Groupe de travail Réseau
Request for Comments : 2196
FYI: 8
RFC rendue obsolète : 1244
Catégorie : Information

B. Fraser, éditeur, SEI/CMU
septembre 1997

Traduction Claude Brière de L'Isle
juillet 2007

Manuel sur la sécurité des sites

Statut de ce mémoire
Le présent mémo fournit des informations pour la communauté de l'Internet. Il ne spécifie aucune norme Internet. La distribution du présent mémo n'est pas limitée.

Résumé
Ce manuel est un guide pour le développement des politiques et procédures de sécurité informatiques pour les sites qui ont des systèmes sur l'Internet. L'objet de ce manuel est de fournir une aide pratique aux administrateurs qui essayent de sécuriser leurs informations et services. Les sujets couverts incluent le contenu et la formation de la politique, une large gamme de sujets sur les systèmes techniques et la sécurité du réseau, et la réponse aux incidents de sécurité.

Table des matières

1 Introduction

Le présent document donne des lignes directrices aux administrateurs de système et de réseau sur la façon de traiter les questions de sécurité en rapport avec la communauté de l'Internet. Il s'établit sur les fondations posées par la RFC 1244 et est le travail collectif d'un certain nombre de contributeurs. Ces auteurs sont :
Jules P. Aronson (aronson@nlm.nih.gov), Nevil Brownlee (n.brownlee@auckland.ac.nz), Frank Byrum (byrum@norfolk.infi.net), Joao Nuno Ferreira (ferreira@rccn.net), Barbara Fraser (byf@cert.org), Steve Glass (glass@ftp.com), Erik Guttman (erik.guttman@eng.sun.com), Tom Killalea (tomk@nwnet.net), Klaus- Peter Kossakowski (kossakowski@cert.dfn.de), Lorna Leone (lorna@staff.singnet.com.sg), Edward.P.Lewis (Edward.P.Lewis.1@gsfc.nasa.gov), Gary Malkin (gmalkin@xylogics.com), Russ Mundy (mundy@tis.com), Philip J. Nesser (pjnesser@martigny.ai.mit.edu), et Michael S. Ramsey (msr@interpath.net).

En plus des principaux rédacteurs, un certain nombre de réviseurs on fourni des commentaires précieux. Ce sont : Eric Luiijf (luiijf@fel.tno.nl), Marijke Kaat (marijke.kaat@sec.nl), Ray Plzak (plzak@nic.mil) et Han Pronk (h.m.pronk@vka.nl).

Des remerciements particuliers vont à Joyce Reynolds, ISI, et Paul Holbrook, CICnet, pour leurs vues, leur initiative et leurs efforts pour la création de la première version de ce manuel. C'est le vœu sincère de tout le groupe de travail que la présente version soit aussi utile à la communauté que l'était la précédente.

1.1 Objet de ce travail

Le présent manuel est un guide pour l'établissement des politiques et procédures de sécurité des ordinateurs pour les sites qui ont des systèmes sur l'Internet (cependant, les informations fournies devraient aussi être utiles pour les sites non encore connectés à l'Internet). Ce guide fait la liste des questions et des facteurs qu'un site doit prendre en considération lors de l'établissement de sa propre politique. Il fait un certain nombre de recommandations et fait un exposé des domaines pertinents.

Ce guide est seulement un cadre pour l'établissement des politiques et procédures de sécurité. Pour avoir un ensemble effectif de politiques et de procédures, un site devra prendre de nombreuses décisions, obtenir des accords, puis communiquer et mettre en œuvre ces politiques.

1.2 Public visé

Le public visé par le présent document est celui des administrateurs de systèmes et de réseau, et les preneurs de décision (normalement "le gestionnaire médian") des sites. Pour faire court, nous utiliserons le terme "administrateur" tout au long du présent document pour désigner les administrateurs de systèmes et de réseau.

Le présent document n'est pas destiné aux programmeurs ou à ceux qui essayent de créer des programmes ou systèmes sécurisés. Le présent document est centré sur les politiques et les procédures qui doivent être en place pour prendre en charge les caractéristiques techniques de sécurité que peut mettre en œuvre un site.

Le principal public visé par ce travail est celui des sites qui sont membres de la communauté de l'Internet. Cependant, le présent document devrait être utile à tout site qui permet la communication avec d'autres sites. En tant que guide général des politiques de sécurité, le présent document peut aussi être utile aux sites de systèmes isolés.

1.3 Définitions

Pour les besoins du présent guide, un "site" est toute organisation qui possède des ordinateurs ou des ressources se rapportant au réseau. Ces ressources peuvent inclure des ordinateurs hôtes qu'utilisent des usagers, des routeurs, des serveurs de terminaux, des micro-ordinateurs ou autres appareils qui ont accès à l'Internet. Un site peut être un utilisateur final des services de l'Internet ou un fournisseur de services tel qu'un réseau de niveau moyen. Cependant, le présent guide est surtout tourné vers ces utilisateurs finaux des services de l'Internet. On suppose que le site a la capacité d'établir pour lui-même des politiques et des procédures avec le concours et le soutien de ceux qui possèdent réellement les ressources. On supposera que les sites qui sont dans de plus grandes organisations sauront quand ils

doivent consulter, collaborer, ou obtenir des recommandations de la part de la plus grande entité.

L'Internet est une collection de milliers de réseaux reliés par un ensemble commun de protocoles techniques qui rendent possibles à l'utilisateur d'un de ces réseaux de communiquer avec un des autres réseaux ou d'utiliser les services qui y sont localisés (FYI4, RFC 1594).

Le terme "administrateur" est utilisé pour parler de tous ces gens qui sont chargés du fonctionnement quotidien des ressources des systèmes et des réseaux. Ce peut être un certain nombre d'individus ou une organisation.

Le terme "administrateur de sécurité" est utilisé pour parler des gens qui sont responsables de la sécurité des informations et des technologies de l'information. Sur certains sites, cette fonction peut être combinée avec celle de l'administrateur (ci-dessus) ; sur d'autres, ce sera une position séparée.

Le terme "décisionnaire" se réfère aux personnes qui sur un site établissent ou approuvent la politique. Ce sont souvent (mais pas toujours) les gens qui possèdent les ressources.

1.4 Travaux voisins

Le groupe de travail du Manuel sur la sécurité des sites travaille sur un Guide de l'utilisateur pour la sécurité de l'Internet. Il donnera des conseils pratiques à l'utilisateur final pour l'aider à protéger ses informations et les ressources qu'elles utilisent.

1.5 Approche de base

Le présent guide a été écrit pour fournir des conseils de base pour le développement d'un plan de sécurité pour votre site. Une approche à suivre généralement acceptée est suggérée par Fites, et. al. [Fites 1989] et comporte les étapes suivantes :

(1) Identifier ce que vous essayez de protéger.
(2) Déterminer contre quoi vous essayez de le protéger.
(3) Déterminer la probabilité des menaces.
(4) Mettre en œuvre les mesures qui protègeront vos biens d'une manière économique.
(5) Revoir continuellement le processus et faire des améliorations chaque fois que vous trouvez des faiblesses.

La plus grande partie du présent document se concentre sur le point (4) ci-dessus, mais les autres étapes ne peuvent être évitées si un plan effectif doit être établi sur votre site. Un vieux truisme en matière de sécurité est que le coût de votre protection contre une menace devrait être inférieur au coût de la récupération si la menace est mise à exécution. On doit se rappeler que dans ce contexte, le coût inclut les pertes subies en argent réel, en réputation, en confiance, et autres mesures moins évidentes. Sans connaissance raisonnable de ce contre quoi vous vous protégez et de ce que sont vraisemblablement les menaces, suivre cette règle pourrait être difficile.

1.6 Évaluation du risque

1.6.1 Discussion générale

Une des raisons les plus importantes pour créer une politique de sécurité informatique est de s'assurer que les efforts déployés pour la sécurité donnent des résultats en rapport avec leurs coûts. Bien que cela puisse sembler évident, il est possible de se tromper lourdement quant à l'endroit où l'effort doit porter. Par exemple, il y a beaucoup de tapage sur les intrusions dans les systèmes informatiques, alors que les enquêtes sur la sécurité informatique montrent que pour la plupart des organisations, les pertes réelles provenant de l'"intérieur" sont bien plus grandes.

L'analyse de risque implique de déterminer ce qu'on veut protéger, contre quoi on veut le protéger, et comment le protéger. C'est le processus d'examen de tous les risques, puis le classement de ces risques par niveau de sévérité. Ce processus implique de prendre des décisions sur le coût de ce qu'on veut protéger. Comme indiqué ci-dessus, on ne devrait probablement pas dépenser plus pour protéger quelque chose que ce que ce quelque chose vaut réellement.

Le traitement complet de l'analyse de risque sort du domaine d'application du présent document. [Fites 1989] et [Pfleeger 1989] seraient une introduction sur ce sujet. Cependant, il y a deux éléments d'analyse de risque qui seront

brièvement traités dans les deux paragraphes suivants :
(1) Identifier les biens
(2) Identifier les menaces

Pour chaque bien, les buts globaux de la sécurité sont la disponibilité, la confidentialité, et l'intégrité. Chaque menace devrait être examinée en gardant toujours en mémoire la façon dont elle affecterait ces domaines.

1.6.2 Identifier les biens

Une étape de l'analyse de risque est l'identification de toutes les choses qu'il faut protéger. Certaines choses sont évidentes, comme les précieux secrets de fabrique, les brevets, et tous les différents éléments du matériel ; mais certains passent inaperçus, comme les personnes qui utilisent en fait les systèmes. Le point essentiel est de faire la liste de toutes les choses qui pourraient être affectées par un problème de sécurité.

Une liste des catégories est suggérée par Pfleeger [Pfleeger 1989] ; la liste suivante en est adaptée :
(1) Matériel : unités de traitement de commande, claviers, terminaux, stations de travail ; ordinateurs, imprimantes, unités de disques, lignes de communication, serveurs terminaux, routeurs.
(2) Logiciel : programmes source, programmes objets, fonctionnalités, programmes de diagnostic, systèmes d'exploitation, programmes de communication.
(3) Données : durant l'exécution, mémorisées en ligne, archivées hors ligne, sauvegardes, enregistrements d'audit, bases de données, en transit sur des supports de communication.
(4) Personnes : utilisateurs, administrateurs, personnels d'entretien du matériel.
(5) Documentation : sur les programmes, sur le matériel, sur les systèmes, procédures administratives locales.
(6) Fournitures : papier, formulaires, disques, supports magnétiques.

1.6.3 Identifier les menaces

Une fois identifiés les biens qui doivent être protégés, il est nécessaire d'identifier les menaces qui pèsent sur ces biens. Les menaces peuvent alors être examinées pour déterminer quel est le potentiel de perte. Il est utile de considérer de quelles menaces vous essayez de protéger vos biens. Les menaces classiques à prendre en compte sont les suivantes. En fonction de votre site, il peut y avoir des menaces spécifiques qui devraient être identifiées et traitées.
(1) Accès non autorisé aux ressources et/ou informations
(2) Divulgation d'information non intentionnelle et/ou non autorisée
(3) Déni de service.

2 Politiques de sécurité

Tout au long de ce document, il y aura de nombreuses références aux politiques.
Souvent, ces références incluront des recommandations de politiques spécifiques. Plutôt que de répéter des conseils sur la façon de créer et communiquer une telle politique, le lecteur devrait appliquer les avis présentés dans la présente section lors du développement de toute politique recommandée plus loin dans ce guide.

2.1 Qu'est ce qu'une politique de sécurité et pourquoi en avoir une ?

Les décisions que vous prenez (ou ne prenez pas) comme administrateur, en ce qui concerne la sécurité, déterminent en grande partie la sécurité ou l'insécurité de votre réseau, quelle quantité de fonctionnalités offrira votre réseau, et leur facilité d'utilisation. Cependant, vous ne pourrez jamais prendre de bonnes décisions sur la sécurité sans déterminer d'abord ce que sont pour vous les objectifs de la sécurité. Tant que vous n'avez pas déterminé ce que sont vos objectifs de sécurité, vous ne pouvez utiliser effectivement aucun ensemble d'outils de sécurité tout simplement parce que vous ne savez pas que rechercher et quelles restrictions imposer.

Par exemple, vos objectifs seront probablement très différent des objectifs d'un vendeur de produits. Les vendeurs essayent de rendre la configuration et le fonctionnement de leurs produits aussi simples que possible, ce qui implique que les configurations par défaut seront souvent aussi ouvertes (c'est-à-dire, insécurisées) que possible. Alors que cela rend plus facile l'installation de nouveaux produits, cela ouvre l'accès à ces systèmes, et à d'autres systèmes à travers eux, ouverts à tout utilisateur qui traîne par là.

Vos objectifs seront largement déterminés par les compromis clés suivants :

(1) Services offerts contre sécurité fournie – Chaque service offert aux utilisateurs porte ses propres risques de sécurité. Pour certains services, les risques dépassent les bénéfices du service et l'administrateur peut choisir d'éliminer le service plutôt que d'essayer de le sécuriser.

(2) Facilité d'utilisation contre sécurité - Le système le plus facile à utiliser permettrait l'accès à tout utilisateur et n'exigerait aucun mot de passe ; c'est-à-dire qu'il n'y aurait pas de sécurité. Exiger un mot de passe rend le système un peu moins commode, mais plus sûr. Exiger des mots de passe à usage unique générés par un automate rend le système encore plus difficile à utiliser, mais beaucoup plus sûr.

(3) Coût de la sécurité contre risque de pertes – Il y de nombreux coûts différents pour la sécurité : monétaires (c'est-à-dire, le coût de l'achat des matériels et logiciels de sécurité comme des pare-feu et des générateurs de mots de passe à usage unique), les performances (c'est-à-dire que le chiffrement et le déchiffrement prennent du temps), et la facilité d'utilisation (comme mentionné précédemment). Il y a aussi de nombreux niveaux de risque : perte de confidentialité (c'est-à-dire, la lecture d'informations par des individus non autorisés), perte de données (c'est-à-dire, corruption ou écrasement des informations), et la perte de service (par exemple, le remplissage de l'espace de mémorisation des données, l'utilisation de ressources de calcul, et le refus de l'accès réseau). Chaque type de coût doit être pondéré par chaque type de perte.

Vos objectifs devraient être communiqués à tous les utilisateurs, personnels d'exploitation et gestionnaires à travers un ensemble de règles de sécurité, appelées une "politique de sécurité." On utilise ce terme, plutôt que "politique de sécurité informatique" dans la mesure où le domaine d'application inclut tous les types de technologies de l'information et les informations mémorisées et manipulées par la technologie.

2.1.1 Définition d'une politique de sécurité

Une politique de sécurité est une déclaration formelle des règles auxquelles les gens à qui on donne accès aux biens technologiques et d'informations d'une organisation doivent se soumettre.

2.1.2 Objet d'une politique de sécurité

Le principal objet d'une politique de sécurité est d'informer les utilisateurs, le personnel et les gestionnaires de leur obligation impérative de protéger les biens technologiques et informationnels. La politique devrait spécifier les mécanismes par lesquels ces exigences doivent être satisfaites. Un autre objet est de fournir la base sur laquelle acquérir, configurer et analyser la conformité des systèmes et réseaux informatiques à cette politique. Et donc essayer d'utiliser un ensemble d'outils de sécurité en l'absence d'une politique de sécurité implicite est absurde.

Une politique d'utilisation appropriée (AUP, *Appropriate Use Policy*) peut aussi faire partie d'une politique de sécurité. On doit souligner ce que les utilisateurs doivent faire et ne pas faire sur les divers composants du système, y compris le type de trafic permis sur les réseaux. La AUP devrait être aussi explicite que possible pour éviter les ambiguïtés ou les incompréhensions. Par exemple, une AUP peut faire la liste de tous les groupes USENET interdits. (Note : politique d'utilisation appropriée se réfère à la politique d'utilisation acceptable par certains sites.)

2.1.3 Qui devrait être impliqué dans la formation d'une politique ?

Pour qu'une politique de sécurité soit appropriée et effective, il est nécessaire d'avoir l'approbation et le soutien de tous les niveaux d'employés au sein de l'organisation. Il est particulièrement important que les gestionnaires de haut niveau soutiennent pleinement le processus de politique de sécurité, sinon il y a peu de chances qu'elle ait l'impact prévu. Une liste des individus qui devraient être impliqués dans la création et la révision des documents de politique de sécurité figure ci-après :

(1) administrateur de la sécurité du site
(2) personnel technique des technologies de l'information (par exemple, personnel du centre informatique)
(3) administrateurs des grands groupes d'utilisateurs au sein de l'organisation (par exemple, divisions d'affaires, département d'informatique d'une université, etc.)
(4) équipe de réponse aux incidents de sécurité
(5) représentants des groupes d'utilisateurs affectés par la politique de sécurité
(6) gestionnaires responsables
(7) conseiller juridique (le cas échéant)

La liste ci-dessus est représentative de nombreuses organisations, mais n'est pas nécessairement complète. L'idée est d'avoir une représentation des actionnaires clés, des dirigeants qui ont une autorité budgétaire et politique, des personnels techniques qui savent ce qui peut et ne peut pas être pris en charge, et du conseiller juridique qui connaît les ramifications légales des divers choix politiques. Dans certains organismes, il peut être approprié d'inclure le personnel d'audit EDP. Il est important d'impliquer ce groupe si on veut provoquer le maximum d'adhésion aux déclarations de politique qui en résultent. Il est aussi pertinent de mentionner que le rôle du conseiller juridique variera selon les pays.

2.2 Qu'est-ce qui fait une bonne politique de sécurité ?

Les caractéristiques d'une bonne politique de sécurité sont :

(1) Il doit être possible de la mettre en œuvre à travers les procédures d'administration du système, en publiant les lignes directrices d'utilisation acceptable, ou autres méthodes appropriées.
(2) Elle doit être mise en application avec les outils de sécurité, là où c'est approprié, et avec des sanctions, lorsque une prévention réelle n'est pas techniquement faisable.
(3) Elle doit clairement définir les domaines de responsabilité des utilisateurs, des administrateurs, et des gestionnaires.

Les composants d'une bonne politique de sécurité incluent :

(1) Des lignes directrices d'acquisition de technologies informatiques qui spécifient les caractéristiques exigées, ou préférées, de sécurité. Elles devraient s'ajouter aux politiques et lignes directrices d'acquisition existantes.
(2) Une politique de confidentialité qui définisse des attentes raisonnables de confidentialité concernant des questions telles que la surveillance de la messagerie électronique, l'enregistrement des clés et l'accès aux fichiers d'utilisateur.
(3) Une politique d'accès qui définisse les droits et privilèges d'accès pour protéger les biens contre la perte ou la divulgation en spécifiant des lignes directrices d'utilisation acceptables pour les utilisateurs, le personnel d'exploitation et les gestionnaires. Elle devrait fournir des lignes directrices pour les connections externes, les communications de données, les appareils qui se connectent à un réseau, et l'ajout de nouveaux logiciels aux systèmes. Elle devrait aussi spécifier tous les messages de notification nécessaires (par exemple, les messages de connexion devraient fournir des avertissements quant à l'usage autorisé et la surveillance, et ne pas dire simplement "Bienvenue").
(4) Une politique de comptabilité qui définisse les responsabilités des utilisateurs, du personnel d'exploitation et des gestionnaires. Elle devrait spécifier des capacités d'audit, et fournir des lignes directrices pour le traitement des incidents (c'est-à-dire, que faire et qui contacter si une possible intrusion est détectée).
(5) Une politique d'authentification qui établisse la confiance au moyen d'une politique effective de mots de passe, et en établissant des lignes directrices pour l'authentification de localisations distantes et l'utilisation d'appareils d'authentification (par exemple, des mots de passe à utilisation unique et les appareils qui les génèrent).
(6) Une déclaration de disponibilité qui fonde les attentes des utilisateurs sur la disponibilité des ressources. Elle devrait traiter des questions de redondance et de récupération, ainsi que la spécification des heures de fonctionnement et des périodes d'arrêt pour la maintenance. Elle devrait aussi inclure des informations sur les contacts pour le système de rapport et les défaillances du réseau.
(7) Une politique du système de technologies de l'information et de la maintenance du réseau qui décrive comment les gens de la maintenance à la fois interne et externe sont autorisés à traiter la technologie et à y accéder. Un sujet important à traiter ici est la question de savoir si la maintenance à distance est admise et comment un tel accès est commandé. Un autre domaine à considérer ici est le recours à des ressources externes et sa gestion.
(8) Une politique de rapport des violations qui indique quels types de violations (par exemple, de la confidentialité et de la sécurité, internes et externes) doivent être rapportés et à qui sont faits les rapports. Une atmosphère non menaçante et la possibilité de rapports anonymes auront pour résultat une plus grande probabilité de rapporter une violation si elle est détectée.
(9) Des informations d'assistance qui fournissent aux utilisateurs, personnels, et gestionnaires, des informations de contacts pour chaque type de violation de politique ; des lignes directrices sur la façon de traiter les enquêtes extérieures sur un incident de sécurité, ou des informations qui pourraient être considérées comme confidentielles ou protégées, et des références croisées entre les procédures de sécurité et les informations qui s'y rapportent, comme les politiques d'entreprise et les lois et réglementations gouvernementales.

Il peut y avoir des exigences réglementaires qui affectent certains aspects de votre politique de sécurité (par exemple, la surveillance des lignes). Les créateurs de la politique de sécurité devraient prendre en considération la recherche d'une assistance juridique pour la création de la politique. Au minimum, la politique devrait être revue par le conseiller juridique.

Une fois votre politique de sécurité établie, elle devrait être communiquée clairement aux utilisateurs, au personnel et aux gestionnaires. Une partie importante du processus est d'avoir une déclaration signée de tout le personnel indiquant qu'ils ont lu, compris et accepté de se soumettre à la politique. Finalement, votre politique devrait être révisée régulièrement pour voir si elle prend en charge avec succès vos besoins de sécurité.

2.3 Garder une politique souple

Pour qu'une politique de sécurité soit viable sur le long terme, elle doit avoir une certaine souplesse, fondée sur un concept de sécurité architecturale. Une politique de sécurité devrait être largement indépendante de situations de matériel et de logiciels spécifiques (car les systèmes spécifiques tendent à être remplacés ou déplacés du jour au lendemain). Les mécanismes de mise à jour de la politique devraient être clairement énoncés. Cela inclut le processus, les gens impliqués, et les gens qui doivent approuver les changements.

Il est aussi important de reconnaître qu'il y a des exceptions à toute règle. Chaque fois que possible, la politique devrait énoncer les exceptions à la politique générale. Par exemple, dans quelles conditions un administrateur de système est-il autorisé à entrer dans un fichier d'utilisateur. Il peut aussi y avoir des cas où plusieurs utilisateurs auront accès au même identifiant d'utilisateur. Par exemple, sur des systèmes avec un utilisateur "racine", plusieurs administrateurs de système peuvent connaître le mot de passe et utiliser le compte racine.

Une autre considération est appelée le "Syndrome du camion poubelle". Cela se réfère à ce qui arriverait à un site si une personne clé était soudain indisponible pour sa fonction (par exemple, était soudainement malade ou quittait brusquement la compagnie). Alors que la plus grande sécurité réside dans le minimum de dissémination de l'information, le risque de perte d'informations critiques augmente lorsque ces informations ne sont pas partagées. Il est important de déterminer l'équilibre approprié pour votre site.

3 Architecture

3.1 Objectifs

3.1.1 Des plans de sécurité complètement définis

Tous les sites devraient définir un plan de sécurité complet. Ce plan devrait être à un plus haut niveau que les politiques spécifiques discutées à la section 2, et il devrait être constitué comme un cadre de travail de larges lignes directrices dans lesquelles s'inscrivent les politiques spécifiques.

Il est important que ce cadre de travail soit en place de telle sorte que les politiques individuelles puissent être cohérentes avec l'architecture globale de sécurité du site. Par exemple, avoir une politique forte en ce qui concerne l'accès Internet et avoir des restrictions faibles sur l'utilisation de modems est incohérent avec une philosophie globale de fortes restrictions de sécurité sur l'accès externe.

Un plan de sécurité devrait définir : la liste des services réseau qui seront fournis ; quels domaines de l'organisation fourniront les services ; qui aura accès à ces services ; comment l'accès sera fourni ; qui administrera ces services ; etc.

Le plan devrait aussi traiter de la façon de régler les incidents. La section 5 fournit un exposé détaillé de cette question, mais il est important que chaque site définisse des classes d'incidents et leurs réponses correspondantes. Par exemple, les sites avec un pare-feu devraient fixer un seuil sur le nombre de tentatives de déjouer le pare-feu avant de déclancher une réponse. Des niveaux d'escalade devraient être définis à la fois pour les attaques et les réponses. Les sites sans pare-feu auront à déterminer si une seule tentative de connexion à un hôte constitue un incident. Qu'en est-il d'un balayage systématique des systèmes ?

Pour les sites connectés à l'Internet, le grossissement d'incidents de sécurité rampants de supports en rapport avec l'Internet peut masquer un problème de sécurité interne (potentiellement) plus sérieux. De même, des compagnies qui n'ont jamais été connectées à l'Internet peuvent avoir des politiques internes bien définies, mais échouer à fixer de façon adéquate une politique de connexion externe.

3.1.2 Séparation des services

Il y a de nombreux services qu'un site peut souhaiter fournir à ses utilisateurs, dont certains peuvent être externes. Il y a diverses raisons de sécurité pour essayer d'isoler des services sur des ordinateurs hôtes dédiés. Il y a aussi des raisons de performance dans la plupart des cas, mais un exposé détaillé de cette question sort du domaine d'application du présent document.

Les services qu'un site peut fournir vont, dans la plupart des cas, avoir différents niveaux de besoin d'accès et de modèle de confiance. Les services qui sont essentiels à la sécurité ou au fonctionnement harmonieux d'un site feraient mieux d'être placés sur une machine dédiée avec un accès très limité (voir au paragraphe 3.1.3 le modèle "Tout refuser"), plutôt que sur une machine qui fournit un service (ou des services) qui ont traditionnellement été moins sécurisés, ou exigent une plus grande accessibilité à des utilisateurs qui pourraient accidentellement mettre en péril la sécurité.

Il est aussi important de distinguer entre les hôtes qui opèrent au sein de différents modèles de confiance (par exemple, tous les hôtes à l'intérieur d'un pare-feu et tout hôte sur un réseau exposé).

Certains des services qui devraient être examinés pour une séparation potentielle sont soulignés au paragraphe 3.2.3. Il est important de se souvenir que la sécurité n'est pas plus forte que le maillon le plus faible de la chaîne. Plusieurs des intrusions les plus médiatisées de ces dernières années l'ont été à travers l'exploitation de faiblesses des systèmes de messagerie électronique. Les intrus n'essayaient pas de voler de la messagerie électronique, mais ils ont utilisé les faiblesses de ce service pour obtenir l'accès à d'autres systèmes.

Si possible, chaque service devrait fonctionner sur une machine différente dont la seule tâche serait de fournir un service spécifique. Cela aide à isoler les intrus et limite les dommages potentiels.

3.1.3 Tout refuser/ Tout permettre

Deux philosophies sous-jacentes diamétralement opposées peuvent être adoptées pour définir un plan de sécurité. Les deux alternatives sont des modèles légitimes, et le choix entre elles dépendra du site et de ses besoins de sécurité.

La première option est de fermer tous les services puis de les activer au cas par cas au fur et à mesure des besoins. Cela peut être fait au niveau de l'hôte ou du réseau selon ce qui est approprié. Ce modèle, qu'on appellera ci-après le modèle "Tout refuser", est généralement plus sûr que l'autre modèle décrit au paragraphe suivant. Plus de travail est nécessaire pour mettre en œuvre avec succès une configuration "tout refuser" ainsi qu'une meilleure compréhension des services. Ne permettre que les services connus donne une meilleure analyse d'un service/protocole particulier et la conception d'un mécanisme de sécurité conforme au niveau de sécurité du site.

L'autre modèle, qu'on appellera ci-après le modèle "Tout permettre", est plus facile à mettre en œuvre, mais est généralement moins sûr que le modèle "Tout refuser". Simplement ouvrir tous les services, normalement par défaut au niveau de l'hôte, et permettre à tous les protocoles de traverser les frontières des réseaux, normalement par défaut au niveau du routeur. Comme les trous dans la sécurité deviennent apparents, ils sont interdits ou bouchés au niveau de l'hôte ou du réseau.

Chacun de ces modèles peut être appliqué à différentes portions du site, selon les exigences fonctionnelles, les contrôles administratifs, la politique du site, etc. Par exemple, la politique peut être d'utiliser le modèle "Tout permettre" lors de l'établissement de stations de travail d'utilisation générale, mais d'adopter un modèle "Tout refuser" lors de l'établissement de serveurs d'informations, comme concentrateur-répartiteur de messagerie électronique. De même, une politique de "Tout permettre" peut être adoptée pour le trafic entre des LAN internes au site, mais une politique "Tout refuser" peut être adoptée entre le site et l'Internet.

Il faut faire attention si on mélange les philosophies comme dans les exemples ci-dessus. De nombreux sites adoptent la théorie de la coquille dure "craquante" et d'un doux centre "mou". Ils souhaitent payer le prix de la sécurité pour leur trafic externe et exigent de fortes mesures de sécurité, mais ils ne veulent pas ou ne peuvent pas fournir en interne une protection similaire. Cela fonctionne tant que les défenses extérieures ne sont pas débordées et que les utilisateurs internes sont de confiance. Une fois que la coquille extérieure (le pare-feu) est franchi, subvertir le réseau interne est trivial.

3.1.4 Identifier les besoins réels des services

Une grande variété de services peut être fournie, à la fois en interne et sur l'Internet. La gestion de la sécurité est, au sens large, la gestion des accès aux services internes au site et la gestion de la façon dont les utilisateurs internes accèdent aux informations sur les sites distants.

Les services tendent à déferler comme des vagues sur l'Internet. Au fil des ans , de nombreux sites ont établi des serveurs FTP anonymes, des serveurs gopher, des serveurs wais, des serveurs WWW, etc. à mesure qu'ils sont connus, mais pas particulièrement nécessaires, sur tous les sites. Évaluez tous les nouveaux services qui sont établis avec une attitude sceptique pour déterminer si ils sont réellement nécessaires ou si ce sont juste la mode en cours sur l'Internet.

Gardez en mémoire que la complexité de la sécurité peut croître de façon exponentielle avec le nombre de services fournis. Les routeurs de filtrage doivent être modifiés pour prendre en charge les nouveaux protocoles. Certains protocoles sont par nature difficiles à filtrer en toute sécurité (par exemple, les services RPC et UDP), et ils fournissent donc plus d'entrées sur le réseau interne. Les services fournis sur la même machine peuvent interagir de façon catastrophique. Par exemple, permettre du FTP anonyme sur la même machine que le serveur WWW peut permettre à un intrus de placer un fichier dans la zone du FTP anonyme qui amène le serveur HTTP à l'exécuter.

3.2 Configuration de service et de réseau

3.2.1 Protéger l'infrastructure

De nombreux administrateurs de réseau vont très loin pour protéger les hôtes sur leurs réseaux. Peu d'administrateurs font l'effort de protéger les réseaux eux-mêmes. Il y a une certaine raison à cela. Par exemple, il est beaucoup plus facile de protéger un hôte qu'un réseau. Aussi, les intrus vont plutôt chercher des données sur les hôtes ; causer des dommages au réseau ne servirait pas leurs fins. Ceci dit, il y a quand même des raisons pour protéger les réseaux. Par exemple, un intrus peut détourner du trafic réseau à travers un hôte externe afin d'en examiner les données (c'est-à-dire, pour rechercher des mots de passe). Aussi, l'infrastructure inclut plus que les réseaux et les routeurs qui les interconnectent. L'infrastructure inclut aussi la gestion du réseau (par exemple, SNMP), des services (par exemple, DNS, NFS, NTP, WWW), et de la sécurité (c'est-à-dire, l'authentification d'utilisateur et les restrictions d'accès).

L'infrastructure a aussi besoin d'être protégée contre les erreurs humaines. Lorsque un administrateur configure mal un hôte, cet hôte peut offrir un service dégradé. Ceci n'affecte que les utilisateurs qui demandent cet hôte et, sauf si cet hôte est un serveur primaire, le nombre d'utilisateurs affectés sera donc limité. Cependant, si un routeur est mal configuré, tous les utilisateurs qui demandent le réseau seront affectés. Visiblement, c'est un bien plus grand nombre d'utilisateurs que ceux dont dépend un seul hôte.

3.2.2 Protéger le réseau

Les réseaux sont vulnérables sous plusieurs aspects. Le problème classique est une attaque de "déni de service". Dans ce cas, le réseau est amené à un état dans lequel il ne peut plus transporter de données d'utilisateurs légitimes. Cela peut se faire de deux façons ordinaires : en attaquant les routeurs et en inondant le réseau avec du trafic parasite. Veuillez noter que le terme de "routeur" est utilisé dans ce paragraphe comme exemple d'une classe plus large de composants actifs d'interconnexion de réseau qui inclut aussi des composants comme les pare-feu, les serveurs mandataires, etc.

Une attaque sur le routeur est conçue pour causer l'arrêt de la transmission des paquets, ou de les lui faire transmettre de façon incorrecte. Le premier cas peut être dû à une mauvaise configuration, à l'injection d'une mise à jour parasite de l'acheminement, ou d'une "attaque de débordement" (c'est-à-dire, le routeur est bombardé de paquets non acheminables, ce qui cause la dégradation de ses performances). Une attaque sur le réseau est similaire à une attaque de débordement sur un routeur, sauf que les paquets du débordement sont généralement en diffusion. Une attaque de débordement idéale serait l'injection d'un seul paquet qui exploite une faute connue dans les nœuds du réseau et les amène à retransmettre le paquet, ou à générer des paquets d'erreur, dont chacun serait reçu et répété par un autre hôte. Un paquet d'attaque bien choisi peut même générer une explosion exponentielle de transmissions.

Un autre problème classique est la "mystification". Dans ce cas, des mises à jour d'acheminement parasites sont envoyées à un ou plusieurs routeurs, ce qui les amène à mal acheminer les paquets. Cela ne diffère d'une attaque en déni de service que par l'objectif qui est derrière l'acheminement parasite. Dans le déni de service, l'objectif est de rendre le routeur inutilisable ; un état qui sera rapidement détecté par les utilisateurs du réseau. Dans la mystification, l'acheminement parasite va causer l'acheminement des paquets vers un hôte à partir duquel un intrus peut surveiller les données des paquets. Ces paquets sont ensuite réacheminés à leurs destinations correctes. Cependant, l'intrus peut avoir ou non altéré le contenu des paquets.

La solution à la plupart de ces problèmes est de protéger les paquets de mise à jour de l'acheminement envoyés par les protocoles d'acheminement utilisés (par exemple, RIP-2, OSPF). Il y a trois niveaux de protection : le mot de passe en clair, la somme de contrôle chiffrée, et le chiffrement. Les mots de passe offrent seulement une protection minimale contre les intrus qui n'ont pas d'accès direct aux réseaux physiques. Les mots de passe offrent aussi une certaine protection contre les routeurs mal configurés (c'est-à-dire, les routeurs qui, à tort, essayent d'acheminer les paquets). L'avantage des mots de passe est qu'ils n'ont qu'une faible redondance, en consommation à la fois de bande passante et de CPU. Les sommes de contrôle protègent contre l'injection de paquets parasites, même si l'intrus a un accès direct au réseau physique. Combinée à un numéro de séquence, ou autre identifiant unique, une somme de contrôle peut aussi protéger contre les attaques "en répétition", dans lesquelles une vieille (mais encore valide) mise à jour d'acheminement est retransmise par un intrus ou un routeur au comportement fautif. Le maximum de sécurité est fourni par le chiffrement complet de mises à jour d'acheminement en séquences numérotées, ou identifiées de façon univoque. Cela empêche un intrus de déterminer la topologie du réseau. Le désavantage du chiffrement est la redondance impliquée dans le traitement des mises à jour.

RIP-2 (RFC 1723) et OSPF (RFC 1583) prennent toutes deux en charge des mots de passe en clair dans leur spécification des concepts de base. Il y a, de plus, des extensions de chaque protocole de base pour prendre en charge le chiffrement MD5.

Malheureusement, il n'y a pas de protection adéquate contre une attaque en débordement, ou contre le mauvais comportement d'un hôte ou d'un routeur qui inonde le réseau. Heureusement, ce type d'attaque est évident lorsqu'elle survient et il peut habituellement y être mis fin relativement simplement.

3.2.3 Protéger les services

Il y a de nombreux types de services et chacun a ses propres exigences de sécurité. Ces exigences vont varier selon la destination du service. Par exemple, un service qui ne devrait être utilisable qu'au sein d'un site (par exemple, NFS) peut requérir des mécanismes de protection différents de ceux d'un service fourni à usage externe. Il peut être suffisant de protéger le serveur interne contre l'accès externe. Cependant, un serveur du WWW, qui fournit une page d'accueil destinée à être vue par les utilisateurs partout sur l'Internet, requiert une protection incorporée. C'est-à-dire que le service/protocole/serveur doit fournir toute la sécurité qui peut être nécessaire pour empêcher l'accès et la modification non autorisée de la base de données de la toile.

Les services internes (c'est-à-dire, les services destinés à n'être fournis qu'aux utilisateurs au sein d'un site) et les services externes (c'est-à-dire, les services rendus délibérément disponibles aux utilisateurs en dehors du site) auront, en général, des exigences de protection qui diffèrent selon la description précédente. Il est donc avisé d'isoler les services internes sur un ensemble d'ordinateurs serveurs d'hôtes et les services externes sur un autre ensemble d'ordinateurs serveurs d'hôtes. C'est à dire que les serveurs internes et externes ne devraient pas être co-localisés sur le même ordinateur hôte. En fait, de nombreux sites vont aussi loin que d'avoir un ensemble de sous-réseaux (ou même des réseaux différents) qui sont accessibles de l'extérieur et un autre ensemble qui ne peut être accessible que de l'intérieur du site. Bien sûr, il y habituellement un pare-feu qui connecte ces partitions. Il faut apporter un grand soin à s'assurer qu'un tel pare-feu fonctionne correctement.

Il y a un intérêt croissant pour l'utilisation d'intranets pour connecter différentes parties d'une organisation (par exemple, les divisions d'une compagnie). Alors que le présent document fait généralement une différence entre externe et interne (public et privé), les sites qui utilisent des intranets devraient être avertis de la nécessité de prendre en compte trois séparations et de prendre les actions appropriées lors de la conception et de l'offre des services. Un service offert à un intranet ne devrait être ni public, ni aussi complètement privé qu'un service à une seule sous-unité organisationnelle. Donc, le service aura besoin de son propre système de soutien, séparé à la fois des services et des réseaux externes et internes.

Une forme de service externe mérite une considération particulière, et c'est l'accès anonyme, ou invité. Cela peut être soit la connexion FTP anonyme soit invitée (non authentifiée). Il est extrêmement important de s'assurer que les identifiants d'utilisateur de connexions de serveurs FTP anonymes et invités sont soigneusement isolés de tout hôte et de système de fichiers auxquels des utilisateurs extérieurs pourraient accéder. Un autre domaine auquel une attention particulière doit être apportée concerne l'accès en écriture anonyme. Un site peut être légalement responsable du contenu des informations accessibles au public, aussi il est conseillé de surveiller attentivement les informations déposées par les utilisateurs anonymes.

Nous allons maintenant examiner les services les plus populaires : le service des noms, le service des mots de

passe/clés, le service d'authentification/mandataire, la messagerie électronique, la Toile mondiale, le transfert de fichiers, et NFS. Comme ce sont les services les plus fréquemment utilisés, ce sont les points d'attaque les plus évidents. Aussi, une attaque réussie de l'un de ces services peut produire un désastre hors de proportion avec l'innocence du service de base.

3.2.3.1 Serveurs de noms (DNS et NIS(+))

L'Internet utilise le système de noms de domaines (DNS) pour effectuer la résolution d'adresse pour les noms d'hôte et de réseau. Le service d'informations réseau (NIS, *Network Information Service*) et NIS+ ne sont pas utilisés sur l'Internet mondial, mais sont soumis au mêmes risques qu'un serveur DNS. La résolution de nom en adresse est critique pour la sécurité de fonctionnement de tout réseau. Un agresseur qui peut réussir à contrôler ou se substituer à un serveur DNS peut réacheminer le trafic pour subvertir les protections de sécurité. Par exemple, du trafic de routine peut être détourné vers un système compromis pour y être surveillé ; ou les utilisateurs peuvent être trompés et fournir des secrets d'authentification. Une organisation devrait créer des sites protégés bien connus, pour agir comme serveurs de noms secondaires et protéger leurs DNS maîtres contre les attaques de déni de service en utilisant des routeurs de filtrage.

Traditionnellement, DNS n'avait pas de capacités de sécurité. En particulier, les informations retournées d'une interrogation ne pouvaient pas faire l'objet d'une vérification des modifications ou de ce qu'elles venaient bien du serveur de nom en cause. Des travaux ont été faits pour incorporer les signatures numériques dans le protocole, ce qui, quand ce sera développé, permettra de vérifier cryptographiquement l'intégrité des informations (voir la RFC 2065).

3.2.3.2 Serveurs de mots de passe / clés (NIS(+) et KDC)

Les serveurs de mot de passe et clés protègent généralement leurs informations vitales (c'est-à-dire, les mots de passe et les clés) par des algorithmes de chiffrement. Cependant, même un mot de passe à chiffrement univoque peut être déterminé par une attaque de dictionnaire (par laquelle les noms communs sont chiffrés pour voir si ils correspondent au chiffrage mémorisé). Il est donc nécessaire de s'assurer que ces serveurs ne sont pas accessibles par des hôtes qui n'envisagent pas de s'en servir pour le service, et même ces hôtes ne devraient être capables que d'accéder au service (c'est-à-dire que des services généraux, tels que Telnet et FTP, ne devraient pas être permis à d'autres que les administrateurs).

3.2.3.3 Serveurs d'authentification/mandataires (SOCKS, FWTK)

Un serveur mandataire fournit un certain nombre d'améliorations de sécurité. Il permet aux sites de concentrer les services à travers un hôte spécifique afin de les surveiller, de cacher la structure interne, etc. Cet entonnoir des services crée une cible attirante pour un intrus potentiel. Le type de protection requise d'un serveur mandataire dépend en grande partie du protocole de mandataire utilisé et des services mandatés. La règle générale de limitation d'accès aux seuls hôtes qui ont besoin des services, et de limitation de l'accès par ces hôtes à ces seuls services, est un bon point de départ.

3.2.3.4 Messagerie électronique

Les systèmes de messagerie électronique ont longtemps été une source pour les intrusions d'attaquants parce que les protocoles de messagerie sont parmi les plus anciens services et les plus largement répandus. Aussi, par sa nature même, un serveur de messagerie électronique exige un accès sur le monde extérieur ; la plupart des serveurs de messagerie électronique acceptent des entrées provenant de n'importe quelle source. Un serveur de messagerie électronique consiste généralement en deux parties : un agent de réception/envoi et un agent de traitement. Comme la messagerie est délivrée à tous les utilisateurs, et est habituellement privée, l'agent de traitement requiert des privilèges système (racine) pour livrer la messagerie. La plupart des mises en œuvre de messagerie effectuent les deux portions du service, ce qui signifie que l'agent récepteur a aussi des privilèges système. Cela ouvre plusieurs trous dans la sécurité que le présent document ne décrira pas. Certaines mises en œuvre disponibles permettent une séparation des deux agents. De telles mises en œuvre sont généralement considérées comme plus sûres, mais exigent cependant de grands soins lors de l'installation pour éviter de créer un problème de sécurité.

3.2.3.5 La Toile mondiale (WWW)

La Toile connaît une croissance exponentielle de sa popularité à cause de sa facilité d'utilisation et de sa puissante capacité à concentrer des services d'information. La plupart des serveurs WWW acceptent certains types de direction et d'action de la part des personnes qui accèdent à leurs services. L'exemple le plus courant est de prendre une demande provenant d'un utilisateur distant et de passer les informations fournies à un programme fonctionnant sur le serveur pour traiter la demande. Certains de ces programmes n'ont pas été écrits avec le souci de la sécurité et peuvent créer des trous de sécurité. Si un serveur de la Toile est disponible pour la communauté de l'Internet, il est particulièrement important que des informations confidentielles ne soient pas colocalisées sur le même hôte que ce serveur. En fait, il est recommandé que le serveur ait un hôte dédié qui ne soit pas "de confiance" pour les autres hôtes internes.

De nombreux sites peuvent vouloir colocaliser le service FTP avec leur service WWW. Mais ceci ne devrait arriver que pour des serveurs non-ftp qui ne font que fournir de l'information (ftp-get). Un serveur non-ftp combiné au WWW peut être dangereux (par exemple, il peut en résulter des modifications des informations que votre site publie sur la toile) et rend par lui-même les considérations de sécurité différentes pour chaque service.

3.2.3.6 Transfert de fichier (FTP, TFTP)

FTP et TFTP permettent tous deux aux utilisateurs de recevoir et envoyer des fichiers électroniques en point à point. Cependant, FTP exige l'authentification alors que TFTP n'en exige aucune. Pour cette raison, TFTP devrait être évité autant que possible.

Les serveurs FTP configurés de façon impropre peuvent permettre aux intrus de copier, remplacer et supprimer des fichiers à volonté, n'importe où sur un hôte, aussi est-il très important de configurer ce service correctement. L'accès à des mots de passe chiffrés et à des données personnelles, et l'introduction de chevaux de Troie, ne sont que quelques unes des menaces qui peuvent survenir pour la sécurité lorsque le service est incorrectement configuré. Les serveurs FTP devraient résider sur leur propre hôte. Certains sites choisissent de colocaliser FTP avec un serveur de la toile, car les deux protocoles partagent des considérations de sécurité communes. Cependant, ce n'est pas recommandé en pratique, en particulier lorsque le service FTP permet l'ajout de fichiers (voir le paragraphe sur WWW ci-dessus). Comme mentionné dans les paragraphes d'ouverture du 3.2.3, les services offerts en interne sur votre site ne devraient pas être colocalisés avec des services offerts en externe. Chacun devrait avoir son hôte propre. TFTP ne prend pas en charge la même gamme de fonctions que FTP, et n'a de toutes façons pas de sécurité. Ce service ne devraient être envisagé qu'en utilisation interne, et il devrait donc être configuré de façon restreinte de sorte que le serveur n'ait accès qu'à un ensemble de fichiers prédéterminés (au lieu de tous les fichiers lisibles dans le monde entier du système). Probablement l'utilisation la plus courante de TFTP est pour télécharger les fichiers de configuration sur un routeur. TFTP devrait résider sur votre propre hôte, et ne devrait pas être installé sur des hôtes acceptant l'accès externe FTP ou à la Toile.

3.2.3.7 NFS

Le service de fichier réseau (NFS, *Network File Service*) permet aux hôtes de partager des disques communs. NFS est fréquemment utilisé par des hôtes sans disque qui dépendent d'un serveur de disques pour tous leurs besoins de mémorisation. Malheureusement, NFS n'a pas de sécurité incorporée. Il est donc nécessaire que le serveur NFS ne soit accessible que par les hôtes qui l'utilisent pour le service. Ceci se fait en spécifiant à quels hôtes le système de fichier est exporté et de quelle manière (par exemple, en lecture seule, en lecture écriture, etc.). Les systèmes de fichiers ne devraient pas être exportés à un hôte en-dehors du réseau local car cela exigerait que le service NFS soit accessible en externe. Dans l'idéal, l'accès externe au service NFS devrait être arrêté par un pare-feu.

3.2.4 Protéger les protections

Il est étonnant de voir si souvent qu'un site néglige les faiblesses les plus évidentes dans sa sécurité en laissant le serveur de sécurité lui-même offert aux attaques. Sur la base des considérations exposées plus haut; il devrait être clair que : le serveur de sécurité ne devrait pas être accessible de l'extérieur du site ; devrait offrir le minimum d'accès, sauf pour une fonction d'authentification, aux utilisateurs sur site ; et ne devrait être colocalisé avec aucun autre serveur. De plus, tous les accès au nœud, y compris l'accès au service lui-même, devraient être enregistrés de façon à fournir une trace papier dans l'éventualité d'une atteinte à la sécurité.

3.3 Pare-feu

Une des mesures de sécurité les plus largement déployées et connues utilisées sur l'Internet est un "pare-feu". Les pare-feu ont la réputation d'une panacée générale pour beaucoup, sinon tous, des questions de sécurité de l'Internet. Ils ne le sont pas. Les pare-feu sont juste un autre outil dans la quête de la sécurité d'un système. Ils fournissent un certain niveau de protection et sont, en général, une façon de mettre en œuvre une politique de sécurité au niveau du réseau. Le niveau de sécurité que procure un pare-feu peut varier autant que le niveau de sécurité sur une machine particulière. Il y a le compromis traditionnel entre la sécurité, la facilité d'utilisation, le coût, la complexité, etc.

Un pare-feu est un des divers mécanismes utilisés pour contrôler et surveiller l'accès à et d'un réseau dans le but de le protéger. Un pare-feu agit comme une passerelle à travers laquelle passe tout le trafic de et vers le réseau et/ou les systèmes protégés. Les pare-feu aident à mettre des limites à la quantité et au type de communications qui ont lieu entre le réseau protégé et un autre réseau (par exemple, l'Internet, ou une autre partie du réseau du site).

Un pare-feu est généralement une façon de construire un mur entre une partie d'un réseau, un réseau interne d'une société, par exemple, et une autre partie, l'Internet mondial, par exemple. La seule caractéristique de ce mur est qu'il est nécessaire qu'il y ait un moyen que certains trafics avec des caractéristiques particulières passent à travers des portes étroitement surveillées ("les passerelles"). La partie difficile est l'établissement des critères selon lesquels les paquets sont admis ou refusés à travers les portes. Les ouvrages écrits sur les pare-feu utilisent des terminologies différentes pour décrire les diverses formes de pare-feu. Cela peut être une source de confusion pour les administrateurs de système qui ne sont pas familiarisés avec les pare-feu. La chose à noter ici est qu'il n'y a pas de terminologie fixée pour la description des pare-feu.

Les pare-feu ne sont pas toujours, ni même normalement, une seule machine. Les pare-feu sont souvent plutôt une combinaison de routeurs, de segments de réseau, et d'ordinateurs hôtes. Donc, pour les besoins de cet exposé, le terme de "pare-feu" peut consister en plus d'un appareil physique. Les pare-feu sont normalement construits en utilisant deux composants différents, des routeurs de filtrage et des serveurs mandataires.

Les routeurs de filtrage sont le composant le plus facile à conceptualiser dans un pare-feu. Un routeur passe et repasse les données entre deux (ou plus) réseaux différents. Un routeur "normal" prend un paquet venant du réseau A et "l'achemine" à sa destination sur le réseau B. Un routeur de filtrage fait la même chose, mais décide non seulement comment acheminer le paquet, mais aussi si il devrait acheminer le paquet. Ceci est fait en installant une série de filtres par lesquels le routeur décide ce qu'il doit faire de chaque paquet de données.

Une discussion des capacités des différentes marques de routeur, fonctionnant sur des versions particulières de logiciels sort du domaine d'application du présent document. Cependant, lors de l'évaluation d'un routeur à utiliser pour le filtrage des paquets, les critères suivants peuvent être importants pour la mise en œuvre d'une politique de filtrage : l'adresse IP de source et de destination, les numéros d'accès TCP de source et de destination, l'état du bit TCP "ack", les numéros d'accès UDP de source et de destination, et la direction du flux de paquets (c'est-à-dire, A vers B ou B vers A). Les autres informations nécessaires pour construite un schéma de filtre sécurisé sont de savoir si le routeur réorganise les instructions de filtre (conçues pour optimiser les filtres, cela peut parfois changer la signification et causer des accès non intentionnels), et de savoir si il est possible d'appliquer les filtres pour les paquets entrants et sortants sur chaque interface (si le routeur ne filtre que les paquets sortants, le routeur est alors "en-dehors" de ses filtres et peut être plus vulnérable aux attaques). En plus de la vulnérabilité du routeur, cette distinction entre l'application des filtres aux paquets entrants ou sortants est particulièrement pertinente pour les routeurs qui ont plus de deux interfaces. Une autre question importante est la capacité à créer des filtres sur la base des options d'en-tête IP et de l'état de fragment d'un paquet. Construire un bon filtre peut être très difficile et exige une bonne compréhension du type des services (protocoles) qui seront filtrés.

Pour une meilleure sécurité, les filtres restreignent habituellement l'accès entre les deux réseaux connectés à un seul hôte, l'hôte bastion. Il n'est possible d'accéder à l'autre réseau que via cet hôte bastion. Comme seul cet hôte, au lieu de quelques centaines d'hôtes, peut être attaqué, il est plus facile de conserver un certain niveau de sécurité parce que seul cet hôte sera à protéger très soigneusement. Pour rendre des ressources disponibles pour les utilisateurs légitimes à travers ce pare-feu, les services devront être retransmis par l'hôte bastion. Certains serveurs ont la retransmission incorporée (comme les serveurs DNS ou les serveurs SMTP), pour d'autres services (par exemple, Telnet, FTP, etc.), des serveurs mandataires peuvent être utilisés pour permettre l'accès sécurisé aux ressources à travers le pare-feu.

Un serveur mandataire est une façon de concentrer les services d'application sur une seule machine. Il y a normalement une seule machine (l'hôte bastion) qui agit comme serveur mandataire pour divers protocoles (Telnet, SMTP, FTP, HTTP, etc.) mais il peut y avoir des ordinateurs hôtes individuels pour chaque service. Au lieu de se connecter directement à un serveur externe, le client se connecte au serveur mandataire qui à son tour initie une connexion avec le serveur externe demandé. Selon le type de serveur mandataire utilisé, il est possible de configurer les clients internes de façon à effectuer automatiquement cette redirection, sans connaissance de l'utilisateur ; d'autres peuvent exiger que l'utilisateur se connecte directement au serveur mandataire, puis initie la connexion selon un format spécifié.

Il y a des bénéfices significatifs pour la sécurité qui découlent de l'utilisation de serveurs mandataires. Il est possible d'ajouter des listes de contrôle d'accès aux protocoles, exigeant des utilisateurs ou des systèmes qu'ils fournissent un certain niveau d'authentification avant que l'accès ne soit accordé. Des serveurs mandataires plus intelligents, parfois appelés passerelles de couche application (ALG, *Application Layer Gateway*) peuvent être montés, qui comprennent des protocoles spécifiques et peuvent être configurés pour ne bloquer que des sous-sections du protocole. Par exemple, un ALG pour FTP peut faire la différence entre la commande "put" et la commande "get" ; une organisation peut souhaiter permettre aux utilisateurs d'obtenir *("get")* des fichiers de l'Internet, mais ne pas leur permettre de mettre *("put")* des fichiers internes sur un serveur distant. À l'inverse, un routeur de filtrage pourrait aussi bien bloquer tous

les accès FTP, ou aucun, mais pas un sous-ensemble. Les serveurs mandataires peuvent aussi être configurés de façon à chiffrer les flux de données sur la base de divers paramètres. Une organisation pourrait utiliser cette caractéristique pour permettre des connexions chiffrées entre deux localisations dont les seuls points d'accès sont l'Internet.

Les pare-feu sont normalement conçus comme un moyen de laisser les intrus à la porte, mais ils sont souvent aussi utilisés comme un moyen pour laisser les utilisateurs légitimes à l'intérieur d'un site. Il y a de nombreux exemples où un utilisateur valide peut avoir besoin d'accéder régulièrement à son site alors qu'il est en déplacement pour des démonstrations et des conférences, etc. L'accès à l'Internet est souvent disponible mais il risque d'être effectué au moyen d'une machine ou réseau qui ne sont pas de confiance. Un serveur mandataire correctement configuré peut admettre des utilisateurs corrects dans le site tout en refusant l'accès aux autres utilisateurs.

Le meilleur des techniques actuelles de pare-feu se trouve dans une combinaison d'une paire de routeurs de scrutation avec un ou plusieurs serveurs mandataires sur un réseau entre les deux routeurs. Ce montage permet au routeur externe de bloquer toute tentative d'utiliser la couche IP sous-jacente pour porter atteinte à la sécurité (usurpation IP, acheminement de source, fragments de paquet), tout en permettant au serveur mandataire de traiter les trous potentiels de la sécurité dans les protocoles de couche supérieure. L'objet du routeur interne est de bloquer tout le trafic sauf pour le serveur mandataire. Si ce montage est mis en œuvre avec fermeté, un haut niveau de sécurité peut être réalisé.

La plupart des pare-feu fournissent un enregistrement de journalisation qui peut être réglé de façon à rendre plus pratique l'administration de la sécurité du réseau. L'enregistrement peut être centralisé et le système peut être configuré pour envoyer des alertes pour les conditions anormales. Il est important de surveiller régulièrement ces enregistrements à la recherche de tous signes d'intrusions ou tentatives d'effraction. Comme certains intrus vont tenter de couvrir leurs traces en éditant des journaux d'événements, il est souhaitable de les protéger. Diverses méthodes sont disponibles, y compris : des pilotes en écriture unique, lecture multiple (WORM) ; journaux sur papier ; journalisation centralisée via l'entité "syslog". Une autre technique est d'utiliser une imprimante série "factice", mais d'avoir le port de série connecté à une machine ou PC isolé, qui conserve les enregistrements.

Les pare-feu sont disponibles dans une large gamme de qualité et de puissances. Les paquetages commerciaux commencent environ à 10 000 US $ et vont jusqu'à 250 000 US $. Des pare-feu "bricolés" peuvent être construits à moindres frais. Il faut se souvenir que le montage correct d'un pare-feu (commercial ou bricolé) exige une grande habileté et la connaissance de TCP/IP. Les deux types exigent une maintenance régulière, l'installation de jeux de logiciels et leurs mises à jour, et une surveillance régulière. Pour budgéter un pare-feu, ces coûts additionnels devraient être pris en considération en plus du coût des éléments physiques du pare-feu.

Ceci mis à part, la construction d'un pare-feu "fait à la maison" exige une grande habileté et une bonne connaissance de TCP/IP. On ne doit pas s'y essayer à la légère parce que la perception d'un sentiment de sécurité est à long terme pire que la connaissance de l'absence de sécurité. Comme avec toutes les mesures de sécurité, il est important de décider sur la menace, de la valeur des biens à protéger, et des coûts de la mise en œuvre de la sécurité.

Une note finale sur les pare-feu. Ils peuvent être d'une grande aide lors de la mise en œuvre de la sécurité pour un site et ils protègent contre une grande diversité d'attaques. Mais il est important de garder présent à l'esprit qu'ils ne sont qu'une partie de la solution. Ils ne peuvent pas protéger votre site contre tous les types d'attaques.

4 Services et procédures de sécurité

La présente section guide le lecteur à travers un certain nombre de sujets qui devraient être traités pour la sécurisation d'un site. Chaque paragraphe touche un service de sécurité ou une capacité qui peut être nécessaire pour protéger les informations et les systèmes sur un site. Les sujets sont présentés dans les grandes lignes pour introduire les concepts auprès du lecteur.

Tout au long de cette section, on trouvera des mentions significatives relatives au chiffrement. Il est en dehors du domaine d'application du présent document d'entrer dans les détails du chiffrement, mais le lecteur intéressé peut obtenir des informations complémentaires des livres et articles mentionnés en référence au présent document.

4.1 Authentification

Pendant de nombreuses années, la méthode prescrite pour l'authentification des utilisateurs a été par l'utilisation de

mots de passe standard, réutilisables. À l'origine, ces mots de passe étaient utilisés par les utilisateurs au niveau du terminal pour s'authentifier auprès d'un ordinateur central. À cette époque, il n'y avait pas de réseaux (internes ou externes), aussi le risque de divulguer les mots de passe en clair était minimal. Aujourd'hui, les systèmes sont connectés ensemble à travers des réseaux locaux, et ces réseaux locaux sont en plus connectés ensemble et avec l'Internet. Les utilisateurs se connectent de tout autour du globe ; leurs mots de passe réutilisables sont souvent transmis à travers les mêmes réseaux en clair, mûrs pour quiconque peut les capturer dans l'intervalle. Et bien sûr, le centre de coordination CERT* et d'autres équipes de réponse voient un nombre incroyable d'incidents qui impliquent des "renifleurs" de paquets qui capturent les mots de passe en clair.

Avec l'avènement de nouvelles technologies comme les mots de passe à une seule utilisation (par exemple, S/Key), PGP, et les appareils d'authentification fondés sur des jetons, les gens utilisent des chaînes de quasi mots de passe comme jetons et broches secrets. Si ces jetons et broches secrets ne sont pas choisis et protégés de façon appropriée, l'authentification sera facilement détournée.

4.1.1 Mots de passe à usage unique

Comme mentionné ci-dessus, étant donné l'environnement de réseau d'aujourd'hui, il est recommandé que les sites concernés par la sécurité et l'intégrité de leurs systèmes et réseaux envisagent de s'éloigner des mots de passe standard réutilisables. Il y a eu de nombreux incidents impliquant des programmes de cheval de Troie de réseau (par exemple, telnet et rlogin) et des programmes d'aspiration de paquets de réseau. Ces programmes capturent des triplets de nom d'hôte/ nom de compte/ mot de passe en texte clair. Les intrus peuvent utiliser les informations capturées pour un accès ultérieur à ces hôtes et comptes. Ceci est possible parce que 1) le mot de passe est utilisé encore et encore (d'où le terme "réutilisable"), et 2) le mot de passe traverse le réseau en clair.

Plusieurs techniques d'authentification ont été développées pour traiter ce problème. Parmi ces techniques figurent les technologies de mise en question/réponse qui fournissent des mots de passe qui ne sont utilisés qu'une seule fois (appelés couramment mots de passe à utilisation unique). Il y a un certain nombre de produits disponibles dont les sites devraient envisager l'utilisation. La décision d'utiliser un produit est de la responsabilité de chaque organisation, et chaque organisation devrait effectuer sa propre évaluation et son propre choix.

4.1.2 Kerberos

Kerberos est un système de sécurité de réseau distribué qui fournit l'authentification à travers des réseaux non sécurisés. Si c'est demandé par l'application, l'intégrité et le chiffrement peuvent aussi être fournis. Kerberos a été développé à l'origine à l'Institut de technologie du Massachusetts (MIT) au milieu des années 1980. Il y a deux versions majeures de Kerberos, les versions 4 et 5, qui sont, pour des raisons pratiques, incompatibles. Kerberos s'appuie sur une base de données de clés symétriques utilisant un centre de distribution de clés (KDC) qui est connu comme le serveur Kerberos. Un utilisateur ou service (appelés le "principal") reçoit des "tickets électroniques" après une communication réussie avec le KDC. Ces tickets sont utilisés pour l'authentification entre principaux. Tous les tickets comportent un horodatage qui limite la durée de validité du ticket. Donc, les clients et serveurs Kerberos doivent avoir une source horaire sécurisée, et être capables de garder une heure précise.

Le côté pratique de Kerberos est son intégration au niveau application. Les applications typiques comme FTP, telnet, POP, et NFS ont été intégrées au système Kerberos. Il y a un grand nombre de mises en œuvre qui ont des niveaux d'intégration variés. Prière de se reporter aux questions les plus courantes de Kerberos disponibles à http://www.ov.com/misc/krb-faq.html pour les dernières informations.

4.1.3 Choix et protection de jetons et numéros d'identification personnelle (PIN) secrets

Lors du choix de jetons secrets, il faut veiller à le faire avec soin. Comme pour le choix des mots de passe, ils doivent être robustes contre les efforts pour les deviner. C'est-à-dire qu'ils ne doivent pas être un seul mot d'une langue, ou un acronyme commun, industriel, ou culturel, etc. Idéalement, ils seront long plutôt que courts et consistent en phrases de passe qui combinent des caractères majuscules et minuscules, des chiffres, et d'autres caractères.

Une fois choisis, la protection de ces jetons secrets est très importante. Certains sont utilisés comme identifiants pour des appareils matériels (comme des cartes à jetons) et ils ne devraient pas être écrits sur ou placés dans les mêmes endroits que l'appareil auquel ils sont associés. D'autres, comme une clé secrète de bonne confidentialité (PGP, *Pretty Good Privacy*), devraient être protégées contre l'accès non autorisé.

Un mot pour terminer ce sujet. Lors de l'utilisation de produits cryptographiques, comme PGP, veillezr à déterminer la longueur de clé appropriée et assurez vous que vos utilisateurs sont entraînés à en faire autant. Avec l'avancée des technologies, la longueur minimum de clé sûre continue de croître. Assurez vous que votre site reste au contact des connaissances les plus récentes sur la technologie de sorte que vous puissiez vous assurer que le chiffrement utilisé vous donne la protection sur laquelle vous comptez.

4.1.4 Garantie des mots de passe

Alors qu'on ne répètera jamais assez la nécessité d'éliminer l'utilisation des mots de passe standard réutilisables, il faut reconnaître que certaines organisations les utilisent encore. Bien qu'il soit recommandé que ces organisations évoluent vers l'utilisation de meilleures technologie, entre temps, l'avis suivant les aidera à choisir et entretenir les mots de passe traditionnels. Mais souvenez vous qu'aucune de ces mesures ne protège contre la divulgation suite à un programme d'aspiration.

(1) Importance de mots de passe robustes – Dans de nombreux cas (sinon tous) de pénétration de systèmes, l'intrus a besoin d'obtenir l'accès à un compte sur le système. Une façon typique d'arriver à cet objectif est de deviner le mot de passe d'un utilisateur légitime. Ceci est souvent accompli en faisant tourner un programme automatisé de cassage de mot de passe, qui utilise un très gros dictionnaire, contre le fichier de mots de passe du système. La seule façon de se garder contre la découverte des mots de passe de cette manière est le soin dans le choix de mots de passe qui ne puissent pas être devinés facilement (c'est-à-dire, combinaisons de chiffres, lettres, et de caractères de ponctuation). Les mots de passe devraient aussi être aussi longs que le système l'accepte et que les utilisateurs peuvent le tolérer.

(2) Changer les mots de passe par défaut – De nombreux systèmes d'exploitation et programmes d'application sont installés avec des comptes et mots de passe par défaut. Ceci doit être changé immédiatement en quelque chose qui ne puisse être deviné ni cassé.

(3) Interdire l'accès au fichier des mots de passe - En particulier, un site veut protéger la portion mots de passe chiffrés du fichier de sorte que les intrus potentiels ne les aient pas à leur disposition pour les déchiffrer. Une technique efficace est d'utiliser des mots de passe fantômes où le champ mot de passe du fichier standard contient un mot de passe factice ou faux. Le fichier contenant les mots de passe légitimes est protégé ailleurs sur le système.

(4) Péremption de mot de passe – Quand et comment expirent les mots de passe est toujours un sujet de controverse dans la communauté de la sécurité. Il est généralement accepté qu'un mot de passe ne devrait pas être conservé après la fin de l'utilisation d'un compte, mais on débat chaudement de la question de savoir si un utilisateur devrait être forcé de changer un bon mot de passe qui est activement utilisé. Les arguments pour le changement des mots de passe se rapportent à la prévention de la poursuite de l'utilisation de comptes violés. Cependant, l'opposition clame que les changements fréquents de mot de passe conduisent les utilisateurs à écrire leurs mots de passe dans des endroits visibles (comme de les afficher sur un terminal), ou à des utilisateurs qui choisissent des mots de passe très simples qui sont faciles à deviner. Il faut dire aussi qu'un intrus utilisera probablement un mot de passe capturé ou deviné plus tôt que plus tard, auquel cas la péremption de mot de passe ne protège que peu ou pas du tout.

Bien qu'il n'y ait pas de réponse définitive à ce dilemme, une politique de mot de passe devrait traiter la question de façon directe et donner des lignes directrices sur la périodicité de changement de mot de passe d'un utilisateur. Certainement, un changement annuel de leur mot de passe n'est pas difficile pour la plupart des utilisateurs, et il faut envisager de l'imposer. Il est recommandé que les mots de passe soient changés au moins chaque fois qu'un compte privilégié est compromis, qu'il y a un changement critique de personnel (particulièrement s'il s'agit d'un administrateur !), ou lorsqu'un compte a été compromis. De plus, si un mot de passe d'un compte privilégié est compromis, tous les mots de passe du système devraient être changés.

(5) Blocage de mot de passe/compte – Certains sites trouvent utile de désactiver les comptes après un nombre prédéfini d'échecs de tentatives d'authentification. Si votre site décide d'employer ce mécanisme, il est recommandé de ne pas publier le mécanisme. Après la désactivation, même si le mot de passe correct est présenté, le message affiché devrait rester celui d'un échec de tentative de connexion. La mise en œuvre de ce mécanisme exigera que les utilisateurs légitimes contactent leur administrateur de système pour demander la réactivation de leur compte.

(6) Un mot sur l'index automatique *(finger daemon)* – Par défaut, l'index automatique affiche des informations système et d'utilisateur considérables. Par exemple, il peut afficher une liste de tous les utilisateurs qui utilisent actuellement un système, ou tout le contenu du fichier plan d'un utilisateur spécifique. Ces informations peuvent être utilisées par des intrus potentiels pour identifier des noms d'utilisateurs et deviner leur mot de passe. Il est recommandé que les sites envisagent de modifier l'index pour interdire l'affichage des informations.

4.2 Confidentialité

Il y a des biens d'information que votre site va vouloir protéger contre la divulgation à des entités non autorisées. Les systèmes d'exploitation ont souvent des mécanismes de protection de fichier incorporés qui permettent à un administrateur de contrôler qui peut accéder aux systèmes, ou "voir" le contenu d'un fichier donné. Une manière plus forte de fournir la confidentialité est le chiffrement. Le chiffrement est effectué par le brouillage des données de telle sorte qu'il soit très difficile et long d'obtenir le texte en clair pour tout autre que les receveurs autorisés ou les propriétaires. Les receveurs autorisés et le propriétaire des informations possèderont les clés de déchiffrement correspondantes qui leur permettent de désembrouiller facilement le texte en une forme lisible (texte en clair). Nous recommandons que les sites utilisent le chiffrement pour fournir la confidentialité et protéger les informations précieuses.

L'utilisation du chiffrement est parfois contrôlée par des règles gouvernementales et de site, de sorte que nous encourageons les administrateurs à se tenir informés des lois ou politiques qui régentent son utilisation avant de l'employer. Il sort du domaine d'application du présent document de discuter des divers algorithmes et programmes disponible pour ce faire, mais nous attirons l'attention sur le fait que le programme UNIX s'est révélé très facile à casser. Nous encourageons chacun à prendre le temps de comprendre la force du chiffrement dans tout algorithme/produit donné avant de l'utiliser. La plupart des produits connus sont bien documentés dans la littérature, et se devrait être une tâche très aisée.

4.3 Intégrité

En tant qu'administrateur, vous voudrez vous assurer que les informations (par exemple, fichiers du système d'exploitation, données de la compagnie, etc.) n'ont pas été altérées d'une façon non autorisée. Cela signifie que vous voulez fournir une certaine assurance quant à l'intégrité des informations sur vos systèmes. Une façon de fournir cela est de produire une somme de contrôle du fichier non altéré, de mémoriser hors ligne cette somme de contrôle, et de vérifier périodiquement (ou quand vous le voulez) pour s'assurer que la somme de contrôle du fichier en ligne n'a pas changé (ce qui indiquerait que les données ont été modifiées).

Certains systèmes d'exploitation viennent avec des programmes de sommes de contrôle, comme le programme UNIX sum. Cependant, cela peut ne pas fournir le niveau de protection dont vous avez réellement besoin. Les fichiers peuvent être modifiés d'une façon telle qu'elle préserve le résultat du programme UNIX sum ! Donc nous vous suggérons d'utiliser un programme cryptographiquement fort, tel que le programme de résumé de message MD5 [ref], pour produire les sommes de contrôle que vous utiliserez pour assurer l'intégrité.

Il y a d'autres applications dans lesquelles l'intégrité doit impérativement être assurée, comme lors de la transmission d'un message électronique entre deux parties. Des produits qui fournissent cette capacité sont disponibles. Une fois que vous avez identifié que c'est une capacité dont vous avez besoin, vous pouvez aller identifier les technologies qui vont vous la fournir.

4.4 Autorisation

Autorisation se réfère au processus d'octroi de privilèges aux processus et, en fin de compte, aux utilisateurs. Cela diffère de l'authentification en ce que l'authentification est le processus utilisé pour identifier un utilisateur. Une fois identifiés (de façon fiable), les privilèges, droits, propriétés, et actions permises de l'utilisateur sont déterminés par l'autorisation.

Il est impossible dans un système raisonnable de faire une liste explicite des activités autorisées de chaque utilisateur (et processus d'utilisateur) par rapport à toutes les ressources (objets). Dans un système réel, certaines techniques sont utilisées pour simplifier le processus d'octroi et de vérification de la ou des autorisations.

Une approche, popularisée dans les systèmes UNIX, est d'allouer à chaque objet trois classes d'utilisateur : propriétaire, groupe et monde. Le propriétaire est soit le créateur de l'objet soit l'utilisateur assigné comme propriétaire par le super utilisateur. Les permissions du propriétaire (lecture, écriture et exécution) ne s'appliquent qu'au propriétaire. Un groupe est une collection d'utilisateurs qui partagent les droits d'accès à un objet. Les permissions de groupe (lecture, écriture et exécution) s'appliquent à tous les utilisateurs du groupe (sauf le propriétaire). Le monde se réfère à tous les autres qui ont accès au système. Les permissions monde (lecture, écriture et exécution) s'appliquent à tous les utilisateurs (sauf le propriétaire et les membres du groupe).

Une autre approche est d'attacher à un objet une liste contenant explicitement l'identité de tous les utilisateurs (ou groupes) permis. C'est une liste de contrôle d'accès (ACL, *Access Control List*). L'avantage des ACL est que leur maintenance est facile (une liste centrale par objet) et il est très aisé de vérifier visuellement qui a accès à quoi. Les désavantages sont les ressources supplémentaires requises pour mémoriser de telles listes, ainsi que le vaste nombre de telles listes nécessaire pour les grands systèmes.

4.5 Accès

4.5.1 Accès physique

Restreindre l'accès physique aux hôtes, ne permettre l'accès qu'aux personnes qui sont censées utiliser les hôtes. Hôtes inclut les terminaux de "confiance" (c'est-à-dire, les terminaux qui permettent une utilisation non authentifiée comme les consoles du système, les terminaux d'opérateur et les terminaux dédiés à des tâches spéciales), et les micro ordinateurs individuels et les stations de travail, en particulier ceux connectés à votre réseau. Assurez vous que les zones de travail des gens sont bien maillées avec les restrictions d'accès ; autrement, ils trouveront des moyens pour contourner votre sécurité physique (par exemple, portes d'obstruction ouvertes).

Garder en sécurité l'original et des copies de sauvegarde de données et des programmes. En plus de les garder en bonne condition pour les besoins de la sauvegarde, elles doivent être protégées contre le vol. Il est important de conserver les sauvegardes dans une localisation séparée des originaux, non seulement pour des considérations de dommages, mais aussi pour les garder contre les voleurs.

Les hôtes portables présentent un risque particulier. Assurez vous qu'ils ne causeront pas de problèmes si un ordinateur d'un des membres du personnel est volé. Envisagez de développer des lignes directrices pour les types de données qu'il serait permis d'avoir sur les disques des ordinateurs portables ainsi que sur la façon dont les données devraient être protégées (par exemple, chiffrement) lorsqu'elles sont sur un ordinateur portable.

Les autres zones où l'accès physique devrait être interdit sont les chambres de câblage et les éléments de réseau importants comme les serveurs de fichiers, les hôtes de serveur de nom, et les routeurs.

4.5.2 Connexions réseau portables

Par connexions "portables", on entend des points de connexion réseau localisés de façon à fournir un moyen pratique pour que les utilisateurs connectent un hôte portable sur votre réseau.

Considérez si vous avez besoin de fournir ce service, en sachant que cela permet à tout utilisateur de raccorder un hôte non autorisé à votre réseau. Cela accroît les risques d'attaque via des techniques telles que l'usurpation d'adresse IP, l'aspiration de paquet, etc. La gestion d'utilisateur et de site doit évaluer les risques que cela implique. Si vous décidez de fournir des connexions portables, planifiez le service avec soin et définissez précisément où vous le fournirez de façon à ce que vous puissiez vous assurer de la sécurité d'accès physique nécessaire.

Un hôte portable devrait être authentifié avant que son utilisateur soit autorisé à accéder aux ressources de votre réseau. En solution de remplacement, il peut être possible de contrôler l'accès physique. Par exemple, si le service doit être utilisé par des étudiants, vous pouvez ne fournir les prises de connexion de portables que dans les laboratoires.

Si vous fournissez des accès portables pour que les visiteurs se connectent à leur réseaux d'origine (par exemple, pour lire leur messagerie, etc.) dans vos locaux, envisagez d'utiliser un sous-réseau séparé qui n'ait pas de connectivité avec le réseau interne.

Gardez un œil sur toute zone qui contient des accès non surveillés au réseau, comme les bureaux vides. Il paraît raisonnable de déconnecter de tels endroits au niveau de la chambre de câblage, et d'envisager l'utilisation de concentrateurs sécurisés et de surveiller les tentatives de connexion des hôtes non autorisés.

4.5.3 Autres technologies réseau

Les technologies considérées ici incluent X.25, le RNIS, SMDS, DDS et le relais de trame. Toutes sont fournies via des liaisons physiques qui passent par des centraux téléphoniques, offrant une possibilité de détournement. Les pirates sont certainement aussi intéressés par les commutateurs téléphoniques que par les réseaux de données !

Avec les technologies commutées, utilisez des circuits virtuels permanents ou des groupes fermés d'utilisateurs chaque fois que possible. Les technologies qui fournissent l'authentification et /ou le chiffrement (comme IPv6) évoluent rapidement ; envisagez de les utiliser sur des liaisons où la sécurité est importante.

4.5.4 Modems

4.5.4.1 Les lignes de modem doivent être gérées

Bien qu'elles fournissent à ses utilisateurs un accès pratique à un site, elles peuvent aussi fournir un détournement efficace des pare-feu du site. Pour cette raison, il est essentiel de garder un contrôle effectif des modems.

Ne permettez pas aux utilisateurs d'installer une ligne de modem sans autorisation appropriée. Cela inclut les installations temporaires (par exemple, brancher du jour au lendemain un modem sur une ligne de télécopie ou de téléphone).

Conserver un registre de toutes vos lignes de modem et tenir votre registre à jour. Effectuez régulièrement (dans l'idéal, automatiquement) des vérification du site pour trouver les modems non autorisés.

4.5.4.2 Les numéros d'utilisateurs entrants doivent être authentifiés

Une vérification du nom d'utilisateur et du mot de passe devrait être effectuée avant qu'un utilisateur puisse accéder à n'importe quelle partie de votre réseau. Les considérations normale de sécurité de mot de passe sont particulièrement importantes (voir au paragraphe 4.1.1).

Rappelez vous que les lignes de téléphone peuvent être sur écoute, et qu'il est assez facile d'intercepter les messages vers les téléphones cellulaires. Les modems modernes à grande vitesse utilisent des techniques de modulation plus sophistiquées, qui les rendent un peu plus difficiles à surveiller, mais il est prudent de supposer que les pirates savent comment espionner sur vos lignes. Pour cette raison, vous devriez utiliser dès que possible des mots de passe à utilisation unique.

Il est bien utile d'avoir un seul point d'entrée des communications (par exemple, un seul grand pool modem) de sorte que tous les utilisateurs soient authentifiés de la même façon.

Les utilisateurs vont occasionnellement faire une faute de frappe sur un mot de passe. Réglez à un court délai – disons deux secondes – après le premier et le second échec de connexion, et forcez la déconnexion après le troisième. Cela va ralentir les attaques automatisées de mot de passe. Ne dites pas à l'utilisateur si le nom d'utilisateur, le mot de passe, ou les deux, était incorrect.

4.5.4.3 Capacité de rappel

Certains serveurs de connexion offrent des facilités de rappel (c'est-à-dire, l'utilisateur appelle et est authentifié, puis le système déconnecte l'appel et rappelle sur un numéro spécifié à l'avance). Le rappel est utile parce que si quelqu'un voulait deviner un nom d'utilisateur et un mot de passe, il est déconnecté, et le système rappelle ensuite le véritable utilisateur dont le mot de passe a été volé ; les appels aléatoires à partir d'un serveur sont suspects, au mieux. Cela signifie en réalité que les utilisateurs ne doivent se connecter que d'une seule localisation (à laquelle le serveur est configuré pour les rappeler), et bien sûr la facturation téléphonique peut être associée à cette localisation de rappel.

Cette caractéristique devrait être utilisée avec prudence ; elle peut facilement être contournée. Au minimum, assurez vous que le rappel n'est jamais fait à partir du même modem que celui de l'appel d'entrée. Par dessus tout, bien que le rappel puisse améliorer la sécurité de modem, vous ne devez pas tout miser sur lui.

4.5.4.4 Tous les identifiant devraient être enregistrés

Toutes les connexions, qu'elles soient réussies ou non, devraient être enregistrées. Cependant, ne conservez pas les bons mots de passe dans le journal. Enregistrez les plutôt simplement comme une tentative de connexion réussie. Comme la plupart des mauvais mots de passe sont des erreurs de frappe par des utilisateurs autorisés, ils ne varient que d'un seul caractère du mot de passe réel. Vous ne pouvez donc pas garder en sécurité un tel enregistrement. Ne l'enregistrez pas du tout.

Si l'identification de l'appelant est disponible, tirez en parti en enregistrant le numéro appelant pour chaque tentative de connexion. Soyez attentifs aux questions de confidentialité découlant de l'identification de l'appelant. Soyez aussi conscient que l'identification de l'appelant n'est pas de confiance (car on sait que des intrus pénètrent dans des centraux téléphoniques et retransmettent des numéros de téléphone ou font d'autres modifications) ; n'utilisez les données que pour des besoins d'information, pas pour l'authentification.

4.5.4.5 Choisissez soigneusement votre accroche d'ouverture

De nombreux sites utilisent un système par défaut contenu dans un message du fichier du jour pour leur page d'accueil. Malheureusement, cela inclut souvent le type de matériel de l'hôte ou du système d'exploitation présent sur l'hôte. Cela peut fournir des informations précieuses à un intrus potentiel. Chaque site devrait à la place créer sa propre page d'accueil spécifique, en prenant soin de n'y inclure que les informations nécessaires.

Affichez une courte page d'accueil, mais ne proposez pas un nom d'"invite" (par exemple, Université de XYZ, Système d'enregistrement des étudiants). Donnez plutôt le nom de votre site, un bref avertissement sur le fait que les sessions peuvent être sous surveillance, et une cartouche nom d'utilisateur/mot de passe. Vérifiez les possibles implications juridiques du texte que vous mettez dans la page d'accueil.

Pour les applications à haute sécurité, envisagez un mot de passe "aveugle" (c'est-à-dire, ne donnez pas de réponse à un appel entrant tant que l'utilisateur n'a pas tapé son mot de passe). Cela simule en fait un modem débranché.

4.5.4.6 Authentification d'accès extérieur

Les utilisateurs d'appels sortants devraient aussi être authentifiés, en particulier dans la mesure où votre site va devoir payer les factures de téléphone.

Ne permettez jamais un appel sortant à partir d'un appel interne non authentifié, et demandez vous si vous allez lui permettre de le faire à partir d'un appel authentifié. Le but ici est d'empêcher les appelants d'utiliser votre pool de modems au titre de la chaîne des connexions. Cela peut être difficile à détecter, en particulier si un pirate construit un chemin à travers plusieurs hôtes de votre site.

Au minimum, ne permettez pas d'utiliser les mêmes modems et lignes téléphoniques à la fois pour les appels entrants et sortants. Cela peut être facilement mis en œuvre si vous faites fonctionner des pools modem séparés pour l'entrée et la sorties.

4.5.4.7 Rendez la programmation de votre modem aussi "à l'épreuve des balles" que possible

Assurez vous que les modems ne peuvent pas être reprogrammés pendant qu'ils sont en service. Au minimum, assurez vous que trois signes plus ne vont pas mettre vos modems d'entrée en mode commande !

Programmez vos modems pour rétablir la configuration standard au début de chaque nouvel appel. Faute de cela, faites les se réinitialiser à la fin de chaque appel. Cette précaution vous protègera contre la reprogrammation accidentelle de vos modems. Réinitialiser à la fin et au début de chaque appel vous assurera même à un plus haut niveau de confiance qu'un nouvel appelant ne va pas hériter de la session d'un appelant précédant.

Vérifiez que vos modems terminent proprement les appels. Lorsque un utilisateur se connecte à un serveur d'accès, vérifiez que le serveur raccroche correctement les lignes téléphoniques. Il est également important que le serveur force à la déconnexion quelles que soient les sessions actives si l'utilisateur raccroche de façon inattendue.

4.6 Audit

Ce paragraphe traite des procédures de collecte des données générées par l'activité réseau, qui peuvent être utiles pour l'analyse de la sécurité d'un réseau et la réponse aux incidents de sécurité.

4.6.1 Que collecter ?

Les données d'audit devraient inclure toute tentative par toute personne, processus ou autre entité du réseau, de réaliser un niveau de sécurité différent. Cela inclut les connexions et déconnexions, les accès de super utilisateur (ou son équivalent non UNIX), la génération de tickets (pour Kerberos, par exemple), et tous autres changements d'accès ou de statut. Il est particulièrement important de noter les accès "anonymes" ou "invités" aux serveurs publics.

Les données réelles à collecter vont différer pour des sites différents et pour différents types de changements d'accès au sein d'un site. En général, les informations que vous voulez collecter incluent : le nom d'utilisateur et le nom d'hôte, pour la connexion et la déconnexion ; les anciens et les nouveaux droits d'accès, pour un changement de droits d'accès ; et un horodatage. Bien sûr, bien plus d'informations peuvent être rassemblées, selon ce que le système met à votre disposition et de la quantité de place disponible pour mémoriser ces informations.

Note très importante : ne collectez pas les mots de passe. Cela crée un énorme potentiel d'atteintes à la sécurité en cas

d'accès indu aux enregistrements d'audit. Ne collectez pas non plus les mots de passe incorrects car ils ne diffèrent souvent des mots de passe valides que par un seul caractère ou une seule transposition.

4.6.2 Processus de collecte

Le processus de collecte devrait être activé par l'hôte ou la ressource à laquelle on accède. Selon l'importance des données et du besoin de les avoir en local dans les instances dans lesquelles les services sont refusés, les données pourraient être conservées en local sur la ressource jusqu'à ce qu'elles soient nécessaires, ou transmises à une mémoire de stockage après chaque événement.

Il y a trois manières de base pour mémoriser les enregistrements d'audit : dans un fichier en lecture/écriture sur un hôte, sur un appareil en écriture unique/lecture multiple (par exemple, un CD-ROM ou un pilote de bande spécialement configuré), ou un appareil en écriture seule (par exemple, une imprimante en ligne). Chaque méthode a ses avantages et ses inconvénients.

La connexion à un système de fichiers est la moins consommatrice de ressource des trois méthodes et la plus facile à configurer. Elle permet un accès instantané aux enregistrements pour les analyser, ce qui peut être important si une attaque est en cours. La connexion à un système de fichiers est aussi la méthode la moins fiable. Si l'hôte de connexion a été compromis, le système de fichiers est normalement la première chose où aller ; un intrus pourrait facilement couvrir les traces de l'intrusion.

La collecte des données d'audit d'un appareil en écriture unique demande légèrement plus d'effort à configurer qu'un simple fichier, mais elle a l'avantage significatif d'une sécurité largement accrue parce que l'intrus ne pourra pas altérer les données sans montrer qu'une intrusion est survenue. Le désavantage de cette méthode est qu'il est nécessaire d'entretenir une alimentation du support de stockage et du coût de ce support. Les données peuvent aussi n'être pas instantanément disponibles.

La connexion à une imprimante en ligne est utile dans les systèmes où des journaux permanents et immédiats sont nécessaires. Un système en temps réel en est un exemple, car le point exact de la défaillance ou de l'attaque doit être noté. Une imprimante laser, ou un autre appareil qui met les données en mémoire tampon (par exemple, un serveur d'impression), peut souffrir des pertes de données si la mémoire tampon contient les données nécessaires à un instant critique. Le désavantage de, littéralement, "la sortie papier" est la nécessité d'alimenter l'imprimante et celle d'examiner les enregistrements à la main. Il y a aussi le problème du stockage de l'énorme volume, potentiel, du papier qui va être généré.

Pour chacune des méthodes de journalisation décrites, il y a aussi la question de la sécurisation du chemin entre l'appareil qui génère le journal et l'appareil réel d'enregistrement (c'est-à-dire, le serveur de fichier, le pilote de bande/CD-ROM, l'imprimante). Si ce chemin est compromis, l'enregistrement peut être arrêté ou usurpé ou les deux. Dans l'idéal, l'appareil d'enregistrement devrait être directement rattaché à un seul simple câble point à point. Comme c'est habituellement impraticable, le chemin devrait passer par le nombre minimum de réseaux et de routeurs. Même si les enregistrements sont bloqués, l'usurpation peut être empêchée avec des sommes de contrôle cryptographiques (il n'est probablement pas nécessaire de chiffrer les enregistrements parce qu'ils ne devraient pas a priori contenir d'informations sensibles).

4.6.3 Charge de la collecte

La collecte des données d'audit peut résulter en une rapide accumulation d'octets de sorte que la disponibilité de capacités de stockage pour ces informations doive être envisagée à l'avance. Il y a peu de moyens de réduire l'espace de stockage nécessaire. D'abord, les données peuvent être compressées, en utilisant une des nombreuses méthodes existantes. Ou bien, l'espace requis peut être minimisé en ne gardant les données que pour une courte période avec seulement des résumés de ces données dans des archives de long terme. Un inconvénient majeur de cette dernière méthode concerne la réponse aux incidents. Souvent, un incident s'est produit pendant un certain temps avant qu'un site ne le remarque et commence à enquêter. À ce moment, il est très utile d'avoir à sa disposition des enregistrements d'audit détaillés. S'il n'y a plus que des résumés, il peut n'y avoir pas de détails suffisants pour traiter pleinement l'incident.

4.6.4 Traitement et préservation des données d'audit

Les données d'audit devraient être les données les plus soigneusement sécurisées du site et dans les sauvegardes. Si un

intrus voulait obtenir l'accès aux journaux d'audit, les systèmes eux-mêmes, en plus des données, seraient en péril.

Les données d'audit peuvent aussi devenir capitales dans les investigations, l'appréhension, et les poursuites sur l'auteur d'un incident. Pour cette raison, il est recommandé de rechercher l'avis d'un conseiller juridique pour décider comment devraient être traitées les données d'audit. Cela devrait se faire avant que ne survienne un incident.

Si un plan de traitement des données n'est pas défini de façon adéquate préalablement à un incident, cela peut signifier qu'on aura aucun recours pour les suites à donner à l'événement, et cela peut entraîner une responsabilité résultant du traitement impropre des données.

4.6.5 Considérations légales

Du fait du contenu des données d'audit, il y a un certain nombre de questions juridiques qui émergent et pour lesquelles il peut être nécessaire d'être assisté par votre conseiller juridique. Si vous collectez et sauvegardez les données d'audit, vous devez être prêt aux conséquences qui résultent à la fois de leur existence et de leur contenu.

Un des domaines est celui de la vie privée des individus. Dans certaines instances, les données d'audit peuvent contenir des informations personnelles. Les recherches dans ces données, même pour une vérification de routine de la sécurité du système, pourraient représenter une invasion de la vie privée.

Un second domaine de préoccupation est la connaissance des comportements intrusifs qui ont votre site pour origine. Si une organisation conserve les données d'audit, est elle responsable de leur examen à la recherche d'incidents ? Si un hôte dans une organisation est utilisé comme point de lancement d'une attaque contre une autre organisation, la seconde organisation peut elle utiliser les données d'audit de la première organisation pour prouver une négligence de la part de cette organisation ?

Les exemples ci-dessus visent à être complets, mais vous devriez motiver votre organisation pour qu'elle envisage les questions juridiques impliquées par les données d'audit.

4.7 Sécurisation des sauvegardes

La procédure de création des sauvegardes est une partie classique du fonctionnement d'un système informatique. Dans le contexte du présent document, les sauvegardes sont traitées au titre du plan de sécurité global d'un site. Plusieurs aspects des sauvegardes sont importants dans ce contexte :

(1) Assurez vous que votre site crée des sauvegardes.
(2) Assurez vous que votre site utilise un stockage hors site pour les sauvegardes. Le site de stockage devrait être choisi avec soin à la fois pour sa sécurité et pour sa disponibilité.
(3) Envisagez le chiffrement de vos sauvegardes pour fournir une protection supplémentaire des informations une fois qu'elles sont hors site. Cependant, sachez que vous aurez besoin d'un bon schéma de gestion de clé de sorte que vous soyez capable de récupérer les données à tout moment à l'avenir. Assurez vous aussi que vous aurez accès aux programmes de déchiffrement nécessaires à ce moment lorsque vous aurez besoin d'effectuer le déchiffrement.
(4) Ne supposez pas que vos sauvegardes seront toujours bonnes. Il y a eu de nombreuses instances d'incidents de sécurité informatique qui ont couru sur de longues durées avant qu'un site remarque l'incident. Dans de tels cas, les sauvegardes des systèmes affectés sont aussi altérées.
(5) Vérifiez périodiquement l'exactitude et la complétude de vos sauvegardes.

5 Traitement des incidents de sécurité

La présente section donne des directives à utiliser avant, pendant et après que survienne un incident de sécurité informatique sur un hôte, un réseau, un site, ou un environnement multisite. La philosophie du comportement à tenir dans le cas d'une atteinte à la sécurité informatique est de réagir conformément à un plan. Cela est vrai que l'atteinte soit le résultat de l'attaque d'un intrus externe, d'un dommage non intentionnel, des essais d'un étudiant sur un programme d'exploitation des faiblesses d'un logiciel, ou d'un employé mécontent. Chacun des types possibles d'événement, tels que ceux qui viennent d'être énoncés, devrait être envisagé à l'avance par un des plans d'urgence adéquats.

La sécurité informatique traditionnelle, quoique assez importante dans le plan de sécurité global du site, ne prête

habituellement que peu d'attention à la façon de traiter réellement une attaque lorsqu'elle survient. Le résultat est que lorsque une attaque est en cours, beaucoup de décisions sont prises à la hâte et peuvent être dommageables pour la recherche de la source de l'incident, pour la collecte des preuves nécessaires aux poursuites, pour la préparation de la récupération du système, et pour la protection des précieuses données contenues dans le système.

Un des plus importants, mais souvent méconnu, bénéfice du traitement efficace d'un incident, est économique. Mobiliser les personnels à la fois techniques et de gestion pour répondre à un incident exige des ressources considérables. Si il est entraîné à traiter efficacement les incidents, moins de personnel est nécessaire lorsqu'il arrive.

Du fait du réseau mondial, la plupart des incidents ne se restreignent pas à un seul site. Les faiblesses des systèmes d'exploitation s'appliquent (dans certains cas) à plusieurs millions de systèmes, et de nombreuses faiblesses sont exploitées au sein du réseau lui-même. Donc, il est vital que tous les sites impliqués soient informés aussitôt que possible.

Un autre bénéfice se rapporte aux relations publiques. Les nouvelles sur les incidents de sécurité informatique tendent à être dommageables pour l'image de marque d'une organisation. Un traitement efficace d'incident minimise le potentiel négatif pour l'image.

Un bénéfice final du traitement efficace d'incident se rapporte aux questions juridiques. Il est possible que dans un proche avenir, les organisations puissent être tenues responsable de l'utilisation d'un de leurs nœuds pour lancer une attaque sur le réseau. Dans la même veine, les gens qui développent des correctifs ou des accessoires peuvent être poursuivis si les correctifs ou accessoires sont inefficaces, et qu'il en résulte la compromission des systèmes, ou, si les correctifs ou accessoires causent eux-mêmes des dommages aux systèmes. Connaître les faiblesses des systèmes d'exploitation et les schémas d'attaques, et prendre en conséquence les mesures appropriées pour contrer ces menaces potentielles est critique pour circonvenir de possibles problèmes juridiques.

Les paragraphes de cette section donnent les contours et le point de départ de la création de la politique de votre site pour le traitement des incidents de sécurité. Les paragraphes sont :

(1) Préparation et planning (que sont les buts et objectifs du traitement d'un incident ?).
(2) Notification (qui devrait être contacté dans le cas d'un incident ?).
- gestionnaires et personnels locaux
- agences d'application de la loi et d'investigation
- équipes de traitement des incidents de sécurité informatique
- sites affectés et impliqués
- communications internes
- relations publiques et communiqués de presse

(3) Identifier un incident (est-ce un incident, quelle est sa gravité ?).
(4) Traitement (ce qui devrait être fait lorsque survient un incident).
- notification (à qui l'incident devrait être notifié)
- protection des preuves et enregistrement d'activité (quels journaux devraient être gardés d'avant, pendant et après l'incident ?)
- confinement (comment limiter les dommages ?)
- éradication (comment éliminer les raisons de l'incident ?)
- récupération (comment rétablir les services et systèmes ?)
- suites (quelles actions devraient être entreprises après l'incident ?)

(5) L'après incident (quelles sont les implications des incidents passés ?).
(6) Réponse administrative aux incidents.

Le reste de cette section précisera les questions impliquées dans chacun des sujets importants énumérés ci-dessus, et donnera quelques indications sur ce qui devrait être inclus dans la politique d'un site pour le traitement des incidents.

5.1 Préparation et planification du traitement d'incident

Une partie du traitement d'un incident est d'être prêt à répondre à un incident avant même que l'incident ne survienne pour la première fois. Cela comporte l'établissement d'un niveau de protections convenable comme expliqué dans les chapitres précédents. Le faire devrait aider votre site à prévenir les incidents aussi bien qu'à limiter les dommages potentiels en résultant lorsqu'ils surviennent. La protection inclut aussi de préparer les lignes directrices du traitement d'incident au titre d'un plan d'urgence pour votre organisation ou site. Avoir des plans écrits élimine beaucoup des ambiguïtés qui surviennent pendant un incident, et conduira à un ensemble de réponses plus approprié et plus resserré.

Il est d'une importance vitale de tester le plan proposé par des "galops d'essai" avant qu'un incident ne survienne. Une équipe peut même envisager de louer une "équipe de tigres" pour agir parallèlement au galop d'essai. (Note : une équipe de tigres est un groupe de spécialistes qui essayent de pénétrer la sécurité d'un système.)

Apprendre à répondre efficacement à un incident est important pour un certain nombre de raisons :
(1) Protéger les biens qui pourraient être compromis
(2) Protéger les ressources qui pourraient être utilisées avec plus de profit si un incident n'exige pas leurs services
(3) Se conformer aux règlements (gouvernementaux ou autres)
(4) Empêcher l'utilisation de vos systèmes dans des attaques contre d'autres systèmes (ce qui pourrait engager votre responsabilité)
(5) Minimiser une atteinte potentielle à votre image de marque

Comme dans tout ensemble de procédures pré planifiées, il faut faire attention à un ensemble d'objectifs pour le traitement d'un incident. Ces objectifs recevront des priorités différentes selon le site. Un ensemble d'objectifs spécifique peut être identifié pour le traitement des incidents :
(1) Déterminer comment c'est arrivé.
(2) Trouver comment éviter une exploitation ultérieure de la même faiblesse.
(3) Éviter l'escalade et des incidents ultérieurs.
(4) Évaluer l'impact et les dommages de l'incident.
(5) Récupérer de l'incident.
(6) Mettre à jour en tant que de besoin les politiques et les procédures.
(7) Trouver le coupable (si c'est approprié et possible).

Du fait de la nature de l'incident, il peut y avoir un conflit entre l'analyse de la source d'origine d'un problème et la restauration des systèmes et services. Les objectifs globaux (comme d'assurer l'intégrité des systèmes critiques) peuvent être la raison pour ne pas analyser un incident. Bien sûr, c'est une décision de gestion importante ; mais toutes les parties impliquées doivent savoir que sans analyse, le même incident peut se produire à nouveau.

Il est aussi important de donner une priorité aux actions à entreprendre durant un incident longtemps avant que l'incident ne survienne. Parfois, un incident peut être si complexe qu'il est impossible de faire à la fois tout ce qui est nécessaire pour y répondre ; affecter les priorités est essentiel. Bien que les priorités doivent varier d'une institution à l'autre, les priorités suggérées suivantes peuvent servir de point de départ pour la définition de la réponse de votre organisation :
(1) Priorité une – protéger la vie humaine et la sécurité des personnes ; la vie humaine a toujours la préséance sur toute autre considération.
(2) Priorité deux – protéger les données secrètes et/ou sensibles. Empêcher l'exploitation des systèmes, réseaux ou sites secrets ou sensibles. Informer les systèmes, réseaux ou sites secrets ou sensibles affectés des pénétrations qui sont déjà survenues. (Soyez au courant des règlements de votre site ou du gouvernement)
(3) Priorité trois – protéger les autres données, y compris les brevets, les données scientifiques, de gestion et les autres, parce que la perte des données est coûteuse en termes de ressources. Prévenir l'exploitation des autres systèmes, réseaux ou sites et informer les systèmes, réseaux ou sites déjà affectés des pénétrations réussies.
(4) Priorité quatre – empêcher les dommages aux systèmes (par exemple, perte ou altération de fichiers système, dommages aux pilotes de disques, etc.). Les dommages aux systèmes peuvent entraîner de coûteux délais d'immobilisation et de récupération.
(5) Priorité cinq -- minimiser l'interruption des ressources de calcul (y compris les processus). Il est meilleur dans de nombreux cas de fermer un système ou de le déconnecter d'un réseau que de risquer d'endommager les données ou systèmes. Les sites devront évaluer les compromis entre la fermeture, la déconnexion, et rester ouvert. Il peut y avoir des accords de service qui exigent que les systèmes restent ouverts même en présence d'une menace de dommage imminent. Cependant, les dommages et la portée d'un incident peuvent être si étendus que les accords de service doivent être outrepassés.

Une implication importante pour la définition des priorités est qu'une fois réglées les considérations de vie humaine et de sécurité nationale, il est généralement plus important de sauver les données que les logiciels et le matériel du système. Bien qu'il ne soit pas souhaitable de subir aucun dommage ou perte durant un incident, les systèmes peuvent être remplacés. Cependant, la perte ou la compromission des données (en particulier des données secrètes ou brevetées) n'est normalement acceptable dans aucune circonstance.

Une autre question importante concerne les effets sur les autres, au delà des systèmes et réseaux où survient l'incident. Dans les limites imposées par les règles légales, il est toujours important d'informer les parties affectées aussitôt que possible. Du fait des implications juridiques de cette question, elle devrait être incluse dans les procédures planifiées pour éviter d'autres retards et incertitudes pour les administrateurs.

Tout plan pour répondre aux incidents de sécurité devrait être guidé par les politiques et règlementations locales. Les sites gouvernementaux et privés qui traitent des dossiers classés défense doivent suivre des règles spécifiques.

Les politiques choisies par votre site sur la façon de réagir aux incidents vont façonner votre réponse. Par exemple, il y a peu de sens à créer des mécanismes pour surveiller et pister les intrus si votre site ne prévoit pas d'entreprendre d'actions contres les intrus, s'ils sont pris. D'autres organisations peuvent avoir des politiques qui affectent vos plans. Les compagnies de téléphone ne livrent souvent les informations sur les écoutes téléphoniques qu'aux agences officielles de répression.

Le traitement des incidents peut être fastidieux et exige un certain nombre de tâches de routine qui peuvent être prises en charge par le personnel de soutien. Pour libérer le personnel technique, il peut être utile d'identifier les personnels de soutien qui vont aider à des tâches telles que photocopie, télécopie, etc.

5.2 Notification et points de contact

Il est important d'établir des contacts avec divers personnels avant l'arrivée d'un incident réel. Souvent, les incidents ne sont pas des urgences réelles. Bien sûr, sous serez souvent capables de traiter les activités en interne. Cependant, il y a de nombreuses fois où des personnes en dehors de votre département immédiat devront être incluses dans le traitement de l'incident. Ces contacts supplémentaires incluent les gestionnaires et administrateurs de système locaux, les contacts administratifs d'autres sites sur l'Internet, et diverses organisations d'investigation. Connaître ces contacts avant que n'arrivent les incidents vous aidera à rendre plus efficace votre processus de traitement d'incident.

Pour chaque type de contact de communication, un "Point de Contact" (POC) spécifique devrait être défini. Ils peuvent être de nature technique ou administrative et peuvent inclure des agences juridiques ou d'investigations aussi bien que des fournisseurs de service et des fabricants. Lors de l'établissement de ces contacts, il est important de décider comment partager le maximum d'informations avec chaque classe de contact. Il est particulièrement important de définir, à l'avance, quelles informations seront partagées avec les utilisateurs d'un site, avec le public (y compris la presse), et avec les autres sites.

Régler des questions est particulièrement important pour la personne responsable locale du traitement de l'incident, car c'est la personne responsable de la notification réelle aux autres. Une liste des contacts dans chacune de ces catégories est une important économie de temps pour cette personne pendant un incident. Il peut être assez difficile de trouver une personne appropriée durant un incident alors que de nombreux événements importants sont en cours. Il est fortement recommandé que tous les numéros de téléphone pertinents (et aussi les adresses de messagerie électronique et les numéros de télécopie) soient inclus dans la politique de sécurité du site. Les informations de noms et de contact de tous les individus qui seront directement impliqués dans le traitement d'un incident devraient être placés au sommet de cette liste.

5.2.1 Gestionnaires et personnels locaux

Lorsque un incident est en cours, une question majeure est de décider qui est responsable de la coordination de l'activité de la multitude des intervenants. Une faute majeure peut être commise qui est d'avoir un certain nombre de gens qui travaillent de façon indépendante, et ne travaillent pas ensemble. Cela va seulement ajouter à la confusion de l'événement et va probablement conduire à des efforts gâchés ou inefficaces.

Le seul POC peut être ou non responsable du traitement de l'incident. Il y a deux rôles distincts à tenir lorsqu'on décide qui sera le POC et qui sera la personne en charge de l'incident. La personne en charge de l'incident prendra des décisions comme l'interprétation de la politique à appliquer à l'événement. À l'inverse, le POC doit coordonner les efforts de toutes les parties impliquées dans le traitement de l'événement.

Le POC doit être une personne ayant une expertise technique pour coordonner avec succès les efforts des gestionnaires de système et utilisateurs impliqués dans la surveillance et la réaction à l'attaque. Il faut faire attention lors de l'identification de cette personne. Il ne devrait pas être nécessaire que cette même personne ait la responsabilité administrative des systèmes compromis car souvent de tels administrateurs ont seulement des connaissances suffisantes pour l'utilisation quotidienne des ordinateurs, et manquent d'expertise technique en profondeur.

Une autre importante fonction du POC est de maintenir le contact avec les agences d'application de la loi et autres agences externes pour s'assurer d'une implication de plusieurs agences. Le niveau d'implication sera déterminé par des

décisions de gestion ainsi que par les contraintes réglementaires.

Un seul POC devrait aussi être la seule personne en charge de la collecte des preuves, car en règle générale, plus il y a de monde qui touche à un élément de preuve potentiel, plus grande est la possibilité qu'elle ne soit pas admissible à la barre. Pour s'assurer que la preuve sera acceptable pour la communauté juridique, la collecte des preuves devrait être effectuée suivant les procédures prédéfinies conformément aux lois et règles locales.

Une des tâches les plus critiques du POC est la coordination de tous les processus pertinents. Les responsabilités peuvent être distribuées sur la totalité du site, impliquant plusieurs départements ou groupes indépendants. Cela exigera un effort bien coordonné afin de réaliser un succès global. La situation devient encore plus complexe si plusieurs sites sont impliqués. Lorsque cela arrive, un seul POC sur un site sera rarement capable de coordonner de façon adéquate le traitement de l'incident entier. Au lieu de cela, des équipes de réponse aux incidents appropriées devraient être impliquées.

Le processus de traitement d'incident devrait disposer d'une sorte de mécanisme d'escalade. Afin de définir un tel mécanisme, les sites auront besoin de créer un schéma de classification interne pour les incidents. Le POC et les procédures appropriées seront associés à chaque niveau d'incident. Lorsque un échelon est franchi dans l'incident, il peut y avoir un changement du POC qui devra être communiqué à tous ceux qui sont impliqués dans la gestion de l'incident. Lorsque survient un changement du POC, l'ancien POC devrait porter à la connaissance du nouveau POC toutes les informations utiles.

Finalement, les utilisateurs doivent savoir comment faire rapport de leurs soupçons sur les incidents. Les sites devraient établir des procédures de rapport qui fonctionnent à la fois pendant et en dehors des heures de travail normales. Les bureaux d'assistance sont souvent utilisés pour recevoir ces rapports pendant les heures de travail normales, et les beepers et téléphones peuvent être utilisés pour les rapports en dehors de ces heures.

5.2.2 Application de la loi et services de sécurité

Dans le cas où un incident a des conséquences juridiques, il est important d'établir un contact avec des agences d'investigation (par exemple, le FBI et le Service secret aux U.S.A) aussitôt que possible. Les services de police locaux, les offices de sécurité locaux, et la police du campus devraient aussi être informés en tant que de besoin. Ce paragraphe décrit un grand nombre des questions auxquelles vous serez confronté, mais il faut savoir que chaque organisation aura ses propres lois et règlements locaux et gouvernementaux qui impacteront la façon dont ils interagissent avec les agences d'investigation et d'application de la loi. Le point le plus important à noter pour l'instant est que chaque site doit résoudre ces questions.

La principale raison de déterminer ces points de contact bien avant l'incident est qu'une fois qu'une attaque majeure est en cours, il reste peu de temps pour appeler ces agences pour déterminer exactement qui est le bon contact. Une autre raison est qu'il est important de coopérer avec ces agences d'une manière qui entretienne de bonnes relations de travail, et cela sera conformément aux procédures de travail de ces agences. Connaître les procédures de travail à l'avance, et les attentes de votre point de contact est un grand pas dans cette direction. Par exemple, il est important de rassembler des preuves qui seront admissibles dans toute procédure juridique ultérieure, et cela exige une connaissance préalable de la façon de rassembler de telles preuves. La dernière raison pour établir les contacts aussitôt que possible est qu'il est impossible de savoir quelle agence particulière sera juridiquement compétente pour tout incident donné. Prendre contact et trouver les canaux appropriés à l'avance vous permettra de répondre considérablement plus confortablement à un incident.

Si votre organisation ou site a un conseiller juridique, vous devez notifier à son bureau qu'un incident est en cours aussitôt que vous l'apprenez. Au minimum, votre conseiller juridique a besoin d'être impliqué pour protéger les intérêts juridiques et financiers de votre site ou organisation. Il y a de nombreuses questions juridiques et pratiques, dont quelques unes sont :

(1) Est-ce que votre site ou organisation veut prendre le risque d'une publicité négative ou s'exposer à coopérer à des efforts de poursuites légales.

(2) Responsabilité vers l'aval – si vous laissez un système compromis comme il est et qu'il soit espionné, et si un autre ordinateur est endommagé par l'attaque dont l'origine est dans votre système, votre site ou organisation peut être responsable des dommages encourus.

(3) Distribution des informations – si votre site ou organisation distribue des informations sur une attaque dans laquelle un autre site ou organisation peut être impliqué ou sur la vulnérabilité d'un produit qui peut affecter la capacité à commercialiser ce produit, votre site ou organisation peut encore être responsable de tous les

dommages (y compris ceux à la réputation).

(4) Responsabilités dues à la surveillance -- votre site ou organisation peut être poursuivie si des utilisateurs de votre site ou d'ailleurs découvrent que votre site surveille l'activités de certains comptes sans en informer les utilisateurs.

Malheureusement, il n'y a pas de précédents clairs actuellement sur la responsabilité des organisations impliquées dans un incident de sécurité ou qui pourraient être impliquées dans la prise en charge d'efforts d'investigation. Les enquêteurs encourageront souvent les organisations à aider à pister et surveiller les intrus. Bien sûr, la plupart des enquêteurs ne peuvent pas poursuivre les intrusions informatiques sans un soutien actif des organisations impliquées. Cependant, les enquêteurs ne peuvent pas fournir de protection pour les engagements de responsabilité, et cette sorte d'efforts peut prendre des mois et demander beaucoup de travail.

D'un autre côté, le conseiller juridique d'une organisation peut recommander une extrême prudence et suggérer d'arrêter les activités de traçage et qu'un intrus ferme le système. En soi, cela ne peut pas fournir de protection contre la responsabilité, et peut empêcher les enquêteurs d'identifier l'agresseur.

L'équilibre entre le soutien aux activités d'investigation et la limitation de responsabilité est délicat ; il faudra que vous preniez en compte les avis de votre conseiller juridique et les dommages que cause l'intrus (s'il y en a) lorsque vous prendrez votre décision sur ce qu'il convient de faire lors d'un incident particulier.

Votre conseiller juridique devrait aussi être impliqué dans toute décision de contacter des agences d'investigation lorsqu'un incident survient sur votre site. La décision de coordonner les efforts avec des agences d'investigation est celle de votre site ou organisation en propre. Impliquer votre conseiller juridique entretiendra la coordination multi niveau entre votre site et l'agence d'investigation particulière impliquée, ce qui ensuite résultera en une efficace division du travail. Un autre résultat est que vous obtiendrez vraisemblablement des conseils qui vous éviteront des erreurs juridiques à l'avenir.

Finalement, votre conseiller juridique devrait évaluer les procédures écrites de votre site pour répondre aux incidents. Il est essentiel d'obtenir un "bulletin de santé" d'un point de vue juridique avant de se lancer réellement dans ces procédures.

Il est vital, quand on traite avec des agences d'investigation, de vérifier que la personne qui appelle pour demander des informations est un représentant légitime de l'agence en question. Malheureusement, de nombreuses personne bien intentionnées ont sans le savoir laissé échapper des détails sensibles sur des incidents, permettant à des personnes non autorisées d'entrer dans leurs systèmes, etc., parce qu'un correspondant s'est présenté comme un représentant d'une agence gouvernementale. (Note : cet appel à la prudence s'applique en fait à tous les contacts externes.)

Une considération similaire est d'utiliser un moyen de communication sécurisé. Comme de nombreux attaquants de réseau peuvent facilement réacheminer la messagerie électronique, éviter d'utiliser la messagerie électronique pour communiquer avec d'autres agences (ainsi qu'avec d'autres pour traiter de l'incident). Les lignes téléphoniques non sécurisées (les téléphones utilisés normalement dans le monde des affaires) sont des cibles fréquentes d'écoutes illégales par les intrus sur les réseaux, aussi, soyez vigilants !

Il n'y a pas d'ensemble de règles établi pour répondre à un incident lorsque l'administration locale y est impliquée. Normalement (aux U.S.A) sauf par décision de justice, aucune agence ne peut vous forcer à surveiller un attaquant présumé, à le déconnecter du réseau, à éviter les contacts téléphoniques avec lui, etc. Chaque organisation aura un ensemble local et national de lois et règlements auquel il devra se tenir lors du traitement des incidents. Il est recommandé que chaque site soit familiarisé avec ces lois et règlements, et identifie et prenne contact avec les agences de sa juridiction bien en avance du traitement d'un incident.

5.2.3 Équipes de traitement des incidents de sécurité informatique

Il y a actuellement un certain nombre d'équipes de réponse aux incidents de la sécurité informatique (CSIRT) comme le centre de coordination CERT, le DFN-CERT allemand, et d'autres équipes dans le monde. Des équipes existent pour de nombreuses agences gouvernementales majeures et de grandes entreprises. Si une telle équipe est disponible, lui notifier l'incident devrait être une des principales tâches à considérer durant les premières étapes d'un incident. Ces équipes sont responsables de la coordination des incidents de sécurité informatique sur une large gamme de sites et d'entités plus grandes. Même si l'incident semble circonscrit au sein d'un seul site, il est possible que les informations disponibles à travers une équipe de réponse puissent aider à résoudre pleinement l'incident.

Si il est déterminé que l'intrusion est due à une faute dans le matériel ou le logiciel du système, le fabricant (ou le fournisseur) et une équipe de traitement des incidents de sécurité informatique devrait en être informés le plus tôt possible. Ceci est particulièrement important parce que de nombreux autres systèmes sont vulnérables, et ces organisations de fabricants et d'équipes de réponse peuvent aider à communiquer l'aide aux autres sites affectés.

En établissant une politique de site pour le traitement des incidents, il peut être souhaitable de créer un sous groupe, un peu comme ces équipes qui existent déjà, qui sera chargé de traiter les incidents de sécurité pour le site (ou l'organisation). Si une telle équipe est créée, il est essentiel d'ouvrir des lignes de communication entre cette équipe et les autres équipes. Une fois qu'un incident est en cours, il est difficile d'ouvrir un dialogue de confiance avec d'autres équipes s'il n'en existait pas auparavant.

5.2.4 Sites affectés et impliqués

Si un incident a un impact sur d'autres sites, il est de bon ton de les en informer. Il peut être évident depuis le début que l'incident n'est pas limité au site local, ou cela peut n'apparaître qu'après analyse.

Chaque site peut choisir de contacter directement les autres sites ou de passer les informations à une équipe appropriée de réponse aux incidents. Il est souvent très difficile de trouver le POC responsable sur des sites distants et l'équipe de réponse aux incidents sera capable de faciliter le contact en utilisant les canaux déjà établis.

Les questions juridiques et de responsabilité qui naissent d'un incident de sécurité vont différer d'un site à l'autre. Il est important de définir une politique pour le partage et l'enregistrement des informations sur les autres sites avant que ne survienne un incident.

Les informations sur les personnes spécifiques sont particulièrement sensibles, et peuvent être soumises à des lois sur la confidentialité. Les problèmes dans ce domaine, les informations non pertinentes, devraient être supprimés et une déclaration sur la façon de traiter les informations restantes devrait être incluse. Une déclaration claire de la façon dont ces informations sont à utiliser est essentielle. Aucun de ceux qui informent un site sur un incident de sécurité ne veut lire cela dans la presse publique. Les équipes de réponse aux incidents sont utiles à cet égard. Lorsqu'elles passent les informations aux POC responsables, elles sont capables de protéger l'anonymat de leur source. Mais, soyez conscients que, dans de nombreux cas, l'analyse des enregistrements et des informations des autres sites va révéler les adresses de votre site.

Tous les problèmes exposés ci-dessus ne devraient pas être pris comme prétexte pour ne pas impliquer d'autres sites. En fait, l'expérience des équipes existantes révèle que la plupart des sites informés de problèmes de sécurité ne savent même pas que leur propre site a été compromis. Sans informations en temps et en heure, les autres sites sont souvent incapables de faire quoi que ce soit contre les intrus.

5.2.5 Communications internes

Il est crucial durant un incident majeur de communiquer les raisons de certaines actions, et ce que l'on attend du comportement des utilisateurs (ou départements de l'entreprise). En particulier, il devrait apparaître très clairement aux utilisateurs ce qu'il leur est permis de dire et ne pas dire à l'extérieur (y compris aux autres départements). Par exemple, il ne serait pas bon pour une organisation que les utilisateurs répondent aux consommateurs quelque chose comme, "Je suis désolé, les systèmes sont en panne, nous avons eu une intrusion et nous essayons de nettoyer tout cela." Il serait préférable qu'ils aient des instructions pour répondre par une déclaration préparée du style, "Désolé que notre système soit indisponible, nous effectuons de la maintenance pour un meilleur service à l'avenir."

Les communications avec les consommateurs et les partenaires contractuels devraient être traités d'une façon intelligente mais sensible. On peut préparer les principales questions en établissant une liste de contrôle. Lorsque survient un incident, la liste de contrôle peut être utilisée avec l'ajout d'une phrase ou deux pour les circonstances spécifiques de l'incident.

Les départements de relations publiques peuvent être d'une grande aide durant les incidents. Ils devraient être impliqués dans tout le planning et peuvent fournir des réponses bien construites à utiliser lors des contacts avec les départements et organisations extérieures si nécessaire.

5.2.6 Relations publiques – communiqués de presse

Il y a eu une croissance phénoménale de la couverture média consacrée aux incidents de sécurité informatique aux États Unis. Une telle couverture de presse va s'étendre aux autres pays avec la croissance de l'Internet et son expansion internationale. Les lecteurs de pays où une telle attention des médias ne s'est pas encore produite peuvent tirer parti de l'expérience des U.S.A et devraient en être avertis et s'y préparer.

Une des questions les plus importantes à considérer est quand, qui et que livrer au grand public à travers la presse. Il y a de nombreuses questions à prendre en compte lors de la prise de décision sur ce sujet particulier. D'abord et avant tout, si un bureau de relations publiques existe pour le site, il est important d'utiliser ce bureau comme liaison avec la presse. Le bureau de relations publiques est entraîné au type et à la formulation des informations à livrer, et il aidera à s'assurer que l'image du site est protégée durant et après l'incident (si possible). Un bureau de relations publiques a l'avantage que vous pouvez communiquer en toute candeur avec lui, et il fait un tampon entre l'attention constante de la presse et le besoin du POC de garder le contrôle sur l'incident.

Si aucun bureau de relations publiques n'est disponible, les informations livrées à la presse doivent être pesées avec soin. Si l'information est sensible, il peut être avantageux de ne fournir que les informations minimales ou générales à la presse. Il est tout à fait possible que toute information fournie à la presse soit rapidement connue de l'auteur de l'incident. Notez aussi que mentir à la presse peut avoir un choc en retour et causer plus de dommages que de livrer des informations sensibles.

Alors qu'il est difficile de déterminer à l'avance quel niveau de détail fournir à la presse, voici quelques lignes directrices pour garder présent à l'esprit de :

(1) Rester au niveau minimum sur les détails techniques. Des informations détaillées sur l'incident peuvent fournir suffisamment d'informations à d'autres pour lancer des attaques similaires sur d'autres sites, ou même endommager la capacité du site à poursuivre le coupable après la fin de l'événement.
(2) Ne faire aucune spéculation dans les déclarations à la pesse. Les spéculations sur la cause de l'incident ou ses motifs seront très vraisemblablement erronées et peuvent causer une aggravation de l'incident.
(3) Travailler avec les professionnels de l'application de la loi pour s'assurer de la protection des preuves. Si des poursuites sont engagées, s'assurer que les preuves collectées ne sont pas divulguées à la presse.
(4) Essayez de ne pas être forcés à une conférence de presse avant d'y être prêt. La presse populaire est réputée pour ses interviews impromptues, où l'objectif est de faire baisser la garde de l'interviewé et obtenir des informations non disponibles autrement.
(5) Ne pas permettre à l'attention de la presse de dénigrer le traitement de l'événement. Toujours se souvenir que la réussite de la clôture d'un incident est d'une importance première.

5.3 Identification d'un incident

5.3.1 Est-il réel ?

Cette étape implique de déterminer si un problème existe réellement. Bien sûr, de nombreux signes, sinon la plupart, souvent associés à une infection par un virus, à des intrusions dans un système, à des utilisateurs malveillants, etc., sont simplement des anomalies comme des défaillances d'un matériel ou un comportement suspect de système/utilisateur. Pour aider à identifier s'il y a réellement un incident, il est habituellement utile d'obtenir et utiliser tout logiciel de détection disponible. Les informations d'audit sont aussi extrêmement utiles, particulièrement pour déterminer s'il y a une attaque du réseau. Il est extrêmement important d'obtenir une photographie du système aussitôt qu'on soupçonne que quelque chose ne va pas. De nombreux incidents causent l'apparition d'une chaîne dynamique d'événements, et une photographie du système initial peut être l'outil le plus précieux pour identifier le problème et la source d'une attaque. Enfin, il est important de lancer un registre logiciel. Enregistrer les événements du système, les conversations téléphoniques, les horodatages, etc., peut conduire à une identification plus rapide et systématique du problème, et c'est la base des étapes suivantes du traitement de l'incident.

Certaines indications ou "symptômes" d'un incident méritent une attention particulière :

(1) Pannes du système.
(2) De nouveaux comptes d'utilisateur (le compte RUMPLESTILTSKIN a été créé de façon inattendue), ou une activité élevée sur des comptes précédemment à faible utilisation.
(3) De nouveaux fichiers (habituellement avec des noms de fichier originaux ou étranges, comme data.xx ou k ou .xx).
(4) Désaccord de comptabilité (dans un système UNIX, vous pourriez remarquer le rétrécissement d'un fichier de comptabilité appelé /usr/admin/lastlog, ce qui devrait vous faire suspecter qu'il pourrait y avoir un intrus).

(5) Des changements de longueur de fichiers ou de dates (un utilisateur devrait se méfier si des fichiers .EXE dans un ordinateur en MS DOS ont crû inexplicablement au-dessus de 1800 octets).
(6) Des tentatives pour écrire sur un système (un gestionnaire de système remarque qu'un utilisateur privilégié d'un système VMS tente de modifier RIGHTSLIST.DAT).
(7) Des modifications ou suppressions de données (des fichiers commencent à disparaître).
(8) Des dénis de service (un gestionnaire de système et tous les autres utilisateurs sont bloqués dans un système UNIX, qui passe en mode d'utilisateur unique).
(9) Faibles performances du système, inexplicables
(10) Anomalies ("GOTCHA" est affiché sur la console ou il y a de fréquents "beeps" inexpliqués).
(11) Sondages suspects (il y a de nombreux échecs de tentatives de connexion provenant d'un autre nœud).
(12) Survols suspects (quelqu'un devient un utilisateur racine sur un système UNIX et accède aux fichiers les uns après les autres sur de nombreux comptes d'utilisateur.)
(13) Incapacité d'un utilisateur à se connecter suite à des modifications de son compte.

Cette liste n'est en aucun cas complète, nous avons juste fait une liste d'un certain nombre d'indicateurs courants. Le mieux est de collaborer avec les autres personnels de sécurité technique et informatique pour prendre une décision en groupe afin de savoir si un incident survient.

5.3.2 Types et portée des incidents

L'évaluation de la portée et de l'impact du problème va de pair avec l'identification de l'incident. Il est important d'identifier correctement les limites de l'incident afin de le traiter efficacement et de donner les priorités convenables aux réponses.

Afin d'identifier la portée et l'impact, un ensemble de critères appropriés au site devraient être définis ainsi que le type de connexions disponibles. Parmi les questions figurent :
(1) Est-ce un incident multisite ?
(2) Y a t'il plusieurs ordinateurs de votre site affectés par cet incident ?
(3) Des informations sensibles sont-elles impliquées ?
(4) Quel est le point d'entrée de l'incident (réseau, ligne téléphonique, terminal local, etc.) ?
(5) La presse est-elle impliquée ?
(6) Quel est le potentiel de dommages de l'incident ?
(7) Quel est le temps estimé pour clore l'incident ?
(8) Quelles ressources pourraient être nécessaires pour traiter l'incident ?
(9) L'application de la loi est-elle concernée ?

5.3.3 Évaluation des dommages et de leur étendue

L'analyse des dommages et l'étendue de l'incident peut prendre un certain temps, mais devrait conduire à une vue d'ensemble de la nature de l'incident, et aider les investigations et les poursuites. Aussitôt que l'infraction a été commise, le système tout entier et tous ses composants devraient être considérés comme suspects. Le logiciel de système est la cible la plus probable. La préparation est la clé de la capacité à détecter tous les changements dans un système éventuellement corrompu. Cela inclut de vérifier tous les supports à partir du fabricant en utilisant un algorithme résistant à l'altération (voir au paragraphe 4.3).

En supposant que le support de distribution original du fabricant soit disponible, une analyse de tous les fichiers système devrait commencer, et toutes les irrégularités devraient être notées et communiquées à toutes les parties impliquées dans le traitement de l'incident. Il peut être très difficile, dans certains cas, de décider quels supports de sauvegarde donnent un statut de système correct. Considérons, par exemple, que l'incident peut s'être poursuivi sur des mois ou des années avant d'être découvert, et le suspect peut être un employé du site, ou avoir autrement une connaissance intime des systèmes ou de leurs accès. Dans tous les cas, la préparation avant l'incident va déterminer quelle récupération est possible.

Si le système prend en charge la centralisation des connexions (la plupart le font), retournez aux journaux d'enregistrement et recherchez les anomalies. Si la comptabilité des processus et des temps de connexion est activée, recherchez les schémas d'utilisation du système. Dans une moindre mesure, l'utilisation des disques peut donner un éclairage sur l'incident. La comptabilité peut fournir des informations très utiles dans une analyse d'un incident et des poursuites ultérieures. Votre capacité à traiter tous les aspects d'un incident spécifique dépend fortement du succès de cette analyse.

5.4 Traitement d'un incident

Certaines étapes sont nécessaires durant le traitement d'un incident. Dans toutes les activités qui se rapportent à la sécurité, le point le plus important est que tous les sites devraient avoir leur politique. Sans politiques et buts définis, les entreprises resteront sans objectif. Les buts de guerre devraient être définis à l'avance par la direction et le conseiller juridique.

Un des objectifs les plus fondamentaux est de restaurer le contrôle des systèmes affectés et de limiter l'impact et les dommages. Dans le scénario du pire cas, la fermeture du système, ou la déconnexion du système du réseau, peut être la seule solution pratique.

Comme les activités impliquées sont complexes, essayez d'obtenir autant d'aide que nécessaire. Pendant que vous essayez de résoudre seul le problème, des dommages réels pourraient survenir à cause du délai ou du manque d'informations. La plupart des administrateurs prennent la découverte d'un intrus comme un défi personnel. En procédant de cette façon, les autres objectifs retenus dans les politiques locales peuvent ne pas toujours être pris en compte. Essayer d'attraper les intrus peut avoir une priorité très faible, par exemple par rapport à l'intégrité du système. Surveilles l'activité d'un pirate est utile, mais on peut penser que cela ne vaut pas le risque que fait courir la poursuite de l'accès.

5.4.1 Types de notification et échange d'informations

Lorsque vous avez la confirmation de la présence d'un incident, le personnel approprié doit en être averti. Comment la notification est réalisée est très important pour conserver le contrôle sur l'événement à la fois d'un point de vue technique et émotionnel. Les circonstances devraient être décrites aussi en détail que possible, afin d'aider à une connaissance et une compréhension rapide du problème. Un grand soin devrait être apporté à la détermination des groupes auxquels des informations techniques détaillées sont données durant la notification. Par exemple, il est utile de passer cette sorte d'information à une équipe de traitement d'incident car ils peuvent vous aider en prodiguant d'utiles conseils pour l'éradication des faiblesses révélées dans un incident. D'un autre côté, mettre des connaissances critiques dans le domaine public (par exemple, via des groupes d'information USENET ou des listes de diffusion) fait potentiellement courir un risque d'intrusion à un grand nombre de systèmes. Il n'est pas valide de supposer que tous les administrateurs qui lisent un bulletin de groupe particulier ont accès au code source des systèmes d'exploitation, et peuvent même comprendre suffisamment bien un avis pour prendre les mesures adéquates.

Tout d'abord, toute notification au personnel local ou hors site doit être explicite. Cela exige que toute déclaration (par messagerie électronique, appel téléphonique, télécopie ou appel de personne, ou sémaphone) fournissant des informations sur l'incident soit claire, concise, et pleinement qualifiée. Lorsque vous notifiez aux autres qui vous aident à traiter un événement, un "écran de fumée" va seulement diviser les efforts et créer de la confusion. Si une division du travail est suggérée, il est utile de fournir les informations à chaque participant sur ce qui est accompli dans les autres groupes. Cela ne réduira pas seulement la duplication de l'effort, mais permettra aux gens qui travaillent sur des parties du problème de savoir où obtenir des informations pertinentes sur leur partie de l'incident.

Une autre considération importante lors de la communication sur l'incident est d'être factuel. Essayer de cacher des aspects de l'incident en fournissant des informations fausses ou incomplètes peut non seulement empêcher la réussite de la résolution de l'incident, mais aussi empirer la situation.

Le choix du langage utilisé quand on notifie l'incident aux gens peut avoir un profond effet sur la façon dont est reçue l'information. Quand on utilise des termes émotionnels ou incendiaires, on augmente le potentiel dommageable et les résultats négatifs de l'incident. Il est important de rester calme dans les communications à la fois écrites et orales.

Une autre considération est que tout le monde ne parle pas la même langue. De ce fait, des malentendus et des retards peuvent naître, en particulier s'il s'agit d'un incident multi national. Un autre problème international concerne les implications juridiques différentes d'un incident de sécurité et les différences culturelles. Cependant, les différences culturelles n'existent pas seulement entre les pays ; elles existent au sein du même pays, entre des groupes sociaux ou d'utilisateurs différents. Par exemple, un administrateur d'un système universitaire peut être très décontracté à l'égard de tentatives de connexion au système via telnet, mais l'administrateur d'un système militaire considèrera vraisemblablement la même action comme une attaque possible.

Une autre question associée au choix du langage est celle de la notification à des personnels non techniciens ou hors site. Il est important de décrire précisément l'incident sans générer d'alarme ou de confusion indues. Bien qu'il soit

plus difficile de décrire l'incident à un public non technique, c'est souvent plus important. Une description non technique peut être nécessaire pour la haute direction, la presse, ou les liaisons avec la police. L'importance de ces communications ne peut être sous estimée et peut faire la différence entre résoudre correctement l'incident ou l'escalade vers un niveau de dommages plus élevé.

Si une équipe de réponse aux incidents est impliquée, il peut être nécessaire de remplir un modèle d'échange d'informations. Bien que cela puisse sembler une charge supplémentaire et que cela rajoute un certain délai, cela aide l'équipe à agir sur cet ensemble minimum d'informations. L'équipe de réponse peut être capable de répondre à des aspects de l'incident dont l'administrateur local ignore tout ; si les informations sont données à quelqu'un d'autre, les informations minimales suivantes devraient être fournies :

(1) zone horaire des connexions, ... en GMT ou heure locale
(2) information sur le système distant, y compris les noms d'hôtes, les adresses IP et (peut-être) les identifiants d'utilisateur
(3) toutes les entrées de connexion pertinentes pour le site distant
(4) le type d'incident (ce qui est arrivé, pourquoi c'est préoccupant)

Si les informations locales (c'est-à-dire, les identifiants d'utilisateur locaux) sont inclus dans les entrées de connexions, il sera nécessaire de purger les entrées avant, pour éviter les questions de confidentialité. En général, toutes les informations qui peuvent aider un site distant à résoudre un incident devraient être communiquées, sauf si les politiques locales l'interdisent.

5.4.2 Protection des preuves et enregistrements d'activités

Quand vous répondez à un incident, documentez tous les détails relatifs à l'incident. Cela donnera des informations précieuses à vous-même et aux autres lorsque vous essayerez de remonter le cours des événements. Documenter tous les détails vous fera finalement gagner du temps. Si vous ne notez pas tous les appels téléphoniques pertinents, par exemple, vous allez vraisemblablement oublier une portion significative des informations que vous avez obtenues, ce qui vous obligera à contacter à nouveau la source des informations. En même temps, l'enregistrement des détails vous fournira des preuves pour les poursuites, au cas où l'affaire évoluerait dans cette direction. Documenter un incident vous aidera aussi à effectuer une évaluation finale des dommages (ce que votre direction aussi bien que la police, voudra savoir), et vous fournira une base pour les phases ultérieures du processus de traitement : éradication, récupération et suites à donner une fois la "leçon reçue."

Durant les phases initiales d'un incident, il est souvent impossible de déterminer si des poursuites sont viables, de sorte que vous devriez documenter comme si vous rassembliez des preuves pour la justice. Au minimum, vous devrez noter :

(1) tous les événements du système (enregistrements d'audit)
(2) toutes les actions entreprises (horodatées)
(3) toutes les conversations externes (y compris la personne à qui vous avez parlé, la date et l'heure et le contenu de la conversation)

La façon la plus directe de tenir la documentation est d'avoir un recueil de journalisation. Cela vous permet d'aller à une source d'informations centralisée, chronologique, quand vous en avez besoin, sans qu'il vous soit nécessaire de feuilleter des pages de papier. La plus grande partie de ces informations sont des preuves potentielles devant une cour de justice. Et donc, lorsque les suites judiciaires sont une possibilité, on devrait suivre les procédures préparées et éviter de couler les suites judiciaires par un traitement impropre des preuves possibles. Si c'est approprié, les étapes ci-après peuvent être suivies :

(1) Faire régulièrement (par exemple, chaque jour) des photocopies signées de votre recueil de journalisation (ainsi que des supports que vous utilisez pour enregistrer les événements système) auprès d'un archiviste.
(2) L'archiviste devrait conserver ces copies dans un lieu sécurisé (par exemple, un coffre-fort).
(3) Quand vous remettez les informations à l'archivage, vous devriez recevoir un récépissé signé et daté de l'archiviste.

Manquer à observer ces procédures peut déboucher devant une juridiction sur une invalidation de toutes les preuves que vous avez obtenues.

5.4.3 Confinement

L'objet du confinement est de limiter l'extension d'une attaque. Une partie essentielle du confinement est la prise de décision (par exemple, se déterminer à fermer un système, à déconnecter du réseau, à surveiller une activité système ou réseau, monter des pièges, désactiver des fonctions comme le transfert de fichiers, etc.).

Parfois, cette décision est triviale ; fermer le système si les informations sont secrètes, sensibles, ou protégées par un brevet. Gardez en mémoire que fermer tous les accès pendant qu'un incident est en cours est une notification évidente à tous les utilisateurs, y compris les utilisateurs auteurs du problème, que les administrateurs sont au courant d'un problème ; cela peut avoir un effet délétère sur les investigations. Dans certains cas, il est prudent de fermer tous les accès ou toutes les fonctions aussitôt que possible, puis de restaurer le fonctionnement normal par étapes limitées. Dans d'autres cas, il vaut mieux courir le risque de quelques dommages au système si garder le système ouvert peut vous permettre d'identifier un intrus.

Cette étape devrait impliquer la mise en application de procédures prédéterminées. Votre organisation ou site devrait, par exemple, définir des risques acceptables dans le traitement d'un incident, et devrait prescrire des actions et stratégies spécifiques en conséquence. Ceci est particulièrement important lorsqu'une décision rapide est nécessaire et qu'il n'est pas possible de contacter d'abord toutes les parties impliquées pour discuter de la décision. En l'absence de procédures prédéfinies, la personne en charge de l'incident va souvent n'avoir pas le pouvoir de prendre des décisions de gestion difficiles (comme de perdre les résultats d'une expérience coûteuse en fermant un système). Une activité finale qui devrait survenir durant cette étape du traitement de l'incident est la notification aux autorités appropriées.

5.4.4 Éradication

Une fois l'incident confiné, il est temps d'éradiquer la cause. Mais avant d'éradiquer la cause, il faut apporter grand soin à la collecte de toutes les informations nécessaires sur le ou les systèmes compromis et la cause de l'incident parce qu'elles seront vraisemblablement perdues lors du nettoyage du système.

Des logiciels peuvent être disponibles pour vous aider dans le processus d'éradication, comme les logiciels anti-virus. Si des fichiers bogués ont été créés, archivez les avant de les détruire. Dans les cas d'infections virales, il est important de nettoyer et reformater tout support contenant des fichiers infectés. Finalement, assurez vous que toutes les sauvegardes sont propres. De nombreux systèmes infectés par des virus deviennent périodiquement réinfectés simplement parce que les gens n'ont pas systématiquement éradiqué le virus des sauvegardes. Après l'éradication, il faudrait faire une nouvelle sauvegarde.

Réparer toutes les faiblesses après qu'un incident soit survenu est difficile. La clé de la réparation des faiblesses est la connaissance et la compréhension de la rupture des défenses.

Il peut être nécessaire de revenir au support de distribution original et de repersonnaliser le système. Pour faciliter ce scénario de plus mauvais cas, un enregistrement du réglage d'origine du système et chaque changement de personnalisation devraient être conservés. Dans le cas d'une attaque fondée sur le réseau, il est important d'installer des pansements pour chaque faiblesse du système d'exploitation qui a été exploitée *(par l'attaque)*.

Comme exposé au paragraphe 5.4.2, un enregistrement de sécurité peut être des plus précieux durant cette phase de réparation des faiblesses. Les enregistrements qui montrent comment l'incident a été découvert et confiné peuvent être utilisés ultérieurement pour aider à déterminer comment s'étendent les dommages à partir d'un incident donné. Les étapes suivies peuvent être utilisées à l'avenir pour s'assurer que le problème ne refait pas surface. Dans l'idéal, on devait automatiser et appliquer régulièrement les mêmes essais qu'utilisés pour détecter l'incident de sécurité.

Si une faiblesse particulière est isolée comme ayant été exploitée, l'étape suivante est de trouver un mécanisme pour protéger votre système. Les listes de diffusion et bulletins de sécurité seraient un bon endroit où chercher ces informations, et vous pouvez y obtenir de bons conseils de la part des équipes de réponse aux incidents.

5.4.5 Récupération

Une fois que la cause d'un incident a été éradiquée, la phase de récupération définit la prochaine étape d'action. Le but de la récupération est de ramener le système à la normale. En général, offrir à nouveau les services à la demande pour minimiser les inconvénients subis par l'utilisateur est le mieux à faire. Comprenez que les bonnes procédures de récupération pour le système sont extrêmement importantes et devraient être spécifiques du site.

5.4.6 Suivi

Une fois que vous pensez qu'un système a été restauré dans un état "sûr", il est toujours possible que des trous, et même des pièges, restent tapis dans le système. Une des plus importantes étapes de la réponse aux incidents est aussi la

plus souvent omise, l'étape de suivi. Dans l'étape de suivi, le système devrait être surveillé sur des éléments qui pourraient avoir été omis durant l'étape de nettoyage. Il serait prudent d'utiliser un des outils mentionnés à la section 7 comme point de départ. Rappelez vous que ces outils ne remplacent pas la surveillance constante du système et les bonnes pratiques de gestion des systèmes.

L'élément le plus important de l'étape de suivi est d'effectuer une analyse post mortem. Qu'est-il arrivé exactement, et à quelle heure ? Comment s'est comporté le personnel impliqué dans l'incident ? De quelles informations le personnel a t'il besoin rapidement et par quel moyen peuvent ils obtenir ces informations aussitôt que possible? Que devrait faire différemment le personnel la prochaine fois ?

Après un incident, il est prudent d'écrire un rapport décrivant la séquence exacte des événements : la méthode de découverte, la procédure de correction, la procédure de surveillance, et un résumé des leçons tirées. Cela vous aidera à une claire compréhension du problème. Créer une chronologie formelle des événements (y compris les horodatages) est aussi important pour les raisons judiciaires.

Un rapport de suivi est précieux pour de nombreuses raisons. Il donne une référence à utiliser en cas d'incidents similaires. Il est aussi important pour, aussi vite que possible, obtenir une estimation financière du montant des dommages causés par l'incident. Cette estimation devrait inclure les coûts associés à toutes les pertes de logiciels et de fichiers (en particulier la valeur des données protégées de l'entreprise qui pourraient avoir été divulguées), les dommages matériels, les coûts de main d'œuvre pour restaurer les fichiers altérés, reconfigurer les systèmes affectés, et ainsi de suite. Cette estimation peut devenir la base des poursuites judiciaires ultérieures. Le rapport peut aussi aider à justifier vis à vis de la direction un effort en faveur de la sécurité informatique dans l'organisation.

5.5 L'après incident

Plusieurs actions devraient prendre leur place dans le sillage d'un incident. Ces actions peuvent être résumées de la façon suivante :

(1) On devrait effectuer un inventaire des actifs du système (c'est-à-dire, un examen soigneux devrait déterminer comment le système a été affecté par l'incident).
(2) Les leçons reçues au titre de l'incident devraient être incluses dans un plan de sécurité révisé pour empêcher le retour d'un tel incident.
(3) Une nouvelle analyse de risque devrait être développée à la lumière de l'incident.
(4) Une enquête et des poursuites judiciaires sur les individus qui ont causé l'incident devraient être lancées, si cela est jugé souhaitable.

Si un incident est fondé sur une mauvaise politique, et si la politique n'est pas changée, le passé est voué à se répéter. Une fois qu'un site a récupéré d'un incident, la politique et les procédures du site devraient être révisées pour accompagner les changements destinés à empêcher des incidents similaires. Même en l'absence d'un incident, il serait prudent de réviser régulièrement les politiques et les procédures. Les révisions sont impératives de nos jours à cause des changements d'environnements informatiques.

L'objet de ce processus post mortem est d'améliorer toutes les mesures de sécurité afin de protéger le site contre les futures attaques. En résultat d'un incident, un site ou organisation devrait acquérir une connaissance pratique fondée sur l'expérience. Un objectif concret de l'examen post mortem est de développer de nouvelles méthodes proactives. Une autre facette importante de l'après incident peut être l'éducation des utilisateurs et des administrateurs pour empêcher le retour de problèmes de sécurité.

5.6 Responsabilités

5.6.1 Ne pas franchir la ligne jaune

Une chose est de protéger son propre réseau, une autre est de supposer qu'on devrait protéger les réseaux des autres. Durant le traitement d'un incident vont devenir apparentes certaines faiblesses systèmiques de vos propres systèmes et aussi des systèmes des autres. Il est assez facile et peut même être tentant de partir à la chasse aux intrus et de les traquer. Gardez en mémoire qu'à un certain point il est possible de "franchir la ligne," et, avec les meilleures intentions du monde, ne pas se conduire mieux que les intrus.

En matière de propriété, la meilleure règle est de ne pas utiliser les facilités des sites distants qui ne sont pas publics. Cela exclut clairement toute entrée sur un système (comme une «remote shell» ou une session de connexion) qui n'est pas expressément permise. Il peut être très tentant après la découverte d'une infraction à la sécurité, pour un administrateur de système qui a les moyens de "faire le suivi", de s'assurer des dommages qui ont été causés au site distant. Ne le faites pas ! Essayez plutôt de joindre le point de contact approprié du site affecté.

5.6.2 La bonne citoyenneté Internet

Durant un incident de sécurité, on peut choisir entre deux solutions. D'abord, un site peut choisir d'observer l'intrus dans l'espoir de la capturer ; ou bien, le site peut tout nettoyer après l'incident et bloquer l'accès de l'intrus aux systèmes. C'est une décision qui doit être prise après mure réflexion car il peut y avoir des suites de responsabilité juridique si vous choisissez de laisser votre site ouvert, sachant qu'un intrus utilise votre site comme base de lancement pour ses attaques contre les autres sites. Être un bon citoyen de l'Internet signifie que vous devriez essayer d'alerter les autres sites qui pourraient avoir été touchés par l'intrus. Ces sites affectés peuvent être facilement découverts d'après un examen séré de vos fichiers de journalisation.

5.6.3 Réponse administrative aux incidents

Lorsque un incident de sécurité implique un utilisateur, la politique de sécurité du site devrait décrire quelle action doit être entreprise. La transgression devrait être prise au sérieux, mais il est très important d'être sûr du rôle joué par l'utilisateur. L'utilisateur est il innocent ? Se trompe t-on en attribuant l'infraction à la sécurité à l'utilisateur ? Appliquer une action administrative qui suppose que l'utilisateur a intentionnellement causé l'incident peut n'être pas approprié pour un utilisateur qui a seulement commis une erreur. Il peut être approprié d'inclure des sanctions plus adaptées à une telle situation dans votre politique (par exemple, éducation ou réprimande d'un utilisateur) en plus de mesures plus sévères pour les actes intentionnels d'intrusion et de détournement de système.

6 Poursuite des activités

À ce moment, votre site a fort heureusement développé une politique de sécurité complète et a développé des procédures pour assister la configuration et la gestion de votre technologie de prise en charge de ces politiques. Que ce serait agréable de pouvoir se renverser dans son fauteuil et de se détendre en songeant que le travail de mise en sécurité est terminé. Malheureusement, ce n'est pas possible. Vos systèmes et vos réseaux ne sont pas un environnement statique, de sorte qu'il est nécessaire de réviser régulièrement les politiques et les procédures. Vous pouvez suivre un certain nombre d'étapes pour vous aider à garder le contact avec les changements qui se produisent autour de vous de sorte que vous puissiez initier les actions correspondantes pour faire face à ces changements. Ce qui suit est un ensemble de départ auquel vous pourrez ajouter en fonction de ce qui convient à votre site.

(1) Suivre les conseils qui sont donnés par les diverses équipes de réponse aux incidents de sécurité, comme ceux du centre de coordination du CERT, et mettre à jour vos systèmes contre les menaces qui s'appliquent à la technologie de votre site.
(2) Surveiller les solutions de sécurité produites par le fabricant de vos équipements et vous procurer et installer tout ce qui s'applique.
(3) Surveiller activement les configurations de vos systèmes pour identifier tout changement qui pourrait survenir, et enquêter sur toutes les anomalies.
(4) Réviser annuellement (au minimum) toutes les politiques et procédures de sécurité.
(5) Lire les diffusions de message et les groupes de discussion USENET pertinents pour vous tenir à jour des dernières informations partagées par vos collègues administrateurs.
(6) Vérifier régulièrement la conformité aux politiques et procédures. Cet audit devrait être effectué par quelqu'un d'autre que les gens qui définissent ou mettent en œuvre les politiques et procédures.

7 Outils et localisations

La présente section donne une brève liste des technologies de sécurité disponibles au public, qui peuvent être téléchargées à partir de l'Internet. Beaucoup des éléments décrits ci-dessous sont indubitablement dépassés ou rendus obsolètes depuis la publication de ce document.

Certains des outils mentionnés sont des applications comme des programmes d'utilisateur final (clients) et leur infrastructure de prise en charge de système (serveur) qu'un utilisateur général ne verra ni n'utilisera jamais, mais qui peuvent être utilisés par les applications, ou par les administrateurs pour dépanner les problèmes de sécurité ou se garder contre les intrus.

Un triste fait est qu'il y a très peu d'applications disponibles qui prennent consciemment en compte la sécurité. Cela est principalement causé par le besoin d'une infrastructure de sécurité préalable pour la plupart des applications afin de fonctionner en toute sécurité. Un effort considérable a lieu actuellement pour construire cette infrastructure pour que les applications puissent tirer parti de communications sécurisées.

La plupart des outils et applications décrits ci-dessous se trouvent dans un des sites d'archive suivants :
(1) CERT Coordination Center ftp://info.cert.org:/pub/tools
(2) DFN-CERT ftp://ftp.cert.dfn.de/pub/tools/
(3) Computer Operations, Audit, and Security Tools (COAST) coast.cs.purdue.edu:/pub/tools

Il est important de noter que de nombreux sites, y compris CERT et COAST sont imités partout sur l'Internet. Soyez vigilants en utilisant un site miroir "bien connu" pour restituer un logiciel, et en utilisant des outils de vérification (md5, sommes de contrôle, etc.) pour valider ce logiciel. Un pirate habile peut faire de la publicité pour des logiciels de sécurité qu'il a intentionnellement conçus pour fournir l'accès aux données ou systèmes.

Outils

COPS
DES
Drawbridge
identd (pas réellement un outil de sécurité)
ISS
Kerberos
logdaemon
lsof
MD5
PEM
PGP
rpcbind/portmapper replacement
SATAN
sfingerd
S/KEY
smrsh
ssh
swatch
TCP-Wrapper
tiger
Tripwire*
TROJAN.PL

8 Listes de diffusion et autres ressources

Il serait impossible de faire la liste de toutes les listes de diffusion et des autres ressources qui traitent de sécurité des sites. Cependant, il y a quelques "points de rebond" par lesquels le lecteur peut commencer. Toutes ces références sont pour le monde "INTERNET". Des ressources plus spécifiques (par fabricant et par zone géographique) peuvent être trouvées à travers ces références.

Listes de diffusion

(1) conseil du CERT(TM)
Envoyer un message à : cert-advisory-request@cert.org
Corps du message : subscribe cert <FIRST NAME> <LAST NAME>

Un conseil du CERT fournit des informations sur la façon d'obtenir un remède ou des détails d'une solution de rechange pour un problème connu de sécurité informatique. Le centre de coordination du CERT travaille avec les fabricants pour produire une solution de rechange ou un remède pour un problème, et ne publie pas d'informations sur des faiblesses tant qu'une solution de rechange ou un remède n'est pas disponible. Un conseil du CERT peut aussi être un avertissement pour votre milieu au sujet d'attaques en cours (par exemple, "CA-91:18.Active.Internet.tftp.Attacks").

Les conseils du CERT sont aussi publiés dans les nouvelles de USENET :
comp.security.announce

Les archives de conseils du CERT sont disponibles via FTP anonyme à info.cert.org dans l'annuaire
/pub/cert_advisories.

(2) Listes de VIRUS-L
Envoyer un message à : listserv%lehiibm1.bitnet@mitvma.mit.edu
Corps du message : subscribe virus-L FIRSTNAME LASTNAME

VIRUS-L est une liste de diffusion contrôlée centrée sur les questions de virus informatiques. Pour des précisions, y compris une copie des lignes directrices du document, voir le fichier "virus-l.README", disponible par FTP anonyme auprès de cs.ucr.edu.

(3) Les pare-feu Internet
Envoyer un message à : majordomo@greatcircle.com
Corps du message : subscribe firewalls utilisateur@host

La liste de diffusion des pare-feu est un forum de discussion pour les administrateurs et développeurs de pare-feu.

USENET newsgroups

(1) comp.security.announce
Le groupe de discussion comp.security.announce est contrôlé et n'est utilisé que pour la distribution des conseils du CERT.

(2) comp.security.misc
comp.sécurité.misc est un forum pour la discussion de la sécurité informatique, en particulier celle qui se rapporte au système d'exploitation UNIX(r).

(3) alt.security
Le groupe de discussion alt.security est aussi un forum pour la discussion de la sécurité informatique, ainsi que d'autres questions comme le verrouillage des automobiles et les systèmes d'alarme.

(4) comp.virus
Le groupe de discussion comp.virus est un groupe de discussion contrôlé centré sur les questions de virus informatiques. Pour plus d'informations, y compris une copie des lignes directrices du groupe, voir le fichier "virus-l.README", disponible via FTP anonyme sur info.cert.org dans le répertoire /pub/virus-l.

(5) comp.risks
Le groupe de discussion comp.risks est un forum contrôlé sur les risques pour le public dans les systèmes informatiques et ce qui s'y rapporte.

Pages du World-Wide Web

(1) http://www.first.org/
Chambre de compensation des ressources de sécurité informatique *(Computer Security Resource Clearinghouse*). Son principal objet est l'information de réponse aux crises ; des informations sur les menaces relatives à la sécurité informatique, les faiblesses, et les solutions. En même temps, la Chambre de compensation s'efforce d'être un index général des informations de sécurité informatique sur une grande variété de sujets, y compris les risques généraux, la confidentialité, les questions juridiques, les virus, l'assurance, la politique, et la formation.

(2) http://www.telstra.com.au/info/security.html
Cet index de référence contient une liste des liens vers les sources d'informations sur la sécurité des réseaux et des ordinateurs. Il n'y a pas de correspondance implicite avec les outils, techniques et documents contenus dans ces archives. Nombre de ces éléments, sinon tous, fonctionnent bien, mais on ne peut pas garantir qu'il en sera ainsi. Ces informations sont seulement pour l'éducation et une utilisation légitime des techniques de la sécurité informatique.

(3) http://www.alw.nih.gov/Security/security.html
Cette page affiche des informations générales sur la sécurité informatique. Les informations sont organisées par source et chaque section est organisée par sujet. Les modifications récentes sont notées à la page What's New *(quoi de neuf)*.

(4) http://csrc.ncsl.nist.gov
Cette archive à la page Computer Security Resource Clearinghouse de l'Institut National des normes et de la technologie (NIST) contient un certain nombre d'annonces, de programmes, et de documents qui se rapportent à la

sécurité informatique.

* CERT et Tripwire sont des marques déposées auprès de l'Office américain des brevets et marques commerciales.

9 Références

Les références suivantes peuvent n'être pas disponibles dans tous les pays.

[Appelman, et. al., 1995] Appelman, Heller, Ehrman, White, and McAuliffe, "The Law and The Internet", USENIX 1995 Technical Conference on UNIX and Advanced Computing, New Orleans, LA, January 16-20, 1995.

[ABA, 1989] American Bar Association, Section of Science and Technology, "Guide to the Prosecution of Telecommunication Fraud by the Use of Computer Crime Statutes", American Bar Association, 1989.

[Aucoin, 1989] R. Aucoin, "Computer Viruses: Checklist for Recovery", Computers in Libraries, Vol. 9, No. 2, Pg. 4, February 1989.

[Barrett, 1996] D. Barrett, "Bandits on the Information Superhighway", O'Reilly & Associates, Sebastopol, CA, 1996.

[Bates, 1992] R. Bates, "Disaster Recovery Planning: Networks, Telecommunications and Data Communications", McGraw-Hill, 1992.

[Bellovin, 1989] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer Communication Review, Vol 19, 2, pp. 32-48, April 1989.

[Bellovin, 1990] S. Bellovin, and M. Merritt, "Limitations of the Kerberos Authentication System", Computer Communications Review, October 1990.

[Bellovin, 1992] S. Bellovin, "There Be Dragon", USENIX: Proceedings of the Third Usenix Security Symposium, Baltimore, MD. September 1992.

[Bender, 1894] D. Bender, "Computer Law: Evidence and Procedure", M. Bender, New York, NY, 1978-present.

[Bloombecker, 1990] B. Bloombecker, "Spectacular Computer Crimes", Dow Jones- Irwin, Homewood, IL. 1990.

[Brand, 1990] R. Brand, "Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery", R. Brand, 8 June 1990.

[Brock, 1989] J. Brock, "November 1988 Internet Computer Virus and the Vulnerability of National Telecommunications Networks to Computer Viruses", GAO/T-IMTEC-89-10, Washington, DC, 20 July 1989.

[BS 7799] British Standard, BS Tech Cttee BSFD/12, Info. Sec. Mgmt, "BS 7799 : 1995 Code of Practice for Information Security Management", British Standards Institution, London, 54, Effective 15 February 1995.

[Caelli, 1988] W. Caelli, Editor, "Computer Security in the Age of Information", Proceedings of the Fifth IFIP International Conference on Computer Security, IFIP/Sec '88.

[Carroll, 1987] J. Carroll, "Computer Security", 2nd Edition, Butterworth Publishers, Stoneham, MA, 1987.

[Cavazos and Morin, 1995] E. Cavazos and G. Morin, "Cyber-Space and The Law", MIT Press, Cambridge, MA, 1995.

[CCH, 1989] Commerce Clearing House, "Guide to Computer Law", (Topical Law Reports), Chicago, IL., 1989.

[Chapman, 1992] B. Chapman, "Network(In) Security Through IP Packet Filtering", USENIX: Proceedings of the Third UNIX Security Symposium, Baltimore, MD, September 1992.

[Chapman and Zwicky, 1995] B. Chapman and E. Zwicky, "Building Internet Firewalls", O'Reilly and Associates, Sebastopol, CA, 1995.

[Cheswick, 1990] B. Cheswick, "The Design of a Secure Internet Gateway", Proceedings of the Summer Usenix Conference, Anaheim, CA, June 1990.

[Cheswick1] W. Cheswick, "An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied", AT&T Bell Laboratories.

[Cheswick and Bellovin, 1994] W. Cheswick and S. Bellovin, "Les pare-feu and Internet Security: Repelling the Wily Hacker", Addison-Wesley, Reading, MA, 1994.

[Conly, 1989] C. Conly, "Organizing for Computer Crime Investigation and Prosecution", U.S. Dept. of Justice, Office of Justice Programs, Under Contract Number OJP-86-C-002, National Institute of Justice, Washington, DC, July 1989.

[Cooper, 1989] J. Cooper, "Computer and Communications Security: Strategies for the 1990s", McGraw-Hill, 1989.

[CPSR, 1989] Computer Professionals for Social Responsibility, "CPSR Statement on the Computer Virus", CPSR, Communications of the ACM, Vol. 32, No. 6, Pg. 699, June 1989.

[CSC-STD-002-85, 1985] Department of Defense, "Password Management Guideline", CSC-STD-002-85, 12 April 1985, 31 pages.

[Curry, 1990] D. Curry, "Improving the Security of Your UNIX System", SRI International Report ITSTD-721-FR-90-21, April 1990.

[Curry, 1992] D. Curry, "UNIX System Security: A Guide for Users and Systems Administrators", Addision-Wesley, Reading, MA, 1992.

[DDN88] Defense Data Network, "BSD 4.2 and 4.3 Software Problem Resolution", DDN MGT Bulletin #43, DDN Network Information Center, 3 November 1988.

[DDN89] DCA DDN Defense Communications System, "DDN Security Bulletin 03", DDN Security Coordination Center, 17 October 1989.

[Denning, 1990] P. Denning, Editor, "Computers Under Attack: Intruders, Worms, and Viruses", ACM Press, 1990.

[Eichin and Rochlis, 1989] M. Eichin, and J. Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988", Massachusetts Institute of Technology, February 1989.

[Eisenberg, et. al., 89] T. Eisenberg, D. Gries, J. Hartmanis, D. Holcomb, M. Lynn, and T. Santoro, "The Computer Worm", Cornell University, 6 February 1989.

[Ermann, Willians, and Gutierrez, 1990] D. Ermann, M. Williams, and C. Gutierrez, Editors, "Computers, Ethics, and Society", Oxford University Press, NY, 1990. (376 pages, includes bibliographical references).

[Farmer and Spafford, 1990] D. Farmer and E. Spafford, "The COPS Security Checker System", Proceedings of the Summer 1990 USENIX Conference, Anaheim, CA, Pgs. 165-170, June 1990.

[Farrow, 1991] Rik Farrow, "UNIX Systems Security", Addison-Wesley, Reading, MA, 1991.

[Fenwick, 1985] W. Fenwick, Chair, "Computer Litigation, 1985: Trial Tactics and Techniques", Litigation Course Handbook Series No. 280, Prepared for distribution at the Computer Litigation, 1985: Trial Tactics and Techniques Program, February-March 1985.

[Fites 1989] M. Fites, P. Kratz, and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.

[Fites, Johnson, and Kratz, 1992] Fites, Johnson, and Kratz, "The Computer Virus Crisis", Van Hostrand Reinhold, 2nd edition, 1992.

[Forester and Morrison, 1990] T. Forester, and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990.

[Foster and Morrision, 1990] T. Forester, and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990. (192 pages avec un index.)

[GAO/IMTEX-89-57, 1989] U.S. General Accounting Office, "Computer Security - Virus Highlights Need for Improved Internet Management", United States General Accounting Office, Washington, DC, 1989.

[Garfinkel and Spafford, 1991] S. Garfinkel, and E. Spafford, "Practical Unix Security", O'Reilly & Associates, ISBN 0-937175-72-2, May 1991.

[Garfinkel, 1995] S. Garfinkel, "PGP:Pretty Good Privacy", O'Reilly & Associates, Sebastopol, CA, 1996.

[Garfinkel and Spafford, 1996] S. Garfinkel and E. Spafford, "Practical UNIX and Internet Security", O'Reilly & Associates, Sebastopol, CA, 1996.

[Gemignani, 1989] M. Gemignani, "Viruses and Criminal Law", Communications of the ACM, Vol. 32, No. 6, Pgs. 669-671, June 1989.

[Goodell, 1996] J. Goodell, "The Cyberthief and the Samurai: The True Story of Kevin Mitnick-And The Man Who Hunted Him Down", Dell Publishing, 1996.

[Gould, 1989] C. Gould, Editor, "The Information Web: Ethical and Social Implications of Computer Networking", Westview Press, Boulder, CO, 1989.

[Greenia, 1989] M. Greenia, "Computer Security Information Sourcebook", Lexikon Services, Sacramento, CA, 1989.

[Hafner and Markoff, 1991] K. Hafner and J. Markoff, "Cyberpunk: Outlaws and Hackers on the Computer Frontier", Touchstone, Simon & Schuster, 1991.

[Hess, Safford, and Pooch] D. Hess, D. Safford, and U. Pooch, "A Unix Network Protocol Security Study: Network Information Service", Texas A&M University.

[Hoffman, 1990] L. Hoffman, "Rogue Programs: Viruses, Worms, and Trojan Horses", Van Nostrand Reinhold, NY, 1990. (384 pages, inclut des références bibliographiques et un index.)

[Howard, 1995] G. Howard, "Introduction to Internet Security: From Basics to Beyond", Prima Publishing, Rocklin, CA, 1995.

[Huband and Shelton, 1986] F. Huband, and R. Shelton, Editors, "Protection of Computer Systems and Software: New Approaches for Combating Theft of Software and Unauthorized Intrusion", Communications présentées à un atelier financé par la National Science Foundation, 1986.

[Hughes, 1995] L. Hughes Jr., "Actually Useful Internet Security Techniques", New Riders Publishing, Indianapolis, IN, 1995.

[IAB-RFC1087, 1989] Internet Activities Board, "Ethics and the Internet", RFC 1087, IAB, January 1989. Apparaît aussi dans les communications de l'ACM, Vol. 32, n° 6, page 710, juin 1989.

[Icove, Seger, and VonStorch, 1995] D. Icove, K. Seger, and W. VonStorch, "Computer Crime: A Crimefighter's Handbook", O'Reilly & Associates, Sebastopol, CA, 1995.

[IVPC, 1996] IVPC, "International Virus Prevention Conference '96 Proceedings", NCSA, 1996.

[Johnson and Podesta] D. Johnson, and J. Podesta, "Formulating A Company Policy on Access to and Use and Disclosure of Electronic Mail on Company Computer Systems".

[Kane, 1994] P. Kane, "PC Security and Virus Protection Handbook: The Ongoing War Against Information Sabotage", M&T Books, 1994.

[Kaufman, Perlman, and Speciner, 1995] C. Kaufman, R. Perlman, and M. Speciner, "Network Security: PRIVATE

Communication in a PUBLIC World", Prentice Hall, Englewood Cliffs, NJ, 1995.

[Kent, 1990] S. Kent, "E-Mail Privacy for the Internet: New Software and Strict Registration Procedures will be Implemented this Year", Business Communications Review, Vol. 20, No. 1, Pg. 55, 1 January 1990.

[Levy, 1984] S. Levy, "Hacker: Heroes of the Computer Revolution", Delta, 1984.

[Lewis, 1996] S. Lewis, "Disaster Recovery Yellow Pages", The Systems Audit Group, 1996.

[Littleman, 1996] J. Littleman, "The Fugitive Game: Online with Kevin Mitnick", Little, Brown, Boston, MA., 1996.

[Lu and Sundareshan, 1989] W. Lu and M. Sundareshan, "Secure Communication in Internet Environments: A Hierarchical Key Management Scheme for End-to-End Encryption", IEEE Transactions on Communications, Vol. 37, No. 10, Pg. 1014, 1 October 1989.

[Lu and Sundareshan, 1990] W. Lu and M. Sundareshan, "A Model for Multilevel Security in Computer Networks", IEEE Transactions on Software Engineering, Vol. 16, No. 6, Page 647, 1 June 1990.

[Martin and Schinzinger, 1989] M. Martin, and R. Schinzinger, "Ethics in Engineering", McGraw Hill, 2nd Edition, 1989.

[Merkle] R. Merkle, "A Fast Software One Way Hash Function", Journal of Cryptology, Vol. 3, No. 1.

[McEwen, 1989] J. McEwen, "Dedicated Computer Crime Units", Report Contributors: D. Fester and H. Nugent, Prepared for the National Institute of Justice, U.S. Department of Justice, by Institute for Law and Justice, Inc., under contract number OJP-85-C-006, Washington, DC, 1989.

[MIT, 1989] Massachusetts Institute of Technology, "Teaching Students About Responsible Use of Computers", MIT, 1985-1986. Republié aussi dans les communications de l'ACM, Vol. 32, n° 6, page 704, Athena Project, MIT, juin 1989.

[Mogel, 1989] Mogul, J., "Simple and Flexible Datagram Access Controls for UNIX-based Gateways", Digital Western Research Laboratory Research Report 89/4, March 1989.

[Muffett, 1992] A. Muffett, "Crack Version 4.1: A Sensible Password Checker for Unix"

[NCSA1, 1995] NCSA, "NCSA Firewall Policy Guide", 1995.

[NCSA2, 1995] NCSA, "NCSA's Corporate Computer Virus Prevention Policy Model", NCSA, 1995.

[NCSA, 1996] NCSA, "Firewalls & Internet Security Conference '96 Proceedings", 1996.

[NCSC-89-660-P, 1990] National Computer Security Center, "Guidelines for Formal Verification Systems", Shipping list no.: 89-660-P, The Center, Fort George G. Meade, MD, 1 April 1990.

[NCSC-89-254-P, 1988] National Computer Security Center, "Glossary of Computer Security Terms", Shipping list no.: 89-254-P, The Center, Fort George G. Meade, MD, 21 October 1988.

[NCSC-C1-001-89, 1989] Tinto, M., "Computer Viruses: Prevention, Detection, and Treatment", National Computer Security Center C1 Technical Report C1-001-89, June 1989.

[NCSC Conference, 1989] National Computer Security Conference, "12th National Computer Security Conference: Baltimore Convention Center, Baltimore, MD, 10-13 October, 1989: Information Systems Security, Solutions for Today - Concepts for Tomorrow", National Institute of Standards and National Computer Security Center, 1989.

[NCSC-CSC-STD-003-85, 1985] National Computer Security Center, "Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments", CSC-STD-003-85, NCSC, 25 June 1985.

[NCSC-STD-004-85, 1985] National Computer Security Center, "Technical Rationale Behind CSC-STD-003-85:

Computer Security Requirements", CSC-STD-004-85, NCSC, 25 June 1985.

[NCSC-STD-005-85, 1985] National Computer Security Center, "Magnetic Remanence Security Guideline", CSC-STD-005-85, NCSC, 15 November 1985.

[NCSC-TCSEC, 1985] National Computer Security Center, "Trusted Computer System Evaluation Criteria", DoD 5200.28-STD, CSC-STD-001- 83, NCSC, December 1985.

[NCSC-TG-003, 1987] NCSC, "A Guide to Understanding DISCRETIONARY ACCESS CONTROL in Trusted Systems", NCSC-TG-003, Version-1, 30 September 1987, 29 pages.

[NCSC-TG-001, 1988] NCSC, "A Guide to Understanding AUDIT in Trusted Systems", NCSC-TG-001, Version-2, 1 June 1988, 25 pages.

[NCSC-TG-004, 1988] National Computer Security Center, "Glossary of Computer Security Terms", NCSC-TG-004, NCSC, 21 October 1988.

[NCSC-TG-005, 1987] National Computer Security Center, "Trusted Network Interpretation", NCSC-TG-005, NCSC, 31 July 1987.

[NCSC-TG-006, 1988] NCSC, "A Guide to Understanding CONFIGURATION MANAGEMENT in Trusted Systems", NCSC-TG-006, Version-1, 28 March 1988, 31 pages.

[NCSC-TRUSIX, 1990] National Computer Security Center, "Trusted UNIX Working Group (TRUSIX) rationale for selecting access control list features for the UNIX system", Shipping list no.: 90-076-P, The Center, Fort George G. Meade, MD, 1990.

[NRC, 1991] National Research Council, "Computers at Risk: Safe Computing in the Information Age", National Academy Press, 1991.

[Nemeth, et. al, 1995] E. Nemeth, G. Snyder, S. Seebass, and T. Hein, "UNIX Systems Administration Handbook", Prentice Hall PTR, Englewood Cliffs, NJ, 2nd ed. 1995.

[NIST, 1989] National Institute of Standards and Technology, "Computer Viruses and Related Threats: A Management Guide", NIST Special Publication 500-166, August 1989.

[NSA] National Security Agency, "Information Systems Security Products and Services Catalog", NSA, Quarterly Publication.

[NSF, 1988] National Science Foundation, "NSF Poses Code of Networking Ethics", Communications of the ACM, Vol. 32, No. 6, Pg. 688, June 1989. Apparaît aussi dans les minutes de la réunion annuelle du Division Advisory Panel for Networking and Communications Research and Infrastructure, Dave Farber, Chair, November 29-30, 1988.

[NTISSAM, 1987] NTISS, "Advisory Memorandum on Office Automation Security Guideline", NTISSAM COMPUSEC/1-87, 16 January 1987, 58 pages.

[OTA-CIT-310, 1987] United States Congress, Office of Technology Assessment, "Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information", OTA-CIT-310, October 1987.

[OTA-TCT-606] Congress of the United States, Office of Technology Assessment, "Information Security and Privacy in Network Environments", OTA-TCT-606, September 1994.

[Palmer and Potter, 1989] I. Palmer, and G. Potter, "Computer Security Risk Management", Van Nostrand Reinhold, NY, 1989.

[Parker, 1989] D. Parker, "Computer Crime: Criminal Justice Resource Manual", U.S. Dept. of Justice, National Institute of Justice, Office of Justice Programs, Under Contract Number OJP-86-C-002, Washington, D.C., August 1989.

[Parker, Swope, and Baker, 1990] D. Parker, S. Swope, and B. Baker, "Ethical Conflicts: Information and Computer

Science, Technology and Business", QED Information Sciences, Inc., Wellesley, MA. (245 pages).

[Pfleeger, 1989] C. Pfleeger, "Security in Computing", Prentice-Hall, Englewood Cliffs, NJ, 1989.

[Quarterman, 1990] J. Quarterman, J., "The Matrix: Computer Networks and Conferencing Systems Worldwide", Digital Press, Bedford, MA, 1990.

[Ranum1, 1992] M. Ranum, "An Internet Firewall", Proceedings of World Conference on Systems Management and Security, 1992.

[Ranum2, 1992] M. Ranum, "A Network Firewall", Digital Equipment Corporation Washington Open Systems Resource Center, June 12, 1992.

[Ranum, 1993] M. Ranum, "Thinking About fire walls", 1993.

[Ranum and Avolio, 1994] M. Ranum and F. Avolio, "A Toolkit and Methods for Internet fire walls", Trustest Information Systems, 1994.

[Reinhardt, 1992] R. Reinhardt, "An Architectural Overview of UNIX Network Security"

[Reinhardt, 1993] R. Reinhardt, "An Architectural Overview of UNIX Network Security", ARINC Research Corporation, February 18, 1993.

[Reynolds-RFC1135, 1989] The Helminthiasis of the Internet, RFC 1135, USC/Information Sciences Institute, Marina del Rey, CA, December 1989.

[Russell and Gangemi, 1991] D. Russell and G. Gangemi, "Computer Security Basics" O'Reilly & Associates, Sebastopol, CA, 1991.

[Schneier 1996] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons, New York, second edition, 1996.

[Seeley, 1989] D. Seeley, "A Tour of the Worm", Proceedings of 1989 Winter USENIX Conference, Usenix Association, San Diego, CA, February 1989.

[Shaw, 1986] E. Shaw Jr., "Computer Fraud and Abuse Act of 1986", Congressional Record (3 June 1986), Washington, D.C., 3 June 1986.

[Shimomura, 1996] T. Shimomura with J. Markoff, "Takedown:The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw- by the Man Who Did It", Hyperion, 1996.

[Shirey, 1990] R. Shirey, "Defense Data Network Security Architecture", Computer Communication Review, Vol. 20, No. 2, Page 66, 1 April 1990.

[Slatalla and Quittner, 1995] M. Slatalla and J. Quittner, "Masters of Deception: The Gang that Ruled Cyberspace", Harper Collins Publishers, 1995.

[Smith, 1989] M. Smith, "Commonsense Computer Security: Your Practical Guide to Preventing Accidental and Deliberate Electronic Data Loss", McGraw-Hill, New York, NY, 1989.

[Smith, 1995] D. Smith, "Forming an Incident Response Team", Sixth Annual Computer Security Incident Handling Workshop, Boston, MA, July 25-29, 1995.

[Spafford, 1988] E. Spafford, "The Internet Worm Program: An Analysis", Computer Communication Review, Vol. 19, No. 1, ACM SIGCOM, January 1989. Aussi publié comme rapport technique Purdue CS CSD-TR-823, 28 November 1988.

[Spafford, 1989] G. Spafford, "An Analysis of the Internet Worm", Travaux de la conférence européenne d'ingénierie logicielle 1989, Warwick UK, septembre 1989. Travaux publiés par Springer- Verlag sous le titre : Lecture Notes in Computer Science #387. Aussi publié comme rapport technique Purdue n° CSD-TR-933.

[Spafford, Keaphy, and Ferbrache, 1989] E. Spafford, K. Heaphy, and D. Ferbrache, "Computer Viruses: Dealing with Electronic Vandalism and Programmed Threats", ADAPSO, 1989. (109 pages.)

[Stallings1, 1995] W. Stallings, "Internet Security Handbook", IDG Books, Foster City CA, 1995.

[Stallings2, 1995] W. Stallings, "Network and InterNetwork Security", Prentice Hall, , 1995.

[Stallings3, 1995] W. Stallings, "Protect Your Privacy: A Guide for PGP Users" PTR Prentice Hall, 1995.

[Stoll, 1988] C. Stoll, "Stalking the Wily Hacker", Communications of the ACM, Vol. 31, No. 5, Pgs. 484-497, ACM, New York, NY, May 1988.

[Stoll, 1989] C. Stoll, "The Cuckoo's Egg", ISBN 00385-24946-2, Doubleday, 1989.

[Treese and Wolman, 1993] G. Treese and A. Wolman, "X Through the Firewall, and Other Applications Relays", Digital Equipment Corporation, Cambridge Research Laboratory, CRL 93/10, May 3, 1993.

[Trible, 1986] P. Trible, "The Computer Fraud and Abuse Act of 1986", U.S. Senate Committee on the Judiciary, 1986.

[Venema] W. Venema, "TCP WRAPPER: Network monitoring, access control, and booby traps", Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands.

[USENIX, 1988] USENIX, "USENIX Proceedings: UNIX Security Workshop", Portland, OR, August 29-30, 1988.

[USENIX, 1990] USENIX, "USENIX Proceedings: UNIX Security II Workshop", Portland, OR, August 27-28, 1990.

[USENIX, 1992] USENIX, "USENIX Symposium Proceedings: UNIX Security III", Baltimore, MD, September 14-16, 1992.

[USENIX, 1993] USENIX, "USENIX Symposium Proceedings: UNIX Security IV", Santa Clara, CA, October 4-6, 1993.

[USENIX, 1995] USENIX, "The Fifth USENIX UNIX Security Symposium", Salt Lake City, UT, June 5-7, 1995.

[Wood, et.al., 1987] C. Wood, W. Banks, S. Guarro, A. Garcia, V. Hampel, and H. Sartorio, "Computer Security: A Comprehensive Controls Checklist", John Wiley and Sons, Interscience Publication, 1987.

[Wrobel, 1993] L. Wrobel, "Writing Disaster Recovery Plans for Telecommunications Networks and LANS", Artech House, 1993.

[Vallabhaneni, 1989] S. Vallabhaneni, "Auditing Computer Security: A Manual with Case Studies", Wiley, New York, NY, 1989.

Considérations sur la sécurité

Ce document tout entier est consacré aux questions de sécurité.

Informations sur l'éditeur

Barbara Y. Fraser
Software Engineering Institute
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213
téléphone : (412) 268-5010
fax : (412) 268-6989
mél : byf@cert.org