Ministeriet for Samfundssikkerhed og Beredskab

Dato: 27. maj 2025
Sagsnr.: 2025 - 1135
Akt-id.: 6193

Besvarelse af spørgsmål nr. 290 (Alm. del) fra Forsvars-, Samfundssikkerheds- og Beredskabsudvalget

Hermed sendes besvarelse af spørgsmål nr. 290 (Alm. del), som Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg har stillet til ministeren for samfundssikkerhed og beredskab den 30. april 2025. Spørgsmålet er stillet efter ønske fra Mike Villa Fonseca (UFG).

Torsten Schack Pedersen

Spørgsmål nr. 290 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg:

> ”Mener ministeren, at Danmark er tilstrækkeligt rustet mod cyberangreb eller nedbrud på elnettet?”

Svar:

Tilrettelæggelsen af beredskabet omkring den samfundskritiske infrastruktur er afgørende for at skabe et sikkert og robust samfund. I Danmark følger det grundlæggende af sektoransvarsprincippet, at den enkelte sektor skal vurdere det konkrete risikobillede og træffe passende foranstaltninger. Det er dog en central opgave for Ministeriet for Samfundssikkerhed og Beredskab at rådgive og vejlede virksomheder og myndigheder på tværs af sektorerne for at sikre et ensartet og tilfredsstillende niveau af cybersikkerhed i Danmark.

Ministeriet for Samfundssikkerhed og Beredskab har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Styrelsen for Samfundssikkerhed, der har oplyst følgende:

> ”Styrelsen for Samfundssikkerhed har en koordinerende og tværgående rolle i at understøtte myndighederne i at løfte sektoransvaret. Dette gøres igennem blandt andet rådgivning og lovgivning.
>
> NIS 2-loven, der skal styrke cybersikkerheden og modstandsdygtigheden i kritiske virksomheder og myndigheder, er for nyligt blevet vedtaget, og der vil dermed fra den 1. juli 2025 blive stillet en række krav til cybersikkerhedsniveauet i samfundets kritiske sektorer. Med NIS 2-loven vil der også blive ført tilsyn med, at kritiske virksomheder og myndigheder har et passende cybersikkerhedsniveau og er rustet mod cyberangreb.
>
> Danmark har siden 2014 arbejdet med en national cyber- og informationssikkerhedsstrategi med formål om at løfte den digitale sikkerhed på tværs af samfundet, hvor der gennem en række initiativer blandt andet er arbejdet med at øge opmærksomheden omkring truslerne for både borgere, virksomheder og myndigheder og stillet sikkerhedskrav til ministerområder, der har ansvar for samfundsvigtige funktioner eller samfundskritiske it-systemer.

> Som udgangspunkt er det op til de enkelte myndigheder eller virksomheder at håndtere et cyberangreb. De kender deres it-systemer, deres brugere og de procedurer, der skal til, for at deres drift kan genoptages.
>
> Når større hændelser indtræffer, eller når der er risiko for større hændelser, vil den Nationale Operative Stab (NOST) også kunne blive indkaldt. Den koordinerer og tager højde for de mulige konsekvenser af større hændelser og iværksætter tiltag for at begrænse omfanget af disse."

For så vidt angår beredskabet i elnettet henvises der til klima-, energi- og forsyningsministerens samtidige besvarelse af spørgsmål nr. 288 (Alm. del) fra Folketingets Forsvars-, Samfundssikkerheds- og Beredskabsudvalg.

Generelt understreger strømnedbruddet i Sydeuropa dog, at et gennemdigitaliseret samfund har sårbarheder, hvor en hændelse på ét område har indvirkning på en række andre områder.

Derfor er det også en bunden opgave, at vi på tværs af sektorer skal styrke beredskabet, så myndigheder og sektorer er forberedt på de risici og trusler, vi står over for. Relevante danske myndigheder ser derfor også på, hvad man fra dansk side kan lære af hændelsen.