ICTRECHT

FACTSHEET

CER/ Wet weerbaarheid kritieke entiteiten (Wwke)

Alles wat je moet weten over de nieuwe regels voor fysieke weerbaarheid

Scope

Wat is de Wet weerbaarheid kritieke entiteiten?

De Wwke is de Nederlandse implementatie van de Europese CER-richtlijn (Richtlijn (EU) 2022/2557 betreffende de weerbaarheid van kritieke entiteiten). De wet is gericht op het **in stand houden van vitale maatschappelijke functies en economische activiteiten** door de weerbaarheid van kritieke entiteiten en hun vermogen om essentiële diensten te verlenen te versterken.

De Wwke is de fysieke tegenhanger van de Cyberbeveiligingswet (Cbw/NIS2): waar de Cbw zich richt op digitale weerbaarheid, richt de Wwke zich op alle overige risico's en dreigingen, zoals natuurrampen, sabotage, terrorisme en hybride dreigingen. De Wwke is uitdrukkelijk niet van toepassing op aangelegenheden die onder de Cyberbeveiligingswet vallen.

Doelstellingen

De wet richt zich op de volgende pijlers:

Risicobeoordeling
Identificeren en beoordelen van relevante (niet-cyber) risico's voor essentiële diensten.

Weerbaarheidsmaatregelen
Nemen van passende technische, beveiligings- en organisatorische maatregelen.

Incidentmelding
Melden van significante verstoringen van essentiële diensten.

Samenwerking & informatie-uitwisseling
Delen van informatie en beste praktijken tussen bevoegde autoriteiten en kritieke entiteiten, ook grensoverschrijdend.

Sectoren (bijlage bij de wet):

De Wwke is van toepassing op entiteiten in de sectoren zoals opgenomen in de bijlage bij de wet:

Sectoren Wwke (bijlage bij de wet)

- Energie (elektriciteit, stadsverwarming/-koeling, olie, gas, waterstof)
- Vervoer
- Bankwezen
- Infrastructuur voor de financiële markt
- Gezondheidszorg
- Drinkwater
- Afvalwater
- Digitale infrastructuur
- Overheid
- Ruimtevaart
- Productie, verwerking en distributie van levensmiddelen

Daarnaast kunnen bij algemene maatregel van bestuur op grond van artikel 7, eerste lid, aanvullende sectoren worden aangewezen.

Voor wie?

De Wwke is van toepassing op kritieke entiteiten: entiteiten die door de bevoegde autoriteit als zodanig zijn aangewezen omdat zij één of meer essentiële diensten verlenen binnen één van de sectoren uit de bijlage bij de wet.

Een entiteit wordt (op basis van de CER-richtlijn waarop de Wwke is gebaseerd) aangewezen als kritieke entiteit wanneer:

1. Zij een essentiële dienst verleent in een sector uit de bijlage;
2. Zij actief is op het Nederlandse grondgebied; én
3. Een incident een significant verstorend effect zou hebben op het verlenen van één of meer essentiële diensten in Nederland of andere lidstaten.

Uitgezonderd:
De wet is niet van toepassing op:

- Het Ministerie van Defensie;
- De inlichtingen- en veiligheidsdiensten (Wiv 2017);
- Het openbaar ministerie;
- De politie;
- De veiligheidsregio's (artikel 9 Wet veiligheidsregio's);
- Overige bij AMvB aangewezen overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving (inclusief opsporing en vervolging van strafbare feiten).

Ook aangelegenheden die onder de Cyberbeveiligingswet vallen, vallen buiten de Wwke.

Let op: samenloop met Cbw/NIS2:
Wanneer je aangewezen wordt als kritieke entiteit onder de Wwke, dan is de Cbw automatisch van toepassing. Ook als je niet aan de toepassingscriteria voldoet van de Cbw.

Kritieke entiteit: aanwijzing en lijst

Anders dan de Cbw (waarbij organisaties zelf beoordelen of zij onder de wet vallen), werkt de Wwke met een **aanwijzingssysteem door de bevoegde autoriteit.**

Wie bepaalt?

De bevoegde autoriteit wijst kritieke entiteiten aan.

Basis

Verlenen van een essentiële dienst + significant verstorend effect bij incident.

Lijst

De bevoegde autoriteit stelt een lijst van kritieke entiteiten op en actualiseert deze **ten minste elke vier jaar** of vaker indien nodig.

Rol van de bevoegde autoriteit

De bevoegde autoriteit (aangewezen op grond van artikel 8) ondersteunt kritieke entiteiten actief. Samenwerking bestaat in ieder geval uit het uitwisselen van informatie en beste praktijken, en kan, na overleg met de Minister, tevens omvatten:

A) het ontwikkelen van richtsnoeren en methodologieën;

B) het verlenen van bijstand in crisis- of noodsituaties;

C) het helpen bij de organisatie van oefeningen om de weerbaarheid te testen;

D) het verstrekken van advies aan personeel van kritieke entiteiten;

E) het geven van opleidingen aan personeel van kritieke entiteiten.

Centraal contactpunt

De Minister van Justitie en Veiligheid is het centrale contactpunt en heeft de volgende taken:

- Verbindingsfunctie met de Europese Commissie;
- Grensoverschrijdende samenwerking met centrale contactpunten van andere EU-lidstaten en met de Groep voor de weerbaarheid van kritieke entiteiten (artikel 19 CER-richtlijn);
- Samenwerking met bevoegde autoriteiten van derde landen;
- Zorgdragen voor sectoroverstijgende en doeltreffende samenwerking tussen de bevoegde autoriteiten binnen Nederland.

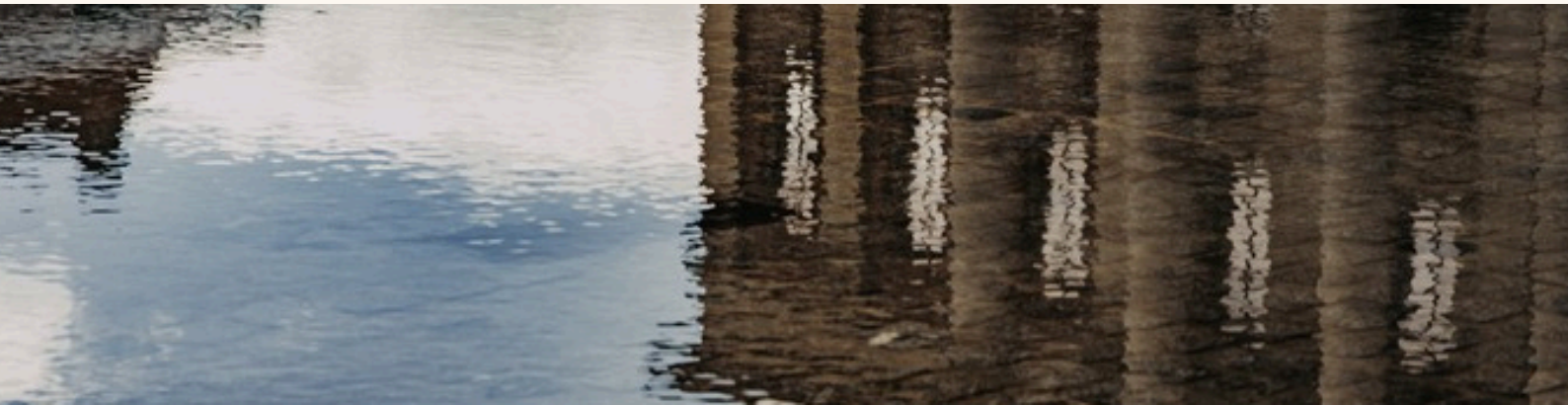
Verplichtingen

Nationale strategie

De Minister van Justitie en Veiligheid stelt, in overeenstemming met de betrokken ministers, een strategie inzake de weerbaarheid van kritieke entiteiten vast. Deze strategie bevat ten minste:

Element	Toelichting
Doelstellingen & prioriteiten	Met inachtneming van grensoverschrijdende en intersectorale afhankelijkheden.
Governancekader	Taken en verantwoordelijkheden van autoriteiten, kritieke entiteiten en andere partijen.
Maatregelen	Inclusief beschrijving van de risicobeoordelingen (artikel 9).
Identificatieproces	Hoe kritieke entiteiten worden geïdentificeerd.
Ondersteunings-proces	Inclusief publiek-private samenwerking.
Autoriteiten & stakeholders	Lijst van belangrijkste betrokken partijen.
Coördinatiekader	Coördinatie met de bevoegde autoriteit onder de Cbw (art. 15 Cyberbeveiligingswet) voor info-uitwisseling over cyber én niet-cyber risico's.
MKB-ondersteuning	Maatregelen om naleving voor kleine en middelgrote kritieke entiteiten te vergemakkelijken.

De strategie wordt **ten minste elke vier jaar** geactualiseerd, na consultatie van relevante partijen.



Verplichtingen voor kritieke entiteiten (artikelen 14, 15, 17)

Kritieke entiteiten moeten (nader uitgewerkt in de wet en onderliggende regelgeving):

Verplichting	Toelichting
Risicobeoordeling	Uitvoeren van een risicobeoordeling van alle relevante (niet-cyber) risico's die essentiële diensten kunnen verstoren.
Weerbaarheids-maatregelen	Nemen van passende en evenredige technische, beveiligings- en organisatorische maatregelen ter voorkoming, bescherming, reactie, weerstand, beperking, herstel en aanpassing.
Incidentmelding	Melden van incidenten die het verlenen van essentiële diensten significant verstoren of kunnen verstoren.
Achtergrondscreening	Kunnen uitvoeren van achtergrondscreenings voor bepaalde functies (voor zover voorzien in nadere regelgeving).
Contactpersoon	Aanwijzen van een verbindingsfunctionaris richting de bevoegde autoriteit.

Uitvoeringshandelingen en gedelegeerde handelingen

Bij of krachtens AMvB kunnen aanvullende regels worden gesteld ter uitvoering van de op grond van de CER-richtlijn vastgestelde uitvoeringshandelingen, gedelegeerde handelingen en richtsnoeren. Houd deze onderliggende regelgeving dus goed in de gaten.

Meldplicht bij incidenten

Kritieke entiteiten melden significante incidenten bij de bevoegde autoriteit. Een incident is significant wanneer het het verlenen van essentiële diensten aanzienlijk verstoort of kan verstoren. De concrete drempelwaarden en meldtermijnen worden nader ingevuld bij AMvB / ministeriële regeling.

Let op:
Wanneer een incident ook een cyberincident betreft, kan er tevens een meldplicht bestaan onder de Cyberbeveiligingswet. En bij een datalek geldt daarnaast de meldplicht bij de Autoriteit Persoonsgegevens.

Toezicht, sancties en tijdslijn

Toezicht

De bevoegde autoriteit (aangewezen op grond van artikel 8 Wwke) houdt toezicht op de naleving van de verplichtingen door kritieke entiteiten. Zij werkt daarbij nauw samen met de bevoegde autoriteit onder de Cyberbeveiligingswet, met het oog op het delen van informatie over zowel cyber- als niet-cybergerelateerde risico's, dreigingen en incidenten.

Sanctieregime

Bij niet-naleving kan de bevoegde autoriteit onder meer de volgende instrumenten inzetten:

Sanctie	Toelichting
Waarschuwing	Bij minder ernstige overtredingen
Bindende aanwijzingen	Verplichte instructies om naleving te bereiken
Last onder dwangsom	Dwangsom tot naleving is bereikt
Bestuurlijke boete	Financiële sanctie (hoogte nader te bepalen bij / krachtens de wet)

De concrete maximale boetehoogtes voor de Wwke wijken af van die onder de Cbw en dienen te worden geverifieerd in de specifieke boetebepalingen van de wet en onderliggende regelgeving.

Relatie met de Cyberbeveiligingswet

Beide wetten vullen elkaar aan:

Aspect	Wwke
Focus	Fysieke / niet-cyber weerbaarheid
EU-basis	CER-richtlijn (2022/2557)
Aanwijzing	Door bevoegde autoriteit
Coördinatie	Verplicht coördinatiekader tussen beide bevoegde autoriteiten

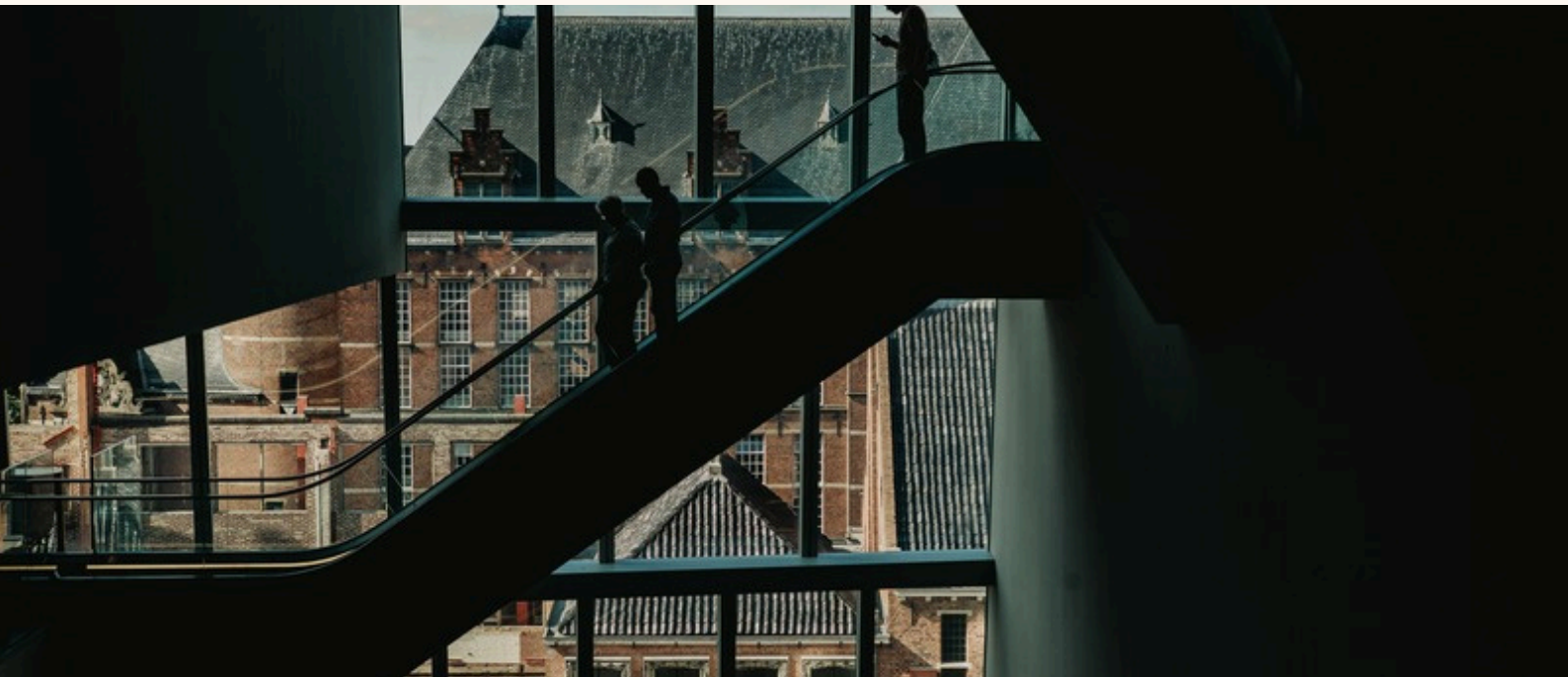
Tijdslijn:

Datum	Gebeurtenis
14 december 2022	CER-richtlijn (EU) 2022/2557 vastgesteld
17 oktober 2024	Uiterste implementatiedatum CER-richtlijn (Nederland heeft vertraging)
Juni 2025	Wetsvoorstel ingediend bij de Tweede Kamer
15 april 2026	Tweede Kamer stemt in met de Wet weerbaarheid kritieke entiteiten
7 juli 2026	Eerste Kamer stemt in met de Wet weerbaarheid kritieke entiteiten
15 augustus 2026	Wet weerbaarheid kritieke entiteiten wordt van kracht

Aanbevolen acties wanneer je aangewezen wordt:

1. Voer een GAP-analyse uit op fysieke en organisatorische weerbaarheid (naast bestaande cyberanalyses);
2. Stel een all-hazards risicobeoordeling en implementatieplan op;
3. Richt de coördinatie tussen je Wwke- en Cbw-compliance in (governance, meldprocedures, contactpersonen);
4. Bereid registratie-, meld- en achtergrondscreeningsprocedures voor.

Dit zijn acties waar ICTRecht mee kan helpen.



ICTRECHT

Benieuwd wat wij voor jouw organisatie kunnen betekenen?

Bezoek onze website voor meer informatie.

www.ictrecht.nl/CER
020 - 663 1941