Da Datatilsynet kom

En skrekkhistorie?

UNINETT 2006, Ålesund 21.06.06

Jan Erik Frantsvåg, Universitetet i Tromsø – janerik.frantsvag@adm.uit.no

Brevet

- Våren 2004 fikk UiTø varsel om stedlig tilsyn fra Datatilsynet (DT)
- DT foreslo dato og ba om raske motforestillinger
- DT ba om spesifikk informasjon innen en gitt frist

Hvor stod vi?

- Som ADB-leder hadde jeg gjort den erkjennelse at vi hadde en del arbeid ugjort
- Regimeendringen fra konsesjon til melding hadde vi ikke tatt inn over oss
- En liten arbeidsgruppe hadde begynt å arbeide med nye retningslinjer og dokumentasjoner
- Vi trodde vi var på rett vei ...

Hva gjorde vi?

- Sendte det vi hadde
- Forklarte litt om hvor vi stod
- Erkjente for oss selv at dette neppe kom til å bli en festforestilling
- Men regnet med at vi kunne lære noe og få en fornuftig dialog ...

Hva var det stedlige tilsynet

- DT ville ha samtaler med institusjonsledelsen
- De ville ha samtaler med de prosjektansvarlige for spesifiserte prosjekter
- De ville ha samtaler med de ansvarlige for datasikkerheten
- De ville se dokumentasjoner

Hva lærte vi?

- Vi tenkte etter den gamle konsesjonsmodellen – Den digitale festning
  - Innestenging ved bruk av teknologi
- DT ser ut til å tenke mer Den digitale løken
  - Flere lag med ulike type sikkerhet, som ikke hver for seg er vanntett men som sammen skaper vansker
  - Dokumenterte vurderinger av hva som egentlig er trusler, hva som er konsekvenser og hva man finner er et forsvarlig sikkerhetsnivå

Hva lærte vi mer?

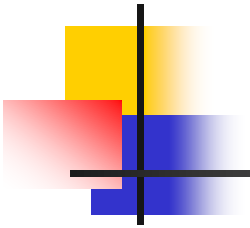
- Datasikkerhet blir ofte et ansvar for den sentrale IT-funksjonen
  - Det bør den ikke være
- Vi er flinke på teknologi
  - Men er det der truslene er?
- Vi trodde alt som hadde med forskning å gjøre, var ivaretatt i og med at NSD var personvernombud
  - Det var det ikke ...

Hva er viktig mht sikkerhet?

- Sikring mot uautorisert tilgang
  - Her er teknologi viktig
  - Men også organisasjon
    - Passordsikkerhet kan skape sikkerhetshull
    - Låsing av dører og PCer viktig, ikke bare brannmurer
    - Oppmerksomhet rundt problemstillingene

… mer sikkerhet

- Sikring av tilgang ved behov
  - Dersom man har persondata, er det for å ivareta behov
    - Da må de som har reelle og legitime behov, faktisk ha tilgang
    - Back-up, nødstrøm, fornuftige tilgangsrettigheter



... mer sikkerhet

- Korrekte data et krav!
  - Feilaktige data kan gi konsekvenser
    - Krever oppdateringsrutiner
    - Krever opplærte og oppegående brukere
- Unødvendige eller ukorrekte data skal slettes
  - Slike data har man ikke hjemmel til å ha

Forskjellig perspektiv

- Vi tenkte teknologisk sikring og administrative data
- DT tenkte organisatoriske tiltak og forskningsdata
  - Det viste seg at de hadde et ”prosjekt” mht forskningsdata i 2004
  - De startet med å be om informasjon om gitte prosjekter, så det var ingen overraskelse

Forskningsdata

- Vi trodde alt var ivaretatt i og med at NSD var personvernombud
  - Det viste seg at dette kun gjaldt en del saksbehandling
  - Resten av sikkerhetsarbeidet skulle vi gjøre selv

Hva opplevde vi

- Én forsker hadde avidentifiserte data på en bærbar datamaskin
  - og identifiseringsnøklene i en annen fil – på samme bærbare maskin
- Hvem som er ansvarlig kan være uklart
- Gamle samtykker var kanskje ikke lengre holdbare
  - Kunne bety gravlegging av forskningsprosjekter som hadde vart lenge

Samtykke og praktisering

- Viktig at samtykket samsvarer med det man faktisk foretar seg
  - Sier man at data skal slettes/anonymiseres innen en dato, skal dette skje
    - Man må altså allerede i samtykket ta høyde for forsinkelser – eks. svangerskap, sykdom, permisjoner
    - Man kan ikke ombestemme seg – men man kan be respondentene om utvidet frist

Studenter

- Studenter kan til tider foreta intervjuer eller på andre måter få personopplysninger
  - De gjør det som studenter ved vår institusjon
  - Ansvaret er vårt
  - Vi har ingen sanksjonsmuligheter
  - Veileder må ta faktisk fysisk kontroll over dataene

Konklusjoner

- Ansvaret må legges utenfor og over IT-direktøren
- Organisasjon like viktig som teknologi
- Begge deler må være på plass
- Bedre med litt dokumentasjon som avspeiler virkeligheten enn masse dokumentasjon som ikke brukes

Sikkerhet generelt

- Det er mange krav til sikkerhet
  - Datatilsynet
  - Riksrevisjonen
  - Utdanningsdepartementet
  - Riksarkivaren
  - NOKUT
  - osv. osv. direktorater instanser departementer tilsyn
- Bruk personopplysningsloven som utgangspunkt for å lage én totalpakke som tilfredsstiller alle krav

Råd om du får DT på besøk

- Vær åpen
- Vær ydmyk – DT kan dette, og det er de som har rett
- Benytt sjansen til å ruste opp sikkerheten din
- Får du kritikk, legg deg flat og samarbeid

Avslutning

- Ja, vi ble ”slaktet”
  - Veldig lærerikt
  - Nyttig dialog med DT – de er en ressurs
  - Slikt skaper ledelsesfokus – prosesser settes i gang
- Nei, det ble ikke da og ikke senere påvist at personopplysninger hadde nådd noen de ikke skulle nå
  - Men vi kan ikke basere oss på å berges av flaks og tilfeldigheter – vi må planlegge og tenke fremover.

Lesestoff

- Rapporten fra DT om datasikkerhet i forskningsprosjekter:

  http://www.datatilsynet.no/upload/Dokumenter/saker/2004/helserapporten_04.pdf