Folketingets Forsvarsudvalg
Christiansborg
1240 København K

Beskæftigelsesministeriet
Ved Stranden 8
1061 København K

T 72 20 50 00
E bm@bm.dk
www.bm.dk

CVR 10172748
EAN 5798000398566

23. juni 2014
Sagsnr. 2014 - 4130

Forsvarsudvalget har i brev af 26. maj 2014 stillet følgende spørgsmål nr. 253 (alm. del), som hermed besvares. Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V).

Spørgsmål nr.: 253
"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."

Endeligt svar:
Det fremgår af Finansministeriets svar på FOU alm. del spørgsmål 250, at der på regeringsniveau og i regi af Statens It er igangsat en række initiativer med henblik på at styrke ministeriernes arbejde for at understøtte it-sikkerheden.

Initiativer af generel karakter gældende for alle ministerområder:

- Alle statslige myndigheder skal implementere sikkerhedsstandarden ISO27001, som stiller en række krav til styringen af sikkerhedsarbejdet.
- Der er nedsat en tværministeriel arbejdsgruppe, som skal udarbejde en strategi for cyber- og informationssikkerhed. Strategien forventes lanceret i år.
- Alle statslige myndigheder med udgangspunkt i en risikovurdering foretager implementering af konkrete sikkerhedstiltag (eksempelvis positivliste af godkendte programmer, opdatering af programmer med sikkerhedsopdateringer, begrænsning af brugeradgange med særlige administratorprivilegier), tiltag, som kan forhindre en væsentlig del af de målrettede cyberangreb.
- Endelig arbejder regeringen på en vejledning til statslige myndigheder om styring af sikkerhed i statens outsourcede drift.

Initiativer gældende for de ministerområder som er kunde hos Statens It:

- Statens It har indført en standardiseret pc-arbejdsplads og et fælles datacenter med en samlet styring af computere og infrastruktur.
- Statens It samarbejder med Center for Cybersikkerhed om monitorering af trafik til og fra Statens It's datacenter for tidligt at opdage og forhindre mulige hackerangreb.
- Statens It har i 2013 gennemført en reduktion af antallet af brugere med domæneadministratorrettigheder og foretager løbende opfølgning.

- Statens It samarbejder løbende med kunderne om sikring mod hackerangreb og beskyttelse af fortrolige data.

Beskæftigelsesministeriets egne initiativer:

- Beskæftigelsesministeriet er i gang med at indgå aftale med Statens It om en handlingsplan for implementering af sikkerhedsstandarden ISO27001, således at der vil blive stillet konkrete krav til styringen af sikkerhedsarbejdet i ministeriet.
- Beskæftigelsesministeriet reviderer løbende aftaler med leverandører – herunder Statens IT – med henblik på at tydeliggøre ansvarsplacering på sikkerhedsområdet. Ministeriet er i den forbindelse også aktiv deltager i arbejdet med en tilretning af Statens It's fremadrettede strategier.
- Beskæftigelsesministeriet har tidligt – siden maj 2012 – været tilsluttet Center for Cybersikkerhed GovCERT's varslingssystem, og herfra løbende modtaget sikkerhedsadvarsler og anbefalinger vedrørende cybertrusler.

Jeg tager virksomhedernes og borgernes cybersikkerhed alvorligt. Jeg vurderer, at de initiativer, som regeringen, Statens It og mit eget ministerium har iværksat, er medvirkende til at sikre mod hackerangreb.

Venlig hilsen

Mette Frederiksen