranciers/ketenpartners
- [ ] Security-awareness training voor medewerkers
- [ ] Toegangsbeheer: rechten op basis van functie
- [ ] Netwerksegmentatie / gescheiden omgevingen

Jouw uitslag in één oogopslag

Stap 1 = ja
Je bent wettelijk verplicht. Meldplicht en zorgplicht gelden nu al, zonder overgangstermijn.

Stap 2 = ja
Nog niet verplicht, wel kwetsbaar. Voorkom dat een klant of groeimoment je verrast.

Alleen stap 3
Nu geen wettelijke druk — wel de kans om je basis alvast op orde te zetten.

Twijfel je, of wil je zekerheid?

KNDIT vertaalt deze checklist naar een concreet actieplan voor jouw organisatie: wat is verplicht, wat is verstandig, en wat kan wachten. In een gratis NIS2-quickscan (30 min) krijg je duidelijkheid.

Plan je gratis NIS2-quickscan

kndit.nl/nis2 · info@kndit.nl · KNDIT — IT & cybersecurity voor het MKB

Deze checklist is een eerste indicatie, gebaseerd op de Cyberbeveiligingswet (NIS2) en NCSC-informatie (augustus 2026), en vervangt geen juridisch advies. Twijfel over jouw exacte status? Neem contact op met KNDIT of raadpleeg het NCSC-loket.