NORMAN

Deres ref.:	*Vår ref.:*	*Dato:*
2001/5605 KDB	POF/2002	2002.11.22

Nærings- og Handelsdepartementet
Postboks 8014 Dep
0030 OSLO

Høring – grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

Vi viser til departementets høringsdokument mottatt 23. oktober.

Norman er generelt meget positivt innstilt til det inititativ som er tatt fra de berørte departement om utarbeidelse av en nasjonal strategi for informasjonssikkerhet. Vi er videre av den oppfatning at det utsendte høringsdokumentet er et gjennomarbeidet og grundig utgangspunkt for en slik stragegi.

Norman har følgende kommentarer til grunnlagsdokumentet:

Generelt om den nasjonale informasjonssikkerhet

I de senere år har vi sett en utvikling av samfunnet som har vært av en karakter hvis dramatiske konsekvenser i forhold til vår måte å organisere alle våre gjøremål og tenkemåter, antagelig best kan sammenlignes med situasjonen under den industrielle revolusjon. Vi er midt oppe i dette paradigmeskiftet, og det er vel ingen grunn til å anta at det neste tiåret vil medføre færre endringer enn det forrige.

Dette medfører spesielt store utfordringer i forhold til alle typer planlegging av den type som omhandles i høringsdokumentet, da utviklingen foregår så raskt. Den eneste mulige strategi i forhold til dette vil være at man om mulig planlegginger i forhold til mer ***generelle overordnede tiltak***, snarere enn konkret detaljplanlegging. Sistnevnte vil uansett etter stor sannsynlighet være utdatert innen det er mulig å implementere tiltakene.

I en situasjon hvor utviklingen skjer så raskt som det vi ser innen IKT-sektoren, er det meget stor fare for at nødvendige og fornuftige sikkerhetstiltak ikke blir oppfylt. Dette kan skyldes flere årsaker – en viss overivrighet etter å ta i bruk den nye teknologien er antagelig en av de mer fremtredende. Et annet forhold er at det er (forholdsvis) lett i ta i bruk denne teknologien, samtidig som det er meget tids- og ressurskrevende å iverksette de tiltak som skal til for å bruke teknologien på en sikker måte.

Et slikt ønske om å nyttigggjøre seg ny teknologi uten at sikkerhet er tilfredsstillende ivaretatt, gjelder både den enkelte virksomhet og person, men ikke minst også leverandører av programvare og utstyr. Disse leverandører er for det meste internasjonale aktører, hvor man har liten mulighet for direkte påvirkning, både som individ/virksomhet og fra nasjonalt nivå fra et land av Norges størrelse. Dette er en situasjon som i seg selv er utfordrende i forhold til hvilken strategi som skal velges for å ivareta det nasjonale sikkerhetsbehov.

Dersom situasjonen er slik som vi har beskrevet over, er det innlysende at samfunnet har pådradd seg en ny sårbarhet med de konsekvenser dette innebærer. Dette gjelder såvel sårbarhet i forhold til målrettede "angrep" mot vitale samfunns- og virksomhetsinteresser, som sårbarhet i forhold til hendelser som måtte inntreffe på grunn av rene uhell.

Norman ASA
NO 835 925 072 MVA

Postal address: P.O. Box 43, N-1324 Lysaker, Norway
Office address: Strandveien 37, Lysaker

Tel.: +47 67 10 97 00 Fax: +47 67 58 99 40
E-mail: norman@norman.no
Web: www.norman.no

En nasjonal strategi for informasjonssikkerhet synes med bakgrunn i dette å være et nødvendig tiltak for å bedre å bli i stand til å ivareta nasjonale interesser i vid forstand.

Et forhold som ikke berøres i det hele tatt i grunnlagsdokumentet – annet enn meget indirekte - er såkalt ***"identity theft"*** – det fenomen at en person mer eller mindre overtar hele eller deler av en annen person. Etter hvert som vår måte å kommunisere på, og identifisere seg ved hjelp av, blir ytterligere basert på elektroniske systemer etc., blir mulighetene for at en person skal kunne utgi seg for en annen – i alle forhold – mye større. Dette vil kunne få dramatiske konsekvenser for den person som "mister" sin identitet, da det bl.a. kan være problematisk å gjenopprette korrekt identitet. Vi har allerede sett de første eksempler på hvilke muligheter/farer som finnes her, men det er grunn til å anta at dette vil bli et betydelig problem allerede på forholdsvis kort sikt. En nasjonal plan for informasjonssikkehet bør ta dette forholdet med i betraktning og søke å sikre det enkelte individs behov for egen identitetssikkerhet.

Konkrete kommentarer til grunnlagsdokumentet

1. Innledning

Ingen kommentarer.

2. Sammendrag

Det foreslås opprettet et permanent koordineringsråd for IT-sikkerhet sammensatt av departementer og tilsynsmyndigheter samt eventuelle andre aktører. Etter Normans syn er det fornuftig at representanter for IT-industrien også er representert i et slikt koordineringsråd. Dette både av hensyn til den verdifulle "input" slike kan komme med, men også i forhold til informasjonsflyten fra drøftinger i koordineringsrådet til industrien selv.

Det pekes på at omfattende svikt i IT-sikkerhet kan få alvorlige konsekvenser for liv, helse og materielle verdier, samt virksomheters konkurranseevne og verdiskapningen i samfunnet. Det er vel grunn til å peke på at ved et koordinert, målrettet angrep fra en nasjon eller en ressurssterk organisasjon, vil selve den nasjonale sikkerhet kunne settes i fare.

Vi viser for øvrig til våre kommentarer under til de enkelte kapitlene til grunnlagsdokumentet.

3. Utviklingstrekk og forhold som påvirker IT-sikkerhet

Som nevnt i vår innledende, generelle kommentarer,er det et problem at leverandørene av applikasjoner ikke ser ut til å ha prioritert sikkerhet så høyt som det som er ønskelig. Man har tradisjonelt "ofret sikkerhet på funksjonalitetens alter". Det synes å være visse tendenser fra aktørene til en bedring av dette forholdet, men det vil antagelig være lenge til sikkerhetsbehovene sett fra samfunnets side vil være tilfredsstillende ivaretatt i de produktene som leveres og de standardinnstillinger som velges.

Grunnlagsdokumentet peker på en del svakheter ved Internett. Norman vil i tillegg peke på den generelle fare som består i et globalt angrep på Internett selv. Dette kan tenkes gjennomført (teoretisk) ved at personer/nasjoner/organisasjoner klarer å spre et ondsinnet program til en betydelig mengde maskiner koblet til Internett og deretter på et gitt tidspunkt setter i gang en aktivitet som blir så stor at Internett ikke klarer den enorme trafikkbelastningen som oppstår – enten ved en mengde DoS-angrep (Denial of Service) eller f.eks. ved masseutsending av email. Et slikt scenario er diskutert i offentlige sikkerhetsfora, og dermed presumptivt også kjent blant dem som måtte ha interesse av å sette i gang et slikt angrep.

Grunnlagsdokumentet peker på at kritisk teleinfrastruktur eies av privat sektor som følge av liberaliseringen av telekommunikasjonssektoren. Det er et tankekors at mens andre deler av samfunnets infrastruktur – vei, jernbane, osv. – kontrolleres/eies av myndighetene, er ikke det

samme tilfellet med den nye infrastrukturen, som også det offentlige er avhengig av for å kunne funksjonere. Dette i seg selv utgjør en sikkerhetsrisiko.

4. Nye utfordringer for IT-sikkerhet

Prosjektgruppen foreslår i grunnlagsdokumentet en endring av Sårbarhetsutvalgets overordnende mål for IT-sikkerhet til:

> *Det er et mål 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.*

Norman er enig i at dette er et mer realisisk og operasjonelt mål enn det mer bastante begrepet "helt usannsynlig" som Sårbarhetsutvalget benytter. Det vil alltid være en avveining mellom de ressurser som settes inn på å unngå en negativ situasjon, og de kostnader en slik situasjon faktisk får dersom den inntreffer. Null-risiko vil i de fleste tilfeller ikke være det mål man bør sette seg.

Vi vil imidlertid antyde at følgende kunne være en ytterligere forbedring av målet for IT-sikkerhet:

> *Det er et mål å øke robustheten i IT-infrastruktur til et nivå slik at risikoen for avbrudd* ***og lengden av et avbrudd*** *i en normalsituasjon er akseptabel for viktige samfunnsfunksjoner. I en krisesituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner.*

Poenget vårt er at et meget kort avbrudd i seg selv neppe vil være kritisk. Det er risikoen for å bli utsatt for et avbrudd av noen lengde i tid som man bør ta sikte på å sikre seg mot.

Det pekes i grunnlagsdokumentet på at den samlede kapasitet innen utdanning og forskning på området IT-sikkerhet er for liten. Norman er enig i dette. Vi savner imidlertid konkrete forslag til tiltak for å bedre på denne situasjonen.

Videre pekes det på at arbeidet med sikkerhet bør innebære at man skaper en ***sikkerhetskultur*** som innebærer en kontinuerlig fokus på sikkerhet. Dette er etter vår mening helt essensielt. Det er viktig å ha klart for seg at IT-sikkerhet ikke er en engangsinnsats som kan gjøres, men en kontinuerlig prosess som har betydelige kostnader både direkte og indirekte.

5. Ansvar for, og koordinering av IT-sikkerhet

I Stortingsmelding 17 (2001-2002) er det lagt opp til opprettelsen av en Nasjonal sikkerhetsmyndighet (NSM) som et direktorat administrativt underlagt Forsvarsdepartementet, med faglig ansvar overfor Forsvarsdepartementet (militær sektor) og Justisdepartementet (sivil sektor). Vi har også det forhold at ansvaret for koordinering av den nasjonale IT-politikken er lagt til Nærings- og handels-departementet.

Det synes for Norman å kunne by på problemer med den foreslåtte administrative forankringen av det foreslåtte direktoratet, og vi anbefaler derfor at man ser på hvorvidt en administrativ forankring av direktoratet til Nærings- og handelsdepartementet ville være en bedre løsning.

Tilsvarende kan det synes som lite optimalt å legge det koordinerende ansvaret for en felles metodikk for identifisering og risiko- og sårbarhetsanalyser etc. til Justisdepartementet, mens koordinering av IT-sikkerhet hva gjelder den daglige oppgaveløsningen, legges til Nærings- og handels-departementet. Det er vanskelig å tenke seg at disse to oppgavene ikke vil medføre noen form for overlapping, med derav følgende suboptimal (dobbel) arbeidsinnsats. Norman anbefaler følgelig at man vurderer hvorvidt det ikke hadde vært mer optimalt om disse to funksjonene ble forankret i samme departement.

Som nevnt i vår kommentar i tilknytning til grunnlagsdokumenets sammendrag, støtter vi opprettelsen av et permanent koordineringsråd for IT-sikkerhet, herunder de tanker man nevner omkring

oppgavene et slikt råd er tenkt å skulle ha. Den administrative forankring til dette rådet må sees i sammenheng med hvordan man fordeler ansvaret for IT-sikkerhet mellom de forskjellige departementene.

6. Forslag til strategier og tiltak for å sikre kritiske infrastrukturer og informasjonssystemer

Norman vil peke på viktigheten av å sørge for gjennomføringen av et opplegg som ivaretar hensynet til nasjonal autonomi i telenettene. Dersom mulighetene for kommunikasjon innad i Norge er avhengig av systemer som ligger utenfor landets grenser, øker dette vår sårbarhet.

Tilsvarende er vi enige i at det arbeides med å øke Internetts robusthet f.eks. ved opprettelse av flere nasjonale tilknytningspunkt til Internett.

Koordinering av internettsikkerhet på et internasjonalt nivå er videre et arbeid som Norge bør støtte/fremme. I større grad enn noe annet kommunikasjonsmedium er Internett globalt, med de fordeler og sikkerhetsrisiki dette innebærer, og tiltak for å bedre sikkerheten ivaretas følgelig best ved internasjonalt samarbeid.

Norman slutter seg til grunnlagsdokumentets forslag om at man bør forsøke å få til økt fokus på sikkerhet hos de aktører som tilbyr forskjellige typer tjenester med tilknytning til Internett og øvrige leverandører av ITK-systemer.

Grunnlagsdokumentet peker på at man i større grad bør ta i bruk "uavhengig revisjon" for å bekrefte at påstått sikkerhet foreligger, f.eks. ved inntrengningstester (punkt 6.2.2). Norman er ikke uenig i dette, men vil imidlertid peke på at dette ***i seg selv*** medfører en sikkerhetsrisiko, da man nødvendigvis vil måtte gi tredjepart innsyn i en virksomhets sikkerhetssystemer og/eller i en periode ikke kan forholde seg til vedkommende tredjeparts inntrengingsforsøk på "adekvat vis". En alternativ metode for virksomheter av noen størrelse er å benytte eget personell til denne kvalitetssjekken – fortrinnsvis personell som ikke har noen befatning med det daglige arbeidet med å sikre systemene, men som har den nødvendige kompetanse til å kunne vurdere kvaliteten på det arbeidet som er gjort.

I avsnittet om økonomiske og administrative konsekvenser pekes det på at bevilgningene til samfunnets behov for å sikre sine kritiske IT-systemer og –struktur primært skal søkes dekket ved omfordeling av ressursene som er tilgjengelige innenfor eksisterende budsjettrammer. Norman er selvsagt enig i at det offentliges ressurser skal utnyttes på en best mulig måte. Imidlertid vil vi peke på at man ikke må sette seg i en situasjon - à priori - som medfører at sikkerhetsnivået må legges på et nivå som ikke er forsvarlig i forhold til de mål som er satt.

7. Forslag til tiltak for å styrke sikkerhetskultur rundt bruk og utvikling av informasjonssystemer og elektronisk kommunikasjon

Ett av de konkrete tiltak som foreslås i grunnlagsdokumentet er tilpasning av regelverket for å lette politiets arbeid med etterforskning av datakriminalitet. Norman er ikke uenig i at regelverket også på dette punktet må tilpasses slik at politiet får muligheten for å utføre sine samfunnsmessige oppgaver. Vi vil imidlertid peke på den iboende konflikt som finnes mellom det å gi politet (og andre) tilgang til informasjon om hva den enkelte har foretatt seg på et område som man kan argumentere for at tilhører den private sfære, og det enkelte individs krav på beskyttelse av sitt privatliv. Sistnevnte er etter Normans mening (også) viktig å bevare.Vi antar at dette forholdet vil bli berørt av Datatilsynets kommentarer til grunnlagsdokumentet.

Norman er glad for at man i høringsutkastet til ny lov om elektronisk kommunikasjon legger opp til at tilbydere av elektroniske nett og tjenester skal ha planer for å sikre minst en forhåndsbestemt periodes fortsatt levering til kunder i tilfelle konkurs. I forbindelse med turbulensen tidligere i år vedrørende ISPen KPNQwest og de problemer dette selskapet fikk internasjonalt, viste det seg tydelig hvor sårbare man er på dette feltet. Det er etter Normans mening imidlertid sannsynlig at to

uker er for kort tid til at alle kunder forsvarlig kan gå over til en annen leverandør i tilfelle konkurs hos eksisterende ISP e.l. Vi anbefaler følgelig at man vurderer å øke denne perioden.

8. Forslag vedrørende en samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring av sensitiv informasjon

Som det hevdes i grunnlagsdokumentet, er PKI-teknologi for tiden den eneste kommersielt tilgjengelige teknikk for å tilby kvalifiserte elektroniske signaturer.

Etter det Norman forstår vil problemstillinger omkring innføring av PKI i Norge håndteres som en egen sak i forbindelse med et eget strategidokument. Norman vil derfor i denne sammenheng nøye seg med å peke på at et av hovedproblemene med PKI-teknologien er håndtering av "det øverste nivået" ved utstedelse av sertifikater til sertifikatutstedere på neste nivå i (det nasjonale) hierarkiet. Slik situasjonen er nå, kan i prinsippet hvem som helst utstede et digitalt sertifikat bare man skaffer seg den nødvendige teknologi for gjøre dette. Etter Normans mening er antagelig denne manglende håndteringen av problemstillinger omkring sertifikatutstederes legitimitet en av hovedårsakene til at innføringen av PKI-løsninger ikke har fått større omfang. Mangelen på forskjellige, definerte "autoritative nivå", er foreløpig ikke er løst på nasjonalt og internasjonalt nivå, noe som innebærer et betydelig problem for PKI-løsningenes autoritet og kompatibilitet mellom de forskjellige aktørene av PKI-løsninger i markedet. Norman ser det som den beste løsningen at det blir et myndighetsansvar å håndtere det norske "toppnivået", på samme måte som det er en offentlig oppgave å utstede pass til landets borgere. Så vidt vi kan forstå vil ikke dette være i konflikt med den løsningsmodell som allerede er under vurdering.

9. Konsekvensanalyse og ressursbehov

Som det påpekes i dokumentet er det like viktig å fokusere på de økonomiske og andre konsekvenser av ***ikke*** å gjennomføre de foreslåtte tiltak, som å fokusere på tiltakenes kostnad. Det er betydelige beløp og øvrige verdier som står på spill for individer, virksomheter og samfunnet ved å undervurdere farene ved et for lavt implementert risikonivå.

Med vennlig hilsen
Norman ASA

Henning Hansen
Administrerende direktør

Per Olav Førland
Corporate Internet Coordinator