Datatilsynet

Nærings- og handelsdepartementet
Pb. 8014 Dep
0030 Oslo

Deres ref	Vår ref (bes oppgitt ved svar)		Dato
	2002/1865-2	as/lta	22.11.2002

HØRING AV GRUNNLAGSDOKUMENT FOR UTARBEIDELSE AV NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET

Vi viser til Deres brev av 21. oktober 2002 vedrørende ovennevnte.

Innledningsvis ønsker vi å kommunisere at vi støtter forslag om en nasjonal strategi innen temaet informasjonssikkerhet. Samfunnets avhengighet av informasjonsteknologi gir klare indikasjoner på behovet for en klar og konkret strategi innen dette viktige område. Datatilsynet konstaterer at strategiplanen spenner vidt og griper inn i store deler av vårt samfunn. Vi vil hevde at planen skisserer interessante ambisjoner innenfor et bredt spekter av tjenester og relasjoner innen informasjonssamfunnet. Sentrale spørsmål som fokus, prioriteringer og ambisjonsnivået er imidlertid av stor betydning i denne sammenheng, hvilket vil være gjenstand for kommentarer i vårt høringssvar.

Generelle kommentarer

Datatilsynet konstaterer at dokumentet "Nasjonal strategi for informasjonssikkerhet" har et meget bredt nedslagsfelt og skisserer ønsket utvikling hos et betydelig antall aktører. På den ene side ser vi verdien i å "inkludere alt og alle", på den annen side ser vi faren for at planen kan bli så omfattende at det vil være vanskelig å realisere de ønskede mål. Det kan imidlertid trolig stryke dokumentet om det på overordnet nivå tydeligere gjøres til kjenne hva som eventuelt bør prioriteres og til hvilken tid. Vi antar at dokumentet vil generere underliggende handlingsplaner hvor dette eventuelt vil konkretiseres, men vi mener dog likevel at man i dette dokumentet bør skisseres visse hovedprioriteringer. I den grad dette ikke gjøres, hva er det ellers som skal styre prioritering av skisserte tiltak?

Strategiplanen tar utgangspunkt i en metodikk hvor fokus og innsats defineres på tre hovednivåer, henholdsvis samfunn, virksomhet/institusjon og individ. Datatilsynet støtter denne form for tilnærming da innsats og virkemiddelbruk innenfor disse nivåene vil ha klare likhetstrekk.

Når det gjelder fokus i forhold til informasjonssikkerhet på samfunnsnivå, mener vi at strategien ikke i tilstrekkelig grad berører forhold knyttet til sabotasje, fysiske eller logiske anslag mot vitale strukturer i informasjonssamfunnet. I begrepet logiske anslag legger vi alt

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

fra uautorisert tilgang til slike strukturer til bruk av ondsinnet programvare i den hensikt å lamme tilsvarende strukturer. Vi konstaterer at dette er berørt i avsnitt 6.1.1, men etter vårt syn bør strategiene i forhold til dette fremstå som noe klarere. Vi viser for øvrig også til merknad senere i dette brevet om at vi mener kritisk infrastruktur er definert noe snevert i denne anledning.

Datatilsynet mener videre at strategien kunne profilert de underliggende drivkrefter for de satsninger som skisseres i dokumentet. Hva er det som gjør at akkurat de nevnte forhold er viktige? Er motivet å sikre storsamfunnets interesser, tilrettelegging for næringsutøvelse, tillit mellom virksomhet/kunde eller vil også vern om den personlige integritet tilsvarende være en drivkraft. Vi ser at de tre overordnede mål peker ut en viss retning i denne sammenheng, men en nærmere stadfesting kunne være nyttig. Datatilsynet ønsker naturlig nok å peke på behovet for å også legge vekt på ideelle hensyn, hvilket personvern representerer i denne sammenheng.

Datatilsynet savner en klarere profil i forhold til definering av mål. En strategiplan bør ha definert klare mål, med tilhørende målkriterier. Dette er nødvendig for å verifisere at innsatsfaktorene tross alt medfører at utviklingen går i den retning strategiplanen peker. I innledning til kapittel 6 og 7 defineres riktignok målsettinger, men disse er av så overordnet karakter at disse samlet sett nærmest fremstår som en samlet visjon for prosjektet. Målsettingen i kapittel 8 må vel i motsetning sies å være konkret nok. Vi anbefaler at nevnte forhold gjøres gjenstand for videre drøftinger i prosjektgruppen.

I strategien synes begrepet "bør" å være benyttet i utstrakt grad, dog i noen tilfeller benyttes begrepet "skal". Vi er usikker på hvordan dette eventuelt skal tolkes, men ønsker å understreke betydningen av å realitetsvurdere hvordan og med hvilke virkemidler disse partielle planer skal nås. Dokumentet vil leses av et vidt spekter av profesjoner og begrepsbruken er derfor av viktig betydning. Videre vil vi igjen understreke betydningen av å ha reelle målbare kriterier som i dette tilfelle bør knyttes til de partielle planer. Det synes åpenbart at formuleringer alene neppe vil resultere i at de enkelte virksomhetene vil la bedriftsøkonomiske vurderinger vike til fordel for storsamfunnets interesser, jf. for eksempel 6.1.1 og 6.2.1.

Vi etterlyser videre en klarere strategi for hvordan storsamfunnet skal sikre at også de virksomheter som alene er tuftet på bedriftsøkonomiske kriterier, vektlegger de føringer som blir fremlagt i strategiplanen. Den reelle kontroll over kritisk/sentral infrastruktur ligger i dag ofte helt eller delvis på privat eierskap, med de konflikter det kan skape mellom bedriftsøkonomiske interesser og storsamfunnets behov. Eksempel på kritisk infrastruktur som helt eller delvis forvaltes etter tilnærmet bedriftsøkonomiske hensyn er kraftforsyning (netteiere), telenett (Telenor, jernbaneverket, kraftselskapene m.v.). Informasjonssikkerhet vil i hovedsak inkludere konfidensialitet, integritet og tilgjengelighet. Tilgjengelighet er et forhold som blir stadig mer viktig, hvilket innebærer at betydningen av pålitelig strømforsyning også vil være av vital betydning.

Datatilsynet tror det kunne vært nyttig å vurdere behovet for å ta inn en kort beskrivelse av kritiske faktorer i forhold til måloppnåelse. Dette kunne med fordel gjøres etter samme struktur som planen for øvrig legger opp til, nemlig samfunn, virksomhet/institusjon og enkeltindivid.

Kommentarer til de enkelte kapitler

De innledende kapitlene (kapittel 1 til 4) synes å ha til formål å gi bakgrunnsinformasjon, generell informasjon og definisjoner rundt temaet informasjonssikkerhet. Dette er informasjon som må sies å være allmenn tilgjengelig, gruppen kan derfor vurdere å korte noe ned på denne informasjon. I den grad informasjon skal beholdes bør dette ha særlig relevans i forhold til de tema som senere berøres i planen.

I kapittel 5 beskrives relevante virksomheter og aktører som helt eller delvis arbeider med informasjonssikkerhet i sitt arbeid. Eksempler på dette er Etterretnings- og Sikkerhetstjenesten, Datatilsynet, Kredittilsynet, Post- og Teletilsynet m.v. Vi tror det kan være nyttig å foreta en slik gjennomgang, men det synes å mangle en videre hensikt med å liste opp disse institusjonene. Av teksten fremgår at man ønsker å kartlegge alle statlige virksomheter som arbeider med temaet informasjonssikkerhet. Det er likevel naturlig å spørre seg: Hvorfor er disse listet opp og hvilken rolle er disse tiltenkt i strategiplanen? Vi antar at man ser for seg at disse institusjonene har og kommer til å ha en rolle i forhold til å implementere deler av planen, i så fall bør dette fremgå mer spesifikt senere i dokumentet. Unntak fra sistnevnte er imidlertid Post og Teletilsynet som tillegges en konkret rolle i kapittel 6.

I kapittel 6 beskrives en rekke forslag til strategier for å sikre kritisk infrastruktur på samfunns- og virksomhetsnivå. Vi konstaterer at svært mye oppmerksomhet når det gjelder kritisk infrastruktur konsentreres om telekommunikasjon alene. Etter vårt syn vil begrepet "kritisk infrastruktur" spenne noe videre, et eksempel på dette kan være kraftforsyning. Vi anbefaler at dette punkt vurderes i den videre prosessen.

Kapittel 7 tar for seg beskrivelse av tiltak for å styrke sikkerhetskulturen på ulike nivåer i samfunnet, virksomhetene og individet. Datatilsynet støtter forslaget om satsning på å opparbeide en bedre bevissthet om informasjonssikkerhet. Holdninger hos enkeltindividene er det som til syvende og sist vil danne sikkerhetskultur både i virksomhetene og i storsamfunnet. Vi konstaterer imidlertid relativt vage formuleringer, som etter ordlyden må sies å være lite forpliktende. Dersom de skisserte ambisjoner skal kunne realiseres, bør det ligge klare og entydige føringer for hvordan disse ambisjonene skal kunne nås. Datatilsynet reagerer på formuleringene i avsnitt 7.1.6 hvor det i strategien nærmest konkluderes med økt behov for lagring av logger ved bruk av internett. Datatilsynet mener at dette tema behandles i andre fora, for eksempel datakrimutvalget, hvor nettopp forhold som omtales i strategien vurderes. Det er derfor etter vårt syn ukorrekt å trekke konklusjoner i en så komplisert og til dels personverntruende problemstilling. Vi foreslår at nevnte avsnitt modereres noe.

Datatilsynet støtter de betraktninger som er gjort i kapittel 8 vedrørende behov for å arbeide videre med å etablere en egnet struktur for sikker elektronisk kommunikasjon ved bruk av PKI. Vi forutsetter imidlertid at grunnleggende personvernhensyn ivaretas i slike strukturer. Behov for eller ønsket om anonymitet i visse tilfeller bør etter Datatilsynets vurdering fortsatt være et naturlig alternativ også i fremtiden. Sistnevnte trenger selvsagt ikke utelukke at spor kan gjøres tilgjengelig politi/påtalemyndighet i den grad det foretas kriminelle handlinger.

Datatilsynet mener at den skisserte nasjonale sikkerhetsstrategi vil kunne gi positive bidrag til å sette informasjonssikkerhet på dagsorden innen opplæring/undervisning, og etablering og sikring av infrastruktur. Vi håper imidlertid at våre anførsler kan bidra til å gjøre dokumentet ytterlig bedre, med klarere prioriteringer.

I den grad prosjektet ønsker ytterlig utdyping av våre synspunkter, ber vi om at det tas kontakt.

Med hilsen

Leif T. Aanensen (e f)
avdelingsdirektør

For Aksel Sogstad
senioringeniør