Vi viser til Deres høringsbrev til ATEA datert 30. mars 2010 og oversender følgende kommentarer til forslaget:

Generelt: Vi tror at strategien i tillegg til kritiske IKT-systemer og virksomheter, skal på relevante områder se hen mot virksomheter i Norge i sin alminnelighet. Hvilke som inngår i kategorien foran, vil endre seg samtidig som omtrent alle virksomheter har behov for cybersikkerhet på et nivå som er avpasset virksomhetens trussel- og risikobilde. Dette gjelder i prinsippet også den enkelte borger som både kan være utsatt for og utilsiktet bidra til cyberUsikkerhet. Ref eksempelet med minnepinner i forslaget. Videre synes vi at det som står på side 5 om "mer tilfeldige påkjenninger" bør tas inn i slik det er nevnt, i relevante i forslag.

Tiltak 1 Kartlegge og verdivurdere kritiske IKT-systemer i alle sektorer

- Vi stiller spørsmålstegn ved om sikkerhetslovens bestemmelser er tilstrekkelige til å få med alle systemer av nasjonal sikkerhetsinteresse. Er det systemer i sektorer som ikke fanges opp av denne loven?

Tiltak 3 Styrke kapasitet etc

- Vi anbefaler at Tilsyn som i dag jobber med informasjonssikkerhet på sektorområder trekkes inn i bildet (Datatilsynet, Finanstilsynet, Post- og teletilsynet etc)

Tiltak 6 Stille felles krav til kritiske IKT-systemer

- Vi tror at krav til sertifiserte systemer må forutsette at det fins et utvalg av sertifiserte systemer som hele tiden speiler tilbudet i det "normale" markedet
- Vi anbefaler at det utvikles, publiseres og vedlikeholdes en "beste praksis" som kan anvendes av alle virksomheter. Status til en enkelt virksomhet kan endres ift nasjonale interesser. Samtidig er det slik at de fleste virksomheter har behov for cybersikkerhet på et nivå som er avpasset virksomhetens trussel- og risikobilde. En "beste praksis" kan gi virksomhetene en veiledning det er behov for

Tiltak 8 Utvikle og implementere kommunikasjonsløsninger for krisehåndtering

- Tiltaket har et snevert omfang. Alle virksomheter har behov for sikre og robuste kommunikasjonsløsninger under krisehåndtering, dette gjelder ikke bare cybersikkerhet. Vi anbefaler at det utvikles en "beste praksis" kan gi virksomhetene en veiledning det er behov for og som dekker både cybersikkerhet og andre kriser

Tiltak 11: Tiltak for bevisstgjøring etc

- Viser til innledende generell kommentar

Tiltak 16: Styrket kapasitet og kompetanse

- Miljøer i privat sektor som jobber med tilsvarende problemstillinger bør trekkes inn i samarbeidet mellom KRIPOS, PST og NSM

Tiltak 17: Lagring av data

- Løsningene må hensynta borgernes rettigheter og demokratiske regler

Tiltak 18: Det legale grunnlaget

- Løsningene må hensynta borgernes rettigheter og demokratiske regler

Tiltak 19: Trusler og trusselaktører

- Miljøer i privat sektor som jobber med tilsvarende problemstillinger bør trekkes inn

Vennlig hilsen

Bjørn A. Tveøy
Sjefkonsulent IT-sikkerhet - BBA, CISSP, CISM, CISA, ISO 27001 Lead Auditor, ITIL, COBIT
+47 908 55 056 bat@atea.no
"Informasjonssikkerhet og personvern - kultur, regler, teknologi/drift - risiko/revisjon"
Atea AS , Postboks 6472 Etterstad, N-0605Oslo
www.atea.no