



2003/2004

**LA VEILLE EN SECURITE SUR INTERNET
ET
LE TRAITEMENT DES ALERTES DE SECURITE**

Thibault Bergeras

François Jeudy

Eric Vence

3BR – MEM10

REMERCIEMENTS

Nous tenons à remercier M. Patrick Devriendt, responsable du département Traitement du signal et Télécommunications de l'ESME Sudria. Nous remercions également M. Joël Couturier qui nous a présenté les sujets et nous a suivi durant la rédaction de ce mémoire.

Ce travail a été rendu possible grâce à l'aide précieuse de M. Jacky Lemée, professeur de sécurité sur les réseaux à l'ESME-Sudria. Outre le fait qu'il ait proposé le sujet, il a su nous guider dans notre travail et a toujours répondu clairement à nos nombreuses questions. Nous l'en remercions.

Nous tenons également à remercier M. Pierre Forget, membre du CERT-IST, qui nous a longuement expliqué le rôle de son organisme ainsi que M. Pierre Queinnec, consultant en sécurité.

SOMMAIRE

INTRODUCTION	3
I ACTIVITÉ DE VEILLE EN SÉCURITÉ	3
I.1 BESOIN DE SÉCURITÉ SUR LES RÉSEAUX INFORMATIQUES.....	3
I.1.1 <i>Notions de sécurité</i>	3
I.2 OBJECTIFS DE LA VEILLE EN SÉCURITÉ	5
I.3 COLLECTE DES INFORMATIONS	6
I.3.1 <i>Mailing Lists (liste de diffusion)</i>	6
I.3.2 <i>Site web</i>	6
I.3.3 <i>Newsgroups</i>	6
I.3.4 <i>IRC (Internet Relay Chat)</i>	7
I.4 QUALIFICATION DES INFORMATIONS	7
I.5 DIFFUSION AU SEIN DE L'ENTREPRISE.....	8
I.6 DÉFINITION DE LA POLITIQUE DE SÉCURITÉ.....	8
I.7 MISE EN PLACE DES MESURES ASSOCIÉES	9
I.7.1 <i>Réinstaller complètement le système d'exploitation à partir d'une version saine</i>	10
I.7.2 <i>Supprimer tous les services inutiles</i>	10
I.7.3 <i>Correctifs de sécurité préconisés pour le système d'exploitation et les logiciels utilisés</i>	10
I.7.4 <i>Restaurer les données d'après une copie de sauvegarde non compromise</i>	10
I.7.5 <i>Changer tous les mots de passe du système d'information</i>	11
I.7.6 <i>Liste des informations ou des procédures ont manqué</i>	11
I.7.7 <i>Points à améliorer</i>	11
II ORGANISATIONS MISES EN PLACE POUR GÉRER LES INCIDENTS	13
II.1 LES DIFFÉRENTS ORGANISMES	13
II.2 HISTORIQUE DE LA CRÉATION DES CERTS.....	16
II.3 RÔLE D'UN CERT (CSIRT)	19
II.4 LA DIFFUSION D'INFORMATION.....	20
II.5 EN CAS D'INCIDENT	21
CONCLUSION	25
RÉFÉRENCES	26

L'essor des échanges informatiques via des réseaux publics et privés a engendré un besoin de confidentialité, d'intégrité et de disponibilité des données. Aujourd'hui des informations très sensibles issues de domaines divers (finances, défense, gouvernement, justice, médical, etc.) transitent sur les réseaux.

Le piratage par loisir mais aussi à des fins plus graves s'est répandu et la lutte contre les intrusions, contre les virus, et l'effort de protéger des informations confidentielles sont devenus des enjeux majeurs pour les entreprises et les particuliers. C'est une priorité pour l'économie comme pour la sécurité des citoyens d'étanchéifier les réseaux.

Aucun organisme ou entreprise n'est épargné. En février 1990, des pirates s'introduisent, par le réseau Internet, dans plusieurs réseaux d'ordinateurs de l'armée et de la marine américaines. Ces intrusions semblent avoir été faites par deux adolescents de Californie qui cherchaient à accéder à des informations confidentielles sur les équipages, le personnel et les soldes des militaires (pendant un certain temps, le Pentagone a cru que ces attaques étaient commanditées par Saddam Hussein). Ces agressions électroniques ne sont pas rares : au cours de l'année 1998, deux tiers des entreprises surveillées par les services américains de contre-espionnage ont été victimes de violations informatiques.

Le besoin de veille en sécurité et de traitement des alertes est donc indispensable. Nous définirons dans un premier temps la mise en place, les besoins et les objectifs de la veille en sécurité. Nous verrons également comment l'information liée à la sécurité pour l'entreprise peut être collectée, qualifiée et diffusée. La mise en place d'une politique de sécurité sera également abordée. Une deuxième partie présentera les différents organismes mis en place pour gérer les incidents. Une attention particulière sera attachée à la présentation des CERTs et de leurs bulletins d'alertes.

I Activité de veille en sécurité

I.1 Besoin de sécurité sur les réseaux informatiques

La veille en sécurité est née d'un besoin des entreprises face à la recrudescence d'actes malveillants sur les réseaux de données.

De nombreux facteurs ont provoqué une prise de conscience des questions de sécurité informatique. Les ordinateurs sont de plus en plus reliés à Internet et utilisés pour effectuer des transactions financières ou des échanges d'informations hautement confidentielles. Le développement de l'informatique a amené, comme dans tous les domaines, un phénomène de violation de règle par des pirates (ou hackers en anglais), des hors la loi du réseau.

La confiance que l'on porte aux ressources informatiques augmente très fortement. Et alors que les ordinateurs occupent une place de plus en plus importante, les problèmes de sécurité peuvent provoquer des catastrophes ayant des ramifications financières et légales. Au minimum, une faille de sécurité provoquera des pertes de temps et une perte de productivité. Mais plus que probablement les résultats seront pires et les pertes lourdes.

I.1.1 Notions de sécurité

Une sécurité informatique efficace repose sur trois éléments principaux : confidentialité, intégrité et disponibilité.

On appelle **confidentialité** le fait selon lequel l'information n'est pas accessible à ceux qui n'en ont pas l'autorisation. Beaucoup de crimes informatiques concernent des fuites et des vols d'informations confidentielles. On appelle contrôle d'accès le fait de n'autoriser l'accès aux informations et aux ressources qu'à ceux qui en ont besoin.

La forme de contrôle d'accès la plus courante est l'utilisation de mots de passe; et la forme la plus courante des infractions de sécurité concerne ces mots de passe. La mise en place d'une politique de mots de passe résistants ne nécessite pas de hautes compétences techniques et doit être prise très au sérieux. Les entreprises doivent créer et mettre en place des politiques de sécurité informatique qui enseignent aux employés la manière de choisir un mot de passe, sa durée d'utilisation et sa confidentialité.

Un autre aspect du contrôle d'accès est la limitation des ressources disponibles pour un employé une fois qu'il a été authentifié sur le réseau d'entreprise. Ce contrôle d'accès très spécifique constitue une barrière de défense supplémentaire pour vos ressources informatiques. Il est le principe même des systèmes d'exploitation multi-utilisateurs tels que les BSD, Linux, MacOS X, Windows XP, etc. Les droits de lecture, écriture et exécution d'un utilisateur sur une donnée peut être défini en fonction d'un groupe ou de lui-même. Ainsi tout un département d'une entreprise peut avoir besoin d'écrire des données sur un espace de stockage, alors qu'un autre département n'est censé que lire ces données. Chaque département sera défini comme un groupe. L'un aura les droits de lecture et d'écriture, l'autre de lecture uniquement.

L'**intégrité** assure que l'information ne peut être modifiée de manière inattendue. Une perte d'intégrité peut provenir d'une erreur humaine ou d'une manipulation intentionnelle. Les conséquences liées à l'utilisation d'informations inexactes peuvent être désastreuses. Des données, si elles ont été modifiées de façon incorrecte peuvent devenir inutiles, ou dangereuses. Des efforts doivent être faits pour assurer l'exactitude et la solidité des données.

Lorsque la validité de l'information est critique, il est souvent utile de mettre en place des contrôles et des vérifications. Il peut être important de s'assurer que l'information est inutilisable si elle est volée. Le cryptage est le processus qui transforme l'information dans un format secret pour éviter que des personnes non autorisées puissent l'utiliser si elles arrivaient à s'en emparer.

La **disponibilité** empêche les données d'être supprimées ou de devenir inaccessibles. Cela s'applique non seulement aux informations mais aussi aux serveurs ou à d'autres entités de l'infrastructure réseau. L'impossibilité d'accéder à des ressources requises est appelée un refus de service (Denial of Service). Des attaques intentionnelles contre des systèmes informatiques ont souvent pour but de désactiver l'accès aux données, et occasionnellement le but est le vol de ces données. Ces attaques sont lancées pour diverses raisons dont des motivations politique et économiques ou par simple défi. Ces attaques peuvent aller de la saturation d'une boîte mail à des actions globales dont le but est par exemple de mettre à terre un système bancaire.

Un autre aspect de la disponibilité est d'assurer que les ressources nécessaires sont utilisables quand et où on a besoin d'elles. Fournir des redondances systèmes, sous la forme de données, machines et sources d'électricité de secours assure souvent une plus grande disponibilité. Le stockage de données critiques hors-site permet de les récupérer et les utiliser en cas de problèmes (comme ce fut le cas après l'incendie qui s'était produit un Dimanche au Crédit Lyonnais, le lendemain les services bancaires étaient opérationnels grâce à une redondance des données sur plusieurs sites).

La stratégie de sécurité doit se focaliser sur ces trois points. En fonction des besoins de l'entreprise, une importance différente doit être accordée à chaque objectif. Par exemple, les politiques de sécurité d'un système de défense nationale placeront une très grande importance dans la confidentialité, les informations stratégiques devant être protégées. Le système de transfert de fonds d'une banque a un grand besoin d'intégrité; les comptes bancaires devant être justes. Enfin, un système d'urgence médicale insistera sur la disponibilité, les informations et les ressources devant être disponibles en permanence et de partout.

Les descriptions concrètes exposées ci-dessus et la compréhension de la sensibilité d'un réseau montre à quel point un administrateur réseau ou chef de département informatique se doit de surveiller la sécurité dans son parc informatique. Il apparaît alors que la compétence de veille en sécurité est complexe car elle fait appel à de nombreuses notions.

I.2 Objectifs de la veille en sécurité

Le concept de veille en sécurité sur les réseaux va au delà de la prévention. Le responsable ou administrateur d'un réseau doit en permanence se tenir au courant des failles, des faiblesses et des mises à jour le concernant, ainsi que des virus et Chevaux de Troie existants. Pour cela il utilise des supports d'information tels que les mailings lists, des sites Web ou des newsgroups.

Il faut également être concerné par la qualité des informations et des bulletins de sécurité que l'on trouve sur Internet. Les annonces peuvent provoquer de l'inquiétude aux responsables de sécurité informatique en raison de leur multitude et de l'incertitude quant à leur fiabilité. Déterminer quelles sont les bonnes sources d'informations de sécurité et éliminer les fausses alertes nécessite du temps et de la recherche. Il faut pour cela avoir des bases solides en technologie réseau et en informatique.

La sécurité absolue n'existant pas, l'administrateur doit s'en rapprocher. Pour ce faire, il doit anticiper les risques, préserver les informations importantes à l'aide de sauvegarde, former les gens qui ont des accès et des droits, et garder à jour une base de données précise de l'équipement hardware et software qu'il a en charge.

Ce dernier point est très important. L'inventaire d'un parc informatique est pour l'administrateur une base d'information essentielle. Cela permet à l'administrateur réseau d'orienter ses recherches en matière de sécurité et de se spécialiser dans ce dont l'entreprise a besoin. Cette base de données doit contenir :

- les entités physiques du réseau (serveurs de fichiers, serveurs Web, serveurs mails, etc.).
- les systèmes d'exploitation (du parc informatique : Windows, MacOS..., et des entités du réseau : Distributions Linux, IOS, NetBSD...).
- les services installés dessus et leur configuration (Apache, postfix, bind, ...).
- les outils de statistiques, de prévention et de tests de vulnérabilités disponibles pour chaque composante du réseau (MRTG, outils SNMP,...).
- les normes de cryptage utilisées (politique de clefs privés/publiques, certificats, AES, DES, ...).
- le plan d'adressage du réseau, le plan des sous-réseaux et des pots de miel (ou honeypots – zone, serveur ou programme volontairement vulnérable destiner à attirer les pirates et garder les zones confidentielles du réseau étanches. Un honeypot permet également d'étudier les méthodes d'attaques).
- les instruments de mesure et d'analyse de réseau ne possédant pas d'adresse (par exemple sondes pour analyser les paquets).
- les équipements physiques dédiés à la sécurité (firewall, routeurs)

Il faut attacher une importance particulière aux versions des services et des systèmes d'exploitation qui sont souvent source de piratage lorsqu'elles ne sont pas récentes.

Des outils et des méthodes d'inventaires automatiques existent et peuvent être utilisées. Les plus courantes sont les approches DMTF et IETF. C'est le cas chez les grosses structures de type opérateurs, grandes entreprises, banques, ou société spécialisées dans les réseaux. Il est également possible d'imaginer à une autre

échelle que l'administrateur réseau tienne à jour un fichier formaté correctement contenant toutes ces informations (par un fichier au format XML) ou une base de données (par exemple une base MySQL, 4D, ...).

I.3 Collecte des informations

Les bulletins d'alertes et autres informations relatives à la sécurité peuvent être obtenues grâce à différentes sources dont nous présenterons les principales.

I.3.1 Mailing Lists (liste de diffusion)

Une mailing list est une méthode de diffusion d'informations, dans laquelle les abonnés de la liste peuvent envoyer des messages qui seront diffusés aux autres. La réponse à un message est diffusée à tous les membres de la liste.

Exemples : BugTraq, FullDisclosure, packet-ninjas

I.3.2 Site web

Ils sont à la fois source d'informations et de vitrines pour les organismes de sécurité. Les forums de discussion sont des lieux d'échanges dans lesquels on trouve de précieuses informations ainsi que des trucs et astuces aidant l'administrateur à maintenir son réseau à jour et éviter les intrusions.

Exemples : cert.org, securityfocus.com

Il existe de nombreux sites Web et mailing lists officiels qui assureront une certaine garantie sur la qualité de l'information diffusée. Cela n'empêche pas l'administrateur d'avoir suffisamment d'esprit critique et de qualités pour prendre des bonnes décisions lorsque les bulletins de sécurité ne lui semblent pas adaptées à son réseau.

D'autres sources d'informations peuvent être intéressantes et ne devraient pas être négligées. Un moyen d'être au courant rapidement des failles de sécurité d'un service ou d'un système d'exploitation est de faire parti soit même de groupes de discussions de passionnés de sécurités informatiques ou de pirates. Ainsi, même si certains newsgroups et channels IRC sont officiels et tenus par des professionnels, on en trouve de nombreux dans lesquels participent des amateurs avertis, parfois de futurs administrateurs réseaux et certains pirates. Cette source d'information est très délicate car on ne peut avoir confiance en personne, et il est recommandé d'être expert pour pouvoir dialoguer ou ne serait ce que profiter de ce qu'il se dit.

I.3.3 Newsgroups

A l'origine, les newsgroups sont des forums thématiques dans lesquels des chercheurs et quelques autres internautes échangeaient des informations. Les newsgroups sont fédérés par le réseau USENET qui fut implémenté en 1979. Il a toujours connu une croissance exponentielle et il regroupe aujourd'hui des milliers de groupes ciblés. Chaque newsgroup, ou forum, Chaque newsgroup, ou forum, Chaque newsgroup se subdivise en une multitude de sujets de conversations (appelés threads) que chacun peut initier librement et auxquels chacun peut contribuer en postant des messages.

Exemple : comp.misc.virii

I.3.4 IRC (Internet Relay Chat)

IRC est un système client-serveur permettant de dialoguer en direct avec plusieurs personnes sur un espace de discussion appelé channel (canal). Les channels sont en général thématiques et la plupart du temps occupés par des amateurs partageant une même passion. On peut donc y trouver des personnes éclairées en matière de sécurité.

Exemple : #poc (Proof Of Concept) sur les serveurs EFnet

I.4 Qualification des informations

On distingue plusieurs étapes dans la qualification des informations. La première est de s'assurer que les alertes et bulletins d'information sont **fiables**. Le support d'un organisme officiel est alors nécessaire. Les CERTs que nous présenterons plus loin sont un exemple d'organisme fiable qui assurera à l'administrateur réseau une certaine confiance quant aux informations diffusées. Comme dans tous les métiers, l'expérience professionnelle est également importante.

Selon les services tournant sur les plateformes réseaux de l'entreprise, un bulletin d'alerte pourra avoir une plus ou moins grande importance. La **criticité** d'une alerte doit donc être jugée et l'action humaine de correction de faille sera d'autant plus urgente que le niveau de criticité est élevé.

Par exemple, un serveur Web fait tourner un site commercial de vente en ligne et contient des informations privées sur les clients. L'administrateur de ce serveur travaille dessus à distance en se connectant par ssh (secure shell - service permettant d'effectuer une liaison sécurisée et de transmettre au serveur des commandes shell). Le service permettant cela au niveau de la machine est nommé sshd. Une faille à ce niveau pourrait autoriser un pirate de passer des commandes shell en mode root (utilisateur ayant tous les droits sur la machine). Le pirate pourrait ensuite lancer son propre service sshd ayant ainsi toute liberté d'opérer sur le serveur, et supprimer celui de l'administrateur. Le malveillant tacherait d'effacer les logs permettant de l'identifier au fur et à mesure de son passage...

Ce scénario montre qu'une alerte indiquant une faille au niveau du service sshd s'avère extrêmement grave et doit être traitée en haute priorité. Si une quelconque information confidentielle est récupérée par un malveillant, la société pourrait être amenée à se confronter à la justice (après plainte de clients), et les usagers du site seraient placés dans une position délicate, des informations sur eux ayant été divulguées.

D'un autre côté, une telle faille sur une machine d'un réseau privé non relié au WAN devra être corrigée mais pas forcément avec la même urgence.

On imagine la gravité que pourraient avoir des exemples similaires dans les domaines de la finance, de la médecine, de la justice, de l'armée et des services secrets. Cela illustre la sensibilité et l'importance que peut avoir un bulletin d'alerte, et le besoin d'évaluer son niveau de criticité.

L'administrateur devrait dans ce cas :

- Vérifier la fiabilité de l'information auprès d'un organisme officiel. Il peut également tester la faille sur son propre matériel non relié au réseau de l'entreprise ni au WAN.
- Contacter le développeur via son site Web pour récupérer un correctif (mise à jour d'un logiciel ou d'un système d'exploitation, patch, application d'un anti-virus, etc.). En général les CERTs indiquent une adresse Internet où trouver le correctif.
- Tester dans un environnement d'homologation le correctif. Le correctif d'une faille de sécurité ne doit pas mettre en péril l'environnement de production. Il faut donc vérifier qu'il n'altère pas les fonctionnalités des applications en production, qu'il soit isoconforme.
- Après qualification, le diffuser dans l'entreprise. Cela peut se faire en installant les correctifs manuellement sur les machines, ou grâce à des systèmes de mises à jour automatisés. En effet, les équipements réseau peuvent communiquer à un serveur central le numéro de version des services utiles et lorsqu'une mise à jour est nécessaire ils pourront la télécharger et l'installer automatiquement.

I.5 Diffusion au sein de l'entreprise

Après réception de bulletin d'alerte, le responsable réseau doit transmettre aux employés de l'entreprise un certain nombre d'informations susceptible de les concerner. Par exemple, un patch Microsoft Office concerne tous les employés de l'entreprise. Une mise à jour de serveur mail ne concerne que les administrateurs réseau.

Les membres de l'équipe de veille et d'administrateurs réseaux pourra communiquer avec les employés par mail (ponctuels, envoie d'un bulletin quotidien, hebdomadaire ou mensuel), par liste de diffusion et par l'intermédiaire d'un site intranet (affichage d'actualité ou forum de discussion).

I.6 Définition de la politique de sécurité

Il est important de définir dès le début de la mise en place d'un réseau les politiques de sécurité. Ce sont des règles destinées à contrôler des les droits d'accès et définir toutes les technologies et méthodes employées dans l'entreprise relatives à la sécurité. Dans ce « règlement », les sociétés doivent désigner un responsable de l'application et de la gestion de ces politiques (en général le responsable de la veille en sécurité, ou l'administrateur réseau), et déterminer le mode d'information des employés à propos des règles et des protections.

Les quatre points suivants doivent être étudiés pour définir une politique de sécurité :

- Décrire les besoins en fonction du métier

Le responsable de la mise en place de la politique de sécurité doit bien cerner les besoins des employés pour adapter le réseau et les autorisations sur les serveurs, ainsi que les méthodes d'accès.

- Identifier les risques associés

Quels sont les risques en cas d'attaque ou d'intrusion ? Quelles seront les conséquences pour l'entreprise ? Ces questions doivent être consciencieusement étudiées afin de protéger au maximum les données sensibles.

- Limiter les risques

Toutes les mesures de limitation de risques doivent être prises. Au niveau des employés (avec des formations, des bulletins d'informations,...) et au niveau du matériel (avec des outils adaptés et performants de tests de vulnérabilité et de prévention).

- Faire évoluer la politique de sécurité

Les besoins de l'entreprise évoluent, les services associés au réseau également. C'est pourquoi la politique de sécurité doit être révisée constamment.

Une politique de sécurité informatique bien équilibrée aura des composants **proactifs** et **réactifs** complémentaires. La partie proactive comprend l'utilisation de contrôles de sécurité forts, alors que l'approche réactive inclut l'analyse et la surveillance de ces contrôles. Dans cette approche, le composant proactif peut être un système configuré de façon appropriée qui enregistre tous les accès système dans un log. L'administrateur réseau exécute le composant réactif en vérifiant les logs pour chercher une activité suspecte ou tout élément anormal. Il est nécessaire de prendre ces deux approches pour avoir un contrôle de sécurité efficace. Le fait de connaître et surveiller les allés venus d'accès à des serveurs pourrait permettre d'identifier un responsable en cas de problème. Il faut néanmoins utiliser le conditionnel car les logs enregistrent les adresses IP entrées, mais les hackers ou Chevaux de Troie en général effacent toute trace de leur passage. Il est également possible pour un hacker de spoofer son IP, c'est à dire de remplacer au niveau de la couche réseau l'adresse source par une autre (spoofing), celle d'une imprimante par exemple. C'est le cas lorsque l'on veut par exemple inonder de requêtes un réseau (ping flooding) en broadcastant des paquets ICMP vers des imprimantes réseaux.

La politique de sécurité doit également définir certaines règles de conduite. Elles peuvent être nombreuses, on peut citer par exemple :

Suppression immédiate des accès d'un employé quittant l'entreprise, changement du mot de passe des employés périodiquement, garder les signatures des anti-virus à jour, etc.

I.7 Mise en place des mesures associées

La veille en sécurité consiste à sécuriser le système d'information, le tenir à jour et prévenir les attaques. Lorsque le mal est fait il faut réagir pour ne pas être victime de nouveau.

Les grandes étapes de **l'analyse de l'intrusion** sont :

- la recherche des modifications dans le système et les fichiers de configuration.
- la recherche des modifications de données.
- la recherche des outils et des données laissés par l'intrus (analyse des logs, historique des commandes, date de modification des fichiers).
- l'examen des fichiers journalistiques.
- la recherche d'un sniffer sur le réseau (un sniffer est un outil logiciel permettant de scruter tous les paquets transitant sur un réseau, et par conséquent permet la lecture de mots de passe lorsque ceux-ci ne sont pas cryptés).
- la vérification des autres machines connectées sur le réseau.

L'analyse de l'intrusion peut permettre d'identifier le malveillant et surtout de comprendre la vulnérabilité de l'environnement réseau existant. Pour repartir sur des bases saines il faut suivre un certain nombre d'étapes.

I.7.1 Réinstaller complètement le système d'exploitation à partir d'une version saine

Sur une machine victime de l'attaque, n'importe quelle partie du système d'information peut avoir été modifiée : noyau, binaires, fichiers de données, processus et mémoire. D'une manière générale, la seule manière de s'assurer qu'une machine ne possède plus de porte dérobée (back door) ou autre modification laissée par l'intrus est de réinstaller entièrement le système d'exploitation à partir d'une distribution saine et de compléter cette installation en appliquant tous les correctifs de sécurité avant de reconnecter la machine à un réseau. Il est également conseillé de tester la machine avec un outil de mesure de vulnérabilités à jour et de corriger les vulnérabilités identifiées, avant de la rebrancher au réseau.

I.7.2 Supprimer tous les services inutiles

La configuration normale d'un système est de ne lancer que les services que celui-ci doit offrir et aucun autre. Il faut par conséquent vérifier qu'il n'y a pas de vulnérabilités dans ces services et qu'ils ne sont ouverts qu'aux personnes extérieures réellement autorisées.

Une bonne manière de procéder est de désactiver tous les services au départ, et de les activer au fur et à mesure qu'ils sont nécessaires.

I.7.3 Correctifs de sécurité préconisés pour le système d'exploitation et les logiciels utilisés

L'administrateur réseau doit s'assurer qu'il dispose de tous les correctifs de sécurité nécessaires. Il doit pour cela utiliser toutes les sources d'informations disponibles (éditeurs de logiciels, CERTs, etc.).

I.7.4 Restaurer les données d'après une copie de sauvegarde non compromise

Les données venant d'une copie de sauvegarde peuvent être porteuse de virus ou de fichiers vulnérables. Il faut donc s'assurer que ces données ne proviennent pas

d'une machine compromise. De plus, il faut s'assurer que les données venant des comptes utilisateurs ne soient pas infectées, n'importe quel fichiers pouvant contenir un cheval de Troie par exemple.

I.7.5 Changer tous les mots de passe du système d'information

Une fois que toutes les vulnérabilités connues du système d'information ont été supprimées, il est très fortement recommandé de modifier les mots de passe de tous les comptes de ce système. En effet, lors de l'intrusion, il est possible que ces mots de passe aient été récupérés le pirate.

Expérimenter une intrusion peut être enrichissant, il faut se poser les bonnes questions et apporter les réponses avec soin.

I.7.6 Liste des informations ou des procédures ont manqué

- pour protéger plus fortement le système d'information sur lequel il y a eu une intrusion
- pour détecter plus rapidement qu'un incident de sécurité était en train de se produire
- pour cerner plus précisément quelles étaient les anomalies de fonctionnement du système
- pour réagir de manière plus adéquate, sans risquer de commettre un geste qui ferait empirer la situation
- pour déterminer plus vite quelle était la marche à suivre et quelles étaient les personnes à contacter
- pour entrer plus facilement en relation avec le CERT qui s'est occupé de votre cas
- pour trouver plus aisément la ou les vulnérabilités qui avaient été utilisées
- pour reconstituer plus efficacement tout l'historique de l'intrusion sur l'ensemble des systèmes d'information
- pour mieux repartir sur de bonnes bases avec des systèmes d'exploitation sains et sans faille de sécurité connue

I.7.7 Points à améliorer

Les réponses aux questions posées dans le paragraphe précédent se déclinent en deux catégories :

- Les réponses techniques
 - outils de protection ou de filtrage
 - outils de détection d'intrusion
 - outils de journalisation des connexions au système d'information (logs)
- Les réponses organisationnelles
 - la politique de sécurité était-elle suffisante, et a-t-elle été respectée ?
 - la recherche systématique et régulière d'une intrusion potentielle est-elle prévue ?
 - la marche à suivre détaillée en cas d'intrusion est-elle écrite et à disposition de tous les acteurs ?

- les relations humaines entre les différentes personnes impliquées ont-elles été déterminantes dans la résolution du problème ?

Finalement, il faut garder une trace écrite (sur papier) de la description de l'incident. Ce document, dont le but est de ne pas reproduire des erreurs passées et d'informer les futures responsables sécurité, doit contenir l'historique des faits et la description technique du matériel impliqué.

II Organisations mises en place pour gérer les incidents

Dans le but de veiller à limiter l'envergure et le nombre des attaques malveillantes, de nombreuses organisations ont été créées. Celles-ci organisent des moyens de défense et de réaction et assurent une certaine prévention en diffusant de l'information.

II.1 Les différents organismes

Il existe de nombreux organismes qui assurent une activité de veille en sécurité. Ils donnent de nombreuses informations permettant d'anticiper les menaces et certains permettent de trouver de l'aide en cas d'attaques.

- **OSSIR** (Observatoire de la Sécurité des Systèmes d'information et des Réseaux)

Créée en 1996, cette association regroupe les utilisateurs intéressés par la sécurité des systèmes d'information et des réseaux. Elle comprend actuellement trois groupes de travail (sécurité Unix, sécurité Windows et sécurité des réseaux) qui organisent des réunions.

Au sein de cette association, interviennent régulièrement des membres des CERTs français et du FIRST. Ces deux structures seront détaillées dans la suite du mémoire.

L'OSSIR fait vivre une base de vulnérabilités concernant la sécurité des systèmes windows.

- **NIPC** (National Infrastructure Protection Center)

C'est une instance gouvernementale américaine hébergée par le FBI et chargée de la sécurité des réseaux essentiels du pays. Son but est de faire de la prospective et de prévenir les catastrophes. Ce centre est accusé d'être inefficace en dépit de ses importants moyens financiers. En effet, le NIPC se contente généralement de reprendre des alertes de sécurité déjà publiées partout. Il n'est pas très réactif ni proactif.

- **SANS** (SysAdmin, Audit, Network, Security)

Il est composé de 96000 administrateurs et professionnels de la sécurité. Il a été fondé en 1989. Cette structure participe à la veille en sécurité. Elle propose un service de prévention et de réaction aux incidents en envoyant des bulletins d'informations. Ceux-ci peuvent être de différents types selon la nature de l'information transmise.

Il existe les bulletins :

- *newsbits* : Chaque mercredi, ce bulletin résume les articles les plus importants concernant la sécurité. Il contient une référence du Web si possible afin que l'utilisateur puisse avoir plus d'information concernant cet article s'il le désire.
- *@risks* : Il est envoyé tous les jeudi matin. Il évoque les vulnérabilités les plus critiques, informe sur les dommages causés par celles-ci et propose des

solutions pour s'en protéger. Il contient également une liste regroupant toutes les vulnérabilités découvertes dans la semaine

- *privacybits* : Tous les mardi ce bulletin donne des informations et des alertes relatives à la propriété privée et aux droits individuels (exemple : Home PC used as Spam Machines le 5 Mars 2004)
- *auditbits* : Une fois toutes les deux semaines, ce bulletin informe sur des nouvelles et des alertes concernant l'audit.
- *networkbits* : Une fois toutes les deux semaines, ce bulletin évoque les dernières informations et les alertes concernant le réseau.

Le SANS propose aussi une liste réactualisée des 20 vulnérabilités les plus fréquentes sur Internet.

Depuis 1999, le SANS offre un service appelé l'Internet Storm Center. Celui ci permet d'analyser les données provenant de firewalls ou de systèmes de détection d'intrusion dans le but de détecter des menaces.

Enfin, le SANS donne des conseils, de la documentation autour des malveillances, des alertes, et des parades et remèdes à appliquer.

- **DCSSI** (Direction Centrale de la Sécurité des Systèmes d'information)

Héritière du Service central de la sécurité des systèmes d'information, centre focal de l'Etat pour la sécurité des systèmes d'information, la DCSSI a été instituée le 31 juillet 2001. Elle est placée sous l'autorité du Secrétaire général de la défense nationale.

Le DCSSI contribue à la politique gouvernementale en matière de sécurité des systèmes d'information (SSI). Il assure la fonction d'autorité nationale de régulation pour la SSI en délivrant les agréments, cautions ou certificats pour les systèmes d'information de l'Etat, les procédés ou les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information (CESTI).

La DCSSI évalue les menaces pesant sur les systèmes d'information, donne l'alerte, développe les capacités à les contrer et à les prévenir grâce à sa subdivision appelée CERTA. Nous verrons cette structure un peu plus loin lorsque nous évoquerons les CERTs.

Le DCSSI assiste les services publics en matière de SSI. Il développe l'expertise scientifique et technique dans le domaine de la SSI, au bénéfice de l'administration et des services publics

Enfin, le DCSSI forme et sensibilise à la SSI (CFSSI : Centre de Formation à la Sécurité des systèmes d'informations).

- **Les listes de diffusion** spécialisées

SecurityFocus est un site sur Internet qui propose de l'information sur la sécurité, des conseils, des produits commerciaux. Ce site héberge un certain nombre de mailing lists. On peut citer la plus connue : *BugTraq*. L'avantage de BugTraq est que son spectre d'information est très large. Il est également très réactifs aux évènements. Cependant, il faut se méfier parfois du contenu. En effet, il est très facile de s'inscrire car il n'est demandé qu'une adresse email. Les auteurs ne sont donc pas toujours très sérieux bien que la liste soit modérée. Les mails transmis contiennent une description de la faille et la plupart du temps ce que l'on appelle un « exploit » ou un « proof of concept », c'est à dire un extrait de code ou un script qui prouve l'existence de la faille et permet de l'exploiter. Une certaine éthique existe néanmoins sur

BugTraq. Lorsqu'une faille est découverte, les développeurs du logiciel concerné sont contactés.

D'autres listes de diffusion peuvent être tout aussi efficace, mais moins consciencieuses. Ainsi, sur *FullDisclosure@list.netsys.com*, des informations assez similaires à BugTraq sont échangées, elles aussi modérées, mais les développeurs ne sont pas contactés en cas de découverte de faille.

Enfin la liste Packet-Ninjas hébergée par birmingham-infragard.org est une liste très fermée qui assure une certaine qualité des interventions.

Il existe de nombreuses autres listes de diffusion, mais les trois précédentes montrent un panel du type de liste que l'on peut rencontrer. Les mailing lists ne sont pas toujours des organismes mais peuvent être considérées comme tels. Elles regroupent des personnes plus ou moins spécialistes dans un domaine et sont sources inépuisables d'informations.

- Le **CVE** (Common Vulnerability Exposure)

Il dépend de l'association Mitre. Le CVE recense, formalise et officialise les vulnérabilités découvertes. Il s'agit d'un index sur toutes les vulnérabilités. A chaque vulnérabilité est associée un numéro. Cela permet, au niveau mondial, que toutes les structures utilisent un même numéro lorsqu'elles parlent de la même vulnérabilité. Lorsqu'on communique à un CERT une vulnérabilité, il peut ainsi rechercher facilement dans sa base s'il a déjà émis un avis dessus. Si oui, il a juste à mettre à jour cet avis. Une plage de valeurs est donnée aux constructeurs ; ce qui permet d'éviter qu'il demande au CVE un numéro pour chaque nouvelle vulnérabilité découverte. Au départ, une vulnérabilité est noté CAN-2004-9600 par exemple car elle est candidate et n'a pas été encore validée comme étant une vulnérabilité. Au bout de 6 mois généralement, elle devient CVE-2004-9600.

- Les **constructeurs et éditeurs** de logiciels

Différentes failles (vulnérabilités) sont découvertes régulièrement dans les systèmes et programmes applicatifs. Ils peuvent être découverts par les constructeurs et éditeurs qui possèdent souvent leur propre structure de veille en sécurité ou alors par un autre organisme qui met alors la pression sur le constructeur ou l'éditeur à qui appartient le système ou le logiciel. Le constructeur ou l'éditeur cherche alors un moyen de résoudre cette vulnérabilité et propose ensuite un patch de sécurité à appliquer.

Les structures des constructeurs et des éditeurs recherchent et diffusent uniquement des informations sur les vulnérabilités de leurs propres systèmes ou programmes, contrairement aux autres organismes.

- **Sociétés commerciales**

Certaines sociétés proposent des services de veille aux entreprises.

On peut citer HSC qui est un cabinet de consultants spécialisé dans la sécurité informatique et réseaux. Il propose notamment un service de veille technologique en sécurité. Il s'agit d'un service de suivi des vulnérabilités des systèmes, d'information et d'analyse technologique et stratégique en sécurité. Ses services de veille sont commercialisés depuis 1997. HSC fournit à ses abonnés les vulnérabilités importantes et propose des correctifs de sécurité à appliquer. Il envoie des avis

courts et clairs en français qui précisent le degré de gravité, le système d'exploitation ou l'application concernée, une description du problème, la parade, le risque induit, et l'avis original. Ces avis sont envoyés par courrier électronique selon le profil de l'utilisateur et sont disponibles sur un serveur web. L'accès au Web permet de visualiser tous les avis et offre des possibilités de recherche par application, par systèmes d'exploitation et sur les différents champs des avis.

HSC suit les avis de sécurité de différents émetteurs : CERT, BuqTraq, Securityfocus, Cisco, Microsoft, HP, SUN, IBM,... Puis il les trie, en sélectionne et rédige ses avis en français qui sont validés puis envoyés à ses abonnés.

A une échelle internationale, la société eEye, spécialisée en sécurité suit de près et participe aux listes de diffusion, et en particulier BugTraq.

Cette activité de veille et d'écoute d'informations diffusées sur Internet est essentielle, elle permet de faire face aux problèmes de sécurité avec un temps de latence réduit.

Il existe beaucoup d'entreprises proposant de tels services. Cependant, les sociétés commerciales ainsi que les éditeurs de firewalls ou d'antivirus sont souvent soupçonnés de créer des virus afin de justifier leurs activités.

- **CERT** (Computer Emergency Response Team)

Contrairement aux autres clubs ou autres associations, les CERTs ne font pas que de la diffusion d'informations. Ils font aussi du traitement d'incidents. De plus, les CERTs coopèrent entre eux et sont les entités les plus sollicitées pour assurer la veille en sécurité. Il est donc facile à comprendre que ces structures ont un rôle très important. C'est la raison pour laquelle nous allons focaliser la suite de notre mémoire sur ces structures.

II.2 Historique de la création des CERTs

En novembre 1988, un étudiant de l'université de Cornell lâcha, sur le réseau Arpanet développé par le DoD (département de la défense américain), un programme qui se propageait et se dupliquait tout seul. Ce programme connu sous le nom de « ver Internet », exploitait diverses failles des systèmes d'exploitation UNIX. Bien que programmé sans intentions malveillantes, ce premier virus contamina 3 à 4% des 60 000 machines connectées au réseau et ce dernier devint alors complètement indisponible pendant plusieurs jours.

Un groupe d'experts analysa le code du virus ; ce qui permit d'identifier et de corriger les failles du système d'exploitation ainsi que de développer et de diffuser des mécanismes de suppression définitive du ver.

A la suite de cet incident, la DARPA (Defence Advanced Research Projects Agency) décida de mettre en place une structure permanente semblable à celle qui avait permis de régler l'incident : ce fut la naissance du CERT-CC (CERT Coordination Center). Il est installé à l'université de Carnegie Mellon.

Assez rapidement d'autres CERTs se sont créés :

- Le CIAC (Computer Incident Advisory Capability)

Peu après l'incident du « ver Internet », le DoE (le département de l'énergie américain) créait son propre centre d'alerte pour servir ses clients.

- Le NASIRST (Nasa Automated Systems Incident Response Capability)
- L'équipe ASSIST (Automated Systems Security Incident Support Team) du DOD
- ...

Il existe plusieurs CERTs en France :

- Le CERTA : dédié au secteur de l'administration française.

Le CERTA a été inauguré en février 2000 et est rattaché à la direction centrale de la sécurité des systèmes d'information (DCSSI). C'est le gouvernement qui décida la création de cette structure afin de renforcer et de coordonner la lutte contre les intrusions dans les systèmes informatiques des administrations de l'Etat. Les deux principaux objectifs du CERTA sont d'assurer la détection des vulnérabilités et la résolution d'incidents concernant la sécurité des systèmes d'information ainsi que l'aide à la mise en place de moyens permettant de se prémunir contre de futurs incidents. Il doit donc pour cela assurer une veille technologique, mettre en place des moyens de protection, et piloter la résolution d'un incident en relation avec le réseau mondial des CERTs s'il en exprime le besoin.

- Le CERT-IST : dédié au secteur de l'Industrie, des Services et du Tertiaire.

Il a été créé à la fin de l'année 1998 par quatre partenaires : ALCATEL, le CNES, ELF et France Télécom. Il est désormais composé de 20 entreprises.

Au niveau international, le CERT-IST est membre du FIRST. Il peut ainsi s'appuyer sur un réseau mondial de plus de 120 CERTs affiliés au FIRST ; ce qui donne accès à un système d'alerte unique au monde en fournissant les points de contact nécessaires à l'investigation des incidents trans-frontaliers et en offrant un accès privilégié aux informations non encore publiques.

En France, il entretient des relations privilégiées avec le CERTA et le CERT-RENATER.

- Le CERT-RENATER : dédié à la communauté des membres du GIP-RENATER (Réseau National de télécommunications pour la Technologie, l'enseignement et la recherche).

La plupart des constructeurs ont leur propre CERT. On peut citer à titre d'exemple le CERT d'IBM : IBM ERS (Emergency Response Service) et le CERT de CISCO : Cisco PSIRT (Products Security Incident Response Team).

Du fait de cette multiplicité de CERTs, une autre structure fut mise en place, nommé FIRST (Forum of Incident Response and Security Teams) en 1990 dans le but d'avoir une meilleure communication entre ces différentes structures. Cette structure a donc pour principale mission de fortifier la coopération entre les différents CERTs en regroupant les efforts et partageant l'expertise.

Elle favorise la coopération entre les équipes pour prévenir, détecter et rétablir un fonctionnement nominal en cas d'incident de sécurité informatique. Elle fournit également un moyen de communication commun pour la diffusion de bulletins et d'alertes sur des failles potentielles et les incidents en cours. Elle aide aussi au développement des activités de ses membres, en particulier la recherche et les activités opérationnelles. Enfin, elle facilite le partage des informations relatives à la sécurité, des outils, des méthodes et des techniques.

Le FIRST organise une conférence annuelle internationale « Computer Security Incident Handling Conference » dont le thème principal est le traitement des incidents de sécurité et de favoriser le partage de l'expérience et de l'expertise dans ces domaines.

Le FIRST regroupe plus d'une centaine d'équipe.

Au niveau européen il y a le TF-CSIRT (Task Force – Computer Security Incident Response Team) qui permet de coordonner les organismes de réponses aux incidents de sécurité.

Le CERT-CC a déposé le nom CERT ; voilà pourquoi on parle parfois de CSIRT (Computer Security Incident Response Team) mais il s'agit de la même chose.

Les CERTs ont été les premiers à s'organiser et à se présenter en tant qu'organismes de veille en sécurité sur Internet.

Aujourd'hui il est difficile de connaître le nombre exact de CERTs dans le monde. Cependant en 2003, il y en avait 188 de connus : 82 en Amérique du nord, 84 (dont 51 étaient membres du FIRST) en Europe, 17 en Asie/Océanie et 5 en Amérique latine.

Ils sont très différents les uns des autres. Le JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) par exemple est dédié à un pays entier, d'autres travaillent pour une université particulière comme Oxford, une société commerciale comme Boeing ou SUN Microsystems. Enfin, certaines organisations proposent des services de CERT pour faire du profit.

Les secteurs dans lesquels on peut trouver des équipes composant des CERTs sont très variés. Le tableau ci-dessous compare les secteurs dans lesquels travaillent les CERTs d'Europe avec ceux d'Amérique du Nord pour l'année 2003.

Catégories	Amérique du Nord	Europe
Banque et Finance	8	4
Fournisseur de service de management de réseaux	15	8
Commerciale	12	5
Fabricants	10	1
Fournisseur d'accès Internet	3	13
Nationale	0	2
Recherche en réseaux	1	28
Recherche	2	2
Universitaire	12	9
Militaire	5	2
Gouvernementale	8	8
Santé	2	1
Individuelle	4	1
Total	82	84

L'Europe est caractérisé par l'importance de ses équipes travaillant dans le domaine de la recherche en réseaux. L'Amérique du Nord a plus d'entités commerciales et de fabricants.

Tous les CERTs n'obtiennent pas des fonds de la même manière. Ceux-ci peuvent être privés pour certains, publiques pour d'autres.

II.3 Rôle d'un CERT (CSIRT)

Les CERTs sont des centres d'alertes et de réaction aux attaques informatiques. Il s'agit d'associations regroupant différents organismes. Il peut s'agir de sociétés, de centres de recherches, d'administrations,...

Un CERT comprend des partenaires et des adhérents. Les partenaires décide de la stratégie et ont accès à tous les services. Les adhérents n'ont accès qu'à un sous-ensemble de services.

Suivant qu'ils sont adhérents ou partenaires, le prix de l'adhésion n'est pas le même.

Pour fonctionner efficacement, le CERT s'appuie sur :

- un réseau de correspondant sécurité au niveau des organismes qui ont passé un contrat avec le CERT pour utiliser ses services. Ces personnes (une ou deux par organisme) sont les interlocuteurs privilégiés du CERT. C'est elles qui préviennent le CERT lors d'un incident sécurité et c'est elles qui assurent la diffusion (conformément aux restrictions demandées) des informations du CERT auprès de leurs organismes.
- un réseau d'experts techniques. Ils appartiennent aux organismes affiliés au CERT ou à d'autres entités (constructeurs notamment). Ils apportent leur compétence dans un domaine d'expertise donné (certification, validation d'information avant diffusion aux correspondants, constitution de documentations, assistance technique en cas d'incidents graves).

Les sources du CERT sont donc ses correspondants sécurité, les experts techniques mais aussi tous les autres CERTs. L'intérêt premier d'un CERT est cette coordination centralisée.

Les tâches d'un CERT sont les suivantes :

- Centralisation des demandes d'assistance suite aux incidents de sécurité (attaques) sur les réseaux et les systèmes d'informations : réception des demandes, analyse des symptômes et éventuelles corrélation des incidents.
- Traitement des alertes et réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERTs, contribution à des études technique spécifiques.
- Etablissement et maintenance d'une base de données des vulnérabilités ;
- Prévention par diffusions d'informations sur les précautions à prendre pour minimiser les risques d'incidents ou au pire leur conséquences.
- Coordination éventuelle avec les autres entités (hors du domaine d'action) : centre de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CERTs nationaux et internationaux.

Les deux objectifs d'un CERT sont la prévention et la réaction en cas d'incident. Concernant la prévention le CERT émet des bulletins d'information qu'il envoie ensuite par mail à ses correspondants. Certains bulletins sont également disponibles sur Internet et consultables par tous. Ces bulletins peuvent être des avis faisant état de vulnérabilités, des alertes en cas de danger immédiat et également des recommandations (voir II.4).

Le deuxième objectif d'un CERT est de réagir en cas d'incident (voir II.5). Il propose un service d'assistance sur incident avec intervention sur site si nécessaire. Ceci

permet d'établir une relation de confiance permettant de traiter les problèmes de sécurité avec toutes les garanties de confidentialité requises. Le service permet de trouver une explication aux problèmes constatés (comportement anormal, perte de disponibilité ou de confidentialité, ...), d'en identifier les causes (volontaires ou involontaires) et l'origine. Il émet différentes recommandations, soit correctives pour pallier l'incident, soit générales pour améliorer le niveau de sécurité global.

Mis à part ces deux principaux objectifs, le CERT propose aussi des formations spécialisées, permettant d'aider à l'acquisition de compétence requise en matière d'analyse de traces et d'investigation sur incident, et de connaissance sur la sécurité des plates-formes.

Un rôle également important des CERTs est la pression mise sur les constructeurs pour qu'ils corrigent rapidement des erreurs de sécurité dans la conception de certains logiciels ou matériels.

Il est très important pour un CERT d'avoir de bonnes relations avec les structures nationales et internationales (notamment les autres CERTs), une bonne organisation avec ses réseaux de correspondants sécurité de ses organismes et des experts techniques, des contacts auprès des constructeurs, une bonne circulation et diffusion de ses informations, une bonne coordination en cas d'alerte, des actions de sensibilisation et de formation.

II.4 La diffusion d'information

Le CERT émet des avis, des alertes, des notes d'information ainsi que des recommandations.

Ces documents résultent de l'analyse et du recoupement des informations recueillies journalièrement auprès de nombreuses sources et de la qualification selon des critères objectifs.

Ces informations sont diffusées vers les correspondants sécurité au niveau des organismes qui assureront ensuite la responsabilité de la diffusion interne.

A titre d'exemple, le CERT-IST émet chaque année plus de 400 avis, une dizaine d'alertes, et met à jour plus de 500 vulnérabilités qui ont évolué.

Les avis sont des documents faisant état de vulnérabilité et des moyens de s'en prémunir.

Exemple : le CERTA a émis un avis sur la vulnérabilité du logiciel Adobe Acrobat Reader le 4 Mars 2004. Cet avis est divisé en 6 parties :

- Le **risque**: une exécution de code arbitraire.
- Les **systèmes affectés** : Adobe Acrobat Reader Version 5.1.
- Un **résumé**: une vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire par le biais d'un fichier .xdf.
- Une **description** du lecteur Adobe Acrobat Reader et un détail de la vulnérabilité.
- La **solution** : la version 6.0 d'Adobe Acrobat Reader corrige cette vulnérabilité.
- La **documentation** (site d'Adobe, Avis de sécurité de NGSSoftware qui est la source de cet avis).

Il existe dans certains avis une partie « **contournement provisoire** » qui permet de résoudre la vulnérabilité dans l'attente d'un correctif. Il peut s'agir de désactiver l'association entre un certain type d'extensions et un lecteur par exemple.

Les alertes sont des documents destinés à prévenir d'un danger immédiat.

Exemple : le CERTA a émis un bulletin d'alerte le 26 février 2004 concernant la propagation du virus Bizex. Il indique que le risque est la compromission du système et le vol d'informations confidentielles. Les systèmes affectés par ce virus sont les plates-formes Microsoft Windows, sauf Windows 3.x. Dans le résumé, on apprend que le virus semble se propager via les messageries instantanées ICQ. La description précise que le virus invite le destinataire d'un message ICQ à cliquer sur un lien HTML. En exploitant plusieurs vulnérabilités de Windows et d'Internet Explorer, il s'installe sur le système de la victime. Il capture ensuite les informations de certaines fenêtres actives dont la liste est décrite sur le bulletin qu'il stocke dans divers fichiers .log du système, et les transfère sur un serveur FTP.

Le virus se propage ensuite à tous les correspondants de la liste de contacts ICQ de la victime. Dans la partie contournement provisoire, il est indiqué de filtrer le protocole FTP en sortie afin de limiter la fuite d'informations. La solution est d'appliquer tous les correctifs sur les systèmes et de mettre à jour le système antivirus. Plusieurs liens Internet sont donnés en documentation concernant plusieurs avis et alertes de sécurité sur Internet Explorer et sur le virus.

Le CERT émet des **recommandations** et **notes d'informations**. Ces recommandations ainsi que les notes d'information permettent de sensibiliser les utilisateurs de tous niveaux.

On peut citer à titre d'exemple les deux plus récentes diffusé par le CERTA. L'une concerne la sécurité des réseaux sans fils utilisant la norme 802.11b (Wi-Fi) du 8 Août 2002. La deuxième (du 28 Mars 2002) évoque l'usage de la messagerie instantanée et les risques encourus. Dans cette dernière, le CERTA indique les précautions à prendre lors de l'utilisation de la messagerie instantanée après avoir détaillé les dangers encourus.

Mis à part l'émission d'avis de sécurité et alertes, le CERT diffuse généralement un bulletin de sécurité mensuel dans lequel il recense les vulnérabilités ayant fait ou n'ayant pas fait l'objet d'une diffusion, et traite de sujets d'actualité au travers d'études spécifiques. Il diffuse également un bulletin de sécurité hebdomadaire dans lequel il recense les évolutions des vulnérabilités. Il offre un accès aux forums pour alerter et diffuser au plus tôt. Il propose aussi un support téléphonique en cas de demande de précision sur un avis émis.

Toutes ces informations peuvent être envoyées par n'importe quel moyen de communication (mail, SMS, ...) par le CERT aux correspondants. Elles sont également disponibles sur le Web afin que les correspondants puissent y avoir accès lorsqu'ils recherchent de l'information. On parle de « push and pull ».

II.5 En cas d'incident

En cas d'alerte (attaque de sites, virus,...), le responsable sécurité du site informe le responsable sécurité de son organisme de tutelle, et contacte le CERT. Le CERT pourra alors conseiller sur l'attitude à adopter (protections immédiates, demande d'enquêtes par les autorités nationales de sécurité, dépôt de plainte) et diffuser l'alerte vers d'autres organismes ou vers les CERTs étrangers, en cas d'attaque extérieure.

Un des principes du CERT est de ne pas se substituer aux organismes impliqués dans des incidents de sécurité. Il ne diffuse d'informations sur l'incident qu'avec l'accord du site attaqué et du correspondant sécurité de l'organisme.

Mis à part ses relations avec les autres CERTs, les correspondants sécurité au niveau des organismes, des experts techniques, le CERT est aussi en relation avec les autorités nationales de sécurité et peut conseiller les sites victimes de tentatives malveillantes sur les démarches à engager vis-à-vis des autorités compétentes. Cependant, le CERT n'a pas vocation à se substituer aux sites pour leurs relations avec les autorités telles que la police ou la justice. La saisie des autorités judiciaires est de la responsabilité du site concerné ou de son autorité de tutelle. Le fait d'informer le CERT ne décharge en aucune façon la direction du site de ses responsabilités civiles et pénales.

Lors d'un incident de sécurité sur un site, un formulaire est envoyé au CERT afin d'être mis en contact rapidement avec les personnes concernées et d'assurer un meilleur suivi ainsi qu'une prévention plus efficace auprès des autres sites. Les CERTs peuvent mieux évaluer l'incident grâce à ce formulaire.

Lors de l'envoi de ce formulaire, le correspondant le signe électroniquement. Cela permet au CERT d'être sûr de l'identité du correspondant et également que le message n'a pas été modifié.

Voici un exemple de formulaire demandé par le CERT-RENATER :

=====

No incident : CERTSVP-

=====

1. VOS COORDONNEES (si vous préférez, votre signature email complète)

- 1.1. Nom:
- 1.2. Email:
- 1.3. Tel:
- 1.4. Fax:

1.5. Nom du SITE :

1.6. Nom de l'ORGANISME de tutelle:

1.7. Etes-vous CORRESPONDANT sécurité (oui/non)

=====

2. Pour chaque MACHINE COMPROMISE, indiquez :

Identification de la machine

- 2.1. Nom Complet:
- 2.2. Adresse IP:
- 2.3. Type d'incident (*):

- et si possible
- 2.4. Constructeur:
 - 2.5. OS (et version):
 - 2.6. Nom du compte compromis:
 - 2.7. Outils de sécurité installés sur cette machine (**)
 - 2.8. Y a t il eu compromission
du système (contenant)?
des informations (contenu)?

=====
Connexions illicites ou traces suspectes VENANT DE, indiquez le plus
précisément possible:

- 2.11 Nom machine:
- 2.12 Adresse machine:

- et si possible
- 2.13. Date des connexions et/ou traces:
 - 2.14. Heure (utilisez si possible une notation en GMT+/-):

- Si vous avez déjà contacté ce site:
- 2.15. Nom - email de la personne contactée:
Pourriez vous nous mettre en copie les correspondances.

=====
Connexions illicites ou traces suspectes ALLANT VERS, indiquez le plus
précisément possible:

- 2.11 Nom machine:
- 2.12 Adresse machine:

- et si possible
- 2.23. Date des connexions et/ou traces:
 - 2.24. Heure (utilisez si possible une notation en GMT+/-):

- Si vous avez déjà contacté ce site:
- 2.25. Nom - email de la personne contactée:
Pourriez vous nous mettre en copie les correspondances.

=====
(*) Choisissez dans cette liste

- Mail Spoofing:
- Pénétration:
 - Cheval de Troie:
 - Acces root:
 - Attaque NIS (pages jaunes):
 - Attaque NFS:
 - Attaque TFTP:
 - Attaque FTP:
 - Attaque Telnet:
 - Attaque Rlogin ou rsh:
- Utilisation d'une vulnérabilité (préciser le logiciel - version):
- Worm:
- Virus:
- Sniffer (nom des fichiers ?):
- Autre (préciser):

(**) Choisissez dans cette liste

COPS (The Computer Oracle and Password System):
Contrôle d'accès TCP (filtrage de paquets):
Contrôle d'accès système (wrappers, daemons modifiés):
Crack:
Tripwire:
Shadow passwords:
Autre (préciser):

=====

Grâce a ces renseignements, nous contacterons les sites impliqués
- soit directement le correspondant sécurité (site Renater)
- soit par leur prestataire de service (autre site français)
- soit par leur CERT (site non français)

Acceptez-vous que nous leur donnions vos coordonnées (oui/non) ?

=====

Avez-vous contacté un service gouvernemental ?
Si non, souhaitez-vous que nous vous mettions en contact ?

=====

Quel type d'AIDE souhaitez-vous de la part du CERT-Renater ?

=====

Ce formulaire va permettre au CERT d'analyser l'incident. Puis, il va en déduire les vulnérabilités exploitées par l'attaquant, supprimer ou réduire ces vulnérabilités, et sécuriser la machine en proposant des patches de sécurité. Il peut aussi proposer à l'organisme concerné l'installation d'outils d'audit et d'administration de sécurité et un outil de traçage.

Cette étude montre bien l'importance d'avoir une équipe chargée de l'activité de veille en sécurité. Cette activité demande du temps, notamment pour trier les informations recueillies et ne garder que celles qui concernent l'entreprise. Puis il faut s'assurer de la validité de l'information. C'est la phase de qualification. Enfin, il faut appliquer les correctifs pour résoudre les vulnérabilités. Il s'agit du premier aspect de la veille en sécurité. Le second concerne la détection d'intrusion grâce à des outils de monitoring, dans le but de savoir si des intrus tentent de pénétrer dans le réseau pour récupérer des informations confidentielles, installer des virus, des chevaux de Troie... Il faut alors revoir sa politique de sécurité et tenter de résoudre la faille qui a permis au pirate de rentrer.

Cette activité de veille en sécurité et de traitement des alertes est indispensable pour limiter le risque d'attaque malveillante. Elle est parfois réalisée, comme nous l'avons vu dans la deuxième partie, par des organismes extérieurs à l'entreprise. Les CERTs sont les plus sollicités, notamment pour leur formidable coopération entre eux. De plus, sans compter les sociétés commerciales, ils sont pratiquement les seuls à faire du traitement d'incident et à intervenir sur les sites.

Malgré toutes ces équipes chargées de détecter des vulnérabilités et de les corriger, on ne pourra pas résoudre le problème du piratage. Il faut cependant tenter de le réduire au maximum et de réagir au plus vite en cas d'incident pour se rapprocher d'une veille en sécurité parfaite, ou du moins plus efficace.

REFERENCES

Cette étude a été réalisée grâce à différentes sources :

Cours et polycopié de M. Jacky Lemée sur la sécurité des réseaux.

Sites Internet :

- <http://www.certa.ssi.gouv.fr>
- <http://www.cert-ist.com>
- http://www.renater.fr/Securite/CERT_Renater.htm
- <http://www.certa.ssi.gouv.fr/certa/certa.htm>
- <http://www.cru.fr/securite/Certs-structures/article-microbulletin>
- <http://www.urec.cnrs.fr/securite/CNRS/quefaire.html>
- <http://perso.wanadoo.fr/fiweb/secuforces.htm>
- <http://www.securityfocus.com>
- <http://www.sans.org>
- <http://www.cisco.fr/go/secu>
- <http://www.hsc.fr/services/veille.html.en>
- <http://searchnetworking.techtarget.com>
- <http://www.peleus.net/security.shtml>
- <http://birmingham-infragard.org>
- <http://www.tout-savoir.net>
- <http://encyclopédie.journaldunet.com>

Contacts avec M. Forget et M. Lemée, et M. Queinnec par *téléphone* ou *email*.