INDENRIGS- OG SUNDHEDSMINISTERIET

Slotsholmsgade 10-12
DK-1216 København K

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

Folketingets Digitalisering og It-udvalg

Dato: 22-10-2024
Enhed: Digitalisering og hjemmebehandling
Sagsbeh: anh
Sagsnr.:2024 - 11679
Dok. nr.: 230152

Hermed sendes besvarelse af spørgsmål nr. 222 (Alm. del), som Folketingets Digitalisering og It-udvalg har stillet til indenrigs- og sundhedsministeren den 24. september 2024. Spørgsmålet er stillet efter ønske fra Dina Raabjerg (KF).

Spørgsmål nr. 222:
"I de seneste år har vi set flere eksempler på ransomware-angreb rettet mod hospitaler i udlandet f.eks. i Rumænien jf. artiklen »Kæmpe ransomware-angreb tvinger 25 hospitaler til at gå offline: Må arbejde med papir«, computerworld.dk, den 13. februar 2024. Sådanne angreb kan få alvorlige konsekvenser for patientbehandlingen. Dette understreger vigtigheden af en robust cybersikkerhed i vores egne hospitaler for at undgå lignende hændelser. Vil ministeren i den forbindelse svarer på følgende spørgsmål:

- Vil ministeren oplyse det samlede antal kritiske sårbarheder i it-systemerne for hver af de fem regioner, opdelt efter, hvor kritiske disse sårbarheder er? Der er ikke et ønske om oplysninger, der afslører specifikke tekniske detaljer eller følsomme oplysninger, men blot en oplysning om antallet af sårbarheder, som kunne udgøre en risiko for regionernes hospitals-IT-systemer, såsom interne servere, computere, røntgensystemer, pumper, scannere og laboratorieudstyr.
- Hvor mange af de kritiske sårbarheder har været kendt og eksisteret siden før sommerferien, og hvor mange har været kendt og eksisteret i over et år? Der ønskes alene sammenfattede data og statistikker og ikke detaljerede oplysninger om individuelle sårbarheder eller deres specifikke karakteristika.
- Vil ministeren vurdere, om de afsatte midler i regeringens strategi for cyber- og informationssikkerhed – herunder de 270 mio. kr., som blev nævnt af finansministeren i svar på L 239 (folketingsåret 2021-22) – spm. 42, er tilstrækkelige til at sikre en robust cybersikkerhed på tværs af regionernes hospitaler? Hvis ikke, hvilke yderligere ressourcer eller initiativer anser ministeren som nødvendige for at sikre, at den nuværende situation med manglende sikkerhedsopdateringer og kendte kritiske sårbarheder ikke udgør en trussel mod danskernes sikkerhed"

Svar:
Indenrigs- og Sundhedsministeriet er ikke i besiddelse af opgørelser over antallet af kritiske sårbarheder i regionernes it-systemer. 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.

Jeg kan oplyse, at den nationale strategi for cyber- og informationssikkerhed 2022-2024 omhandler en styrkelse af Danmarks digitale sikkerhed generelt. Den har bl.a. fokus på samfundsvigtige funktioner og den understøttende kritiske it-infrastruktur, som statslige myndigheder har ansvaret for, såvel som på erhvervslivet og borgere.

Jeg kan i øvrigt henvise til Ministeriet for Samfundssikkerhed og Beredskab ved spørgsmål om den nationale strategi for cyber- og informationssikkerhed.

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.

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