JUSTITSMINISTERIET

Folketinget
Forsvarsudvalget
Christiansborg
1240 København K

Dato: 8. september 2014
Kontor: Økonomistyrings-kontoret
Sagsbeh: Sidse Hansen Ünal
Sagsnr.: 2014-0032-1316
Dok.: 1184373

Hermed sendes endelig besvarelse af spørgsmål nr. 254 (Alm. del), som Folketingets Forsvarsudvalg har stillet til justitsministeren den 26. maj 2014. Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V).

Karen Hækkerup

/

Anette Görtz

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 254 (Alm. del) fra Folketingets Forsvarsudvalg:

> ”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 indledningsvis oplyse, at der er igangsat en række fællesstatslige initiativer med henblik på at styrke ressortministeriernes arbejde for at understøtte it-sikkerheden.

Regeringen har således 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 endvidere nedsat en tværministeriel arbejdsgruppe, som skal udarbejde en strategi for cyber- og informationssikkerhed. Justitsministeriet deltager i den tværministerielle arbejdsgruppe.

Derudover har regeringen truffet beslutning om, at alle statslige myndigheder med udgangspunkt i en risikovurdering skal implementere konkrete sikkerhedstiltag (eksempelvis positivliste af godkendte programmer, opdatering af programmer med sikkerhedsopdateringer, begrænsning af brugeradgange med særlige administrator-privilegier). Tiltag som, i henhold til *Beretning til Statsrevisorerne om forebyggelses af hackerangreb*, kan forhindre en væsentlig del af de målrettede cyberangreb.

På Justitsministeriets område er der et stort fokus på beskyttelse af ministeriets data, herunder på implementeringen af de tiltag som er anbefalet i vejledningen *Cyberforsvar der virker* fra Digitaliseringsstyrelsen og Center for Cybersikkerhed.

Samtlige institutioner på Justitsministeriets område er i den forbindelse i gang med implementeringen af sikkerhedsstandarden ISO27001. Justitsministeriets departement følger implementeringsarbejdet.

I *Cyberforsvar der virker* er der anført fire sikringstiltag, som kan styrke cyberforsvaret. Samtlige institutioner på ministerområdet har forholdt sig til anbefalingerne og har iværksat opfølgende tiltag.

I alle institutioner foreligger der endvidere vejledninger og politikker for it-sikkerheden. Herudover udøver PET sin funktion som it-sikkerhedsmyndighed gennem løbende rådgivning af myndighederne på Justitsministeriets område. Departementet fører desuden tilsyn med it-sikkerheden på ministerområdet.

Afslutningsvis kan det oplyses, at det følger af Statsministeriets cirkulære nr. 9846 af 20. december 2013 (sikkerhedscirkulæret) § 26, at alle former for elektroniske informationssystemer og netværk beregnet til frembringelse, bearbejdning, kommunikation eller lagring af informationer klassificeret HEMMELIGT eller FORTROLIGT skal sikkerhedsgodkendes af den relevante it-sikkerhedsmyndighed, dvs. PET for Justitsministeriets område. PET fører løbende tilsyn med disse systemer.