KLIMA-, ENERGI- OG BYGNINGSMINISTERIET

Forsvarsudvalget
Christiansborg
1240 København K

Stormgade 2-6
1470 København K
Tlf. 3392 2800
Fax 3392 2801
kebmin@kebmin.dk
www.kebmin.dk

Forsvarsudvalget har i brev af 26. maj 2014 stillet mig følgende spørgsmål 263, alm. del, stillet efter ønske fra Troels Lund Poulsen (V), som jeg hermed skal besvare.

Spørgsmål 263

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 virksomheder.

Ministeren

19. juni 2014

J nr. 2014-1502

/

Svar
Nedenfor redegør finansministeren, under hvis ressort Digitaliseringsstyrelsen og Statens It er placeret, for de generelle tiltag på tværs af staten, inden jeg redegør for de konkrete tiltag på Klima-, Energi- og Bygningsministeriets område.

Generelle initiativer for alle ministerområder
Regeringen har besluttet, at alle statslige myndigheder skal implementere sikkerhedsstandarden ISO27001, som stiller en række krav til styringen af sikkerhedsarbejdet, herunder at der arbejdes risikobaseret med sikkerhed, og at sikkerheden forankres i topledelsen.

Med henblik på en forbedret koordinering af sikkerhedsindsatsen på tværs af den offentlige sektor har regeringen nedsat en tværministeriel arbejdsgruppe, som skal udarbejde en strategi for cyber- og informationssikkerhed. Strategien forventes lanceret i år.

Derudover har regeringen truffet beslutning om, at 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 administrator-privilegier), som i henhold til Rigsrevisionens beretning til statsrevisorerne 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 for ministerområder der er kunde hos Statens It

Hovedparten af Klima-, Energi- og Bygningsministeriet er kunde hos Statens It. Hermed er dele af de sikkerhedsmæssige tiltag varetaget gennem den infrastruktur, Statens It tilbyder, samt de ydelser der er indgået aftale om.

Initiativer hos Statens It, som giver forbedret beskyttelse mod hackerangreb hos Statens It's kunder, er blandt andre følgende:

- Statens It har indført en standardiseret pc-arbejdsplads og et fælles datacenter med en samlet styring af computere og infrastruktur. Herunder er der indført strukturerede sikkerhedsopdateringer og mulighed for begrænsning af lokale administrative rettigheder og download.
- 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 tydeliggørelse af ansvarsplacering, herunder om sikring mod hackerangreb og beskyttelse af fortrolige data.
- Aftalegrundlaget mellem Statens It og kunderne er opdateret i 2014 med yderligere præcisering af roller og ansvar i forbindelse med it-sikkerhed og eventuel skærpelse af krav vedrørende beskyttelse af systemer og data, herunder øget anvendelse af databehandleraftaler.

Indenfor Klima-, Energi- og Bygningsministeriets område
Klima-, Energi- og Bygningsministeriet indgik i beretning 3/2013 om forebyggelse af hackerangreb og afgav i den forbindelse en ministerredegørelse.

Af ministerredegørelsen fremgår, at der vil blive taget initiativ til, at virksomhederne under Klima-, Energi- og Bygningsministeriet udbygger deres respektive risikovurderinger med beretningens tre sikringstiltag, og at der etableres en procedure, der sikrer, at risikovurderingen godkendes af virksomhedens ledelse.

Herudover nævnes i ministerredegørelsen, at kendskab til og anvendelse af vejledningen "Cyberforsvar der virker – køreplan for et godt cyberforsvar" vil være et fokusområde for ministeriet.

Endelig nævnes i ministerredegørelsen, at overgangen til statens it-arbejdsplads med automatisk softwareopdatering, oprettelse af et Koncern-it-forum, udarbejdelse af en koncernfælles it-strategi, opdatering af institutionernes it-sikkerhedsstrategier, så de overholder sikkerhedsstandard ISO27001, sikkerhedstest af egne hjemmesider og en løbende dialog med Center for Cybersikkerhed vil blive implementeret i hele eller dele af koncernen.

Med venlig hilsen

Rasmus Helveg Petersen