Sammanfattning

Post- och telestyrelsen fick 2002 uppdraget att etablera en så kallad "rikscentral för IT-incidentrapportering". Verksamheten inom enheten Sitic byggdes upp successivt från 2003 och framåt. I enlighet med den ursprungliga uppgiftsformuleringen etablerades Sitic som en enhet inom PTS. Sitic har i dagsläget en personalstyrka på tio personer och en årlig budget på femton miljoner kronor. Verksamhet är etablerad i enlighet med den ursprungliga uppgiftsformuleringen och Sitic är idag en komplett, fungerande och internationellt etablerad CSIRT-organisation med verksamhet under kontorstid.

I 2006 års regleringsbrev fick Post- och telestyrelsen i uppdrag att lämna förslag på hur Sitics internationella roll kan stärkas, hur balansen mellan informationsspridning och rapportering bör se ut samt hur uppgifterna kan utvecklas. Förslag efterfrågas också på hur den modifierade verksamhetsinriktningen kan anges i Post- och telestyrelsens instruktion.

Rapporten beskriver en verksamhet strukturerad enligt en internationellt etablerad tjänstemodell. Innehåll och prioriteringar för den föreslagna verksamhetsprofilen grundas på flera underlag: Erfarenheter från de första årens aktiviteter inom Sitic, internationell utveckling inom området, erfarenheter från liknande organisationer, underlag från Sitics hittillsvarande målgrupp samt underlag från andra organisationer i Sitics närhet.

Den föreslagna verksamhetsprofilen innebär tydligare kategorisering av målgruppen, med tillhörande tjänstedifferentiering över målgruppens undergrupper. Verksamheten under kontorstid kompletteras med viss kvälls- och helgaktivitet samt med jour dygnet runt för en avgränsad del av incidenthanteringstjänsterna. Större kraft läggs på incidentrespons, samhällsviktig verksamhet samt aktivt bidragande till internationella samarbets- och utvecklingsprojekt. Tydligare fokus läggs på förmågan att inhämta underlag genom drift av system för trafikstudier. Egenproducerad periodstatistik ersätts med kontinuerlig lägesbild.

De högst prioriterade tjänsterna är de som inhämtar, behandlar eller sprider tidskritisk information och som har relevans för hela målgruppen. Därefter följer processinriktade tjänster med längre genomförandetider eller tjänster som rör åtgärder vid incidenter. Tredje och sista gruppen domineras av tjänster med djupt teknikinnehåll.

När det gäller juridiken bedöms nuvarande sekretesslagstiftning vara tillfyllest för Sitics ändamål, medan ett förtydligande kan behövas kring organisationens möjligheter till hantering av IP-adresser.

Den föreslagna verksamhetsprofilen förutsätter tilldelning av ytterligare medel.