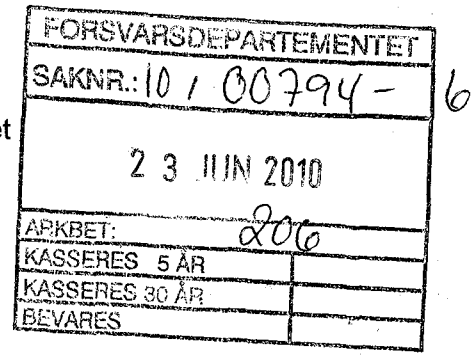
difi Direktoratet for forvaltning og IKT

Vår dato	Vår referanse
18.juni 2010	10/283
Deres dato	Deres referanse
30. mars 2010	2010/00794-1/FD I 15/OFD

Forsvarsdepartementet
Postboks 8126 Dep

0032 OSLO



Høringsuttalelse: Forslag til strategi for cybersikkerhet

Difi viser til Deres høringsbrev av 30. mars med forslag til nasjonal strategi for cybersikkerhet. Strategien konkretiserer og utdyper de nasjonale retningslinjene for informasjonssikkerhet for den del som gjelder de mest samfunnskritiske systemer.

Difi tiltrer oppfatningen om at det er nødvendig med en helhetlig nasjonal strategi, og er i all hovedsak positivt til forslaget. Strategiens seks hovedmål og forslagene til tiltak synes i hovedsak å være vel begrunnede og fornuftige. Det fremstår som hensiktsmessig å bygge på de nasjonale retningslinjene for informasjonssikkerhet, og at det også retter seg mot forebygging og håndtering av alvorlige IKT-hendelser. Difi har likevel noen synspunkter på enkelte områder.

Når det gjelder bruk av det norsk-engelske ordet "cybersikkerhet" er Difi skeptisk. Offentlig sektor bør søke å benytte alternative norske ord og begreper i denne type dokumenter. Difi kan for øvrig ikke se at begrepet reelt sett favner videre, eller er lettere tilgjengelig, enn det nå velkjente og innarbeidede "informasjonssikkerhet".

Kriterier for identifisering av "samfunnskritisk infrastruktur", eller "samfunnskritisk funksjon" har vært på agendaen fra sårbarhetsutredningen i 1986 ("Seip-utvalget", NOU 1986:12, *Datateknikk og samfunnets sårbarhet*). Strategiens mål om å etablere en felles situasjonsoversikt og forståelse, fremstår derfor som hensiktsmessig.

I tiltak nr. 6, om å stille felles krav til kritiske IKT-systemer, presiseres at virksomhetene bør anskaffe godkjente og veldokumenterte løsninger ved å bruke etablerte sertifiseringsordninger og følge anerkjente internasjonale standarder. Det pekes på SERTIT under NSM og ISO/IEC 27001. Omtrent tilsvarende kommer også til uttrykk i de nasjonale retningslinjene for informasjonssikkerhet 2007-2010, punkt 3.7.

Difi mener tiden er moden for å stille konkrete krav om at samfunnsviktige funksjoner må følge tiltak nevnt i nr 6 og retningslinjene punkt 3.7, eventuelt som et krav om selv å vurdere dette, i den enkelte konkrete anskaffelsesprosessen. Et pålegg bør ikke være uforholdsmessig belastende for virksomheten, eventuelt bør kompensasjonsordning vurderes.

Hva som gir best effekt, enten det gjelder pålegg eller andre tiltak som styringsmiddel for sentrale myndigheter, bør etter Difis mening vurderes nærmere. Det er usikkert om et eksternt krav om sertifisering vil fungere mer effektivt enn om virksomheten selv rår over en slik beslutning – basert på egen sikkerhetsstrategi og risikoanalyse. Et eksternt krav kan være at

Direktoratet for Forvaltning og IKT (Difi)
Postboks 8115 Dep, 0032 Oslo
Telefon: 22 45 10 00

Besøksadresse Oslo:
Sandakerveien 24C,
inngang D 9, 4. etasje
Telefaks Oslo: 22 45 10 01

Besøksadresse Leikanger:
Skrivarvegen 2
Telefaks Leikanger: 57 65 50 55

postmottak@difi.no
Org.nr.: NO 991 825 827
www.difi.no

virksomheten må ha gjennomført en selvstendig vurdering av behovet for og eventuelt valg av sertifisert løsning. En slik vurdering kan kreves begrunnet og dokumentert på vanlig måte, for virksomhetens egen kontroll og eventuelt tilsyn.

Difi, ved Standardiseringrådet, er nå for øvrig i ferd med å vurdere aktuelle standarder for informasjonssikkerhet til inkludering i Referansekatalogen, enten som obligatoriske eller anbefalte standarder, for offentlig sektor, men uten at det der skilles mellom "normale" og kritiske IKT-systemer.

IKT-systemer bundet sammen i cyberspace er som sådan preget av internasjonale rettslige premisser. Difi tiltrer antakelsen om behov for regulatorisk forankring av cybersikkerhet, slik det er foreslått i tiltak nr. 10. Det savnes imidlertid en noe mer konkret beskrivelse av hva problemet antas å være, hva som mangler rettslig forankring, eventuelt hvilke regelverk som antas ikke å være oppdatert, samt en vurdering av hva som kan antas å gi en løsning. Endring av rettslige parametre som vil kunne påvirke relasjonene til andre stater bør skje i regi av kompetente internasjonale organer, ikke minst gjelder dette hvis eventuelle endringer kan ha berøringsflater mot menneskerettighetene. Sikkerhetstiltak trenger normalt ikke eget rettsgrunnlag med mindre tiltakene er egnet til å begrense borgernes rettigheter, eller det ønskes å gi pålegg utover rammen av instruksjonsmyndighet.

Difi er positiv til forslaget om nedsettelse av et utvalg, eventuelt arbeidsgruppe, for helhetlig gjennomgang av eksisterende relevant regelverk. En gjennomgang hvor fokus også rettes mot samordning og ensartede begreper, vil kunne gjøre helheten i regelsettene lettere tilgjengelig. Direktoratet er imidlertid usikkert på om det er behov for ny lov på feltet. Ved en slik gjennomgang vil det være naturlig å bygge på eller se hen til det arbeidet som Koordineringsutvalget for informasjonssikkerhet (KIS) allerede har gjort.

Difi vil også peke på behovet for at det allerede ved utformingen av nasjonal strategi ses hen til sammenhengen mellom eksisterende regelverk og ansvarsområder, og det nye en ønsker. I strategiutkastet uttrykkes at mye av dette må følges opp med mer detaljerte handlingsplaner, med identifisering og involvering av aktuelle interessenter/aktører. Dette tror Difi innebærer en for sen forankring av en så overgripende strategi. Difi er av den oppfatning at det er en forutsetning for en omforent strategi og oppfølging av den, at de mest sentrale aktørene deltar i arbeidet og får "medeierskap" i strategien, ikke bare i oppfølgende handlingsplaner. I utkastet kunne med fordel derfor de mest sentrale områdene vært identifisert og omtalt, og en type samarbeid gjennomført.

Begrepet "andre vitale nasjonale sikkerhetsinteresser" er dekkende for viktige samfunnsfunksjoner, kritisk IKT-infrastruktur og andre viktige deler av "cyberspace". På mange av disse sektorområdene finnes det egne lov- og forskriftsverk, myndighetsorganer og tilsynsorganer, som tar ansvar for også de kritiske IKT-systemene på sine områder. Disse nevnes i strategiforslaget, men bare i begrenset utstrekning, og uten å trekke sammenhengen til sikkerhetsloven.

I tråd med forslaget mener Difi at det er viktig at det legges til rette for en effektiv etterforskning av denne form for datakriminalitet. Det internasjonale samarbeidet er sentralt, og en eventuell harmonisering av regelverket og forenkling av internasjonal etterforsking kan være et ledd i utviklingen av dette. Forslagets punkt 17 og 18 reiser enkelte av de samme problemstillingene som omtalt under punkt 10 ovenfor.

Sikkerhetsmyndighetene har allerede relativt vide fullmakter. Eventuelle endringer av det rettslige grunnlaget for etterforskning av datakriminalitet vil være komplisert, og forutsetter at kravene til åpenhet, forutberegnelighet og demokratihensyn ivaretas. At også

personvernhensyn ivaretas er viktig for at tjenestene skal ha den nødvendige tillit i samfunnet. De offentlige debattene knyttet til det såkalte datalagringsdirektivet og arbeidet med Instruks for sikkerhetstjenestene i forsvaret kan være nyttige innspill også i denne sammenheng.

I tilknytning til forslagets punkt 22 konstateres at det er behov for en operativ funksjon knyttet til ivaretakelse av cybersikkerhet, og det foreslås å etablere et nasjonalt cybersenter. Funksjonen ønskes rettet mot nye og endrede behov. De tre tjenestene NSM, PST og E-tjenesten har funksjoner fra tilstøtende virksomhetsgrunnlag. Begrunnelsen for, og i hvilken grad det er behov for, å opprette et eget senter for å bringe relevante deler av tjenestenes virksomhet tettere sammen, fremstår ikke som innlysende i forslaget. Det er også noe uklart hvordan denne funksjonen skal organiseres og hvilke oppgaver det eventuelt skal utføre. Det er derfor vanskelig å gi kvalifisert vurdering av forslaget for denne del. Spørsmålet om etablering av et nytt organ bør også ses i sammenheng med spørsmålene om ny rettslig regulering, og eventuelle behov som måtte vise seg i den forbindelse. Difi antar også at øvrige viktige sektormyndigheter bør vurderes tett opp mot et slikt fornyet, nasjonalt senter for cybersikkerhet.

Strategiforslaget kunne med fordel vært tydeligere på om det foreslår endringer i det eksisterende regelverket på strategiens ansvarsområder. Det er etter vårt skjønn vanskelig å se hva strategien tilbyr eller "pålegger", som ikke allerede er regulert av gjeldende regelverk. Sammenhengen mellom forslaget til strategi og eksisterende regelverk ville videre vært lettere tilgjengelig dersom det hadde vært knyttet opp mot de viktigste ansvarsgrensene på strategiområdet slik de er i dag, og dermed identifisert tydeligere hva som er nytt med forslaget.

Difi er enig med NSM i at det er ønskelig med en sterkere samordning på cybersikkerhetsfeltet enn i dag.

I oversikten over *eksisterende roller, ansvar og myndighet nasjonalt (vedlegg A),* bør for øvrig Difi nevnes under FAD og FADs ansvar. FAD har som kjent forvalteransvar for flere sentrale forskrifter med krav om ivaretakelse av informasjonssikkerhet med grunnlag i sikkerhetsstrategi og risikovurderinger. Difi bidrar til å operasjonalisere regjeringens politikk på bl.a. e-forvaltningsområdet, inkludert informasjonssikkerhet. Ved siden av e-forvaltnings- og rådgivningstjenester, har Difi utviklings- og driftsansvar for enkelte viktige forvaltningstjenester i "cyberspace", herunder felles autentiseringsløsninger for det offentlige (MinID og ID-porten).

Vennlig hilsen
for Difi

FOR Tone Bringedal
avdelingsdirektør

Sverre Engelschiøn
seniorrådgiver

Kopi: FAD, Pb 8004 Dep, 0030 Oslo