INFOFICHE · CYBERSECURITY & REGELGEVING

NIS2 in België: wat betekent dit voor uw organisatie?

De Belgische NIS2-wet en het CyberFundamentals-kader van het CCB — in één overzicht.

BRICK9

NIS2 is de Europese richtlijn (EU) 2022/2555 rond cyberveiligheid, in België omgezet door de **wet van 26 april 2024** en van kracht sinds **18 oktober 2024**. Het **Centrum voor Cybersecurity België (CCB)** is de nationale cyberbeveiligingsautoriteit, het nationale CSIRT én de toezichthouder met een eigen inspectiedienst. Waar NIS1 enkele honderden organisaties raakte, vallen nu meer dan 4.000 Belgische entiteiten in scope — en via de toeleveringsketen voelen nog veel meer bedrijven de gevolgen.

1 Valt u onder NIS2?

Twee criteria bepalen dit samen: **uw sector** (18 sectoren, o.a. energie, transport, zorg, digitale infrastructuur, ICT-dienstbeheer, voeding, chemie, afvalbeheer, productie en overheid) en **uw grootte** (vanaf 50 werknemers of €10 mln omzet). Er is geen actieve aanduiding meer: u beoordeelt dit zelf.

Categorie	Toezicht
Essentiële entiteit groot, meest kritieke sectoren	Proactief, regelmatig toezicht. Verplichte conformiteitsbeoordeling door een externe instantie.
Belangrijke entiteit vaak middelgrote spelers	Toezicht achteraf. Geen audit vooraf, maar u moet **aantoonbaar** in orde zijn als het CCB langskomt.

Niet in scope? Toch relevant. NIS2-entiteiten moeten hun toeleveringsketen beoordelen en schuiven die eisen contractueel door naar leveranciers en IT-partners. Het CCB adviseert elke organisatie in de keten om minimaal **CyFun Basic** te halen. Bovendien kan het CCB cruciale organisaties, ongeacht hun omvang, achteraf alsnog aanduiden.

2 De kernverplichtingen

- **Registratie** bij het CCB via het portaal Safeonweb@work.
- **Risicobeheersmaatregelen** (art. 21): risicoanalyse en beveiligingsbeleid, incidentbehandeling, back-up en continuïteit, ketenbeveiliging, patch- en kwetsbaarhedenbeheer, cryptografie, toegangs- en activabeheer, **MFA**, cyberhygiëne en opleiding, plus periodieke evaluatie van de effectiviteit.
- **Meldplicht** bij significante incidenten: **24 u** vroegtijdige waarschuwing → **72 u** incidentmelding → **1 maand** eindrapport. Bij ransomware gelden extra vragen.
- **Verantwoordelijkheid van het bestuur**: de directie keurt de maatregelen goed, houdt toezicht op de uitvoering en volgt zelf opleiding. Persoonlijke aansprakelijkheid is mogelijk.

3 CyberFundamentals (CyFun®)

CyFun is het kader van het CCB dat de wettekst omzet in concrete, controleerbare maatregelen, gebaseerd op NIST CSF 2.0, ISO 27001, de CIS Controls en IEC 62443. Een CyFun- of ISO/IEC 27001-verificatie geeft een **vermoeden van conformiteit**. Drie op vier entiteiten kiest CyFun, omdat het toegankelijker is voor kmo's.

Niveau	Maatregelen	Dekking*	Doelgroep
Small	7 (gratis)	—	micro-organisaties, instapniveau
Basic	34	±82%	kmo's en leveranciers in de keten
Important	±132	±94%	belangrijke entiteiten
Essential	±217	±100%	essentiële entiteiten, kritieke infrastructuur

* Door het CCB geschatte dekking van de meest voorkomende aanvalstechnieken. Elk niveau bouwt op het vorige voort.

Het traject: **(1)** risicobeoordeling en keuze van het niveau, **(2)** zelfevaluatie met bewijsvoering, **(3)** verificatie of certificering door een door BELAC geaccrediteerde conformiteitsbeoordelingsinstantie (CAB). Let op: een CyFun-label alleen is geen volledige NIS2-conformiteit — onder meer de meldtermijnen legt u apart vast in uw procedures.

4 Tijdlijn

18 okt 2024	Belgische NIS2-wet in werking.
18 mrt 2025	Uiterste datum registratie bij het CCB.
18 apr 2026	Essentiële entiteiten leggen hun eerste conformiteitsbeoordeling voor: een CAB-verificatie op niveau Basic of Important, of hun ISO 27001-scope en Verklaring van Toepasselijkheid. Wie het inspectietraject volgt, dient een zelfbeoordeling in.
18 apr 2027	Doelniveau bereikt: volledige Essential- of ISO 27001-certificering, of een voortgangsrapport onder inspectietoezicht. Wie later wordt aangeduid, krijgt dezelfde termijnen (18 en 30 maanden) vanaf de kennisgeving.

5. Sancties. Voor essentiële entiteiten gaan de administratieve boetes tot **€10 mln of 2%** van de wereldwijde jaaromzet, voor belangrijke entiteiten tot **€7 mln of 1,4%**. Daarnaast zijn bindende instructies, openbaarmaking van de inbreuk, tijdelijke schorsing van de dienst en persoonlijke aansprakelijkheid van bestuurders mogelijk. Het CCB stelt zich coachend op, maar wie geen inspanningen kan aantonen, staat zwak.

Hoe Brick9 u hierin begeleidt

1. Scope & nulmeting

Vaststellen of en hoe u in scope valt, keuze van het juiste CyFun-niveau en een gap-analyse van uw omgeving tegenover dat niveau, met prioriteitenlijst en budgettering.

2. Technische remediëring

Identiteit en MFA/conditionele toegang, endpointbescherming en 24/7 detectie, next-gen firewall en segmentatie, back-up en herstelbaarheid, patchbeheer, logging en monitoring.

3. Bewijs & volhouden

Beleid en procedures, incidentresponsplan met de 24/72-uursflow, gedocumenteerd bewijs per maatregel, awarenesstraining en begeleiding tot en met de CAB-verificatie.

Bronnen: ccb.belgium.be · atwork.safeonweb.be · wet van 26 april 2024 (NIS2) en het uitvoerend koninklijk besluit. | Deze fiche is informatief en algemeen van aard, opgemaakt in juli 2026, en vormt geen juridisch advies; uw concrete verplichtingen hangen af van uw sector, omvang en risicobeoordeling. | **Brick9** · brick9.com — vragen of een vrijblijvende NIS2-scan? Neem contact op met uw accountmanager.