DET KONGELIGE
UTENRIKSDEPARTEMENT

Forsvarsdepartementet
Postboks 8126 Dep
0032 Oslo

Deres ref.:	Vår ref.:	Dato:
2010/00794-1/FD I 5/0FD	10/03264-2	15.10.2010

Høring – Nasjonal strategi for cybersikkerhet

Det vises til Forsvarsdepartementets høringsbrev av 30. mars 2010.

Utenriksdepartementet slutter seg til "Nasjonal strategi for cybersikkerhet" og mener det er et godt dokument. I lys av utviklingen globalt, samt det generelle trusselbildet, anser vi strategien som et nødvendig og tidsriktig tiltak. Det er dessuten i samsvar med NATOs og en del andre lands satsing på området.

På bakgrunn av studiene om "Beskyttelse av samfunnet" (BAS) er det gjennomført en rekke gode tiltak, men dagens utfordringer krever bedre koordinering av dette arbeidet samt etablering av et rammeverk for å koordinere aktivitetene. Vi mener at Nasjonal strategi for cybersikkerhet ivaretar dette behovet.

Utenriksdepartementet har følgende kommentarer til de ulike tiltakene under hovedmålene;

Etablere en felles situasjonsoversikt og forståelse
Utenriksdepartementet mener det er et svært viktig tiltak å etablere sektorvise Computer Security Incident Response Team (CSIRT).

I pkt. 4 under tiltakene foreslår vi følgende tekstendring:
Utfordringer knyttet til cybersikkerhet kan ikke løses innenfor rammene av nasjonalstaten. Industrialiserte land harmoniserer sine tiltak gjennom overnasjonale og mellomstatlige organer som eksempelvis NATO og EU. I dag skjer dette samarbeidet basert på tillit og er i liten grad forpliktende regulert i internasjonale avtaler. Norge bør bidra til en klarere forståelse av hvordan forsvaret mot digitale

Postadresse:	Kontoradresse:	Bank innbetalinger:	Telefon:	Saksbehandler:
Postboks 8114 Dep	7. juni plass 1	6345.05.02822	+47 22 24 36 00	
0032 Oslo, Norge	0251 Oslo	Org. nr.: 972 417 920	Telefaks:	post@mfa.no
			+47 22 24 95 80/81	www.odin.dep.no/ud

trusler kan samordnes internasjonalt og hva som må være nasjonalt ansvar. Der det er naturlig bør Norge søke å inngå i et forpliktende internasjonalt samarbeid for effektiv håndtering gjennom informasjonsdeling, men også etterforskning og straffeforfølging av kriminell aktivitet. For å fremstå som en profesjonell part i det internasjonale samarbeidet, er det viktig med kompetanse, å være koordinert, delta aktivt i debatter og bidra med forslag til løsninger.

Vi ser samtidig viktigheten av å etablere et forpliktende internasjonalt samarbeid om cybersikkerhet. Dette er et tema som etter vår mening bør drøftes på politisk nivå.

Bygge og opprettholde robuste og sikre IKT-systemer
Utenriksdepartementet har erfaring med å håndtere kriser og opplever at det er behov for å utvikle og implementere sikre kommunikasjonsløsninger for krisehåndtering på nasjonalt nivå.

Styrke evnen til å oppdage, varsle og håndtere IKT-hendelser
Utenriksdepartementet opplever at dagens ordning med Varslingsystem for digital infrastruktur (VDI) fungerer godt, og vi støtter forslaget om å utvide ordningen til å gjelde alle virksomheter med kritiske samfunnsfunksjoner.

Etterforske og bekjempe IKT-hendelser
Vi er av den formening at det er nødvendig å styrke kapasiteten og kompetansen for håndtering av målrettede dataangrep. Vi anbefaler at det etableres en ressursgruppe som kan rykke ut og bistå virksomheter med samfunnskritiske funksjoner under alvorlige sikkerhetshendelser.

Styrke samordningen av cybersamarbeidet
Erfaringsmessig er operativ håndtering av IKT-sikkerhetshendelser hvor de nasjonale sikkeretstjenestene blir involvert, en tung og tidkrevende prosess. Tidsaspektet er en kritisk faktor under håndtering av alvorlige sikkerhetshendelser. Det er derfor svært viktig å etablere rutiner mellom de ulike tjenestene og organisatorisk samarbeid som kan redusere unødvendig tidstap.

Fra vårt ståsted er det en naturlig konsekvens av ovennevnte tiltak at det etableres et nasjonalt cybersenter. Dette vil etter vår mening forsterke reaksjonsevnen og slagkraften mot IKT-trusler som kan true vitale nasjonale interesser.

Med vennlig hilsen

Monica Nagelgaard
Avdelingsdirektør

Soner Sevin
Seniorrådgiver