

Vedrørende Beretning nr. 18/2002 om revisionen af statsregnskabet for 2002

Jeg har den 16. december 2003 modtaget Rigsrevisors Beretning nr. 18/2002 til Folketinget om revisionen af statsregnskabet for 2002.

I henhold til § 18, stk. 2 i lov om revisionen af statens regnskaber m.v. skal jeg bemærke følgende: I beretningen anføres på baggrund af den udførte revision, at Rigsrevisionen har vurderet, at regnskabsforvaltningen på Miljøministeriets område samlet set har været tilfredsstillende, at regnskaberne på Miljøministeriets område er rigtige, og at dispositionerne har været i overensstemmelse med bevillinger, love m.v.

Dog har følgende punkter givet Rigsrevisionen anledning til bemærkninger:

- Resultatet af IT-revision ved Miljøministeriets departement karakteriseres som ikke helt tilfredsstillende.
- Resultatet af IT-revision ved Centret for Informatik, Skov- og Naturstyrelsen (Cfl) karakteriseres som ikke tilfredsstillende.

For så vidt angår IT-revisionen ved departementet anfører Rigsrevisionen, at der ikke var udarbejdet en risikoanalyse af IT-anvendelsen, som ledelsen havde taget stilling til. Endvidere var der væsentlige sikkerhedsmæssige svagheder vedrørende adgang fra hjemmearbejdspladser til departementets netværk og i driftspersonalets adgang til egentlige backup-sæt.

Det skal i denne forbindelse bemærkes, at IT-sikkerhed er en kompleks problemstilling, som omfatter alle ministeriets pc'ere, servere, applikationer og tjenester samt ikke mindst brugerne og deres opmærksomhed og accept af det sikkerhedsniveau, der er besluttet.

Miljøministeriet er enig i, at en samlet overordnet risikovurdering, der foretages med jævne mellemrum, er et egnet redskab til at sikre, at der er klare mål for IT-sikkerheden, og at niveauet for IT-sikkerheden fastlægges som en overordnet ledelsesbeslutning.

Ministeriet vil derfor tage initiativ til, at der udarbejdes en overordnet risikovurdering, som kan indgå i ministeriets sikkerhedsramme og i ministeriets IT-strategi.

For så vidt angår de anførte sikkerhedsmæssige svagheder i forbindelse med adgang fra hjemmearbejdspladser til departementets netværk bemærkes, at Miljøministeriet har en instruks, der skal bidrage til, at behandlingen af data på eksternt opkoblet udstyr sker med tilsvarende sikkerhed som for faste PC-arbejdspladser med intern forbindelse til netværkene. Af denne fremgår det, at medarbejderne skal være opmærksom på, at databehandling på eksternt opkoblet udstyr er mere risikabelt end på den almindelige arbejdsplads, hvorfor meget fortrolige data kun bør behandles på internt opkoblet udstyr.

Hjemmearbejdspladser er enten etableret med ISDN-linier eller ADSL-linier. ISDN-linjerne er ikke krypteret i modsætning til ADSL. ISDN-linjerne har dog A-nummerverifikation, hvilket betyder, at der kun kan ringes op fra det godkendte nummer. Der er herved tale om en acceptabel og forsvarlig sikkerhed, selvom sikkerheden er mindre end for ADSL-linjerne.

Det er imidlertid besluttet, at ISDN-linjerne skal udfases til fordel for ADSL, hvor det er teknisk muligt. I departementet er der kun ganske få ISDN-hjemmearbejdspladser tilbage, og disse vil blive konverteret til ADSL i løbet af foråret 2004.

Vedrørende driftspersonalets adgang til backupsæt skal bemærkes, at der er indført regler, der sikrer, at medarbejdere ikke samtidigt har adgang til alle udgaver af systemer og data. I henhold til retningslinierne for backup afleverer den backup ansvarlige backupbåndene til betjentstuen, der er ansvarlig for at lægge bånd i brandskab og tage bånd ud af brandskab.

For så vidt angår IT-revisionen ved Centret for Informatik er Rigsrevisionens vurdering primært begrundet i forholdene omkring centrets administration af sikkerheden i den såkaldte firewall, som beskytter mod uautoriseret adgang til ministeriets netværk. Firewall'en omfatter også Danmarks og Grønlands Geologiske Undersøgelse, Danmarks Miljøundersøgelser og Forskningscentret for Skov & Landskab. Rigsrevisionen har fundet ansvaret for sikkerheden bag firewall'en uklar, idet institutionerne var indbyrdes afhængige. Centret stillede ikke krav til de tilkoblede institutioner, hvorfor det samlede sikkerhedsniveau var ukendt. Herudover anfører Rigsrevisionen, at der manglede en ledelsesgodkendt sikkerhedsvurdering, ligesom der ikke var udført test mod uautoriseret netadgang.

Baggrunden for konstruktionen med den fælles firewall er, at ministeriet siden starten af 1990'erne har praktiseret et tæt samarbejde mellem IT-afdelingerne i de enkelte institutioner om fælles netværk, fælles e-postsystem og andre fælles faciliteter, herunder fælles adgang til Internet og fælles firewall.

På baggrund af Rigsrevisionens bemærkninger har centret iværksat en undersøgelse af forskellige løsninger, der kunne sikre den fornødne kontrol med aktiviteterne inden for den fælles firewall.

Overvejelserne er mundet ud i en løsningsmodel, hvor der etableres en ny struktur, hvor netværkene opdeles i fire zoner baseret på virtuel firewall teknologi. De virtuelle firewalls vil som i dag blive drevet centralt af centret på vegne af de fire zoner ved indgåelse af servicekontrakter. Det er de ansvarlige for de fire zoner, som suverænt bestemmer, hvad der skal tillades på de respektive zonenet.

Der oprettes tillige et fælles udvekslingsnet for hele ministerområdet, som håndterer fælles services og kommunikationsveje mellem de forskellige zoner.

Den nye netværks- og firewall struktur har så megen fleksibilitet, at fremtidige organisatoriske ændringer kan imødekommes, og en tilstrækkelig kapacitet til at serviceydelse på tværs af organisatoriske enheder kan fungere ved høj hastighed. Der indbygges så megen logning at alle nuværende og forudsigelige fremtidige overvågningskrav kan imødekommes. Løsningsmodellen har været til review hos Netplan, der har givet en meget positiv vurdering af løsningen.

Implementering af løsningen er påbegyndt og forventes afsluttet omkring 1. april 2004.

For så vidt angår Rigsrevisionens bemærkninger om manglen på en ledelsesgodkendt sikkerhedsvurdering skal bemærkes, at den ovenfor under departementet nævnte risikovurdering vil dække Miljøministeriets samlede netværk.

Det kan endelig oplyses, at der blev foretaget en penetrationstest omkring årsskiftet 2002/2003 med helt tilfredsstillende resultat, og at der planlægges foretaget en ny penetrationstest, når den nye firewall-løsning er implementeret.

Beretningen giver mig ikke herudover anledning til bemærkninger eller særlige foranstaltninger. Nærværende redegørelse er samtidig sendt til Rigsrevisor.

Med venlig hilsen
Hans Chr. Schmidt