RIGSREVISIONEN

Notat til Statsrevisorerne om beretning om forebyggelse af hackerangreb

Februar 2014

revision

revision

revision

Vedrører:
Statsrevisorernes beretning nr. 3/2013 om forebyggelse af hackerangreb

Klima-, energi- og bygningsministerens redegørelse af 13. december 2013
Finansministerens redegørelse af 20. december 2013
(Finansministerens redegørelse er modtaget i Rigsrevisionen den 22. december 2013)

22. januar 2014

RN 1402/14

1. Dette notat handler om de initiativer, som klima-, energi- og bygningsministeren og finansministeren har iværksat som følge af Statsrevisorernes bemærkninger og beretningens indhold og konklusioner.

KONKLUSION

Klima-, energi- og bygningsministeren og finansministeren har oplyst, at der er taget en række initiativer for at styrke forebyggelsen af hackerangreb i ministerierne. Rigsrevisionen finder initiativerne tilfredsstillende og vurderer, at beretningssagen kan afsluttes.

Rigsrevisionens årsrevision vil dog i forbindelse med it-revisionen af Statens It fortsat følge de tværgående initiativer, som har betydning for de virksomheder, der er tilsluttet Statens It. Det gælder dels hindring af spredning af hackerangreb blandt de tilsluttede virksomheder, dels udarbejdelsen af en forbedret kundeaftale.

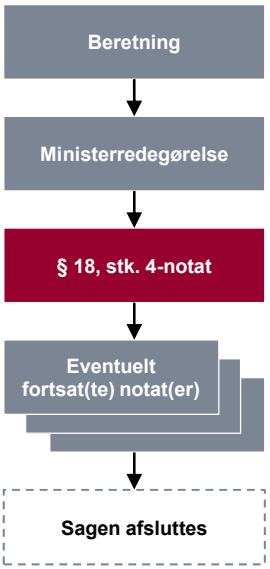
Rigsrevisionens årsrevision vil ligeledes i forbindelse med de kommende års it-revisioner af statslige virksomheder have fokus på deres implementering af sikkerhedsstandarden ISO 27001, og om anbefalingerne i den nye vejledning "Cyberforsvar der virker" er fulgt.

Hvis Rigsrevisionen ikke finder initiativerne tilstrækkelige, vil Rigsrevisionen orientere Statsrevisorerne herom i beretning om revisionen af statsregnskabet.

Rigsrevisionen baserer konklusionen på følgende:

- Klima-, energi- og bygningsministeren vil tage initiativ til, at virksomhederne på ministerområdet udbygger deres risikovurderinger med de 3 sikringstiltag, og at der etableres en procedure, som sikrer, at risikovurderingen godkendes af virksomhedens ledelse.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

- Finansministeren har igangsat initiativer, der – ud over at sikre håndtering af beretningens specifikke anbefalinger – også medfører en bredere sikring af Finansministeriets virksomheder mod hackerangreb, herunder indførelse af en standardiseret pc-arbejdsplads, den såkaldte Statens It-Arbejdsplads (SIA).

- Finansministeriet har endvidere etableret et samarbejde med Center for Cybersikkerhed om udarbejdelse af vejledninger til sikringstiltag mod hackerangreb.

- Endelig arbejder Finansministeriet på at tydeliggøre ansvarsplaceringen i en forbedret kundeaftale mellem Statens It og virksomhederne, og har igangsat separering af netværk for at hindre, at et hackerangreb mod en virksomhed med utilstrækkelige sikringstiltag spreder sig til andre statslige virksomheder.

I. Baggrund

2. Rigsrevisionen afgav i oktober 2013 en beretning om forebyggelse af hackerangreb. Beretningen handlede om, hvorvidt de undersøgte statslige virksomheder i lyset af den stigende digitalisering havde håndteret risikoen for hackerangreb og havde implementeret 3 aktuelle og væsentlige sikringstiltag, og om Statens It havde håndteret risikoen for spredning af hackerangreb mellem virksomheder, der er tilsluttet Statens It.

Beretningen viste, at de undersøgte virksomheder ikke systematisk havde forebygget hackerangreb ved teknisk at begrænse download af programmer fra internettet og brugen af lokaladministratorer, ligesom det kun var 2 ud af 4 virksomheder, der systematisk sørgede for at sikkerhedsopdatere deres programmer. Der var endvidere ikke i virksomhedernes risikovurderinger dokumentation for, at ledelsen havde taget stilling til den risiko, virksomheden udsatte sig for ved ikke at have implementeret de 3 sikringstiltag.

Beretningen viste også, at Statens It ikke i tilstrækkelig grad havde undersøgt risikoen for, at et hackerangreb på én virksomhed med utilstrækkelige sikringstiltag kunne sprede sig til andre virksomheder. Endelig viste beretningen, at opgavesplittet mellem Statens It og virksomhederne – hvad angår sikring mod hackerangreb – ikke er klart.

3. Da Statsrevisorerne behandlede beretningen, bemærkede de, at de fandt det foruroligende, at der i de undersøgte statslige virksomheder havde været utilstrækkelig sikring mod hackerangreb og utilstrækkelig beskyttelse af it-systemer og fortrolige digitale data. Statsrevisorerne fandt det endvidere utilfredsstillende, at der på undersøgelsestidspunktet var en unødig stor risiko for hackerangreb, som kunne føre til misbrug af it-systemer og fortrolige data.

4. Som det fremgår af beretningen, er det Rigsrevisionens vurdering, at undersøgelsens resultater kan være gældende for en større kreds af statslige virksomheder end de netop undersøgte på Klima-, Energi- og Bygningsministeriets og Finansministeriets områder.

Dette notat indeholder alene Rigsrevisionens vurdering af de initiativer, som klima-, energi- og bygningsministeren og finansministeren har iværksat som følge af beretningen. Flere af de initiativer, som Statens It under Finansministeriet iværksætter, vil dog have betydning for de p.t. ca. 80 statslige virksomheder, der er tilsluttet Statens It.

Hele sagen og dens dokumenter kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

II. Gennemgang af ministrenes redegørelser

5. I det følgende gennemgår Rigsrevisionen klima-, energi- og bygningsministerens og finansministerens initiativer.

Undersøgelse af de 3 sikringstiltag

6. Beretningen viste, at ingen af de 4 undersøgte virksomheder systematisk havde implementeret de anbefalede 3 sikringstiltag mod hackerangreb. Således havde ingen af virksomhederne teknisk begrænset medarbejdernes download af programmer fra internettet eller deres brug af lokaladministratorrettigheder, mens kun 2 af de 4 virksomheder systematisk sikkerhedsopdaterede deres programmer. Rigsrevisionen anbefalede derfor, at Finansministeriet eller Forsvarsministeriet udarbejder vejledning til statslige virksomheder om sikringstiltag mod hackerangreb.

Desuden havde ingen af de 4 virksomheder i deres risikovurdering begrundet deres praksis vedrørende de 3 sikringstiltag, hvormed der ikke var dokumentation for, at ledelsen havde taget stilling til den risiko, som den manglende sikring indebar. Rigsrevisionen anbefalede derfor, at statslige virksomheder i deres risikovurdering forholder sig til hackerangreb, herunder de 3 sikringstiltag.

7. Statsrevisorerne fandt det utilfredsstillende, at der på undersøgelsestidspunktet var en unødig stor risiko for hackerangreb, som kunne føre til misbrug af it-systemer og fortrolige data i ministerierne, og at ledelsen i de undersøgte virksomheder ikke havde foretaget tilstrækkelige risikovurderinger.

8. Finansministeren er generelt enig i Rigsrevisionens observationer og i, at tiltag på baggrund af beretningens anbefalinger styrker sikkerheden i forhold til at forebygge hackerangreb. Ministeren oplyser, at løbende tilpasning af sikkerhedsindsatsen, herunder indførelse af konkrete sikringstiltag, er et fokusområde i Finansministeriet – særligt i forbindelse med indførelsen af sikkerhedsstandarden ISO 27001. Den særlige rolle som it-leverandør har derudover ført til beslutning om certificering af Statens It efter ISO 27001-standarden.

Finansministeren oplyser endvidere, at ministeriets virksomheder allerede har gennemført aktiviteter og igangsat initiativer, der – ud over at sikre håndtering af beretningens specifikke anbefalinger – også medfører en bredere sikring af koncernen mod hackerangreb. Et af initiativerne er at indføre en standardiseret pc-arbejdsplads, den såkaldte Statens It-Arbejdsplads (SIA), med automatiseret softwareopdatering og mulighed for begrænsede rettigheder, herunder for download. Desuden har ministeriet taget initiativ til såkaldte *awareness aktiviteter* med introduktion af informationssikkerhed for nye medarbejdere og udsendelse af sikkerhedsråd til alle medarbejdere. Endelig har ministeriet etableret samarbejde med Center for Cybersikkerhed om udarbejdelse af vejledninger til sikringstiltag mod hackerangreb. Vejledningen ”Cyberforsvar der virker” udkom primo december 2013.

Endelig oplyser finansministeren, at ministeriet vil følge op på de igangsatte initiativer, herunder de aktiviteter, der er relateret til beretningens konkrete anbefalinger.

9. Klima-, energi- og bygningsministeren finder, at Rigsrevisionens anbefalinger kan bidrage til at forbedre it-sikkerheden og forebygge hackerangreb. Ministeren vil derfor tage initiativ til, at virksomhederne på ministerområdet udbygger deres risikovurderinger med de 3 sikringstiltag, og at der etableres en procedure, som sikrer, at risikovurderingen godkendes af virksomhedernes ledelser. Desuden vil ministeren sikre sig, at virksomhederne er bekendt med den nye vejledning ”Cyberforsvar der virker”, og at dens principper bliver anvendt.

Klima-, energi- og bygningsministeren oplyser endvidere, at flere af ministeriets virksomheder har igangsat initiativer, som skal bidrage til at mindske risikoen for hackerangreb, herunder anvendelsen af den standardiserede pc-arbejdsplads (SIA). Desuden vil ministeriet udarbejde en koncernfælles it-strategi og bidrage til erfaringsudveksling ved at oprette et Koncern-it-forum og opdatere institutionernes it-sikkerhedsstrategier, så de overholder sikkerhedsstandarden ISO 27001. Endelig vil ministeriet sikkerhedsteste egne hjemmesider og føre løbende dialog med Center for Cybersikkerhed.

10. Rigsrevisionen finder ministrenes initiativer, herunder udsendelsen af vejledningen "Cyberforsvar der virker", tilfredsstillende. Rigsrevisionens årsrevision vil ved de kommende it-revisioner have fokus på virksomhedernes implementering af sikkerhedsstandarden ISO 27001, og om anbefalingerne i den nye vejledning "Cyberforsvar der virker" er fulgt.

Undersøgelse af særlige sikringstiltag i Statens It

11. Beretningen viste, at Statens It ikke havde vurderet risikoen for eller testet, om et hackerangreb på én virksomhed kan kompromittere it-sikkerheden i andre virksomheder, der er tilsluttet Statens It, dvs. sprede sig såvel inden for samme som på tværs af flere ministerområder.

12. Statsrevisorerne fandt det utilfredsstillende, at Statens It ikke i tilstrækkelig grad havde undersøgt, om et hackerangreb mod en virksomhed med utilstrækkelige sikringstiltag kunne sprede sig til andre statslige virksomheder.

13. Finansministeren oplyser, at man har taget initiativ til separering af netværk gennem firewalls for at hindre spredning mellem kunder og har indgået aftale med Center for Cybersikkerhed om monitorering af trafik til og fra datacenteret.

14. Rigsrevisionen finder det tilfredsstillende, at Statens It har igangsat initiativer for at hindre spredning af hackerangreb. Rigsrevisionens årsrevision vil i forbindelse med kommende it-revisioner af Statens It følge op på disse initiativer, herunder om Statens It har udført test af, om hackerangreb kan sprede sig til andre statslige virksomheder.

Ansvaret for virksomhedernes sikring

15. Beretningen viste, at man på baggrund af kundeaftalen mellem Statens It og virksomhederne ikke entydigt kan afgøre opgavesplittet vedrørende de sikringstiltag, der er behandlet i beretningen.

Rigsrevisionen vurderede, at ansvaret for databeskyttelse gennem sikring af informationssikkerheden i sidste ende ligger hos dataejer i det enkelte ministerium, men anbefalede, at Finansministeriet præciserer opgavesplittet hvad angår sikring mod hackerangreb.

16. Klima-, energi- og bygningsministeren deler Rigsrevisionens opfattelse af, at opgavesplittet ikke er klart og ser frem til, at der sker en præcisering heraf.

17. Finansministeren oplyser, at ministeriet har igangsat et initiativ om forbedret aftalegrundlag mellem Statens It og kunderne med tydeliggørelse af ansvarsplacering, herunder for sikring af persondata.

18. Rigsrevisionen finder det tilfredsstillende, at Statens It har igangsat et initiativ, der kan tydeliggøre ansvarsplaceringen mellem Statens It og virksomhederne. Rigsrevisionens årsrevision vil i forbindelse med kommende it-revisioner følge op på den nye kundeaftales præcisering af opgavesplittet.

III. Afslutning

19. Rigsrevisionen finder klima-, energi- og bygningsministerens og finansministerens initiativer tilfredsstillende og vurderer, at beretningssagen kan afsluttes, idet Rigsrevisionen dog i årsrevisionens it-revision bl.a. vil følge de tværgående initiativer, som berører de virksomheder, der er tilsluttet Statens It. Hvis Rigsrevisionen ikke finder initiativerne tilstrækkelige, vil Rigsrevisionen orientere statsrevisorerne herom i beretning om revisionen af statsregnskabet.

Lone Strøm