

UN APPROCCIO GRADUALE ALLA CREAZIONE DI UN CSIRT

Documento WP2006/5.1(CERT-D1/D2)

Indice

1 Sintesi gestionale 2

2 Avviso legale 2

3 Ringraziamenti 2

4 Introduzione 3

4.1 DESTINATARI 4
4.2 COME USARE IL DOCUMENTO 4
4.3 CONVENZIONI PRESENTI NEL DOCUMENTO 5

5 Strategia generale per pianificare e creare un CSIRT 5

5.1 COS'È UN CSIRT? 5
5.2 SERVIZI POSSIBILI FORNITI DA UN CSIRT 10
5.3 ANALISI DELLA COMUNITÀ DI RIFERIMENTO E DEFINIZIONE DEL MANDATO 12

6 Sviluppare il piano di attività 18

6.1 DEFINIRE IL MODELLO FINANZIARIO 18
6.2 DEFINIRE LA STRUTTURA ORGANIZZATIVA 20
6.3 ASSUMERE PERSONALE IDONEO 24
6.4 UTILIZZO E ATTREZZATURE DELL'UFFICIO 26
6.5 SVILUPPARE UNA POLITICA DI SICUREZZA DELL'INFORMAZIONE 28
6.6 RICERCA DI COLLABORAZIONE TRA ALTRI CSIRT E POSSIBILI INIZIATIVE NAZIONALI 29

7 Promuovere il piano di attività 31

7.1 DESCRIZIONE DEI PIANI DI ATTIVITÀ E LEVE DIREZIONALI 33

8 Esempi di procedure operative e tecniche (flussi di lavoro) 36

8.1 VALUTARE LA BASE D'INSTALLAZIONE DELLA COMUNITÀ DI RIFERIMENTO 37
8.2 EMETTERE SEGNALAZIONI, AVVISI E ANNUNCI 38
8.3 EFFETTUARE LA GESTIONE DEGLI INCIDENTI 45
8.4 UN MODELLO DEI TEMPI DI RISPOSTA 51
8.5 STRUMENTI A DISPOSIZIONE DEI CSIRT 51

9 Formazione CSIRT 54

9.1 TRANSITS 54
9.2 CERT/CC 55

10 Esercizio: produrre un bollettino informativo 56

11 Conclusione 61

12 Descrizione del piano di attuazione del progetto 62

APPENDICE 64

A.1 ULTERIORI LETTURE 64
A.2 SERVIZI CSIRT 65
A.3 ESEMPI 74
A.4 MATERIALE CAMPIONE DAI CORSI CSIRT 78

1 Sintesi gestionale

Il presente documento descrive il processo di creazione di un gruppo per la sicurezza informatica e la risposta agli incidenti (CSIRT, *Computer Security and Incident Response Team*), tenendo conto di tutti gli aspetti, tra cui la gestione generale e dei processi nonché i profili tecnici. Il documento dà attuazione a due dei documenti descritti nel programma di lavoro 2006 dell'ENISA, al capitolo 5.1:

- Il presente documento: *Relazione scritta su un approccio graduale alla creazione di un CERT o di strutture analoghe, esempi compresi.* (**CERT-D1**)
- Il capitolo 12 e dossier esterni: *Estratto della tabella di marcia in forma dettagliata per una facile applicazione pratica della tabella di marcia.* (**CERT-D2**)

2 Avviso legale

Si noti che questa pubblicazione rispecchia le opinioni e le interpretazioni degli autori e redattori, salvo altrimenti indicato. La presente pubblicazione non deve essere considerata un'azione dell'ENISA o degli organi dell'ENISA se non in caso di adozione ai sensi del regolamento (CE) n. 460/2004 che istituisce l'ENISA. Essa non rappresenta necessariamente lo stato dell'arte e potrebbe essere periodicamente aggiornata.

Le fonti terze sono debitamente citate. L'ENISA declina ogni responsabilità in merito ai contenuti delle fonti esterne, compresi i siti web esterni menzionati in questo documento.

La presente pubblicazione è stata prodotta a mero scopo informativo e didattico. Né l'ENISA né chiunque altro che agisca per conto dell'ENISA può essere responsabile dell'uso che potrebbe essere fatto delle informazioni contenute nella presente pubblicazione.

Tutti i diritti riservati. È vietata la riproduzione anche parziale della presente pubblicazione o il suo salvataggio in un sistema di recupero nonché la sua trasmissione in qualsiasi forma o con qualsiasi mezzo, sia esso meccanico o elettronico, compresi la fotocopiatura, la registrazione o altro, senza la previa autorizzazione scritta dell'ENISA o in contrasto con le disposizioni espressamente previste dalla legge o con i termini concordati con le autorità competenti in materia di diritti d'autore. È obbligatoria la riproduzione con citazione della fonte. Le richieste di riproduzione possono essere inviate all'indirizzo della persona di contatto indicato in questa pubblicazione.

© Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), 2006

3 Ringraziamenti

L'ENISA desidera ringraziare tutte le istituzioni e le persone che hanno contribuito a questo documento. Un ringraziamento speciale va a:

- Henk Bronk, che ha prodotto la prima versione del documento nella veste di consulente;
- il CERT/CC e in particolare il gruppo di sviluppo CSIRT, che hanno fornito molto materiale utile e il materiale campione per il corso in allegato;

- GovCERT.NL per aver fornito *CERT-in-a-box*;
- il gruppo TRANSITS, che ha fornito il materiale campione per il corso in allegato;
- i colleghi della sezione Politiche di sicurezza presso il Dipartimento tecnico, che hanno fornito il capitolo 6.6;
- le innumerevoli persone che hanno rivisto questo documento.

4 Introduzione

Le reti di comunicazione e i sistemi informativi sono diventati un fattore essenziale nello sviluppo economico e sociale. L'informatica e le reti stanno man mano divenendo utenze al pari dell'erogazione di acqua o elettricità.

La sicurezza delle reti di comunicazione e dei sistemi informativi e, in special modo, la loro accessibilità sono quindi sempre più al centro dell'interesse della società. Ciò alla luce del rischio di problemi ai sistemi informativi chiave, che si annida nella complessità dei sistemi, nelle probabilità di incidente, errore e attacco alle infrastrutture fisiche che offrono servizi essenziali per il benessere dei cittadini dell'Unione europea.

Il 10 marzo 2004 è stata istituita un'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)[1] con lo scopo di assicurare un alto ed efficace livello di sicurezza delle reti e dell'informazione nella Comunità come pure di sviluppare una cultura della sicurezza delle reti e dell'informazione rivolta ai cittadini, ai consumatori, alle imprese e alle organizzazioni pubbliche nell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno.

Da alcuni anni, ormai, taluni organismi preposti alla sicurezza in Europa come CERT/CSIRT, gruppo antiabuso e WARP collaborano per rendere Internet più sicuro. L'ENISA intende sostenere i loro sforzi fornendo informazioni sulle misure da adottare per garantire un livello adeguato di qualità dei servizi. L'ENISA intende inoltre migliorare la sua capacità di consulenza agli Stati membri dell'UE e agli organismi comunitari in merito a questioni relative alla copertura di gruppi specifici di utenti di IT (tecnologia dell'informazione) con servizi appropriati di sicurezza. Pertanto, partendo dai risultati del gruppo di lavoro ad hoc CERT per la cooperazione e il supporto, istituito nel 2005, questo nuovo gruppo di lavoro si occuperà di questioni inerenti alla fornitura di servizi di sicurezza adeguati ("servizi CERT") a (categorie o gruppi di) utenti specifici.

L'ENISA sostiene la creazione di nuovi CSIRT con la pubblicazione della presente relazione "*Un approccio graduale alla creazione di un CSIRT con una lista di controllo supplementare*", che vi aiuterà a formare uno CSIRT.

[1] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione. Un'"agenzia della Comunità europea" è un organismo creato dall'Unione europea per svolgere un compito tecnico, scientifico o gestionale estremamente specifico nell'ambito della "dimensione comunitaria" ("primo pilastro") dell'Unione europea.

4.1 Destinatari

I destinatari principali di questa relazione sono le istituzioni governative e non che decidono di costituire un CSIRT al fine di proteggere la propria infrastruttura informatica o quella delle loro parti interessate.

4.2 Come usare il documento

Questo documento fornirà informazioni su cos'è un CSIRT, quali servizi è in grado di offrire e qual è il suo iter di avvio. Il lettore otterrà così una panoramica pragmatica e soddisfacente dell'approccio, della struttura e dei contenuti su come creare un CSIRT.

Capitolo 4 *"Introduzione"*
Introduzione alla presente relazione

Capitolo 5 *"Strategia generale per pianificare e creare un CSIRT"*
Nella prima sezione si trova una descrizione di cos'è un CSIRT. Essa fornisce inoltre informazioni sui diversi ambienti in cui i CSIRT possono lavorare e su quali servizi sono in grado di offrire.

Capitolo 6 *"Sviluppare il piano di attività"*
Questo capitolo descrive l'approccio al processo di costituzione in termini di gestione aziendale.

Capitolo 7 *"Promuovere il piano di attività"*
Questo capitolo si occupa degli argomenti commerciali e delle questioni di finanziamento.

Capitolo 8 *"Esempi di procedure operative e tecniche"*
Questo capitolo descrive la procedura per ottenere informazioni e tradurle in un bollettino sulla sicurezza. Esso fornisce anche una descrizione di un flusso di lavoro per la gestione degli incidenti.

Capitolo 9 *"Formazione CSIRT"*
Questo capitolo presenta una sintesi della formazione CSIRT disponibile. A titolo illustrativo, l'allegato contiene del materiale campione per il corso.

Capitolo 10 *"Esercizio: produrre un bollettino informativo"*
Questo capitolo contiene un esercizio per imparare a svolgere uno dei servizi base (o essenziali) di un CSIRT: la produzione di un bollettino informativo (o *advisory*) sulla sicurezza.

Capitolo 12 *"Descrizione del piano di attuazione del progetto"*
Questo capitolo si concentra sul piano supplementare di attuazione del progetto (lista di controllo) fornito con questa guida. Tale piano intende essere uno strumento di facile utilizzo per l'attuazione della guida.

4.3 Convenzioni presenti nel documento

Per fornire un orientamento al lettore, ogni capitolo inizia con una sintesi delle fasi compiute fino a quel momento nel processo di creazione di un CSIRT. Tali sintesi sono riportate in caselle come la seguente:

Prima fase conclusa

Ogni capitolo si chiuderà con un esempio pratico dei passaggi discussi. In questo documento il "CSIRT simulato" sarà un piccolo CSIRT indipendente per una società o istituzione di medie dimensioni. Nell'appendice si può trovare un riassunto.

CSIRT simulato

5 Strategia generale per pianificare e creare un CSIRT

Per iniziare brillantemente il processo di creazione di un CSIRT, è importante farsi una chiara idea dei servizi che il gruppo può offrire ai suoi clienti (noti nel "mondo dei CSIRT" come "constituents"). È quindi necessario comprendere quali sono le esigenze degli utenti di riferimento per fornire i servizi appropriati con l'adeguata tempestività e qualità.

5.1 Cos'è un CSIRT?

CSIRT significa Computer Security Incident Response Team (gruppo di gestione degli incidenti di sicurezza informatica). Il termine CSIRT viene usato prevalentemente in Europa per il termine protetto CERT, che è registrato negli Stati Uniti dal *CERT Coordination Center* (CERT/CC).
Esistono varie abbreviazioni usate per lo stesso genere di gruppi:

- CERT o 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*)

La prima grande epidemia di worm (categoria particolare di "malware" in grado di autoreplicarsi) nell'infrastruttura IT globale si è verificata verso la fine degli anni Ottanta. Il worm si chiamava Morris[2] e si è diffuso con grande rapidità, infettando gravemente un numero elevato di sistemi IT in tutto il mondo.

Questo incidente è servito da scossone: all'improvviso ci si è resi conto del grande bisogno di cooperazione e coordinamento tra gli amministratori di sistema e i responsabili dell'IT per affrontare casi come questo. Poiché il tempo era un fattore critico, occorreva stabilire un approccio più organizzato e strutturale alla gestione degli incidenti di sicurezza informatica. Qualche giorno dopo l'"incidente Morris", la *Defence*

[2] Maggiori informazioni sul worm Morris http://en.wikipedia.org/wiki/Morris_worm

Advanced Research Projects Agency (DARPA) ha quindi creato il primo CSIRT: il *CERT Coordination Center* (CERT/CC[3]), situato presso la Carnegie Mellon University a Pittsburgh (Pennsylvania).

Questo modello è stato ben presto adottato in Europa e nel 1992 la rete di ricerca olandese SURFnet ha lanciato il primo CSIRT europeo, con il nome di SURFnet-CERT[4]. Ad esso si sono poi aggiunti molti gruppi e, attualmente, l'*Inventario delle attività CERT in Europa*[5] dell'ENISA elenca più di 100 gruppi conosciuti dislocati in tutta Europa.

Con il passare degli anni i CERT hanno esteso le loro capacità da semplice forza di reazione a fornitore di servizi di sicurezza completi, compresi servizi preventivi come allarmi, bollettini informativi sulla sicurezza, servizi di formazione e gestione della sicurezza. Il termine "CERT" è apparso presto insufficiente. Alla fine degli anni Novanta è stato quindi introdotto il nuovo termine "CSIRT". Al momento i due termini (CERT e CSIRT) sono usati come sinonimi, dei quali CSIRT è il termine più preciso.

5.1.1 La comunità di riferimento (*constituency*)

D'ora innanzi il ben noto (nelle comunità CSIRT) termine "comunità di riferimento" (o *constituency*) sarà usato per fare riferimento all'insieme di clienti di un CSIRT. Un singolo cliente sarà definito "utente di riferimento" (o *constituent*), mentre un gruppo sarà identificato come "utenti di riferimento" (o *constituents*).

5.1.2 Definizione di un CSIRT

Un CSIRT è un gruppo di esperti in sicurezza IT, la cui attività principale consiste nel reagire a incidenti di sicurezza informatica. Esso fornisce i servizi necessari per affrontare tali incidenti e aiutare i relativi utenti di riferimento a riprendersi dalle violazioni.

Al fine di attenuare i rischi e ridurre al minimo il numero di interventi richiesti, la maggior parte dei CSIRT fornisce anche servizi preventivi e didattici per la propria comunità di riferimento. Essi emettono bollettini informativi sulle vulnerabilità presenti nei software e hardware in uso e informano gli utenti in merito agli exploit (attacchi finalizzati a produrre accesso a un sistema o incrementi di privilegio) e ai virus che approfittano di queste debolezze. Gli utenti di riferimento possono quindi porvi rapidamente rimedio e aggiornare i loro sistemi. Cfr. il capitolo *5.2 Servizi possibili* per un elenco completo dei servizi disponibili. .

5.1.3 I vantaggi di avere un CSIRT

Avere un gruppo di sicurezza IT dedicato aiuta un'organizzazione ad attenuare e prevenire gli incidenti gravi nonché a proteggere i suoi beni di valore.

Altri possibili vantaggi sono:

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

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

[5] Inventario ENISA http://www.enisa.europa.eu/cert_inventory/

- Avere un coordinamento centralizzato per le questioni di sicurezza IT all'interno dell'organizzazione (punto di contatto, PoC).
- Gestione e risposta centralizzata e specializzata agli incidenti IT.
- Avere a portata di mano la competenza per sostenere e aiutare gli utenti a riprendersi rapidamente dagli incidenti di sicurezza.
- Trattare gli aspetti giuridici e conservare la documentazione nel caso di un'azione legale.
- Tenersi al corrente degli sviluppi nel campo della sicurezza.
- Stimolare la cooperazione all'interno della comunità di riferimento in merito alla sicurezza IT (sensibilizzazione).

CSIRT simulato (fase 0)
Capire cos'è un CSIRT: Il CSIRT campione dovrà servire un'istituzione media, composta da 200 dipendenti. L'istituzione ha un proprio dipartimento IT e altre due filiali nello stesso paese. L'IT svolge un ruolo fondamentale per la società, in quanto viene usata per la comunicazione interna, la rete di dati e il commercio elettronico sempre disponibile. L'istituzione ha una propria rete e dispone di una connessione ridondante a Internet tramite due diversi ISP.

5.1.4 Descrizione dei diversi tipi di ambienti CSIRT

Prima fase compiuta 1. Capire cos'è un CSIRT e quali vantaggi può offrire. >> La prossima fase consisterà nel rispondere alla domanda: "A quale settore saranno forniti i servizi CSIRT?"

Quando si avvia un CSIRT (come del resto qualunque altra attività), è molto importante farsi il prima possibile una chiara idea di chi siano gli utenti di riferimento e del tipo di ambiente per il quale saranno sviluppati i servizi del CSIRT. Al momento distinguiamo i seguenti "settori":

- CSIRT settore accademico
- CSIRT commerciale
- CSIRT settore CIP/CIIP
- CSIRT settore governativo
- CSIRT interno
- CSIRT settore militare
- CSIRT nazionale
- CSIRT settore piccole e medie imprese (PMI)
- CSIRT venditori

CSIRT settore accademico
Finalità
Un CSIRT del settore accademico fornisce servizi CSIRT a istituti accademici e d'istruzione, come università o enti di ricerca, e ai loro ambienti Internet nei campus.

Utenti di riferimento
Gli utenti di riferimento tipici di questo genere di CSIRT sono il personale e gli studenti delle università.

CSIRT commerciale
Finalità
Un CSIRT commerciale fornisce servizi CSIRT di natura commerciale ai propri utenti di riferimento. Nel caso di un ISP, il CSIRT fornisce prevalentemente servizi contro gli abusi agli utenti finali (dial-in, ADSL) e servizi CSIRT ai clienti professionali.

Utenti di riferimento
CSIRT commerciali in genere forniscono i loro servizi agli utenti di riferimento dietro corrispettivo.

CSIRT settore CIP/CIIP
Finalità
I CSIRT in questo settore si concentrano prevalentemente sulla protezione delle informazioni critiche (CIP) e/o sulla protezione delle informazioni e infrastrutture critiche (CIIP). Nella maggior parte dei casi, questo CSIRT specializzato collabora strettamente con un dipartimento CIIP governativo. Esso si occupa di tutti i settori IT critici nel paese e protegge i cittadini di quella nazione.

Utenti di riferimento
Governo, attività IT critiche, cittadini

CSIRT settore governativo
Finalità
Un CSIRT governativo fornisce servizi ad agenzie governative e, in alcuni paesi, ai cittadini.

Utenti di riferimento
Governo e relative agenzie governative; in alcuni paesi si forniscono anche servizi di allarme ai cittadini (per esempio in Belgio, Ungheria, Paesi Bassi, Regno Unito o Germania).

CSIRT interno
Finalità
Un CSIRT interno fornisce servizi soltanto all'organizzazione che lo ospita. Questo descrive più il funzionamento che un settore. Per esempio, molte organizzazioni di telecomunicazione e banche hanno propri CSIRT interni. In genere non hanno un sito web per il pubblico.

Utenti di riferimento
Personale interno e dipartimento IT dell'organizzazione ospitante

CSIRT settore militare
Finalità
Un CSIRT in questo settore fornisce servizi alle organizzazioni militari responsabili dell'infrastruttura IT necessaria per fini di difesa.

Utenti di riferimento
Personale degli enti militari o di enti strettamente correlati, per esempio il Dipartimento della difesa

CSIRT nazionale
Finalità
Un CSIRT attivo a livello nazionale, considerato un punto di contatto per la sicurezza di un paese. In alcuni casi lo CISRT governativo agisce anche da punto di contatto nazionale (come UNIRAS nel Regno Unito).

Utenti di riferimento
Questo tipo di CSIRT non ha in genere utenti di riferimento diretti, in quanto CSIRT nazionale svolge soltanto un ruolo da intermediario per tutto il paese

CSIRT settore piccole e medie imprese (PMI)
Finalità
Un CSIRT auto-organizzato che fornisce servizi al proprio settore di attività o a un gruppo analogo di utenti.

Utenti di riferimento
Gli utenti di riferimento di questi CSIRT possono essere le PMI e il loro personale, oppure particolari gruppi di interesse come l'"Associazione delle città e dei comuni" di un paese.

CSIRT venditori
Finalità
Un CSIRT dei venditori si concentra sul sostegno ai prodotti specifici di un venditore. Il suo scopo consiste solitamente nello sviluppare e fornire soluzioni al fine di rimuovere le vulnerabilità e attenuare i potenziali effetti negativi dei punti deboli.

Utenti di riferimento
Proprietari dei prodotti

Come descritto nel paragrafo sui CSIRT nazionali, è possibile che un gruppo serva più di un settore. Ciò si ripercuote per esempio sull'analisi della comunità di riferimento e delle sue esigenze.

CSIRT simulato (fase 1)
Fase iniziale Nella fase iniziale il nuovo CSIRT viene concepito come CSIRT interno che fornisce i suoi servizi alla società ospitante, al dipartimento IT locale e al personale. Inoltre, esso sostiene e coordina la gestione degli incidenti relativi alla sicurezza IT tra diverse filiali.

5.2 Servizi possibili forniti da un CSIRT

Prime due fasi compiute

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?

>> La prossima fase consiste nel rispondere alla domanda: *quali servizi fornire agli utenti di riferimento*.

I servizi che un CSIRT può offrire sono molti, ma finora nessun CSIRT esistente li fornisce tutti. La selezione dell'insieme appropriato di servizi è quindi una decisione di cruciale importanza. Di seguito si riporta una breve panoramica di tutti i servizi CSIRT

conosciuti, come specificato nel "*Handbook for CSIRTs*" (Manuale per CSIRT) pubblicato dal CERT/CC[6].

Servizi reattivi	**Servizi proattivi**	**Gestione degli artefatti**
• **Allarmi e avvisi** • **Gestione degli incidenti** • **Analisi degli incidenti** • **Sostegno della risposta agli incidenti** • **Coordinamento della risposta agli incidenti** • Risposta agli incidenti in loco • Gestione delle vulnerabilità • Analisi delle vulnerabilità • Risposta alle vulnerabilità • Coordinamento della risposta alle vulnerabilità	• **Annunci** • Controllo tecnologico • Revisioni e valutazioni della sicurezza • Configurazione e mantenimento della sicurezza • Sviluppo di strumenti di sicurezza • Servizi di rilevamento intrusioni • Divulgazione di informazioni relative alla sicurezza	• *Analisi degli artefatti* • *Risposta agli artefatti* • *Coordinamento della risposta agli artefatti* **_Gestione della qualità della sicurezza_** • *Analisi dei rischi* • *Continuità operativa e ripristino in caso di disastro* • *Consulenza sulla sicurezza* • *Sensibilizzazione* • *Istruzione/formazione* • *Valutazione o certificazione dei prodotti*

Fig. 1 Elenco dei servizi CSIRT da CERT/CC[7]

I servizi chiave (scritti in grassetto): si opera una distinzione tra i servizi reattivi e quelli proattivi. I servizi proattivi servono a prevenire gli incidenti attraverso la sensibilizzazione e la formazione, mentre i servizi reattivi servono a gestire gli incidenti e ad attenuare il danno conseguente.

La **gestione degli artefatti** comprende l'analisi di qualunque file od oggetto rinvenuto in un sistema che possa essere coinvolto in azioni dolose, come residui di virus, worm, script, cavalli di Troia ecc. Comprende inoltre la gestione e distribuzione delle informazioni ottenute ai venditori e ad altre parti interessate al fine di prevenire l'ulteriore diffusione di malware (vale a dire qualsiasi software creato con il solo scopo di causare danni al computer su cui viene eseguito) e attenuare i rischi.

I **servizi di gestione della qualità e sicurezza** sono servizi con obiettivi a più lungo termine e comprendono consulenza e misure didattiche.

Cfr. appendice per una spiegazione dettagliata dei servizi CSIRT.

Scegliere i servizi giusti per i propri utenti di riferimento è un passo importante, di cui si parlerà ulteriormente nel capitolo *6.1 Definire il modello finanziario*.

La maggior parte dei CSIRT inizia col distribuire "allarmi e avvisi", fare "annunci" e fornire la "gestione degli incidenti" ai propri utenti di riferimento. Questi servizi chiave in

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

[7] Elenco dei servizi CSIRT da CERT/CC: http://www.cert.org/csirts/services.html

genere creano un buon profilo e valore di attenzione nella comunità di riferimento e sono prevalentemente considerati come il vero "valore aggiunto".

È buona prassi iniziare con un piccolo gruppo "pilota" di utenti di riferimento, offrire i servizi chiave per un periodo di prova e quindi sollecitare un riscontro.
Gli utenti pilota interessati forniscono un riscontro costruttivo e aiutano a sviluppare servizi su misura.

CSIRT simulato (fase 2)
Scegliere i giusti servizi Nella fase iniziale viene deciso che il nuovo CSIRT si concentrerà prevalentemente sulla fornitura di alcuni dei servizi chiave per i dipendenti. Si decide che dopo una fase pilota si potrà pensare all'espansione del portafoglio di servizi, aggiungendo alcuni "servizi di gestione della sicurezza". Tale decisione sarà presa sulla base del riscontro dal gruppo pilota di utenti di riferimento e in stretta collaborazione con il dipartimento di garanzia della qualità.

5.3 Analisi della comunità di riferimento *e definizione del mandato*

Prime tre fasi compiute

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?
3. Quali tipi di servizi può offrire un CSIRT alla sua comunità di riferimento.

>> La prossima fase consiste nel rispondere alla domanda: *quale tipo di approccio si deve scegliere per avviare un CSIRT?*

La prossima fase consiste in uno sguardo più approfondito alla comunità di riferimento, al fine principale di scegliere i canali di comunicazione corretti:

- Definire l'approccio comunicativo agli utenti di riferimento
- Definire la dichiarazione del compito
- Elaborare un piano di attuazione/del progetto realistico
- Definire i servizi del CSIRT
- Definire la struttura organizzativa
- Definire la politica per la sicurezza dell'informazione
- Assumere personale idoneo
- Utilizzare il proprio ufficio CSIRT
- Cercare la collaborazione tra altri CSIRT e possibili iniziative nazionali

Questi passi saranno descritti in maniera più dettagliata nei paragrafi seguenti e possono essere utilizzati come spunto per il piano di attività e di attuazione del progetto.

5.3.1 Approccio comunicativo alla comunità di riferimento

Come sopra illustrato, è molto importante conoscere le esigenze della comunità di riferimento e la propria strategia di comunicazione, compresi i canali comunicativi più appropriati per la trasmissione di informazioni.

La teoria gestionale conosce diversi approcci possibili a questo problema dell'analisi di un gruppo di destinatari. Nel presente documento ne descriveremo due: l'analisi SWOT e PEST.

Analisi SWOT
Un'analisi SWOT è uno strumento di pianificazione strategica usato per valutare i punti di forza (***S**trengths*) e quelli di debolezza (***W**eakenesses*), le opportunità (***O**pportunities*) e le minacce (***T**hreats*) insiti in un progetto o iniziativa imprenditoriale o in qualunque altra situazione che richiede una decisione. La tecnica è attribuita ad Albert Humphrey, che ha guidato un progetto di ricerca presso la Stanford University negli anni Sessanta e Settanta, utilizzando i dati delle società dell'indice Fortune 500.[8]

Punti di forza	**Punti di debolezza**
Opportunità	**Minacce**

Fig. 2 Analisi SWOT

[8] Analisi SWOT in Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Analisi PEST

L'analisi PEST è un altro strumento importante e ampiamente utilizzato per analizzare la comunità di riferimento al fine di comprendere le circostanze politiche, economiche, socio-culturali e tecnologiche dell'ambiente in cui sta operando un CSIRT. Essa aiuta a stabilire se la pianificazione è ancora in linea con l'ambiente e se può aiutare a evitare di intraprendere azioni sulla base di ipotesi sbagliate.

Circostanze politiche	**Circostanze economiche**
• Questioni ecologiche/ambientali • Attuale legislazione del mercato nazionale • Legislazione futura • Normativa europea/internazionale • Organi e processi regolamentari • Politiche governative • Durata in carica e cambio di governo • Politiche commerciali • Finanziamenti, sovvenzioni e iniziative • Gruppi di pressione/lobby sul mercato nazionale • Gruppi di pressione internazionali	• Situazione dell'economia nazionale • Tendenze dell'economia nazionale • Economie e tendenze internazionali • Questioni fiscali generali • Tassazione specifica per prodotti/servizi • Stagionalità/questioni climatiche • Cicli di mercato e congiunturali • Fattori specifici di settore • Procedure di entrata sul mercato e tendenze di distribuzione • Motori dei consumatori/utenti finali • Tassi d'interesse e di cambio
Circostanze sociali	**Circostanze tecnologiche**
• Tendenze degli stili di vita • Demografia • Atteggiamenti e opinioni dei consumatori • Visione dei media • Modifiche di legge che influiscono sui fattori sociali • Immagine dei marchi, società, tecnologia • Modelli di acquisto dei consumatori • Modelli di ruolo e moda • Eventi e influenze importanti • Accesso agli acquisti e tendenze • Fattori etnici/religiosi • Pubblicità	• Sviluppo di tecnologie competitive • Finanziamento della ricerca • Tecnologie associate/dipendenti • Tecnologia/soluzioni sostitutive • Maturità della tecnologia • Maturità e capacità di produzione • Informazione e comunicazione • Tecnologia/meccanismi di acquisto dei consumatori • Legislazione in materia di tecnologia • Potenziale d'innovazione • Accesso alla tecnologia, licenze, brevetti • Questioni di proprietà intellettuale

Fig. 3 Modello di analisi PEST

In Wikipedia si trova una descrizione dettagliata dell'analisi PEST[9].

Entrambi gli strumenti forniscono una panoramica completa e strutturata delle esigenze degli utenti di riferimento. I risultati andranno a integrare la proposta di attività, aiutando così a ottenere i finanziamenti per la creazione del CSIRT.

Canali di comunicazione

Un tema importante da includere nell'analisi sono i possibili metodi di comunicazione e distribuzione dell'informazione ("come comunicare con la comunità di riferimento?").

Ove possibile, è bene considerare l'opportunità di effettuare visite personali regolari agli utenti di riferimento. È un fatto provato che gli incontri faccia a faccia facilitano la

[9] Analisi PEST in Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

cooperazione. Se entrambe le parti sono disposte a collaborare, questi incontri consentono di instaurare un rapporto più aperto.

Solitamente i CSIRT utilizzano diversi canali di comunicazione, tra cui quelli elencati di seguito si sono rivelati efficaci nella pratica e meritano una menzione a parte:

- Sito web pubblico
- Area riservata ai membri nel sito web
- Moduli web per la segnalazione di incidenti
- Mailing list
- Posta elettronica personalizzata
- Telefono / fax
- SMS
- Lettere cartacee tradizionali
- Rapporti mensili o annuali

Oltre a usare messaggi elettronici, moduli web, telefono o fax per agevolare la gestione degli incidenti (ricevere rapporti sugli incidenti dalla comunità di riferimento, coordinarsi con altri gruppi o fornire riscontro e sostegno alla vittima), la maggior parte dei CSIRT pubblica i propri bollettini sulla sicurezza su un sito web accessibile al pubblico e attraverso una mailing list.

! Ove possibile, le informazioni devono essere distribuite in maniera sicura. Per esempio i messaggi di posta elettronica possono essere firmati digitalmente con PGP, mentre i dati riservati sugli incidenti devono essere sempre inviati in forma cifrata.

Per ulteriori informazioni cfr. il capitolo *8.5 Strumenti disponibili dei CSIRT*. Cfr. inoltre capitolo *2.3* di *RFC2350*[10].

CSIRT simulato (fase 3a)

Svolgere un'analisi della comunità di riferimento e dei canali di comunicazione appropriati

Una sessione di brainstorming con alcune figure chiave della direzione e della comunità di riferimento ha offerto spunti sufficienti per un'analisi SWOT. Questa ha portato alla conclusione che servono i servizi chiave:

- Allarmi e avvisi
- Gestione degli incidenti (analisi, sostegno della risposta e coordinamento della risposta)
- Annunci

Bisogna garantire che l'informazione sia distribuita in maniera ben organizzata al fine di raggiungere la più ampia parte possibile della comunità di riferimento. Si prende quindi la decisione di pubblicare allarmi, avvisi e annunci sotto forma di bollettini sulla sicurezza su un sito web dedicato e di distribuirli attraverso una mailing list. Il CSIRT favorisce l'uso di posta elettronica, telefono e fax per ricevere i rapporti sugli incidenti. Un modulo web unificato viene programmato per la fase successiva.

Cfr. la pagina seguente per un'analisi SWOT campione.

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

Punti di forza • Sono presenti conoscenze all'interno della società • Apprezzano il piano e sono desiderosi di collaborare • Sostegno e finanziamento dal consiglio di amministrazione	**Punti di debolezza** • Non molta comunicazione tra i diversi dipartimenti e filiali • Nessun coordinamento con gli incidenti IT • Gran numero di "piccoli dipartimenti"
Opportunità • Enorme flusso di informazioni non strutturate sulle vulnerabilità • Grande bisogno di coordinamento • Ridurre le perdite dovute a incidenti • Gran numero di questioni aperte sulla sicurezza IT • Istruire il personale sulla sicurezza IT	**Minacce** • Non molto denaro disponibile • Non molto personale • Aspettative elevate • Cultura

Fig. 4 *Analisi SWOT campione*

5.3.2 Definizione del mandato

Dopo aver analizzato le esigenze e i desideri della comunità di riferimento in merito ai servizi CSIRT, il passo successivo deve essere la definizione del mandato.

La definizione del mandato descrive la funzione di base dell'organizzazione nella società, in termini di prodotti e servizi forniti ai propri utenti di riferimento. Essa permette di comunicare chiaramente l'esistenza e la funzione del nuovo CSIRT.

È buona prassi formulare una definizione del mandato che sia compatta ma non troppo stringata, in quanto in genere rimarrà invariata per un paio di anni.

Di seguito sono riportati alcuni esempi riferiti a CSIRT operativi:

"<Nome del CSIRT> fornisce informazioni e assistenza ai suoi <utenti di riferimento (definire i propri utenti di riferimento)> nell'attuazione di misure proattive volte a ridurre i

rischi di incidenti di sicurezza informatica e nella risposta a tali incidenti quando questi si verificano."

"Offrire sostegno agli <utenti di riferimento> sulla prevenzione e risposta agli incidenti di sicurezza relativi all'IT"[11]

La definizione del mandato rappresenta una fase cruciale da cui iniziare. Si rimanda al capitolo *2.1* di *RFC2350*[12] per una descrizione più dettagliata di quali informazioni debbano essere pubblicate da un CSIRT.

CSIRT simulato (fase 3b)
La gestione del CSIRT simulato ha formulato la seguente dichiarazione del compito: *"Il CSIRT simulato fornisce informazioni e assistenza al personale della sua società ospitante per ridurre i rischi di incidenti di sicurezza informatica e rispondere a tali incidenti quando questi si verificano."* Con essa, il CSIRT simulato chiarisce di essere un CSIRT interno e che la sua attività principale consiste nell'affrontare questioni legate alla sicurezza IT.

[11] Dichiarazione del compito di Govcert.nl: http://www.govcert.nl

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

6 Sviluppare il piano di attività

Le seguenti fasi sono state compiute:

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?
3. Quali tipi di servizi può offrire un CSIRT alla sua comunità di riferimento.
4. Analisi dell'ambiente e degli utenti di riferimento
5. Definizione del mandato

>> Il prossimo passo consisterà nel formulare il piano di attività

Il risultato dell'analisi fornisce una buona panoramica delle esigenze e delle (presunte) debolezze della comunità di riferimento e viene quindi usato come spunto per il passaggio successivo.

6.1 Definire il modello finanziario

Dopo l'analisi sono stati selezionati un paio di servizi chiave da cui iniziare. Il passaggio successivo consisterà nel pensare al modello finanziario: quali parametri per la fornitura di servizi sono disponibili e pagabili.

In un mondo perfetto il finanziamento sarebbe adattato alle esigenze della comunità di riferimento, ma nella realtà il portafoglio di servizi disponibili deve adattarsi a un dato bilancio. È quindi più realistico iniziare dalla pianificazione delle questioni monetarie.

6.1.1 Modello di costo

I due fattori principali che influenzano i costi sono la determinazione delle ore di servizio e il numero (e qualità) dei dipendenti da destinarvi. È necessario offrire una risposta agli incidenti e sostegno tecnico 24x7, oppure questi servizi saranno forniti soltanto durante l'orario di ufficio?

A seconda della disponibilità desiderata e delle attrezzature d'ufficio (per esempio, è possibile lavorare da casa?), può risultare vantaggioso lavorare con un registro del servizio di guardia o un registro del servizio programmato.

Uno scenario ipotizzabile è quello dell'offerta di servizi sia proattivi sia reattivi durante l'orario di ufficio. Fuori dell'orario di ufficio, un membro del personale fornirà un servizio di guardia solo per servizi limitati, per esempio soltanto nel caso di disastri e incidenti gravi.

Un'altra opzione consiste nel cercare la cooperazione internazionale tra altri gruppi CSIRT. Vi sono già alcuni esempi di cooperazione funzionante sul modello "following the sun" (seguendo il sole). Per esempio, la cooperazione tra gruppi europei e americani è risultata vantaggiosa e si è rivelata un buon metodo per condividere le capacità

reciproche. Sun Microsystems CSIRT, per esempio, che ha filiali multiple in diversi fusi orari in tutto il mondo (le quali filiali fanno però tutte parte dello stesso gruppo CSIRT), offre servizi 24x7 trasferendo continuamente i compiti tra i gruppi attorno al mondo. Ciò consente di limitare i costi, in quanto i gruppi lavorano sempre soltanto durante il normale orario di ufficio e forniscono anche servizi alla "parte addormentata" del mondo.

È buona prassi, in particolare, analizzare a fondo l'esigenza di servizi 24x7 nella comunità di riferimento. Allarmi e avvisi trasmessi durante le ore notturne non hanno molto senso se il destinatario li leggerà soltanto la mattina successiva. Esiste un confine sottile tra "l'aver bisogno di un servizio" e "il volere un servizio", ma soprattutto gli orari di lavoro fanno un enorme differenza in termini di numero del personale e di strutture necessarie e, per questo, hanno un'elevata incidenza sul modello di costo.

6.1.2 Modello di ricavo

Quando si conosce il costo, il passo successivo deve essere quello di pensare ai possibili modelli di ricavo, ossia a come si possono finanziare i servizi pianificati. A questo proposito vi sono alcuni scenari possibili da valutare:

Utilizzo delle risorse esistenti
È sempre utile valutare le risorse già presenti in altre parti della società. Si dispone già del personale adatto (per esempio nel dipartimento IT esistente), con la necessaria preparazione e competenza? Probabilmente si possono trovare accordi con la direzione per distaccare questo personale al CSIRT nella fase iniziale o perché fornisca sostegno ad hoc al CSIRT.

Quota di adesione
Un'altra possibilità consiste nel vendere i propri servizi alla comunità di riferimento attraverso una quota di adesione annuale/trimestrale. Ulteriori servizi potrebbero essere acquistati in "pay-per-use" (pagare in funzione dell'utilizzo), per esempio servizi di consulenza o revisioni della sicurezza.

Altro scenario ipotizzabile: i servizi per la comunità di riferimento (interna) sono offerti gratuitamente, ma è possibile richiedere il pagamento dei servizi forniti ai clienti esterni. Un'altra idea sarebbe quella di pubblicare bollettini informativi di ogni tipo sul sito web pubblico e di avere una sezione "per soli membri" contenente informazioni specifiche, più dettagliate o personalizzate.

La pratica ha dimostrato che l'"abbonamento a servizio CSIRT" ha un utilizzo troppo limitato per fornire un finanziamento sufficiente, soprattutto nella fase di avvio. Vi sono per esempio costi base fissi per il gruppo e l'attrezzatura che devono essere pagati in anticipo. Il finanziamento di questi costi attraverso la vendita di servizi CSIRT è difficile e richiede un'analisi finanziaria estremamente dettagliata per trovare il "punto di equilibrio".

Sovvenzione
Un'altra possibilità che vale la pena considerare potrebbe essere quella di chiedere una sovvenzione per il progetto al governo o a un organo governativo, in quanto oggigiorno molti paesi mettono a disposizione fondi per i progetti sulla sicurezza IT. Contattare il ministero degli Interni potrebbe essere un buon inizio.

Naturalmente è possibile realizzare un mix dei diversi modelli di ricavo.

6.2 Definire la struttura organizzativa

La struttura organizzativa adatta di un CSIRT dipende grandemente dalla struttura esistente dell'organizzazione ospitante e dalla comunità di riferimento, nonché dall'accessibilità di esperti competenti da assumere in modo permanente o ad hoc.

Un CSIRT tipico definisce i seguenti ruoli all'interno del gruppo:

Generale
- Direttore generale

Personale
- Capoufficio
- Contabile
- Consulente di comunicazione
- Consulente legale

Gruppo tecnico operativo
- Responsabile del gruppo tecnico
- Tecnici CSIRT per l'erogazione dei servizi CSIRT
- Ricercatori

Consulenti esterni
- Assunti quando necessario

È estremamente utile avere uno specialista legale in squadra, soprattutto durante la fase iniziale del CSIRT. Questo aumenterà i costi, ma a conti fatti farà risparmiare tempo e problemi giuridici.

A seconda della varietà di competenze all'interno della comunità di riferimento e anche quando il CSIRT ha un profilo elevato a livello di media, si è rivelato utile avere un esperto di comunicazione anche all'interno del gruppo. Tali esperti possono dedicarsi a tradurre questioni tecniche difficili in messaggi più comprensibili per gli utenti o i partner nei media. L'esperto di comunicazione fornirà anche un riscontro dalla comunità di riferimento agli esperti tecnici, agendo quindi da "traduttore" e "facilitatore" tra questi due gruppi.

Di seguito sono riportati alcuni esempi di modelli organizzativi utilizzati da CSIRT operativi.

6.2.1 Il modello di attività indipendente

Il CSIRT viene sviluppato e agisce come organizzazione indipendente, con una propria direzione e propri dipendenti.

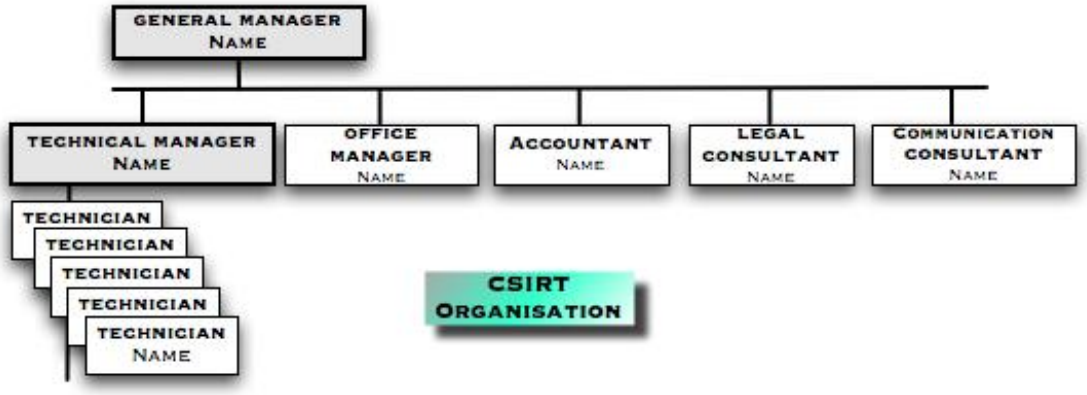


Fig. 5 Modello di attività indipendente

6.2.2 Il modello incorporato

Questo modello può essere usato se si deve creare un CSIRT all'interno di un'organizzazione esistente, per esempio utilizzando un dipartimento IT già costituito. Il CSIRT è guidato da un responsabile di gruppo che risponde delle attività del CSIRT. Il responsabile di gruppo riunisce i tecnici necessari per risolvere gli incidenti o lavorare alle attività del CSIRT. Può inoltre chiedere assistenza all'interno dell'organizzazione esistente per ricevere un sostegno specialistico.

Il modello può anche essere adattato a situazioni specifiche, man mano che queste si presentano. In tal caso, al gruppo viene assegnato un numero fisso o equivalente a tempo pieno (ETP). La sezione abusi di un ISP, per esempio, è senza dubbio un lavoro a tempo pieno per uno o (nella maggior parte dei casi) più di un ETP.

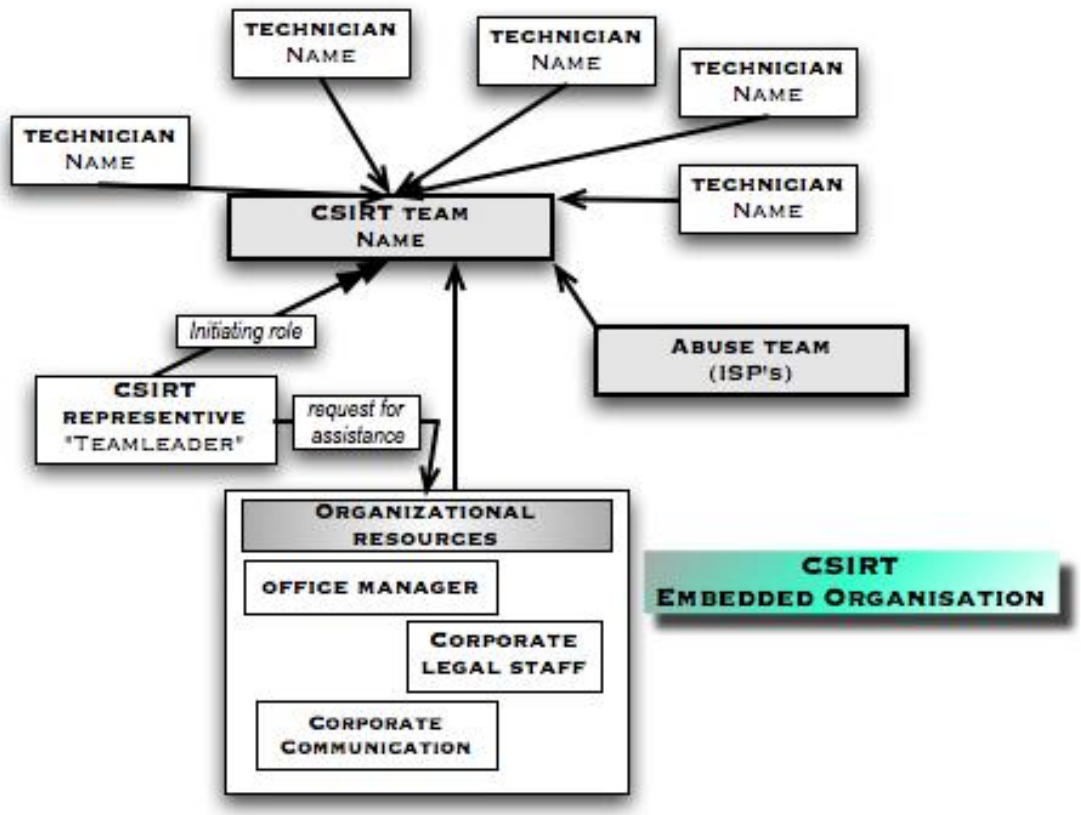


Fig. 6 Modello organizzativo incorporato

6.2.3 Il modello campus

Come suggerisce il nome stesso, il modello campus viene adottato prevalentemente da CSIRT accademici e di ricerca. La maggior parte delle organizzazioni accademiche e di ricerca comprende diverse università e campus in luoghi differenti, sparsi in una regione o addirittura in tutto il paese (come nel caso delle NREN, le reti di ricerca nazionali). Solitamente queste organizzazioni sono indipendenti le une dalle altre e spesso hanno un proprio CSIRT. Tali CSIRT sono in genere organizzati sotto l'egida del CSIRT "madre" o chiave. Il CSIRT chiave svolge una funzione di coordinamento ed è l'unico punto di contatto per il mondo esterno. Nella maggior parte dei casi il CSIRT chiave fornirà anche i servizi CSIRT chiave, oltre a divulgare le informazioni su eventuali incidenti al CSIRT di campus appropriato.

Alcuni CSIRT erogano i loro servizi chiave CSIRT insieme ad altri CSIRT di campus, abbassando così i costi generali per il CSIRT chiave.

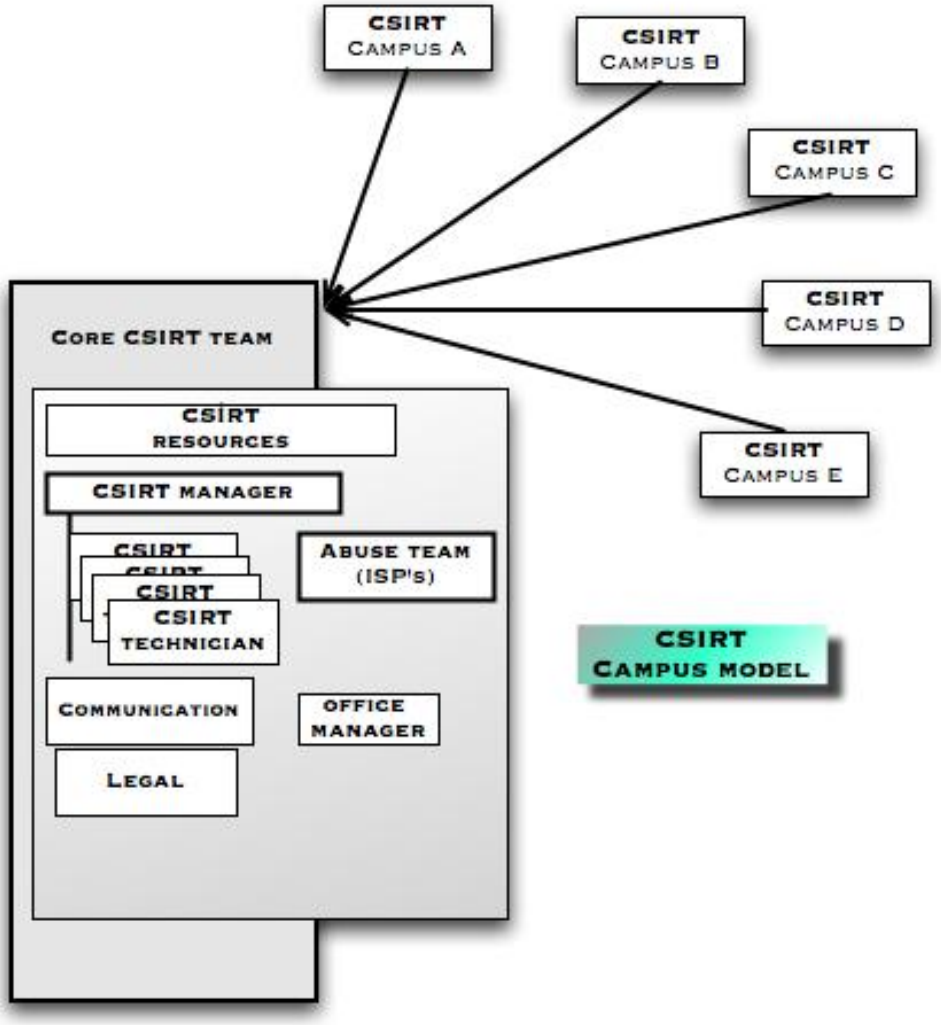


Fig. 7 Modello campus

6.2.4 Il modello volontario

Questo modello organizzativo descrive un gruppo di specialisti che si uniscono per fornire volontariamente consulenza e sostegno reciproci (e a terzi). Si tratta di una comunità priva di vincoli, che dipende fortemente dalla motivazione dei partecipanti.

Questo modello viene per esempio adottato dalla comunità WARP[13].

6.3 Assumere personale idoneo

Una volta decisi i servizi e il livello di sostegno da garantire e dopo aver scelto un modello organizzativo, il passaggio successivo consiste nel trovare il giusto numero di soggetti competenti per il lavoro.

È praticamente impossibile fornire cifre sicure sul numero di addetti tecnici necessari da questo punto di vista, ma i seguenti valori chiave si sono rivelati un buon approccio:

- Per fornire i due servizi chiave di distribuzione dei bollettini informativi e gestione degli incidenti: un minimo di **4** ETP.
- Per un CSIRT a pieno servizio durante l'orario di ufficio e la manutenzione dei sistemi: un minimo di **6-8** ETP.
- Per un turno 24x7 con personale al completo (2 turni fuori dell'orario di ufficio), il minimo è di **12** ETP circa.

Queste cifre comprendono anche le ridondanze in caso di malattia, ferie ecc. È altresì necessario verificare i contratti collettivi di lavoro locali. Lavorare fuori dell'orario di ufficio può comportare costi aggiuntivi sotto forma di indennità aggiuntive da pagare.

[13] L'iniziativa WARP http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Di seguito è riportata una breve panoramica delle competenze chiave richieste agli esperti tecnici di un CSIRT.

Voci descrittive del lavoro del personale tecnico generale:

Competenze personali

- Flessibilità, creatività e buono spirito di squadra
- Elevate capacità analitiche
- Capacità di spiegare argomenti tecnici difficili con parole semplici
- Una buona propensione alla riservatezza e a lavorare secondo le procedure
- Buone capacità organizzative
- Resistenza allo stress
- Elevate capacità comunicative e di scrittura
- Apertura mentale e desiderio di apprendimento

Competenze tecniche

- Ampia conoscenza della tecnologia e dei protocolli Internet
- Conoscenza dei sistemi Linux e Unix (a seconda delle dotazioni della comunità di riferimento)
- Conoscenza dei sistemi Windows (a seconda delle dotazioni della comunità di riferimento)
- Conoscenza delle attrezzature per l'infrastruttura di rete (router, commutatori, DNS, proxy, posta elettronica ecc.)
- Conoscenza delle applicazioni Internet (SMPT, HTTP, FTP, telnet, SSH ecc.)
- Conoscenza dei rischi per la sicurezza (DDoS, phishing, defacing, sniffing ecc.)
- Conoscenza della valutazione dei rischi e attuazioni pratiche

Ulteriori competenze

- Disponibilità a lavorare 24x7 o con servizio di guardia (a seconda del modello di servizio)
- Distanza massima di viaggio (in caso di emergenza disponibilità in ufficio; tempo massimo di viaggio)
- Livello d'istruzione
- Esperienza di lavoro nel campo della sicurezza IT

CSIRT simulato (fase 4)

Definire il piano di attività

Modello finanziario

Poiché la società ha un dipartimento per il commercio elettronico (e-business) 24x7 e anche un dipartimento IT 24x7, si opta per l'attività a pieno sevizio durante l'orario di ufficio e il servizio di guardia fuori dell'orario di ufficio. I servizi per la comunità di riferimento saranno forniti gratuitamente, ma si valuterà la possibilità di offrire prestazioni ai clienti esterni durante la fase pilota e di valutazione.

Modello di ricavo

Durante la fase iniziale e pilota, il CSIRT sarà finanziato dalla società ospitante. Durante la fase pilota e di valutazione si discuteranno ulteriori finanziamenti, compresa la possibilità di vendere i servizi a clienti esterni.

Modello organizzativo
L'organizzazione ospitante è una piccola società, quindi si sceglie il modello incorporato. Durante l'orario di ufficio, un gruppo di tre dipendenti fornirà i servizi chiave (distribuzione di bollettini informativi sulla sicurezza e gestione/coordinamento degli incidenti).

Il dipartimento IT della società dispone già di personale adeguato. Si giunge a un accordo con tale dipartimento affinché il nuovo CSIRT possa chiedere sostegno ad hoc, ove necessario. Si potrà usare anche la 2ª linea dei loro tecnici in servizio di guardia.
Ci sarà un gruppo CSIRT chiave con quattro membri a tempo pieno, più altri cinque membri del gruppo CSIRT. Uno di essi sarà disponibile anche a rotazione.

Personale
Il responsabile del gruppo CSIRT è preparato in materia di sicurezza e sostegno di 1° e 2° livello, oltre ad aver lavorato nel campo della gestione delle crisi di resistenza. Gli altri tre membri del gruppo sono specialisti della sicurezza. I membri a tempo parziale del gruppo CSIRT, provenienti dal dipartimento IT, sono specialisti per quanto concerne la loro parte dell'infrastruttura della società.

6.4 Utilizzo e attrezzature dell'ufficio

Le attrezzature e l'utilizzo dello spazio dell'ufficio, come pure la sicurezza fisica, sono argomenti di ampia portata che non possono essere trattati in maniera esaustiva in questo documento. Il presente capitolo intende quindi fornire soltanto una breve panoramica dell'argomento.

Maggiori informazioni sulla sicurezza fisica sono reperibili agli indirizzi:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

"Rinforzare l'edificio"
Poiché i CSIRT solitamente maneggiano informazioni molto riservate, è buona prassi che il gruppo assuma il controllo della sicurezza fisica dell'ufficio. Ciò dipenderà in larga misura dall'infrastruttura e dalle strutture esistenti, come pure dalla politica di sicurezza dell'informazione adottata dalla società ospitante.

I governi, per esempio, lavorano con schemi di classificazione e sono molto rigorosi in merito alla manipolazione delle informazioni riservate. È bene verificare le norme e politiche locali insieme alla propria società o istituzione.

Solitamente un nuovo CSIRT deve dipendere dalla cooperazione della sua organizzazione ospitante per venire a conoscenza delle norme locali, delle politiche e di altre questioni giuridiche.

Una descrizione esaustiva di tutte le attrezzature e misure di sicurezza necessarie non rientra nell'oggetto del presente documento. Si riporta comunque un breve elenco delle strutture di base per un CSIRT.

Regole generali per l'edificio
- Utilizzare controlli di accesso
- Rendere almeno l'ufficio CSIRT accessibile soltanto al personale CSIRT
- Monitorare gli uffici e gli ingressi con telecamere
- Archiviare le informazioni riservate in armadietti con serratura o in una cassaforte
- Utilizzare sistemi IT sicuri

Regole generali per l'attrezzatura IT
- Usare attrezzature supportate dal personale
- Rinforzare tutti i sistemi
- Correggere e aggiornare tutti i sistemi prima di collegarli a Internet
- Utilizzare software di sicurezza (firewall, scanner anti-virus multipli, anti-spyware ecc.)

Mantenere canali di comunicazione
- Sito web pubblico
- Area riservata ai membri nel sito web
- Moduli web per la segnalazione di incidenti
- Posta elettronica (supporto PGP / GPG / S/MIME)
- Software per mailing list
- Avere un numero di telefono dedicato disponibile per la comunità di riferimento:
    - Telefono
    - Fax
    - SMS

Sistema/i di reperimento delle registrazioni
- Banca dati dei contatti con i dettagli dei membri del gruppo, di altri gruppi ecc.
- Strumenti CRM
- Sistema ticket per la gestione degli incidenti

Usare lo "stile aziendale" dall'inizio per
- Il layout standard di messaggi di posta elettronica e bollettini informativi
- Lettere cartacee tradizionali
- Rapporti mensili o annuali
- Modulo di segnalazione incidenti

Altro
- Prevedere una comunicazione fuori banda in caso di attacchi
- Prevedere la ridondanza sulla connettività Internet

Per ulteriori informazioni sugli strumenti specifici dei CSIRT cfr. il capitolo *8.5 Strumenti disponibili dei CSIRT*.

6.5 Sviluppare una politica di sicurezza dell'informazione

In base al tipo di CSIRT, si avrà una politica personalizzata di sicurezza dell'informazione. Oltre a descrivere le condizioni desiderate delle procedure e dei processi operativi e amministrativi, tale politica deve essere in linea con la legislazione e gli standard, in particolare in merito alla responsabilità del CSIRT. Il CSIRT è solitamente vincolato alle leggi e ai regolamenti nazionali, che sono spesso recepiti nell'ambito della legislazione europea (in genere direttive) e di altri accordi internazionali. Gli standard non sono necessariamente vincolanti in maniera diretta, ma possono essere imposti o raccomandati dalle leggi e dai regolamenti.

Di seguito si riporta un breve elenco delle leggi e politiche possibili:

Nazionali
- Varie leggi sulla tecnologia dell'informazione, telecomunicazione, media
- Leggi sulla vita privata e sulla protezione dei dati
- Leggi e regolamenti sulla conservazione dei dati
- Legislazione in materia di finanza, contabilità e gestione aziendale
- Codici di condotta per il governo societario e il governo IT

Europee
- Direttiva sulle firme elettroniche (1993/93/CE)
- Direttive sulla protezione dei dati (1995/46/CE) e sulla vita privata nelle comunicazioni elettroniche (2002/58/CE)
- Direttive sulle reti e sui servizi di comunicazione elettronica (2002/19/CE – 2002/22/CE)
- Direttive sul diritto societario (per esempio l'8ª direttiva sul diritto societario)

Internazionali
- Accordo Basilea II (soprattutto in merito alla gestione del rischio operativo)
- Convenzione del Consiglio d'Europa sulla criminalità informatica
- Convenzione del Consiglio d'Europa sui diritti umani (articolo 8 sulla vita privata)
- Principi contabili internazionali (IAS; essi prescrivono in certa misura i controlli IT)

Standard
- British Standard BS 7799 (sicurezza dell'informazione)
- Standard internazionali ISO2700x (sistemi di gestione della sicurezza dell'informazione)
- IT-Grundschutzbuch tedesco, EBIOS francese e altre varianti nazionali

Al fine di determinare se il proprio CSIRT agisce in conformità con la legislazione nazionale e internazionale, si consiglia di rivolgersi al proprio consulente legale.

Le domande principali cui bisogna rispondere nelle proprie politiche di gestione dell'informazione sono:

- Come sono "contrassegnate" o "classificate" le informazioni in entrata?
- Come vengono gestite le informazioni, soprattutto in merito all'esclusività?

- Quali considerazioni si adottano per la divulgazione di informazioni, soprattutto se si trasmettono informazioni relative a un incidente ad altri gruppi o siti?
- Vi sono considerazioni giuridiche di cui tenere conto in rapporto alla gestione delle informazioni?
- Avete una politica sull'utilizzo della crittografia per proteggere l'esclusività e integrità negli archivi e/o nella comunicazione dei dati, soprattutto via posta elettronica?
- Questa politica comprende possibili condizioni limite legali, tra cui il sistema di deposito della chiave o l'applicabilità della decifratura in caso di azioni legali?

CSIRT simulato (fase 5)

Attrezzatura d'ufficio e ubicazione

Poiché la società ospitante dispone già di un'efficiente sicurezza fisica, il nuovo CSIRT vanta una buona copertura a questo riguardo. Viene messa a disposizione una cosiddetta "sala della guerra" per consentire il coordinamento in caso di emergenza. Si provvede ad acquistare una cassaforte per il materiale di cifratura e i documenti riservati. È stata predisposta una linea telefonica separata comprensiva di centralino per supportare la linea diretta durante l'orario di ufficio e il cellulare del servizio "di guardia" fuori dell'orario di ufficio con lo stesso numero di telefono.

Si possono usare anche l'attrezzatura esistente e il sito web aziendale per annunciare le informazioni relative al CSIRT. Una mailing list viene installata e mantenuta, con una parte riservata alla comunicazione tra i membri del gruppo e con altri gruppi. Tutti i dettagli dei contatti dei membri del personale sono archiviati in una banca dati e una stampa viene conservata nella cassaforte.

Regolamento

Poiché il CSIRT è incorporato in una società con politiche esistenti in materia di sicurezza dell'informazione, le relative politiche per il CSIRT sono state elaborate con l'ausilio del consulente legale della società.

6.6 Ricerca di collaborazione tra altri CSIRT e possibili iniziative nazionali

L'esistenza di altre iniziative CSIRT e l'elevata esigenza di cooperazione tra di esse sono già state menzionate un paio di volte nel presente documento. È buona prassi contattare il prima possibile altri CSIRT per stabilire il necessario rapporto con le comunità CSIRT. In genere gli altri CSIRT sono molto disponibili ad aiutare i gruppi appena costituiti nella loro fase di avvio.

L'*Inventario delle attività CERT in Europa*[14] dell'ENISA è un ottimo punto d'inizio per la ricerca di altri CSIRT nel paese o per attività di cooperazione nazionale tra CSIRT.

Per ricevere sostegno nella ricerca di una fonte adatta di informazioni sui CSIRT, contattare gli esperti CSIRT dell'ENISA all'indirizzo:

CERT-Relations@enisa.europa.eu

[14] Inventario ENISA: http://www.enisa.europa.eu/cert_inventory/

Di seguito è riportata una panoramica delle attività della comunità CSIRT. Si rimanda all'*Inventario* per una descrizione più approfondita e per ulteriori informazioni.

Iniziativa CSIRT europea

TF-CSIRT[15]
La task force TF-CSIRT promuove la collaborazione tra i Computer Security Incident Response Team (CSIRT) in Europa. Gli obiettivi principali di questa task force consistono nel mettere a disposizione un forum per lo scambio di esperienze e conoscenze, nell'instaurare servizi pilota per la comunità degli CSIRT europei e nel sostenere la creazione di nuovi CSIRT.

Gli obiettivi principali della task force sono:
- Mettere a disposizione un forum per lo scambio di esperienze e conoscenze
- Instaurare servizi pilota per la comunità dei CSIRT europei
- Promuovere standard e procedure comuni per rispondere agli incidenti di sicurezza
- Sostenere la creazione di nuovi CSIRT e la formazione del loro personale
- Le attività di TF-CSIRT si concentrano sull'Europa e sui paesi confinanti, in conformità con i mandati approvati dal Comitato tecnico TERENA il 15 settembre 2004.

Iniziativa CSIRT globale

FIRST[16]
FIRST è l'organizzazione più importante e il leader globale riconosciuto nella risposta agli incidenti. L'adesione a FIRST consente ai gruppi di risposta agli incidenti di reagire in maniera più efficace agli incidenti di sicurezza, in modo sia reattivo sia proattivo.

FIRST riunisce una varietà di gruppi di risposta agli incidenti di sicurezza informatica appartenenti a organizzazioni governative, commerciali e d'istruzione. FIRST intende incentivare la cooperazione e il coordinamento nella prevenzione degli incidenti, stimolare una reazione rapida agli incidenti e promuovere la condivisione delle informazioni tra i membri e la comunità nel suo complesso.

Oltre a dare vita a una rete di fiducia nella comunità globale di risposta agli incidenti, FIRST offre anche servizi a valore aggiunto.

CSIRT simulato (fase 6)
Alla ricerca di cooperazione Utilizzando l'Inventario dell'ENISA sono stati trovati rapidamente e contattati alcuni CSIRT nello stesso paese. Una visita in loco è stata concordata con uno di essi per il responsabile del gruppo appena assunto. Questi ha appreso le attività dei CSIRT nazionali e ha partecipato a un incontro. Tale incontro è stato più che utile per raccogliere esempi dei metodi di lavoro e ottenere il sostegno di un paio di altri gruppi.

[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 Promuovere il piano di attività

Finora abbiamo compiuto i seguenti passi:

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?
3. Quali tipi di servizi può offrire un CSIRT alla sua comunità di riferimento.
4. Analisi dell'ambiente e degli utenti
5. Definire la dichiarazione del compito
6. Sviluppare il piano di attività
    a. Definire il modello finanziario
    b. Definire la struttura organizzativa
    c. Iniziare ad assumere personale
    d. Utilizzare e attrezzare l'ufficio
    e. Sviluppare una politica di sicurezza dell'informazione
    f. Cercare partner di cooperazione

>> Il prossimo passo consisterà nel riunire quanto precede in un piano di attuazione del progetto e prendere il via!

Un buon modo per iniziare a definire i vostri progetti è sottoporre un argomento commerciale. Tale argomento commerciale sarà usato come base per il piano di attuazione del progetto nonché per chiedere il sostegno della direzione od ottenere lo stanziamento di un bilancio preventivo o di altre risorse.

Si è rivelato utile riferire costantemente alla direzione per mantenere alta la consapevolezza dei problemi di sicurezza IT e, quindi, del sostegno continuo al proprio CSIRT.

Per introdurre un argomento commerciale si inizia dall'analisi dei problemi e delle opportunità utilizzando un modello di analisi, descritto nel capitolo *5.3 Analisi della* comunità di riferimento, e cercando di entrare in stretto contatto con la potenziale comunità di riferimento.

Come precedentemente descritto, sussistono numerosi aspetti di cui tener conto nella fase di avvio di un CSIRT. L'ideale è adeguare il suddetto materiale alle esigenze dei CSIRT man mano che questi si sviluppano.

È buona prassi, quando si riferisce alla direzione, rendere il proprio argomento il più attuale possibile usando articoli recenti presi dai giornali o da Internet e spiegare perché l'assistenza e il coordinamento interno degli incidenti da parte del CSIRT sono fondamentali per la sicurezza delle attività commerciali. È altresì necessario chiarire che soltanto un sostegno costante in questioni di sicurezza IT permette di avere un'attività stabile, soprattutto per una società o un'istituzione che dipende dall'IT

(Una frase significativa di Bruce Schneier sintetizza brillantemente questo concetto: *"La sicurezza non è un prodotto ma un processo[17]!"*).

Un famoso strumento per illustrare i problemi di sicurezza è il grafico seguente messo a disposizione dal CERT/CC:

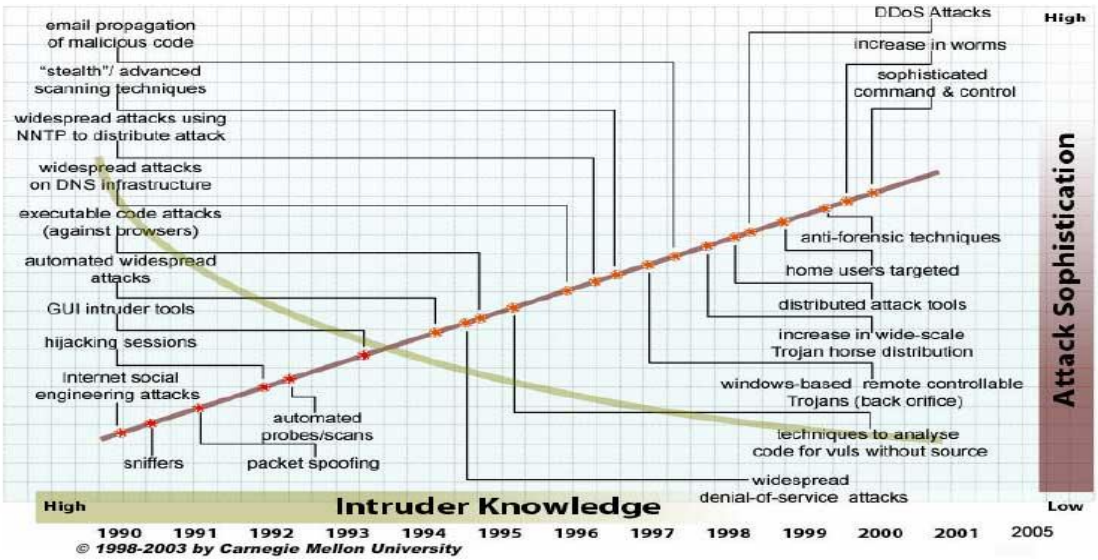


Fig. 8 Conoscenza degli intrusi contro sofisticazione degli attacchi (fonte CERT-CC[18])

Esso visualizza le tendenze in atto nella sicurezza IT, in particolare l'abbassamento delle capacità necessarie per effettuare attacchi sempre più sofisticati.

Un altro punto da menzionare è il continuo restringimento della finestra temporale tra la disponibilità degli aggiornamenti software per le vulnerabilità e l'inizio di attacchi contro di essi:

Patch -> Exploit		**Velocità di diffusione**	
Nimda:	11 mesi	Code red:	Giorni
Slammer:	6 mesi	Nimda:	Ore
Nachi:	5 mesi	Slammer:	Minuti
Blaster:	3 settimane		
Witty:	1 giorno (!)		

I dati raccolti sugli incidenti, i miglioramenti potenziali e gli insegnamenti tratti contribuiscono anch'essi a una buona presentazione.

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

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

7.1 Descrizione dei piani di attività e leve direzionali

Una presentazione per la direzione comprendente la promozione del CSIRT non costituisce da sola un argomento commerciale, ma se svolta in maniera appropriata permetterà di ottenere il sostegno della direzione al CSIRT nella maggioranza dei casi. L'argomento commerciale, d'altro canto, non deve essere visto solamente come un esercizio gestionale, ma deve anche essere usato per la comunicazione al gruppo e alla comunità di riferimento. L'espressione argomento commerciale può suonare più inerente al commercio e distante dalla prassi giornaliera del CSIRT, ma fornisce un buon orientamento e oggetto d'interesse per la creazione di un CSIRT.

Le risposte alle seguenti domande possono essere usate per elaborare un buon argomento commerciale (gli esempi forniti sono ipotetici e usati a solo titolo illustrativo. Le risposte "reali" dipendono notevolmente dalle circostanze "reali").

- Qual è il problema?
- Cosa si vuole realizzare con i propri utenti?
- Cosa succede se non si fa niente?
- Cosa succede se si prende l'iniziativa?
- Quanto costerà?
- Cosa si guadagnerà?
- Quando si comincia e quando si finisce?

Qual è il problema?
Nella maggior parte dei casi, l'idea di creare un CSIRT sorge quando la sicurezza IT è divenuta una componente essenziale dell'attività chiave di una società o istituzione e quando gli incidenti di sicurezza IT diventano un rischio per l'attività, facendo dell'attenuazione delle minacce una normale operazione aziendale.

La maggior parte delle società o istituzioni dispone di un regolare dipartimento di sostegno o helpdesk, ma nella maggioranza dei casi gli incidenti di sicurezza sono gestiti in maniera insufficiente e non adeguatamente strutturata. In genere l'ambito di lavoro degli incidenti di sicurezza richiede speciali capacità e attenzione. Anche adottare un approccio più strutturato è vantaggioso e aiuterà ad attenuare i rischi aziendali e i danni per la società.

Il problema nella maggior parte dei casi consiste nella mancanza di coordinamento e nel fatto che le conoscenze esistenti non vengono usate per gestire gli incidenti, impedendo così che si ripetano nel futuro ed evitando possibili perdite finanziarie e/o danni alla reputazione di un'istituzione.

Quali sono gli obiettivi da raggiungere con la comunità di riferimento?
Come sopra illustrato, il vostro CSIRT servirà i suoi utenti e li aiuterà a risolvere problemi e incidenti di sicurezza IT. Ulteriori obiettivi sono l'innalzamento del livello di conoscenza della sicurezza IT e la realizzazione di una cultura consapevole della sicurezza.

Tale cultura si sforza di adottare sin dall'inizio misure proattive e preventive, riducendo così i costi operativi.

Introdurre una simile cultura della cooperazione e assistenza in una società o istituzione può stimolare l'efficienza in generale in un gran numero di casi.

Cosa succede se non si fa niente?
Un modo non strutturato di trattare la sicurezza IT può provocare ulteriori danni, non da ultimo alla reputazione dell'istituzione. Altre conseguenze possono essere perdite finanziarie e implicazioni legali.

Cosa succede se si prende l'iniziativa?
Aumenta il livello di sensibilizzazione riguardo a eventuali problemi di sicurezza. Questo aiuta a risolverli in maniera più efficiente e a prevenire perdite future.

Quanto costerà?
A seconda del modello organizzativo, il costo comprenderà gli stipendi dei membri del gruppo CSIRT e dell'organizzazione, l'attrezzatura, gli strumenti e le licenze software.

Cosa si guadagnerà?
A seconda dell'attività e delle perdite passate, si guadagnerà più trasparenza nelle procedure e prassi di sicurezza, proteggendo così le attività commerciali fondamentali.

Qual è la tempistica?
Cfr. il capitolo *12. Descrizione del piano di attuazione del progetto* per la descrizione di un piano campione.

Esempi di argomenti commerciali e approcci esistenti
Di seguito sono elencati alcuni esempi di argomenti commerciali CSIRT che merita studiare:

- http://www.cert.org/csirts/AFI_case-study.html
  Creare il CSIRT di un istituto finanziario: un caso studio

  Lo scopo di questo documento consiste nel condividere gli insegnamenti tratti da un istituto finanziario (denominato nel presente documento AFI) durante lo sviluppo e l'attuazione di un piano per affrontare i problemi di sicurezza e di un Computer Security Incident Response Team (CSIRT).

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Riassunto dell'argomento commerciale di CERT POLSKA (presentazione di diapositive in formato PDF).

- http://www.auscert.org.au/render.html?it=2252
  Costituire un gruppo IRT (*Incident Response Team*, gruppo di risposta agli incidenti) negli anni Novanta può essere un compito scoraggiante. Molte delle persone che costituiscono un gruppo IRT non hanno alcuna esperienza in quest'ambito. Questo documento esamina il ruolo che un gruppo IRT può svolgere nella comunità e gli aspetti che devono essere affrontati sia durante la costituzione sia dopo l'inizio delle operazioni. Può essere utile ai gruppi IRT esistenti, in quanto può sensibilizzare in merito a questioni precedentemente trascurate.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Caso studio sulla sicurezza dell'informazione, rendere sicura l'impresa, di: Roger Benton

  Si tratta di un caso studio pratico della migrazione di una società assicurativa verso un sistema di sicurezza a livello aziendale. Lo scopo di questo caso pratico consiste nel fornire un percorso da seguire quando si crea o migra verso un sistema di sicurezza. All'inizio un primitivo sistema di sicurezza online era l'unico meccanismo per controllare l'accesso ai dati aziendali. Le esposizioni erano elevate e mancavano controlli sull'integrità al di fuori dell'ambiente online. Chiunque avesse nozioni base di programmazione poteva aggiungere, modificare e/o cancellare i dati di produzione.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Strategia di sicurezza elettronica di Marriott: collaborazione impresa-IT

  Secondo l'esperienza di Chris Zoladz di Marriott International Inc., la sicurezza del commercio elettronico è un processo, non un progetto. È stato questo il messaggio lanciato da Zoladz in occasione della recente conferenza ed esposizione sulla sicurezza elettronica tenutasi a Boston e sponsorizzata da Intermedia Group. Nella sua veste di vicepresidente della protezione dell'informazione per Marriott, Zoladz riferisce attraverso il dipartimento legale, pur non essendo un avvocato. La sua funzione consiste nell'individuare dove sono archiviate le informazioni aziendali più preziose di Marriott e come queste si muovono all'interno e all'esterno della società. Marriott ha definito una responsabilità separata per l'infrastruttura tecnica che sostiene la sicurezza, assegnandola all'architetto della sicurezza IT.

CSIRT simulato (fase 7)

Promuovere il piano di attività

Si decide di raccogliere fatti e cifre sulla storia della società, la qual cosa è estremamente utile per avere una panoramica statistica della situazione della sicurezza IT. Tale raccolta dovrà continuare quando il CSIRT sarà costituito e funzionante, al fine di mantenere la statistica aggiornata.

Altri CSIRT nazionali sono stati contattati e intervistati in merito ai loro argomenti commerciali e hanno fornito supporto compilando alcune diapositive con le informazioni sui recenti sviluppi negli incidenti di sicurezza IT e sui costi degli incidenti.

In questo caso esemplificativo di CSIRT simulato non vi era alcun bisogno pressante di convincere la direzione dell'importanza dell'attività IT e quindi non è stato difficile ottenere il nullaosta per il primo passo. Sono stati preparati un argomento commerciale e un piano di attuazione del progetto, compresa una stima dei costi di costituzione e del costo di esercizio.

8 Esempi di procedure operative e tecniche (flussi di lavoro)

Finora abbiamo compiuto i seguenti passi:

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?
3. Quali tipi di servizi può offrire un CSIRT alla sua comunità di riferimento.
4. Analisi dell'ambiente e degli utenti.
5. Definire la dichiarazione di mandato.
6. Sviluppare il piano di attività.
   a. Definire il modello finanziario
   b. Definire la struttura organizzativa
   c. Iniziare ad assumere personale
   d. Utilizzare e attrezzare l'ufficio
   e. Sviluppare una politica di sicurezza dell'informazione
   f. Cercare partner di cooperazione
7. Promuovere il piano di attività
   a. Far approvare l'argomento commerciale
   b. Inserire tutto in un piano di attuazione del progetto

>> Il prossimo passo consisterà nel rendere il CSIRT operativo

Avere in atto flussi di lavoro ben definiti migliorerà la qualità e il tempo necessario per ogni incidente o caso di vulnerabilità.

Come descritto nelle caselle esemplificative, il CSIRT simulato offrirà i servizi chiave di base del CSIRT:

- Allarmi e avvisi
- Gestione degli incidenti
- Annunci

Questo capitolo propone esempi di flussi di lavoro che descrivono i servizi chiave di un CSIRT. Contiene inoltre informazioni sulla raccolta di informazioni da fonti diverse, sulla verifica della loro pertinenza e autenticità e sulla loro redistribuzione alla comunità di riferimento. Infine, riporta esempi delle procedure più basilari e di strumenti CSIRT specifici.

8.1 Valutare la base d'installazione della comunità di riferimento

Il primo passo consiste nell'ottenere una panoramica dei sistemi IT installati presso la propria comunità di riferimento. Così facendo il CSIRT può valutare la pertinenza delle informazioni in entrata e filtrarle prima della redistribuzione, in modo che gli utenti non siano sommersi da informazioni per loro sostanzialmente inutili.

È buona prassi iniziare in maniera semplice, per esempio utilizzando un foglio di excel come il seguente:

Categoria	Applicazione	Prodotto software	Versione	OS	Versione OS	*Utente*
Desktop	Office	Excel	x-x-x	Microsoft	XP-prof	A
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A
Rete	Router	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Servizi	Web server	Apache		Unix	x-x-x	B

Con la funzione del filtro di excel, è molto facile selezionare il software adatto e vedere quale utente sta usando quale tipo di software.

8.2 Emettere segnalazioni, avvisi e annunci

La generazione di segnalazioni, avvisi e annunci segue sempre gli stessi flussi di lavoro:

- Raccolta di informazioni
- Valutazione della pertinenza e della fonte delle informazioni
- Valutazione del rischio sulla base delle informazioni raccolte
- Distribuzione delle informazioni

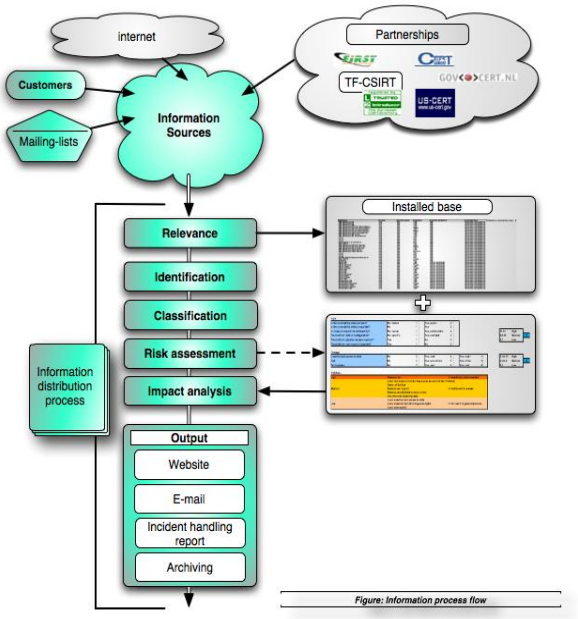


Fig. 9 : Flusso del processo informativo

Nei paragrafi seguenti questo flusso di lavoro sarà descritto in maniera più dettagliata.

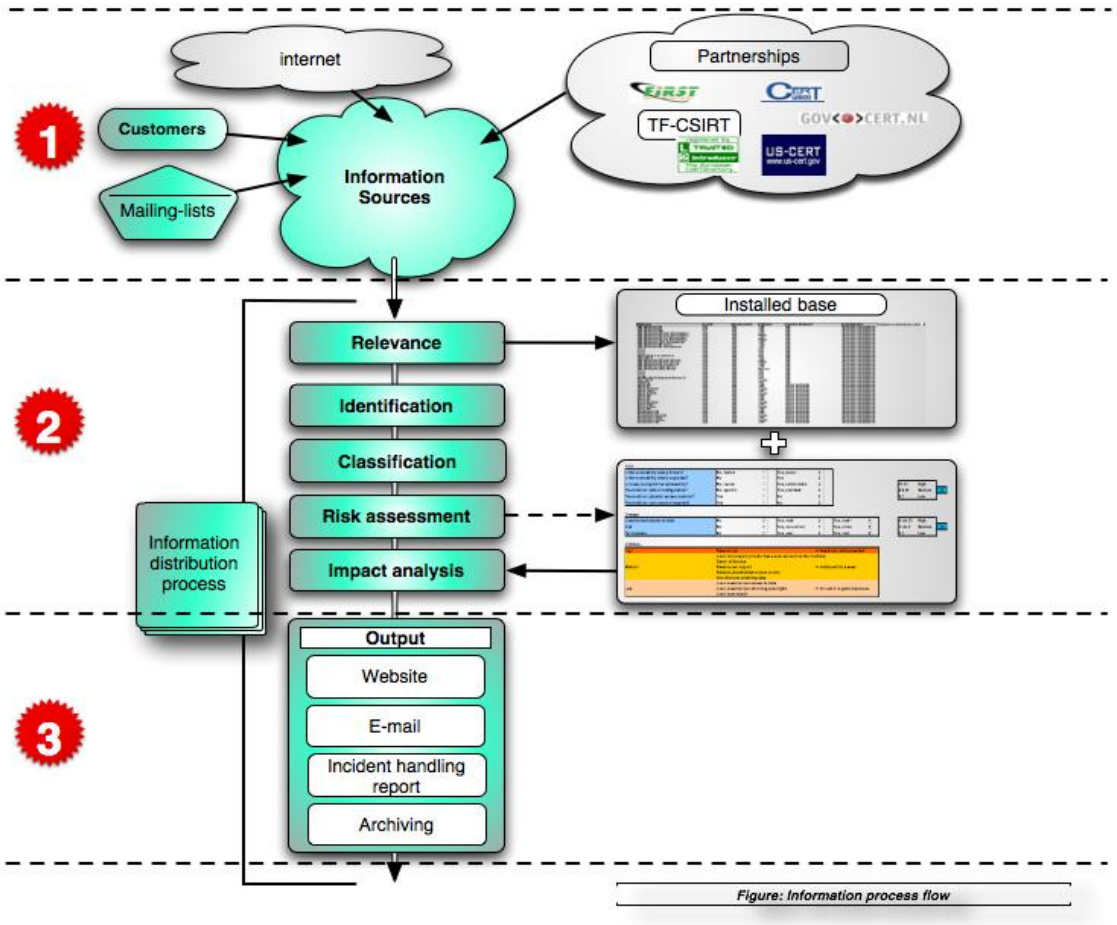


Figure: Information process flow

Fase 1: Raccogliere informazioni sulle vulnerabilità.

In genere esistono due tipi principali di fonti d'informazione che forniscono informazioni a titolo di contributo ai servizi:

- Le informazioni sulle vulnerabilità dei (propri) sistemi IT
- I rapporti sugli incidenti

A seconda del tipo di attività e dell'infrastruttura IT, vi sono molte fonti pubbliche e riservate di informazioni sulle vulnerabilità:

- Mailing list pubbliche e riservate
- Informazioni sulle vulnerabilità dei prodotti dei venditori
- Siti web
- Informazioni su Internet (Google ecc.)
- Partenariati pubblici e privati che forniscono informazioni sulle vulnerabilità (FIRST, TF-CSIRT, CERT-CC, US-CERT ecc.)

Tutte queste informazioni contribuiscono al livello di conoscenza in merito a vulnerabilità specifiche nei sistemi IT.

Come sopra accennato, in Internet è presente un gran numero di fonti di informazioni sulla sicurezza di buona qualità e facilmente accessibili. Nel momento in cui scriviamo, il gruppo di lavoro ad hoc dell'ENISA "servizi CERT" per il 2006 sta stilando un elenco più completo della situazione ipotizzata alla fine del 2006[19].



Fase 2: Valutazione delle informazioni e valutazione del rischio

Questa fase implicherà un'analisi dell'impatto di una vulnerabilità specifica sull'infrastruttura IT della comunità di riferimento.

Identificazione
Le informazioni in entrata sulle vulnerabilità devono sempre essere identificate in termini di fonte e bisogna stabilire se la fonte è affidabile prima di trasmettere le informazioni alla comunità di riferimento. In caso contrario si rischierebbe di allarmare inutilmente le persone, causando inutili interferenze nei processi aziendali e finendo per danneggiare la reputazione del CSIRT.

[19] Servizi del gruppo di lavoro ad hoc CERT:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

La procedura seguente mostra un esempio di identificazione dell'autenticità di un messaggio:

Procedura su come identificare l'autenticità di un messaggio e la sua fonte

Lista di controllo generale

1. La fonte è nota e registrata come tale?
2. Le informazioni sono pervenute attraverso un canale regolare?
3. Contengono informazioni "strane" che "suonano" errate?
4. Fidatevi delle vostre sensazioni: se avete dubbi su un'informazione, non agite ma verificate di nuovo!

Posta elettronica – Fonti

1. L'indirizzo della fonte è noto all'organizzazione e noto all'elenco delle fonti?
2. La firma PGP è corretta?
3. In caso di dubbio, controllare l'intestazione completa del messaggio.
4. In caso di dubbio, effettuare una ricerca per verificare il dominio del mittente[20].

WWW – Fonti

1. Controllare i certificati browser quando ci si connette a un sito web garantito (https://).
2. Controllare la fonte per verificare contenuto e validità (tecnica).
3. In caso di dubbio, non cliccare su nessun link né scaricare alcun software.
4. In caso di dubbio, effettuare una ricerca sul dominio e ricostruire il percorso.

Telefono

1. Ascoltare attentamente il nome.
2. Riconoscete la voce?
3. In caso di dubbio, chiedere un numero di telefono e di poter richiamare chi vi ha telefonato.

Fig. 10 Esempio di procedura per l'identificazione delle informazioni

Pertinenza

La panoramica sopra riportata degli hardware e software installati può essere utilizzata per filtrare le informazioni in entrata sulle vulnerabilità in base alla loro pertinenza, al fine di dare una risposta alle domande: "La comunità di riferimento utilizza questo software?"; "Le informazioni sono di sua pertinenza?"

Classificazione

Alcune informazioni ricevute possono essere classificate o contrassegnate come riservate (per esempio i rapporti in entrata sugli incidenti trasmessi da altri gruppi). Tutte le informazioni devono essere trattate secondo la richiesta del mittente e conformemente alla propria politica sulla sicurezza dell'informazione. Una buona regola di base è "*Non distribuire informazioni se non si è certi di poterlo fare; in caso di dubbio, chiedere il permesso al mittente.*"

[20] Strumenti per controllare le identità in CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Valutazione del rischio e analisi dell'impatto
Esistono diversi metodi per determinare il rischio e l'impatto di una (potenziale) vulnerabilità.

Il rischio si definisce come la potenziale possibilità che la vulnerabilità sia sfruttata. Vi sono diversi fattori importanti (tra gli altri):

- La vulnerabilità è notoria?
- La vulnerabilità è diffusa?
- È facile sfruttare la vulnerabilità?
- È una vulnerabilità sfruttabile a distanza?

Tutte queste domande danno un'idea chiara di quanto sia grave una vulnerabilità.
Un approccio molto semplice per calcolare il rischio è la formula seguente:

Impatto = rischio x danno potenziale

Il danno potenziale può essere

- L'accesso non autorizzato ai dati
- Il rifiuto di servizio (DOS)
- L'ottenimento o l'estensione dei permessi

(Per schemi di classificazione più elaborati si rimanda alla fine di questo capitolo).

Rispondendo a queste domande è possibile integrare il bollettino informativo con una valutazione generale, informando in merito ai potenziali rischi e danni. Spesso si usano termini semplici come BASSO, MEDIO e ALTO.

Altri schemi più completi di valutazione del rischio sono:

Schema di valutazione di GOVCERT.NL[21]

Il CSIRT governativo olandese GOVCERT.NL ha sviluppato una matrice per la valutazione del rischio, che è stata elaborata nella fase iniziale di Govcert.nl e continua a essere aggiornata secondo le tendenze più attuali.

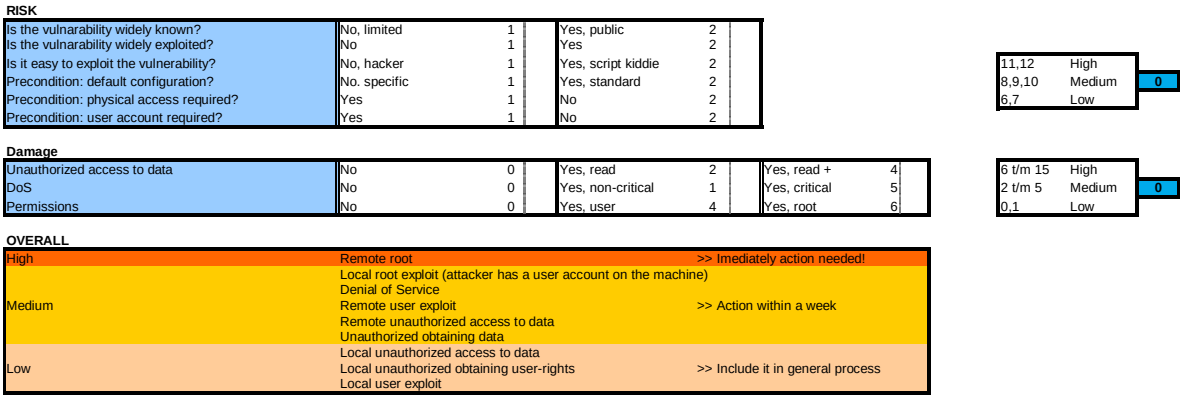


Fig. 11 Lo schema di valutazione di GOVCERT.NL

EISPP *Common Advisory Format Description*[22]

Il progetto EISPP (*European Information Security Promotion Programme*, programma europeo di promozione della sicurezza informatica) è un progetto finanziato anche dalla Comunità europea nell'ambito del quinto programma quadro. Il progetto EISPP ha come obiettivo lo sviluppo di una rete europea, non solo per condividere le conoscenze sulla sicurezza, ma anche per definire i contenuti e i canali attraverso i quali mettere a disposizione servizi di sicurezza alle PMI. Fornendo i necessari servizi di sicurezza IT alle PMI europee, queste saranno incoraggiate ad accrescere la loro fiducia e utilizzo del commercio elettronico, creando maggiori e migliori opportunità per la nuova attività. L'EISPP è un pioniere nella visione della Commissione europea di costituire una rete europea di competenze all'interno dell'Unione europea.

DAF *Deutsches Advisory Format*[23]

DAF è un'iniziativa del CERT-Verbund tedesco ed è una componente chiave di un'infrastruttura per la generazione e lo scambio di bollettini informativi sulla sicurezza da parte di gruppi diversi. DAF è studiato appositamente per le esigenze dei CERT tedeschi ed è sviluppato e mantenuto da CERT-Verbund, DFN-CERT, PRESECURE e Siemens-CERT.

[21] Matrice di vulnerabilità: 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



Fase 3: Distribuzione delle informazioni

Un CSIRT può scegliere tra diversi metodi di distribuzione a seconda dei desideri degli utenti e della propria strategia di comunicazione.

- Sito web
- Posta elettronica
- Rapporti
- Archiviazione e ricerca

I bollettini informativi sulla sicurezza distribuiti da un CSIRT devono sempre avere la stessa struttura al fine di migliorare la leggibilità e consentire al lettore di reperire velocemente le informazioni pertinenti.

Un bollettino informativo deve contenere almeno le seguenti informazioni:

Titolo del bollettino informativo (o *advisory*) ……
Numero di riferimento …… **Sistemi interessati** **-** …… **-** …… **OS correlato + versione** …… **Rischio** (alto-medio-basso) …… **Impatto/danno potenziale** (alto-medio-basso) …… **ID esterni:** (CVE, ID dei bollettini sulle vulnerabilità) ……
Panoramica delle vulnerabilità …… **Impatto** …… **Soluzione** …… **Descrizione (dettagli)** …… **Appendice** ……

*Fig. 12 Schema campione di un bollettino informativo (*advisory*)*

Cfr. capitolo *10. Esercizio* per un esempio completo di un bollettino informativo sulla sicurezza.

8.3 Effettuare la gestione degli incidenti

Come anticipato nell'introduzione di questo capitolo, il processo di gestione delle informazioni durante la gestione degli incidenti è molto simile a quello usato durante la compilazione di allarmi, avvisi e annunci. La differenza risiede solitamente nella parte dedicata alla raccolta delle informazioni, in quanto i dati relativi agli incidenti si ottengono in genere ricevendo rapporti sugli incidenti dalla comunità di riferimento o da altri gruppi, oppure ricevendo un riscontro dalle parti interessate durante il processo di gestione degli incidenti. Le informazioni sono generalmente trasmesse via posta elettronica (cifrata), anche se talvolta si rende necessario l'uso del telefono o del fax.

Quando si ricevono informazioni via telefono, è buona prassi annotare subito ogni singolo dettaglio usando uno strumento di gestione/segnalazione degli incidenti oppure compilando un promemoria. È necessario generare immediatamente (prima della fine della chiamata) un numero incidente (se non esiste ancora per tale incidente) e comunicarlo alla persona al telefono (oppure tramite posta elettronica riassuntiva inviata in un secondo momento) come riferimento per ulteriori comunicazioni.

Il resto del capitolo descrive il processo di base per la gestione degli incidenti. Un'analisi molto approfondita del processo completo di gestione degli incidenti e di tutti i flussi di lavoro primari e secondari coinvolti è reperibile nella documentazione del CERT/CC *Definire i processi di gestione degli incidenti per i CSIRT*[24].

[24] Definire i processi di gestione degli incidenti: http://www.cert.org/archive/pdf/04tr015.pdf

Sostanzialmente la gestione degli incidenti adotta il seguente flusso di lavoro:

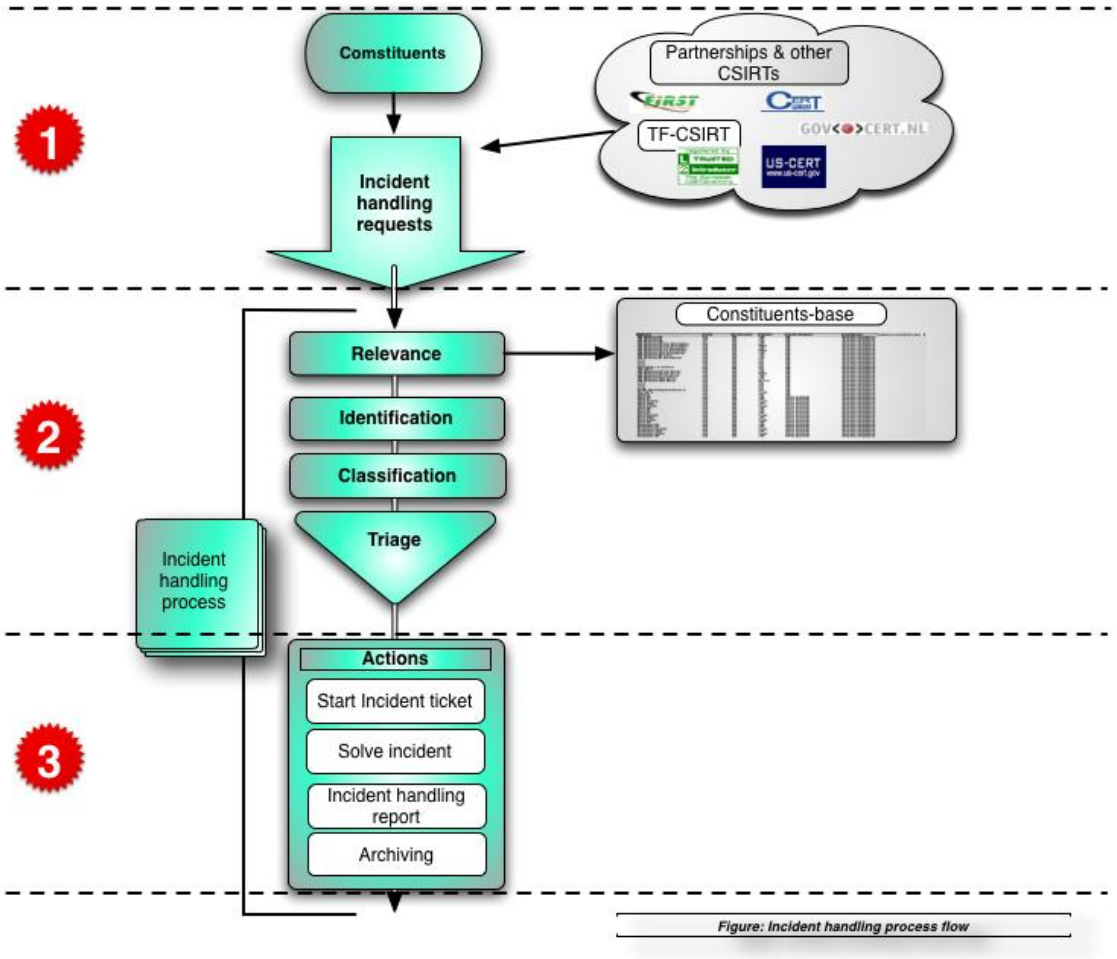


Fig. 13 Flusso del processo degli incidenti

Fase 1: Ricevere i rapporti sugli incidenti

Come sopra menzionato, i rapporti sugli incidenti raggiungono un CSIRT attraverso diversi canali, soprattutto via posta elettronica ma anche tramite telefono o fax.

È buona prassi annotare tutti i dettagli in forma fissa mentre si riceve un rapporto su un incidente. Così facendo si evita di tralasciare informazioni importanti. Di seguito è riportato uno schema campione:

MODULO DI SEGNALAZIONE DEGLI INCIDENTI

Compilare questo modulo e inviarlo tramite fax o posta elettronica a: ……..
I campi contrassegnati con un asterisco (*) sono obbligatori.

Nome e organizzazione
1. Nome*:
2. Denominazione dell'organizzazione*:
3. Tipo di settore:
4. Paese*:
5. Città:
6. Indirizzo di posta elettronica*:
7. Numero di telefono*:
8. Altro:

*Server o computer (*host) *interessato/i*
9. Numero di host:
10. Nome dell'host & IP*:
11. Funzione dell'host*:
12. Fuso orario:
13. Hardware:
14. Sistema operativo:
15. Software colpito:
16. File colpiti:
17. Sicurezza:
18. Nome dell'host & IP:
19. Protocollo/porta:

Incidente:
20. Numero di riferimento # rif:
21. Tipo di incidente:
22. Incidente iniziato:
23. Questo è un incidente in corso: SÌ NO
24. Tempo e metodo di scoperta:
25. Vulnerabilità note:
26. File sospetti:
27. Contromisure:
28. Descrizione dettagliata*:

Fig. 14 Contenuto di un rapporto su un incidente



Fase 2: Valutazione dell'incidente

In questa fase si verificano l'autenticità e la pertinenza di un incidente segnalato e si classifica l'incidente.

Identificazione

Al fine di prevenire qualunque azione non necessaria, è buona prassi verificare se l'autore è affidabile ed è uno dei vostri utenti di riferimento o di un CSIRT collega. Si applicano regole analoghe a quelle descritte nel capitolo *8.2 Generare allarmi*.

Pertinenza

In questa fase si verifica se la richiesta di gestione dell'incidente proviene dalla comunità di riferimento del CSIRT o se l'incidente segnalato coinvolge sistemi IT della comunità di riferimento. Se non è questo il caso, il rapporto viene solitamente reindirizzato al giusto CISRT[25].

Classificazione

In questa fase si prepara il triage, classificando l'incidente per gravità. L'approfondimento dei dettagli della classificazione degli incidenti va oltre l'ambito di questo documento. Un buon punto di partenza consiste nell'utilizzare lo schema di classificazione dei casi CSIRT (esempio per un CSIRT aziendale):

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 Schema di classificazione degli incidenti (fonte: FIRST)[26]

[25] Strumenti per controllare le identità in CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] Classificazione dei casi CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

Triage

Il triage (o categorizzazione) è un sistema usato in campo medico o in caso di emergenza per razionare le limitate risorse mediche quando il numero di feriti bisognosi di cure supera le risorse disponibili per fornire assistenza, in modo da riuscire a trattare il maggior numero possibile di pazienti[27].

Il CERT/CC fornisce la seguente descrizione:

Il triage è un elemento essenziale di qualunque funzione di gestione degli incidenti, in particolare per qualsiasi CSIRT costituito. Il triage si inserisce nel percorso critico per comprendere cosa viene segnalato attraverso tutta l'organizzazione. Esso funge da veicolo tramite il quale tutte le informazioni confluiscono verso un unico punto di contatto, rendendo possibile una visione aziendale dell'attività in corso e una correlazione completa di tutti i dati segnalati. Il triage consente una valutazione iniziale di un rapporto in entrata e lo mette in coda per l'ulteriore elaborazione. Esso offre inoltre un contesto per avviare la documentazione iniziale e l'inserimento dei dati di un rapporto o richiesta, ove ciò non sia già avvenuto nel processo di rilevamento.

La funzione di triage offre un'istantanea immediata della situazione corrente di tutte le attività segnalate: quali rapporti sono aperti o chiusi, quali azioni sono in corso e quanti rapporti di ogni tipo sono stati ricevuti. Questo processo può aiutare a individuare i problemi potenziali di sicurezza e a stabilire le priorità nel carico di lavoro. Le informazioni raccolte in tal modo possono essere usate anche per generare tendenze e statistiche delle vulnerabilità e degli incidenti per gli alti dirigenti[28]*.*

Il triage deve essere effettuato solamente dai membri più esperti del gruppo, in quanto richiede una profonda comprensione degli impatti potenziali degli incidenti su parti specifiche della comunità di riferimento e la capacità di decidere quale sia il membro del gruppo più adatto a gestire l'incidente in questione.

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

[28] Definire i processi di gestione degli incidenti: http://www.cert.org/archive/pdf/04tr015.pdf



Fase 3: Azioni

In genere gli incidenti categorizzati vengono inseriti in una coda di richiesta all'interno di uno strumento di gestione degli incidenti utilizzato da una o più persone incaricate della gestione, che si attengono sostanzialmente ai seguenti passaggi.

Creare il ticket dell'incidente
Il numero di ticket dell'incidente potrebbe essere già stato generato in una fase precedente (per esempio quando l'incidente è stato segnalato al telefono). In caso contrario, il primo passaggio consiste nel creare tale numero che verrà usato in tutte le ulteriori comunicazioni in merito a questo incidente.

Ciclo vitale dell'incidente
La gestione di un incidente non segue una linea di passaggi che portano a una soluzione, bensì segue piuttosto un ciclo di passaggi che si applicano ripetutamente finché l'incidente non viene definitivamente risolto e tutte le parti coinvolte ottengono tutte le informazioni necessarie. Tale ciclo, spesso denominato anche "ciclo vitale dell'incidente", contiene i seguenti processi:

Analisi:	Tutti i dettagli dell'incidente segnalato vengono analizzati.
Ottenere informazioni sui contatti:	Per poter diramare informazioni sull'incidente a tutte le parti coinvolte, come altri CSIRT, vittime e probabilmente i proprietari dei sistemi che possono essere stati oggetto di abuso per un attacco.
Fornire assistenza tecnica:	Aiutare le vittime a riprendersi rapidamente dalle conseguenze dell'incidente e raccogliere più informazioni sull'attacco.
Coordinamento:	Informare le altre parti coinvolte, come il CSIRT responsabile del sistema IT usato per un attacco, o altre vittime.

Questa struttura viene chiamata "ciclo vitale" perché un passaggio porta al seguente e l'ultimo, la parte relativa al coordinamento, potrebbe di nuovo portare a un'analisi e riavviare il ciclo. Il processo termina quando tutte le parti coinvolte hanno ricevuto e riferito tutte le informazioni necessarie.

Per una descrizione più dettagliata del ciclo vitale degli incidenti, si rimanda al manuale CSIRT del CERT/CC [29].

Rapporto sulla gestione degli incidenti
Prepararsi alle domande della direzione sugli incidenti compilando un rapporto. È anche buona prassi redigere un documento (ad esclusivo uso interno) sulle "conoscenze acquisite" da trasmettere al personale ed evitare errori nei futuri processi di gestione degli incidenti.

[29] Manuale CSIRT: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Archiviazione
Consultare le regole sull'archiviazione precedentemente descritte nel capitolo *6.6 Sviluppare una politica di sicurezza dell'informazione*.

Si rimanda all'Allegato sezione *A.1 Ulteriori letture* per una guida completa sulla gestione degli incidenti e sul ciclo vitale degli incidenti.

8.4 Un modello dei tempi di risposta

La definizione dei tempi di risposta viene spesso trascurata, ma deve far parte di ogni accordo sul livello di servizio ben strutturato tra un CSIRT e la sua comunità di riferimento. Fornire un riscontro puntuale agli utenti di riferimento durante la gestione degli incidenti è essenziale sia per le responsabilità proprie degli utenti di riferimento sia per la reputazione del gruppo.
I tempi di risposta devono essere comunicati chiaramente alla comunità di riferimento onde evitare aspettative errate. Il seguente calendario molto essenziale può essere usato come punto di partenza per un SLA più dettagliato con la comunità di riferimento di un CSIRT.

Di seguito è riportato un esempio di un calendario pratico di risposta dal momento dell'arrivo di una richiesta di assistenza:

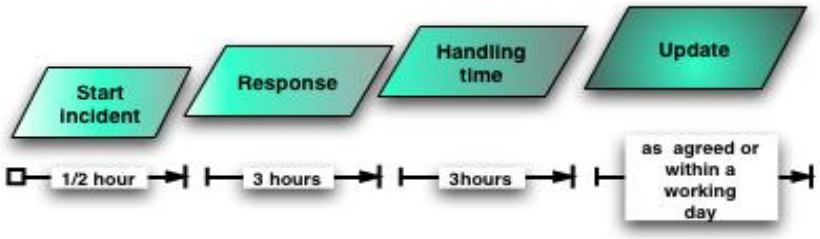


Fig. 16 Esempio di calendario di risposta

È anche buona prassi istruire la comunità di riferimento in merito ai suoi tempi di risposta, soprattutto per quando contattare il CSIRT in caso di emergenza. Nella maggior parte dei casi è meglio contattare il CSIRT in una fase iniziale ed è buona prassi incoraggiare la comunità di riferimento a farlo in caso di dubbio.

Strumenti a disposizione dei CSIRT

Questo capitolo fornisce alcune indicazioni sugli strumenti comuni usati dai CSIRT. Esso riporta soltanto esempi; maggiori indicazioni sono reperibili in *Clearinghouse of Incident Handling Tools*[30] (CHIHT).

Software di cifratura dei messaggi e dei messaggi di posta elettronica
- GnuPG http://www.gnupg.org/

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

GnuPG è l'implementazione gratuita e completa da parte del progetto GNU dello standard OpenPGP secondo la definizione data in RFC2440. GnuPG permette di cifrare e firmare i propri dati e comunicazioni.

- PGP http://www.pgp.com/
  Variante commerciale

Strumento di gestione degli incidenti
Gestire gli incidenti e le loro conseguenze, tenendosi aggiornati sulle azioni.

- RTIR http://www.bestpractical.com/rtir/
  RTIR è un sistema di gestione degli incidenti free open source (ovvero relativi a software basati sull'apertura del codice sorgente e sulla sua libera circolazione), progettato tenendo conto delle esigenze dei gruppi CERT e di altri gruppi di risposta agli incidenti.

Strumenti CRM
Una banca dati CRM (*customer relationship management*, sistema di gestione delle relazioni con il cliente) può essere utile in presenza di molti utenti di riferimento diversi per cui è necessario gestire incontri e dettagli. Di seguito sono riportati alcuni esempi delle diverse varianti disponibili:

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

- Sugarforce (versione free open source) http://www.sugarforge.org/

Verifica delle informazioni
- Website watcher http://www.aignes.com/index.htm
  Questo programma monitora gli aggiornamenti e le modifiche dei siti web.

- Watch that page http://www.watchthatpage.com/
  Il servizio invia informazioni sui cambiamenti intervenuti nei siti web tramite posta elettronica (gratuite e commerciali).

Trovare le informazioni sui contatti
Trovare il giusto contatto cui segnalare gli incidenti non è compito facile. A tal fine si possono usare un paio di fonti d'informazione:

- RIPE[31]
- IRT-object[32]
- TI[33]

CHIHT elenca inoltre alcuni strumenti per reperire le informazioni sui contatti[34].

CSIRT simulato (fase 8)
Stabilire flussi di processo e procedure operative e tecniche Il CSIRT simulato si concentra sull'erogazione di servizi CSIRT chiave: • Allarmi e avvisi • Annunci • Gestione degli incidenti Il gruppo ha sviluppato procedure funzionanti e facilmente comprensibili per ogni membro del gruppo. Il CSIRT simulato ha anche assunto un esperto legale che si occuperà degli aspetti riguardanti responsabilità e politica di sicurezza dell'informazione. Discutendo con altri CSIRT, il gruppo ha adottato alcuni strumenti utili e reperito informazioni interessanti sulle questioni operative. È stato generato un modello fisso per i bollettini informativi sulla sicurezza e i rapporti sugli incidenti. Il gruppo utilizza RTIR per la gestione degli incidenti.

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

[32] IRT-object nella banca dati 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] Strumenti per controllare le identità in CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Formazione CSIRT

Fasi svolte:

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?
3. Quali tipi di servizi può offrire un CSIRT alla sua comunità di riferimento.
4. Analisi dell'ambiente e degli utenti di riferimento.
5. Definizione del mandato.
6. Sviluppare il piano di attività.
   a. Definire il modello finanziario
   b. Definire la struttura organizzativa
   c. Iniziare ad assumere personale
   d. Utilizzare e attrezzare l'ufficio
   e. Sviluppare una politica di sicurezza dell'informazione
   f. Cercare partner di cooperazione
7. Promuovere il piano di attività.
   a. Ottenere l'approvazione del business case (o giustificazioni specifiche)
   b. Inserire tutto in un piano di attuazione del progetto
8. Rendere il CSIRT operativo.
   a. Creare flussi di lavoro
   b. Attuare gli strumenti CSIRT

>> La prossima fase consiste nel formare il personale

Questo capitolo elenca due fonti principali per una formazione CSIRT dedicata: TRANSITS e i corsi CERT/CC.

9.1 TRANSITS

TRANSITS è un progetto europeo volto a promuovere la creazione di Computer Security Incident Response Team (CSIRT) e a potenziare i CSIRT esistenti affrontando il problema della carenza di personale CSIRT competente. Questo obiettivo viene perseguito offrendo corsi di formazione specialistica per formare il personale dei (nuovi) CSIRT sulle materie organizzative, operative, tecniche, di mercato e giuridiche interessate dai servizi CSIRT.

In particolare, TRANSITS ha:

- sviluppato, aggiornato e rivisto regolarmente il materiale modulare dei corsi di formazione;
- organizzato laboratori di formazione in cui è stato distribuito il materiale dei corsi;
- consentito la partecipazione dei membri del personale dei (nuovi) CSIRT a questi laboratori di formazione, con particolare attenzione alla partecipazione dei nuovi Stati dell'UE;
- distribuito i materiali dei corsi di formazione e garantito lo sfruttamento dei risultati[35].

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

L'ENISA favorisce e sostiene i corsi TRANSITS. Per sapere come presentare domanda per i corsi e quali sono i requisiti e i costi, contattare gli esperti CSIRT dell'ENISA all'indirizzo:

CERT-Relations@enisa.europa.eu

L'allegato al presente documento contiene del materiale campione per i corsi.

9.2 CERT/CC

La complessità delle infrastrutture informatiche e di rete e il difficile compito amministrativo intralciano una gestione adeguata della sicurezza di rete. Gli amministratori di rete e di sistema non hanno a disposizione personale e prassi di sicurezza sufficienti per difendersi dagli attacchi e ridurre al minimo i danni. Ciò determina un numero crescente di incidenti di sicurezza informatica.
Quando tali incidenti si verificano, le organizzazioni devono rispondere in maniera rapida ed efficace. Quanto più tempestivamente un'organizzazione riconosce, analizza e risponde a un incidente, tanto meglio riuscirà a limitare i danni e a ridurre i costi di ripristino. Costituire un Computer Security Incident Response Team (CSIRT) è il modo ideale per fornire questa funzione di risposta rapida e aiutare a prevenire incidenti futuri.

Il CERT-CC offre corsi per i dirigenti e il personale tecnico in aree quali la creazione e gestione di Computer Security Incident Response Team (CSIRT), la risposta e analisi degli incidenti di sicurezza e il miglioramento della sicurezza di rete. Salvo altrimenti indicato, tutti i corsi si tengono a Pittsburgh, PA. I membri del nostro personale tengono inoltre corsi sulla sicurezza presso la Carnegie Mellon University.

Corsi CERT/CC disponibili[36] dedicati ai CSIRT

Creare un Computer Security Incident Response Team (CSIRT)
Gestire i Computer Security Incident Response Team (CSIRT)
Fondamenti della gestione degli incidenti
Gestione avanzata degli incidenti per il personale tecnico

L'allegato al presente documento contiene del materiale campione per i corsi.

CSIRT simulato (fase 9)
Formare il personale Il CSIRT simulato decide di inviare tutto il suo personale tecnico ai prossimi corsi TRANSITS disponibili. Il responsabile del gruppo frequenta inoltre il corso *Gestire un CSIRT* organizzato dal CERT/CC.

[36] Corsi CERT/CC: http://www.sei.cmu.edu/products/courses

10 Esercizio: produrre un bollettino informativo

Fasi svolte:

1. Capire cos'è un CSIRT e quali vantaggi può offrire.
2. A quale settore il nuovo gruppo fornirà i suoi servizi?
3. Quali tipi di servizi può offrire un CSIRT alla sua comunità di riferimento.
4. Analisi dell'ambiente e degli utenti di riferimento.
5. Definizione del mandato.
6. Sviluppare il piano di attività.
   a. Definire il modello finanziario
   b. Definire la struttura organizzativa
   c. Iniziare ad assumere personale
   d. Utilizzare e attrezzare l'ufficio
   e. Sviluppare una politica di sicurezza dell'informazione
   f. Cercare partner di cooperazione
7. Promuovere il piano di attività.
   a. Ottenere l'approvazione del business case (o giustificazioni specifiche)
   b. Inserire tutto in un piano di attuazione del progetto
8. Rendere il CSIRT operativo.
   a. Creare flussi di lavoro
   b. Attuare gli strumenti CSIRT
9. Formare il personale

>> La prossima fase consisterà nell'esercitarsi e prepararsi al lavoro reale!

A titolo illustrativo, questo capitolo propone un esercizio campione per un compito rientrante fra quelli che un CSIRT svolge quotidianamente, vale a dire la creazione di un bollettino informativo sulla sicurezza.

Lo spunto è venuto dal seguente bollettino informativo originale sulla sicurezza inviato da Microsoft:

Identificativo bollettino	**Bollettino sulla sicurezza di Microsoft MS06-042**
Titolo del bollettino	**Aggiornamento cumulativo sulla sicurezza per Internet Explorer (918899)**
Sintesi	Questo aggiornamento risolve diverse vulnerabilità presenti in Internet Explorer che potrebbero consentire l'esecuzione di codice da remoto.
Valutazione della gravità massima	Critico
Impatto della vulnerabilità	Esecuzione di codice da remoto
Software colpito	**Windows, Internet Explorer.** Per ulteriori informazioni, cfr. la sezione Software colpito e locazioni per il download.

Questo bollettino del venditore riguarda una vulnerabilità scoperta di recente in Internet Explorer. Il venditore pubblica correzioni multiple per questo software per versioni multiple di Microsoft Windows.

Il CSIRT simulato, dopo aver ricevuto l'informazione sulla vulnerabilità attraverso una mailing list, avvia il processo illustrato nel capitolo *8.2 Generare allarmi, avvisi e annunci*.

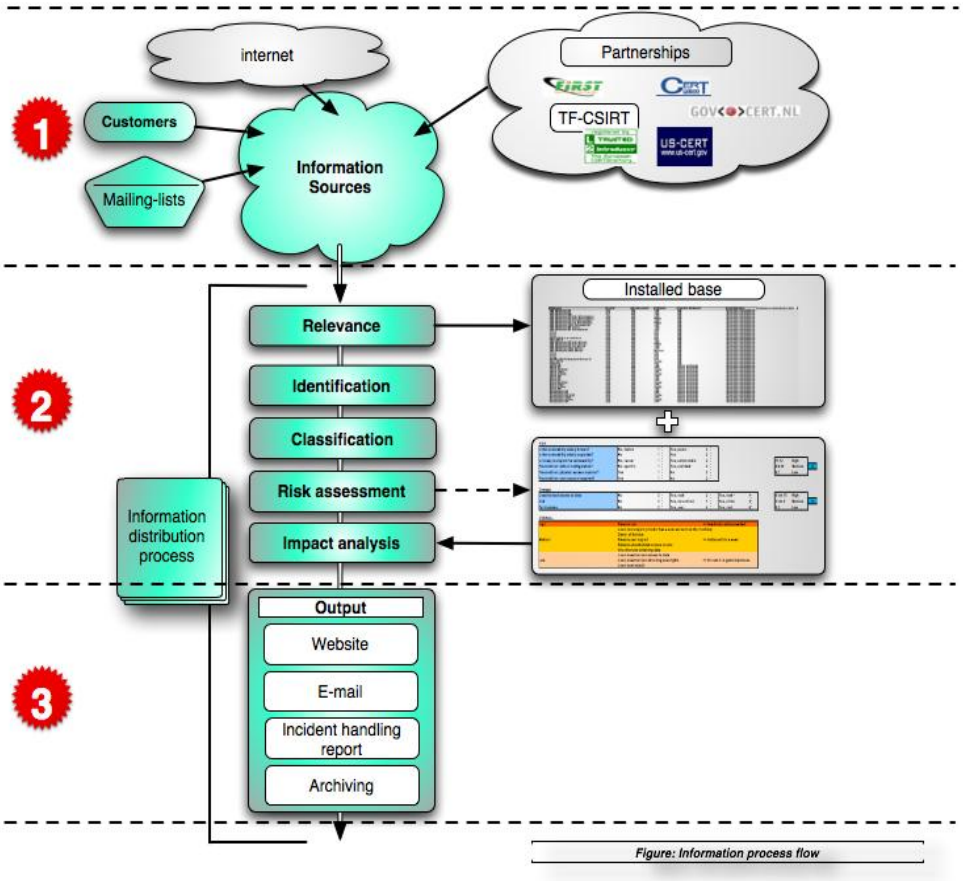


Figure: Information process flow

1 Fase 1: Raccogliere informazioni sulle vulnerabilità.

Il primo passo consiste nel visitare il sito web del venditore. Qui il CSIRT simulato verifica l'autenticità dell'informazione e raccoglie ulteriori dettagli sulla vulnerabilità e sui sistemi IT colpiti.



Fase 2: Valutazione delle informazioni e valutazione del rischio

Identificazione
L'informazione è già stata verificata tramite controllo incrociato dell'informazione sulla vulnerabilità ricevuta via posta elettronica con il testo pubblicato sul sito web del venditore.

Pertinenza
Il CSIRT simulato confronta l'elenco dei sistemi colpiti reperito sul sito web con l'elenco dei sistemi utilizzati nella comunità di riferimento. Poiché almeno uno degli utenti di riferimento utilizza Internet Explorer, l'informazione sulla vulnerabilità è rilevante.

Categoria	Applicazione	Prodotto software	Versione	OS	Versione OS	Utente di riferimento
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A

Classificazione
L'informazione è di pubblico dominio e può quindi essere usata e ridistribuita.

Valutazione del rischio e analisi dell'impatto
Le risposte alle domande mostrano che il rischio e l'impatto sono *alti* (giudicati *critici* da Microsoft).

RISCHIO

La vulnerabilità è notoria?	Sì
La vulnerabilità è diffusa?	Sì
È facile sfruttare la vulnerabilità?	Sì
È una vulnerabilità sfruttabile a distanza?	Sì

DANNO
Gli impatti possibili sono l'accessibilità remota e, potenzialmente, l'esecuzione di codice da remoto. Questa vulnerabilità comprende aspetti multipli che rendono *alto* il rischio di danno.



Fase 3: Distribuzione

Il CSIRT simulato è un CSIRT interno. Utilizza la posta elettronica, il telefono e il sito web interno come canali di comunicazione. Il CSIRT produce questo bollettino informativo, tratto dal modello contenuto nel capitolo *8.2 Generare allarmi, avvisi e annunci*.

Titolo del bollettino informativo
Vulnerabilità multiple rinvenute in Internet Explorer

Numero di riferimento
082006-1
Sistemi colpiti

- Tutti i sistemi desktop che utilizzano Microsoft

OS correlato + versione

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 e Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 e Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 per sistemi basati su Itanium e Microsoft Windows Server 2003 con SP1 per sistemi basati su Itanium
- Microsoft Windows Server 2003 x64 Edition

Rischio (alto-medio-basso)
ALTO
Impatto/danno potenziale (alto-medio-basso)
ALTO
ID esterni: (CVE, ID dei bollettini sulle vulnerabilità)
MS-06-42

Panoramica delle vulnerabilità
Microsoft ha rinvenuto diverse vulnerabilità critiche in Internet Explorer che possono determinare un'esecuzione di codice da remoto.

Impatto
Un aggressore potrebbe assumere il pieno controllo del sistema, installando programmi, aggiungendo utenti e visualizzando, modificando e cancellando dati. Il fattore attenuante è che questo può accadere soltanto se l'utente ha effettuato il log-in con diritti di amministratore. Gli utenti che effettuano il log-in con diritti minori potrebbero essere meno colpiti.

Soluzione
Installare immediatamente la patch (connessione provvisoria) per IE

Descrizione (dettagli)
Per maggiori informazioni cfr. ms06-042.mspx

Appendice

Per maggiori informazioni cfr. ms06-042.mspx

Il bollettino informativo è ora disponibile per la distribuzione. Trattandosi di un bollettino critico, è consigliabile chiamare anche gli utenti di riferimento ove possibile.

CSIRT simulato (fase 10)

Esercitarsi

Durante le prime settimane di attività, il CSIRT simulato si è avvalso di una serie di casi tipo (ricevuti come esempi da altri CSIRT) per esercitarsi. Ha inoltre emesso un paio di bollettini informativi sulla sicurezza in base alle reali informazioni sulle vulnerabilità distribuite dai venditori di hardware e software, dopo averle affinate e adeguate alle esigenze della comunità di riferimento.

11 Conclusione

La guida termina qui. Il presente documento intende fornire una sintesi generale dei processi necessari per creare un CSIRT, senza pretese di esaustività e senza dilungarsi eccessivamente in dettagli specifici. A tal fine, si rimanda alla sezione *A.1 Ulteriori letture* nell'allegato per la letteratura consigliata sull'argomento.

A questo punto, le fasi successive per il CSIRT simulato sarebbero:

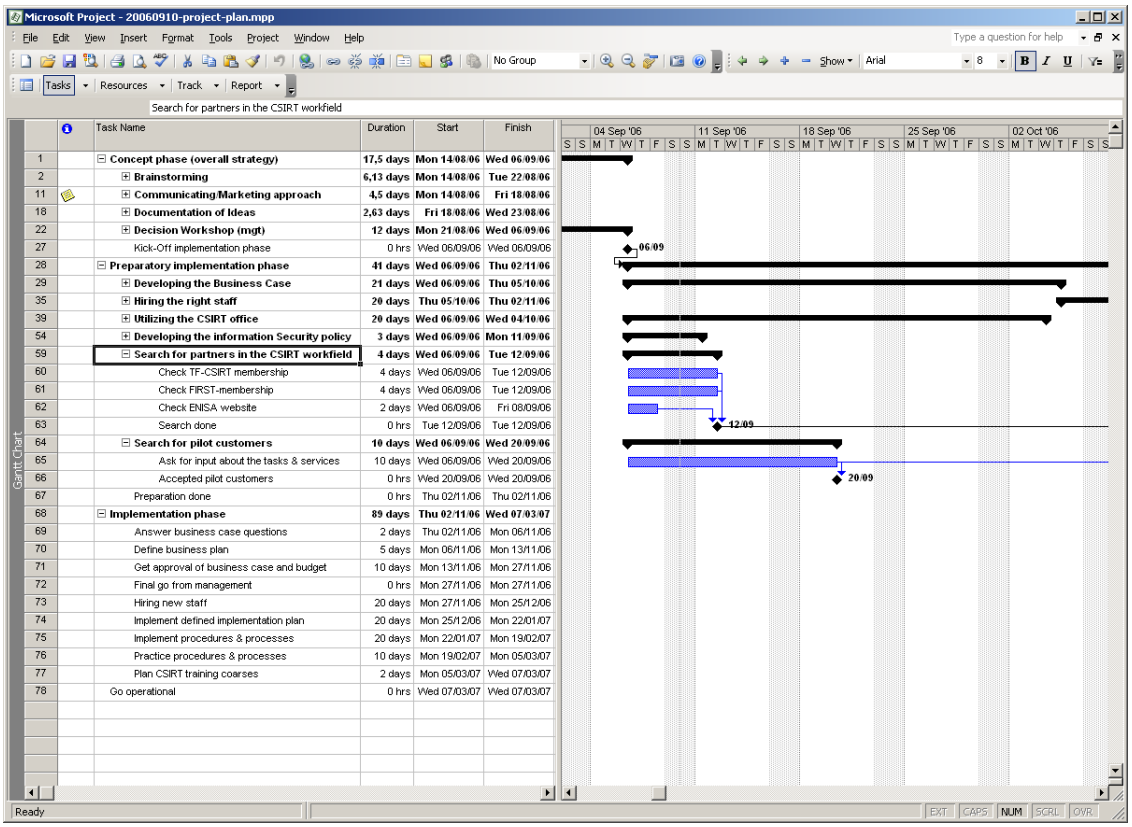
- Ricevere un riscontro dalla comunità di riferimento per affinare i servizi forniti
- Entrare nella routine del lavoro giornaliero
- Esercitarsi in situazioni di emergenza
- Tenersi in stretto contatto con le varie comunità CSIRT al fine di contribuire un giorno al loro lavoro volontario.

12 Descrizione del piano di attuazione del progetto

NOTA: Il piano di attuazione del progetto è una prima stima del tempo necessario. A seconda delle risorse disponibili, la durata reale del progetto potrebbe essere diversa.

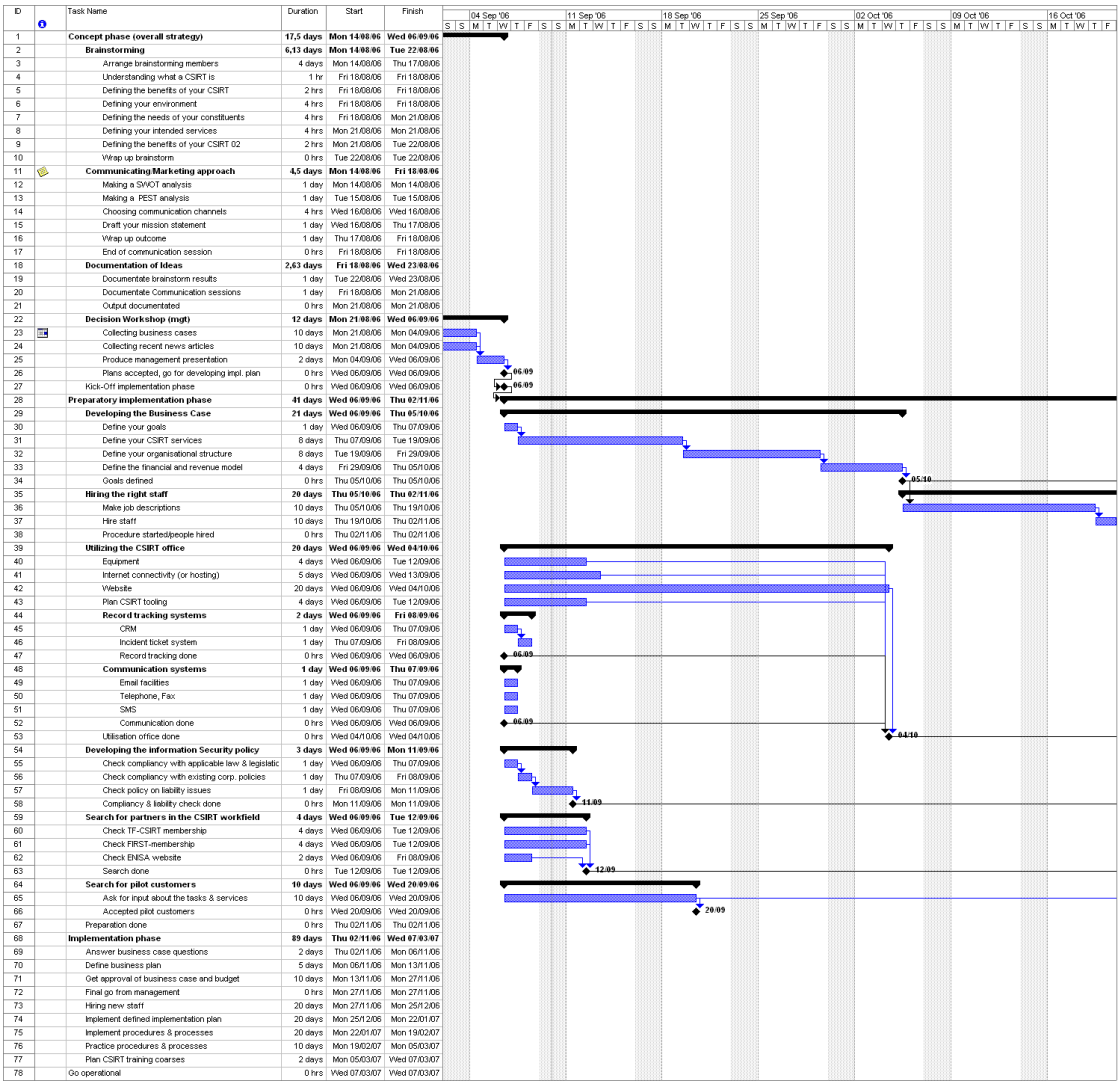
Il piano di attuazione del progetto è disponibile in diversi formati su CD e sul sito web dell'ENISA. Esso comprende tutti i processi descritti nel presente documento.

Il formato principale sarà Microsoft Project, che potrà quindi essere usato direttamente in questo strumento di gestione dei progetti.



	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
11	Communicating/Marketing approach	4,5 days	Mon 14/08/06	Fri 18/08/06
18	Documentation of Ideas	2,63 days	Fri 18/08/06	Wed 23/08/06
22	Decision Workshop (mgt)	12 days	Mon 21/08/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	Preparatory implementation phase	41 days	Wed 06/09/06	Thu 02/11/06
29	Developing the Business Case	21 days	Wed 06/09/06	Thu 05/10/06
35	Hiring the right staff	20 days	Thu 05/10/06	Thu 02/11/06
39	Utilizing the CSIRT office	20 days	Wed 06/09/06	Wed 04/10/06
54	Developing the information Security policy	3 days	Wed 06/09/06	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 coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Fig. 17 Piano di attuazione del progetto



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**	**41 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	Utilisation office 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 coarses	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 Il piano di attuazione del progetto con tutti i compiti e una parte del diagramma di Gant

Il piano di attuazione del progetto è disponibile anche in formato CVS e XML. Ulteriori utilizzi possono essere richiesti agli esperti CSIRT dell'ENISA all'indirizzo: CERT-Relations@enisa.europa.eu

APPENDICE

A.1 Ulteriori letture

Handbook for CSIRTs (Manuale per CSIRT) **(CERT/CC)**
Un testo di riferimento molto completo per tutti gli argomenti rilevanti per il lavoro di un CSIRT
Fonte: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress
(Definire i processi di gestione degli incidenti per CSIRT: lavori in corso)
Un'analisi approfondita della gestione degli incidenti
Fonte: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs)
(La prassi attuale dei CSIRT)
Un'analisi completa della situazione effettiva inerente al panorama mondiale dei CSIRT, compresa la storia, le statistiche e molto altro
Fonte: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Una descrizione completa degli insegnamenti tratti dalla creazione di GOVCERT.NL e "De Waarschuwingsdienst", il servizio di allarme nazionale olandese
Fonte: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response
(RFS 2350: le aspettative nella risposta a incidenti di sicurezza informatica)
Fonte: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide
(NIST: guida alla gestione degli incidenti di sicurezza informatica)
Fonte: http://www.securityunit.com/publications/sp800-61.pdf

Inventario delle attività CERT in Europa dell'ENISA
Un testo di riferimento che elenca le informazioni sui CSIRT in Europa e sulle loro varie attività
Fonte: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: National Institute of Standards and Technologies

A.2 Servizi CSIRT

Un ringraziamento speciale va al CERT/CC, che ha fornito questo elenco

Servizi reattivi	***Servizi proattivi***	***Gestione degli artefatti***
• Allarmi e avvisi • Gestione degli incidenti • Analisi degli incidenti • Risposta agli incidenti in loco • Sostegno della risposta agli incidenti • Coordinamento della risposta agli incidenti • Gestione delle vulnerabilità • Analisi delle vulnerabilità • Risposta alle vulnerabilità • Coordinamento della risposta alle vulnerabilità	• Annunci • Controllo tecnologico • Revisioni e valutazioni della sicurezza • Configurazione e mantenimento della sicurezza • Sviluppo di strumenti di sicurezza • Servizi di rilevamento intrusioni • Divulgazione di informazioni relative alla sicurezza	• Artifact analysis • Analisi degli artefatti • Coordinamento della risposta agli artefatti ***Gestione della qualità della sicurezza*** • Analisi dei rischi • Continuità operativa e ripristino in caso di disastro • Consulenza sulla sicurezza • Sensibilizzazione • Istruzione/formazione • Valutazione o certificazione dei prodotti

Fig. 19 Elenco dei servizi CSIRT da CERT/CC

Descrizioni dei servizi

Servizi reattivi

I servizi reattivi sono concepiti per rispondere alle richieste di assistenza, ai rapporti sugli incidenti provenienti dalla comunità di riferimento CSIRT e a qualunque rischio o attacco nei confronti dei sistemi CSIRT. Alcuni servizi possono prendere origine da notifiche di terzi o dalla visualizzazione di log e allarmi IDS e di monitoraggio.

Allarmi e avvisi

Questo servizio consiste nel divulgare informazioni che descrivono un attacco di intrusi, vulnerabilità della sicurezza, allarme di intrusione, virus o hoax informatico e nel raccomandare azioni a breve termine per la risoluzione del relativo problema. L'allarme, avviso o bollettino informativo viene inviato sotto forma di reazione al problema corrente per informare gli utenti di riferimento dell'attività e fornire un orientamento alla protezione dei loro sistemi o al ripristino dei sistemi che sono stati colpiti. L'informazione può essere creata dal CSIRT oppure ridistribuita dai venditori, altri CSIRT, esperti di sicurezza o altre parti della comunità di riferimento.

Gestione degli incidenti

La gestione degli incidenti comprende il ricevimento, il triage (o categorizzazione) e la risposta a richieste e rapporti nonché l'analisi di incidenti ed eventi. Particolari attività di risposta consistono

- nell'intraprendere azioni per proteggere i sistemi e le reti colpite o minacciate dall'attività di intrusi;
- nel fornire soluzioni e strategie di attenuazione attraverso i relativi bollettini informativi o allarmi;
- nel cercare l'attività di intrusi in altre parti della rete;
- nel filtrare il traffico di rete;
- nel ricostruire i sistemi;
- nell'installare patch (connessioni provvisorie) o riparare i sistemi;
- nello sviluppare altre strategie di risposta o espedienti.

Poiché le attività di gestione degli incidenti sono svolte in vario modo da tipi diversi di CSIRT, questo servizio viene ulteriormente categorizzato, in base al tipo di attività svolta e al tipo di assistenza fornita, nel modo qui di seguito.

Analisi degli incidenti

Esistono molti livelli di analisi degli incidenti e molti sottoservizi. Sostanzialmente, l'analisi degli incidenti è un esame di tutte le informazioni e prove disponibili o degli artefatti relativi a un incidente o evento. Lo scopo dell'analisi consiste nell'individuare la portata dell'incidente, l'estensione del danno provocato dall'incidente, la natura dell'incidente e le strategie di risposta o espedienti disponibili. Il CSIRT può utilizzare i risultati dell'analisi delle vulnerabilità e degli artefatti (descritta di seguito) per comprendere e fornire l'analisi più completa e aggiornata possibile di ciò che è accaduto in un sistema specifico. Il CSIRT mette in correlazione l'attività tra gli incidenti al fine di determinare qualunque interrelazione, tendenza, modello o firma di intrusi. Due sottoservizi che possono rientrare nell'analisi degli incidenti, a seconda del compito, degli obiettivi e dei processi del CSIRT, sono i seguenti.

Raccolta di prove forensi

La raccolta, conservazione, documentazione e analisi delle prove relative a un sistema informatico compromesso per determinare i cambiamenti intervenuti nel sistema e collaborare alla ricostruzione degli eventi che hanno portato a questa situazione. Tale raccolta di informazioni e prove deve avvenire in un modo che documenti una catena dimostrabile di custodia ammissibile davanti a un tribunale ai sensi delle norme in materia di elementi probatori. I compiti rientranti nella raccolta di prove forensi comprendono (ma non solo) la realizzazione di una copia in immagine bit del disco rigido del sistema colpito; la verifica dei cambiamenti intervenuti nel sistema, come nuovi programmi, file, servizi e utenti; l'osservazione dei processi in atto e delle porte aperte e la ricerca di cavalli di Troia e kit di strumenti. Il personale del CSIRT che svolge questa funzione può anche dover essere preparato a intervenire quale teste esperto in procedure giurisdizionali.

Individuazione o monitoraggio

Il monitoraggio delle origini di un intruso o l'identificazione dei sistemi cui l'intruso ha avuto accesso. Questa attività può comprendere l'individuazione o il monitoraggio di

come l'intruso è entrato nei sistemi colpiti e nelle reti correlate, di quali sistemi sono stati usati per ottenere tale accesso, di dove l'attacco ha avuto origine e di quali altri sistemi e reti sono stati usati nell'ambito dell'attacco. Può inoltre consistere nel tentativo di determinare l'identità dell'intruso. Questo lavoro può essere svolto autonomamente, ma in genere presuppone la collaborazione con personale di polizia, fornitori di servizi Internet o altre organizzazioni coinvolte.

Risposta agli incidenti in loco

Il CSIRT fornisce assistenza diretta in loco per aiutare gli utenti di riferimento a riprendersi da un incidente. Il CSIRT stesso analizza fisicamente i sistemi colpiti ed effettua la riparazione e il ripristino dei sistemi, anziché limitarsi a fornire assistenza nella risposta agli incidenti via telefono o posta elettronica (cfr. di seguito). Questo servizio comprende tutte le azioni intraprese a livello locale e necessarie in caso di sospetto o effettivo verificarsi di un incidente. Qualora il CSIRT non si trovi presso il sito interessato, i membri del gruppo si recheranno in loco per rispondere all'incidente. In altri casi un gruppo locale può essere già presente in loco e fornire la risposta agli incidenti nell'ambito del suo ordinario lavoro. Ciò accade soprattutto quando la gestione degli incidenti rientra nell'ambito delle normali funzioni degli amministratori di sistema, rete o sicurezza e non di un CSIRT.

Sostegno della risposta agli incidenti

Il CSIRT assiste e guida la/e vittima/e dell'attacco nel ripristino dopo un incidente via telefono, posta elettronica, fax o documentazione. Ciò può comprendere l'assistenza tecnica nell'interpretazione dei dati raccolti, la trasmissione di informazioni sui contatti o l'orientamento in termini di strategie di attenuazione e ripristino. Non sono comprese le azioni dirette di risposta agli incidenti in loco, come sopra descritto. Il CSIRT fornisce invece assistenza a distanza, in modo che il personale in loco possa effettuare personalmente il ripristino.

Coordinamento della risposta agli incidenti

Il CSIRT coordina gli sforzi di risposta tra le parti coinvolte nell'incidente. Queste comprendono solitamente la vittima dell'attacco, altri siti coinvolti nell'attacco e qualunque sito che richieda assistenza nell'analisi dell'attacco. Possono inoltre comprendere le parti che forniscono sostegno IT alla vittima, quali i fornitori di servizi Internet, altri CSIRT e gli amministratori di rete e sistema in loco. L'opera di coordinamento può includere la raccolta di informazioni sui contatti, la comunicazione ai siti del loro potenziale coinvolgimento (quali vittime o fonti di un attacco), la raccolta di statistiche sul numero di siti coinvolti e l'agevolazione dello scambio e analisi di informazioni. Parte dell'opera di coordinamento può riguardare la notifica e collaborazione con il consulente legale, le risorse umane o i dipartimenti preposti alle pubbliche relazioni di un'organizzazione, nonché con gli organi di polizia. Il servizio non presuppone la risposta diretta agli incidenti in loco.

Gestione delle vulnerabilità

La gestione delle vulnerabilità consiste nel ricevere informazioni e rapporti sulle vulnerabilità di hardware e software, analizzare la natura, la meccanica e gli effetti delle vulnerabilità e sviluppare strategie di risposta per rilevare e riparare le vulnerabilità. Poiché le attività di gestione delle vulnerabilità sono svolte in vario modo da tipi diversi di

CSIRT, questo servizio viene ulteriormente categorizzato, in base al tipo di attività svolta e al tipo di assistenza fornita, nel modo seguente.

Analisi delle vulnerabilità

Il CSIRT svolge l'analisi tecnica e l'esame delle vulnerabilità presenti in hardware e software. Sono compresi la verifica delle sospette vulnerabilità e l'esame tecnico della vulnerabilità dell'hardware o software per determinare dove essa risiede e come può essere sfruttata. L'analisi può comprendere la revisione del codice sorgente, usando un debugger (programma di correzione errori) per determinare dove ha luogo la vulnerabilità o cercando di riprodurre il problema in un sistema di prova.

Risposta alle vulnerabilità

Questo servizio consiste nel determinare la risposta appropriata per attenuare o riparare la vulnerabilità e può includere lo sviluppo o la ricerca di patch (connessioni provvisorie), fix ed espedienti. Comprende anche la notifica della strategia di attenuazione ad altri soggetti, possibilmente attraverso la creazione e distribuzione di bollettini informativi o allarmi. Questo servizio di risposta può prevedere anche l'installazione di patch, fix o espedienti.

Coordinamento della risposta alle vulnerabilità

Il CSIRT informa le varie parti dell'impresa o della comunità di riferimento in merito alla vulnerabilità e condivide le informazioni su come correggere o attenuare la vulnerabilità. Verifica inoltre che la strategia di risposta alle vulnerabilità sia stata attuata correttamente. Il servizio può comprendere la comunicazione con i venditori, altri CSIRT, esperti tecnici, membri della comunità di riferimento e gli individui o gruppi che hanno inizialmente scoperto o segnalato la vulnerabilità. Le attività consistono nell'agevolare l'analisi di una vulnerabilità o di un rapporto sulle vulnerabilità, nel coordinare i programmi di emissione dei documenti, patch (connessioni provvisorie) o espedienti corrispondenti e nel sintetizzare l'analisi tecnica effettuata da parti diverse. Il servizio può inoltre comprendere il mantenimento di un archivio pubblico o privato o di una base di conoscenze relative alle informazioni sulle vulnerabilità e alle corrispondenti strategie di risposta.

Gestione degli artefatti

Un artefatto è qualunque file od oggetto rinvenuto in un sistema che potrebbe essere coinvolto nell'esplorazione o nell'attacco di sistemi e reti, oppure che viene utilizzato per sconfiggere misure di sicurezza. Gli artefatti possono comprendere, ma non solo, virus informatici, cavalli di Troia, worm, exploit script e kit di strumenti.
La gestione degli artefatti consiste nel ricevere informazioni e copie inerenti agli artefatti che vengono utilizzati negli attacchi di intrusi, ricognizioni e altre attività non autorizzate o di disturbo. Una volta ricevuto, l'artefatto viene esaminato. Si procede cioè all'analisi della natura, meccanica, versione e utilizzo degli artefatti e allo sviluppo (o suggerimento) di strategie di risposta per rilevare, rimuovere e difendersi da questi artefatti. Poiché le attività di gestione degli artefatti sono svolte in vario modo da tipi diversi di CSIRT, questo servizio viene ulteriormente categorizzato, in base al tipo di attività svolta e al tipo di assistenza fornita, nei modi qui di seguito.

Analisi degli artefatti

Il CSIRT svolge un esame tecnico e analisi di qualunque artefatto rinvenuto in un sistema. L'analisi svolta può consistere nell'identificare il tipo di file e la struttura dell'artefatto, confrontare un nuovo artefatto con gli artefatti esistenti o con altre versioni dello stesso artefatto per rilevare affinità e differenze, oppure decompilare o disassemblare il codice per determinare scopo e funzione dell'artefatto.

Risposta agli artefatti

Questo servizio consiste nel determinare le azioni appropriate per rilevare e rimuovere gli artefatti da un sistema nonché le azioni atte a prevenire l'installazione degli artefatti. Può quindi riguardare la creazione di firme da aggiungere al software antivirus o IDS (sistemi di rilevamento delle intrusioni).

Coordinamento della risposta agli artefatti

Questo servizio consiste nel condividere e sintetizzare i risultati dell'analisi e le strategie di risposta inerenti a un artefatto con altri ricercatori, CSIRT, venditori e altri esperti di sicurezza. Le attività comprendono la notifica ad altri soggetti e la sintesi dell'analisi tecnica eseguita da una serie di fonti. Possono inoltre comprendere il mantenimento di un archivio pubblico o riservati agli utenti di riferimento degli artefatti noti, del loro impatto e delle corrispondenti strategie di risposta.

Servizi proattivi

I servizi proattivi sono concepiti per migliorare l'infrastruttura e i processi di sicurezza della comunità di riferimento prima che si verifichi o sia rilevato qualunque incidente o evento. Gli obiettivi principali consistono nell'evitare gli incidenti e nel ridurne l'impatto e la portata quando si verificano.

Annunci

Comprendono, ma non solo, allarmi di intrusione, avvisi di vulnerabilità e bollettini informativi sulla sicurezza. Tali annunci informano gli utenti di riferimento in merito ai nuovi sviluppi con un impatto a medio e lungo termine, come le vulnerabilità appena scoperte o gli strumenti usati dagli intrusi. Gli avvisi permettono agli utenti di riferimento di proteggere i loro sistemi e reti contro i problemi appena scoperti prima che possano essere sfruttati.

Controllo tecnologico

Il CSIRT monitora e osserva i nuovi sviluppi tecnici, le attività degli intrusi e le tendenze correlate per aiutare a individuare i rischi futuri. Gli argomenti esaminati possono essere estesi fino a includere ordinanze giuridiche e legislative, rischi sociali e politici e tecnologie emergenti. Il servizio consiste nel leggere le mailing list sulla sicurezza, i siti web sulla sicurezza e le notizie e gli articoli di giornale attuali nei campi della scienza, tecnologia, politica e governo, al fine di estrapolare informazioni rilevanti per la sicurezza dei sistemi e delle reti degli utenti di riferimento. Ciò può comprendere la comunicazione con le autorità in questi campi per garantire l'ottenimento delle informazioni o interpretazioni migliori e più precise. Il risultato di questo servizio può essere un qualunque tipo di annuncio, linea guida o raccomandazione incentrata su questioni di sicurezza a medio e lungo termine.

Revisioni e valutazioni della sicurezza

Questo servizio fornisce una revisione e analisi dettagliata dell'infrastruttura di sicurezza di un'organizzazione in base ai requisiti definiti dall'organizzazione o da altri standard applicabili del settore. Può inoltre comprendere una revisione delle prassi organizzative di sicurezza. Si possono fornire molti tipi diversi di revisioni o valutazioni, tra cui i seguenti.

Revisione dell'infrastruttura

Rivedere manualmente le configurazioni hardware e software, router, firewall, server e dispositivi desktop per garantirne la conformità con le migliori prassi, politiche di sicurezza e configurazioni standard dell'organizzazione o settore.

Revisione delle migliori prassi

Intervistare i dipendenti e gli amministratori di rete e sistema per stabilire se le loro prassi di sicurezza sono conformi alla politica organizzativa di sicurezza definita o a determinati standard specifici di settore.

Scansione

Utilizzare scanner delle vulnerabilità o virus per determinare quali sistemi e reti sono vulnerabili.

Tentativi di violazione

Testare la sicurezza di un sito attaccandone deliberatamente i sistemi e le reti.
È necessario ottenere l'approvazione degli alti dirigenti prima di svolgere questo tipo di revisioni e valutazioni. Alcuni di questi approcci possono essere vietati dalla politica organizzativa. L'erogazione di questo servizio può comprendere lo sviluppo di una serie di prassi comuni da sottoporre alle prove o valutazioni, unitamente allo sviluppo di una serie di capacità richieste e requisiti di certificazione per il personale che svolge le prove, valutazioni, revisioni o esami. Questo servizio può anche essere esternalizzato a un appaltatore terzo o a un *Managed Security Service Provider* dotato delle competenze appropriate per lo svolgimento di revisioni e valutazioni.

Configurazione e manutenzione degli strumenti di sicurezza, applicazioni, infrastrutture e servizi

Questo servizio individua o fornisce gli orientamenti appropriati su come configurare e mantenere in maniera sicura strumenti, applicazioni e l'infrastruttura informatica generale utilizzata dalla comunità di riferimento del CSIRT o dal CSIRT stesso. Oltre a fornire orientamenti, il CSIRT può svolgere l'aggiornamento delle configurazioni e la manutenzione degli strumenti e servizi di sicurezza come IDS (sistemi di rilevamento delle intrusioni), sistemi di scansione o monitoraggio delle reti, filtri, wrapper, firewall, reti private virtuali (VPN) o meccanismi di autenticazione. Può inoltre fornire questi servizi nell'ambito delle sue funzioni principali e configurare e mantenere server, desktop, laptop, assistenti digitali personali (PDA) e altri dispositivi senza fili conformemente alle linee guida sulla sicurezza. Il servizio comprende il trasferimento al livello superiore della direzione di qualunque questione o problema con le configurazioni o l'utilizzo di strumenti e applicazioni, che il CSIRT ritiene possa rendere il sistema vulnerabile agli attacchi.

Sviluppo di strumenti di sicurezza

Questo servizio comprende lo sviluppo di qualunque nuovo strumento specifico degli utenti di riferimento, che sia richiesto o desiderato dalla comunità di riferimento o dal CSIRT stesso. Sono compresi, per esempio, lo sviluppo di patch (connessioni provvisorie) di sicurezza per i software personalizzati usati dalla comunità di riferimento o la distribuzione di software garantiti che possono essere usati per ricostruire host compromessi. Ad essi può inoltre aggiungersi lo sviluppo di strumenti o script che estendono la funzionalità degli strumenti di sicurezza esistenti, come un nuovo collegamento per uno scanner delle vulnerabilità o di rete, script che agevolano l'utilizzo della tecnologia di cifratura o meccanismi di distribuzione automatica delle patch (connessioni provvisorie).

Servizi di rilevamento delle intrusioni

I CSIRT che svolgono questo servizio rivedono i log IDS esistenti, analizzano e avviano una risposta per qualunque evento che rientra nella loro soglia definita, oppure inoltrano qualunque avviso secondo un contratto predefinito a livello di servizi o una strategia di trasferimento al livello superiore. Il rilevamento delle intrusioni e l'analisi dei log di sicurezza associati possono essere un compito scoraggiante, non solo nel determinare dove devono essere posizionati i sensori nell'ambiente, ma anche nel raccogliere e quindi analizzare le grandi quantità di dati ottenuti. In molti casi servono competenze o strumenti specializzati per sintetizzare e interpretare le informazioni atte a identificare falsi allarmi, attacchi o eventi di rete, oppure per attuare strategie volte a eliminare o ridurre al minimo tali eventi. Alcune organizzazioni scelgono di esternalizzare questa attività ad altri soggetti più competenti nello svolgimento di tali servizi, quali i Managed Security Service Provider.

Divulgazione di informazioni relative alla sicurezza

Questo servizio fornisce agli utenti di riferimento una raccolta completa e facile da reperire di informazioni utili per migliorare la sicurezza. Tali informazioni possono comprendere:

- linee guida sulla segnalazione e informazioni sui contatti per il CSIRT,
- archivi di allarmi, avvisi e altri annunci,
- documentazione in merito alle migliori prassi correnti,
- orientamenti generali sulla sicurezza informatica,
- politiche, procedure e liste di controllo,
- informazioni sullo sviluppo e distribuzione di patch (connessioni provvisorie),
- link dei venditori,
- statistiche e tendenze correnti nella segnalazione degli incidenti,
- altre informazioni che possono migliorare le prassi generali di sicurezza.

Tali informazioni possono essere sviluppate e pubblicate dal CSIRT o da un'altra parte dell'organizzazione (IT, risorse umane o relazioni con i media) e possono comprendere informazioni provenienti da fonti esterne quali altri CSIRT, venditori ed esperti di sicurezza.

Servizi di gestione della qualità della sicurezza

I servizi che rientrano in questa categoria non sono specifici della gestione degli incidenti o dei CSIRT in particolare. Si tratta anzi di servizi affermati e conosciuti, concepiti per migliorare la sicurezza generale di un'organizzazione. Facendo leva sulle esperienze

maturate nella fornitura dei servizi reattivi e proattivi sopra descritti, un CSIRT può conferire prospettive uniche a questi servizi di gestione della qualità che non sarebbero altrimenti disponibili. Tali servizi sono concepiti per incorporare i riscontri e gli insegnamenti tratti sulla base delle conoscenze acquisite rispondendo a incidenti, vulnerabilità e attacchi. Convogliare queste esperienze negli affermati servizi tradizionali (descritti di seguito) nell'ambito di un processo di gestione della qualità della sicurezza può migliorare gli sforzi per la sicurezza a lungo termine all'interno di un'organizzazione. A seconda delle responsabilità e strutture organizzative, un CSIRT può fornire questi servizi oppure parteciparvi nel quadro degli sforzi di un gruppo organizzativo più ampio.
Le seguenti descrizioni illustrano come la competenza dei CSIRT può andare a vantaggio di ciascuno di questi servizi di gestione della qualità della sicurezza.

Analisi dei rischi

I CSIRT possono valorizzare l'analisi e le valutazioni dei rischi. Ciò può migliorare la capacità dell'organizzazione di valutare le minacce reali, fornire valutazioni qualitative e quantitative realistiche dei rischi per l'informazione e valutare le strategie di protezione e risposta. I CSIRT che svolgono questo servizio condurranno o parteciperanno alle attività di analisi dei rischi per la sicurezza dell'informazione di nuovi sistemi e processi aziendali, oppure valuteranno le minacce e gli attacchi contro i beni e i sistemi degli utenti di riferimento.

Continuità operativa e ripristino in caso di disastro

Sulla base dei casi passati e delle future previsioni sulle tendenze emergenti negli incidenti e nella sicurezza, risulta che sempre più incidenti hanno il potenziale per causare una grave degradazione delle operazioni aziendali. Gli sforzi di pianificazione devono quindi considerare l'esperienza e le raccomandazioni dei CSIRT per determinare il modo migliore di rispondere a tali incidenti onde garantire la continuità delle operazioni aziendali. I CSIRT che svolgono questo servizio sono coinvolti nella pianificazione della continuità operativa e del ripristino in caso di disastro per eventi associati a minacce e attacchi alla sicurezza informatica.

Consulenza sulla sicurezza

I CSIRT possono essere usati per fornire consulenza e orientamento sulle prassi migliori in materia di sicurezza da adottare per le operazioni aziendali degli utenti di riferimento. Un CSIRT che eroga questo servizio è coinvolto nella preparazione di raccomandazioni o nell'identificazione dei requisiti per acquistare, installare o garantire nuovi sistemi, dispositivi di rete, applicazioni software o processi operativi a livello aziendale. Il servizio comprende la fornitura di orientamento e assistenza nello sviluppo di politiche di sicurezza organizzative e della comunità di riferimento. Può inoltre riguardare la fornitura di testimonianze o consulenze a organi legislativi o altri organi governativi.

Sensibilizzazione

I CSIRT possono essere in grado di individuare gli ambiti in cui gli utenti di riferimento necessitano di maggiore informazione e assistenza per adeguarsi al meglio alle prassi accettate in materia di sicurezza e alle politiche organizzative sulla sicurezza. Sensibilizzare la popolazione degli utenti di riferimento in merito alla sicurezza in generale non solo migliora la loro comprensione delle questioni di sicurezza, ma li aiuta anche a svolgere le proprie operazioni quotidiane in maniera più sicura. Ciò può ridurre il

numero di attacchi andati a buon fine e aumentare la probabilità che gli utenti di riferimento rilevino e segnalino gli attacchi, abbassando così i tempi di ripristino ed eliminando o riducendo al minimo le perdite.
I CSIRT che svolgono questo servizio cercano opportunità per sensibilizzare in merito alla sicurezza attraverso articoli, manifesti, note informative, siti web o altre risorse informative che spiegano le prassi migliori in materia di sicurezza e forniscono consulenza sulle precauzioni da adottare. Le attività possono comprendere anche la programmazione di incontri e seminari per tenere aggiornati gli utenti di riferimento sulle procedure di sicurezza in atto e sulle potenziali minacce ai sistemi organizzativi.

Istruzione/formazione

Questo servizio consiste nel fornire informazioni agli utenti di riferimento su questioni di sicurezza informatica attraverso seminari, laboratori, corsi e guide. Gli argomenti possono spaziare dalle linee guida sulla segnalazione degli incidenti ai metodi appropriati di risposta, strumenti di risposta agli incidenti, metodi di prevenzione degli incidenti e altre informazioni necessarie per proteggere, rilevare, segnalare e rispondere agli incidenti di sicurezza informatica.

Valutazione o certificazione dei prodotti

Per questo servizio, il CSIRT può svolgere valutazioni dei prodotti su strumenti, applicazioni o altri servizi, al fine di garantire la sicurezza dei prodotti e la loro conformità alle prassi accettabili di sicurezza del CSIRT o dell'organizzazione. Gli strumenti e le applicazioni riviste possono essere prodotti commerciali od open source. Questo servizio può essere fornito sotto forma di valutazione o attraverso un programma di certificazione, secondo gli standard applicati dall'organizzazione o dal CSIRT.

A.3 Esempi

CSIRT simulato

Fase 0 - Cos'è un CSIRT

Il CSIRT campione dovrà servire un'istituzione media, composta da 200 dipendenti. L'istituzione ha un proprio dipartimento IT e altre due filiali nello stesso paese. L'IT svolge un ruolo fondamentale per l'ente, servendo per la comunicazione interna, la rete di dati e il commercio elettronico 24x7. L'istituzione ha una propria rete e dispone di una connessione ridondante a Internet tramite due diversi ISP (fornitori di servizi Internet).

- - - -

Fase 4: Definizione del mandato

La gestione del CSIRT simulato ha formulato la seguente definizione del mandato:
"Il CSIRT simulato fornisce informazioni e assistenza al personale della sua società ospitante per ridurre i rischi di incidenti di sicurezza informatica e rispondere a tali incidenti quando questi si verificano."

Con essa, il CSIRT simulato chiarisce di essere un CSIRT interno e che la sua attività principale consiste nell'affrontare questioni legate alla sicurezza IT.

- - - -

Fase 5: Utilizzazione dell'ufficio e politica di sicurezza dell'informazione
Attrezzatura d'ufficio e ubicazione
Poiché l'ente ospitante dispone già di un'efficiente sicurezza fisica, il nuovo CSIRT vanta una buona copertura a questo riguardo. Viene messa a disposizione una cosiddetta "sala della guerra" per consentire il coordinamento in caso di emergenza. Si provvede ad acquistare una cassaforte per il materiale di cifratura e i documenti riservati. È stata predisposta una linea telefonica separata comprensiva di centralino per supportare la linea diretta durante l'orario di ufficio e il cellulare del servizio "di guardia" fuori dell'orario di ufficio con lo stesso numero di telefono.

Si possono usare anche l'attrezzatura esistente e il sito web aziendale per annunciare le informazioni relative al CSIRT. Un software per mailing list viene installato e mantenuto, con una parte riservata alla comunicazione tra i membri del gruppo e con altri gruppi. Tutti i dettagli dei contatti dei membri del personale sono archiviati in una banca dati e una copia stampata viene conservata nella cassaforte.

Regolamento
Poiché il CSIRT è incorporato all'interno di un ente dotato di politiche in materia di sicurezza dell'informazione, le relative politiche per il CSIRT sono state elaborate con l'ausilio del consulente legale della società.
- - - -

Fase 9: Stabilire flussi di processo e procedure operative e tecniche
Il CSIRT simulato si concentra sull'erogazione di servizi CSIRT chiave:

- Allarmi e avvisi
- Annunci
- Gestione degli incidenti

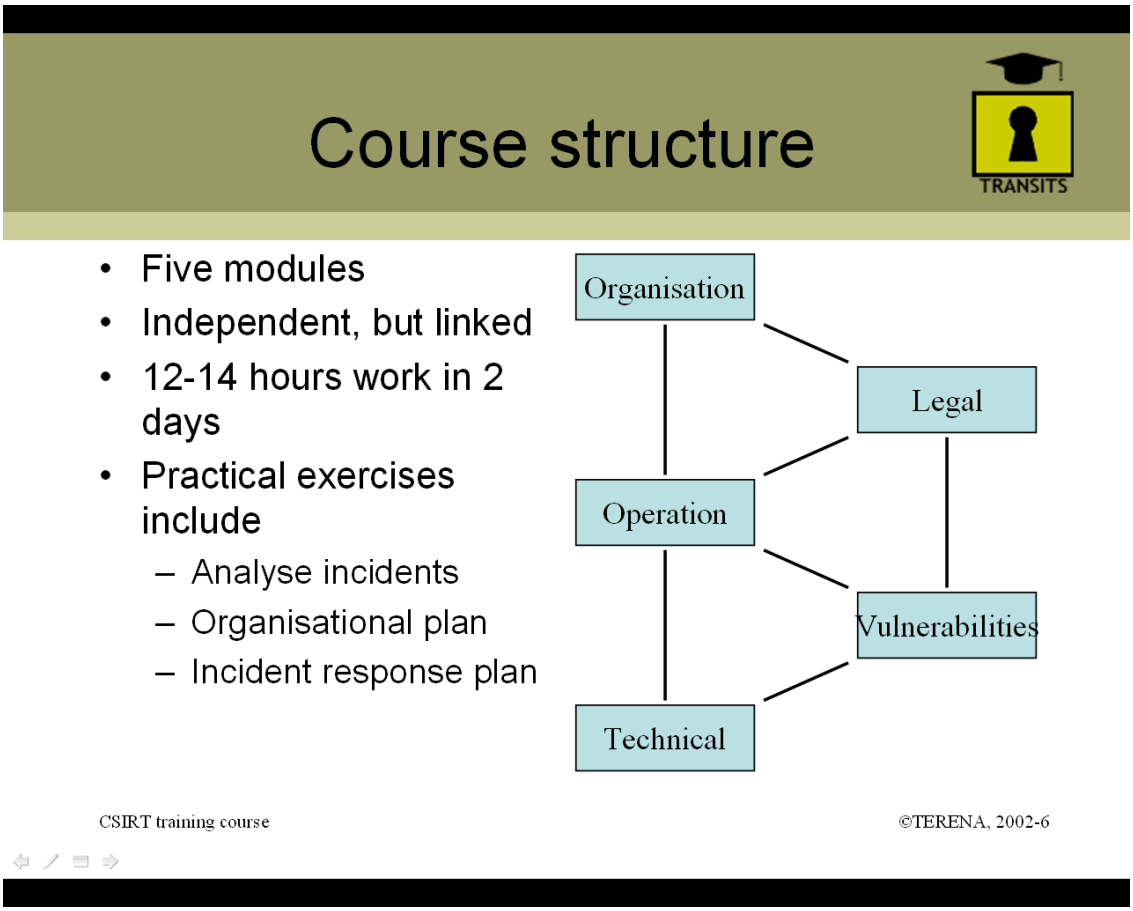
Il gruppo ha sviluppato procedure ben funzionanti e facilmente comprensibili per ogni membro del gruppo stesso. Il CSIRT simulato ha anche assunto un esperto legale che si occuperà delle responsabilità e della politica di sicurezza dell'informazione. Discutendo con altri CSIRT, il gruppo ha adottato alcuni strumenti utili e reperito informazioni interessanti su questioni operative.

È stato generato un modello fisso per i bollettini informativi sulla sicurezza e i rapporti sugli incidenti. Il gruppo utilizza RTIR (sistema di tracciabilità della richiesta in caso di risposta a incidente) per la gestione degli incidenti.

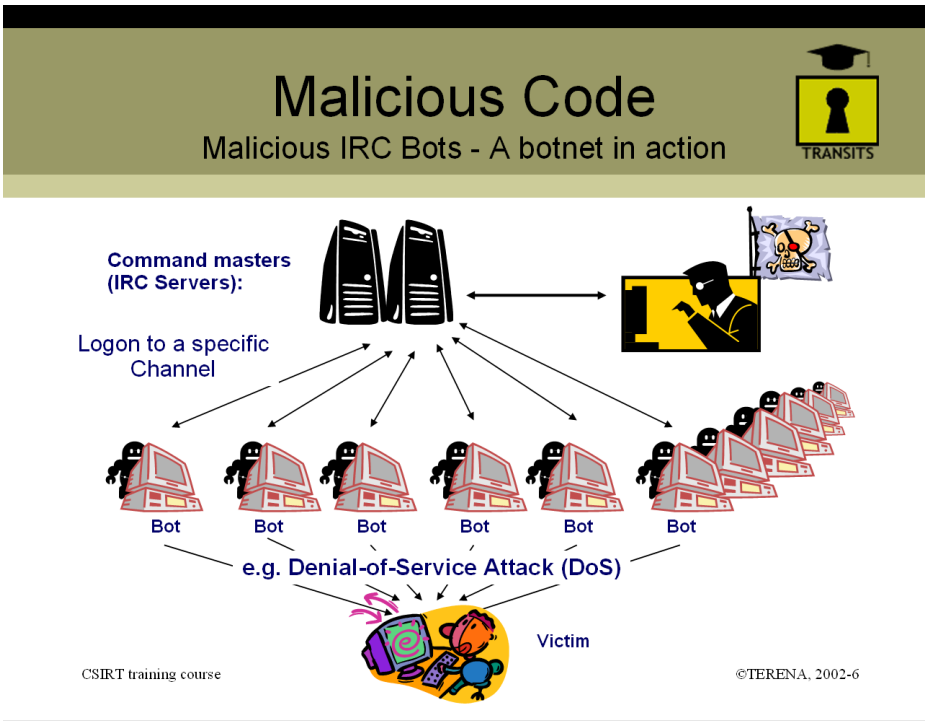
- - - -

A.4 Materiale campione dai corsi CSIRT

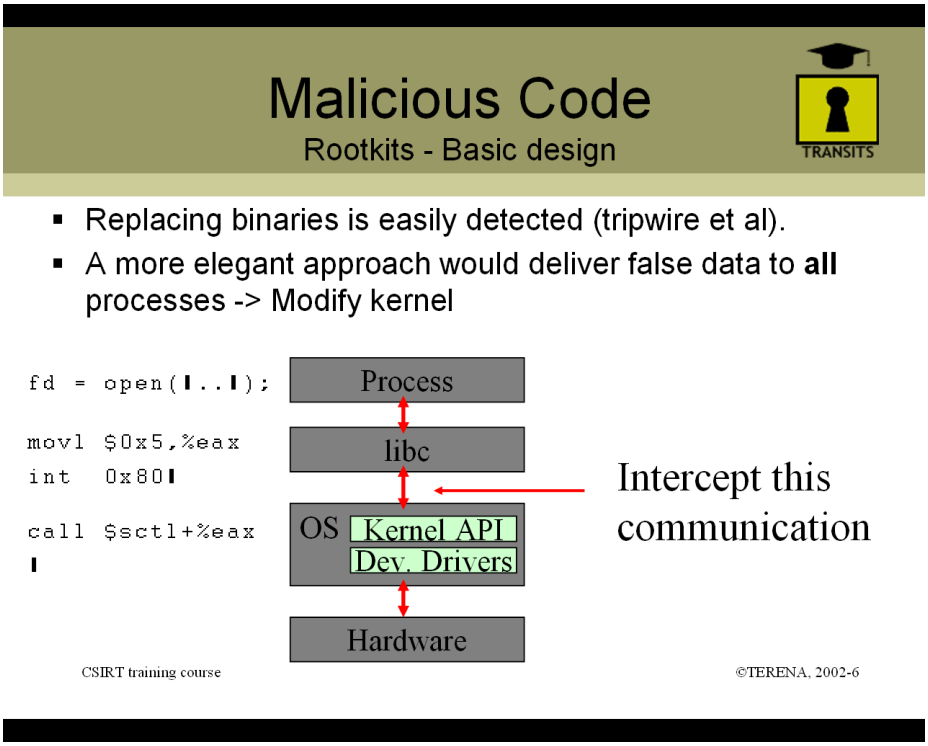
TRANSITS (per gentile concessione di Terena, http://www.terena.nl)



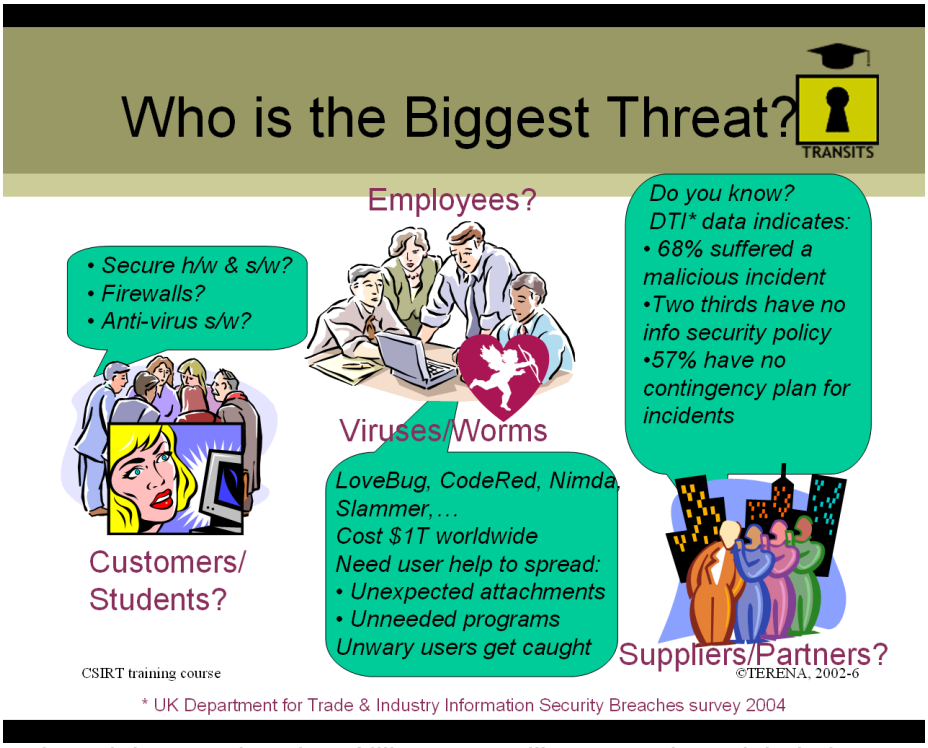
Panoramica: La struttura del corso



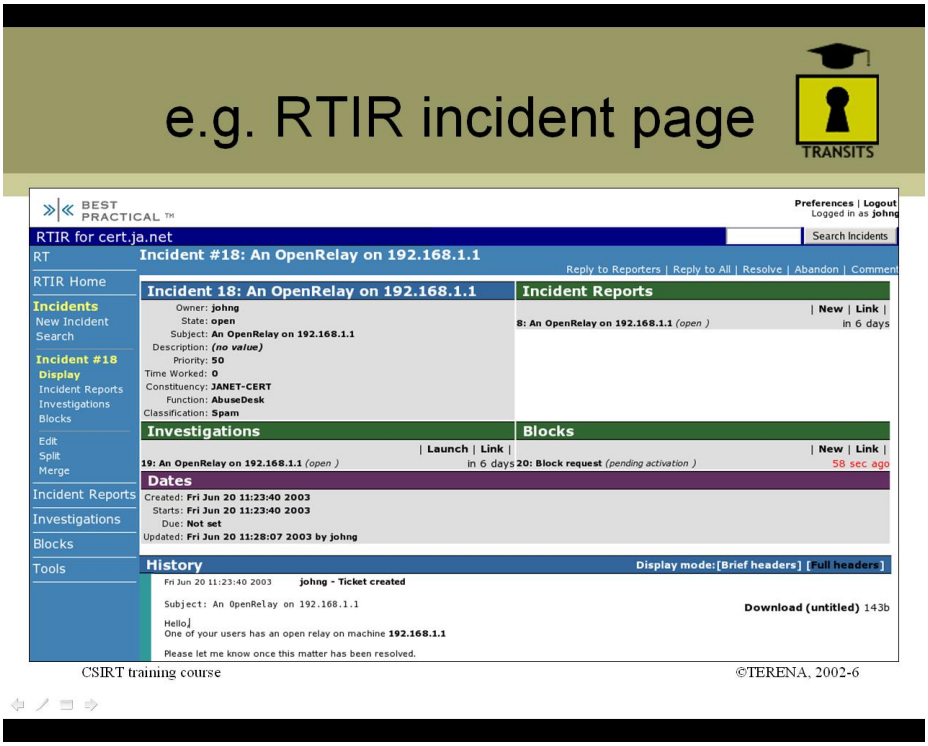
Dal *Modulo tecnico*: Descrizione di una botnet (rete di computer collegati a Internet, infettati da virus informatici, che consentono ai creatori di controllare il sistema da remoto).



Dal *Modulo tecnico*: Progettazione di base di un rootkit (tecnologia software in grado di occultare la propria presenza all'interno del sistema operativo).



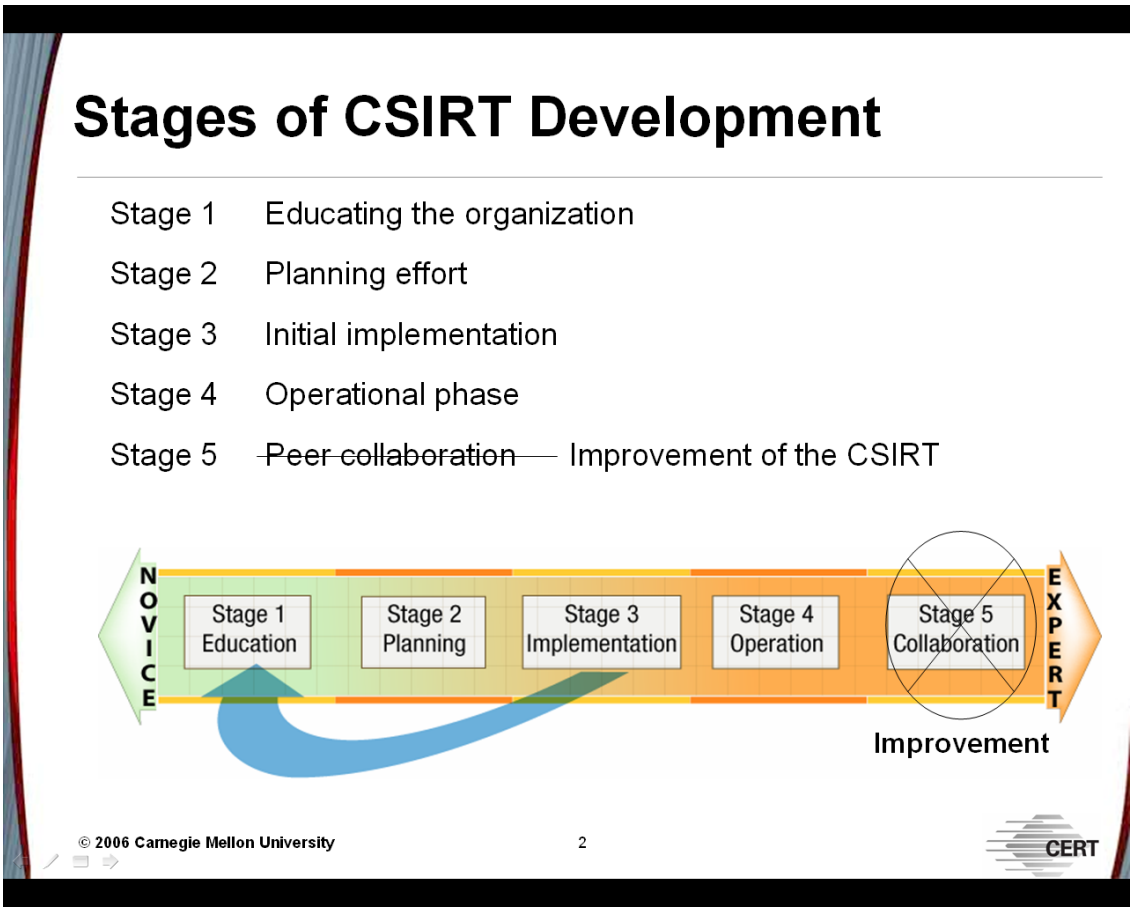
Dal *Modulo organizzativo*: All'interno o all'esterno: dove risiede la maggiore minaccia?



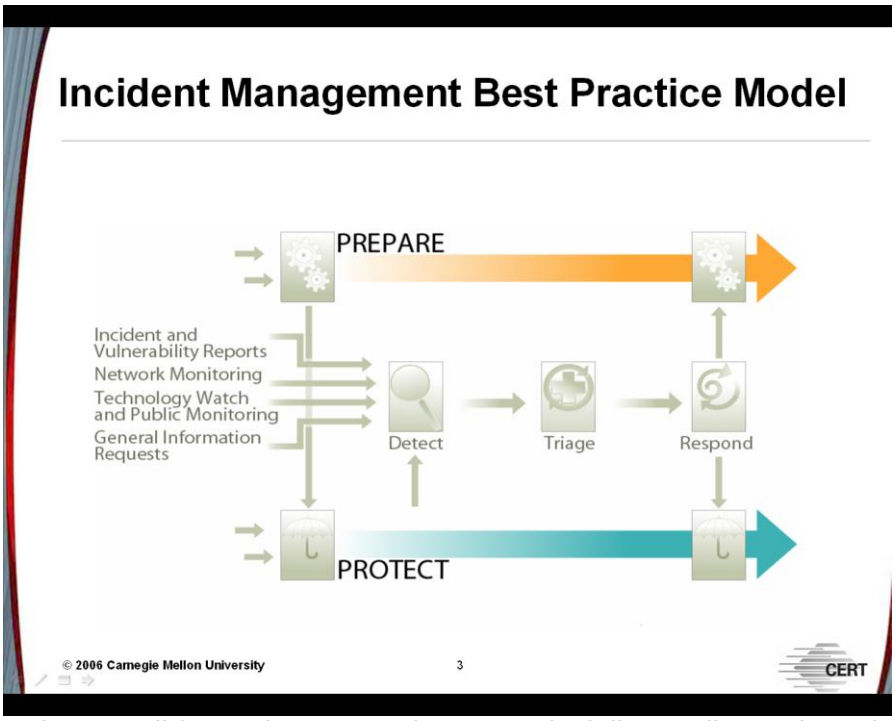
Dalla *Traccia operativa*: Request Tracker for Incident Response (RTIR, sistema di tracciabilità della richiesta in caso di risposta a incidente)

"Creazione dei CSIRT" (per gentile concessione del CERT/CC, http://www.cert.org)

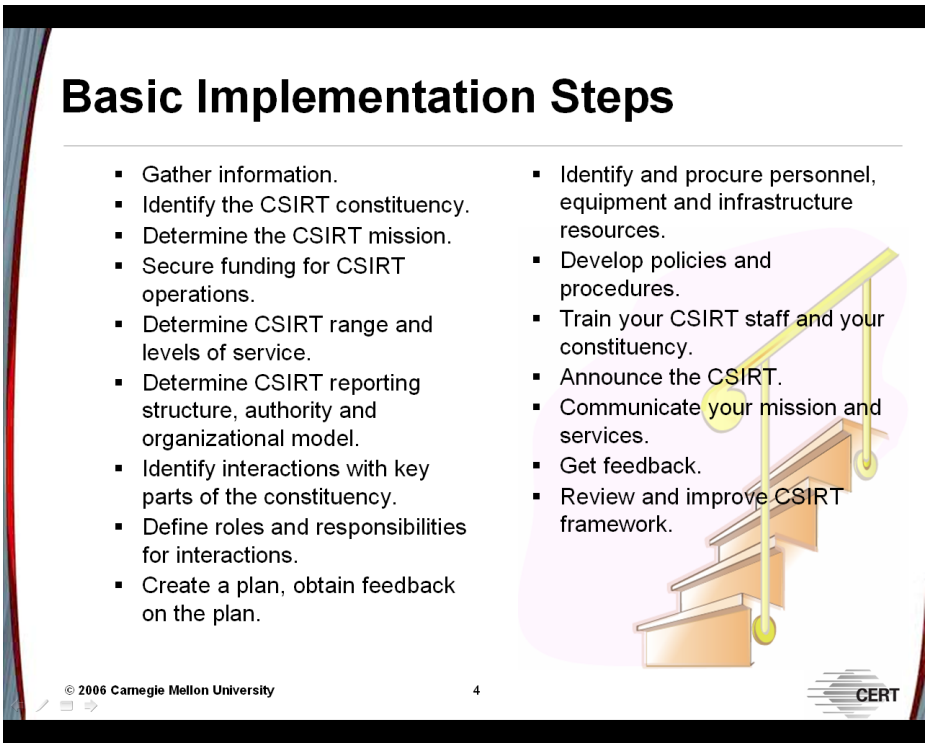
L'ENISA esprime i suoi più sentiti ringraziamenti al gruppo di sviluppo CSIRT del Programma CERT per averci consentito di utilizzare i contenuti dei loro corsi di formazione!



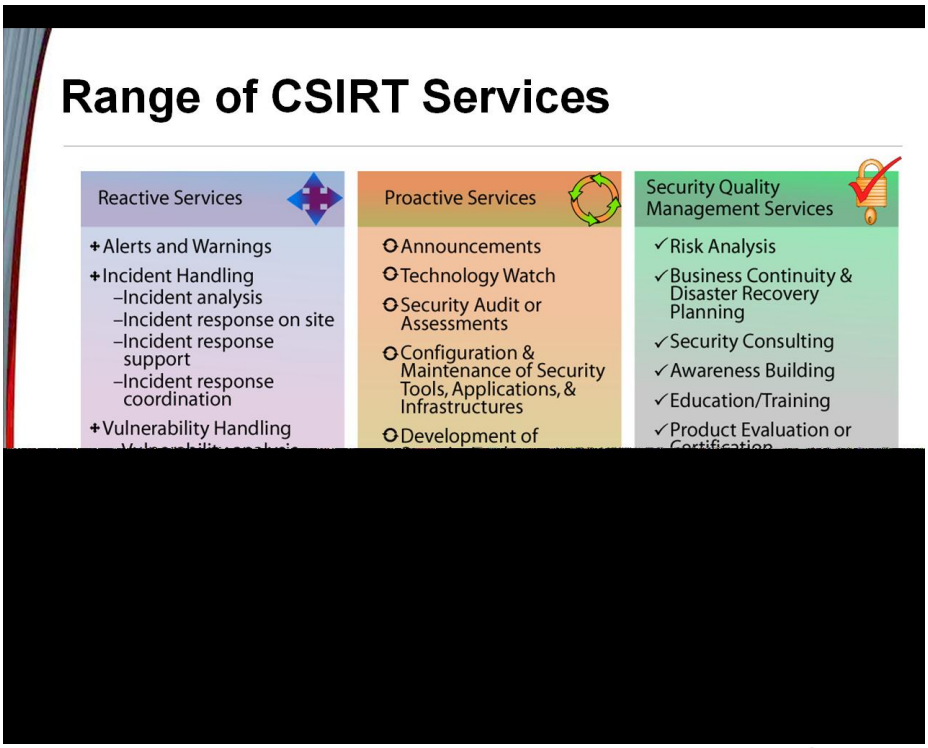
Dal *Corso di formazione CERT/CC*: Fasi di sviluppo di un CSIRT



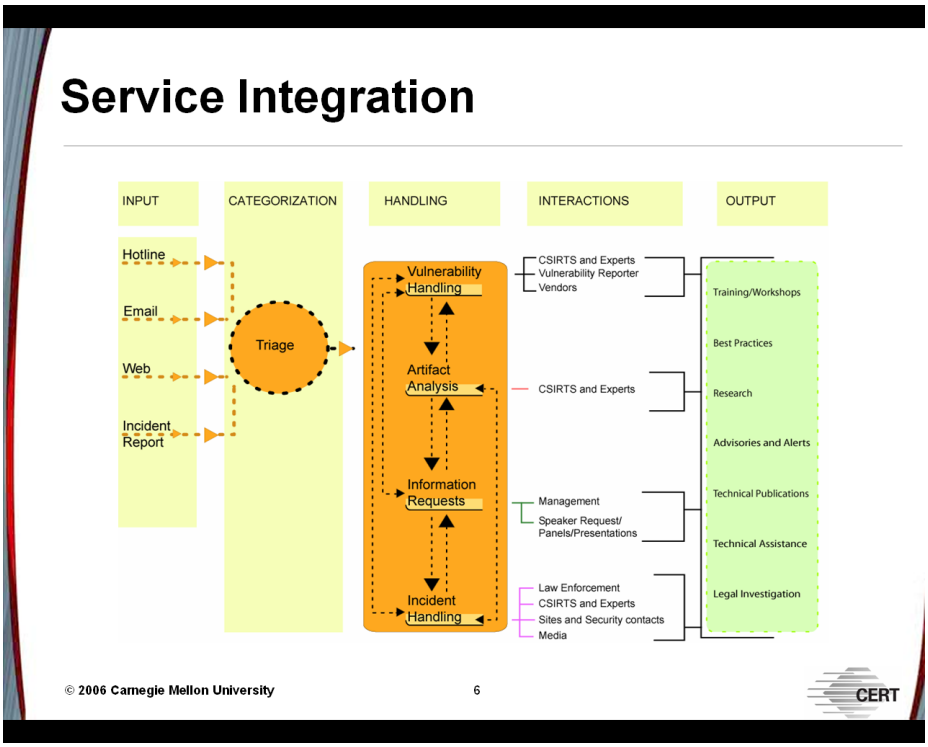
Dal *Corso di formazione CERT/CC*: Prassi migliore nella gestione degli incidenti



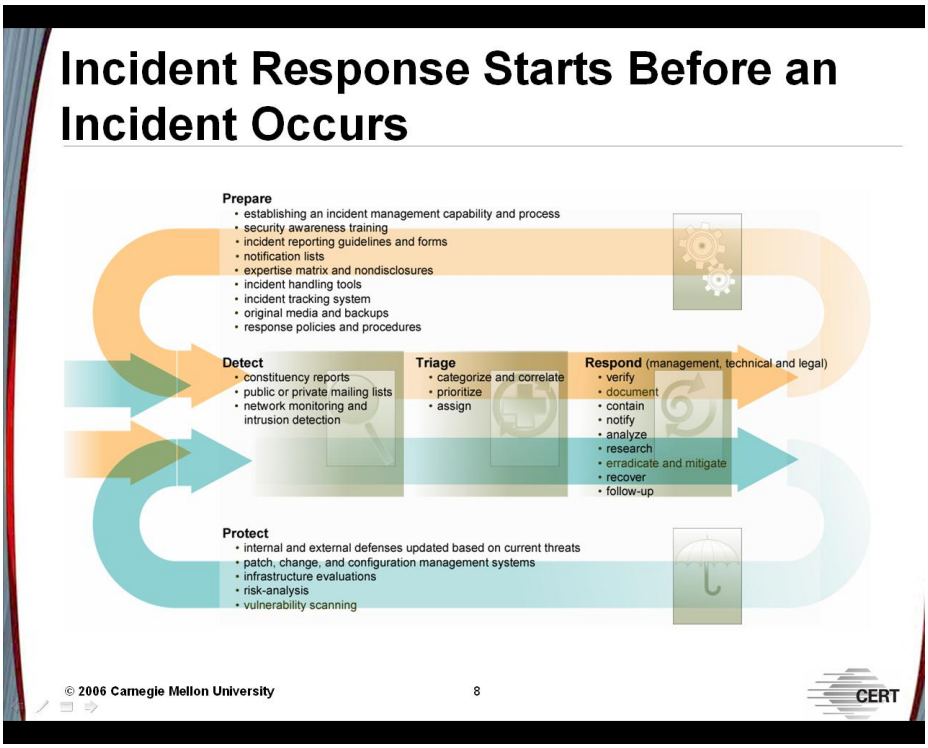
Dal *Corso di formazione CERT/CC*: Le fasi di creazione di un CSIRT



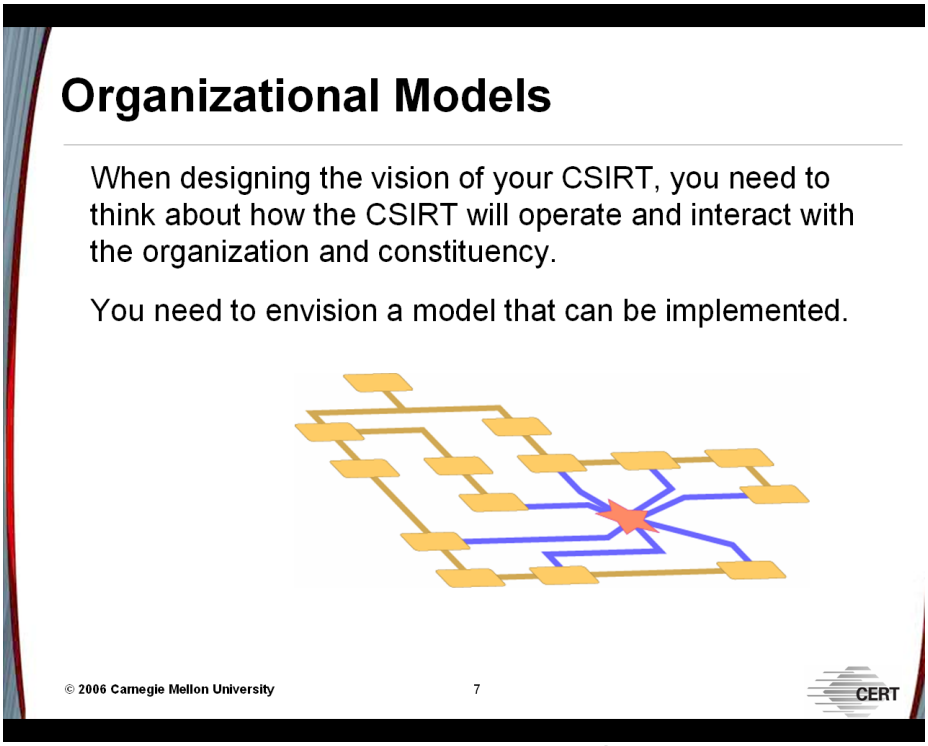
Dal *Corso di formazione CERT/CC*: I servizi che un CSIRT può offrire



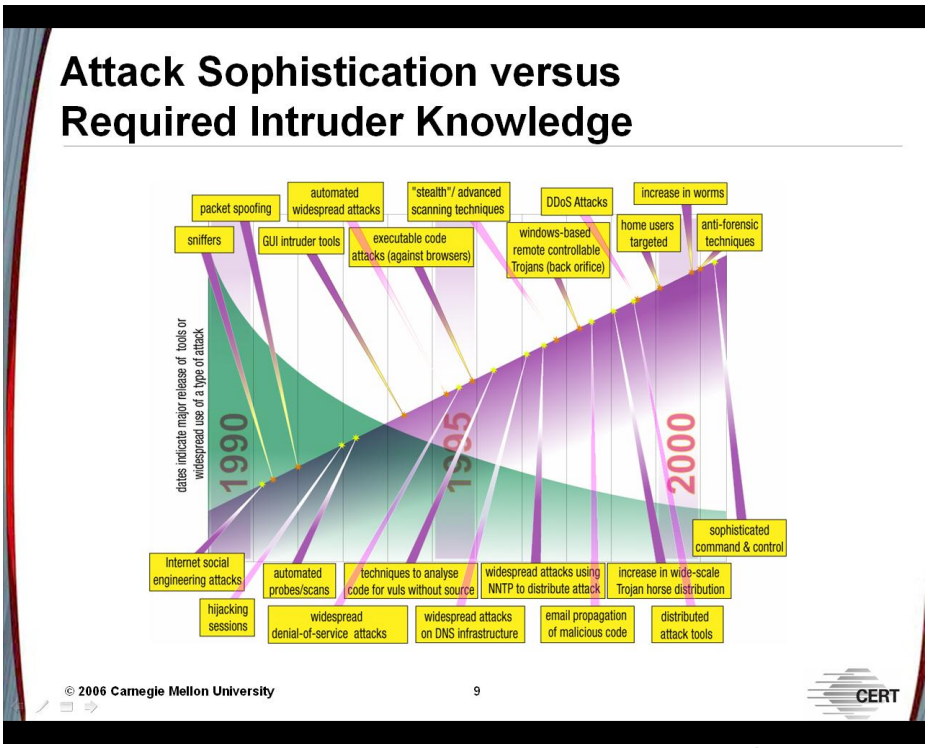
Dal *Corso di formazione CERT/CC*: Il flusso di lavoro della gestione degli incidenti



Dal *Corso di formazione CERT/CC*: Risposta agli incidenti



Dal *Corso di formazione CERT/CC*: Come sarà organizzato il CSIRT?



Dal *Corso di formazione CERT/CC*: Meno conoscenze, più danni