STATENS FORVALTNINGSTJENESTE

Administrasjon

Saksbehandler, innvalgstelefon
Else Spilling, 22 24 96 19

Vår dato	Vår referanse
21.11.02	02/00525
Deres dato	Deres referanse
21.10.02	2001/5605 KDB

Det kongelige Nærings- og Handelsdepartement
Postboks 8014 Dep
0030 OSLO

Høring – grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

Vi viser til deres brev datert 21.10.2002 ang. ovennevnte. Statens forvaltningstjeneste (Ft) har følgende merknader:

1. Mål og innretning av strategien

Mandat og målsetting som beskrevet i kap. 1.3 i kulepunktene i første avsnitt virker dekkende. Det er liten tvil om at samfunnsviktig teknologisk infrastruktur p.t. er for sårbar.

Å skulle lage en strategi for informasjonssikkerhet som legger til rette for økt elektronisk samhandling synes imidlertid å være for ambisiøst. Hvis dette punktet skal være med bør det gjøres en prioritering mellom målsettingene hvor dette punktet prioriteres lavest.

Dette punktet må også sees i sammenheng med den tredje av målene for strategien som er beskrevet senere i samme kapittel:

> "Norge skal ha en allment tilgjengelig samfunnsinfrastruktur for elektroniske signatur, autentisering av kommunikasjonspartnere samt sikker overføring av sensitiv informasjon."

Dette målet er av en annen natur enn de to foregående og er langt mer spesifikt og teknologisk rettet mot spesifikke løsninger. Det stilles spørsmålstegn ved om man bør ha med denne typen mål i en nasjonal strategi for informasjonssikkerhet, og anbefales at man vurderer å overlate denne typen satsninger til sterke brukergrupper og private aktører i markedet.

Definisjonen av IT-sikkerhet i kap. 1.5 har en implisitt avgrensning som virker lite hensiktsmessig:

> "Beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet for den informasjon som behandles av informasjonsystemet og beskyttelse av systemet i seg selv."

Dette kan tolkes dithen at det kun er preventive tiltak som hindrer selve bruddet som defineres inn under IT-sikkerhet. Normalt vil man imidlertid også definere

Postadresse	Kontoradresse	Telefon	Telefaks	Bankgiro	Web: www.ft.dep.no
Postboks 8129 Dep 0032 Oslo	Regjeringskvartalet	22 24 90 90 Se saksbehandlers innvalgsnummer	22 24 95 95	7694.05.12073	Internett: postmottak@ft.dep.no

PX-0102 05.01 formulas

skadebegrensende tiltak som iverksettes etter at ett brudd faktisk har skjedd inn under begrepet IT-sikkerhet (krise- og reserve-planer). Spesielt i en slik strategi bør man ikke avgrense seg vekk fra skadebegrensende tiltak.

2. Identifiserte utviklingstrender av betydning for nasjonalt arbeid med IT-sikkerhet

Beskrivelsen i kap. 3 virker stort sett dekkende, men det savnes en beskrivelse av den økende tendensen til integrasjon og samarbeide på tvers av virksomheter. Det er en økende tendens til etablering av kunde-leverandør forhold og strategiske partnerskap med tilgang til hverandres spesialsystemer, samt offentlige virksomheters bruk av fagsystemer på tvers av virksomhetsgrensene (ekstranett). Denne trenden som har vart noen år og høyst sannsynlig vil forsterkes ytterligere. Dette stiller spesielle krav til bevissthet omkring IT-sikkerhet i den enkelte virksomhet.

Det er heller ikke nevnt noe om statistikk omkring hva og hvem de hyppigst forekommende IT-sikkerhetsbrudd forårsakes av. Virksomheters egne ansatte forårsaker en svært stor andel av de brudd som forekommer og de aller fleste av bruddene skyldes menneskelige feil eller feil i programvare/konfigurasjon og er ikke bevisste handlinger ment å skade virksomheten.

Kapittel 3.3, "Elektronisk kommunikasjon og elektroniske tjenester", fokuseres det særdeles lite på hvilke behov og utfordringer som eksisterer. I stedet beskrives hva som er gjort på området og hva som gjenstår å gjøre, spesielt innen feltet PKI.

3. Identifiserte utfordringer for IT-sikkerhet

Vurderingen i innledningen i kap. 4 om realismen i å gjøre det helt usannsynlig å stanse viktige sammfunnsfunksjoner synes noe pessimistisk. For de aller viktigste funksjonene i samfunnet bør det være mulig å etablere teknologiske eller manuelle beredskap- og reserveløsninger som kan ta over for den infrastrukturen som normalt benyttes dersom denne skulle falle bort.

I kapittel 4.10, "Utbredelse av infrastruktur for sikker elektronisk kommunikasjon", er det kun elektroniske/digitale signaturer som trekkes frem av teknologiske løsninger til tross for at noen av de største utfordringene kan løses med andre typer tiltak. Det finnes andre og enklere typer løsninger som f.eks. VPN og engangspassord-løsninger som kan løse mange problemstillinger knyttet til ekstranett og mobilitet, men hvor man fortsatt har utfordringer knyttet til kompatibilitet på linje med det man har for X.509-baserte PKI-løsninger.

Ft har for øvrig nylig erstattet en PKI-basert fjernaksessløsning med en løsning nettopp basert på VPN og engangspassord. Bakgrunnen for dette valget var særdeles dårlige erfaringer med den PKI-løsningen (og TTP-tjenesten fra ekstern leverandør) vi tidligere benyttet.

PKI-løsninger er imidlertid for øyeblikket den beste løsningen for sikker dokumentutveksling og mindre pilotprosjekter med fokus på interoperabilitet mellom TTP'er bør etableres. Som tidligere hevdet bør imidlertid ikke dette være en del av en nasjonal strategi for informasjonssikkerhet da man lett kan komme i en situasjon hvor PKI av ukyndige feilaktig oppfattes som en "silver bullet" som løser alle

sikkerhetsproblemer. Man bør heller overlate til store brukergrupper og private aktører å etablere slike pilotprosjekter.

Manglende interoperabilitet er en utfordring man ikke bare støter på for PKI-løsninger men også for andre teknologiske og organisatoriske sikkerhets-løsninger. På teknologi-området er det manglende samvirke mellom systemer fra forskjellige leverandører som er hovedproblemet. Dette støter man f.eks. på når man forsøker å opprette kommunikasjon mot en annen virksomhet via VPN. På det organisatoriske området er det differanser i sikkerhetspolicy'er som er hovedproblemet. Hvis man f.eks. gir andre virksomheter store tilganger til egne ressurser via VPN vil man ønske at de andre virksomhetene har et sikkerhetsnivå som svarer til ens eget nivå. På det siste problemet vil f.eks. sertifisering i ht. ISO 17799 bidra til den nødvendige tillit mellom virksomhetene.

Andre utfordringer som burde være nevnt er:

Koordinering av sikkerhetskrav og andre standarder

Det synes å være manglende koordinering mellom de sikkerhetskrav som stilles av for eksempel NSM og Datatilsynet i forhold til andre typer nasjonal standardisering som for eksempel NOARK. Konsekvensen av dette er at leverandører av for eksempel NOARK-systemer ser ut til å ha lite kjennskap til de krav som stilles av overordnede sikkerhetsmyndigheter. Virksomheter som har behov for å benytte slike systemer til behandling av sensitive personopplysninger eller gradert informasjon vil derfor ofte måtte leve med doble løsninger siden sikkerhet må legges på nettverksnivå i stedet for på OS/database/applikasjonsnivå. I forbindelse med nytt arkiv og saksbehandlersystem for departementene er dette særlig aktualisert i forhold til begge de nevnte sikkerhetsmyndigheter.

Tydeliggjøring av sikkerhetskrav fra sikkerhetsmyndigheter og i standard-profiler

Det er svært vanskelig, ressurskrevende og uforutsigbart å planlegge og gjennomføre prosjekter for etablering av spesielt graderte løsninger da de krav som stilles til nå har vært for dårlig dokumentert. Erfaringene fra etableringen av Depnett/B har vært at mye tid har gått med på å definere kravene til løsningen i samarbeide med NSM. Samarbeidet har imidlertid gått bra og vi har inntrykk av at det fra NSM sin side har blitt satt av store ressurser til dette prosjektet.

Dette problemet har imidlertid vært tydelig når det gjelder tidligere FO/S i hvert fall de siste 10 år og det synes fortsatt å være et problem i forhold til Datatilsynet.

Generelt bør det fra disse myndigheters side legges stor vekt på å utvikle standard-profiler for sikring av systemer som gjør sikring av IT-systemer til en mer forutsigbar prosess. Kravene fra de ulike sikkerhetsmyndigheter og standardiseringsorganer bør så langt som overhodet mulig koordineres slik at det for virksomheter med et operativt ansvar blir mulig å etterleve kravene.

4. Foreslåtte strategier og tiltak i kap. 5-8

1.1 Ansvar for, og koordinering av, IT-sikkerhet

I kapittel 5.3 foreslås en fordeling av ansvar for IT-sikkerhet hvor også forvaltningstjenesten tildeles en rolle når det gjelder å definere krav og implementere disse for sentraladministrasjonen. Dette er i stor grad en rolle vi allerede har i dag. Det må imidlertid presiseres at departementene selv har det fulle og hele ansvar for sikkerheten i egne systemer og sikringen av egen informasjon.

Forvaltningstjenesten kan utelukkende ta ansvar for å definere og implementere sikkerhetskrav felles-tjenestene vi ellers har ansvar for. Dette omfatter bl.a. de sentrale deler av Depnett med tilhørende tjenester. I den forbindelse vil Ft også kunne stille krav til sikkerhet i departementene før en fellestjeneste kan tas i bruk. Et eksempel på dette er Depnett/B (gradert stamnett for departementene) hvor det stilles krav til at departementene skal ha en løsning godkjent av NSM før de tillates å knytte seg til nettet.

Departementenes egne lokalnett og sikkerheten i disse er departementenes ansvar. I de tilfellene hvor Ft drifter systemer for departementene for behandling av beskyttelsesverdig informasjon er det departementenes ansvar å definere sikkerhetsmessige krav mens det som oftest vil være Ft's ansvar å implementere kravene.

Forslaget om etablering av et *koordineringsråd for IT-sikkerhet* synes fornuftig. Det er imidlertid behov for koordinering også mot myndigheter, tilsyn og standardiseringsorganer som pr. i dag ikke har noe sikkerhetsansvar, men hvor man kan risikere at systemer som utvikles for å samsvare med en gitt standard ikke legges til rette for også å tilfredsstille sikkerhetsmessige krav. Som et minimum bør det der hvor det er relevant gis kryssreferanser også til IT-sikkerhetsrelaterte lover, forskrifter og standarder, på samme måte som det ofte henvises til NOSIP som et grunnlagsdokument som systemer forutsettes å tilfredsstille (se for eksempel NOARK).

1.2 Kapittel 6, 7 og 8

> "Forslag til strategier og tiltak for å sikre kritiske infrastrukturer og informasjonssystemer"
>
> "Forslag til strategier og tiltak for å styrke sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk kommunikasjon"
>
> "Forslag vedrørende en samfunnsinfrastruktur for elektroniske signaturer, autentisering og sikker overføring av sensitiv informasjon"

I disse kapitlene er det beskrevet mange gode intensjoner men med noen unntak er det for lite konkretisert hvordan disse intensjonene skal oppfylles. Et eksempel på dette er kapittel 6.1.2, punkt 1:

> "Fokus på IT-sikkerhet bør økes hos de aktørene som tilbyr tjenester innen Internett. Aktørene må synliggjøre hvilken grad av tilgjengelighet, kapasitet og driftsstabilitet som kan forventes, samt hvilken brukerhjelp som kan ytes ved feilsituasjoner. Eksempler på tilbud som bør gis, kan være virusskanning, filtrering av "spam" e-post, sikker ADSL og lignende."

Dette avsnittet sier utelukkende noe om hva man ønsker fra disse aktørene, ikke noe om hvordan man skal få aktørene til å oppfylle disse ønskene. Strategien blir dermed svært lite operasjonell.

Intensjonene som sådan inneholder imidlertid mye bra. Det bør dog sørges for at også de utfordringene som er beskrevet over er dekket av adekvate tiltak (se dette punkt 3).

5. Andre forslag som kan bidra til slagkraft og oversiktlighet på området

Grunnlagsdokumentet kan med fordel kortes noe ned ved at man unngår lettere omformulerte gjentagelser av de samme poenger. Dette vil øke lesbarheten (se f.eks. Kap. 1.3).

Generelt gis det mye plass til elektroniske signaturer som løsning på forskjellige sikkerhetsmessige utfordringer. Dette gjør grunnlagsmaterialet skjevt i forhold til det som oppfattes som de viktigste målene med strategien, nemlig en helhetlig nasjonal tilnærming til informasjonssikkerhet, og redusert sårbarhet.

Med hilsen

Erik Logstein
fung. avdelingsdirektør

Else Spilling
førstekonsulent