MINISTERIET FOR BØRN, LIGESTILLING, INTEGRATION OG SOCIALE FORHOLD

Folketingets Forsvarsudvalg

Departementet
Holmens Kanal 22
1060 København K

Tlf. 33 92 93 00
Fax. 33 93 25 18
E-mail sm@sm.dk

Dato: 27. juni 2014

Ansvarlig: PHG
Sagsnr. 2014 - 4762

Under henvisning til Folketingets Forsvarsudvalgs brev af 26. maj 2014 følger hermed ministeren for børn, ligestilling, integration og sociale forholds endelige svar på spørgsmål nr. 261 (FOU alm. del). Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V).

Spørgsmål nr. 261:

"I det forsvarsministeren på et åbent samråd i Forsvarsudvalget den 23. maj 2014 om cybersikkerhed opfordrede udvalget til at spørge de enkelte ministre om, hvad der gøres for at beskytte sig imod cybertrusler, bedes ministeren redegøre for, hvad der er gjort eller vil blive gjort indenfor ministerens ansvarsområde m.h.t. at beskytte it-systemer og fortrolige data samt m.h.t. at sikre sig imod hackerangreb, jf. statsrevisorernes beretning 3/2013 om forebyggelse af hackerangreb, hvor statsrevisorerne bl.a. udtaler foruroligelse over utilstrækkelig beskyttelse mod cybertrusler i en række undersøgte statslige virksomheder."

Svar:

Ministeriet har forholdt sig til de generelle initiativer, som regeringen har besluttet, og som er beskrevet i finansministerens svar på samme spørgsmål af 18. juni 2014. Dette vedrører:

- Brugen af ISO27001 til styring af sikkerhedsarbejdet, risikovurderinger og topledelsens involvering
- Strategi for cyber- og informationssikkerhed
- Rigsrevisionens anbefalede tiltag så som begrænsning af download af programmer, sikkerhedsopdateringer, begrænsning af brugeradgange
- Styring af sikkerhed i statens outsourcede drift.

I forlængelse heraf kan jeg meddele at:

Ministeriet har en opdateret informationssikkerhedspolitik. Departementet selv er overgået til den nye ISO27001 sikkerhedsstandard, og de tilknyttede styrelser og organisationer er på vej.

Ministeriets sikkerhedsleder deltager aktivt i Statens informationssikkerheds-forum (SISF).

Ministeriet har en politik for de tre væsentlige sikringstiltag vedr. forebyggelse af hackerangreb:

Begrænsning af download af programmer fra internettet
Sikkerheden opnås ved at forhindre og begrænse mulighederne for at kunne installere og køre programmer i pc-miljøet, som ikke er godkendte. Udrulning af pc-programmer i koncernen foregår centralt fra it-afdelingen Koncern-it.

Begrænsning i brugen af lokaladministratorer
Der er etableret sikringsforanstaltninger i departementet og styrelserne for styring og begrænsning af lokaladminstratorer i pc-miljøet.

Systematiske sikkerhedsopdateringer
Der er idriftsat et centralt system til at sikre, at opdateringer af slutbruger-pc'ere kan styres centralt fra Koncern-it. Serverdriften i koncernen er blevet outsourcet til en ekstern leverandør og systematiske opdateringer af servere er en del af denne ydelse.

Generelt
Herudover benytter ministeriet følgende generelle foranstaltninger for at beskytte sig imod cybertrusler:

Alle driftskritiske systemer er anbragt i beskyttet miljø bag firewalls.

Al trafik til og fra departementet og dets styrelser er overvåget af GovCert.

Personfølsomme oplysninger opbevares i sagsbehandlingssystemer på dansk jord, med den sikkerhed som er krævet i bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning.

Udveksling af personfølsomme oplysninger foretages ved hjælp af sendsikker løsninger, som krypterer informationerne.

Manu Sareen

/Annie Stahel