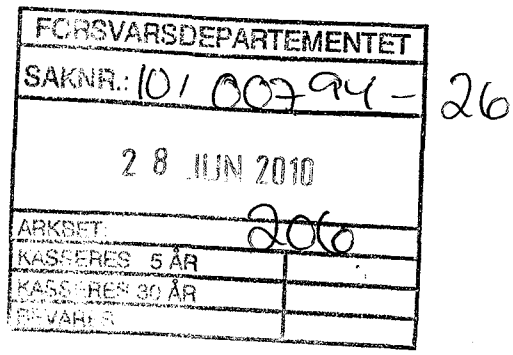
DET KONGELIGE FORNYINGS-,
ADMINISTRASJONS- OG KIRKEDEPARTEMENT



Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Deres referanse	Vår referanse	Dato
2010/00794-1/FD I 5/OFD	201001472-/NZM	24.6.2010

Høring – forslag til strategi for cybersikkerhet

Vi viser til Forsvarsdepartementets brev av 30.03.2010 om ovennevnte.

Fornyings-, administrasjons- og kirkedepartementet (FAD) mener det er positivt at strategien legger opp til en helhetlig beskyttelse av IKT- systemer, og fokuserer på samordning og sektorovergripende tiltak. Ut fra et personvernperspektiv er det svært viktig med sikkerhetsløsning som fungerer på tvers av sektorer. I den grad sikkerhetsløsningene skal ivareta personopplysninger må dette skje på lik linje uavhengig av hvilke sektor en befinner seg innenfor. Økt samhandling på tvers av sektorer innebærer en økt grad av informasjonsutveksling og økte informasjonsmengder innen hver sektor, hvilket nødvendiggjør gode løsninger for informasjonssikkerhet.

Det er videre positivt at strategien fokuserer både på forebygging og effektiv håndtering av hendelser. Man vil alltid måtte ta høyde for at informasjon kan lekke, og dersom dette skjer, er det avgjørende at det finnes systemer som effektivt avverger at personopplysninger sprer seg. Cyberbaserte løsninger blir i stadig større grad tatt i bruk. Det benyttes flere nye teknologiske lagringsformer, for eksempel "cloud computing" som innebærer internettbasert lagring. Det er derfor viktig at det kommer tydelig informasjon til allmennheten om økte sikkerhetstrusler, og hvordan disse i størst mulig grad kan forhindres og avhjelpes. At behandlingsansvarlig har kunnskap om eksisterende trusler er etter FADs syn av stor betydning for å kunne forhindre utilsiktede hendelser.

Nasjonal sikkerhetsmyndighet (NSM) peker på et behov for en helhetlig gjennomgang

Postadresse	Kontoradresse	Telefon	Administrasjonsavdelingen	Saksbehandler
Postboks 8004 Dep	Akersg. 59	22 24 90 90	Telefaks	Anne Kristine Hage
N-0030 OSLO		Org no. 972 417 785	22 24 27 14	22 24 48 51

av eksisterende relevant regelverk og foreslår at det bør nedsettes et lovutvalg som ser på rettslige aspekter knyttet til cybersikkerhet. FAD mener et lovutvalg som foreslått kan ha gode grunner for seg.

FAD har følgende merknader til strategidokumentet:

Om bruken av enkelte kjernebegreper (jf. side 5 i dokumentet)
I strategien lanserer NSM begrepet *"cybersikkerhet"*. Innholdet i begrepet er ment å gjenspeile samfunnets stadig økende avhengighet av IKT-systemer bundet sammen i cyberspace. Ordet cybersikkehet er – i norsk sammenheng – relativt nytt. Meningsinnholdet i begrepet er derimot godt kjent for dem som arbeider med informasjonssikkerhet. Innføring av et nytt sikkerhetsord for en allerede kjent tilstand bidrar til å skape en kommunikasjonsutfordring. Dette gjelder spesielt overfor eksterne aktører som ikke forholder seg til dette fagområdet til daglig. Disse aktørene vil sannsynligvis ha et problem med å forstå forskjellen mellom begrepene cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet. Dersom det på et senere tidspunkt blir besluttet at det skal lanseres nye nasjonale retningslinjer for informasjonssikkerhet, kan det raskt kunne komme spørsmål fra disse aktørene om hvorvidt det er behov for dette ettersom det allerede foreligger en nasjonal strategi for cybersikkerhet. FAD ber derfor NSM vurdere hvorvidt det er mulig å bruke et mer anerkjent sikkerhetsbegrep for å beskrive formålet med strategien.

NSM bruker definisjonen "kritiske IKT-systemer" for å beskrive de systemene som kritiske samfunnsfunksjoner er avhengig av. Av hensyn til kommunikasjon med eksterne aktører anbefaler FAD NSM å presisere at deres strategi primært er opptatt av å beskytte det som kan defineres som *samfunnskritiske IKT-systemer*, og ikke det som kan betegnes som virksomhetskritiske IKT-systemer, med mindre disse har en samfunnsviktig funksjon eller betydning.

Ad. Pkt. 1.2. Forholdet til Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010.
Den nasjonale strategien for cybersikkerhet konkretiserer og utdyper de nasjonale retningslinjene for informasjonssikkerhet på innsatsområdet knyttet til beskyttelse av de mest samfunnskritiske systemer.

Det kan være formålstjenlig med en oversikt over hvilke innsatsområder på informasjonssikkerhetsområdet som blir ivaretatt helt eller delvis av cybersikkerhetsstrategien. Mange av temaene som blir omtalt i strategien, herunder bevisstgjøring, varsling, rådgivning og styrket samordning, kan gjenfinnes i nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010, om enn i noe forskjellig form og betoning når det gjelder tilnærming og tiltak. Ved hjelp av en oversikt over hvilke tema og tiltak som er dekket av cybersikkerhetsstrategien vil en lettere kunne se hvilke innsatsområder som gjenstår – og som eventuelt må revurderes – i forbindelse med eventuell utvikling av nye nasjonale retningslinjer på området.

FAD mener at Koordineringsutvalget for informasjonssikkerhet (KIS) er en passende arena for en gjennomgang og sammenstilling av disse dokumentene. Prosessen bør starte når en endelig cybersikkerhetsstrategi har blitt fastsatt av Forsvarsdepartementet og Justisdepartementet.

Om roller og ansvar for forebyggende IKT-sikkerhet
NSM legger opp til at strategiforslaget skal følges opp med mer detaljerte handlingsplaner. I denne forbindelse legger direktoratet opp til å identifisere og involvere aktuelle interessenter – både private og offentlige aktører – som utvikler, regulerer, drifter, eier, eller er brukere av kritiske IKT-systemer.

I denne prosessen kan NSM komme i berøring med FADs samordningsansvar for forebyggende informasjonssikkerhet. FAD ber derfor om at det legges opp til en dialog mellom NSM og FAD i forbindelse med utarbeidelse av handlingsplanene slik at eventuelle uklarheter omkring roller og ansvar for samordning av informasjonssikkerhet kan få en rask avklaring.

Ad. tiltak 22 Etablere et nasjonalt cybersenter
FAD støtter NSMs forslag om å etablere et nasjonalt cybersenter. Det er viktig at NorCERT-konseptet og Varslingssystem for digital infrastruktur (VDI) videreutvikles slik at Norge til enhver tid har tilstrekkelig kapasitet og kompetanse til effektivt å håndtere og respondere på alvorlige IKT-hendelser og -situasjoner som kan true samfunnets stabilitet generelt eller samfunnskritiske funksjoner spesielt.

Med hilsen

Marianne Haugan Molstad (e.f.)
avdelingsdirektør

Anne Kristine Hage
rådgiver