MINISTERIET FOR SUNDHED OG FOREBYGGELSE

Holbergsgade 6
DK-1057 København K

T +45 7226 9000
F +45 7226 9001
M sum@sum.dk
W sum.dk

Folketingets Forsvarsudvalg

Dato: 23. juni 204
Enhed: Sundhedsøkonomi
Sagsbeh.: DEPMOA
Sags nr.: 1403421
Dok nr.: 1478914

Folketingets Forsvarsudvalg har den 26. maj 2014 stillet følgende spørgsmål nr. 259 (Alm. del) til ministeren for sundhed og forebyggelse, som hermed besvares. Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V).

Spørgsmål nr. 259:
"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:
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 på Ministeriet for Sundhed og Forebyggelses ministerområde
Ministeriet for Sundhed og Forebyggelse har i foråret 2014 udarbejdet en ny koncern it-strategi, som blandt andet omfatter informationssikkerhed. Således

vil Ministeriet for Sundhed og Forebyggelse benytte sig af relevante standarder, herunder ISO27001, som nu implementeres.

Endvidere har National Sundheds-IT (NSI), som har det overordnet ansvar for informationssikkerheden på ministerområdet i forlængelse af Forsvarets Efterretningstjenestes Center for Cybersikkerhed's (CfC) vejledning "Cyberforsvar, der virker" iværksat en række tiltag for at begrænse risikoen for cyberangreb mod Ministeriet for Sundhed og Forebyggelse

1. Systematisk registrering af informationsaktiver (systemer, data m.v.) og risikovurdering af ministeriets systemportefølje

Som et af de første skridt mod et højere sikkerhedsniveau anbefaler vejledningen, at topledelsen får overblik over de væsentligste informationsaktiver som f.eks. systemer, data og netværk og tager stilling til, hvor kritiske de er for organisationens opgaveløsning.

NSI er i gang med at etablere et systemkatalog, der giver et overblik over de systemer og services på ministeriets område, som enten driftes af NSI eller hvor NSI står for aftalen med en ekstern driftsleverandør. En oversigt forventes at ligge klar i begyndelsen af 4. kvartal 2014.

2. Begrænsning af lokaladministratorrettigheder på SSI
Det anbefales i vejledningen, at man begrænser medarbejdernes lokale administratorrettigheder, så disse ikke længere selv direkte kan downloade programmer fra internettet.

I Departementet, Sundhedsstyrelsen og Patientombuddet er der i dag begrænsninger på anvendelsen af lokaladministratorrettigheder, mens pc'ere på Statens Seruminstitut (SSI) stadig opsættes med lokale administratorrettigheder.

NSI vil i 3. kvartal 2014 igangsætte et projekt med henblik på at afklare, hvordan man kan begrænse brugen af lokale administratorrettigheder på SSI og samtidig give medarbejderne de nødvendige it-værktøjer til understøttelse af deres arbejdsopgaver. I den forbindelse vil der ligeledes bliver udarbejdet en positivliste over programmer. På grund af bredden i SSI's virksomhed anvendes der mange hundrede programmer og applikationer på instituttet i dag, hvilke NSI i fremtiden skal tilbyde en sikker adgang til – ud fra den nævnte positivliste.

3. Løbende sikkerhedsopdateringer af programmer og operativsystemer
SSI laver løbende sikkerhedsopdateringer af programmer og operativsystmer, så alle institutionerne i koncernen lever op til vejledningens anbefalinger vedr. brug af operativsystem.

4. Løbende sikkerhedsanalyser og penetrationstests
NSI vil løbende lave penetrationstests for at lokalisere evt. svagheder for efterfølgende at kunne udbedre disse. Senest lavede NSI en penetrationstest i december 2013, hvilket førte til diverse udbedringer. Den næste penetrationstest gennemføres i løbet af 2. halvår 2014.

5. Løbende opfølgning på eksterne leverandører
En række store forretningskritiske systemer så som Landspatientregisteret, Det fælles Medicinkort og Dansk Patientsikkerhedsdatabase er placeret hos eksterne driftsleverandører.

NSI holder løbende kontakt med de eksterne leverandører vedr. deres sikkerhedsforanstaltninger i relation til cyberangreb, herunder modtager vi årligt deres revisionserklæring vedr. de generelle it-kontroller til opfølgning.

Fremadrettet vil NSI i forbindelse med driftsudbud stille krav om, at de eksterne leverandører skal redegøre for deres sikkerhedsforanstaltninger i relation til cyberangreb, så dette kommer til at indgå som en del af kontraktgrundlaget

6. Monitorering af ministeriets internetforbindelser
Som et led i forsvaret mod cyberangreb anbefaler vejledningen, at der opbygges kapacitet til at opdage og undersøge angreb. Dette kan ske gennem løbende overvågning og logning af trafikken på internetforbindelserne.

I den forbindelse har NSI igangsat initiativer, der skal indhøste erfaringer med monitoreringen og højne kompetenceniveauet hos relevante medarbejdere.

Med venlig hilsen

Nick Hækkerup / Morten Andersen