KREDITTILSYNET
The Banking, Insurance and Securities Commission of Norway

Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 Oslo

Att.: Katarina de Brisis

Saksbehandler: Per Steinar Davidsen | Dir.linje: 22 93 98 77

Vår ref.:	Arkivnr.:	Deres ref.:	Dato:
2002/09072-1	008	2001/5605 KDB	29.11.2002

HØRINGSUTTALELSE

GRUNNLAGSDOKUMENT FOR UTARBEIDELSE AV NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET

Generelt

Generelt sett er grunnlagsdokumentet i samsvar med Kredittilsynets syn på området.

Gjennom tilsyn med finansinstitusjonene har Kredittilsynet observert at den operasjonelle risiko i institusjonene har økt vesentlig de siste årene. Det er blitt mer krevende å administrere, utvikle, drifte, vedlikeholde og sikre IT-systemer og IT-tjenester. Feil som oppstår i felles IT-infrastruktur er kritiske og kan lamme store deler av en bransje i lengre perioder. Et annet forhold er at finansforetakene samarbeider mer for å bedre konkurranseevne og lønnsomhet. Interaksjon mellom de ulike foretakene er blitt større og det er mer krevende å ha oversikt og kontroll.

Vi har forstått at styringsgruppen i prosjektet ønsker å få tilbakemelding innenfor områdene nedenfor:

Mål og innretning av strategiarbeidet:

- Strategiarbeidet er dynamisk og må tilpasses underveis.
- Privat sektor må bli pålagt større deltagelse i IT-sikkerhetsarbeidet innenfor de områder som har stor betydning for samfunnet.

Identifisere utviklingstrender av betydning for nasjonalt arbeid med IT-sikkerhet:

- En dynamisk strategi vil fange opp utviklingstrender.

Identifisere utfordringer for IT-sikkerhet:

Postadresse: Postboks 100 Bryn 0611 OSLO
Besøksadresse: Østensjøveien 43 0667 OSLO
Telefon: 22 93 98 00
Telefax: 22 63 02 26
Org.nr: 840747 972
E-post: post@kredittilsynet.no
URL: www.kredittilsynet.no

- Det permanente koordineringsrådet for IT-sikkerhet eller eventuelle tilsynsorganer, må påse at det innenfor de enkelte sektorer blir gjennomført regelmessige/løpende vurderinger av IT-risiko og IT-sårbarhet. Spesielt gjelder dette for fellessystemer i IT-infrastrukturen hvor svikt kan påvirke flere foretak. Kvaliteten på IT-sikkerhetsarbeidet er avhengig av kvaliteten på risikoanalysene. Spesielt er det viktig at risikovurderinger blir utført før ny teknologi tas i bruk. En eventuell sentralt opprettet instans bør ha ansvar for å sikre at alle områder er dekket i risikovurderingene og videre påse at det er etablert eiere av de enkelte deler av infrastrukturen med tilhørende risiko. Fagområdene innenfor det offentlige og det private næringslivet må selv ta stilling til og ha oversikt over kritiske systemer/enheter innenfor sitt område.
- Det bør vurderes om de som har kritiske funksjoner for samfunnet bør reguleres og føres tilsyn med. Kredittilsynets IKT-forskrift er et eksempel på hvilke krav som kan stilles til systemer som defineres som IT-systemer med kritiske funksjoner..
- Sikkerhet koster og det kan skje at en aktør ikke er villig til å ta alle kostnadene ved et tiltak eller en sikkerhetsfunksjon når det også kommer andre brukere til gode. Det samme gjelder når krav til sikkerhet er høyere enn det en selv trenger.

Foreslåtte strategier og tiltak, ref. til kap. 5-8:

- Kredittilsynet støtter styringsgruppens forslag om at det opprettes et permanent IT-koordineringsråd for IT-sikkerhet med representanter fra det offentlige og det private næringsliv. Antallet representanter bør ikke være for mange, men må være tilstrekkelig for å dekke de sektorer eller enheter som har betydning for den nasjonale informasjonssikkerheten. Representantene kan ha interessegrupper bak seg. De ordninger vi har i dag for å ivareta IT-sikkerhet innenfor de enkelte sektorer bør beholdes, men koordineres på et samordnet nivå.
- Kredittilsynet mener at det er viktig at man innfører bruken av elektronisk signatur. Denne teknologien vil bli en sentral funksjon i fremtidige elektroniske sikkerhetsløsninger. Av denne grunn bør det, slik høringsdokumentet foreslår, oppfordres til et samarbeid om etablering av en felles infrastruktur for elektronisk identifisering og elektronisk signatur. Det kan tenkes at det tas i bruk ulike løsninger for ulike deler av næringslivet, men offentlig sektor bør satse på en felles løsning.

Andre forslag som kan bidra til slagkraft og oversiktlighet på området:

- Alle aktører som utsteder nøkler og utfører sertifikat- og nøkkeladministrasjon for kvalifiserte elektroniske signaturer og identifikasjon, må ha konsesjon og underordnes offentlig tilsyn. Kredittilsynet mener det bør vurderes grundig om at det er tilstrekkelig at en slik kritisk samfunnsmessig sikkerhetsfunksjon skal være selvregulerende.

Med hilsen

Anne Merethe Bellamy, e.f.
Avdelingsdirektør

Frank Robert Berg
Spesialrådgiver

Kopi: Finansdepartementet