Nærings- og handelsdepartementet
Postboks 8014

0030 Oslo

Att: Katarina de Brisis

SSI 249/02/HTh/hth/07/20.03 Arendal, 26.11.02

Kommentarer til grunnlagsdokument for utarbeidelse av nasjonal strategi for informasjonssikkerhet

En utfordring ved alt strategiarbeid er å få omsatt overordnede mål og strategier til praktiske og realiserbare tiltak der resultatene fra tiltakene i ettertid er målbare. Med dette perspektivet, har System Sikkerhet ASA etter gjennomlesing av dokumentet valgt ut ett sentralt tema for å belyse hvordan dette kanskje kan oppnås for IT-sikkerhet. Valg av tema er styrt av de erfaringer System Sikkerhet har fra sine mange år med arbeid innen IT-sikkerhet, og hvor man ser at nasjonal drahjelp vil kunne ha vesentlige positive effekter for å redusere samfunnets sårbarhet.

Sikkerhetssertifisering av leverandører

Bruk av ekstern drift av tjenester innebærer i seg selv en ekstra trussel da man selv ikke lenger har den direkte kontrollen. Dersom virksomheten behandler informasjon som er underlagt Personopplysningsloven eller Helseregisterloven, vil virksomheten måtte avtale nødvendig sikkerhet, internkontroll og sikkerhetsadministrasjon med sin partner. Det vil likevel være den enkelte virksomhets ansvar at sikkerheten blir behørig tatt vare på også ved ekstern drift. Det påhviler også den eksterne leverandøren et visst ansvar ved drift av tjenester hvor behandlingen er underlagt Personopplysningsloven eller Helseregisterloven.

Den virksomhet som ikke er underlagt lovverket på tilsvarende måte, har ikke den drahjelp i krav mot leverandør som beskrevet i forrige avsnitt. Videre er det ikke et automatisk fokus på sikkerhetsaspektet, siden det ikke er representert ved lovverk og tilsynsmulighet. Håndtering og krav til sikkerhet er den enkelte virksomhets ansvar, men sikkerhet vil fort kunne betraktes som utgift i stedet for nødvendig og fornuftig

sikkerhet.no
epost: post@sikkerhet.no
telefon 37 05 81 00, telefax 37 05 81 09
Serviceboks 721, 4808 ARENDAL
Arendal Oslo

risikohåndtering, med de konsekvenser det har for både den enkelte virksomhet og nasjonen sett samlet.

Bruk av ekstern drift er i tillegg ofte begrunnet ut fra virksomhetens manglende kompetanse innen IT generelt og sikkerhet spesielt. Man overlater dette til den eksterne parten, og regner med at siden det er et kjent og respektert firma tjenesten blir satt bort til, at sikkerheten blir tilfredsstillende ivaretatt. Driftsoperatør på sin side har ikke fått spesifisert nødvendig sikkerhetsnivå i avtalen, og etablerer et nivå ut fra skjønnsmessig vurdering og rasjonell drift.

Denne innledning synliggjør at mange virksomheter, selv de som er underlagt refererte lover, vil kunne ha store utfordringer relatert til å vite hva som er god nok sikkerhet. Det er vanskelig for enkeltvise virksomheter å få vurdert og verifisert hvilken sikkerhet som tilbys fra driftsleverandør.

Siden kundene til dels ikke vet å stille krav om sikkerhet, og leverandør ikke ønsker å prise seg ut av markedet med å tilby ekstra sikkerhet, innebærer dagens situasjon en ukjent risiko nasjonalt sett. I tillegg til at den enkelte virksomhet sannsynligvis sitter med en ukjent risiko.

Det synes derfor fornuftig at nasjonal strategi for informasjonssikkerhet setter krav til at driftsoperatører for å kunne tilby slike tjenester, sikkerhetsmessig må sertifiseres. Nasjonal ordning for sertifisering iht BS7799 er allerede på plass og forvaltet av Norsk Akkreditering. De krav om etablering av sikkerhetsadministrasjon som er pålagt virksomheter som behandler personopplysninger samsvarer med kravene i BS7799.

Et slikt krav om sertifisering vil gi viktig drahjelp både for enkeltvise virksomheter og nasjonalt sett. Dette ville ikke fjerne den enkelte virksomhets eget fokus og ansvar ifm håndtering av sikkerheten, og fremdeles vil hver enkelt måtte stille sine krav til sikkerhet til driftsoperatør. Man ville imidlertid oppnå et målbart krav rettet mot leverandører som er en viktig part for å styrke den nasjonale informasjonssikkerhet. Eksempler i grunnlagsdokumentet underbygger dette.

En slik sertifisering iht BS7799 vil videre i større grad fremtvinge at driftsoperatør på tilsvarende måte som krav om oppetid og levering av tjeneste, også vil måtte ha et tilsvarende fokus på sikkerhetskravene, for å kunne avtale tjeneste som skal leveres. Dette vil videre naturlig styrke den enkelte virksomhets fokus på bruk av risikovurdering som verktøy for av avklare sikkerhetsbehov.

Et krav om ansvar og fokus på internkontroll og sikkerhetsadministrasjon rettet mot operatørene, vil tilsvarende påvirke hver virksomhet. Dette vil totalt sett gi en bedre sikkerhet og risikohåndtering.

Vennlig hilsen
System Sikkerhet ASA

Heidi Thorstensen
sjefskonsulent