NTNU
Rektor

Vår dato	Vår referanse
25.06.2010	2010/5152/RA
Deres dato	Deres referanse
30.03.2010	2010/00794

Forsvarsdepartementet

Postboks 8126 Dep.
0032 Oslo

Høringsvar fra NTNU - Forslag til strategi for cybersikkerhet

I strategien foreslås en rekke tiltak mot alvorlige IKT-hendelser. Tiltakene skal styrke Norges evne til å forebygge angrep og håndtere hendelser som oppstår som resultat av angrep eller som resultat av annen sårbarhet innen IKT. Strategien har derfor som ambisjon å håndtere ikke bare IKT-sikkerhet, men også pålitelighetsaspekter ved IKT-systemer. Dette er en naturlig konsekvens av målsetningen: "helhetlig beskyttelse av kritiske IKT-systemer mot alvorlige IKT-hendelser".

Generelle kommentarer

Samfunnets avhengighet av IKT-systemer er allerede betydelig, og utviklingen i retningen av økende avhengighet er entydig. Økt funksjonalitet og brukervennlighet gjør at stadig flere brukere, bedrifter så vel som enkeltpersoner benytter et stadig større repertoar av IKT-baserte tjenester. Den alminnelig bruker har ingen reell mulighet til å foreta en relevant trussel- eller risikoanalyse, og muligheten for å stille krav til sikkerheten som er tilpasset brukssituasjonen, er derfor liten eller helt fraværende. Også innen bedriftsmiljøer vil en ofte kunne observere at sikkerhetskravene er satt tilfeldig uten grundige risiko- og behovsanalyser, enten for høyt eller for lavt eller i verste fall utelatt fullstendig. Oftest vil dette kunne spores tilbake til økonomiske avveininger. I noen tilfeller vil også kravet om brukervennlighet kunne komme i konflikt med sikkerhetskrav, og systemeier vil lett kunne renonsere på forebyggende sikkerhetstiltak som kan fortone seg kostbare og tungvinte i bruk. En felles nasjonal strategi for cybersikkerhet som er klart og presist begrunnet og vidt kunngjort kan være til stor nytte for både bedrifter og organisasjoner, i tillegg til at den vil kunne bidra til økt bevissthet omkring sikkerhetsspørsmål også for den enkelte sluttbruker. Det foreliggende strategidokumentet synes langt på vei å være en god begynnelse på en generell bevisstgjøringsprosess for IKT-bransjen og dens forskjellige aktører i forskjellige roller.

Kommentar til strategi for cybersikkerhet

Gjennomføringen av strategien som er skissert i dokumentet vil kunne lettes vesentlig dersom økte ressurser tilføres relevante forsknings- og utdanningsinstitusjoner i Norge, slik at framtidige teknologiske og administrative løsninger kan bygges på et solid faglig grunnlag av både teoretisk og praktisk art, og at det legges til rette for et tett og nært samarbeid mellom enheter innen forskning, utdanning, industri og offentlig administrasjon. At tiltak på forskjellige nivåer av praktisk og

Postadresse
7491 Trondheim

Org.nr. 974 767 880
E-post:
postmottak@adm.ntnu.no

Besøksadresse
Høgskoleringen 1,
Hovedbygningen

Telefon
+47 73 59 80 11
Telefaks

Saksbehandler
Roar Aspli

teoretisk art er sektorovergripende vil være avgjørende når helheten i sikkerhetsarbeidet skal ivaretas. For eksempel vil en effektiv beskyttelse av nasjonal kritisk infrastruktur involvere kompetanse og ressurser fra mange (alle) samfunnssektorer, og samordning av regelverk og innsatsfaktorer vil være av avgjørende betydning. Det foreliggende strategidokumentet belyser og vektlegger dette på en god måte. Konsekvent vektlegging av tett integrert samarbeid mellom offentlige myndigheter og private bedrifter/organisasjoner (PPP) er en styrke ved strategien slik den er beskrevet. Det er likevel en forutsetning for at et slikt samarbeid skal fungere optimalt at aktørene har klart definerte roller, og at bevisstheten om hvilket ansvar som er tillagt rollen, er tilsvarende klart definert og kommunisert til alle parter. Hovedmålet som er beskrevet som "Etablere en felles situasjonsoversikt og forståelse" bør ytterligere konkretiseres slik at det blir klart på hvilket nivå og med hvilke innsatsfaktorer slik felles forståelse skal oppnås. Ikke minst er det avgjørende å avklare hvordan kostnadene i kartleggingsfasen skal dekkes. Dagens manglende finansiering av en målrettet langsiktig satsning på forskning og utvikling er også en helt sentral problemstilling.

Det er en mangel ved strategidokumentet at det ikke tas stilling til i hvilken grad en ønsker å stimulere arbeidet med forebyggende sikkerhetsmekanismer gjennom å styrke eksisterende sikkerhetsevaluerings- og sertifiseringsordninger basert på internasjonale standarder som ISO/IEC 27000 og ISO/IEC15408 m.fl., som i Norge er under SERTIT sitt ansvarsområde. Offentlig sektor bør kunne gå foran og få utarbeidet kravspesifikasjoner som tilfredsstiller kravene i ISO/IEC 15408, og kreve at systemer, produkter og tjenester som leveres under offentlige kontrakter er evaluert og sertifisert i henhold til relevante standarder. Leverandører bør som et minimum oppfylle kvalitetskravene i ISO/IEC 27000 - serien av standarder, og sertifiseringsordingen bør brukes aktivt, noe som utvilsomt vil øke bevisstheten om verdien av kvalitetssikring generelt og nødvendigheten av tredjeparts evaluerte sikkerhetsløsninger spesielt.

Med hilsen

for Trond Singsaas
Direktør for organisasjon og informasjon