FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

Folketingets Forsvarsudvalg
Christiansborg

FORSVARSMINISTEREN

23. juni 2014

Folketingets Forsvarsudvalg har den 26. maj 2014 stillet følgende spørgsmål nr. 260 til forsvarsministeren, som hermed besvares. Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V).

Spørgsmål nr. 260:
"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:
Forsvarets Efterretningstjeneste (FE) er anmodet om en udtalelse til brug for Forsvarsministeriets besvarelse. FE har i den anledning oplyst følgende:

"Forsvarets Efterretningstjenestes Center for Cybersikkerhed er national it-sikkerhedsmyndighed, og som en direkte opfølgning på Statsrevisorernes beretning har Center for Cybersikkerhed sammen med Digitaliseringsstyrelsen udgivet vejledningen "Cyberforsvar der virker". Vejledningen beskriver en række konkrete sikringstiltag, som myndigheder og virksomheder bør overveje for at imødegå den stadigt stigende risiko for alvorlige cyberangreb.

Som led i den styrkelse af den forebyggende indsats på cybersikkerhedsområdet, som skete ved etableringen af Center for Cybersikkerhed, udgiver centeret i øvrigt løbende

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

vejledninger og giver anbefalinger til især de statslige myndigheder om cybersikkerhed. Den forebyggende indsats supplerer et andet vigtigt indsatsområde for Center for Cybersikkerhed, nemlig centerets netsikkerhedstjeneste, der bistår andre myndigheder samt virksomheder, der varetager samfundsvigtige funktioner, ved at opdage, analysere og bidrage til at imødegå cyberangreb. Det bemærkes i den forbindelse, at en række myndigheder under Forsvarsministeriet er tilsluttet Center for Cybersikkerheds netsikkerhedstjeneste.

Derudover kan det nævnes, at Center for Cybersikkerhed samarbejder med uddannelses- og forskningsinstitutioner med henblik på at sikre, at Danmark også i fremtiden har de nødvendige kompetencer til at beskytte den digitale infrastruktur mod cybertrusler.

For at styrke fokus på cybersikkerheden hos topledelsen i ministerierne og øge ministeriernes viden om det aktuelle trusselsbillede på cybersikkerhedsområdet har Forsvarsministeriet endvidere netop taget initiativ til at nedsætte en tværministeriel kontaktgruppe vedrørende cybersikkerhed. Denne gruppe ventes at holde sit første møde i september 2014.

På Forsvarsministeriets område fastlægger Center for Cybersikkerhed – som led i funktionen som it-sikkerhedsmyndighed – de militære it-sikkerhedsbestemmelser. Heraf følger blandt andet, at Center for Cybersikkerhed skal inddrages i alle it-udviklingsprojekter, hvor it-systemerne skal behandle højere klassificerede informationer. Inddragelsen omfatter såvel rådgivning som sikkerhedsgodkendelse.

Herudover har Center for Cybersikkerhed en regelmæssig dialog med Forsvarets myndigheder om trusler, it-sikkerhed og it-sikkerhedshændelser. Center for Cybersikkerhed gennemfører også i samarbejde med den militære sikkerhedsmyndighed it-sikkerhedseftersyn ved Forsvarets myndigheder og bidrager med sikkerhedsteknisk analyse af it-sikkerhedshændelser.

Center for Cybersikkerhed forventer indenfor kort tid at udsende en opdatering af de militære it-sikkerhedsbestemmelser, således at bestemmelserne følger principperne i den internationale standard ISO 27001 og bliver bredt dækkende for alle Forsvarets it-systemer uanset klassifikation. Det indebærer blandt andet, at der for alle systemer skal gennemføres en risikovurdering."

Med venlig hilsen

Nicolai Wammen