

Nieuwe strengere regels gaan van toepassing voor de cyber- en fysieke veerkracht van kritieke entiteiten en netwerken

Twee belangrijke richtlijnen over kritieke en digitale infrastructuur zijn onlangs in werking getreden en zullen de EU beter bestand maken tegen online- en offline-dreigingen, van cyberaanvallen tot criminaliteit, risico's voor de volksgezondheid of natuurrampen.



iStock photo Getty images plus

Recente bedreigingen voor de kritieke infrastructuur van de EU hebben geprobeerd onze collectieve veiligheid te ondermijnen. Reeds in 2020 had de Commissie voorgesteld de EU-regels inzake de veerkracht van kritieke entiteiten en de beveiliging van netwerk- en informatiesystemen aanzienlijk te verbeteren.

De 2 richtlijnen die in werking treden, zijn:

- **[Richtlijn betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie \(NIS 2-richtlijn\)](https://eur-lex.europa.eu/eli/dir/2022/2555)** (<https://eur-lex.europa.eu/eli/dir/2022/2555>)
- **[Richtlijn betreffende de veerkracht van kritieke entiteiten \(CER-richtlijn\)](https://eur-lex.europa.eu/eli/dir/2022/2557/oj)** (<https://eur-lex.europa.eu/eli/dir/2022/2557/oj>)

De NIS 2-richtlijn zal zorgen voor een **veiliger en sterker Europa** door de **sectoren en soorten kritieke entiteiten die onder het toepassingsgebied ervan vallen aanzienlijk uit te breiden.**

Het gaat onder meer om aanbieders van openbare elektronische-communicatienetwerken en -diensten, datacentra, afvalwater- en afvalbeheer, de productie van kritieke producten, post- en koeriersdiensten en overheidsinstanties, alsook de gezondheidszorg in ruimere zin. Voorts zullen de **vereisten inzake risicobeheer op het gebied van cyberbeveiliging waaraan bedrijven moeten voldoen, worden aangescherpt** en zullen de verplichtingen inzake melding van incidenten worden gestroomlijnd met **preciezer bepalingen inzake rapportage, inhoud en tijdschema**. De NIS2-richtlijn vervangt de [regels inzake de beveiliging van netwerk- en informatiesystemen](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG&oc=OJ%3AL%3A2016%3A194%3ATOC) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG&oc=OJ%3AL%3A2016%3A194%3ATOC), de eerste EU-brede wetgeving inzake cyberbeveiliging.

Tegen de achtergrond van een steeds complexer risicolandschap vervangt de nieuwe **CER-richtlijn** de richtlijn Europese kritieke infrastructuur van 2008. De nieuwe regels zullen kritieke infrastructuur weerbaarder maken tegen een reeks bedreigingen, waaronder natuurrampen, terroristische aanslagen, dreigingen van binnenuit of sabotage. Er zullen 11 **sectoren** worden bestreken: energie, vervoer, bankwezen, infrastructuur van de financiële markten, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur, ruimtevaart en voedsel. De lidstaten zullen een **nationale strategie** moeten vaststellen en **regelmatig risicobeoordelingen** moeten uitvoeren om vast te stellen welke entiteiten als cruciaal of essentieel voor de samenleving en de economie worden beschouwd.

De lidstaten hebben 21 maanden de tijd om beide richtlijnen in nationaal recht om te zetten. Gedurende deze periode stellen de lidstaten de maatregelen vast die nodig zijn om hieraan te voldoen en maken zij deze bekend.

In december 2022 heeft de Raad een **aanbeveling** (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6238) aangenomen **over een EU-wijde coördinatieaanpak om de veerkracht van kritieke infrastructuur te versterken**, waarbij de lidstaten wordt verzocht vaart te zetten achter de voorbereidende werkzaamheden voor de omzetting en toepassing van NIS 2 en van de richtlijn betreffende de veerkracht van kritieke entiteiten (CER).

Meer informatie

- [NIS2-richtlijn](https://digital-strategy.ec.europa.eu/en/news/new-stronger-cybersecurity-rules-kicking-safer-e-u-digital-landscape)
(<https://digital-strategy.ec.europa.eu/en/news/new-stronger-cybersecurity-rules-kicking-safer-e-u-digital-landscape>)
- [NIS-vraag a\)](https://digital-strategy.ec.europa.eu/en/faqs/revision-network-and-information-security-directive-questions-and-answers)
(<https://digital-strategy.ec.europa.eu/en/faqs/revision-network-and-information-security-directive-questions-and-answers>)
- [Factsheet over netwerk- en informatiebeveiliging](https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2)
(<https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2>)
- [CER-richtlijn](https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en)
(https://home-affairs.ec.europa.eu/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en)

Dit is een machinevertaling die door de Europese Unie wordt verstrekt. □ De dienst eTranslation van de Commissie helpt u deze pagina te begrijpen. □ [Alstublieft □ lees de gebruiksvoorwaarden](https://ec.europa.eu/info/use-machine-translation-europa-exclusion-liability_en) (https://ec.europa.eu/info/use-machine-translation-europa-exclusion-liability_en). Om de oorspronkelijke versie te lezen, □ [zie de brontekst](https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resil) (<https://digital-strategy.ec.europa.eu/en/news/new-stronger-rules-start-apply-cyber-and-physical-resil>)

[ience-critical-entities-and-networks](#)).

Source URL:

<https://digital-strategy.ec.europa.eu/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks>

© European Union, 2025 - [Shaping Europe's digital future \(https://digital-strategy.ec.europa.eu/nl\)](https://digital-strategy.ec.europa.eu/nl) - PDF generated on 08/04/2025

Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license).

For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.