DET KONGELIGE
FORSVARSDEPARTEMENT

Nærings- og handelsdepartementet

Tidl ref	Vår ref	Dato
2001/5605 KDB	2002/02112-7-/FD I/SV/350	29 NOV 2002

GRUNNLAGSDOKUMENT FOR NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET

Det vises til brev av 21. oktober d.å. fra Nærings- og handelsdepartementet.

Forsvarsdepartementet deler det syn at målsettingen med strategien bør være mest mulig vidtfavnende og helhetlig i forhold til de ulike behov for informasjonssikkerhet i samfunnet. Det innebærer at strategien må rette seg mot et meget bredt trusselspekter.

Vi har i hovedsak ingen innvendinger til det som fremkommer i grunnlagsdokumentets virkelighetsbeskrivelse eller til de foreslåtte strategier/tiltak. Vi kan imidlertid ikke se at utkastet til strategi har en slik helhet og dybde som er nødvendig for å møte hele spekteret av fremtidige trusler mot samfunnet. Vi vil særlig fremheve at det i liten grad er tatt hensyn til trusselen mot samfunnskritiske IKT-systemer fra aktører som innehar høy evne til å gjennomføre rettede og koordinerte angrep med høy intensitet. Vi savner også en bredere beskrivelse av informasjonssikkerhet med utgangspunkt i sikkerhetslovens virkeområde. Strategien vektlegger også behovet for basissikkerhet for næringslivets og privatpersoners anvendelse av kommersielle IKT-tjenester i for stor grad, fremfor nasjonal sikkerhet. Det foreslås derfor at strategien videreutvikles for å favne hele trusselspekteret.

Det foreslås opprettet et permanent koordineringsråd for IT-sikkerhet. Forsvarsdepartementet støtter forslaget, men vil understreke at en effektiv samordning på området vil kreve en reduksjon av myndighetsorganer og en kraftsamling om en utøvende tverrsektoriell fag- og tilsynsmyndighet på området.

Vedlegg 1

Postadresse	Kontoradresse	Fellesavdeling	Saksbehandler
Postboks 8126 Dep	Myntgata 1	Telefon 23 09 20 21	Severin Vikanes
0032 Oslo	Org nr 972 417 823	Telefaks 23 09 20 88	Telefon 23092091

I det videre arbeid med å utvikle strategien, foreslås det at Forsvarets militære organisasjon (FMO), som landets største virksomhet på området IKT-sikkerhet, og Nasjonal sikkerhetsmyndighet, med sine betydelige fag- og tilsynsoppgaver innen IT-sikkerhet, trekkes direkte inn i prosjektgruppens arbeid.

Vedlagt følger kopi av høringssvar datert 25. november d.å. fra Forsvarets forskningsinstitutt.

Med hilsen

Monica Lütken (e.f.)
avdelingsdirektør

Severin Vikanes
seniorrådgiver

Kopi:
FO/S
FFI
FD I 1,II 2,III 2

37/2002

FORSVARETS FORSKNINGSINSTITUTT

Vedlegg 1 av: 1
Sak:

Dato
25. november 2002
Vår referanse
2002/04514-2/FFIS/ KON/PNa/BSB/350
Tidl referanse

Forsvarsdepartementet

HØRINGSUTTALELSE - GRUNNLAGSDOKUMENT FOR NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET

Det vises til Forsvarsdepartementets skriv av 11. november 2002 (ref 2002/02112-5/FD I/SV/350), der det blir bedt om merknader til Grunnlagsdokument for nasjonal strategi for informasjonssikkerhet". Vedlagt følger Forsvarets forskningsinstitutts (FFI) høringsuttalelse.

FFIs uttalelse er basert på Forsvarets behov for anvendelse av militærmakt ut fra i hovedsak to hensyn. Forsvaret er med grunnlag i Totalforsvarskonseptet avhengig av en rekke sivile samfunnsfunksjoner for å gjennomføre militære operasjoner effektivt. I takt med at disse samfunnsfunksjonene blir stadig mer avhengige av kommersielle tjenester basert på informasjons- og kommunikasjonsteknologi (IKT) blir også Forsvaret indirekte mer avhengig av disse tjenestene. Forsvaret forventes som følge av utviklingen innen militær teknologianvendelse også å bli mer direkte avhengig av offentlige IKT-baserte tjenester, slik som f eks offentlige kommunikasjonstjenester. FFI legger også til grunn for uttalelsen den direkte betydningen samfunnets økende sårbarhet som følge av økende avhengighet av IKT-baserte tjenester har for nasjonal sikkerhet.

FFI har i hovedsak ingen innvendinger til den generelle virkelighetsbeskrivelse slik den presenteres punkt for punkt. I hovedsak har FFI heller ingen vesentlige kommentarer til de enkelte strategier og tiltak i den ramme de fremmes i. Alle disse vurderes i større eller mindre grad å kunne fremme målet. FFI antar at disse vil bli nærmere konkretisert i det videre arbeidet.

FFI mener imidlertid at utkastet som nasjonal strategi *samlet sett* ikke representerer den helhet og dybde som er nødvendig for å møte hele spekteret av fremtidig trusler mot samfunnet. Det synes i svært liten grad å være tatt hensyn til trusselen mot samfunnskritiske IKT-systemer fra aktører som innehar høy evne til å gjennomføre rettede og koordinerte angrep med høy intensitet. Selv om forekomsten av slike angrep *i dag* vurderes som lite sannsynlig, vil dette raskt kunne endres. Dersom slike angrep skulle bli gjennomført vil konsekvensene for samfunnet kunne bli svært høy. Det kan som eksempel nevnes at det i dag er anslått å være mer enn 20 nasjoner som innehar eller er i ferd med å opparbeide en evne til å gjennomføre slike angrep. Computer Network Operations (CNO) er i ferd med å

Vedlegg: 0

Adresse:	Postboks 25, 2027 Kjeller	Sentralbord:	63 80 70 00	Organisasjonsnr:	NO 970 963 340 MVA
Saksbehandler:	Kjell Olav Nystuen	Innvalg:	63 80 77 28	Mil retn nr:	0505
E-post:	kjell-olav.nystuen@ffi.no	Telefaks:	63 80 72 12	WWW-adresse:	www.ffi.no

bli viktige virkemidler i mange nasjoners anvendelse av militærmakt, både mot militære og sivile mål. Det synes heller ikke i strategien å være tatt hensyn til trusselen fra fremmed signaletterretning.

FFI mener at strategien i for stor grad vektlegger behovet for basissikkerhet for næringslivets og privatpersoners anvendelse av kommersielle IKT-tjenester, fremfor nasjonal sikkerhet. Denne basissikkerheten er et viktig fundament for all samfunnssikkerhet, men er etter FFIs syn langt fra tilstrekkelig. Eksempelvis fokuseres det i utkastets avsnitt 3.2.6 på teknologianvendelse knyttet til hjemmebruk og hjemmearbeidsplasser, mens det i kapittel 6.1.2 benyttes eksempler på tiltak som spam-filtrering og ADSL-sikkerhet. Dette er vel og bra, men er etter FFIs syn – selv som eksempler – mindre relevant for et dokument som skal omtale en nasjonal strategi.

Det blir i første del av hovedmålsettingen for strategidokumentet lagt vekt på *akseptabel risiko overfor de trusler samfunnskritisk infrastruktur for elektronisk informasjonsutveksling utsettes for*. Det blir imidlertid ikke gått inn på hva som legges i trusler og trusselnivå, ei heller hva man legger i akseptabel risiko. Etter FFIs syn må det i strategien klargjøres hvilken analyse og hvilke analysekriterier som ligger til grunn for valg av strategi og enkelttiltak. Som eksempel kan det nevnes at behovet for sikkerhet og beredskap innen telesektoren er klart plassert som tiltak, noe FFI er tilfreds med. Dette er imidlertid tiltak som i vesentlig grad er basert på Totalforsvarets behov. På den annen side oppfattes tiltaket Senter for informasjonssikring (SIS), slik det foreligger i prøveperioden, avgrenset til ikke å omfatte Totalforsvarets behov. Dette viser en manglende presishet og konsistens i tiltakenes innretning i forhold til målsettingen - en målsetting som er for dårlig beskrevet i forhold til nivået på øvrig beskrivelse.

Kapittel 5 omhandler blant annet behovet for grenseoppgang i det sektorovergripende ansvaret for IT-sikkerhet på myndighetsnivå, spesielt mellom FD, JD og NHD. Denne foreslås i høringsutkastet løst ved at det opprettes et råd for samordnet koordinering av IT-sikkerhet mellom aktuelle departementer. Dette kan være en del av en løsning, men løser etter FFIs syn ikke det grunnleggende problemet. Sett opp mot større trusler mot samfunnskritiske IKT-infrastrukturer, som er dynamiske og komplekse av natur, vil det være svært vanskelig til en hver tid å bestemme hvem som har ansvaret. IKT-infrastruktur går i sin natur på tvers av sektorinteressene og krever derfor også en helhetlig tverrsektoriell tilnærming, uavhengig av trusler og trusselnivå. Problemstillingen dreier seg fundamentalt om teknologi og systemer, men like viktig om anvendelsen av tjenester og om konsekvenser av svikt både for den enkelte virksomhet og samfunnet som helhet. I så vidt komplekse og dynamiske omgivelser er det behov for å få i stand en eller annen form for helhetlig tilsyn. Dette vil imidlertid kreve effektiv samhandling mellom ulike typer eksperter på ulike nivå, så vel som mellom alle involverte sektorer.

IKT-basert informasjon som benyttes til ulike former for kommersiell tjeneste- og vareproduksjon betraktes i dag svært sjelden som skjermingsverdig i henhold til sikkerhets- eller beskyttelsesinstruksen. Dette gjelder selv om tjenestene og varene i eventuell krig og krise vil være av vital betydning for både Det sivile beredskap og Forsvaret. Dette har nok dels sin forklaring i de negative praktiske konsekvensene det får for den enkelte virksomhet å få sine IKT-systemer underlagt de krav som følger av disse instruksene. Særlig gjelder dette for virksomheter som daglig opererer ut fra strenge bedriftsøkonomiske føringer. En samfunnskristisk virksomhet vil imidlertid i løpet av relativt kort tid måtte kunne gå fra en hverdagssituasjon med lavnivå trusler, til å måtte møte større trusler mot egen virksomhet.

Systemene som ligger til grunn er imidlertid de samme. Dersom disse svikter vil det i den aktuelle situasjon kunne føre til alvorlige konsekvenser både for Det sivile beredskap og Forsvaret. Det vurderes av FFI som helt nødvendig å finne metoder å sikre disse systemene på i alle fasene av fred, krise og krig, på en måte som er mest mulig tilfredsstillende for systemeieren, og som samtidig heller ikke medfører unødig høy risiko for samfunnet. Det bør i denne sammenhengen også vurderes om Sikkerhetsloven med forskrifter slik de foreligger i dag er egnet til å møte disse på mange måter nye utfordringene for samfunnet.

I kapittel 8 beskrives forslag til samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring av sensitiv informasjon. Dette synes i liten grad å være samordnet med Forsvarets arbeid på området. Sett i lys av Totalforsvarskonseptet vil det etter FFIs syn være sterkt ønskelig med en form for samordning på dette området.

FFI vil videre peke på at Forsvarets militære organisasjon (FMO) med støtteenheter er landets største virksomhet på området IKT-sikkerhet, og innehar også kompetanse ut over de institusjoner som er nevnt i strategien. Det bør vurderes om ikke også disse bør trekkes inn i det videre arbeidet med strategien, dersom den skal fange hele utfordringsspekteret det moderne samfunnet står overfor.

FFI mener at det er behov for en nasjonal strategi for IKT-sikkerhet, og at det foreliggende utkastet kan utvikles videre til en slik strategi. Imidlertid er det nødvendig å gjøre strategien og tiltakene betydelig klarere og mer konsistent. Strategiene og tiltakene må også enkeltvis forankres til en mer konkret målsetting tilpasset hele trusselspekteret. Det er videre svært viktig at tiltak settes i ut i livet parallelt med at strategien utvikles. En rekke av de tiltak som presenteres i strategien er resultat av tidligere utredninger og trenger ikke flere runder med utredninger. De mest åpenbare eksemplene på dette er SIS og nytt regime innen telesikkerhet og -beredskap. Forskning og utdanning er et tilsvarende område, men selv om det er en bred enighet om viktigheten av dette synes det likevel å skje lite. Mye tyder tvert i mot på at sivil forskning innen teknologi og IKT-sikkerhet er i tilbakegang. Det er viktig at arbeidet med strategiutvikling ikke forsinker realisering av nødvendige enkelttiltak.

Med vennlig hilsen

Paul Narum

Paul Narum
Adm direktør