Svar på Rigsrevisionens rapport om it-sikkerheden på IT-Universitetet

Niels Hallenberg
Flemming Lindblad
It-afdelingen
IT-Universitetet

Journalnr. 340-0001-5

6. maj 2004

Indhold

0 Indledning

IT-Universitetet har modtaget Rigsrevisionens rapport af 23. marts 2004 om it-anvendelsen på IT-Universitetet. Rapporten påpeger en række forhold som bør overvejes og forbedres for at opfylde kravene til tilfredsstillende brug af it.

IT-Universitetet anerkender at der er en række forhold som i egen interesse bør forbedres og vil tage initiativ til at få udbedret forholdene. På baggrund af Rigsrevisionens detaljerede rapport er der lavet en konkret handlingsplan for opfyldelse af målene.

1 Kommentarer til de enkelte punkter i rapporten

1.1 It-strategi

IT-Universitetet vil udarbejde et strategidokument som med en konkret indgangsvinkel behandler strategien for udvikling og drift af it. Dokumentet vil indeholde visioner samt de nærmere planer for fremtiden på bl.a. følgende punkter:

- Licenser
- Brugerpolitik
- Brugersupport
- Netværksservicer
- Backup
- In- og outsourcing
- Softwareanskaffelser
- Indkøb og anskaffelser i øvrigt
- Udlånspolitik
- Egenudviklede systemer, herunder
  - Beslutningsproces
  - Krav til kravspecifikation
  - Krav til test
  - Krav til dokumentation
  - Frigivelse og versionskontrol
  - Krav til driftinstruks

IT-Universitetet betragter it-strategien som et væsentligt dokument hvorfor det er vigtigt at gennemarbejde alle detaljer omhyggeligt. It-strategien forventes færdigrevideret og godkendt af ledelsen pr. 1. april 2005.

En risikovurdering planlægges og udarbejdes i forbindelse med en beredskabsplan (se 1.2).

I relation til såvel risikovurdering som it-strategi vil der ligeledes blive udarbejdes en sikkerhedspolitik hvor der søges inspiration i DS-484 2, Anneks A. Sikkerhedspolitikken forventes færdig 1. april 2005.

1.2 Beredskabsplan

IT-Universitetet vil udarbejde en beredskabsplan med en bruttoliste af systemer med angivelse af vigtighed, hvor lang tid der må gå før systemerne er tilgængelige igen, samt de konkrete planer for reetablering af hvert enkelt system.

Beredskabsplanen skal sikre dels at reetablering sker på baggrund af en ledelsesmæssig beslutning så systemer reetableres i en prioriteret rækkefølge og med afsættelse af den rigtige mængde resurser, og dels at reetablering kan ske hurtigst muligt. I planen skal det endvidere fremgå hvilke ledelsesbeslutninger der skal tages i forbindelse med alvorlige nedbrud.

Der skelnes mellem forskellige former for nedbrud, og systemernes vigtighed prioriteres i forhold til organisationens behov.

I forbindelse med beredskabsplanen udarbejdes en risikovurdering, herunder risikoer i forbindelse med in- og outsourcing. Risikovurderingen udarbejdes som et selvstændigt dokument i papirform.

Oplæg til beslutning i ledelsen forventes klar december 2004, og endeligt dokument forventes klar februar 2005.

1.3 Fysisk sikkerhed. Adgang til serverrum

I IT-Universitetets nye bygninger i Ørestad er der elektronisk adgangskontrol på døren til hovedserverrummet. Der kan derfor opnås fuld kontrol over hvilke personer der har fysisk adgang til servere og data, og adgangsgtilladelse vil kun blive givet til it-medarbejdere. Rettigheder for det elektroniske adgangssystem administreres af en medarbejder fra afdeling for Intern Service.

I krydsfelter/sekundære serverrum er adgangskontrol baseret på fysiske nøgler; til sekundære serverrum vil kun It-afdelingen, rektor og lederen af Intern Service have adgang.

For alle serverrum vil eksterne personer med legalt ærinde i serverrum og/eller krydsfelter (fx konsulenter) skulle ledsages af en it-medarbejder. Ved udflytning til bygningen i Ørestad vil Rigsrevisionens anbefalinger således være imødekommet.

1.4 Sikkerhedskopier - adgangsret og opbevaring

For at undgå tab af backupsæt vil IT-Universitetet fremover opbevare en kopi af fulde backupsæt (som tages fire gange årligt) i en bankboks. Den daglige inkrementalbackup vil blive kopieret til en server uden for huset. På den måde sikres at data vil kunne genskabes selv i tilfælde af alvorlige ulykker på IT-Universitetets fysiske adresse. IT-Universitetet vil fortsat bevare en arbejdskopi i huset af hensyn til nem rekonstruktion af brugerdata; disse arbejdskopier vil blive opbevaret i internt arkiv hvortil kun it-medarbejdere har adgang. Endvidere er der pr. 1. maj 2004 indgået aftale med Danmarks Natur- og Lægevidenskabelige Bibliotek (DNLB) om gensidig opbevaring af hinandens daglige backup; således opstilles der en server hos DNLB til opbevaring af online- kopi af den daglige inkrementalbackup. Data udveksles via en krypteret forbindelse.

Sikkerheden i forbindelse med opbevaring af originale program-cd'er og licenser/licensnøgler vil blive skærpet. Originalsoftware med licensaftaler anbringes i pengeskab. It-medarbejdere må tage kopi af software i det omfang det er nødvendigt for at kunne udføre daglige opgaver efter retningslinjer udstukket af it-chefen. Originale cd'er kopieres efter behov til software-filserver hvortil kun it-medarbejdere har adgang. Speciel software som fx MSDN som må benyttes af alle ansatte og studerende, sættes til download fra server hvor al adgang logges.

De skærpede sikkerhedsforanstaltninger i forbindelse med opbevaring af backupdata forventes

implementeret 1. juni 2004, og i forbindelse med opbevaring og adgang til originalsoftware og licenser 1. oktober 2004.

1.5 Driftinstrukser og driftsovervågning

IT-Universitetet vil udarbejde retningslinjer for den daglige systemdrift. Der udarbejdes overordnede retningslinjer for indhold og omfang af en driftinstruks, og herefter laves driftinstrukser for de enkelte systemer.

Sikkerhedskopiering behandles i forbindelse med it-strategien (1.1) for så vidt angår de overordnede principper og i forbindelse med beredskabsplanen (1.2) hvad angår de konkrete implementeringer.

System- og dataejerskaber. Retningslinjer for disse indgår som en del af it-strategien (1.1). Der vil herefter blive udpeget system- og dataejere for kursusbase, optag-systemet, mit.ITU, HSAS m.v. System- og dataejerskab for hvert enkelt vil fremgå af driftinstruksen for det pågældende system.

Brugeradministration/logisk adgangskontrol. For systemer som mit.ITU, optagsystemet, HSAS m.v. fastsættes retningslinjer for brugeradministration og tildeling af rettigheder af hvert enkelt systems systemejer. Retningslinjer for tildeling af adgang til netværksservicer fastlægges som en del af sikkerhedspolitikken (1.1).

Driftovervågning. I forbindelse med udarbejdelse med beredskabsplaner og risikovurdering (1.2) fastsættes principper for driftovervågning. De konkrete tiltag for hvert enkelt system vil indgå i driftinstruksen for det pågældende system.

1.6 Firewall - overvågning og penetrationtest

Procedurer for administration af brandmur indføres i sikkerhedspolitikken. Penetrationtest udført af eksternt firma er bekosteligt; IT-Universitetet har derfor indgået aftale med en anden institution om gensidige portskanninger for at afprøve sikkerheden i brandmuren.

På kort sigt laves portskanning fra ITU's server i Ørestad. Den er p.t. på ekstern IP-adresse og derfor at betragte som ekstern. Fremover vil der på regelmæssig basis blive lavet gensidige portskanninger til/fra Danmarks Natur- og Lægevidenskabelige Bibliotek.

Portskanningen fra serveren i Ørestad er gennemført første gang ppr. 1. maj 2004, og de gensidige portskanninger til/fra DNLB påbegyndes oktober 2004.

1.7 Systemadministratorrettigheder

Principperne for tildeling af systemadministratorrettigheder vil indgå som en del af sikkerhedspolitikken. Konkret vil der blive foretaget tiltag for at begrænse antallet af personer med fulde adgangsrettigheder til alle systemer. Dette implementeres konkret ved indførelse af rettighedsadministrationsprogrammet "sudo" på serverne så administratorerne kun tildeles de nødvendige rettigheder og kan tilgå de relevante funktioner ved brug af eget password (ikke det overordnede administratorpassword). Et system er udviklet pr. 1. maj 2004, og forventes fuldt ud implementeret 1. september 2004.

1.8 Change management

Der udarbejdes procedurer for implementeringer, opgraderinger og afviklinger af væsentlige systemer som p.t. kan grupperes som følger:

- Servere (operativsystemer, servicer)
- Klienter (operativsystemer, applikationer)
- Egenudviklede systemer (mit.ITU m.v.)
- Outsourcede systemer (HSAS, Luvit, Synkron m.v.)
- Insourcede systemer (Studenterrådgivningen)

2 Afslutning

It-Universitetet vil følge op på Rigsrevisionens anbefalinger og har lavet en handlingsplan for at sikre en udførlig og gennemarbejdet forøgelse af sikkerheden for anvendelse af it-systemer. Der er allerede taget konkrete tiltag vedrørende portskanning/penetrationtest, opbevaring af backup, fysisk adgang til serverrum samt begrænsning af systemadministratorrettigheder.
I oversigtsform ser It-Universitetets handlingsplan ud som følger:

Tidspunkt	**Aktivitet**
1. maj 2004	Portskanning fra Ørestad gennemført
1. juni 2004	Sikkerhedskopier opbevares eksternt
1. juli 2004	Sikkerhed vedr. fysisk adgang til serverrum skærpet
1. september 2004	Systemadministratorrettigheder begrænset
1. oktober 2004	Gensidige portskanninger påbegyndt
1. oktober 2004	Sikkerhedsforanstaltninger for opbevaring af originalsoftware skærpet
1. marts 2005	Beredskabsplan foreligger
1. marts 2005	Risikovurdering foreligger
1. april 2005	Sikkerhedspolitik foreligger
1. april 2005	It-strategi foreligger