

Gracieuseté de 

# La TI et la petite entreprise

POUR

# LES NULS<sup>MD</sup>

Chapitre 4

**Sachez protéger  
votre réseau**

**À mettre  
entre toutes  
les mains!**<sup>TM</sup>

Conseils gratuits à [dummies.com](http://dummies.com)

**Chey Cobb  
Heather Ball**



## La TI et la petite entreprise Pour les Nuls<sup>4e</sup>

Publié par

**John Wiley & Sons Canada, Ltd.**

6045 Freemont Blvd.

Mississauga (Ontario) L5R 4J3

[www.wiley.com](http://www.wiley.com)

© 2008 John Wiley & Sons Canada, Ltd. Tous droits réservés.

Toute reproduction, même partielle, du contenu, de la couverture ou des icônes, par quelque procédé que ce soit (électronique, photocopie, bande magnétique ou autre) est interdite sans l'autorisation écrite de la maison d'édition.

ISBN : 978-0-470-15983-5

Pour des détails sur la façon de créer un livre personnalisé pour votre compagnie ou organisation, ou pour obtenir plus de renseignements sur le programme d'édition personnalisée de John Wiley & Sons Canada, veuillez composer le 416-646-7992 ou envoyer un courriel à [cupubcan@wiley.com](mailto:cupubcan@wiley.com).

Pour toute information d'ordre général sur John Wiley & Sons Canada, Ltd., y compris sur tous les livres publiés par Wiley Publishing, inc., veuillez communiquer avec notre dépôt au 1-800-567-4797. Pour toute information concernant les revendeurs, y compris les rabais et les ventes à primes, veuillez appeler notre service des ventes au 416-646-7992. Pour obtenir des copies des critiques de presse, des entrevues avec l'auteur ou toute autre information publicitaire, veuillez communiquer avec notre service de marketing par téléphone au 416-646-4584 ou par télécopieur au 416-236-4448.

**LIMITE DE RESPONSABILITÉ/DÉNI DE GARANTIE : L'ÉDITEUR ET L'AUTEUR N'ÉMETTENT AUCUNE REPRÉSENTATION OU GARANTIE QUANT À L'EXACTITUDE OU À L'INTÉGRALITÉ DU CONTENU DU PRÉSENT OUVRAGE; EN PARTICULIER, ILS NIENT TOUTE GARANTIE, Y COMPRIS, SANS Y ÊTRE LIMITÉ, LES GARANTIES D'APPROPRIATION POUR UN USAGE PARTICULIER. AUCUNE GARANTIE NE PEUT ÊTRE CRÉÉE OU OFFERTE PAR LES REPRÉSENTANTS COMMERCIAUX OU DANS LES DOCUMENTS DE VENTE. LES CONSEILS ET STRATÉGIES CONTENUS DANS CET OUVRAGE PEUVENT NE PAS CONVENIR À VOTRE SITUATION. LE PRÉSENT OUVRAGE EST PUBLIÉ, ÉTANT ENTENDU QUE L'ÉDITEUR N'OFFRE PAS DE SERVICES JURIDIQUES, COMPTABLES OU AUTRES SERVICES PROFESSIONNELS. LES LECTEURS QUI VEULENT OBTENIR UNE AIDE PROFESSIONNELLE DOIVENT S'ADRESSER À UN PROFESSIONNEL COMPÉTENT. NI L'ÉDITEUR NI L'AUTEUR NE SERONT TENUS RESPONSABLES DE DOMMAGES QUELCONQUES DÉCOULANT DU CONTENU DU PRÉSENT OUVRAGE. LA MENTION D'UNE ORGANISATION OU D'UN SITE WEB DANS LE PRÉSENT OUVRAGE EN CITATION ET/OU COMME SOURCE POTENTIELLE DE RENSEIGNEMENTS NE SIGNIFIE PAS QUE L'AUTEUR OU L'ÉDITEUR ENTÉRINENT LES RENSEIGNEMENTS OU LES RECOMMANDATIONS QUE PEUVENT FOURNIR L'ORGANISATION OU LE SITE WEB. EN OUTRE, LES LECTEURS DOIVENT SAVOIR QUE LES SITES WEB MENTIONNÉS DANS LE PRÉSENT OUVRAGE PEUVENT AVOIR CHANGÉ OU DISPARU DEPUIS LA RÉDACTION DE L'OUVRAGE.**

**Marques de commerce :** Wiley, le logo de Wiley Publishing, Pour les Nuls, le logo du personnage Dummies Man, A Reference for the Rest of Us!, À mettre entre toutes les mains!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com, ainsi que la présentation des produits sont des marques de commerce ou des marques déposées de John Wiley & Sons, inc. aux États-Unis, au Canada et tout autre pays, et ne doivent pas être utilisés sans autorisation écrite. La maison d'édition John Wiley & Sons Canada, Ltd. n'est pas associée aux produits ou aux fournisseurs mentionnés dans le présent ouvrage.



## Chapitre 4

---

# La sécurité des réseaux



### *Dans ce chapitre*

- ▶ L'importance de la sécurité des réseaux
- ▶ Les menaces potentielles à la sécurité
- ▶ Les mesures de sécurité



**L**e chemin à parcourir pour assurer la sécurité d'un réseau n'est pas obligatoirement long ou ardu. Nombreux sont les spécialistes dans l'industrie qui aimeraient vous faire croire qu'il s'agit d'une entreprise complexe et coûteuse et qu'il vaut mieux la laisser entre leurs mains expertes. En vérité, toute personne possédant un niveau moyen d'expérience des ordinateurs et des réseaux est capable de mettre en œuvre les mesures de base pour protéger son réseau. Des études du FBI ont révélé que plus de 80 pour cent des attaques contre des réseaux pourraient être évitées avec des mesures élémentaires de sécurité. Le présent chapitre vous aidera à cerner les principaux problèmes de sécurité des réseaux et vous montrera comment protéger le vôtre.

## *L'importance de la sécurité des réseaux*

Bien des propriétaires de petite entreprise font la même erreur. Ils se disent : « J'ai juste une petite entreprise qui ne vaut pas grand-chose. Mon réseau d'ordinateurs n'intéresse pas les pirates informatiques. » Nous ne saurions trop insister sur le fait qu'il n'y a rien de plus faux.

Si vous ne prenez pas les mesures adéquates pour protéger votre réseau, vous faites courir un grave risque à votre entreprise. Au cours des sections qui suivent, nous nous pencherons sur les sources potentielles d'atteinte à la sécurité des réseaux.

## *Les faiblesses en matière de sécurité*

Bien que les réseaux soient organisés différemment et aient des fonctions spécifiques, ils sont étonnamment similaires sur le plan des exigences fondamentales en matière de sécurité. Il faut un mot de passe pour accéder à un réseau, et tous les réseaux sont vulnérables (un virus pourrait infecter le vôtre, par exemple, ce dont traite la section « Les virus » plus loin dans ce chapitre). Il est donc essentiel de mettre en place de solides mesures de sécurité pour protéger votre réseau, de discuter de toutes ces questions avec votre conseiller en TI, de déterminer si vous avez besoin d'une protection et d'en choisir la forme.



La *posture de sécurité* d'une organisation est définie par sa méthode de protection, la solidité de ses mesures de protection et sa philosophie de protection. Si vous prenez un minimum de mesures de protection et que vous ne sentez pas vraiment le besoin d'en faire plus, on peut dire que vous avez une posture de sécurité faible ou passive. Par contre, ceux qui mettent en œuvre de solides mesures de protection, qui ont un programme complet de formation et d'instruction en la matière et qui surveillent régulièrement leur niveau de sécurité ont une posture forte.

## *Les mots de passe faibles*

Les mots de passe sont souvent la seule mesure de protection des systèmes informatiques. L'identificateur d'utilisateur n'est en fait qu'un nom et il ne confirme pas réellement l'identité de l'utilisateur, ce que fait par contre le mot de passe qui y est associé. Les mots de passe sont donc les clés de votre réseau — et il n'y a rien de plus facile à trouver pour un pirate. Un seul mot de passe non protégé peut permettre à n'importe qui de se connecter à l'un de vos ordinateurs et d'accéder à votre réseau.



N'importe quel pirate informatique peut obtenir les mots de passe de votre réseau très facilement. Les mots de passe circulent constamment dans un réseau, et un simple programme d'interception illicite bien placé (qu'on appelle un *renifleur de mots de passe*) permet de recueillir des centaines, voire des milliers de mots de passe en quelques heures. « Ah », dites-vous, « mais ces mots de passe sont cryptés! » Parfois, oui, mais la plupart du temps, la méthode de cryptage employée n'est pas très sûre. Il est facile de trouver sur Internet des logiciels de décryptage de mots de passe, qui les décodent en général sans trop de difficulté.



Nous recommandons fortement de faire en sorte que tout utilisateur du réseau informatique de votre entreprise change régulièrement de mot de passe.

L'emploi de mots de passe forts et difficiles à décrypter est un moyen facile de protéger la sécurité de votre réseau. Votre personnel et vous devez vous efforcer de créer des mots de passe forts. Et que signifie exactement un mot de passe fort ? Grosso modo, un *mot de passe fort* est un mot qui ne figure dans aucun dictionnaire, français ou autre, et que personne ne peut deviner facilement. Les longs mots de passe, par exemple, sont plus difficiles à décrypter ou à deviner que ceux plus courts.

Les conseils qui suivent vous aideront à établir des mots de passe forts pour tous les utilisateurs de votre réseau :

- ✔ **Ne pas choisir un mot de passe qui fasse référence à un élément de sa vie personnelle.** Évitez de prendre comme mot de passe le nom de votre chat, le titre de votre émission de télé favorite, votre date de naissance ou le nom de l'équipe de soccer de votre enfant. S'il est possible que quelqu'un le devine, ce n'est pas un bon mot de passe.
- ✔ **Utiliser une combinaison de lettres qui ne représente rien.** Les meilleurs mots de passe sont ceux qui ne sont pas des mots. Par exemple, si vous prenez la première lettre de chaque mot du proverbe « La parole est d'argent, mais le silence est d'or », vous obtenez « lpedamlsedo ». C'est un bon mot de passe et il est facile à mémoriser, mais lisez le point suivant pour savoir comment le rendre encore plus sûr.



- ✓ **Mélanger les minuscules et les majuscules.** Placez des majuscules ailleurs qu'au début du mot de passe et employez des chiffres. Par exemple, puisque la lettre « L » minuscule ressemble au chiffre « 1 », vous pouvez substituer ce chiffre à la lettre; votre mot de passe deviendra alors « 1pedam1sedo ».
- ✓ **Créer un mot de passe d'au moins huit caractères.** Les meilleurs mots de passe sont les plus longs.
- ✓ Les administrateurs de système avec *avantages de base* (c'est-à-dire sans restriction d'accès et avec la capacité d'effectuer toutes sortes de modifications) doivent avoir le mot de passe le plus fort possible et obéir aux plus strictes règles concernant son changement et sa réutilisation.
- ✓ **Changer son mot de passe régulièrement.** Chaque utilisateur devrait modifier son mot de passe tous les 60 jours, même s'il est très fort. Plusieurs systèmes d'exploitation vous permettent de programmer ce changement pour chacun des utilisateurs. Certains d'entre eux trouvent cette pratique fastidieuse, mais c'est une sage mesure de sécurité.
- ✓ **Créer de nouveaux mots de passe au lieu de toujours réutiliser les mêmes.** Attendez un an, voire 18 mois, avant de réutiliser un mot de passe.
- ✓ **Ne pas utiliser de suites de caractères telles qu'elles apparaissent sur un clavier.** Ne jamais prendre « qwerty », « 12345678 », « asdfghj » ou tout autre enchaînement similaire comme mot de passe. Bien que ces combinaisons n'aient pas de sens comme tel, elles suivent un patron clair de succession sur le clavier, et les décrypteurs peuvent les deviner en quelques secondes.
- ✓ **Traiter son mot de passe comme un renseignement top secret.** Ne divulguez jamais votre mot de passe. Ne l'écrivez pas sur un bout de papier que vous collez sur votre ordinateur ou que vous glissez sous le clavier, là où tout le monde peut le trouver.
- ✓ **Ne pas hésiter à changer son mot de passe.** Si l'un de vos employés soupçonne qu'on a décrypté son mot de passe, faites-le-lui changer immédiatement.



Avoir un mauvais mot de passe est aussi dangereux que ne pas avoir de mot de passe du tout.

## Les virus

Le courrier électronique est un outil extraordinaire. Il accroît la productivité et facilite la communication. Malheureusement, c'est aussi l'un des moyens les plus courants de transmission de virus et de programmes malveillants, qui peuvent ravager votre réseau et endommager les données qu'il renferme.

Les virus ne sont pas la seule menace que représentent les courriels. Votre réseau compte-t-il des utilisateurs qui ouvrent les pièces jointes aux courriels qu'ils reçoivent ou encore des fichiers exécutables, comme les jeux et les économiseurs d'écran? Plusieurs programmes malveillants emploient ces moyens pour pénétrer dans les systèmes informatiques. On nomme ces programmes des *chevaux de Troie* (ou des *programmes troyens*). Ils peuvent affecter votre ordinateur directement (en effaçant le disque dur, par exemple) ou indirectement (notamment en y installant un renifleur pour recueillir les noms d'utilisateurs et les mots de passe).

Les logiciels antivirus constituent votre meilleure protection possible. Bien qu'ils ne soient pas sûrs à cent pour cent, il serait stupide de ne pas s'en servir, en particulier pour un réseau. Sans un tel logiciel, rien ne protège votre réseau contre l'infection. Les logiciels antivirus comprennent deux éléments : le moteur de balayage et les fichiers signature. Le *moteur de balayage* dit au logiciel où et comment chercher les problèmes, et les *fichiers signature* sont essentiellement une base de données des virus connus et de leurs effets. Le moteur de balayage compare les fichiers qui se trouvent dans votre ordinateur aux données sur les virus connus des fichiers signature. Quand le fabricant d'un de ces logiciels découvre de nouveaux virus, il produit une mise à jour de ses fichiers de données pour y inclure cette nouvelle souche.

Vous devez mettre à jour le moteur de balayage et les fichiers signature de façon régulière, sinon votre logiciel antivirus perdra de son efficacité. Il est habituellement possible de programmer les antivirus pour qu'ils effectuent automatiquement leur propre mise à jour. Si ce n'est pas le cas, vous pouvez y procéder manuellement avec la fonction de mise à jour du logiciel, ou consulter le site Web du fournisseur.



Pour qu'un logiciel antivirus soit vraiment efficace, vous devez l'installer sur tous les ordinateurs qui composent votre réseau ainsi que sur le serveur. C'est le seul moyen d'attraper les virus à tous les points d'entrée.

## Les failles logicielles

Tous les logiciels et systèmes d'exploitation ont des lacunes sur le plan de la sécurité. Certaines sont plus problématiques que d'autres, mais elles permettent toutes à des utilisateurs non autorisés d'entrer dans votre réseau.

Les programmes contiennent des millions et des millions de lignes de texte, ce qu'on appelle du *code*, et il est extrêmement difficile et exigeant d'identifier les sections du code correspondant à des lacunes sur le plan de la sécurité. La plupart des fabricants de logiciels ne considèrent pas que les dépenses à encourir pour rendre leurs produits plus sûrs soient justifiées. Les pirates informatiques expérimentés, par contre, consacrent leur temps à étudier le code et les fonctionnalités des logiciels, à la recherche de tels défauts, puis à créer des programmes qui les exploitent. Ces pirates diffusent ensuite leurs logiciels gratuitement sur Internet afin que n'importe qui puisse s'en servir.

Les fabricants savent que leurs logiciels ont des milliers de failles et ils publient assez fréquemment des corrections, nommées *corrections de bogue*, *réparations à chaud*, *retouches*, *programmes de correction* et parfois *mises à jour*. En général, il est assez facile de télécharger et d'installer ces corrections, mais leur installation prend souvent plusieurs heures. Les *pare-feu* sont des programmes conçus pour empêcher les utilisateurs non autorisés de pénétrer dans votre réseau. Ils parviennent à combler certaines failles des logiciels. Cela dit, pour une protection adéquate, il est toujours recommandé d'installer les corrections dès qu'elles sont disponibles. Demandez à votre conseiller en TI comment effectuer la recherche et l'installation régulières des mises à jour et des corrections pour les logiciels que votre entreprise utilise.

## Les arnaques

Les employés sont probablement le plus grand atout d'une entreprise, mais ils peuvent malheureusement aussi être le maillon le plus faible de son système de sécurité de réseau, et

ce, bien malgré eux. La majorité des gens sont de nature confiante, ce qui les rend particulièrement vulnérables à l'ingénierie sociale. L'*ingénierie sociale* est un terme élégant pour désigner une arnaque. Tous les jours, des tas de gens se font manipuler et vont jusqu'à divulguer leurs mots de passe et d'autres données très importantes.

Vous avez probablement déjà entendu parler de personnes qui se sont fait avoir par l'un de ces courriels dans lesquels un prince d'un pays lointain affirmait qu'il transférerait des millions de dollars à leur compte bancaire si seulement elles lui en donnaient le numéro. On peut se demander comment on peut faire preuve d'une telle crédulité, mais il ne faut jamais oublier que l'erreur est humaine.

Supposons que vous avez un nouvel employé, que nous appellerons Jacques. Il reçoit un appel d'une personne affirmant travailler pour le fournisseur d'accès Internet (FAI) de votre entreprise. Elle explique à Jacques qu'il doit changer certains réglages de son ordinateur et qu'il faut tester son mot de passe. Jacques veut bien sûr se montrer obligeant. Il ne lui vient pas à l'esprit de s'assurer d'abord que l'appel provient bel et bien du FAI; de toutes façons, il n'a aucune idée du nom du FAI de l'entreprise. Ça pourrait d'ailleurs être un véritable employé du FAI à l'autre bout du fil... ou encore un pirate informatique qui vient d'obtenir un nom d'utilisateur et un mot de passe valides pour pénétrer dans votre réseau.



Pour que votre programme de sécurité soit efficace, non seulement vous devez protéger votre réseau, mais vous devez également être capable d'empêcher les intrus éventuels d'arnaquer vos employés. Aucun pare-feu ni aucun programme de retouche ne peuvent éliminer cette menace. La formation et la prise de conscience des employés sont les seules mesures de sécurité utiles à cette fin.

Assurez-vous qu'aucun de vos employés ne révèle d'information concernant votre réseau, notamment son nom d'utilisateur, son mot de passe et même le nom des logiciels que vous utilisez, sans savoir d'abord à qui il s'adresse et pourquoi cette personne a besoin du renseignement demandé.

## Les pirates informatiques

Les pirates sont des gens ferrés en informatique qui parviennent à accéder à des réseaux sans autorisation et qui s'appliquent à y semer le chaos. Certaines personnes, souvent même celles qui en ont été les victimes, décrivent les pirates comme des terroristes informatiques. En général, ces pirates savent élaborer des programmes d'attaque ordinaires et ont une connaissance approfondie de la façon dont les réseaux communiquent. Les pirates informatiques constituent une menace sérieuse : ils sont capables de s'introduire dans votre réseau (ou dans n'importe quel autre), si vous y avez laissé des brèches. Comme ils connaissent bien les systèmes, ils peuvent voler des renseignements exclusifs à votre entreprise.

Tous les ordinateurs reliés à un réseau — et Internet aussi est un réseau — ont un numéro d'identification, un peu comme un numéro de téléphone. Un pirate ne peut pas deviner à partir du numéro d'un ordinateur si le réseau auquel il est connecté est petit ou grand; alors, si vous croyez qu'ils ne s'attaquent pas aux petites entreprises, détrompez-vous.



Aux yeux des pirates informatiques, vous n'êtes qu'une cible de plus. Ils recherchent tout ce qui peut leur sembler intéressant. S'ils ne trouvent rien d'intéressant dans votre réseau, il est possible qu'ils s'en servent pour attaquer d'autres réseaux.

Lorsqu'un pirate s'introduit dans votre réseau, il a accès à tous les renseignements et à toutes les données qui appartiennent à votre entreprise, y compris ceux concernant vos clients, votre personnel, votre situation financière et vos opérations.

Les pirates informatiques ne disparaîtront pas. Vous devez donc faire tout en votre pouvoir pour les empêcher d'entrer dans votre réseau. Voici les meilleurs moyens de se défendre contre eux :

- ✓ Créer des mots de passe forts et en changer régulièrement.
- ✓ Faire preuve de prudence avant d'ouvrir une pièce jointe à un courriel, même si on en connaît l'expéditeur. Si on

n'est pas sûr qu'une pièce jointe est sans danger, il vaut mieux en parler à son conseiller en TI avant de l'ouvrir.

- ✓ Télécharger les corrections de sécurité pour les logiciels dès qu'elles sont disponibles.
- ✓ S'assurer que son système d'exploitation est muni d'un pare-feu et activer ce dernier.
- ✓ Échanger des fichiers uniquement avec les employés et autres contacts en qui on a confiance.

## *Les anciens employés*

Les gens qui quittent votre organisation représentent une menace réelle à la sécurité de votre système informatique. Vos employés emportent-ils des dossiers de l'entreprise quand ils s'en vont? Qu'y a-t-il pour les en empêcher? Réfléchissez sérieusement à ces questions et répondez-y en toute honnêteté.

Des employés qui croient que votre entreprise les a traités de façon irrégulière ou contraire à l'éthique peuvent partir en vous en gardant rancune. Ils envisageront peut-être alors de s'introduire dans votre réseau pour créer des dommages ou pour voler des données importantes. Si un tel employé ne parvient pas à pénétrer dans votre système, il peut recruter un complice parmi ses ex-collègues pour l'aider à concrétiser ses intentions malicieuses.

La liste ci-dessous énumère quelques précautions qu'une entreprise devrait prendre pour protéger la sécurité de son réseau à la suite d'un renvoi.

- ✓ **Annuler l'accès au réseau.** Quand un employé s'en va, annulez immédiatement son accès au courriel et au réseau. Si vous avez besoin des dossiers de son répertoire personnel, l'administrateur du système dispose des outils nécessaires pour les récupérer. Assurez-vous de ne laisser aucune possibilité pour vos anciens employés d'entrer dans votre système informatique.
- ✓ **Reprendre les clés et la carte d'identité.** La plupart des entreprises demandent à leurs employés de leur remettre leurs clés et leur carte d'identité au moment de leur

départ. Cette pratique garantit que les anciens employés ne peuvent revenir sur les lieux par la suite.

- ✓ **Effectuer des entrevues de fin d'emploi.** Si votre entreprise fait des entrevues de fin d'emploi, conservez tous les dossiers relatifs au processus d'entrevue. En cas de menaces de l'employé, même voilées, vous avez la preuve de ce qu'il a dit et à qui.

## *Protéger un réseau*

Il existe de nombreuses précautions concrètes qui sont faciles à mettre en œuvre pour assurer la sécurité d'un réseau d'entreprise. Les sections qui suivent vous donnent des conseils qu'il vaut la peine de suivre.

### *Changer la configuration par défaut*

L'une des erreurs les plus fréquemment commises par ceux qui souhaitent établir un réseau informatique est probablement celle d'installer le système tel quel, avec la configuration par défaut (les réglages standard que le fabricant installe sur tous les exemplaires du système). Les comptes d'administrateurs et les mots de passe des configurations par défaut sont connus par les pirates informatiques du monde entier.

Cette erreur affecte les routeurs, les concentrateurs, les interrupteurs, les systèmes d'exploitation, les systèmes de courrier électronique et d'autres applications serveurs, dont les bases de données et les serveurs Web. Nous ne connaissons aucun logiciel qui en soit à l'abri.

En plus du fait que les mots de passe des configurations par défaut sont connus, celles-ci renferment de multiples failles sur le plan de la sécurité qu'il vous faudra combler. Avant de brancher un ordinateur sur l'Internet, assurez-vous d'en avoir modifié les noms de compte et les mots de passe par défaut et d'avoir installé les retouches de sécurité. Vous vous épargnerez bien des peines ultérieures si vous consacrez un peu plus de temps à la configuration de vos ordinateurs à

cette étape. Moins vous laisserez de failles dans votre réseau, plus il sera difficile pour quelqu'un de s'introduire dans votre système informatique.

## *L'installation des mises à jour de sécurité*

Presque tous les logiciels contiennent des failles sur le plan de la sécurité. Des sites Web comme celui de la *Computer Emergency Response Team* (CERT, au [www.cert.org](http://www.cert.org), en anglais seulement) et *Security Focus* (au [www.securityfocus.com](http://www.securityfocus.com), également en anglais) donnent des dizaines de nouvelles alertes chaque jour. Il est essentiel que la personne responsable de la sécurité de votre réseau soit au courant de ces alertes. Elle devrait s'abonner à l'un des nombreux services d'alerte qui informe leurs clients par courriel de problèmes précis. Plusieurs de ces services vous permettent de ne vous abonner qu'aux alertes qui concernent votre système informatique. Dès qu'une telle alerte est émise, on vous fournit la correction pour que vous l'installiez sur vos ordinateurs. Bien que ces activités prennent beaucoup de temps et qu'il ne soit pas toujours pratique de s'y adonner, c'est une des mesures de sécurité les plus efficaces pour votre réseau. Aucun pare-feu au monde ne peut empêcher les pirates informatiques d'entrer dans votre système si vous laissez la porte arrière ouverte.



Dès que les fabricants de logiciels publient une alerte, les pirates informatiques commencent à chercher dans Internet les ordinateurs connectés qui sont vulnérables aux attaques ayant rendu l'alerte nécessaire. Dès qu'ils en trouvent, ils en communiquent l'adresse à d'autres pirates qu'ils rencontrent dans des clavardoirs et sur des sites Web spécialisés.

## *La sauvegarde des données*

Quand un intrus saccage un système informatique, la meilleure chose à faire est de mettre le système en mode autonome et de le remettre à l'état initial à partir de la copie de sauvegarde. Vous avez bien fait une copie de sauvegarde récemment, n'est-ce pas? Excellent. Êtes-vous sûr qu'elle est *récupérable*? (Nous ne vous accordons vraiment aucun répit,

n'est-ce pas?) Certains types de sauvegardes servent uniquement à des fins d'archivage et ne sont pas conçus pour remettre un système à son état initial. Il arrive aussi parfois qu'on découvre, trop tard, que les copies de sauvegarde sont inutiles parce que leur répertoire contient des données altérées. Il est essentiel que vous testiez vos copies de sauvegarde à l'occasion pour vous assurer qu'elles sont en bon état.

Effectuer une copie de sauvegarde d'un système informatique, c'est comme utiliser la soie dentaire : tout le monde sait qu'il faut le faire à fond et fréquemment, mais peu de gens le font très souvent et encore moins, adéquatement. Comme il existe des centaines de fournisseurs de solutions de sauvegarde, il nous est impossible d'en parler ici en détail. Cela dit, nous vous proposons une méthode pour éviter le chaos dans le processus de sauvegarde :

- ✓ **Le premier jour de chaque semaine** : Procédez à la sauvegarde complète du système, y compris les fichiers qui se trouvent sur chacun des ordinateurs.
- ✓ **Les autres jours de la semaine** : Faites une sauvegarde incrémentielle, qui ne touche que les fichiers créés ou mis à jour depuis la dernière sauvegarde.
- ✓ **Une fois par mois** : Gardez l'une des copies de sauvegarde à des fins d'archivage. Ainsi, s'il vous faut restaurer votre système, vous n'aurez jamais à remonter à plus d'un mois.



Ne jamais conserver son support de sauvegarde au même endroit que ses ordinateurs. Ainsi, si les locaux qui abritent vos ordinateurs sont affectés par un sinistre, comme un incendie ou une tornade, au moins votre copie de sauvegarde est en lieu sûr et vous pouvez remettre votre réseau sur pied en peu de temps.

La sauvegarde d'un système n'empêche pas les intrusions dans votre réseau ni le piratage, mais elle peut vous aider à récupérer d'une telle attaque. Comme les vandales d'Internet s'en prennent souvent aux serveurs Web, bien des gens choisissent de se créer un *réflecteur* (aussi appelé *site miroir*) pour contrer cette menace. Si votre site Web se fait attaquer, il vous est alors facile de relancer une version qui fonctionne, après bien entendu avoir réglé la faille qui a permis à un intrus de s'introduire dans votre système.

## La protection contre la surtension et les pertes

La protection contre la surtension et les pertes va de pair avec la sauvegarde régulière du système. En réseautique, il est essentiel que le système reste en fonction. Si votre réseau tombe en panne, votre entreprise pourrait en être sérieusement affectée.

Si votre entreprise est située rue des Éclairs, vous apprendrez assez rapidement la nécessité d'avoir des *limiteurs de surtension*, qui empêchent les hausses de tension électrique d'éteindre et d'endommager votre réseau, et des *unités d'alimentation sans coupure* (ou *UPS*, pour « unintermittible power supply »), qui gardent votre réseau en marche — grâce à leur batterie — lors des pannes d'électricité.



Tout système essentiel requiert une certaine mesure de redondance au cas où certains de ses éléments tomberaient en panne, que ce soit à cause d'un acte de piratage ou d'une catastrophe naturelle. On peut, par exemple, faire une copie de son site Web sur un autre appareil. De cette façon, si le site Web principal souffre d'ennuis mécaniques ou de l'attaque d'un pirate, on n'a qu'à débrancher le site affecté et brancher le site redondant.



Il n'est pas nécessaire de prévoir l'achat d'équipement haut-de-gamme dans votre plan de redondance. Souvent, les appareils dont on pensait se défaire peuvent très bien faire l'affaire dans les situations d'urgence.

## La téléconnexion

Permettez-vous la *téléconnexion* à votre réseau, c'est-à-dire la connexion d'utilisateurs étant à l'extérieur de vos bureaux? Si oui, vous pouvez l'ajouter à la liste de vos faiblesses sur le plan de la sécurité. La téléconnexion par modem est une préoccupation importante, car elle implique que vous laissez des gens entrer dans votre réseau depuis l'extérieur de l'édifice. Il est impératif que l'ordinateur employé pour se téléconnecter soit aussi bien protégé que le réseau interne; le contraire équivaut tout simplement à chercher des problèmes.

Prenons l'exemple des ordinateurs portatifs. Bien des employés en voyage d'affaires se connectent au réseau de leur employeur avec un ordinateur portable de l'entreprise. Pour accélérer le branchement et s'éviter la tâche répétitive d'inscrire leur nom d'utilisateur et leur mot de passe, plusieurs de ces employés demandent à leur ordinateur de mémoriser ces renseignements. Malheureusement, si quelqu'un vole l'ordinateur portable et que celui-ci n'a pas de dispositif de sécurité pour empêcher le voleur de s'en servir, il peut se connecter très rapidement au réseau de l'entreprise. Le pire, c'est qu'il n'y a pas moyen de savoir qu'il s'agit d'un utilisateur non autorisé, puisque le voleur se connecte avec un nom d'utilisateur et un mot de passe légitime... sans déclencher de signal d'alarme!



Il est essentiel que vous protégiez tous les ordinateurs qui se téléconnectent à votre réseau contre leur utilisation non autorisée, par exemple en créant un mot de passe pour le *système d'entrée-sortie de base* (aussi nommé BIOS). Le BIOS est le programme qui sert à lancer le système d'un ordinateur quand on l'allume. Un mot de passe est alors requis pour que le BIOS s'active et fasse démarrer l'ordinateur. Vous devriez aussi envisager le cryptage des données de vos ordinateurs portatifs, car la plupart des voleurs ne se donnent pas la peine d'essayer de décrypter les données. Ils ne font que reformater le disque dur et vendre l'ordinateur.



Certains emploient des logiciels de connexion à distance comme PCAnywhere, qui permettent l'échange de données entre deux ordinateurs. Ces programmes ont leurs propres lacunes sur le plan de la sécurité. Il est alors prudent de demander à son fournisseur si des corrections ont été émises pour ce produit.

Telnet et FTP sont deux protocoles de transfert de fichiers à distance dont les gens tendent à oublier les faiblesses en matière de sécurité. *Telnet* est un programme de connexion qui permet à l'utilisateur de travailler comme s'il était assis devant l'ordinateur dont il modifie les fichiers. Les administrateurs de système s'en servent fréquemment pour apporter des modifications importantes à des ordinateurs qui se trouvent dans un autre bureau ou dans un autre édifice. En utilisant Telnet, il n'ont pas à faire l'effort de s'y rendre en

personne. Malheureusement, comme Telnet donne aux personnes autorisées l'accès à un ordinateur situé ailleurs, il est possible que des intrus malveillants entrent eux aussi dans le réseau. Si un pirate parvient à deviner ou à déchiffrer votre mot de passe de Telnet, il lui est facile de changer vos configurations ou d'installer des logiciels indésirables dans votre système informatique.

Les programmes FTP ont toutes sortes de faiblesses, ce que les pirates informatiques ont su exploiter récemment. L'abréviation *FTP* signifie « file transfer protocol », ou *protocole de transfert de fichiers*. On se sert des FTP pour déplacer, copier ou effacer des fichiers. Comme Telnet, ils permettent de se connecter à un ordinateur situé dans un autre endroit. On peut télécharger des retouches de sécurité et obtenir en ligne des conseils sur la configuration, et il faut créer des comptes utilisateurs et obtenir des permissions pour employer ce type de service. Et comme toujours, vous devez avoir des mots de passe forts! (Consultez la section « Les faiblesses en matière de sécurité » pour savoir comment élaborer un mot de passe fort.)

## *Savoir en qui avoir confiance*

Évidemment, vous connaissez les gens qui travaillent avec vous au bureau, mais qu'en est-il de ceux qui sont connectés en aval ? Les *connexions en aval* sont celles qui dépassent les limites du réseau d'une entreprise, comme celles des partenaires d'affaires ou des clients. Posez-vous les questions suivantes pour savoir si votre réseau est protégé adéquatement :

- Avez-vous configuré vos ordinateurs pour qu'ils fassent confiance aux ordinateurs d'autres entreprises pour l'échange de données?
- Êtes-vous sûr d'avoir l'adresse IP exacte de ces entreprises?
- Y a-t-il une limite au nombre de réseaux que vous considérez fiables?
- Si vous permettez la téléconnexion, savez-vous exactement qui se branche sur votre réseau?

Votre réseau contient des fichiers qui donnent la liste de vos connexions considérées comme fiables. Assurez-vous que les adresses de ces réseaux sont exactes. N'oubliez pas de vérifier si vos pare-feu et routeurs ont eux aussi les bonnes adresses pour ces connexions. Prenez l'habitude de réviser régulièrement tous ces renseignements afin d'éviter les erreurs et d'avoir en tout temps des données à jour et exactes. Si vous mettez fin à une entente avec un autre réseau, éliminez-en dès que possible l'adresse et prenez les mesures nécessaires pour bloquer toute tentative de connexion à partir de ce réseau.