Folketingets Forsvarsudvalg
Christiansborg

Finansministeren
18. juni 2014

Svar på Forsvarsudvalgets spørgsmål nr. 250 stillet af Troels Lund Poulsen (V) den 26. maj 2014.

Spørgsmål:
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:
Jeg kan oplyse, at der er igangsat en række initiativer med henblik på at styrke ressortministeriernes arbejde for at understøtte it-sikkerheden.

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), tiltag, 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
Finansministeriet 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 Finansministeriets område
Finansministeriet har udarbejdet handlingsplaner for implementering af sikkerhedsstandarden ISO27001 og gennemført væsentlige dele af planerne. Konkret er Statens It i februar 2014 blevet certificeret i henhold til standarden.

Aftalerne med leverandører, herunder Statens It revideres løbende med henblik på at tydeliggøre ansvarsplacering.

Det er besluttet, at de standardiserede pc-arbejdspladser i Finansministeriet udnytter muligheden for at begrænse administrative rettigheder og dermed download, og at afvigelse herfra kræver eksplicit chefgodkendelse.

Med venlig hilsen

Bjarne Corydon