FNH Finansnæringens Hovedorganisasjon
Finansnæringens Servicekontor

SPAREBANK FORENINGEN

Det Kongelige Nærings- og Handelsdepartement
Postboks 8014 Dep
0030 Oslo

Deres ref.	Deres brev	Vår ref.	Dato
2001/5605 KDB	21.10.2002	2002/000471 FNH 200200148 Sparebankforeningen	25.11.2002

HØRINGSSVAR – GRUNNLAGSDOKUMENT FOR UTARBEIDELSE AV NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET

Det vises til Deres brev av 21.10.02 hvor blant annet BankID, Bankenes Standardiseringskontor, Finansnæringens Hovedorganisasjon og Sparebankforeningen er bedt om å gi tilbakemelding på Grunnlagsdokument for Nasjonal strategi for informasjonssikkerhet, datert 21. oktober 2002.

De fire ovennevnte høringsinstanser har valgt å avgi en felles uttalelse.

Innledning.

Vi stiller oss positive til initiativet om utarbeidelse av en nasjonal strategi for sikker utvikling og bruk av IT og er enige i de tre overordnete mål for strategien:

a. Samfunnskritisk infrastruktur for elektronisk informasjonsutvikling skal være robust og sikker i forhold til de trusler den utsettes for og at kritiske informasjonssystemer skal være sikret slik at skadevirkningene ved sikkerhetsbrudd ikke er større enn hva som kan defineres som akseptabel risiko.
b. Det skal bygges en sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk informasjonsutveksling i Norge. IT-sikkerhet skal være en sentral faktor ved forbrukernes og norske virksomheters bruk av IT.
c. Norge skal ha en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering av kommunikasjonspartnere samt sikker overføring av sensitiv informasjon.

Vi mener at disse tre overordnete mål gir en god bærebjelke for et en Nasjonal strategi for informasjonssikkerhet.

Postboks 2473 Solli
0202 Oslo
Tlf.: 23 28 42 00
Fax.: 23 28 42 01
Org. 969 000 938

Postboks 6772 St. Olavs plass
0130 Oslo
Tlf.: 22 11 00 75
Fax.: 22 36 25 33
Org.: 971 526 610

Kommentarer.

I punkt 1.5 (side 10) er det definert en del sentrale ord og begreper innen IT-sikkerhet og risikostyring. I forhold til hva som følger senere av dokumentet, ber vi om at det vurderes å ta inn flere sentrale ord og begreper. Eksempler på dette er "cyber crime", "cyber terrorism", og "hacking". Ordet "tillit" er et sentralt begrep når det gjelder sikkerhetsspørsmål, og vi mener at dokumentet burde gi en omtale av eller redegjørelse for dette.

I punkt 3.2.4 Konvergens, siste avsnitt (side 18) står det: " Risikoen forbundet med å kontrollere konvertering fra analog til digital teknologi vil være betydelige." Slik det står er dette en påstand som bør forklares nærmere eller bør gis en bredere omtale.

I punkt 3.2.7 Bortsetting av tjenester, siste avsnitt (side 19) står det: "Siden forretningsutvikling i dag i stor grad involverer IT, viser trenden at det igjen er et behov for å styrke intern IT-kompetanse i virksomhetene. Dette kan igjen også medføre at virksomheten ikke ønsker å gi fra seg kontroll med spesielle tjenester, som IT-sikkerhet."
Vi er enige i at bortsetting av tjenester kan medføre kompetansesvikt i virksomhetene, men vi mener samtidig at det bør fremheves at det også normalt medfører profesjonalisering ved en del prosesser, eksempelvis endringsprosesser. Vi savner en bredere omtale av problemstillinger omkring bortsetting av tjenester: hvem som har det overordnete ansvar ved bortsetting av tjenester, hvilke aktiviteter som må iverksettes ved bortsetting av tjenester mv. Slik omtale ville naturlig hørt hjemme under punkt 6.2 Virksomhetsnivå.

I punkt 4 Nye utfordringer for IT-sikkerhet nederst på side 22 er det en ramme hvor følgende står: "Det ber et mål for å øke robustheten i IT-infrastruktur til et nivå slik at risikoen for avbrudd i en normalsituasjon er akseptabel for viktige samfunnsfunksjoner. I en krisesituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner." I denne forbindelse mener vi at det også bør angis at det innen en viss tid skal skje en gjenopprettelse til normalsituasjon ved avbruddssituasjoner.

I punkt 4.1 Generelle utfordringer for IT-sikkerhetsarbeidet, nest siste avsnitt på side 23, står det i siste setning: "I arbeidet med samfunnssikkerhet følges også et likhetsprinsipp, kriseorganisasjonen skal være mest mulig lik ordnær organisasjon og et nærhetsprinsipp, kriser skal handteres på lavest mulig nivå i forvaltningen." Dette er et utsagn som kan være egnet til misforståelse. Vi antar at man mener at kriser skal håndteres på et forsvarlig nivå, men ikke høyere enn nødvendig.

I punkt 5.1.3 Samarbeidsarenaer (side 35) er det nevnt en rekke instanser. Vi savner omtale av Bankenes Standardiseringskontor som forvalter standarder og setter sikkerhetskrav innen transaksjonsutveksling mellom bankene.

I punkt 5.1.4 på side 36 under "Tilsynsrolle" mener vi at "Kredittilsynet" også bør nevnes.

Øverst på side 39 er det et diagram. Vi er av den oppfatning av at "Intern rutinesvikt" i gitte situasjoner kan medføre et relativt høyt skadepotensiale på nasjonalt plan.

Under pkt. 5.2.2 Samfunnskritisk IT-infrastruktur og – IT-systemer (side 41) er det listet opp en rekke samfunnskritiske IT-infrastrukturer. Strekpunkt nr. 2 mener vi bør lyde slik: "IT-systemer som støtter avregning av nasjonale og internasjonale finansielle transaksjoner mellom finansinstitusjoner. Vi savner i listen over samfunnskritisk IT-infrastruktur både nsjonale og internasjonale systemer for betalingstjenester, jfr. Lov om betalingstjenester.

Under oversikten i punkt 5.3.1 (side 42) mener vi at Kredittilsynet også burde vært nevnt i linje 2.

Under punkt 5.3.2 Samordnet koordinering av IT-sikkerhet på side 44, tredje siste avsnitt finner vi det naturlig at Bankenes Standardiseringskontor bør delta i det permanente koordineringsråd for IT-sikkerhet som representant fra andre aktører. Dette begrunnes ut fra banknæringens samfunnsnasjonale betydning.

Under punkt 6.2 Virksomhetsnivå (side 53 flg.) bør også nevnes beredskapsarbeide i form av etablering av rutiner dersom først krisen skulle inntre, for eksempel varslingsrutiner internt og eksternt, rutiner for nøddrift osv.

Når det gjelder punkt 8 Forslag vedrørende en samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring av sensitiv informasjon vises det til synspunktene i vårt brev av 13. september 2002 til Nærings- og Handelsdepartementet vedrørende Strategi for bruk av elektronisk signatur og elektronisk ID i Norge – Høring.

Med vennlig hilsen

for Finansnæringens Hovedorganisasjon
Trond Bakkerud

for Sparebankforeningen i Norge
Gunnar Harstad

Bankenes Standardiseringskontor
Knut Kvalheim

BankID Samarbeidet
Grete Sørensen