Nærings- og Handelsdepartementet
v/ Katarina De Brisis

Pb 5490 Majorstua
0305 Oslo
Tlf: 23 08 80 70
Faks: 23 08 80 71
Org. nr. 983489060

Oslo, 25.11.2002

Høringssvar – Nasjonal strategi for IT-sikkerhet

Vi viser til brev av 21.10.2002 der Abelia inviteres til å komme med synspunkter på Grunnlagsdokumentet for Nasjonal strategi for IT-sikkerhet. Abelia er en bransjeorganisasjon innenfor NHO som organiserer i overkant av 300 IKT- og kunnskapsbedrifter med i alt 31000 ansatte.

Generelt

Grunnlagsdokumentet er svært omfattende og gir etter vårt syn et godt grunnlag for å utvikle en nasjonal strategi for IT-sikkerhet. Vi synes dokumentet gir en god beskrivelse av dagens organisering og status på området og en god gjennomgang av ulike utfordringer vi står overfor som et resultat av teknologiutviklingen.

Vi vil imidlertid peke på at tiltakene slik de er foreslått i dokumentet framstår mer som ønsker og anbefalinger om områder som må konkretiseres ytterligere enn som elementer som til sammen utgjør en helhetlig strategi. Abelia mener det vil være viktig å:

- Legge til grunn av det overordnede lov- og regelverket i Norge skal være harmonisert med lov- og regelverket i EU og globalt.
- Sørge for at lov- og regelverket ikke er til hinder for næringsutvikling og innovasjon. Den økte globale oppmerksomheten rundt IT-sikkerhet bør i stedet føre til at vi ser dette som et viktig marked der norske bedrifter med gode produkter og tjenester innen IT-sikkerhet kan konkurrere internasjonalt.
- Foreta en ytterligere rolleavklaring mellom ulike offentlige etater for å unngå dobbeltarbeid og uklar ansvarsfordeling.
- Avklare rollefordelingen mellom offentlig og privat sektor. Tiltakene som i dokumentet er definert som virksomhetenes eget ansvar er viktige, men de skiller ikke godt nok mellom ulike typer virksomhet. Strategien er heller ikke presis i forhold til hva som er leverandørers ansvar og hva som er brukerbedrifters ansvar.
- Være mer presis i forhold til krav og forventninger til private bedrifters arbeid med IT-sikkerhet. De enkelte virksomheters ansvar må tydeliggjøres.
- Finne fram til gode verktøy bedriftene kan bruke i sine risikovurderinger og i sin kompetanseutvikling. Dette bør skje i et samspill mellom offentlig og privat sektor, og gjerne med stor medvirkning fra bransjeorganisasjoner.

Utviklingstrender

Dette kapitlet i dokumentet gir en god beskrivelse av hvordan teknologiutviklingen skaper nye utfordringer innenfor IT-sikkerhet. Kapitlet beskriver også arbeidet med regelverk og standarder. Abelia vil framheve at det i tillegg til dette er viktig å fokusere på noen andre utviklingstrekk som skaper nye utfordringer og som ikke er direkte knyttet til selve teknologiplattformene, men til organisatoriske og forretningsmessige virkninger av å ta i bruk ny teknologi:

- Teknologien utvikler seg raskere enn evnen til å overskue konsekvensene av å ta i bruk ny teknologi. Derfor er forebyggende arbeid for å redusere sikkerhetsrisiko ved bruk av IT veldig knyttet til å endre kultur og adferd, tydeliggjøre roller og ansvar, øke kompetansen og å synliggjøre konsekvenser av ulike handlinger.
- Verdikjedene inkluderer flere aktører i og med at bedrifter i større grad konsentrer seg om kjerneområder og outsourcer virksomhet de tidligere drev selv. Teknologien gjør det mulig å jobbe med partnere i sanntid på samme IT-plattform og på tvers av landegrenser. Dette skaper nye utfordringer i forhold til rolle- og ansvarsfordeling i forhold til IT-sikkerhet.
- Det er i økende grad ren maskin til maskin kommunikasjon i forretningsprosessene, uten manuelle kontroller underveis. Også i vårt dagligliv vil vi få en utvikling der elektroniske komponenter i mye større grad kommuniserer direkte med hverandre. Dette innebærer sikkerhetsmessige fordeler ved at det reduserer risikoen for menneskelige feil, men det betyr også at konsekvensene kan blir mer alvorlige når feil oppstår.
- Teknologiplattformene i IT og telesektoren er i økende grad globale mens utvikling av lovgivning og regelverk fortsatt skjer nasjonalt. Forskjeller i lovgivning, regelverk og strategier i ulike land er med på å redusere mulighetene for å få til effektive strategier for sikkerhet.

Elektroniske signaturer

Abelia mener det er positivt at dokumentet legger stor vekt på elektronisk ID og elektroniske signaturer som et virkemiddel for å oppnå økt IT-sikkerhet. Effektiviseringen av offentlig sektor er avhengig av at sikkerheten ivaretas. Kommunikasjon mellom ulike forvaltingsorganer og med brukere stiller krav til beskyttelse av sensitiv informasjon. En rask utrulling av elektroniske signaturer i befolkningen vil være en stor fordel for ivaretakelsen av sikkerheten i denne kommunikasjonen. Abelia mener derfor det er viktig at staten er med på å etablere et marked for elektroniske signaturer ved å sørge for at statlige etater tar slike løsninger i bruk. Da kan staten også opptre som krevende kunde og stille krav til sikkerhetsnivåer og samtrafikk mellom ulike infrastrukturer. Strategidokumentet fra PKI-Forum bør legges til grunn for statens videre arbeid her.

Samordning av regelverk

Nasjonale lover, regler, strategier og føringer produseres og forvaltes av flere departementer, direktorater, etater og organer. Regelverket må derfor samordnes. Spørsmålet i dag er ikke om regelverket skal samordnes, men hvor regelverket skal samordnes. I dag samordnes kravene fra ulike myndigheter i de enkelte virksomhetene. Abelia mener dette er en ineffektiv bruk av ressurser som dessuten fører til både misforståelser og svært ulike løsninger. Den nasjonale strategien for IT-sikkerhet bør derfor legge en klar forventning om at mer samordning skal

skje på myndighetsnivå. Dersom sikkerhetsnivået i Norge skal heves må regelverket også forenkles og koordineres bedre.

Et dynamisk sikkerhetsarbeid

For å oppnå tilstrekkelig dynamikk og et sikkerhetsnivå som er tilpasset virksomhetens behov til enhver tid må den enkelte bedrift definere sitt risikonivå. For å oppnå at dette gjøres på en god nok måte må det utvikles metoder for risikovurdering av IT-systemer og infrastruktur. Den enkelte virksomhet må risikovurdere på bakgrunn av lov- og regelverk og ut fra sine egne og sine kunders forretningsmessige og kommersielle interesser. Myndighetene må risiko- og sårbarhetsvurdere samfunnskritisk infrastruktur ut fra en vurdering av de samfunnsmessige konsekvensene. Myndighetene må også bidra med oppdaterte trusselvurderinger som gjøres tilgjengelig for private operatører av samfunnskritisk infrastruktur.

Forholdet til ny lov om elektronisk kommunikasjon – reguleringer i konkurssituasjoner

Dokumentet nevner i punkt 7.1 en rekke aktiviteter som tar sikte på å samordne lov og regelverk på IT-sikkerhetsområdet. Denne samordningen er positiv.

Når det gjelder lov om elektronisk kommunikasjon vil Abelia vise til den høringsuttalelsen vi sendte Samferdselsdepartementet i september. Her har vi blant annet kritisert forslagets bestemmelser om leveringsplikt i konkurssituasjoner. Levering i to uker etter konkurs kan innebære at an driver for kreditors regning. Dette er i andre sammenhenger ulovlig og bør ikke være praksis i telesektoren heller, blant annet fordi det vil øke risikoen for at underleverandører også rammes av konkurs. En kan da risikere massekonkurser som gir langt mer negative konsekvenser for IT-sikkerheten enn en enkelt konkurs.

Forskning

Dokumentet beskriver hvordan forskning er viktig for å få en bedre forståelse av problemstillinger rundt IT-sikkerhet. Abelia er helt enig i at dette må være et viktig satsingsområde framover. Som en del av en forsterket forskningsinnsats på dette området er det viktig å satse på forskning i bedrifter og forskningsmiljøer i Norge som arbeider med å utvikle produkter og tjenester som tar sikte på å øke IT-sikkerheten. Denne type IKT-forskning må komme i tillegg til forskning på de mer økonomiske og organisatoriske problemstillingene knyttet til IT-sikkerhet.

Tiltakene i dokumentet

Abelia velger i denne omgang å ikke gå inn å kommentere hvert enkelt tiltak som er foreslått. Vi mener at intensjonene bak samtlige forslag som er foreslått er gode, men vi synes ikke tiltakene er lagt fram i en form som gjør det mulig å ha en helt presis oppfatning av hva de vil gi av kostnader og gevinster. Derfor regner vi med at dette vil bli konkretisert i framtidige dokumenter fra myndighetene.

Et eksempel på en slik mangelfull konkretisering er punkt 7.3.2, første og andre strekpunkt om å produsere en serie om IT-sikkerhet i massemedia. Mens intensjonen om å nå det brede publikum med informasjon om IT-sikkerhet er meget god, er det ikke slik at leverandører, forsiktingsselskaper eller myndigheter kan pålegge redaktører i mediebedrifter å sende bestemte programmer. Det er heller ikke noen vurdering i dokumentet av hva et slikt tiltak

skal koste. Dette er derfor et av mange tiltak i dokumentet som må konkretiseres for at vi skal kunne ta stilling til det.

Vennlig hilsen
Abelia

Paul Chaffey
Adm. direktør

Arve Aasmundseth
HMS-leder