ERHVERVS- OG VÆKSTMINISTERIET

ERHVERVS- OG
VÆKSTMINISTEREN

23. juni 2014

ERHVERVS- OG
VÆKSTMINISTERIET

Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax. 33 12 37 78
CVR-nr. 10092485
EAN nr. 5798000026001
evm@evm.dk
www.evm.dk

Besvarelse af spørgsmål 262 alm. del stillet af Folketingets Forsvarsudvalg den 26. maj 2014 efter ønske fra Troels Lund Poulsen (V).

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:
I Erhvervs- og Vækstministeriet varetages opgaver i relation til beskyttelse af it-systemer og fortrolige data samt sikring mod hackerangreb på tre niveauer.

For det første er Erhvervs- og Vækstministeriet omfattet af regeringens generelle initiativer.

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.

Erhvervs- og Vækstministeriet er tilsluttet Center for Cybersikkerheds varslingstjeneste for internettrusler, GovCert. Erhvervs- og Vækstministeriet modtager således oplysninger om konkrete cybertrusler, som GovCert måtte identificere og informere sin brugerkreds om.

For det andet er Erhvervs- og Vækstministeriets departement og underliggende styrelser i varierende omfang alle kunder i 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.

For det tredje vedtog Erhvervs- og Vækstministeriet i september 2013 et sæt koncernfælles retningslinjer for it og it-sikkerhed. Hvad it-sikkerhed angår, er retningslinjerne fokuseret omkring koncernens faktiske it-sikkerhed. I efteråret 2013 og i foråret 2014 gennemførtes der med bistand fra eksterne it-sikkerhedskonsulenter to it-sikkerhedsafprøvninger med henblik på at afdække og vurdere it-sikkerhedsniveauet inden for et afgrænset område.

Der følges op på disse it-sikkerhedsafprøvninger i samarbejde med Digitaliseringsstyrelsen og Statens It samt øvrige relevante eksterne leverandører.

Endelig deltog Søfartsstyrelsen i krisestyringsøvelsen i november 2013, som havde til formål at afprøve, hvordan myndigheder, herunder Den Nationale Operative Stab (NOST), og ramte aktører håndterer en situation, hvor Danmark bliver offer for et cyberangreb, og hvor kritisk infrastruktur og digitale kommunikationskanaler sættes ud af kraft.