Bech, Kristin Solberg

Fra: Tore Larsen Orderløkken [tore.orderlokken@norsis.no]
Sendt: 25. juni 2010 12:29
Til: Postmottak FD
Emne: Høring nasjonal strategi for cybersikkerhet
Vedlegg: Høring strategi cybersikkerhet fra NorSIS.pdf

Vedlagt følger Norsk senter for informasjonssikring sine kommentarer til nasjonal strategi for cybersikkerhet.

Med vennlig hilsen

Tore Larsen Orderløkken
Administrerende direktør
Norsk senter for informasjonssikring
NorSIS
Mobil: +47 907 30 675
Tlf: +47 40 00 58 99
E-post: tore.orderlokken@norsis.no
Web: www.norsis.no
Adresse: Merkantilvn 2, 2815 GJØVIK

NorSIS
Norsk senter for informasjonssikring

Forsvarsdepartementet
Postboks 8126 Dep,
0032 Oslo

Gjøvik, 25. juni 2010

Vår ref.: NorSIS/2010-62/TLO

Deres ref.:2010/00794-1/FD I
5/OFD 30 mar 2010

Høring om forslag til strategi for cybersikkerhet

Bakgrunn

Norsk senter for informasjonssikring (NorSIS) viser til høringsbrev fra Forsvarsdepartementet 30. mars 2010 om forslag til nasjonal strategi for cybersikkerhet.

Det norske samfunn er i dag avhengig av et velfungerende IKT system der man har behov for tilgang til sine daglige applikasjoner og programmer som ansatt, som privatperson eller i andre roller. Tilgang til tjenester fra det offentlige, hos næringslivet eller i kommunikasjon mellom privatpersoner er blitt en selvfølge og dette har gitt oss bedre samhandling og økt effektivisering. Denne økte IKT bruken forutsetter en stor grad av tillitt til IKT systemene samt en robusthet i å motstå misbruk og angrep. Gjennom utallige reportasjer i media, rapporter fra myndigheter og sikkerhetsleverandører ser vi at organiserte kriminelle, fremmede stater og motiverte angripere stadig forsøker å bryte den robustheten som er lagt inn i dagens IKT systemer. Det vil være ødeleggende for tilliten til IKT systemene om slike angrep enten kompromitterer eller ødelegger tilgjengeligheten til våre IKT systemer.

Nasjonal sikkerhetsmyndighet har blant annet som sin oppgave å koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden i de virksomheter som omfattes av sikkerhetsloven. I dette ligger det å sikre skjermingsverdig informasjon og skjermingsverdige objekter mot sikkerhetstruende virksomhet som spionasje, sabotasje og terrorhandlinger. Det er informasjon og objekter med betydning for rikets selvstendighet og sikkerhet som i denne sammenheng regnes som skjermingsverdige.

NorSIS høringskommentarer er gitt med bekgrunn i denne definisjonen.

Drøfting

NorSIS mener at strategiforslagets seks hovedmål er gode, og at med en god implementering kan forslaget gi mulighet for å øke Norges kompetanse og evne til å utføre forebyggende informasjonssikkerhet samt gi en tilstrekkelig reaktiv evne for å håndtere sikkerhetshendelser. NorSIS mener at det å håndtere sikkerhetshendelser defineres klarere i strategien og at det bør klargjøres hvem som har ansvar. Normalt skal

Besøksadresse
Merkantilvegen 2
2815 Gjøvik

Postadresse
Postboks 104
2801 Gjøvik

Tlf.: +47 4000 5899
Fax: +47 6117 0900
Org.nr. 995 195 003

E-post: post@norsis.no
Nett: www.norsis.no

hendelser håndteres der de skjer og av ansvarlig virksomhet/etat og det bør derfor klargjøres hvilke hendelser som omfattes av strategien.

I strategidokumentet mener NorSIS at det mangler diskusjon knyttet til øvrige lover og forskrifter som gir føringer for kritisk infrastruktur, f.eks. Ekomloven.
En diskusjon knyttet til roller og ansvarsforhold mellom berørte myndigheter er også etter vår mening noe som bør inn i strategidokumentet.

NorSIS mener løsningen med et nasjonalt cyberssenter er en god løsning, men stiller spørsmål ved fordelene ved å legge alt ansvar til en slik sentralisert løsning hos NSM. Dette kan medføre en ensidighet, og kan gi lav redundans. Ensidighet forkaster nytteverdien av flere perspektiver som flere organer og en distribuert løsning gir, og eventuelt miste muligheten til å skape et helhetlig og korrekt situasjonsbilde.

Forslaget om sektorvise CSIRT miljøer er godt, og kan bidra til å øke nasjonens reaksjonsevne på sikkerhetshendelser. For at dette skal fungere må det utredes klare retningslinjer for administrativt ansvar, krav til sektorvise CSIRT og klare rammer for hvordan dette skal fungere.

Vedrørende strategiforslagets hovedmål nr. 3 "bevisstgjøre, opplyse og påvirke" er dette noe NorSIS arbeider målrettet for. Viktigheten av å bevisstgjøre om trusler og sårbarheter, opplyse om konkrete tiltak og påvirke til gode holdninger må ikke undervurderes. Mennesket omtales ofte som det svakeste leddet i sikkerheten, det er derfor essensielt at det fokuseres på nettopp å bevisstgjøre, opplyse og påvirke. I tillegg er arbeidet med sikkerhetskultur viktig og må få plass i arbeidet under dette punktet.

NorSIS er fornøyd med hovedtrekkene i strategiforslaget, som å opprette et nasjonalt cyberssenter og etablere sektorvise CSIRT miljøer, men mener rammene og ansvarsfordelingen for en slik løsning må beskrives klarere. Cyberssenteret bør ha en koordinerende rolle, og ikke overta funksjoner som allerede er tilstede og som fungerer godt. NorSIS ser også behovet for å ivareta andre deler av samfunnet som ikke er underlagt sikkerhetsloven slik at å legge senteret til en virksomhet med tilsynsansvar for sikkerhetsloven vil etter NorSIS mening ikke nå bredt nok ut. Vår erfaring tilsier at sikkerhetsutfordringene er like farlige for kritisk infrastruktur om angrepet kommer via utdatert eller ikke oppgraderte private eller offentlige IKT systemer som ikke er underlagt sikkerhetsloven. Dette er utfordringer som finnes i alle deler av samfunnets IKT systemer og det forebyggende arbeidet gjelder alle. Her er NorSIS allerede en aktør som kan utfylle denne rollen.

Det bør utredes klarere retningslinjer, rammer og ansvarsområder i strategiforslaget. Strategiforslaget virker noe diffust på enkeltområder, og beskriver ikke alltid klart hvordan tiltakene skal gjennomføres eller tilhørende ansvarsroller. Strategiforslaget bør være så klart som overhodet mulig når det angår organisering, ansvarsroller og rammer. Når det gjelder økonomi ser vi at de fleste tiltakene vil ha en kostnad uten at vi har sett nærmere på størrelsen eller fordelingen.

Kommentarer til punkter.

Ad punkt 1
Det er referert til mange utenlandske hendelser, vi har i Norge også en mengde hendelser som bør kunne refereres til for å understreke nærheten til problemet.

Det bør tilkjennegis/defineres bedre hvem som er målgruppen.

Ad punkt 2.1 underpunkt 2
Sikkerhetsmiljøet ved Høgskolen i Gjøvik er et av de ledende i Europa og bør ha en naturlig plass i et slikt FoU-program.

Ad punkt 2.3 tiltak 11
Et obligatorisk kurs innen sikkerhet for virksomhetens ledere på linje med HMS kurs er et alternativ.

Ad punkt 2.5
Det må klargjøres om grunnlaget for at etterforskning og bekjempelse skal ligge til senteret er riktig.

AD pkt 2.5 tiltak 16
Det bør etableres et eget akademisk master studie innen faget dataetterforskning/forensics.

Med vennlig hilsen

Tore L. Orderløkken

Tore Larsen Orderløkken
Administrerende direktør
NorSIS