Illustration af Rasmus Juul Pedersen

CER: RETTIDIG OMHU REDUCERER RISICI

Virksomheder inden for kritisk infrastruktur skal forebygge hændelser. Det foreskriver EU-direktivet CER. Andreas Norstedt, sikkerhedsrådgiver hos DBI, giver her opskriften på, hvordan man griber det an.

Hvad går forebyggelse af hændelser ud på i CER-direktivet?

Forebyggelse af hændelser handler om at identificere og mindske de risici, som kan forstyrre virksomheder inden for kritisk infrastruktur i at levere deres tjenester til samfundet. Det omfatter tekniske, organisatoriske og sikkerhedsmæssige tiltag, som sikrer, at potentielle hændelser ikke udvikler sig til kritiske forstyrrelser.

CER-direktivet fokuserer på fysiske trusler mod kritisk infrastruktur, hvor NIS2-direktivet primært omfatter digitale risici. Aktualiteten af CER-direktivet blev bl.a. understreget af Nord Stream-sabotagen, som gjorde det tydeligt, hvor sårbar Europas infrastruktur kan være over for målrettede angreb.

Hvordan skal virksomhederne helt konkret gøre?

For at forebygge hændelser i tråd med CER-direktivet skal virksomheder arbejde systematisk med risikohåndtering. Første skridt er at lave en grundig risikovurdering, hvor man finder ud af, hvad der kan gå galt, og hvilke konsekvenser det kan få. Det kan være alt fra naturkatastrofer som oversvømmelser til bevidste handlinger som sabotage og terrorangreb. Formålet er at vurdere sandsynligheden for, at disse hændelser sker – og deres potentielle konsekvenser – så indsatsen kan prioriteres mod de mest kritiske risici, der skal behandles i en beredskabsplan.

Samtidig er det vigtigt at forstå, hvordan forskellige sektorer og forsyningskæder hænger sammen. Hvis strømmen f.eks. forsvinder i én sektor, kan det få konsekvenser for andre sektorer. Derfor bør virksomheder tage højde for disse "kaskadeeffekter", når de laver deres risikovurderinger.

Når risiciene er afdækket, er næste skridt forebyggende tiltag – i det omfang, det er muligt og giver mening i forhold til risikobilledet. Det kan være mekanisk sikring som hegn, porte og pullerter, der forhindrer uautoriseret adgang. Det suppleres af elektronisk overvågning, herunder videoovervågning, alarmsystemer og adgangskontrol, der sikrer løbende monitorering og hurtig detektion af trusler.

Foranstaltningerne skal integreres i virksomhedens samlede risikostyring og bør dokumenteres i en sikringsplan. Regelmæssig evaluering, test og øvelser sikrer, at tiltagene bliver ved med at være effektive og tilpasset et omskifteligt risikobillede.

Hvad er en god fremgangsmåde?

En god måde at komme i gang på er at samle nøglepersoner fra forskellige afdelinger i virksomheden til en risikoworkshop. Det omfatter personer fra centrale afdelinger som økonomi, drift/produktion, HR og IT. Workshoppen skal identificere og kortlægge de væsentligste risici for

virksomhedens kritiske aktiver. Ved at få viden fra forskellige perspektiver opnår man et mere nuanceret billede af potentielle trusler og sårbarheder. Brug gerne en kombination af interne erfaringer og offentligt tilgængelige risikovurderinger til at identificere risici.

Efter workshoppen skal der laves en detaljeret risikovurdering, hvor de identificerede risici analyseres. Resultaterne er grundlaget for at prioritere indsatsen mod de mest kritiske risici. Dernæst bør man implementere målrettede forebyggende tiltag, som skal tilpasses virksomhedens specifikke behov og kontekst.

Er der "faldgruber", man bør være opmærksom på?

En af de største fejl, virksomheder kan begå, er at undervurdere risici. Mange overser deres afhængighed af leverandørkæder og andre sektorer, som kan forstærke konsekvenserne af en hændelse. Derfor er det vigtigt at bruge tid på at kortlægge afhængigheder og forstå de potentielle konsekvenser.

Data er en uvurderlig ressource i risikohåndtering, men det er en balance mellem at indsamle tilstrækkelige data og undgå at bruge for meget tid på analyse. Effektivitet handler om at identificere de væsentligste risici og reagere rettidigt i stedet for at stræbe efter perfektion.

Utilstrækkelige ressourcer kan være en barriere for effektiv forebyggelse. Hvis der ikke investeres nok i både menneskelige og teknologiske løsninger, risikerer man at stå med foranstaltninger, der ikke lever op til kravene i CER-direktivet og dermed svækker virksomhedens modstandsdygtighed. Ressourcerne bør derfor prioriteres på baggrund af en risikobaseret tilgang, så de områder, der er mest kritiske, får den nødvendige opmærksomhed.

Særlige forhold for energisektoren

Energisektoren har særlige regler og krav, når det kommer til forebyggelse af hændelser. De skal bl.a. lave ROS-analyser (risiko- og sårbarhedsanalyser), hvor de vurderer fastsatte scenarier udstukket af Energistyrelsen. Det er endnu uvist, om andre sektorer vil få tilsvarende krav, da det afhænger af, hvordan CER-direktivet bliver implementeret af de respektive/enkelte ministerier.

Læs mere om CER-direktivet

Læs mere om NIS2-direktivet