INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

T +45 7226 9000
M sum@sum.dk
W sum.dk

Folketingets Digitaliserings- og It-udvalg

Dato: 29-11-2024
Enhed: Digitalisering og hjemmebehandling
Sagsbeh: kkc
Sagsnr.:2024 - 13408
Dok. nr.: 250695

Hermed sendes besvarelse af spørgsmål nr. 20 (Alm. del), som Folketingets Digitaliserings- og It-udvalg har stillet til indenrigs- og sundhedsministeren den 1. november 2024. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF).

Spørgsmål nr. 20:
"Vil ministeren oplyse, om det er regeringens vurdering, at man i sundhedssektoren i dag gør tilstrækkeligt for at sikre, at man er modstandsdygtige overfor cyberangreb? Der henvises til, at der er flere eksempler fra udlandet og Danmark, der indikerer, at sundhedssektoren er udsat."

Svar:
Center for Cybersikkerhed vurderer, at der fortsat er en alvorlig cybertrussel mod sundhedssektoren i Danmark. Samtidig er cybertruslen er omskiftelig og stiller derfor krav om, at arbejdet med cyber- og informationssikkerhed er en risikobaseret og dynamisk indsats, der kan tilpasses de løbende skift i trusselsbilledet.

Jeg kan oplyse, at arbejdet med cyber- og informationssikkerhed i Danmark er baseret på sektoransvarsprincippet, hvilket betyder, at regioner, kommuner og sundhedssektorens øvrige aktører har ansvaret for egen sikkerhed.
Sundhedssektoren består af mange forskellige aktører; både offentlige og private, og store, mellemstore og små aktører. Derfor er modenhedsniveauet for cyber- og informationssikkerhed også meget forskelligt aktørerne imellem. Jeg kan dog oplyse, at EU's NIS2-direktiv, som implementeres i dansk lov til næste år, har til formål i højere grad at ensarte cybersikkerheden og modstandsdygtigheden over for cybertrusler på tværs af EU, herunder også inden for sundhedssektoren.

Jeg kan desuden oplyse, at sundhedssektoren har en sektorstrategi for cyber- og informationssikkerhed 2023-2025, som er udarbejdet af stat, regioner og kommuner i fællesskab. Strategien danner rammen om sundhedsvæsenets fælles indsatser for at styrke cyber- og informationssikkerheden på tværs af sundhedsvæsnet, som koordineres og understøttes af sundhedssektorens decentrale cyber- og informationssikkerhedsenhed (DCISSund) i Sundhedsdatastyrelsen. DCISSund er bl.a. ansvarlig for sundhedssektorens sikkerhedsanalysecenter og følger løbende det aktuelle trusselsbillede og deler denne viden med aktørerne i sundhedssektoren.

Sektorstrategien indeholder bl.a. initiativer rettet mod cybersikkerheden hos sektorens mindre aktører, fælles rammer og værktøjer til løbende test af cybersikkerheden og fælles beredskabsøvelser.

Det er helt afgørende, at digitaliseringen af sundhedsvæsenet foregår i trygge og sikre rammer. Når vi digitaliserer sundhedsvæsenet, skal sikkerheden naturligvis også følge med. Borgerne skal kunne stole på, at sundhedsvæsenet er tilgængeligt, når de har brug for det, og at sundhedsvæsenet passer godt på de følsomme

personoplysninger, som de betror sundhedsvæsenet i forbindelse med et behandlingsforløb.

Med venlig hilsen

Sophie Løhde