Norsk Regnesentral
Norwegian Computing Center

NR

Høringsuttalelse fra Norsk Regnesentral

Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 Oslo

Deres ref.	Vår ref.	Dato
2001/5605 KDB		22.11.2002

Adresse - Address:
Postboks 114 Blindern,
N-0314 Oslo, Norway

Kontoradresse - *Office Address:*
Gaustadalléen 23,
N-0371 Oslo

Telefon - *Telephone:*
+47 22 85 25 00

Telefax - *Telefax:*
+47 22 69 76 60

Bankkonto - *Bank account:*
8200.01.48888

Foretaksnummer *Enterprise no.:*
NO 952125001 VAT

Internet
http://www.nr.no/
nr@nr.no

Grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

Grunnlagsdokument for nasjonal strategi for informasjonssikkerhet er et solid stykke arbeid som gir en omfattende helhetlig beskrivelse av dagens situasjon når det gjelder informasjonssikkerhet, samt de utfordringer man står overfor i tida framover. Behovet for, og kravene til, informasjonssikkerhet er stadig økende, og Norsk Regnesentral (NR) vil spesielt understreke viktigheten av arbeidet med å gjøre sikkerhet til en integrert del av systemer og arbeidsprosesser både i offentlige og private virksomheter.

Som forskningsinstitutt med en betydelig aktivitet over lang tid innen informasjonssikkerhet, er NR naturlig nok meget positiv til det foreslåtte forskningsprogrammet innen informasjonssikkerhet. NR mener at langsiktige satsinger har stor betydning hvis man ønsker å videreutvikle eksisterende kompetansemiljøer. Konkurranse om prosjektmidler for å oppnå kvalitetssikring av forskningen er sunt, men må ikke kreve for stor andel av forskningsmiljøenes tid og ressurser. Forutsigbarhet i forhold til finansiering av forskningsinnsats er meget viktig for å sikre tilstrekkelig fokus og dybde. Det kreves en god balanse mellom sunn konkurranse og forutsigbarhet for å skape gode forskningsmiljøer.

Norge har ingen industri av betydning innen informasjonssikkerhet. Et unntak er noen få produsenter av militært utstyr som i liten grad er synlige på det kommersielle markedet. NR mener at en sterk, norsk sikkerhetsindustri ville gitt store, positive ringvirkninger i form av økt kompetansenivå og generelt større sikkerhetsbevissthet. NR foreslår derfor at man i arbeidet med den nasjonale strategien vurderer økte incentiver for oppbygging av slik industri. Instituttsektoren kan bidra i en slik oppbygging ved å utføre anvendt forskning som leder til kommersialisering av resultater. Forskningsinstituttene har en viktig rolle som bindeledd mellom grunnforskningen på universitetene og private og offentlige virksomheter som kan dra nytte av resultatene. Grunnforskningen er meget viktig, men uten den anvendte forskningen og kommersialiseringen får man ikke høstet gevinstene.

NRs største ankepunkt mot grunnlagsdokumentet er mangelen på tiltak som øker incentivene for både offentlige og private virksomheter til å gjennomføre tilstrekkelige sikkerhetstiltak og etterstrebe den sikkerhetskultur man ønsker å oppnå. Private virksomheter har naturlig nok sterkest fokus på å skaffe inntekter, og offentlige virksomheter får stadig sterkere krav om

innsparinger. Målet med sikkerhetstiltak er i de fleste tilfeller å unngå mulige fremtidige tap, og vil lett bli en salderingspost, noe man skyver foran seg, i en presset økonomisk situasjon. Det er anbefalt mange tiltak virksomheter bør iverksette, og de fleste av disse vil det koste en del å gjennomføre, men det foreslås få tiltak som vil anspore virksomhetene til å ta ekstrakostnader som ikke er påkrevd. Strengere lovregulering er én mulighet, men i de aller fleste tilfeller fungerer gulroten bedre enn pisken, i hvert fall når holdningsendringer er en viktig del av det man vil oppnå.

NR mener videre at organisasjonsperspektivet er for dårlig dekket i grunnlagsdokumentet, og er usikker på om høringslisten i tilstrekkelig grad har med instanser med kompetanse innen organisasjon og organisasjonsteorier. Dette perspektivet er spesielt viktig når et av hovedmålene i den foreslåtte strategien er å styrke sikkerhetskulturen. NRs erfaring er at sikkerhetskulturen i en virksomhet er en funksjon av organisasjonskulturen.

I grunnlagsdokumentet anbefales det bruk av internasjonale standarder, men NR er av den oppfatning at ISO 17799 og tilsvarende standarder er dårlig egnet for norske små og mellomstore virksomheter som blant annet ikke har ressurser til den omfattende sikkerhetsorganisasjonen slike standarder legger opp til. NR mottar signaler fra mange hold som tilsier at det er et sterkt behov for standarder og retningslinjer for sikkerhetsorganisasjon som passer bedre til typiske norske virksomheter, og anbefaler derfor at det gjøres en forskningsinnsats på dette området.

Når det gjelder PKI, elektronisk ID og elektroniske signaturer, har utviklingen gått mye tregere enn forventet. Det skyldes, slik NR ser det, i stor grad at alle sitter på gjerdet og venter på at "kritisk masse" (av brukere og/eller tjenester) skal oppstå. At private aktører vegrer seg for å ta kostnadene ved å være først ute er forståelig, men myndighetene har vært overraskende passive. De offentlige instanser vil kunne høste en meget stor effektiviseringsgevinst ved utstrakt innføring av elektronisk kommunikasjon, og når i tillegg ut til store deler av befolkningen som ikke er så raskt ute med å ta i bruk ny teknologi. Offentlige virksomheter bør derfor pålegges et større ansvar for å ta i bruk mulighetene som teknologien tilbyr på dette området.

Et av de store problemene i forbindelse med PKI og elektronisk signatur er mangelen på sikre signaturfremstillingssystemer. Myndighetene har formulert nokså detaljerte krav til selve sertifikatproduksjonen og nødvendig infrastruktur, men har kommet med få krav til teknologiske løsninger for fremstilling av digitale signaturer. Sikring av at "det du ser er det du signerer" er et meget vanskelig problem som fortjener adskillig mer oppmerksomhet (se kap. 8.2, punkt 11 i grunnlagsdokumentet).

Personvern er et annet sikkerhetsaspekt som bare er overfladisk dekket i grunnlagsdokumentet. Vi har en personopplysningslov som understreker individets rettigheter i forhold til kontroll med lagrede personopplysninger, og som har sitt motstykke i tilsvarende EU-direktiv. Disse rettighetene er ofte til hinder for effektiv beskyttelse av både samfunnet som helhet og enkeltindivider mot kriminelle og terrorister, og vil lett skyves til side i tider hvor terrortrusselen oppleves som stor. NR mener at en nasjonal strategi for informasjonssikring bør understreke viktigheten av å opprettholde et sterkt personvern, spesielt i forbindelse med fremtidige endringer i regelverk, nye politimetoder og internasjonalt samarbeid om bekjempelse av datakriminalitet.

I kapittel 3.2.1 i grunnlagsdokumentet er det tatt med en kommentar om sikkerhet av nettbanker. Det nevnes at antall oppdagede sikkerhetshendelser i forbindelse med bruk av nettbank er ubetydelig, men det er ikke gjort noe forsøk på å forklare hvorfor det er slik. Mange synes å oppfatte bruk av nettbank som noe av det mest sikkerhetskritiske man gjør på

Adresse - *Address:*
Postboks 114 Blindern,
N-0314 Oslo, Norway

Kontoradresse - *Office Address:*
Gaustadalléen 23,
N-0371 Oslo

Telefon - *Telephone:*
+47 22 85 25 00

Telefax - *Telefax:*
+47 22 69 76 60

Bankkonto - *Bank account:*
8200.01 48888

Foretaksnummer *Enterprise no.:*
NO 952125001 VAT

Internet
http://www.nr.no/
nr@nr.no

internett fordi det direkte involverer penger. En naturlig konsekvens av en slik oppfatning er at man mener at det som er sikkert nok for nettbank også må være sikkert nok for de fleste andre anvendelser. NRs erfaring er derimot at nettbank ikke kan sammenlignes med andre internettapplikasjoner. Det spesielle med nettbank er bankenes ekstremt gode kontroll med alle transaksjoner som foregår i de bakenforliggende systemene. Penger ut av én konto er alltid koblet til penger inn på en annen konto. Alt logges med tidsstempel, rimelighetskontroller utføres automatisk, og mistanke om uregelmessigheter fører til umiddelbar sperring av konto. Å lykkes med svindel mot nettbank uten å bli oppdaget er derfor svært vanskelig. Det er få andre anvendelser av internett (kjøp og salg, offentlig innrapportering, avtaleinngåelser, informasjonsutveksling osv.) som har mulighet til å oppnå tilnærmelsesvis like god kontroll som nettbankene har, samtidig som potensialet for tap av penger og andre skadevirkninger kan være minst like stort. Sikkerhetskravene til andre applikasjoner vil derfor i mange tilfeller være adskillig større enn hva som anses tilstrekkelig for nettbank.

Sikring av informasjon blir i stadig større grad avhengig av teknologiske løsninger. Dårlig designet programvare er opphav til mange sårbarheter som utgjør en trussel mot både individer, virksomheter og staten. Mulighet for inngående analyse av systemer er viktig for å sikre at de tilfredsstiller kravene man har til informasjonssikkerhet. NR mener derfor at en nasjonal strategi for informasjonssikring bør fremme bruken av åpne, internasjonale standarder for sikkerhetssystemer og andre programvareløsninger, fremfor proprietære løsninger.

Avslutningsvis vil Norsk Regnesentral understreke at en god nasjonal strategi for informasjonssikring er svært viktig å få på plass, og at det er viktig å dra nytte av eksisterende kompetansemiljøer i arbeidet med å sette strategiens intensjoner ut i livet.

Med vennlig hilsen

Norsk Regnesentral

Ragni Ryvold Arnesen
Forsker

E-post: Ragni.Ryvold.Arnesen@nr.no

Adresse - *Address:*
Postboks 114 Blindern,
N-0314 Oslo, Norway

Kontoradresse - *Office Address:*
Gaustadalléen 23,
N-0371 Oslo

Telefon - *Telephone:*
+47 22 85 25 00

Telefax - *Telefax:*
+47 22 69 76 60

Bankkonto - *Bank account:*
8200.01.48888

Foretaksnummer *Enterprise no.:*
NO 952125001 VAT

Internet
http://www.nr.no/
nr@nr.no