Direktoratet for sivilt beredskap
samarbeid for sikkerhet

[redacted]

Vår dato: 25.11.2002
Deres dato: 21.10.02
Vår saksbehandler: Tonje Grunnan

Vår referanse: 0200278 PLA/TGR/309
Deres referanse: 2001/5605 KDB

Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 Oslo

HØRINGSUTTALELSE – GRUNNLAGSDOKUMENT FOR UTARBEIDELSE AV NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET

Direktoratet for sivilt beredskap (DSB) viser til brev av 21.10.02 angående høring på grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet. DSB støtter behovet for en nasjonal strategi for IKT-sikkerhet og mener grunnlagsdokumentet tar opp mange interessante aspekter knyttet til informasjonssikkerhet.

Mål og innretning av strategiarbeidet
DSB støtter i hovedsak innretningen av strategiarbeidet og henviser i den sammenheng også til at direktoratet gjennom Justisdepartementet og prosjektgruppa har blitt trukket inn i arbeidet med utarbeidelsen av grunnlagsdokumentet. DSB vil samtidig påpeke behovet for å vurdere ytterligere tiltak for å sikre en best mulig beskyttelse av kritiske IKT-systemer.

Identifiserte utviklingstrender av betydning for nasjonalt arbeid med IT-sikkerhet
Grunnlagsdokumentet identifiserer en rekke utviklingsstrender som påvirker og er av betydning for nasjonalt arbeid med IT-sikkerhet. Dokumentet viser til flere utredninger om sårbarhet ved anvendelse av IT og kritisk infrastruktur som er blitt gjennomført. DSB ønsker å være en pådriver for å sette i gang tiltak mot de mest alvorlige trusler mot kritisk infrastruktur. DSB understreker betydningen av kontinuerlig å kartlegge risiko og sårbarhet knyttet til kritiske IT-systemer. Vi vil i den forbindelse vise til Forsvarets Forskningsinstitutts prosjektforslag til forskningsprosjektet "Sårbarhet i nasjonalt viktige IKT-systemer" (BAS5).

BAS5-prosjektet kan anses som et supplement til den nasjonale strategien for informasjonssikkerhet. Prosjektet skal gi en god oversikt over trusler og danne grunnlag for tiltak som skal sikre de mest samfunnskritiske infrastrukturer. Den uttalte hovedmålsetting for prosjektet er å gi anbefalinger om tiltak for å sikre at samfunnskritiske virksomheter, med stor avhengighet av systemer basert på informasjons- og kommunikasjonsteknologi, gjøres mest mulig robuste. Hovedresultatet fra prosjektet vil være en anbefalt helhetlig strategi med tiltak for å redusere samfunnets sårbarhet knyttet til avhengighet av IKT-systemer.

Postadresse Postboks 8136 Dep. 0033 Oslo
Besøksadresse Sandakerveien 12 Oslo
Telefon Telefon 22 35 84 00 Telefaks 22 35 17 81
Informasjonsseksjonen Telefon 22 35 84 64 Telefaks 22 35 17 81
Administrasjonsavd. Telefon 22 35 84 02 Telefaks 22 35 17 81
Sivilforsvarsavd. Telefon 22 35 84 77 Telefaks 22 71 52 87
Plan- og tilsynsavd. Telefon 22 35 85 63 / 85 59 Telefaks 22 38 28 24
E-postadresse postmottak@dsb.dep.no
Internettadresse: www beredskapsnett no

Vi anbefaler at styringsgruppen også ser til målsettingene som dette prosjektet har, og evt. resultater som kommer i prosjektet, i sitt videre arbeid med å lage et Strategidokument. Under utformingen av Strategidokumentet anbefaler vi at fokuset i større grad rettes mot målsettingene som foreligger i BAS5-prosjektet slik at det legges vekt på nasjonalt viktige IKT-systemer, særlig i forhold til sabotasje- og terrorangrep.

Identifiserte utfordringer for IT-sikkerhet
DSB mener at grunnlagsdokumentet ivaretar beskrivelsen av de viktigste utfordringene for IT-sikkerhet på en god måte. Vi viser videre til målsettingen: "Det er et mål å øke robustheten i IT-infrastruktur til et nivå slik at risikoen for avbrudd i en normalsituasjon er akseptabel for viktige samfunnsfunksjoner. I en krisesituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner." Vi forutsetter at denne målsettingen senere operasjonaliseres for den enkelte sektor. Vi anbefaler i tillegg å vurdere en tilføyelse vedrørende beredskap, f eks: "I den grad kritiske IT-systemer likevel faller bort skal det sikres en god beredskap og konsekvenshåndtering i samfunnet."

Foreslåtte strategier og tiltak i kap. 5-8
Det er et viktig og krevende arbeid som her er igangsatt. Det er dokumentert reelle og omfattende behov for en helhetlig og nasjonal tilnærming til IT-sikkerhet. Grunnlagsdokumentet inneholder forslag til en rekke strategier og tiltak som hver på sin måte vil bidra til å bedre IT-sikkerheten.

IT-sikkerhet er av natur både tverrfaglig og tverrsektoriell. I dag preges temaet av til dels fragmentert og sektorbasert tilnærming. Det er derfor viktig å få på plass organisatoriske mekanismer som bidrar til å samordne og harmonisere regelverk og pålegg. Spesielt viktig vil det være å tilpasse og utvikle regelverk i tråd med en rask teknologisk utvikling. Et permanent koordineringsråd for IT-sikkerhet er foreslått å utføre nevnte oppgave. Vi forutsetter at et slikt koordineringsråd ses i sammenheng med allerede eksisterende organer slik at man begrenser råd og utvalg med overlappende mandat. TRSTI er f eks et råd hvor en rekke IKT-relaterte risiki blir tatt opp. Dersom man velger å opprette dette koordineringsrådet foreslår DSB et *permanent* sekretariat som settes sammen på en formålstjenlig måte. Forslaget i grunnlagsdokumentet, om et sekretariat som ivaretas etter rotasjonsprinsippet, kan komme til å gi uklart fokus og ikke tilfredsstillende kontinuitet i sitt arbeid.

Når det gjelder omtalen av DSBs nåværende og fremtidige rolle har vi ingen innvendinger mot de beskrivelser som er gjort. DSB synes imidlertid det ville vært fordelaktig å få en avklaring med hensyn til konkretisering av ansvarsfordelingen i forhold til Nasjonal sikkerhetsmyndighet (NSM) allerede i grunnlagsdokumentet. Det anses som viktig å skape en ryddig grenseoppgang mellom DSB og NSM som begge fra 01.01.03 vil bli fagmyndigheter under Justisdepartementet med ansvar innen IT-sikkerhetsområdet.

Andre forslag som kan bidra til slagkraft og oversiktlighet på området
DSB vil anbefale økt bruk av Fylkesmannen som et bindeledd mellom lokalt/regionalt nivå og NSM innen sikkerhetslovgivning og utføring av beredskapsoppgaver og øvelser.

Arbeid for å redusere IT-sårbarhet må generelt sett også følges opp gjennom internasjonalt samarbeid. Når det gjelder DSB vil vi følge opp dette i forhold til EU og NATO, og i BAS5-prosjektet er en av målsettingene å vurdere etablering et nordisk samarbeid.

Avslutningsvis vil vi komme med noen synspunkter på utviklingen i de samarbeidsfora DSB er med i innenfor IT-sikkerhetsområdet. Gjennom praktisk deltakelse i VDI er det erfart et reelt behov for sentraliserte og koordinerte sikkerhetssystemer for beskyttelse av norsk kritisk infrastruktur. VDI bør vurderes videreutviklet og gjøres til en permanent ordning, eventuelt med en døgnkontinuerlig varslingsenhet. I tillegg bør man vurdere å øke analysekapasiteten på grunn av store datamengder. VDI-samarbeidet har i vesentlig grad bidratt til å høyne kompetanse og innsikt innen IT-trusselbildet, sårbarheter og aktuelle mottiltak hos de deltakende bedrifter og etater. Vi vil i forlengelsen av dette understreke viktigheten av at det etableres nære og gode relasjoner mellom VDI og det nyopprettede Senter for informasjonssikring (SIS).

Oppsummering
DSB anser at strategiarbeidet bidrar til økt vektlegging av IKT-sikkerhet i samfunnet. Vi vil samtidig gi til kjenne en anbefaling om *ytterligere* vektlegging av tiltak for å sikre samfunnskritiske IKT-systemer, gjerne i tråd med målsettinger i BAS5-prosjektet. Grunnlagsdokumentet vektlegger i stor grad behovet for IKT-sikkerhet knyttet til privatpersoners og næringslivets bruk av IT framfor nasjonal sikkerhet. I forlengelsen av arbeidet med grunnlagsdokumentet og tilhørende strategi bør det tas større hensyn til alvorlige trusler mot samfunnskritiske infrastrukturer, som f eks terrorisme. Selv om slike trusler kan anses som lite sannsynlige i Norge vil dette raskt kunne endre seg og bør derfor vurderes.

Den overordnete målformuleringen i grunnlagsdokumentet er av generell karakter. DSB forutsetter imidlertid at det i oppfølgingen vil bli operasjonalisert mer presise mål for de enkelte tiltak. DSB vil bidra aktivt til å videreføre tiltak og strategier som går inn på vårt ansvarsområde, bl a i forhold til kriseplanlegging og beredskapsøvelser.

Med vennlig hilsen

Arthur Gjengstø
avdelingsdirektør

Nils Ivar Larsen
underdirektør

Kopi:
Justisdepartementet v/Rednings- og beredskapsavdelingen
Fylkesmennene