Näringsdepartementet
Enheten för IT, forskning och utveckling
103 33 STOCKHOLM

Remissvar över rapporten Utveckling av Sitic, Sveriges IT-incidentcentrum

.SE har bjudits in att lämna synpunkter på ovanstående remiss.

Generella synpunkter

.SE anser att Sitic utför en viktig uppgift genom att sprida information om aktuella och akuta säkerhetsproblem till framför allt myndigheter och deras lokala säkerhetsansvariga. Verksamheten är än så länge mindre känd inom näringslivet och bland allmänheten.

Relevanta och aktuella rapporter om incidenter och sårbarheter är viktiga och centrala verktyg för alla som arbetar operativt med säkerhetsfrågor. Sitic behöver organiseras på ett sådant sätt att enskilda organisationer på ett enkelt sätt kan samverka med IT-incidenthanteringsfunktionen.

Något som många tidigare utredningar pekat på är vikten av att få till stånd en funktion där IT-säkerhetsarbetet kan **koordineras**. Området är under snabb utveckling och är för de allra flesta verksamheter alltför resurskrävande att bevaka helt på egen hand. För att få en överblick som kan ge underlag för säkerhetshöjande åtgärder eller för att kunna se trender, finns det behov av en möjlighet att rapportera incidenter till en central instans som har till uppgift att göra sammanställning och analys. I rapporten om utveckling av Sitic saknar .SE en redovisning av hur Sitic samverkar med andra myndigheter som har ansvar på området, och förslag till tydliga åtgärder i syfte att öka samverkan med andra ansvariga myndigheter för att förbättra funktionen som helhet.

Sitics uppdrag

En CERT (Computer Emergency Response Team) som Sitic ska ha till uppgift att koordinera säkerhetsproblem. En lämplig form är som "help desk" som via olika kanaler och distributionsformer sprider information och koordinerar insatser vid händelser som till exempel:

Stiftelsen för Internetinfrastruktur (.SE)

Postadress Box 7399, 103 91 STOCKHOLM
Besöksadress Ringvägen 100A, 9 tr, STOCKHOLM
Telefon 08-452 35 00
Telefax 08-452 35 02
Internet info@iis.se, www.se
Org. Nr 802405-0190

- intrångsförsök, intrång
- brister i programvaror och andra produkter
- problem med skadlig kod
- serverattacker mot till exempel webbservrar m.m.

Rapporteringen från Sitic sker idag per elektronisk post och på webbplatsen genom särskilda råd, blixtmeddelanden och kungörelser. Informationen har också kunnat göras avsevärt mer tillgänglig genom att man använder fler distributionsformer som t.ex. RSS.

.SE delar i stort bedömningen att Sitics roll beträffande inhämtning, behandling och spridning av tidskritisk säkerhetsrelaterad information kan behöva stärkas för att den ska fylla sin funktion. Samtidigt vill .SE erinra om att sådan information också kan köpas i form av kommersiella tjänster eller erhållas gratis genom öppna källor. I avsaknad av ett författningsmässigt stöd för att ålägga statliga myndigheter skyldighet att rapportera incidenter så är det inte självklart att en sådan funktion läggs inom myndighetssfären. Enligt .SE kan det kan trots detta ur ett samhällsperspektiv vara angeläget att en statlig myndighet som inte styrs av kommersiella intressen har ett utpekat ansvar att tillhandahålla sådan information alternativt peka ut andra källor till sådan information.

.SE saknar i förslagen en uppgift för Sitic att samla information om och hänvisa till ett nätverk av konsulter och produkter. Sitic bör enligt .SE även ha beredskap för att samverka inte bara med IP-operatörer utan även med organisationer som utvecklar och distribuerar säkerhetslösningar i Sverige, och virtuella organisationer som exempelvis Ubuntu/Debian.

En central funktion för hantering av IT-incidenter i Sverige bör långsiktigt kunna tjäna användarintressen hos stora, små och medelstora företag, offentlig förvaltning, utbildningsväsende, Internetleverantörer, andra organisationer och privatpersoner. Genom att samla resurserna kring dessa frågor minskar förhoppningsvis kostnader och problem med kompetensbrist i enskilda organisationer. Sitic kan bidra med kompetenshöjning i form av vägledning och rådgivning. För att en central funktion för IT-incidenter ska ha förutsättningar att lyckas måste emellertid också varje organisation etablera egna interna incidenthanteringsfunktioner. En viktig uppgift för Sitic blir då enligt .SE att ge råd och vägledning om hur sådana interna funktioner kan organiseras inom en verksamhet.

Gränsdragning till andra myndigheter ansvarsområden

Det finns idag fyra myndigheter som har ett utpekat ansvar för att stödja samhällets arbete med informationssäkerhet. Dessa myndigheter är Försvarets radioanstalt (FRA), Krisberedskapsmyndigheten (KBM-SEMA), Försvarets Materielverk (FMV) samt Post- och Telestyrelsen (PTS) som driver Sitic. Det faktum att flera aktörer är involverade i arbetet innebär både fördelar och nackdelar. Fördelen som .SE ser är att de sammanlagda resurserna för arbetet är relativt omfattande, och att myndigheternas olika roller och inbördes konkurrens tvingar fram kontinuerliga förbättringar i utbudet av service och tjänster. Nackdelen är att man med ett uppdelat ansvar riskerar att skapa en otydlig organisationsstruktur och bristande helhetssyn.

Enligt .SE:s uppfattning finns det en uppenbar risk för gränsdragningsproblem mot andra myndigheters uppgifter både när det gäller ansvarsfördelningen inom myndigheter med uppgifter inom informationssäkerhetsområdet och kanske framför allt mot brottsutredande myndigheter.

.SE saknar i rapporten en långsiktig strategi för Sitic, där man beskriver vägen fram till en nationell, sektorsövergripande funktion för IT-incidenthantering som bygger på lämplig ansvarsfördelning mellan aktörerna, på klarläggande av behovet av samarbete och kanaler för informationsutbyte samt på samverkan mellan ansvariga myndigheter och samverkan med aktörer inom den privata sektorn. Enligt .SE kan Sitic utforma strategin för och påverka de olika aktörerna inom området att ansluta sig till strategin för att eliminera eventuella svagheter och bygga upp en stark incidentberedskap hos myndigheter, företag och inom infrastrukturer för elektronisk kommunikation. En viktig samverkanspartner i det sammanhanget är Verva.

Omvärldsbevakning, forskning och utveckling

Sitics uppdrag bör enligt .SE även omfatta att hantera omvärldsbevakning i samarbete med de forskare och de företag som arbetar med säkerhet och incidentområdet. Sitic kan samtidigt initiera forskning inom området på universitet och högskolor. Sitic kan också vara den som initierar utbildning på området inom gymnasieskolan, högskolan, universiteten samt forskarutbildningen. Ett tidigare medvetandegörande hos medborgarna kommer sannolikt att innebära att antalet incidenter och följderna av varje incident kan komma att minska.

Såvitt .SE känner till medverkar Sitic inte i arbetet med öppna standarder inom säkerhetsområdet eller inom utveckling respektive granskning av fri programvara vilket också skulle kunna ingå i Sitics uppdrag.

.SE har inga synpunkter på förslag om Sitics internationella engagemang. Det förefaller lämpligt att Sitic är den myndighet som har kontakt med andra liknande myndigheter och organisationer internationellt för att utbyta information om händelser eller möjliga hot som konstateras i rapporten.

Sitics tjänster

I rapporten föreslås en ny verksamhetsstruktur för Sitic baserad på ett antal tjänster. Inom området reaktiva tjänster föreslås bl.a. objektanalys som innebär undersökning av ett objekt funnet på en dator som kan ha varit inblandad i en incident eller som använts för att kringgå säkerhetsanordningar. Beträffande den typen av analys är det enligt .SE:s bedömning viktigt att det finns en mycket tydlig gräns för när analys inte ska genomföras av Sitic utan överlämnas till polisen för brottsutredning.

Inom området Proaktiva tjänster anges bl.a. intrångsdetekteringstjänster som innefattar analys av data från intrångsdetekteringssystem. Vid sådan verksamhet finns det enligt .SE:s bedömning risk för gränsdragningsproblem gentemot polisens brottsutredande verksamhet. Inom området föreslås bland annat säkerhetsgranskningar eller bedömningar och intrångsdetekteringstjänster. Det föreslaget innebär enligt .SE:s bedömning inte bara en risk för gränsdragningsproblem gentemot Försvarets radioanstalt och dess ansvar för att tillhandahålla teknisk informa-

tionssäkerhetskompetens och stödja statliga myndigheter t.ex. med IT-säkerhetsanalyser och annat tekniskt stöd, utan också en uppenbar risk för att Sitics verksamhet kommer i konflikt med kommersiella aktörer och deras intressen.

Sitic skulle enligt .SE också kunna vara den myndighet som påpekar behovet av regler för incidentområdet och i viss mån övervakar att dessa regler följs. Till stöd för detta kan Sitic samverka med Verva vars föreskriftsrätt ger ett instrument att påverka införandet av åtgärder inom den offentliga förvaltningen.

.SE menar att förebyggande skyddsåtgärder är det mest effektiva skyddet mot IT-incidenter, och att incidenthantering inte kan ersätta utan bara komplettera sådana skyddsåtgärder. Det innebär dock inte självklart att det är Sitics uppgift att ge kvalificerat stöd vid utformningen av myndigheternas skyddsåtgärder. Även här riskerar man att komma i konflikt med kommersiella aktörer och deras intressen. Förebyggande skyddsåtgärder är en utmärkt uppgift för den privata marknaden i avtal med statliga myndigheter, efter väl specificerade krav och offentlig upphandling.

En sådan uppgift faller däremot väl inom Verva:s uppgift att bidra till en effektiv e-förvaltning som i sin helhet kännetecknas av hög produktivitet, god kvalitet och bra service till nytta för beslutsfattare, medborgare och näringsliv.

Inom området säkerhets- och kvalitetsstyrningstjänster nämns säkerhetskonsulttjänster som omfattar rådgivning beträffande informationssäkerhet till t.ex. myndigheter. Även vid utövande av den här typen av tjänst kan det enligt .SE:s bedömning finnas en risk för gränsdragningsproblem gentemot såväl FRA som KBM. FMV bedriver dessutom verksamhet kring evaluering och certifiering av IT-säkerhetsprodukter.

Incidenthantering utanför kontorstid

.SE har svårt att bedöma behovet av en utökad roll för Sitic som innebär bemanning 24/7/365. En utveckling i flera steg kan enligt .SE behöva anges. Att befinna sig i händelsernas centrum är något som främst operatörerna har möjlighet till. .SE föreställer sig dock att det kan finnas behov av en ”jourkontakt” på Sitic till vilken man kan vända sig. Att inrätta en fullständig skiftgång i verksamheten förefaller i .SE:s ögon vara ett mycket stort steg för vilket det krävs ett utförligare beslutsunderlag. Frekvensen blixtmeddelanden och särskilda råd ger t.ex. i sig inte några indikationer för att utöka verksamheten på ett sådant sätt.

Sitics hantering av personuppgifter

Uppgift om IP-adress kan utgöra personuppgift och .SE anser att en utredning bör företas innan man fastställer i vilken utsträckning Sitic kan behandla personuppgifter i sin verksamhet.

Konsekvensanalys

.SE har ingenting att invända mot att Sitic även i fortsättningen är en del av PTS verksamhet. När det gäller förslag till en ökad budget med fem miljoner mer än för nuvarande verksamhet så framgår inte vad den bedömningen baserar sig på. Det gör det svårt för .SE att bedöma rele-

vansen i den delen av förslaget. Samtidigt innebär förslagen i rapporten en viss omprioritering av verksamheten, vilket tyder på att verksamheten skulle kunna utvecklas inom ramen för den befintliga anslagsnivån.

Danny Aerts
VD