STATSMINISTERIET
CHRISTIANSBORG
Prins Jørgens Gård 11, 1218 København K
Telefon 33 92 33 00 - Telefax 33 11 16 65
CVR-NR. 10-10-39-40
EAN-lokationsnummer 5798000000032

Dato: 24-06-2014
Sagsnr.: 2014 - 3467

Folketingets Forsvarsudvalg
Christiansborg

Statsministerens besvarelse af spørgsmål nr. 248 (FOU alm. del). Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen, (V).

Spørgsmål nr. 248:

"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:

Indledningsvis kan det oplyses, at Statsministeriet løbende arbejder med at efterleve sikkerhedsstandarden ISO27001, som stiller en række krav til styringen af sikkerhedsarbejdet.

Det gælder også, for så vidt angår kravene til organiseringen af sikkerhedsarbejdet, som er forankret i ministeriets it-sikkerhedsudvalg, som konkret drøfter ministeriets it-sikkerhedspolitik og -strategi, konkrete sikkerhedshændelser mv.

Statsministeriet vil desuden deltage i den netop nedsatte tværministerielle arbejdsgruppe, som skal udarbejde en strategi for cyber- og informationssikkerhed.

Statsministeriet har en individuel tilpasset it-sikkerhedsløsning. Det betyder, at ministeriet selv udvikler egne sikre it-løsninger på eget udstyr tilpasset det til enhver tid gældende trusselsbillede.

Statsministeriet har således gennem et mangeårigt fokus på udarbejdelse af sikre it-løsninger opnået en robust it-infrastruktur med høje krav til kontrol og dokumentation.

Centrale mål i Statsministeriets it-sikkerhedsstrategi er, at et højt it-sikkerhedsniveau skal sikre, at uvedkommende ikke kan få adgang til Statsministeriets netværk, at der ikke mistes eller ændres data, og at Statsministeriet ikke kompromitteres gennem driftsnedbrud og/eller sikkerhedstrusler.

Dette opnås gennem en løbende risiko- og omkostningsvurdering, som skal sikre det fornødne grundlag for at vurdere behovet for nye sikkerhedstiltag.

Løsningerne udarbejdes med tostrengede sikkerhedsstrategier. Det skal sikre, at der for alle væsentlige systemer arbejdes med to adskilte lag af sikkerhed. Hermed sikres data, selv ved fejl mv. i det enkelte software og udstyr.

Der anvendes funktionsadskillelse, opdeling af datatyper samt fokus på brugernes efterlevelse af it-sikkerheden gennem løbende kontrol, ledelsesrapportering og efteruddannelse.

Der er endnu ikke konstateret hændelser, hvor det er lykkedes udefra kommende at opnå uretmæssig adgang til Statsministeriets data.

Med venlig hilsen

Helle Thorning-Schmidt