Kommittédirektiv

Viss översyn av ansvarsfördelning och organisation när det gäller samhällets informationssäkerhet

Dir. 2009:110

Beslut vid regeringssammanträde den 19 november 2009

Sammanfattning av uppdraget

En särskild utredare ska utreda formerna och konsekvenserna av att flytta ansvaret för dels Sveriges IT-incidentcentrum (Sitic) från Post- och telestyrelsen, dels Sveriges certifieringsorgan för IT-säkerhet (CSEC) från Försvarets materielverk. Verksamheterna ska inordnas i antingen Myndigheten för samhällskydd och beredskap (MSB) eller Försvarets radioanstalt (FRA). Utredaren ska undersöka vilken av dessa två myndigheter som bedöms bäst lämpad att vara ansvarig utifrån de behov och målsättningar som regeringen angett när det gäller bl.a. att samla informationssäkerhetsfrågorna. Utredaren ska slutligen föreslå en myndighet som ska vara signatär för de internationella organen CCRA och SOGIS-MRA vilket bl.a. innebär att underteckna fördrag.

Uppdraget ska redovisas senast den 22 januari 2010.

Behovet av en utredning

Det finns ett behov av att samla resurserna för att skapa bättre förutsättningar att förebygga respektive hantera IT-incidenter. Rapporteringen av IT-incidenter som utgör hot mot eller medför allvarliga konsekvenser för samhällsviktig verksamhet och kritisk infrastruktur i samhället behöver förbättras och anpassas till de olika behov som finns bland relevanta parter i samhället.

Ansvaret för informationssäkerhet på nationell nivå är uppdelat på ett flertal myndigheter, bl.a. MSB, PTS inkl. Sitic

och FRA vilket innebär att ansvaret är splittrat. Detta betyder att styrningen och samordningen av arbetet försvåras och att resurser riskerar att inte nyttjas på ett optimalt sätt. Regeringen anser att ansvaret för informationssäkerhet bör samlas. I budgetpropositionen för 2010 (prop 2009/10:1, utgiftsområde 6 Försvar och samhällets krisberedskap sidan 79) har regeringen redovisat att det finns anledning att se över informationssäkerhetsfrågorna och att formerna och konsekvenserna av en överföring av Sitic ska utredas.

Enligt regeringens bedömning i budgetpropositionen (utgiftsområde 22 Kommunikationer) är informations-säkerhetsfrågor viktiga i den vardagliga IT-användningen och fokus bör ligga på förebyggande arbete och en höjd vardagssäkerhet för individer och företag. Konsumenter och små- och medelstora företag måste ha kunskap om vilka åtgärder de kan vidta för att öka sin säkerhet.

I den av riksdagen antagna propositionen Stärkt krisberedskap för säkerhets skull (prop. 2007/08:92, bet. 2007/08:FöU12, rskr. 2007/08:193) angav regeringen att den informationssäkerhetsverksamhet som funnits vid Krisberedskapsmyndigheten (KBM) skulle överföras till MSB och stärkas. Regeringen framförde även att informations-säkerhetsfrågorna är sektorsövergripande.

Det tvärsektoriella informationssäkerhetsarbetet bör bli mer renodlat. Ett färre antal inblandade aktörer ger bättre förutsättningar för ett mer sammanhållet informations-säkerhetsarbete. Detta innebär att verksamheterna hos Sitic och CSEC bör överföras till MSB eller FRA. Varje myndighet har enligt ansvarsprincipen att i första hand tillförsäkra den egna verksamheten en tillräcklig informationssäkerhet. Detta innebär dock inte att förtroendeskapande åtgärder som skapar tillit för informationssamhället hos medborgarna ska koncentreras till färre aktörer. Att arbeta med vardagssäkerheten i informationssamhället för att skapa förtroende är viktigt för att utnyttja den tekniska utvecklingens möjligheter på bästa sätt inom alla samhällsområden. Användningen av informationstekniken bidrar till bl.a. innovation och utveckling av nya tjänster vilket bidrar till tillväxt och konkurrenskraft.

Därför behöver många aktörer inom olika samhällssektorer arbeta för att förtroendet fortsatt vidareutvecklas och situationsanpassas på bästa sätt.

Sitics uppgift är att stödja samhället med att hantera och förebygga IT-incidenter. Arbetet omfattar bl.a. att bevaka trafikflöden i elektroniska kommunikationsnät, IT-incidentrapportering, rapportering om sårbarheter i system, att tillhandahålla olika testverktyg via nätet, seminarier m.m.. I uppgifterna ingår att agera skyndsamt vid inträffade IT-incidenter exempelvis genom att sprida information samt vid behov medverka i samordning av åtgärder som krävs för att avhjälpa eller lindra effekter av det inträffade, att samverka med relevanta nationella och internationella aktörer inom nätsäkerhetsområdet, att lämna råd och stöd avseende förebyggande arbete samt att vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder.

CSEC ansvarar för uppbyggnad, drift och förvaltning av ett system för evaluering och certifiering av IT-säkerhet i produkter och system i enlighet med standarden ISO/IEC IS 15408 (Common Criteria). CSEC som i dag bedriver sin verksamhet vid FMV stödjer såväl Försvarsmakten som det civila samhället på informationssäkerhetsområdet. CSEC är en autonom funktion inom FMV.

Krisberedskapsmyndigheten var Sveriges signatär inom CCRA[1] vilket bl.a. innebär att underteckna fördrag. CCRA är en internationell samarbetsorganisation som erkänner ömsesidigt utfärdade certifikat. Inom CCRA utvecklas såväl Common Criteria som metoder och regelverk för att stödja CCRA avtalet. För närvarande är 26 nationer medlemmar inom avtalet. I samband med inrättandet av MSB är signatärskapet en utestående fråga men MSB hanterar för närvarande de ärenden som ligger inom ramen för signatärskapet. En motsvarighet till CCRA är SOGIS-MRA[2] som också bygger på standarden Common Criteria där bara EU-länder kan ingå och där FMV är

[1] CCRA (Common Criteria Recognition Arrangement)
[2] SOGIS-MRA Senior Officials Group for Information Security – Mutual Recognition Agreement

signatär. Signatärskapet för SOGIS-MRA och CCRA bör utövas av samma myndighet.

Uppdraget

En särskild utredare ska i nära samverkan med MSB, FRA, PTS, Försvarsmakten, Polisen/Säkerhetspolisen, FMV, Swedac och övriga relevanta aktörer

- utreda och redovisa formerna för och konsekvenserna av en överföring av Sitics verksamhet till MSB eller FRA,
- utreda och redovisa formerna för och konsekvenserna av en överföring av CSEC:s verksamhet till MSB eller FRA med beaktande av gällande regler kring teknisk kontroll och principen om kontrollordningar i öppna system,
- utreda och ange vilken av myndigheterna MSB eller FRA som är bäst lämpad att vara ansvarig för CSEC och Sitic,
- föreslå en myndighet att vara signatär för både CCRA och SOGIS-MRA,
- redovisa kostnader och intäkter för de resp. verksamheter som ska flyttas och föreslå lämplig finansiering,
- redovisa eventuella rationaliseringar som kan uppstå i samband med samordningen, varvid engångskostnader som t. ex. kan uppstå i samband med flyttning, anpassning av nya eller avveckling av befintliga lokaler ska anges särskilt,
- lämna förslag till författningsändringar till följd av utredningens förslag, samt
- redovisa en tidsplan för ändrade ansvarsförhållanden och gemensam signatär.

Utredaren ska, utöver de verksamhetsmässiga och ekonomiska konsekvenserna även redovisa de personella konsekvenserna av sitt förslag.

Redovisning av uppdraget och andra utredningar

Utredaren ska fortlöpande hålla Regeringskansliet (Försvarsdepartementet) informerat om arbetets bedrivande. Utredaren ska beakta bl.a. det fortsatta arbetet med anledning av Stödutredningens rapport Ett användbart och tillgängligt försvar - Stödet till Försvarsmakten (Fö 2009:A), det arbete som Delegationen för e-förvaltning (2009:19) genomför samt Infosäkutredningens delrapport och betänkanden (SOU 2004:32, 2005:42, 2005:71).

Uppdraget ska redovisas senast den 22 januari 2010.

(Försvarsdepartementet)