Compliance readiness Wwke/CER

Europees kader: CER en NIS2

De Europese Unie heeft de **Critical Entities Resilience (CER)-richtlijn** geïntroduceerd. Deze richtlijn richt zich op de fysieke weerbaarheid van vitale infrastructuren en organisaties. Samen met de **NIS2-richtlijn**, die zich focust op digitale cyberweerbaarheid, vormt CER een stevig fundament voor het beschermen van essentiële diensten in Europa.

Nationaal: Wwke in Nederland

In Nederland is de **Wet weerbaarheid kritieke entiteiten (Wwke)** ingevoerd als nationale vertaling van de CER-richtlijn. Deze wet verplicht organisaties in kritieke sectoren om hun fysieke en digitale weerbaarheid structureel te versterken. Dit betekent dat jouw organisatie moet voldoen aan nieuwe eisen op het gebeid van risicobeheer, continuïteit en governance.

Wat betekent dit voor jouw organisatie?

- **Verhoogde bestuurlijke verantwoordelijkheid**: Bestuurders kunnen persoonlijk aansprakelijk worden gesteld bij incidenten.
- **Nieuwe compliance-eisen**: Organisaties moeten aantonen dat zij risico's identificeren, beheersen en rapporteren.
- **Integratie van fysieke en digitale weerbaarheid**: Het samenbrengen van cyber- en fysieke security in één strategie.
- **Leverancierskketenrisico's**: Derde partijen en toeleveranciers vallen nu ook onder strengere eisen.

Meer weten? Neem contact op met

Hokkie Blogg
Partner Cyber Security, Resilience & Crisis Management
blogg.hokkie@kpmg.nl
+31 (0) 653 355 232

Wwke in vier stappen

Verplichte onderdelen Wwke

Risicobeoordeling

Kritieke entiteiten Moeten alle potentiële risico's (natuurrampen, gezondheidscrises, menselijke dreigingen) in kaart brengen die hun dienstverlening kunnen verstoren.

- Helpt om preventieve maatregelen te nemen tegen verstoringen van essentiële diensten.

Zorgplicht

Kritieke entiteiten zijn verplicht passende maatregelen nemen om vitale infrastructuur en dienstverlening te beschermen.

- Met als doel het voorkomen van incidenten, beperken van schade en snel herstel na verstoringen.

Meldplicht

Kritieke entiteiten zijn verplicht incidenten te melden (binnen 24 uur) die een aanzienlijke verstoring veroorzaken.

- Als gevolg kan de overheid juist en adequaat reageren en assistentie bieden.

Wat kan KPMG betekenen?

Risico- & compliance-analyses

- Identificeert dreigingen (cyber, fysiek, keten) en impact op continuïteit.
- Wwke-assessments: toetsing op risicobeoordeling, zorgplicht en meldplicht.

Monitoring

- Selectie & implementatie van real time monitoring (cyber en fysiek).
- Heldere procedures voor drempels, escalatie en melding conform Wwke.

Business continuity & crisismanagement (BCM)

- BCM-plannen voor snelle herstart: alternatieve ketens, personeels-beschikbaarheid, fysieke beveiliging.
- Oefeningen & simulaties: testen respons, coördinatie en besluitvorming.

Hoe doen wij dit?

Door middel van interviews en documentanalyse beoordelen wij de Wwke-vereisten aan de hand van een gestructureerde gap-analyse. Elke vraag wordt beoordeeld op een schaal van 1 (volledige tekortkoming) tot 5 (geen tekortkoming). Deze aanpak maakt inzichtelijk waar compliance- of prestatieverbeteringen het meest nodig zijn, zodat gerichte acties kunnen worden ondernomen om kritieke hiaten te dichten en de algehele aansluiting op de Wwke-standaarden te versterken.