SINTEF

Det kongelige forsvarsdepartement
Attn Ole Felix Dahl
Postboks 8126 Dep
0032 OSLO

SINTEF IKT

Postadresse:
7465 Trondheim
Besøksadresse:
S P Andersens v 15
7031 Trondheim
Telefon:
73 59 30 00
Telefaks:
73 59 29 77

Foretaksregisteret:
NO 948 007 029 MVA

Deres ref.:	Vår ref.:	Direkte innvalg:	
2010/00794-1/FD I 5/OFD	905130.01/ML/eh	73592957	Trondheim, 2010-06-22

Høringsuttalelse – strategi for cybersikkerhet

Vi viser til brev fra Forsvarsdepartementet 30.03.2010 med anmodning om høringsuttalelser angående Forslag til strategi for cybersikkerhet. SINTEF leverer med dette våre kommentarer til strategiforslaget.

Med vennlig hilsen
for SINTEF IKT

for
Aage Thunem
forskningsdirektør

Maria B. Line
Maria B. Line
forskningsleder

SINTEF

Tiltak nr. 2: Målrettet satsning på forskning og utvikling
Dette tiltaket vil være svært viktig i årene framover. Norges forskningsråd har allerede VERDIKT-programmet, hvor informasjonssikkerhet er et viktig fagområde, men SINTEF mener det vil være en stor fordel om det etableres et eget forskningsprogram for informasjonssikkerhet. Under VERDIKT taper ellers gode informasjonssikkerhetsprosjekter i konkurransen med andre gode prosjekter rettet mer generelt mot IKT. For noen år tilbake eksisterte forskningsprogrammet IKT SOS – Sikkerhet og sårbarhet, et program som kun varte i fire år. Dette programmet kunne med fordel videreføres, da det genererte stor aktivitet på forskningsfronten innen informasjonssikkerhet.

Tiltak nr. 3: Styrke kapasitet for vedlikehold og formidling av IKT-risikobildet
Det nevnes at man savner empiri for et større analysegrunnlag enn i dag. Vi støtter opp om dette ønsket, da empiriske data er nødvendig for å kunne si noe om dagens situasjon samt identifisere forbedringsmuligheter og framtidige behov. Denne typen empiri er noe som et målrettet forskningsprosjekt kunne bidra sterkt til, hvilket igjen viser at tiltak nr. 2 er viktig å prioritere.

Norsk senter for informasjonssikring (NorSIS)
NorSIS er ikke nevnt noe sted i strategiforslaget, noe som synes litt merkelig. Blant annet under tiltakene nr. 3, 5 og 11 vil NorSIS kunne ha en tydelig rolle, men også knyttet til andre tiltak burde NorSIS komme på banen.

Tiltak nr. 6: Stille krav til kritiske IT-systemer
Tiltaket er i utgangspunktet godt og bør helt klart være med, men vi stiller spørsmål ved hvordan dette kan følges opp. Vi etterlyser derfor en beskrivelse av hvem og hvordan knyttet til oppfølging.

Tiltak nr. 11: Styrke tiltak for bevisstgjøring, utdanning og holdningsskapende arbeid
Innunder dette tiltaket burde man legge til sikker programvareutvikling som en obligatorisk del av grunnutdanningen for alle IKT-studier. Med sikker programvareutvikling mener vi kompetanse hos programvareutviklere for å bygge sikre og robuste systemer som håndterer feilsituasjoner på en ryddig måte og som ikke inneholder svakheter som kan utnyttes av angripere.

Tiltak nr. 15: Etablere sektorvise CSIRT-miljøer i samfunnsviktige sektorer og i de største enkeltvirksomheter
Vi slutter oss spesielt til forslaget om å etablere et CSIRT innen olje og gass, på grunn av integrerte operasjoner.

Tiltak nr. 17: Sikre mulighet til nødvendig lagring av data ved hendelser med tanke på å muliggjøre effektiv etterforskning
Dersom man greier å legge til rette for mer effektiv etterforskning gjennom nye eller endrede teknologiske løsninger, må dette gjøres i samsvar med personvernet for den enkelte borger.

Generelt
Vi konstaterer at enkeltbrukere ikke er tenkt på i det hele tatt, bortsett fra som ansatte i virksomheter. Vi mener at hjemmebrukere er en viktig sårbarhet; de har ansvar for å drifte sin egen PC i en Internettverden som er overbelastet av ondsinnet kode, og den vanlige mannen i gata har verken kompetanse eller interesse av å ha dette ansvaret. Vel er ikke hjemme-PCer ansett som kritiske IKT-systemer, men som et ledd i et større angrep mot nasjonal infrastruktur, er hjemme-PCer en av de naturlige førsteskansene.