Politiets sikkerhetstjeneste
Den sentrale enhet

Postboks 4773 Nydalen,
0421 OSLO
post@pst.politiet.no
Tlf.nr. 23 30 50 00
Faksnr. 23 30 51 20
Besøksadresse:
Nydalen allé 35, Oslo

Kontaktperson:

Deres ref.: 2010/00794-1/FDL5/OFD
Vår ref.: 201000663-3 008
Dato: 22. juni 2010

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

Høring - Forslag til strategi for cybersikkerhet

Det vises til høringsbrev av 30.03.2010 vedrørende forslag til strategi for cybersikkerhet.

Politiets sikkerhetstjeneste (PST) finner det positivt at det er igangsatt et arbeid med en strategisk tilnærming til viktige og vanskelige utfordringer knyttet til å beskytte samfunnskritisk infrastruktur. Det foreligger et klart behov for en samlet strategi på området, og det er viktig at de ulike aktørene arbeider sammen i det videre. Forslaget til strategi synes i så måte å være et godt utgangspunkt for en videre prosess.

Arbeidet med en samlet strategi for cybersikkerhet er nytt i Norge, og PST har forståelse for den utfordring det er å kartlegge og beskrive dagens situasjon slik at dette kan danne grunnlag for nødvendige tiltak. PST finner imidlertid ikke at det forslag til strategi for cybersikkerhet som nå er sendt på høring er et tilstrekkelig grunnlag for spesifikke tiltak i sin nåværende form. Vi vil komme nærmere inn på bakgrunnen for vårt syn nedenfor, men vil innledningsvis poengtere at verken det begrepsmessige grunnlag, beskrivelsen av de enkelte etaters myndighet og kapasiteter på området i dag, eller konsekvenser av opprettelse av et nasjonalt cybersenter synes tilfredsstillende utredet i forslaget til strategi.

1. Begrepsbruk
IKT-trusler/IKT-risikobildet
Slik PST ser det er mye av det begrepsmessige grunnlaget for forslaget uklart. Det vises eksempelvis til bruken av begrepene *IKT-trusler* og *IKT-trusselbildet*, på side 9 i forslaget. En trussel er knyttet til aktører og måles som funksjon av disse aktørens intensjon og kapasitet. PST stiller derfor spørsmål ved forslagets definisjon av en IKT-trussel som *"uønskede handlinger, herunder reelle og potensielle, som kan rettes mot nettverk og elektroniske informasjonssystemer"*.

Det følger ikke av definisjonen hva som representerer en slik uønsket handling eller hvem som definerer hva som anses å være en slik uønsket handling. Videre utelukker definisjonen det intensjonelle ved IKT-trusler, noe som er helt sentralt i arbeidet med analyse av truslene.

I høringsnotatet introduseres videre *IKT-risikobildet* som et nytt begrep. Begrepet innebærer en videreutvikling av den tradisjonelle forståelsen av risiko som funksjon av en hendelses sannsynlighet og konsekvens. I forslaget til strategi er imidlertid bruken av begrepet uklart behandlet og presentert. Det er blant annet uklart når man mener trussel (IKT-trusselbildet) og når man mener risiko (IKT-risikobildet). Det vises her for eksempel til tiltak 3 på side 15 hvor det beskrives et tiltak for å *"styrke kapasitet for vedlikehold og formidling av IKT-risikobildet"*. Omtale av tiltaket handler imidlertid kun om forhold rundt IKT-trusselbildet.

De uklarheter som er heftet ved helt sentrale begreper som IKT-trussel og IKT-risikobildet gjør at PST ser behov for at det brukes mer tid på å diskutere de ulike praktiske sidene ved implementeringen av strategien.

Hendelseshåndtering
Hendelseshåndtering er et sentralt og gjennomgående tema i forslaget til strategi. Det synes likevel uklart hva dette konkret innebærer. Strategien har som ett av sine hovedmål å *"styrke evnen til å oppdage, varsle og håndtere IKT-hendelser"*, jf også høringsbrevet, men det er uklart hva man legger i begrepet *håndtere.*

Det vises til side 18 hvor går frem at formålet med håndteringen er å gjenopprette sikkerhet og funksjonsevne i virksomhetens systemer. Samtidig er det andre steder i strategien snakk om *"offensive aktørfokuserte tiltak"* og om *"bekjempelse av ulovlig/uønsket cyberaktivitet"* i sammenheng med hendelseshåndteringen. Det virker således som om det ligger mer i begrepet hendelseshåndtering enn hva formålet tilsier. Dette bør i så fall komme klart fram i forslaget.

Likeledes er det gjennomgående benyttet begreper som *"forebygge", "aktivt forebygge", "motvirke", "aktivt avverge" og "bekjempe"* ulike steder i strategien, uten at det er klart hva som skiller de enkelte.

PST finner at det er av avgjørende betydning at det arbeides videre med å oppnå et ensartet begrepsapparat som grunnlag for de vurderinger og tiltak som skal nedfelles i en strategi.

2. Beskrivelse av ansvar og kapasiteter/etablering av nasjonalt cybersenter
Forslag til strategi foreslår som tiltak 22 å etablere et nasjonalt cybersenter. Tiltaket er foreslått som ett av flere tiltak for å styrke samordningen av cybersikkerhetsarbeidet, men trekkes også fram som et viktig virkemiddel for å styrke evnen til å etterforske og bekjempe IKT-hendelser og samle fagmiljøer. PST synes i utgangspunktet at dette er et positivt tiltak, men at begrunnelsen og beskrivelsen av oppgaver og ansvar virker noe mangelfull.

Innledningsvis må det påpekes at behovet for senteret ikke kan ses særlig dokumentert. Det vises til side 22 hvor det slås fast at *"Det er behov for en operativ funksjon rettet inn mot nye og endrede behov knyttet til ivaretakelse av cybersikkerheten."* uten at det framkommer hvilke behov det siktes til. Det konkluderes i neste setning med at *"Dette behovet dekkes gjennom etableringen av et nasjonalt cybersenter"*. Det er mulig at cybersenteret vil dekke en del av de behov og problemstillinger som påpekes i strategien. Ettersom disse behovene, eller hvorvidt opprettelsen av et cybersenter vil møte disse behovene ikke i særlig grad dokumenteres, finner PST likevel at det vil være formålstjenlig å gjennomføre en grundigere utredning før det konkluderes med opprettelse av et eventuelt cybersenter.

Videre finner vi det uklart hvilke analysefunksjoner forslaget omfatter. I forslag til opprettelse av et nasjonalt cybersenter foreslås det at et nasjonalt cybersenter bør omfatte *"tverrfaglige analysefunksjoner [...] for å sikre en helhetlig analyse og vurdering av IKT-risikobildet"*, jf side 22. Det kan synes som om dette i praksis er en videreutvikling og operasjonalisering av Koordineringsgruppen for IKT-trusselbildet. PST har ingen motforestillinger mot å etablere et analysemiljø knyttet til behandlingen av tekniske data. I og med at det i forslaget foreslås en videreutvikling og operasjonalisering av koordineringsgruppen så virker det imidlertid som om forslaget her beskriver et analysemiljø for å analysere de større linjene i trusselbildet relatert til IKT. Dette er PST sterkt kritisk til.

Det vises for det første til vår kommentar innledningsvis vedrørende uklare begreper. Uklarheten reiser blant annet spørsmål om hvorvidt et slikt senter representerer en egnet arena for helhetlig analyse og vurdering av IKT-trusselbildet.

For det andre kan PST heller ikke se at eksisterende miljøer eller kapasiteter er tilfredsstillende kartlagt og beskrevet i forhold til forslaget om opprettelse av et nasjonalt cybersenter. Ansvaret for analyser av trusselbildet knyttet til terror, sabotasje og etterretning er i dag forankret i PST og Etterretningstjenesten. Det er følgelig også her de største miljøene som utarbeider helhetlige vurderinger på taktisk og strategisk nivå er etablert. Hvis et slikt senter skal fungere ut fra intensjonen i forslaget så innebærer dette at en del analysekapasitet fra disse miljøene i Etterretningstjenesten og PST skal overføres til senteret. Tiltaket vil derfor bidra til å svekke eksisterende miljøer, uten at det er utredet hvorvidt et fellessenter faktisk vil bidra til å styrke det samlede kontraetterretnings- og kontraterror-analysearbeidet.

For det tredje synes det også uklart hvorvidt informasjonsgrunnlaget i senteret vil være tilstrekkelig godt til å rettferdiggjøre en slik overføring av analysekapasitet. PST har i løpet av de siste 3 årene høstet erfaringer fra felles analysesamarbeid innenfor rammen av Felles analyseenhet (FAE). Blant annet så ser vi fra FAE at effektiviteten til et fellessenter er avhengig av en klar og desentralisert beslutningsmyndighet når det gjelder informasjonsdeling. Tilgang til informasjon må være avklart og det må foreligge et klart eksternt behov for analyseprodukter fra senteret. Så lenge disse grunnleggende forutsetningene ikke er utredet og implementert så vil det være lite hensiktsmessig å samlokalisere analytikere i et slik senter.

Avslutningsvis vil vi peke på at forslaget til strategi legger til grunn at *"juridiske forutsetninger og spørsmål knyttet til formelt ansvar må avklares nærmere, og detaljerte prosessbeskrivelser utarbeides."*, jf forslaget side 23. Dette er sentralt og en grunnleggende forutsetning for iverksettelse av tiltak. Dette synes spesielt viktig dersom cybersenteret også skal være et viktig virkemiddel for å styrke evnen til å etterforske og bekjempe IKT-hendelser, oppgaver som i dag ikke tilligger NSM.

På bakgrunn av den uklarhet om ansvar, oppgaver og bruk av eksisterende kapasiteter som foreligger, ser PST det som helt nødvendig å kartlegge og utrede hvilke oppgaver senteret skal ivareta, hvem som skal lede/bemanne det, og hvordan roller/oppgaver/ansvar skal fordeles mellom de deltakende etater. Vi kan ikke se at tiltaket kan iverksettes før disse forholdene er tilstrekkelig belyst.

3. Avslutning

PST finner at forslaget til strategi for cybersikkerhet vil være et godt utgangspunkt for en videre prosess knyttet til arbeidet med å sikre samfunnskritisk infrastruktur. Vi finner imidlertid ikke at forslaget kan ses å være et tilstrekkelig grunnlag for spesifikke tiltak i sin nåværende form. Først når nødvendige begrepsavklaringer, kartlegging av behov og eksisterende kapasiteter, juridiske avklaringer og en nærmere utredning knyttet til et nasjonalt cybersenter er gjennomført, kan det bli aktuelt å beslutte tiltak. Som en av de sentrale aktørene på dette feltet, vil PST gjerne delta i den videre prosessen knyttet til disse spørsmålene.

Janne Kristiansen