Forum for IT-sikkerhet

Referat

Møte om:	Høringsmøte–Gr.lagsdok. nasjonal strategi for informasjonssikkerhet
Saksnr.:	
Til stede:	Se vedlagt liste
Dato:	07.11.02
Møteleder:	Jon Ølnes
Referent:	Cort Archer Dreyer
Kopi til:	

Grunnlagsdokument for nasjonal strategi for informasjonssikkerhet – Høringsmøte 06.11.02

1. Åpning

Jon Ølnes var møteleder ettersom Forumets leder, Jon Bing, hadde meldt forfall.

Nye medlemmer i Forumet
Per Bjørkum, Norsk Hydro ASA, Åse Nilsen, Winlink AS, Jørn Andreas Arnesen, Deloitte & Touche og Inger Johanne Fanneløp, Nera Broadband Satellite

Siri Mollatt, Norsk Hydro ASA, går ut.

Forumets arbeidsutvalg:
Leder Jon Bing, IRI, Inger Marie Sunde, Økokrim, Jon Ølnes, PKI Consulting Services, Leif Aanensen, Datatilsynet, Jørn Andreas Arnesen, Deloitte & Touche og Cort Archer Dreyer, NHD.

2. Høring Grunnlagsdokumentet

Prosjektleder Katarina de Brisis, NHD, innledet høringsmøtet med å sette grunnlagsdokumentet inn i et internasjonalt perspektiv. Videre ble de mest sentrale forslagene i dokumentet gjennomgått før hun avsluttet med en kort orientering om den videre prosess etter høringsfristens utløp.

Generelle merknader
Dokumentets begrepsbruk kan forbedres. Begrepslisten bør strammes opp og brukes mer aktivt i dokumentet.

Dokumentet er uklart mht. å få frem hva som er genuint nye forslag fra gruppen, og hva som er eller vil bli iverksatt uavhengig av det pågående strategiarbeidet.

Det bør fokuseres mer på forholdet mellom IT-sikkerhet og beredskap samt skadeopprettende tiltak. Hvordan innlemme dette i beredskapsplaner - når det gjelder å utarbeide IT-sikkerhetsstrategi? Bør det være en fast prosedyre å utarbeide krisehåndterings- og beredskapsplan for gjenoppretting av skade?

Dokumentet er utydelig mht. sikkerheten til privatpersoner (systemeier-begrepet).

Dokumentet har forholdsvis stor fokus på kostnadsdrivende aktiviteter som f.eks. risikoanalyser og sertifisering. Hva med enkle og billige tiltak med god effekt?

Forholdet mellom sikkerhet og tillit er ikke godt nok dekket i dokumentet slik det foreligger.

Kapittel 5 Ansvar for, og koordinering av, IT-sikkerhet
de Brisis redegjorde for prosessen internt i prosjektet mht. utvikling av dette kapittelet.

Forumet mener det er et klart behov for en samordning. En etablering av et permanent koordineringsråd for IT-sikkerhet–slik det er fremstilt i dokumentet–vil være et steg i riktig retning. Rådet må imidlertid gis et klarere mandat vedr. hva man skal gjøre og hvordan i Rådet skal gjennomføre en koordinering av regelverket.

Selv om koordinering foregår sentralt vil utfordringen mht. til implementering av regelverk og tiltak ligge hos den enkelte virksomhet. Det ble drøftet hvorvidt implementering av tiltak mv. kan forenkles ved f.eks. at ev. nye forskrifter tar mal av de eksisterende, som f.eks. forskrift til Personopplysningsloven, standardisering av verktøy for å gjennomføre tiltak mv. Dette gjelder spesielt for kommuner og SMB som ofte kan ha vansker med å gjennomføre en risikovurdering. Det er ønskelig med gode/håndterbare standarder som lett kan iverksettes i praksis.

Kap. 5.2.2. Samfunnskritisk IT-infrastruktur og–IT-systemer må følges opp. Det er ønskelig for å få klarlagt hvilken infrastruktur og hvilke systemer som faller inn under kategorien "samfunnskritisk".

Kapittel 6 Forslag til strategier og tiltak for å sikre kritiske infrastrukturer og informasjonssystemer
de Brisis ønsket–om mulig–å få bistand til å få definert når et virksomhetskritisk system går over til å bli oppfattet som et samfunnskritisk system. Tilsvarende var det også ønskelig å få klarlagt hva som skal til for å sikre Internett som er kritisk infrastruktur for mange virksomheter.

Forumet mener at risikovurderinger er helt essensielt. Enkelte tok til orde at dette burde lovpålegges. Det bør også utvikles en egen metode for en slik risikovurdering av

kritiske systemer. Objektsikkerhetsforskriften vil trolig si noe om hvilke kriterier som bør legges til grunn for en slik vurdering.

Pkt. 6.1.3. vedr. definering/presisering av det samfunnsmessige beskyttelsesbehov mht. til integritet og tilgjengelighet. Det må i denne sammenheng tas hensyn til de forretningsmessige prinsipper. Det kan være et problem med privateid kritisk infrastruktur. Har man virkemidler/makt til å få eiere av slike infrastrukturer til å ivareta samfunnets interesser?

Internett har blitt virksomhetskritisk for mange virksomheter. Hvilken rolle skal ISP-er ha? Skal de underlegges lovkrav og forskrifter med egnet tilsynsmyndighet?

Inntrengningstester–Er tiltaket for detaljert for dette dokumentet? Hvem skal i så fall være godkjenningsinstans for dem som foretar disse testene? Hvilke krav skal gjelde?

Pkt. 6.1.4. vedr. Generelle statlige IT-sikkerhetsnormer. En bør i størst mulig utstrekning referere til det regelverket som allerede finnes/knagger man kan henge felles normer på, formulere hvilke hjelpemidler vi kan tilby. Felles statlige normer? Vi har allerede en mal i BS7799, trenger vi noe nytt?

Klassifisering av informasjon er vanskelig. En bør unngå å lage overordnede/felles systemer som kan bli en tvangstrøye for virksomhetene. De må få lov å lage sine egne systemer, basert på egne behov for klassifisering. Det bør i stedet lages en metodikk for risikovurdering der også tilgjengeligheten og integriteten til informasjonen vektlegges. Ifm. en slik risikovurdering er det viktig å få klarlagt eierskapet til informasjonen. Det samme gjelder for eiers forventninger/ønsker til hvordan informasjonsbehandler skal opptre. Viktig at systemeier deltar i denne prosessen.

Ifm. gjennomføring av en risikovurdering er det ønskelig at systemeieren har/kan gi en definisjon av hva som skal oppfattes som akseptabel risiko.

Innledningen til kap. 6.2 Virksomhetsnivå bør bli klarere i sin omtale av forholdet til regelverket og hvordan dette slår inn i virksomhetene.

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

Anbefalingene omkring FOU innebærer høye kostnader, og forutsetter en vilje til oppfølging gjennom bevilgninger over statsbudsjettet. Dette bør nevnes i kap 7.1.4 Forskning og utvikling innen IT-sikkerhet.

Kap. 7.1.6 Datakrimutvalget. Det er ønskelig med en mer presis omtale av utvalget og at utvalget er oppnevnt av JD.

Sertifisering av organisasjoner er ikke nevnt. En omtale av dette bør inngå i kap. 7.2.1 Styring av IT-sikkerhet.

Kap. 7.2.1 punkt 1 Utarbeide rammeverk, mål, sikkerhetsstrategi og sikkerhetspolicy er uklart formulert. Se bl.a. på språkføringen.

Kap. 7.2.2 punkt 3: Bør omformuleres. Fjern "sikkerhetsmessig lønnsomhet" og presiser "ansvarlig instans".

I utgangspunktet mener Forumet at privatpersoner/brukere har et ansvar for å sikre seg selv. Det forutsettes at den enkelte selv skal skaffe seg kunnskap og kompetanse. Dette må de imidlertid få hjelp til. Hvordan? Er offentlige infokampanjer nok eller bør myndighetene også ta et grep når det gjelder f.eks. markedsføringsloven? Bør noe av ansvaret legges på leverandøren?

Alternativer som ble nevnt for å få opp kunnskapsnivået var bl.a.:

- Få infosikkerhet inn som en del av opplæring i Datakortet
- Forbrukerrådet bør kunne rangere og vurdere sikkerhetsprodukter og -tjenester
- Det offentlige bør vise vei ved å definerer krav til sikkerhetsprodukter–slik at leverandørene kan forholder seg til dette
- Implementering av vedtatt regelverk fungerer ikke alltid som forventet. Regelverksforvaltere bør derfor få en plikt til å sørge for relevante opplæringstiltak som kan hjelpe brukere å etterleve regelverket.
- Myndighetene kan stille felles krav til bruksegenskaper i sikkerhetsprodukter og -tjenester.
- Kan sertifiseringsordninger ivareta dette aspektet? Bør bransjeorganisasjonene oppfordre til bruk av sertifisering?
- Regelverksforvaltere bør tillegges et ansvar for å revurdere sikkerhetsregelverket regelmessig. - jfr. solnedgangsbestemmelser og e-kommforskriftens regler om oppbevaring av elektroniske saksdokumenter.

Kapittel 8 Forslag vedrørende en samfunnsinfrastruktur for elektronisk infrastruktur, autentisering og sikker overføring av sensitiv informasjon

Det foregår en egen separat prosess på PKI-strategi i Nasjonalt PKI-Forum. Følgelig ble det ikke brukt mye tid på å behandle dette kapittelet. Forum for IT-sikkerhet mener imidlertid at dette bør betraktes som en samfunnsinfrastruktur, og det bør være et offentlig ansvar (myndighetens) ansvar å dra dette i gang.

Infrastrukturen er på plass (ZebSign, Bank ID). Problemet er at brukerne ikke er modne til å ta dette i bruk. Det som skal til for å få brukerne til å benytte dette er bl.a. å utvikle allerede etablerte tjenester.

3. Orientering om fremdrift og status i arbeidet med ISO/IEC JTC1 SC27 WG1 vedr. sikkerhetsstandarden IS 17799 samt ny versjon av BS 7799-2

Rune Ask har deltatt på et arbeidsgruppemøte i Warszawa oktober 2002 vedr. ovennevnte. Til møtet i Warszawa forelå det et dokument der en hel del endringsforslag

var innarbeidet. I løpet av møtet ble 650 nye forslag fremmet. Det er besluttet å ha et nytt arbeidsgruppemøte i Quebec i april 2003.

BS 7799-2 versjon 3 kom september 2002 (i regi av IUG). Det foreligger et forslag om å lage et sertifiseringsregime for ISO 17799 - vil man da foreslå at også BS7799-2 blir en IS?

Det foreligger et forslag om å lage en del 3 om hvordan standarden skal brukes. Det er liten enighet om å bruke IS 17799 som en sertifiseringsstandard. Det foreslås at dette heller bør forbli en code of practice (god praksis).

BS7799 - introdusert skalering til SMB og tankegang om kontinuerlig vurdering av sikkerhet, prosessorientering fremfor dokumentorientering.
Pr. d.d. er det 153 virksomheter som er sertifisert iht. standarden på verdensbasis, derav 6 i Norge (4 i Sverige).

ISO TR 13335 (GMITS) skal bli en standard. Det foreligger også et forslag om å gjøre ISO TR 18028 IT network security til en standard.

Til stede:

Katarina de Brisis, NHD
Tor Ottersen, Shdir
Johs. Hansen Hammer, Hammer ITS
Randi Elisabeth Johansen, PT
Siri Mollatt, Norsk Hydro
Liv Føre, Troms FK
Torgeir Jonvik, FIN
Amund Eriksen, Statskonsult
Jørn Andreas Arnesen, Deloitte & Touche
Kjell Bergan, FO/S
Hege B. Sæveraas, SD
Kristian Bergem, ZebSign
Torbjørn Faller, Thales
Tore Holth, EDB Fellesdata
Anne Reinsnes, Telenor
Arve Aasmundseth, Abelia
Berit Børset Solstad, NSO
Arne Johan Helle, PWC
Roar Gulbrandsen, PWC
Dagfinn Buset, JD
Jon Ølnes, PKI Consulting Services
Rune Ask, IT-sikkerhetsforum
Cort Archer Dreyer, NHD