Groupe de travail Réseau
Request for Comments : 2350
BCP: 21
Catégorie : Bonnes pratiques actuelles

N. Brownlee, The University of Auckland
E. Guttman, Sun Microsystems
juin 1998
Traduction Claude Brière de L'Isle

Attentes pour la réponse à un incident de sécurité informatique

Statut de ce mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
L'objet de ce document est d'exprimer les attentes de la communauté générale de l'Internet en ce qui concerne les équipes de réponse aux incidents de sécurité informatique (CSIRT, *Computer Security Incident Response Team*). Il n'est pas possible de définir un ensemble d'exigences qui serait approprié pour toutes les équipes, mais il est possible et utile de faire la liste et de décrire l'ensemble général des sujets et des questions qui se posent et intéressent les communautés du secteur.

Les mandants des CSIRT ont un besoin légitime et le droit de pleinement comprendre les politiques et procédures de 'leur' équipe de réponse aux incidents de sécurité informatique. Une façon de prendre en charge cette compréhension est de fournir les informations détaillées que les usagers peuvent prendre en compte, sous la forme d'un gabarit formel complété par le CSIRT. On fournit une description d'un tel gabarit et un exemple rempli.

Table des Matières

1 Introduction....1
2 Domaine d'application....2
2.1 Publication des politiques et procédures de CSIRT....2
2.2 Relations entre différentes CSIRT....3
2.3 Établissement de communications sûres....4
3. Information, politiques et procédures....4
3.1 Obtention du document....5
3.2 Informations de contact....5
3.3 Statuts....5
3.4 Politiques....6
3.5 Services....8
3.6 Formulaires de rapport d'incident....9
3.7 Déclinaison de responsabilité....9
Appendice A Glossaire des termes....10
Appendice B Questions annexes....10
Appendice C Équipes de réponse aux incidents de sécurité informatique connues....11
Appendice D Grandes lignes d'un gabarit de CSIRT....12
Appendice E Exemple de gabarit 'rempli' pour une CSIRT....12
4. Remerciements....19
5. Références....19
6. Considérations pour la sécurité....19
7. Adresse des auteurs....19
8. Déclaration complète de droits de reproduction....19

1 Introduction

Le groupe de travail GRIP a été formé pour créer un document qui décrive les attentes de la communauté en ce qui concerne les équipes de réponse aux incidents de sécurité informatiques (CSIRT). Bien que le besoin d'un tel document trouve son origine dans la communauté générale de l'Internet, les attentes exprimées devraient aussi correspondre étroitement à celles de communautés plus restreintes.

Il y a eu dans le passé une certaine incompréhension sur ce qu'on attend des CSIRT. L'objectif du présent document est de fournir un cadre pour présenter les sujets importants (sur la réponse aux incidents) qui concernent la communauté.

Avant de continuer, il est important de bien comprendre ce que signifie l'expression "équipe de réponse aux incidents de sécurité informatique". Pour les besoins de ce document, une CSIRT est une équipe qui effectue, coordonne et prend en charge la réponse aux incidents de sécurité qui impliquent des sites dans un domaine défini (voir une définition plus complète à l'Appendice A). Tout groupe se baptisant CSIRT pour un domaine spécifique doit donc réagir aux incidents de sécurité rapportés, et aux menaces sur "son" domaine selon des modalités dont la communauté en question s'accorde sur le fait qu'elles sont dans son intérêt général.

Comme il est vital que chaque membre d'une communauté du domaine soit capable de comprendre ce qu'il est raisonnable d'attendre de son équipe, une CSIRT devrait préciser qui appartient à son domaine et définir les services que l'équipe offre à la communauté. De plus, chaque CSIRT devrait publier sa politique et ses procédures de fonctionnement. De même, ces mêmes membres ont besoin de savoir ce qui est attendu d'eux pour qu'ils puissent recevoir les services de leur équipe. Cela exige aussi que l'équipe publie comment et où faire rapport des incidents.

Le présent document donne le détail d'un gabarit qui sera utilisé par les CSIRT pour communiquer ces informations aux membres de leur domaine. Ceux-ci devraient certainement s'attendre à ce qu'une CSIRT fournisse les services qu'ils décrivent dans le gabarit rempli.

On doit souligner que sans une active participation des usagers, l'efficacité des services de la CSIRT peut être gravement diminuée. Ceci est particulièrement le cas avec les rapports. Au minimum, les usagers doivent savoir qu'ils devraient faire rapport des incidents de sécurité, et savoir comment et à qui ils devraient en faire rapport.

De nombreux incidents de sécurité informatique ont leur origine en dehors des frontières de la communauté locale et affectent les sites intérieurs, d'autres ont leur origine à l'intérieur de la communauté locale et affectent des hôtes ou usagers extérieurs. Souvent, le traitement des incidents de sécurité va impliquer plusieurs sites et éventuellement plusieurs CSIRT. Résoudre des incidents exige une coopération entre des sites individuels et des CSIRT, et entre des CSIRT.

Les communautés concernées ont besoin de savoir exactement comment leur CSIRT va travailler avec les autres CSIRT et les organisations en dehors de leur domaine, et quelles informations seront partagées.

Le reste de ce document décrit l'ensemble des sujets et questions que les CSIRT ont besoin de développer pour leur domaine. Cependant, on ne tente pas de spécifier la réponse "correcte" aux divers sujets. Chaque sujet est plutôt exposé sous l'aspect de sa signification.

La Section 2 donne un aperçu général des trois secteurs majeurs : la publication des informations par une équipe de réponse, la définition des relations de l'équipe de réponse avec les autres équipes de réponse, et le besoin de communications sûres. La Section 3 décrit en détails tous les types d'informations que la communauté a besoin de connaître au sujet de son équipe de réponse.

Pour en faciliter l'utilisation par la communauté, ces sujets sont rassemblés dans un modèle présenté à l'Appendice D. Ce modèle peut être utilisé par les intéressés pour obtenir des informations de leur CSIRT.

Le souhait sincère du groupe de travail est que grâce aux éclaircissements sur ces sujets dans le présent document, la compréhension soit améliorée entre la communauté et ses CSIRT.

2 Domaine d'application

Les interactions entre une équipe de réponse aux incidents et la communauté constituante de cette équipe de réponse exigent tout d'abord que la communauté comprenne la politique et les procédures de l'équipe de réponse. Ensuite, comme de nombreuses équipes de réponse collaborent pour traiter les incidents, la communauté doit aussi comprendre les relations entre son équipe de réponse et les autres équipes. Finalement, de nombreuses interactions vont tirer parti des infrastructures publiques existantes, de sorte que la communauté a besoin de savoir comment ces communications vont être protégées. Chacun de ces sujets va être décrit plus en détails dans les trois paragraphes suivants.

2.1 Publication des politiques et procédures de CSIRT

Chaque utilisateur qui a accès à une équipe de réponse aux incidents de sécurité informatique devrait en savoir autant qu'il est possible sur les services de cette équipe et les interactions avec elle avant qu'il en ait réellement besoin.

Une déclaration claire des politiques et procédures d'une CSIRT aide le domaine à comprendre comment rapporter au mieux les incidents et quel soutient attendre après coup. La CSIRT va t-elle assister à la résolution de l'incident ? Va t-elle fournir une aide pour éviter les incidents à l'avenir ? Des attentes claires, en particulier sur les limitations des services fournis par une CSIRT, vont rendre l'interaction avec elle plus efficace et effective.

Il y a différentes sortes d'équipes de réponse : certaines ont un très large domaine (par exemple, le centre de coordination CERT et l'Internet) ; d'autres ont un domaine plus limité (par exemple, DFN-CERT, CIAC), et d'autres encore ont un domaine très restreint (par exemple, des équipes de réponse commerciales, des équipes de réponse d'entreprise). Sans considération du type d'équipe de réponse, le domaine pris en charge par elles doit être connaissable par les politiques et procédures de l'équipe. Donc, il est obligatoire que les équipes de réponse rendent publiques de telles informations dans leur domaine.

Une CSIRT devrait communiquer toutes les informations nécessaires sur sa politique et ses services sous une forme convenable pour les besoins de son domaine. Il est important de comprendre que toutes les politiques et procédures n'ont pas besoin d'être disponibles au public. Par exemple, il n'est pas nécessaire de comprendre le fonctionnement interne d'une équipe pour interagir avec elle, comme lorsque on rapporte un incident ou qu'on reçoit des directives sur la façon d'analyser ou sécuriser son système.

Dans le passé, certaines équipes ont fourni une sorte de cadre de fonctionnement, d'autres ont fourni une liste de questions fréquemment posées (FAQ), alors que d'autres ont écrit des articles à distribuer à des conférences d'usagers ou envoyé des lettres d'information.

On recommande que chaque CSIRT publie ses lignes directrices et ses procédures sur son propre serveur d'informations (par exemple, un serveur de la Toile mondiale). Cela permettrait à chaque domaine d'y accéder facilement, bien que reste le problème de savoir comment un usager peut trouver son équipe ; les gens au sein d'un domaine ont à découvrir qu'il y a une CSIRT "à leur disposition".

On pense que bientôt un formulaire de CSIRT complété pourra être trouvé par les moteurs de recherche modernes, ce qui va aider à distribuer les informations sur l'existence des CSIRT et les informations de base nécessaires pour y accéder.

Il serait très utile d'avoir un répertoire central contenant tous les modèles de CSIRT complétés. Il n'en existe pas au moment de la rédaction du présent mémoire, mais cela pourrait changer à l'avenir.

Sans considération de la source d'où les informations sont restituées, l'utilisateur du modèle doit vérifier son authenticité. Il est fortement recommandé que des documents aussi vitaux soient protégés par des signatures numériques. Cela permettra à l'utilisateur de vérifier que le modèle a bien été publié par la CSIRT et qu'il n'a pas été altéré. Le présent document suppose que le lecteur est familier du bon usage des signatures numériques pour déterminer si un document est authentique.

2.2 Relations entre différentes CSIRT

Dans certains cas une CSIRT peut être capable de fonctionner effectivement par elle même et en étroite coopération avec son domaine. Mais avec les réseaux internationaux d'aujourd'hui, il est plus probable que la plupart des incidents traités par une CSIRT vont impliquer des parties externes à son domaine. L'équipe aura donc besoin d'interagir avec les autres CSIRT et sites en dehors de son domaine.

La communauté constituante devrait comprendre la nature et l'extension de cette collaboration, car des informations très sensibles sur les participants individuels peuvent être divulguées dans le processus.

Les interaction entre CSIRT pourraient inclure de demander un avis aux autres équipes, disséminant la connaissance des problèmes, et en travaillant de façon coopérative pour résoudre un incident de sécurité qui affecte un ou plusieurs des domaines des CSIRT.

En établissait des relations pour prendre en charge de telles interactions, les CSIRT doivent décider quelles sortes d'accords peuvent exister entre eux afin de partager des informations tout en les sauvegardant, si ces relations peuvent être divulguées, et à qui.

Noter qu'il y a une différence entre un accord sur un pied d'égalité, par lequel les CSIRT impliquées s'accordent pour travailler ensemble et partager les information, et une simple coopération, où une CSIRT (ou toute autre organisation) contacte simplement une autre CSIRT et lui demande aide ou avis.

Bien que l'établissement de telles relations soit très important et affecte la capacité d'une CSIRT à prendre en charge son domaine, il appartient aux équipes impliquées de décider des détails. Il sort du domaine d'application du présent document

de faire des recommandations sur ce processus. Cependant, le même ensemble d'informations utilisées pour établir les attentes d'une communauté d'utilisateurs en ce qui concerne le partage des informations va aider d'autres parties à comprendre les objectifs et les services d'une CSIRT spécifique, à l'appui d'un premier contact.

2.3 Établissement de communications sûres

Une fois qu'une partie a décidé de partager les informations avec une autre partie, ou que deux parties se sont mises d'accord pour partager les informations ou travailler ensemble – comme exigé pour la coordination de la réponse à un incident de sécurité informatique – toutes les parties impliquées ont besoin de canaux de communications sécurisés. (Dans ce contexte, "sécurisé" se réfère à la transmission protégée des informations partagées entre les différentes parties, et non à l'utilisation appropriée des informations par les parties.)

Les buts de la communication sécurisée sont :
- Confidentialité : quelqu'un d'autre peut-il accéder au contenu de la communication ?
- Intégrité : quelqu'un d'autre peut-il manipuler le contenu de la communication ?
- Authenticité : Suis-je en communication avec la "bonne" personne ?

Il est très facile d'envoyer un message électronique falsifié, et pas difficile d'établir une (fausse) identité par téléphone. Les techniques cryptographiques, par exemple la très bonne confidentialité (PGP, *Pretty Good Privacy*) ou la messagerie à confidentialité améliorée (PEM, *Privacy Enhanced Mail*) peuvent fournir des moyens efficaces pour sécuriser la messagerie électronique. Avec l'équipement correct, il est aussi possible de sécuriser une communication téléphonique. Mais avant d'utiliser de tels mécanismes, les deux parties ont besoin de la "bonne" infrastructure, qui est de préparer les choses à l'avance. La préparation la plus importante est de s'assurer de l'authenticité des clés de chiffrement utilisées dans une communication sécurisée :
- Clés publiques (pour des techniques comme PGP et PEM) : Comme les clés sont accessibles par l'Internet, les clés publiques doivent être authentifiées avant utilisation. Alors que PGP s'appuie sur une "toile de confiance" (où les utilisateurs signent les clés des autres utilisateurs) PEM s'appuie sur une hiérarchie (où des autorités de certification signent les clés des usagers).
- Clés secrètes (pour des techniques comme DES et PGP/chiffrement conventionnel) : Comme elles doivent être connues de l'envoyeur et du receveur, les clés secrètes doivent être échangées avant la communication via un canal sûr.

La communication est critique pour tous les aspects de la réponse à un incident. Une équipe peut mieux prendre en charge l'utilisation des techniques susmentionnées en collectant toutes les informations pertinentes, d'une façon cohérente. Des exigences spécifiques (telles qu'appeler un numéro spécifique pour vérifier l'authenticité des clés) devraient être précisées depuis le début. Le gabarit de CSIRT fournit un véhicule standardisé pour la livraison de ces informations.

Il sort du domaine d'application du présent document de traiter des problèmes techniques et administratifs des communications sécurisées. Le point est que les équipes de réponse doivent prendre en charge et utiliser une méthode pour sécuriser les communications entre elles-mêmes et leurs clients (ou les autres équipes de réponse). Quel que soit le mécanisme, le niveau de protection qu'il fournit doit être acceptable pour la communauté des clients.

3. Information, politiques et procédures

À la Section 2, on a mentionné que les politiques et procédures d'une équipe de réponse ont besoin d'être publiées pour sa communauté de clients. Dans cette section, on va faire la liste de tous les types d'informations que la communauté a besoin de recevoir de la part de son équipe de réponse. Comment ces informations sont communiquées à la communauté va différer d'une équipe à l'autre, comme le contenu des informations spécifiques. L'intention est ici de décrire clairement les diverses sortes d'informations qu'une communauté de clients attend de son équipe de réponse.

Pour rendre plus facilement compréhensibles les problèmes et sujets pertinents pour l'interaction des clients avec "leur" CSIRT, on suggère qu'une CSIRT publie toutes les informations, politiques, et procédures concernant ses clients dans un document, suivant le modèle donné à l'Appendice D. La structure du modèle arrange les éléments, rendant facile la fourniture des informations spécifiques ; dans l'Appendice E on fournit un exemple d'un modèle rempli pour l'université fictive XYZ. Bien qu'aucune recommandation ne soit faite quant à ce qu'une CSIRT devrait adopter comme politique ou procédures, différentes possibilités sont présentées pour donner des exemples. La chose la plus importante est qu'une CSIRT ait une politique et que ceux qui interagissent avec la CSIRT soient capables de l'obtenir et de la comprendre.

Comme toujours, tous les aspects de tous les environnements et/ou équipes ne peuvent être couverts. Cette présentation devrait être vue comme une suggestion. Chaque équipe devrait se sentir libre d'inclure ce qu'elle estime nécessaire pour prendre en charge sa clientèle.

3.1 Obtention du document

Les détails d'une CSIRT vont changer au fil du temps, de sorte que le modèle complété doit indiquer quand il a été mis à jour. De plus, des informations devraient être fournies sur la façon de se tenir au courant des mises à jour futures. Sans cela, il est inévitable qu'apparaissent des incompréhensions et de mauvaises interprétations ; des documents périmés peuvent faire plus de mal que de bien.

- Date de la dernière mise à jour : cela devrait être suffisant pour permettre à toute personne intéressée d'évaluer l'actualité du document.

- Liste de distribution : les listes de diffusion sont un mécanisme pratique pour distribuer des informations à jour à un grand nombre d'utilisateurs. Une équipe peut décider d'utiliser sa propre liste ou une liste déjà existante pour notifier aux usagers chaque changement du document. La liste peut normalement être celle des groupes avec lesquels la CSIRT a de fréquentes interactions. Des signatures numériques devraient être utilisées pour les messages de mise à jour envoyés par une CSIRT.

- Localisation du document : c'est le site sur lequel une version actuelle du document est accessible à travers les services d'information en ligne de l'équipe. Les clients peuvent alors facilement en apprendre plus sur l'équipe et vérifier les mises à jour récentes. Cette version en ligne devrait aussi être accompagnée d'une signature numérique.

3.2 Informations de contact

Tous les détails sur la façon de contacter la CSIRT devraient figurer sous cette rubrique, bien qu'ils puissent être très différents pour des équipes différentes ; par exemple, certaines peuvent choisir de ne pas publier les noms des membres de l'équipe. On ne donnera pas d'autres éclaircissements lorsque la signification de l'élément est évidente.

- Nom de la CSIRT
- Adresse postale
- Zone horaire : elle est utile pour coordonner les incidents qui s'étendent sur plusieurs fuseaux horaires.
- Numéro de téléphone
- Numéro de télécopie
- Autres moyens de télécommunication : certaines équipes peuvent fournir des communications vocales sécurisées (par exemple, STU III).
- Adresse de messagerie électronique
- Clés publiques et chiffrement : l'utilisation de techniques spécifiques dépend de la capacité des partenaires de la communication a avoir accès aux programmes, clés et ainsi de suite. On devrait y donner les informations pertinentes pour permettre aux usagers de déterminer si et comment ils peuvent faire usage de communication chiffrée lorsque ils interagissent avec la CSIRT.
- Membres de l'équipe
- Heures d'ouverture : Le programme des heures d'ouverture et des jours fériés devrait être fourni ici. Y a t-il un numéro d'accueil permanent ?
- Informations de contact supplémentaires : Y a t-il des informations de contact spécifiques de cette clientèle ?

Des informations de contact plus détaillées peuvent être fournies. Cela pourrait inclure des contacts différents pour différents services, ou pourrait être une liste de services d'information en ligne. Si il existe des procédures spécifiques pour l'accès à certains services (par exemple des adresses pour les demandes de listes de diffusion) cela devrait être expliqué ici.

3.3 Statuts

Chaque CSIRT doit avoir des statuts qui spécifient ce qu'elle doit faire, et l'autorité sous laquelle elle doit le faire. Les statuts devraient inclure au moins les éléments suivants :
- Énoncé de la mission
- Domaine d'application
- Patronage / affiliation
- Autorité

3.3.1 Énoncé de la mission

La déclaration de mission devrait se concentrer sur les activités centrales de l'équipe, déjà mentionnées dans la définition

d'une CSIRT. Pour être considérée comme une équipe de réponse aux incidents de sécurité informatique, l'équipe doit prendre en charge le rapport des incidents et assurer le soutien de sa clientèle en traitant ces incidents.

Les objectifs et propos d'une équipe sont particulièrement importants, et requièrent une définition claire, sans ambiguïté.

3.3.2 Domaine d'application

Le domaine d'application d'une CSIRT peut être déterminé de plusieurs façons. Par exemple, ce pourrait être les employés d'une entreprise ou ses abonnés payants, ou il pourrait être défini en termes de technologie, comme les utilisateurs d'un système d'exploitation particulier.

La définition du domaine d'application devrait créer un périmètre autour du groupe auquel l'équipe va fournir le service. La section politique du document (voir ci-dessous) devrait expliquer comment seront traitées les demandes provenant de l'extérieur de ce périmètre.

Si une CSIRT décide de ne pas divulguer son domaine d'application, elle devrait expliquer les raisons de cette décision. Par exemple, les CSIRT à abonnement payant ne vont pas donner la liste de leurs clients mais vont déclarer qu'elles fournissent un service à un large groupe d'utilisateurs qui reste confidentiel à cause de ses engagements contractuels.

Les domaines d'application peuvent se chevaucher, comme lorsque un FAI fournit une CSIRT qui assure des services à des sites d'utilisateurs qui ont aussi des CSIRT. La section Autorité de la description de la CSIRT (voir ci-dessous) devrait préciser de telles relations.

3.3.3 Patronage / affiliation

L'organisation patronne, qui autorise les actions de la CSIRT, devrait être indiquée ensuite. Savoir cela aide les utilisateurs à comprendre les tenants et les aboutissants de la CSIRT, et c'est une information vitale pour établir la confiance entre un client et la CSIRT.

3.3.4 Autorité

Cette section va varier largement d'une CSIRT à l'autre, sur la base des relations entre l'équipe et son domaine d'application Alors qu'une CSIRT organisationnelle va recevoir son autorité de la gestion de l'organisation, la CSIRT d'une communauté sera prise en charge et choisie par la communauté, généralement dans un rôle consultatif.

Une CSIRT peut avoir ou non l'autorité pour intervenir dans le fonctionnement de tous les systèmes au sein de son périmètre. Elle devrait identifier la portée de son contrôle comme distinct du périmètre de sa clientèle. Si d'autres CSIRT fonctionnent hiérarchiquement dans son périmètre, cela devrait être mentionné à cet endroit, et les CSIRT en question identifiées.

La divulgation de l'autorité d'une équipe peut l'exposer à des actions en responsabilité. Chaque équipe devrait consulter un conseil juridique sur ces questions (voir plus de développement sur les questions de responsabilité au paragraphe 3.7).

3.4 Politiques

Il est critique que les équipes de réponse aux incidents définissent leur politique. Les paragraphes qui suivent discutent la communication de ces politiques à la communauté de la clientèle.

3.4.1 Types d'incidents et niveau de prise en charge

Les types d'incident que l'équipe est capable de traiter, et le niveau de prise en charge que l'équipe va offrir lors de la réponse à chaque type d'incident, devraient être résumés ici sous forme de liste. La section Services (voir ci-dessous) donnera des descriptions plus détaillées, et traitera des questions qui ne se rapportent pas aux incidents.

Le niveau de prise en charge dépend de facteurs comme la charge de travail de l'équipe, la complétude des informations disponibles. De tels facteurs devraient être mentionnés et leur impact devrait être expliqué. Comme une liste des types d'incidents connus serait incomplète à l'égard des incidents possibles ou futurs, une CSIRT devrait aussi donner quelques éléments de base sur le traitement "par défaut" des types d'incident non mentionnés par ailleurs.

L'équipe devrait déclarer si elle va agir sur les informations qu'elle reçoit sur les faiblesses qui créent des opportunités

d'incidents futurs. Un engagement à agir sur de telles informations au nom de sa clientèle est considéré comme une politique proactive de service facultative plutôt que comme une exigence de cœur de service pour une CSIRT.

3.4.2 Coopération, interaction et divulgation d'informations

Ce paragraphe devrait rendre explicite avec quels groupes la CSIRT interagit de façon habituelle. De telles interactions ne se rapportent pas nécessairement à la réponse aux incidents de sécurité informatique fournie, mais sont utilisées pour faciliter une meilleure coopération sur les sujets ou services techniques. Il n'a absolument pas besoin de détailler les accords de coopération ; le principal objet de ce paragraphe est de donner à la clientèle la compréhension de base de la sorte d'interactions qui sont établies et de ce à quoi elles servent.

La coopération entre les CSIRT peut être facilitée par l'utilisation d'une allocation d'un numéro de ticket unique combinée à des procédures explicites de relais. Cela réduit les risques d'incompréhension, de duplications des efforts, aide au retraçage des incidents et empêche les 'boucles' de communication.

La politique de rapport et de divulgation devrait dire clairement qui sont ceux qui reçoivent le rapport d'une CSIRT dans chaque circonstance. Elle devrait aussi noter si l'équipe va s'attendre à fonctionner à travers une autre CSIRT ou directement avec un membre d'un autre domaine sur les questions qui concernent spécifiquement ce membre.

Les groupes avec lesquels une CSIRT va interagir sont énumérés ci-dessous :

Équipes de réponse aux incidents :
Une CSIRT va souvent avoir besoin d'interagir avec d'autres CSIRT. Par exemple, une CSIRT dans une grande société peut devoir faire rapport des incidents à une CSIRT nationale, et une CSIRT nationale peut devoir rapporter les incidents aux CSIRT nationales des autres pays pour traiter avec tous les sites impliqués dans une attaque à grande échelle. La collaboration entre les CSIRT peut conduire à la divulgation d'informations. Voici des exemples d'une telle divulgation, mais cette liste ne prétend pas être exhaustive :

- Rapport des incidents au sein de la clientèle aux autres équipes. Si cela est fait, les informations propres au site peuvent passer dans le domaine public, accessibles à tous, en particulier, la presse.
- Traitement des incidents survenant au sein de la clientèle, mais rapportés de l'extérieur (ce qui implique que certaines informations ont déjà été divulguées hors site).
- Rapport des observations provenant de l'intérieur de la clientèle, indiquant des incidents suspectés ou confirmés à l'extérieur d'elle.
- Action sur des rapports d'incidents provenant de l'extérieur de la clientèle.
- Passage d'informations sur les faiblesses aux fabricants, aux CSIRT partenaires ou directement au sites affectés à l'intérieur ou l'extérieur de la clientèle.
- Rétroaction aux parties pour rapporter les incidents ou vulnérabilités.
- La fourniture des informations de contact se rapportant aux membres de la clientèle, aux membres d'autres clientèles, aux autres CSIRT, ou aux agences administratives.

Fabricants :
Certains fabricants ont leurs propres CSIRT, mais d'autres peuvent ne pas en avoir. Dans de tels cas, une CSIRT va devoir travailler directement avec un fabricant pour suggérer des améliorations, pour analyser les problèmes techniques ou vérifier les solutions proposées. Les fabricants jouent un rôle particulier dans le traitement d'un incident si les faiblesses de leurs produits sont impliquées dans l'incident.

Agences administratives :
Cela inclut la police et autres agences d'investigation. Les CSIRT et les utilisateurs du modèle devraient être sensibles aux lois et réglementations locales, qui peuvent varier considérablement d'un pays à l'autre. Une CSIRT peut donner des conseils sur les détails techniques des attaques ou rechercher des avis sur les implications légales d'un incident. Les lois et règlements locaux peuvent inclure des rapports spécifiques et des exigences de confidentialité.

Presse :
Une CSIRT peut être de temps en temps approchée par la presse pour des informations et des commentaires.
Une politique explicite concernant la divulgation à la presse peut aider, en particulier pour préciser les attentes de la clientèle d'une CSIRT. La politique à l'égard de la presse devra préciser les mêmes sujets que ci-dessus de façon plus spécifique, car la clientèle sera généralement très sensible aux contacts avec la presse.

Autres :
Cela peut inclure des activités de recherche ou les relations avec l'organisation patronnesse.

Le statut par défaut de toutes les informations que reçoit une équipe en rapport avec la sécurité sera normalement

'confidentiel', mais une application rigide de ce principe ferait apparaître l'équipe comme un “trou noir” informationnel, qui pourrait réduire la probabilité que l'équipe obtienne la coopération des clients et des autres organisations. Le modèle de CSIRT devrait définir quelles informations elle va divulguer ou rapporter, à qui et quand.

Des équipes différentes vont vraisemblablement être soumises à des contraintes juridiques différentes pour exiger ou limiter la divulgation, en particulier si elles travaillent dans des juridictions différentes. De plus, elles peuvent avoir des exigences en matière de rapports qui sont imposées par les organisations qui les patronnent. Chaque modèle d'équipe devrait spécifier ces contraintes, à la fois pour préciser les attentes des utilisateurs, et pour informer les autres équipes.

Les conflits d'intérêt, particulièrement en matière commerciale, peuvent aussi restreindre la divulgation des informations par une équipe. Le présent document ne fait pas de recommandation sur la façon de traiter de tels conflits.

Une équipe va normalement collecter des statistiques. Si des informations statistiques sont distribuées, la politique de rapport et de divulgation du modèle devrait le dire, et devrait décrire comment obtenir de telles statistiques.

3.4.3 Communication et authentification

On doit avoir une politique qui décrit les méthodes de communication sûre et vérifiable qu'on va utiliser. C'est nécessaire pour la communication entre les CSIRT et entre une CSIRT et sa clientèle. Le modèle devrait inclure des clés publiques ou des pointeurs sur elles, incluant des empreintes de clé, avec des lignes directrices sur la façon d'utiliser ces informations pour en vérifier l'authenticité et sur la façon de traiter les informations corrompues (par exemple où faire rapport de ce fait).

Pour l'instant, il est recommandé qu'au minimum chaque CSIRT ait (si possible) une clé PGP disponible. Une équipe peut aussi rendre d'autres mécanismes disponibles (par exemple, PEM, MOSS, S/MIME) selon ses besoins et ceux de sa clientèle. Noter cependant que les CSIRT et les usagers devraient être sensibles aux lois et règlements locaux. Certains pays ne permettent pas de chiffrement fort, ou appliquent des politiques spécifiques à l'utilisation des technologies de chiffrement. En plus des informations sur la sensibilité au chiffrement, chaque fois que possible, la correspondance devrait inclure les signatures numériques. (Prière de noter que dans la plupart des pays, la protection de l'authenticité à l'aide de signatures numériques n'est pas affectée par les règlements existants sur les chiffrements.)

Pour les communications par téléphone ou télécopie, une CSIRT peut conserver des données d'authentification secrètes pour les parties avec lesquelles elle va traiter, comme un mot ou phrase de passe sur lequel il y a eu accord. Évidemment, de telles clés secrètes ne doivent pas être publiées, bien que leur existence puisse l'être.

3.5 Services

Les services fournis par une CSIRT peuvent être grossièrement divisés en deux catégories : activités en temps réel directement en rapport avec la tâche principale de réponse aux incidents, et activités proactives non en temps réel de la tâche de réponse aux incidents. La seconde catégorie et une partie de la première catégorie consistent en services qui sont facultatifs au sens que toutes les CSIRT ne vont pas les offrir.

3.5.1 Réponse à un incident

La réponse à un incident comporte normalement la prise en compte des rapports qui arrivent sur les incidents ("Triage des incidents") et des suites qui leur sont données par les autres CSIRT, FAI et sites ("Coordination des incidents"). Une troisième gamme de services, aider un site local à récupérer d'un incident ("Résolution d'incident") est comprise dans les services normalement facultatifs, que toutes les CSIRT ne vont pas offrir.

3.5.1.1 Triage d’incidents

Le triage d'incident va normalement inclure :

- La prise en compte des rapports : l'interprétation des rapports d'incident qui arrivent, leur attribuer une priorité, et les mettre en rapport avec les incidents en cours et dégager des tendances.
- La vérification : aider à déterminer si un incident s'est réellement produit, et quelle est sa portée.

3.5.1.2 Coordination d'incident

La coordination d'incident inclut normalement :

- la catégorisation des informations : catégorisation des informations en rapport avec l'incident (fichiers de journalisation, informations de contact, etc.) par rapport à la politique de divulgation des informations.

- Notification de la coordination aux autres parties impliquées en fonction du besoin qu'elles ont d'en être informées, selon la politique de divulgation des informations.

3.5.1.3 Résolution d'incident

Habituellement supplémentaires ou facultatifs, les services de résolution d'incident incluent :
- l'assistance technique Cela peut inclure l'analyse des systèmes compromis.
- l'éradication Élimination de la cause d'un incident de sécurité (la vulnérabilité exploitée) et ses effets (par exemple, la poursuite de l'accès au système par l'intrus).
- récupération de l'incident Aide à la restauration des systèmes et services affectés à leur état d'avant l'incident.

3.5.2 Activités proactives

Habituellement supplémentaires ou facultatifs, les services proactifs peuvent inclure :
- la fourniture d'informations : cela peut inclure une archive des faiblesses connues, des remèdes ou de la résolution des problèmes passés, ou de listes de diffusion conseillées.
- des outils de sécurité : cela peut inclure des outils pour faire l'audit de la sécurité d'un site.
- éducation et formation.
- évaluation de produit.
- audit et consultation sur la sécurité d'un site.

3.6 Formulaires de rapport d'incident

L'"utilisation de formulaires de rapport rend plus simple aux utilisateurs et aux équipes de traiter les incidents. Le client peut préparer les réponses à diverses questions importantes avant de contacter effectivement l'équipe, et peut donc arriver bien préparé. L'équipe obtient en une seule fois toutes les informations nécessaires avec le premier rapport et peut travailler efficacement.

Selon les objectifs et services d'une CSIRT particulière, plusieurs formes peuvent être utilisées, par exemple un formulaire de rapport pour une nouvelle vulnérabilité peut être très différent du formulaire utilisé pour rapporter les incidents.

Le plus efficace est de fournir les formulaires dans les services d'information en ligne de l'équipe. Les pointeurs exacts sur ces services devraient être donnés dans le document de description de la CSIRT, avec les déclarations sur l'utilisation appropriée, et les lignes directrices sur la façon d'utiliser les formulaires. Si des adresses de messagerie électronique distinctes sont à utiliser pour les rapports fondés sur les formulaires, elles devraient être données à nouveau à cet endroit.

Un exemple d'un tel formulaire est celui qui est fourni par le Centre de coordination du CERT pour le rapport d'incident :
- https://www.cert.be/pro/report-incident

3.7 Déclinaison de responsabilité

Bien que le document de description d'une CSIRT ne constitue pas un contrat, on peut concevoir qu'une certaine responsabilité puisse résulter de ses descriptions de services et objets. L'inclusion d'une déclinaison de responsabilité la fin du modèle est donc recommandée et devrait avertir les usagers sur de possibles limitations.

Dans des situations où la version originale d'un document doit être traduite en une autre langue, la traduction devrait porter un déclinatoire de responsabilité et un pointeur sur l'original. Par exemple :
"Bien qu'on ait essayé de traduire avec soin le document original d'allemand en anglais, on ne peut être certain que les deux documents expriment les mêmes choses avec le même niveau de détail et d'exactitude. Dans tous les cas, lorsque il y a une différence entre les deux versions, c'est la version allemande qui prévaut".

L'utilisation d'une protection par des déclinatoires de responsabilité est affectée par les lois et règlements locaux, dont chaque CSIRT devrait être bien informée. Dans le doute, la CSIRT devrait vérifier avec un juriste.

Appendice A Glossaire des termes

Ce glossaire définit les termes utilisés pour décrire les incidents de sécurité et les équipes de réponse aux incidents de sécurité informatique. Il ne contient qu'un nombre limité de termes. Pour d'autres définitions prière de se référer à d'autres sources, par exemple, le glossaire des utilisateurs de l'Internet [RFC1983].

Clientèle : implicite dans l'objet d'une équipe de réponse aux incidents de sécurité informatique est l'existence d'une clientèle. C'est le groupe d'utilisateurs, sites, réseaux ou organisations servis par l'équipe. L'équipe doit être reconnue par sa clientèle pour être efficace.

Incident de sécurité : pour les besoins du présent document, ce terme est synonyme d'incident de sécurité informatique : tout événement contraire qui compromet un aspect de la sécurité de l'ordinateur ou du réseau. La définition d'un incident peut varier selon les organisations, mais les catégories suivantes sont au moins généralement applicables :
- perte de la confidentialité des informations.
- compromission de l'intégrité des informations.
- déni de service.
- mauvais usage des services, systèmes ou informations.
- dommage aux systèmes.

Ces catégories sont très générales. Par exemple le remplacement d'un programme utilitaire du système par un cheval de Troie est un exemple de 'compromission de l'intégrité', et la réussite d'une attaque contre un mot de passe est un exemple de 'perte de confidentialité'. Les attaques, même quand elles ont échoué à cause d'une protection appropriée, peuvent être considérées comme des incidents.

Dans la définition d'un incident est utilisé le mot 'compromis'. Parfois, un administrateur peut seulement 'suspecter' un incident. Durant la réponse, il doit être établi si un incident s'est réellement produit ou non.

Équipe de réponse aux incidents de sécurité informatique : sur la base de deux des définitions données ci-dessus, une CSIRT est une équipe qui coordonne et prend en charge la réponse aux incidents de sécurité qui impliquent des sites au sein d'un domaine défini.

Pour être considérée comme une CSIRT, une équipe doit :
- fournir un canal (sûr) pour recevoir les rapports sur les incidents suspectés,
- fournir assistance aux membres de son domaine pour le traitement de ces incidents,
- disséminer les informations relatives aux incidents à son domaine et aux autre parties impliquées.

Noter qu'on ne se réfère pas ici aux autres organismes d'application de la loi qui peuvent investiguer sur les crimes relatifs à l'informatique. Les membres d'une CSIRT n'ont pas besoin, bien sûr, d'avoir d'autres pouvoirs que ceux des citoyens ordinaires.

Fabricant *(Vendor)* : un 'fabricant' est toute entité qui produit une technologie de réseautage ou d'informatique, et est responsable du contenu technique de cette technologie. Parmi les exemples de 'technologie' on citera les matériels (ordinateurs portables, routeurs, commutateurs, etc.) et les logiciels (systèmes d'exploitation, systèmes de messagerie, etc.).

Noter que le fournisseur d'une technologie n'est pas nécessairement le 'fabricant' de cette technologie. Par exemple, un fournisseur d'accès Internet (FAI) peut fournir des routeurs à chacun de ses clients, mais le 'fabricant' est le constructeur, car le constructeur, plus que le FAI est l'entité responsable du contenu technique du routeur.

Vulnérabilité : une 'vulnérabilité' est une caractéristique d'un élément de technologie qui peut être exploitée pour perpétrer un incident de sécurité. Par exemple, si un programme permettait involontairement à des utilisateurs ordinaires d'exécuter des commandes arbitraires du système d'exploitation en mode privilégié, cette "caractéristique" serait une vulnérabilité.

Appendice B Questions annexes

Les questions importantes de la réponse aux incidents de sécurité au niveau d'un site sont contenues dans la [RFC2196], le guide de la sécurité des sites, produit par le groupe de travail SSH (*Site Security Handbook*). Ce document est mis à jour par le groupe de travail SSH et donne des recommandations sur les politiques et procédures locales, principalement en rapport avec la façon d'éviter les incidents de sécurité.

D'autres documents intéressants pour l'exposé sur les CSIRT et leurs tâches sont disponibles auprès du centre de coordination du CERT et de l'ENISA

- https://www.cert.org/incident-management/csirt-development/index.cfm

Une collection de documents du centre de coordination CERT sur le développement des CSIRT.
- http://www.enisa.europa.eu/activities/cert/support

Cette page contient des conseils pratiques qui visent à aider les états membres de l'Union européenne, mais aussi tout intéressé, à établir en douceur, et faire fonctionner des CERT / CSIRT.

Prière de se référer au fichier 01-README pour plus d'informations sur le contenu de ce répertoire.

On trouvera des documents particulièrement intéressants en relation avec ce document à :
- ftp://ftp.nic.surfnet.nl/surfnet/net-security/cert-nl/docs/reports/R-92-01
Ce rapport contient le cadre fonctionnel du CERT-NL, le CSIRT de SURFnet (opérateur réseau aux Pays-Bas).

- Pour les lecteurs intéressés par le fonctionnement de FIRST (Forum des équipes de réponse aux incidents de sécurité) ils trouveront plus d'informations à l'Appendice C.

- http://hightop.nrl.navy.mil/news/incident.html
Ce document permet d'accéder au Manuel de réponse aux incidents de NRL.

- http://www.cert.dfn.de/eng/team/kpk/certbib.html
Ce document contient une bibliographie commentée des matériaux, documents et fichiers disponibles sur le fonctionnement des CSIRT avec des liens sur nombre des éléments référencés.

- ftp://info.cert.org/incident_reporting_form
Ce formulaire de rapport d'incident est fourni par le centre de coordination CERT pour collecter les informations sur les incidents, et pour éviter les délais supplémentaires causés par le besoin de demander des informations détaillées supplémentaires au site qui fait rapport.

- http://www.cert.org/cert.faqintro.html
Collection de questions fréquemment posées au centre de coordination du CERT.

Appendice C Équipes de réponse aux incidents de sécurité informatique connues

Il y a aujourd'hui de nombreuses CSIRT différentes, mais il n'y a pas une ‚source unique pour faire la liste de toutes. La plupart des équipes majeures et établies depuis longtemps (la première CSIRT a été fondée en 1988) sont de nos jours membres de FIRST, le forum mondial des équipes de réponse aux incidents de sécurité. Au moment de cette rédaction, plus de 55 équipes sont membres (1 en Australie, 13 en Europe, toutes les autres en Amérique du nord). On trouvera les informations sur FIRST à :
- http://www.first.org/

La liste actuelle des membres est aussi disponible, avec les informations de contact pertinentes et des information supplémentaires fournies par chaque équipe :

- http://www.first.org/team-info/

Pour les CSIRT qui veulent devenir membres de ce forum (prière de noter qu'une équipe doit être parrainée par une équipe qui est déjà membre à part entière de FIRST) le fichier suivant contient plus d'informations :

- http://www.first.org/about/op_frame.html

Le cadre du fonctionnement de FIRST.
- http://www.first.org/docs/newmem.html

Lignes directrices pour les équipes qui veulent devenir membres de FIRST.

Beaucoup des équipes européennes, sans considération de leur appartenance à FIRST, sont énumérées par pays sur une page tenue par le service Trusted Introducer (TI) :
- http://www.trusted-introducer.org/directory/index.html

Pour savoir quelles sont les équipes existantes convenables pour les besoins de chacun, il est souvent utile de demander aux équipes connues ou à un fournisseur d'accès Internet quel est le "bon" contact.

Appendice D Grandes lignes d'un gabarit de CSIRT

Ces grandes lignes résument sous forme de points les questions traitées dans le présent document, et c'est le gabarit recommandé pour un document de description de CSIRT. Sa structure est conçue pour faciliter la communication des politiques, procédures et autres informations pertinentes d'une CSIRT à son domaine de compétence et aux organisations extérieures, telles que les autres CSIRT. Un exemple 'rempli' de ce gabarit est donné à l'Appendice E.

1. Informations sur le document
1.1 Date de dernière mise à jour
1.2 Liste de distribution des notifications
1.3 Endroits où on peut trouver le document

2. Informations de contact
2.1 Nom de l'équipe
2.2 Adresse
2.3 Fuseau horaire
2.4 Numéro de téléphone
2.5 Numéro de télécopie
2.6 Autres numéros de télécommunications
2.7 Adresse de messagerie électronique
2.8 Informations de clés publiques et de chiffrement
2.9 Membres de l'équipe
2.10 Autres informations
2.11 Points de contact client

3. Mandat
3.1 Déclaration de mission
3.2 Domaine d'action
3.3 Parrainage et/ou affiliation
3.4 Autorité

4. Politiques
4.1 Types d'incidents et niveau de prise en charge
4.2 Coopération, interaction et divulgation d'informations
4.3 Communication et authentification

5. Services
5.1 Réponse aux incidents
5.1.1. Tri des incidents
5.1.2. Coordination d'incident
5.1.3. Résolution d'incident
5.2 Activités proactives

6. Formulaires de rapport d'incident

7. Déclinatoire de responsabilité

Appendice E Exemple de gabarit 'rempli' pour une CSIRT

Voici un exemple de gabarit rempli d'une CSIRT fictive nommée XYZ-CSIRT. Ce texte n'est destiné qu'à des fins d'illustration et ne constitue en aucun cas un aval par le groupe de travail ou l'IETF d'un ensemble particulier de procédures ou de politiques. Bien que les CSIRT soient encouragées à utiliser tout ou partie de ce texte si elles le souhaitent, une telle utilisation n'est, bien sûr, ni obligatoire, ni appropriée dans la plupart des cas.

Description de CSIRT pour XYZ-CERT

1. Sur ce document
1.1 Date de dernière mise à jour
Cette version 1.01 a été publiée le 31/03/1997.

1.2 Liste de distribution des notifications
Les notifications de mises à jour sont soumises à notre liste de diffusion à <xyz-cert-info@xyz-univ.ca>. Les demandes d'abonnement à cette liste devraient être envoyées au gestionnaire à <xyz-cert-info-request@xyz-univ.ca> ; le corps du message devrait contenir le mot "abonner". Envoyer le mot "aide" à la place si vous ne savez pas comment utiliser un gestionnaire de liste. Cette liste de diffusion est soumise à un contrôle.

1.3 Sites où ce document peut être trouvé
La version actuelle de ce document de description de CSIRT est disponible sur le site XYZ-CERT WWW ; son URL est http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.txt
Une version française de ce document est également disponible :
http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.txt
Assurez vous que vous utilisez la dernière version.

1.4 Authentification de ce document
Les deux versions anglaise et française de ce document ont été signées avec la clé PGP de XYZ-CERT. Les signatures sont aussi sur notre site de la Toile sous :
http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.asc
http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.asc

2 Informations de contact
2.1 Nom de l'équipe
"XYZ-CERT" : Équipe de réponse aux urgences informatiques de l'Université XYZ.

2.2 Adresse
XYZ-CERT
Université XYZ, Département des Services Informatiques
12345 Rue Principale
UniversityTown, Quebec
Canada H0H 0H0

2.3 Zone horaire
Canada/Est (GMT-0500, et GMT-0400 d'avril à octobre)

2.4 Numéro de téléphone
+1 234 567 7890 (demander le XYZ-CERT)

2.5 Numéro de télécopie
+1 234 567 7899 (ce N'EST PAS une télécopie sécurisée)

2.6 Autres moyens de télécommunications
Non disponible.

2.7 Adresse de messagerie électronique
<xyz-cert@xyz-univ.ca> C'est un alias qui relaye les messages aux personnes en charge de XYZ-CERT.

2.8 Clés publiques et autres informations de chiffrement
Le XYZ-CERT a une clé PGP, dont l'identifiant de clé est 12345678 et dont l'empreinte est
11 22 33 44 55 66 77 88 88 77 66 55 44 33 22 11.
La clé et ses signatures se trouvent sur les serveurs de clés grand public usuels.

Comme PGP est encore une technologie relativement nouvelle à l'Université XYZ, cette clé a relativement peu de signatures ; des efforts sont en cours pour augmenter le nombre de liens à cette clé dans le "réseau de confiance" PGP. En attendant, comme la plupart de nos universités collègues du Québec ont au moins un membre de leur personnel qui connaît la coordinatrice Zoe Doe du XYZ-CERT, Zoe Doe a signé la clé XYZ-CERT, et sera heureuse de confirmer son empreinte et celle de sa propre clé à toute personne qui voudra la connaître, par téléphone ou en personne.

2.9 Membres de l'équipe
Zoe Doe des services informatiques est la coordinatrice XYZ-CERT. Les coordinateurs auxiliaires et les autres membres de l'équipe, ainsi que leurs domaines d'expertise et les informations de contact, figurent dans les pages de la Toile de XYZ-CERT à http://www.xyz-univ.ca/xyz-cert/teamlist.html

La gestion, les liaisons et la supervision sont assurées par Steve Tree, Directeur adjoint (services techniques) des services

informatiques.

2.10 Autres informations
Les informations générales sur le XYZ-CERT, ainsi que les liens avec les diverses ressources de sécurité recommandées se trouvent à http://www.xyz-univ.ca/xyz-cert/index.html

2.11 Points de contact client
La méthode préférée pour contacter le XYZ-CERT est via messagerie électronique à <xyz-cert@xyz-univ.ca> ; les messages envoyés à cette adresse vont "toucher" la personne responsable, ou être automatiquement transmis immédiatement à la personne de secours appropriée. Si vous avez besoin d'une assistance d'urgence, mettez "urgent" dans votre ligne d'objet.

Si il n'est pas possible (ou pas conseillé pour des raisons de sécurité) d'utiliser la messagerie électronique, le XYZ-CERT peut être joint par téléphone durant les heures de bureau normales. Les messages téléphoniques sont regardés moins souvent que les électroniques.

Les heures d'ouverture du XYZ-CERT se restreignent généralement aux heures de bureau normales (09:00-17:00 du lundi au vendredi, sauf jours fériés).

Si possible, lors de la soumission de votre rapport, utilisez le formulaire mentionné à la section 6.

3. Mandat
3.1 Déclaration de mission
L'objet du XYZ-CERT est, d'abord, d'assister les membres de la communauté de l'Université XYZ à mettre en œuvre des mesures proactives pour réduire les risques d'incidents de sécurité informatique, et ensuite, d'aider la communauté XYZ à répondre à de tels incidents lorsque ils surviennent.

3.2 Domaine d'action
Le domaine d'action de la XYZ-CERT est la communauté de l'Université XYZ, comme défini dans le contexte de la "politique de l'Université XYZ pour les facilités informatiques". Cette politique est disponible à http://www-compserv.xyz-univ.ca/policies/pcf.html

Prière cependant de noter que nonobstant ce qui précède, les services de XYZ-CERT ne seront fournis que pour les systèmes situés sur le site de l'Université.

3.3 Parrainage et/ou affiliation
Le XYZ-CERT est parrainé par le réseau de recherche canadien ACME. Il est affilié à diverses CSIRT d'université dans tout le Canada et les USA en tant que de besoin.

3.4 Autorité
Le XYZ-CERT fonctionne sous les auspices de, et avec l'autorité déléguée par, le département des services informatiques de l'Université XYZ. Pour d'autres informations sur le mandat et l'autorité du département des services informatiques, prière de se référer aux "Politiques de facilités informatiques" de l'Université XYZ, disponible à
http://www-compserv.xyz-univ.ca/policies/pcf.html

Le XYZ-CERT se doit de travailler en coopération avec les administrateurs et utilisateurs de systèmes de l'Université XYZ, et, dans la mesure du possible, d'éviter des relations d'autorité. Cependant, si les circonstances l'exigeaient, le XYZ-CERT fera appel aux services informatiques pour exercer son autorité, directe ou indirecte, en tant que de besoin. Tous les membres du XYZ-CERT sont membres de la CCSA (Comité des administrateurs de systèmes informatiques) et ont tous les pouvoirs et responsabilités alloués aux administrateurs de système par la Politique sur les facilités informatiques, ou sont membres de la direction de l'Université.

Les membres de la communauté de l'Université XYZ qui souhaitent faire appel des actions du XYZ-CERT devraient contacter le Directeur Adjoint (Services techniques) des services informatiques. Si ce recours ne leur donne pas satisfaction, la question peut être portée devant le Directeur des services informatiques (dans le cas de problèmes avec la politique existante) ou devant le Bureau des Droits et Responsabilités de l'Université XYZ (dans le cas d'erreurs ressenties dans l'application de la politique existante).

4. Politiques
4.1 Types d'incidents et niveau de prise en charge
Le XYZ-CERT est autorisé à traiter tous les types d'incidents de sécurité informatique qui surviennent, ou menacent de survenir, à l'Université XYZ.

Le niveau de prise en charge apporté par XYZ-CERT va varier selon le type et la sévérité de l'incident ou problème, le type de domaine, la taille de la communauté d'utilisateurs affectée, et les ressources du XYZ-CERT à ce moment, bien que dans tous les cas, une réponse sera faite dans les vingt quatre heures ouvrables. Les ressources seront allouées selon les priorités suivantes, indiquées en ordre décroissant :
- Menaces pour la sécurité physique des personnes.
- Attaques au niveau racine ou système sur tout système d'informations de gestion, ou toute partie de l'infrastructure de cœur de réseau.
- Attaque au niveau racine ou système contre toute grande machine du service public, multi-utilisateur ou dédiée.
- Compromission de comptes de service confidentiel ou installations logiciel en accès réservé, en particulier ceux utilisés pour les applications MIS contenant des données confidentielles, ou celles utilisées pour l'administration de système.
- Attaques de déni de service contre un des trois éléments ci-dessus.
- Tous les cas précédents sur d'autres sites, générés à partir de l'Université XYZ.
- Attaques à grande échelle de toute sorte, par exemple, attaques de reniflage, attaques IRC "d'ingénierie sociale", attaques de cassage de mot de passe.
- Menaces, harcèlement, et autres délits impliquant des comptes d'utilisateur individuel.
- Compromission des comptes d'utilisateur individuel sur des systèmes multi utilisateurs.
- Compromission de systèmes de bureau.
- Falsifications et fausses représentations, et autres violations de règles et règlements locaux en rapport avec la sécurité, par exemple, falsification de netnews et de messages électroniques, utilisation non autorisée de robots IRC.
- Déni de service sur des comptes d'utilisateur individuel, par exemple, bombardement de messages.

Les types d' incidents autres que ceux mentionnés ci-dessus recevront une priorité selon leur sévérité et extension apparente.

Noter qu'il ne sera pas apporté de soutien direct aux utilisateurs finaux ; ils sont supposés contacter leur administrateur système, l'administrateur réseau, ou leur chef de département pour l'assistance. Le XYZ-CERT apportera son soutien à ces personnes.

Bien que le XYZ-CERT comprenne qu'il existe une grande diversité du niveau d'expertise des administrateurs système à l'Université XYZ, et bien que le XYZ-CERT s'efforce de présenter les informations et son assistance au niveau approprié à chaque personne, le XYZ-CERT ne peut pas entraîner les administrateurs système à brûle pourpoint, et il ne peut pas effectuer la maintenance des systèmes en leur nom. Dans la plupart des cas, le XYZ-CERT fournira des pointeurs sur les informations nécessaires pour mettre en œuvre les mesures appropriées.

Le XYZ-CERT s'engage à tenir informée la communauté des administrateurs système de l'Université XYZ des vulnérabilités potentielles, et lorsque possible, à informer cette communauté de telles vulnérabilités avant qu'elles soient activement exploitées.

4.2 Coopération, interaction et divulgation des informations

Alors qu'il y a des restrictions légales et éthiques aux flux d'informations qui proviennent du XYZ-CERT, dont beaucoup sont mentionnées dans la politique de l'Université XYZ sur les facilités informatiques, et qui seront toutes respectées, le XYZ-CERT reconnaît qu'il se soumettra, et déclare son intention de contribuer à l'esprit de coopération qui a créé l'Internet. Donc, bien que les mesures appropriées soient prises pour protéger l'identité des membres de son domaine de compétence et des membres des sites du voisinage lorsque nécessaire, le XYZ-CERT partagera librement les informations lorsque cela aide les autres à résoudre ou prévenir les incidents de sécurité.

Dans les paragraphes qui suivent, "parties affectées" se réfère aux possesseurs légitimes, opérateurs, et usagers des facilités informatiques pertinentes. Cela ne se réfère pas aux utilisateurs non autorisés, y compris les utilisateurs par ailleurs autorisés qui font un usage non autorisé d'une facilité; de telle sorte que les intrus ne peuvent s'attendre à aucune confidentialité de la part du XYZ-CERT. Ils peuvent avoir ou non des droits légaux à la confidentialité ; de tels droits seront bien sûr respectés lorsque ils existent.

Les informations dont la divulgation est à considérer sont classées comme suit :
- Les informations d'utilisateur privé sont des informations sur des utilisateurs particuliers, ou dans certains cas, des applications particulières, qui doivent être considérées comme confidentielles pour des raisons légales, contractuelles, et/ou éthiques. Les informations d'utilisateur privé ne seront pas livrées sous une forme identifiable à l'extérieur du XYZ-CERT, sauf dans le cas ci-après. Si l'identité de l'usager est déguisée, l'information peut être livrée librement (par exemple pour donner un échantillon, un fichier .cshrc tel que modifié par un intrus, ou pour montrer une attaque d'ingénierie sociale particulière).

- Les informations sur les intrus sont similaires aux informations d'utilisateur privé, mais concernent les intrus.
  Bien que les informations sur les intrus, et en particulier les informations d'identification, ne soient pas révélées au public (sauf si cela devient une affaire portée à la connaissance du public, par exemple parce que des poursuites

criminelles sont engagées) elles seront échangées librement avec les administrateurs de système et les CSIRT qui traquent les auteurs d'un incident.

- Les informations de site privé sont des informations techniques sur des systèmes ou sites particuliers.
  Elles ne seront pas révélées sans la permission du site en question, sauf comme mentionné ci-dessous.

- Les informations de vulnérabilité dont des informations techniques sur les vulnérabilités ou les attaques, y compris fixes et contournements.
  Les informations de vulnérabilité seront révélées librement, bien que tous les efforts soient faits pour informer le fabricant concerné avant le grand public.

- Les informations embarrassantes incluent la déclaration qu'un incident s'est produit, et les informations sur son extension ou sévérité. Les informations embarrassantes peuvent concerner un site ou un utilisateur ou groupe d'utilisateurs particulier.
  Les informations embarrassantes ne seront pas révélées sans la permission du site ou des utilisateurs en question, sauf comme mentionné ci-dessous.

- Les informations statistiques sont des informations embarrassantes dont les informations d'identification ont été retirées.
  Les information statistiques seront divulguées à la discrétion du Département des services informatiques.

- Les informations de contact expliquent comment joindre les administrateurs système et les CSIRT.
  Les informations de contact seront divulguées librement, sauf lorsque la personne ou entité de contact a demandé que ce ne soit pas le cas, ou lorsque le XYZ-CERT a des raisons de croire que la dissémination de cette information ne serait pas appréciée.

Les receveurs potentiels des informations provenant du XYZ-CERT peuvent être classés comme suit :

- À cause de la nature de leurs responsabilités et des attentes de confidentialité qui en découlent, les membres de la direction de l'Université XYZ sont habilités à recevoir toute information nécessaire pour faciliter le traitement des incidents de sécurité informatique qui surviennent dans leurs juridictions.
- Les membres de l'Office des droits et responsabilités sont en droit de recevoir toute information qu'ils demandent concernant un incident de sécurité informatique ou une affaire qui s'y rapporte qui leur a été soumise pour résolution. Il en va de même pour le département de sécurité de XYZ, lorsque son assistance a été demandée dans une investigation, ou lorsque l'investigation a été conduite à sa demande.
- Les administrateurs système à l'Université XYZ qui sont membres de la CCSA sont aussi, en vertu de leurs responsabilités, dépositaires d'informations confidentielles. Cependant, sauf si ces personnes sont aussi membres du XYZ-CERT, ils ne recevront que les informations confidentielles qu'ils doivent avoir afin de les aider dans leurs investigations, ou afin de sécuriser leurs propres systèmes.
- Les utilisateurs de l'Université XYZ sont en droit de recevoir les informations qui relèvent de la sécurité de leurs propres comptes informatiques, même si cela signifie de révéler des "informations sur les intrusions", ou des "informations embarrassantes" sur un autre utilisateur. Par exemple, si le compte aaaa est cassé et si l'intrus attaque le compte bbbb, l'utilisateur bbbb est en droit de savoir que aaaa a été cassé, et comment a été exécutée l'attaque contre le compte bbbb. L'utilisateur bbbb est aussi en droit, si il le demande, d'avoir les informations sur le compte aaaa qui pourraient permettre à bbbb de mener des investigations sur l'attaque. Par exemple, si bbbb a été attaqué par quelqu'un connecté à distance à aaaa, on devrait dire à bbbb la provenance des connexions à aaaa, même si cette information serait d'ordinaire considérée comme appartenant en privé à aaaa. Les utilisateurs de l'Université de XYZ sont en droit d'avoir notification de l'éventuelle compromission de leur compte.
- La communauté de l'Université XYZ ne recevra aucune information réservée, sauf lorsque les parties affectées ont donné leur permission à la dissémination des informations. Les informations statistiques peuvent être mises à la disposition de la communauté XYZ générale. Il n'y a pas d'obligation de la part du XYZ-CERT de faire rapport des incidents à la communauté, bien qu'il puisse choisir de le faire ; en particulier, il est vraisemblable que le XYZ-CERT informera toutes les parties affectées de la façon dont elles ont été affectées, ou va encourager le site affecté à le faire.
- Le grand public ne recevra pas d'informations réservées. En fait, aucun effort particulier ne sera fait pour communiquer avec le grand public, bien que le XYZ-CERT reconnaisse que, pour ce qui le concerne, les informations mises à la disposition de la communauté de l'Université XYZ sont en effet mises à la disposition de l'ensemble de la communauté, et ajustera ces informations en conséquence.
- La communauté de la sécurité informatique sera traitée de la même façon que le grand public. Bien que les membres du XYZ-CERT puissent participer à des discussions au sein de la communauté de la sécurité informatique, telles que des groupes de nouvelles, des listes de diffusion (incluant la liste pleinement ouverte "bugtraq") et des conférences, ils traiteront de tels forums comme le grand public. Bien que des question techniques (incluant des vulnérabilités) puissent être discutées à tout niveau de détail, tous les exemples tirés de l'expérience de XYZ-CERT seront déguisés pour éviter d'identifier les parties affectées.
- La presse sera aussi considérée comme partie du grand public. Le XYZ-CERT n'interagira pas directement avec la

presse concernant les incidents de sécurité informatique, sauf pour l'orienter vers les informations déjà livrées au grand public. Si nécessaire, des informations seront fournies au département des relations publiques de l'Université XYZ, et au groupe Relations client du département des Services informatique. Toutes les questions en rapport avec les incidents seront renvoyées à ces deux organismes. Ceci n'affecte pas la capacité des membres du XYZ-CERT d'accorder des interviews sur les sujets généraux de la sécurité informatique ; en fait, ils sont encouragés à le faire, comme un service public de la communauté.

- Les autres sites et CSIRT, lorsque ils sont partenaires des investigations sur un incident de sécurité informatique, seront dans certains cas dépositaires d'informations confidentielles. Ceci n'arrivera que si la bonne foi du site étranger peut être vérifiée, et si les informations transmises se limitent à ce qui sera vraisemblablement utile à la résolution de l'incident. Un tel partage d'informations va probablement arriver dans le cas de sites bien connus de XYZ-CERT (par exemple, plusieurs autres université du Québec ont des relations de travail informelles mais bien établies avec l'Université XYZ sur de tels sujets).
  Pour les besoins de résolution d'un incident de sécurité, des informations d'utilisateur par ailleurs semi privées mais relativement anodines, telles que la provenance de connexions à des comptes d'utilisateur ne seront pas considérées comme étant très sensibles, et pourront être transmises à un site étranger sans précautions excessives. Les "informations sur les intrus" seront transmises librement aux autres administrateurs système et CSIRT. Les "informations embarrassantes" peuvent être transmises lorsque il y a des assurances raisonnables qu'elles vont rester confidentielles, et lorsque elles sont nécessaires pour résoudre un incident.
- Les fabricants seront considérés comme des CSIRT étrangères pour la plupart des cas. Le XYZ-CERT souhaite encourager les fabricants de toutes les sortes d'équipements de réseautage et de matériel informatique, de logiciels et de services à améliorer la sécurité de leurs produits. Pour aider à cela, une vulnérabilité découverte dans de tels produits fera l'objet d'un rapport au fabricant, avec tous les détails techniques nécessaires pour identifier et réparer le problème. Les détails d'identification ne seront pas donnés au fabricant sans la permission des parties affectées.
- Les officiers chargés de l'application de la loi recevront la pleine coopération du XYZ-CERT, incluant toute information qu'ils demandent pour poursuivre des investigations, conformément à la politique sur les facilités informatiques.

4.3 Communication et authentification

Vus les types d'informations que le XYZ-CERT va vraisemblablement traiter, le téléphone sera considéré suffisamment sûr pour être utilisé même non chiffré. La messagerie non chiffrée ne sera pas considérée particulièrement sûre, mais sera suffisante pour la transmission de données peu sensibles. Si il est nécessaire d'envoyer des données très sensibles par message électronique, PGP sera utilisé. Les transferts de fichiers sur le réseau seront considérés de la même façon que la messagerie électronique de ce point de vue : les données sensibles devraient être chiffrées pour la transmission.

Lorsque il est nécessaire d'établir la confiance, par exemple avant de s'appuyer sur des informations données au XYZ-CERT, ou avant de divulguer des informations confidentielles, l'identité et la bonne foi de l'autre partie seront vérifiées à un degré de confiance raisonnable. Au sein de l'Université XYZ, et avec les sites voisins connus, la référence à des personnes de confiance connues devrait suffire pour identifier quelqu'un. Autrement, les méthodes appropriées seront utilisées, comme une recherche des membres de FIRST, l'utilisation de WHOIS et autres informations enregistrées dans l'Internet, etc., ainsi que le rappel téléphonique ou le message électronique en retour, pour s'assurer que la partie n'est pas un imposteur. Les messages électroniques entrants dont les données doivent être de confiance seront vérifiées quant à l'origine personnelle, ou au moyen de signatures numériques (en particulier, PGP est pris en charge).

5. Services

5.1 Réponse aux incidents

Le XYZ-CERT assistera les administrateurs systèmes dans le traitement des aspects techniques et organisationnels des incidents. En particulier, il apportera son assistance ou ses avis par rapport aux aspects suivants de la gestion d'incident :

5.1.1 Triage des incidents

- Investiguer si un incident s'est bien produit.
- Déterminer l'étendue de l'incident.

5.1.2 Coordination des incidents

- Déterminer la cause initiale de l'incident (vulnérabilité exploitée).
- Faciliter le contact avec les autres sites qui pourraient être impliqués.
- Faciliter le contact avec le service de sécurité de l'Université XYZ et/ou les officiels appropriés pour l'application de la loi, si nécessaire.
- Faire rapport aux autres CSIRT.
- Composer les annonces aux usagers, si applicable.

5.1.3 Résolution des incidents

- Supprimer la vulnérabilité.
- Sécuriser le système à partir des effets de l'incident.
- Évaluer si certaines actions sont susceptibles de donner des résultats en proportion de leur coût et risque, en particulier

les actions visant à d'éventuelles poursuites ou actions disciplinaires : collecte des preuves après les faits, observation d'un incident en cours, établissement de pièges pour les intrus, etc.
- Collecter des preuves lorsque des poursuites criminelles, ou une action disciplinaire de l'Université, sont envisagées.

De plus, le XYZ-CERT collectera des statistiques concernant les incidents qui surviennent au sein de la communauté de l'Université XYZ, ou l'impliquent, et le notifiera à la communauté lorsque nécessaire pour aider à la protection contre les attaques connues.

Pour utiliser les services de réponse aux incidents de XYZ-CERT, prière d'envoyer un message selon les modalités du paragraphe 2.11 ci-dessus. Prière de se souvenir que la quantité d'assistance disponible va varier selon les paramètres décrits au paragraphe 4.1.

5.2 Activités proactives

Le XYZ-CERT coordonne et entretient les services suivants dans la mesure du possible selon les ressources :

Services d'information
- Liste des contacts de sécurité par département, administratifs et techniques. Ces listes seront disponibles au grand public, via les canaux communément disponibles comme la Toile mondiale et/ou les service des noms de domaine.
- Listes de diffusion pour informer les contacts de sécurité de nouvelles informations pertinentes pour leur environnement informatique. Ces listes ne seront disponibles qu'aux administrateurs système de l'Université XYZ.
- Répertoire des réparations fournies par les fabricants et autres en rapport avec la sécurité pour les divers systèmes d'exploitation. Ce répertoire sera disponible au grand public chaque fois que les restrictions de licence le permettent, et sera fourni via les canaux communément disponibles tels que la Toile mondiale et/ou ftp.
- Répertoire des outils et documentation de sécurité à l'usage des administrateurs système. Lorsque possible, des versions pré compilées prêtes à installer seront fournies. Elles seront fournies au grand public via www ou ftp comme ci-dessus.
- Service de "coupures de presse" pour les diverses ressources existantes, telles que les listes de diffusion majeures et les groupes de nouvelles. Les coupures résultantes seront mises à disposition sur la liste de diffusion restreinte ou sur le site de la Toile, selon leur sensibilité et leur urgence.

Services de formation
- Les membres du XYZ-CERT tiendront des séminaires périodiques sur les sujets en rapport avec la sécurité informatique ; ces séminaires seront ouverts aux administrateurs système de l'Université XYZ.

Services d'audit
- Service central de vérification d'intégrité de fichier pour machines Unix, et pour toutes les autres plateformes capables de fonctionner avec "tripwire".
- Allocation de niveaux de sécurité ; les machines et sous-réseaux de l'Université XYZ seront examinés et se verront allouer un niveau de sécurité. Ces informations de niveau de sécurité seront disponibles à la communauté de l'Université XYZ, pour faciliter l'établissement des privilèges d'accès appropriés. Cependant, les détails des analyses de sécurité resteront confidentiels, et ne seront disponibles qu'aux parties concernées.

Services d'archivage
- Un service central d'enregistrement pour les machines à capacité d'enregistrement à distance de style Unix. Les entrées d'enregistrement seront surveillées par un programme automatique d'analyse de journaux, et les événements ou tendances indicatives d'un problème potentiel de sécurité seront rapportés aux administrateurs système affectés.
- Les enregistrements des incidents de sécurité traités seront conservés. Bien que les enregistrements restent confidentiels, des rapports périodiques statistiques seront mis à la disposition de la communauté de l'Université XYZ.

Les descriptions détaillées des services ci-dessus, ainsi que les instructions pour se joindre aux listes de diffusion, les informations de téléchargement, ou la participation à certains services tels que les services centraux d'enregistrement et de vérification d'intégrité de fichier sont disponibles sur le site de la Toile de XYZ-CERT, conformément au paragraphe 2.10.

6. Formulaires de rapport d'incident

Aucun formulaire local n'a encore été développé pour faire rapport des incidents au XYZ-CERT. Si possible, prière d'utiliser le formulaire de rapport d'incident du centre de coordination CERT (Pittsburgh, PA). La version actuelle est disponible à : ftp://info.cert.org/incident_reporting_form

7. Déclinatoire de responsabilité

Bien que toutes les précaution soient prises dans la préparation des informations, notifications et alertes, XYZ-CERT ne porte aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultants de l'utilisation des informations contenues ici.

4. Remerciements

Les éditeurs remercient Anne Bennett de ses contributions et de ses corrections rédactionnelles. Merci aussi à Don Stikvoort pour son assistance dans la révision de la description des services de l'équipe de réponse aux incidents.

5. Références

[RFC2196] B. Fraser, "Manuel de la sécurité des sites", septembre 1997. (FYI0008) *(Information)*

[RFC1983] G. Malkin, "Glossaire des utilisateurs de l'Internet", FYI 18, août 1996.

6. Considérations pour la sécurité

Le présent document expose le fonctionnement des équipes de réponse aux incidents de sécurité informatique, et les interactions des équipes avec leur domaine d'intervention et avec les autres organisations. Il n'est donc pas directement concerné par la sécurité des protocoles, applications, ou systèmes réseau elle-même. Il n'est même pas concerné par les réponses et réactions particulière aux incidents de sécurité, mais seulement par la description appropriée des réponses fournies par les CSIRT.

Néanmoins, il est vital que les CSIRT elles-mêmes fonctionnent de façon sûre, ce qui signifie qu'elles doivent établir des canaux de communication sécurisés avec les autres équipes, et avec les membres de leur domaine d'application. Elles doivent aussi sécuriser leurs propres systèmes et infrastructures, pour protéger les intérêts de leur domaine et conserver la confidentialité de l'identité des victimes et rapporteurs des incidents de sécurité.

7. Adresse des auteurs

Nevil Brownlee
ITSS Technology Development
The University of Auckland
téléphone : +64 9 373 7599 x8941
mél : n.brownlee@auckland.ac.nz

Erik Guttman
Sun Microsystems, Inc.
Bahnstr. 2
74915 Waibstadt Germany
téléphone : +49 7263 911484
mél : Erik.Guttman@sun.com

8. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d’éditeur des RFC est actuellement fourni par la Internet Society.