Ministeriet for
Samfundssikkerhed og Beredskab

Dato:	29. november 2024
Kontor:	Kontor for Cyber- og Informationssikkerhed
Sagsbeh:	Josefine Boolsen
Sagsnr.:	Sagsnummer
Dok.:	Dokumentnummer

Besvarelse af spørgsmål nr. 21 (Alm. del) fra Udvalget for Digitalisering og It

Hermed sendes besvarelse af spørgsmål nr. 21 (Alm. del), som Folketingets Udvalg for Digitalisering og It har stillet til ministeren for samfundssikkerhed og beredskab den 1. november 2024. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF).

Torsten Schack Pedersen

Spørgsmål nr. 21 (Alm. del) fra Folketingets Udvalg for Digitalisering og It:

> ”Vil ministeren oplyse, om man i dag foretager tests lokalt for at vurdere og sikre, at virksomheder, installationer og organisationer i samfundskritiske sektorer er modstandsdygtige overfor cyberangreb – eksempelvis på hospitaler, men også energikraftværker, myndigheder med ansvar for udbetaling af sociale ydelser og forsyningsselskaber? Der henvises til, at blandt andet visse typer af finansielle virksomheder er pålagt at foretage tests af it- og cybersikkerheden, jf. § 333 i Lov om finansiel virksomhed. Såfremt man ikke udfører konkrete sikkerhedstests (penetrationstests), kan ministeren så bekræfte, at vurderingen af cybersikkerheden alene baserer sig på formel overholdelse af krav og regler og ikke virkelighedsnære test, der sikrer, at offentlige virksomheder reelt er modstandsdygtige overfor cyberangreb?

Svar:

Ministeriet for Samfundssikkerhed og Beredskab har med den kongelige resolution den 29. august 2024 fået ressortoverført en række sagsområder fra blandt andet Forsvarsministeriet og det daværende Digitaliserings- og Ligestillingsministerium vedrørende cybersikkerhed og digital informationssikkerhed. Det omfatter bl.a. opgaven med at vejlede og rådgive borgere, virksomheder og myndigheder inden for området. Det er en vigtig opgave, som bl.a. implementeringen af NIS 2-direktivet vil være med til at sætte rammerne for.

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 vil dog være 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 Center for Cybersikkerhed (CFCS), der har oplyst følgende:

”CFCS er bekendt med, at nogle myndigheder og virksomheder – som led i varetagelsen af ansvaret for deres cyber- og informationssikkerhed – anvender sikkerhedstest, herunder penetrationstest. CFCS har dog ikke nærmere kendskab til anvendelsen af test i de enkelte sektorer.

Det følger af § 1, stk. 1, i lov om Center for Cybersikkerhed, at centeret har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur som samfundsvigtige funktioner er afhængige af.”

Herudover har Ministeriet for Samfundssikkerhed og Beredskab indhentet en udtalelse fra Forsvarsministeriet, der har oplyst følgende:

”Forsvarsministeriet har den 21. november 2024 anmodet Forsvarets Efterretningstjeneste (FE) om at bidrage til besvarelsen af spørgsmål nr. 21 (alm. del) fra Udvalget for Digitalisering og It, som er stillet til ministeren for samfundssikkerhed og beredskab.

FE kan til brug for besvarelsen oplyse følgende:

”Med henblik på at kunne rådgive myndigheder og virksomheder om forebyggelse af sikkerhedshændelser kan FE gennemføre forebyggende sikkerhedstekniske undersøgelser, herunder penetrationstest, når en myndighed eller en virksomhed har anmodet centeret herom, jf. § 6 a. i lov om Center for Cybersikkerhed.

Som led i en penetrationstest kan der udføres et simuleret angreb på et system eller netværk, hvor sårbarheder og potentielle angrebsvektorer identificeres. På baggrund af undersøgelsen kan myndigheden eller virksomheden rådgives om, hvilke konkrete tiltag der kan gennemføres for at opnå et højere sikkerhedsniveau.””