Forsvarets overkommando
Sikkerhetsstaben

Vår dato 2002-11-22 | Vår referanse 2002/06085-2 /FO/S 433

Vår saksbehandler
Sen.rådg. Anders Bjønnes
+47 23 09 80 65, 510 8065
abjoennes@mil.no

Tidligere dato 2002-10-21 | Tidligere referanse NHD/2001/5605 KDB

Til
Det kgl nærings- og handelsdepartement

Kopi til
Det kgl Forsvarsdepartement

Internt

Intern kopi til
AssDir, Sj S1, Sj S2, Sj S3

Strategi for informasjonssikkerhet - grunnlagsdokument

Forsvarets overkommando/Sikkerhetsstaben er i ref bedt om å avgi høringsuttalelse i forhold til et meget bredt anlagt grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet. FO/S har tidligere hatt anledning til å komme i inngrep med prosjektet gjennom orientering om FO/S, Nasjonal sikkerhetsmyndighet og sikkerhetsloven for prosjektgruppen, orientering om forslag til forskrift om objektsikkerhet for styringsgruppen, og indirekte ved dialog med Forsvarsdepartementets representant i styringsgruppen. Det nå fremlagte grunnlagsdokumentet har vært viet interesse i de relevante fagmiljøene og i ledelsen ved FO/S. Synspunkter på deler av dokumentet skal redegjøres for i det følgende.

1 Omfanget av strategien – FO/S' deltakelse i prosjektgruppen

FO/S er enig i at målsettingen med strategien – og dermed rammen for grunnlagsdokumentet - bør være mest mulig vidtfavnende og helhetlig i forhold til de ulike behov for informasjonssikkerhet som finnes i samfunnet. Dette innebærer imidlertid at et meget bredt spekter av risiki, tiltaksområder og utviklingstrekk må redegjøres for, utfordringer identifiseres, målsettinger etableres og forslag til tiltak utformes. Faren er dermed til stede for at delområder ikke blir dekket i nødvendig grad.

FO/S savner i den forbindelse en bredere beskrivelse av informasjonssikkerhet med utgangspunkt i sikkerhetsloven, herunder igangsatte tiltak og satsninger. En forutsetning for en slik helhetlig tilnærming i strategiarbeidet burde etter vår mening dessuten ha medført at FO/S som Nasjonal sikkerhetsmyndighet (NSM), med betydelige fag- og tilsynsoppgaver innen IT-sikkerhet rettet mot det offentlige og private, var med i prosjektgruppen.

2 Koordinering av IT-sikkerhet

Grunnlagsdokumentet omfatter en rekke konkrete forslag til tiltak. Et av de mer omfattende forslag innebærer etablering av et koordineringsråd for IT-sikkerhet hvor blant andre myndighetsorganer og aktører med oppgaver innen IT-sikkerhet skal møtes. Dette tiltaket foreslås for å få til en nødvendig koordinering slik at brukerperspektivet kan bli tilgodesett i nødvendig grad. Rådet foreslås dessuten supplert med et sekretariat med til dels selvstendige og initierende oppgaver.

FO/S er enig i at myndigheter med ansvar innen IT-sikkerhet må samarbeide slik at de samfunnsmessige krav og forventninger som stilles til virksomhetene oppleves som relevante, koordinerte og mulige å tilfredsstille. FO/S er imidlertid ikke overbevist om at svaret på utfordringen med å ha flere regelverk og flere myndighetsorganer, er å kreere enda et nytt organ, og i særdeleshet ikke å etablere et sekretariat som i henhold til forslaget skal besitte "supplerende kompetanse" i forhold til departementer og myndigheter. Norge er et lite land, og IT-sikkerhetsmiljøene relativt små. Tiltak som kan bidra til fragmentering og bygging av alternative miljøer - som i hvert fall rekrutteringsmessig vil måtte konkurrere med hverandre - bør ikke etterstrebes. Etter FO/S' mening bør man "for å gripe ondet ved roten" tvert i mot se på en mulig reduksjon av antallet sentrale myndighetsorganer og utøvende organer på IT-sikkerhetsområdet. Man bør kraftsamle om få, men utviklingsdyktige miljøer, som samtidig kan ivareta et helhetlig brukerperspektiv i forhold til konfidensialitet, integritet og tilgjengelighetsproblematikk. Etter FO/S' mening bør Justisdepartementets nå etablerte overordnete ansvar for samfunnssikkerhet og beredskap i sivil sektor følges opp også innen IT-sikkerhetsområdet. Dette ved at Arbeids- og administrasjonsdepartementets og Nærings- og handelsdepartementets nåværende ansvar for IT-sikkerhet revurderes.

Som det vil være kjent for prosjektgruppen har FO/S (Nasjonal sikkerhetsmyndighet), i tillegg til oppgaven som fag- og tilsynsmyndighet i henhold til sikkerhetsinstruksen og senere sikkerhetsloven, også i en årrekke ivaretatt tilsvarende rolle for IT-sikkerhet (datasikkerhet) i henhold til Beskyttelsesinstruksen etter avtale med Statsministerens kontor. Dette har medført en samordning på tiltakssiden som har kommet statlige etater (som er bundet av Beskyttelsesinstruksen) til gode. Et tiltak som ville bidra til ytterligere samordning og et bedre brukerperspektiv er om denne modellen, med NSM som aktør i forhold til utvikling av tiltak og tilsyn, kunne bli videreført til å gjelde også for andre regelverk som foreskriver krav til IT-sikkerhet (herunder personopplysningsloven og kredittilsynsloven).

3 Inntregningstesting

NSM skal i henhold til sikkerhetsloven kunne gjennomføre inntregningstesting i informasjonssystemer som behandler skjermingsverdig informasjon. I fremtiden vil denne oppgaven sannsynligvis også omfatte styringssystemer som selv klassifiseres som skjermingsverdige objekter eller som understøtter slike objekter. Grunnlagsdokumentet understreker betydningen av at slike tester også gjennomføres i telenettet generelt (s 50) og mot samfunnskritiske IT-systemer som ikke faller inn under sikkerhetslovens bestemmelser (s 52). Prosjektgruppen anbefaler at Justisdepartementet og Forsvarsdepartementet i fellesskap avklarer hvilket departement som skal ha ansvaret for dette.

Etter FO/S' mening er det vesentlig at kompetansen til å gjennomføre slike tester ikke spres, og at den er under samfunnsmessig kontroll. Med bakgrunn i at NSM alt har en oppgave innen inntregningstesting med hjemmel i sikkerhetsloven, og i fremtiden vil være begge departementers utøvende ledd, finner FO/S' det naturlig at ansvaret for utførelsen av slike tester av samfunnsmessig betydning generelt legges til NSM.

4 Gjenbruk av tiltak

Som nevnt tidligere bør brukerperspektivet være viktig på IT-sikkerhetsområdet. Generell økonomisering i forhold til tiltak bør også være vesentlig. En strategi som tilfredsstiller begge disse hensyn, men som ikke i særlig grad er nevnt i grunnlagsdokumentet, er gjenbruk av mekanismer og tiltak innen IT-sikkerhet på tvers av regelverks- og virkeområder. Sikkerhetsloven med forskrifter skal motvirke særlig kraftfulle trusler som spionasje, sabotasje og terrorhandlinger som kan tenkes å ramme informasjon og objekter av betydning for Rikets sikkerhet og vitale nasjonale sikkerhetsinteresser. Tiltakene på IT-sikkerhetssiden vil derfor være

rettet inn mot å skape en særlig grad av robusthet. En rekke av disse tiltakene bør enkeltvis eller i system kunne anvendes, slik de er eller nedskalert, innenfor andre regelsett eller for andre formål. Dette gjelder for hele spekteret av forebyggende sårbarhetsreduserende tiltak, så som innen systemsikkerhet, kommunikasjonssikkerhet, fysisk sikring, personellsikkerhet, industrisikkerhet og sikkerhetsadministrasjon.

Etter FO/S' mening bør tiltak og veiledninger utformet med tanke på sårbarhetsreduksjon i forhold til sikkerhetslovens formål, også kunne være et godt utgangspunkt for å dekke andre IT-sikkerhetsbehov i samfunnet.

5 PKI

FO/S er sentral i arbeidet med å utvikle en PKI-tjeneste for Forsvaret. Etter vår mening bør det - slik prosjektgruppen foreslår - være et mål å utvikle en felles statlig PKI som kan legge til rette for ivaretakelse av de ulike samfunnsmessige beskyttelsesbehov. Det kan reises innvendinger mot at staten søker å utvikle og ivareta en slik tjeneste og ikke overlater dette til det private initiativ og marked, herunder med den begrunnelse at det kan bli vanskelig å holde tilstrekkelig tritt med utviklingen på området, kostnadene kan bli for store, etc.

Etter FO/S' mening er det imidlertid vesentlig at man får til høy grad av interoperabilitet på dette området og at systemet gjennomgående bygger på tillit. Det kan derfor være hensiktsmessig at det etableres en ordning hvor et statlig sikkerhetsorgan (NSM) er Root CA, og utsteder sertifikater til private tilbydere eller til virksomheter med egne PKI-systemer. Dette bidrar til høy tillit og brukerne kan kommunisere med hverandre uavhengig av hvem som er tilbyder (samtrafikk).

6 Avslutning

Som kjent har Regjeringen foreslått overfor Stortinget å nedlegge FO/S 1/1 2003 og fra samme dag opprette funksjonen NSM som et direktorat. Forsvarssjefens sikkerhetsansvar innen egen etat utøves av et nytt organ benevnt Forsvarets sikkerhetsavdeling (FSA). NSM vil være administrativt underlagt FD, men med faglig rapporterings- og ansvarslinje for hhv sivil sektor til Justisdepartementet og for militær sektor til FD. Endringene vil bli endelig bestemt gjennom vedtakelse av statsbudsjettet for 2003 (St prp nr 1). Det nye direktoratet vil i tillegg til oppgaven som NSM etter sikkerhetsloven også ha oppgaver knyttet til Beskyttelsesinstruksen. Sannsynligvis vil direktoratet også få oppgaver knyttet til Lov om forsvarshemmeligheter og Lov om oppfinnelser av betydning for rikets forsvar. Videre vil direktoratet ha oppgaven med å ivareta sertifiseringsordningen i forhold til produkter og systemer (SERTIT), og bidra i VDI-samarbeidet.

Med bakgrunn i den ovennevnte oppgaveportefølje og faglig kompetanse innen IT-sikkerhet ønsker FO/S (fra 1/1 2003 NSM) å bidra konstruktivt til det fortsatte arbeidet med en nasjonal strategi for informasjonssikkerhet.

Jan Erik Larsen (ef)
Direktør
Sjef Sikkerhetsstaben