w weerbaarheid

k kritieke

e entiteiten

Informatiebrochure

Wet weerbaarheid kritieke entiteiten

Wwke

mei 2024

Inleiding

Om de weerbaarheid van Europese lidstaten te versterken heeft de Europese Unie eind 2022 de Critical Entities Resilience Directive (CER-richtlijn) aangenomen. Het doel daarvan is om onze vitale infrastructuur en economische activiteiten in Europa zo veel mogelijk te beschermen. De Rijksoverheid werkt aan de omzetting van de CER-richtlijn naar nationale wetgeving: de Wet weerbaarheid kritieke entiteiten (Wwke).

Het doel van deze wet is het verhogen van de weerbaarheid van kritieke entiteiten die een essentiële dienst verlenen in Nederland. Het gaat hierbij om weerbaarheid ten aanzien van alle relevante door de natuur en door de mens veroorzaakte risico's die de verlening van haar essentiële dienst of diensten kunnen verstoren. In het wetsvoorstel zijn voorschriften vastgesteld op het gebied van technische, beveiligings-, en organisatorische eisen waar kritieke entiteiten aan moeten voldoen. De digitale weerbaarheid van kritieke entiteiten valt onder de Cyberbeveiligingswet.

Wat zijn de belangrijkste onderdelen van de Wet weerbaarheid kritieke entiteiten

Aanwijzing kritieke entiteiten

Risicobeoordeling, zorgplicht en meldplicht

Toezicht en handhaving

Ondersteuning

Inhoud

w weerbaarheid

k kritieke

e entiteiten

1

Valt uw organisatie onder de Wet weerbaarheid kritieke entiteiten?

Valt uw organisatie onder de Wet weerbaarheid kritieke entiteiten?

U kunt niet zelf bepalen of uw organisatie onder de Wet weerbaarheid kritieke entiteiten valt. De ministeries identificeren welke organisaties essentiële diensten aanbieden en daarmee wie er onder de wet valt.

Deze vallen ofwel binnen de sectoren uit het wetsvoorstel ofwel onder nog nader te identificeren sectoren. Op basis van een risicoanalyse wijst verantwoordelijk ministerie kritieke entiteiten aan met behulp van de hieronder genoemde criteria. Daarbij kijken zij in ieder geval naar de mate van impact die de organisatie heeft op de uitvoering van maatschappelijke functies en/of economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu.

Binnen de in de Wet weerbaarheid kritieke entiteiten genoemde sectoren kunnen kritieke entiteiten worden aangewezen: Energie, transport, bankwezen, infrastructuur voor de financiële markt, gezondheidszorg, drinkwater, afvalwater, digitale infrastructuur, overheid, ruimtevaart en de productie en verwerking en distributie van levensmiddelen.

De criteria waar een organisatie in ieder geval aan moet voldoen om als kritieke entiteiten te kunnen worden aangewezen zijn de volgende:

- De organisatie verleent één of meer essentiële diensten. Het gaat om diensten die van cruciaal belang zijn voor de instandhouding van vitale maatschappelijke functies, vitale economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu;
- De organisatie is actief in Nederland en haar kritieke infrastructuur bevindt zich in Nederland. Dat houdt ten eerste in dat de organisatie met haar kritieke infrastructuur geheel of gedeeltelijk actief is op het grondgebied van Nederland (inclusief het luchtruim en de maritieme binnenwateren en territoriale zee), en ten tweede dat de activiteiten van de organisatie noodzakelijk zijn om essentiële dienst of diensten te verlenen.

- Een incident binnen deze entiteit zou aanzienlijke verstorende effecten hebben op de verlening van de essentiële dienst(en) of via cascade-effecten op andere essentiële diensten (een onvoorziene reeks van gebeurtenissen die zich voordoet wanneer een gebeurtenis in een systeem een negatief effect heeft op andere, verwante systemen).

Organisaties die nu al als een vitale aanbieder zijn aangemerkt door een vakminister en binnen één van bovengenoemde sectoren vallen zullen naar verwachting ook worden aangewezen als kritieke entiteit.

V

Aanwijzingsproces

1. Risicobeoordeling
De vakminister voert een sectorale risicobeoordeling uit.

2. Identificatie
De vakminister identificeert welke organisaties essentiële diensten verlenen binnen een (sub)sector en een kritieke entiteit zijn.

3. Informeren
De organisatie wordt door de vakminister geinformeerd dat de organisatie is aangewezen als kritieke entiteit op basis van een regeling of besluit.

4. Verplichtingen
Binnen 9 maanden na de aanwijzing moet een kritieke entiteit zelf een risicobeoordeling hebben uitgevoerd. In de aanwijzing staat ook vanaf wanneer de overige verplichtingen uit de wet gelden.

5. Risicobeoordeling
Kritieke entiteiten zijn automatisch ook essentiële entiteiten in de zin van de Cyberbeveiligingswet en moeten – direct na aanwijzing als kritieke entiteit - ook aan die verplichtingen voldoen.

2

Wat betekent de Wet weerbaarheid kritieke entiteiten?

Welke verplichtingen schrijft de Wet weerbaarheid kritieke entiteiten voor?

Verplichtingen voor de overheid

Uitvoeren risicobeoordeling en aanwijzen kritieke entiteit

De Rijksoverheid is verplicht tot het periodiek opstellen van een nationale strategie over de weerbaarheid van kritieke entiteiten en het periodiek uitvoeren van een (sectorale) risicobeoordeling. Zo brengen we risico's in kaart voor de continuïteit van essentiële diensten. Het ministerie van Justitie en Veiligheid stelt samen met de betrokken ministeries de strategie vast. De vakminister voert een sectorale risicobeoordeling uit voor de sectoren die onder het vakdepartement vallen. De informatie uit de sectorale risicoanalyse wordt gedeeld met kritieke entiteiten zodat zij deze kunnen gebruiken bij het uitvoeren van de eigen risicobeoordeling.

Verplichtingen voor kritieke entiteiten

Risicobeoordeling

Kritieke entiteiten moeten een eigen risicobeoordeling uitvoeren ten aanzien van alle relevante risico's die hun dienstverlening kunnen verstoren. Het doel is om potentiële relevante dreigingen, kwetsbaarheden en gevaren die tot een incident kunnen leiden, in kaart te brengen en om in te schatten hoe groot de impact van een incident is op de essentiële dienstverlening. Het gaat om alle risico's die mens en natuur kunnen veroorzaken en tot een incident kunnen leiden zoals:

- risico's van sectoroverstijgende of grensoverschrijdende aard;
- ongevallen;
- natuurrampen;
- noodsituaties op het gebied van volksgezondheid;
- hybride dreigingen en andere antagonistische dreigingen (zoals terroristische misdrijven)

Kritieke entiteiten moeten in ieder geval gebruik maken van de informatie die uit de sectorale risicobeoordeling naar voren komt. Naast deze informatie kunnen organisaties gebruik maken van openbare bronnen.

Voorbeelden hiervan zijn de Rijksbrede Risicoanalyse Nationale Veiligheid, het Cybersecuritybeeld Nederland, het Dreigingsbeeld Statelijke Actoren en het Dreigingsbeeld Terrorisme Nederland. Waar nodig en relevant kan de overheid uiteraard ook meer specifieke informatie aanbieden.

De kritieke entiteit moet de risicobeoordeling periodiek uitvoeren en herzien. De eerste risicobeoordeling moet uiterlijk negen maanden nadat een organisatie is aangewezen als kritieke entiteit plaatsvinden. Vanaf dat moment is de kritieke entiteit verplicht om de risicobeoordeling ten minste om de vier jaar uit te voeren, of eerder als daar aanleiding toe is. Bijvoorbeeld als gevolg van actualiteiten, ontwikkelingen of dreigingen.

De risicobeoordeling kan verder worden uitgewerkt en geconcretiseerd in een algemene maatregel van bestuur.

Zorgplicht

Kritieke entiteiten zijn primair zelf verantwoordelijk voor hun weerbaarheid. Op basis van de risicobeoordelingen moeten zij daarom passende en evenredige maatregelen nemen om incidenten die de essentiële dienstverlening kunnen verstoren waar mogelijk te voorkomen, de gevolgen van incidenten te beperken en zo spoedig mogelijk kunnen herstellen als er een incident plaatsvindt. Denk hierbij in ieder geval aan het volgende:

- **Voorkomen dat incidenten zich voordoen.** De organisatie houdt rekening met alle risico's die mens en natuur kunnen veroorzaken en neemt maatregelen om het risico op rampen en gevolgen van klimaatverandering te beperken.
- **Zorgen voor adequate fysieke bescherming van gebouwen en kritieke infrastructuur.** Zoals het plaatsen van barrières, het inzetten van instrumenten en routines voor bewaking van de omgeving. De organisatie kan denken aan het plaatsen van barrières tegen schade door water of het op (brand)veilige locaties plaatsen van kwetsbare onderdelen voor de verlening van de essentiële dienst.
- **De gevolgen van incidenten bestrijden**, beperken en tegengaan, door uitvoering van risico- en crisisbeheersingsprocedures, protocollen en waarschuwingsroutines.
- **Herstellen van incidenten,** gebruikmakend van bedrijfscontinuïteitsmaatregelen, bijvoorbeeld de identificatie van alternatieve toeleveringsketens die de verlening van de essentiële dienst kunnen hervatten.
- **Zorgen voor de organisatie van personeelsbeveiliging.** Voorbeelden van maatregelen zijn: het vaststellen van categorieën personeelsleden die kritieke functies bekleden; het instellen van procedures voor antecedentenonderzoeken. Het vaststellen van passende opleidingsvoorschriften en kwalificaties. Hierbij houden organisaties rekening met het personeel van externe dienstverleners die kritieke functies vervullen en treffen zij passende maatregelen om risico's die daaruit kunnen voortvloeien te beperken. Het voorkomen van ongeautoriseerde toegang door het vaststellen van het recht van toegang tot gebouwen, kritieke infrastructuur en gevoelige informatie.
- **Personeel bewust** maken van al deze genoemde maatregelen, onder meer door middel van opleidingen/trainingen, informatiemateriaal en oefeningen.

Meldplicht

Kritieke entiteiten moeten incidenten die de verlening van hun essentiële diensten aanzienlijk verstoren of kunnen verstoren zo spoedig mogelijk (binnen 24 uur) melden bij de bevoegde autoriteit. Het doel van de melding is om de bevoegde autoriteit in staat te stellen om te reageren op incidenten en waar nodig en mogelijk ondersteuning te bieden. Daarom moet een melding een volledig overzicht van de impact, aard, oorzaak en de mogelijke gevolgen van een incident bieden.

Hoe wordt toezicht gehouden?

De ministeries wijzen toezichthouders aan die controleren op de naleving van de verplichtingen die gelden voor kritieke entiteiten, waarbij met name de zorgplicht een grote rol speelt. De Wwke geeft de toezichthouder daarnaast de mogelijkheid om handhavend op te treden indien blijkt dat verplichtingen niet worden nageleefd. De toezichthouder kan bijvoorbeeld een audit of een te verrichten handeling opleggen, en uiteindelijk ook een last onder bestuursdwang of een bestuurlijke boete opleggen.

Wat kunnen organisaties van de overheid verwachten?

De overheid ondersteunt kritieke entiteiten bij het verhogen van hun weerbaarheid Die ondersteuning kan bestaan uit informatie-uitwisseling, het bieden van methodieken en weerbaarheid verhogende instrumenten. Daarnaast kan de overheid helpen met het organiseren van oefeningen om de weerbaarheid van de kritieke entiteiten te testen, en advies en opleidingen bieden aan het personeel van kritieke entiteiten.

Tot slot kan een kritieke entiteit ook ondersteuning krijgen als er een incident plaatsvindt.

De vormen van ondersteuning kunnen worden uitgewerkt in lagere regelgeving en in afstemming met de toezichthouder, het betrokken ministerie en de NCTV.

Hoe kunt u uw organisatie voorbereiden?

Wacht niet af en begin alvast met de voorbereidingen die nodig zijn om uw organisatie weerbaar te maken. Het is raadzaam hiermee te beginnen zodat u op tijd voldoet aan de Wet weerbaarheid kritieke entiteiten. Met de volgende maatregelen kunt u zich voorbereiden:

- Maak een risicoanalyse van de risico's die de dienstverlening van uw organisatie kunnen verstoren en benut hiervoor de informatie uit bijvoorbeeld de Rijksbrede Risicoanalyse Nationale Veiligheid, het Cybersecuritybeeld Nederland, het Dreigingsbeeld Statelijke Actoren en het Dreigingsbeeld Terrorisme Nederland.
- Neem waar mogelijk maatregelen die uw organisatie (beter) beschermen tegen deze risico's.
- Zorg voor procedures die uw organisatie in staat stellen om incidenten die bedrijfsprocessen (kunnen) verstoren te detecteren, monitoren, op te lossen en te melden.

Kijk hier voor meer informatie over deze voorbereidende stappen:
Hoe kan uw organisatie zich voorbereiden op de CER- en NIS2-richtlijnen? | CER- en NIS2-richtlijnen | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)