Dr. Tage Stabell-Kulø
Casa dei Norvegesi
56010 Castelmaggiore
Italia

Pisa, 22. november 2002

Nærings- og Handelsdepartementet
Postboks 8014 Dep
0030 Oslo
Norvegia

Deres ref.: 2001/5605 KDB

Hørinsuttalelse til "Grunnlagsdokument for Nasjonal strategi for informasjonssikkerhet"

På engelsk kan man skille mellom "safety" og "security". Det første begrepet er inneholdt i det mer generelle siste. Begrepet "safety" tilsvarer det norske ordet "sikkerhet" slik vi bruker det i "sikkerhetsbelte" og "sikkerhetsventil". På norsk, derimot, har vi ikke noen god måte å opprettholde dette skillet, og vi er tvunget til å benytte det generelle ordet "sikkerhet" til begge. Derfor er det i Grunnlagsdokument (GD) behov for en begrepsavklaring, og den finnes i innledningen. Fra diskusjonen og begrepene som defineres er det åpenbart at GD er fokusert på "safety", herunder pålitelighet.

GD gir en god og dekkende gjenomgang av situasjonen i Norge, og problematiserer en rekke felter av interesse. Man er opptatt av hvordan vi kan sikre den infrastrukturen samfunnet nå har blitt avhengig av mot alle mulig former for angrep. Generellt er forslagene som fremkommer fornuftige, og de er innen rekkevidde. Dette siste poenget er svært viktig.

Basert på egen teknologisk forståelse er jeg overbevist om at i det store og hele så eksisterer den teknologien som er nødvendig for å oppnå de mål som er ønskelig Det betyr at GD i essens handler om hvordan samfunnet skal legge forholdene til rette for "opplysning" av sammfunnet om disse spørsmålene; håpet er at forståelse av problemene fører til at de riktige valgene tas av aktørene. Fokus på forskning og undervisning, med opprettelsen av et eget program innen sikkerhet, er derfor både riktig og viktig.

Imidlertid er et sentralt tema innen "sikkerhet", nemlig *privathet*, ikke på noen måte uførlig behandlet. Eftersom fokus er på infrastruktur, drift av denne og koordinering av informasjon og aksjoner for å sikre infrastrukturen burde man kunne vente at følgende problemstilling ville bli utførlig diskutert:

> Hvordan sikre brukernes *privathet*, samtidig som man sikrer samfunnets interesser knyttet til pålitelig og "sikker" drift av infrastrukturen.

I møte med en (eiermessig) liberalisert infrastruktur, er det efter min mening en av samfunnets viktigste oppgaver å sikre borgernes privathet. Det vil jo nesten alltid være slik at manøvreringsrom for løsninger på samfunnets problemer i større eller mindre grad må skapes på bekostning av den enkelts (følelse av) press mot den private sfære. Dette er en viktig premiss jeg synes ikke på noen måte er tilfedstillende diskutert.

Denne grunnleggende mangel kommer for eksempel til syne i Kapittel 1.5, definisjonen av Konfidensialitet, hvor det konsekvent omtales som «følsom eller gradert informasjon» og helt utelater betraktninger om det private, og beskyttelse av den private sfære som et poeng med betydelig egenverdi.

Videre har det sneket seg inn i GD poeng som ikke har noe med sikkerhet i betydningen pålitelighet å gjøre. Faktisk, ved sin blotte eksistens setter noen av disse privatheten under sterkt press. Dette er svært beklagelig eftersom diskusjonen om viktigheten av det private sett i relasjon til "nasjonale behov" ikke er tatt med i sin fulle bredde. Det gis derfor et feilaktig inntrykk av at forslagene er uproblematiske.

Dette gjelder i særdeleshet følgende deler:

1. I Kapittel 6.2.1 «Krav til leverandører» er «filtrering av "spam" epost» brukt som eksempel. Denne typen filtrering er i utgangspunktet meget tvilsom, og benyttes vanligvis av leverandører, og kamufleres som en tjeneste, uten at brukere har anledning til å reservere seg. Årsaken til at dette er kontroversiellt er at det legger press på leverandøren om å vurdere *innholdet* i andres epost.
   Denne typen filtrering er et svar fra leverandører av båndbredde (ISPer) på et problem som ligger utenfor deres rekkevidde, nemlig dårlig designet, dårlig realisert, og dårlig konfigurert programvare hos brukeren.
   Dette er et komplisert diskusjon med både tekniske og etiske elementer, og det berører betente felter som hvorvidt produsenter av programvare bør være ansvarlig for feil i programvaren (slik produsenter av biler kostnadsfritt må tilbakekalle sine produkter for feilretting). Det skal ikke stikkes under en stol at leverandører med tilnærmet monopol på enkelt kategorier av programvare sterkt motsetter seg å skulle ta reellt ansvar for sine produkter, og derfor bidrar til å legitimere en slik filtrering av andres epost.
   Legg her merke til at ISPene i dag, under dekke av "sikkerhet", har presset seg til retten å inspisere all epost efter egen forgodtbefinnende. Jeg mener det er et klart overtramp, og at innsatsen heller burde vært mot den ansvarlige: Leverandører av programvare.
   Eftersom GD handler om pålitelighet bør ikke et slikt følsomt eksempel anvendes. Faktisk mener jeg at GD isteden burde diskutere den motsatte problemstilling, nemlig hvordan man sikrer at tiltak i "beste mening" og i "sikkerhetens navn" ikke trenger seg inn borgernes private sfære. Eventuellt, om slike inngrep er helt nødvendig, hvordan man sikrer demokratisk kontroll med dem.
2. I Kapittel 7.1.6 «Tilpassing av regelverk» finner vi en svært uheldige formulering. Det refereres til «Datakrimutvalget», til «Metodeutvalget» og til «et tredje utvalg er oppnevnt for å gjennomgå gjeldende regler om forbrytelser mot statens sikkerhet. . .». Dette brukes så i en glidende overgang til å hevde at «For å lette politiets arbeid med å avdekking og straffeforfølging av datakriminalitet må det arbeides videre for. . ..»
   Igjen unnlater man å problematisere hvilke implikasjoner dette vil ha for privatheten. Alltid når man diskuterer politiets midler snakker man indirekte om en tilsvarende innskrenkning av rettigheter, hvor retten til et omfattende privatliv er demokratiets grunnmur. Dette er (også) en meget omfattende diskusjon som ikke bør behandes såvidt lempfeldig.
   Man kan gjerne ha sympati for politiets ønske om å kunne skaffe seg tilgang til massive mengder informasjon om den mistenkte for å kunne oppklare for brytelser. Dette må dog veies opp mot det grunnleggende prinsipp at den jevne borger ikke skal underkastes

overvåkning uten grunn. Retten til privathet i alle sine lovlige aktiviteter er helt grunnleggende i vårt samfunn, og at det er viktig å holde datanettene i drift er på ingen måte grunn god nok til å trenge inn i den private sfære til alle og enhver.

3. Hele Kapittel 8 handler om PKI. En samfunnsinfrastruktur for elektroniske signaturer vil gi mulighet for nye tjenester, skape verdier, forenkle grensesnittet til offentlig forvaltning, og så videre. Men efter mine mening bør ikke en diskusjon om PKI inngå i GD. Årsaken er at hensikten med dokumentet er en strategi for å oppnå økt pålitelighet i infrastrukturen. Tiltak for økt bruk av den, og tilhørende nye tjenester, vil forstyrre argumentasjonen. Et viktig poeng i denne sammenhengen er nemlig at det finnes mange og vektige argumenter *mot* opprettelsen av en nasjonal PKI. Men på samme måte som dette ligger utenfor diskusjonen her, ligger det utenfor fokus i GD.

GD har som implisitt, og korrekt, utgangspunkt at infrastrukturen for kommunikasjon nå har blitt så viktig for oss alle at det ikke lenger kan overlates til de enkelte aktører å drive den videre uten en viss kontroll og styring fra samfunnets side. Det er helt avgjørende at samfunnets behov defineres og det skapes mekanismer som sikrer at disse behovene møtes. Men, som sagt, ett av samfunnets viktigste behov er å sikre retten for den enkeltes privatliv , og i dette kommer GD til kort.

Vennlig hilsen

Tage Stabell-Kulø
Amanuensis
Institutt for Informatikk
Universitetet i Tromsø