DET KONGELIGE
ARBEIDSDEPARTEMENT



Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

| Deres ref | Vår ref | Dato |
|---|---|---|
| 2010/00794-1 | 201001462-/AHE | 25.06.2010 |

**Svar på høring om forslag til strategi for cybersikkerhet**

Vi viser til brev fra Forsvarsdepartementet av 30. mars 2010 om overnevnte tema. Arbeidsdepartementet (AD) har forelagt høringen for underlagte virksomheter og vi gir med dette en samlet tilbakemelding fra vår sektor.

## 1. Generelle merknader

På bakgrunn av samfunnets økende avhengighet av oppegående IKT-systemer mener AD at det er behov for en overordnet nasjonal tilnærming på cybersikkerhet. En realisering av strategiforslaget vil kunne medvirke til en styrket samfunnsmessig evne til å motstå angrep på vår IKT-infrastruktur, en begrensning av skadeomfanget ved et eventuelt angrep og til en raskere gjenoppbygning av systemer.

De skisserte hovedmålene fremstår som dekkende, og de 22 foreslåtte tiltakene virker i utgangspunktet hensiktsmessige for å sikre en helhetlig nasjonal tilnærming for cybersikkerhet. Det er imidlertid noe uklart hvem som skal gjøre hva under de ulike tiltakene, og AD ber om at dette klargjøres i det videre arbeidet. Dette gjelder blant annet ansvarsfordelingen mellom defensive og forretningsmessige virksomheter og rene forsvarsmessige deler.

## 2. Merknader til forslaget om hovedmål og tiltak

### *Ad hovedmål 1 – Etablere en felles situasjonsoversikt og forståelse*

Det fremgår i begrunnelsen for dette hovedmålet at *"Alle samfunnsfunksjoner i dag er sterkt avhengig av velfungerende IKT-systemer"*. Vi mener at det i tillegg til IKT-systemer også bør fremgå infrastruktur og tjenester i denne sammenheng.

Postadresse
Postboks 8019 Dep
0030 Oslo

Kontoradresse
Einar Gerhardsens plass 3

Telefon
22 24 90 90
Org no.
983 887 457

Administrasjons- og
utviklingsavdelingen
Telefaks
22 24 87 11

Saksbehandler
Ann Kristin Henriksen
22248429

Det fremgår videre at det skal *"etableres prosesser for å identifisere de mest kritiske IKT-systemene, som representerer den største sårbarheten (...)"* Vi tilrår at en også starter med prosesser som er samfunnskritiske og sektorkritiske.

Tiltak 1. Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer
Under dette tiltaket fremgår det at en bør iverksette en *"løpende verdivurdering av kritiske IKT-systemer i alle sektorer."* Vi mener at begrepet "verdivurdering" her er noe uklart og at det kan bli litt for snevert. Et objekt kan være av relativt lav verdi, men kan utgjøre et stort skadepotensial og dermed få et høyt beskyttelses- og sikkerhetsbehov. På denne bakgrunnen mener vi en bør vurdere et begrep som kan favne bredere, og som favner selve skadepotensialet eller sikkerhetsbehovet.

Tiltak 3. Styrke kapasitet for vedlikehold og formidling av IKT-risikobildet
Det fremgår at *"Kunnskap om IKT-risikobildet er viktig med tanke på cybersikkerhetsarbeidet generelt (...)"* Vi mener at det her bør understrekes at også forståelse av risikobildet er sentralt med tanke på risikobildet knyttet til cybersikkerhet. Videre vil vi påpeke at det er viktig å legge til rette for en dekkende og presis rapportering fra sektorene om saken.

Tiltak 4. Styrke det internasjonale samarbeidet om cybersikkerhet
Det fremgår at *"Norge må søke å inngå i et forpliktende internasjonalt samarbeid for effektiv håndtering gjennom informasjonsdeling, men også etterforskning og straffeforfølging av kriminell aktivitet."* Vi mener det er noen uklarheter når det gjelder etterforskningsdelen i dette. Punktet griper også inn i juridiske problemstillinger, som er et krevende arbeidsfelt når det gjelder harmonisering og samarbeid. Det bør vurderes en avklaring av hva som skal være tillatt etterforskning/etterretning for ulike aktørtyper.

***Ad hovedmål 2 – Bygge og opprettholde robuste og sikre IKT-systemer***
Ingen av tiltakene under hovedmål 2 trekker fram noen potensiell eller aktuell ansvarshaver. I større grad enn under flere av de andre tiltakene er det derfor uklart hvem som er/bør være ansvarlig for iverksetting og gjennomføring. Dette vil kunne vanskeliggjøre en videreutvikling og oppbygging av samordnende løsninger mellom ulike sektorer og myndighetsorganer. Vi mener derfor at det for tiltakene 6. til og med 10. er et særlig behov i det videre arbeidet å klargjøre hvem som bør gjøre hva.

Tiltak 6. Stille felles krav til kritiske IKT-systemer
I tråd med våre innledende merknader til hovedmål 1 mener vi at også dette tiltaket bør suppleres med krav til infrastruktur og tjenester.

Tiltak 7. Styrke tilsyn med IKT-sikkerhet
Vi mener at de ulike tilsyn bør søke å bidra til en samlet fremstilling av utfordringer knyttet til prosessene internt i virksomhetene. Hvem som har ansvar for å initiere en slik samlet gjennomgang på tvers av tilsynene bør komme fram. En samlet fremstilling

kan bidra til kompetanseoverføring og gi de enkelte etater et godt grunnlag til å forbedre interne prosesser. Det bør derfor fremheves at styrket tilsyn med IKT-sikkerhet også har en kompetansehevende rolle.

Tiltak 9. Videreutvikle beredskapsplaner med tanke på cybersikkerhetstiltak
Det må gis føringer og veiledning fra overordnet hold med hvordan en skal videreutvikle beredskapsplaner med tanke på cybersikkerhet slik at sektorene jobber på samme måte. Det vil bidra til at det samlede planverket fungerer og at en kan opprettholde samfunnskritiske funksjoner.

Tiltak 10. Behov for regulatorisk forankring av cybersikkerhet
Det bør skilles mellom de normer som angår defensiv sikring og håndtering, og offensive tiltak. Det bør vurderes om de offensive tiltak tas ut fra cybersikkerhets-strategien og heller håndteres som cyberetterretning, jf. våre merknader til tiltak 19. og 20. Dette kan også bidra til å forenkle videre arbeidet.

***Ad hovedmål 3 – Bevisstgjøre, opplyse og påvirke***
Tiltak 11. Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid
Det bør innføres krav til roller og hvilken kompetanse innehavere av rollene skal besitte, slik at virksomhetene får tydelige signaler.

Tiltak 12. Arrangere og delta i øvelser (sektorvise, nasjonale og internasjonale)
Det bør presiseres under tiltaket at et viktig formål med øvelser blant annet skal være et grunnlag for evaluering og forbedring.

***AD hovedmål 4 – Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser***
Tiltak 13. Styrke samfunnets evne til å oppdage trusler og sårbarheter
Arbeidsdelingen (oppgavedeling og ansvar) under dette tiltaket er noe uklart, herunder hva som er etatenes, politiets og Forsvarets ansvar. Vi ber om at dette klargjøres i det videre arbeidet med tiltakene.

Tiltak 15. Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter
Vi vil påpeke at det er viktig å bygge opp en struktur slik at de som er "interessenter" i en hendelse og en håndtering av denne effektivt blir betjent. Her vil sikkerhetsmessige avhengigheter spille en rolle, og går i stor grad på tvers av sektorgrenser. Vi vil videre påpeke at muligheten for rask varsling av de dette gjelder er sentralt å få med i det videre arbeidet.

***Ad hovedmål 5 – Etterforske og bekjempe IKT-hendelser***
Tiltak 16. Styrket kapasitet og kompetanse for håndtering av målrettede dataangrep
Dette er et viktig forslag. Vi vil påpeke at virksomhetenes kompetanse og opplæring på dette feltet også må styrkes, slik at de kan håndtere dataangrep på en god og profesjonell måte.

## 3. Økonomiske og administrative konsekvenser innenfor eget ansvarsområde

Tiltakene vil ha økonomisk-administrative konsekvenser for Arbeids- og velferdsetaten. Ut fra den informasjon som foreligger har det ikke vært mulig å estimere kostnadene for de ulike tiltakene. Det er noe AD vil måtte komme tilbake til når tiltakene er presisert.

Med hilsen

for Gard Kjølhaldt (e.f.)
avdelingsdirektør

Ann Kristin Henriksen
seniorrådgiver