Det kongelige forsvarsdepartement
Postboks 8126 Dep
0032 OSLO
Deres referanse: 2010/00794-1/FD I5/OFD

Oslo, 24. juni 2010

Høringsuttalelse Nasjonal strategi for cybersikkerhet

Takk for anledningen til å kommentere det foreliggende utkast til strategi for cybersikkerhet.

SpareBank 1 deler vurderingen av behov for en nasjonal strategi for cybersikkerhet. Dette med tanke på hendelser som kan få kritiske samfunnsfunksjoner til å bryte sammen, og av hensyn til informasjon som av nasjonale grunner vurderes som sensitiv. SpareBank 1 deltok i øvelse IKT-08. Erfaringer fra øvelsen peker på behov for bedre nasjonal beredskap og koordinering av IKT- hendelser med store samfunnsmessige skadefølger. Vi ser derfor svært positivt på utarbeidelse av nasjonal strategi for cybersikkerhet.

SpareBank 1 er spesielt opptatt av beredskap mot hendelser som kan få IKT- systemer til å bryte sammen over en lengre periode. For eksempel gjennom DDoS -angrep mot våre IKT- systemer. Robuste IKT- systemer er av vesentlig betydning for de tjenester SpareBank 1 leverer våre kunder. Samtidig er internett en stadig større del av vår virksomhet blant annet fordi stadig flere av våre tjenester leveres til kunden på nettet.

Cyberstrategien beskriver begrepet "sårbarheter" og omtaler årsaker til at sårbarheter oppstår. Vår vurdering er at mangelfull kravstilling og oppfølging av sikkerhet ved utvikling og endring av IKT- systemer er en vesentlig årsak til at sårbarheter oppstår. Gode kvalitetssystemer med krav til sikkerhet og verifikasjon av sikkerheten er avgjørende. Vi er for øvrig enig i at økt grad av sammenkopling av systemer bidrar til økt kompleksitet. Økt grad av sammenkopling stiller derfor høye krav til modenhet for virksomhetenes IKT- styringssystemer (IKT Governance).

Etablere en felles situasjonsoversikt og forståelse
SpareBank 1 ser positivt på kartlegging og verdivurdering av kritiske IKT- systemer i alle sektorer. Samtidig er det viktig at eventuelle krav som stilles til slike systemer ikke forhindrer konkurranse i markedet, favoriserer internasjonale aktører som leverer tjenester i det norske markedet eller svekker konkurransen mellom IKT- leverandørene.

Vi er enig i at en felles situasjonsoversikt og forståelse forutsetter målrettet satsning på forskning og utvikling. Denne type forskningsprosjekter er etter vår vurdering velegnet for offentlig/ privat samarbeid. Vi mener imidlertid at strategien bør peke på mer konkrete områder hvor forskning er påkrevet for å bedre cybersikkerhet. Etter vår mening er det behov for mer kunnskap om aktive trusselaktører og organisert IKT- kriminalitet. Det er også behov for kunnskap om hvordan langsiktige internasjonaliseringstrender påvirker sikkerhetsrisiko og aktuelle virkemidler for å ivareta nasjonal beredskap i en internasjonal IKT- verden.

Internasjonalt samarbeid vil etter vår vurdering være avgjørende for å lykkes. Vi er enig i at Norge bør være pådriver for internasjonal harmonisering og regulering av cybersikkerhet, herunder internasjonalt forpliktende samarbeid.

NSMs åpne trusselvurdering bidrar til økt forståelse og kompetanse om trusselbildet. Finansnæringen drar allerede nytte av NSMs kompetanse ved utarbeidelse av sektorspesifikke trusselvurderinger. Det bør samtidig som skjermingsbehov ivaretas, vurderes om man i større grad enn i dag kan systematisere informasjonsdeling for å få en så god trusselforståelse som mulig.

I strategien blir det foreslått å stille felles krav til kritiske IKT- systemer. SpareBank 1 mener man fremfor å stille felles krav, bør lage veiledninger, beste praksisbeskrivelser og anbefalte krav. Eventuell kravstilling kan vurderes dersom veiledning ikke viser seg effektivt. SpareBank 1 har gode erfaringer samarbeid på tvers av offentlig og privat sektor blant annet gjennom samarbeid med NorCert og NorSIS. Samarbeid med NorCert er verdifullt fordi SpareBank 1 får tilgang til spesialistkompetanse samtidig som NorCert får forståelse av reelle sikkerhetsbehov i finansnæringen. Vi har tilsvarende gode erfaringer med NorSIS. Vi ser positivt på videreutvikling av offentlig-privat samarbeid basert på modeller fra disse aktørene.

SpareBank 1 ser et behov for å heve basiskompetansen om informasjonssikkerhet i samfunnet generelt. Både barnehager, skoler og eldresentre er eksempler på arenaer som kan benyttes som utgangspunkt for å heve kompetansen, slik at alle oppnår basiskompetanse på området.

Bevisstgjøre, opplyse og påvirke
Strategien legger stor vekt på opplysning av brukere. Videre peker man på behov for sikkerhetsforståelse hos driftspersonell og på behov for økt bevissthet i organisasjoner om betydningen av sikkerhetskultur i organisasjonen. SpareBank 1 mener strategien i større grad må vektlegge behovet for ledelsesforankring av informasjonssikkerhet. Det er tilsvarende avgjørende at sikkerhetsansvar forankres på forretningssiden i virksomhetene. Det er normalt forretningssiden som har "bestiller- rollen" i henhold til moderne IKT styringssystemer. Det er derfor svært viktig den bevisstgjøres sitt sikkerhetsansvar. Vi er samtidig enig i at brukere og driftspersonell vil ha nytte av økt sikkerhetskompetanse. Vi mener imidlertid tiltak for å styrke informasjonssikkerhet og kampanjer også må rette seg mot ledere og personer med "bestillerrolle" i virksomhetene.

Styrke evnen til å oppdage, varsle og håndtere IKT- hendelser
Den nasjonale operative koordineringen av dataangrep mot Norge er i dag lagt til NorCert. I enkelte sektorer er det etablert CSIRT- miljøer. SpareBank 1 ser behov for nærmere vurdering av behovet for eget CSIRT- miljø i finansnæringen. Det bør alternativt vurderes å styrke NorCert styrkes med personell som kan ha et særlig ansvar for koordinering mot finansnæringen.

SpareBank 1 har for øvrig gode erfaringer med hendelsesrapportering til Finanstilsynet. Vi oppfordrer til å bygge videre på allerede etablert rapportering til Finanstilsynet for varsling og håndtering av IKT- hendelser i finansnæringen.

Etterforske og bekjempe IKT- kriminalitet
SpareBank 1 er enig i at kompetanse og evne til å etterforske og håndtere målrettede dataangrep må styrkes. Etterforskning av datakriminalitet må prioriteres også for mindre hendelser. Dette for å bygge kompetanse på etterforskning og være forberedt for eventuell håndtering av mer alvorlig kriminalitet. Vi er enig i at etterforskning av datakriminalitet krever spesialistkompetanse. Vi savner en vurdering av om politiet i dag er organisert tilstrekkelig hensiktsmessig med tanke på effektiv etterforskning av datakriminalitet.

Styrke samordningen av cybersikkerhet
SpareBank 1 ser behovet for å samordne cybersikkerhetsarbeidet. Etablering av nasjonalt cybersenter som foreslått i strategien, vil etter vår vurdering bidra til å styrke cybersikkerhetsarbeidet. SpareBank 1 stiller seg positiv til å bidra som privat samarbeidspart i en slik modell både med fagkompetanse og ressurser. Vi vil også være med på å påvirke finansnæringen gjennom våre interesseorganisasjoner, til å bidra i et slikt samarbeid.

Med vennlig hilsen
Eivind Gjemdal
Konserndirektør IT
SpareBank1 Gruppen AS