DBI

FÅ STYR PÅ CER-DIREKTIVETS KRAV

Det nye EU-direktiv træder snart i kraft.
Få indsigt i hvilke sektorer som bliver omfattet,
og hvordan du forbereder din virksomhed
bedst muligt.

HVAD ER CER-DIREKTIVET?

CER-direktivet fokuser på kritisk infrastruktur – hvad angår f.eks. naturkatastrofer, sabotage og forstyrrelser af forsyningskæder.

Formålet er at styrke modstandsdygtigheden i den kritiske infrastruktur i EU. CER skal sikre, at vigtige sektorer er i stand til at forebygge, modstå og reagere på forskellige former for kriser som fx hybride angreb, terrorangreb, folkesundhedskriser og naturkatastrofer og dermed beskytte samfundet og opretholde kontinuiteten i vitale tjenester og funktioner.

Hvad står CER-direktivet for?

CER står for Critical Entities Resilience Directive og stiller krav til modstandsdygtighed for virksomhederindenfor kritisk infrastruktur.

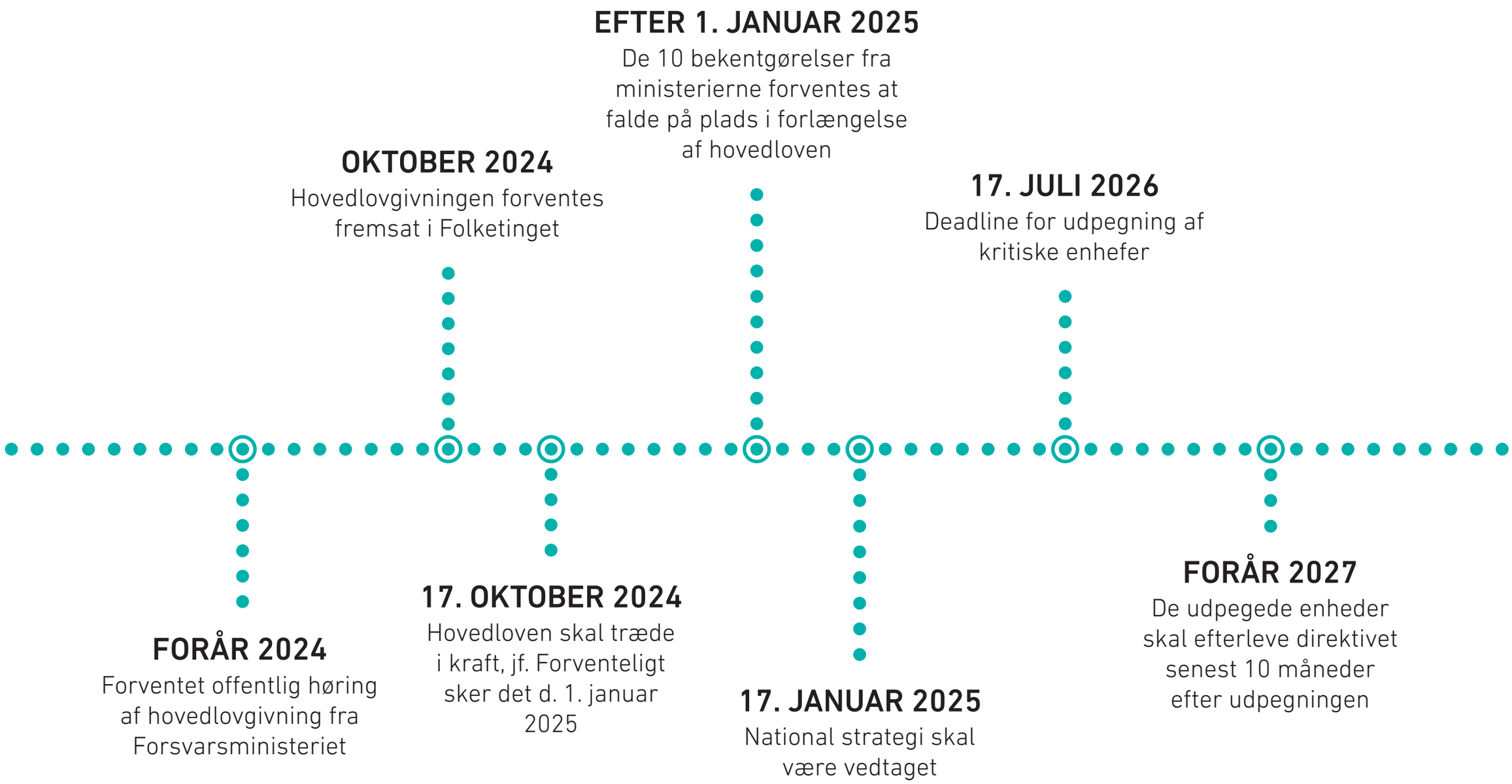
Hvem er omfattet af CER-direktivet?

CER omfatter sektorerne energi, transport, bankvæsen, finansmarkedsinfrastruktur, sundhed, drikkevand, spildevand, digital infra-struktur, offentlig administration, rumfart og fødevarer.

Bemærk at du som underleverandør til disse brancher også kan blive omfattet af kravene i direktivet.

HVORNÅR TRÆDER CER-DIREKTIVET I KRAFT?

Du kan se udrulningsplanen for CER-direktivet herunder:



Kilde: SikkerhedsBranchen

Danmark er imidlertid forsinket. Forsvarsministeriet meddeler på deres website, at der forventes en forsinkelse på omkring to måneder.

HVILKE KRAV STILLER CER-DIREKTIVET TIL DIN ORGANISATION?

Risikovurdering:

Virksomheder skal regelmæssigt foretage og opdatere en omfattende risikovurdering for at identificere trusler og sårbarheder i samfundskritiske tjenester.

Hændelsesrapportering:

Etablering af procedurer for hurtig identifikation og rapportering af væsentlige hændelser til de relevante nationale myndigheder, ofte inden for stramme tidsrammer.

Risikostyring:

Risikovurdering og implementering af passende og proportionale tekniske og organisatoriske foranstaltninger for at håndtere identificerede risici, herunder forebyggelse, beskyttelse, og beredskabsplanlægning.

Genopretningsplaner:

Udvikling af effektive genopretningsplaner for at sikre hurtig genopretning af kritiske funktioner efter en hændelse, inklusiv regelmæssig øvelse af disse planer.

HVILKE KRAV STILLER CER-DIREKTIVET TIL DIN ORGANISATION?

Sikkerhedsaudits:

Gennemførelse af regelmæssige sikkerheds-audits for at vurdere effektiviteten af foranstaltningerne og overholdelsen af direktivet.

Leverandørstyring:

Sikring af, at leverandører og samarbejdspartnere også opfylder strenge sikkerhedsstandarder for at beskytte værdikæden mod potentielle trusler.

Informationsdeling:

Fremme af informationsdeling om trusler, sårbarheder, og hændelser med andre kritiske enheder og de relevante myndigheder for at styrke samfundsmæssig sikkerhed og modstandsdygtighed.

Awareness og uddannelse:

Implementering af programmer for at øge bevidstheden og uddannelsesniveauet om sikkerhedstiltagene blandt medarbejdere og interessenter.

HVILKE KRAV STILLER CER-DIREKTIVET TIL DIN ORGANISATION?

Nationale kontaktpunkter:

Etablering af kontakt med nationale kontaktpunkter for kritisk infrastruktur for at sikre koordinering og støtte i forbindelse med direktivets implementering og overholdelse.

Baggrundsundersøgelser

Virksomheder bør etablere baggrundsundersøgelser som en central del af deres CER-overholdelsesplan. Baggrundsundersøgelser er med til at afsløre skjulte risici og sikrer, at dit team lever op til standarderne i direktivet.

Tværgående samarbejde:

Deltagelse i tværsektorielt og tværnationalt samarbejde for at fremme udveksling af bedste praksis og styrke modstandsdygtigheden på tværs af grænser og sektorer.

Disse krav er designet til at sikre, at kritiske enheder er forberedt på og kan modstå alle typer af trusler, samtidig med, at de opretholder kontinuiteten i deres kritiske tjenester.

DBI KAN HJÆLPE JER MED AT LEVE OP TIL DE NYE LOVKRAV

Konkret kan vi hjælpe med:

Risikoanalyse:

Vi udfører detaljerede risikoanalyser for at identificere specifikke trusler og sårbarheder, som en virksomhed står over for, og hjælper med at udarbejde en tilpasset risikostyrings-strategi.

Udarbejdelse af genopretningsplaner:

Vi kan assistere med udviklingen af robuste genopretningsplaner, der sikrer hurtig genop-retning og minimal driftsforstyrrelse efter sikkerhedshændelser.

Beredskabsplaner:

Vi kan hjælpe med at designe og implementere omfattende beredskabsplaner, der adresserer både fysiske og cybertrusler, baseret på de identificerede risici.

Krise- og beredskabsøveler:

Gennem regelmæssige krise- og beredskabs-øvelser kan vi sammen med din virksomhed vurdere effektiviteten af implementerede sikkerhedsforanstaltninger og anbefale forbedringer.

Leverandørstyring:

Vi kan rådgive om bedste praksisser for at sikre, at leverandørkæden overholder de nødvendige sikkerhedsstandarder.

Læs mere her

Dansk Brand- og sikringsteknisk Institut · 36 34 90 00 · brandogsikring.dk