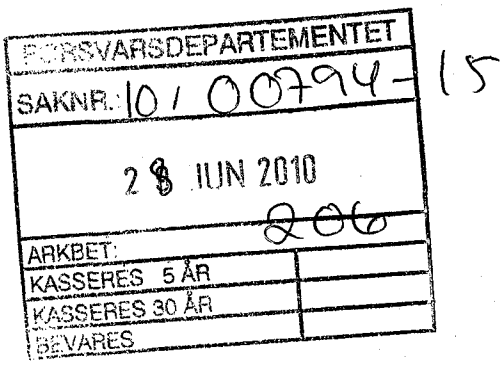
Forsvarets forskningsinstitutt

Dato
21. juni 2010
Vår referanse
10/00835-2/FFI/008
Deres referanse
2010/00794-1

Forsvarsdepartementet
Postboks 8126 DEP
0032 OSLO



Høringsuttalelse - Forslag til strategi for cybersikkerhet

Vår bakgrunn

FFI har og har hatt forskning innen flere av områdene som behandles i strategien.
Prosjektet BAS5 ("Critical Information Infrastructure Protection") fremstår i denne sammenheng som spesielt relevant da hovedformålet med prosjektet var å:

- Utvikle og anvende en metodikk for risiko og sårbarhetsanalyse av samfunnsviktige IKT-systemer
- Utvikle og anvende en metodikk for å rangere tiltak som reduserer sårbarheten
- Utvikle og anvende en metodikk for å rangere samfunnsviktige funksjoner og tilhørende IKT-systemer

Synspunktene som fremkommer i dette høringsnotatet er forankret i erfaringer fra BAS-forskningen og FFIs øvrige forskning innen informasjonssikkerhet.

Utvidelse av NorCERT

FFI støtter den foreslåtte utvidelsen av NorCERT med følgende hovedpresiseringer:

- En styrking av NorCERT bør gjøres samtidig som man etablerer og styrker sektorvise CSIRT-miljøer.
- NorCERT må ha et sterkt fokus på relasjoner til offentlige og private aktører, som NorSIS, EKOM-operatører, FAD og eiere av kritisk infrastruktur.
- NorCERT må synliggjøre og promotere behovene for forskning innen cybersikkerhet.

Etterforskning av datakriminalitet

Tiltak 18 (utrede behov for endringer i det legale grunnlaget for etterforskning) angir et mulig behov for å kunne endre det legale grunnlaget for etterforskning av datakriminalitet. Dette tiltaket bør nok

Vedlegg: 0

Postadresse:	Postboks 25, 2027 Kjeller	Mil retn nr:	505	Organisasjonsnr:	NO 970 963 340 MVA
Kontoradresse:	*Instituttveien 20, 2007 Kjeller*	*Sentralbord:*	63 80 70 00	WWW-adresse:	www.ffi.no
Saksbehandler:	Vidar Stensrud Andersen	Innvalg:	63 80 72 06	Offisiell e-post:	ffi@ffi.no
Personlig e-post:	Vidar-S.Andersen@ffi.no	Telefaks:	63 80 71 15		

forklares bedre, og det bør settes som forutsetning at det kun er Politiet skal kunne etterforske datakriminalitet.

Tiltak 17 (sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning) bør klargjøre relasjonen til Datalagringsdirektivet. Vi henviser for øvrig til Forsvarets høringsuttalelse om Datalagringsdirektivet.

Prioriteringer
Strategidokumentet mangler prioritering mellom de foreslåtte tiltakene. Prioriteringer bør foreslås basert på hvilke tiltak som vil vurderes å gi mest effekt og ha størst gjennomførbarhet. Prioriteringen trenger ikke nødvendigvis være på detaljnivå.

Gjennomførbarhet
De fleste av tiltakene som foreslås har god intensjon, men tidligere erfaring innen området beskyttelse av kritiske IKT-systemer har vist at tiltakene bør vurderes med hensyn på gjennomførbarhet før de iverksettes. Særlig gjelder dette i forhold til kostnader og krav om dybdekompetanse på alle nivåer. Dette gjelder spesielt tiltak 1 (kartlegging og verdivurdering av kritiske IKT-systemer i alle sektorer), tiltak 7 (styrke tilsyn med IKT-sikkerhet), tiltak 8 (utvikle og implementere sikre og robuste kommunikasjonsløsninger for krisehåndtering), tiltak 14 (legge til rette for innrapportering av hendelser), tiltak 15 (etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter) og tiltak 16 (styrket kapasitet og kompetanse for håndtering av målrettede dataangrep).

Sektorvise CSIRT-miljøer og håndtering på virksomhetsnivå
FFI støtter tanken om håndtering av hendelser på virksomhets- og sektornivå. Disse nivåene håndterer best slike hendelser under forutsetning av at de bemannes med rett kompetanse. Med andre ord må kompetansen i en CSIRT inneholde både bred/dyp IKT-sikkerhetskompetanse og sektorspesifikk kompetanse.

Eksempelvis har FFI arbeidet mye med fagområdene olje-prosess og kraftforsyning og deres knytning opp mot det offentlige telenettet (EKOM-infrastruktur) som er svært kompleks. Vi understreker på den bakgrunn viktigheten av adekvat kompetanse i CSIRT-ene.

Lover og forskrifter innen informasjonssikkerhet kan være en utfordring i forhold til strategiens ambisjon om tilsyn og dens berøring med ulike sektorer. Et konkret eksempel er bank/finans-sektoren og energisektoren der det allerede er etablerte tilsynsprosesser innen informasjonssikkerhet. En nærmere avklaring av strategien i forhold til nærhet, likhet og ansvarsprinsippet bør også gjøres.

Relasjoner til andre aktører
Strategien bør ha som ambisjon å legge til rette for god relasjonsbygging mellom aktuelle aktører. FFI mener at relasjoner til andre aktører, blant annet NorSIS, EKOM-operatører og FAD, bør belyses bedre i dokumentet. Dette vil også synliggjøre grensene cybersikkerhet har mot resten av informasjonssikkerhetsrommet.

Strategien bør omhandle hvilket offentlig-privat samarbeid man ser for seg. Dette samarbeidet må være tydelig, åpent og formalisert.

FFI registrerer at Datatilsynet ikke er inkludert som høringsinstans.

Forskning og utdanning

Å opprettholde og styrke den nasjonale ekspertisen innen robust/sikker IKT-utvikling generelt og informasjonssikkerhet spesielt er et strategisk mål. På høgskole- og universitetsnivå må informasjonssikkerhet *integreres* i den generelle IKT-utdanningen. I tillegg må spesifikke studieretninger for informasjonssikkerhet framheves og utbygges. I tillegg bør IKT-sikkerhetsopplæring inn i utdanningen på masternivå i andre teknologifag og i blant annet økonomi og samfunnsfag.

For ansatte innen kritisk infrastruktur er det viktig å heve kunnskapsnivået innen IKT-sikkerhet. En løsning kan være kurs eller "awareness"-trening innen IKT-sikkerhet, for alle aktuell ansatte.

Nasjonal forskning innen informasjonssikkerhet bør styrkes. Sentrale områder er sikkerhet i kommunikasjonssystemer, tillitverdige (trusted) systemer, sikker programvareutvikling samt bedre metoder for risikohåndtering.

Offensive kapasiteter
Tiltak 20 (offensive militære kapasiteter) bør ikke omtales i strategien. Alternativt kan man foreslå et utvalg for å avklare/undersøke hvilke offensive tiltak som kan settes i kraft utenfor militær regi.

Andre avsnitt i tiltak 20 kan også misforstås til at det er CNO-enheten som står for alle militære informasjonsoperasjoner (som også omfatter PSYOPS, villedning, EK, ...). Selv om formuleringen kan spores til et annet offentlig dokument, er den etter vår mening likefullt faglig upresis.

Generelle kommentarer til dokumentet
Det vurderes som nyttig med en vurdering av det proaktive (f eks å bygge og opprettholde robuste og sikre samfunnskritiske infrastrukturer og systemer) kontra det reaktive (f eks å håndtere uønskete IKT-hendelser).

Generelt har dokumentet for lite fokus på selve *infrastrukturen*, se eksempelvis avsnittet *Sårbarheter* i første kapittel. Dette gjelder også andre kapittel.

En nasjonal strategi bør være konsis. FFI anbefaler å samordne begreper og definisjoner med arbeidet i *Felles begrepsbruk i regelverk som berører informasjonssikkerhet* (FAD) som nå er til høring. Det er uheldig med språklig inkonsistens mellom ulike sterkt beslektede dokumenter.

Med hilsen

Vidar S. Andersen

Vidar S Andersen
Avdelingssjef