Steria AS
Biskop Gunnerus gt 14
Postboks 2
N-0051 OSLO
Tlf.: +47 22 57 56 00
Faks: +47 22 57 59 60
Foretaksnummer: NO 910 909 088 mva.
Bankgiro: 7001 05 38155
www.steria.no

Det Kongelige Forsvarsdepartement
Postboks 8126 Dep
0032 Oslo

Deres ref: 2010/00794-1/FD I 5/OFD Vår ref.: ROR1010 Dato: 25.06.2010

Forslag til nasjonal strategi for cybersikkerhet – svar på høring

Steria AS vil med dette besvare høring av forslag til nasjonal strategi for cybersikkerhet, og vil i dette svaret understreke forhold som Steria AS er opptatt av.

Steria AS har en grunnleggende positiv holdning til forslaget om en sentralisering av strategien for cybersikkerhet, men ser at det er utfordringer knyttet til ansvar, myndighet og kommando for et slikt initiativ. Dette brevet søker primært å belyse disse forhold.

Trygghet

For å styrke tilliten mellom individ og samfunn er det viktig at individet vet at det er beskyttet, og at rettssikkerheten blir ivaretatt. Fravær av internasjonal kriminalitet, datakriminalitet, terror og overgrep er med på å legge forholdene til rette for at individet på en fri måte kan delta i samfunnet og bruke tjenester som man i forslaget ønsker å beskytte mot angrep.

Det framgår av strategiforslaget at begrepet cybersikkerhet er en videreutvikling av informasjonssikkerhetsbegrepet, som gjenspeiler samfunnets økende avhengighet av IKT-systemer som er knyttet sammen i cyberspace.

Forslaget oppleves å ha stort fokus på det tekniske perspektivet, og i mindre grad på en helhetlig og samordnet beskyttelse av virksomheten Norge.

Steria er langt på vei enig i behovet for en samordnet overnasjonalitet, men stiller spørsmål ved eierskap til styring, prioritering, koordinering og ansvar ved etableringen av et overnasjonalt senter.

Ansvar

Informasjonssikkerhet og beskyttelse av virksomheten er et lederansvar innenfor alle samfunnsområder. Dette innebærer at også overvåkning og kontroll av virksomhet er et lederansvar. Ansvarliggjøring er nøkkelen til alt vellykket sikkerhetsarbeid. Dette ligger til grunn for den dominerende standarden for styringssystemer for sikkerhet: ISO/IEC 27001:2005. Denne standarden ligger til grunn for sikkerhetsarbeidet i en rekke offentlige og private virksomheter, og brukes blant annet av Riksrevisjonen som utgangspunkt for revisjoner i statlige virksomheter.

Steria har lagt til grunn at ansvarsforholdet på samfunnsnivå for å levere viktige tjenester i fred, krise og krig allerede er godt definert og tydelige avklart og forankret. En slik forutsetning er av vesentlig betydning for ethvert samfunn. Nøkkelen til varige sikkerhetsforbedringer ligger i å synliggjøre og klargjøre dette ansvaret.

For eksempel har de som har ansvar for matforsyningen til befolkningen, også ansvaret for å overvåke utviklingen og sikre et akseptabelt sårbarhets- og trygghetsnivå i fred, krise og krig. En overvåkning eller kontroll av de ulike virksomhetsområdene i samfunnet, må ivaretas av de som har det direkte ansvaret for å levere tjenester til befolkningen og samfunnet generelt.

En overnasjonalitet innenfor en utvidet definisjon av informasjonssikkerhet må derfor forholde seg til virksomhetslederne, og en eventuell overvåkning og rapportering av utvikling må fokusere på det de ulike lederne er opptatt av og har behov for.

Avhengigheten mellom samfunnsområdene i fred, krise og krig er også noe som krever overnasjonal tilnærming. Matforsyning er bl.a. avhengig av transport, logistikk og betalingsformidling. Eksemplet synliggjør behovet for å verdikjedebetraktninger med samfunnsperspektiv for å tydeliggjøre avhengigheter, ansvarsforhold og hva som er viktig å overvåke og ha tilstrekkelig kontroll på. Dette bidrar også til å fokusere på virksomhet av nasjonal betydning, og ikke bare IKT slik høringsutkastet i stor grad gjør.

Generelt er det Sterias refleksjon at forslaget til nasjonal strategi har et IKT perpektiv og ikke et samfunns- og virksomhetsperspektiv. Steria mener derfor at det gjennomgående perspektivet bør være sterkt orientert mot beskyttelse av virksomheter av nasjonal betydning og deres gjensidige avhengigher. En viktig konsekvens av en slik tenkning er igjen plassering av ansvar og identifisering.

Situasjonen

Stadig flere nasjoner bygger opp offensiv og defensiv kapasitet innen såkalt "cyberwar". Grunnen er enkel: Vårt moderne samfunn er basert på informasjonsteknologi, og et angrep som setter infrastrukturen ut av spill vil være svært ødeleggende, både for enkeltindivider og for samfunnet. "Cyberspace" har blitt vårt fjerde forsvarsrom, men har også blitt en arena for offensive angrep mot andre nasjoner.

Realiteten er at "cyberangrep" mot vesentlige norske interesser ikke er et fjernt og mulig scenario, men noe som faktisk oppleves flere ganger per sekund.

Fokus i "Nasjonal strategi for cybersikkerhet" oppfattes å være rettet mot en situasjon som kun innebærer forsvar mot koordinerte og omfattende angrep mot Norge. For å møte disse ønsker man å etablere et overvåkningssenter. Man har tidligere hatt tilsvarende overvåkningsoperasjoner, blant annet E-tjenestens lyttepunkter for å oppdage ubåttrafikk i Norskehavet.

Det nye senteret er i likhet med tidligere tiders signaletterretning skissert med omfattende lyttepunkter, men få definerte prosedyrer for tilbakemeldinger. Og tilbakemeldinger vil være nøkkelen til effektive mottiltak.

Kun et breddeforsvar med aktiv deltakelse fra alle samfunnsfunksjoner vil kunne gi oss en grad av sikkerhet.

Vi tror at "angrep mot nasjonal infrastruktur" i et "Cyberwar" scenario vil tilhøre sjeldenhetene. Likevel vil vesentlige samfunnsfunksjoner kunne være ute av drift som følge av rettede eller opportunistiske angrep.

Det er ikke gitt at en angripende nasjon vil erklære "cyberkrig". Steria anser det som mer sannsynlig at vi vil oppleve angrep hvor mye innsats legges i å skjule at angrepet pågår og hvor det kommer fra. Følgelig vil "utbrudd av cyberwar" ende opp som en skjønnsmessig definisjon, hvor nasjonens generelle IT-sikkerhetssituasjon er en nøkkelparameter.

Ved å bedre den generelle sikkerhetssituasjonen, reduseres derfor sjansen for at en vellykket cyberwar rammer Norge.

Forsvaret versus sivile myndigheter

Truslene som er beskrevet i høringsutkastet er kriminelle handlinger. I det norske samfunnet er det justissektoren som er ansvarlig for proaktivt å bekjempe kriminalitet og også etterforske dette. Justissektoren har også et koordinerende ansvar for nasjonal sikkerhet i forbindelse med kriser.

Et forsvarssenter vil ha militære regler for gradering av informasjon. Dette vil kunne utgjøre en barriere i forhold til informasjonsutveksling til parter som har behov for å motta informasjon raskt under angrep, men som ikke er sikkerhetsklarert.

Det er av avgjørende betydning at en overnasjonalitet for å beskytte nasjonale interesser har sitt utspring og forankring i et miljø som særskilt er opptatt av rettsikkerhet for individet, har ekspertise på all type overvåkning og kontroll og ikke minst er satt til å bekjempe kriminalitet. Videre må bevis som samles inn sikres slik at de kan fremlegges for og aksepteres av rettsystemet, ikke bare i Norge men også i land som måtte være kilden for angrep på norske interesser.

Kritisk Nasjonal Infrastruktur

Begrepet "Kritisk Nasjonal Infrastruktur" oppfattes dessuten å være flytende definert. Det er klart at strømtilførsel og telekommunikasjon er kritisk. Det kan argumenteres at dagligvarehandel også er det. I så fall må man også inkludere bestillingsrutiner, varetransport og drivstofforsyning. Store dagligvarebutikker benytter web-bestilling av varer, og vil kun ha begrensede muligheter for ordremottak om Internett er nede.

I stedet for å se på forsvar mot "kritisk nasjonal infrastruktur" bør man derfor i stedet la sivile myndigheter se på alle angrep mot Norge, og trekke inn Forsvaret dersom angrepsvirksomheten passerer visse terskelverdier, uavhengig av hvilke spesifikke mål i Norge som blir angrepet.

Dessuten: Med en flytende grense for "kritisk nasjonal infrastruktur" blir det opp til overvåkerne å definere overvåkningsomfanget. Steria anser dette som prinsipielt uheldig ut fra demokratiske prinsipper.

Høringsdokumentets hovedmål

I kapittel 2 i høringsdokumentet nevnes seks hovedmål med strategien:

1. Etablere en felles situasjonsoversikt og forståelse

2. Bygge og opprettholde robuste og sikre kritiske IKT-systemer
3. Bevisstgjøre, opplyse og påvirke aktuelle målgrupper
4. Styrke evnen til å oppdage, varsle og håndtere hendelser i kritiske IKT-systemer
5. Aktivt avverge, bekjempe og etterforske hendelser i kritiske IKT-systemer
6. Styrke samordning av cybersikkerhetsarbeidet.

Mål 1, 2 og 3 vil best kunne ivaretas av en sivil myndighet. For mål 4 og 5 er situasjonen litt mer uklar. Nøkkelen ligger det diffuse begrepet "kritiske". Dette vil det bli mer og mer vanskelig å skille fra "øvrige" systemer. Et koordinert, effektivt angrep mot vår infrastruktur hører klart inn under Forsvarets mandat. Samtidig opplever enkeltpersoner og virksomheter daglig slike angrep. Svært mye "feies under teppet". Når angrepsaktiviteten først blir kartlagt, er det svært mange virksomhetseiere som blir meget overrasket over det store omfanget.

For å gi oss et mer robust samfunn, anbefales det at sikkerheten i alle ledd, og ikke bare innen kritisk nasjonal infrastruktur bedres radikalt. I et totalperspektiv vil derfor også punkt 4 og 5 være best ivaretatt av en sivil myndighet.

Mål 6 beskriver en koordineringsrolle. Denne rollen bør ikke ligge i en spesifikk fagetat, men på departementsnivå. Behovet for koordinering er til stede i rekke sektorer, ikke bare i Forsvaret.

Oppsummering

Dokumentet er utformet av NSM og bærer preg av militær tankegang og teknologipersspektiv. Samtidig endrer informasjonssystemer radikalt måten forsvar må bygges på i informasjonssamfunnet. Nasjonal beskyttelse vil kunne oppnås gjennom et systematisk og omfattende arbeid som rettes mot å styrke beskyttelse og forsvar av alle samfunnsfunksjoner, og som kan oppdage og varsle angrep på betydelig lavere nivå enn nasjonal skala. Dette gjøres best ved å bygge en robust nasjonal infrastruktur.

Med hilsen

Stein A. J. Møllerhaug
Seniorrådgiver

Ronny Robinsson-Stavem
Senior IT consultant