DET KONGELIGE
SAMFERDSELSDEPARTEMENT

Forsvarsdepartementet

Postboks 8126 Dep
0032 OSLO

Deres ref	Vår ref	Dato
2010/00794-1/FD I 5/OFD	10/662- HK	24.06.2010

Forslag til strategi for cybersikkerhet - Høring

Vi viser til brev av 30. mars 2010 om forslag til strategi for cybersikkerhet.

Nasjonal sikkerhetsmyndighets (NSM) forslag til strategi er en konkretisering av innsatsområdet "Samfunnskritisk IKT-infrastruktur må beskyttes bedre" i *"Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010"*.
Samferdselsdepartementet er en av utgiverne av de nevnte retningslinjer og er følgelig godt kjent med de ulike innsatsområdene som retningslinjene skisserer. På lik linje med andre sektormyndigheter har vi iverksatt tiltak og vi vil komme til å foreslå regelverksendringer blant annet med tanke på oppfølging av retningslinjene.

Samferdselsdepartementet har det regulatoriske ansvaret for IKT-sikkerhet innenfor hele samferdselssektoren, og vi har flere virksomheter innenfor vår sektor som har samfunnskritiske IKT-systemer. Vi er myndighet med ansvar for elektronisk kommunikasjon og regulerer den sektoren som eier og drifter den basisinfrastruktur og de tjenestene som ligger til grunn for all aktivitet på nett.

Generelle merknader

Samferdselsdepartementet stiller spørsmål ved at NMS har valgt å bruke begrepet "cybersikkerhet". Dette er etter vårt syn et lite innarbeidet begrep på et meningsinnhold som er godt kjent i det norske samfunnet. Det å bruke et delvis engelsk uttrykk mener vi er uheldig, og vi tilråder at NSM forsøker å finne et mer kjent norsk begrep.

Postadresse:
Postboks 8010 Dep
0030 OSLO

Kontoradresse:
Akersg. 59
www.regjeringen.no/sd

Telefon
22 24 90 90 / 22248353
Org. nr.:
972 417 904

Luft- post- og
teleavdelingen
Telefaks:
22 24 56 09

Saksbehandler:
Heidi Karlsen
22 24 81 48

Høringsinstansene er bedt om å kommentere hvorvidt man mener strategien er dekkende innenfor sin sektor, og innenfor områder som ikke ligger under NSMs ansvarsområde. Samferdselsdepartementet stiller spørsmål ved at høringsinstansene skal kommentere det som ligger utenfor NSMs ansvarsområde. NSMs ansvar er i henhold til sikkerhetsloven og det er NSM som har utformet utkast til strategi. Vi antar at det vil være NSM som i fremtiden vil få i oppgave å forvalte strategien. Strategien bør i så fall kun omfatte virksomheter som omfattes av sikkerhetsloven. Grunnlaget for at høringsinstansene skal vurdere om strategien er dekkende også for det som faller *utenfor* NSMs ansvarsområde er derfor uklart og må klargjøres. Grenseflaten og forholdet mellom cybersikkerhet og øvrig IKT-sikkerhet er etter vårt syn heller ikke tilfredsstillende forklart i strategien. Utgangspunktet er, som nevnt ovenfor, ett av flere innsatsområder som de nasjonale retningslinjene skisserer, men det kan virke som om strategien favner også andre innsatsområder som for eksempel varsling og hendelseshåndtering.

Vi har merket oss at strategien skal følges opp med mer detaljerte handlingsplaner, og at aktuelle interessenter skal involveres i arbeidet med disse planene. Forslaget til strategi kan kritiseres for at det i liten grad fremgår hvem som har ansvar for tiltakene. Vi oppfatter imidlertid strategien slik at ansvaret for tiltakene vil bli plassert senere. Det er de store linjene som skisseres i strategien, mens de mer konkrete tiltakene og handlingene vil bli uformet senere. Vi forutsetter da at i den grad ekomsektoren involveres i handlingsplanene, vil Samferdselsdepartementet bli underrettet om dette.

Merknader til enkelte kapitler i strategien

Til kap 1.2
Midt på siden er det utarbeidet en illustrasjon som viser hvordan den nasjonale strategien for cybersikkerhet utdyper de nasjonale retningslinjene. Samferdselsdepartementet mener denne illustrasjonen ikke er helt heldig i den forstand at man kan få inntrykk av at de nasjonale retningslinjene springer ut av strategien og ikke omvendt. Vi viser i den forbindelse til diskusjonen i KIS-møte 5. mai, hvor nettopp rangordningen mellom disse to dokumentene ble påpekt. Vi tilrår at det blir utarbeidet en illustrasjon som viser denne rangordningen.

Til kap 1.3
Det fremgår av avsnittet at det er forutsatt at EU tar sikte på å innta IKT-sektoren i ECIP-direktivet på et senere tidspunkt. Samferdselsdepartementet vil i den forbindelse vise til det pågående arbeidet i DG INFSO i EU-kommisjonen når det gjelder utveksling av informasjon og beste praksis om sikkerhet og beskyttelse av kritisk informasjonsinfrastruktur (CII). Post- og teletilsynet er bedt av Samferdselsdepartementet om å følge dette arbeidet. Oss bekjent har også NSM tidvis deltatt i arbeidet. Etter vår oppfatning bør dette arbeidet følges videre for å sikre en viss

harmonisering når det gjelder kriterier som skal identifisere og kategorisere kritisk IKT-infrastruktur.

Til kap 2.1
Det fremgår av andre avsnitt i pkt 1 at *"Post- og teletilsynet (PT) på sin side arbeider med prioriteringsordninger knyttet til elektroniske informasjonssystemer"*. Det er uklart for Samferdselsdepartementet hva som menes her. Post- og teletilsynet foretar en kontinuerlig kartlegging av den viktigste infrastrukturen for elektronisk kommunikasjon i Norge. Denne kartleggingen er viktig for at ekommyndigheten i samarbeid med tilbyderne av ekomnett og -tjenester skal kunne iverksette nødvendige sikkerhets- og beredskapstiltak.

Til kap 2.2
Under pkt 7 fremgår det at tilsyn med IKT-sikkerhet gjennomføres i dag av flere myndighetsorganer som i liten grad utveksler tilsynserfaringer. Knyttet til dette er det viktig å minne om at IKT-sikkerhet gjerne inngår som en del av det øvrige tilsynet som våre tilsyn utfører. Innenfor ekomsektoren er det en noe annen praksis og Post– og teletilsynet har for eksempel samarbeidsavtaler både med Datatilsynet og NSM. Det er imidlertid departementets oppfatning at det er rom for forbedringer når det gjelder samordning av tilsyn.

Under pkt 10 fremmes det forslag om at det bør settes ned et lovutvalg som skal se på de rettslige aspekter knyttet til cybersikkerhet. Samferdselsdepartementet mener man i vurderingen av behovet for et slikt utvalg må se hen til hva som allerede er gjort, blant annet av Datakrimutvalget, innenfor dette feltet.

Til kap 2.4
Under pkt 13 foreslås det å utvide omfanget av Varslingssytem for Digital Infrastruktur (VDI) til å dekke en større andel av virksomheter med kritiske IKT-systemer. Samferdselsdepartementet antar det her er ment å skulle stå virksomheter med *samfunnskritiske* IKT-systemer og i så fall er vi enig i dette forslaget. Vi ser ingen grunn til å skulle utvide VDI til å gjelde alle virksomheter med virksomhetskritisk IKT-infrastruktur. Det vil være å gå langt utenfor det mandat vi mener VDI bør ha. For øvrig vil vi påpeke at så lenge det koster noe å delta i VDI-samarbeidet, vil en slik utvidelse måtte være basert på frivillighet for de private aktørene man ønsker å inkludere.

Til kap 2.5
Under pkt 17 om lagring av data. Samferdselsdepartementet ser at det er utfordringer knyttet til etterforskning av datakriminalitet, og at det er behov for data for å kunne gjøre en god etterforskning. Politiet har i dag tilgang til data som er lagret hos tilbydere av ekomnett og -tjenester for fakturerings- og kommunikasjonsformål. Hvorvidt regelverket for lagring/sletting av data og tilgang til data skal endres, er gjenstand for stor debatt i det norske samfunnet. Det er ut fra et personvernperspektiv betenkelig

med lagring av data til kriminalitetsbekjempende formål. Vi viser for øvrig til debatten om eventuell innføring av EUs datalagringsdirektiv i norsk rett.

Under pkt 20 om offensive kapasiteter vises det til at Forsvaret har en viss kapasitet for å påvirke en motstanders informasjonssystemer. Uten at vi vet hvilke kapasiteter det her siktes til, ønsker vi å påpeke at kapasiteter som påvirker andres informasjonssystemer ofte har den sideeffekt at det rammer uskyldige brukere av elektronisk kommunikasjon, og at denne inngripen i den vanlige borgers rett til fri kommunikasjon, ikke må tilsidesettes i bestrebelsene på å styrke den nasjonale evnen til etterretning og kontraetterretning.

Under pkt 22, aller siste avsnitt understrekes det at nærhets-, likhets- og ansvarsprinsippene fortsatt skal være styrende i forhold til beredskapsarbeidet. Samferdselsdepartementet forutsetter at også krisehåndteringen, IKT-kriser inkludert, i fremtiden skal følge de samme prinsippene.

Med hilsen

Jørn Ringlund e.f.

Heidi Karlsen