SINTEF Tele og data

Postadresse:
7465 Trondheim
Besøksadresse Trondheim:
S.P. Andersens v 15
Besøksadresse Oslo:
Forskningsveien 1
Telefon:
73 59 30 00
Telefaks:
73 59 43 02

Foretaksregisteret:
NO 948 007 029 MVA

SINTEF

Nærings- og handelsdepartementet
Postboks 8014 Dep.

0030 OSLO

Seniorrådgiver Katarina de Brisis

Deres ref.:2001/5605 KDB Vår ref.: Odd Helge Longva Direkte innvalg: 73 59 28 66

Trondheim,
2002-11-22

Høring – grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet.

Tilbakemelding fra SINTEF

Ref. til brev datert 2002.10.21

Generelle og overordnede kommentarer på dokumentet som helhet.

1. Det er et meget fyldig dokument og et godt utgangspunkt for å utarbeide strategidokumentet. Samtidig inneholder det en mengde detaljer som lett kan ta oppmerksomheten vekk fra hovedpunktene.
   Det foreslås derfor at det i kapittel 2. Sammendrag gjøres tydeligere hva som er de viktigste konkrete forslag til strategi og tiltak.

2. Det er satt tre overordnede mål for strategien. I de to første legges det vekt på robust samfunnskritisk infrastruktur og sikkerhetskultur .
   Dette peker på en defensiv holdning, et forsvar. Det er nødvendig men ikke tilstrekkelig linje for en nasjonal strategi.
   Det foreslås derfor at det føyes til et mål hvor det sies at IT-sikkerhet skal utvikles til å være en viktig konkurransefaktor for norsk næringsliv, offentlig forvaltning og det norske samfunn.

   Det siste målet i dokumentet går på en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring. Denne er avgjørende for å utvikle IT-sikkerhet som konkurransefaktor. Det anses derfor som meget viktig og bør framheves mer enn det som er gjort ellers i dokumentet.

3. Det er tre hovedfaktorer i informasjonssikkerhet: teknologi, organisasjon, mennesket. Inntrykket er at det i dette dokumentet legges for lite vekt på organisasjon og mennesket i forhold til teknologi. Mennesket er nå det svakeste leddet i kjeden og det må legges til rette, gjennom teknologi og organisering, for at mennesket kan fungere etter de forutsetninger som legges til grunn for konfidensialitet, integritet og tilgjengelighet.

4. Det bør understrekes tydeligere (ref kap 5.4) at informasjonssikkerhet bør inngå i en sammenheng med HMS og kvalitetssikring i organisasjoner/bedrifter.

5. Vi ser positivt på at det etableres et permanent koordineringsråd for IT-sikkerhet. Det er viktig at det raskt etableres ett klart ansvarsregime (ref 5.3.1 i rapporten). Det er positivt at det fokuseres på dette i dokumentet da det er viktig at ansvaret presiseres og tydeliggjøres.

Kommentarer til detaljer i de enkelte kapitler og/eller utsagn.

- *Konkurransefaktor*: Det bør legges vekt på at informasjonssikkerhet ikke bare er en utgiftspost, det er en konkurransefaktor, direkte og indirekte, for Norge, både næringsliv og offentlig sektor.

- *Konfidensialitet, integritet og tilgjengelighet*: Grunnlagsdokumentet nedprioriterer en hovedkomponent, konfidensialitet, innen det totale IT-sikkerhetsbildet. Det er lagt hovedvekt på integritet og tilgjengelighet gjennom hele dokumentet. Dette tegner et helt skjevt bilde av IT-sikkerhet. Samspillet mellom de tre komponentene er vital for et komplett sikkerhetsgrunnlag og –strategi. Dokumentet nevner ikke kryptering og autentisering før kapittel 8.

- *Interne sikkerhetsbrudd*: Grunnlagsdokumentet legger lite vekt på problematikken rundt IT-sikkerhet og personell. Ofte beskyttes det mot eksterne farer med perimeterkontroll (f.eks. brannmur) og Virtual Private Network (VPN), men den interne trusselen fra personell er ofte glemt. Undersøkelser har vist at store menger av verdigrunnlaget for norske bedrifter og organisasjoner er lekket, ødelagt eller manipulert. Vi trenger en økende bevisstgjøring om den interne trusselen. Dokumentet burde derfor gå nærmere inn på den sårbarhet introdusert ved utro tjenere og liten sikkerhetskompetanse av personell.

- *Det offentlige som pådriver:* For å fremme informasjonssikkerheten i både offentlig og privat sektor bør det offentlige, stat og kommuner, etablere minimumskrav til sertifisering i forbindelse med statlige innkjøp.

- Ad kap 1.5. "elektronisk" og "digital" signatur er ikke det samme - de burde defineres i ordforklaringen og brukes konsekvent i dokumentet. Tilsvarende bør "datakriminalitet" tas med.

- Ad kap 3.3.3. SINTEF har ansvaret for prøveprosjektet SIS. Vi slutter oss til det som står i dokumentet og understreker at det som der sies står sentralt i prosjektet.

- Ad kap 4. Her trekkes den meget riktige konklusjonen at vi aldri kan nå et stadium hvor systemet og nettverket er sikkert og det ikke finnes noen sårbarheter. Det beste vi kan gjøre er å leve med en nøye gjennomtenkt og valgt risiko. Grunnlagsdokumentet burde presisere dette nøyere

- Ad kap 4.5. Siste avsnitt. Under eksemplene på kontroll og sikkerhetsmekanismer bør også IDS(inntrengingsdeteksjon) nevnes.

- Ad kap 7. Det foreslås en rekke viktige tiltak. Sett i sammenheng med prøveprosjektet SIS ville det vært ønskelig med en understreking av alle bør rapportere hendelser av brudd på informasjonssikkerheten til SIS.

- Ad kap 7.2. På virksomhetsnivå er dokumentet mangelfullt. Styring av IT-sikkerhet er ikke det samme som sikkerhetskultur. En effektiv sikkerhetsledelse består av to dimensjoner, strukturdimensjonen og kulturdimensjonen. Struktur omfatter planer, regler, prosedyrer og formelle systemer. Kultur omfatter samhandling, atferd - hvordan ting gjøres i praksis, og kommer til syne gjennom språk, handlinger, historier og symboler. Grunnlagsdokumentet burde derfor heller forklare hva kultur egentlig er for så å si at dette er et område hvor det må stilles krav til ledelsen i virksomhetene.

- Ad kap 8. Det er viktig at det etableres en felles infrastruktur for sikker meldingsformidling, digitale sertifikater og elektroniske signaturer. Alle samfunnsinstitusjoner bør ha ett digitalt sertifikat. Det offentlige er tungen på vektskålen for å få en rask løsning, hvis det overlates til markedet slik det nå fungerer vil det kunne ta lang tid og Norge vil miste konkurransefortrinn.

Sluttord

Informasjonssikkerhet er et viktig aktivitetsområde for SINTEF, som en del av SINTEF totalaktivitet innen sikkerhet/sårbarhet/risikostyring mot offentlig og privat sektor.
Vi er glad for at det nå blir utarbeidet en nasjonal strategi og vil gjerne bidra i det videre arbeid.

Med vennlig hilsen
SINTEF

Odd Helge Longva