w  wet

w  weerbaarheid

k  kritieke

e  entiteiten

Wet weerbaarheid kritieke entiteiten

Handreiking voor kritieke entiteiten

augustus 2026

Inleiding

Om de weerbaarheid van Europese lidstaten te versterken heeft de Europese Unie eind 2022 de Critical Entities Resilience Directive (CER-richtlijn) vastgesteld. Het doel van deze richtlijn is om kritieke infrastructuur en essentiële diensten in Europa beter te beschermen tegen risico's die de continuïteit daarvan kunnen verstoren. Denk hierbij aan sabotage, natuurrampen, noodsituaties op het gebied van de volksgezondheid of andere incidenten met een grote maatschappelijke impact.

In Nederland is de CER-richtlijn uitgewerkt in de Wet weerbaarheid kritieke entiteiten (Wwke).

De Wwke heeft als doel de weerbaarheid te vergroten van organisaties die essentiële diensten verlenen in Nederland. Deze organisaties zijn aangemerkt als kritieke entiteit.
Het gaat om de weerbaarheid tegen uiteenlopende dreigingen en risico's, zoals natuurrampen en ongevallen, maar ook (terroristische) misdrijven en sabotage, die de levering van essentiële diensten aanzienlijk kunnen verstoren.

Cyberbeveiligingswet

Naast de Wwke is ook de herziening van de Europese Network and Information Security Directive (NIS2-richtlijn) in Nederlandse wetgeving omgezet via de Cyberbeveiligingswet (Cbw). De Cyberbeveiligingswet richt zich op de digitale weerbaarheid van organisaties. De Wwke heeft een all-hazard benadering. Dit betekent dat organisaties zich richten op de fysieke, organisatorische en andere risico's die essentiële diensten kunnen verstoren. Beide wetten vullen elkaar aan en dragen bij aan een weerbare samenleving.

Voor welke organisaties geldt de Wwke?

De Wwke is van toepassing op organisaties die essentiële diensten verlenen binnen verschillende sectoren.

Verantwoordelijke ministeries beoordelen welke organisaties als kritieke entiteit worden aangewezen. Daarbij kijken zij onder meer naar de mogelijke gevolgen die een verstoring van de dienstverlening kan hebben voor maatschappelijke functies, economische activiteiten, de volksgezondheid, de openbare veiligheid of het milieu.

Meer informatie over de sectoren waarop de Wwke op dit moment van toepassing is en de criteria voor aanwijzing is te vinden op de **website** van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Voor **sectorspecifieke vragen** over de toepassing van de Wwke kunnen organisaties terecht bij het ministerie dat verantwoordelijk is voor hun sector.

Voor wie is deze handreiking bedoeld?

Deze handreiking helpt organisaties die zijn aangewezen als kritieke entiteit om te begrijpen welke verplichtingen gelden, welke termijnen belangrijk zijn en welke ondersteuning beschikbaar is.

Voor welke sectoren geldt de Wwke?

Inhoud

w  wet

w  weerbaarheid

k  kritieke

e  entiteiten

1.

U bent aangewezen als kritieke entiteit: wat nu?

Wat houdt de Wet weerbaarheid kritieke entiteiten in?

Uw organisatie is aangewezen als kritieke entiteit onder de Wet weerbaarheid kritieke entiteiten (Wwke) door de voor uw sector verantwoordelijke vakminister. Met deze aanwijzing gelden voor uw organisatie verschillende wettelijke verplichtingen. Ook kan uw organisatie gebruikmaken van ondersteuning om de weerbaarheid van essentiële diensten te versterken.

In dit hoofdstuk leest u welke stappen uw organisatie moet zetten na de aanwijzing en welke verplichtingen en ondersteuningsmogelijkheden daarbij horen.

Wat zijn de belangrijkste onderdelen van de Wet weerbaarheid kritieke entiteiten?

Voer een risicobeoordeling uit

Voldoe aan de zorgplicht

Voldoe aan de meldplicht

Maak gebruik van ondersteuning

Toezicht en handhaving

Wat betekent de Wwke voor uw organisatie?

Hieronder vindt u een overzicht van de belangrijkste stappen en de bijbehorende verplichtingen. Daarnaast zijn er nog overige verplichtingen, waaronder het aanwijzen van een verbindingsfunctionaris.

Stap 1: Voer een risicobeoordeling uit

Binnen negen maanden na de aanwijzing moet uw organisatie een eigen risicobeoordeling uitvoeren. Hiermee brengt uw organisatie in kaart welke risico's de continuïteit van uw essentiële diensten kunnen verstoren en welke gevolgen deze risico's kunnen hebben.

Meer informatie hierover staat in hoofdstuk 2.

Stap 2: Voldoe aan de zorgplicht

Binnen tien maanden na de aanwijzing moet uw organisatie passende technische, organisatorische en fysieke maatregelen hebben getroffen om de weerbaarheid van uw essentiële diensten te vergroten.

Meer informatie hierover staat in hoofdstuk 3.

Stap 3: Voldoe aan de meldplicht

Als kritieke entiteit bent u verplicht binnen 24 uur incidenten te melden die een aanzienlijke verstoring veroorzaken of kunnen veroorzaken van uw essentiële diensten. Het doel van de melding is om de bevoegde autoriteit, bestaande uit het verantwoordelijke ministerie en de toezichthouder, in staat te stellen om te reageren op incidenten en waar nodig en mogelijk kan het ministerie ondersteuning bieden aan uw organisatie.

Meer informatie hierover staat in hoofdstuk 4.

Stap 4: Maak gebruik van ondersteuning

Als kritieke entiteit kunt u gebruikmaken van verschillende vormen van ondersteuning die de overheid mogelijk maakt. Denk hierbij aan informatie over dreigingen en risico's, waarschuwingen en andere hulpmiddelen die bijdragen aan het versterken van de weerbaarheid van uw organisatie. De beschikbare ondersteuning kan verschillen per sector.

Meer informatie hierover staat in hoofdstuk 5.

Stap 5: Toezicht en handhaving

De bevoegde autoriteit houdt toezicht op de naleving van de Wwke. Deze kan informatie opvragen of onderzoeken uitvoeren om te beoordelen of aan de wettelijke verplichtingen wordt voldaan.

Meer informatie hierover staat in hoofdstuk 6.

Van aanwijzing naar naleving

Termijn	*Verplichting*
Dag 1	Ontvangst aanwijzingsbrief
Binnen 9 maanden	Risicobeoordeling uitvoeren
Binnen 10 maanden	Voldoen aan de zorgplicht en meldplicht
Doorlopend	Incidenten melden en maatregelen actueel houden
Iedere vier jaar	Evalueren van uw risicobeoordeling - ten minste iedere vier jaar of eerder wanneer ontwikkelingen daartoe aanleiding geven.

Let op:
uw organisatie valt ook onder de Cyberbeveiligingswet

Alle organisaties die als kritieke entiteit zijn aangewezen onder de Wwke, worden automatisch aangemerkt als essentiële entiteit onder de **Cyberbeveiligingswet** (Cbw).

Andersom geldt dit niet: een essentiële entiteit onder de Cyberbeveiligingswet is niet automatisch een kritieke entiteit. Daarvoor is een formele aanwijzing door het verantwoordelijke ministerie nodig.

Door de aanwijzing als kritieke entiteit en de automatische kwalificatie als essentiële entiteit zijn ook de rechten en verplichtingen van de Cbw die gelden voor essentiële entiteiten van toepassing op uw organisatie. Dit betekent onder meer dat uw organisatie zich moet registreren in het **MijnNCSC-portaal**. Meer informatie over de stappen en verplichtingen onder de Cbw is te vinden op de **website** van de NCTV.

2.

Voer een risicobeoordeling uit

Voer een risicobeoordeling uit

Binnen negen maanden nadat uw organisatie is aangewezen als kritieke entiteit, moet u een risicobeoordeling uitvoeren. Hiermee brengt u in kaart welke risico's de continuïteit van uw essentiële diensten kunnen bedreigen en welke maatregelen nodig zijn om deze risico's te beheersen. Het is belangrijk om deze beoordeling schriftelijk vast te leggen.

Wat is een risicobeoordeling?

Met een risicobeoordeling brengt u de dreigingen, kwetsbaarheden en gevaren in kaart die kunnen leiden tot een incident. Daarnaast beoordeelt u welke impact een incident kan hebben op de verlening van uw essentiële diensten. Deze beoordeling geeft inzicht in het huidige weerbaarheidsniveau van uw organisatie en de maatregelen die nog nodig zijn om risico's te beperken en de weerbaarheid te versterken.

Wat brengt u in kaart?

In de risicobeoordeling brengt u in ieder geval in kaart:

- welke dreigingen en risico's de continuïteit van uw essentiële diensten kunnen verstoren;
- hoe groot de impact van een incident op uw dienstverlening kan zijn;
- welke maatregelen nodig zijn om risico's te voorkomen, beperken of beheersen;
- wat het huidige weerbaarheidsniveau van uw organisatie is.

Let op: sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur zijn uitgezonderd van de verplichting tot het uitvoeren van een risicobeoordeling.

De risicobeoordeling helpt u inzicht te krijgen in de kwetsbaarheden van uw organisatie en vormt de basis voor de maatregelen die u neemt om de weerbaarheid verder te versterken.

Welke informatie gebruikt u?

De manier waarop u de risicobeoordeling uitvoert is vormvrij. Het is belangrijk dat u bij de risicobeoordeling in ieder geval de informatie betrekt die u van uw ministerie hebt ontvangen. Deze informatie heeft ertoe geleid dat u bent aangewezen als kritieke entiteit. U kunt hiervoor aansluiten bij bestaande processen en documenten binnen uw organisatie, zoals:

- bestaande risicomanagementsystemen en risicoanalyses met daarbinnen bijvoorbeeld een business impact analyse (BIA);
- risicoanalyses die zijn uitgevoerd in het kader van de Cyberbeveiligingswet;
- andere bestaande risicomanagementprocessen.

Met welke risico's houdt u rekening?

Bij de risicobeoordeling houdt u in ieder geval rekening met:

- risico's van sectoroverstijgende of grensoverschrijdende aard;
- ongevallen;
- natuurrampen;
- noodsituaties op het gebied van de volksgezondheid;
- hybride dreigingen of andere opzettelijke dreigingen, zoals terroristische misdrijven.

Evalueren en actualiseren

De risicobeoordeling evalueert u ten minste iedere vier jaar, of eerder wanneer ontwikkelingen of incidenten daartoe aanleiding geven. Wanneer nodig past uw organisatie de risicobeoordeling en het daarop gebaseerde beleid aan.

3.

Voldoe aan de zorgplicht

Voldoe aan de zorgplicht

Als kritieke entiteit ben u verplicht passende en evenredige maatregelen te nemen om risico's voor uw organisatie te beperken en de weerbaarheid van uw essentiële diensten te vergroten. De zorgplicht geldt vanaf tien maanden nadat uw organisatie is aangewezen als kritieke entiteit.

Wat is het doel van de zorgplicht?

Het doel van de zorgplicht is om de weerbaarheid van uw organisatie en de continuïteit van de essentiële diensten te versterken. Door passende en evenredige maatregelen te nemen, kunnen incidenten zoveel mogelijk worden voorkomen. Als zich toch een incident voordoet, helpen deze maatregelen om de gevolgen te beperken, de dienstverlening zo veel mogelijk in stand te houden en na een incident zo snel mogelijk te herstellen.

De maatregelen die u neemt, zijn gebaseerd op:

- de resultaten van uw eigen risicobeoordeling;
- de relevante informatie uit de sectorale risicobeoordeling die u van uw ministerie hebt ontvangen;
- relevante waarschuwingen, adviezen en informatie van andere organisaties.

De zorgplicht is opgenomen in de Wet weerbaarheid kritieke entiteiten (Wwke) en is verder uitgewerkt in **onderliggende regelgeving**, zoals het Besluit weerbaarheid kritieke entiteiten. Hierin worden maatregelen beschreven waaraan kritieke entiteiten in ieder geval aandacht moeten besteden. Deze maatregelen vormen een algemeen kader.

Op basis van de uitkomsten van uw risicobeoordeling en de sectorale risicobeoordeling die u van uw ministerie heeft ontvangen, bepaalt u welke maatregelen passend en evenredig zijn voor uw organisatie en de essentiële diensten die u verleent. De getroffen maatregelen legt u schriftelijk vast.

Let op: de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur zijn uitgezonderd van de zorgplicht voor de Wwke, omdat zij al soortgelijke verplichtingen kennen uit andere regelgeving. Organisaties in de sector digitale infrastructuur moeten wel voldoen aan de zorgplicht voor de Cyberbeveiligingswet.

Passende en evenredige maatregelen

Niet iedere maatregel is voor iedere organisatie op dezelfde manier van toepassing. De Wwke, inclusief de onderliggende regelgeving, bevat een algemeen kader met maatregelen waaraan kritieke entiteiten aandacht moeten besteden. Voor de concrete invulling is ruimte voor een eigen afweging.

Uw organisatie bepaalt zelf welke maatregelen redelijkerwijs nodig zijn om risico's te beheersen. Daarbij houdt u onder meer rekening met:

- de uitkomsten van uw risicobeoordeling;
- de mate waarin uw organisatie is blootgesteld aan risico's;
- de omvang van uw organisatie;
- de kans dat zich incidenten voordoen;
- de mogelijke impact op de maatschappij en economie;
- de verhouding tussen de kosten van een maatregel en het beoogde effect daarvan.

Een passende maatregel kan daardoor per organisatie verschillen.

Onderwerpen waarop uw organisatie maatregelen moet nemen

De maatregelen die kritieke entiteiten in het kader van de zorgplicht moeten nemen, zijn nader uitgewerkt in het **Besluit weerbaarheid kritieke entiteiten (Bwke)**. Hierbij moet uw organisatie in ieder geval maatregelen treffen op de volgende onderwerpen:

Kritieke infrastructuur

- Identificeer uw kritieke infrastructuur (een voorziening, een faciliteit, apparatuur, een netwerk of een systeem of onderdelen daarvan die noodzakelijk zijn voor de verlening van een essentiële dienst) en houd hiervan een actueel overzicht bij;
- Leg het beheer van deze infrastructuur vast in beleid;
- Stel beleid op voor het verwerven, ontwikkelen, onderhouden, herstellen en beëindigen van kritieke infrastructuur.

Leveranciers en dienstverleners

- Identificeer de rechtstreekse leveranciers en dienstverleners die van belang zijn voor uw essentiële dienstverlening;
- Stel beleid vast over hun rol ten aanzien van de essentiële diensten en de weerbaarheid daarvan.

Fysieke beveiliging

Neem passende maatregelen voor de bescherming van gebouwen en kritieke infrastructuur, zoals:

- het instellen van beveiligingszones;
- het inrichten van toegangsbeveiliging;
- het beveiligen van kantoren, ruimten, faciliteiten, bedrijfsmiddelen buiten het terrein en nutsvoorzieningen;
- het monitoren van de beveiliging;
- het veilig plaatsen en beschermen van kritieke apparatuur. Denk bijvoorbeeld aan servers, procesbesturingssystemen, netwerkapparatuur of andere systemen die essentieel zijn voor de verlening van de essentiële dienst.

Personeelsbeveiliging

Breng de rollen, bevoegdheden en verantwoordelijkheden van medewerkers die verantwoordelijk zijn voor de weerbaarheid van uw organisatie in kaart en leg dit vast in beleid.

Denk hierbij onder meer aan:

- het identificeren van personeelsleden met kritieke functies;
- het vaststellen van toegangsrechten;
- regelmatige bewustwordings- en opleidingsactiviteiten;
- oefeningen voor personeel.

Crisisbeheersing en bedrijfscontinuïteit

Zorg voor vastgestelde plannen voor:

- het beheersen van crises en incidenten;
- het waarborgen van de continuïteit van de essentiële diensten.

Bescherming van gevoelige informatie

Neem maatregelen om de beveiliging, integriteit en vertrouwelijkheid van gevoelige informatie die van belang is voor de weerbaarheid van uw organisatie te waarborgen.

Bestaande maatregelen als uitgangspunt

Beschikt uw organisatie al over vergelijkbare maatregelen, beleid, procedures of plannen? Dan kan dit een goede basis vormen om te voldoen aan de verplichtingen uit de Wwke.

Het blijft daarbij belangrijk om rekening te houden met de risico's uit zowel de sectorale risicobeoordeling van het ministerie als de risicobeoordeling van uw eigen organisatie. Daarbij wordt uitgegaan van een zogenoemde all-hazard benadering, waarbij rekening wordt gehouden met alle typen dreigingen.

Evalueren en actualiseren

De risicobeoordeling en de getroffen maatregelen evalueert u ten minste iedere vier jaar, of eerder wanneer ontwikkelingen of incidenten daartoe aanleiding geven. Daarbij toetst u ook of de maatregelen nog doeltreffend zijn en aansluiten bij de actuele risico's voor uw organisatie.

4.

Voldoe aan de meldplicht

Voldoe aan de meldplicht

De Wet weerbaarheid kritieke entiteiten (Wwke) verplicht kritieke entiteiten om incidenten te melden die de verlening van hun essentiële diensten aanzienlijk verstoren of kunnen verstoren. De meldplicht geldt vanaf tien maanden nadat uw organisatie is aangewezen als kritieke entiteit.

Hoe werkt de meldplicht?

De meldplicht bestaat uit twee fasen:

- een eerste melding binnen 24 uur nadat uw organisatie kennis heeft genomen van het incident;
- een gedetailleerd eindverslag binnen één maand na de eerste melding.

Meldingen doet u via het **MijnNCSC-portaal.**

Welke incidenten moet u melden?

De meldplicht geldt voor incidenten die de verlening van uw essentiële diensten aanzienlijk verstoren of kunnen verstoren. Dit kunnen zowel fysieke als digitale incidenten zijn.

Om te bepalen of een verstoring significant is, wordt onder andere gekeken naar:

- het aantal getroffen gebruikers;
- de duur van de verstoring;
- het getroffen geografische gebied;

De exacte drempelwaarden verschillen per sector en zijn uitgewerkt in **ministeriële regelingen**.

Kritieke entiteiten worden daarnaast aangemoedigd om vrijwillige meldingen te doen, bijvoorbeeld van incidenten die relevant kunnen zijn voor de weerbaarheid van de sector. Deze meldingen kunnen bijdragen aan een beter inzicht in dreigingen en risico's en daarmee aan het versterken van de weerbaarheid van de sector.

Waar doet u een melding?

U doet een melding via het centrale meldpunt op **MijnNCSC.nl**.
Dit is hetzelfde portaal dat wordt gebruikt voor meldingen onder de **Cyberbeveiligingswet**. Via dit centrale meldpunt kunnen kritieke entiteiten meldingen doen voor zowel de Cyberbeveiligingswet als de Wet weerbaarheid kritieke entiteiten.

Let op: de sectoren bankwezen, infrastructuur voor de financiële markt en digitale infrastructuur zijn uitgezonderd van de meldplicht voor de Wwke, omdat zij al soortgelijke verplichtingen kennen uit andere regelgeving. Organisaties in de sector digitale infrastructuur moeten wel voldoen aan de meldplicht voor de Cyberbeveiligingswet.

Uw organisatie dient zich voor dit portaal te registreren. Meer informatie over registratie kunt u vinden op de **website** van het NCSC.

Let op: zolang uw organisatie deze registratie niet heeft voltooid, kunnen geen meldingen worden gedaan onder de Wwke.

Welke informatie bevat een melding?

Voor het doen van een melding vult u in het **MijnNCSC-portaal** een korte vragenlijst in. Hiermee kan de bevoegde autoriteit beoordelen:

- wat de aard van het incident is;
- wat de vermoedelijke oorzaak is;
- wat de mogelijke gevolgen van het incident zijn;
- of sprake is van vermoedelijke grensoverschrijdende gevolgen.

Daarnaast verstrekt u de contactgegevens van een contactpersoon binnen uw organisatie, zodat - indien nodig - contact kan worden opgenomen over het incident.

Wat gebeurt er met uw melding?

De melding wordt via het **MijnNCSC-portaal** doorgestuurd naar de bevoegde autoriteit.

De melding stelt de bevoegde autoriteit in staat om adequaat te reageren op incidenten en inzicht te krijgen in de aard, oorzaak, impact en mogelijke gevolgen daarvan.
Uw organisatie ontvangt in ieder geval een ontvangstbevestiging. Waar mogelijk verstrekt de bevoegde autoriteit aanvullende informatie of advies om adequaat op het incident te kunnen reageren.

Een melding van een incident leidt niet tot verhoogde aansprakelijkheid voor uw organisatie. Meldingen worden vertrouwelijk behandeld.

Tijdlijn meldplicht

1. Incident ontdekt
Zo snel mogelijk melding maken, binnen 24 uur na kennisname.

2. Eerste melding
- aard van het incident;
- vermoedelijke oorzaak;
- mogelijke gevolgen;
- beschikbare informatie op dat moment.

De melding wordt via het MijnNCSC-portaal doorgestuurd naar de bevoegde autoriteit (ministerie en toezichthouder).
Uiterlijk één maand na de eerste melding.

3. Gedetailleerd eindverslag
- aanvulling op de eerste melding;
- nadere analyse van het incident;
- aanvullende informatie over oorzaak, impact en gevolgen.

5.

Maak gebruik van ondersteuning

Maak gebruik van ondersteuning

De Rijksoverheid ondersteunt organisaties bij het vergroten van hun weerbaarheid. Die ondersteuning helpt organisaties om zich voor te bereiden op verstoringen van essentiële diensten en om te voldoen aan de verplichtingen uit de Wet weerbaarheid kritieke entiteiten (Wwke).

Waar bestaat de ondersteuning uit?

De ondersteuning bestaat bijvoorbeeld uit:

- sectorspecifieke handreikingen en informatie;
- uitleg over de wettelijke verplichtingen;
- informatiebijeenkomsten of webinars;
- ondersteuning bij sectorale risico-informatie;
- verwijzingen naar relevante hulpmiddelen, normen en samenwerkingsverbanden;
- het verlenen van bijstand in het geval van crisis- of noodsituaties.

De wijze waarop deze ondersteuning wordt aangeboden, kan per sector verschillen en wordt waar nodig nader uitgewerkt in lagere regelgeving, in afstemming met de toezichthouder, het betrokken ministerie en de NCTV.

6.

Toezicht en handhaving

Toezicht en handhaving

De verantwoordelijke ministeries wijzen toezichthouders aan die toezicht houden op de naleving van de verplichtingen uit de Wet weerbaarheid kritieke entiteiten (Wwke). De toezichthouder controleert of uw organisatie voldoet aan de verplichtingen die gelden voor kritieke entiteiten. Daarbij wordt onder meer gekeken naar de uitvoering van de risicobeoordeling, de meldplicht en de zorgplicht. Het is daarom van belang om deze stappen goed vast te leggen en zorgvuldig te bewaren.

Wat kunt u verwachten?

De toezichthouder kan informatie opvragen of onderzoek doen om te beoordelen of uw organisatie voldoet aan de verplichtingen uit de Wwke. Daarbij kan bijvoorbeeld worden gekeken naar:

- de uitgevoerde risicobeoordeling;
- de maatregelen die uw organisatie heeft getroffen in het kader van de zorgplicht;
- de wijze waarop incidenten worden gemeld en afgehandeld;
- de vastlegging van beleid, procedures en maatregelen.

Handhaving

Wanneer blijkt dat een organisatie niet voldoet aan de verplichtingen uit de Wwke, kan de toezichthouder besluiten om een inspectie uit te voeren bij uw organisatie. U bent verplicht om daaraan mee te werken.

De toezichthouder kan daarbij verschillende acties inzetten, zoals:

- communicatie en voorlichting;
- bestuurlijk gesprek, bedrijfsbezoek, etc.;
- het geven van een aanwijzing of opdracht om bepaalde maatregelen te treffen;
- het laten uitvoeren van een audit;
- het opleggen van een last onder bestuursdwang of een last onder dwangsom;
- het opleggen van een bestuurlijke boete.

Voor meer informatie over de Wet weerbaarheid kritieke entiteiten kunt u terecht op de **website** van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Medegefinancierd door
de Europese Unie