Vår saksbehandler	Vår dato	Vår referanse
Udir C Rapp og sening H C Eriksen	2002-11-26	200202295-5 /FO/E/350.2
	Tidligere dato	Tidligere referanse
	2002-10-21	NHD/2001/5605 KDB

Til
Nærings- og handelsdepartementet

Kopi til

Internt

Intern kopi til

Høringsuttalelse – grunnlagsdokument for nasjonal strategi for informasjonssikkerhet

1 Bakgrunn

Nærings- og Handelsdepartementet har bedt om høringsuttalelse i forbindelse med grunnlagsdokument for nasjonal strategi for informasjonssikkerhet. Initiativet til grunnlagsdokumentet er tatt i fellesskap av Justisdepartementet (JD), Forsvarsdepartementet (FD) og Nærings- og Handelsdepartementet (NHD). Prosjektarbeidet er ledet av NHD, og dokumentet er produsert av representanter fra NHD, JD og rådgivningsselskapet PriceWaterhouseCoopers DA.

2 Hovedinntrykk

Forsvarets etterretningstjeneste er av den oppfatning at det ovennevnte grunnlagsdokumentet gir et godt utgangspunkt for en videre utarbeidelse av en helhetlig strategi på området. Dokumentets struktur er velorganisert, terminologien er i det vesentlige god og innholdet i sin form lettlest. Strukturen og innholdet favner alle kritiske momenter i IT-sikkerhet og beskriver på en god måte sikkerhetstrusler, sårbarhet og administrative og tekniske sikkerhetstiltak for ulike formål og situasjoner.

Forsvarets etterretningstjeneste synes detaljnivået i grunnlagsdokumentet er noe ujevnt. På enkelte områder er det meget grundig redegjort for problemstillingene, f eks om sikkerhetskultur, kommunikasjonssikkerhet og PKI. På enkelte andre områder som kan være like viktig i et helhetsperspektiv er det derimot noe mangelfull redegjørelse, f eks om identifisering av trusler og vurdering av deres kapasitet og intensjon samt om sikkerhetsmekanismer i systemer uavhengig av om informasjonen er ment overført mellom ulike (del)systemer eller ikke. Grunnlagsdokumentet favner imidlertid såpass bredt at det er vanskelig å gi en jevn fremstilling. I tillegg forstår vi det slik at det som er mest omtalt anses å være de største utfordringene på området vi har pr i dag. Det er derfor forståelig at detaljnivået kan synes noe selektivt.

3 Kommentarer til et utvalg emner

3.1 Dokumentets tittel kontra innhold – informasjonssikkerhet og IT-sikkerhet

Dokumentet bruker begrepet informasjonssikkerhet i tittelen. Innholdet dreier seg likevel hovedsakelig om IT-sikkerhet (eller IKT-sikkerhet).

Informasjonssikkerhet omfatter også sikkerhet f eks ved manuelle dokumenter og lagringsmedier som ikke er produsert elektronisk og verbal kommunikasjon utenom tekniske

kommunikasjonsmidler. Selv om IT-sikkerhet i praksis er den mest dominerende del av området, er ikke all informasjonssikkerhet ensbetydende med IT-sikkerhet. Dette kan illustreres ved å vise til struktur og innhold i forskrift om informasjonssikkerhet (som feilaktig er kalt "forskrift om IT-sikkerhet" i grunnlagsdokumentets side 20 første avsnitt) gitt i medhold av sikkerhetsloven.

Også de andre internasjonale standardene som er bakgrunnen for mye av dokumentet gjelder IT-sikkerhet, noe som er gjenspeilet i titlene for disse.

Dokumentets tittel oppleves derfor noe misvisende og bør endres til "IT-sikkerhet", "IKT-sikkerhet" eller lignende. I tillegg bør skillet mellom informasjonssikkerhet og IT-sikkerhet forklares innledningsvis i dokumentets tekst.

3.2 Harmonisering og samordning

Den enkelte virksomhet (både forvaltningsorganer og til dels private virksomheter) må ofte forholde seg til flere ulike regelverk og tilsynsmyndigheter for informasjonssikkerhet. Det er unødvendig vanskelig å orientere seg og sammenholde ulike regelverk på området, hvilket er en kompliserende og dermed også fordyrende faktor for mange virksomheter. Forsvarets etterretningstjeneste støtter derfor spesielt forslaget i grunnlagsdokumentet om at ulike regelverk og normer for informasjonssikkerhet/IT-sikkerhet i større grad må harmoniseres og "effektiviseres".

Vi deler også oppfatningen om at ansvars- og myndighetsområdet for kritisk infrastruktur/objektsikkerhet i "høyrisikoområdet" må avklares nærmere. DSB og NSM har et ansvars- og myndighetsområde som, i hvertfall tilsynelatende, i stor grad overlapper hverandre.

3.3 Prioritering av tiltak

Grunnlagsdokumentet har forslag som innebærer dels langsiktige og dels kortsiktige perspektiver. I konsekvensanalysen til slutt konkluderes det bl a med at det er et politisk prioriteringsspørsmål hvilke tiltak som skal være satsningsområder og hvilke som skal tas innen ordinære budsjettrammer.

Forsvarets etterretningstjeneste mener at det ville vært en fordel om det, som grunnlag for slike beslutninger, ble foreslått en nærmere prioritering av forslagene/tiltakene. Dersom dette var tatt inn i grunnlagsdokumentet, ville høringsinstansene fått anledning til å uttale seg også om slike prioriteringsspørsmål.

På denne bakgrunn mener Forsvarets etterretningstjeneste at forslagene/tiltakene mht gjennomføringen bør gis en klarere oppdeling i hhv langsiktige og umiddelbare tiltak. F eks kan en rekke tiltak i/for den enkelte virksomhet pålegges eller anbefales gjennomføres forholdsvis raskt, mens det på nasjonalt nivå derimot vil være mer langsiktige perspektiver som må legges til grunn. Prioriteringen bør gjøres på grunnlag av en vurdering av hva som er viktigst å få på plass ut i fra risikobildet isolert sett (trussel, sårbarhet og skadepotensial), antatte administrative og økonomiske konsekvenser og den antatte tid gjennomføringen vil ta i praksis.

3.4 Trusselinformasjon til bruk i risikovurderinger

Trusselvurdering er en sentral del av risikobegrepet, hvilket også fremgår i grunnlagsdokumentets side 11 og 12 (definisjoner) og side 23 to første avsnitt. Sentrale myndigheter som PST, FO/E, ØKOKRIM's datakrimsenter og DSB (sistnevnte mht naturgitte og utilsiktede trusler/hendelser) kan bidra med å innhente og vurdere opplysninger i denne sammenheng. Grunnlagsdokumentet påpeker at Senter for informasjonssikring (SIS) og til dels forbrukermyndighetene har en rolle i å bl a formidle helhetlig trusselinformasjon, men da primært til private virksomheter og befolkningen.

Forsvarets etterretningstjeneste savner likevel en større fokusering på at tilstrekkelig informasjon om sikkerhetstrusler er en nødvendig forutsetning for gode risikovurderinger i enhver

virksomhet. Det fremstår noe uklart hvordan den enkelte virksomhet eller etat, offentlig eller privat, i praksis kan tilegne seg oppdatert og helhetlig trusselinformasjon, dvs unngå å måtte rette enkelthenvendelser til alle ovennevnte organer. Informasjonsflyt basert på utelukkende enkelthenvendelser er meget ineffektivt, både for virksomhetene selv og organene som kan levere informasjonen, unntatt for virksomheter med et særskilt behov eller ved ekstraordinære situasjoner. Er bare SIS tiltenkt oppgaven med å gi samordnet informasjon om trusler mot IT-sikkerheten til den enkelte virksomhet, og er SIS i så fall dimensjonert for dette?

For øvrig vil vi vise til kommentaren vår under avsnitt 2 i dette brev om at redegjørelsen for sikkerhetstruslene virker noe mangelfull. Også enkelte forskningsmiljøer mener sikkerhetstiltak (mot terrortrusler) i større grad bør innrettes etter sannsynlighet for inntreden fremfor utelukkende objektiv sårbarhet. I denne sammenheng bør den enkelte virksomhet i større grad pålegges eller anbefales å lage beredskapsplaner for lokalt tilpasset reaksjonsmønster ved inntreden av ulike typer trusler mot bl a IT-sikkerhet (spesielt virus og såkalte DoS-angrep). Et eksempel på slike planer er de som pålegges etter Forsvarssjefens terrorberedskapsdirektiv. Iht direktivet pålegges den enkelte virksomhet å ha planer for tiltak ved ulike eskaleringsnivåer (fire ulike tiltaksnivåer, hhv ALFA, BRAVO, CHARLIE og DELTA, som skal iverksettes ut i fra antatt terrortrusselnivå). En forutsetning for slike planer og tiltak er imidlertid at rutiner for formidling av trusselinformasjon og -varsling er etablert.

Forsvarets etterretningstjeneste mener ovennevnte problemstillinger bør synliggjøres bedre i strategien enn tilfellet er i grunnlagsdokumentet.

3.5 Høyere utdanning innen sikkerhet

Grunnlagsdokumentet påpeker at det bør etableres høyskoleutdanning på masternivå og høyere innen sikkerhet. Det fremkommer ikke at det nylig ble opprettet et godkjent masterstudium for IT-sikkerhet ved Høyskolen på Gjøvik (så vidt vi vet godkjent av et svensk universitet).

Forsvarets etterretningstjeneste mener det er vel så viktig at det etableres høyere utdanning med en *helhetlig* tilnærming til informasjonssikkerhet og objektsikkerhet, herunder IT-sikkerhet. De utdanningsretninger som finnes i dag er ofte spesialiserte. Det er fremdeles behov for flere spesialister på en rekke områder innen sikkerhet, men det er nok like stort behov for ledere og generalister som kan se mer helhetlig på metodikk og utfordringer innen faget. Dette gjelder spesielt for små og mellomstore virksomheter/forvaltningsorganer som ut i fra begrensede ressurser eller behov har mer behov for ledere og generalister med sikkerhetskompetanse fremfor mange ulike spesialister.

3.6 Koordineringsråd for IT-sikkerhet

Forsvarets etterretningstjeneste mener det bør utvises varsomhet med å utnevne nok et råd eller forum innen IT-sikkerhet. Som det påpekes i grunnlagsdokumentet er det allerede nok av organer på området. Et slikt råd vil også lett komme til å overlappe Forum for IT-sikkerhet. Koordineringsrådet bør komme ut av en eksisterende organisasjon eller en sammenslåing av flere eksisterende.

Ut i fra dette synes Forsvarets etterretningstjeneste det er bedre om Forum for IT-sikkerhet utvides og kanskje splittes i en "kjernegruppe" med de mest sentrale myndighetene og en "referansegruppe" med representasjon fra mer perifere myndigheter, næringslivet og akademisk miljø. SIS kan med fordel knyttes opp mot en slikt råd/forum. Rapporteringslinjene må da også endres noe i forhold til hva som er tilfelle for det eksisterende Forum for IT-sikkerhet. Det må også tas stilling til hvilke type beslutninger et slikt organ kan ta – slik at det ikke bare begrenses til mer "uforpliktende" råd og utsagn. I vurderingen av dette kan mønsteret for Koordinerings- og rådgivningsutvalget for EOS-tjenestene (KRU) være et nyttig utgangspunkt.

3.7 Diverse mindre forhold

Side 5, første avsnitt:
Avsnittet påpeker at sikkerhet og tillit til teknologi er viktig for at samfunnsøkonomien skal fungere tilfredsstillende. Forsvarets etterretningstjeneste mener at sikring av andre nasjonale interesser, liv og helse, rettssikkerhet, personvern og velferd er vel så viktige hensyn, noe som burde vært omtalt i avsnittet.

Side 11 og 12:
Definisjonene av kritikalitet og skadeomfang/skadevirkning synes å være meget like. For å unngå forvirring bør en av definisjonene tas ut eller presiseres slik at forskjellen blir tydeligere.

Side 30, siste avsnitt:
Det er noe misvisende at Forsvarsdepartementet etter sikkerhetsloven har ansvaret for sikre personell og anskaffelser i seg selv. Det som skal sikres etter sikkerhetsloven er informasjon og objekter (materiell). Kapittelet om personellsikkerhet gjelder ikke sikring av personell, men sikkerhetsklarering, personkontroll og autorisering av personell som et spesialtiltak for å sikre informasjon eller objekt. Reglene om anskaffelsessikkerhet gjelder i det vesentlige klarering av juridiske personer av samme hensyn som etter personellsikkerheten.

Side 37, pkt 5.2.1:
Avsnittet om inndeling basert på type informasjon kan gi inntrykk av at det nærmest er valgfritt om man skal gradere etter sikkerhetsloven eller beskyttelsesinstruksen, og at hvis så ikke er gjort, kommer disse regelverkene ikke til anvendelse.
Hva som skal graderes er presisert i regelverkene og formulert som pliktregler. Det sentrale er derfor ikke om informasjonen *er* gradert, men om den *omfattes* av graderingsreglene i sikkerhetsloven eller beskyttelsesinstruksen (herunder om den *skulle vært* gradert).
Å vise til at det er en rekke av forvaltningens dokumenter som pga følsom informasjon er unntatt offentlighet, uten at det finnes regler for sikkerhet, er ikke korrekt. Dersom skade kan oppstå ved kompromittering og dokumentet kan unntas fra offentlig, *skal* gradering skje iht beskyttelsesinstruksen. Problemet er at beskyttelsesinstruksen av ulike grunner ikke etterleves i tilstrekkelig grad og at det ikke er noe aktivt tilsynsregime for etterlevelse. Det bør derfor vurderes om reglene på området heller bør gis i eller i medhold av lov fremfor "bare" som instruks fra Kongen, samt gjennomføring av et aktivt tilsyn for etterlevelse.
Skillet mellom type informasjon og skadepotensialet er ikke logisk fremstilt. Dette er ikke to ulike prinsipper for inndeling når gradering av informasjon (nevnt under type informasjon) nettopp er å ta stilling til skadepotensialet (nevnt under skadepotensialet).
I tillegg er det bare en mindre del av tiltakene som må godkjennes av NSM. Svært mange regler om tiltak er gitt i forskrifter fra Kongen og Forsvarsdepartementet, og godkjenningsmyndigheten for mange typer informasjonssystemer er her "delegert" til den enkelte virksomhetsleder.

Side 38 første linje:
Forsvarets etterretningstjeneste oppfatter ikke personopplysningsloven § 13 slik at den i første rekke gjelder konfidensialitet og i andre rekke integritet og tilgjengelighet. En naturlig tolkning av ordlyden tilsier at de tre sikkerhetsinteressenes i prinsippet er likestilt. Det er først etter en konkret vurdering av verdi/skadepotensial i det enkelte tilfelle at det kan sies noe om hvilken vekt de ulike sikkerhetsinteressene skal tillegges.

Side 40 første avsnitt siste setning:
Andre steder i grunnlagsdokumentet er det gjort et konsekvent skille mellom forebyggende sikkerhet (kalt sikkerhet i den daglig oppgaveløsning) og beredskap (ved eskalering av kriser og unormale hendelser). I dette avsnittet er imidlertid disse to områdene blandet sammen ved at Justisdepartementets fagansvar for forebyggende sikkerhet etter sikkerhetsloven settes i sammenheng med samme departements ansvar for den sivile beredskap hjemlet i

en egen instruks, jf det som står i parentes. Det som står i parentes burde derfor etter vårt syn vært fjernet.

Side 42 første avsnitt siste setning: Forsvarets etterretningstjeneste er enig i at systemeiere bør trekkes tungt inn i vurdering av skjermingsverdien til systemer. Erfaring fra arbeidet med nøkkelpunkter og distriktsobjekter viser imidlertid at manglende oversikt over helheten kan medføre at lokale ledd overvurderer betydningen av egne objekter, noe som igjen kan gjøre at hele sektorer overvektes i forhold til andre. Det er derfor like viktig at det skjer en *overordnet* prioritering/beslutning om skjermingsverdighet der systemeiers innspill bare er en del av grunnlaget.

4 Konklusjon

Forsvarets etterretningstjeneste mener grunnlagsdokumentet er et godt utgangspunkt for en nasjonal strategi for informasjonssikkerhet. Vi ber om at ovennevnte innspill blir vurdert i den videre utformingen av strategien.

Arne Karstad (ef)
Assisterende direktør
Assisterende sjef Etterretningstjenesten