EN STEGVIS STRATEGI FÖR ATT INRÄTTA ETT CSIRT

Dokument WP2006/5.1(CERT-D1/D2)

Index

1 Sammanfattning

I detta dokument beskrivs utförligt hur man inrättar ett CSIRT (Computer Security and Incident Response Team), bland annat sådant som gäller företagsledning, processtyrning och teknik. Dokumentet omfattar två av de produkter som beskrivs i kapitel 5.1 i ENISA:s (Europeiska byrån för nät- och informationssäkerhet) arbetsprogram för 2006:

- Denna rapport: *Skriftlig rapport om en stegvis strategi för att inrätta en CERT (organisation för incidenthantering) eller liknande, inklusive exempel.* (**CERT-D1**)
- Kapitel 12 och externa filer: *Utdrag ur vägkarta i punktform som möjliggör en enkel tillämpning av vägkartan i praktiken.* (**CERT-D2**)

2 Rättsligt meddelande

3 Tack

ENISA vill tacka alla de institutioner och personer som bidragit med material. Ett särskilt tack går till följande:

- Henk Bronk, som i egenskap av konsult framställde den första versionen av dokumentet.
- CERT/CC och framför allt deras CSIRT-utvecklingsteam, som bidrog med mycket användbart material och exemplen på kursmaterial i bilagan.
- GovCERT.NL som tillhandahöll *CERT-in-a-box.*
- TRANSITS-teamet som bidrog med exemplen på kursmaterial i bilagan.

- Kollegerna från den tekniska avdelningens sektion för säkerhetspolicy som bidrog med kapitel 6.6.
- Alla de oräkneliga människor som har granskat detta dokument.

4 Inledning

Kommunikationsnät och informationssystem har blivit en avgörande faktor för den ekonomiska och sociala utvecklingen. Databehandling och nätverk börjar nu bli lika allmänt förekommande nyttigheter som el- och vattenförsörjning.

Kommunikationsnätens och informationssystemens säkerhet, och framför allt deras tillgänglighet, är därför något som uppmärksammas alltmer av samhället. I centrum för uppmärksamheten står risken för problem med centrala informationssystem på grund av deras komplexitet, olyckor, misstag och attacker på de fysiska infrastrukturer som tillhandahåller tjänster som är avgörande för EU-medborgarnas välbefinnande.

Den 10 mars 2004 inrättades ENISA, Europeiska byrån för nät- och informationssäkerhet ([1]). ENISA:s uppgift är att säkerställa en hög nivå på nät- och informationssäkerhet i gemenskapen och utveckla en kultur av nät- och informationssäkerhet till förmån för medborgare, konsumenter, företag och den offentliga sektorns organisationer i Europeiska unionen och på det sättet bidra till att den inre marknaden fungerar väl.

I flera år har ett antal säkerhetsorgan i Europa, såsom CERT/CSIRT-enheter, missbruksteam och WARP-grupper samarbetat för att skapa ett säkrare Internet. ENISA har för avsikt att stödja samtliga dessa organisationer i deras ansträngningar genom att tillhandahålla information om åtgärder för att säkra en god servicekvalitet. ENISA har dessutom för avsikt att förstärka sina möjligheter att ge EU:s medlemsstater och organ råd i frågor som gäller hur man förser särskilda grupper av IT-användare med lämpliga säkerhetstjänster. Denna nya arbetsgrupp bygger vidare på resultaten från ad hoc-arbetsgruppen CERT Cooperation and Support som inrättades 2005 och kommer följaktligen att ägna sig åt frågor som gäller hur man tillhandahåller lämpliga säkerhetstjänster (”CERT-tjänster”) åt särskilda (kategorier eller grupper av) användare.

ENISA stödjer bildandet av nya CSIRT-enheter genom att offentliggöra denna ENISA-rapport, *En stegvis strategi för att inrätta ett CSIRT med kompletterande checklista,* som kommer att hjälpa dig att inrätta ett eget CSIRT.

([1]) Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet. En ”gemenskapsbyrå” är ett organ som inrättas av EU för att utföra en mycket speciell teknisk, vetenskaplig eller styrande uppgift inom EU:s ”gemenskapsdomän” (första pelaren).

4.1 Målgrupper

De primära målgrupperna för denna rapport är statliga och andra institutioner som beslutar sig för att inrätta ett CSIRT för att skydda sin egen eller sina berörda parters IT-infrastruktur.

4.2 Hur man använder detta dokument

I detta dokument lämnas information om vad ett CSIRT är, vilka tjänster det kan erbjuda och vilka åtgärder som krävs för att komma igång. Det bör ge läsaren en bra och pragmatisk översikt över strategi, struktur och innehåll när det gäller att inrätta ett CSIRT.

Kapitel 4 *”Inledning”*
Inledningen till denna rapport.

Kapitel 5 *”Allmän strategi för att planera och inrätta ett CSIRT”*
I första avsnittet lämnas en beskrivning av vad ett CSIRT är. Det avsnittet innehåller också information om de olika miljöer som ett CSIRT kan arbeta i och vilka tjänster det kan erbjuda.

Kapitel 6 *”Att utarbeta affärsplanen”*
I detta kapitel beskrivs vilken ledningsstrategi som bör tillämpas i samband med inrättandet av ett CSIRT.

Kapitel 7 *”Att genomföra affärsplanen”*
Detta kapitel handlar om den affärsmässiga delen och finansieringsfrågor.

Kapitel 8 *”Exempel på operativa och tekniska förfaranden”*
I detta kapitel beskrivs hur man skaffar information och översätter den till en säkerhetsbulletin. Kapitlet innehåller också en beskrivning av ett arbetsflöde för incidenthantering.

Kapitel 9 *”CSIRT-utbildning”*
Kapitlet innehåller en sammanfattning av tillgänglig CSIRT-utbildning. Som en illustration visas exempel på utbildningsmaterial i bilagan.

Kapitel 10 *”Övning: att framställa en bulletin”*
Detta kapitel innehåller en övning i hur man utför en av de grundläggande (eller centrala) CSIRT-tjänsterna: att framställa en säkerhetsbulletin (eller ett säkerhetsmeddelande).

Kapitel 12 ”Beskrivning av projektplanen”
I detta kapitel hänvisas till den kompletterande projektplan (checklista) som medföljer denna guide. Planen är tänkt som ett användarvänligt verktyg för att tillämpa guiden.

4.3 Dispositionsregler för detta dokument

Som en vägledning för läsaren inleds varje kapitel med en sammanfattning av de steg som tagits dittills i processen för att inrätta ett CSIRT. Sammanfattningarna visas i rutor på följande sätt:

Vi har tagit det första steget.

Varje kapitel kommer att avslutas med ett praktiskt exempel på de steg som diskuterats. I detta dokument kommer vårt ”fiktiva CSIRT” att vara en liten, fristående CSIRT-enhet för ett medelstort företag eller en medelstor institution. En sammanfattning finns i bilagan.

Fiktivt CSIRT

5 Allmän strategi för att planera och inrätta ett CSIRT

För att processen att inrätta ett CSIRT ska få en bra start är det viktigt att man har en tydlig vision av de eventuella tjänster som teamet kan erbjuda sina kunder, i ”CSIRT-världen” mera kända som ”medlemmar”. Det är därför nödvändigt att förstå vad medlemmarna behöver för att kunna erbjuda rätt tjänster i rätt tid och till rätt kvalitet.

5.1 Vad är ett CSIRT?

Förkortningen CSIRT står för *Computer Security Incident Response Team*. CSIRT används allmänt i Europa i stället för den skyddade termen CERT, som har registrerats i USA av CERT Coordination Center (CERT/CC).
Det finns flera olika förkortningar som används för samma typ av team:

- CERT eller CERT/CC (Computer Emergency Response Team/Coordination Center)
- CSIRT (Computer Security Incident Response Team)
- IRT (Incident Response Team)
- CIRT (Computer Incident Response Team)
- SERT (Security Emergency Response Team)

Den första större attacken från en ”mask” i den globala IT-infrastrukturen ägde rum i slutet av 1980-talet. Masken döptes till Morris ([2]) och den spreds snabbt och smittade ett stort antal IT-system världen över.

Denna incident blev en väckarklocka: plötsligt blev människor medvetna om att det fanns ett stort behov av samarbete och samordning mellan systemadministratörer och IT-chefer för att hantera liknande fall. Eftersom tiden var en avgörande faktor måste man etablera en mer organiserad och strukturerad strategi för att hantera IT-säkerhetsincidenter. Och ett par dagar efter ”Morrisincidenten” inrättade DARPA (Defence Advanced Research Projects Agency) därför ett första CSIRT: CERT/CC ([3]), (CERT Coordination Center) på Carnegie Mellon-universitetet i Pittsburgh (Pennsylvania).

Den här modellen infördes snart i Europa, och 1992 startade den nederländska akademiska Internetleverantören SURFnet Europas första CSIRT med namnet SURFnet-CERT ([4]). Många team följde därefter, och för närvarande upptar ENISA:s *Inventory of CERT activities in Europé* ([5]) (Förteckning över CERT-aktiviteter i Europa) över 100 kända europeiska team.

Med åren har CERT-enheterna utökat sin verksamhet från att vara rena utryckningsstyrkor till att bli leverantörer av kompletta säkerhetstjänster, inklusive preventiva tjänster, såsom varningar, säkerhetsbulletiner, utbildning och tjänster inom säkerhetshantering. Termen ”CERT” betraktades snart som otillräcklig. Följaktligen

([2]) Mer information om masken Morris finns på http://en.wikipedia.org/wiki/Morris_worm

([3]) CERT-CC, http://www.cert.org

([4]) SURFnet-CERT: http://cert.surfnet.nl/

([5]) ENISA:s förteckning: http://www.enisa.europa.eu/cert_inventory/

infördes den nya termen ”CSIRT” i slutet av 1990-talet. För tillfället används båda termerna (CERT och CSIRT) synonymt, men CSIRT är en mer exakt beteckning.

5.1.1 Termen *basgrupp*

I fortsättningen kommer den (i CSIRT-sammanhang) väletablerade termen ”basgrupp” att användas för att beteckna kundbasen för en viss CSIRT-enhet. En enskild kund kommer att betecknas ”medlem”, en grupp av kunder ”basgrupp”.

5.1.2 Definition av ett CSIRT

Ett CSIRT är ett team av experter på IT-säkerhet, som har till huvuduppgift att reagera på datasäkerhetsincidenter. Teamet tillhandahåller de tjänster som krävs för att hantera incidenterna och hjälpa sina medlemmar att återhämta sig efter intrång.

För att minska riskerna och minimera antalet insatser som krävs tillhandahåller de flesta CSIRT dessutom förebyggande och pedagogiska tjänster åt sin basgrupp. De skickar ut instruktioner om luckor i den program- och hårdvara som används, samt informerar användarna om olika virus som utnyttjar dessa luckor så att medlemmarna snabbt kan täppa till luckorna och uppgradera sina system. Se kapitel *5.2 Tänkbara tjänster* för en komplett förteckning över möjliga tjänster.

5.1.3 Fördelarna med att ha ett CSIRT

Att ha ett dedicerat IT-säkerhetsteam hjälper en organisation att mildra effekterna av och att förebygga allvarliga incidenter. Det bidrar också till att skydda organisationens värdefulla tillgångar.

Bland övriga tänkbara fördelar:

- Att ha en central samordning för IT-säkerhetsfrågor inom organisationen, en kontaktpunkt (PoC, Point of Contact).
- Centraliserad och specialiserad hantering av och reaktion på IT-incidenter.
- Expertis finns till hands för att stödja och hjälpa användarna att snabbt återställa sina system efter säkerhetsincidenter.
- Hantera rättsliga frågor och förvara bevis inför en eventuell rättegång.
- Följa utvecklingen inom säkerhetsområdet.
- Stimulera samarbetet inom basgruppen om IT-säkerhet (bygga upp medvetenheten).

Fiktivt CSIRT (steg 0)
Att förstå vad ett CSIRT är: Vårt fiktiva CSIRT ska betjäna en medelstor institution med 200 anställda. Institutionen har en egen IT-avdelning och två andra lokalkontor i samma land. IT spelar en avgörande roll för företaget, eftersom det används för internkommunikation, datanät och e-handel dygnet runt, sju dagar i veckan. Institutionen har ett eget nätverk och en redundant Internetanslutning via två olika tjänsteleverantörer.

5.1.4 Beskrivning av de olika typerna av CSIRT-miljöer

Vi har tagit det första steget.

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.

>> Nästa steg blir att besvara följande fråga: ”Vilka sektorer kommer CSIRT-tjänsterna att levereras till?”

När man startar ett CSIRT (precis som alla andra verksamheter) är det mycket viktigt att man snabbt får en klar bild av vilka medlemmarna är och vilken miljö CSIRT-tjänsterna ska utvecklas för. För tillfället kan vi urskilja följande ”CSIRT-sektorer”:

- Akademisk sektor
- Kommersiell sektor
- CIP/CIIP-sektor
- Statlig sektor
- Internt
- Militär sektor
- Nationellt
- Små och medelstora företag
- Försäljare

Akademisk sektor
Fokus
Ett CSIRT för den akademiska sektorn erbjuder CSIRT-tjänster åt akademiska institutioner och utbildningsinstitutioner, såsom universitet och forskningsinstitutioner och deras Internetmiljöer på campus.

Medlemmar
Typiska medlemmar i denna typ av CSIRT är universitetens personal och studenter.

Kommersiell sektor
Fokus
Ett kommersiellt CSIRT erbjuder CSIRT-tjänster mot betalning åt sina medlemmar. Om det gäller en tjänsteleverantör erbjuder CSIRT i första hand missbrukstjänster åt slutanvändare (inval, ADSL) och CSIRT-tjänster åt deras professionella kunder.

Medlemmar
Kommersiella CSIRT levererar i regel sina tjänster åt medlemmar som betalar för dem.

CIP/CIIP-sektorn
Fokus
Ett CSIRT inom denna sektor fokuserar i första hand på skydd av kritisk information och/eller skydd av kritisk information och infrastruktur. I de flesta fall samarbetar denna specialiserade CSIRT nära med en statlig CIIP-enhet. Den täcker alla viktiga IT-sektorer i landet och skyddar landets medborgare.

Medlemmar
Regeringar, viktiga IT-företag, medborgare.

Statlig sektor
Fokus
Ett statligt CSIRT erbjuder sina tjänster åt statliga organ och i vissa länder åt medborgarna.

Medlemmar
Regeringar och statliga organ. I vissa länder erbjuds också varningstjänster åt medborgarna (till exempel i Belgien, Ungern, Nederländerna, Storbritannien och Tyskland).

Internt
Fokus
Ett internt CSIRT erbjuder enbart tjänster åt sin värdorganisation. Detta beskriver mer funktionen än en sektor. Många telekommunikationsorganisationer och banker har till exempel ett eget internt CSIRT. De har i regel ingen webbplats som är öppen för allmänheten.

Medlemmar
Värdorganisationens interna personal och IT-avdelning.

Militär sektor
Fokus
Ett CSIRT inom den militära sektorn erbjuder tjänster åt militära organisationer med ansvar för den IT-infrastruktur som krävs för försvarsändamål.

Medlemmar
Personalen på militära institutioner eller nära anslutna enheter, till exempel försvarsministeriet.

Nationell sektor
Fokus
Ett CSIRT med nationellt fokus som betraktas som en säkerhetskontaktpunkt för ett visst land. I vissa fall kan ett statligt CSIRT även fungera som en nationell kontaktpunkt (som UNIRAS i Storbritannien).

Medlemmar
Den här typen av CSIRT har i regel inga direkta medlemmar, eftersom ett nationellt CSIRT enbart spelar en förmedlande roll för hela landet.

Små och medelstora företag
Fokus
Ett CSIRT som organiserats av och som erbjuder sina tjänster åt sin egen grupp av företag eller en liknande användargrupp.

Medlemmar
Medlemmarna i denna typ av CSIRT kan vara små och medelstora företag och deras personal eller särskilda intressegrupper, såsom ett lands stads- och kommunföreningar.

Försäljare
Fokus
Ett försäljar-CSIRT fokuserar på att lämna support på försäljarspecifika produkter. Syftet är i regel att utveckla och tillhandahålla lösningar för att avlägsna säkerhetsluckor och lindra de potentiellt negativa effekterna av olika brister.

Medlemmar
Produkternas ägare.

Som vi beskrivit i avsnittet om nationella CSIRT är det möjligt för ett visst team att betjäna flera sektorer än en. Detta får betydelse för bland annat analysen av basgruppen och dess behov.

Fiktivt CSIRT (steg 1)
Startfasen I startfasen planeras vårt nya CSIRT som ett internt CSIRT som ska tillhandahålla tjänster åt värdföretaget, den lokala IT-avdelningen och personalen. Det stödjer och samordnar dessutom hanteringen av incidenter som gäller IT-säkerhet mellan de olika lokalkontoren.

5.2 Tänkbara tjänster som ett CSIRT kan leverera

Vi har tagit de första två stegen.

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska leverera sina tjänster till.

>> Nästa steg blir att besvara följande fråga: ”Vilka tjänster ska erbjudas medlemmarna?”

Ett CSIRT kan tillhandahålla många olika tjänster, men hittills finns det inget CSIRT som tillhandahåller samtliga. Att bestämma urvalet av lämpliga tjänster blir därför ett viktigt beslut. Nedan finns en kortfattad översikt över alla kända CSIRT-tjänster enligt definitionen i ”Handbook for CSIRTs” (Handbok för CSIRT-enheter) som publicerats av CERT/CC ([6]).

([6]) CERT/CC:s CSIRT-handbok http://www.cert.org/archive/pdf/csirt-handbook.pdf

Reaktiva tjänster	***Proaktiva tjänster***	***Artefakthantering***
• Larm och varningar • Incidenthantering • Incidentanalys • Stöd för incidentrespons • Samordning av incidentrespons • Incidentrespons på plats • Sårbarhetshantering • Sårbarhetsanalys • Sårbarhetsrespons • Samordning av sårbarhetsrespons	• Meddelanden • Teknikbevakning • Säkerhetsrevision eller kontroll • Säkerhetens utformning och underhåll • Utveckling av säkerhetsverktyg • Detektering av inkräktare • Spridning av säkerhetsrelaterad information	• Artefaktanalys • Artefaktrespons • Samordning av artefaktrespons
		Säkerhetskvalitets-styrning
		• Riskanalys • Kontinuitet och katastrofåterställning • Säkerhetsrådgivning • Medvetandebyggande • Utbildning • Utvärdering och certifiering av produkter

Fig. 1. Förteckning över CSIRT-tjänster från CERT/CC ([7])

Kärntjänsterna (markerade med fetstil): det görs en åtskillnad mellan reaktiva och proaktiva tjänster. De proaktiva tjänsterna syftar till att förebygga incidenter genom att öka medvetenheten och utbilda, medan de reaktiva tjänsterna syftar till att hantera incidenter och lindra de skador som uppkommer.

Artefakthantering omfattar analysen av en viss fil eller ett visst objekt som upptäcks i ett system och som skulle kunna utgöra en del av skadlig verksamhet, t.ex. rester av virus, maskar, skript, trojaner etc. Det omfattar också att hantera och distribuera den information som blir resultatet till försäljare och andra intresserade parter för att förebygga ytterligare spridning av skadlig programvara och för att lindra riskerna.

Säkerhets- och kvalitetshanteringstjänster är tjänster med mer långsiktiga mål och inkluderar rådgivning och utbildning.

Se den detaljerade förklaringen av CSIRT-tjänster i bilagan.

Att välja rätt tjänster för dina medlemmar är ett viktigt steg, och det kommer att behandlas ytterligare i kapitel *6.1 Att definiera finansieringsmodellen*.

De flesta CSIRT-enheter börjar med att distribuera ”Larm och varningar”, utfärda ”Meddelanden” och tillhandahålla ”Incidenthantering” åt sina medlemmar. Dessa kärntjänster ger i regel teamet en bra profil och stor uppmärksamhet gentemot medlemmarna och betraktas i regel som ett reellt ”mervärde”.

En bra rutin är att starta med en liten grupp av ”pilotmedlemmar”, tillhandahålla kärntjänsterna under en pilotperiod och begära in feedback efteråt.

([7]) Förteckning över CSIRT-tjänster från CERT/CC: http://www.cert.org/csirts/services.html

Intresserade pilotanvändare lämnar i regel konstruktiv feedback och hjälper till att utveckla skräddarsydda tjänster.

Fiktivt CSIRT (steg 2)
Att välja rätt tjänster I startfasen bestämde vi att vårt nya CSIRT i första hand skulle fokusera på att erbjuda några av kärntjänsterna åt de anställda. Vi har bestämt att en utvidgning av tjänsteportföljen efter pilotfasen kan bli aktuell och att vissa ”säkerhetsadministrativa tjänster” skulle kunna läggas till. Det beslutet kommer att fattas på grundval av feedback från pilotmedlemmarna och i nära samarbete med avdelningen för kvalitetsstyrning.

5.3 Analys av basgruppen och formulering av uppdraget

Vi har tagit de första tre stegen:

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska leverera sina tjänster till.
3. Att bestämma vilka typer av tjänster ett CSIRT kan erbjuda sin basgrupp.

>> Nästa steg blir att besvara följande fråga: ”Vilken strategi bör väljas för att starta vårt CSIRT?”

Nästa steg blir en grundligare analys av basgruppen i syfte att välja rätt kommunikationskanaler:

- Definiera strategin för att kommunicera med basgrupperna.
- Ange uppdraget.
- Utarbeta en realistisk genomförande- eller projektplan.
- Bestämma CSIRT-tjänster.
- Bestämma organisationsstrukturen.
- Bestämma policy för informationssäkerhet.
- Anställa rätt personal.
- Använda CSIRT-kontoret.
- Undersöka möjligheterna till samarbete mellan andra CSIRT och eventuella nationella initiativ.

Dessa steg kommer att beskrivas mer i detalj i följande avsnitt och kan användas som underlag för affärs- och projektplanen.

5.3.1 Kommunikationsstrategi för basgruppen

Som vi har sagt tidigare är det mycket viktigt att känna till basgruppens behov och den egna kommunikationsstrategin, inklusive vilka kommunikationskanaler som är de lämpligaste för att nå basgruppen med information.

Inom managementteorin finns det många olika strategier för att lösa problemet att analysera en målgrupp. I det här dokumentet beskriver vi två av dem: SWOT- och PEST-analys.

SWOT-analyser
En SWOT-analys är ett strategiskt planeringsverktyg som används för att analysera starka sidor, svagheter, möjligheter och hot (**S**trengths, **W**eaknesses, **O**pportunities and **T**hreats) i samband med ett projekt eller en affärssatsning eller i någon annan situation som kräver ett beslut. Tekniken brukar tillskrivas Albert Humphrey, som ledde ett forskningsprojekt vid Stanforduniversitetet på 1960- och 1970-talen som byggde på data från företagen på Fortune 500 ([8]).

Starka sidor	**Svagheter**
Möjligheter	**Hot**

Fig. 2. SWOT-analys.

([8]) SWOT-analys på Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

PEST-analys

PEST-analysen är ett annat viktigt och allmänt använt verktyg för att analysera basgruppen i syfte att förstå de **P**olitiska, **E**konomiska, **S**ociokulturella och **T**ekniska faktorerna i den miljö där ett CSIRT är verksamt. PEST-analysen kan hjälpa till att bestämma om planeringen fortfarande ligger i linje med miljön och hjälper förmodligen till att undvika åtgärder som vidtas på felaktiga grunder.

Politiska	**Ekonomiska**
• Ekologiska frågor/miljöfrågor • Gällande lagstiftning, hemmamarknaden • Framtida lagstiftning • Europeisk/internationell lagstiftning • Tillsynsorgan och processer • Statlig politik • Mandatperiod och förändring • Handelspolicy • Finansiering, bidrag och initiativ • Lobby/intressegrupper, hemmamarknad • Internationella intressegrupper	• Ekonomisk situation hemma • Ekonomiska trender hemma • Ekonomier och trender utomlands • Allmänna skattefrågor • Beskattning typisk för produkt/tjänster • Säsongsvariationer/klimatfrågor • Marknads- och handelscykler • Specifika branschfaktorer • Marknadsrutter och distributionstrender • Motivation för kund/slutanvändare • Räntenivåer och växelkurser
Sociala	**Tekniska**
• Livsstilstrender • Demografiska trender • Konsumentattityder och -åsikter • Mediesynpunkter • Lagändring som påverkar sociala faktorer • Varumärkes-, företags- och teknikimage • Konsumenternas köpmönster • Mode och förebilder • Viktiga händelser och inflytanden • Köptillträde och trender • Etniska/religiösa faktorer • Reklam och publicitet	• Konkurrerande teknikutveckling • Forskningsfinansiering • Näraliggande/beroende teknikområden • Ersättningsteknik/ersättningslösningar • Teknikens mogenhetsgrad • Tillverkningens mogenhetsgrad och kapacitet • Information och kommunikation • Kundernas köpmekanismer/-teknik • Teknisk lagstiftning • Innovationspotential • Tekniktillträde, licenser, patent • Immateriella rättigheter

Fig. 3. Modell för PEST-analys

En detaljerad beskrivning av PEST-analysen finns i Wikipedia ([9]).

Båda verktygen ger en heltäckande och strukturerad bild av basgruppernas behov. Resultaten kommer att komplettera affärsförslaget och därigenom bidra till att erhålla finansiering för att upprätta ett CSIRT.

Kommunikationskanaler

En viktig fråga att ta med i analysen är de tänkbara metoderna för kommunikation och informationsspridning (”Hur kommunicerar man med basgruppen?”)

Om möjligt bör man överväga regelbundna personliga besök hos basgruppens medlemmar. Det är ett känt faktum att personliga möten underlättar samarbetet. Om båda sidor är villiga att samarbeta kommer dessa möten att leda till en öppnare relation.

([9]) PEST-analys på Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

I regel driver ett CSIRT en hel uppsättning kommunikationskanaler. Följande har visat sig vara användbart i praktiken och kan vara värt att pröva:

- Offentlig webbplats
- Slutet medlemsområde på webbplatsen
- Digitala blanketter för att rapportera incidenter
- Sändlistor
- Personlig e-post
- Telefon/fax
- Sms
- Gamla hederliga pappersbrev
- Månads- eller årsrapporter

Förutom att använda e-post, digitala blanketter, telefon eller fax för att underlätta incidenthanteringen (för att få incidentrapporter från basgruppen, samordna med andra team eller ge feedback och stöd åt offret) offentliggör de flesta CSIRT sina säkerhetsbulletiner på en offentligt tillgänglig webbplats och via sändlistor.

! Helst ska informationen skickas på ett säkert sätt. E-post kan till exempel undertecknas digitalt med PGP, och känsliga incidentuppgifter ska alltid skickas krypterade.

Se punkt *8.5 Tillgängliga CSIRT-verktyg* för mer information. Se också kapitel *2.3* i *RFC2350 ([10])*.

Fiktivt CSIRT (steg 3 a)
Att göra en analys av basgruppen och lämpliga kommunikationskanaler

En idékläckningssession med nyckelpersoner från ledningen och basgruppen gav tillräckligt med material för en SWOT-analys. Detta ledde till slutsatsen att det fanns behov av följande centrala tjänster:

- Larm och varningar
- Incidenthantering (analys, åtgärdsstöd och samordning av åtgärder)
- Meddelanden

Man måste se till att informationen fördelas på ett väl organiserat sätt för att nå en så stor del av basgruppen som möjligt. Därför fattas beslutet att larm, varningar och meddelanden i form av säkerhetsbulletiner ska offentliggöras på en särskild webbplats och distribueras via en sändlista. Ett CSIRT underlättar e-post, telefon och fax för att ta emot incidentrapporter. En enhetligt utformad webbplats planeras för nästa steg.

Se nästa sida för ett exempel på SWOT-analys.

([10]) http://www.ietf.org/rfc/rfc2350.txt

Starka sidor • Det finns vissa kunskaper inom företaget. • De anställda gillar planen och är villiga att samarbeta. • Stöd och finansiering från ledningen.	**Svagheter** • Inte mycket kommunikation mellan olika avdelningar och lokalkontor. • Ingen samordning med IT-incidenter. • Många ”småavdelningar”.
Möjligheter • Stort flöde av ostrukturerad sårbarhetsinformation. • Stort behov av samordning. • Minskade förluster på grund av incidenter. • Många lösa trådar i samband med IT-säkerhet. • Utbilda personalen om IT-säkerhet.	**Hot** • Inte så mycket pengar tillgängliga. • Liten personal. • Stora förväntningar. • Kulturen.

Fig. 4. Exempel på SWOT-analys.

5.3.2 Formulering av uppdraget

Efter en analys av basgruppens behov och önskningar rörande CSIRT-tjänster bör nästa steg bli att formulera uppdraget.

Uppdragsbeskrivningen beskriver organisationens grundfunktion i samhället utifrån de produkter och tjänster som den erbjuder basgruppens medlemmar. Genom uppdragsbeskrivningen kan förekomst och funktion kommuniceras tydligt för en ny CSIRT.

Det är bra om man kan göra uppdragsbeskrivningen kompakt, men inte för snäv, eftersom den förmodligen kommer att förbli oförändrad under ett par år.

Här följer ett par exempel av uppdragsbeskrivningar från befintliga CSIRT:

“<Namn på CSIRT> tillhandahåller information och hjälper <basgruppen (definiera medlemmarna)> att genomföra proaktiva åtgärder för att minska risken för datasäkerhetsincidenter samt reagera på sådana incidenter om de inträffar.”

”För att hjälpa <basgruppens medlemmar> att förebygga och reagera på IT-relaterade säkerhetsincidenter.” ([11])

([11]) Uppdragsbeskrivningen för Govcert.nl: http://www.govcert.nl

Uppdragsbeskrivningen är ett mycket viktigt och nödvändigt steg att börja med. Se punkt *2.1* i *RFC2350 ([12])* för en mer detaljerad beskrivning av vilken information ett CSIRT bör offentliggöra.

Fiktivt CSIRT (steg 3 b)
Ledningen för vårt fiktiva CSIRT har formulerat följande uppdragsbeskrivning: *”Vårt fiktiva CSIRT tillhandahåller information åt och hjälper de anställda i värdföretaget att minska riskerna för datasäkerhetsincidenter och reagera på sådana incidenter när de inträffar.”* Genom uppdragsbeskrivningen gör vårt fiktiva CSIRT klart att det är ett internt CSIRT och att dess kärnverksamhet är att hantera frågor i samband med IT-säkerhet.

([12]) http://www.ietf.org/rfc/rfc2350.txt

6 Att utarbeta affärsplanen

Vi har tagit följande steg:

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska leverera sina tjänster till.
3. Att bestämma vilka typer av tjänster ett CSIRT kan erbjuda sin basgrupp.
4. Analys av miljö och basgruppens medlemmar.
5. Formulering av uppdragsbeskrivningen.

>> Nästa steg blir att definiera affärsplanen.

Resultatet av analysen ger dig en bra överblick över basgruppens behov och (antagna) svagheter, så den informationen används som ingångsdata för nästa steg.

6.1 Att definiera finansieringsmodellen

Efter analysen valdes ett antal centrala tjänster ut för att starta med. Nästa steg är att fundera på finansieringsmodellen: vilka parametrar för tjänsteutbudet är både lämpliga och lönande?

I en perfekt värld skulle finansieringen anpassas efter basgruppens behov, men i verkligheten måste den portfölj av tjänster som kan erbjudas anpassas efter en viss given budget. Därför är det mera realistiskt att börja planera ekonomiska frågor.

6.1.1 Kostnadsmodell

De båda viktigaste faktorerna som påverkar kostnaderna är fastställandet av antalet arbetstimmar och antalet personer som ska anställas (och deras kvalitet). Finns det ett behov av att leverera incidentrespons och teknisk support dygnet runt, sju dagar i veckan, eller kommer dessa tjänster enbart att erbjudas under kontorstid?

Beroende på kontorsutrustningens önskade tillgänglighet (är det till exempel möjligt att arbeta från hemmet?) kan det vara lämpligt att arbeta med jourberedskap eller fast tjänstgöring.

Ett tänkbart scenario är att man erbjuder både proaktiva och reaktiva tjänster under kontorstid. Efter kontorstid erbjuds enbart begränsade tjänster, till exempel enbart i samband med större katastrofer och incidenter av en anställd som har jour.

Ett annat alternativ är att försöka bygga upp ett internationellt samarbete med andra CSIRT-enheter. Det finns redan exempel på fungerande samarbete efter principen ”följ solen”. Samarbete mellan europeiska och amerikanska team har till exempel visat sig vara fruktbara och ett bra sätt att utnyttja varandras kapacitet. Sun Microsystems CSIRT som har flera lokalkontor i olika tidszoner världen över (men där samtliga ingår i samma CSIRT) kan till exempel erbjuda tjänster dygnet runt sju dagar i veckan genom att hela tiden flytta uppgifterna mellan teamen världen över. Detta sänker kostnaderna, eftersom

teamen alltid enbart arbetar under normal kontorstid och även erbjuder tjänster åt sin ”sleeping partner” på andra sidan jorden.

Det är alltid en bra idé att göra en grundlig analys av behovet av service dygnet runt, sju dagar i veckan i hela basgruppen. Larm och varningar som skickas ut under natten är knappast meningsfulla om mottagaren läser dem först nästa morgon. Det går en fin skiljelinje mellan att ”behöva en tjänst” och att ”vilja ha en tjänst”, men framför allt arbetstiden gör en enorm skillnad i antalet anställda och den utrustning som behövs och får därför stor betydelse för kostnadsmodellen.

6.1.2 Intäktsmodellen

När man väl känner till kostnaderna är det bra som nästa steg att fundera på tänkbara intäktsmodeller: hur kan de planerade tjänsterna finansieras? Nedan följer ett par tänkbara scenarier att analysera.

Användning av befintliga resurser
Det är alltid en bra idé att analysera de befintliga resurserna i andra delar av företaget. Finns det redan lämplig personal (till exempel i den befintliga IT-avdelningen) med den bakgrund och de kunskaper som behövs? Det går förmodligen att komma överens med ledningen om att låna ut den personalen till CSIRT-enheten under startfasen, eller så kan de ge support åt vårt CSIRT vid behov.

Medlemsavgift
En annan möjlighet är att sälja dina tjänster till basgruppens medlemmar genom en års- eller kvartalsavgift. Ytterligare tjänster skulle kunna betalas per användningstillfälle, till exempel konsulttjänster eller säkerhetsrevisioner.

Ett annat tänkbart scenario: tjänster för (den interna) basgruppen erbjuds gratis, men tjänster som levereras till externa kunder måste betalas. En annan idé är att offentliggöra råd och informationsbulletiner på den offentliga webbplatsen och ha en sektion enbart för medlemmar med speciell, mer detaljerad eller skräddarsydd information.

Det har i praktiken visat sig att ”prenumeration per CSIRT-tjänst” endast har begränsad effekt för att tillhandahålla tillräcklig finansiering, framför allt under startfasen. Det finns till exempel fasta baskostnader för teamet och utrustningen som måste betalas i förskott. Att finansiera dessa kostnader genom att sälja CSIRT-tjänster är svårt och kräver en mycket detaljerad finansiell analys för att man ska hitta ”den kritiska punkten”.

Bidrag
En annan möjlighet som det kunde vara värt att undersöka är att söka projektbidrag från staten eller ett statligt organ, eftersom de flesta länder nu för tiden har särskilda fonder för IT-säkerhetsprojekt. Att kontakta inrikesministeriet kan vara en bra start.

Man kan naturligtvis tänka sig en kombination av olika intäktsmodeller.

6.2 Att bestämma organisationsstrukturen

Vilken organisationsstruktur som är lämplig för ett CSIRT beror i hög grad på värdorganisationens och basgruppens befintliga strukturer. Den beror också på tillgången på skickliga experter som ska få fast eller tillfällig anställning.

I ett typiskt CSIRT återfinns följande roller i teamet:

Allmänt
- Verkställande direktör

Personal
- Kontorschef
- Räkenskapsförare
- Kommunikationskonsult
- Juristkonsult

Operativt tekniskt team
- Teknisk teamchef
- CSIRT-tekniker som levererar CSIRT-tjänsterna
- Analytiker

Externa konsulter
- Anställs vid behov

Det underlättar oerhört om man har en juridisk expert i teamet, framför allt när man startar ett CSIRT. Det innebär ökade kostnader, men i slutändan sparar man tid och slipper rättsliga problem.

På grund av den stora mångfalden av experter i basgruppen, och också när CSIRT har en hög medieprofil, har det visat sig mycket klokt att även ha en kommunikationsexpert i teamet. Dessa experter kan fokusera på att översätta svåra tekniska frågor till lättbegripligare budskap för basgruppens medlemmar eller partner inom medier. Kommunikationsexperten förmedlar också feedback från basgruppen till de tekniska experterna, så han/hon kan fungera som ”översättare” och ”moderator” mellan de båda grupperna.

Nedan följer ett par exempel på organisationsmodeller som används i fungerande CSIRT.

6.2.1 Den fristående affärsmodellen

Detta CSIRT läggs upp och fungerar som en fristående organisation med egen ledning och personal.

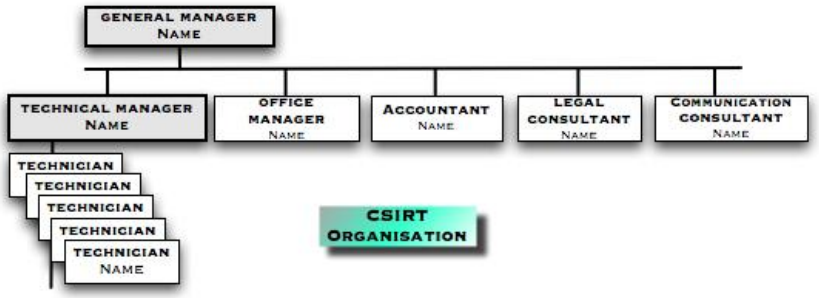


Fig. 5. Fristående affärsmodell.

6.2.2 Den inbäddade modellen

Denna modell kan utnyttjas om ett CSIRT ska inrättas inom ramen för en redan befintlig organisation, till exempel med utnyttjande av en befintlig IT-avdelning. Detta CSIRT leds av en teamledare som har ansvar för aktiviteterna i CSIRT. Teamledaren samlar de tekniker som krävs när man löser incidenter eller arbetar med CSIRT-aktiviteter. Han eller hon kan begära assistans inom den befintliga organisationen för specialiststöd.

Den här modellen kan också anpassas till speciella situationer när sådana uppkommer. I det här fallet har ett fast antal personer eller heltidsekvivalenter avsatts till teamet. Klagomuren hos en tjänsteleverantör är till exempel ett heltidsjobb för en eller (i de flesta fall) mer än en heltidsekvivalent.

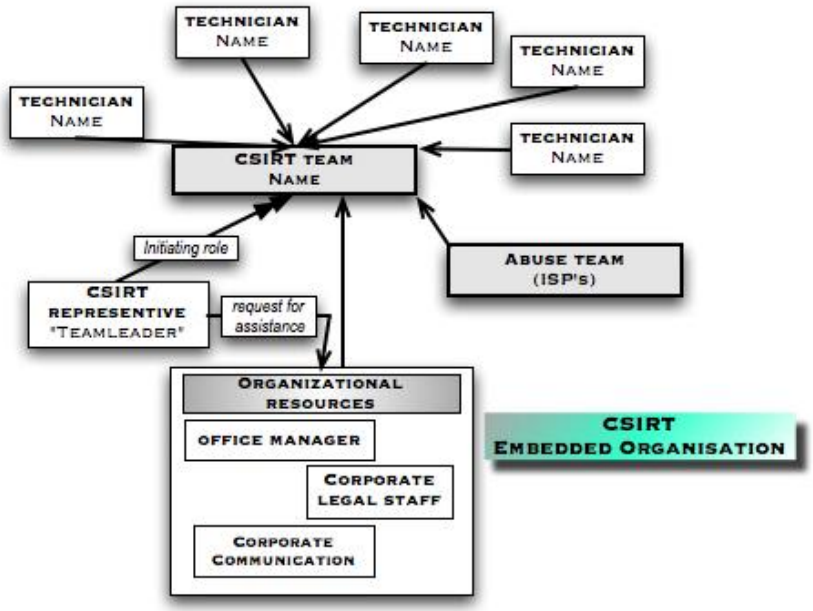


Fig. 6. Inbäddad organisationsmodell.

6.2.3 Campusmodellen

Campusmodellen används som namnet antyder i första hand av CSIRT inriktade på universitet och forskningsinstitutioner. De flesta akademiska organisationer och forskningsorganisationer består av olika universitet och anläggningar på olika platser, utspridda över en region eller till och med ett helt land (som i fallet NREN, National Research Networks). I regel är dessa organisationer fristående från varandra, och de driver ofta sina egna CSIRT. Dessa CSIRT är ofta organiserade under ett moder- eller kärn-CSIRT. Ett sådant kärn-CSIRT samordnar och är enda kontaktpunkt med omvärlden. I de flesta fall kommer ett kärn-CSIRT också att tillhandahålla centrala CSIRT-tjänster, förutom att distribuera incidentinformation till rätt campus-CSIRT.

I vissa CSIRT som byggts upp på det här viset roterar de centrala CSIRT-tjänsterna bland olika campus-CSIRT, vilket ger lägre fasta kostnader för kärnenheten.

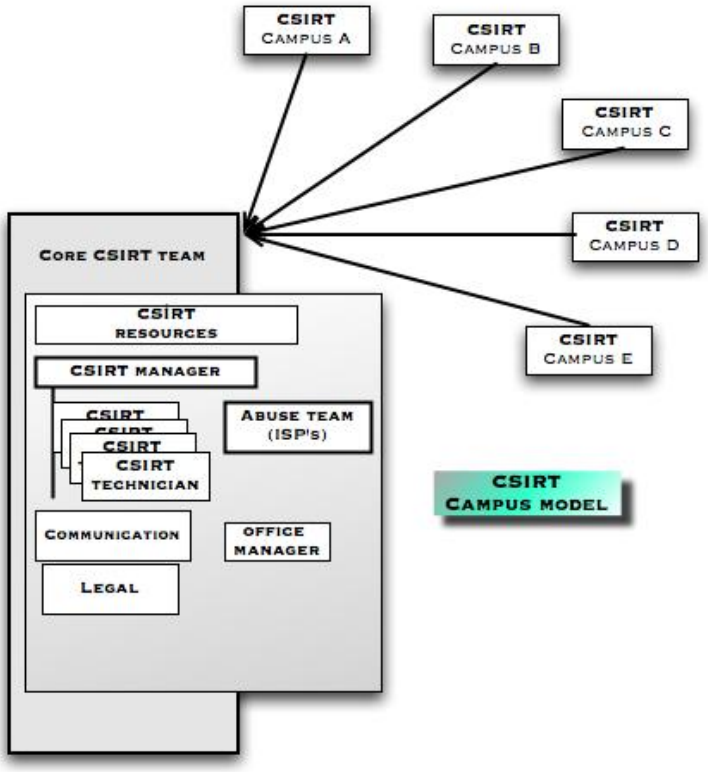


Fig. 7. Campusmodellen.

6.2.4 Frivilligmodellen

Denna organisationsmodell utgår från en grupp av människor (specialister) som kommer samman för att ge råd och stöd åt varandra (och utomstående) på frivillig grund. Det är en mycket löst sammansatt grupp, och den är i hög grad beroende av deltagarnas motivation.

Denna modell tillämpas till exempel av WARP-gruppen ([13]).

6.3 Att anställa rätt personal

När man väl har beslutat vilka tjänster och vilken supportnivå som ska erbjudas blir nästa steg att hitta rätt antal kunniga personer för uppgiften.

Det är nästan omöjligt att lämna exakta uppgifter om hur stor teknisk personal som behövs ur detta perspektiv, men följande nyckelvärden har visat sig vara en bra utgångspunkt:

- För att leverera de två kärntjänsterna, nämligen att distribuera en informationsbulletin och hantera incidenter: minst **4** heltidsekvivalenter.
- För ett CSIRT som erbjuder fullständig service under kontorstid och underhåller systemen: minst **6 till 8** heltidsekvivalenter.
- För ett fullbemannat CSIRT som erbjuder tjänster dygnet runt, sju dagar i veckan (två skift efter kontorstid), krävs cirka **12** heltidsekvivalenter eller fler.

Dessa siffror inkluderar också viss övertalighet för sjukdom, semestrar etc. Det är också nödvändigt att kontrollera lokala kollektivavtal. Om några av de anställda arbetar efter kontorstid kan detta resultera i extrakostnader i form av övertidsersättningar som måste betalas.

([13]) WARP-initiativet http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Nedan följer en kortfattad översikt över nyckelkompetenser för de tekniska experterna i ett CSIRT.

Arbetsbeskrivning för allmän teknisk personal:

Personlig kompetens

- Flexibel, kreativ och bra laganda
- Stor analytisk skicklighet
- Förmåga att förklara svåra tekniska frågor på ett enkelt språk
- En god känsla för konfidentialitet och att följa arbetsrutiner
- God organisatorisk förmåga
- Stresstålig
- Lätt för att kommunicera och god skribent
- Öppen och villig att lära

Teknisk kompetens

- Breda kunskaper om Internetteknik och Internetprotokoll
- Kunskaper om Linux och Unix (beroende på basgruppens utrustning)
- Kunskaper om Windowsbaserade system (beroende på basgruppens utrustning)
- Kunskaper om nätverksutrustning (router, switchar, DNS, proxy, mejl etc.)
- Kunskaper om Internetapplikationer (SMTP, HTTP(S), FTP, telnet, SSH etc.)
- Kunskaper om säkerhetshot (DDoS, nätfiske, defacing, sniffing etc.)
- Kunskaper om riskvärdering och praktiska tillämpningar

Ytterligare kompetensområden

- Villig att arbeta dygnet runt, sju dagar i veckan eller som jour (beroende på servicemodell)
- Maximalt reseavstånd (vid kristillgänglighet på kontoret; maximal restid)
- Utbildningsnivå
- Erfarenhet av att arbeta med IT-säkerhet

Fiktivt CSIRT (steg 4)

Att utarbeta affärsplanen

Finansieringsmodell

Eftersom företaget driver e-handel och även en IT-avdelning dygnet runt, sju dagar i veckan har man beslutat att tillhandahålla fullständig service under kontorstid och jourtjänst efter kontorstid. Tjänsterna åt basgruppen är gratis, men möjligheterna att erbjuda tjänster åt externa kunder kommer att utvärderas under pilot- och utvärderingsfasen.

Intäktsmodell

Under start- och pilotfasen kommer CSIRT-enheten att finansieras från värdföretaget. Under pilot- och utvärderingsfasen kommer ytterligare finansiering att diskuteras, inklusive möjligheten att sälja tjänster till externa kunder.

Organisationsmodell

Värdorganisationen är ett litet företag, så den inbäddade modellen valdes.
Under kontorstid kommer en personal bestående av tre personer att tillhandahålla kärntjänsterna (utskick av säkerhetsbulletiner och incidenthantering/samordning).

Företagets IT-avdelning har redan anställda med rätt kunskaper. Ett avtal med den avdelningen har tecknats så att vårt nya CSIRT kan begära stöd vid behov. Även deras jourtekniker i andra linjen kan användas.
Det kommer att finnas ett kärnteam med fyra heltidsanställda medlemmar och fem ytterligare medlemmar av CSIRT-teamet. En av dem är också tillgänglig i ett roterande skift.

Personal
CSIRT-teamets ledare har en bakgrund inom säkerhet och support på nivå 1 och 2 och har arbetat med att hantera kriser inom systemtålighet. De övriga tre medlemmarna är säkerhetsspecialister. Deltidsanställd CSIRT-personal från IT-avdelningen är specialister på sina respektive delar av företagets infrastruktur.

6.4 Kontorets användning och utrustning

Hur kontorsutrymmet ska utrustas och användas är mycket omfattande frågor. Därför kan ingen utförlig beskrivning ges i detta dokument. Syftet med detta avsnitt är att ge en kortfattad översikt över ämnet.

Mer information om fysisk säkerhet återfinns på
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

”Att säkra byggnaden”
Eftersom ett CSIRT ofta hanterar mycket känslig information är det en bra idé att låta teamet ta kontroll över kontorets fysiska säkerhet. Den kommer i hög grad att vara beroende av befintliga resurser och infrastrukturer och den informationssäkerhetspolicy som tillämpas av värdföretaget.

Statliga organ arbetar till exempel med klassificeringssystem och är väldigt noggranna när det gäller att hantera konfidentiell information. Kontrollera vilka lokala regler och rutiner som gäller på ditt eget företag eller din egen institution.

I regel är ett nytt CSIRT beroende av samarbetet med sin värdorganisation för att få information om lokala regler och rutiner och andra rättsliga frågor.

En utförlig beskrivning av all utrustning och alla säkerhetsåtgärder som kan bli aktuella faller utanför ramen för detta dokument. Nedan följer emellertid en kort förteckning över grundfaciliteterna för ditt CSIRT.

Allmänna regler för byggnaden
- Tillämpa tillträdeskontroller.
- Se till att enbart CSIRT-anställda får tillträde till CSIRT-kontoret.
- Övervaka kontoren och entréerna med kameror.
- Arkivera sekretessbelagd information i låsta skåp eller kassaskåp.
- Använd säkra IT-system.

Allmänna regler för IT-utrustningen
- Använd utrustning som personalen kan ge support på.
- Säkra samtliga system.
- Komplettera och uppdatera samtliga system innan de ansluts till Internet.
- Använd säkerhetsprogram (brandväggar, olika antivirusprogram, antispyware-program etc.)

Underhåll av kommunikationskanaler
- Offentlig webbplats
- Slutet medlemsområde på webbplatsen
- Digitala blanketter för att rapportera incidenter
- E-post (PGP, GPG, S/MIME-stöd)
- Programvara för sändlistor
- Ett speciellt telefonnummer för basgruppen:
    - Telefon
    - Fax
    - Sms

Registersystem
- Kontaktdatabas med uppgifter om teammedlemmar, övriga team etc.
- CRM-verktyg.
- Biljettorienterat system för incidenthantering.

Använd ”företagsstilen” från början i följande fall:
- Utformning av standard-e-post och informationsbulletin.
- Gamla hederliga pappersbrev.
- Månads- eller årsrapporter.
- Blankett för incidentrapportering.

Övriga frågor
- Förbereda för kommunikation utom bandet vid en eventuell attack.
- Förbereda backup för Internetanslutningen.

Se punkt *8.5 Tillgängliga CSIRT-verktyg* för mer information om olika CSIRT-verktyg.

6.5 Utveckling av en policy för informationssäkerhet

Du kommer att ha en policy för informationssäkerhet som är särskilt utformad för den aktuella typen av CSIRT. Förutom att beskriva det önskade tillståndet för operativa och administrativa processer och förfaranden måste en sådan policy följa lagar och standarder, framför allt vad gäller teamets ansvar. Ett CSIRT är i regel bundet av nationella lagar och förordningar, som ofta genomförs i anslutning till europeisk lagstiftning (oftast direktiv) och andra internationella överenskommelser. Standarder är inte nödvändigtvis direkt bindande, men de kan vara en följd av eller rekommenderade i lagar och förordningar.

Nedan följer en kortfattad lista över tänkbara lagar och förordningar:

Nationella
- Olika lagar om informationsteknik, telekommunikationer, medier.
- Lagar om uppgiftsskydd och integritetsskydd.
- Lagar och förordningar om lagring av uppgifter.
- Lagstiftning om ekonomi, redovisning och företagsledning.
- Uppträdandekoder för företagsledningar och IT-ansvariga.

Europeiska
- Direktivet om elektroniska signaturer (1999/93/EG).
- Direktiven om dataskydd (1995/46/EG) och behandling av personuppgifter i elektroniska meddelanden (2002/58/EG).
- Direktiven om elektroniska kommunikationsnät och tjänster (2002/19/EG – 2002/22/EG).
- Direktiven om bolagslagar (t.ex. det åttonde bolagsrättsliga direktivet).

Internationella
- Basel II-överenskommelsen (framför allt vad gäller hanteringen av operativa risker).
- Europarådets konvention om cyberbrottslighet.
- Europarådets konvention om de mänskliga rättigheterna (artikel 8 om integritetsskydd).
- Internationella redovisningsstandarder (IAS; ger i viss mån mandat för IT-kontroll).

Standarder
- Den brittiska standarden BS 7799 (informationssäkerhet).
- De internationella standarderna ISO2700x (system för hantering av informationssäkerhet).
- Tyska IT-Grundschutzbuch, franska EBIOS och andra nationella varianter.

Samråd med din rättsexpert för att kontrollera om ditt CSIRT följer nationell och internationell lag.

De viktigaste frågorna som ska besvaras av din policy för informationshantering är följande:

- Hur ”taggas” eller ”klassificeras” inkommande information?
- Hur hanteras informationen, framför allt vad gäller exklusiv tillgång?
- Vilka regler gäller för yppande av information, framför allt om incidentrelaterad information förs vidare till andra team eller platser?
- Finns det några rättsliga aspekter som måste beaktas i samband med informationshanteringen?
- Har du någon policy för användning av kryptering för att skydda tillträdet till och integriteten för arkiv och/eller datakommunikation, framför allt e-post?
- Omfattar denna policy eventuella rättsliga gränsdragningar, såsom säker förvaring av nycklar eller dekrypteringsmöjligheter vid eventuella stämningar?

Fiktivt CSIRT (steg 5)

Kontorets utrustning och placering

Eftersom värdföretaget redan har en tillräckligt god fysisk säkerhet på plats är vårt nya CSIRT väl skyddat i det avseendet. En så kallad ”stridsledningscentral” ställs till förfogande för att underlätta samordningen i ett krisläge. Ett kassaskåp har köpts in för att förvara krypteringsmateriel och känsliga dokument. En separat telefonlinje har upprättats för att underlätta heta linjen under kontorstid och en mobil jourtelefon för perioden efter kontorstid med samma telefonnummer.

Befintlig utrustning och företagets webbplats kan också användas för att meddela CSIRT-relaterad information. En sändlista har upprättats och förvaltas aktivt, med en särskild del med begränsat tillträde för kommunikationen mellan teamets medlemmar och med andra team. Alla kontaktuppgifter för personalen lagras i en databas, och en utskrift förvaras i kassaskåpet.

Reglering

Eftersom vårt CSIRT är inbäddat i ett företag med befintlig policy för informationssäkerhet har motsvarande regler ställts upp för CSIRT-enheten med hjälp av företagets rättsexpert.

6.6 Undersöka möjligheterna till samarbete med andra CSIRT och eventuella nationella initiativ

Förekomsten av andra CSIRT-initiativ och det starka behovet av samarbete med dem har redan nämnts ett par gånger i detta dokument. Det är en bra rutin att kontakta andra CSIRT så tidigt som möjligt för att etablera den nödvändiga kontakten med CSIRT-grupperna. I regel är övriga CSIRT mycket öppna när det gäller att hjälpa nya team att komma igång.

ENISA:s *Inventory of CERT activities in Europé* ([14]) (förteckning över CERT-aktiviteter i Europa) är en mycket bra utgångspunkt för att leta efter andra CSIRT i landet eller nationella samarbetsaktiviteter mellan olika CSIRT.

För att få hjälp att hitta lämpliga källor till CSIRT-information kan man kontakta ENISA:s CSIRT-experter:

([14]) ENISA:s Inventory: http://www.enisa.europa.eu/cert_inventory/

CERT-Relations@enisa.europa.eu

Nedan följer en översikt över CSIRT-aktiviteter. Se ovannämnda förteckning för en mer fullständig beskrivning och ytterligare information.

Europeiskt CSIRT-initiativ

TF-CSIRT ([15])
Arbetsgruppen TF-CSIRT främjar samarbetet mellan olika CSIRT i Europa. Arbetsgruppens huvuduppgift är att erbjuda ett forum för att utbyta erfarenheter och kunskaper, upprätta pilottjänster för CSIRT-samfundet och hjälpa till att upprätta nya CSIRT-enheter.

Arbetsgruppens viktigaste mål är att
- erbjuda ett forum för att utbyta erfarenheter och kunskaper,
- upprätta pilottjänster för det europeiska CSIRT-samfundet,
- främja gemensamma standarder och förfaranden för att reagera på säkerhetsincidenter,
- hjälpa till att upprätta nya CSIRT och utbilda CSIRT-personal.
- TF-CSIRT:s aktiviteter fokuserar på Europa och grannländerna i enlighet med mandatet från TERENA:s tekniska kommitté av den 15 september 2004.

Globalt CSIRT-initiativ

FIRST ([16])
FIRST är den viktigaste organisationen och erkänd global ledare inom incidenthantering. Genom medlemskapet i FIRST kan incidentresponsteamen reagera effektivare på säkerhetsincidenter – såväl reaktivt som proaktivt.

FIRST är samlingspunkt för ett antal olika CSIRT från statliga, kommersiella och pedagogiska organisationer. FIRST syftar till att främja samarbete och samordning inom incidentförebyggande, stimulera till snabba reaktioner på incidenter och främja informationsdelning bland medlemmarna och i samhället i stort.

Förutom det nätverk som FIRST utgör för globala grupper av incidentresponsteam tillhandahåller organisationen även mervärdestjänster.

Fiktivt CSIRT (steg 6)
På jakt efter samarbete
Genom att använda ENISA:s förteckning kunde vi snabbt hitta och kontakta några CSIRT i samma land. Ett besök på platsen arrangerades med ett av dem för den nyanställde teamledaren. Han lärde sig om nationella CSIRT-aktiviteter och var med under ett möte.
Det mötet var mycket fruktbart för att samla in exempel på arbetsmetoder och få stöd av ett par andra team.

([15]) TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

([16]) FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

7 Att genomföra affärsplanen

Vi har tagit följande steg:

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska leverera sina tjänster till.
3. Att bestämma vilka typer av tjänster ett CSIRT kan erbjuda sin basgrupp.
4. Analys av miljö och basgruppens medlemmar.
5. Formulering av uppdragsbeskrivningen.
6. Att utarbeta affärsplanen.
    a. Att definiera finansieringsmodellen.
    b. Att bestämma organisationsstrukturen.
    c. Att börja anställa personal.
    d. Att använda och utrusta kontoret.
    e. Att utveckla en policy för informationssäkerhet.
    f. Att leta efter samarbetspartner.

>> Nästa steg blir att föra in allt detta i en projektplan och komma igång!

En bra start för att definiera projektet är att utforma ett scenario. Scenariot kommer att användas som grund för projektplanen, och det kommer också att användas för att söka ledningsstöd och få budgetmedel och andra resurser.

Det visade sig vara nyttigt att löpande rapportera till ledningen för att hålla medvetenheten om IT-relaterade säkerhetsproblem och därigenom behovet av ett löpande stöd för ett eget CSIRT på en hög nivå.

Att utarbeta ett affärsscenario börjar med att man analyserar problem och möjligheter genom att tillämpa en analysmodell, vilket beskrivs i avsnitt *5.3 Analys av basgruppen*, och försöker skapa nära kontakter med den potentiella basgruppen.

Som framhållits tidigare är det mycket att tänka på när man startar ett CSIRT. Det bästa är att anpassa ovanstående material till teamets behov, allteftersom de visar sig.

När man rapporterar till ledningen är det en bra idé att se till att det egna affärsscenariot är så aktuellt som möjligt genom att använda aktuella artiklar från tidningar eller Internet och förklara varför CSIRT-enhetens tjänster och interna incidentsamordning är avgörande för att säkra företagets tillgångar. Det är också nödvändigt att göra klart att enbart ett kontinuerligt stöd för IT-säkerheten ger en stabil verksamhet, framför allt för ett företag eller en institution som är beroende av IT.

(Ett berömt yttrande av Bruce Schneier ställer detta på sin spets: *"Säkerhet är inte en produkt, utan en process!"* ([17]))

Ett berömt verktyg för att illustrera säkerhetsproblem är följande diagram från CERT/CC:

([17]) Bruce Schneier: http://www.schneier.com/

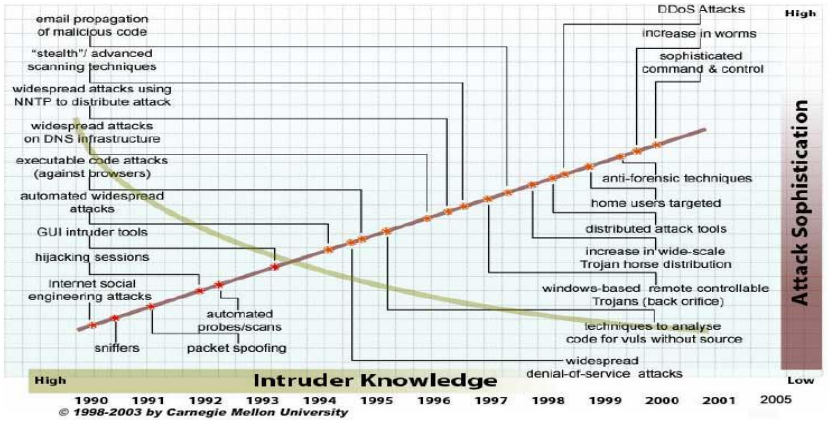


Fig. 8. Inkräktarens kunskaper jämfört med attackernas grad av sofistikering (källa: CERT-CC ([18])).

Diagrammet visar trenderna inom IT-säkerhet, framför allt de allt lägre kunskaper som krävs för att genomföra alltmer sofistikerade attacker.

En annan viktig punkt är det hela tiden krympande tidsfönstret mellan tillgången på nya uppdaterade och säkrare programversioner och nya attacker mot dem:

Patch -> Utnyttja		**Spridningstakt**	
Nimda:	11 månader	Code red:	Dagar
Slammer:	6 månader	Nimda:	Timmar
Nachi:	5 månader	Slammer:	Minuter
Blaster:	3 veckor		
Witty:	1 dag (!)		

Insamlade incidentdata, potentiella förbättringar och gjorda erfarenheter bidrar också till en bra presentation.

([18]) http://www.cert.org/archive/pdf/info-sec-ip.pdf

7.1 Beskrivning av affärsplaner och faktorer som motiverar ledningen

En föredragning för ledningen som inkluderar att göra reklam för CSIRT-enheten utgör inget scenario i sig, men om den görs på rätt sätt kommer den att leda till att ledningen i de flesta fall stödjer tanken på ett CSIRT. Scenariot bör å andra sidan inte enbart betraktas som ett exempel för ledningen, utan det bör också användas vid kommunikation till teamet och basgruppen. Termen affärsscenario kan verka väldigt kommersiell och svår att förena med CSIRT-enhetens dagliga arbete, men den ger en god fokusering och inriktning när ett CSIRT inrättas.

Svaren på följande frågor kan användas för att bygga upp ett bra scenario. (De exempel som nämns är enbart hypotetiska och används enbart som illustration. De ”verkliga” svaren är i hög grad beroende av ”verkliga” omständigheter.)

- Vad är problemet?
- Vad vill du uppnå med basgruppens medlemmar?
- Vad händer om du inte gör någonting?
- Vad händer om du gör någonting?
- Vad kommer det att kosta?
- Vad kommer du att vinna?
- När börjar du och när är det färdigt?

Vad är problemet?
I de flesta fall uppkommer idén att inrätta ett CSIRT när IT-säkerheten har blivit en viktig del av kärnverksamheten för ett företag eller en institution och när IT-säkerhetsincidenterna blir en affärsrisk som gör riskhanteringen till en normal affärsoperation.

De flesta företag eller institutioner har riktiga supportenheter eller en hjälpcentral, men i de flesta fall hanteras säkerhetsincidenterna inte tillräckligt grundligt och inte på det strukturerade sätt som de borde kräva. I de flesta fall kräver arbetet med säkerhetsincidenter speciella kunskaper och särskild uppmärksamhet. Att tillämpa en mer strukturerad strategi är också nyttigt och kommer att minska affärsriskerna och skadorna på företaget.

Problemet är i de flesta fall bristen på samordning och att befintliga kunskaper inte utnyttjas för att hantera incidenter, vilket skulle kunna hindra att de inträffar i framtiden och förhindra eventuella ekonomiska förluster och/eller skador på organisationens rykte.

Vad är målet för arbetet med basgruppens medlemmar?
Som vi har förklarat tidigare kommer ditt CSIRT att betjäna sina medlemmar och hjälpa dem att lösa IT-säkerhetsincidenter och -problem. Ytterligare vinster är att man ökar medvetenheten om IT-säkerhet och skapar en säkerhetsmedveten kultur.

Denna kultur gör det möjligt att vidta proaktiva och förebyggande åtgärder från start och därigenom att sänka de operativa kostnaderna.

Att införa denna kultur präglad av samarbete och stöd i ett företag eller en institution kan i de flesta fall stimulera till en allmän effektivisering.

Vad händer om inget görs?
Ett ostrukturerat sätt att hantera IT-säkerheten kan leda till ytterligare skador, inte minst på institutionens rykte. Ekonomiska förluster och rättsliga konsekvenser kan bli andra resultat.

Vad händer om något görs?
Medvetenheten om att det förekommer säkerhetsproblem ökar. Detta bidrar till att lösa dem effektivare och att förebygga framtida förluster.

Vad kommer det att kosta?
Beroende på organisationsmodell kommer kostnaderna att utgöras av lönerna för CSIRT-enhetens medlemmar och organisation, samt av utgifterna för utrustning, verktyg och programlicenser.

Vad kommer du att vinna?
Beroende på företag och tidigare förluster kommer du att vinna ökad insyn i förfaranden och säkerhetsrutiner, vilket bidrar till att skydda viktiga affärstillgångar.

Vilken är tidsplanen?
Se kapitel *12. Beskrivning av projektplanen* för en beskrivning av en tänkt projektplan.

Exempel på befintliga scenarier och strategier
Här följer ett par exempel på CSIRT-scenarier som det kan vara värt att studera:

- http://www.cert.org/csirts/AFI_case-study.html
  Att skapa ett CSIRT för en finansiell institution: ett scenario.

  Syftet med detta dokument är att sprida de erfarenheter som gjordes av en finansiell institution (som i dokumentet kallas AFI) när den utvecklade och genomförde en plan för att ta itu med säkerhetsproblem och upprätta ett CSIRT.

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Sammanfattning av exemplet CERT POLSKA (bilder i pdf-format).

- http://www.auscert.org.au/render.html?it=2252
  Att bilda ett IRT (Incident Response Team) på 1990-talet kunde vara en svår uppgift. Många som bildade IRT hade inga erfarenheter av hur man skulle göra. I den här uppsatsen undersöks vilken roll ett IRT kan spela i samhället och de problem som borde ha tagits upp, såväl när teamet bildades som när verksamheten hade inletts. Det kan vara nyttigt för befintliga IRT, eftersom det kan öka medvetenheten om frågor som inte tidigare tagits upp.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Case Study in Information Security, Securing the Enterprise, av Roger Benton

  Det här exemplet handlar om hur ett försäkringsbolag går över till ett företagsövergripande säkerhetssystem. Syftet med exemplet är att peka på en väg att gå när man skapar eller går över till ett säkerhetssystem. Från början fanns det bara ett primitivt säkerhetssystem online för att kontrollera tillträdet till företagets data. Exponeringarna var allvarliga – det fanns inga integritetskontroller utanför onlinemiljön. Alla med grundläggande kunskaper i programmering kunde lägga till, ändra och/eller radera produktionsdata.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriotts strategi för e-säkerhet: samarbete affärssidan-IT

  Enligt Marriott International Inc.:s Chris Zoladz är e-handelns säkerhet en process, inte ett projekt. Detta var budskapet som Zoladz framförde vid den konferens och utställning om e-säkerhet som ägde rum nyligen i Boston, sponsrad av Intermedia-koncernen. I sin egenskap av vice vd med ansvar för informationsskydd för Marriott rapporterar Zoladz via rättsenheten, trots att han inte är advokat. Hans uppdrag är att ange var Marriotts viktigaste affärsinformation är lagrad och hur den rör sig inom och utanför företaget. Marriott har angett ett separat ansvarsområde för säkerheten för teknisk infrastruktursupport, som ges till IT-säkerhetens arkitekt.

Fiktivt CSIRT (steg 7)

Att genomföra affärsplanen

Vi beslutar att samla in uppgifter från företagets historia. Detta är mycket produktivt för att skapa en statistisk översikt över läget vad gäller IT-säkerhet. Insamlingen av data bör fortsätta när CSIRT har kommit igång, för att hålla statistiken à jour.

Övriga nationella CSIRT-enheter kontaktades och intervjuades om sina scenarier. De gav stöd genom att ställa samman bilder med information om den senaste utvecklingen inom IT-säkerhetsincidenter och om kostnaderna för incidenterna.

I vårt exempel med ett fiktivt CSIRT fanns det inget tvingande behov av att övertyga ledningen om betydelsen av IT-verksamheten, och därför var det inte svårt att få grönt ljus för första steget. Ett affärsscenario och en projektplan utarbetades, inklusive en beräkning av uppstartkostnader och driftkostnader.

8 Exempel på operativa och tekniska förfaranden (arbetsflöden)

Vi har tagit följande steg:

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska tillhandahålla sina tjänster till.
3. Att bestämma vilka typer av tjänster ett CSIRT kan erbjuda sin basgrupp.
4. Analys av miljö och basgruppens medlemmar.
5. Formulering av uppdragsbeskrivningen.
6. Att utarbeta affärsplanen.
   a. Att definiera finansieringsmodellen.
   b. Att bestämma organisationsstrukturen.
   c. Att börja anställa personal.
   d. Att använda och utrusta kontoret.
   e. Att utveckla en policy för informationssäkerhet.
   f. Att leta efter samarbetspartner.
7. Att genomföra affärsplanen.
   a. Att godkänna affärsscenariot.
   b. Att få med allt i en projektplan.

>> Nästa steg: se till att vårt CSIRT blir operativt.

Med väl definierade arbetsflöden på plats förbättras kvaliteten och den tid som krävs för varje incident eller fall av sårbarhet.

Som vi har beskrivit i exempelrutorna kommer vårt fiktiva CSIRT att erbjuda de grundläggande kärntjänsterna för ett CSIRT:

- Larm och varningar
- Incidenthantering
- Meddelanden

I det här avsnittet ger vi exempel på arbetsflöden för kärntjänsterna i ett CSIRT. Det här kapitlet innehåller också information om hur man samlar in information från olika källor, kontrollerar att den är relevant och autentisk och skickar den vidare till basgruppen. Slutligen innehåller avsnittet exempel på de mest grundläggande förfarandena och särskilda CSIRT-verktyg.

8.1 Kontrollera vilka system som finns i basgruppen

Det första steget blir att skapa en översikt över de IT-system som finns installerade i din basgrupp. Tack vare den kan CSIRT-enheten bedöma om den inkommande informationen är relevant och filtrera den innan den skickas ut igen, så att basgruppens medlemmar inte dränks i information som de egentligen inte har någon nytta av.

Det är alltid bra att börja enkelt, till exempel med ett Excel-blad enligt följande:

Kategori	Applikation	Program-vara	Version	Operativ-system	Operativ-system version	Medlem
Desktop	Office	Excel	x-x-x	Microsoft	XP-prof	A
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A
Network	Router	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Tjänster	Webb-server	Apache		Unix	x-x-x	B

Tack vare filterfunktionen i Excel är det mycket enkelt att välja rätt programvara och se vilken medlem som använder vilken programvara.

8.2 Att skapa larm, varningar och meddelanden

Samma arbetsflöde används för att skapa larm, varningar och meddelanden:

- Insamling av information.
- Utvärdering av information om relevans och källa.
- Riskbedömning utifrån den insamlade informationen.
- Distribution av informationen.

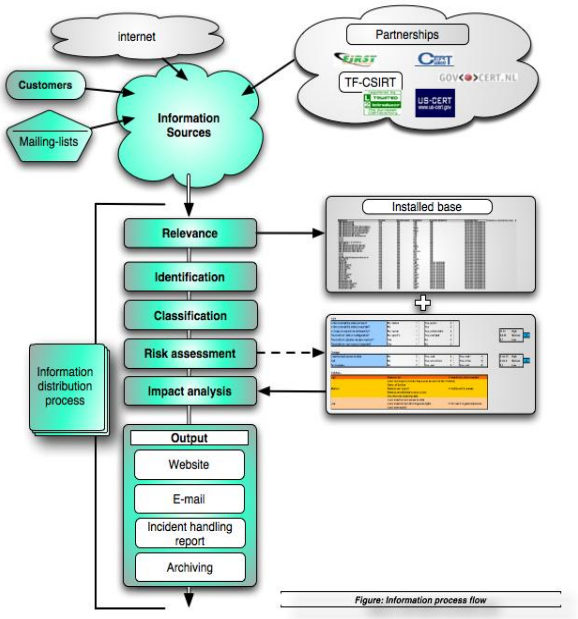
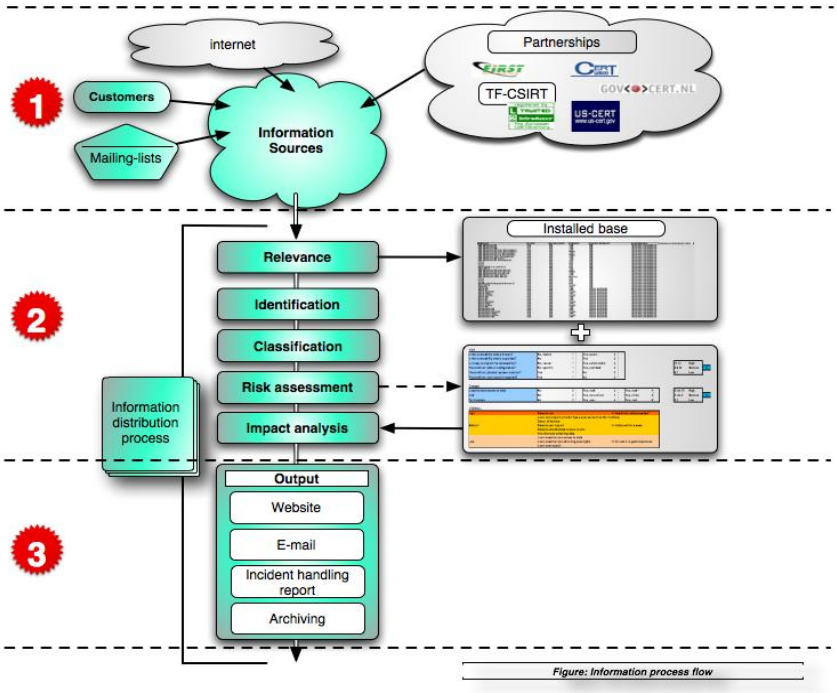


Fig. 9. Informationsbehandlingsflödet.

I följande avsnitt beskrivs detta arbetsflöde mer i detalj.



Steg 1: Insamling av sårbarhetsinformation

I regel finns det två huvudtyper av informationskällor som bidrar med basinformation för tjänsterna:

- Sårbarhetsinformation om (dina) IT-system.
- Incidentrapporter.

Det finns många öppna och slutna källor för sårbarhetsinformation, beroende på typen av verksamhets- och IT-struktur:

- Offentliga och slutna sändlistor.
- Försäljarens information om produktens sårbarhet.
- Webbplatser.
- Information på Internet (Google etc.).
- Offentliga och privata partnerskap som tillhandahåller sårbarhetsinformation (FIRST, TF-CSIRT, CERT-CC, US-CERT osv.).

All denna information bidrar till att höja nivån på kunskaperna om specifika sårbarheter i IT-systemen.

Som redan nämnts tidigare finns det gott om bra och lättillgängliga källor för säkerhetsinformation på Internet. ENISA:s ad hoc-arbetsgrupp ”CERT-tjänster” för 2006

håller i skrivande stund på att sammanställa en mer heltäckande lista som ska offentliggöras i slutet av 2006 ([19]).

Steg 2: Utvärdering av informationen och riskbedömning

Detta steg kommer att resultera i en analys av effekterna av speciella sårbarheter på basgruppens IT-infrastruktur.

Identifiering
Källan för inkommande sårbarhetsinformation måste alltid identifieras, och det måste avgöras om källan är pålitlig innan någon information lämnas till basgruppen. I annat fall kan falska varningar skickas ut, vilket skulle kunna leda till onödiga störningar i affärsprocesserna och i slutändan skada CSIRT-enhetens rykte.

([19]) Ad hoc-arbetsgruppen CERT-tjänster:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Nedan visas ett exempel på förfarandet för att kontrollera att ett meddelande är autentiskt:

Förfarande för att kontrollera autenticiteten för ett meddelande och dess källa

Allmän checklista
1. Är källan känd och registrerad som sådan?
2. Kommer informationen via en känd kanal?
3. Finns det ”konstig” information som ”känns” fel?
4. Följ dina instinkter – agera inte utan kontrollera igen om du är osäker!

Information via e-post
1. Är källans adress känd för organisationen och upptagen på listan över källor?
2. Är PGP-signaturen korrekt?
3. Kontrollera hela rubriken till ett budskap om du är osäker.
4. Använd ”nslookup” eller ”dig” för att verifiera sändarens domän ([20]).

Information via www
1. Kontrollera browsercertifikat när du ansluter dig till en säker webbplats (https://).
2. Kontrollera källans innehåll och validitet (tekniskt).
3. Klicka inte på några länkar och ladda inte ner några program om du är osäker.
4. Kör en “lookup” och en ”dig” på domänen, och gör en ”traceroute” om du känner dig osäker.

Telefon
1. Lyssna noga på namnet.
2. Känner du igen rösten?
3. Be om ett telefonnummer och begär att få ringa tillbaka om du är osäker.

Fig. 10. Exempel på förfarande för identifiering av information

Relevans
Den översikt över installerad hård- och programvara som visades tidigare kan användas för att filtrera inkommande sårbarhetsinformation efter relevans i syfte att hitta ett svar på frågorna ”Använder basgruppen den här programvaran?” och ”Är informationen relevant för medlemmarna i gruppen?”

Klassificering
En del av den information som mottagits kan klassificeras eller taggas som sekretessbelagd (till exempel inkommande incidentrapport från andra team). All information måste hanteras enligt sändarens krav och enligt den egna säkerhetspolicyn. En bra grundregel är denna: ”*Distribuera inte information om det inte klart framgår att det är meningen att den ska distribueras; be sändaren om lov att få distribuera den om du är osäker.”*

([20]) Verktyg för att kontrollera identiteter på CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Riskbedömning och effektanalys
Det finns olika metoder för att bedöma risker och effekter för en (potentiell) sårbarhet.

Risk definieras som möjligheten att en viss sårbarhet kan utnyttjas. Det finns flera viktiga faktorer (bland annat):

- Är sårbarheten välkänd?
- Är sårbarheten allmänt spridd?
- Är det lätt att utnyttja sårbarheten?
- Är det en sårbarhet som kan utnyttjas på distans?

Alla dessa frågor ger en bra uppfattning om hur allvarlig sårbarheten är.
En mycket enkel strategi för att beräkna risken erbjuder följande formel:

Effekt = risk × potentiell skada

Den potentiella skadan skulle kunna vara

- icke auktoriserad tillgång till data,
- tillgänglighetsförlust (DoS, Denial of Service),
- att erhålla eller utsträcka tillstånd.

(Se slutet av detta kapitel för mer detaljerade klassificeringssystem.)

När ovanstående frågor har besvarats kan en övergripande rating läggas till i informationsbulletinen med information om potentiella risker och skador. Ofta används enkla termer som LÅG, MEDIUM och HÖG.

Bland de övriga, mer omfattande riskbedömningssystemen finns till exempel:

GOVCERT.NL:s ratingsystem ([21])

Det nederländska statliga CSIRT GOVCERT.NL har utvecklat en mall för riskvärdering som utvecklades när Govcert.nl startade och som fortfarande uppdateras med de senaste trenderna.

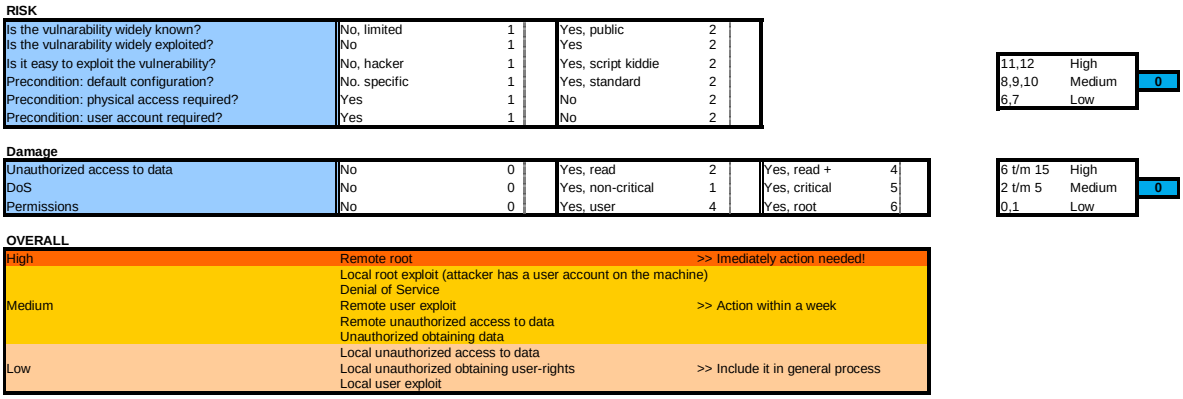


Fig. 11. GOVCERT.NL:s ratingsystem.

EISPP:s gemensamma format för informationsbulletiner ([22])

EISPP (European Information Security Promotion Programme) är ett projekt som medfinansieras av Europeiska gemenskapen genom femte ramprogrammet. EISPP-projektet syftar till att utveckla ett europeiskt ramverk, inte bara för att sprida säkerhetsinformation, utan också för att definiera innehåll och sätten att sprida säkerhetsinformation till små och medelstora företag. Genom att förse europeiska små och medelstora företag med de nödvändiga IT-tjänsterna kommer de att få ökat förtroende för och i större utsträckning utnyttja e-handel, vilket leder till fler och bättre möjligheter till nya affärer. EISPP är pionjär inom Europeiska kommissionens vision för att skapa ett europeiskt nätverk av experter inom Europeiska unionen.

DAF Deutsches Advisory Format ([23])

DAF är ett initiativ från det tyska CERT-Verbund och en central komponent i en infrastruktur för att utarbeta och utbyta säkerhetsbulletiner mellan olika team. DAF är speciellt utformat för behoven hos tyska CERT. Standarden utvecklas och underhålls av CERT-Bund, DFN-CERT, PRESECURE och Siemens-CERT.

([21]) Sårbarhetsmall: http://www.govcert.nl/download.html?f=33

([22]) EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

([23]) DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

Steg 3: Distribution av informationen

Ett CSIRT kan välja mellan flera olika distributionsmetoder beroende på basgruppens önskningar och den egna kommunikationsstrategin:

- Webbplats
- E-post
- Rapporter
- Arkivering och forskning

Säkerhetsbulletinerna som distribueras av ett CSIRT bör alltid följa samma struktur. Det förbättrar läsbarheten och gör att läsaren snabbt hittar all relevant information.

En bulletin bör minst innehålla följande information:

Bulletinens rubrik ……
Referensnummer …… **Påverkade system** **-** …… **-** …… **Aktuellt operativsystem + version** …… **Risk** (Hög-Medel-Låg) …… **Effekt/potentiell skada** (Hög-Medel-Låg) …… **Externa id:** (CVE, ID för sårbarhetsbulletin) ……
Översikt över sårbarheten …… **Effekt** …… **Lösning** …… **Beskrivning (detaljer)** …… **Bilaga** ……

Fig. 12. Exempel på bulletin.

Se kapitel *10. Övning* för ett utförligt exempel på bulletin.

8.3 Incidenthantering

Som vi redan har nämnt i inledningen till detta kapitel påminner processen för informationshantering under incidenthanteringen mycket om den process som tillämpas när larm, varningar och meddelanden ställs samman. Men informationsinsamlingsdelen kan se olika ut, eftersom det normala sättet att få incidentrelaterade uppgifter är att antingen ta emot incidentrapporter från basgruppens medlemmar eller andra team, eller att ta emot feedback från berörda parter under incidenthanteringsprocessen. Informationen kommer i regel via (krypterade) e-postbrev. Ibland måste man använda telefon eller fax.

När man tar emot information via telefon kan det vara bra att skriva ner alla detaljer omedelbart, antingen med hjälp av ett incidenthanterings- eller rapporteringsverktyg eller i en minnesanteckning. Det är nödvändigt att omedelbart (innan telefonsamtalet avbryts) skapa ett incidentnummer (om inget sådant finns för den aktuella incidenten) och att ge den som ringer det (eller meddela det i ett sammanfattande e-postbrev som skickas i efterhand) som en referens för vidare kommunikationer.

I resten av detta kapitel beskrivs grundprocessen för incidenthantering. En mycket grundlig analys av hela processen för incidenthantering och alla arbetsflöden och delflöden som berörs återfinns i CERT/CC-dokumentet *Defining Incident Management processes for CSIRTs (Att definiera incidentrapporteringsprocesser för ett CSIRT) ([24])*.

([24]) Att definiera incidenthanteringsprocesser: http://www.cert.org/archive/pdf/04tr015.pdf

Incidenthanteringen följer i stort sett följande arbetsflöde:

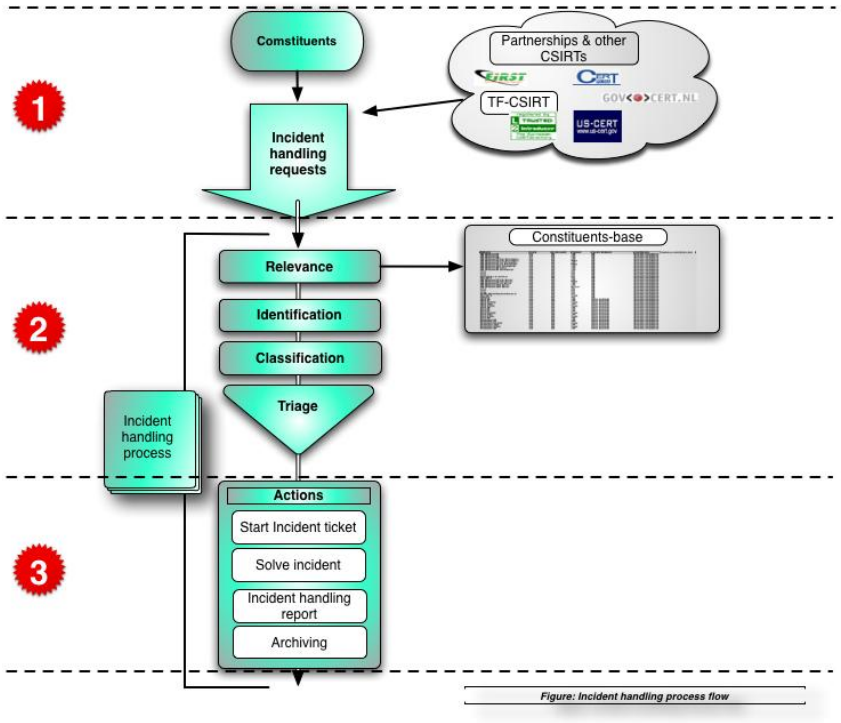


Fig. 13. Incidentprocessens flöden.

Steg 1: Att ta emot incidentrapporter

Som vi redan har nämnt kommer incidentrapporterna till ett CSIRT via flera olika kanaler, i första hand e-post, men också via telefon eller fax.

Det är, som vi också har nämnt tidigare, en bra rutin att anteckna alla detaljer i ett fast format medan man tar emot en incidentrapport. På så vis kan man garantera att ingen viktig information utelämnas. Nedan följer ett exempel på rapportformat.

BLANKETT FÖR INCIDENTRAPPORTERING

Fyll i denna blankett och faxa eller skicka via e-post till: ……..
*Uppgifterna markerade med * är obligatoriska.*

Namn och organisation
1. Namn*:
2. Organisationens namn*:
3. Sektortyp:
4. Land*:
5. Stad:
6. E-postadress:
7. Telefonnummer*:
8. Övrigt:

Påverkade värdar
9. Antalet värdar:
10. Värdens namn och IP*:
11. Värdens funktion*:
12. Tidszon:
13. Hårdvara:
14. Operativsystem:
15. Påverkad programvara:
16. Påverkade filer:
17. Säkerhet:
18. Värdens namn och IP*:
19. Protokoll/port:

Incident
20. Referensnummer ref #:
21. Typ av incident:
22. Incidenten startade den:
23. Detta är en pågående incident: JA NEJ
24. Tid och metod för upptäckten:
25. Kända sårbarheter:
26. Misstänkta filer:
27. Motåtgärder:
28. Detaljerad beskrivning*:

Fig. 14. Innehållet i en incidentrapport.

Steg 2: Incidentutvärdering

Under detta steg kontrolleras autenticitet och relevans för en rapporterad incident och incidenten klassificeras.

Identifiering

För att undvika onödiga åtgärder är det en god vana att kontrollera om den som skickat rapporten är pålitlig och om det är en av dina egna eller en närstående CSIRT-enhets basgruppmedlemmar. Liknande regler som dem som beskrivs i kapitel *8.2 Att skapa larm* gäller.

Relevans

Med detta steg kan du kontrollera om begäran om incidenthantering ursprungligen kommer från CSIRT-enhetens basgrupp, eller om den rapporterade incidenten avser IT-system som används inom basgruppen. Om ingetdera av ovanstående gäller skickas i regel rapporten vidare till rätt CSIRT ([25]).

Klassificering

Genom det här steget förbereds triagen (sorteringen) genom att man klassificerar hur allvarlig incidenten är. Det faller utanför detta dokuments omfattning att bestämma detaljerna i en incidentklassificering. En bra början kan vara att använda ett klassificeringssystem för CSIRT-fall (exempel för företags-CSIRT):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Fig. 15. Incidentklassificeringssystem (källa: FIRST ([26])).

([25]) Verktyg för att kontrollera identiteter på CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

([26]) Klassificering av CSIRT-fall http://www.first.org/resources/guides/csirt_case_classification.html

Triage

Triage är ett system som tillämpas inom sjukvården för att ransonera begränsade medicinska resurser och behandla största möjliga antalet patienter när antalet skadade som behöver vård överstiger de tillgängliga vårdresurserna ([27]).

I CERT/CC lämnas följande beskrivning:

Triage är ett centralt inslag i all incidenthantering, framför allt för etablerade CSIRT. Triage är en viktig del av processen att förstå vad som rapporteras i organisationen. Det är det instrument som gör att all information flödar till en enda kontaktpunkt, och som möjliggör en verksamhetscentrerad syn på pågående aktiviteter och en heltäckande analys av alla rapporterade data. Triage gör det möjligt att göra en inledande värdering av en inkommande rapport och att prioritera den för vidare behandling. Det erbjuder också en möjlighet att påbörja den inledande dokumenteringen av och införandet av data från en rapport eller begäran, om detta inte redan har gjorts i detekteringsprocessen.

Triagefunktionen ger en ögonblicksbild av aktuell status för alla rapporterade aktiviteter, vilka rapporter som är öppna och slutna, vilka åtgärder som ska vidtas och hur många av varje enskild typ av rapport som har mottagits. Processen kan bidra till att identifiera potentiella säkerhetsproblem och prioritera arbetsbelastningen. Information som samlats in under triagen kan också användas för att skapa sårbarhets- och incidenttrender och statistik för den högsta ledningen ([28]).

Triagen bör endast utföras av de mest erfarna teammedlemmarna, eftersom den kräver en grundlig förståelse av de potentiella effekterna av incidenter på specifika delar av basgruppen och förmågan att besluta om vem som skulle vara den lämpligaste teammedlemmen för att hantera den aktuella incidenten.

([27]) Triage på Wikipedia: http://en.wikipedia.org/wiki/Triage

([28]) Att definiera incidenthanteringsprocesser: http://www.cert.org/archive/pdf/04tr015.pdf

Steg 3: Åtgärder

I regel hamnar de incidenter som sorterats i en triage i en åtgärdskö i något incidenthanteringsverktyg som används av en eller flera incidenthandläggare som i regel följer följande steg.

Påbörja incidentbiljetten
Incidentbiljettens nummer kan redan ha genererats i ett föregående steg (till exempel när incidenten rapporterades via telefon). I annat fall blir det första steget att skapa ett sådant nummer som kommer att användas i all ytterligare kommunikation om denna incident.

Incidentens livscykel
Att hantera en incident följer inte linjärt upplagda steg som i slutändan leder till en lösning, utan processen följer snarare en cirkel av steg som upprepas till dess incidenten slutligen har lösts och alla berörda parter har fått all nödvändig information. Denna cirkel, som ofta kallas för ”incidentens livscykel”, omfattar följande processer:

Analys:	Alla detaljer i den rapporterade incidenten analyseras.
Erhålla kontaktinformation:	För att kunna föra vidare information som gäller incidenten till alla berörda parter, till exempel andra CSIRT-enheter, offer och förmodligen ägarna av system som kan ha missbrukats för en attack.
Lämna tekniskt stöd:	Hjälpa offren att snabbt återhämta sig efter resultaten av incidenten och samla in mer information om attacken.
Samordning:	Informera andra berörda parter, såsom det CSIRT som har ansvaret för IT-systemet som använts för en attack, eller andra offer.

Denna struktur kallas för en ”livscykel”, eftersom ett steg leder till nästa och det sista, samordningsdelen, kan igen leda till en ny analys, varefter cykeln börjar på nytt. Processen slutar när alla berörda parter har tagit emot och rapporterat all nödvändig information.

Se CERT/CC:s CSIRT-handbok för en mer detaljerad beskrivning av incidentens livscykel ([29]).

Incidenthanteringsrapport
Förbered dig på ledningens frågor om incidenter genom att utarbeta en rapport. Det är också en bra idé att skriva ett dokument (enbart för internt bruk) om vad man lärt sig för att kunna lära upp de anställda och undvika misstag i framtida incidenthantering.

Arkivering
Se arkiveringsreglerna som beskrivits tidigare i kapitel *6.6 Utveckling av en policy för informationssäkerhet*.

([29]) CSIRT:s handbok: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Se avsnitt A.1 *Ytterligare läsning* i bilagan för en heltäckande guide om incidenthantering och incidentens livscykel.

8.4 Exempel på tidsplan för responsen

Angivandet av responstider försummas ofta, men det måste vara en del av alla välkonstruerade servicenivåavtal (SLA) mellan ett CSIRT och dess basgrupp. Att ge snabb feedback till basgruppens medlemmar under incidenthanteringen är av avgörande betydelse, såväl för medlemmarnas egna skyldigheter som för teamets rykte.

Basgruppen måste få tydlig information om responstiderna för att undvika felaktiga förväntningar. Följande mycket enkla tidtabell kan användas som en utgångspunkt för ett mer detaljerat SLA med CSIRT-enhetens basgrupp.

Här visas ett exempel på tidsplan för realistiska responstider från det att en begäran om hjälp kommer in:

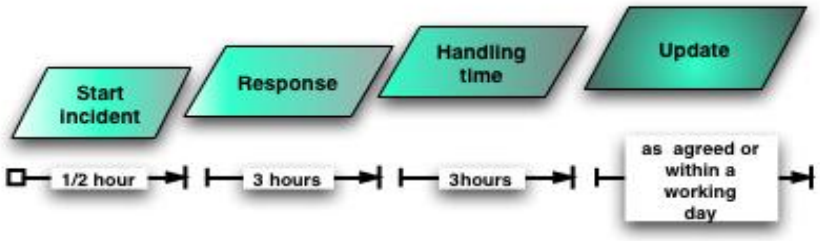


Fig. 16. Exempel på responstidtabell.

Det kan också vara bra att instruera basgruppen om deras egna responstider, framför allt när de ska kontakta CSIRT-enheten i ett nödläge. I de flesta fall är det bättre att de kontaktar sitt CSIRT i ett tidigt skede, och det är en god vana att uppmuntra basgruppen att alltid göra det i tveksamma fall.

8.5 Tillgängliga CSIRT-verktyg

I detta kapitel ges viss information om vanliga verktyg som används av CSIRT-enheten. Detta är enbart exempel. Mer information finns hos CHIHT, *Clearinghouse of Incident Handling Tools* ([30]).

Krypteringsprogram för e-post och meddelanden

- GnuPG http://www.gnupg.org/
  GnuPG är GNU-projektets kompletta, kostnadsfria tillämpning av standarden OpenPGP enligt definitionen i RFC2440. Med GnuPG kan du kryptera och underteckna dina data och dina meddelanden.

- PGP http://www.pgp.com/
  Kommersiell variant.

Verktyg för incidenthantering

För att administrera och följa upp incidenter och hålla ordning på vidtagna åtgärder.

- RTIR http://www.bestpractical.com/rtir/
  RTIR är ett gratissystem med öppen källa för incidenthantering som konstruerats med tanke på CERT-teamens och andra incidentresponsteams behov.

CRM-verktyg

När din basgrupp har många olika medlemmar och du måste hålla ordning på alla möten och detaljer kan en CRM-databas vara nyttig. Det finns många olika varianter. Här följer ett par exempel:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (gratisversion med öppen källa) http://www.sugarforge.org/

Informationskontroll

- Website watcher http://www.aignes.com/index.htm
  Det här programmet övervakar om webbplatser uppdateras och ändras.

- Watch that page http://www.watchthatpage.com/
  Denna tjänst skickar information om ändringar på webbplatser via e-post (gratis- och betalversion).

([30]) CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Att hitta kontaktinformation
Att hitta rätt kontakt att rapportera incidenter till är inte helt enkelt. Det finns ett par informationskällor som kan användas:

- RIPE ([31])
- IRT-objekt ([32])
- TI ([33])

Dessutom har CHIHT en förteckning över verktyg för att hitta kontaktinformation ([34]).

Fiktivt CSIRT (steg 8)

Att skapa processflöden och operativa och tekniska förfaranden
Vårt fiktiva CSIRT fokuserar på att leverera kärntjänster inom CSIRT:

- Larm och varningar
- Meddelanden
- Incidenthantering

Teamet utvecklade förfaranden som fungerar bra och som alla teamets medlemmar lätt kan förstå. Vårt fiktiva CSIRT anställde också en juridisk expert för att hantera ansvarsfrågor och informationens säkerhet. Teamet införde vissa användbara verktyg och fick nyttig information om operativa frågor genom att diskutera med andra CSIRT.

En fast mall för säkerhetsbulletiner och incidentrapporter togs fram. Teamet använder RTIR för incidenthanteringen.

([31]) RIPE whois: http://www.ripe.net/whois

([32]) IRT-objekt på databasen RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

([33]) Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

([34]) Verktyg för att kontrollera identiteter på CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 CSIRT-utbildning

Vi har tagit följande steg:

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska tillhandahålla sina tjänster till.
3. Att bestämma vilka typer av tjänster ett CSIRT kan erbjuda sin basgrupp.
4. Analys av miljö och basgruppens medlemmar.
5. Formulering av uppdragsbeskrivningen.
6. Att utarbeta affärsplanen.
   a. Att definiera finansieringsmodellen.
   b. Att bestämma organisationsstrukturen.
   c. Att börja anställa personal.
   d. Att använda och utrusta kontoret.
   e. Att utveckla en policy för informationssäkerhet.
   f. Att leta efter samarbetspartner.
7. Att genomföra affärsplanen.
   a. Att godkänna affärsscenariot.
   b. Att få med allt i en projektplan.
8. Att se till att vårt CSIRT blir operativt.
   a. Att skapa arbetsflöden.
   b. Att förse CSIRT med verktyg.

>> Nästa steg: att utbilda personalen.

I det här avsnittet tar vi upp två av huvudkällorna för riktad CSIRT-utbildning: TRANSITS- och CERT/CC-kurserna.

9.1 TRANSITS

TRANSITS har varit ett europeiskt projekt för att främja upprättandet av nya CSIRT (Computer Security Incident Response Teams) och förstärka befintliga CSIRT genom att lösa problemet med bristen på utbildad CSIRT-personal. Lösningen har varit att tillhandahålla riktade kurser för att utbilda anställda i (nya) CSIRT i administrativa, driftsmässiga, tekniska, marknadsmässiga och juridiska frågor i samband med CSIRT-enhetens tjänster.

TRANSITS har framför allt

- ett utvecklat, aktuellt, moduluppbyggt utbildningsmaterial som revideras regelbundet,
- organiserat workshopar där kursmaterialet har använts,
- gjort det möjligt för personalen vid (nya) CSIRT att delta i dessa workshopar, med särskild tonvikt vid deltagare från EU:s kandidatländer,
- spridit utbildningsmaterial och sett till att resultaten utnyttjas ([35]).

([35]) TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

ENISA administrerar och stödjer TRANSITS-kurserna. Om du vill veta hur man ansöker om att få delta i kurserna samt krav och kostnader kan du kontakta ENISA:s CSIRT-experter:

CERT-Relations@enisa.europa.eu

Exempel på kursmaterial hittar du i bilagan till detta dokument.

9.2 CERT/CC

De datoriserade systemens och nätverkens komplexitet och utmaningen att administrera dem gör det svårt att hantera nätverkssäkerheten korrekt. Nätverks- och systemadministratörerna har inte tillräckligt med personal och säkerhetsrutiner på plats för att kunna försvara sig mot attacker och minimera skadorna. Resultatet blir ett ökande antal datasäkerhetsincidenter.

När det inträffar datasäkerhetsincidenter måste organisationerna reagera snabbt och effektivt. Ju snabbare en organisation känner igen, analyserar och reagerar på en incident, desto bättre kan den begränsa skadorna och sänka återställningskostnaderna. Att inrätta ett team med ansvar för att hantera incidenter i samband med datasäkerhet (ett CSIRT) är ett bra sätt att skapa denna snabbinsatskapacitet och att minska risken för framtida incidenter.

CERT-CC erbjuder kurser för chefer och teknisk personal inom områden som hur man skapar och leder team med ansvar för att hantera incidenter i samband med datasäkerhet (CSIRT), hur man reagerar på och analyserar säkerhetsincidenter och hur man förbättrar nätverkssäkerheten. Om inte annat anges kommer samtliga kurser att äga rum i Pittsburgh, PA. Våra anställda undervisar också vid kurser på Carnegie Mellon-universitetet.

Tillgängliga CERT/CC-kurser ([36]) inriktade på CSIRT:

Hur man skapar ett CSIRT
Hur man leder ett CSIRT
Grunderna i incidenthantering
Avancerad incidenthantering för teknisk personal

Exempel på kursmaterial hittar du i bilagan till detta dokument.

Fiktivt CSIRT (steg 9)
Att utbilda personalen Vårt fiktiva CSIRT har beslutat att skicka alla sina tekniker till nästa tillgängliga TRANSITS-kurs. Teamets ledare kommer dessutom att gå en av CERT/CC:s kurser i *att leda ett CSIRT*.

([36]) CERT/CC:s kurser: http://www.sei.cmu.edu/products/courses

10 Övning: att framställa en bulletin

Vi har tagit följande steg:

1. Att förstå vad ett CSIRT är och vilka fördelar det kan erbjuda.
2. Att bestämma vilken sektor det nya teamet ska tillhandahålla sina tjänster till.
3. Att bestämma vilka typer av tjänster ett CSIRT kan erbjuda sin basgrupp.
4. Analys av miljö och basgruppens medlemmar.
5. Formulering av uppdragsbeskrivningen.
6. Att utarbeta affärsplanen.
   a. Att definiera finansieringsmodellen.
   b. Att bestämma organisationsstrukturen.
   c. Att börja anställa personal.
   d. Att använda och utrusta kontoret.
   e. Att utveckla en policy för informationssäkerhet.
   f. Att leta efter samarbetspartner.
7. Att genomföra affärsplanen.
   a. Att godkänna affärsscenariot.
   b. Att få med allt i en projektplan.
8. Att se till att vårt CSIRT blir operativt.
   a. Att skapa arbetsflöden.
   b. Att förse CSIRT med verktyg.
9. Att utbilda personalen.

>> Nästa steg är att öva sig och bli redo för det verkliga arbetet.

Det här avsnittet innehåller ett exempel på hur man hanterar ett rutinuppdrag i ett CSIRT: att skapa en säkerhetsbulletin.

Den utlösande faktorn var följande ursprungliga säkerhetsbulletin från Microsoft:

Bulletinens identifiering	**Microsofts säkerhetsbulletin MS06-042**
Bulletinens titel	**Cumulative Security Update for Internet Explorer (918899)**
Samman-fattning	Uppdateringen åtgärdar flera sårbarheter i Internet Explorer som skulle kunna medge exekvering av fjärrkoder.
Maximal grad av skaderisk	Kritisk
Sårbarhetens effekt	Exekvering av fjärrkod
Påverkad programvara	**Windows, Internet Explorer.** Se avsnitten Påverkad programvara och Adress för nedladdning för mer information.

Denna bulletin som vänder sig till försäljare avser en sårbarhet som nyligen påträffats i Internet Explorer. Försäljaren offentliggör flera olika lösningar för programvaran för flera olika versioner av Microsoft Windows.

Sedan vårt fiktiva CSIRT har mottagit denna sårbarhetsinformation via en sändlista börjar det med arbetsflödet i kapitel *8.2 Att skapa larm, varningar och meddelanden*.

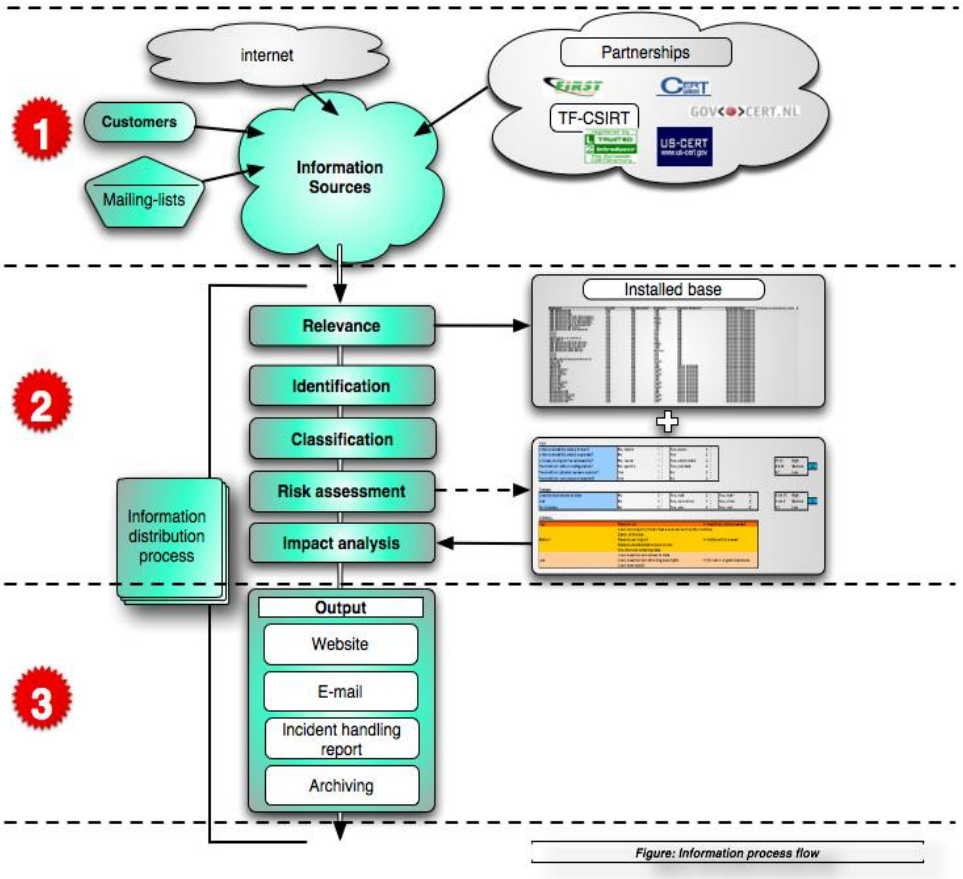


Figure: Information process flow

Steg 1: Insamling av sårbarhetsinformation

Det första steget är att söka på försäljarens webbplats. Där kan vårt fiktiva CSIRT kontrollera att informationen är autentisk och samla in fler detaljer om sårbarheten och de påverkade IT-systemen.

Steg 2: Utvärdering av informationen och riskbedömning

Identifiering
Informationen har redan verifierats genom att vi jämförde sårbarhetsinformationen som kom via e-post med texten på försäljarens webbplats.

Relevans
Vårt fiktiva CSIRT kontrollerar förteckningen över påverkade system på webbplatsen med listan över system som används i basgruppen. Det upptäcker att minst en av basgruppens medlemmar använder Internet Explorer, så sårbarhetsinformationen är verkligen relevant.

Kategori	Applikation	Program-produkt	Version	Operativ-system	Operativ-system, version	Medlem
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A

Klassificering
Informationen är offentlig, så den kan användas och skickas vidare.

Riskbedömning och effektanalys
Genom att besvara frågorna kommer vi fram till att risk och effekt är *höga* (*kritiska* enligt Microsoft).

RISK

Är sårbarheten välkänd?	Ja
Är sårbarheten allmänt spridd?	Ja
Är det lätt att utnyttja sårbarheten?	Ja
Är det en sårbarhet som kan utnyttjas på distans?	Ja

SKADA
Tänkbara effekter är fjärrtillträde och eventuell exekvering av fjärrkoder. Denna sårbarhet omfattar flera olika problem, vilket gör att skaderisken är *hög*.

Steg 3: Distribuering

Vårt fiktiva CSIRT är ett internt CSIRT. Det förfogar över e-post, telefon och den interna webbplatsen som kommunikationskanaler. CSIRT-enheten utarbetar följande bulletin med hjälp av mallen i kapitel *8.2 Att skapa larm, varningar och meddelanden*.

Bulletinens titel
Flera olika sårbarheter har påträffats i Internet Explorer

Referensnummer
082006-1
Påverkade system
- Alla desktopsystem som kör Microsoft

Aktuellt operativsystem + version
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 och Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 och Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 för Itanium-baserade system och Microsoft Windows Server 2003 med SP1 för Itanium-baserade system
- Microsoft Windows Server 2003 x64 Edition

Risk (Hög-Medel-Låg)
HÖG
Effekt/potentiell skada (Hög-Medel-Låg)
HÖG
Externa id: (CVE, ID för sårbarhetsbulletin)
MS-06-42

Översikt över sårbarheten
Microsoft har påträffat flera allvarliga sårbarheter i Internet Explorer som kan leda till exekvering av fjärrkoder.

Effekt
Den som attackerar kan ta över systemet helt, installera program, lägga till användare och gå in och ändra eller radera data. En lindrande faktor är att detta endast kan ske om användaren är inloggad som administratör. Användare som loggat in med färre rättigheter skulle kunna påverkas i mindre grad.

Lösning
Komplettera ditt IE omedelbart.

Beskrivning (detaljer)
Se ms06-042.mspx för mer information.

Bilaga
Se ms06-042.mspx för mer information.

Denna information är nu redo för distribution. Eftersom det handlar om en kritisk bulletin är det också lämpligt att ringa upp medlemmarna.

Fiktivt CSIRT (steg 10)
Övning Under de första veckorna använde vårt fiktiva CSIRT flera fiktiva fall (som de fick som exempel från andra CSIRT) som övningar. Dessutom utfärdades ett antal säkerhetsbulletiner som byggde på äkta sårbarhetsinformation från hårdvaru- och programvaruförsäljare som sedan anpassades efter basgruppens behov.

11 Slutsats

Här slutar själva vägledningen. Syftet med detta dokument var att ge en mycket kortfattad översikt över de olika processer som behövdes för att inrätta ett CSIRT. Vi hävdar inte att vägledningen är komplett, och den går inte heller alltför djupt in på detaljer. Se avsnittet *A.1 Ytterligare läsning* i bilagan för att hitta litteratur i frågan som det kan vara värt att läsa.

Nästa viktiga steg för vårt fiktiva CSIRT skulle nu bli

- att ta emot feedback från basgruppen för att finslipa de tjänster som erbjuds,
- att skapa rutiner för det dagliga arbetet,
- att öva nödsituationer,
- att hålla en nära kontakt med de olika CSIRT-grupperna för att en dag kunna bidra till deras frivilliga arbete.

12 Beskrivning av projektplanen

Anm.: Projektplanen är en första uppskattning av den tid som behövs. Beroende på tillgängliga resurser kan projektets faktiska varaktighet variera.

Projektplanen finns tillgänglig i olika format på cd och på ENISA:s webbplats. Den täcker helt samtliga de processer som beskrivits i detta dokument.

Huvudformatet blir Microsoft Project, som kan användas direkt i detta verktyg för programplanering.

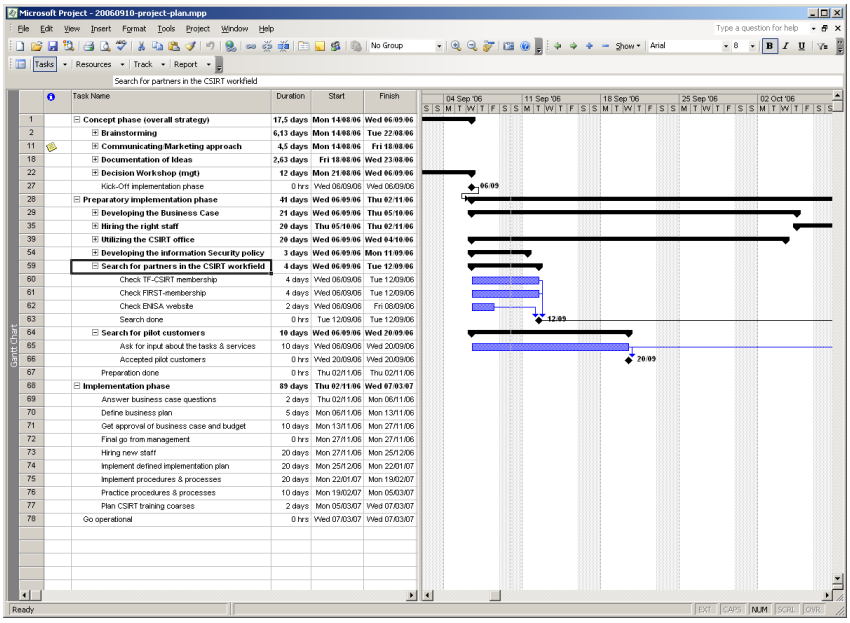
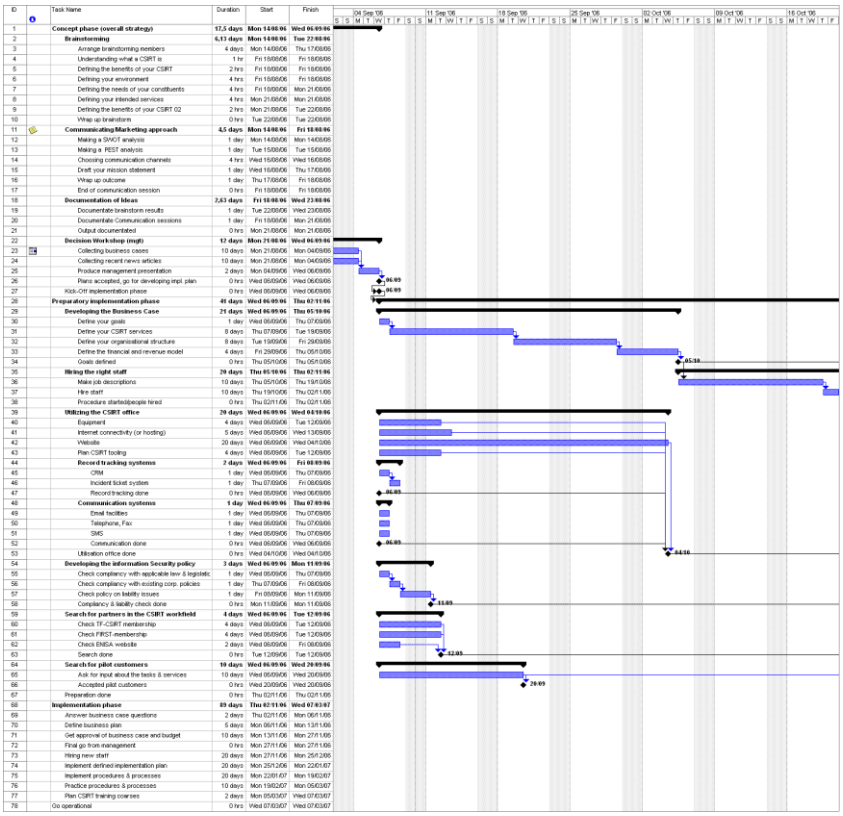


Fig. 17. Projektplan.



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**45 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilization done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training courses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Fig. 18. Projektplanen med samtliga uppgifter och en del av Gantdiagrammet.

Projektplanen finns också tillgänglig i cvs- och xml-format. Råd om ytterligare användning ges av ENISA:s CSIRT-experter: CERT-Relations@enisa.europa.eu

BILAGA

A.1 Ytterligare läsning

Handbook for CSIRTs (CERT/CC)
Ett mycket omfattande referensverk för alla frågor som gäller arbetet i ett CSIRT.
Källa: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress
En grundlig analys av incidenthantering.
Källa: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs)
En heltäckande analys av dagsläget för det globala CSIRT-landskapet, inklusive historia, statistik och mycket annat.
Källa: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
En heltäckande beskrivning av vilka lärdomar man drog av att inrätta GOVCERT.NL och ”De Waarschuwingsdienst”, den nederländska nationella larmtjänsten.
Källa: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response
Källa: http://www.ietf.org/rfc/rfc2350.txt

NIST ([37]) Computer Security Incident Handling Guide
Källa: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe
Ett referensverk som innehåller information om CSIRT-enheter i Europa och deras olika aktiviteter.
Källa: http://www.enisa.europa.eu/cert_inventory/

([37]) NIST: National Institute of Standards and Technologies.

A.2 CSIRT-tjänster

Ett särskilt tack till CERT/CC, som försåg oss med denna lista.

Reaktiva tjänster	***Proaktiva tjänster***	***Artefakthantering***
• Larm och varningar • Incidenthantering • Incidentanalys • Incidentrespons på plats • Stöd för incidentrespons • Samordning av incidentrespons • Sårbarhetshantering • Sårbarhetsanalys • Sårbarhetsrespons • Samordning av sårbarhetsrespons	• Meddelanden • Teknikbevakning • Säkerhetsrevision eller kontroll • Säkerhetens utformning och underhåll • Utveckling av säkerhetsverktyg • Detektering av inkräktare • Spridning av säkerhetsrelaterad information	• Artefaktanalys • Artefaktrespons • Samordning av artefaktrespons ***Säkerhetskvalitets-styrning*** • Riskanalys • Kontinuitet och katastrofåterställning • Säkerhetsrådgivning • Medvetandebyggande • Utbildning • Utvärdering och certifiering av produkter

Fig. 19. Förteckning över CSIRT-tjänster från CERT/CC.

Beskrivning av tjänsterna

Reaktiva tjänster

Reaktiva tjänster är avsedda att reagera på förfrågningar om hjälp, incidentrapporter från CSIRT-enhetens basgrupp och alla hot eller attacker mot CSIRT-system. Initiativet till vissa tjänster kan komma från meddelanden från tredje part eller genom att man granskar övervaknings- eller IDS-loggar och larm.

Larm och varningar

Denna tjänst omfattar spridning av information som beskriver en attack eller säkerhetssårbarhet, ett intrångslarm, datavirus eller en bluff, och att rekommendera åtgärder på kort sikt för att hantera det problem som uppkommit. Larmet, varningen eller bulletinen skickas som en reaktion på det uppkomna problemet för att meddela basgruppens medlemmar om aktiviteten och hjälpa dem att skydda sina system eller återställa system som påverkats. Information kan skapas av CSIRT eller skickas ut från försäljare, andra CSIRT eller säkerhetsexperter, eller andra delar av basgruppen.

Incidenthantering

Incidenthantering omfattar att ta emot, sortera och reagera på förfrågningar och rapporter och att analysera incidenter och händelser. De särskilda responsaktiviteterna kan omfatta

- att vidta åtgärder för att skydda system och nätverk som påverkats eller hotas av inkräktarens aktivitet,
- att erbjuda lösningar och strategier från bulletiner eller larm,
- att leta efter en inkräktare i andra delar av nätverket,

- att filtrera nätverkstrafiken,
- att bygga upp systemen igen,
- att komplettera eller reparera systemen,
- att utveckla andra strategier för respons eller för att undvika problemet.

Eftersom incidenthanteringen genomförs på olika sätt av olika slags CSIRT, delas denna tjänst upp i ytterligare kategorier beroende på typen av aktivitet som utförs och den typ av hjälp som erbjuds enligt följande:

Incidentanalys

Det finns många nivåer inom incidentanalys och många deltjänster. Incidentanalys är i allt väsentligt ett sätt att undersöka all tillgänglig information och stödjande bevisning eller artefakter i samband med en incident eller händelse. Syftet med analysen är att identifiera incidentens omfattning, skadorna som incidenten orsakat, incidentens natur och tillgängliga responsstrategier eller sätt att undvika problemet. CSIRT-enheten kan använda resultaten från sårbarhets- och artefaktanalysen (beskrivs nedan) för att förstå och ge den mest kompletta och uppdaterade analysen av vad som hänt i ett visst system. CSIRT gör aktiva jämförelser mellan olika incidenter för att avgöra om det föreligger kopplingar, trender, mönster eller inkräktarsignaturer. Två deltjänster som kan utföras som ett led i incidentanalysen, beroende på CSIRT-enhetens uppdrag, syfte och processer är följande:

Insamling av kriminalteknisk bevisning

Insamling, förvaring, dokumentering och analys av bevis från ett drabbat datasystem för att avgöra vilka ändringar som gjorts i systemet och för att hjälpa till att återskapa de händelser som ledde fram till skadan. Denna insamling av information och bevis måste göras på ett sätt som dokumenterar en händelsekedja som kan styrkas och som kan användas som bevisning i en domstol. De uppgifter som ingår i insamlingen av kriminalteknisk bevisning omfattar (men är inte begränsade till) att göra en bit-image-kopia av det drabbade systemets hårddisk, kontrollera om det finns ändringar i systemet såsom nya program, filer och användare, undersöka körprocesser och öppna portar och att kontrollera om det finns trojaner i form av program eller verktyg. CSIRT-enhetens anställda som utför denna funktion måste också vara beredda att uppträda som expertvittnen i domstolsförfaranden.

Spårning

Att spåra ursprunget för en inkräktare eller identifiera system som inkräktaren hade tillgång till. Denna aktivitet kan innebära att man undersöker hur inkräktaren tog sig in i de drabbade systemen och tillhörande nätverk, vilka system som användes för att få tillträde, var attacken påbörjades och vilka övriga system och nätverk som användes som en del av attacken. Det kan också innebära att man försöker bestämma inkräktarens identitet. Detta arbete kan man utföra på egen hand, men i regel innebär det att man arbetar tillsammans med polismyndigheter, leverantörer av Internettjänster eller andra berörda organisationer.

Incidentrespons på platsen

CSIRT-enheten erbjuder direkt assistans på platsen för att hjälpa basgruppens medlemmar att återställa efter en incident. CSIRT-enheten analyserar de drabbade systemen fysiskt och utför reparation och återställning på systemen, i stället för att enbart erbjuda incidentsupport per telefon eller e-post (se nedan). Tjänsten omfattar alla åtgärder som vidtas på lokal nivå och som är nödvändiga om en incident misstänks eller har inträffat. Om CSIRT-enheten inte är placerad på den drabbade arbetsplatsen skulle teamets medlemmar resa till platsen och utföra responsåtgärderna. I andra fall kan ett lokalt team redan finnas på platsen och ge incidentrespons som en del av sitt rutinarbete. Detta stämmer framför allt om incidenthanteringen erbjuds som en del av system-, nätverks- eller säkerhetsadministratörers normala arbetsuppgifter, trots att ett CSIRT har inrättats.

Incidentresponssupport

CSIRT-enheten assisterar och vägleder dem som utsatts för en attack när de ska återställa sina system. Hjälpen ges via telefon, e-post, fax eller dokumentation. Detta kan innebära teknisk hjälp med att tolka insamlade data, erbjuda kontaktinformation eller vidarebefordra vägledning om lindrings- och återställningsstrategier. Det omfattar inte direkt incidentrespons på platsen på det sätt som beskrivits ovan. CSIRT-enheten erbjuder i stället hjälp på distans så att personalen på platsen själva kan utföra återställningen.

Samordning av incidentrespons

CSIRT-enheten samordnar responsinsatserna bland de parter som berörs av incidenten. Detta omfattar i regel offren för attacken, andra platser som berörs av attacken och alla platser som kan behöva hjälp med att analysera attacken. Det kan också omfatta de parter som erbjuder IT-stöd åt offret, såsom leverantörer av Internettjänster, andra CSIRT-enheter och system- och nätverksadministratörer på platsen. Samordningsarbetet kan omfatta att samla in kontaktinformation, meddela de olika platserna om risken för att eventuellt drabbas (som offer för eller källor till en attack), insamling av statistik om antalet platser som drabbats, och att underlätta informationsutbyte och analys. En del av samordningsarbetet kan omfatta att meddela och samarbeta med en organisations avdelningar för rättsliga frågor, HR eller PR. Det skulle också kunna omfatta samordning med polismyndigheter. Denna tjänst omfattar inte direkt incidentrespons på platsen.

Sårbarhetshantering

Sårbarhetshantering omfattar att ta emot information och rapporter om hårdvarans och programvarans sårbarhet, att analysera sårbarheternas natur, mekanismer och effekter och att utveckla responsstrategier för att upptäcka och reparera sårbarheten. Eftersom sårbarhetshanteringen genomförs på olika sätt av olika CSIRT delas denna tjänst upp i ytterligare kategorier beroende på typen av aktivitet som utförs och den typ av hjälp som erbjuds, enligt följande:

Sårbarhetsanalys

CSIRT-enheten utför en teknisk analys och undersökning av sårbarheter i hårdvara eller programvara. Detta omfattar att verifiera misstänkta sårbarheter och en teknisk undersökning av hårdvarans eller programvarans sårbarhet för att avgöra var den är

placerad och hur den kan utnyttjas. Analysen kan omfatta en granskning av källkoden, att man använder ett felsökningsprogram för att avgöra var sårbarheten inträffar eller att man försöker återskapa problemet i ett testsystem.

Sårbarhetsrespons

Denna tjänst omfattar att man fastställer lämplig respons för att lindra eller reparera sårbarheten. Detta kan omfatta att man utvecklar eller analyserar programrättning, fixar eller andra typer av tillfälliga lösningar. Det kan också innebära att man meddelar andra om strategin för att mildra effekterna, eventuellt genom att skapa och distribuera bulletiner eller larm. Tjänsten kan också omfatta att man utför åtgärder genom att installera programrättningar, fixar eller tillfälliga lösningar.

Samordning av sårbarhetsrespons

CSIRT-enheten meddelar de olika delarna av verksamheten eller basgruppen om sårbarheten och sprider information om hur sårbarheten ska rättas till eller mildras. CSIRT-enheten kontrollerar att strategin för sårbarhetsrespons har genomförts framgångsrikt. Tjänsten kan omfatta att kommunicera med försäljare, andra CSIRT-enheter, tekniska experter, basgruppens medlemmar och de individer eller grupper som ursprungligen upptäckte eller rapporterade sårbarheten. Bland aktiviteterna ingår att underlätta analysen av en sårbarhet eller sårbarhetsrapport, att samordna utgivningen av motsvarande dokument, programrättningar eller tillfälliga lösningar och att sammanfatta de tekniska analyser som utförts av olika parter. Tjänsten kan också omfatta att man för offentliga eller privata arkiv eller kunskapsbaser över sårbarhetsinformation och motsvarande responsstrategier.

Artefakthantering

En artefakt är en fil eller ett objekt som upptäcks i ett system som skulle kunna delta i att testa eller attackera system eller nätverk eller som används för att motverka säkerhetsåtgärder. Artefakter kan omfatta, men är inte begränsade till, datavirus, trojanska hästar, maskar, exploateringskoder och verktygslådor.
Artefakthanteringen omfattar att ta emot information om och kopior på artefakter som används i inkräktares attacker, rekognoscering och andra icke auktoriserade eller störande aktiviteter. När artefakten väl har mottagits granskas den. Detta omfattar en analys av artefaktens natur, mekanismer, version och användning samt att utveckla (eller föreslå) responsstrategier för att upptäcka, avlägsna och försvara sig mot dessa artefakter. Eftersom artefakthanteringen genomförs på olika sätt av olika CSIRT delas denna tjänst upp i ytterligare kategorier beroende på typen av aktivitet som utförs och den typ av hjälp som erbjuds enligt följande:

Artefaktanalys

CSIRT-enheten utför en teknisk undersökning och analys av eventuella artefakter som upptäcks i ett system. Analysen kan omfatta att man identifierar filtyp och struktur för artefakten, jämför en ny artefakt med befintliga artefakter eller andra versioner av samma artefakt för att se om det finns likheter och skillnader, eller utför bakåtkompilering eller uppackning av koder för att avgöra vad som är artefaktens syfte och funktion.

Artefaktrespons

Denna tjänst omfattar att bestämma lämpliga åtgärder för att upptäcka och avlägsna artefakter från ett system samt åtgärder för att förhindra att artefakter installeras. Detta kan omfatta att man skapar signaturer som kan läggas till i antivirusprogram eller IDS.

Samordning av artefaktrespons

Denna tjänst omfattar att man sammanfattar och sprider analysresultat och responsstrategier som hör till en viss artefakt till andra forskare, CSIRT-enheter, försäljare och andra säkerhetsexperter. Aktiviteterna inkluderar att man underrättar andra och sammanfattar tekniska analyser från många olika källor. Aktiviteterna kan också omfatta att man för ett arkiv som är offentligt eller enbart avsett för basgruppens medlemmar över kända artefakter och deras effekter samt motsvarande responsstrategier.

Proaktiva tjänster

Proaktiva tjänster är avsedda att förbättra basgruppens infrastruktur och säkerhetsprocesser innan en incident eller händelse inträffar eller upptäcks. Huvudmålet är att undvika incidenter och att minska deras effekter och omfattning när de faktiskt inträffar.

Meddelanden

Detta omfattar, men är inte begränsat till, intrångslarm, sårbarhetsvarningar och säkerhetsbulletiner. Sådana meddelanden informerar basgruppens medlemmar om nya händelser med medellång till långsiktig verkan, till exempel nyligen upptäckta sårbarheter eller verktyg för inkräktare. Genom meddelanden blir det möjligt för basgruppens medlemmar att skydda sina system och nätverk mot nyupptäckta problem innan de kan utnyttjas.

Teknikbevakning

CSIRT-enheten bevakar och observerar den tekniska utvecklingen och inkräktarnas aktiviteter och trender i samband därmed för att hjälpa till att identifiera framtida hot. De granskade områdena kan utsträckas till att omfatta domstolsbeslut och ny lagstiftning, sociala eller politiska hot och framväxande teknikområden. I tjänsten ingår att läsa sändlistor med säkerhetsinformation, webbplatser och artiklar i dags- och specialtidningar inom områdena vetenskap, teknik, politik och statlig verksamhet för att få fram information som är relevant för säkerheten för basgruppens system och nätverk. Detta kan omfatta att kommunicera med andra parter som är auktoriteter på dessa områden för att se till att man får bästa tänkbara information eller tolkning. Resultatet av denna tjänst skulle kunna vara någon typ av meddelanden, riktlinjer eller rekommendationer med inriktning på säkerhetsfrågor med effekt på medellång till lång sikt.

Säkerhetsrevisioner eller utvärderingar

Genom denna tjänst erbjuds en detaljerad granskning och analys av en organisations säkerhetsinfrastruktur, baserat på de krav som angetts av organisationen eller i andra gällande industristandarder. Det kan också omfatta en granskning av organisationens säkerhetsrutiner. Det finns många olika typer av revisioner eller granskningar som kan erbjudas, bland annat följande:

Granskning av infrastruktur

Att manuellt granska hårdvara och programvara med avseende på konfigurering, routrar, brandväggar, servrar och desktopenheter för att se till att de motsvarar bästa praxis vad gäller organisationens eller branschens säkerhetspolicy och standardkonfigurering.

Granskning av bästa praxis

Intervjuer med de anställda och system- och nätverksadministratörer för att fastställa om deras säkerhetsrutiner motsvarar accepterad säkerhetsstandard för organisationen eller någon specifik branschstandard.

Skanning

Att använda sårbarhets- eller virusskannrar för att avgöra vilka system eller nätverk som är sårbara.

Penetrationstestning

Att testa säkerheten för en viss plats genom att avsiktligt attackera dess system och nätverk.
Den högsta ledningens godkännande krävs innan man genomför sådana revisioner eller kontroller. Några av dessa strategier kan vara förbjudna enligt organisationens policy. Att tillhandahålla denna tjänst kan inkludera att utveckla en gemensam uppsättning rutiner mot vilka testen eller kontrollerna utförs, tillsammans med att man fastställer vilken uppsättning kunskaper eller certifieringskrav som ska gälla för att personalen ska få utföra testning, kontroll, revisioner eller granskningar. Denna tjänst skulle också kunna läggas ut på tredje part eller en egen speciell leverantör av säkerhetstjänster med lämpliga expertkunskaper när det gäller att utföra revisioner och kontroller.

Konfigurering och underhåll av säkerhetsverktyg, tillämpningar, infrastruktur och tjänster

Genom denna tjänst identifieras eller tillhandahålls lämplig vägledning för hur man säkert ska konfigurera och använda verktyg, tillämpningsprogram och den datainfrastruktur som används av CSIRT-enhetens basgrupp eller CSIRT-enheten själv. Förutom att tillhandahålla vägledning kan CSIRT-enheten utföra uppdatering av konfigureringar och underhåll av säkerhetsverktyg och tjänster, såsom IDS, nätverksskanning eller övervakning av system, filter, wrappers, brandväggar, virtuella privata nät (VPN) eller autenticeringsmekanismer. CSIRT-enheten kan till och med erbjuda dessa tjänster som en del av sin huvudfunktion. Den kan också konfigurera och underhålla servrar, desktopdatorer, personliga digitala assistenter (PDA) och andra trådlösa apparater enligt gällande säkerhetspolicy. Tjänsten omfattar att informera ledningen om alla frågor eller problem som gäller konfigurering eller användning av verktyg och applikationer som CSIRT-enheten tror kan göra systemet sårbart för en attack.

Utveckling av säkerhetsverktyg

Denna tjänst omfattar utvecklingen av nya, medlemsspecifika verktyg som kan krävas eller önskas av basgruppen eller av CSIRT-enheten själv. Detta kan till exempel omfatta utveckling av programrättningar för specialutvecklad programvara som används av basgruppen eller säker distribution av programvara som kan användas för att återställa drabbade värddatorer. Det kan också omfatta att man utvecklar verktyg eller skript som utökar funktionen eller befintliga säkerhetsverktyg, till exempel en ny plug-in för en

sårbarhet eller nätverksskanner, skript som underlättar användningen av krypteringsteknik eller mekanismer för automatisk distribution av programrättningar.

Tjänster för detektering av inkräktare

CSIRT-enheter som utför denna typ av tjänster granskar befintliga IDS-loggar, analyserar och inleder en respons för alla händelser som motsvarar deras definierade tröskel, eller vidarebefordrar alla larm enligt ett i förväg överenskommet avtal om servicenivå eller en i förväg bestämd eskaleringsstrategi. Detektering av inkräktare och analys av respektive säkerhetsloggar kan vara en svår uppgift – inte bara när det gäller att bestämma var sensorerna ska placeras i miljön, utan när det gäller att samla in och sedan analysera stora mängder data. I många fall krävs det specialverktyg eller expertkunskaper för att sammanfatta och tolka informationen för att kunna identifiera falska larm, attacker eller nätverkshändelser och att genomföra strategier för att eliminera eller minimera sådana händelser. Vissa organisationer väljer att lägga ut denna verksamhet på andra som har mer erfarenhet av att utföra dessa tjänster, till exempel särskilda leverantörer av säkerhetstjänster.

Spridning av säkerhetsrelaterad information

Genom denna tjänst får basgruppens deltagare en heltäckande och lättillgänglig samling av användbar information som bidrar till att förbättra säkerheten. Sådan information kan omfatta

- att rapportera CSIRT-enhetens riktlinjer och kontaktinformation,
- arkiv över larm, varningar och andra meddelanden,
- dokumentering av nuvarande bästa praxis,
- allmänna riktlinjer för datasäkerhet,
- policy, procedurer och checklistor,
- information om utveckling och spridning av programrättningar,
- länkar till försäljare,
- aktuell statistik och trender inom incidentrapportering,
- övrig information som kan förbättra den allmänna säkerheten.

Denna information kan utvecklas och offentliggöras av CSIRT-enheten eller någon annan del av organisationen (IT, personalavdelning eller mediekontakter), och kan omfatta information från externa källor såsom andra CSIRT-enheter, försäljare och säkerhetsexperter.

Tjänster avseende säkerhetskvalitetsstyrning

Tjänster som faller inom denna kategori är inte unika för just incidenthantering eller CSIRT-enheter. Det är välkända, etablerade tjänster som utformats för att förbättra den allmänna säkerheten i en viss organisation. Genom att utnyttja de erfarenheter man gjort av att tillhandahålla reaktiva och proaktiva tjänster som beskrivits ovan kan en CSIRT-enhet tillföra dessa kvalitetsstyrningstjänster unika perspektiv som annars kanske inte skulle vara tillgängliga. Tjänsterna är utformade för att inkorporera feedback och de lärdomar som dragits utifrån de kunskaper som vunnits genom att reagera på incidenter, sårbarheter och attacker. Att mata in sådana erfarenheter i etablerade traditionella tjänster (beskrivs nedan) som en del av processen för säkerhetskvalitetsstyrningen kan förbättra de långsiktiga säkerhetsinsatserna i en organisation. Beroende på organisationsstrukturer och ansvarsområden kan en

CSIRT-enhet tillhandahålla dessa tjänster eller ingå i en större teaminsats inom organisationen.
Nedan beskrivs hur CSIRT-enhetens expertkunskaper kan vara till nytta för var och en av dessa tjänster inom säkerhetskvalitetsstyrning.

Riskanalys
CSIRT-enheter kan tillföra riskanalyser och utvärderingar ett mervärde. Detta kan förbättra organisationens förmåga att utvärdera verkliga hot, ge realistiska kvalitativa och kvantitativa utvärderingar av riskerna för informationstillgångar och att utvärdera skydds- och responsstrategier. CSIRT-enheter som utför denna tjänst skulle genomföra eller hjälpa till med riskanalyser avseende informationssäkerhet för nya system och affärsprocesser eller utvärdera hot och attacker mot basgruppens tillgångar och system.

Planering för fortsatt drift och katastrofåterställning
Att döma av tidigare händelser och framtida prognoser om framväxande incident- eller säkerhetstrender kan allt fler incidenter leda till en allvarlig försämring av affärsverksamheten. Därför bör planeringsinsatserna beakta CSIRT-enhetens erfarenhet och rekommendationer för att avgöra hur man bäst kan reagera på sådana incidenter för att garantera att affärsverksamheten kan fortsätta utan avbrott. CSIRT-enheter som tillhandahåller denna tjänst arbetar med planering för fortsatt drift och återställning efter katastrofer för händelser i samband med hot och attacker mot datasäkerhet.

Säkerhetsrådgivning
CSIRT-enheter kan användas för att ge råd och vägledning om bästa säkerhetspraxis som bör genomföras för basgruppens affärsoperationer. En CSIRT-enhet som tillhandahåller denna tjänst förbereder rekommendationer eller identifierar krav för att köpa, installera eller säkra nya system, nätverksutrustning, program eller företagsövergripande affärsprocesser. Tjänsten omfattar att tillhandahålla vägledning och assistans för att utveckla organisationens eller basgruppens säkerhetspolicy. Den kan också omfatta att vittna inför eller ge råd till lagstiftare eller andra statliga organ.

Medvetandebyggande
CSIRT-enheter kan eventuellt identifiera var basgruppens medlemmar behöver mer information och vägledning för att bättre kunna följa accepterade säkerhetsrutiner och organisationens säkerhetspolicy. Genom att öka den allmänna medvetenheten i säkerhetsfrågor bland basgruppens medlemmar förbättras inte bara deras förståelse av säkerhetsfrågor, utan det hjälper dem dessutom att utföra sin dagliga verksamhet på ett säkrare sätt. Detta kan minska förekomsten av framgångsrika attacker och öka chansen för att basgruppens medlemmar ska upptäcka och rapportera attacker, vilket i sin tur minskar återställningstiden och eliminerar eller minskar förlusterna.
CSIRT-enheter som erbjuder denna tjänst försöker hitta möjligheter att öka säkerhetsmedvetenheten genom att ta fram artiklar, postrar, nyhetsbrev, webbplatser eller andra informationsresurser som förklarar bästa säkerhetspraxis och ger råd om vilka försiktighetsåtgärder man bör vidta. Aktiviteterna kan också inkludera att man planerar möten och seminarier för att hålla basgruppens medlemmar uppdaterade om pågående säkerhetsförfaranden och potentiella hot mot organisationens system.

Utbildning

Denna tjänst omfattar att tillhandahålla information åt basgruppens medlemmar om datasäkerhet genom seminarier, workshopar, kurser och handledning. Ämnena kan inkludera riktlinjer för incidentrapportering, lämpliga responsmetoder, verktyg för incidentrespons, metoder för incidentförebyggande och annan information som är nödvändig för att skydda mot, detektera, rapportera och reagera på datasäkerhetsincidenter.

Produktutvärdering eller certifiering

Denna tjänst kan innebära att CSIRT-enheten genomför produktutvärderingar på verktyg, program eller andra tjänster för att garantera produkternas säkerhet och att de överensstämmer med CSIRT-enhetens eller organisationens accepterade säkerhetsrutiner. Verktyg och program som granskas kan vara gratisprodukter eller kommersiella produkter. Denna tjänst kan tillhandahållas som en utvärdering eller genom ett certifieringsprogram, beroende på vilken standard som tillämpas av organisationen eller CSIRT-enheten.

A.3 Exemplen

Fiktivt CSIRT

Steg 0: Att förstå vad ett CSIRT är

Vårt fiktiva CSIRT ska betjäna en medelstor institution med 200 anställda. Institutionen har en egen IT-avdelning och två andra lokalkontor i samma land. IT spelar en avgörande roll för företaget, eftersom det används för internkommunikation, datanät och e-handel dygnet runt, sju dagar i veckan. Institutionen har ett eget nätverk och en redundant anslutning till Internet via två olika tjänsteleverantörer.

- -

Steg 1: Startfasen

I startfasen planeras vår nya CSIRT-enhet som en intern enhet som ska tillhandahålla tjänster åt värdföretaget, den lokala IT-avdelningen och personalen. Den stödjer och samordnar dessutom hanteringen av incidenter som gäller IT-säkerhet mellan de olika lokalkontoren.

- -

Steg 2: Att välja rätt tjänster

I startfasen bestämde vi att vår nya CSIRT-enhet i första hand skulle fokusera på att erbjuda några av kärntjänsterna åt de anställda.

Vi har bestämt att en utvidgning av tjänsteportföljen kan bli aktuell efter pilotfasen och att vissa ”säkerhetsadministrativa tjänster” skulle kunna läggas till. Det beslutet kommer att fattas på grundval av feedback från pilotmedlemmarna och i nära samarbete med avdelningen för kvalitetssäkring.

- -

Steg 3: Att göra en analys av basgruppen och lämpliga kommunikationskanaler

En idékläckningssession med nyckelpersoner från ledningen och basgruppen gav tillräckligt med material för en SWOT-analys. Detta ledde till slutsatsen att det fanns behov av följande centrala tjänster:

- Larm och varningar
- Incidenthantering (analys, åtgärdsstöd och samordning av åtgärder)
- Meddelanden

Man måste tillse att informationen fördelas på ett väl organiserat sätt för att nå en så stor del som möjligt av basgruppen. Därför fattades beslutet att larm, varningar och meddelanden i form av säkerhetsbulletiner ska offentliggöras på en särskild webbplats och distribueras via en sändlista. En CSIRT-enhet underlättar e-post, telefon och fax för att ta emot incidentrapporter. En enhetligt utformad webbplats planeras för nästa steg.

Steg 4: Formulering av uppdraget

Ledningen för vår fiktiva CSIRT-enhet har formulerat följande uppdragsbeskrivning:
”Vårt fiktiva CSIRT tillhandahåller information och hjälper de anställda i värdföretaget att minska riskerna för datasäkerhetsincidenter och att reagera på sådana incidenter när de inträffar.”

Genom uppdragsbeskrivningen gör vår fiktiva CSIRT-enhet klart att den är en intern enhet och att dess kärnverksamhet är att hantera frågor i samband med IT-säkerhet.

- -

Steg 5: Att utarbeta affärsplanen

Finansieringsmodell
Eftersom företaget driver e-handel och även en IT-avdelning dygnet runt, sju dagar i veckan, har man beslutat att tillhandahålla fullständig service under kontorstid och jourtjänst efter kontorstid. Tjänsterna åt basgruppen är gratis, men möjligheterna att erbjuda tjänster åt externa kunder kommer att utvärderas under pilot- och utvärderingsfasen.

Intäktsmodell
Under start- och pilotfasen kommer CSIRT-enheten att finansieras från värdföretaget. Under pilot- och utvärderingsfasen kommer ytterligare finansiering att diskuteras, inklusive möjligheten att sälja tjänster till externa kunder.

Organisationsmodell
Värdorganisationen är ett litet företag, så den inbäddade modellen valdes.
Under kontorstid kommer en personal bestående av tre personer att tillhandahålla kärntjänsterna (utskick av säkerhetsbulletiner och incidenthantering/samordning).

Företagets IT-avdelning har redan anställda med rätt kunskaper. Ett avtal med den avdelningen har tecknats så att vårt nya CSIRT kan begära stöd vid behov. Även deras jourtekniker i andra linjen kan användas.
Det kommer att finnas ett kärnteam bestående av fyra heltidsanställda medlemmar och fem ytterligare medlemmar av CSIRT-enheten. En av dem är också tillgänglig i ett roterande skift.

Personal
CSIRT-enhetens ledare har en bakgrund inom säkerhet och support på nivå 1 och 2 och har arbetat med krishantering inom systemtålighet. De övriga tre medlemmarna är säkerhetsspecialister. De deltidsanställda CSIRT-medlemmarna från IT-avdelningen är specialister på sina respektive delar av företagets infrastruktur.

Steg 5: Att använda kontor och informationssäkerhetspolicy
Kontorets utrustning och placering
Eftersom värdföretaget redan har en tillräckligt god fysisk säkerhet på plats är vårt nya CSIRT väl skyddat i det avseendet. En så kallad ”stridsledningscentral” ställs till förfogande för att underlätta samordningen i ett krisläge. Ett kassaskåp har köpts in för att förvara krypteringsmateriel och känsliga dokument. En separat telefonlinje har upprättats för att underlätta heta linjen under kontorstid, och en mobil jourtelefon finns tillgänglig för perioden efter kontorstid med samma telefonnummer.

Befintlig utrustning och företagets webbplats kan också användas för att meddela CSIRT-relaterad information. En digital sändlista har installerats och förvaltas aktivt, med en särskild del med begränsat tillträde för kommunikationen mellan teamets medlemmar och med andra team. Alla personalens kontaktuppgifter lagras i en databas, och en utskrift förvaras i kassaskåpet.

Reglering
Eftersom vårt CSIRT är inbäddat i ett företag med befintlig policy för informationssäkerhet har motsvarande rutiner för CSIRT-enheten utarbetats med hjälp av företagets rättsexpert.

- -

Steg 7: Att söka samarbete
Genom att använda ENISA:s förteckning kunde vi snabbt hitta och kontakta några CSIRT-enheter i samma land. Ett besök på platsen arrangerades med en av enheterna för den nyanställde teamledaren. Han lärde sig om nationella CSIRT-aktiviteter och deltog i ett möte.
Det mötet var mycket fruktbart för att samla in exempel på arbetsmetoder och få stöd av ett par andra team.

- -

Steg 8: Att genomföra affärsplanen

Vi beslutar att samla in uppgifter från företagets historia. Detta är mycket användbart för att ge en statistisk översikt över läget vad gäller IT-säkerhet. För att hålla statistiken à jour bör insamlingen av data fortsätta när CSIRT-enheten har kommit igång.

Övriga nationella CSIRT-enheter kontaktades och intervjuades om sina affärsscenarier. De gav stöd genom att ställa samman bilder med information om den senaste utvecklingen inom IT-säkerhetsincidenter och om incidenternas kostnader.

I vårt exempel med ett fiktivt CSIRT fanns det inget tvingande behov av att övertyga ledningen om betydelsen av IT-verksamheten, och därför var det inte svårt att få grönt ljus för första steget. Ett affärsscenario och en projektplan utarbetades, inklusive en beräkning över uppstartkostnader och driftkostnader.

- -

Steg 9: Att skapa processflöden och operativa och tekniska rutiner
Vårt fiktiva CSIRT fokuserar på att leverera kärntjänster inom CSIRT:

- Larm och varningar
- Meddelanden
- Incidenthantering

Teamet utvecklade rutiner som fungerar bra och som alla teamets medlemmar lätt kan förstå. Vårt fiktiva CSIRT anställde också en juridisk expert för att hantera frågor om ansvar och policyn för informationssäkerhet. Teamet införde vissa användbara verktyg och hittade användbar information om operativa frågor genom att diskutera med andra CSIRT-enheter.

En fast mall för säkerhetsbulletiner och incidentrapporter togs fram. Teamet använder RTIR för incidenthanteringen.

- -

Steg 10: Utbildning av personalen
Vårt fiktiva CSIRT har beslutat att skicka alla sina tekniker till nästa tillgängliga TRANSITS-kurs. Teamets ledare kommer dessutom att gå en av CERT/CC:s kurser i *att leda ett CSIRT*.

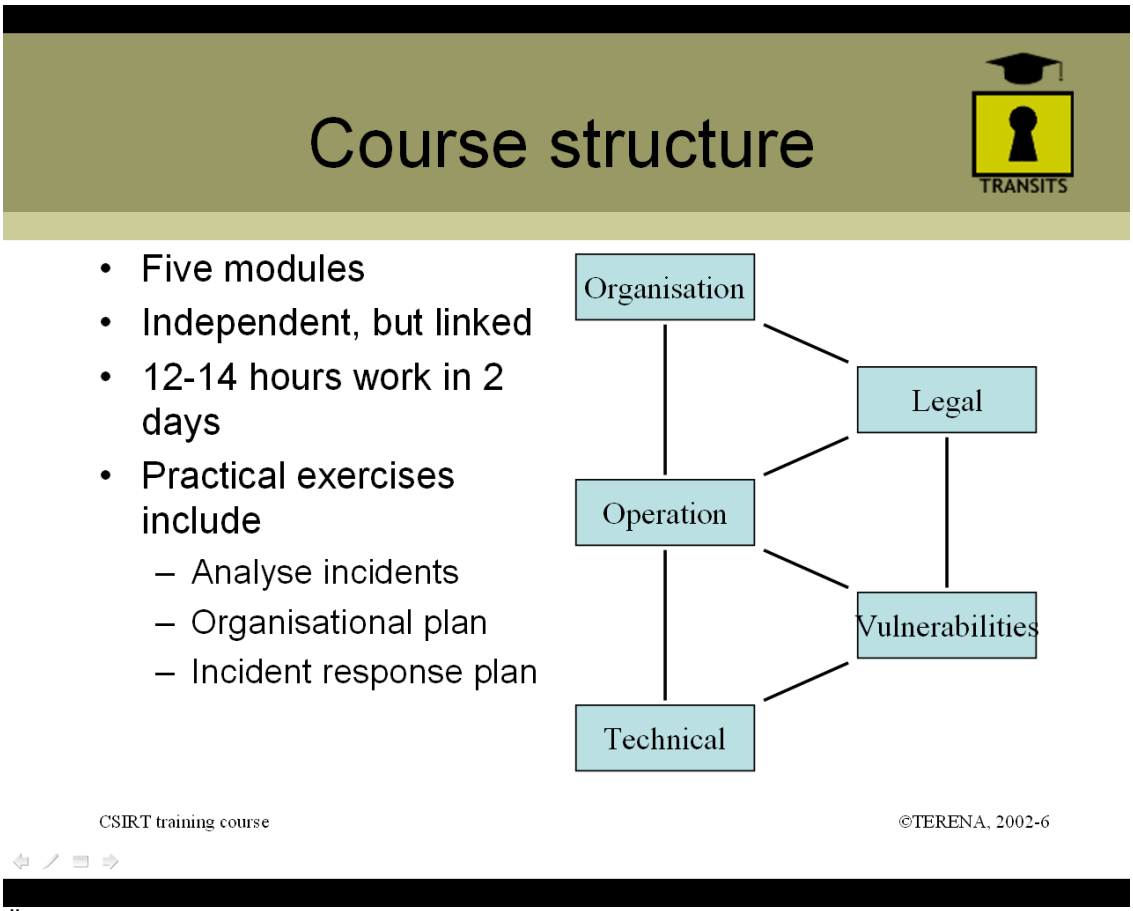
- -

Steg 11: Övning

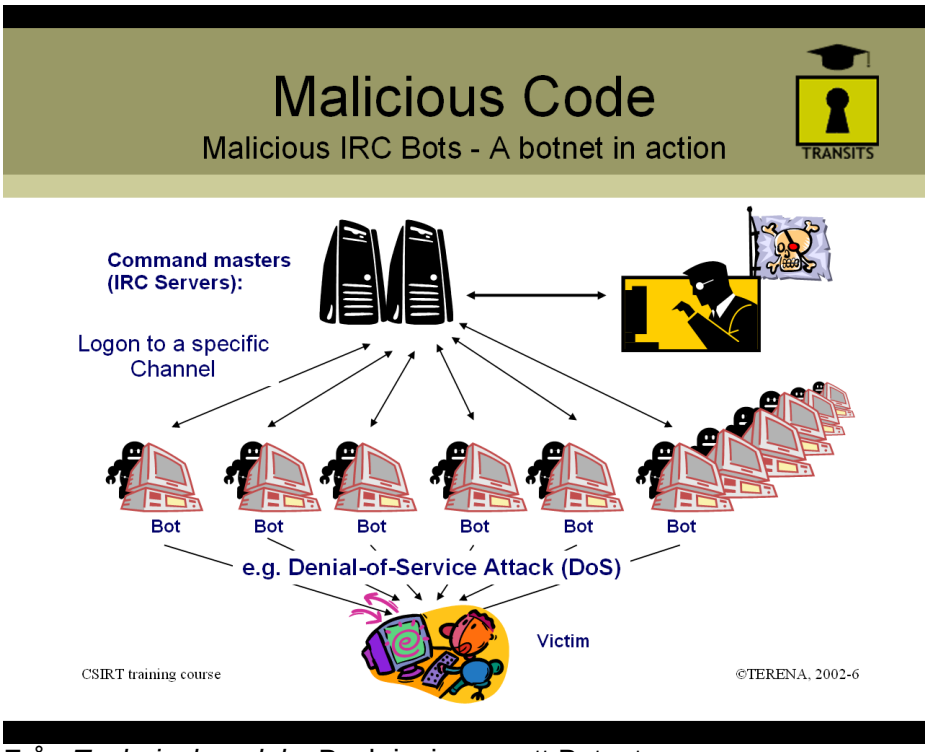
Under de första veckorna använde vårt fiktiva CSIRT flera fiktiva fall (som det fick som exempel från andra CSIRT-enheter) som övning. Dessutom utfärdades ett antal säkerhetsbulletiner som byggde på äkta sårbarhetsinformation som skickats ut av försäljare av hårdvara och programvara och som sedan anpassades efter basgruppens behov.

A.4 Exempel på material från CSIRT-kurser

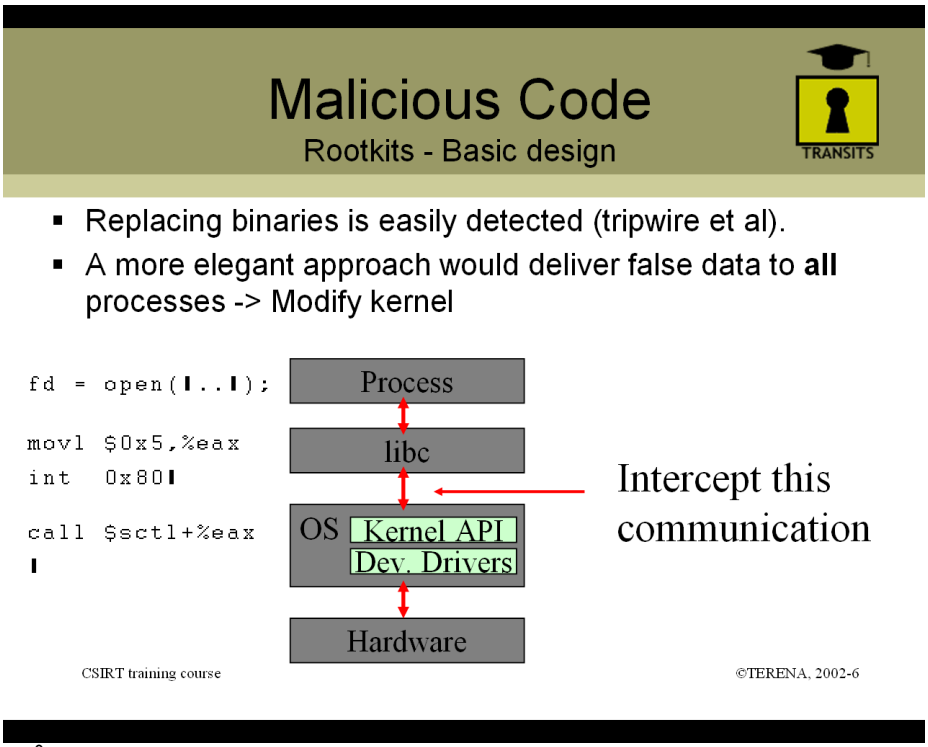
TRANSITS (med vänligt tillstånd från Terena, http://www.terena.nl)



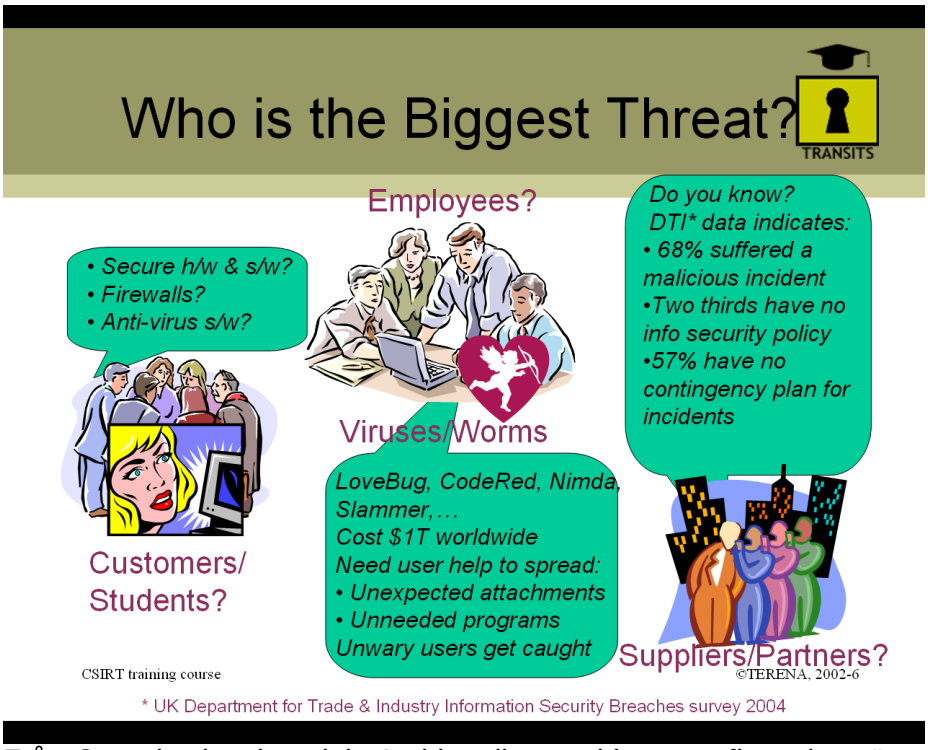
Översikt: Kursens struktur.



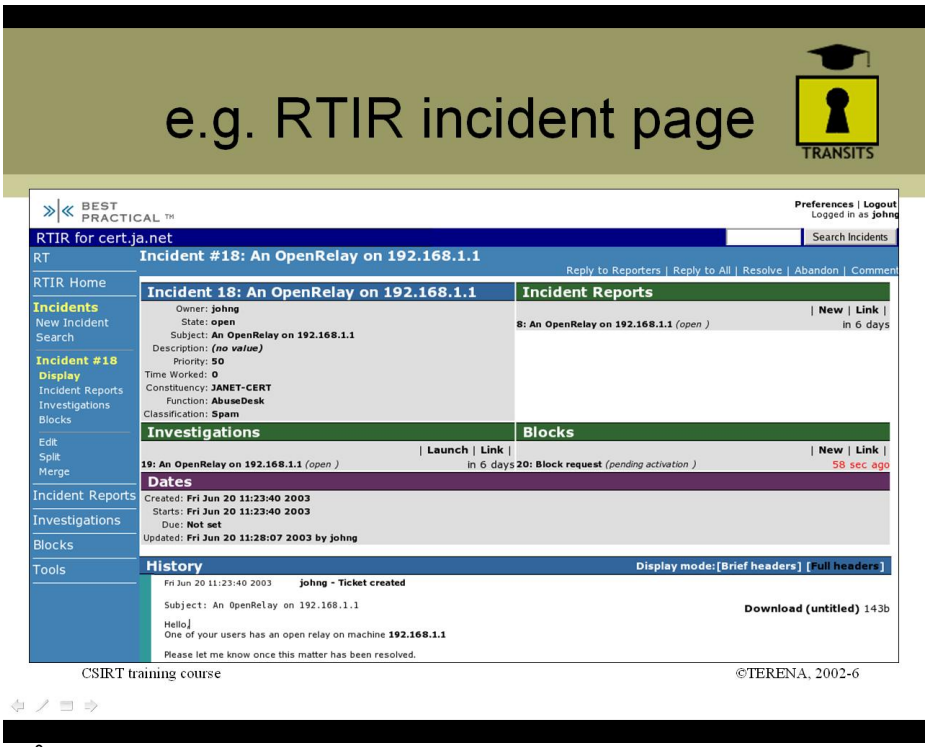
Från *Technical module*: Beskrivning av ett Botnet.



Från *Technical module*: Grunddesignen för ett rotkit.



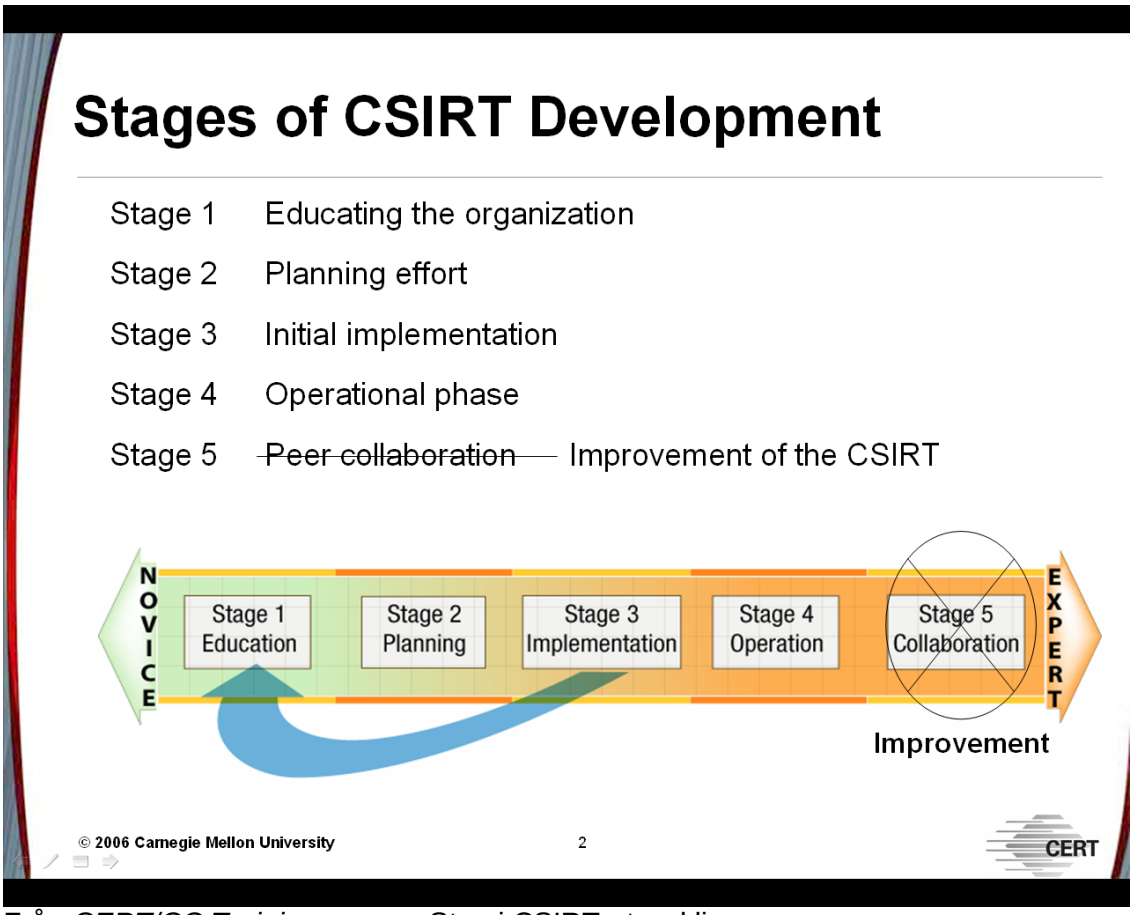
Från *Organisational module*: Insider eller outsider – var finns det största hotet?



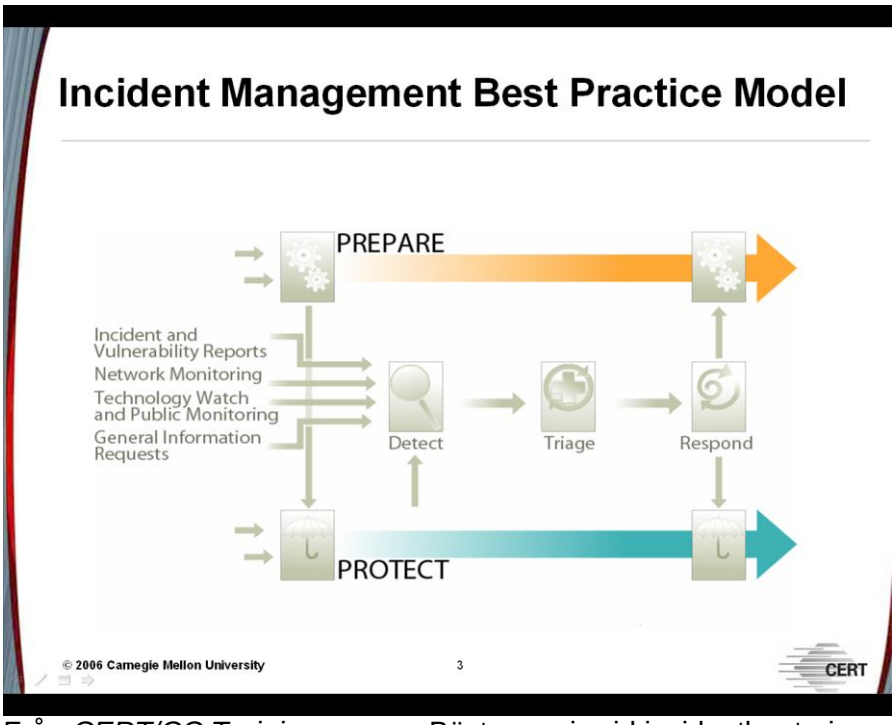
Från *Operational track*: Begäran om incidentrespons (RTIR, Request Tracker for Incident Response).

”Att inrätta en CSIRT-enhet” (med vänligt tillstånd från CERT/CC, http://www.cert.org)

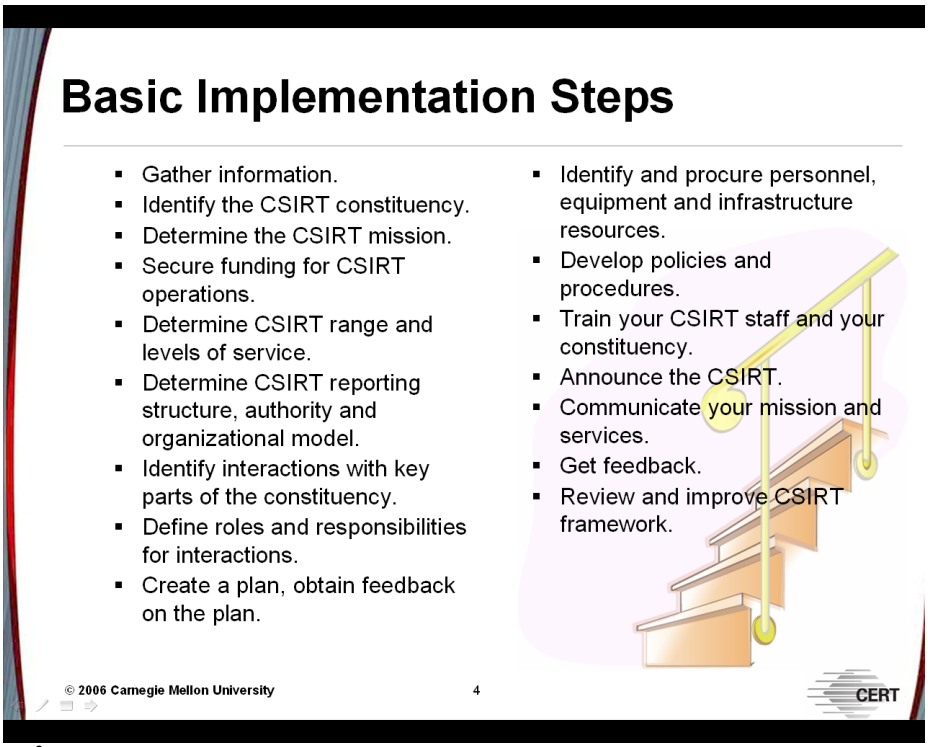
ENISA tackar CERT-programmets team för CSIRT-utveckling för tillståndet att använda innehållet i deras utbildningar.



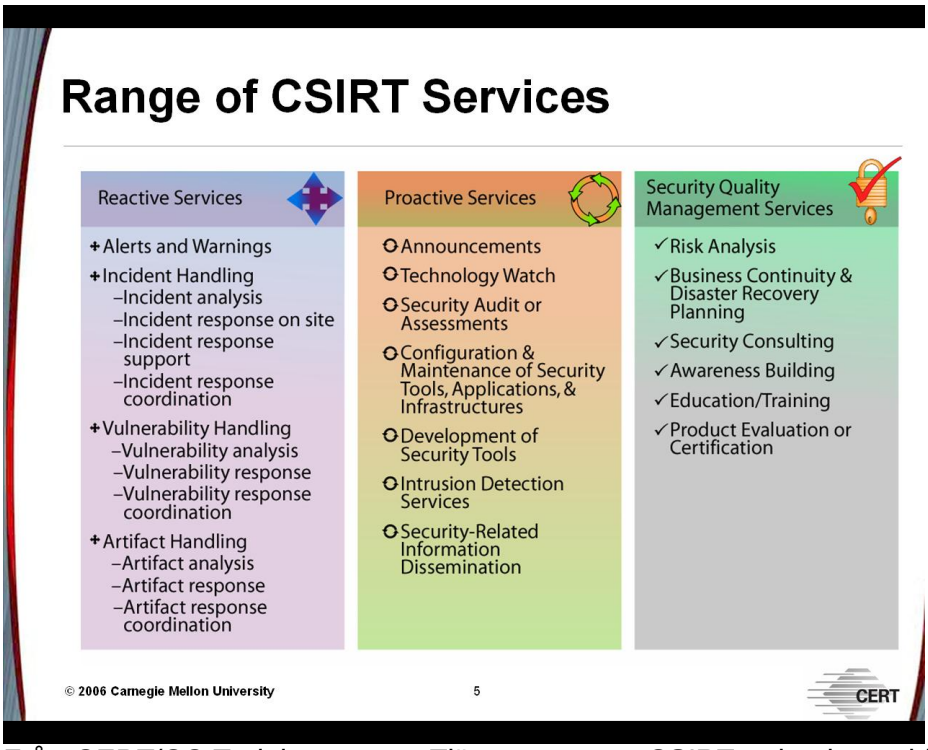
Från *CERT/CC Training course*: Steg i CSIRT-utvecklingen.



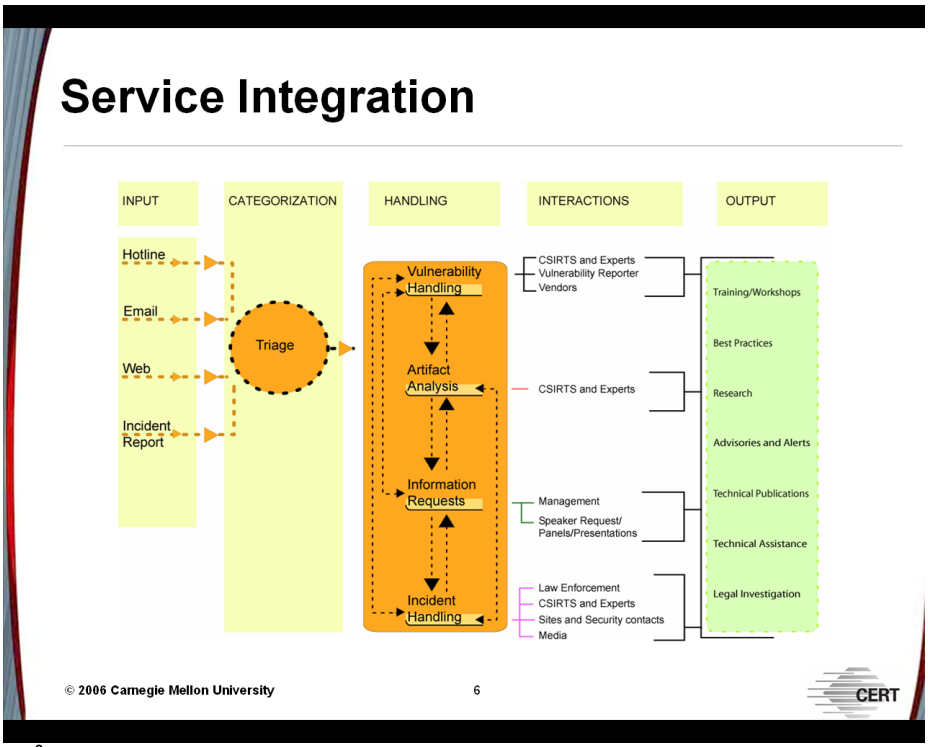
Från *CERT/CC Training course*: Bästa praxis vid incidenthantering.



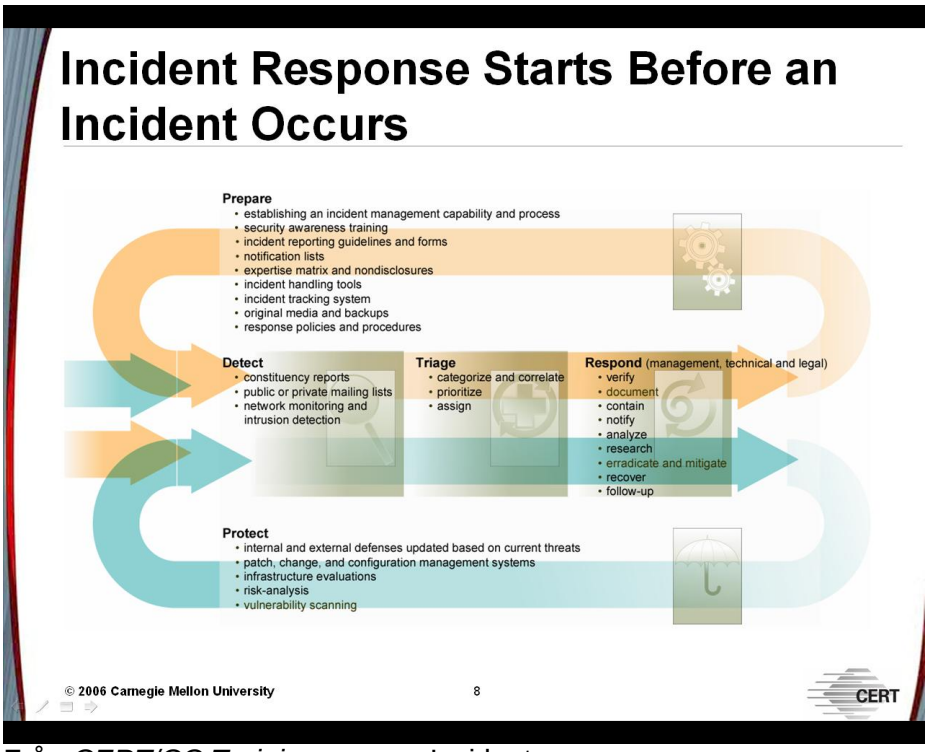
Från *CERT/CC Training course*: Steg som ska följas när en CSIRT-enhet inrättas.



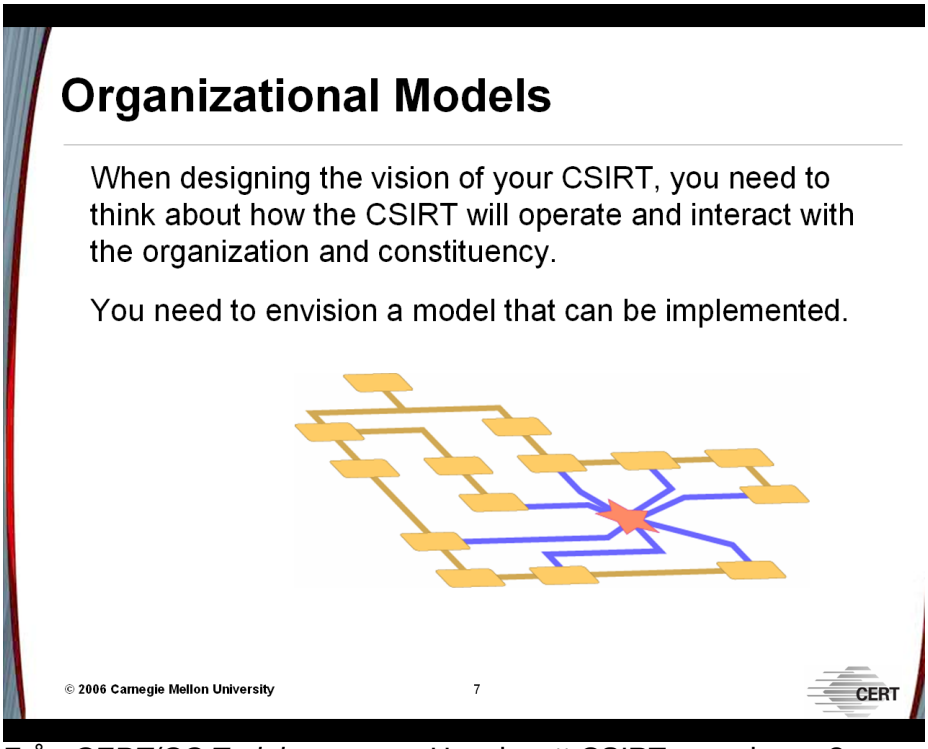
Från *CERT/CC Training course*: Tjänster som en CSIRT-enhet kan erbjuda.



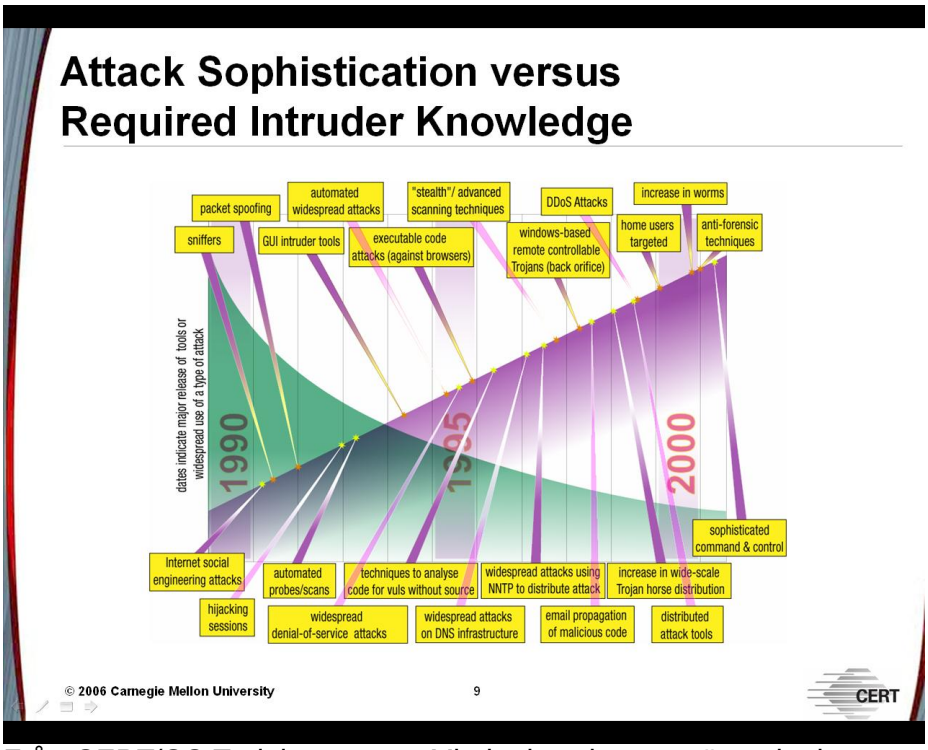
Från *CERT/CC Training course*: Arbetsflödet vid incidenthantering.



Från *CERT/CC Training course*: Incidentrespons.



Från *CERT/CC Training course*: Hur ska ett CSIRT organiseras?



Från *CERT/CC Training course*: Mindre kunskaper, större skador.