Nærings- og Handelsdepartementet
Postboks 8014 Dep
0030 Oslo

Sak: 2001/5605 KDB

Porsgrunn 25. november 2002

Kommentarer til Sak: 2001/5605 KDB, Grunnlagsdokument for Nasjonal strategi for informasjonssikkerhet.

VincIT Risk Management står ikke oppført på listen over høringsinstanser, men da vi mener å kunne bidra i prosessen har vi tatt oss den frihet å gi noen kommentarer til grunnlagsdokumentet. Synes at grunnlagsdokumentet får bra frem utviklingstrekk og utfordringer mht. informasjonssikkerhet/IT-sikkerhet.

Informasjonssikkerhet kontra IT-sikkerhet

Grunnlagsdokumentet har tittelen "Nasjonal strategi for informasjonssikkerhet". Jeg mener bestemt at det må gjøres klart hva som forstås med informasjonssikkerhet kontra IT-sikkerhet. Jeg registrerer at IT-sikkerhet benyttes bl.a. i overskriften til bl.a. kap. 1.5. Noe som blir galt når innholdet i kapitlet leses. I denne overskriften burde IT-sikkerhet vært endret til informasjonssikkerhet. Jeg sitter igjen med inntrykk av at uttrykket "IT-sikkerhet er benyttet ukritisk i store deler av dokumentet. IT-sikkerhet burde i store deler, eller i hele rapporten vært byttet ut med "Informasjonssikkerhet". Informasjonssikkerhet slik jeg forstår det favner både det organisatoriske, kommunikasjon, IT, kontinuitet, aksesskontroll, opplæring, kryptering, PKI, etc. Ved å bruke ordet IT-sikkerhet mener jeg prosessen med å få til en nasjonal strategi for informasjonssikkerhet får helt feil fokus.

Mål og innretning av strategiarbeidet

Kap. 2. Sammendrag, 3. avsnitt, 2. setning;

" Videre har målsettingene vært å etablere en sikkerhetskultur som innebærer at IT-sikkerhet integreres i større grad ved bruk av IT, og etablering av en allment tilgjengelig samfunnsinfrastruktur for elektronisk signatur, autentisering av kommunikasjonspartnere samt sikker overføring av sensitiv informasjon."

Kommentar: Intensjonen med at IT-sikkerhet i større grad skal integreres i bruken av IT er jeg i utgangspunktet helt enig i, men problemet er at i tilnærmet all utvikling innen IT er ikke informasjonssikkerhet eller IT-sikkerhet en del av utviklingsprosjektet. Jeg mener at myndighetene må sette krav til at det kun skal velges løsninger/systemer som er sertifisert iht. Common Criteria og hvor krav til sikkerhet har vært satt på dagsorden fra dag 1. Sikkerhet må inn innarbeides på alle lag og det har lite for seg med PKI løsninger når den tekniske og organisatoriske sikkerheten ikke holder mål. Sikkerheten blir som kjent ikke sterkere enn det svakeste ledd.

Kap. 2. Sammendrag, 5. avsnitt;

*"Det foreslås at sikkerheten i **kritiske systemer** innenfor offentlige og private virksomheter sikres bl.a. gjennom klargjøring av behov, klassifisering av informasjon og systemer, veiledning for hvordan IT-sikkerhet skal implementeres og bruk av evaluerings og sertifiseringsordninger."*

Kommentar: Det skapes et inntrykk av at det er kun i et fåtall offentlige og private virksomheter at det finnes kritiske systemer. Med den avhengigheten virksomheter i dag har til IKT påstår jeg at de aller fleste av en viss størrelse har **minst ett kritiske system**. Mao, evaluering og sertifiseringsordninger kan være aktuelle løsninger for å møte sikkerhetsutfordringene til de fleste virksomheter av en viss størrelse.

Foreslåtte strategier og tiltak i kap. 5-8.

Kap. 6 Forslag til strategier og tiltak for å sikre infrastruktur og informasjonssystemer.

Kommentar: Kapitlene 6.1 og 6.2 ramser i hovedsak opp diverse tiltak. Hvorfor? Alle disse tiltakene omhandles i NS-ISO/IEC 17799 Administrasjon av informasjonssikkerhet. Jeg foreslår at det i sterkere grad henvises til standarden som en retningslinje for aktuelle tiltak som kan iverksettes. I den grad standarden har mangler bør vi arbeide for å gjøre den mer fullstendig. Videre kan dette følges opp med at myndighetene stiller krav til at private og offentlige virksomheter, som skal bidra til å gjøre nasjonen sikrere eller som har ansvaret for deler av den samfunnskritiske infrastrukturen, skal være sertifisert iht. NS-ISO/IEC 17799 innen utgangen av 2004.

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

Kommentar: Har store problemer med å forstå hvorfor PKI har fått et eget kapitel i grunnlagsdokumentet. PKI er kun et tiltak på lik linje med andre tekniske og organisatoriske tiltak og bør definitivt ikke omhandles i et eget kapittel. PKI isolert sett løser ikke de sikkerhetsutfordringene vi står ovenfor. Satt på spissen så er mange virksomheter, både private og offentlige, i dag fornøyde med sikkerheten hvis de har en løsning for antivirus og en brannmur. Slikt som tilstrekkelig sikkerhetsmessig vedlikehold av løsningene og ikke minst organisering og bevisstgjøring av egne ansatte er tilnærmet fullstendig mangelvare.

PKI er viktig men jeg tror de fleste virksomheter må fokusere langt sterkere på bl.a. organisatorisk sikkerhet i første omgang. De alvorligste bruddene på informasjonssikkerhet gjøres av egne ansatte. Jeg vil påstå at det vil hjelpe lite med å ta i bruk teknisk tilfredsstillende PKI-løsninger når den organisatoriske sikkerheten i virksomheten er særdeles mangelfull.

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

I det videre arbeid med å få til en slagferdig strategi er mitt budskap kort og godt:

- Ansvaret for oppfølging og motivering fra myndighetene må samles på langt færre hender enn hva som er faktum i dag.
- Det må satses mer på bevisstgjøring og opplæring. Foreslår at det offentlige gjennomfører kampanjer for å bevisstgjøre oss alle mot den risikoen vi daglig er utsatt for.
- Hele det offentlige Norge, gjerne i samarbeid med private virksomheter, bør i fellesskap definere et minste felles sikkerhetsnivå på den tekniske delen. Sikkerhetsnivået kan omsettes i tekniske løsninger ved å velge kun systemer og produkter som er sertifisert iht. Common Criteria. Dette vil tvinge alle utviklere og produsenter til å tenke sikkerhet fra dag.1 når nye systemer skal utvikles. Det er som kjent tilnærmet umulig å implementere sikkerhet i etterkant. Med dette forslaget tror jeg at vi alle, i løpet av noen år, kunne fått handlet "hyllevare" med tilstrekkelig sikkerhet og til fornuftige priser.
- Det må fokuseres langt sterkere på organisatorisk sikkerhet. Informasjonssikkerhet handler i stor grad om å ha orden i eget hus og et bevisst forhold til de man utveksler informasjon med.
- NHD har selv stått i bresjen for sertifiseringsordning iht. BS 7799 (eller NS-ISO/IEC 17799 Administrasjon av informasjonssikkerhet. Del 2 av BS 7799 er fortsatt ikke en ISO standard. Virksomheter i Norge sertifiseres etter BS 7799 del 2, finnes for øvrig i ny utgave nå i høst hvor standarden er mer harmonisert med ISO standardene for kvalitet og miljø). Hvorfor stilles det ikke krav om at virksomheter med kritiske systemer skal være sertifisert iht. standarden og hvorfor har ikke NHD valgt å la seg sertifisere? Det beste vi har i dag er BS 7799 standarden. Så lenge vi ikke har noe som er bedre innenfor informasjonssikkerhet er det viktig at dette understøttes og tas i bruk av offentlige virksomheter.

Med vennlig hilsen

Frank-Arne Stamland
Daglig leder i VincIT Risk Management AS

PB. 70, Skjelsvik
3906 Porsgrunn
Kontor: 35 57 41 38
Mobil: 90 57 67 57
Faks: 90 31 56 20
www.vincit.no