ERHVERVSMINISTERIET

Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

ERHVERVSMINISTEREN

ERHVERVSMINISTERIET

Slotsholmsgade 10-12
1216 København K

Tlf. 33 92 33 50
Fax. 33 12 37 78
CVR-nr. 10092485
EAN nr. 5798000026001
evm@evm.dk
www.evm.dk

Ministerens supplerende redegørelse til Statsrevisorerne vedrørende beretning nr. 25/2015 om revisionen af statsregnskabet for 2015

Statsrevisorerne har anmodet om min supplerende redegørelse for de foranstaltninger og overvejelser vedrørende it-sikkerhed, som afsnit *3.2. Status for logning og overvågning af dataaktivitet* i beretning nr. 25/2015 om revisionen af statsregnskabet for 2015 har givet anledning til.

Rigsrevisionen vurderer i sin beretning, at de undersøgte virksomheder, herunder Finanstilsynet, i deres logning og overvågning har mangler.

Logning og overvågning af dataaktivitet og trafik er vigtige elementer i en tidssvarende it-sikkerhedshåndtering. Finanstilsynet har bl.a. derfor gennem flere år anvendt et internationalt anerkendt it-sikkerhedsrådgivningsfirma til løbende at få en vurdering af, hvilke it-sikkerhedsmæssige tiltag, der skulle iværksættes for at imødekomme det gældende trusselsniveau.

Det har bl.a. betydet, at udvikling af sikkerhedsmæssige specifikke krav til eksterne leverandører, interne sårbarhedsscanninger, Network Access Control (automatisering således at "fremmede" enheder ikke kan komme på Finanstilsynets netværk) samt reel Application Whitelistning (aktiv styring af, hvilke programmer som må køre på en maskine), har været højere prioriteret end tiltag for at øge overvågning af dataaktivitet.

I 2015, forud for Rigsrevisionens undersøgelse, tog Finanstilsynet i den prioriterede sikkerhedsindsats beslutning om at investere i et egentligt overvågnings- og logningssystem, et såkaldt SIEM-system.

Efter implementeringen af systemet lagres alle logs nu centralt i logmanagement-systemet. Systemet giver endvidere mulighed for alarmer og løbende rapportering, hvorfor der fremadrettet vil være en løbende proces med at optimere overvågningen af logs.

Finanstilsynet har i 2016 arbejdet med tilsynets driftsleverandør om at begrænse antallet af administratorer mest muligt, under hensyntagen til en fortsat stabil drift. Det har betydet implementering af en såkaldt rollebaseret rettighedsmodel i hele Finanstilsynets it-miljø. Endvidere indebærer

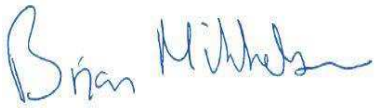
føromtalte centrale logmanagement-system, at medarbejdere i Finanstilsynet og hos tilsynets driftsleverandør ikke længere har mulighed for at fjerne eller ændre i logdata.

Fra og med 2016 lever Finanstilsynet op til ISO 27001-standarden. Det indebærer blandt andet, at ledelsen tager stilling til de overordnede principper for it-sikkerhed, herunder for logning af data. Ledelsen deltager også i udarbejdelsen af den årlige risikovurdering på it-området med udgangspunkt i det aktuelle trusselsbillede og forretningens aktuelle behov.

Det er derfor min vurdering, at Finanstilsynet med de igangsatte og allerede gennemførte initiativer imødegår de påpegede mangler vedrørende logning og overvågning.

Jeg skal bemærke, at ministeriet har sendt eksemplar af ovenstående til rigsrevisor på rr@rigsrevisionen.dk.

Med venlig hilsen



Brian Mikkelsen