FINANSMINISTERIET

Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

Finansministeren

20. december 2013

Finansministeriets redegørelse vedrørende Statsrevisorernes beretning nr. 3/2013 om forebyggelse af hackerangreb.

Under henvisning til Statsrevisorernes skrivelse af 22. oktober 2013, hvormed fulgte beretning nr. 3/2013 om forebyggelse af hackerangreb skal jeg hermed – i overensstemmelse med § 18, stk. 2 i lov om revisionen af statens regnskaber m.m. – redegøre for de foranstaltninger og overvejelser, som beretningen giver anledning til.

Statsrevisorerne konstaterer i beretningen, at de undersøgte statslige virksomheder, herunder Finansministeriet, ikke har tilstrækkelig sikring mod hackerangreb eller tilstrækkelig beskyttelse af systemer og personlige data. Jeg har noteret mig dette.

Jeg er generelt enig i Rigsrevisionens observationer og finder konklusionerne retvisende ud fra en aktuel status på tidspunktet for Rigsrevisionens undersøgelse. Jeg er dermed også enig i, at tiltag på baggrund af beretningens anbefalinger, styrker sikkerheden i forhold til at forebygge hackerangreb rettet mod det interne netværk via pc-arbejdspladser i koncernen.

I forlængelse af dette kan jeg oplyse, at en løbende tilpasning af sikkerhedsindsatsen, herunder indførelse af konkrete sikringstiltag, er et fokusområde i Finansministeriet. En væsentlig del af denne indsats indgår i Finansministeriets aktiviteter i forbindelse med indførelsen af sikkerhedsstandarden ISO27001.

Desuden har Finansministeriets styrelser allerede gennemført aktiviteter og igangsat initiativer, der ud over at sikre håndtering af beretningens specifikke anbefalinger også adresserer andre sikkerhedsmæssige risici i forbindelse med en bredere sikring af koncernens netværk mod hackerangreb. Af konkrete initiativer på området kan nævnes:

- Indførelse af standardiseret pc-arbejdsplads med automatiseret softwareopdatering og mulighed for begrænsede rettigheder, herunder for download;
- Forbedret aftalegrundlag mellem Statens It og kunderne med tydeliggørelse af ansvarsplacering, herunder for sikring af persondata;

- Samarbejde med Center for Cybersikkerhed om udarbejdelse af vejledninger til sikringstiltag mod hackerangreb;
- Separering af netværk gennem firewalls, for at hindre spredning mellem kunder;
- Aftale med Center for Cybersikkerhed om monitorering af trafik til og fra datacenteret;
- Awareness aktiviteter med introduktion af informationssikkerhed for nye medarbejdere og udsendelse af sikkerhedsråd til alle medarbejdere.

Statens Its særlige rolle som leverandør har endvidere ført til beslutning om certificering efter ISO27001-standarden, som ventes opfyldt i løbet af få måneder.

Jeg er derfor af den opfattelse, at igangværende og planlagte indsatser vil imødekomme beretningens anbefalinger.

Jeg tager Statsrevisorernes beretning til efterretning og vil følge op på de igangsatte initiativer, herunder de aktiviteter der er relateret til beretningens konkrete anbefalinger.

Eksemplar af nærværende redegørelse fremsendes samtidig til Rigsrevisionen.

Med venlig hilsen

Bjarne Corydon