Deloitte & Touche
Karenslyst allé 20
Postboks 347, Skøyen
N-0213 Oslo

Tel: +47 23 27 90 00
Fax. +47 23 27 90 01

Deloitte
& Touche

31. October 2002

Nærings- og handelsdepartementet
Cort Archer Dreyer
Postboks 8014 Dep
0030 Oslo

NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET - MERKNADER TIL GRUNNLAGSDOKUMENTET

Undertegnede har gått igjennom oversendt grunnlagsdokument som forberedelse til møtet i Forum for it-sikkerhet 6. november, og ønsker å knytte følgende kommentarer til dokumentet:

Økt bruk av IT gir økt sårbarhet i alle samfunnsledd, og alle ledd må involveres i arbeidet med informasjonssikkerhet. Den overordnede ansvarsdeling for sikkerhetsarbeidet må nødvendigvis bli at den enkelte virksomhet har hovedansvar for egen sikkerhet og implementering av konkrete tiltak – mens føringer, koordinering og infrastruktur er et ansvar for fellesskapet. Som grunnlagsdokument for en nasjonal informasjonssikkerhetsstrategi, er det naturlig å fokusere på det siste for å oppnå det første.

Grunnlagsdokumentet berører en rekke elementer med sikkerhetsmessig betydning. Etter vår oppfatning bør èn enda klarere fremheve noen få elementer som det er realistisk å få gjennomført til en overkommelig kostnad, og som samtidig gir god sikkerhetsfaglig "gevinst":

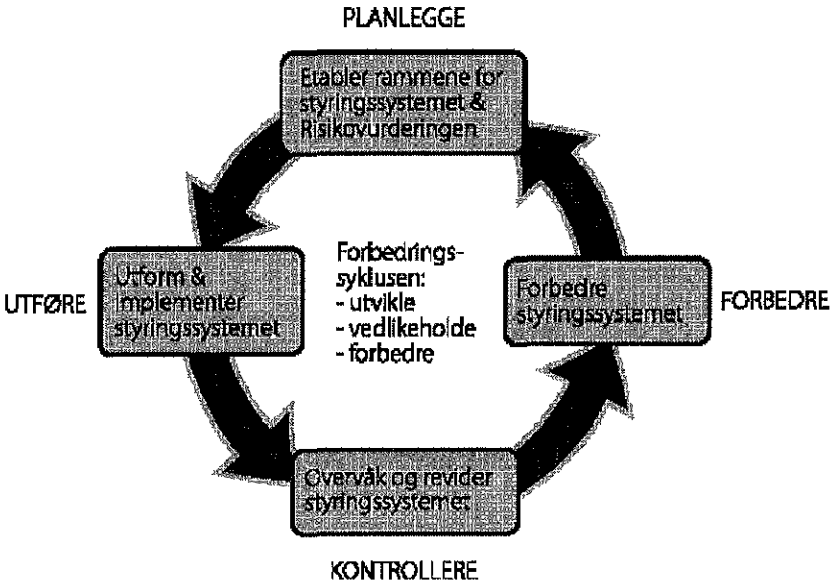
1. Sikkerhetsadministrasjon i samsvar med kravene i BS 7799

Det kan gis en rekke eksempler på avanserte informasjonssystem som er blitt dramatisk påvirket av hendelser som i seg selv ikke er særlig "avanserte". Eksempelene i grunnlagsdokumentet – brudd på telesambandet på Sørlandet, og driftsstans hos Fellesdata – er blant dem. Dette er begge sikkerhetshendelser som skyldes rutinesvikt, det vil si sammenbrud i virksomhetens styringssystem/kvalitetssystem.

Det er derfor mulig å påstå at etablering av formelle styringssystemer vil kunne bidra vesentlig til å hindre sikkerhetsbrudd. Bruk av anerkjente standarder for slikt arbeid gjør innsatsen synlig – gjør det mulig også for utenforstående å ha tillit til sikkerhetsarbeidet. Nærings- og handelsdepartementet har erkjent dette, og derfor bidratt aktivt til etablering av ordning for tredjepartsvurdering av sikkerhetsadministrasjon (sertifisering iht. BS 7799).

Deloitte
& Touche

Styringssystem for sikkerhet omfatter mål og strategi for sikkerhetsarbeidet, risikovurdering som grunnlag for tiltak og oppfølgingsaktiviteter. Formålet er å oppnå kontinuerlig forbedring av sikkerheten, som beskrevet i modellen:



Alle virksomheter som behandler personopplysninger er pålagt[1] etablering sikkerhetsadministrasjon – i praksis i samsvar med kravene i BS 7799. Identiske krav gjelder for Politiet, Utenrikstjenesten, UDI mfl. ved behandling av informasjon ifb. Schengen Informasjonssystemet (ikke kun personopplysninger – all informasjon). Videre gjelder de facto[2] de samme krav ved behandling av helseopplysninger i helsevesenet.

Alle disse virksomhetene skal altså etablere kvalitetssystem som dekker informasjonsbehandlingen. Siden det er vanskelig å etablere flere parallelle styringssystem i en å samme virksomhet, vil kravene nevnt over gi føringer – for ikke å si diktere – disse virksomhetenes sikkerhetsadministrasjon. Etter vår oppfatning gjør dette at "krav" om tilpassing til BS 7799 blir spesielt interessant: Lovverket vil gi viktig drahjelp for å virkeliggjøre en slik strategi, samtidig som det vanskelig kan påstås at elementet er kostnadsdrivende – det er ikke snakk om et nytt krav, kun presisering av et gammelt.

[1] Jf personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.
[2] Jf helseregisterloven § 14 med kommentarer.

Deloitte
& Touche

2. Risikovurdering som grunnlag for sikkerhetsarbeidet

Det har vært tradisjon å basere sikkerhetsarbeid/ implementering av sikkerhetstiltak på klassifisering av informasjon/systemer, og på samsvar med så kalt "best practise". Økt samhandling, og økt "gjenbruk" av informasjon til vidt forskjellige formål, har gjort dette vanskelig – for ikke å si umulig. Samtidig gjør en rivende teknologisk utvikling det til en uoverkommelig oppgave å holde "minimum baselines" og sjekklister oppdaterte.

Sikkerhetsbehov kan i dag ikke knyttes entydig til informasjon eller dataelement. Sikkerhetsbehovet må knyttes til formålet med den prosess informasjonen benyttes i. Eksempelvis vil en ved behandling av helseopplysninger for å gi akutt helsehjelp først og fremst ha behov for tilgjengelighet og integritet, mens en ved behandling av de samme opplysningene for refusjon av behandlingskostnader i første rekke vil stille krav om integritet og konfidensialitet. Som eksempelet viser, vil en og samme opplysning kunne representere vidt forskjellige sikkerhetsbehov.

Dette medfører at kun avgrensede sektorer eller bransjer med helt spesielle sikkerhetsbehov og veldefinerte behandlingsprosesser (eksempelvis Forsvaret) kan basere sikkerhetsarbeidet på det klassifiseringsregimet som skisseres i grunnlagsdokumentet og/eller på detaljspesifiserte sikkerhetsløsninger. Det vil ikke være mulig å klassifisere seg ut av situasjons- og formålsbestemte sikkerhetsbehov. En slik fremgangsmåte vil dessuten være i strid med eksisterende sikkerhetsregelverk.

Alternativet er risikovurdering, det vil si å avdekke konsekvens av og sannsynlighet for hendelser, som underlag for sikkerhetsarbeidet. Dermed blir sikkerhetsarbeidet tilpasset den situasjon den enkelte virksomhet befinner seg i, det vil si optimalisert i forhold til et konkret sikkerhetsbehov. Dette for øvrig i samsvar med anbefalingene i OECD guidelines.

Alle virksomhetene nevnt i forrige punkt er pålagt å benytte risikovurderinger som underlaget for sikkerhetsarbeidet (gjennom de samme bestemmelser som er nevnt). Merknadene foran knyttet til drahjelp for implementering av strategien, og knyttet til kostnader, er derfor også gyldig her.

Det kan anføres at risikovurdering som pålagt i personopplysningsforskriften har som mål å avdekke følgene av en hendelse overfor de mennesker som involveres. Risikovurderingen vil ikke ivareta virksomhetens eller fellesskapets egne behov. Dette er riktig. Som nevnt er risiko kombinasjonen av sannsynlighet og konsekvens. "Sannsynlighet" er i hovedsak knyttet til det miljø opplysningene behandles i (informasjonssystem, organisasjon), og vil være uavhengig av følgene av en hendelsen. Sannsynlighetsvurderinger vil derfor ha gyldighet nærmest uavhengig av hvilke hensyn risikovurderingen er rettet inn mot.

Deloitte
& Touche

Vurdering av "personvernkonsekvens" er imidlertid nært knyttet til personvern som rettighet/verdi. Denne delen av risikovurderingen er derfor mindre anvendbar når andre hensyn skal berøres (forretningsrisiko, "samfunnets sårbarhet" mv). Dette er imidlertid ikke et sentralt poeng. Det viktige er at alle virksomhetene nevnt over har krav om på ta verktøyet risikovurdering i bruk som underlag for sikkerhetsarbeidet. Det må også anføres at det er relativt enkelt å "konvertere" risikovurdering fra personvernorientering til forretningsrisiko – ved å endre konsekvenskriteriene.

3. Harmonisering av sikkerhetsarbeidet

Det er nok flere virksomheter enn det er sikkerhetsregelverk[3] i Norge, men forskjellen i antall er kanskje ikke så stort som enkelte kunne ønske. Svært mange virksomheter berøres av mer enn ett regelsett. Dette medfører behov for koordinering, og regelsettene vil bli koordinert – om ikke andre steder så i alle fall i den enkelte virksomhet. Å overlate ansvaret for, og arbeidet med slik harmonisering til den enkelte virksomhet, kan umulig være fornuftig ressursbruk.

Mange mener at bestemmelsene i beskyttelsesinstruksen gjelder for sikring av "noens personlige forhold" ved informasjonsbehandling i forvaltningen. Personopplysningsforskriftens kapittel 2. gjelder for all behandling av personopplysninger (også i forvaltningen). De to regelsettene er på vesentlige punkter svært forskjellige – hvorfor?

Personopplysningsforskriften gjelder for informasjonsbehandling i finansinstitusjoner. I disse dager har Kredittilsynet foreslått ny IT-sikkerhetsforskrift for de samme virksomhetene. De to regelsettene er forskjellige – hvorfor?

Bildet er likevel ikke helt svart. Som nevnt foran er sikkerhetsreglene som gjelder ved behandling av personopplysninger, helseopplysninger, og informasjon i SIS nærmest prikk like. Derved kan eksempelvis helseforetakene noe enklere etablere sikkerhetstiltak som både gjelder bruk av helseopplysninger og for andre personopplysninger i foretaket.

Harmonisering av sikkerhetsregelverk må gjennomføres der regelene utformes, ikke der de etterleves. Alle ny regelverk bør gjennomgås for å avdekke (unødvendige) forskjeller fra eksisterende krav. Samtidig bør gjeldene regelverk gjennomgås for å vurdere om eventuelle forskjeller faktisk er nødvendige.

Personvern og sikkerhet

Det er en utbredt oppfatning at bestemmelsene om sikring av personopplysninger har et helt annet mål enn virksomhetenes behov og formålet med den informasjonsbehandling som

[3] De fleste regelverkene er nevnt i grunnlagsdokumentet. Sikkerhetsbestemmelsene knyttet til SIS ser ut til å være glemt. Det er muligvis også aktuelt å berøre de forslag som ev. kommer fra strafferegistreringsutvalget.

gjennomføres. Misforståelsen presenteres gjerne som del av spørsmålet: Hvis NSM sikrer vitale nasjonale interesser, og Datatilsynet sikrer personvernet , hvem sikrer da andre hensyn?

Det er viktig å understreke at personvern i denne sammenheng innebærer sikring av konfidensialitet, tilgjengelighet og integritet. Konkret betyr dette at å påstå at personopplysningsloven "til dels" springer ut fra behovet for å bevare konfidensialitet (og ikke de øvrige sikkerhetshensyn) er feil. Og for ordens skyld: personopplysningsloven har ingen særskilte krav til sikring av sensitive personopplysninger. "Sensitiv" er ingen sikkerhetsklassifisering.

Personvern er ikke en egenskap som kan løsrives fra den virkelighet virksomheter og enkeltmennesker befinner seg i. Sikring av konfidensialitet, tilgjengelighet og integritet betyr å sikre at et lovlig formål med behandling av personopplysninger oppfylles. Slike sett er det ingen interessekonflikt mellom individ og virksomhet[4], og det er derfor ikke behov for dobbeltregulering av informasjonsbehandling som allerede dekkes av personopplysningsforskriften.

Da gjenstår kun informasjonsbehandling som ikke er dekket hverken av eller personopplysningslov, helseregisterlov og SIS-loven. For slik informasjonsbehandling bør det være mer aktuelt å ta en av de eksisterende regelverkene i bruk enn å utarbeide helt nye regler[5]. En slik fremgangsmåte benyttes faktisk i dag gjennom Beskyttelsesinstruksen, ved at regler utarbeidet for å beskytte vitale nasjonale interesser tas i bruk også for sikring i forhold til helt andre behov.

PKI

Av alle sikkerhetsrelaterte utfordringer Norge står foran er etablering av PKI etter vår oppfatning den viktigste. Sikker elektronisk meldingstjeneste i vid betydning, er en forutsetning for å kunne ta moderne telekommunikasjon i bruk fullt ut. Grunnlagsdokumentet beskriver dette – og gjør det godt. Tiltaksoversiktene i kapittel 8 er de klareste og mest presise i hele dokumentet.

Det kan stilles spørsmål om etablering av PKI er et strategisk mål i seg selv. Etter vår oppfatning er det et tiltak for å oppnå de målene strategien peker mot, ikke et mål i seg selv. Det kan derfor være aktuelt å revidere målbeskrivelsene i dokumentet – som en formell tilpassing, ikke som et signal om at PKI er mindre viktig.

---

[4] Det er en nyanse her ved at konsekvenselementet i risikovurderingen kun fokuserer på individets behov. Den praktiske løsningen er beskrevet tidligere: Utvidelse av risikovurdering til også å ivareta andre behov så langt disse avviker fra individets interesser.

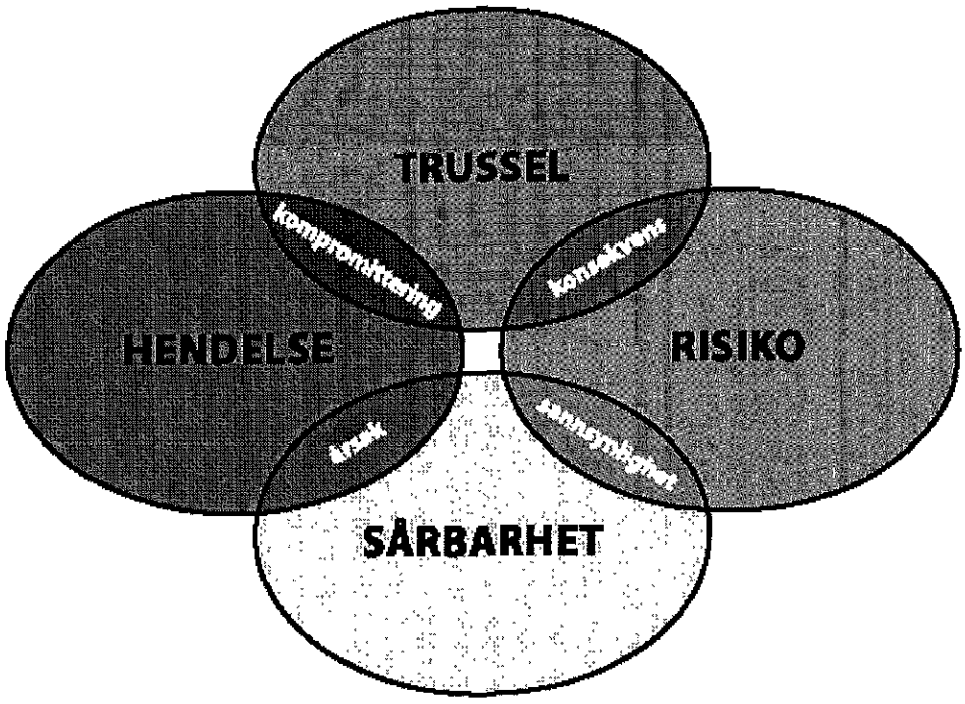
[5] Under enhver omstendighet må grunnlagsdokumentets 6.1.4 gjennomgås siden det her ser ut som det fremmes forslag om utarbeidelse av egen sikkerhetsregler uavhengig av om sikkerhetskrav allerede eksisterer – så lenge informasjonsbehandlingen ikke omfattes av sikkerhetsloven.

Deloitte
&Touche

Viktigere enn om etablering av PKI er mål eller tiltak, er spørsmålet om hvordan infrastrukturen skal etableres. PKI må betraktes som samfunnskritisk infrastruktur. Ansvar for etablering og vedlikehold av slik infrastruktur påhviler fellesskapet. Tar ikke fellesskapet dette ansvaret blir det ingen PKI (like lite som det i sin tid da ville blitt bergensbane, rikstelefon eller kortbaneflyplasser).

Terminologi og språk

Informasjonssikkerhet er et komplekst tema som er vanskelig tilgjengelig for mange. I grunnlagsdokumentet er dette søkt avhjulpet ved innledningsvis å definere sentrale begreper. Etter vår oppfatning fungerer ikke dette helt. Begrepsbruken i dokumentet er ikke konsistent, og begreper og definisjoner er uklare og delvis overlappende. Vi foreslår å legge følgende modell til grunn for sentrale deler av begrepsbruken i dokumentet:



Her er en hendelse beskrevet ved årsak og hvorvidt konfidensialitet, tilgjengelighet eller integritet kompromitteres. En trussel oppstår dersom en kompromittering kan få konsekvenser (for samfunnet, virksomheten, enkeltmennesker), og sårbarhet er et utrykk for hvor sannsynlig det er at hendelsen forårsakes. Risiko er som tidligere beskrevet, kombinasjon av konsekvens og sannsynlighet. Erfaringsmessig bidrar denne modellen til en effektiv introduksjon til saksområdet – også for mennesker som ikke til daglig benytter begreper som informasjonssikkerhet, sårbarhet og risiko.

Deloitte
& Touche

Grunnlagsdokumentet er omfangsrikt. Dette skyldes selvsagt at det beskriver et stort saksområde. Men omfanget skyldes også formuleringer som:

" ... Tjenestekonvergensen kommer til uttrykk ved at både innhold, redigering og tjenestelevering tar opp i seg hverandres formelementer. Et eksempel kan være et forlag som utgir en CD-rom med tekst, levende bilder og lyd, et teleselskap som tilbyr telefoni i kombinasjon med tekstbaserte tjenester, og en Internett-aktør som utvikler tilbud som kombinerer både tekst, lyd, bilde og video. Et annet eksempel kan være en publikasjonsom presenteres i ulike formater, f.eks. ved at bøker utgis både på CD og papir, aviserpubliseres både på nett og papir og at kringkastere publiserer sitt stoff over bådetradisjonelle kanaler og Internett. Et tredje aspekt er fremveksten av flere interaktivetjenester ..."

Her er det to spørsmål å stille: Hvem leser sånt, og hvem har glede av det ? En kritisk gjennomgang av dokumentet med formål å forkorte og forenkle bør gjennomføres.

Et annet bidrag – om ikke til omfang, så muligvis til forvirring – er formuleringer som:

" ... De fleste aktører i samfunnet er enige om at det ikke lenger er behov for ny, omfattende regulering av IT-sikkerhet ..."

Er det dekning for denne typen påstand? Og til det konkret sitatet: Er det samsvar med påstanden og forslaget om nye generelle klassifiseringssystemer ?

Oppsummering

En nasjonal strategi for informasjonssikkerhet er en forutsetning for å takle de sikkerhetsutfordringer vi står midt oppe i, og som ligger foran oss. Grunnlagsdokumentet er et viktig verktøy i så måte. Vi foreslår ytterligere forbedring ved å fremheve noen sentrale, og realistiske elementer:

- Behov for sikkerhetsadministrasjon i samsvar med BS 7799.
- Bruk av risikovurdering som grunnlag for sikkerhetsarbeid.
- Samordning av regelverk.

Vi ser videre for oss at behovet for etablering av PKI ytterligere presiseres, og at det understrekes at dette i første rekke er fellesskapets ansvar.

Deloitte
& Touche

Etter vår oppfatning er det lite trolig at etablering av generelle klassifikasjonssystemer vil bidra til økt sikkerhet. Det er også grunn til å tro at en slik fremgangsmåte vil være i strid med sentrale sikkerhetsregelverk.

Vi håper disse merknadene er til hjelp i det videre arbeid, og bistår gjerne dersom det skulle være ønskelig

Med vennlig hilsen
DELOITTE & TOUCHE
Enterprise Risk Services

Jørn Andreas Arnesen
Manager

Lars Erik Fjørtoft
Manager