GUIDE DE CREATION D'UN CSIRT PAS A PAS

Résultats WP2006/5.1(CERT-D1/D2)

Index

1 Synthèse pour la direction (*Management Summary*) 2

2 Notice légale 2

3 Remerciements 3

4 Introduction 3

4.1 PUBLIC CIBLE 4
4.2 GUIDE D'UTILISATION DU PRESENT DOCUMENT 4
4.3 CONVENTIONS UTILISEES 5

5 Stratégie générale de planification et de création d'un CSIRT 6

5.1 QU'EST-CE QU'UN CSIRT? 6
5.2 QUELS SERVICES UN CSIRT PEUT-IL OFFRIR? 10
5.3 ANALYSE DES PARTIES PRENANTES ET DECLARATION DE MISSION 12

6 Élaboration du plan d'activités 19

6.1 DEFINITION DU MODELE FINANCIER 19
6.2 DEFINITION DE LA STRUCTURE ORGANISATIONNELLE 21
6.3 RECRUTEMENT DU PERSONNEL ADEQUAT 25
6.4 UTILISATION ET EQUIPEMENT DE L'ESPACE DE BUREAU 27
6.5 DEVELOPPEMENT D'UNE POLITIQUE DE SECURITE DE L'INFORMATION 29
6.6 COOPERATION AVEC D'AUTRES CSIRT ET D'EVENTUELLES INITIATIVES NATIONALES 31

7 Promotion du plan d'activités 32

7.1 DESCRIPTION DU PLAN D'ACTIVITES ET DES FACTEURS DECLENCHEURS 35

8 Exemples de procédures opérationnelles et techniques (workflows) 38

8.1 ÉVALUATION DES INSTALLATIONS DES PARTIES PRENANTES 39
8.2 LANCEMENT D'ALERTES, D'AVERTISSEMENTS ET D'ANNONCES 40
8.3 TRAITEMENT DES INCIDENTS 47
8.4 EXEMPLE DE DELAI DE REPONSE 53
8.5 OUTILS A LA DISPOSITION DES CSIRT 54

9 Formation du personnel des CSIRT 56

9.1 TRANSITS 56
9.2 CERT/CC 57

10 Exercice: établissement d'un bulletin de sécurité 59

11 Conclusion 64

12 Description du plan de projet 65

ANNEXE 67

A.1 LECTURES COMPLEMENTAIRES 67
A.2 SERVICES FOURNIS PAR UN CSIRT 68
A.3 EXEMPLES 78
A.4 EXTRAITS DE COURS DE FORMATION CONCERNANT LES CSIRT 82

1 Synthèse pour la direction (*Management Summary*)

Le présent document décrit le processus de création d'un CSIRT (*Computer Security Incident Response Team* – Équipe de réponse aux incidents de sécurité informatique) en abordant tous les aspects en jeu, en ce compris la gestion d'entreprise, la gestion des processus et le point de vue technique. Il concrétise deux tâches visées au point 5.1 du programme de travail 2006 de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA):

- **CERT-D1** *(Written report on step-by-step approach on how to set up a CERT or similar facilities, including examples)* en ce qui concerne le document proprement dit;
- **CERT-D2** *(Excerpt of roadmap in itemised form allowing an easy application of the roadmap in practice)* en ce qui concerne le chapitre 12 et les fichiers externes.

2 Notice légale

La présente publication exprime, sauf indication contraire, les points de vue et interprétations des auteurs et des éditeurs. Elle ne doit pas être considérée dès lors comme une action de la part de Agence européenne chargée de la sécurité des réseaux et de l'information (*European Network and information Security Agency*, ENISA) ou de ses organes à moins d'être adoptée en vertu du règlement (CE) n° 460/2004 instituant l'Agence. Elle ne reflète pas nécessairement l'état de la technologie la plus récente et pourrait faire l'objet de mises à jour.

Les sources tierces sont citées, le cas échéant. L'ENISA n'est pas responsable du contenu des sources extérieures, y compris les sites Web externes auxquels la présente publication fait référence.

La présente publication a une vocation strictement éducative et informative. Ni l'ENISA ni aucune autre personne agissant en son nom n'est responsable de l'usage qui pourrait être fait des informations qui y sont contenues.

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise sous quelque forme ou par quelque moyen que ce soit – électronique, mécanique, photocopie, enregistrement ou autre – sans l'accord préalable écrit de l'ENISA, sauf dans la mesure expressément autorisée par la loi ou aux conditions convenues avec les organismes compétents en matière de droits. Dans tous les cas, la mention de la source est obligatoire. Les demandes de reproduction doivent être envoyées à l'adresse de contact figurant dans la présente.

© European Network and information Security Agency (ENISA), 2006

3 Remerciements

L'ENISA tient à remercier toutes les institutions et personnes ayant contribué au présent document, et plus spécialement:

- Henk Bronk, consultant qui en a élaboré la première version;
- le CERT/CC et son équipe de développement CSIRT en particulier, qui ont fourni des éléments d'information particulièrement utiles, ainsi que les extraits de cours présentés en annexe à titre d'exemples;
- GovCERT.NL pour la fourniture du *CERT-in-a-box*
- l'équipe TRANSITS pour la fourniture des extraits de cours présentés en annexe;
- les collègues de la section «Security Policies» du département technique pour la rédaction de la section 6.5;
- les innombrables personnes qui ont révisé les pages qui vont suivre.

4 Introduction

Les réseaux de communication et les systèmes d'information sont devenus un facteur clé du développement économique et social. L'électronique et la réseautique sont désormais des services aussi omniprésents que l'approvisionnement en électricité ou en eau.

La sécurité des réseaux de communication et des systèmes d'information, et leur disponibilité en particulier, sont devenues dès lors une préoccupation croissante pour la société en raison des risques y afférents, à savoir que des systèmes d'information clés pourraient, en raison de leur complexité, d'un accident, d'une erreur ou d'une attaque, connaître des problèmes se répercutant sur les infrastructures physiques qui fournissent des services vitaux pour le bien-être des citoyens de l'Union européenne.

Une Agence européenne chargée de la sécurité des réseaux et de l'information (*European Network and information Security Agency*, ENISA) a été instituée le 10 mars 2004[1] aux fins d'assurer un niveau élevé et efficace de sécurité des réseaux et de l'information au sein de la Communauté et en vue de favoriser l'émergence d'une culture de la sécurité des réseaux et de l'information dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, contribuant ainsi au bon fonctionnement du marché intérieur.

Toute une série de communautés de sécurité - CERT/CSIRT, Abuse Teams et WARP - collaborent depuis plusieurs années en Europe en vue de sécuriser davantage l'Internet. L'ENISA a l'intention de soutenir les efforts de ces communautés en les informant de

[1] Règlement (CE) N° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information. Une «Agence de la Communauté européenne» est un organe créé par l'UE pour accomplir une tâche technique, scientifique ou de gestion très spécifique relevant de la dimension communautaire («premier pilier») de l'UE.

mesures propres à garantir un niveau adéquat de qualité de service. L'Agence a l'intention en outre de renforcer sa capacité de conseiller les États membres et les organes de l'UE pour ce qui concerne la protection de groupes particuliers d'utilisateurs des TI à l'aide de services de sécurité adéquats. S'appuyant sur les acquis du groupe de travail ad hoc «CERT Cooperation and Support», créé en 2005, ce nouveau groupe de travail traitera donc de questions touchant à la fourniture de services de sécurité adéquats («services CERT») à l'intention (de catégories ou groupes) d'utilisateurs spécifiques.

L'ENISA soutient la création de nouveaux CSIRT en publiant le présent rapport qui, intitulé «Guide de création d'un CSIRT pas à pas» et complété d'une liste de contrôle, permettra au lecteur de créer son propre CSIRT.

Public cible

Les principaux groupes destinataires du présent rapport sont les institutions publiques et autres chargées de créer un CSIRT pour protéger leur propre structure informatique et celle de leurs parties prenantes.

Structure du présent document

Le document qui va suivre s'attache à décrire le concept de CSIRT, les services qu'il peut fournir et les étapes indispensables à son démarrage. Il veut ainsi donner au lecteur un bon aperçu pragmatique de l'approche, de la structuration et du contenu de la création d'un CSIRT.

Chapitre 4 «*Introduction*»
Présentation du rapport.

Chapitre 5 «*Stratégie générale de planification et de création d'un CSIRT*»
Cette première section décrit le concept de CSIRT, de même que les différents environnements dans lesquels il peut fonctionner et les types de services qu'il peut offrir.

Chapitre 6 «*Élaboration du plan d'activités*»
Ce chapitre décrit l'approche du processus de création du CSIRT dans une perspective de gestion d'entreprise.

Chapitre 7 «*Promotion du plan d'activités*»
Ce septième chapitre traite de la justification stratégique et commerciale (*business case*) et des questions de financement.

Chapitre 8 «*Exemples de procédures opérationnelles et techniques*»
Ce chapitre décrit la procédure allant de l'obtention d'informations à leur transposition en bulletin de sécurité. Il propose également la description du déroulement des opérations de traitement (workflow).

Chapitre 9 «*Formation du personnel d'un CSIRT*»
Ce chapitre contient une liste récapitulative des cours de formation proposés dans le domaine des CSIRT. Des extraits de cours sont fournis en annexe à titre d'exemples.

Chapitre 10 «*Exercice: établissement d'un bulletin de sécurité*»

Ce chapitre montre, à l'aide d'un exercice, comment assurer l'un des services élémentaires (ou de base) d'un CSIRT, en l'occurrence la production d'un bulletin ou d'un avis de sécurité.

Chapitre 12 «Description du plan de projet»
Ce dernier chapitre est consacré au plan de projet (liste de contrôle) qui, fourni en complément du présent guide, se veut un outil convivial d'utilisation de ce dernier.

Conventions utilisées dans le présent document

En vue de mieux orienter le lecteur, chaque chapitre commence par un récapitulatif des étapes de création d'un CSIRT qui ont déjà été franchies. Cette liste récapitulative est présentée dans un encadré tel que celui-ci:

Nous avons franchi la première étape

Chaque chapitre s'achève sur un exemple concret des étapes décrites. Le «CSIRT fictif» choisi pour illustrer le présent document est un petit CSIRT indépendant destiné à une entreprise ou une institution de taille moyenne. Une synthèse est présentée en annexe.

CSIRT fictif

5 Stratégie générale de planification et de création d'un CSIRT

Le bon déroulement de la création d'un CSIRT exige d'avoir, dès l'amorce du processus, une vision très claire des services qu'il peut offrir à ses clients, généralement désignés dans l'univers des CSIRT comme ses parties prenantes. Il convient en effet de comprendre les attentes de celles-ci pour leur fournir des services répondant à leurs besoins et offrant le délai de réponse et le niveau de qualité escomptés.

Qu'est-ce qu'un CSIRT?

L'acronyme CSIRT, qui signifie *Computer Security Incident Response Team,* est principalement utilisé en Europe comme synonyme du terme protégé CERT, déposé aux États-Unis par le CERT Coordination Center (CERT/CC).

Plusieurs abréviations désignent les centres de ce type:

- CERT ou 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 première apparition d'un ver dans l'infrastructure informatique mondiale remonte à la fin des années 1980 avec Morris[2], qui s'est rapidement propagé pour contaminer de très nombreux systèmes TI dans le monde entier.

Cet incident a été un véritable signal d'alarme, dans la mesure où il a fait prendre conscience de la nécessité impérative d'une coopération et d'une coordination au niveau des administrateurs systèmes et des responsables informatiques pour lutter contre ce type de phénomène. Le temps étant un facteur critique, il convenait d'adopter une approche davantage organisée et structurée de la gestion des incidents de sécurité informatique. Aussi, quelques jours à peine après «l'incident Morris», la DARPA (*Defence Advanced Research Projects Agency*) créait-elle le premier CSIRT, en l'occurrence le *CERT Coordination Center* (CERT/CC[3]), implanté à la Carnegie Mellon University de Pittsburgh (Pennsylvanie).

Le modèle en a rapidement été reproduit en Europe et, dès 1992, le fournisseur d'accès Internet des universités néerlandaises SURFnet inaugurait le premier CSIRT européen, baptisé SURFnet-CERT[4]. De nombreuses équipes ont été créées dans la foulée et l'inventaire des activités CERT publié par l'ENISA (*Inventory of CERT activities in Europe*[5]) comprend aujourd'hui plus d'une centaine de centres recensés en Europe.

[2] Pour en savoir plus à propos du ver Morris: http://fr.wikipedia.org/wiki/Ver_informatique

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

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

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

Les CERT ont développé leurs capacités au fil des années: simple force de réaction au départ, ils sont désormais des fournisseurs de services de sécurité à part entière, y compris de services préventifs couvrant notamment les alertes, les bulletins de sécurité, la formation et la gestion de la sécurité. Le terme «CERT» a été rapidement jugé insuffisant et un nouveau terme - «CSIRT» - a été créé à la fin des années 1990. Les deux termes sont aujourd'hui utilisés de manière synonyme, CSIRT étant cependant le plus précis.

5..1 Le terme *Partie prenante (Constituency)*

Le terme désormais bien établi (au sein des communautés CSIRT) de «parties prenantes» désignera ci-après la base de clientèle d'un CSIRT, un client particulier étant désigné comme «une partie prenante».

5..2 Définition d'un CSIRT

Un CSIRT est une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet.

La plupart des CSIRT offrent également à leurs parties prenantes, dans le but d'atténuer les risques et de minimiser le nombre d'interventions requises, des services à caractère préventif et éducatif. Ils publient des bulletins et avis de vulnérabilités concernant les logiciels et matériels en usage, et informent les utilisateurs des exploits et virus tirant parti des failles constatées. Les parties prenantes sont dès lors en mesure de procéder rapidement à l'application de correctifs et à la mise à jour de leurs systèmes. Voir la liste complète des services possibles au point *5.2*.

5..3 Les avantages d'un CSIRT

Disposer d'une équipe spécialisée en sécurité informatique aide toute organisation à réduire, voir à prévenir, les incidents majeurs et à protéger un patrimoine précieux.

Le CSIRT peut offrir en outre les avantages suivants:

- la centralisation de la coordination en matière de sécurité informatique au sein de l'organisation (point de contact);
- la centralisation et la spécialisation du traitement et de la réponse aux incidents informatiques;
- la disponibilité d'une expertise permettant de soutenir les utilisateurs et de les aider à la restauration de leur système après un incident de sécurité;
- la gestion des aspects juridiques et la protection des preuves en cas d'action en justice;
- le suivi des évolutions dans le domaine de la sécurité;
- l'incitation des parties prenantes à coopérer en matière de sécurité informatique (sensibilisation).

CSIRT fictif (étape 0)
Comprendre le concept de CSIRT: Le CSIRT choisi à titre exemplatif est appelé à desservir une organisation de taille moyenne occupant 200 personnes. Elle a son propre département informatique et deux succursales dans le même pays. L'informatique y joue un rôle essentiel puisqu'elle est utilisée pour la communication interne, pour un réseau de transmission de données et pour une activité de commerce électronique 24 heures par jour et 7 jours par semaine. L'organisation possède son propre réseau et dispose d'une connexion redondante à l'Internet via deux fournisseurs d'accès différents.

5..4 Description des différents contextes de création d'un CSIRT

Nous avons franchi la première étape

1. Comprendre le concept du CSIRT et les avantages qui y sont associés.

>> L'étape suivante consiste à répondre à la question: «À quel secteur les services du CSIRT sont-ils destinés?»

Il est très important, au moment d'entamer la création d'un CSIRT (comme de toute autre activité), d'avoir d'emblée une idée très claire des parties prenantes visées et de l'environnement dans lequel les services du CSIRT vont être développés. Nous distinguons actuellement les «secteurs» suivants (cités par ordre alphabétique):

- commercial
- fournisseur (*vendor*)
- gouvernemental
- interne
- militaire
- national
- PIC/PIIC
- PME (petites et moyennes entreprises)
- universitaire

CIRST dans le secteur commercial
Axe prioritaire
La fourniture de services à titre commercial aux parties prenantes. Dans le cas d'un fournisseur d'accès Internet (FAI), le CSIRT propose principalement des services anti-abus aux utilisateurs finals (Dial-in, ADSL) et l'ensemble des services CSIRT aux utilisateurs professionnels.

Parties prenantes
Les CSIRT commerciaux fournissent généralement leurs services à des parties prenantes contre paiement.

CSIRT dans le secteur des fournisseurs (*vendors*)
Axe prioritaire
Le soutien de produits propres à un fournisseur, le but étant généralement de développer et de proposer des solutions qui permettent d'en supprimer les vulnérabilités et d'atténuer les effets négatifs éventuels de leurs failles.

Parties prenantes
Propriétaires de produits.

CSIRT gouvernemental
Axe prioritaire
La fourniture de services aux organismes publics et, dans certains pays, aux citoyens.

Parties prenantes
Administration publique et organismes officiels; des services d'alerte sont également proposés aux citoyens dans un certain nombre de pays (Belgique, Hongrie, Pays-Bas, Royaume-Uni et Allemagne notamment).

CSIRT interne
Axe prioritaire
La fourniture exclusive de services à l'organisation hôte (il s'agit de la description d'un mode de fonctionnement plutôt que d'un secteur). Bon nombre d'organisations de télécommunication et de banques, par exemple, gèrent leur propre CSIRT interne, et ne proposent généralement pas de site Web au grand public.

Parties prenantes
Membres du personnel et département informatique de l'organisation hôte.

CSIRT dans le secteur militaire
Axe prioritaire
La fourniture de services à des organisations militaires chargées de l'infrastructure informatique nécessaire à la défense.

Parties prenantes
Personnel des institutions militaires ou entités étroitement liées à celles-ci (ministère de la Défense, par exemple).

CSIRT national
Axe prioritaire
Un CSIRT à vocation nationale se veut le point de contact du pays dans le domaine de la sécurité. Il arrive également que le CSIRT gouvernemental remplisse ce rôle (tel est le cas de l'UNIRAS au Royaume-Uni).

Parties prenantes
Le CSIRT national n'a généralement pas de parties prenantes directes, étant donné qu'il ne joue le plus souvent qu'un rôle d'intermédiaire pour l'ensemble du pays.

CSIRT dans le secteur de la PIC/PIIC
Axe prioritaire
La protection des infrastructures critiques (PIC) et/ou la protection de l'infrastructure d'information critique (PIIC). Ce type de CSIRT spécialisé travaille le plus souvent en étroite coopération avec un service officiel opérant dans le même domaine. Il couvre l'ensemble des secteurs informatiques critiques nationaux et protège les citoyens du pays concerné.

Parties prenantes
Administration publique; entreprises TI critiques; citoyens.

CSIRT dans le secteur des PME (petites et moyennes entreprises)
Axe prioritaire
CSIRT auto-organisé offrant ses services à l'intérieur de sa propre branche d'activité ou à des groupes d'usagers analogues.

Parties prenantes
Des PME et leur personnel, ou des groupes d'intérêts particuliers, telle l'Association des villes et municipalités d'un pays donné.

CSIRT dans le secteur universitaire
Axe prioritaire
La fourniture de services destinés aux établissements de l'enseignement supérieur, tels que des universités et des instituts de recherche, et à leur environnement Internet au niveau du campus.

Parties prenantes
Les parties prenantes de ce type de CSIRT sont en général les membres du personnel et les étudiants des universités.

Comme indiqué au paragraphe relatif aux CSIRT nationaux, une même équipe peut desservir plusieurs secteurs – ce dont il convient de tenir compte lors de l'analyse de ses parties prenantes et de leurs besoins.

CSIRT fictif (étape 1)
Phase de démarrage Il est décidé lors de la phase de démarrage de planifier le nouveau CSIRT en tant que CSIRT interne, destiné à offrir ses services à l'entreprise hôte, au département informatique local et au personnel. Il sera également appelé à fournir un soutien technique et à coordonner le traitement des incidents de sécurité informatique qui surviendraient entre les succursales.

5.2 Quels services un CSIRT peut-il offrir?

Nous avons franchi les deux premières étapes

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.

2. Définir les secteurs auxquels la nouvelle équipe destine ses services

>> L'étape suivante consiste à répondre à la question «Quels services offrir aux parties prenantes?»

Un CSIRT peut proposer un très large éventail de services, mais aucun CSIRT n'en propose actuellement la gamme complète. La sélection des services les mieux adaptés apparaît donc comme une décision essentielle. Le lecteur trouvera ci-après un bref aperçu de l'ensemble des services CSIRT connus, tels que définis dans le «*Handbook for CSIRT*» publié par le CERT/CC[6].

Services réactifs	**Services proactifs**	**Traitement des artefacts**
• **Alertes et avertissements** • **Traitement des incidents** • **Analyse des incidents** • **Appui à la réponse aux incidents** • **Coordination de la réponse aux incidents** • Réponse aux incidents sur place • Traitement des vulnérabilités • Analyse des vulnérabilités • Réponse aux vulnérabilités • Coordination des réponses aux vulnérabilités	• **Annonces** • Veille technologique • Audits ou évaluations de la sécurité • Configuration et maintenance de la sécurité • Développement d'outils de sécurité • Services de détection des intrusions • Diffusion d'informations relatives à la sécurité	• *Analyse des artefacts* • *Réponse aux artefacts* • *Coordination des réponses aux artefacts* ***Gestion de la qualité de la sécurité*** • *Analyse des risques* • *Continuité de l'activité et reprise après sinistre* • *Consultance en matière de sécurité* • *Sensibilisation* • *Éducation/formation* • *Évaluation ou certification des produits*

Fig. 1 Liste des services CSIRT du CERT/CC[7]

Les services de base (indiqués en caractères gras): une distinction est faite entre les services réactifs et les services proactifs. Les seconds visent à prévenir les incidents par des actions de sensibilisation et de formation, tandis que les premiers visent à gérer les incidents et à réduire les dommages qui en découlent.

Le traitement des artefacts comprend l'analyse de tout fichier ou objet présent dans un système et susceptible de participer à un acte malveillant (traces de virus, vers, script, cheval de Troie, etc.). Il inclut également le traitement et la diffusion des informations

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

[7] Liste des services CSIRT du CERT/CC: http://www.cert.org/csirts/services.html

obtenues aux fournisseurs (*vendors*) et autres parties intéressées, afin d'arrêter la propagation du logiciel malveillant et de limiter les risques.

Les services de gestion de la qualité de la sécurité poursuivent des objectifs de plus longue haleine et comportent des mesures axées sur le conseil et l'éducation.

Le lecteur trouver en annexe la description détaillée de ces différents services CSIRT.

Le choix des services les mieux adaptés à vos parties prenantes est une étape très importante qui sera décrite plus en détail au point *6.1 Définition du modèle financier*.

La plupart des CSIRT commencent par diffuser des «Alertes et avertissements», par faire des «Annonces» et par proposer un «Traitement des incidents» à l'intention de leurs parties prenantes. Ces services de base contribuent généralement à dresser un bon profil et à servir d'accroche auprès des parties prenantes, et sont perçus comme une réelle «valeur ajoutée».

Il est recommandé de débuter avec un groupe restreint de parties prenantes «pilotes», de prester les services de base pendant une période pilote déterminée, et de demander ensuite un retour d'information.
Les utilisateurs pilotes intéressés ont généralement des réactions constructives qui permettent d'affiner les services proposés.

CSIRT fictif (étape 2)

Choix des bons services

Il a été décidé à la première étape que le nouveau CSIRT axerait principalement son activité sur la fourniture de certains services de base aux membres du personnel.

Il est envisagé maintenant d'étendre la gamme des services à l'issue d'une phase pilote et d'y ajouter certains «Services de gestion de la sécurité». La décision sera prise sur la base du retour d'information en provenance des parties prenantes pilotes et en concertation avec le département Assurance qualité.

5.3 Analyse des parties prenantes et déclaration de mission

Nous avons franchi les trois premières étapes:

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.
2. Définir les secteurs auxquels la nouvelle équipe destine ses services.
3. Choisir les services que le CSIRT va offrir à ses parties prenantes.

>> L'étape suivante consiste à se demander «*Quel type d'approche adopter lors de la création du CSIRT?»*

Le moment est venu de procéder à une étude plus approfondie des parties prenantes dans le but d'opter pour les voies de communication les mieux adaptées. Il s'agit ici de définir:

- l'approche des parties prenantes en termes de communication;
- la déclaration de mission;
- un plan réaliste de mise en œuvre / de projet;
- les services CSIRT à offrir;
- la structure organisationnelle;
- la politique de sécurité de l'information;
- le profil du personnel à embaucher;
- l'utilisation de l'espace de bureau réservé au CSIRT;
- les possibilités de coopération avec d'autres CSIRT et d'éventuelles initiatives nationales.

Ces différentes démarches font l'objet d'une description plus approfondie dans les paragraphes qui vont suivre, et peuvent servir à l'élaboration du plan d'activités / de projet.

5.3.1 Approche des parties prenantes en termes de communication

Comme nous l'avons déjà indiqué, il est très important de connaître, outre votre propre stratégie de communication, les besoins de vos futures parties prenantes – en ce compris les voies de communication les mieux adaptées à la transmission des informations qui leur sont destinées.

Les théories de gestion décrivent plusieurs approches possibles de l'analyse du groupe cible. Nous en retiendrons deux: l'analyse FFOM (ou SWOT) et l'analyse PEST.

Analyse FFOM
Une analyse FFOM est un outil de planification stratégique permettant d'évaluer les **F**orces, **F**aiblesses, **O**pportunités et **M**enaces propres à un projet ou à une entreprise commerciale, voire à toute autre situation exigeant une décision. La technique est attribuée à Albert Humphrey, qui a dirigé à l'université de Stanford, au cours des années 1960 et 1970, un projet de recherche basé sur les 500 entreprises répertoriées par *Fortune*.[8]

Forces	**Faiblesses**
Opportunités	**Menaces**

Fig. 2 Matrice FFOM

Analyse PEST

[8] Analyse FFOM sur Wikipedia: http://fr.wikipedia.org/wiki/SWOT

L'analyse PEST est un autre instrument utile et largement utilisé pour mieux connaître les parties prenantes et, plus précisément, le contexte **P**olitique, **É**conomique, **S**ocioculturel et **T**echnologique dans lequel le CSIRT est appelé à fonctionner. Elle permet d'établir si la planification correspond bien à l'environnement et elle évite probablement l'adoption de mesures fondées sur de mauvaises hypothèses.

Politique	**Economique**
• Aspects écologiques/environnementaux • Législation en vigueur sur le marché national • Législation future • Législation européenne/internationale • Organismes et processus de réglementation • Politiques gouvernementales • Durée du mandat gouvernemental et changement de gouvernement • Politiques commerciales • Financement, subventions et initiatives • Actions de lobby/groupes de pression sur le marché national • Groupes de pression internationaux	• Conjoncture économique nationale • Tendances de l'économie nationale • Economies et tendances à l'étranger • Fiscalité générale • Fiscalité en matière de produits/services spécifiques • Aspects à caractère saisonnier/climatique • Cycles du marché et commerciaux • Facteurs propres à des secteurs spécifiques • Voies commerciales et évolution de la distribution • Stimulants au niveau du consommateur/de l'utilisateur final • Taux d'intérêt et de change
Socioculturel	**Technologique**
• Évolution du mode de vie • Démographie • Attitude et opinion des consommateurs • Avis des médias • Modifications législatives affectant les facteurs sociaux • Image de la marque, de l'entreprise, de la technologie • Habitudes d'achat des consommateurs • Mode et modèle d'identification • Grands évènements et influences • Accès et tendances en matière d'achat • Facteurs ethniques/religieux • Publicité	• Développement de technologies compétitives • Financement de la recherche • Technologies associées/liées • Technologies/solutions de substitution • Maturité des technologies • Maturité et capacité de l'industrie manufacturière • Information et communications • Technique/mécanismes d'achat des consommateurs • Législation en matière de technologies • Potentiel d'innovation • Accès aux technologies, octroi de licences, brevets • Aspects liés à la propriété intellectuelle

Fig. 3 Exemple d'analyse PEST

Une description détaillée de l'analyse PEST est proposée (en anglais) sur Wikipedia[9].

Les deux outils donnent un aperçu complet et structuré des besoins des parties prenantes. Les résultats obtenus viendront compléter la proposition d'activité et faciliteront ainsi l'obtention d'un financement pour la création du CSIRT.

Voies de communication

[9] Analyse PEST sur Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

L'examen des modes possibles de communication et de diffusion de l'information est un élément important de l'analyse («Comment communiquer avec les parties prenantes?»).

Des visites personnelles régulières auprès des parties prenantes sont recommandées dans la mesure du possible. Il a été établi en effet que les rencontres en face à face facilitent la coopération. Elles conduisent, pour autant que les interlocuteurs aient la volonté de collaborer, à l'instauration d'une relation plus ouverte.

Les CSIRT font généralement appel à toute une série de voies de communication. Il convient de citer, parmi celles qui ont fait la preuve de leur efficacité pratique et méritent donc d'être prises en considération:

- le site Web public;
- une zone du site Web réservée aux membres (groupe fermé d'utilisateurs);
- des formulaires électroniques pour signaler les incidents;
- les listes de distribution;
- le courriel personnalisé;
- le téléphone / la télécopie;
- le SMS;
- le «bon vieux» courrier postal;
- les rapports mensuel ou annuels.

Parallèlement à l'utilisation du courriel, des formulaires électroniques, du téléphone ou de la télécopie pour faciliter le traitement des incidents (réception des rapports d'incidents de la part des parties prenantes, coordination avec d'autres équipes ou retour d'information et soutien à la victime), la plupart des CSIRT publient leurs bulletins de sécurité sur un site Web accessible au grand public ou les diffusent à l'aide de listes de distribution.

! Il convient de veiller à ce que la diffusion de l'information soit, si possible, sécurisée. Ainsi par exemple, un courriel peut faire l'objet d'une signature numérique à l'aide d'un logiciel PGP, et les données relatives à un incident sensible devraient toujours être envoyées sous forme cryptée.

Pour informations complémentaires, voir le point *8.5 Outils à la disposition des CSIRT*. Voir également le point *2.3* du mémo *RFC2350*[10].

CSIRT fictif (étape 3a)

Analyse des parties prenantes et des voies de communication adéquates

Une réunion de brainstorming avec quelques représentants clés de la direction et les parties prenantes a permis d'obtenir suffisamment d'éléments pour procéder à une analyse FFOM. Celle-ci a conclu à la nécessité des services de bases suivants:

- Alertes et avertissements
- Traitement des incidents (analyse, soutien et coordination de la réponse)

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

- Annonces

L'information doit être diffusée de manière structurée, afin de parvenir au plus grand nombre possible de parties prenantes. Il est donc décidé que les alertes, avertissements et annonces seront publiés sous la forme de bulletins de sécurité sur un site Internet dédié et diffusés sur la base d'une liste de distribution. Le CSIRT privilégie l'utilisation du courriel, du téléphone et de la télécopie pour la réception des signalements d'incidents. Un formulaire électronique harmonisé est prévu à l'étape suivante.

Voir ci-après un exemple d'analyse FFOM.

Fig. 4

Forces • Il existe une certaine connaissance au sein de l'entreprise. • Le plan est bien accueilli et il existe une volonté de coopérer. • Soutien et financement par le conseil d'administration.	**Faiblesses** • Peu de communication entre les différents départements et les succursales. • Pas de coordination au niveau des incidents informatiques • Beaucoup de «petits départements»
Opportunités • Important afflux d'informations non structurées concernant les vulnérabilités • Important besoin de coordination • Réduction des pertes engendrées par les incidents • Nombreuses questions en suspens en matière de sécurité informatique • Education du personnel en matière de sécurité informatique	**Menaces** • Peu de trésorerie disponible • Peu de personnel à disposition • Attentes importantes • Culture

Exemple d'analyse FFOM

5.3.2 Déclaration de mission

L'étape qui fait suite à l'analyse des besoins et des attentes des parties prenantes en matière de services CSIRT est l'élaboration de la déclaration de mission.

Cette dernière décrit la fonction essentielle de l'organisation au sein de la société en termes de produits et de services fournis aux parties prenantes. Elle permet de faire connaître clairement l'existence et le rôle du nouveau CSIRT.

Il est recommandé de rédiger une déclaration de mission condensée, mais pas trop étroite, dans la mesure où elle ne subira probablement pas de modification avant plusieurs années.

Voici quelques exemples de déclarations de mission émanant de CSIRT déjà en activité: *«Le <nom du CSIRT> fournit des informations à ses <parties prenantes (les définir)> et les aide à mettre en œuvre des mesures proactives visant à réduire les risques*

d'incidents de sécurité informatique et à répondre à ce type d'incidents lorsqu'ils surviennent.»

«Offrir aux <Parties prenantes> une assistance en matière de prévention et de réponse aux incidents de sécurité liés à l'informatique»[11]

La déclaration de mission est une étape nécessaire et extrêmement importante au moment du démarrage. Voir le point 2.1 du mémo *RFC2350*[12] pour une description plus détaillée des informations qu'un CSIRT devrait publier.

CSIRT fictif (étape 3b)
La direction du CSIRT fictif a fait la déclaration de mission suivante: *« Le CSIRT fictif apporte des informations et une aide au personnel de sa société hôte en vue de réduire les risques d'incidents de sécurité informatique et de répondre à ce type d'incidents lorsqu'ils surviennent. »* Le CSIRT fictif précise ainsi clairement qu'il a une fonction interne essentiellement axée sur les questions de sécurité informatique.

[11] Déclaration de mission de Govcert.nl: http://www.govcert.nl

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

6 Élaboration du plan d'activités

Nous avons franchi les étapes ci-après:

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.
2. Définir les secteurs auxquels la nouvelle équipe destine ses services
3. Choisir les services que le CSIRT va offrir à ses parties prenantes.
4. Analyser l'environnement et les parties prenantes
5. Élaborer la déclaration de mission.

>> L'étape suivante est l'élaboration du plan d'activités.

L'analyse vous a donné un bon aperçu des besoins et des faiblesses (supposées) des parties prenantes, et ces différents éléments seront pris en compte à l'étape suivante.

6.1 Définition du modèle financier

Une série de services de base initiaux ont été sélectionnés à l'issue de l'analyse. Il convient de songer maintenant au modèle financier – autrement dit, de définir des conditions de prestation des services en question qui soient à la fois adaptées et payables.

Dans un monde parfait, le financement correspondrait aux besoins des parties prenantes; dans la réalité, toutefois, la gamme des services proposés doit tenir compte d'un budget déterminé. Mieux vaut donc commencer par la planification des aspects pécuniaires.

6.1.1 Modèle des coûts

Les deux principaux éléments qui déterminent les coûts sont la fixation des heures de service et le nombre (et la qualité) des effectifs à y affecter. Faut-il assurer une réponse aux incidents 24 heures par jour et 7 jours par semaine, ou ces services doivent-ils être uniquement accessibles durant les heures ouvrables?

Selon la disponibilité souhaitée et le matériel de bureau utilisé (est-il possible, par exemple, de travailler à domicile?), c'est le tableau de service basé sur des permanences ou le tableau de service prévoyant un horaire fixe qui sera le plus indiqué.

Le scénario suivant peut être envisagé: la prestation de services à la fois proactifs et réactifs durant les heures ouvrables, et la prestation de services restreints en dehors de celles-ci (intervention d'un membre du personnel de garde uniquement en cas de sinistre ou d'incident majeur, par exemple).

Une autre possibilité réside dans l'organisation d'une coopération internationale avec d'autres CSIRT pour assurer une prestation ininterrompue. On peut citer à cet égard

l'exemple de la mise en commun de leurs capacités par des équipes européennes et américaines: ainsi le CSIRT de Sun Microsystems, qui compte de très nombreuses succursales dans le monde et, partant, dans plusieurs fuseaux horaires (tout en faisant partie du même CSIRT), assure un service 24 heures par jour et 7 jours par semaine grâce à un roulement permanent de ses équipes réparties partout sur la planète. Cette manière de procéder limite les coûts, étant donné que les équipes travaillent uniquement pendant les heures normales de bureau tout en offrant leurs services à ceux qui en feraient la demande en dehors de leurs propres heures ouvrables.

Il est recommandé d'examiner de près avec les parties prenantes la nécessité réelle d'offrir des services 24 heures par jour et 7 jours par semaine. Les alertes et avertissements lancés durant la nuit ne servent pas à grand-chose si le destinataire ne les découvre que le lendemain matin. Il est parfois difficile de tracer la ligne de partage entre «avoir besoin d'un service» et «vouloir un service», mais il convient de souligner que l'horaire de travail fait une différence énorme en termes d'effectifs et d'installations, et qu'il a, par conséquent, un impact majeur sur le modèle de coûts.

6.1.2 Modèle des recettes

Une fois les coûts déterminés, il convient de se tourner vers les modèles de recettes possibles: comment les services planifiés peuvent-ils être financés? Plusieurs scénarios sont envisageables, parmi lesquels:

Utilisation de ressources existantes
Il est toujours utile d'évaluer les ressources qui existent ailleurs dans l'entreprise. Celle-ci occupe-t-elle déjà, au sein du département informatique en place, par exemple, des personnes suffisamment qualifiées en termes d'expérience et d'expertise? Des accords peuvent probablement être trouvés avec la direction en vue de détacher ce personnel auprès du CSIRT au moment de son démarrage, ou pour qu'il lui apporte un soutien ponctuel en cas de nécessité.

Cotisations
Une autre possibilité consiste à vendre les services du CSIRT aux parties prenantes en leur demandant une cotisation annuelle ou trimestrielle. Des services supplémentaires pourraient être rémunérés en fonction de leur utilisation (consultance ou audits de sécurité, par exemple).

Autre scénario envisageable: les services sont gratuits pour les parties prenantes (internes), mais payants pour les clients extérieurs. Une autre idée encore consisterait à publier les bulletins d'information et de sécurité sur le site Web public et de réserver aux membres une partie du site contenant des informations plus précises ou plus spécialisées.

L'expérience a montré que «l'abonnement par service CSIRT» ne permet pas réellement de générer des ressources financières suffisantes, surtout en phase de démarrage. Un certain nombre de frais fixes de base, inhérents à l'équipe et au matériel, doivent être payés à l'avance. Le financement de ce type de coûts par la vente de services CSIRT s'avère donc difficile et une analyse approfondie s'impose pour calculer le seuil de rentabilité.

Subvention
Une autre piste mérite d'être examinée, à savoir la demande d'une subvention au gouvernement ou à un organisme officiel – la plupart des pays consacrant aujourd'hui des fonds aux projets de sécurité informatique. Une prise de contact avec le ministère de l'Intérieur peut être une première démarche utile à cette fin.

Rien n'empêche, bien entendu, de conjuguer différents modèles de recettes.

6.2 Définition de la structure organisationnelle

La structure organisationnelle adéquate d'un CSIRT dépend largement de la structure déjà en place au sein de l'organisation hôte et des parties prenantes. Elle est également liée à l'accessibilité des experts qui seront recrutés à titre permanent ou sur une base ad hoc.

Un CSIRT type définit les rôles suivants au sein de son équipe:

Direction
- Directeur général

Personnel
- Responsable administratif
- Comptable
- Conseiller en communication
- Conseiller juridique

Équipe technique opérationnelle
- Chef d'équipe technique
- Techniciens prestant les services CSIRT
- Chercheurs

Consultants externes
- Recrutés en fonction des besoins

Il est extrêmement utile d'avoir un spécialiste des questions juridiques au sein de l'équipe, surtout lors de la phase de démarrage du CSIRT. Sa présence génère des coûts supplémentaires mais elle permettra, en définitive, de gagner beaucoup de temps et d'éviter les problèmes au plan légal.

Il s'avère également utile, selon la diversité des expertises parmi les parties prenantes et lorsque le CSIRT a un haut profil médiatique, d'inclure un spécialiste de la communication au sein de l'équipe. Ce type d'expert est en mesure de traduire les aspects techniques parfois difficiles en messages compréhensibles pour les parties prenantes ou les interlocuteurs des médias. Il/elle peut également assurer la remontée des informations des parties prenantes vers les techniciens, ou agir en qualité de «traducteur» ou de «facilitateur» entre ces deux groupes.

Voici quelques exemples de modèles organisationnels appliqués par des CSIRT déjà en activité.

6.2.1 Le modèle organisationnel indépendant

Le CSIRT est conçu et agit comme une organisation indépendante, dotée de sa propre direction et de son propre personnel.

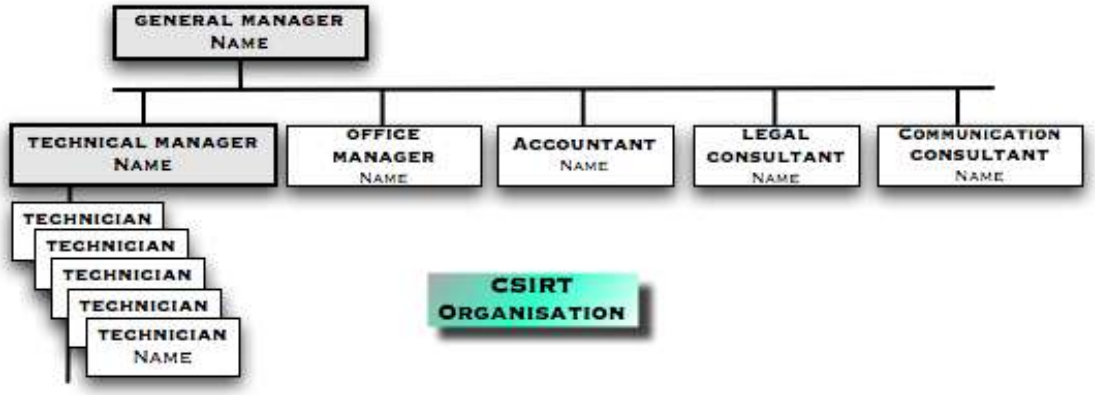


Fig. 5 Modèle organisationnel indépendant

6.2.2 Le modèle organisationnel intégré

Ce modèle peut être appliqué lorsque un CSIRT est créé au sein d'une organisation existante en faisant appel à un département informatique déjà en place, par exemple. Le CSIRT est dirigé par un chef d'équipe qui, responsable des activités confiées au CSIRT, réunit les techniciens nécessaires pour résoudre des incidents ou pour mener à bien les tâches qui lui sont assignées, et peut demander une aide spécialisée au sein de l'organisation existante.

Ce modèle convient également lorsque des situations particulières se présentent. On attribue alors à l'équipe un nombre déterminé d'ETP (équivalents temps plein). Le service des abus chez un fournisseur d'accès Internet, par exemple, requiert au minimum un équivalent temps plein, voire (le plus souvent) plusieurs.

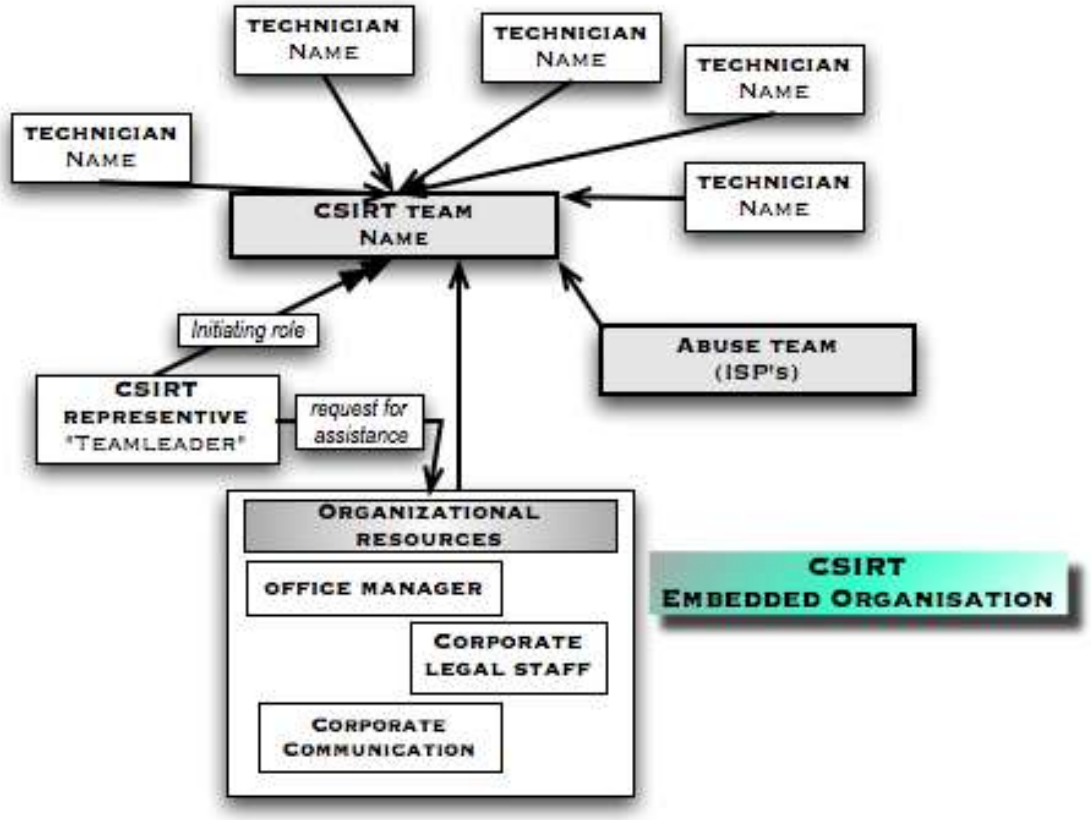


Fig. 6 Modèle organisationnel intégré

6.2.3 Le modèle «campus»

Comme son nom le laisse entendre, le modèle «campus» est principalement adopté par des CSIRT du monde universitaire et de la recherche. La plupart des organisations de ce domaine comprennent plusieurs universités et campus disséminés sur un territoire régional, voire sur l'ensemble du territoire national (tel est notamment le cas des réseaux nationaux de recherche ou RNR). Ces organisations fonctionnent le plus souvent indépendamment les unes des autres, et gèrent chacune leur propre CSIRT. Ces équipes sont néanmoins chapeautées par un CSIRT «mère» ou «de base», qui en assure la coordination et constitue le point de contact unique pour le monde extérieur. Il assure en outre, dans la plupart des cas, les services CSIRT essentiels, et la transmission des informations relatives aux incidents aux CSIRT «campus» concernés.
Certains CSIRT communiquent eux-mêmes leurs services de base aux autres CSIRT «campus», ce qui réduit les frais généraux pour le CSIRT central.

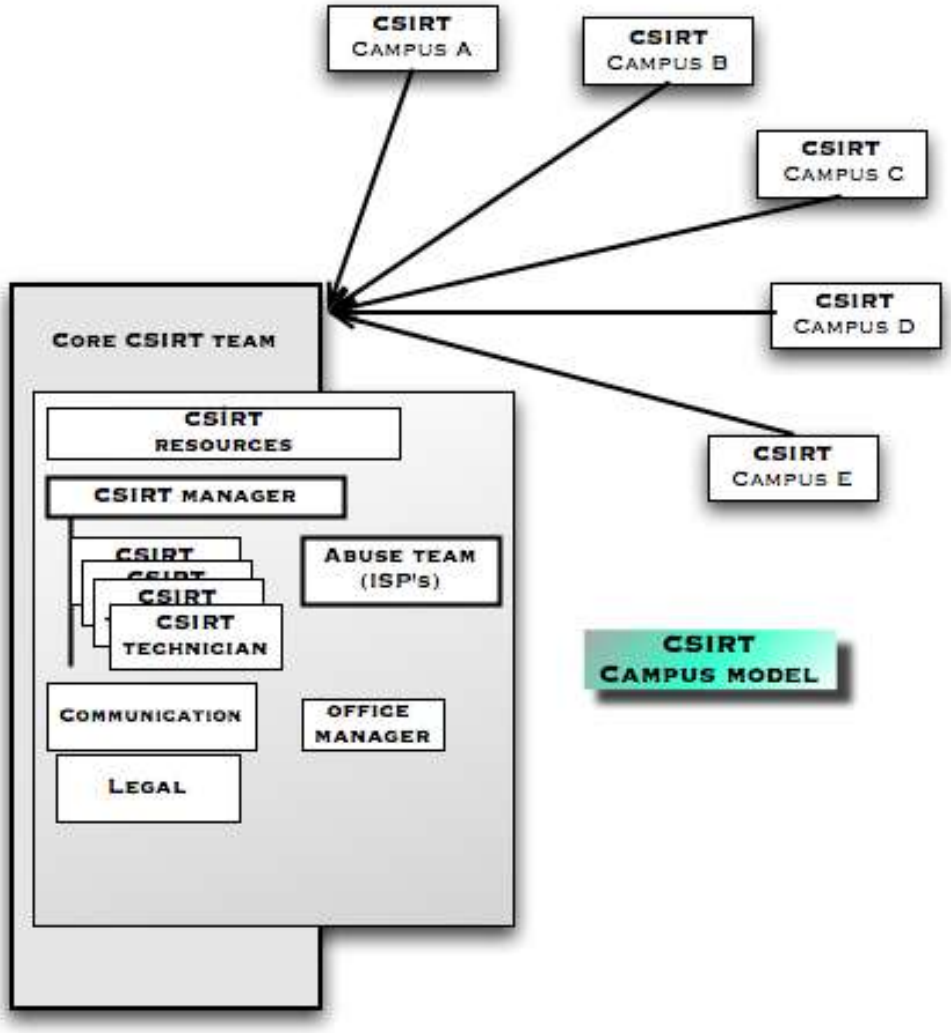


Fig. 7 Modèle «Campus»

6.2.4 Modèle volontaire

Ce modèle organisationnel désigne le regroupement de personnes (spécialistes) en vue d'un échange mutuel – et de la communication vers l'extérieur – de conseils et d'assistance à titre volontaire. Il s'agit d'une communauté peu structurée et largement dépendante de la motivation des participants.

Ce modèle a notamment été choisi par la communauté WARP[13].

6.3 Recrutement du personnel adéquat

Après avoir déterminé les services et le niveau de soutien à fournir, et après avoir choisi un modèle organisationnel, le moment est venu de trouver les personnes qualifiées nécessaires à la réalisation des objectifs fixés.

Il est pratiquement impossible de citer des chiffres fermes en ce qui concerne le nombre de techniciens requis à cette fin, mais les valeurs suivantes peuvent être considérées comme une approche valable:

- pour assurer deux services de base, à savoir la diffusion de bulletins de sécurité et le traitement des incidents: **4** ETP au minimum;
- pour assurer un service CSIRT complet pendant les heures ouvrables, et la maintenance des systèmes: **6 à 8** ETP au minimum;
- pour assurer une rotation de personnel complet 24 heures par jour et 7 jours par semaine (2 équipes en dehors des heures de bureau) le minimum est de l'ordre de **12** ETP.

Ces chiffres incluent la redondance en cas de maladie, de congé, etc. Il convient également de vérifier les conventions collectives locales. Des coûts supplémentaires doivent parfois être assumés sous la forme de primes lorsque les travailleurs prestent en dehors des heures habituelles de bureau.

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

Ci-après un bref aperçu des principales compétences escomptées des techniciens spécialisés des CSIRT

Compétences personnelles

- Flexibilité, créativité et bon esprit d'équipe
- Grande capacité d'analyse
- Capacité d'expliquer des questions techniques complexes en termes simples
- Bonne perception de la confidentialité et du travail basé sur des procédures
- Aptitudes à l'organisation
- Résistance au stress
- Bonnes aptitudes à la communication et à la rédaction
- Ouverture d'esprit et volonté d'apprendre

Compétences techniques

- Large maîtrise de la technologie et des protocoles Internet
- Connaissance des systèmes Linux et Unix (selon l'équipement des parties prenantes)
- Connaissance des systèmes Windows (selon l'équipement des parties prenantes)
- Connaissance des équipements d'infrastructure de réseau (routeurs, commutateurs, DNS, Proxy, courriel, etc.)
- Connaissance des applications Internet (SMTP, HTTP(s), FTP, telnet, SSH, etc.)
- Connaissance des menaces pour la sécurité (déni de service distribué (DDoS), hameçonnage, refonte de site Web (*Defacing*), reniflage, etc.)
- Maîtrise de l'évaluation des risques et des applications pratiques

Compétences supplémentaires

- Disposition à travailler dans un système de 24 heures par jour et 7 jours par semaine ou dans un système de permanence (selon le type de service)
- Distance maximale de déplacement (en cas de disponibilité d'urgence au bureau: temps maximum de déplacement)
- Niveau de formation
- Expérience professionnelle dans le domaine de la sécurité informatique

CSIRT fictif (étape 4)

Élaboration du plan d'activités

Modèle financier

Étant donné que la société a une activité en ligne et un département informatique fonctionnant l'une et l'autre 24 heures par jour et 7 jours par semaine, elle a décidé de proposer un service complet durant les heures ouvrables et un service de garde en dehors de celles-ci. Les services destinés aux parties prenantes seront fournis gratuitement, mais l'éventualité de services prestés à l'intention de clients extérieurs sera envisagée lors de la phase pilote et d'évaluation.

Modèle des recettes

Au cours de la phase de démarrage et pilote, le CSIRT sera financé par la société hôte. Un financement complémentaire sera examiné au cours de la phase pilote et d'évaluation, en envisageant notamment la vente de services à des clients extérieurs.

Modèle organisationnel
L'organisation hôte étant une petite entreprise, c'est le modèle intégré qui est retenu.
Une équipe de trois personnes assurera les services de base pendant les heures ouvrables (diffusion des bulletins de sécurité et traitement/coordination des incidents).

Le département informatique de l'entreprise occupe déjà du personnel doté des compétences requises. Un accord est conclu avec ce département, afin que le nouveau CSIRT puisse faire appel à une aide ponctuelle, le cas échéant. Le deuxième niveau de leurs techniciens de garde pourra également être mobilisé.
Une équipe CSIRT de base comprenant quatre membres à temps plein et cinq membres supplémentaires sera mise en place. L'un d'eux est également disponible en rotation.

Personnel
Le chef d'équipe CSIRT a des antécédents professionnels en matière de sécurité et de support au premier et au second niveau d'intervention, et il a déjà travaillé dans un contexte de gestion de crise. Les trois autres membres de l'équipe sont des spécialistes de la sécurité. Les membres de l'équipe CSIRT détachés à temps partiel par le département informatique sont, pour leur part, des spécialistes de l'infrastructure en place dans la société.

6.4 Utilisation et équipement de l'espace de bureau

L'équipement et l'utilisation de l'espace de bureau, et la sécurité physique, sont des thèmes extrêmement vastes, dont nous ne pouvons faire ici la description exhaustive. Nous nous contenterons donc d'en proposer un bref aperçu.

Des informations complémentaires à propos de la sécurité physique peuvent être consultées sur:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

«Renforcer le bâtiment»
Étant donné que les CSIRT traitent souvent des informations très sensibles, mieux vaut confier à leur équipe le soin d'assurer la sécurité physique des locaux. Les mesures à prendre à cette fin dépendent largement des installations et infrastructures en place, et de la politique déjà pratiquée par la société hôte en matière de sécurité de l'information.

Les gouvernements, par exemple, appliquent des systèmes de classification sécuritaire et se montrent très rigoureux en ce qui concerne le traitement des informations confidentielles. Assurez-vous auprès de votre propre entreprise ou institution des règles et politiques locales en la matière.

Un nouveau CSIRT doit généralement compter sur la coopération de son organisation hôte pour se familiariser avec ces règles et politiques locales, et autres aspects juridiques.

Une description exhaustive de l'ensemble des mesures à prendre au niveau des équipements et de la sécurité sortirait du cadre du présent document. Nous récapitulons néanmoins ci-dessous les éléments que votre CSIRT doit impérativement prendre en compte:

Règles générales concernant le bâtiment
- Instaurer un contrôle des accès.
- Réserver au minimum l'accès du bureau du CSIRT à son propre personnel.
- Surveiller les bureaux et les entrées à l'aide de caméras.
- Archiver les informations confidentielles dans des armoires fermées à clé ou dans un coffre-fort.
- Utiliser des systèmes informatiques sûrs.

Règles générales concernant le matériel informatique
- Utiliser un matériel que le personnel maîtrise
- Consolider tous les systèmes
- Appliquer des correctifs et procéder à la mise à jour de tous les systèmes avant leur connexion à Internet
- Utiliser des logiciels de sécurité (pare-feu, scanners anti-virus multiples, anti-logiciel espion, etc.)

Règles concernant les canaux de communication
- Site Web public
- Partie du site réservée aux membres (groupe fermé d'utilisateurs)
- Formulaires électroniques pour le signalement des incidents
- Courriel (support de PGP / GPG / S/MIME)
- Logiciel de liste de distribution
- Mettre un numéro téléphonique dédié à la disposition des parties prenantes:
    - téléphone
    - télécopie
    - SMS

Système(s) de localisation des enregistrements
- Base de données de contact contenant les coordonnées des membres de l'équipe, d'autres équipes, etc.
- Outils de gestion des relations-clients
- Système de ticket pour le traitement des incidents

Utiliser dès le départ le style de l'entreprise pour
- La présentation standard des courriels et des bulletins de sécurité
- Le «bon vieux» papier à lettre
- Les rapports mensuels ou annuels
- Le formulaire de signalement d'incident

Autres aspects
- Prévoir un mode de communication hors bande en cas d'attaque
- Prévoir une redondance pour la connectivité Internet

Se référer au point 8.5 pour des outils plus spécifiques mis à la disposition des CSIRT.

6.5 Développement d'une politique de sécurité de l'information

Une politique de sécurité de l'information «sur mesure» est mise en place selon le type de CSIRT. Outre la description des procédures et processus opérationnels et administratifs souhaités, elle devra veiller au respect des lois et normes applicables, notamment en matière de responsabilité du CSIRT. Celui-ci est généralement tenu de se conformer aux dispositions législatives et réglementaires nationales en vigueur, souvent mises en œuvre dans le cadre du droit communautaire (directives en général) et d'autres accords internationaux. Les normes n'ont pas nécessairement d'effet contraignant direct, mais peuvent être rendues obligatoires ou recommandées par les dispositions législatives et réglementaires.

Ci-après une brève énumération des lois et politiques susceptibles d'être d'application:

Au plan national
- Lois diverses sur les technologies de l'information, les télécommunications, les médias
- Loi sur la protection des données et de la vie privée
- Lois et règlements sur la rétention des données
- Législation en matière de finances, de comptabilité et de gestion d'entreprise
- Codes de conduite en matière de gouvernance d'entreprise et de gouvernance informatique

Au plan européen
- Directive sur un cadre communautaire pour les signatures électroniques (1999/93/CE)
- Directives relatives à la protection des données (1995/46/CE) et à la protection de la vie privée dans le secteur des communications électroniques (2002/58/CE)
- Directives relatives à l'accès et aux services de réseaux de communications électroniques (2002/19/CE – 2002/22/CE)
- Directives relatives au droit des sociétés (huitième directive sur le droit des sociétés, par exemple)

Au plan international
- Accord de Bâle II (en ce qui concerne plus particulièrement la gestion du risque opérationnel)
- Convention du Conseil de l'Europe sur la cybercriminalité
- Convention du Conseil de l'Europe sur la sauvegarde des droits de l'homme (article 8 relatif au respect de la vie privée)
- Normes comptables internationales (IAS – elles exigent, dans une certaine mesure, des contrôles informatiques)

Normes

- British Standard BS 7799 (Sécurité informatique)
- Normes internationales ISO2700x (Systèmes de gestion de la sécurité de l'information)
- IT-Grundschutzbuch (Allemagne), EBIOS (France) et autres variantes nationales

Pour déterminer si votre CSIRT respecte la législation nationale et internationale, veuillez consulter votre conseiller juridique.

Les questions les plus élémentaires auxquelles votre politique de traitement de l'information doit fournir une réponse sont les suivantes:

- Comment l'information entrante est-elle «étiquetée» ou «classifiée»?
- Comment l'information est-elle traitée, en termes d'exclusivité plus particulièrement?
- Quelles sont les considérations prises en compte pour ce qui concerne la divulgation de l'information, en particulier lorsqu'une information relative à un incident est transmise à d'autres équipes ou sites?
- Des considérations légales doivent-elles être prises en compte pour ce qui concerne le traitement de l'information?
- Avez-vous une politique concernant le recours à la cryptographie pour protéger l'exclusivité et l'intégrité de la communication de données et/ou d'archives, par courrier électronique en particulier?
- Cette politique s'accompagne-t-elle éventuellement de conditions légales limites telles qu'une disposition de mise en dépôt de clés ou le caractère exécutoire du décryptage en cas de poursuites en justice?

CSIRT fictif (étape 5)

Équipement et localisation de l'espace de bureau

Étant donné que la société hôte s'est déjà dotée d'une sécurité physique efficace, le nouveau CSIRT est lui-même bien protégé. Un «centre de crise» est prévu pour permettre la coordination en cas d'urgence. Un coffre-fort est acheté pour le matériel d'encryptage et les documents sensibles. Une ligne téléphonique séparée a été installée, central compris, pour faciliter l'accès au numéro d'urgence pendant les heures ouvrables et au téléphone mobile «de garde» en dehors de celles-ci en utilisant le même numéro d'appel.

Le matériel et le site Internet de la société déjà en place peuvent également servir à diffuser les informations relevant du CSIRT. Une liste de distribution est établie et tenue à jour; elle est partiellement réservée à la communication entre les membres de l'équipe, ainsi qu'avec d'autres équipes. Toutes les coordonnées de contact des membres du personnel sont stockées dans une base de données, dont une version imprimée est conservée dans le coffre-fort.

Réglementation

Étant donné que le CSIRT est intégré dans une société ayant déjà adopté une politique en matière de sécurité de l'information, les mesures correspondantes au niveau du CSIRT ont été prises avec l'aide du conseiller juridique de l'entreprise.

6.6 Coopération avec d'autres CSIRT et d'éventuelles initiatives nationales

Nous avons déjà mentionné à plusieurs reprises dans ce document l'existence d'autres initiatives en matière de CSIRT et la nécessité impérative d'une coordination à leur niveau. Il est recommandé de prendre contact le plus rapidement possible avec d'autres CSIRT, afin d'être introduit auprès de leurs communautés. Ces dernières se montrent généralement très disposées à aider les nouvelles équipes à démarrer.

Le répertoire ENISA des activités des CERT en Europe (*Inventory of CERT activities in Europe*[14]) constitue un excellent point de départ pour rechercher d'autres CSIRT dans le pays ou des activités menées en coopération à l'échelon national.

Si vous souhaitez une assistance dans la recherche d'une source d'information concernant les CSIRT, il vous suffit de contacter les spécialistes de l'ENISA dans ce domaine:

CERT-Relations@enisa.europa.eu

Voici un aperçu des activités des communautés CSIRT. Il convient de se référer au répertoire (*Inventory*) pour une description plus complète et des informations complémentaires.

Initiative CSIRT européenne

TF-CSIRT[15]

La Task force CSIRT (TF-CSIRT) favorise la collaboration entre les centres d'alerte et de réaction aux incidents de sécurité informatique d'Europe. Elle a pour mission de mettre en place un forum d'échange d'expériences et de connaissances, d'instaurer des services pilotes à l'intention de la communauté européenne des CSIRT et d'aider à la création de nouveaux CSIRT.

Les objectifs principaux de la TF-CSIRT sont donc:

- la création d'un forum d'échange d'expériences et de connaissances;
- l'instauration de services pilotes à l'intention de la communauté européenne des CSIRT;
- la promotion de normes et procédures communes de réponse aux incidents de sécurité
- l'aide à la création de nouveaux CSIRT et à la formation de leur personnel;
- les activités de la TF-CSIRT sont focalisées sur l'Europe et les pays voisins, conformément aux termes de référence approuvés par le comité technique TERENA en date du 15 septembre 2004.

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

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

Initiative CSIRT mondiale

FIRST[16]

FIRST est la première organisation reconnue en tant que leader mondial du secteur de la réponse aux incidents. En s'affiliant à FIRST, les équipes opérant dans ce domaine peuvent agir plus efficacement, que ce soit de manière réactive ou proactive.

FIRST regroupe un large éventail d'équipes de réponse aux incidents informatiques, puisqu'elles représentent des organisations gouvernementales, commerciales et éducatives. FIRST vise à stimuler la coopération et la coordination en matière de prévention des incidents, à accélérer les réactions en cas d'incident et à promouvoir le partage d'informations entre ses membres et dans l'ensemble de la communauté.

Outre le réseau de confiance qu'il constitue au sein de la communauté mondiale de la réponse aux incidents, FIRST fournit également une série de services à valeur ajoutée.

CSIRT fictif (étape 6)
Recherche de coopération Plusieurs CSIRT opérant dans le pays ont été rapidement recensés grâce au répertoire de l'ENISA, et des contacts ont été pris. Une visite du chef d'équipe récemment recruté a été organisée chez l'un d'eux. Il a été informé à cette occasion des activités CSIRT menées au plan national. Il a également participé à une réunion qui lui a permis de rassembler des exemples de méthodes de travail et de bénéficier du soutien de plusieurs autres équipes.

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

7 Promotion du plan d'activités

Nous avons déjà franchi les étapes ci-après:

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.
2. Définir les secteurs auxquels la nouvelle équipe destine ses services
3. Choisir les services que le CSIRT va offrir à ses parties prenantes.
4. Analyser l'environnement et les parties prenantes
5. Élaborer la déclaration de mission
6. Développer le plan d'activité
    a. Définition du modèle financier
    b. Définition de la structure organisationnelle
    c. Début du recrutement de personnel
    d. Utilisation et équipement de l'espace de bureau
    e. Développement d'une politique de sécurité de l'information
    f. Recherche de partenaires en vue d'une coopération

>> L'étape suivante consiste à intégrer ce qui précède dans un plan de projet et à démarrer!

L'une des meilleures manières de planifier un projet consiste à en établir la justification stratégique et commerciale (*business case*), laquelle servira, en outre, à obtenir l'appui de la direction, ainsi que des ressources budgétaires ou autres.

L'expérience montre qu'il est utile de tenir constamment la direction au courant, afin de la maintenir très sensibilisée à l'égard des problèmes de sécurité informatique et de mobiliser, partant, son soutien permanent à l'égard du CSIRT.

L'établissement des arguments économiques commence par l'analyse des problèmes et des opportunités à l'aide du modèle décrit au point *5.3 Analyse des parties prenantes*, et par un contact étroit avec les parties prenantes éventuelles.

Comme nous l'avons déjà indiqué, il y a beaucoup d'aspects à prendre en compte au moment du démarrage d'un CSIRT, et mieux vaut garder la possibilité d'adapter les composantes du projet au fur et à mesure que les besoins du CSIRT se précisent.

Il est recommandé, lorsque l'on fait rapport à la direction, de présenter une argumentation aussi actualisée que possible en s'appuyant sur des articles récemment publiés dans la presse ou sur Internet, et en expliquant pourquoi le service CSIRT et la coordination interne des incidents sont indispensables à la protection du patrimoine de l'entreprise. Il convient également d'insister sur le fait que seul un soutien permanent en matière de sécurité informatique permet d'assurer la stabilité de l'activité, en particulier s'il s'agit d'une entreprise ou d'une institution liée aux technologies de l'information.

(Comme le dit très justement Bruce Schneier: «*La sécurité n'est pas un produit, mais un processus*[17]*!»)*

Le schéma ci-après, qui provient du CERT/CC, est l'illustration par excellence des problèmes de sécurité:

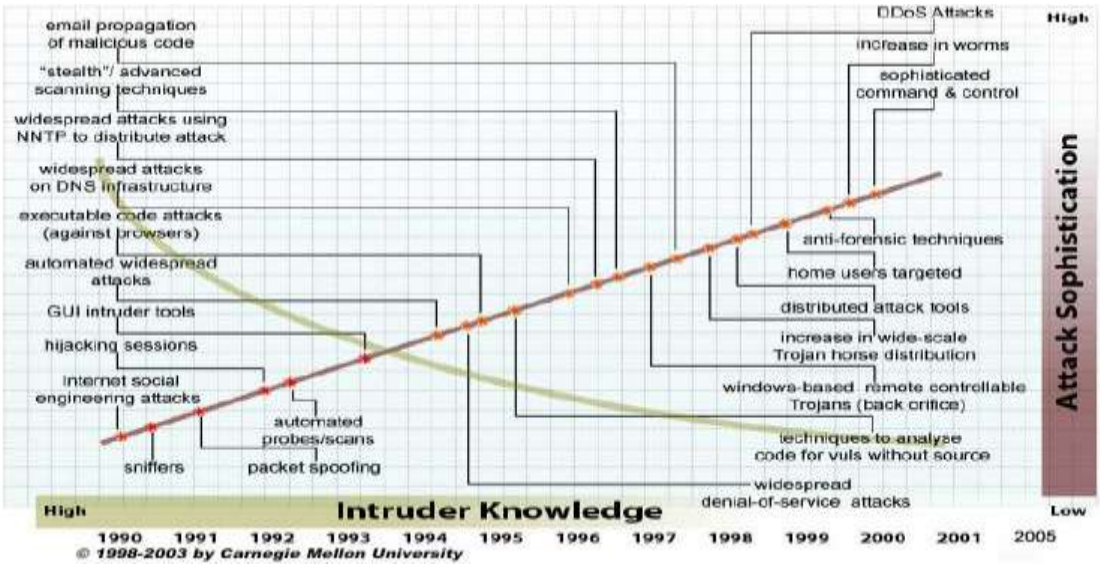


Fig. 8 La connaissance des intrus par rapport à la sophistication des attaques (source CERT-CC[18]*)*

Il montre bien l'évolution en matière de sécurité informatique, et plus particulièrement la diminution des compétences requises pour procéder à des attaques de plus en plus sophistiquées.

Il est intéressant de souligner également le délai de plus en plus court qui s'écoule entre la mise sur le marché de mises à jour destinées à remédier aux vulnérabilités des logiciels et la survenance d'attaques à leur encontre:

Correctif -> Exploit		**Vitesse de propagation**	
Nimda:	11 mois	Code Red:	Jours
Slammer:	6 mois	Nimda:	Heures
Nachi:	5 mois	Slammer:	Minutes
Blaster:	3 semaines		
Witty:	1 jour (!)		

Il est également utile d'inclure dans la présentation certaines données rassemblées à propos d'incidents, les améliorations possibles et les enseignements tirés.

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

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

7.1 Description du plan d'activités et des éléments déclencheurs

Une présentation à la direction, y compris la promotion du CSIRT, ne constitue pas à elle seule une justification stratégique et commerciale; mais, bien menée, elle permet le plus souvent d'obtenir l'appui de la direction au projet. L'argumentation en question ne doit d'ailleurs pas être envisagée comme un simple exercice de gestion: elle doit également étayer la communication vers l'équipe et les parties prenantes. L'expression «*justification stratégique et commerciale*» - ou *business case* – peut avoir une consonance très commerciale et sembler très éloignée de la pratique d'un CSIRT au quotidien, mais elle est utile pour définir les priorités et les orientations au départ.

Répondre aux questions ci-après peut être une bonne approche de l'élaboration de ce type d'argumentation – étant entendu que les exemples sont fictifs et uniquement fournis à titre d'illustration, et que les vraies réponses dépendront des circonstances réelles.

- Quel est le problème?
- Que souhaitez-vous réaliser pour vos parties prenantes?
- Qu'arrivera-t-il si vous ne faites rien?
- Qu'arrivera-t-il si vous agissez?
- Qu'est-ce que cela va coûter?
- Quels seront les acquis?
- Quel sera le calendrier d'exécution?

Quel est le problème?
L'idée de créer un CSIRT naît le plus souvent lorsque la sécurité informatique devient un élément essentiel de l'activité de base d'une entreprise ou d'une institution; les incidents de sécurité informatique deviennent dès lors un risque d'exploitation dont la limitation doit faire partie de l'activité courante.

La plupart des entreprises et des institutions disposent d'un département de support technique permanent ou d'un service d'assistance, mais les incidents de sécurité ne sont généralement pas traités de manière suffisamment rigoureuse et structurée. Le domaine des incidents de sécurité requiert, dans la plupart des cas, des compétences et une attention plus poussées, et l'adoption d'une approche davantage structurée permet notamment d'atténuer les risques d'exploitation et de préjudice à l'entreprise.

Le problème réside le plus souvent dans le manque de coordination et dans la non utilisation des connaissances existantes pour traiter les incidents, ce qui permettrait pourtant d'éviter qu'ils se reproduisent et de prévenir les risques de pertes financières et/ou de préjudice à la réputation de l'entreprise ou de l'institution.

Quels sont les objectifs à réaliser vis-à-vis des parties prenantes?
Comme nous l'avons déjà expliqué, votre CSIRT sera au service de ses parties prenantes en les aidant à résoudre les incidents et problèmes de sécurité informatique. Relever le niveau des connaissances dans ce domaine et instaurer une culture de sensibilisation à la sécurité constituent des objectifs complémentaires.

Cette culture encourage les mesures proactives et préventives qui, adoptées dès le départ, réduisent les coûts opérationnels.

Ce type de culture de coopération et d'assistance stimule en outre, le plus souvent, une volonté d'efficience dans l'ensemble de l'entreprise ou de l'institution où elle est introduite.

Que se passe-t-il si rien n'est fait?
Une approche non structurée du traitement de la sécurité informatique risque d'entraîner des dommages supplémentaires, dont le moindre n'est pas le préjudice causé à l'image de l'institution ou de l'entreprise. Des pertes financières et des répercussions juridiques peuvent également survenir.

Que se passe-t-il si des mesures sont prises?
La sensibilisation à la survenance de problèmes de sécurité est renforcée, ce qui permet de les résoudre plus efficacement et d'éviter des pertes futures.

Qu'est-ce que cela va coûter?
Le coût comprendra, selon le modèle organisationnel, les salaires des membres de l'équipe CSIRT et de l'organisation, les équipements, les outils et les licences d'utilisation des logiciels.

Quels seront les acquis?
L'entreprise ou l'institution gagnera, en fonction de son activité et de ses pertes antérieures, davantage de transparence au niveau des procédures et des pratiques de sécurité, et protégera ainsi des éléments essentiels de son patrimoine.

Quel sera le calendrier d'exécution?
Voir le chapitre 12 pour la description d'un exemple de plan de projet.

Exemples d'approches et d'arguments économiques
Ci-après quelques exemples d'études de cas qui méritent un examen plus approfondi:

- http://www.cert.org/csirts/AFI_case-study.html
  Création d'un CSIRT au sein d'une institution financière

  Ce document vise à faire connaître les enseignements qu'une institution financière (appelée en l'occurrence AFI) a tiré du développement et de la mise en œuvre d'un plan destiné à remédier aux préoccupations en matière de sécurité, d'une part, et d'un CSIRT, d'autre part.

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Résumé de la justification stratégique et commerciale (*business case*) du CERT POLSKA (diaporama en format PDF).

- http://www.auscert.org.au/render.html?it=2252
  Constituer une équipe de réponse aux incidents (IRT - *Incident Response Team*) durant les années 1990 était un défi de taille, faute d'expérience en la matière. Le document montre le rôle qu'une IRT peut jouer dans la communauté, et les différents

aspects à envisager, tant lors de sa création qu'après le démarrage de ses activités. Il constitue également une lecture intéressante pour des IRT déjà en place en attirant leur attention sur des aspects qu'elles n'auraient pas encore abordés.

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

  Cette étude de cas décrit la migration d'une société d'assurance vers un système de sécurité à l'échelon de l'entreprise: un exemple d'application qui indique une voie à suivre lors de la création d'un système de sécurité ou d'une migration vers ce type de système. Seul un système très élémentaire de sécurité en ligne contrôlait, au départ, l'accès aux données de l'entreprise. Les risques étaient donc importants – aucun contrôle d'intégrité n'étant prévu en dehors de l'environnement en ligne. Toute personne ayant des connaissances élémentaires de programmation pouvait compléter, modifier et/ou supprimer les données de production.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriott's e-security strategy: business-IT collaboration, par John Desmond

  De l'expérience de Chris Zoladz (Marriott International, Inc.), la sécurité du commerce électronique est un processus, et non pas un projet. Tel a été son message lors de la récente conférence-exposition sur la sécurité électronique, organisée à Boston avec le parrainage de l'Intermedia Group. En sa qualité de vice-président chargé de la protection de l'information pour le groupe Marriott, Zoladz rapporte au département juridique, bien qu'il ne soit pas juriste. Il a pour mission de repérer où sont stockées les informations commerciales les plus précieuses du groupe, et de déterminer de quelle manière elles circulent à l'intérieur et à l'extérieur de celui-ci. Marriott a établi une responsabilité distincte en ce qui concerne l'infrastructure technique qui sous-tend la sécurité; elle est confiée à l'architecte en sécurité informatique.

CSIRT fictif (étape 7)
Promotion du plan d'activités

Il est décidé de rassembler des faits et des chiffres à partir de l'historique de l'entreprise – une démarche particulièrement utile pour avoir un aperçu statistique de la situation en matière de sécurité informatique. Cette collecte de données doit se poursuivre après la mise en service du CSIRT, afin de maintenir les statistiques à jour.

D'autres CSIRT nationaux ont été contactés et interrogés à propos de la présentation de leurs arguments économiques (*business case*). Ils ont apporté une aide sous la forme de diapositives contenant des informations relatives aux développements récents en matière d'incidents liés à la sécurité informatique et aux coûts qu'ils engendrent.

Il n'a pas été nécessaire, dans notre exemple de CSIRT fictif, de déployer beaucoup d'efforts pour convaincre la direction de l'importance de l'activité informatique: le feu vert pour la première étape a donc été facilement obtenu. Une justification stratégique et commerciale et un plan de projet ont été élaborés, y compris une estimation des coûts de création et d'exploitation.

8 Exemples de procédures opérationnelles et techniques (workflows)

Nous avons déjà franchi les étapes ci-après:

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.
2. Définir les secteurs auxquels la nouvelle équipe destine ses services.
3. Choisir les services que le CSIRT va offrir à ses parties prenantes.
4. Analyser l'environnement et les parties prenantes.
5. Élaborer la déclaration de mission.
6. Développer le plan d'activités
   a. Définition du modèle financier.
   b. Définition de la structure organisationnelle.
   c. Début du recrutement de personnel.
   d. Utilisation et équipement de l'espace de bureau.
   e. Développement d'une politique de sécurité de l'information.
   f. Recherche de partenaires en vue d'une coopération.
7. Promouvoir le plan d'activités
   a. Approbation de la justification stratégique et commerciale (*business case*).
   b. Intégration de tous les éléments dans un plan de projet.

>> La prochaine étape consiste à rendre le CSIRT opérationnel.

L'instauration de flux de travail clairement définis va améliorer la qualité et la vitesse de traitement des incidents ou vulnérabilités.

Comme précisé dans les encadrés, notre CSIRT fictif veut offrir les services proposés par tout CSIRT de base, à savoir:

- Les bulletins d'alertes et les avertissements
- Le traitement des incidents
- Les annonces

Ce huitième chapitre présente des exemples de workflows illustrant le fonctionnement des services de base d'un CSIRT. Il contient également des précisions concernant la collecte d'informations auprès de différentes sources, la vérification de leur pertinence et de leur authenticité, et leur rediffusion auprès des parties prenantes. Il s'achève par la présentation d'exemples des procédures les plus élémentaires et d'outils plus spécifiques à l'usage des CSIRT.

8.1 Évaluation des installations des parties prenantes

La première étape consiste à dresser le bilan des systèmes informatiques installés chez les parties prenantes. Le CSIRT peut ainsi mesurer la pertinence des informations qui en proviennent, et les filtrer avant de les redistribuer, de manière à ce que les parties prenantes ne soient pas envahies d'informations sans intérêt pour elles.

Il est recommandé de commencer simplement, en utilisant par exemple une feuille Excel se présentant comme suit:

Catégorie	Application	Logiciel	Version	SE	Version SE	Partie prenante
PC	Office	Excel	x-x-x	Microsoft	XP-prof	A
PC	Navigateur	IE	x-x-	Microsoft	XP-prof	A
Réseau	Routeur	CISCO	x-x-x	CISCO	x-x-x-	B
Serveur	Serveur	Linux	x-x-x	L-distro	x-x-x	B
Services	Serveur Web	Apache		Unix	x-x-x	B

La fonction filtre d'Excel permet de sélectionner très facilement le bon logiciel, et de déterminer le type de logiciel utilisé par chacune des parties prenantes.

8.2 Lancement d'alertes, d'avertissements et d'annonces

Le lancement d'alertes, d'avertissements et d'annonces suit toujours le même déroulement:

- La collecte d'informations
- L'évaluation des informations en termes de pertinence et de source
- L'évaluation des risques sur la base des informations recueillies
- La diffusion de l'information

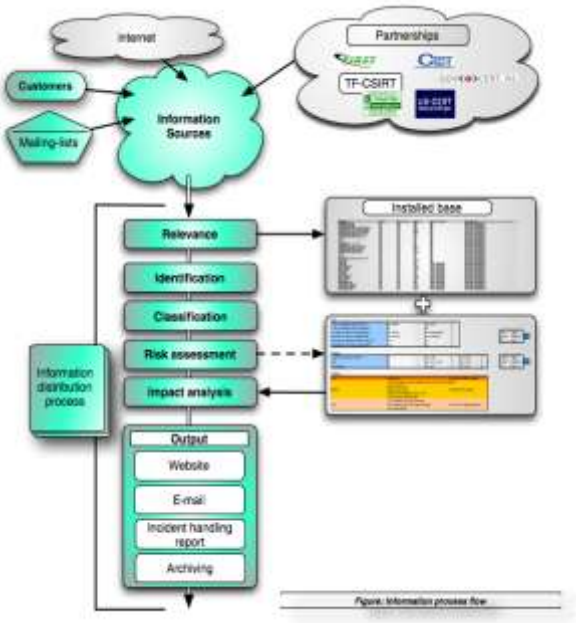


Fig. 9 : Déroulement du traitement de l'information

Ces différentes étapes sont décrites de manière plus détaillée aux paragraphes suivants.

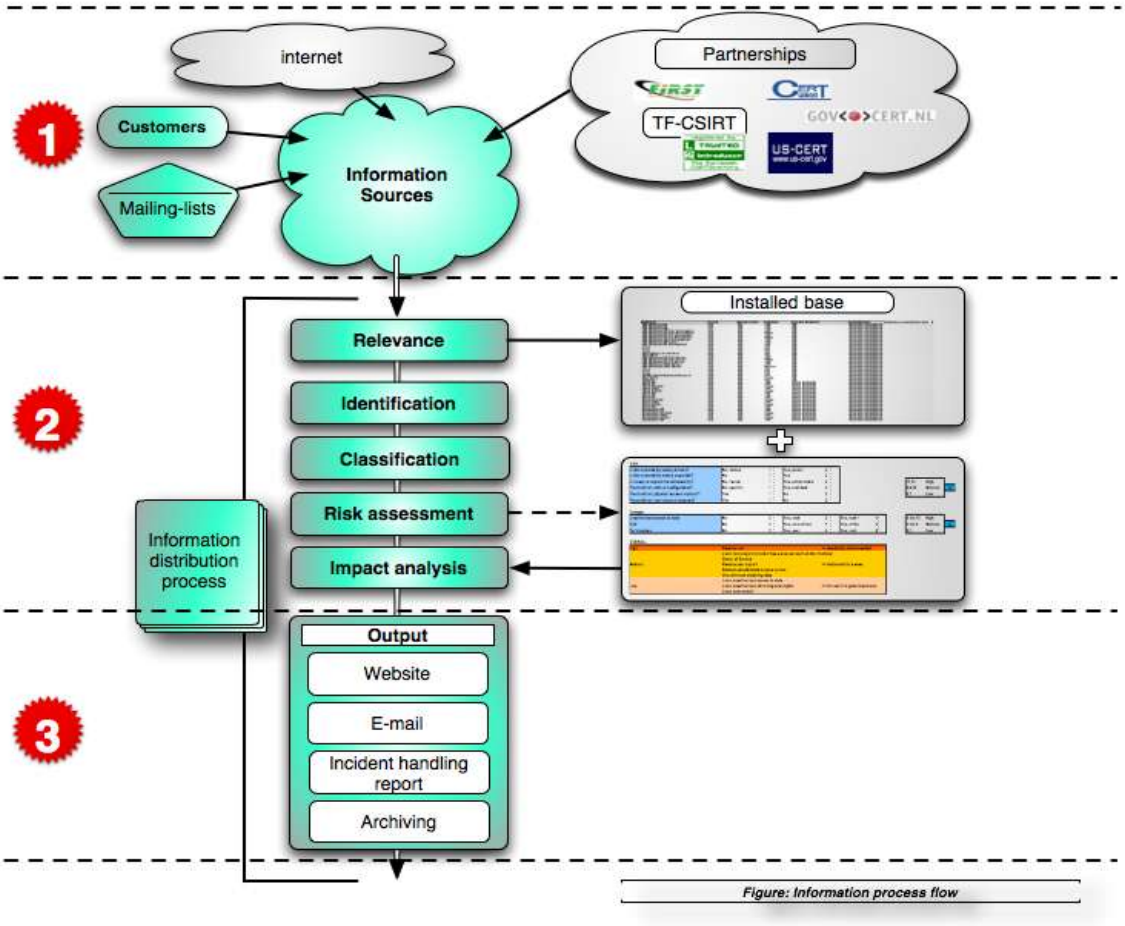


Figure: Information process flow

1 Première étape: Collecte des informations concernant les vulnérabilités

Deux sources principales fournissent généralement les informations nécessaires à la prestation des services visés ici:

- les informations relatives à la vulnérabilité des (de vos) systèmes informatiques
- les signalements d'incidents

Il existe, selon le type d'activité et d'infrastructure informatique, de nombreuses sources publiques ou réservées d'informations concernant les vulnérabilités:

- Listes de distribution publiques et non publiques
- Information produit du fournisseur concernant les vulnérabilités
- Sites Web
- Informations sur Internet (Google, etc…)
- Partenariats publics et privés fournissant des informations concernant les vulnérabilités (FIRST, TF-CSIRT, CERT-CC, US-CERT….)

L'ensemble de ces informations détermine le niveau de connaissance de vulnérabilités spécifiques des systèmes informatiques.

Comme déjà indiqué, il existe sur Internet toute une série de sources d'information valables et aisément accessibles concernant la sécurité. Le groupe de travail ad hoc «CERT services» de l'ENISA établit, à l'heure où nous écrivons ces lignes, une liste plus exhaustive qui devrait être disponible fin 2006[19].

Deuxième étape: Évaluation de l'information et du risque

Cette deuxième étape analyse l'impact d'une vulnérabilité particulière sur l'infrastructure informatique des parties prenantes.

Identification
Les informations entrantes concernant des vulnérabilités doivent toujours être identifiées en termes de source, la fiabilité de cette dernière devant être établie avant que les informations en question soient transmises aux parties prenantes. Faute de cette vérification, de fausses alertes pourraient inutilement perturber les procédures d'entreprise et nuire, en définitive, à la réputation du CSIRT.

[19] Ad-hoc WG CERT services: http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

La procédure ci-après illustre l'identification et l'authentification d'un message:

Procédure d'identification et d'authentification d'un message et de sa source

Vérifications générales

1. La source est-elle connue et enregistrée en tant que telle?
2. Les informations sont-elles acheminées par voie régulière?
3. Une information vous paraît-elle «étrange» ou vous donne-t-elle l'impression que «quelque chose ne va pas»?
4. Suivez votre intuition: en cas de doute à propos d'une information, vérifiez-la une nouvelle fois avant d'agir!

Vérifications des courriers électroniques

1. L'adresse de la source est-elle connue de l'organisation et figure-t-elle sur la liste des sources?
2. La signature PGP est-elle correcte?
3. En cas de doute, vérifiez l'en-tête complet du message.
4. En cas de doute, utilisez l'outil «Nslookup» ou «Dig» pour vérifier le nom de domaine de l'émetteur[20].

Vérifications des sources WWW

1. Vérifiez le certificat du navigateur lors d'une connexion à un site Web sécurisé (https ://).
2. Vérifiez la source en termes de contenu et de validité (technique).
3. En cas de doute, ne cliquez sur aucun lien et ne téléchargez aucun logiciel.
4. En cas de doute, faites un «Lookup» ou un «Dig» du nom de domaine, ou un «traceroute».

Vérifications des messages téléphoniques

1. Écoutez attentivement le nom.
2. Reconnaissez-vous la voix?
3. En cas de doute, demandez le numéro de téléphone pour rappeler plus tard.

Fig. 10 Exemple de procédure d'identification des informations

Pertinence

Le bilan des installations matérielles et logicielles, antérieurement effectué, peut également servir à filtrer les informations entrantes concernant les vulnérabilités en termes de pertinence, afin de trouver des réponses à ces deux questions: «Les parties prenantes utilisent-elles le logiciel en question?» et « l'information peut-elle leur être utile?»

Classification

Certaines informations reçues peuvent être classifiées ou étiquetées comme «confidentielles» (rapports communiqués par d'autres équipes à propos d'incidents, par exemple). Toutes les informations doivent être traitées conformément aux exigences de

[20] Outils de vérification des identités recensés sur le site CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

l'expéditeur et à la propre politique de sécurité du destinataire. La règle de base suivante a fait ses preuves: «*Ne pas diffuser une information dont il n'est pas clairement précisé qu'elle est destinée à la diffusion; en cas de doute, demander l'autorisation de l'émetteur.*»

Évaluation du risque et analyse d'impact
Plusieurs méthodes permettent de déterminer le risque et l'impact d'une vulnérabilité (potentielle).

Le risque est défini comme l'éventualité d'exploitation de la vulnérabilité. Plusieurs facteurs importants interviennent à cet égard, parmi lesquels:

- La vulnérabilité est-elle bien connue?
- La vulnérabilité est-elle largement répandue?
- La vulnérabilité est-elle aisément exploitable?
- La vulnérabilité est-elle exploitable à distance?

Ces différentes questions permettent de mesurer la gravité de la vulnérabilité.
Une approche très simple du calcul du risque consiste à appliquer la formule suivante:

Impact = Risque X Dommage potentiel

Le dommage potentiel peut être

- Un accès non autorisé aux données
- Un déni de service (DoS)
- L'obtention ou l'extension d'autorisations

(Se référer à la fin du présent chapitre pour des systèmes de classification plus élaborés).

La réponse aux questions ci-dessus permet d'ajouter un indice général au bulletin de sécurité informant d'un risque ou dommage potentiel. Cet indice s'exprime généralement en termes simples tels que «FAIBLE», «MOYEN» ou «ÉLEVÉ».

Il existe des systèmes d'évaluation des risques plus sophistiqués:

Système GOVCERT.NL d'appréciation des risques[21]
Le CSIRT officiel néerlandais GOVCERT.NL propose une matrice d'évaluation des risques développée lors de son propre démarrage, mais qui continue d'être mise à jour pour intégrer les évolutions les plus récentes.

[21] Matrice de vulnérabilité: http://www.govcert.nl/download.html?f=33

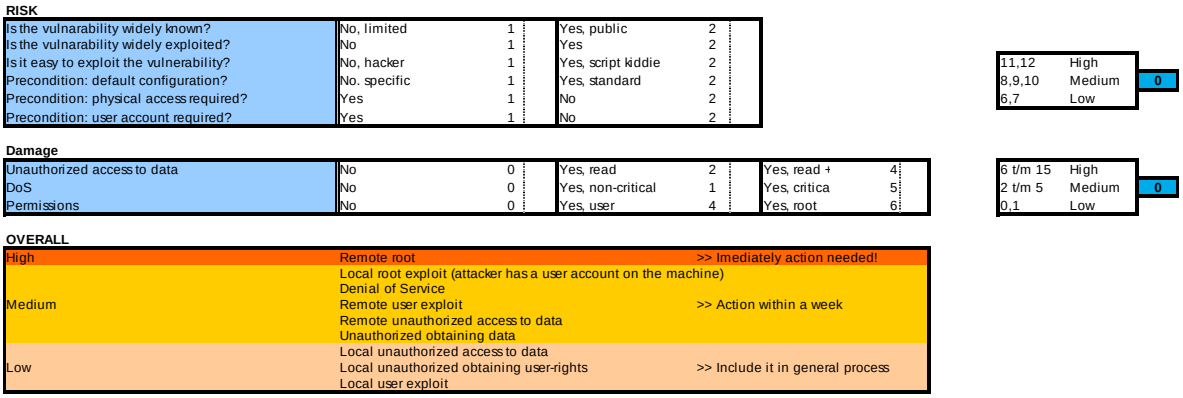


Fig. 11 Système GOVCERT.NL d'appréciation des risques

Common Advisory Format de l'EISPP[22]

L'EISPP (*European Information Security Promotion Programme*) est un projet cofinancé par la Communauté européenne au titre du cinquième programme cadre. Il vise à développer un cadre européen destiné non seulement à la mise en commun des connaissances en matière de sécurité, mais également à la définition du contenu et des modalités de diffusion des informations de sécurité aux PME. Dotées de services adéquats dans le domaine de la sécurité informatique, les PME européennes seront incitées à faire davantage confiance au commerce électronique et à y recourir plus systématiquement pour étendre leurs activités. L'EISPP est une première avancée vers la création d'un réseau d'expertise au sein de l'UE dont la Commission européenne a lancé l'idée.

DAF (Deutsches Advisory Format)[23]

Le DAF, initiative du CERT-Verbund (Allemagne), est un élément central d'une infrastructure destinée au lancement et à l'échange de bulletins de sécurité entre plusieurs équipes. Le DAF a été plus particulièrement conçu pour répondre aux besoins des CERT allemands: le développement et la maintenance de la norme sont assurés par CERT-Bund, DFN-CERT, PRESECURE et Siemens-CERT.

[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

Troisième étape: Diffusion de l'information

Le CSIRT choisit l'une des nombreuses voies de diffusion possibles en tenant compte des desiderata des parties prenantes et de sa propre stratégie de communication:

- Site Web
- Courriel
- Rapports
- Archivage et recherche

Les bulletins de sécurité diffusés par un CSIRT doivent toujours présenter la même structure, afin de faciliter sa lecture et la localisation rapide des informations utiles.

Un bulletin de sécurité doit contenir au minimum les informations suivantes:

Titre du bulletin de sécurité
……

Numéro de référence
……
Systèmes concernés
- ……
- ……

SE associé + version
……
Risque (Élevé-Moyen-Faible)
……
Impact/dommage potentiel (Élevé-Moyen-Faible)
……
Identificateurs externes: (CVE, identificateurs de bulletins de vulnérabilité)
……

Bilan de la vulnérabilité
……

Impact
……

Solution
……

Description (détails)
……

Annexe
……

Fig. 12 Exemple de bulletin de sécurité

Voir le chapitre *10. Exercice* pour un exemple complet de bulletin de sécurité.

8.3 Traitement des incidents

Comme signalé dans l'introduction de ce huitième chapitre, le processus appliqué aux informations lors du traitement d'un incident est très similaire à celui appliqué lors de la compilation d'alertes, d'avertissements et d'annonces. Il existe néanmoins une différence en ce qui concerne le volet «collecte de l'information», deux sources les plus courantes de données relatives à un incident étant son signalement par les parties prenantes ou d'autres équipes, et le retour d'information en provenance des parties concernées au cours du processus de traitement de l'incident. Ces informations sont généralement communiquées par courriel (sous forme cryptée); le recours au téléphone ou à la télécopie s'avère parfois nécessaire.

Lors de la réception d'informations par téléphone, il est recommandé de consigner immédiatement le moindre détail en utilisant un outil de traitement/signalement des incidents ou en rédigeant une note. Il est indispensable d'attribuer tout de suite (avant la fin de l'appel) un numéro de référence à l'incident (si celui-ci n'en a pas encore reçu) et de le communiquer à l'interlocuteur au téléphone (ou dans un courriel récapitulatif envoyé par la suite) en vue des communications ultérieures.

La suite de ce chapitre est consacrée à la description du processus de base appliqué au traitement des incidents. Pour l'analyse en profondeur du déroulement complet de ce processus et des workflows primaires et secondaires qui y sont associés, voir la documentation publiée par le CERT/CC sous le titre *Defining Incident Management processes for CSIRTs*[24].

[24] Définition des processus de traitement des incidents: http://www.cert.org/archive/pdf/04tr015.pdf

Le traitement des incidents se déroule essentiellement de la manière suivante:

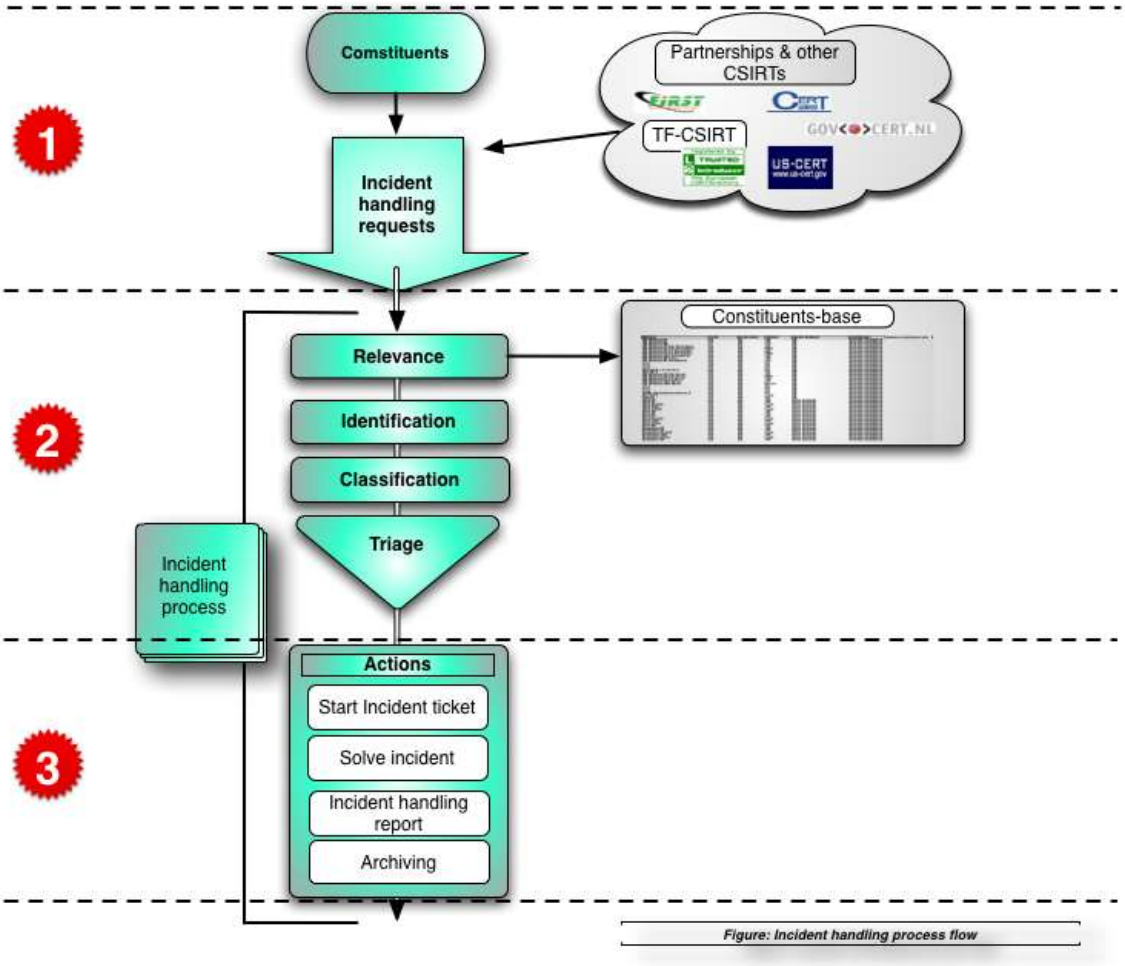


Fig. 13 Déroulement du traitement d'un incident

Première étape: Réception des signalements d'incident

Comme nous l'avons déjà indiqué, les signalements d'incident peuvent parvenir au CSIRT par différentes voies: par courriel dans la plupart des cas, mais également par téléphone ou par télécopie.

Nous avons déjà précisé également qu'il est recommandé de noter, au moment où le rapport d'incident est communiqué, tous les détails selon une présentation prédéfinie, afin de s'assurer qu'aucune information essentielle n'est omise. Voici un exemple de formulaire de ce type:

FORMULAIRE DE SIGNALEMENT D'INCIDENT
Veuillez compléter le présent formulaire et le retourner par télécopie ou par courriel à: …….. *Les mentions avec * doivent impérativement être complétées.* *Nom et organisation* 1. Nom*: 2. Nom de l'organisation*: 3. Secteur d'activité: 4. Pays*: 5. Ville: 6. Adresse électronique*: 7. Numéro de téléphone*: 8. Autre: *Hôte(s) affecté(s)* 9. Nombre d'hôtes: 10. Nom de l'hôte & FAI*: 11. Fonction de l'hôte*: 12. Fuseau horaire: 13. Matériel: 14. Système d'exploitation: 15. Logiciel affecté: 16. Fichiers affectés: 17. Sécurité: 18. Nom d'hôte & FAI: 19. Protocole/port: *Incident* 20. Numéro de référence: 21. Type d'incident: 22. Début de l'incident: 23. Il s'agit d'un incident permanent: OUI NON 24. Méthode et moment de la découverte: 25. Vulnérabilités connues: 26. Fichiers suspects: 27. Contre-mesures: 28. Description détaillée*:

Fig. 14 Contenu d'un signalement d'incident

2 Deuxième étape: Évaluation de l'incident

La deuxième étape consiste à vérifier l'authenticité et la pertinence de l'incident signalé, et à le classifier.

Identification

Il est bon, pour éviter toute action inutile, de vérifier si l'expéditeur est digne de foi et s'il s'agit de l'une des parties prenantes de votre CSIRT ou d'un CSIRT homologue. Les règles décrites au point *8.2 Lancement d'alertes* sont d'application.

Pertinence

La démarche consiste à s'assurer que la demande de traitement d'incident émane d'une partie prenante du CSIRT ou que l'incident signalé implique des systèmes informatiques installés chez des parties prenantes. Si aucune de ces conditions n'est remplie, le signalement de l'incident est généralement réorienté vers le CISRT concerné[25].

Classification

Cette étape prépare le triage en classant l'incident en fonction de sa gravité. La description détaillée de cette classification sortirait du cadre du présent document; nous nous contenterons donc de recommander l'utilisation, comme point de départ, du système FIRST (exemple pour un CSIRT destiné aux entreprises):

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.		

[25] Outils de vérification des identités recensés sur le site CHIHT:
http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Fig. 15 Système de classification des incidents (source: FIRST)[26]

Triage

Le triage est une procédure appliquée par le personnel médical ou des services d'urgence pour économiser des ressources médicales limitées et traiter le plus grand nombre possible de victimes: c'est le fait de déterminer le degré de gravité des blessés, et donc de déterminer l'ordre dans lequel ils seront traités[27].

Le CERT/CC en propose la description suivante (traduction libre):

Le triage est un élément essentiel de toute fonction de traitement des incidents, en particulier au niveau d'un CSIRT. Il fait partie du chemin critique conduisant à comprendre la teneur de ce qui est signalé dans l'ensemble de l'organisation. Il assure l'acheminement de toutes les informations vers un point de contact unique afin d'avoir une vision globale de l'activité observée et d'établir la corrélation entre toutes les données reçues. Le triage procède à une première évaluation du signalement entrant, et le place dans une file d'attente en vue de son traitement ultérieur. Il est aussi l'étape privilégiée pour entamer la documentation et encoder les données d'un signalement ou d'une demande, si cela n'a pas été fait lors du processus de détection.

La fonction de triage donne un instantané immédiat du statut de l'ensemble des activités signalées — quels sont les dossiers de signalement ouverts et quels sont ceux qui sont fermés, quelles sont les actions en cours, et en combien d'exemplaires chaque type de signalement a été reçu. Ce processus peut aider à recenser les problèmes potentiels de sécurité et à organiser les tâches par ordre prioritaire. Les informations rassemblées au cours du triage peuvent également servir à l'établissement de tendances en matière de vulnérabilités et d'incidents, et de statistiques à l'intention de la haute direction[28]*.*

Le triage doit être exclusivement effectué par les membres les plus expérimentés de l'équipe, car il exige une connaissance approfondie des effets qu'un incident particulier peut avoir sur certaines parties prenantes, et la capacité de désigner le membre de l'équipe le plus compétent pour traiter l'incident.

[26] CSIRT Case Classification http://www.first.org/resources/guides/csirt_case_classification.html

[27] Triage dans Wikipedia: http://fr.wikipedia.org/wiki/Triage

[28] Définition des processus de traitement des incidents: http://www.cert.org/archive/pdf/04tr015.pdf

Troisième étape: Actions

Les incidents sont généralement acheminés, après triage, vers un outil à l'aide duquel une ou plusieurs personnes les prendront successivement en charge et les traiteront selon la procédure de base suivante:

Numérotation de l'incident (ticket)
Il se peut qu'un numéro ait été attribué lors d'une étape précédente (notamment lorsque l'incident a été signalé par téléphone). Si tel n'est pas le cas, il convient de l'attribuer sans délai, ce numéro allant servir de référence lors de toute communication ultérieure à propos de l'incident.

Cycle de vie de l'incident
Traiter un incident ne consiste pas à effectuer une succession d'étapes aboutissant à une solution, mais plutôt à effectuer un cycle d'étapes à répéter jusqu'à ce que l'incident soit finalement résolu et que toutes les parties impliquées disposent des informations requises. Ce «cycle de vie de l'incident» inclut les processus suivants:

Analyse: Examen approfondi de tous les détails concernant l'incident signalé.

Obtention de coordonnées de contact: Démarche visant à permettre de relayer les informations relatives à l'incident à toutes les parties concernées, à savoir d'autres CSIRT, les victimes et probablement les propriétaires des systèmes susceptibles d'avoir été utilisés à mauvais escient pour une attaque.

Apport d'une assistance technique: Aide fournie aux victimes en vue de remédier rapidement aux effets de l'incident et de rassembler des informations complémentaires à propos de l'attaque.

Coordination: Diffusion de l'information à d'autres parties concernées, telles que le CSIRT responsable du système informatique utilisé pour l'attaque, ou d'autres victimes.

Cette structure est appelée «cycle de vie» parce que chaque étape conduit à la suivante et que la dernière, consacrée à la coordination, peut elle-même donner lieu à une nouvelle analyse et faire ainsi redémarrer le cycle. Le processus s'achève lorsque toutes les parties concernées ont reçu et signalé les informations nécessaires.

Le lecteur peut utilement se référer au manuel CSIRT du CERT/CC CSIRT pour une description plus détaillée du cycle de vie de l'incident[29].

Rapport concernant le traitement de l'incident
Soyez prêt à répondre aux questions de la direction à propos des incidents en rédigeant un rapport. Il est également utile de consigner par écrit (à usage interne uniquement) les «enseignements tirés», afin d'en faire bénéficier le personnel et d'éviter certaines erreurs lors du traitement d'incidents futurs.

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

Archivage
Voir les règles d'archivage décrites au point *6.5 Développement d'une politique de sécurité de l'information*.

Il est recommandé au lecteur de consulter l'annexe *A.1 Lectures complémentaires* pour s'informer des manuels détaillés consacrés au traitement et au cycle de vie des incidents.

8.4 Exemple de délai de réponse

La fixation des temps de réponse est souvent négligée, alors qu'elle devrait faire partie intégrante de tout accord sur le niveau de service (ANS) entre un CSIRT et ses parties prenantes. Il est essentiel d'assurer un retour d'information en temps utile vers les parties prenantes au cours du processus de traitement des incidents, tant dans la perspective des responsabilités incombant aux parties prenantes elles-mêmes que pour être à la hauteur de la réputation de l'équipe.
Les délais de réponse doivent être clairement précisés aux parties prenantes pour éviter toute attente non fondée. Le schéma très succinct ci-dessous peut servir de point de départ pour un ANS avec les parties prenantes d'un CSIRT.

Exemple de délai concret de réponse à compter de l'arrivée d'une demande d'assistance:

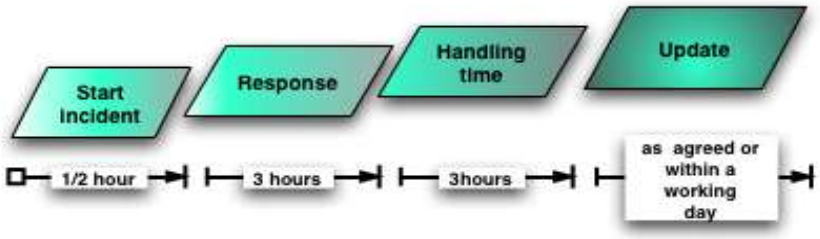


Fig. 16 Exemple de délai de réponse

Il est également recommandé de donner certaines instructions aux parties prenantes quant à leurs propres délais de réaction, et notamment quant au moment où elles doivent contacter le CSIRT en cas d'urgence. Mieux vaut, dans la plupart des cas, que les parties prenantes prennent contact très rapidement avec leur CSIRT, et il est utile de les encourager à le faire en cas de doute.

8.5 Outils à la disposition des CSIRT

Cette section donne quelques indications quant aux outils les plus couramment utilisés par les CSIRT. Il ne s'agit que d'exemples, et des informations complémentaires peuvent être trouvées sur le site pilote CHIHT (*Clearinghouse of Incident Handling Tools*[30].

Logiciel cryptographique pour courriels et messages

- GNUPG http://www.gnupg.org/
  GnuPG est l'implémentation complète et libre de la norme OpenGPG (RFC2440) du projet GNU. GnuPG est un outil qui permet d'encrypter et de signer vos données et vos communications.

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

Outil de traitement des incidents

Pour gérer les incidents et leur suivi, garder trace des actions.

- RTIR http://www.bestpractical.com/rtir/
  RTIR est un système libre (*open source*) conçu pour répondre aux besoins des CERT et autres équipes chargées de traiter des incidents, qui peuvent le télécharger gratuitement.

Outils CRM

Une base de données CRM (gestion des relations avec la clientèle) peut s'avérer utile si vous comptez beaucoup de parties prenantes et que vous tenez à retrouver aisément tous les rendez-vous et contacts. Il en existe de multiples versions, dont voici quelques exemples:

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

- Sugarforce (version «open source» gratuite) http://www.sugarforge.org/

Vérification des informations

- WebSite-Watcher http://www.aignes.com/index.htm
  Ce programme suit toutes les mises à jour et modifications apportées aux sites Web.

- Watch that page http://www.watchthatpage.com/
  Ce service informe par courriel des changements apportés aux sites Web (gratuit pour les particuliers et payant pour les utilisateurs professionnels).

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

Recherche de coordonnées de contact
Trouver le bon interlocuteur auquel signaler un incident n'est pas toujours facile, et quelques sources d'information peuvent s'avérer utiles à cet égard:

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

Le site pilote CHIHT contient également la liste de quelques outils de recherche de coordonnées de contact[34].

CSIRT fictif (étape 8)

Établissement des processus de traitement et des procédures opérationnelles et techniques

Le CSIRT fictif concentre son activité sur la prestation de services de base:

- Alertes et avertissements
- Annonces
- Traitement des incidents

L'équipe a mis au point des procédures qui fonctionnent bien et qui sont aisément compréhensibles par tous les membres de l'équipe. Le CSIRT fictif a également engagé un expert juridique pour les questions de responsabilité et la politique de sécurité de l'information. L'équipe a adopté plusieurs outils utiles et a obtenu de précieux renseignements à propos de certains aspects opérationnels en discutant avec d'autres CSIRT.

Un formulaire type a été établi pour les bulletins de sécurité et les signalements d'incidents. L'équipe traite les incidents à l'aide du système RTIR.

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

[32] IRT-object dans la base de données 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] Outils de vérification des identités sur CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Formation du personnel des CSIRT

Nous avons déjà franchi les étapes ci-après:

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.
2. Définir les secteurs auxquels la nouvelle équipe destine ses services.
3. Choisir les services que le CSIRT va offrir à ses parties prenantes.
4. Analyser l'environnement et les parties prenantes.
5. Élaborer la déclaration de mission.
6. Développer le plan d'activités
   a. Définition du modèle financier.
   b. Définition de la structure organisationnelle.
   c. Début du recrutement de personnel.
   d. Utilisation et équipement de l'espace de bureau.
   e. Développement d'une politique de sécurité de l'information.
   f. Recherche de partenaires en vue d'une coopération.
7. Promouvoir le plan d'activités
   a. Approbation de la justification stratégique et commerciale (*business case*).
   b. Intégration de tous les éléments dans un plan de projet.
8. Rendre le CSIRT opérationnel
   a. Mettre les workflows en place
   b. Implémenter les outils CSIRT

>> L'étape suivante consiste à former le personnel.

Nous donnons ci-après un aperçu des deux principales sources de formation spécialisée en CSIRT, en l'occurrence TRANSITS et le CERT/CC.

9.1 TRANSITS

TRANSITS est un projet européen qui avait pour but de promouvoir la création de nouveaux CSIRT et l'amélioration la performance des équipes déjà en place en remédiant au problème de la pénurie de personnel qualifié dans ce domaine. Cet objectif a été réalisé en proposant au personnel des (nouveaux) CSIRT des cours spécialisés portant sur les aspects organisationnels, opérationnels, techniques, commerciaux et juridiques de la prestation de services CSIRT.

TRANSITS a plus particulièrement

- développé, actualisé et régulièrement révisé les modules de formation
- organisé des sessions de formation utilisant ce matériel
- permis aux membres du personnel des (nouveaux) CSIRT de participer à ces sessions de formation avec un accent particulier sur la participation des pays adhérents (nouveaux États membres de l'UE et pays candidats)
- diffusé le matériel de formation et veillé à l'exploitation des résultats[35].

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

L'ENISA facilite et soutient les cours de formation TRANSITS. Pour toute information concernant l'inscription, les conditions et le prix des cours, veuillez contacter les experts CSIRT de l'ENISA à l'adresse suivante:

CERT-Relations@enisa.europa.eu

Des extraits de ces cours sont proposés en annexe du présent document à titre d'exemple.

9.2 CERT/CC

La complexité des infrastructures informatiques et de réseaux, et le défi que constitue leur administration, ne facilitent guère la bonne gestion de leur sécurité. Les administrateurs systèmes et réseaux ne disposent ni d'effectifs suffisants ni de pratiques adéquates pour assurer une défense efficace contre les attaques et minimiser les préjudices - une situation qui explique la multiplication du nombre des incidents.
Lorsqu' un incident de sécurité se produit, les organisations doivent réagir de manière rapide et efficace. Plus vite une organisation reconnaît, analyse et répond à un incident, mieux elle sera en mesure de limiter les dommages et les coûts de récupération. La création d'un CSIRT est une excellente façon d'assurer cette rapidité de réaction, et de prévenir de futurs incidents.

Le CERT-CC propose des cours à l'intention du personnel d'encadrement et technique dans des domaines tels que la création et la gestion d'une équipe d'alerte et de réaction aux attaques informatiques (CSIRT), la réponse aux incidents de sécurité et leur analyse, et l'amélioration de la sécurité des réseaux. Sauf indication contraire, tous les cours sont organisés à Pittsburgh, PA (États-Unis). Les membres de notre personnel dispensent également des cours de sécurité à la Carnegie Mellon University.

Cours spécialisés pour CSIRT proposés par le CERT/CC[36]

Creating a Computer Security Incident Response Team (CSIRT) (Création d'un CSIRT)
Managing Computer Security Incident Response Teams (CSIRTs) (Gestion d'un CSIRT)
Fundamentals of Incident Handling (Principes fondamentaux du traitement des incidents)
Advanced Incident Handling for Technical Staff (Traitement avancé des incidents pour personnel technique)

Vous trouverez quelques extraits de ces cours en annexe du présent document!

CSIRT fictif (étape 9)

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

Formation du personnel
Le CSIRT fictif décide d'envoyer tous les membres de son personnel technique à la prochaine session de cours TRANSITS. Le chef d'équipe suivra en outre le cours *Managing a CSIRT* (gestion d'un CSIRT) du CERT/CC.

10 Exercice: établissement d'un bulletin de sécurité

Nous avons déjà franchi les étapes ci-après:

1. Comprendre le concept de CSIRT et les avantages qui y sont associés.
2. Définir les secteurs auxquels la nouvelle équipe destine ses services.
3. Choisir les services que le CSIRT va offrir à ses parties prenantes.
4. Analyser l'environnement et les parties prenantes.
5. Élaborer la déclaration de mission.
6. Développer le plan d'activités
   a. Définition du modèle financier.
   b. Définition de la structure organisationnelle.
   c. Début du recrutement de personnel.
   d. Utilisation et équipement de l'espace de bureau.
   e. Développement d'une politique de sécurité de l'information
   f. Recherche de partenaires en vue d'une coopération.
7. Promouvoir le plan d'activités
   a. Approbation de la justification stratégique et commerciale (*business case*).
   b. Intégration de tous les éléments dans un plan de projet.
8. Rendre le CSIRT opérationnel.
   a. Mettre les workflows en place
   b. Implémenter les outils CSIRT
9. Former le personnel

>> L'étape suivante consiste à faire un exercice pratique pour être prêt à entrer réellement en action!

Ce dixième chapitre comprend un exercice destiné à illustrer l'une des tâches les plus courante des CSIRT, à savoir l'établissement d'un bulletin de sécurité.

Le facteur déclencheur est l'envoi initial par Microsoft du bulletin de sécurité suivant:

Identificateur du Bulletin	**Bulletin de sécurité Microsoft MS06-042**
Intitulé du Bulletin	**Mise à jour de sécurité cumulative pour Internet Explorer (918899)**
Synthèse	Cette mise à jour corrige plusieurs vulnérabilités d'Internet Explorer susceptibles de permettre l'exécution de code à distance.
Indice de gravité maximal	Critique
Type de vulnérabilité	Exécution de code à distance
Logiciels concernés	**Windows, Internet Explorer.** Pour informations complémentaires, voir la section «Logiciels concernés et adresses de téléchargement des mises à jour».

Ce bulletin décrit une vulnérabilité récemment découverte dans Internet Explorer. Publié par le fournisseur, il propose toute une série de correctifs à appliquer à ce logiciel en fonction de la version de Microsoft Windows utilisée.

Informé via une liste de distribution par courriel, le CSIRT fictif entame la séquence d'opérations décrite sous *8.2 Lancement d'alertes, d'avertissements et d'annonces*.

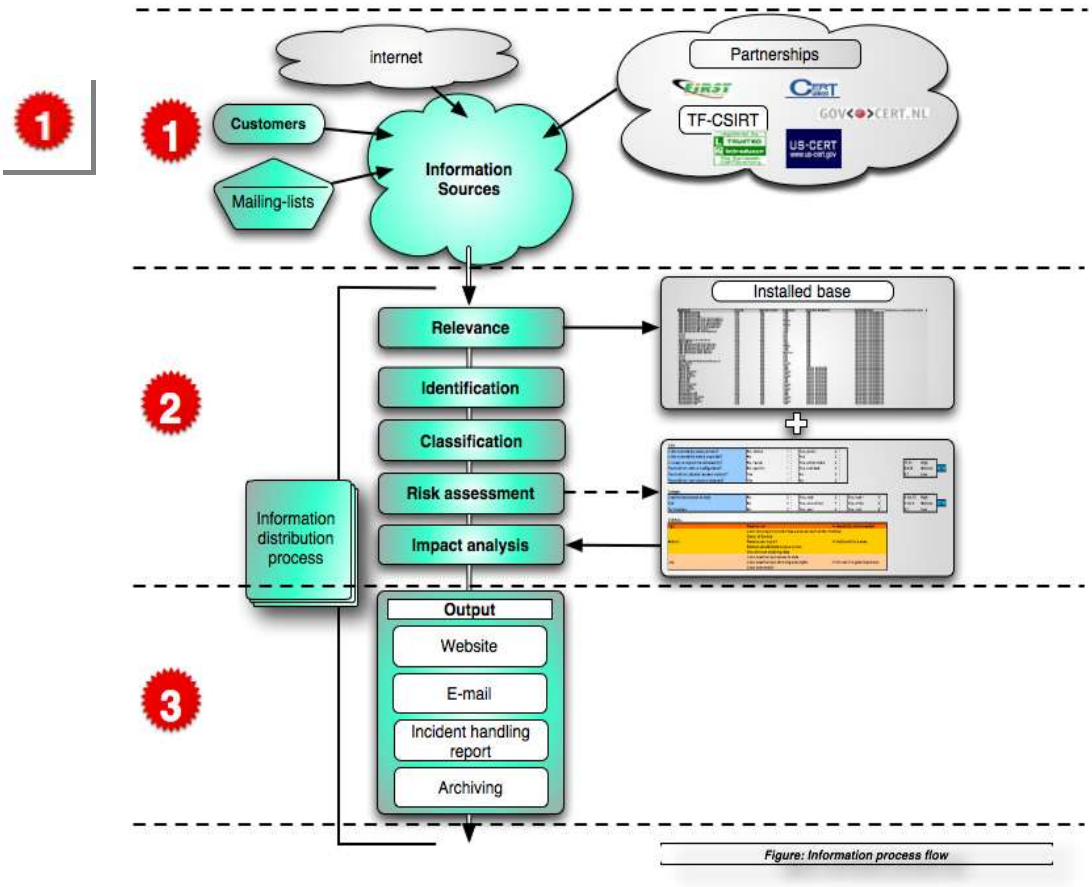


Figure: Information process flow

Première étape: Collecte d'informations concernant la vulnérabilité

La première étape consiste pour le CISRT fictif à effectuer une recherche sur le site Web du fournisseur pour s'assurer de l'authenticité de l'information et obtenir des précisions concernant la vulnérabilité et les systèmes informatiques concernés.

Deuxième étape: Évaluation des informations et du risque

Identification
Les informations ont déjà été vérifiées en recoupant les informations concernant la vulnérabilité reçue par courriel et celles qui figurent sur le site Web du fournisseur.

Pertinence
Le CSIRT fictif compare la liste des systèmes concernés affichée sur le site Web avec la liste des systèmes utilisés par ses parties prenantes. S'il constate que l'une au moins parmi celles-ci utilise Internet Explorer, l'information concernant la vulnérabilité est effectivement pertinente.

Catégorie	Application	Logiciel	Version	OS	Version OS	Partie prenante
PC	Navigateur	IE	x-x-	Microsoft	XP-prof	A

Classification
L'information est publique et peut donc être utilisée et rediffusée.

Évaluation du risque et analyse d'impact
La réponse aux questions ci-après montre que le risque et l'impact sont *élevés* (indice *critique* attribué par Microsoft).

RISQUE

La vulnérabilité est-elle bien connue?	OUI
La vulnérabilité est-elle largement répandue?	OUI
La vulnérabilité est-elle aisément exploitable?	OUI
La vulnérabilité est-elle exploitable à distance?	OUI

DOMMAGE
Les impacts éventuels sont l'accessibilité à distance et l'exécution potentielle de code à distance. Cette vulnérabilité comporte de multiples aspects, ce qui rend le risque de dommage *élevé*.

Troisième étape 3: Diffusion

Le CSIRT fictif est un CSIRT interne, qui dispose du courrier électronique, du téléphone et d'un Intranet comme moyens de communication. Le CSIRT établit le bulletin de sécurité suivant en s'inspirant du modèle présenté au point *8.2 Lancement d'alertes, d'avertissements et d'annonces*.

Titre du bulletin de sécurité
Vulnérabilités multiples constatées dans Internet Explorer

Numéro de référence
082006-1

Systèmes concernés

- Tous les ordinateurs de bureau (PC) utilisant Microsoft

SE concernés + version

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 et Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professionel Édition x64
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 pour systèmes Itanium et Microsoft Windows Server 2003 avec SP1 pour les systèmes Itanium
- Microsoft Windows Server 2003 Édition x64

Risque (Élevé-Moyen-Faible)
ÉLEVÉ

Impact/dommage potentiel (Élevé-Moyen-Faible)
ÉLEVÉ

Identificateur externe: (CVE, Identificateurs de bulletins de vulnérabilité)
MS-06-42

Bilan de la vulnérabilité
Microsoft a découvert dans Internet Explorer plusieurs vulnérabilités critiques susceptibles de permettre une exécution de code à distance.

Impact
Un attaquant pourrait prendre le contrôle intégral d'un système affecté, installer des programmes, ajouter des utilisateurs et afficher, modifier ou supprimer des données – le facteur d'atténuation étant l'obligation pour lui d'ouvrir la session avec des privilèges d'administrateur. Les utilisateurs dont les comptes sont configurés avec des privilèges moins élevés subiraient moins d'impact.

Solution
Appliquer immédiatement un correctif à votre IE

Description (détails)
Voir informations complémentaires sur ms06-042.mspx

Annexe

Voir informations complémentaires sur ms06-042.mspx

Le bulletin est prêt à la diffusion. Étant donné son caractère critique, il est également recommandé de prévenir, si possible, les parties prenantes par téléphone.

CSIRT fictif (étape 10)

Exercice

Au cours de ses premières semaines de fonctionnement, le CSIRT fictif s'est exercé à l'aide de plusieurs cas fictifs (communiqués par d'autres CSIRT à titre d'exemples). Il a publié en outre quelques bulletins de sécurité basés sur de véritables informations concernant des vulnérabilités diffusées par les fournisseurs de matériel et de logiciel, qu'il a adaptées aux besoins de ses propres parties prenantes.

11 Conclusion

C'est ici que s'achève notre manuel. Conçu pour vous donner un aperçu très condensé des différents processus nécessaires à la création d'un CSIRT, il ne prétend pas à l'exhaustivité et n'entre pas véritablement dans le détail. Le lecteur trouvera à la première annexe (*A.1 Lectures complémentaires*) des liens vers plusieurs autres documents utiles sur le même thème.

Les prochaines étapes importantes pour le CSIRT consisteront à:

- Obtenir une remontée d'informations de la part des parties prenantes, afin d'affiner les services proposés
- Acquérir une routine dans les tâches courantes
- S'exercer à des situations d'urgence
- Rester en contact étroit avec les différentes communautés CSIRT en vue de contribuer un jour à leur travail volontaire

12 Description du plan de projet

NOTE: Le plan de projet est une première estimation du temps requis. La durée réelle du projet peut s'avérer différente en fonction des ressources disponibles.

Le plan de projet existe en divers formats sur CD et sur le site Web de l'ENISA. Il couvre intégralement les divers processus décrits dans le présent document.

Le format de base sera le Microsoft Project, qui peut donc être directement utilisé dans le présent outil de gestion de projet.

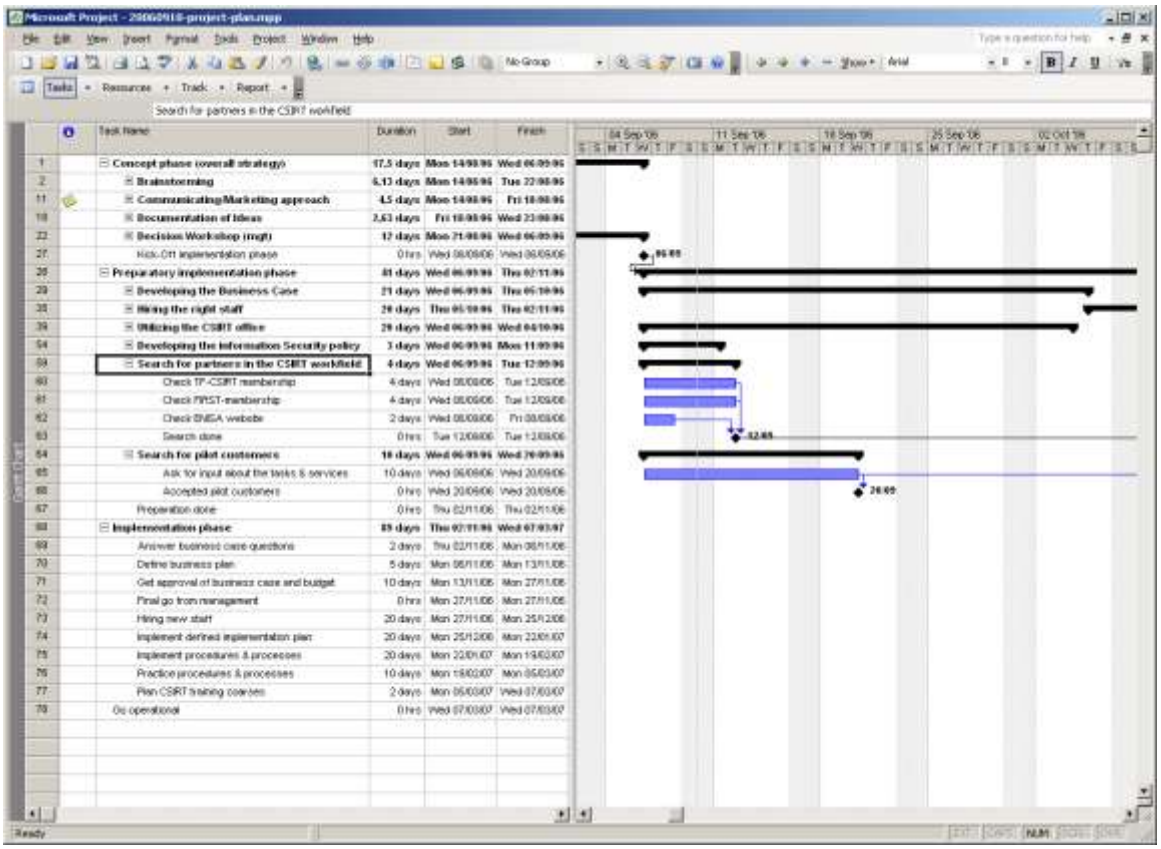


Fig. 17 Plan de projet

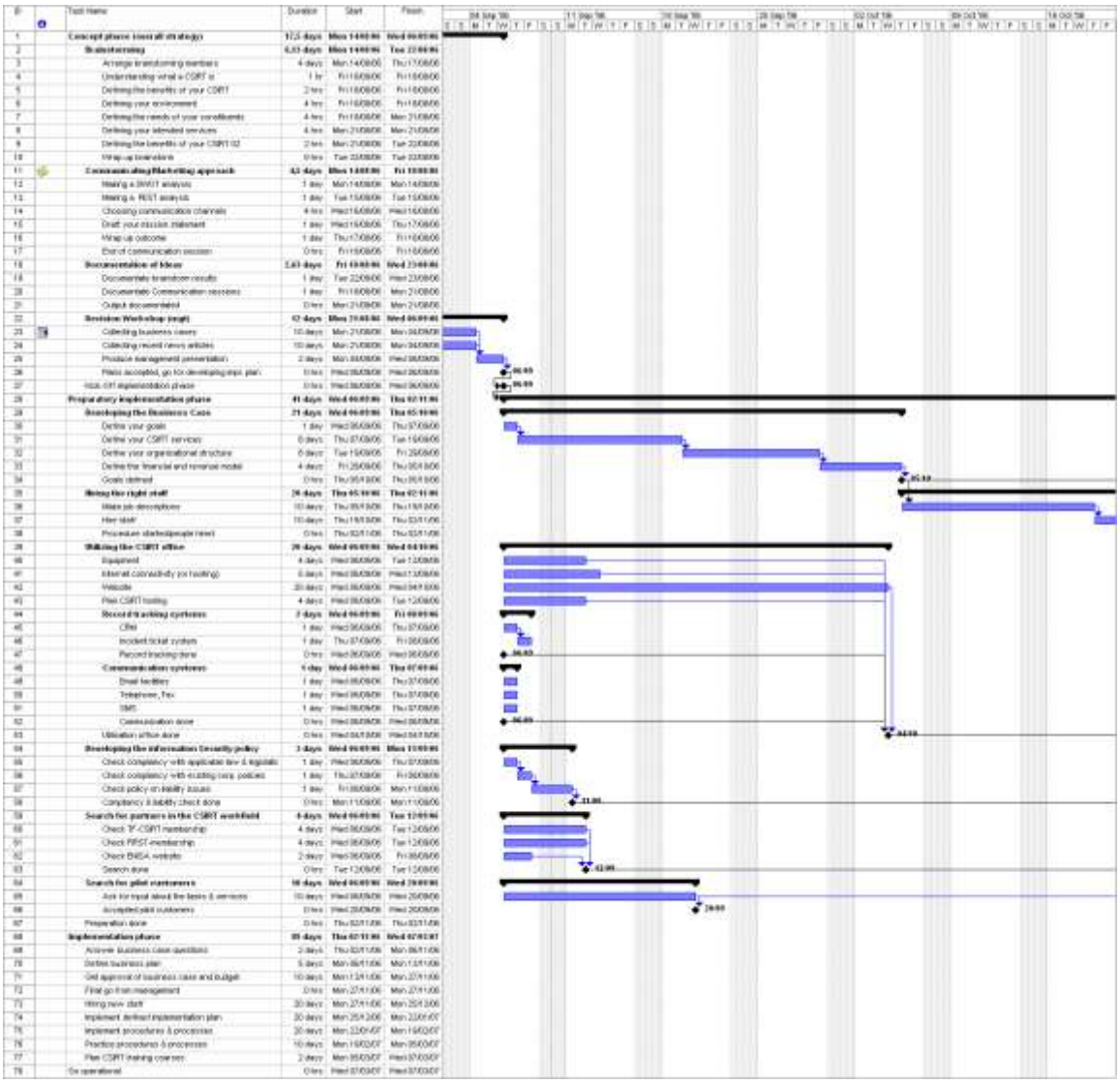


Fig. 18 Plan de projet incluant toutes les tâches et partie du diagramme de Gantt

Le plan de projet existe également en format CVS et XML. Des informations complémentaires peuvent être demandées aux experts CSIRT de l'ENISA:

CERT-Relations@enisa.europa.eu !

ANNEXE

A.1 Lectures complémentaires

Handbook for CSIRTs (CERT/CC) (Manuel à l'usage des CSIRT)
Un ouvrage de référence très complet abordant tous les thèmes utiles à l'exécution de la mission d'un CSIRT.
Source: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress (Définir les processus de traitement des incidents à l'intention des CSIRT: un chantier en cours)
Analyse approfondie de la gestion des incidents.
Source: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs) (État d'avancement de la pratique des CSIRT)
Analyse exhaustive de la situation mondiale dans le domaine des CSIRT, y compris un historique, des statistiques et beaucoup d'autres informations.
Source: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
Description complète des enseignements tirés de la création de GOVCERT.NL et du service national néerlandais d'alerte «De Waarschuwingsdienst».
Source: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response (Attentes vis-à-vis de la réponse aux incidents de sécurité informatique)
Source: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide (Manuel de traitement des incidents de sécurité informatique du NIST)
Source: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe (Répertoire des activités CERT recensées en Europe par l'ENISA)
Récapitulatif de référence contenant des informations concernant les CSIRT opérationnels en CSIRT en Europe et leurs diverses activités
Source: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: National Institute of Standards and Technologies

A.2 Services CSIRT

Nous adressons des remerciements tous particuliers au CERT/CC, qui nous a fourni la liste ci-après

Services réactifs	***Services proactifs***	***Traitement des artefacts***
• Alertes et avertissements • Traitement des incidents • Analyse des incidents • Réponse aux incidents sur place • Appui à la réponse aux incidents • Coordination de la réponse aux incidents • Traitement des vulnérabilités • Analyse des vulnérabilités • Réponse aux vulnérabilités • Coordination des réponses aux vulnérabilités	• Annonces • Veille technologique • Audits ou évaluations de la sécurité • Configuration et maintenance de la sécurité • Développement d'outils de sécurité • Services de détection des intrusions • Diffusion d'informations relatives à la sécurité	• Analyse des artefacts • Réponse aux artefacts • Coordination des réponses aux artefacts ***Gestion de la qualité de la sécurité*** • Analyse des risques • Continuité de l'activité et reprise après sinistre • Consultance en matière de sécurité • Sensibilisation • Éducation/formation • Évaluation ou certification des produits

Fig. 19 Liste des services CSIRT (CERT/CC)

Description des services

Services réactifs

Les services réactifs sont conçus pour répondre aux demandes d'assistance, aux signalements d'incidents par des parties prenantes du CSIRT et à toute menace ou attaque à l'encontre de systèmes membres du CSIRT. Certains services peuvent être prestés en réaction à un avis émanant d'un tiers ou à la lecture des journaux de surveillance ou de détection d'intrusion, voire d'alertes.

Alertes et avertissements

Ce service consiste à diffuser des informations décrivant une attaque, une vulnérabilité de sécurité, une alerte d'intrusion, un virus informatique ou un canular, et à recommander des mesures à court terme pour remédier aux problèmes qui en découlent. Le bulletin d'alerte, d'avertissement ou de sécurité est envoyé en réaction au problème survenu, afin d'en prévenir les parties prenantes et de leur donner des conseils pour protéger leurs systèmes ou pour les restaurer s'ils ont été affectés. Le CSIRT peut être l'auteur de ces informations ou relayer des informations en provenance de fournisseurs, d'autres CSIRT ou experts en sécurité, ou de certaines parties prenantes.

Traitement des incidents

Le traitement des incidents consiste à recevoir, trier et répondre aux demandes et aux signalements, et à analyser les incidents et évènements. Les actions de réponse peuvent plus particulièrement consister à

- prendre des mesures pour protéger les systèmes et réseaux concernés ou menacés par une intrusion;
- proposer des solutions et des actions d'atténuation à partir des alertes et bulletins de sécurité pertinents;
- rechercher une activité éventuelle de l'intrus sur d'autres parties du réseau;
- filtrer le trafic sur le réseau;
- restaurer les systèmes;
- appliquer des correctifs aux systèmes ou les réparer;
- développer d'autres stratégies de réponse ou solutions temporaires.

Étant donné que les divers types de CSIRT ont une approche différente du traitement des incidents, ce service est lui-même divisé en catégories correspondant au type d'activité exercée et au type d'aide fournie:

Analyse des incidents

Il existe de nombreux niveaux d'analyse des incidents et de nombreux services connexes. L'analyse des incidents consiste essentiellement à examiner toutes les informations disponibles, ainsi que les éléments probants ou artefacts relatifs à un incident ou un évènement donné. L'analyse a pour but de déterminer l'ampleur de l'incident, l'étendue du dommage causé, la nature de l'incident et les stratégies de réponse ou solutions temporaires. Le CSIRT peut se servir des résultats de l'analyse des vulnérabilités et de l'analyse des artefacts (décrites toutes deux ci-après) pour comprendre ce qui est arrivé à un système spécifique, et proposer une analyse aussi complète et actualisée que possible du phénomène. Le CSIRT établit des corrélations entre différents incidents, afin d'établir d'éventuelles interactions, des tendances et des profils, voire la signature des intrus. Deux services connexes peuvent être proposés dans le cadre de l'analyse des incidents selon la mission, les objectifs et les processus du CSIRT:

Rassemblement de preuves légales

La collecte, la préservation, la documentation et l'analyse des preuves d'un système informatique compromis en vue de déterminer les changements intervenus et d'aider à la reconstitution des évènements ayant porté atteinte à l'intégrité du système. Ce rassemblement d'éléments informationnels et probants doit être organisé de manière à constituer un enchaînement de garde démontrable et recevable devant un tribunal en vertu des règles de preuve. La collecte des preuves légales comprend les tâches suivantes (liste non exhaustive): procéder à une copie d'image binaire du disque dur du système affecté; vérifier les changements apportés au système tels que nouveaux programmes, fichiers, services et utilisateurs; examiner les applications en cours d'exécution et les ports ouverts; et vérifier la présence de programmes « cheval de Troie » et boîtes à outils. Le personnel du CSIRT assumant cette fonction doit

également être formé à remplir le rôle de témoins-experts dans le cadre de poursuites judiciaires.

Suivi ou traçage

Il s'agit de remonter à l'origine de l'intrusion ou d'identifier les systèmes auxquels l'intrus a eu accès. Cette activité peut comprendre le suivi ou le traçage de la manière dont l'intrus a pénétré dans les systèmes affectés et les réseaux connexes; l'identification des systèmes utilisés pour cet accès; et la détermination de l'origine de l'attaque, et des autres systèmes et réseaux éventuellement utilisés dans ce contexte. La mission peut s'étendre à l'identification de l'intrus. Elle peut être menée de façon individuelle, mais elle s'organise le plus souvent en collaboration avec des représentants de la loi, des fournisseurs de services Internet ou d'autres organisations concernées.

Réponse aux incidents sur place

Le CSIRT fournit une assistance directe à ses parties prenantes en facilitant sur place la reprise après sinistre. Le CSIRT procède lui-même à l'examen physique des systèmes affectés et procède à leur réparation et leur restauration, plutôt que de se limiter à un support technique par téléphone ou par courriel (voir plus loin). Ce service couvre toutes les actions à prendre au plan local en cas de suspicion ou de survenance d'un incident. Si le CSIRT n'est pas implanté sur le site affecté, des membres de l'équipe se rendent sur place et exécutent les mesures de réponse. Dans d'autres cas, une équipe locale peut déjà se trouver sur place et répondre à l'incident dans le cadre de son travail de routine. Cette situation se présente notamment lorsque le traitement des incidents relève de la fonction habituelle des administrateurs de systèmes, de réseaux ou de sécurité, plutôt que d'un CSIRT en tant que tel.

Appui à la réponse aux incidents

Par téléphone, par courriel, par télécopie ou par l'envoi de documentation, le CSIRT fournit aux victimes d'une attaque l'assistance et les orientations dont elles ont besoin pour restaurer leurs systèmes après un incident. Ce service peut inclure l'interprétation des données collectées, la fourniture de coordonnées de contact ou le relais de conseils en matière de stratégies d'atténuation et de restauration. Il ne s'étend pas aux mesures directes de réponse sur place (voir ci-dessus). Le CSIRT fournit plutôt à distance des conseils permettant au personnel local de procéder lui-même à la restauration.

Coordination de la réponse aux incidents

Le CSIRT coordonne les actions de réponse menées par toutes les parties concernées – à savoir, de manière générale, la victime de l'attaque, les autres sites visés par celle-ci et tout autre site réclamant une aide dans le cadre de l'analyse de l'attaque, mais également les responsables du support informatique à la victime (fournisseurs de services Internet, autres CSIRT et administrateurs systèmes et réseaux sur place notamment). Le travail de coordination peut comprendre la collecte de coordonnées de contact, la notification aux sites de leur implication éventuelle (en tant que victime ou que source d'une attaque), la compilation de statistiques concernant le nombre de sites concernés, et la facilitation de l'échange et de l'analyse des informations. Le travail de coordination peut également couvrir la notification et la collaboration avec le département juridique, le département des ressources humaines ou le département des relations publiques de l'organisation, de même que la coordination avec des

représentants de la loi. Le rôle de coordination ne s'accompagne d'aucune réponse directe sur le site de l'incident.

Traitement des vulnérabilités

Le traitement des vulnérabilités comprend la réception des informations et signalements concernant des vulnérabilités au niveau des matériels et des logiciels; l'analyse de la nature, du fonctionnement et des effets des vulnérabilités; et l'élaboration de stratégies de réponse permettant de détecter les vulnérabilités et d'y remédier. Étant donné que les divers types de CSIRT ont une approche différente du traitement des vulnérabilités, ce service est lui-même divisé en catégories correspondant au type d'activité exercée et au type d'aide fournie:

Analyse des vulnérabilités

Le CSIRT procède à l'examen technique des vulnérabilités et à leur analyse, tant au niveau matériel que logiciel. Cette tâche couvre la vérification des vulnérabilités suspectées et l'examen technique de la vulnérabilité du matériel ou du logiciel en vue d'en déterminer la localisation et les possibilités d'exploitation. L'analyse peut inclure le réexamen du code source, l'utilisation d'un débogueur pour déterminer où survient la vulnérabilité et la reproduction du problème sur un système test.

Réponse aux vulnérabilités

Ce service vise à déterminer la réponse la plus adéquate pour atténuer la vulnérabilité ou y remédier. Il peut donc couvrir l'étude et le développement de nouveaux correctifs ou de solutions temporaires. Il peut s'étendre à la notification de la stratégie d'atténuation à d'autres parties intéressées par l'établissement et la diffusion de bulletins de sécurité ou d'alertes, par exemple. Ce service peut comprendre l'exécution des mesures de réponse, à savoir l'installation des correctifs ou des solutions temporaires.

Coordination de la réponse aux vulnérabilités

Le CSIRT avertit les différents départements de l'entreprise ou les parties prenantes de l'existence de la vulnérabilité, et fournit des informations sur les moyens d'y remédier ou d'en atténuer les effets. Le CSIRT s'assure que la stratégie de réponse a été appliquée avec succès. Ce rôle peut exiger de communiquer avec les fournisseurs, d'autres CSIRT, des techniciens spécialisés, certaines de ses parties prenantes, et les personnes ou les groupes qui ont initialement découvert ou signalé la vulnérabilité. Les activités couvrent la facilitation de l'analyse d'une vulnérabilité ou de son signalement; la coordination du calendrier de publication des documents, correctifs ou solutions temporaires y afférents; et la synthèse des analyses techniques effectuées par différents intervenants. Ce service peut également prévoir la maintenance d'archives ou d'une base de connaissances publiques ou privées contenant des informations concernant les vulnérabilités et les stratégies de réponse correspondantes.

Traitement des artefacts

Un artefact est un fichier ou objet quelconque trouvé dans un système et susceptible d'avoir servi à une tentative d'attaque ou à une attaque de systèmes et de réseaux, ou qui sert à contrecarrer les mesures de sécurité. Les artefacts comprennent – sans que cette liste soit exhaustive – les virus informatiques, les programmes «cheval de Troie», les vers, les scripts d'exploitation et les boîtes à outils.

Le traitement consiste à recevoir des informations concernant les artefacts, voire des copies de ceux-ci, utilisés pour des intrusions, des reconnaissances et d'autres activités non autorisées ou perturbatrices. À réception, l'artefact fait l'objet d'un examen couvrant sa nature, son fonctionnement, sa version et son utilisation – ce qui conduit au développement (ou à la proposition) de stratégies de réponse en vue de sa détection, de son élimination et de sa prévention. Étant donné que les divers types de CSIRT ont une approche différente du traitement des artefacts, ce service est lui-même divisé en catégories correspondant au type d'activité exercée et au type d'aide fournie:

Analyse des artefacts

Le CSIRT procède à l'examen technique de l'artefact détecté sur le système. Cette analyse peut couvrir l'identification du type de fichier et de structure de l'artefact, la comparaison d'un nouvel artefact par rapport à des artefacts existants ou à d'autres versions pour établir les similitudes et les différences, ou une rétroingénerie (désassemblage du code) pour déterminer le but et la fonction de l'artefact.

Réponse aux artefacts

Ce service a pour but de définir les actions les plus adéquates pour détecter et éliminer les artefacts présents dans un système, ainsi que les mesures destinées à prévenir leur installation. Il peut impliquer la création de signatures à ajouter au logiciel antivirus ou au système de détection d'intrusion (IDS).

Coordination de la réponse aux artefacts

Ce service prévoit le partage et l'analyse des résultats et des stratégies de réponse à un artefact donné avec des chercheurs, des CSIRT, des fournisseurs et d'autres experts en sécurité. Les activités visent notamment à une information réciproque et à la synthèse des analyses techniques en provenance de sources diverses. Elles peuvent également prévoir la maintenance d'archives publiques ou réservées aux parties prenantes contenant les artefacts connus, leurs effets et les stratégies de réponse correspondantes.

Services proactifs

Les services proactifs sont destinés à améliorer l'infrastructure et les processus sécuritaires des parties prenantes avant qu'un incident ou un évènement survienne ou soit détecté. Leur but principal est donc de prévenir les incidents et d'en réduire l'impact et l'étendue s'ils surviennent.

Annonces

Ce service vise de manière non limitative les alertes d'intrusion, les avertissements de vulnérabilité et les bulletins de sécurité. Ces annonces informent les parties prenantes de développements nouveaux appelés à avoir un impact de court à moyen terme, tels que les vulnérabilités et outils d'intrusion récemment découverts. Elles permettent donc aux parties prenantes de protéger leurs systèmes et réseaux contre les problèmes récemment détectés, avant même qu'ils puissent être exploités.

Veille technologique

Le CSIRT suit et observe les nouvelles évolutions techniques, les activités des intrus et les tendances en la matière, afin de contribuer à l'identification des menaces futures. Les domaines examinés peuvent être étendus aux dispositions législatives et aux décisions judiciaires, aux menaces d'ordre social ou politique, et aux technologies émergentes. Ce service comprend la lecture des listes de diffusion par courriel et des sites Internet consacrés à la sécurité, ainsi que des actualités et des articles publiés dans des revues scientifiques, technologiques, politiques et officielles, afin d'en extraire les informations touchant la sécurité des systèmes et réseaux des parties prenantes. Cette mission peut impliquer de communiquer avec d'autres parties compétentes dans ces domaines, afin de garantir l'obtention des informations les plus précises ou une interprétation aussi correcte que possible de celles-ci. L'exécution de ce service peut donner lieu à certaines annonces, orientations ou recommandations axées sur des questions de sécurité relevant davantage du moyen ou long terme.

Audits ou évaluations de sécurité

Ce service assure l'examen approfondi de l'infrastructure de sécurité d'une organisation sur la base des exigences fixées par celle-ci ou par d'autres normes industrielles d'application. Il peut également procéder à l'examen des pratiques organisationnelles en matière de sécurité. Les types d'audit ou d'évaluation proposés sont très variés et comprennent notamment

L'examen de l'infrastructure:

Examen manuel des configurations matérielles et logicielles, des routeurs, des pare-feux, des serveurs et des équipements de bureau, afin de s'assurer de leur conformité aux bonnes pratiques de l'entreprise ou du secteur en matière de politique de sécurité et de configurations standard.

L'examen des bonnes pratiques:

Il s'agit d'interroger le personnel et les administrateurs systèmes et réseaux en vue de déterminer si leurs pratiques de sécurité correspondent à la politique définie par l'organisation en la matière ou à des normes industrielles spécifiques.

Le scannage:

Tests automatiques de vulnérabilités ou de virus, effectués à l'aide de scanners, pour déterminer les systèmes et réseaux vulnérables.

Le test de pénétration:

Examen des fonctions de sécurité d'un site en vue d'en attaquer délibérément les systèmes et réseaux.
L'accord de la haute direction est requis avant de procéder à ce type d'audit ou d'évaluation. Il se peut même que certaines de ces approches soient interdites par la politique de l'organisation. La prestation du service visé ici peut inclure le développement d'un ensemble commun de pratiques par rapport auxquelles les tests ou évaluations sont effectués, parallèlement au développement des aptitudes requises de la part du personnel pour l'exécution des tests, évaluations, audits ou réexamens. Ce service peut également être sous-traité à un contractant tiers ou à un prestataire de services de sécurité gérés qualifié pour procéder à des audits et évaluations.

Configuration et maintenance des outils de sécurité, des applications, des infrastructures et des services

Ce service précise ou donne des indications quant à la manière de configurer et d'entretenir en toute sécurité les outils, les applications et l'infrastructure informatique générale utilisés par les parties prenantes du CSIRT ou le CSIRT lui-même. Au-delà de l'apport de conseils, le CSIRT peut procéder à des mises à jour et à la maintenance au niveau des outils et des services de sécurité: IDS, scannage des réseaux ou surveillance des systèmes, filtres, wrappers, pare-feux, réseaux virtuels privés (RVP) ou autres mécanismes d'authentification. Le CSIRT peut même proposer ces services dans le cadre de sa mission principale. Il peut également configurer et assurer la maintenance de serveurs, d'ordinateurs de bureau, d'ordinateurs portables, d'assistants numériques personnels (PDA) et d'autres équipements sans fil conformément aux lignes directrices en matière de sécurité. Ce service inclut de faire remonter au niveau de la direction toute question ou problème de configuration ou d'utilisation des outils et applications que le CSIRT juge susceptible d'exposer le système à une attaque.

Développement d'outils de sécurité

Ce service porte sur le développement de tout outil nouveau spécifiquement destiné à répondre aux besoins ou aux souhaits des parties prenantes ou du CSIRT lui-même. Il peut s'agir, par exemple, de la mise au point de correctifs de sécurité spécialement conçus pour les logiciels utilisés par les parties prenantes ou de la distribution de logiciels sécurisés pouvant servir à la restauration d'hôtes après compromission. Ce service peut également prévoir le développement d'outils ou de scripts destinés à étendre la fonctionnalité des outils de sécurité déjà en place: dispositif supplémentaire en vue du branchement d'un scanner de vulnérabilité ou de réseau, scripts facilitant l'application de la technologie de chiffrement ou mécanismes de distribution automatique de correctifs, par exemple.

Services de détection d'intrusion

Les CSIRT qui offrent ce type de service examinent les journaux IDS, les analysent et initient une réponse pour tout évènement correspondant au seuil fixé ou lancent une alerte conformément à l'accord sur le niveau de service ou à la stratégie de remontée de l'information préalablement définie. La détection des intrusions et l'analyse des journaux de sécurité qu'elle implique peuvent représenter une tâche considérable — non seulement pour déterminer à quels endroits de l'environnement concerné les capteurs doivent être placés, mais également pour rassembler puis analyser le volume important de données saisies. Des outils ou des compétences spécifiques sont souvent nécessaires à la synthèse et à l'interprétation des informations, afin de déceler les fausses alertes ou attaques, ou les faux évènements survenant au niveau des réseaux, et de mettre en place des mesures destinées à supprimer ou à réduire ce type d'occurrences. Certaines organisations préfèrent sous-traiter cette activité à des contractants extérieurs plus spécialisés, tels que des prestataires de services de sécurité gérés.

Diffusion d'informations relatives à la sécurité

Ce service fournit aux parties prenantes une série exhaustive et aisément accessible d'informations utiles à l'amélioration de la sécurité. On peut citer à cet égard:

- des lignes directrices en matière de signalement et des coordonnées de contact pour le CSIRT;
- des archives d'alertes, d'avertissements et d'autres annonces;
- de la documentation concernant les bonnes pratiques en vigueur;
- des conseils concernant la sécurité informatique en général;
- des politiques, procédures et listes de contrôle;
- des informations concernant la mise au point et la diffusion de correctifs;
- des liens vers les fournisseurs (*vendors*);
- les statistiques et tendances en matière de signalement d'incidents;
- d'autres informations susceptibles de contribuer à l'amélioration des pratiques générales de sécurité.

Ce type d'information peut être développé et publié par le CSIRT ou par un autre département de l'organisation (TI, ressources humaines ou relations avec la presse), et inclure des renseignements en provenance de sources extérieures (autres CSIRT, fournisseurs et experts en sécurité notamment).

Services de gestion de la qualité de la sécurité

Les services inclus de cette catégorie ne relèvent pas spécifiquement du traitement des incidents ou des CSIRT: il s'agit de services bien établis visant à améliorer la sécurité générale d'une organisation. En valorisant les expériences acquises dans le cadre de la prestation de services réactifs et proactifs, un CSIRT peut ouvrir à l'intention de ces services de gestion de la qualité des perspectives qu'ils n'auraient sans doute pas eues autrement. Ses propres services sont effectivement conçus de manière à pouvoir intégrer les remontées d'information, de même que les enseignements et connaissances acquis lors de la réponse à certains incidents, vulnérabilités et attaques. Faire bénéficier les services traditionnels (décrits plus loin) du fruit de ces expériences dans le cadre du processus de gestion de la qualité de la sécurité peut améliorer les efforts menés à long terme par une organisation pour renforcer sa sécurité. Selon les structures et les responsabilités organisationnelles, un CSIRT peut prester ces services ou prendre part à un effort collectif plus général au niveau de l'organisation.
Les descriptions ci-après illustrent l'apport que la compétence des CSIRT peut représenter pour chacun des services de gestion de la qualité de la sécurité.

Analyse des risques

Les CSIRT sont en mesure d'apporter une valeur ajoutée à l'analyse et à l'évaluation des risques et d'améliorer ainsi la capacité de l'organisation d'apprécier les menaces réelles, de procéder à une évaluation qualitative et quantitative réaliste des risques pour son patrimoine informationnel, et de jauger les stratégies de protection et de réponse. La prestation de ce service consiste pour les CSIRT à effectuer ou à étayer l'analyse des risques pour la sécurité des informations dans le cadre de nouveaux systèmes et de nouvelles procédures d'entreprise, ou à évaluer les menaces et attaques contre le patrimoine ou les systèmes des parties prenantes.

Plan de continuité d'activité et reprise après sinistre

Les observations et les prévisions en matière d'incidents de sécurité conduisent à penser qu'ils seront de plus en plus nombreux à causer un préjudice important au

fonctionnement de l'organisation concernée. Il convient donc de tenir compte des expériences et recommandations des CSIRT au moment de définir la meilleure manière d'assurer la continuité de ce fonctionnement en cas d'incident. Les CSIRT qui prestent ce service participent à la planification de la continuité de l'activité et de sa reprise après sinistre en cas d'évènements relevant de menaces et d'attaques contre la sécurité informatique.

Consultance

Le CSIRT peut fournir des conseils et des orientations concernant les pratiques de sécurité les mieux adaptées à l'activité des parties prenantes. Le CSIRT participe, dans le cadre de cette prestation, à l'élaboration de recommandations ou à la définition des exigences concernant l'achat, l'installation ou la sécurisation de nouveaux systèmes, équipements de réseaux, applications logicielles ou processus à l'échelon de l'entreprise. Ce service inclut l'apport de conseils et d'une aide au développement des politiques de sécurité de l'organisation ou de la partie prenante concernée. Il peut également prévoir l'apport d'un témoignage ou de conseils à des organes législatifs ou autres instances officielles.

Sensibilisation

Les CSIRT sont bien placés pour savoir dans quels domaines les parties prenantes ont besoin d'informations ou de lignes directrices complémentaires pour se conformer plus rigoureusement aux pratiques de sécurité généralement convenues et aux politiques de sécurité définies par l'organisation. En sensibilisant davantage l'ensemble des parties prenantes à l'égard de la sécurité en général, les CSIRT leur permettent non seulement de mieux comprendre les questions de sécurité, mais également d'exécuter leurs tâches courantes de manière plus sûre. Cette démarche peut donc contribuer à réduire le nombre des attaques qui atteignent leur objectif et à augmenter la probabilité de voir les parties prenantes détecter et signaler les attaques dont elles sont victimes, ce qui réduirait les délais de reprise et supprimerait, ou du moins minimiserait, les pertes.
Les CSIRT proposant ce service multiplient les opportunités d'accroître la sensibilisation à l'égard de la sécurité. Ils font appel à des articles, des affiches, des bulletins d'information, des sites Web et d'autres ressources d'information pour expliquer les bonnes pratiques et recommander certaines précautions en matière de sécurité. Les activités dans ce domaine peuvent également comprendre la programmation de réunions et de séminaires destinés à tenir les parties prenantes informées des procédures de sécurité les plus récentes et de la découverte de menaces éventuelles pour leurs systèmes.

Éducation/formation

Ce service consiste à fournir aux parties prenantes des informations touchant aux questions de sécurité informatique dans le cadre de séminaires, d'ateliers, de cours et de didacticiels. Les thèmes les plus courants sont les lignes directrices en matière de signalement d'incidents, les méthodes de réponse les plus adéquates, les outils de réponse et la prévention. Ces formations contiennent toutes les informations utiles en matière de prévention, de détection, de signalement et de réponse aux incidents de sécurité informatique.

Évaluation ou certification des produits

Le CSIRT peut, dans le cadre de ce service, procéder à des évaluations portant sur des outils, des applications ou tout autre service, en vue de s'assurer de la sécurité des produits et de leur conformité à des normes de sécurité considérées comme acceptables par le CSIRT ou l'organisation concernée. Les outils et applications examinés dans cette perspective peuvent être des produits libres (*open source*) ou des produits commerciaux. Ce service peut être proposé en tant qu'évaluation ou dans le cadre d'un programme de certification en fonction des normes appliquées par l'organisation ou par le CSIRT.

A.3 Exemples

CSIRT fictif

Étape 0 – Comprendre le concept de CSIRT:

Le CSIRT choisi à titre exemplatif est appelé à desservir une organisation de taille moyenne occupant 200 personnes. Elle a son propre département informatique et deux succursales dans le même pays. L'informatique y joue un rôle essentiel puisqu'elle est utilisée pour la communication interne, pour un réseau de transmission de données et pour une activité de commerce électronique 24 heures par jour et 7 jours par semaine. L'organisation possède son propre réseau et dispose d'une connexion redondante à l'Internet via deux fournisseurs d'accès différents.

\- -

Étape 1: Phase de démarrage

Il est décidé lors de la phase de démarrage de planifier le nouveau CSIRT en tant que CSIRT interne, destiné à offrir ses services à l'entreprise hôte, au département informatique local et au personnel. Il sera également appelé à fournir un soutien technique et à coordonner le traitement des incidents de sécurité informatique qui surviendraient entre les succursales.

\- -

Étape 2: Choix des bons services

Il a été décidé à la première étape que le nouveau CSIRT axerait principalement son activité sur la fourniture de certains services de base aux membres du personnel.

Il est envisagé maintenant d'étendre la gamme des services à l'issue d'une phase pilote et d'y ajouter certains «Services de gestion de la sécurité». La décision sera prise sur la base du retour d'information en provenance des parties prenantes pilotes et en concertation avec le département Assurance qualité.

\- -

Étape 3: Analyse des parties prenantes et des voies de communication adéquates

Une réunion de brainstorming avec quelques représentants clés de la direction et les parties prenantes a permis d'obtenir suffisamment d'éléments pour procéder à une analyse FFOM. Celle-ci a conclu à la nécessité des services de base suivants:

- Alertes et avertissements
- Traitement des incidents (analyse, soutien et coordination de la réponse)
- Annonces

L'information doit être diffusée de manière structurée, afin de parvenir au plus grand nombre possible de parties prenantes. Il est donc décidé que les alertes, avertissements et annonces seront publiés sous la forme de bulletins de sécurité sur un site Internet dédié et diffusés sur la base d'une liste de distribution. Le CSIRT privilégie l'utilisation du courriel, du téléphone et de la télécopie pour la réception des signalements d'incidents. Un formulaire électronique harmonisé est prévu à l'étape suivante.

Étape 4: Déclaration de mission

La direction du CSIRT fictif a fait la déclaration de mission suivante:
« Le CSIRT fictif apporte des informations et une aide au personnel de sa société hôte en vue de réduire les risques d'incidents de sécurité informatique et de répondre à ce type d'incidents lorsqu'ils surviennent. »

Le CSIRT fictif précise ainsi clairement qu'il a une fonction interne essentiellement axée sur les questions de sécurité informatique.

- -

Étape 5: Élaboration du plan d'activités

Modèle financier
Étant donné que la société a une activité en ligne et un département informatique fonctionnant l'une et l'autre 24 heures par jour et 7 jours par semaine, elle a décidé de proposer un service complet durant les heures ouvrables et un service de garde en dehors de celles-ci. Les services destinés aux parties prenantes seront fournis gratuitement, mais l'éventualité de services prestés à l'intention de clients extérieurs sera envisagée lors de la phase pilote et d'évaluation.

Modèle des recettes
Au cours de la phase de démarrage et pilote, le CSIRT sera financé par la société hôte. Un financement complémentaire sera examiné au cours de la phase pilote et d'évaluation, en envisageant notamment la vente de services à des clients extérieurs.

Modèle organisationnel
L'organisation hôte étant une petite entreprise, c'est le modèle intégré qui est retenu.
Une équipe de trois personnes assurera les services de base pendant les heures ouvrables (diffusion des bulletins de sécurité et traitement/coordination des incidents).

Le département informatique de l'entreprise occupe déjà du personnel doté des compétences requises. Un accord est conclu avec ce département, afin que le nouveau CSIRT puisse faire appel à une aide ponctuelle, le cas échéant. La deuxième ligne de leurs techniciens de garde pourra également être utilisée.
Une équipe CSIRT de base comprenant quatre membres à temps plein et cinq membres supplémentaires sera mise en place. L'un d'eux est également disponible en équipe mobile.

Personnel
Le chef d'équipe CSIRT a des antécédents professionnels en matière de sécurité et de soutien au premier et au second niveau, et il a déjà travaillé dans le domaine de la tolérance aux pannes et de la gestion de crise. Les trois autres membres de l'équipe sont des spécialistes de la sécurité. Les membres de l'équipe CSIRT détachés à temps partiel par le département informatique sont, pour leur part, des spécialistes de l'infrastructure en place dans la société.

Étape 5 Utilisation de l'espace de bureau et politique de sécurité de l'information
Équipement et localisation de l'espace de bureau
Étant donné que la société hôte s'est déjà dotée d'une sécurité physique efficace, le nouveau CSIRT est lui-même bien protégé. Un «quartier général» est prévu pour permettre la coordination en cas d'urgence. Un coffre-fort est acheté pour le matériel d'encryptage et les documents sensibles. Une ligne téléphonique séparée a été installée, central compris, pour faciliter l'accès au numéro d'urgence pendant les heures ouvrables et au téléphone mobile «de garde» en dehors de celles-ci en utilisant le même numéro d'appel.

Le matériel et le site Internet de la société déjà en place peuvent également servir à diffuser les informations relevant du CSIRT. Une liste de distribution est établie et tenue à jour; elle est partiellement réservée à la communication entre les membres de l'équipe, ainsi qu'avec d'autres équipes. Toutes les coordonnées de contact des membres du personnel sont stockées dans une base de données, dont une version imprimée est conservée dans le coffre-fort.

Réglementation
Étant donné que le CSIRT est intégré dans une société ayant déjà adopté une politique en matière de sécurité de l'information, les mesures correspondantes au niveau du CSIRT ont été prises avec l'aide du conseiller juridique de l'entreprise.
- -
Étape 7 Recherche de coopération
Plusieurs CSIRT opérant dans le pays ont été rapidement recensés grâce au répertoire de l'ENISA, et des contacts ont été pris. Une visite du chef d'équipe récemment recruté a été organisée chez l'un d'eux. Il a été informé à cette occasion des activités CSIRT menées au plan national. Il a également participé à une réunion qui lui a permis de rassembler des exemples de méthodes de travail et de bénéficier du soutien de plusieurs autres équipes.
- -
Étape 8 Promotion du plan d'activités
Il est décidé de rassembler des faits et des chiffres à partir de l'historique de l'entreprise – une démarche particulièrement utile pour avoir un aperçu statistique de la situation en matière de sécurité informatique. Cette collecte de données doit se poursuivre après la mise en service du CSIRT, afin de maintenir les statistiques à jour.

D'autres CSIRT nationaux ont été contactés et interrogés à propos de la présentation de leurs arguments économiques (*business case*). Ils ont apporté une aide sous la forme de diapositives contenant des informations relatives aux développements récents en matière d'incidents liés à la sécurité informatique et aux coûts qu'ils engendrent.

Il n'a pas été nécessaire, dans notre exemple de CSIRT fictif, de déployer beaucoup d'efforts pour convaincre la direction de l'importance de l'activité informatique: le feu vert pour la première étape a donc été facilement obtenu. Une justification stratégique et commerciale et un plan de projet ont été élaborés, y compris une estimation des coûts de création et d'exploitation.
- -

Étape 9 Établissement des processus de traitement et des procédures opérationnelles et techniques

Le CSIRT fictif concentre son activité sur la prestation de services de base:

- Alertes et avertissements
- Annonces
- Traitement des incidents

L'équipe a mis au point des procédures qui fonctionnent bien et qui sont aisément compréhensibles par tous les membres de l'équipe. Le CSIRT fictif a également engagé un expert juridique pour les questions de responsabilité et la politique de sécurité de l'information. L'équipe a adopté plusieurs outils utiles et a obtenu de précieux renseignements à propos de certains aspects opérationnels en discutant avec d'autres CSIRT.

Un formulaire type a été établi pour les bulletins de sécurité et les signalements d'incidents. L'équipe traite les incidents à l'aide du système RTIR.

- -

Étape 10 Formation du personnel

Le CSIRT fictif décide d'envoyer tous les membres de son personnel technique à la prochaine session de cours TRANSITS. Le chef d'équipe suivra en outre le cours *Managing a CSIRT* (gestion d'un CSIRT) du CERT/CC.

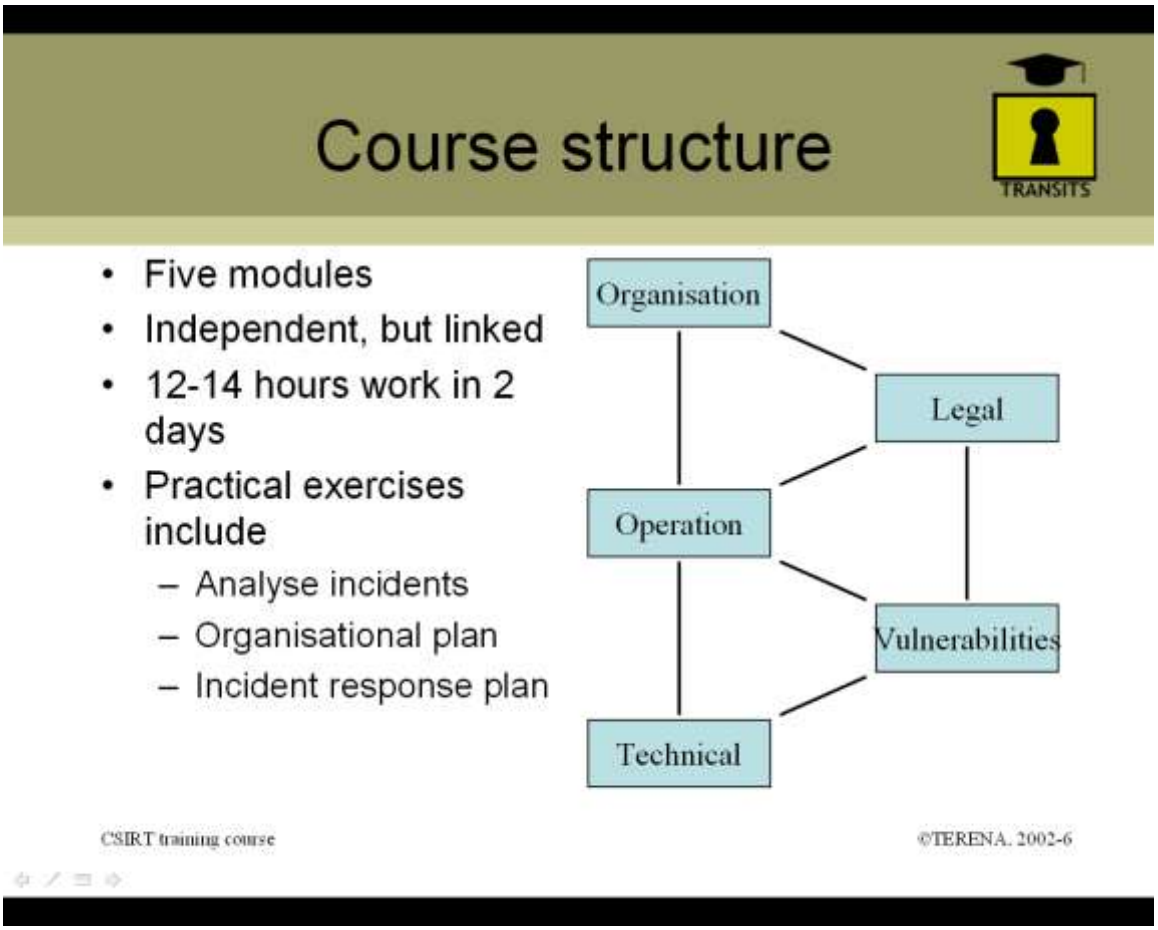
- -

Étape 11: Exercice

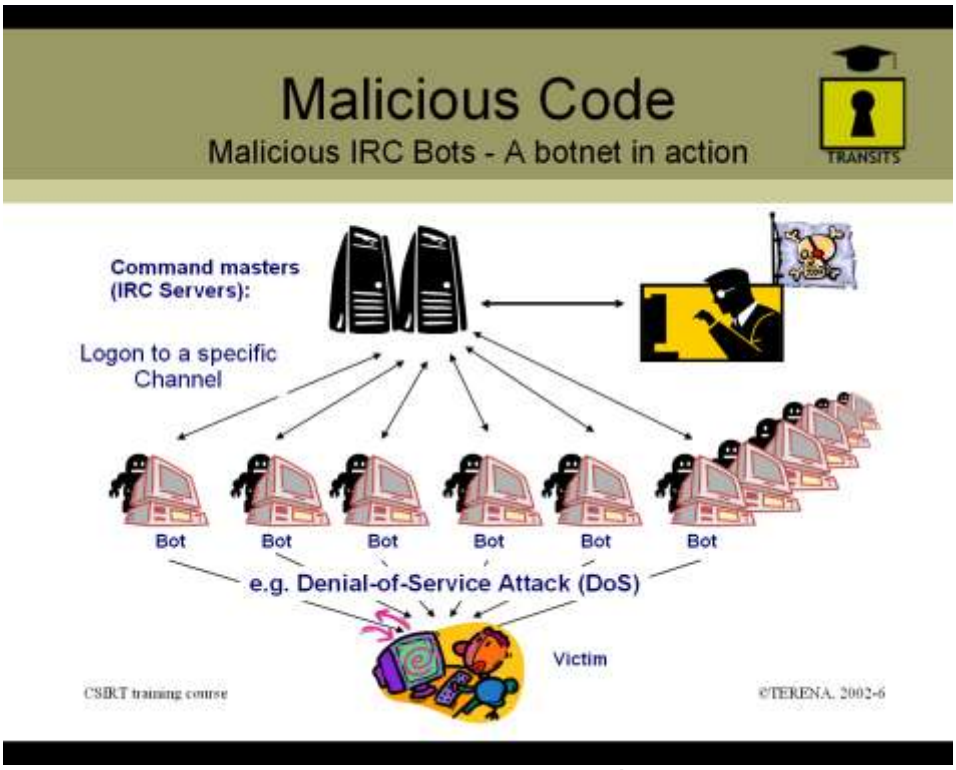
Au cours de ses premières semaines de fonctionnement, le CSIRT fictif s'est exercé à l'aide de plusieurs cas fictifs (communiqués par d'autres CSIRT à titre d'exemples). Il a publié en outre quelques bulletins de sécurité basés sur de véritables informations concernant des vulnérabilités diffusées par les fournisseurs de matériel et de logiciel, qu'il a adaptées aux besoins de ses propres parties prenantes.

A.4 Extraits de cours de formation concernant les CSIRT

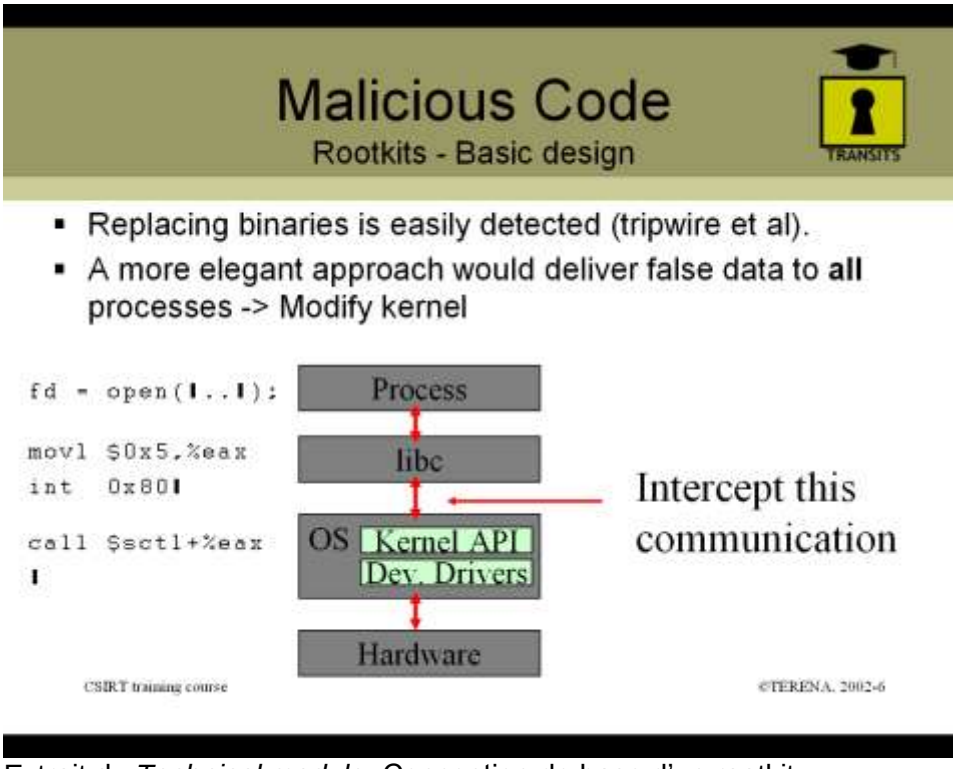
TRANSITS (avec l'aimable autorisation de Terena, http://www.terena.nl)



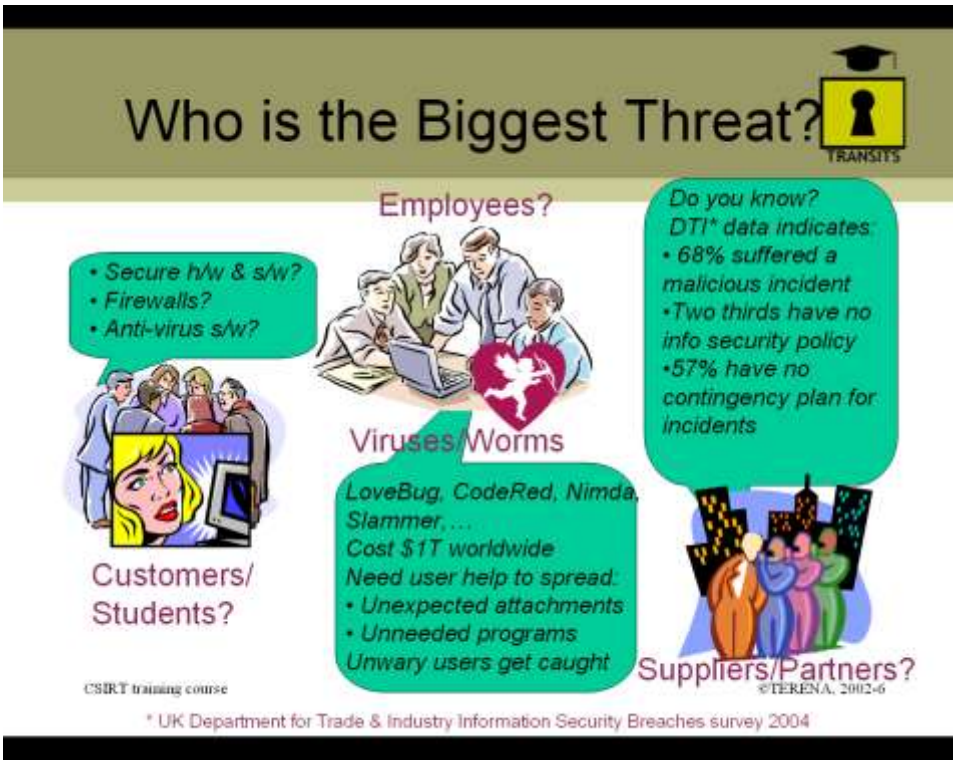
Aperçu de la structure du cours



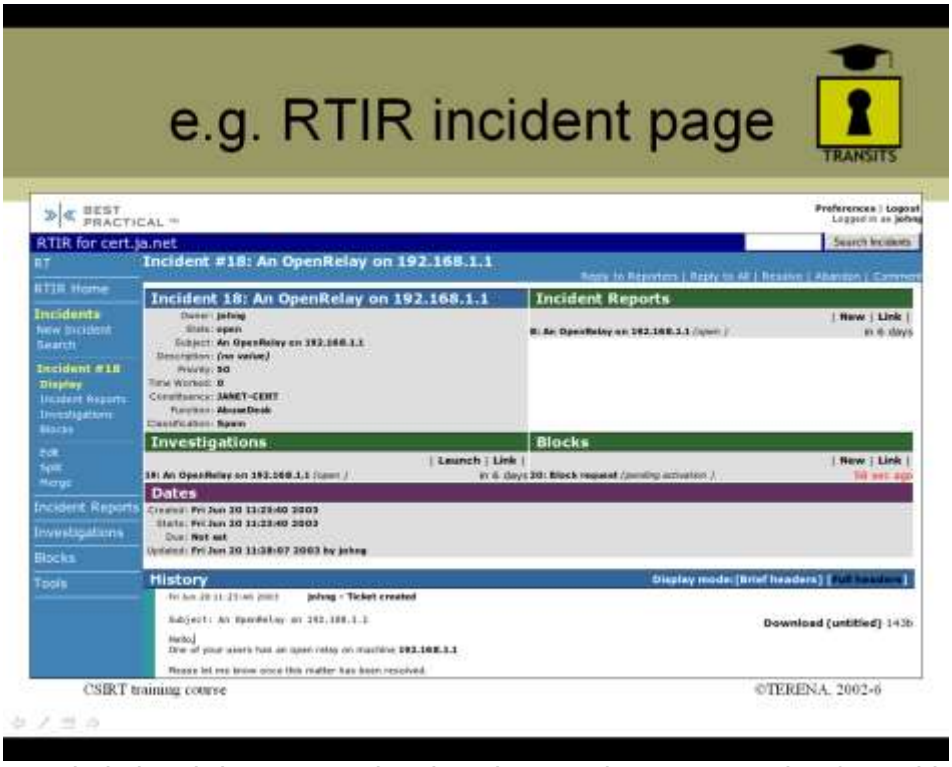
Extrait du *Technical module*: Description d'un réseau de type Botnet



Extrait du *Technical module*: Conception de base d'un rootkit



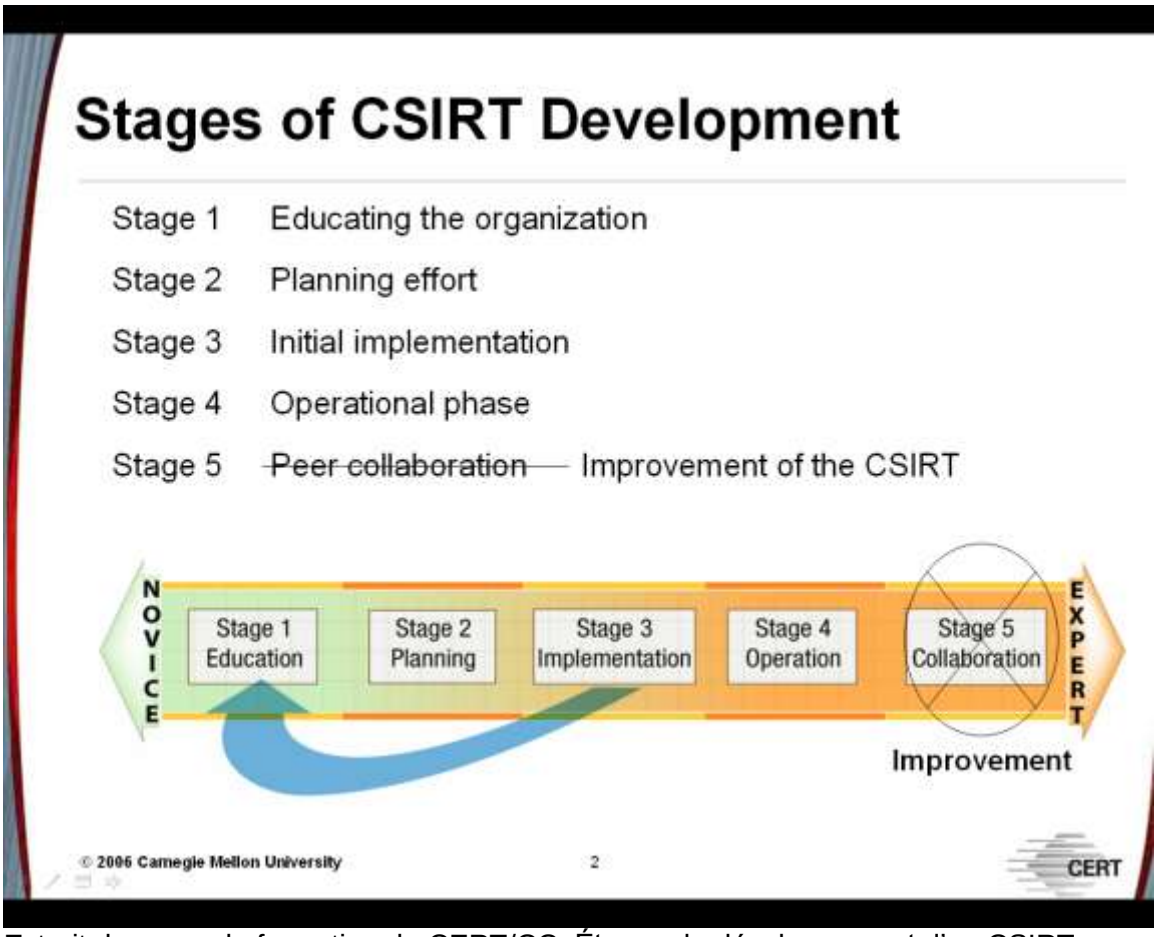
Extrait de l'*Organisational module*: La plus grande menace se trouve-t-elle à l'intérieur ou à l'extérieur?



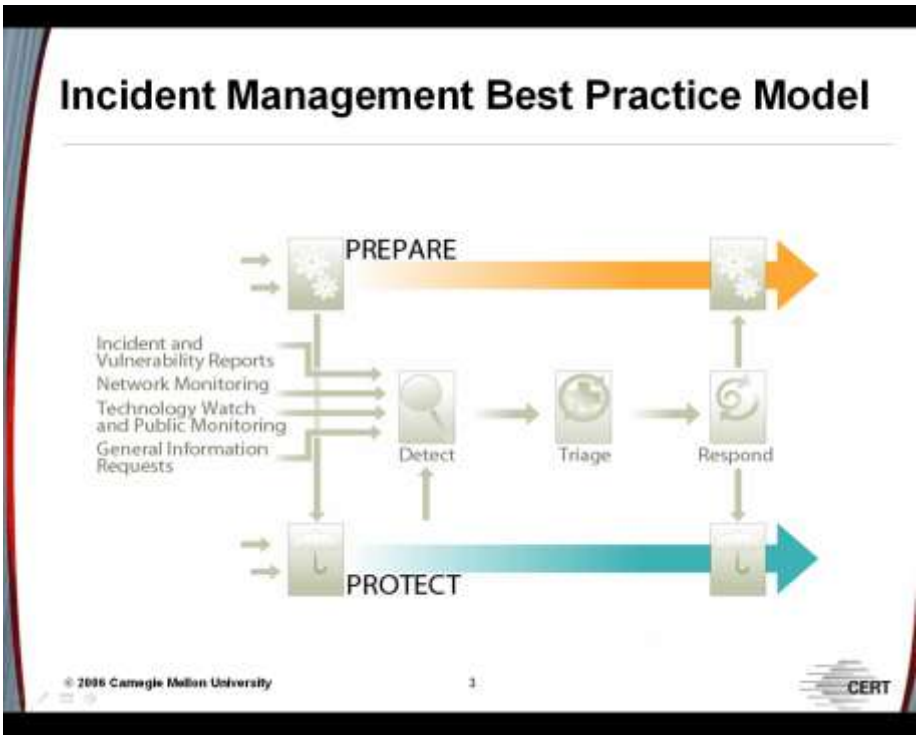
Extrait de la rubrique *Operational track*: RTIR (Request Tracker for Incident Response)

«Création de CSIRT» (avec l'aimable autorisation du CERT/CC http://www.cert.org)

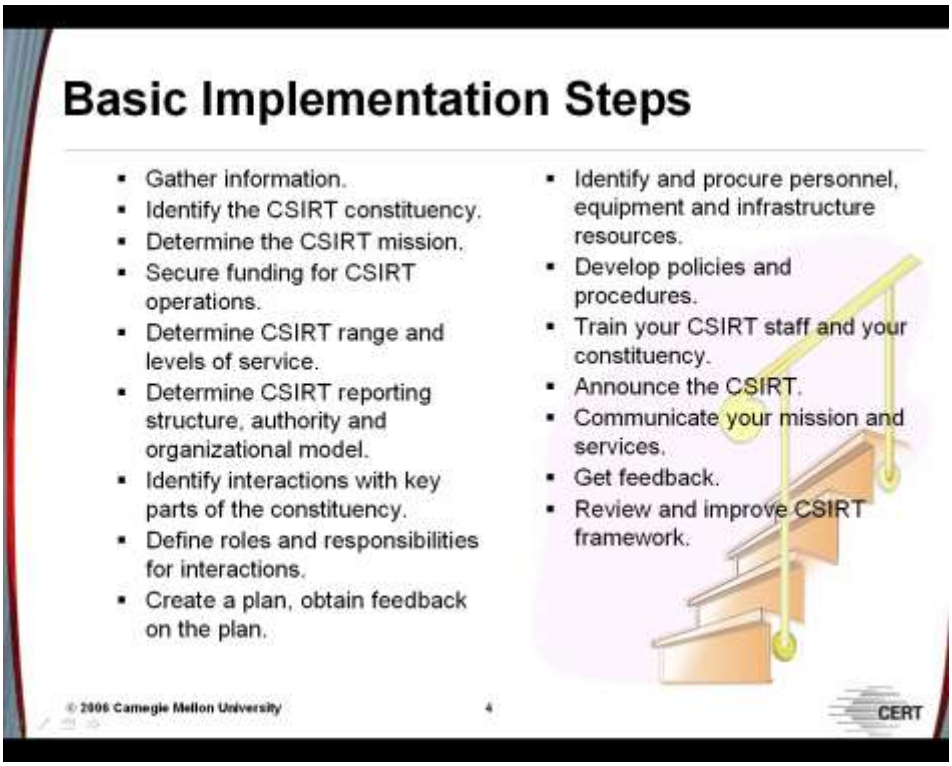
L'ENISA exprime toute sa reconnaissance à la CSIRT Development Team du programme CERT pour nous avoir permis d'utiliser le contenu de ses cours de formation!



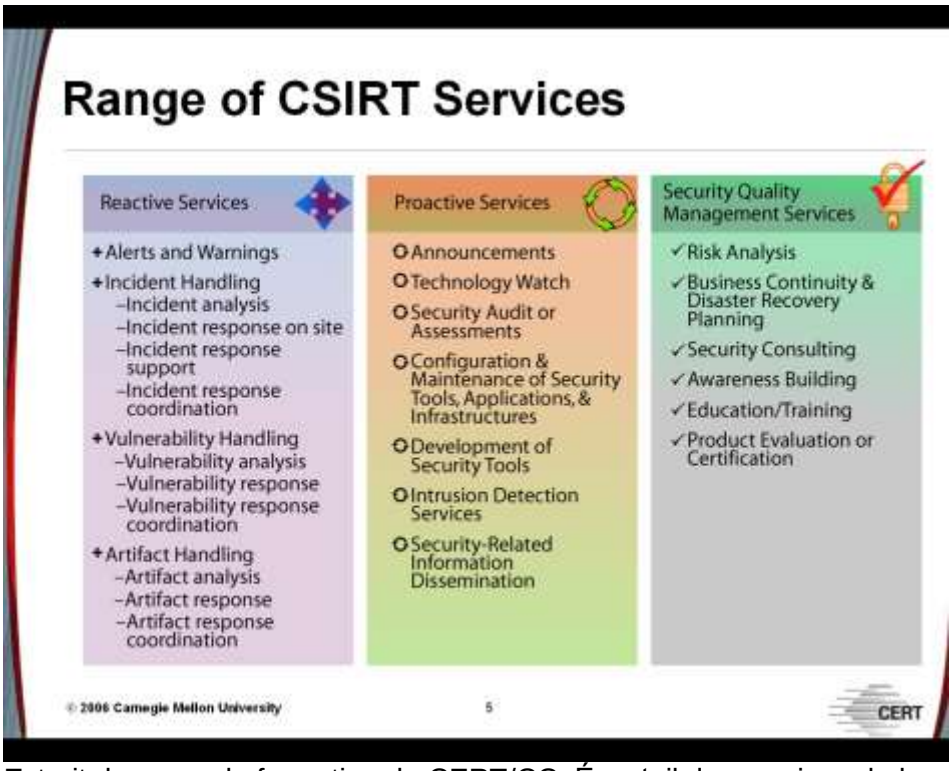
Extrait du cours de formation du CERT/CC: Étapes de développement d'un CSIRT



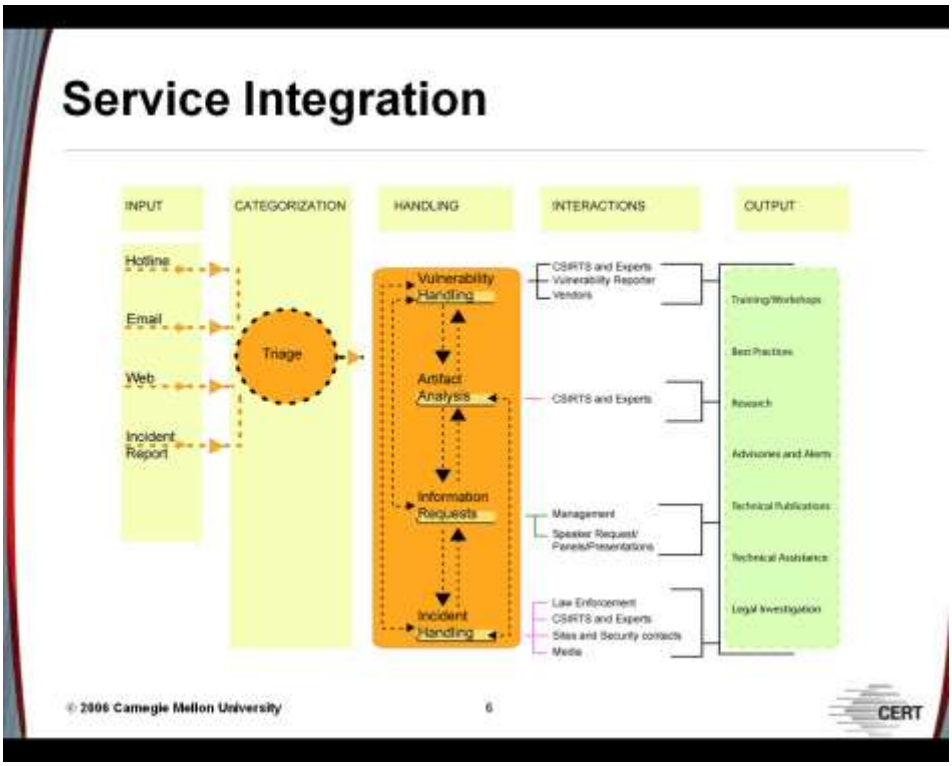
Extrait du cours de formation du CERT/CC: Bonnes pratiques en matière de traitement des incidents



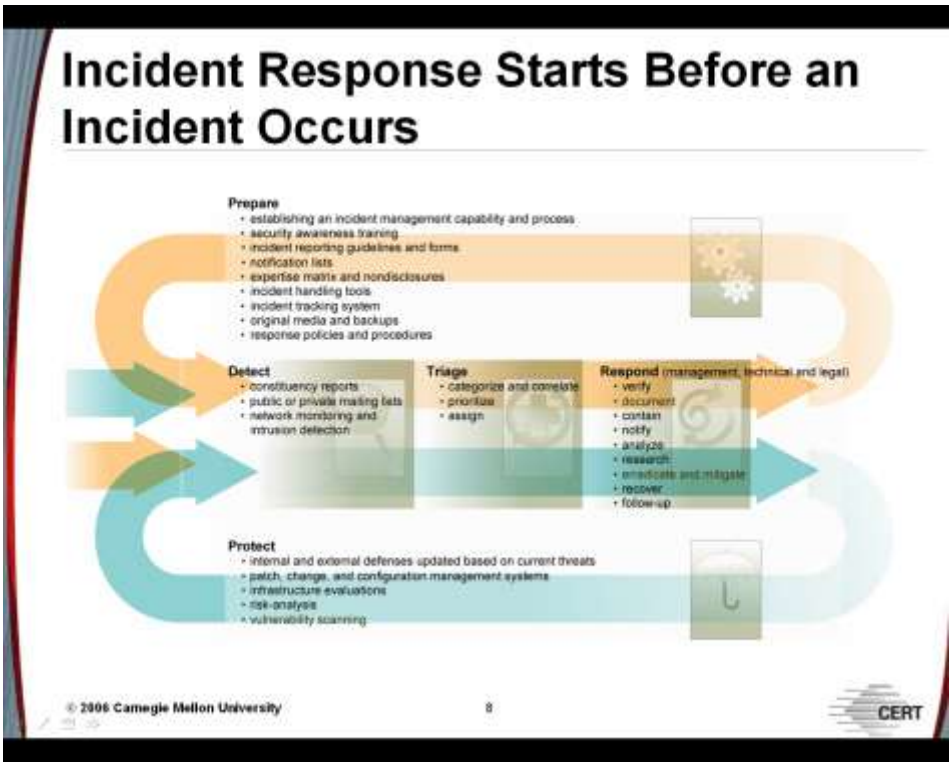
Extrait du cours de formation du CERT/CC: Les étapes de création d'un CSIRT



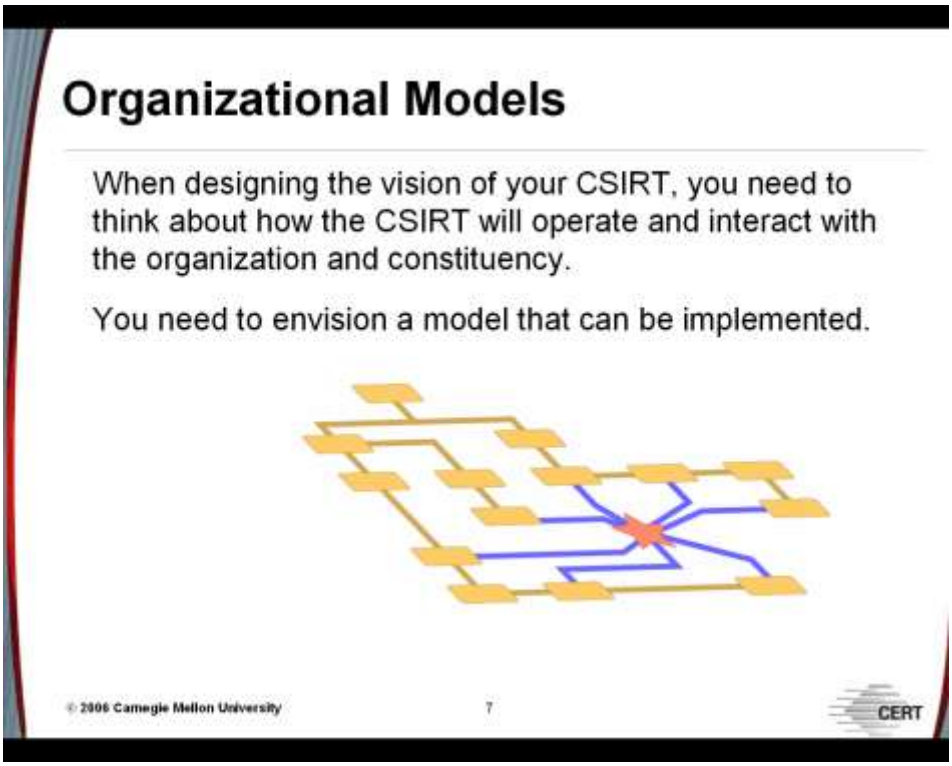
Extrait du cours de formation du CERT/CC*:* Éventail des services de base d'un CSIRT



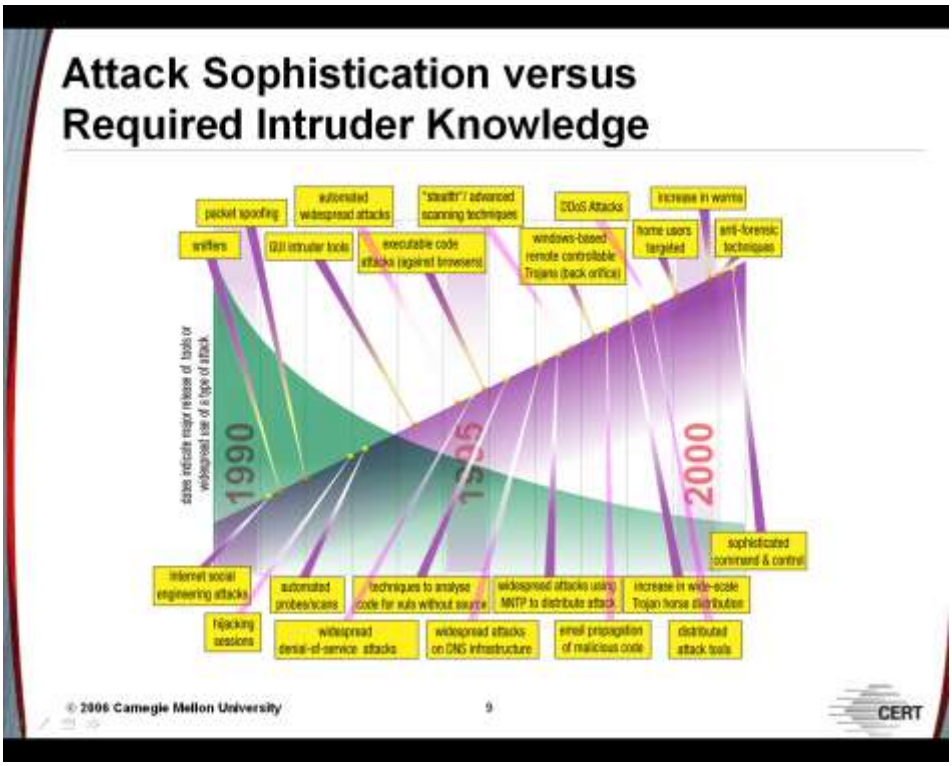
Extrait du cours de formation du CERT/CC*:* Déroulement du traitement des incidents



Extrait du cours de formation du *CERT/CC:* Réponse aux incidents



Extrait du cours de formation du CERT/CC*:* Comment structurer le CSIRT?



Extrait du cours de formation du CERT/CC*:* Moins de savoir-faire pour davantage de dégâts