1.oktober 2006

Høringssvar fra Norges forskningsråd til Det Kongelige Justis og Politidepartement på NOU 2006-6 – Når sikkerheten er viktigst.

Forskningsrådet har gått gjennom innstillingen og finner den meget omfattende og god. Den berører primært områder som ligger på siden av hva Forskningsrådet har som primærvirksomhet, men spesielt på to områder er den meget relevant; **Beredskapsarbeide og IT-sikkerhet.** Vi har følgende kommentarer til disse to områdene:

Beredskapsarbeide:

Forskningsrådet merker seg i kapittel 13.3.2, at NOU-en tar for seg videre satsing på SAMRISK – et program som ***"skal gi økt kunnskap om trusler og farer, sårbarhet og risikohåndtering og dermed bidra til å ivareta sikkerhet og beredskap på tvers av sektorer og aktivitetsområder".*** (Dette program ble anbefalt av Forskningsrådet, gjennom en utredningsgruppe , nedsatt i 2005.)

Videre understreker NOU-en verdien av at forskningsprogrammer ved Norges forskningsråd, som er relevante for beskyttelse av kritisk infrastruktur og kritiske samfunnsfunksjoner, innarbeider og gir prioritet til sikkerhets og beredskapsmessige utfordringer. Dette kan for eksempel gjelde prosjekter innenfor Energiprogrammet og NORKLIMA.
Dette er noe Forskningsrådet støtter.

Hva gjelder Forskningsrådets **eget** beredskapsarbeid, som også NOU-en gir klare føringer til at institusjonene skal innarbeide som basis i sitt daglige virke, vil vi vise til rapporter som tidligere er sendt til Kunnskapsdepartementet, samt til møte med departementet for å redegjøre for status i dette arbeidet:

Norges forskningsråd har gitt dette arbeidet høy prioritet og kan informere om følgende vedr. planarbeidet:

Planarbeidet:
Hvilke tiltak har virksomheten gjennomført for å styrke krisehåndteringsevnen i eget ansvarsområde i planperioden?

- Forskningsrådet startet høsten 2001 med utarbeidelse av egen kriseplan. Saken ble behandlet første gang i Direktørmøtet 12.11.2001.
- Første kriseøvelse ble avholdt onsdag 6.12.2001 i samarbeid med eksternt byrå, som er spesialister på området. Dette var en såkalt "table-top" øvelse, dvs. at den kun involverte medlemmene i beredskapsgruppa – og ikke resten av organisasjonen.
- Kriseplanen ble i løpet av vinteren ferdigprodusert og ble så behandlet i DM mandag 6.5.2002. Den ble godkjent på alle punkter som grunnlag for vårt videre beredskapsarbeid.
- Planen er bygget opp rundt to hovedoppgaver når kriser inntreffer:
    - Handlingsbehov
    - Informasjonsbehov

Planen er senere revidert ved flere anledninger, senest august 2005

Forskningsrådet arrangerer kriseøvelse minst en gang årlig – og har ved jevne mellomrom møter i Beredskapsgruppen.

IT-Sikkerhet

Definisjon fra NOU:

Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.

Ut i fra denne definisjonen kan vi ikke se at det er noe i Forskningsrådet på IT- eller telefoni-siden som kan defineres som kritisk infrastruktur for landet som helhet.

Kriseberedskap ligger også implisitt i IT, da man har bygget sikkerhetssystemer og andre tiltak for å sikre IT funksjonens funksjonalitet under forskjellige forhold. Derfor må også beredskap innenfor IT-begrepet behandles.

Vi har derfor valgt å se på hva som er kritisk infrastruktur for Forskningsrådet og hva vi har gjort for å sikre den:

Datarom

Elektrisitet	UPS-sikring av alt utstyr på datarommet samt telefonsentral. Kapasitet til kontrollert stopp av utstyret.
Kjøling	Dobbel kjølemaskinkapasitet for å håndtere stopp i den ene.
Brann	Datarommet er sikret med gassanlegg i tilfelle brann eller tilløp til brann

Servere/systemer

Kritiske komponenter er dublisert for å unngå singel point of failure
Systemer med behov for 24/7 oppetid er plassert hos ekstern driftsleverandør
Kritiske servere er clustret mot felles SAN
Kontinuerlig sikkerhets-patching av alle servere

Backup / Lagring

Servernivå – speiling og raid på alle disker
Katastrofebackup er plassert eksternt i eget bygg.
Siste versjon av alle filer blir kopiert ut hver natt.

Diverse

Utarbeidet sikkerhetsinstruks og beredskapsplan på IT-siden
Vi har i tillegg en informasjonssikkerhetsstrategi som er implementert ved at vi behandler alle FoU-dokumenter som sensitive og kun gir tilgang til disse for medarbeidere som må ha dette av hensyn til saksbehandlingen. (Need to know-prinsipp).