UDENRIGSMINISTERIET

Dato: 23. juni 2014
Spørgsmål: FOU alm. del. spm. nr. 251 af 26. maj 2014 stillet til udenrigsministeren af Troels Lund Poulsen (V).

FOU alm. del, spørgsmål nr. 251:
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:
Udenrigsministeriet har et tæt samarbejde med de nationale sikkerhedsmyndigheder om cybersikkerhed og optimering af it-sikkerhed i bred forstand.

Udenrigsministeriets IT-netværk er bygget op på en måde, hvor der tilføjes stadig mere robuste "sikkerhedslag" i takt med, at følsomheden stiger. Disse sikkerhedsforanstaltninger skal løbende opdateres, testes, og hærdes yderligere i forhold til trusselsbilledet. Udenrigsministeriet har gennem flere år implementeret de 4 sikringstiltag, som Center for Cybersikkerhed fremhæver som værende de absolut vigtigste: Applikationsstyring, opdatering af programmer og styresystemer, samt udvidet rettighedsstyring. Samtidig er Udenrigsministeriet i gang med implementering af sikkerhedsstandarden ISO27001, som Regeringen har besluttet skal være gældende for samtlige statslige myndigheder.

Foruden de tekniske sikkerhedsforanstaltninger gør Udenrigsministeriet meget ud af at højne medarbejdernes sikkerhedsbevidsthed, gennem introduktionskurser og kampagner. Udenrigsministeriets it-bestyrelse, hvor også ministeriets øverste ledelse er repræsenteret, følger sikkerhedsarbejdet tæt og inddrages i væsentlige beslutninger om IT-sikkerhed.