Visiting address:
Martin Lingesvei 15-25, Fornebu
P.O. Box 134
NO-1325 Lysaker, Norway
Telephone: +47 67 82 82 00
Telefax: +47 67 82 82 01
www.simula.no

Oslo, 26. november 2002

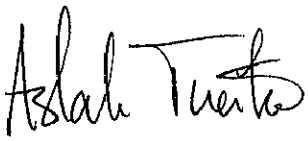
Nærings og handelsdepartementet
Postboks 8014 Dep
0030 Oslo

Høring – grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet.

Vi viser til tilsendt høringsdokument og oversender herved vår høringsuttalelse.

Vi ønsker lykke til med det videre arbeidet.

Vennlig hilsen
Simula Research Laboratory



Aslak Tveito
Professor
Administrerende Direktør (Konst.)

Name	Direct:	Fax:	Email
Aslak Tveito	+47 67 82 82 82	+47 67 82 82 01	aslak@simula.no

Grunnlagsdokument for Nasjonal strategi for informasjonssikkerhet

Høringsuttalelse fra Simula Research Laboratory

Vedlegg 1 av: 1
Sak:

Vi vil først takke for anledningen til å lese igjennom og kommentere grunnlagsdokumentet. Vi vil i all hovedsak gi vår tilslutning til dokumentets konklusjoner. Spesielt anser vi forslagene vedrørende en samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring av sensitiv informasjon både som betimelige og viktige for den videre utviklingen. Vi har likevel enkelte kommentarer til dokumentet som sådan.

En gjennomgående bekymring fra er at dokumentet gir inntrykk å være utarbeidet av en komité med begrenset teknologisk kompetanse. I seksjon 1.4 er det listet opp hvem som har deltatt i arbeidet. Med unntak av konsulentene fra PWC synes både arbeidsgruppen og styringsgruppen utelukkende å være sammensatt av representanter fra forskjellige berørte enheter i sentraladministrasjonen.

Vi har intet grunnlag for å bedømme enkeltpersonenes teknologiske fagkunnskap. Likeledes har vi merket oss at Forum for IT-sikkerhet har vært referansegruppe for prosjektet. Det er imidlertid enkelte punkter hvor dokumentet er både teknisk/faglig mangelfullt og inkonsistent. Dette er gjerne ikke dramatisk for den anvendelse dokumentet skal ha, men på den annen side skal de avgjørelser som fattes på bakgrunn av dokumentet iverksettes av teknologer. En manglende teknologifaglig forståelse både av trusselbildet og av sikkerhetsrisikoer anses derfor som en svakhet.

Under har vi listet opp de viktigste punktene hvor vi vil anbefale at dokumentet vurderes endres:

- I seksjon 1.5 gis det en gjennomgang av hvilke egenskaper beskyttelse av informasjon bør omfatte. Den fraviker det som gjennom de siste tiårene har nedfelt seg som en faglig terminologi på området. Dette kan det i og for seg være gode grunner til å gjøre, men i den definisjonen som er valgt er det et antall sikkerhetsproblemer som ikke er dekket. Den viktigste av disse er beskyttelse mot uautorisert endring av data. Videre er autentisering i dokumentet kun knyttet opp mot konfidensialitet. Dette er imidlertid et viktig begrep også når man snakker om beskyttelse mot sabotasje.

  Det er vanlig å angi *konfidensialitet, autentisering og integritet* som de tre basale byggesteinene i informasjonssikkerhet. Egenskaper som sikring av informasjon mot uautorisert innsyn, uautorisert endring/sabotasje, håndtering av mistro og ikke-benekting bygges opp ved bruk av disse tre begrepene. Det er imidlertid god grunn til å legge til *tilgjengelighet* som et basalt begrep i denne sammenhengen, slik dokumentet gjør.

- Det er prisverdig at dokumentet i seksjonene 7.1.3 og 7.1.4 tar for seg undervisning og forskning som et virkemiddel for å oppnå informasjonssikkerhet, og vi vil gi vår støtte til alle de forslagene som der er

gitt. Vi vil imidlertid minne om at ingen enkeltutdannelser eller enkeltfagområder kan omfatte alle de teknologiske aspekter som det trengs kunnskap om. Det er derfor etter vårt syn nødvendig, men ikke tilstrekkelig, å etablere IT-sikkerhet som fag ved Universiteter og høyskoler, samt å opprette forskningsprogram innen sikkerhet. Det bør i tillegg sikres at nasjonen har tilstrekkelig kompetanse innen sikkerhetsrelevante spesialfelter. Nederst på side 59 sies det noe løselig at dette gjelder "fagdisipliner som naturlig vil inngå i avanserte anvendelser". Innen informatikk gjelder dette særlig datamaskinarkitektur, operativsystemer, kommunikasjon og distribuerte systemer.

- Et utviklingstrekk som bare i liten grad blir trukket frem er at trusselbildet for datamaskinbaserte informasjonsløsninger er i konstant endring. Det er derfor vanskelig å se for seg at det finnes enkle grep som kan gjøres nå, og som løser problemet i overskuelig fremtid. Kompleksiteten i denne materien illustreres av at man fra tid til annen opplever datainbrudd hvor metodene som har vært brukt for å komme seg igjennom sikkerhetssystemet ikke har vært påtenkt, selv ikke av høyst kompetent sikkerhetspersonale. Vi anser derfor at utvikling og vedlikehold av dyp teknologisk kompetanse som er i stand til å både følge og forstå utviklingen på dette området som meget viktig. Videre vil vi igjen understreke betydningen av tekologisk kompetanse i det videre arbeidet med nasjonal strategi.

- På side 12 angis det at reviderbarhet og sporbarhet må ivaretas for å sikre integritet. Integritet i teknologisk forstand – slik det er definert på side 11- sikres med helt andre mekanismer enn de som brukes for sporbarhet og reviderbarhet. Vi foreslår derfor at reviderbarhet og sporbarhet begrunnes med dekning av et kontrollbehov, gjerne klarert med Datatilsynet, og ikke med integritet.

- På side 17 angis Konvergens som et utviklingstrekk som bidrar til å utvide risikobildet. Vi ser ikke at konvergens i seg selv er en sikkerhetsrisiko. *Gjennomføringsfasen av konvergensen* fører imidlertid til at det vil kunne oppstå midlertidige kompetansehull hva gjelder sikkerhet, da tidligere sikkerhetsstrategier for hver enkelt-teknologi ikke lenger vil være gyldige. Det er imidlertid uheldig hvis det fester seg et bilde av at man kan få langsiktige sikkerhetsgevinster ved å motarbeide teknologikonvergens i landets infrastruktur.

- På side 44 foreslås det å vurdere behovet for å etablere et "permanent koordineringsråd for IT-sikkerhet". Videre kommer det et forslag til hvordan dette rådet kan være sammensatt. Vi anser det som spesielt viktig at det sitter teknologisk kompetanse i et slikt råd, jamfør flere av punktene over.

For Simula Research Laboratory

Olav Lysne