Skatteministeriet

23. juni 2014
J.nr. 14-3131464

Til Folketinget – Forsvarsudvalget

Hermed sendes svar på spørgsmål nr. 252 af 26. maj 2014 (alm. del). Spørgsmålet er stillet efter ønske fra Troels Lund Poulsen (V).

Morten Østergaard

/ Kiann Stenkjær Hein

Spørgsmål

Idet 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 henholde mig til følgende, som jeg har modtaget fra SKAT:

"SKAT indsamler og modtager dagligt informationer om trusler og sårbarheder, som potentielt kan udgøre en risiko for sikkerheden. Som en del af risikostyringen sikrer SKAT, at der bliver etableret modforanstaltninger, som på passende vis kan imødegå risici. SKAT sikkerhedsauditerer sine it-leverandører med henblik på at sikre, at de overholder gældende standarder på sikkerhedsområdet. Endvidere indgår Skatteministeriet i et tæt samarbejde med Forsvarets Efterretningstjeneste, hvori der indgår en tæt overvågning af de udadvendte digitale kommunikationskanaler.

SKAT forsøger til enhver tid at sikre, at de administrative processer, der er knyttet til drift af SKATs systemer, er af høj kvalitet og følger best practice på området. Statsrevisorernes beretning 3/2013 har ikke givet anledning til en ændret praksis i SKAT.

SKAT arbejder målrettet med at kvalitetssikre styringen af SKATs aktiver, herunder at etablere procedurer og cyklusser, som understøtter den daglige drift. SKAT har sikret nedenstående områder, som er eksplicit nævnt i Statsrevisorernes beretning 3/2013, så de kan modsvare de trusler, der forventeligt måtte opstå:

1. Begrænsning i download af programmer

SKAT har som standard blokeret for download af programmer og eksekverbare filer. Dog har enkelte medarbejdere mulighed for at foretage downloads, hvis dette er påkrævet i deres jobfunktion.

2. Brugen af lokaladministratorer og om anvendte programmer mv.

SKAT har begrænset brugen af lokaladministratorer, så kun de medarbejdere, hvis jobfunktion kræver det, er lokaladministratorer.

3. Systematisk sikkerhedsopdatering af systemer

SKAT gennemfører en vedvarende og systematisk sikkerhedsopdatering af SKATs systemer.

Som en del af Skatteministeriets udvikling på sikkerhedsområdet er ministeriet, som besluttet af regeringen, i gang med at overgå til den internationale sikkerhedsstandard, den såkaldte ISO27001. Standarden giver en forenkling af arbejdet med informationssikkerhed, men kræver også løbende opfølgning og evaluering af bl.a. risikovurderingen og SOA-dokumenter (Statement Of Applicability, som er en kvalitetsmanual). ISO-standarden stiller færre bindende krav til institutionerne, hvormed sikkerhedsforanstaltningerne i højere grad vil afhænge af den enkelte institutions behov. ISO-standarden forventes fuldt implementeret i løbet af 2014."