



Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

FORSVARSMINISTEREN

6. december 2016

Hermed fremsender jeg min supplerende redegørelse til beretning 25/2015 om statsregnskabet for 2015. Den supplerende redegørelse omhandler de foranstaltninger og overvejelser, som beretningens punkter 50-60 vedrørende logning og overvågning af dataaktivitet har givet anledning til.

Jeg konstaterer med tilfredshed, at Rigsrevisionen samlet set vurderer, at Forsvarets Koncernfælles Informatiktjeneste, der har ændret navn til Kapacitetsansvarlig Koncern IT og nu er en del af Forsvarsministeriets Materiel- og Indkøbsstyrelse, er blandt de to virksomheder i den tværministerielle undersøgelse, der er nået længst med deres indsats på området. Ligeledes konstaterer jeg, at Rigsrevisionen finder, at Kapacitetsansvarlig Koncern IT er den eneste af de undersøgte virksomheder, der overvåger relevante logdata systematisk.

Jeg noterer mig, at en virksomheds ledelse efter Rigsrevisionens opfattelse jævnligt bør tage stilling til behovet for logning og overvågning ud fra det aktuelle trusselsbillede og karakteren af de data, som virksomheden har ansvaret for. Forsvarsministeriets Materiel- og Indkøbsstyrelse har på baggrund af implementeringen af Information Security Management System (ISO27001), herunder risikostyring, tilsikret en tydeligere ledelsesforankring, som i stigende grad sikrer kontrol og opfølgning på logning på baggrund af det aktuelle trusselsbillede og forretningens aktuelle behov.

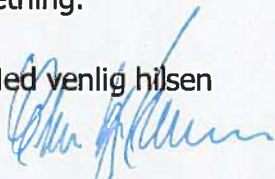
Jeg konstaterer, at Rigsrevisionens finder, at Kapacitetsansvarlig Koncern IT anvender centrale logservere, men ikke opsamler alle relevante logdata på serveren. Rigsrevisionen finder også, at virksomhederne bør styrke det tekniske fundament for deres logning og etablere et

samlet overblik over deres logdata. Generelt kan jeg tilslutte mig synspunktet om, at man bør opsamle relevante data og analysere på disse så effektivt som muligt. I den forbindelse vil jeg nævne, at Kapacitetsansvarlig Koncern IT har igangsat implementeringen af yderligere logningsaktiviteter, herunder log-management.

Jeg noterer mig afslutningsvis, at Rigsrevisionen finder, at Kapacitetsansvarlig Koncern IT har tildelt privilegerede rettigheder til et uforholdsmæssigt stort antal administratorer enten internt i virksomheden eller hos den eksterne driftsleverandør. Rigsrevisionen finder, at virksomhederne skal begrænse adgangen til logdata mest muligt for at minimere risikoen for uautoriseret adgang til disse data. Efter min opfattelse er spørgsmålet om antal af administratorrettigheder et eksempel på et område, hvor de statslige myndigheder til stadighed må afveje hensynet til sikkerhed i forhold til hensynet til effektivitet og opgaveløsning. Kapacitetsansvarlig Koncern IT har derfor tilstræbt sig på kun at tildele det nødvendige antal med de smallest mulige adgangsrettigheder til, at opgaverne kan udføres. Uagtet dette er Forsvarsministeriets nye it-infrastruktur, der implementeres fra 2017, baseret på en ny metode til adgangsrettigheder, idet meget få (ingen som standard) har permanente og generelle rettigheder, men tildeles en specifik rettighed, når en opgave skal udføres på det pågældende system. Det er en kompleks, men meget sikker måde at drive servere på.

Det bemærkes, at den supplerende redegørelse samtidig sendes til Rigsrevisionen til efterretning.

Med venlig hilsen



Claus Hjort Frederiksen