Forsvarsudvalget
Christiansborg

UNI•C - Styrelsen for It og Læring

Vester Voldgade 123
1552 København V
Tlf. 3587 8889
Fax 3587 8890
E-mail uni-c@uni-c.dk
www.uni-c.dk
CVR nr. 13223459

23-06-2014

Svar på spørgsmål 258 (Alm. del):
I brev af 26. maj har udvalget efter ønske fra Troels Lund Poulsen (V) stillet mig følgende spørgsmål:

Spørgsmål 258:
"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:
Undervisningsministeriet har implementeret sikkerhedsstandarden ISO27001, som stiller en række krav til styringen af sikkerhedsarbejdet, herunder at der arbejdes risikobaseret med sikkerhed, og at sikkerheden forankres i topledelsen.

I Undervisningsministeriets koncern varetages it-sikkerheden af UNI-C – Styrelsen for It og Læring. Styrelsen foretager i henhold til den gældende it-sikkerhedspolitik en regelmæssig vurdering af risikobilledet.

Den seneste vurdering, foretaget i april 2013, tager afsæt i statusrapporter og trusselsvurderinger fra Center for Cybersikkerhed, og har resulteret i en igangværende implementering af følgende modforanstaltninger:

- Teknisk sikring og beredskab mod ondsindet overbelastning af koncernens it-systemer ("Denial of Service"-angreb)
- Automatisk opdatering af software på medarbejder-pc'er

- Forbedret adgangskontrol ved adgang til koncernens it-systemer fra internettet

Dette suppleres nu af, at styrelsen er i færd med at vurdere de konkrete modforanstaltninger foreslået i Rigsrevisionens beretning om it-sikkerhed i staten. Denne vurdering forventes afsluttet i efteråret 2014.

Styrelsen foretager efter behov test af sikkerheden i koncernens it-systemer med særlig fokus på cybertrusler. Styrelsens efterbehandling omfatter prioritering og udbedring af de afdækkede sårbarheder.

Styrelsen er i færd med at kategorisere ministeriets it-systemer og har i den forbindelse særligt fokus på behovet for datasikkerhed i ministeriets it-systemer.

Med venlig hilsen

Christine Antorini