Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Forsvarsdepartementet
Postboks 8126 Dep.
0030 Oslo

Oslo, 25. juni 2010

Vår ref. · our ref.: NR-FD-20100625
Direktenr. · direct no.: 22852500
Deres ref. · your ref.: 2010/00794-1/FD I 5/OFD

Høringsuttalelse Cybersikkerhet

Høringsuttalelse – Forslag til strategi for cybersikkerhet

Norsk Regnesentral (NR) stiller seg positiv til hovedmålene i strategien. NR mener også at tiltakene i strategien er hensiktsmessige og at de foreslåtte tiltak bør gjennomføres. Vi er enige i prinsippet om at det ikke bør utvikles sektorspesifikke løsninger eller tiltak innen feltet med mindre det er eksplisitte krav som tilsier slike behov. Vi merker oss også at behov for kompetanse innen feltet er gjennomgående for mange av tiltakene. NR vil understreke betydningen av å bygge opp og forvalte kritisk kompetanse innen feltet på en slik måte at denne kompetanse er tilgjengelig i et langsiktig perspektiv. NR har også gjennom sine nettverks og seminaraktiviteter erfart at det er stort behov for toveis dialog mellom FoU miljøene og operative organisasjoner.

Med tanke på de konkrete tiltakene foreslår vi noen presiseringer og tillegg.

Tiltak 2, Målrettet satsning på forskning og utvikling.

Det bør opprettes et nytt forskningsprogram som administreres av Norges Forskningsråd med øremerket finansiering fra Justis og Forsvarsdepartementet. Dette programmet må koordineres og samordnes med tilstøtende programmer i NFR; Verdikt og SamRisk programmene spesielt. Det samme bør gjøres i forhold til EUs FoU programmer og støtteaktiviteter.

- Forskningsprogram skal inkludere forskere i styregruppen som setter målene og foretar evalueringene ut fra langsiktige strategier.

- Integrering og samarbeid med næringsliv som lager eller driver kritiske infrastrukturer. Etablering av støtteordninger og rammeordninger som motiverer deltakelse ut over eksisterende næringsrettete innovasjonsprogrammer. Formålet er tilfredsstillende deltakelse av kritiske bedrifter.

Norsk Regnesentral
Norwegian Computing Center
Postboks 114, Blindern
NO-0314 Oslo, Norway

Besøksadresse
office address
Gaustadalléen 23
NO-0373 Oslo, Norway

Telefon · telephone
(+47) 22 85 25 00
Telefaks · telefax
(+47) 22 69 76 60

Bankkonto · bank account
8200.01.48888
Foretaksnr. · enterprise no.
NO 952125001 VAT

Internett · internet
www.nr.no
E-post · e-mail
nr@nr.no

- Fast involvering av instituttssektor fra alle ekspertmiljøer i forskningsaktiviteter. Involvere industri og offentlig sektor for å sikre et anvendt perspektiv og at kompetansen benyttes.
- Forskningsaktiviteter og infrastrukturer (institutter, laborer, ekspertgrupper) bør bygges opp. Det er viktig å vedlikeholde sikkerhetskompetanse med langsiktige og stabile støtteordninger. NR foreslår å skape et langtidsinstrument innenfor forskningsprogram, for eksempel inspirert av STORIKT eller SFF/SFI-ordninger hos Norges Forskningsråd.

- Samordning av norske initiativer med EUs forskningsaktiviteter, slik at det norske forskningsmiljøet øker samarbeidet med ledende europeiske miljøer..

- Nye sikkerhetsteknologi ofte skaper utfordringer i personvern, spionasje og å redusere risikoen i kritisk infrastruktur. Forskningsprogrammet bør ta hensyn til personvernsutfordninger, spionasjepotensjal og kritisk infrastruktur. NR foreslår at programmet skal motivere forskningsaktiviteter som tar opp disse tema.

- Sikkerhetsbansjen er for tiden for reaktiv, og gjerne oppdaterer sikkerhetstiltak og risikometrikkene etter noen uønsket hendelse har skjedd – slik at tiltakene justeres for sent. Proaktiv styring av sikkerhetstiltakene som tilpasser og balanserer tiltakene bør utvikles og fortløpende evalueres. Metrikkene og rutiner til proaktiv styring bør utvikles innenfor forsknings.

- Eksisterende forskningsprogrammer er ikke i stand til å bygge opp og opprettholde ekspertmiljøene innen feltet. Derfor bør det etableres et forskningsprogram i cybersikkerhet som en selvstendig program med forbindelser til andre programmer.

Utenfor forskningsprogrammet foreslår NR å etablere standardiseringsaktiviteter med involvering av forskere. Mange kritiske bedrifter i samfunnet har liten egen ekspertise eller ressurser for å håndtere dynamiske sikkerhetstiltak. For effektiv bruk av programmets innovativ kunnskap foreslår NR å etablere insentiver til standardisering og sertifisering av tiltakene innenfor cybersikkerhets-området. Standarder og sertifisering hjelper næringslivet med å ta opp innovasjoner og nye tiltak. Standardiseringsaktiviteter skal støttes med en støtteordning til næringsorganisasjoner og instituttssektoren, og skal koordineres hos Standard Norge. Slik kan næringslivet få tak i aktuelle best-practice-rutiner og tiltak.

Tiltak 22, Etablere et nasjonalt cybercenter.

Dette bør også inneha en funksjon for samarbeid med aktuelle utdanningsinstitusjoner og uavhengige institutter vedrørende høyere grads studier og etterutdanning.

NR foreslår et nytt tiltak, etablering av et formidlingsnettverk (for eksempel et ressursnettverk).

Det bør etableres et uavhengig organ i form av et Formidlingsnettverk eller et ”Center of Exellence”. Dette bør inkludere de viktigste aktørene i FoU sektoren inkludert universitetene og de uavhengige instituttene. Formålet vil være å bygge bro fra den mer teoretiske kompetansen som bygges opp i et FoU program (Tiltak 2) og dermed aktivt gi kontinuerlig støtte og kompetanseoverføring til de operative miljøene, spesielt det nasjonale cybersenteret og de sektorvise CSIRT-miljøene. Et slikt nasjonalt nettverk/senter vil bidra til en nødvendig og kontinuerlig kompetansespredning til de operative miljøene, både i privat og offentlig sektor. Samtidig vil tilbakemeldinger og diskusjon med FoU miljøene gjøre innholdet i FoU programmet (Tiltak 2) mer relevant og anvendbart. Et slikt senter bør innholde følgende funksjoner:

- Monitorering og oppdatert kunnskap om den internasjonale forskningsfronten
- Kontinuerlig kompetanseoverføring fra FoU til operative miljø
- Møteplass for samordning og koordinering av FoU aktivitet, gjerne i form av seminarer, arbeidsmøter, utredninger, forstudier og pilotering
- Koordinering, etablering og gjennomføring av spesielt tilpassede kurs og etterutdanning innen ulike spesialfelt for de operative miljøene

Med vennlig hilsen
Norsk Regnesentral

Åsmund Skomedal
Forskningssjef