økonomi og indenrigsministeriet

Folketingets Forsvarsudvalg

Slotsholmsgade 10-12
1216 København K
Telefon 72 28 24 00
Fax 72 28 24 01
oim@oim.dk
www.oim.dk

Sagsnr.
2014 - 16477

Doknr.
146404

Dato
19-06-2014

Folketingets Forsvarsudvalg har den 26. maj 2014 stillet følgende spørgsmål nr. 249 til økonomi- og indenrigsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V)

Spørgsmål nr. 249:

"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:

Regeringen har igangsat en række initiativer med henblik på at styrke de enkelte ministeriers arbejde med at understøtte it-sikkerheden. Finansministerens svar på udvalgets spørgsmål nr. 250 af 23. maj 2014 indeholder en nærmere redegørelse for generelle initiativer på området, hvortil jeg kan henvise.

Som det fremgår af finansministerens svar, skal alle statslige myndigheder implementere sikkerhedsstandarden ISO 27001. For Økonomi- og Indenrigsministeriet indebærer dette bl.a., at ministeriet har udarbejdet risikovurderinger for sine væsentligste it-systemer, og at der på baggrund af risikovurderingerne er truffet proportionelle sikringsforanstaltninger og procedurer i forhold til det enkelte system.

Beskyttelse mod cybertrusler er navnlig relevant i forhold til CPR-systemet, hvilket afspejles i de sikringsforanstaltninger og procedurer, der er truffet for dette system.

CPR-systemet er bl.a. genstand for regelmæssig sikkerhedskontrol i form af uvildig it-revision af, om driftsleverandøren har gennemført de kontroller, der følger af ISO 27001, ligesom systemet udsættes for penetrationstest (hacker-test) med bistand fra eksterne sikkerhedseksperter.

I forbindelse med et nylig gennemført platformskifte har Økonomi- og Indenrigsministeriet endvidere foranstaltet en ekstraordinær uvildig it-revision af den nye platform. Der er desuden gennemført en sikkerhedsvurdering af den nye platform i samarbejde med Center for Cybersikkerhed, og der er gennemført penetrationstest (hacker-test) af eksterne eksperter.

Med den nye platform er der gennemført en række sikkerhedsmæssige forbedringer. F.eks. er der indført krav om anvendelse af stærkere passwords, kun whitelistede

(godkendte) IP-adresser kan tilgå systemet, og der kan kun anvendes kommunikationsprotokoller, hvor trafikken krypteres.

CPR-systemets firewall er endvidere blevet suppleret med en såkaldt IDS (Intrusion Detection System) løsning, der automatisk kan opdage skadelig trafik, hvorved muligheden for at detektere og stoppe eventuelle angreb forbedres. IDS løsningen giver tillige et bedre logningsgrundlag til anvendelse i et eventuelt efterforskningsarbejde.

Der er herudover iværksat løbende automatiske kontroller, som advarer, hvis relevante sikkerhedsopdateringer ikke er installeret på CPR-systemets servere.

Det kan tilføjes, at Økonomi- og Indenrigsministeriet som opfølgning på det hackerangreb, der i 2012 blev gennemført mod Rigspolitiets systemer, med bistand fra Center for Cybersikkerhed har iværksat en undersøgelse af, hvorvidt angrebet giver anledning til at træffe yderligere sikkerhedsforanstaltninger i forhold til CPR-systemet. De anbefalinger, som er fremkommet i forbindelse med undersøgelsen, er løbende blevet implementeret.

Det skal understreges, at de sikkerhedsforanstaltninger, der er truffet for CPR-systemet, ikke udgør en garanti mod hacking, men de er udtryk for, at Økonomi- og Indenrigsministeriet tager cybertrusler alvorligt, og at sikkerheden hviler på et godt fundament, som løbende udbygges i forhold til den aktuelle risikovurdering.

Med venlig hilsen
Margrethe Vestager