KITH
INFORMASJONSTEKNOLOGI
FOR ET BEDRE HELSEVESEN

Nærings- og handelsdepartementet
Postboks 8014 Dep
0030 Oslo

Deres ref.:	Deres dato:	Vår ref.: 424/02	Vår dato: 25.11.2002
2001/5605 KDB	21.10.2002		

Høringssvar – grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

Det vises til brev av 21.10.2002 om grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet. Helsesektoren er inne i en omfattende omstillingsprosess hvor elektronisk samhandling i stadig større grad vil erstatte eksisterende rutiner for informasjonsflyt og informasjonsdeling og hvor avhengigheten av elektroniske systemer vil være stadig økende. I anerkjennelse av dette har KITH bla. utarbeidet rapporter om hvordan driftssikkerhet bør ivaretas for kritiske IT-systemer i helsesektoren og opprettеholder et sterkt fokus på informasjonssikkerhet generelt gjennom bla. rådgivningsarbeid og risikovurderinger. Vi stiller oss derfor positive til utarbeidelsen av en nasjonal strategi for informasjonssikkerhet og ønsker at strategien best mulig skal ivareta helsesektorens behov.

Grunnlagsdokumentet gjør en god jobb i å beskrive utviklingstrekk som påvirker trusselbildet og gir et bredt perspektiv på de trusler det moderne informasjonssamfunnet står overfor. KITH støtter i all hovedsak de tiltak som foreslås gjennomført. Særlig viktig er fokuset på økt kunnskap om sikkerhetsutfordringer gjennom veiledning og undervisning og styrking av sikkerhetskulturen på alle nivåer i samfunnet.

Omformuleringen av sårbarhetsutvalgets målsetning om å "øke robustheten i kritisk IT-infrastruktur til et nivå som gjør det helt usannsynlig at viktige samfunnsfunksjoner stanses i en normalsituasjon" til en formulering om at "risikoen for avbrudd er akseptabel" synes noe passiv og mindre klar. Selv om den opprinnelige målsetningen i liten grad synes oppnåelig er den i større grad klar på hva målsetningen bør være. Å operere med idealiserte målsetninger er heller ikke ukjent og har sin klare parallell f.eks. i null-visjonen for trafikkdødelighet på norske veier. Hvis den omformulerte målsetningen skal kommunisere på en tydelig måte er det behov for klare definisjoner av hva akseptabel risiko innebærer for de konkrete samfunnsfunksjonene. Formuleringen om avbrudd virker også ensidig rettet mot tilgjengelighet på bekostning av konfidensialitet og integritet.

Grunnlagsdokumentet legger opp til en plassering av sikkerhetsansvar i helsesektoren hvor helse- og sosialdepartementene gis ansvar for å koordinere oppfølgingen av krav til IT-systemer, Sosial- og helsedirektoratet gis ansvaret for å definere krav til IT-systemer og følge opp disse. Helseforetakene og private helseinstitusjoner gis ansvar for å implementere krav i aktuelle IT-systemer.

Postadresse: Sukkerhuset, NO-7489 Trondheim, Besøksadresse: Sverresgt. 15
Tlf: 73 59 86 00, Fax: 73 59 86 11 www.kith.no
FNR: 959925496

KITH finner denne ansvarsfordelingen rimelig. Det kan bemerkes at en del helsetjenester også faller innenfor et kommunalt ansvarsområde. Det må avklares hvordan Sosial- og helsedirektoratets rolle ift. å definere krav til IT-systemer skal gjøres gjeldende overfor private helseinstitusjoner og kommunal helsetjeneste.

De regionale helseforetakene og deres respektive helsenett vil ha en sentral rolle i å legge til rette for funksjonell og sikker elektronisk samhandling på regional plan. Særlig vil helsenettene kunne ha en sentral rolle i å bistå og legge til rette for mindre helseinstitusjoner som ikke selv har kompetanse og ressurser til å håndtere en omfattende sikkerhetsfunksjon internt i virksomheten. Dette kan særlig foregå ved å legge til rette for de risikovurderinger den enkelte virksomhet må gjennomføre samt å bistå og legge til rette for en fornuftig avvikshåndtering.

Helsenettene har økt potensialitet for en mer rasjonell fordeling av ansvaret for etablering og drift av IT-tjenester på regionalt nivå. Den samordning av en rekke kritiske IT-tjenester som dette legger til rette vil stille store krav til håndtering av sårbarhet og trusler. Helsenettene vil på mange områder bli en samfunnskritisk infrastruktur, og det kan derfor være behov for et koordinerende organ som kan definere akseptansekriterier og vurdere kritikalitet og sårbarhet for systemene. Dette er et aktuelt område hvor særskilte bevilgninger til styrket IT-sikkerhet vil være aktuelle, og hvor, som beskrevet i kapittel 6.3, leverandør- og kundefinansiering ikke vil være tilstrekkelig.

Grunnlagsdokumentet legger vekt på bl.a. sikkerhetsrevisjon og inntrengningstester som verktøy for å kontrollere status og oppfølging av sikkerheten på virksomhetsnivå. Ift. sikkerhetsrevisjon er det viktig at offentlige myndigheter legger et omforent og tydelig meningsinnhold i begrepet. Inntrengningstester kan være en viktig del av dette arbeidet, men revisjon bør også innbefatte en mer omfattende vurdering av at rutiner og sikkerhetstiltak (både teknisk og organisatorisk) er korrekt implementert og fungerer formålstjenlig. Særlig må en sikkerhetsrevisjon omfatte mer enn en gjennomgang av forhåndsdefinerte sjekklister som ikke gir mulighet for grundigere vurderinger av spesielle forhold av betydning for sikkerheten. På lik linje med de godkjenningsordningene som allerede er etablert for evaluering av sikkerhet i virksomheter (ISO/IEC 17799:2000) og systemer (Common Criteria) bør det vurderes å stille konkrete krav til revisjonsform og innhold basert på internasjonale og anerkjente standarder.

KITH har en sentral rolle i arbeidet med rammeavtale for PKI for helsesektoren som foregår i regi av Rikstrygdeverket. Ift forslaget om samfunnsinfrastruktur for elektronisk signatur, autentisering og sikker overføring av sensitiv informasjon ønsker vi å legge vekt på følgende momenter:

- Det må vektlegges åpne løsninger basert på standardiserte protokoller og teknologi
- Felles krav fra offentlig sektor bør gå langt i å spesifisere konkrete minstekrav for funksjonalitet, tjenester, protokoller og sikkerhetsnivå som skal støttes av infrastrukturen.
- Det må vektlegges å redusere kompleksiteten i løsningene så mye som mulig, bl.a. ved å velge pragmatiske og funksjonelle løsninger for samtrafikk, særlig ved å legge vekt på standardiserte løsninger for sertifikatformat og profiler samt sertifikatvalidering.

Med vennlig hilsen

Jacob Hygen
Adm. Dir.