TECHnologies
Cahier spécial
LES AFFAIRES
L'informatique et la gestion

Espionnage

Seulement 10 % des incidents informatiques seraient le fait de *hackers*. Selon des experts, une bonne partie des bris de sécurité dans les entreprises proviennent de l'interne **p. T2**

Sondage

Les infections par virus sont les ennuis les plus souvent rencontrés, mais malgré tout, près de 90 % des entreprises québécoises se disent bien protégées **p. T4**

Virus

La lutte aux virus informatiques est un combat de tous les instants. Les technologies se raffinent pendant que les attaques des intrus se perfectionnent. Il existe par contre plus d'une façon de parer les coups **p. T6**

Vulnérabilité

La protection par simple mot de passe ne suffit plus. Désormais, tout système d'exploitation doit offrir des garanties en ce qui concerne la sécurité des services réseau. Le géant américain **Microsoft** a doté son système d'exploitation *Windows 2000* de plusieurs fonctions de sécurité, mais la question demeure entière. Est-ce que ce sera suffisant ? **p. T13**

Trop d'entreprises se sentent faussement en sécurité

La confiance en la fiabilité du système n'est pas justifiée partout

Yan Barcelo

« Une mauvaise sécurité est pire que pas de sécurité du tout : parce qu'on se fie alors sur un système qui ne justifie pas notre confiance. »

La maxime est d'**Éric Maurice**, directeur d'**eTrust**, une filiale de **Computer Associates** qui se spécialise dans les solutions de sécurité pour les entreprises.

La principale erreur que commettent les entreprises, dit M. Maurice, est de se fier sur un seul outil majeur de sécurité, ou de quelques-uns qui, en fait, ne comblent qu'une partie des besoins de sécurité.

En d'autres termes, on s'occupe de barricader la porte avant et la porte arrière de notre maison, mais on néglige de fermer les fenêtres.

Une image fréquente qu'ont les entreprises de la sécurité est celle d'une forteresse où les entrées sont surveillées par des sentinelles qui vérifient les papiers de tous les passants. C'est la fonction qu'on confie aux pare-feu (*firewalls*).

Ils sont autorisés de laisser passer à Montréal toutes les voitures en provenance de l'autoroute 20, et de bloquer toutes les autres. « Mais cette vérification ne dit pas ce que la voiture transporte; elle ne dit que d'où elle vient », affirme M. Maurice.

Par exemple, ce contenu peut très bien être un virus, dont il faudrait identifier le code. Mais après une attaque comme celle du virus *ILoveYou*, il est clair que les entreprises ne sont pas équipées pour s'en protéger. « J'ai été sidéré de voir le nombre d'entreprises qui croyaient que leur pare-feu était supposé les protéger de ce genre d'attaque », dit M. Maurice.

Il existe bien sûr des antivirus. Mais ces logiciels ne peuvent fonctionner qu'en identifiant une similitude d'empreintes entre un nouveau virus et un ancien. Un virus qui porte une toute nouvelle empreinte échappera complètement à leur surveillance.

Comment alors se protéger d'un *ILoveYou* qui présente un nouveau *code génétique* ? eTrust propose un logiciel, *eTrust Content Inspection*, qui vérifie et valide les opérations de base où les virus tentent de mener leurs actions illicites : accès aux disques durs, accès aux *cookies*, commande *format* du disque dur.

Il reste qu'il faut être bien conscient que le système de sécurité parfait n'existe pas, avertit M. Maurice. Mais trop de gens ont une vue statique de leur sécurité, l'imaginant comme une forteresse. M. Maurice propose plutôt de la voir comme une course.

« C'est une course où je cours plus vite que les pirates et les intrus. Il faut faire en sorte que s'il y a intrusion, le malfaiteur ne partira pas avec le fonds de commerce, mais seulement avec quelques petits morceaux de l'entreprise. » ■

Cinq secteurs à couvrir

Selon **Éric Maurice**, directeur d'**eTrust**, un bon plan de sécurité doit se déployer dans cinq secteurs :

1 - Le premier est celui dont on a parlé dans l'article ci-haut : le contrôle d'entrée et la vérification des *bagages*. C'est ici que prennent place les pare-feu et les outils de validation de contenu comme celui d'eTrust. C'est également ici qu'on peut désamorcer les genres d'attaque *interdiction d'accès* dont ont été victimes en février dernier plusieurs grands sites comme ceux de **Yahoo!** et d'**E*Trade**.

2 - Le deuxième secteur est celui de la confiance et de l'identification des interlocuteurs. Il s'agit d'une infrastructure d'authentification des personnes et de gestion de leurs certificats.

3 - Vient ensuite la confidentialité, où il s'agit d'empêcher que des pirates interceptent les communications. C'est ici que prennent place les outils d'encryption et ceux qui établissent des réseaux privés virtuels (VPN) entre les parties.

4 - Dans le contrôle d'accès, il s'agit pour le directeur des réseaux de l'entreprise de faire une gestion régulière des niveaux d'autorisation des employés et des interlocuteurs externes. Une des grandes vulnérabilités à ce chapitre tient au système d'exploitation *UNIX* qui offre un mode d'accès *fondamental* (*root access*). C'est un niveau auquel une opération simulée de 40 000 attaques au département de la **Défense** américaine a donné accès à 36 pirates. Le premier besoin pour le contrôle de l'accès en est un de gestion, mais eTrust dispose aussi d'outils qui renforcent les opérations à ce niveau.

5 - Le dernier palier est celui de l'administration des systèmes de sécurité. Il s'agit de veiller à ce qu'ils fonctionnent bien entre eux et avec les systèmes de l'entreprise. Cela représente souvent un labyrinthe. « Une personne responsable d'un système n'est pas responsable d'un autre, de telle sorte qu'en tant qu'usager, je pourrais être désactivé sur un système, mais pas sur l'autre », dit M. Maurice. « Les registres de tous les systèmes UNIX, *Novell*, *NT*, pare-feu et autres sont tellement nombreux qu'il faut consulter des dizaines de registres pour tirer au clair une attaque de *hacker*. C'est pourquoi on ne peut souvent pas retracer les pirates. » (YB) ■

La sécurité informatique, une question de gestion

Les attaques contre les sites de Yahoo! et de CNN ont sensibilisé beaucoup de gens

André Mondoux

Si de plus en plus d'entreprises sont conscientes des impératifs de la sécurité informatique, peu de firmes ont cependant traduit cette préoccupation en véritable stratégie de gestion. De toute évidence, il y a encore place à l'amélioration.

Beaucoup de gens ont été sensibilisés aux actes de piratage informatique, en février dernier, alors que des sites vedettes comme le répertoire *Yahoo!* et le site de la chaîne d'informations continue **CNN** s'effondraient sous le poids d'attaques électroniques. Ce fut également l'heure du réveil pour un bon nombre d'entreprises.

Ironiquement, les attaques externes de pirates constituent un phénomène plutôt isolé de la problématique de la sécurité informatique. « Seulement 10 % des incidents liés à la sécurité informatique sont le fait de *hackers* », affirme **Rino Granito**, directeur des solutions de sécurité chez **AGP**, une firme-conseil spécialisée notamment en solutions de commerce électronique.

Selon Rino Granito, une bonne partie des bris de sécurité proviennent de l'interne. « Cela peut être des employés mécontents qui désirent se venger ou encore des personnes présentes de façon temporaire dans l'entreprise et qui en profitent pour s'adonner à des activités d'espionnage industriel », précise M. Granito.

Pas de la science fiction

Espionnage industriel. Pour beaucoup de gens, cela ressemble davantage à un scénario de *Mission Impossible*...

C'est que ce genre d'activité est plutôt discrète par nature. D'une part, les grandes institutions publiques sont réticentes à publiciser le fait qu'elles ont été victimes d'un vol électronique, et la plupart préfèrent régler le problème elles-mêmes.

Il faut aussi reconnaître, d'autre part, qu'un vol électronique d'information (lire ou copier un fichier) ne laisse guère de traces. Selon Rino Granito, les entreprises peuvent ainsi ne pas savoir qu'elles ont été victimes d'espionnage.

« Lorsque nous implantons des solutions de sécurité, nous effectuons un contrôle général des activités du réseau. Il nous est ainsi arrivé de découvrir des activités d'espionnage. Je me souviens d'un cas, par exemple, où nous avions observé des vols d'informations stratégiques au département de marketing de l'entreprise. »

Oui, l'espionnage industriel est bel et bien réel.

Commerce électronique

Le piratage électronique et le vol d'informations, même si ce sont des risques à ne jamais négliger, ne sont pas les seules raisons d'assurer la sécurité d'un service informatique. Avec la venue du commerce électronique, la plupart des entreprises sont appelées à porter une attention toute particulière à la sécurité.

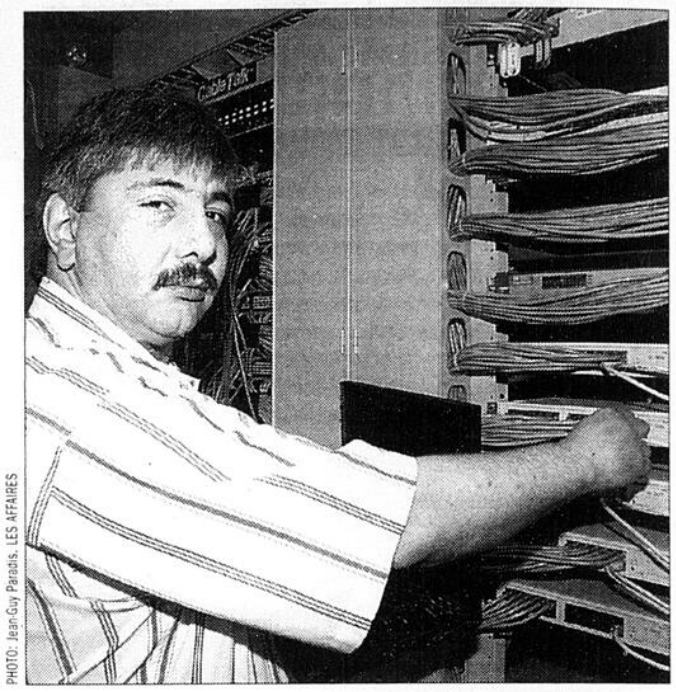


PHOTO: Jean-Guy Paradis, LES AFFAIRES

■ **Rino Granito : « La sécurité est d'abord un tout. Elle doit englober des mesures, des pratiques et des politiques. »**

Premièrement, les impératifs économiques sont indéniables : si un service informatique de commerce électronique venait à être perturbé à la suite d'un acte de vandalisme ou de sabotage informatique, ce sont les revenus de la firme qui seraient directement touchés.

Deuxièmement, qu'il s'agisse d'échanges entre entreprises (*B2B*) ou avec des clients (*B2C*), le commerce électronique implique l'envoi et le partage de données personnelles et stratégiques. Les entreprises doivent donc offrir des garanties que ces renseignements sont adéquatement protégés par des mesures de sécurités appropriées.

■ **L'espionnage industriel est bien réel. Seulement 10 % des incidents informatiques sont le fait de *hackers*.** ■

« Toute la question de la protection des données personnelles et confidentielles est inhérente au commerce électronique et relève directement de la sécurité informatique », souligne M. Granito.

La sécurité est un tout

Cependant, une bonne sécurité ne relève pas uniquement de matériel et de logiciels.

« La sécurité est d'abord un tout : elle doit englober également des mesures, des pratiques et des politiques », soutient M. Granito.

« Prenez l'exemple du courrier électronique, poursuit-il. Combien de personnes en entreprise envoient des informations en mode *clear text*, c'est-à-dire simplement insérées dans la zone de saisie du message électronique ? Combien d'informations confidentielles circulent ainsi ? Or, ces messages, techniquement parlant, peuvent être lus par l'administrateur du courrier ou un membre du personnel de soutien technique de l'entreprise. »

Les entreprises devraient donc mettre en place une politique de chiffrement des données, de façon à assurer l'intégrité des échanges stratégiques et confidentiels. « Ces politiques devraient également couvrir qui à accès à quoi et dans quelles circonstances. »

La sécurité informatique n'est donc pas l'affaire d'un produit isolé qui, une fois mis en place, restera inchangé. La sécurité doit non seulement s'intégrer aux autres facettes de la gestion d'un réseau informatique, mais aussi à la gestion globale de l'entreprise.

À l'ère du numérique, l'information peut dans bien des cas s'avérer l'élément crucial d'une entreprise. Et puisque nous vivons dans un monde où le changement est la norme, assurer la sécurité du réseau est un processus dynamique par nature. ■

Jamais vu. Jamais entendu parler.

Peu de clients. Alors quel est l'intérêt ?

Dans une nouvelle entreprise de communications

comme la nôtre, on ne suit pas les mêmes vieilles recettes.

Parce qu'on n'a pas de vieilles recettes.

On utilise une toute nouvelle technologie.

Parce qu'on n'est pas rattaché à une ancienne.

On travaille plus fort et plus intelligemment.

Parce qu'on veut attirer des clients et les garder.

On ne se bouscule pas pour faire partie du futur.

Parce qu'on est le futur.

Appelez-nous pour en savoir plus sur notre portefeuille

de services La source. Une seule facture, un seul point de

service pour tous vos besoins en communications d'affaires.

1 877 822-6281 ou www.norigen.com

NORIGEN

Un nouveau monde pour toutes vos communications

Les entreprises québécoises se disent bien protégées

Les infections par virus sont les incidents les plus fréquemment rencontrés

Yan Barcelo

Près de 90 % des grandes entreprises du Québec estiment que leurs systèmes d'information sont bien protégés, selon un sondage publié en avril dernier par le **CEFRIO**, dans un document intitulé *La sécurité et la protection de l'information*.

Des 500 plus importantes entreprises sollicitées, 315 ont répondu aux questions du CEFRIO, soit un taux de réponse de 63 %. L'enquête est donc représentative. Il en ressort que les firmes voient la sécurité comme une préoccupation importante et qu'elles font un bon travail à ce chapitre.

Reste à voir si elles se protègent des bonnes choses, ce que l'enquête du CEFRIO ne permet pas toujours d'évaluer.

Transactions électroniques

L'enquête permet de constater que, en ce qui concerne Internet, l'élite industrielle et financière du Québec, a fait un bon bout de chemin. La proportion des organisations qui ont au moins un site d'information Internet grand public est de 83 %.

Par contre, quand on en vient au coeur de la consommation dans Internet, soit le commerce électronique, les chiffres sont nettement moins forts : seulement 14 % d'entre elles ont mis en place des mécanismes de transaction et de paiement par carte de crédit.

Le portrait est plus reluisant du côté des transactions interentreprises (*B2B*) : 55 % des répondants disent s'y livrer avec leurs partenaires d'affaires. Que ce soit pour les sites de commerce électronique avec les consommateurs ou les sites interentreprises, les mesures de sécurité employées sont nombreuses, utilisées par relativement peu d'entreprises, et somme toute superficielles.

Quant aux échanges avec les consommateurs, les deux mesures les plus utilisées, dans une proportion de seulement 45 %, sont le chiffrement des courriels et des données recueillies sur le Web auprès des clients. La signature électronique n'est implantée que dans 20 % des cas et le recours aux certificats d'identité des personnes et des sites Web, que dans 19 % et 16 % des cas respectivement.

80 % des délits informatiques proviennent d'employés ou d'ex-employés.

Dans les échanges avec les partenaires, la mesure la plus répandue, mais seulement dans une proportion de 66 %, est également la plus élémentaire : la restriction d'accès à certaines adresses *Internet Protocol* (IP), sans doute par un système pare-feu (ce que le rapport ne précise pas).

On a par ailleurs recours au chiffrement des échanges (49 %), aux réseaux privés virtuels (VPN) (40 %), à la signature électronique (24 %) et aux certificats d'identité des personnes (21 %) et du site Web (20 %).

Les principaux incidents

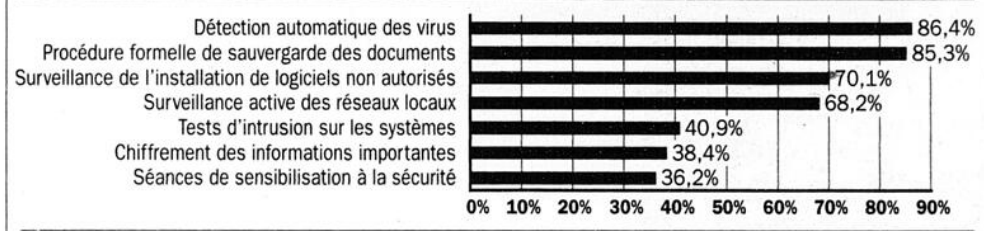
Selon **Tom Pownall**, analyste de la gestion du programme contre les délits informatiques à la **Gendarmerie royale du Canada**, 80 % des délits informatiques proviennent d'employés ou d'ex-employés de l'entreprise. Les procédures de sécurité à l'endroit de ces infractions relèvent essentiellement de politiques et de pratiques de gestion. Malheureusement, l'enquête du CEFRIO ne nous renseigne pas sur les mesures que les entreprises ont mis en place à ce chapitre.

Étonnamment, les incidents les plus fréquemment rapportés par les entreprises sont d'un tout autre ordre. En premier lieu viennent les infections par virus informatique, qui ont touché 65 % des entreprises au cours de l'année qui a précédé l'enquête. Suivent les pannes majeures (29 %), la perte ou l'incapacité de restituer des copies de sauvegarde (13 %) et, en tout dernier lieu, l'usurpation d'identité.

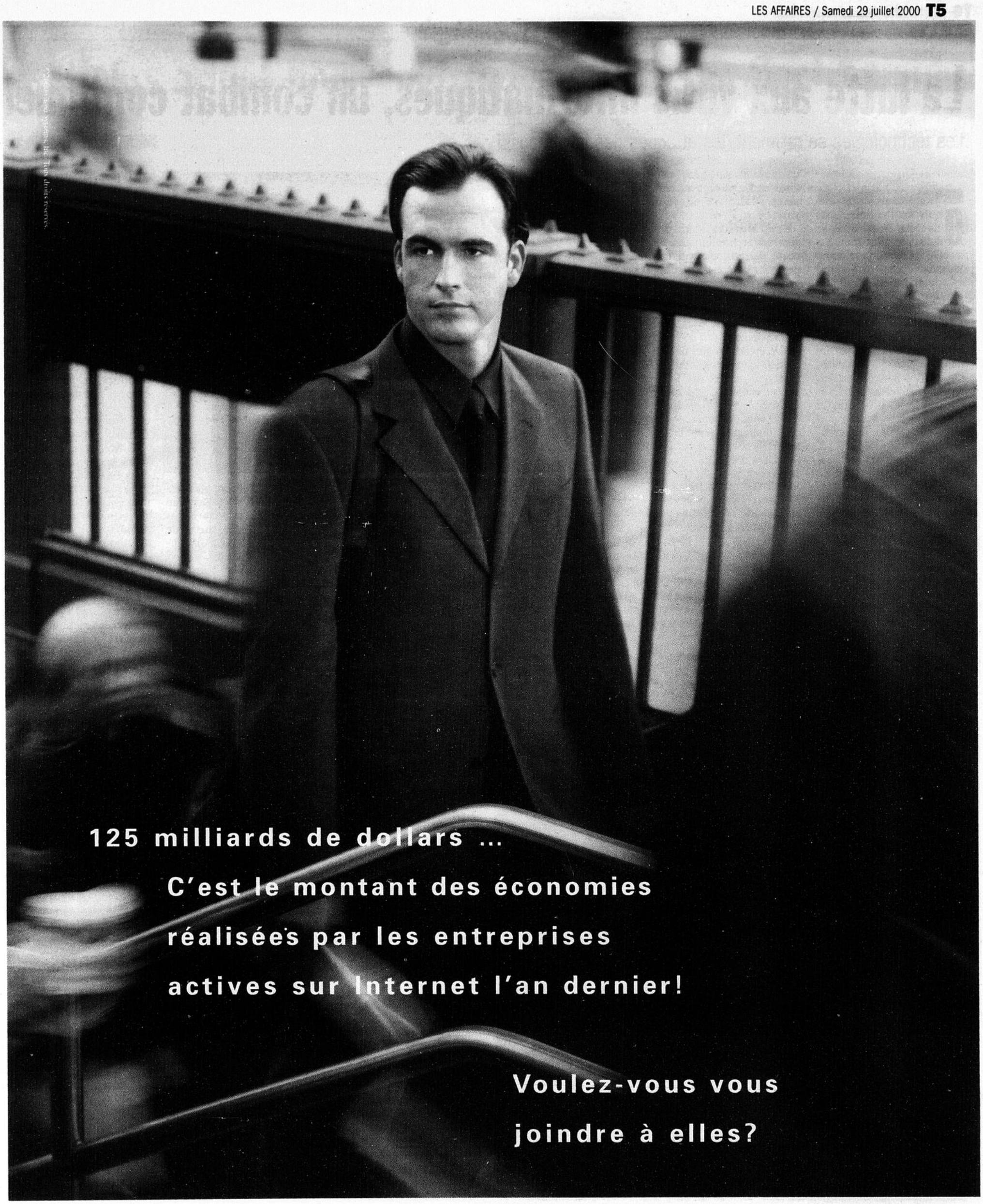
Par ailleurs, l'enquête nous apprend que les entreprises sont conscientes de la part que jouent leurs employés dans la sécurité. C'est ainsi que 49 % croient que le principal obstacle à la sécurité relève du manque de sensibilisation des employés à la question.

Les autres obstacles identifiés sont le coût des mesures à mettre en place (40 %), la diversité des technologies (38 %), le manque d'expertise à l'interne (32 %) et, enfin, le fait que 25 % des entreprises ne considèrent pas la sécurité comme une priorité. ■

Les actions des entreprises pour assurer la sécurité et la protection de leurs systèmes



Source : CEFRIO, *La sécurité et la protection de l'information*, avril 2000 — Graphique : LES AFFAIRES



C'est le moment. Internet est en train de changer notre monde. Sachez en profiter! Votre entreprise pourrait devenir plus rapide, plus mobile. Plus interactive que jamais. Nous pouvons vous aider. Nous sommes Cisco Systems. La presque totalité du trafic Internet circule sur notre équipement.

Testez le Quotient Internet[MC] de votre entreprise: remplissez notre questionnaire au www.cisco.com/go/iqtest.

CISCO SYSTEMS®
POUR UNE GÉNÉRATION INTERNET AUTONOME[MS]

La lutte aux virus informatiques, un combat continuel

Les technologies se raffinent, les attaques des intrus aussi

André Salwyn

On ne sait vraiment pas combien de millions de dollars le virus *ILoveYou* a coûté à l'industrie informatique mondiale.

Certains parlent de 10 M$, d'autres de 20 M$. Qu'importe ! C'est un virus qui a fait mal à tous ceux qui se sont laissés prendre.

Pourtant, ce ne sont pas les mises en garde qui manquent. On connaît la règle numéro un : ne jamais ouvrir une pièce jointe à un courriel à moins de savoir de quoi il s'agit et d'être sûr de sa provenance.

Mais c'est une chose beaucoup plus facile à dire qu'à faire : il suffit de voir l'étendue des dégâts causés par *ILoveYou* pour en avoir la preuve !

C'est que bien des utilisateurs d'ordinateurs faisaient confiance aux logiciels antivirus pour les protéger contre les attaques malicieuses. *ILoveYou* aura au moins eu le mérite de leur démontrer qu'en réalité, un logiciel antivirus ne les protège aucunement contre un nouveau virus.

Ron Moritz, chef des services technologiques au centre de recherche antivirus de **Symantec** à Cupertino, en Californie, reconnaît qu'il est pratiquement impossible de repérer et de détruire un nouveau virus avant qu'il ne se manifeste.

« De grands progrès ont été accomplis pour protéger les personnes contre des virus qui copient en partie d'autres virus. Si le *modus operandi* d'un virus est semblable à celui d'un autre, il est possible de l'arrêter avant qu'il ne cause des dommages à celui qui le reçoit », dit-il.

Mais c'est une tout autre affaire lorsqu'un nouveau virus comme *Melissa* et *ILoveYou* sont lancés dans Internet.

Pas le temps de réagir

Pour les chercheurs qui luttent contre les virus, le principal problème est leur propagation ultrarapide. Avec Internet et les listes d'adresses électroniques, un virus se propage si rapidement qu'il cause d'importants dommages avant même que les chercheurs aient trouvé un antidote.

« Et au fur et à mesure que nous trouvons un moyen de combattre un certain type de virus, les pirates informatiques s'arrangent pour en créer un autre », souligne M. Moritz.

Par exemple, le virus *Melissa* n'est pas seulement un virus; c'est aussi un ver informatique, ce qui fait qu'on est en présence de deux mécanismes de propagation.

« Le virus se charge d'infecter l'ordinateur du receveur et de se propager chaque fois qu'un document infecté est lu ou utilisé par un autre utilisateur. Le ver, quant à lui, se charge de propager le virus dans Internet en envoyant un document infecté aux 50 premières adresses électroniques contenues dans l'agenda de l'utilisateur », explique-t-il.

Règle numéro un : ne jamais ouvrir une pièce jointe à un courriel à moins de savoir de quoi il s'agit et d'être sûr de sa provenance.

En plus de changer la forme des documents et, souvent, de les détruire, les nouveaux virus et vers informatiques peuvent être encore plus destructeurs en s'attaquant au bios même (système d'entrée-sortie de base d'un ordinateur), paralysant l'ordinateur et détruisant tout ce qu'il contient. Dans le cas du virus *Chernobyl*, plusieurs victimes ont dû changer la carte-mère de leur ordinateur, assumant ainsi des coûts non négligeables, en plus d'être confrontées à la destruction de toutes leurs données.

Comment se protéger

Il ne fait aucun doute qu'avec un bon logiciel antivirus, tout utilisateur est désormais protégé contre les *Melissa*, *ILoveYou* et *Chernobyl*. Il n'en reste pas moins qu'il demeure exposé à tout nouveau virus.

Comment se protéger dans un tel cas ? Ron Moritz recommande notamment de sauvegarder tout fichier important et qui n'a pas besoin de retouches dans un format *lecture seule*, ce qui, techniquement, empêche un virus d'en changer le format.

Mais il recommande aussi de se méfier de tout courriel non sollicité, surtout s'il contient une pièce jointe, et d'utiliser des pare-feu pour empêcher toute intrusion dans son système. C'est le cas si on est branché en permanence à Internet.

M. Moritz affiche quand même une certaine confiance dans l'avenir, avec l'émergence de technologies de plus en plus sophistiquées, comme celles qui permettent de détecter instantanément tout comportement inhabituel d'un ordinateur.

« Il est très rare qu'un utilisateur décide d'envoyer un message à tous ses contacts à la fois, ou qu'il décide de changer le format de tous les fichiers contenus dans un répertoire. On sera bientôt en mesure d'alerter tout utilisateur dès qu'une telle commande sera effectuée et de la bloquer en attendant une confirmation. »

Une autre bonne façon de limiter les dégâts est de sauvegarder tout le contenu de son système dans son ensemble.

Les cédéroms coûtent de moins en moins cher et permettent de sauvegarder pratiquement toutes les données d'un ordinateur moyen.

En faisant régulièrement des sauvegardes, les pertes causées par un virus se limitent seulement aux données non sauvegardées. ■

Aucune entreprise n'est à l'abri des intrusions

Qu'il s'agisse de vandalisme électronique ou d'espionnage industriel, votre réseau d'entreprise peut être la cible d'intrusions électroniques. Êtes-vous à l'abri ?

Aussi longtemps qu'il y aura de l'information, le monde sera divisé entre ceux qui savent, ceux qui ne savent pas... et ceux qui désirent savoir à tout prix !

Voilà pourquoi les intrusions électroniques constituent un phénomène inévitable de l'univers de l'informatique contemporaine et ce, plus particulièrement à l'heure où Internet a relié des millions d'ordinateurs entre eux.

Soudainement, à des milliers de kilomètres de vous, quelqu'un peut accéder aux données stratégiques de votre entreprise. Si cette perspective est déplaisante à envisager, les intrusions électroniques demeurent néanmoins réelles.

Il y a plusieurs façons de procéder à une intrusion électronique. À la base, il y a l'attaque dite de *force brute* : les assaillants utilisent un logiciel qui tentera de découvrir un mot de passe en épluchant, une à une, toutes les combinaisons possibles.

Un fabricant de ce type de logiciels affirme avoir pu ainsi découvrir le mot de passe dans 90 % des cas en utilisant un simple ordinateur *Pentium II* de 300 MHz.

Une autre approche consiste à infiltrer une machine d'un réseau local (le maillon le plus faible de la chaîne) et à y installer un logiciel de *sniffer* (littéralement, un renifleur).

Ce renifleur peut ainsi *écouter* le trafic des paquets circulant sur le réseau et intercepter ceux qui véhiculent les procédures d'accès au réseau. Il est ainsi possible de mettre la main sur les mots de passe lorsqu'ils sont transmis au serveur.

Enfin, il y a les solutions de contrôle à distance, comme celles rendues célèbres par **Back Orifice**, **SubSeven** et **NetBus**.

Il s'agit de compromettre un ordinateur en y installant un logiciel serveur furtif qui pourra, à l'insu de la victime, être contrôlé à distance. (AM) ■

Plusieurs armes pour contrer les intrusions électroniques

André Mondoux

Pour contrer les intrusions électroniques, une des solutions consiste à mettre à jour les logiciels pare-feu.

C'est ainsi que des fabricants de pare-feu ont rehaussé leurs produits afin qu'ils puissent détecter et filtrer tout trafic suspect et éliminer la menace d'intrusion à la source.

Il existe aussi une génération de produits conçus pour contrer les intrusions électroniques : les solutions IDS (*Intrusion Detection Systems*). Ces logiciels peuvent revêtir plusieurs formes.

Outils de diagnostic : Ce type de produits, comme *CyberCop Scanner* de **Network Associates**, effectue une tournée d'inspection des points de vulnérabilité connus du réseau et de ses ordinateurs, de même que de tous les périphériques servant à acheminer les données (routeurs, concentrateurs et commutateurs).

Ces outils peuvent aussi tester le pare-feu, générer un rapport sur l'état du réseau et suggérer les actions à prendre pour colmater les brèches.

Anti-renifleurs : Ces outils permettent d'évaluer les ordinateurs individuels d'un réseau afin de dépister ceux qui sont susceptibles d'être dans une situation de promiscuité électronique, c'est-à-dire qui peuvent être manipulés par un logiciel renifleur pour épier l'ensemble des activités du réseau.

Détecteurs d'attaques : Ces logiciels servent à sonner l'alarme dès que survient une attaque électronique connue. Deux approches sont habituellement retenues.

La première (comme celle adoptée par *Alert* d'**Axent**) consiste à observer le trafic sur le réseau, généralement en observant le contenu des paquets de données qui circulent d'une machine à l'autre, afin de détecter un profil d'attaque (ou signature) connu.

L'autre approche (comme *RealSecure* d'**ISS**) consiste à utiliser le journal où sont consignées les activités du réseau, et de les comparer au trafic actuel. L'idée générale est la même qu'avec l'approche précédente : il s'agit de reconnaître des séquences connues d'opérations qui sont les signes distinctifs d'un type d'intrusion.

Les leurres : Enfin, il y les leurres informatiques. Certains produits, dont *ManTrap* de **Recourse Technologies**, simulent un serveur ayant des failles connues. Ces serveurs bidons attirent ainsi l'attention loin des véritables serveurs critiques, en plus de noter les actions des intrus pour documenter d'éventuelles poursuites. ■

La promotion des certificats d'authentification reste à faire

Ils offrent une protection supplémentaire pour les transactions électroniques

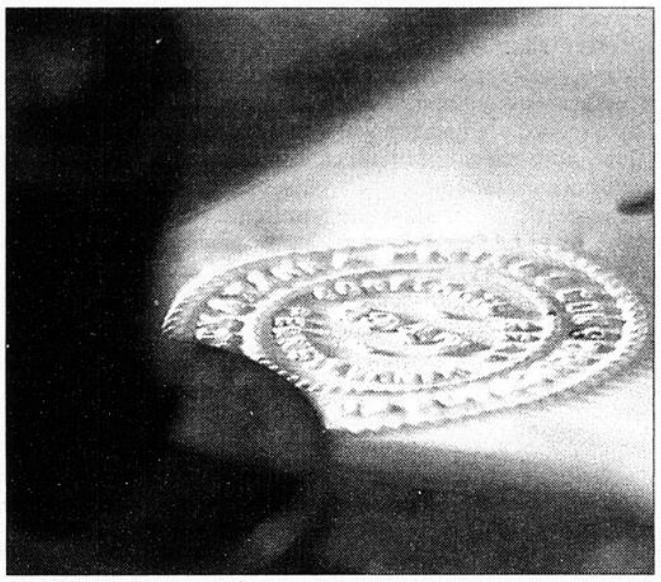
Yan Barcelo

Avec tout ce qu'on entend et lit au sujet de la sécurité Internet et des certificats d'authentification, on pourrait croire que les mesures nécessaires se mettent rapidement en place. Tout ne se passe-t-il pas sept fois plus vite dans Internet ? Ce n'est pourtant pas le cas en ce qui concerne la certification des transactions.

En fait, la diffusion des mesures de certification suit très loin derrière l'expansion de la population Internet.

Pourtant, il y a un bon moment qu'on nous vante la vertu des certificats. Ils constituent un outil additionnel et fort bienvenu qu'on ajoute habituellement à ceux du mot de passe et du nom d'utilisateur.

Ce sont surtout les institutions financières qui s'en font les porte-étendards afin de renforcer la sécurité des



transactions qu'elles entretiennent avec leurs clients.

Protection peu fiable

Actuellement, au mot de passe et au nom d'utilisateur, une troisième protection est utilisée généralement dans les transactions financières courantes, soit un mode de transmission encryptée de type SSL (*Secure Socket Layer*).

Or, la seule véritable clé dans ce trio est le mot de passe, qui s'avère relativement peu fiable et que bien des gens se font dérober assez facilement. Une fois qu'un intrus dispose d'un mot de passe *emprunté*, le nom d'utilisateur est, en général, facile à deviner.

Quant à l'encryption, elle n'empêchera rien puisqu'elle ne fera qu'encoder une transmission à laquelle l'intrus a droit en raison du fait qu'il possède le mot de passe.

Question d'identité

Certaines sociétés, comme **Verisign** et **RSA**, ont donc mis au point les certificats d'authentification afin de renforcer l'identité des citoyens du Web.

Ce certificat est constitué d'une clé publique, que le certificateur remet à l'utilisateur, et d'une *serrure* privée, qu'il conserve.

Avant de décerner cette clé publique, le certificateur a fait une vérification de l'identité de l'internaute pour confirmer qu'il est bel et bien celui qu'il dit être. Et quand cet internaute veut effectuer une transaction, sa clé publique doit fonctionner dans la serrure privée dont dispose l'institution.

Ce système de clés remplit une autre fonction capitale pour les institutions en agissant comme une signature électronique. « Une fois la transaction faite, le client ne peut la répudier », explique **Richard Groot**, directeur général adjoint, commerce électronique Québec, à la **Banque Scotia**.

Certaines sociétés, comme Verisign et RSA, ont mis au point les certificats d'authentification afin de renforcer l'identité des citoyens du Web.

Fort beau schéma, mais voilà, il ne s'est pas beaucoup répandu encore.

« La Banque Scotia est le principal émetteur de certificats au monde », affirme M. Groot. Or, la Scotia n'en a diffusé qu'environ 100 000 à ce jour, ce qui dépasse le nombre émis par des acteurs tels que **eCertify**, **EDF**, **IBM**, **General Network Services**. Sur une population Internet qui avoisine les 200 M, ce n'est pas beaucoup.

Par contre, la Banque Scotia compte sur les législations qui se multiplient et exigent qu'acheteurs et vendeurs dans Internet puissent être identifiés.

De plus, **Postes Canada** agira sans doute comme un multiplicateur puisque son service de poste électronique utilisera les certificats de la Scotia. Est-ce dire que la diffusion des certificats s'accélère ? « Absolument ! », répond Richard Groot. ■

Les technologies de chiffrement des données, une solution en émergence

André Mondoux

Les technologies de chiffrement s'imposent de plus en plus comme la meilleure solution, qu'il s'agisse d'assurer l'intégrité du commerce électronique, de préserver sa vie privée ou, encore, de veiller aux secrets d'État.

L'encodage des données, l'opération consistant à rendre des données illisibles pour les personnes non autorisées, n'est pas une approche nouvelle. Ayant de tout temps eu des secrets à préserver, les humains ont toujours fait preuve d'imagination afin de mettre au point les techniques nécessaires pour les préserver.

En cette ère de révolution numérique, les informations sont non seulement multipliées, mais elles circulent en tous sens grâce à l'interconnexion des réseaux.

Les secrets à garder sont plus nombreux que jamais et l'ordinateur est mis à profit pour veiller sur eux.

L'approche la plus couramment utilisée pour rendre des données illisibles est le chiffrement. Il s'agit d'utiliser de complexes fonctions mathématiques (nommées algorithmes) afin de transformer un contenu en un ensemble de données qui, en apparence, n'a ni queue ni tête. On dit alors que le document est chiffré (ou encrypté). La fonction mathématique qui sert au chiffrement est nommée clé de chiffrement (ou d'encryption).

Clé de longueur variable

À moins de posséder la clé de chiffrement, il n'y qu'une seule façon pour décoder un message chiffré : dépouiller une à une toutes les possibilités avant de découvrir le code unique qui le déverrouillera.

La clé de chiffrement peut être d'une longueur variable. Elle est mesurée en bits (40, 56, 128, etc.). Plus la clé est longue, plus il sera difficile de découvrir le code unique de déchiffrement.

Ainsi, il est généralement admis qu'une clé de chiffrement à 40 bits peut être décodée en quelques semaines avec un simple ordinateur personnel.

Par contre, une clé à 128 bits peut exiger, avec un super-ordinateur gouvernemental, jusqu'à des milliers d'années avant que l'on puisse découvrir son code.

Une question de sécurité... nationale

De prime abord, la solution semble donc aisée : pour assurer la meilleure sécurité possible, il n'y a qu'à offrir des produits de chiffrement à 128 bits. Cependant...

La plupart des pays, initialement du moins, étaient réticents à l'idée de voir se propager de puissants produits de sécurité qui, il n'y a pas si longtemps, étaient le lot exclusif des grandes agences gouvernementales de renseignements.

L'idée d'un groupe terroriste ou d'une organisation criminelle s'échangeant des messages quasi inviolables n'était pas sans heurter les conceptions traditionnelles de sécurité du territoire.

Voilà pourquoi il fut question, pendant un certain temps, d'autoriser ce type de produit, mais en y incorporant une *porte arrière* ou en forçant le dépôt des clés de chiffrement afin de permettre aux autorités policières ou gouvernementales d'y avoir accès en cas de nécessité majeure.

Cette idée se heurta aux lobbyistes voués à la défense des droits fondamentaux des citoyens. Pour eux, les technologies de chiffrement sont une forme de protection de la liberté individuelle.

Le dilemme pour les gouvernements était donc d'interdire l'utilisation et l'exportation d'outils pouvant menacer la sécurité nationale, ou de donner carte blanche à une nouvelle industrie promise à une croissance spectaculaire.

Pour résoudre l'impasse, la plupart des pays industrialisés ont choisi de jouer sur les deux tableaux en signant l'*Arrangement de Wassenaar*.

Cet accord permet d'exporter des produits de chiffrement aux pays *responsables*, tout en obligeant à contrôler l'exportation des logiciels de chiffrement avec les pays susceptibles d'avoir des liens avec des organisations terroristes.

En octobre 1998, le gouvernement canadien a décidé de ne pas imposer aucun régime de récupération des clés de chiffrement et de promouvoir l'exportation et l'importation de produits de cryptographie non controversés, de façon à laisser les citoyens canadiens libres d'utiliser les produits de chiffrement de leur choix. Seuls les États-Unis maintiennent un contrôle rigoureux, quoique celui-ci ait été assoupli récemment.

Là pour rester

Malgré un départ un peu cahoteux, les technologies de chiffrement sont présentement très en demande.

À ce chapitre, les Canadiens sont choyés, puisque le Canada n'est pas soumis aux contrôles d'exportation américains.

Nous pouvons ainsi importer librement les puissants produits de chiffrement américains à 128 bits, ce qui n'est pas le cas des autres pays. (AM) ■

RSA propose une approche pour colmater les brèches

Le système *Keon* vient combler les lacunes de l'infrastructure à clé publique

André Mondoux

Même si les notions de chiffrement, d'infrastructures à clé publique (ICP) et de signatures numériques sont à l'honneur, certaines firmes, comme **RSA**, estiment qu'il faut pousser encore plus loin. Selon RSA, il faut miser sur un système complet qui assure l'intégrité des données tout en comblant les faiblesses de l'ICP.

La multiplication des échanges électroniques et la venue du commerce électronique mettent en évidence le besoin d'assurer l'intégrité des données. Personne, en effet, ne désire voir son numéro de carte de crédit être intercepté par des gens malintentionnés. Et une entreprise pourrait se retrouver dans un sérieux pétrin si ses documents stratégiques venaient à tomber entre les mauvaises mains.

Pour assurer la protection des données, de plus en plus d'organisations se tournent vers l'ICP. Le principe de l'ICP est d'appliquer un code secret (une clé) afin de rendre les données illisibles à autrui.

Plutôt que d'utiliser une seule clé de chiffrement pour coder et décoder les données, l'ICP s'appuie sur deux clés de chiffrement. La clé publique d'un individu, librement distribuée, sert à encoder les données. Une fois encodées, celles-ci ne peuvent être déchiffrées qu'avec la clé privée (secrète) du récipiendaire.

L'approche de l'ICP permet donc de recevoir des données chiffrées de tous, sans jamais trahir l'intégrité de sa clé privée.

Est-ce suffisant ?

Malgré l'attrait et l'indéniable souplesse de l'approche ICP, plusieurs estiment que ce n'est pas suffisant. Le noeud du problème réside dans le fait que les certificats numériques, qui contiennent les deux clés de chiffrement, sont stockés sur l'appareil de l'usager.

Dans un tel contexte, rien ne garantit que la personne en ligne sur l'appareil de l'usager soit bel et bien le ou la propriétaire des certificats numériques. Quiconque a accès à la machine devient, aux yeux des autres usagers, le propriétaire des clés de chiffrement.

Un autre défi pour l'approche ICP est qu'elle ne peut offrir à elle seule la flexibilité nécessaire pour permettre aux usagers d'utiliser n'importe quel périphérique d'entrée au réseau, car les certificats sont stockés sur une machine déterminée. Il serait possible de copier les certificats sur plusieurs machines, mais cela augmenterait la vulnérabilité du système et les risques de confusion.

Enfin, un autre problème hante l'approche ICP : que faire si le périphérique d'entrée au réseau, un bloc-notes par exemple, est volé ? Une fois les certificats en main, les voleurs pourraient virtuellement incarner le propriétaire légitime de l'appareil.

Une architecture globale

Reconnaissant ces limites, la firme de sécurité RSA propose un système complet, l'architecture ICP évoluée *RSA Keon*.

L'atout principal du système *Keon* est que les certificats numériques (qui peuvent être générés par un serveur *Keon* complémentaire ou le système d'un autre vendeur de certificats) n'ont pas à résider nécessairement sur l'appareil client.

Les certificats peuvent être stockés électroniquement sur une carte à puce. Lors de l'entrée sur le réseau, l'usager doit fournir son nom d'identification, son mot de passe et insérer sa carte à puce avant d'avoir accès au réseau et de pouvoir utiliser ses certificats numériques.

Les avantages conférés par cette approche sont multiples. D'une part, l'utilisateur peut employer n'importe quel appareil pour entrer sur le réseau et toujours avoir accès à ses certificats numériques.

D'autre part, même si l'appareil est volé, les certificats restent toujours en possession de l'usager. Et même si la carte à puce venait à être perdue ou volée, elle est inutile à quiconque ne possède pas le mot de passe pour l'entrée sur le réseau.

Cependant, les lecteurs de cartes à puce ne sont pas encore répandus et ce secteur ne bénéficie pas encore de normes et pratiques universelles. Voilà pourquoi RSA a doté son système *Keon* de fonctions de cartes à puce *virtuelles*.

Le jeton de RSA génère un nouveau code aléatoire à toutes les 60 secondes.

Avec cette approche, les usagers doivent s'authentifier lors de l'ouverture au réseau avant de pouvoir recevoir automatiquement leurs certificats numériques.

La clé : un jeton

Afin d'assurer l'intégrité de cette opération cruciale, RSA propose plusieurs solutions, dont l'utilisation d'un jeton. Ce jeton, synchronisé avec un serveur central, génère un nouveau code aléatoire toutes les 60 secondes. Lorsqu'il veut entrer sur le réseau, l'usager doit inscrire son nom d'identification, son numéro d'identification personnel et ensuite inscrire le code qui apparaît sur le jeton.

Le jeton sera alors reconnu par le serveur qui autorisera l'accès aux ressources du réseau. Sans le jeton, l'accès au réseau devient impossible et par le fait même, l'intégrité des certificats numériques est assurée.

La sécurité n'est pas l'affaire de solutions individuelles, mais relève plutôt d'une approche globale. De plus en plus de solutions démontrent qu'il est possible d'assurer la sécurité dans une optique de puissance et de flexibilité, deux attributs vedettes du nouvel environnement informatique suscité par Internet. ■

LES SOLUTIONS LOGICIELLES SAN OUVERTES DE COMPAQ. ÇA VOUS SURPREND, N'EST-CE PAS ?

Attention ! Les solutions SANworks[MC] de Compaq sont là ! Lorsque le premier fournisseur de solutions de stockage et l'un des chefs de file de solutions SAN applique son expertise à la création de solutions de stockage ouvertes, ça fait de l'effet. Vous en voulez d'autres ? Visitez le site www.compaq.ca/sanworks

COMPAQ

Le Réseau Unique. Plongez.

Le poisson, on le sait, ne grandit qu'à la mesure de son aquarium. Ce n'est pas en tournant en rond tout seul dans son petit bocal que l'on conquiert le monde des affaires électroniques. L'information doit circuler plus librement afin qu'employés, fournisseurs et clients puissent travailler ensemble. Tous leurs systèmes d'exploitation, leurs intranets et Internet peuvent former un Réseau Unique… en toute sécurité et fiabilité. C'est là la force des logiciels de services réseau de Novell. Ils harmonisent les technologies déjà en place et permettent à vos solutions d'affaires électroniques d'évoluer au même rythme que l'économie de réseaux. N'hésitez plus et plongez vers **www.novell.com/canada**

Novell
the power to change

Windows 2000 va plus loin dans les garanties de sécurité

Le nouveau système d'exploitation permet de gérer l'infrastructure à clé publique

André Mondoux

L'arrivée de *Windows 2000* marque un jalon important : désormais, tout système d'exploitation doit offrir des garanties en ce qui concerne la sécurité des services réseau. La protection par simple mot de passe ne suffit plus.

En un sens, **Microsoft** n'avait guère le choix. Si le géant de Redmond voulait prendre pied dans le marché des serveurs d'entreprises, il devait confronter les deux grandes réalités du marché.

La première est qu'Internet a fait basculer le marché dans une infrastructure de services répartis. Désormais, les ordinateurs ne sont plus isolés et les serveurs, les ordinateurs hôtes auxquels il faut se connecter pour accéder aux services (Web, courrier électronique, etc.), deviennent des éléments hautement stratégiques.

La seconde réalité est que dans cet univers d'interconnexions, la fiabilité et la sécurité des services sont primordiales. Si Microsoft entendait mener une lutte digne de ce nom aux serveurs *UNIX*,dont Internet est la chasse gardée traditionnelle, la multinationale se devait donc de proposer un système d'exploitation conforme aux nouvelles exigences du marché.

Voilà pourquoi Microsoft a doté *Windows 2000* de plusieurs fonctions de sécurité. Le nouveau système d'exploitation se démarque nettement de son prédécesseur *Windows NT*. Mais est-ce suffisant ?

Infrastructure à clé publique

Une des grandes nouveautés de *Windows 2000* sur le plan de la sécurité est le soutien intégré pour l'infrastructure à clé publique (ICP). L'ICP offre un environnement de chiffrement (encoder les données pour les rendre illisibles à autrui) à deux clés : une clé publique (accessibles à tous) pour chiffrer les données et une clé privée (secrète) pour les déchiffrer.

En plus d'assurer la confidentialité des données, l'ICP offre un système de signature électronique permettant aux fournisseurs de services et aux clients de valider leur identité entre eux. Dans un cadre de commerce électronique, cette dernière fonctionnalité peut être cruciale.

Windows 2000 offre non seulement les outils pour gérer une infrastructure à clé publique, tant du point de vue du serveur que de celui du client; il permet également la mise sur pied d'une autorité de certification (AC).

L'AC est un service responsable de l'émission des certificats de sécurité qui contiennent les deux clés (publique et privée) de chiffrement. Il y a fort à parier que le déploiement de services commerciaux numériques inclura l'émission de certificats de sécurité, afin de protéger les transactions entre vendeurs et clients en validant leur identité respective.

Votre billet svp !

Internet a également incité à la décentralisation des réseaux : désormais, les usagers peuvent utiliser le Net pour accéder à distance aux divers services et ressources de leur réseau d'entreprise. Il y a donc lieu d'offrir un seuil de sécurité adéquat afin de s'assurer que les bonnes personnes ont accès aux bonnes ressources.

■ *Windows 2000* permet également la mise sur pied d'une autorité de certification. ■

Pour ce faire, Microsoft a adopté le système *Kerberos* (nom grec du gardien des enfers, **Cerbère**), une approche éprouvée relevant du domaine public. Le système *Kerberos* consiste à assujettir l'utilisation de services et ressources réseau à l'obtention d'un billet virtuel.

Ce billet est distribué aux usagers par le serveur, par l'entremise d'échanges complexes de données chiffrées avec les clés publiques et privées des participants. Les billets ne sont émis qu'après validation de l'identité des requérants et ne sont valables que pour une ressource précise. Ils peuvent également être limités dans le temps.

Windows 2000 innove aussi en permettant de chiffrer automatiquement les données lors de leur sauvegarde.

Intégrée à même la structure de gestion des fichiers, cette fonction assure donc l'intégrité des données en cas de perte, vol et intrusion électronique. De plus, elle est complètement transparente pour les usagers : les fichiers chiffrés sont automatiquement déchiffrés lorsqu'ils sont ouverts ou manipulés par une application.

Ces nouvelles fonctions sont certes les bienvenues. Cependant, le déploiement et la gestion de solutions comme l'ICP et le système *Kerberos* sont complexes. On peut douter que les petites entreprises aient le temps, l'argent et le savoir-faire à l'interne pour les faire.

En ce sens, *Windows 2000* est principalement destiné à la grande et à la moyenne entreprise. Cela forcera sans doute les PME à se tourner vers des solutions d'hébergement de services (comme les fournisseurs de services d'application, ou ASP selon l'acronyme anglophone), ou encore d'embaucher des consultants externes.

Il n'est donc pas assuré, contrairement à ce qui est parfois suggéré avec les solutions de commerce électronique, que petites et grandes entreprises jouiront ici des mêmes avantages. ■

Une carte à puce pour sécuriser l'accès aux réseaux

GemSafe trouve plusieurs applications dans le commerce électronique

Yan Barcelo

La multinationale française **Gemplus** a lancé récemment une carte à puce sécuritaire qui, selon les mots de son président canadien, **Guy Dartigues**, « cherche à résoudre les problèmes de sécurité dans un monde Internet ouvert ». Son nom : *GemSafe*.

La solution est simple : chaque utilisateur possède sa propre carte à puce et pour pouvoir accéder à un réseau, il doit l'introduire dans un lecteur relié à l'ordinateur. L'ordinateur décode l'information contenue sur la carte et garantit au réseau que l'utilisateur est autorisé à y accéder.

Cette solution peut aussi s'appliquer au commerce électronique et être particulièrement intéressante pour sécuriser les transactions sur le Web.

En effet, sur la carte *GemSafe*, la puce dispose de la puissance nécessaire pour effectuer tous les savants calculs liés à des communications de certificats sécurisés à clés publiques. Gemplus espère donc qu'elle remplacera les cartes de crédit actuelles dont la sécurité est minimale.

Une carte *GemSafe* offre de nombreux avantages. D'abord, les données y sont beaucoup plus difficiles à lire que sur la bande magnétique d'une carte classique. Cette carte réaliserait une encryption de toutes ses transactions, elle servirait à authentifier le porteur par transmission d'un certificat d'identité.

Les données sont plus difficiles à lire sur la carte à puce GemSafe que sur une carte à bande magnétique conventionnel.

Enrayer la fraude par carte de crédit

De plus, en effectuant une signature électronique de toutes les transactions, elle empêcherait la répudiation des transactions.

Les cartes de crédit magnétiques permettent déjà cela, notamment dans des transactions électroniques. Les institutions financières nord-américaines ont déjà choisi la technologie plus simple et moins coûteuse de la carte à bande magnétique. Pourquoi adopteraient-elles maintenant la carte à puce ?

Pour deux raisons majeures, pense Guy Dartigues, président de **Gemplus Canada**. D'abord, la fraude va en augmentant sur les cartes classiques. « Avec la multiplication du nombre de cartes à puce, les fraudeurs se rabattent sur ce qu'il y a de plus facile à frauder, c'est-à-dire les cartes de crédit. »

Ensuite, Internet change toutes les équations. La carte de crédit a été conçue pour des réseaux de transaction fermés où les interventions des pirates étaient rarissimes. Désormais, dans l'environnement du commerce électronique, les transactions par cartes de crédit sont appelées à s'effectuer dans un réseau ouvert, où les besoins de sécurité ne peuvent être satisfaits avec la technologie traditionnelle des bandes magnétiques.

Comme des micro-ordinateurs

Surtout associée aux cartes téléphoniques prépayées, la technologie de la carte à puce a évolué bien au-delà de cette application élémentaire, au point qu'il s'agit maintenant de micro-ordinateurs ultraminiaturisés.

« La puissance de ces microprocesseurs correspond à la puissance des premiers PC des années 1980, avec leur capacité mémoire de 64 kilo-octets et leur horloge cadencée à 0,5 mégahertz », explique M. Dartigues.

C'est dire que les domaines où la carte peut trouver place se sont considérablement élargis. Par exemple, un marché peu connu, mais auquel on promet un avenir fabuleux, est celui des téléphones cellulaires obéissant au standard GSM, le plus répandu dans le monde, et qui intègre la technologie de la carte à puce.

Gemplus est le principal fabricant de ces cartes au format spécial, qui permetttent aux fabricants de produire des téléphones *génériques*.

Il s'agit d'appareils dotés d'une flexibilité de programmation qui permet à chaque opérateur régional d'y intégrer les services de son choix. Plus encore, « dans certains appareils, on intégrera un lecteur de carte, précise M. Dartigues. **Motorola**, par exemple, offre un modèle de ses *Startac* doté d'un tel lecteur ».

On peut s'attendre à ce que la diffusion de ces lecteurs intégrés contribue à faire exploser le secteur. Les applications qui en tirent avantage ne font que commencer à se mettre en place.

Par exemple, il y a à Singapour des postes de péage électroniques pour certaines voies de circulation. Le paiement se fait par transmission de fréquences radio à partir d'un boîtier logé dans l'automobile. Or, pour recharger ce boîtier en argent, on y glisse une carte de prépaiement.

Comment recharger cette carte de prépaiement ? En l'insérant dans le lecteur de carte à puce de son cellulaire qui permet un téléchargement avec sa banque. ■

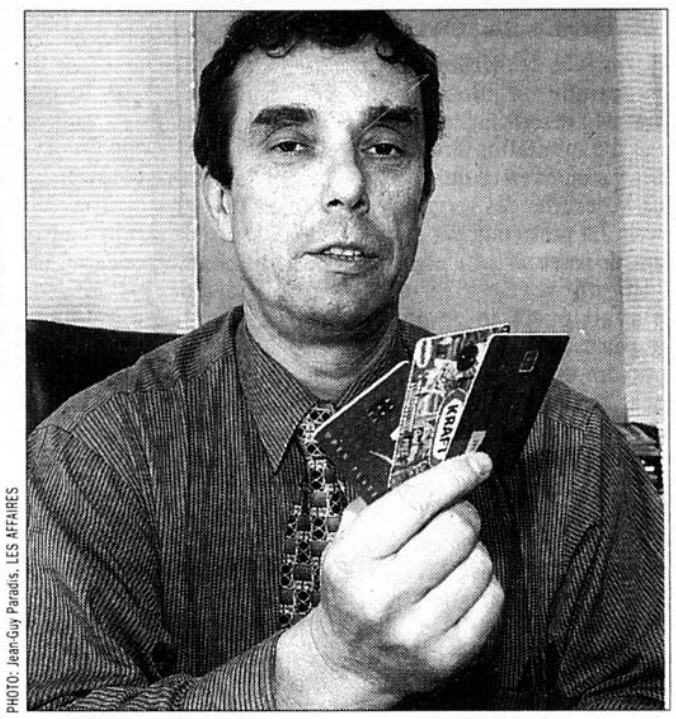


PHOTO: Jean-Guy Paradis, LES AFFAIRES

■ **Guy Dartigues : « Avec la multiplication du nombre de cartes à puce, les fraudeurs se rabattent sur ce qu'il y a de plus facile à frauder, les cartes de crédit. »**

Gemplus voit tous les continents dans sa mire

Avec *GemSafe*, **Gemplus** dispose d'une carte de plus dans son jeu pour assurer sa croissance sur tous les continents.

Fondée en 1988 et ayant engrangé des revenus de 1,1 milliard de dollars en 1999, Gemplus domine le marché des cartes à puce avec une part de 39 %. L'entreprise française compte 6 500 employés répartis dans 30 pays. Le concurrent principal, **Schlumberger**, est également français et détient une part de 35 %.

Une croissance de 60 %

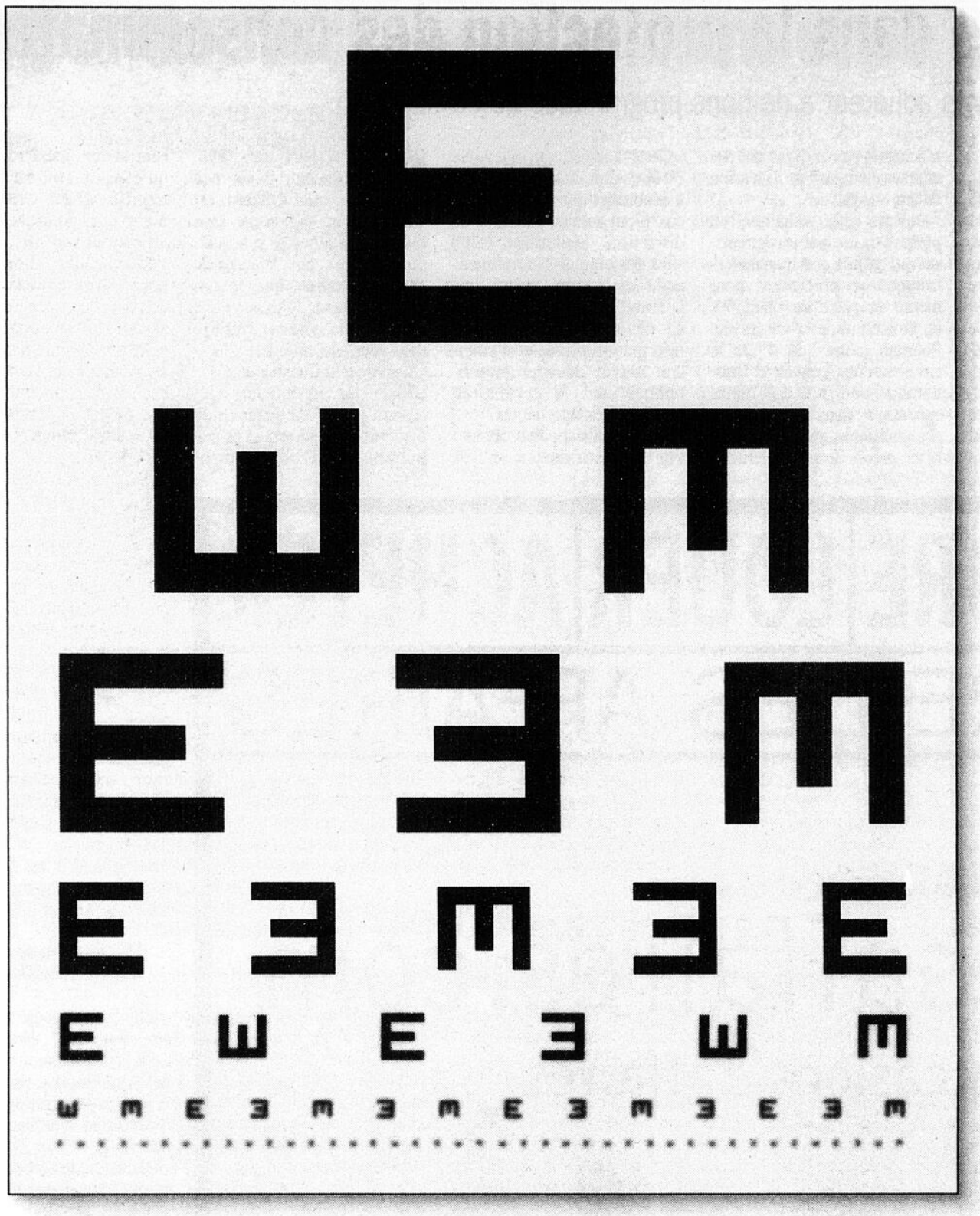
Ce marché est loin d'avoir atteint son point de saturation. L'Amérique du Nord reste à conquérir ainsi que toute l'Asie. À la fin de 2000, la Chine dépassera en termes de cartes vendues la France et l'Angleterre, les deux châteaux-forts jusqu'ici de cette technologie, prévoit **Guy Dartigues**, président de **Gemplus Canada**.

« En 1999, 1,2 milliard de cartes ont été vendues dans le monde. D'ici trois ans, on calcule que ce chiffre passera à six milliards », précise-t-il. C'est pourquoi Gemplus s'attend à connaître une croissance d'environ 60 % à la fin de l'année financière en cours.

Un secret bien gardé

Le laboratoire de l'Île-des-Soeurs est un autre indice de la croissance étonnante de Gemplus. Créé il y a trois ans, il compte déjà 180 employés, ce qui en fait un des secrets les mieux gardés de l'activité de recherche et développement au Québec.

M. Dartigues vise à atteindre les 1 000 employés dans cinq ans. Pour l'instant, il ne voit qu'un obstacle à la réalisation de cet objectif : la capacité de recruter le nombre d'employés qualifiés requis. (YB) ■



Vous rappelez-vous à quel point le E était facile?

EDS solved.
eds.com

Avez-vous une assez bonne vue pour déchiffrer les détails des systèmes d'affaires électroniques? Notre gamme complète de services Web vous offre tout ce dont vous avez besoin pour aller dans le E – en toute sécurité et fiabilité – de l'hébergement aux applications, en passant par le traitement des commandes. EDS peut même intégrer vos systèmes Web et vos anciens systèmes. Et si vous ne souhaitez pas commander tout de suite le menu complet, nous offrons également chaque élément à la carte. Avec différents niveaux de service pour combler des besoins distincts. Pour savoir comment nous pouvons vous aider à gérer la complexité des affaires électroniques, composez le 800 566 9337 ou visitez le www.eds.com, un site pour les yeux fatigués.

Des trous dans la protection des consommateurs en ligne

Peu de commerçants adhèrent à de bons programmes de certification

Yan Barcelo

Il reste encore beaucoup à faire en matière de protection des consommateurs dans l'univers du commerce électronique.

Un sondage mené l'année dernière par *Business Week* indiquait que plus de 75 % des gens qui magasinent dans Internet disent qu'ils achèteraient davantage si la vie privée était mieux protégée. Et ceux qui n'achètent pas en ligne ont des craintes en regard de l'invasion de leur vie privée.

Devant cette situation, on pourrait croire que les entreprises qui font du commerce électronique se précipitent pour mettre en place des garanties de protection de la vie privée. Pourtant, c'est loin d'être le cas, selon une enquête d'**Enonymous**, de San Diego, qui se spécialise dans l'évaluation des politiques pour préserver la vie privée de sites Internet.

Cette société, qui a évalué 30 000 sites bien fréquentés, a découvert que 75 % d'entre eux n'ont aucune politique de discrétion. Seulement 1 200 sites ont obtenu la cote maximale de quatre étoiles que la firme réserve aux sites qui ne dévoilent jamais aucune information privée et n'émettent aucun courriel promotionnel sans la permission explicite des internautes.

Enonymous apparaît comme l'un des certificateurs de sites les plus sérieux du Web. Malheureusement, il est peu connu. Le plus célèbre est **TRUSTe**, un organisme sans but lucratif lancé il y a quelques années par **Electronic Frontier Foundation**. En juin 1999, quelque 700 membres arboraient le symbole *TRUSTe* dans leur site Internet, témoignage de leur transparence.

Mais les internautes qui croient y voir une garantie de discrétion se leurrent. Les politiques de TRUSTe n'imposent aucun standard. Tout ce qu'elles exigent est que l'entreprise adhère scrupuleusement aux politiques qu'elle affiche sur son site.

Par exemple, si un site annonce qu'il se réserve le droit de faire tout ce qu'il veut avec les informations qu'il récolte sur les internautes et de les vendre à qui veut les acheter, pas de problème. Il pourrait même fièrement arborer le sceau d'approbation de TRUSTe !

La réputation de TRUSTe a d'ailleurs souffert récemment. **RealPlayer**, qui affichait ce sceau et disait préserver la vie privée de ses clients, faisait tout le contraire en accumulant d'importants fichiers d'information sur leurs habitudes musicales.

Selon **Eric Schmitt**, analyste chez **Forrester Research**, la situation des firmes comme TRUSTe est intenable. « Les groupes qui sont supposés veiller sur les intérêts des consommateurs sont financés par les compagnies qui vendent dans Internet. »

Selon lui, il est inévitable que le gouvernement réglemente le secteur.

Programmes de certification

Un autre obstacle important au commerce électronique tient à la question que bien des internautes se posent : À qui ai-je affaire ? Vais-je recevoir la marchandise que j'ai payée ?

Là encore, on pourrait croire que devant les hésitations suscitées par de telles questions, les entreprises se précipiteraient pour mettre en place des processus qui garantissent leur bonne foi.

Ce n'est pas le cas. Le programme le plus vieux, celui du **Better Business Bureau** (BBB) (*www.bbbonline.com*), qui date de 1997, a récolté jusqu'ici environ 4 000 membres.

Le plus prestigieux et le plus structuré, *WebTrust*, lancé en 1998 par l'**American Institute of Chartered Public Accountants**, n'a récolté à ce jour que 27 candidats, dont **Bell Canada** et **Fortune 1000** au Québec. Il a fallu attendre jusqu'au 14 mars dernier pour qu'un premier site (*shopcsc.com*) obtienne sa certification WebTrust dans la très populaire catégorie des produits informatiques.

Bien qu'il soit le plus populaire, le programme du Better Business Bureau n'est certainement pas le plus musclé - ce qui explique peut-être sa popularité. Essentiellement, il demande aux entreprises de démontrer qu'elles ont mis au point un processus de résolution de plaintes satisfaisant dans le passé.

Par ailleurs, le BBB fait une vérification des propriétaires de la compagnie et effectue une visite à ses bureaux.

De plus, le BBB offre un programme de protection de l'information semblable à celui de TRUSTe : on peut faire ce qu'on veut, à la condition de le déclarer.

Une originalité du BBB tient à son programme d'*auto-surveillance* de la publicité, qui vise à empêcher sur les sites toute publicité mensongère ou offensante à l'endroit des enfants.

Vérification fouillée

WebTrust n'est guère plus solide au chapitre de la protection de l'information. Par contre, pour confirmer le sérieux des pratiques commerciales d'un site, il n'a pas son égal.

Pour obtenir un sceau *WebTrust*, la compagnie doit faire la démonstration à un comptable qualifié qu'elle déclare toutes ses pratiques commerciales : prise de commandes, procédures de livraison et de retour de marchandise, règlement des transactions, etc. Par dessus tout, le comptable s'assure que la compagnie livre la marchandise selon les termes et les conditions convenues avec le client.

De plus, ses pratiques sont vérifiées aux 90 jours. Elles doivent être approuvées, sinon le sceau est révoqué.

Plutôt coûteux

Ces services ne sont pas donnés. Par bonheur, leurs prix sont ajustés en fonction de la taille des compagnies. Ils varient de 150 $ à 5 000 $. Le plus coûteux est WebTrust : 1 400 $ pour la certification initiale, plus les frais de la vérification trimestrielle.

Paradoxalement, ces programmes visent à rassurer en premier lieu les consommateurs - qui sont les moins à risque. Étant donné que les paiements se font la plupart du temps par carte de crédit, le client n'est responsable que pour les 50 premiers dollars de la transaction, un montant déductible qui, le plus souvent, ne lui est même pas facturé.

« Si le client ne reçoit pas une marchandise, le problème devient celui de la banque et du marchand. Le risque n'est pas du côté du consommateur, mais de **Visa** ou de **MasterCard**, par exemple », explique **Richard Groot**, directeur général adjoint, commerce électronique Québec, à la **Banque Scotia**. ■

Les technologies de stockage foisonnent et se raffinent

André Mondoux

La numérisation générale des sources d'information a engendré un autre phénomène, plus discret celui-là, mais tout aussi répandu : l'utilisation de technologies de stockage pour conserver les données.

Les unités de stockage sont au coeur des processus de numérisation de contenu, qu'il s'agisse d'Internet, de commerce électronique, de photographie numérique, d'archivage de documents ou de diffusion d'informations. Si la révolution numérique est une locomotive qui fonce à toute allure, les technologies de stockage sont le charbon qui fait tourner les bielles.

Le journal LES AFFAIRES a dressé un portrait des principales nouveautés. ■

Les disques durs sont loin d'être démodés

Malgré toutes les innovations technologiques, le bon vieux disque dur continue non seulement de tenir la rampe, mais il réussit également à faire preuve d'innovation.

Les disques rigides, une technologie qui date des débuts de la micro-informatique, sont plus populaires que jamais. Face à la hausse des quantités de données à stocker, à l'augmentation de la taille des logiciels et des fichiers-documents et à la prolifération des fichiers lourds contenant images, son et vidéo, les fabricants de disques durs ont répliqué par des disques plus volumineux, plus rapides et plus flexibles.

Aujourd'hui, il n'est pas rare de voir une station de travail dotée d'un disque dur de 13 Go et plus, une capacité de stockage qui, il y a quelques années à peine, aurait fait rêver n'importe quel administrateur de serveurs d'entreprise.

Pour leur part, les serveurs peuvent désormais bénéficier des modèles de disques pouvant contenir 70 Go et plus.

Au cours de la dernière année, les fabricants de disques durs se sont tour à tour disputé le record de la plus haute densité de stockage au pouce carré. Actuellement détenu par **IBM**, le record en vigueur est de 11,6 gigabits par pouce carré, soit l'équivalent de 725 000 pages de texte !

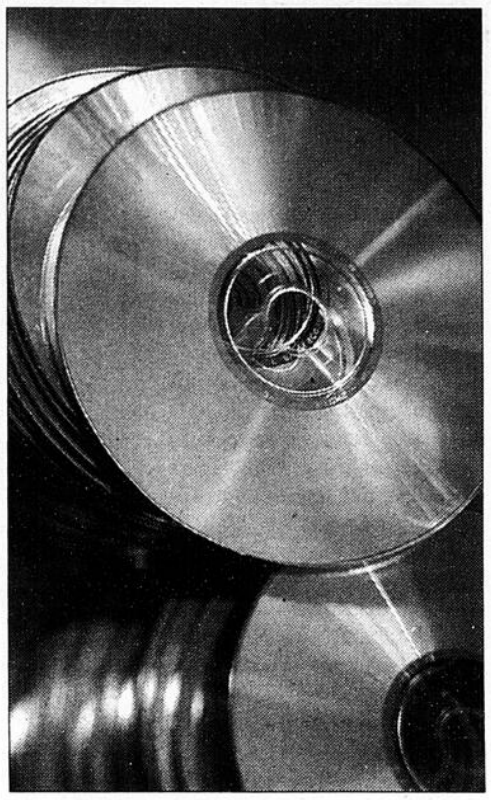
L'augmentation de la capacité des disques durs, qui se traduit notamment par une plus grande densité linéaire (plus de données stockées par piste), a rendu cruciale l'utilisation de technologies assurant le transfert efficace de ces importantes quantités d'informations entre le disque et l'ordinateur.

Voilà pourquoi les fabricants ont conçu des normes comme l'*Ultra ATA-2* (taux de transfert rapide) et des disques durs capables d'une vélocité de 7200 rpm dans le but d'éviter les goulets d'étranglement dans le traitement des données.

Contenant des informations souvent critiques, les disques durs doivent être d'une fiabilité sans faille. Dans une initiative qui risque d'en inspirer d'autres, **Seagate** a lancé l'automne dernier l'utilitaire logiciel *SeaTools*, qui permet de diagnostiquer l'état de santé d'un disque dur en exécutant une batterie de tests. (AM) ■

Internet, le plus gros disque dur au monde

À l'époque des ordinateurs centraux, il était de mise d'assurer des copies de sécurité des informations critiques et de sauvegarder ces précieuses données sur un site physiquement



distinct de celui qui abrite les infrastructures informatiques.

Cela permettait de récupérer les données en cas de désastre touchant les bâtiments d'hébergement. Cependant, la pratique de conserver les données sur un autre site physique s'est estompée, à mesure que la micro-informatique s'étendait dans toutes les sphères.

Curieusement, on doit à Internet, un agent de décentralisation s'il en est, le retour à cette pratique.

En effet, de plus en plus de firmes offrent des services d'archivage de sécurité dans Internet. Le concept est simple : en utilisant un logiciel client, les utilisateurs peuvent transférer leurs données sur un serveur Internet distant.

Ces services sont offerts aux utilisateurs individuels (on songe notamment à *@Backup* et aux nouveaux services *iTools* d'**Apple**), aux entreprises (environ 500 $ US par année pour 10 usagers) et aux fournisseurs d'accès Internet (qui, ainsi, peuvent devenir des fournisseurs de services logiciel, les ASP (*Application Service Provider*).

Pour plus de sécurité, certains des services chiffrent (encodage) les données stockées avec des algorithmes à 128 bits, un seuil d'encryption réputé quasi inviolable.

Les services d'archivage dans Internet ont plusieurs avantages. D'une part, ils sont accessibles en tout temps, tout au long de l'année.

De plus, les copies archivées étant sauvegardées sur un serveur distant, les entreprises sont donc parées à toute éventualité, y compris un sinistre sur les lieux de leurs équipements informatiques.

Par ailleurs, ces services d'archivage permettent aux usagers d'avoir accès aux données à partir de n'importe quel point de liaison Internet; ils peuvent ainsi servir également d'entrepôt commun où divers usagers peuvent partager des données. (AM) ■

Les CD inscriptibles tiennent leurs promesses

Depuis le temps qu'on en parlait, et bien, c'est maintenant chose faite : les lecteurs CD (disques compacts) inscriptibles (*CD-R* ou *CD-RW*) sont en train de supplanter les lecteurs cédéroms traditionnels. Il est de plus en plus fréquent pour les fabricants et les revendeurs de proposer des ordinateurs personnels dotés d'un lecteur CD-RW.

La principale raison de cette popularité est d'abord et avant tout de nature économique. Le prix d'achat des lecteurs CD inscriptibles a diminué de façon importante au cours des dernières années. Le coût est maintenant de 300 $ à 400 $ pour des lecteurs *4X* ou *6X*, un prix qui les place à la portée des PME et du grand public.

Les lecteurs CD inscriptibles sont également plus économiques à l'utilisation : un CD vierge de 650 Mo coûte entre 1,50 $ et 2 00 $, tandis qu'il faut débourser de 15 à 20 $ pour des disquettes *Zip* de 100 ou 250 Mo seulement.

Enfin, il faut souligner la grande versatilité des CD. Un CD *gravé* maison peut être lu par n'importe quel *PC* équipé d'un lecteur CD traditionnel, contrairement aux disquettes *Zip* qui exigent un lecteur approprié.

Maintenant abordables, les lecteurs CD inscriptibles offrent donc un coût de stockage par méga-octet moindre, tout en offrant un média universel pour la diffusion des données. Avec de tels attraits, il n'est guère surprenant qu'ils soient une force montante incontournable.

Ainsi, même **Iomega**, le fabricant des célèbres lecteurs *Zip*, s'est recyclé dans la fabrication de lecteurs CD inscriptibles.

Contrairement au marché des lecteurs DVD (*Digital Versatil Disk*) inscriptibles, le marché des CD inscriptibles s'est rapidement rallié autour de la norme *CD-RW*, c'est-à-dire des lecteurs CD réinscriptibles. Ces lecteurs ont l'avantage de pouvoir lire et graver les CD conventionnels, et de se transformer en un petit disque dur de 650 Mo, grâce à l'utilisation de disques *CD-RW* permettant la réécriture à volonté de données. (AM) ■

Le rôle des lecteurs DVD se précise

Sur papier, l'idée était spectaculaire : utiliser un disque optique à haute densité pour stocker 4 Go et plus de données. Malheureusement, le projet est toujours plus ou moins à l'état de rêve.

En effet, les divergences entre deux clans de manufacturiers de lecteurs DVD (*Digital Versatil Disk*) font en sorte que le marché est divisé entre deux normes : les *DVD-RAM* (disques réinscriptibles de 9,4 Go) et les *DVD-RW* (disques réinscriptibles de 4,7 Go).

Aucun accord ne semble en vue pour l'instant et même **Hewlett-Packard**, qui était sur le point de lancer un premier lecteur *DVD-RW*, a reporté la sortie du produit à l'automne prochain.

Malgré ces difficultés, il semblerait que les lecteurs *DVD* réinscriptibles seront appelés à jouer un rôle dominant.

Entre autres, la norme *DVD* commence à se tailler une place sur le marché des lecteurs vidéo pour téléviseurs.

Côté PC, les fabricants d'ordinateurs misent de plus en plus sur le *DVD-ROM* afin de placer leurs produits comme des appareils de l'ère de la convergence. Ainsi, en plus de pouvoir visionner les films, les utilisateurs pourront également éditer leurs propres films numériques.

Enfin, les caméscopes prendront bientôt le virage numérique et pour ce faire, ils auront besoin d'un média de stockage à forte capacité. Le scénario suivant sera très attrayant : utiliser le *DVD* pour stocker les films, l'insérer dans l'ordinateur pour effectuer le montage et faire jouer le produit final avec le lecteur *DVD* relié au téléviseur.

Ce format sera donc fort probablement le média universel entre les industries. Voilà donc un effet de convergence auquel il sera difficile de résister. (AM) ■

Stockage pour tous

Au cours de la prochaine année, il est assuré que nous assisterons à la venue de nouvelles générations d'appareils domestiques qui feront partie intégrante du décor numérique.

Ces *info-ménagers* puiseront leur *intelligence* dans leur capacité à effectuer le traitement de données. Ils auront donc besoin d'une capacité de stockage de données, mais celle-ci devra être flexible et versatile.

Voilà pourquoi les cartes-mémoire, comme celles de **CompactFlash** et d'**Iomega** (cartes *Click*), sont de plus en plus utilisées avec les appareils photographiques numériques, les lecteurs *MP3* portatifs et les plus récents modèles de caméscopes numériques.

Même si les quantités d'informations en circulation se sont multipliées au point d'atteindre des proportions extraordinaires, rien n'indique que cette prolifération sera la goutte qui fera déborder le vase. Au contraire, grâce aux technologies de stockage, ce vase pourra recevoir une véritable vague. (AM) ■

Des solutions abordables pour partager l'accès à Internet

Des dispositifs multifonctions pour la petite entreprise

Nelson Dumais

Depuis que l'accès Internet à haute vitesse est en voie de devenir banal, un phénomène prend de l'ampleur dans la petite entreprise et chez les travailleurs autonomes : le partage d'une même connexion. On veut que tous les ordinateurs du bureau ou de la maison aient un accès au Net, cela à bon compte.

Si plusieurs y arrivent par logiciel, on tend de plus en plus à le faire par l'entremise d'une petite boîte intelligente appelée, selon la marque, routeur, dispositif de partage, passerelle résidentielle ou boîte noire, même si la plupart ne sont pas de cette couleur.

Les ventes de dispositifs de partage augmentent rapidement, mois après mois, confirme **Benoît Massicotte**, directeur du marketing de **MicroSource**, un revendeur spécialisé de Saint-Laurent.

Le principe du partage de la connexion est basé sur l'expérience *RNIS* ou *T1* qu'on retrouve dans la PME et dans la grande entreprise. Dès qu'un ordinateur est ajouté au réseau, il devient automatiquement branché dans Internet et bien protégé derrière le dispositif pare-feu.

Les employés savent qu'ils peuvent compter sur une connexion à vitesse très acceptable à partir de n'importe quel ordinateur. Quant aux techniciens, ils apprécient le fait qu'ils n'aient pas de modem à installer et à configurer dans les ordinateurs.

Rapide et peu onéreux

Les entreprises de taille plus modeste hésitent à se doter d'un tel attirail en raison des coûts qui leur paraissent prohibitifs. D'où l'alternative câblée ou *xDSL*, des technologies très rapides et peu onéreuses qui s'avèrent simples à partager.

Il suffit de connecter le modem à un dispositif de partage, au lieu de le faire à un ordinateur du réseau, pour que le signal Internet soit redistribué partout.

En prime, ce type d'appareil vient régler deux problèmes importants : la mise en réseau local (dans le cas de petites sociétés où les ordinateurs sont isolés) et de la mise en sécurité par rapport au cyberespace. Autrement dit, ces bidules agissent à la fois comme concentrateurs Ethernet (*hub*), routeurs Internet et murs pare-feu (*firewalls*).

Ils deviennent des serveurs *Dynamic Host Configuration Protocol* (DHCP), ce qui signifie que le réseau les perçoit comme un ordinateur avec adresse *Internet Protocol* (IP) qui est spécialisé dans le partage de l'accès au réseau Internet.

En fait, dès qu'ils sont configurés et opérationnels, les dispositifs procèdent immédiatement à l'attribution d'adresses IP pour chacun des ordinateurs branchés sur le réseau, des adresses qui n'ont de sens qu'à l'intérieur du réseau.

Les dispositifs de partage font la gestion des adresses IP sans que le fournisseur de services (**Bell**, **Vidéotron**, etc.) ne s'en rende compte. C'est que l'adresse IP que le fournisseur a octroyée à son abonné n'est plus celle d'un ordinateur isolé, mais celle du dispositif.

« Le fait d'être *matériel* présente un gros avantage par rapport aux solutions logicielles comme *Wingate*, explique M. Massicotte.

« On ne dépend pas d'un PC (ordinateur personnel) sur lequel travaille un employé, ce qui prend du temps de processeur, un PC avec lequel il lui arrive de se *planter*, ce qui bloque temporairement l'accès Internet. »

Plusieurs produits

Popularité oblige, plusieurs fabricants de boîtes intelligentes s'escriment sur le marché. Mentionnons **Watchguard** avec son *SOHO* (hérité de **BeadleNet**), **D-Link** avec son *Residential Gateway*, **Linksys** avec son *EtherFast Cable/DSL Router* et **NexLand** avec son populaire *ISB2LAN* (*Internet Sharing Box to Local Area Network*).

« C'est de loin le produit qu'on vend le plus », affirme Benoît Massicotte. En fait, son entreprise est le distributeur exclusif du *ISB2LAN* au Québec.

Le *ISB2LAN* est non seulement le précurseur de toute la fournée, mais il est le seul à se conformer au *Point to Point Protocol Over Ethernet* (PPPOE), un protocole élaboré spécifiquement pour les cas de partage d'accès Internet sur réseau Ethernet, précisément celui qu'utilise Bell pour *Sympatico Haute Vitesse*. ■

PHOTO: Jean-Guy Paradis, LES AFFAIRES

■ Les ventes de dispositifs de partage d'accès augmentent rapidement, mois après mois, dit Benoît Massicotte, directeur du marketing de MicroSource.

Comment réussir l'installation d'un dispositif de partage

En installant un dispositif de partage d'accès Internet à haute vitesse dans une petite entreprise ou chez un travailleur autonome, il faut préa-lablement s'assurer que les ordinateurs soient en réseau et que ce réseau soit opérationnel.

Autrement dit, il faut que les ordinateurs se voient et puissent s'échanger des fichiers.

Dans le cas d'ordinateurs personnels (PC), il faut vérifier s'ils disposent du protocole *NetBEUI* et si leurs disques rigides sont en mode partage.

On peut ensuite se donner le maximum de chances en allant détruire toute trace du protocole *TCP/IP* dans les PC et les faire redémarrer.

Ensuite, on y réinstalle le même protocole en s'assurant que le mode *DHCP* est bien activé. (ND) ■

Modem haute vitesse : lisez attentivement le contrat

Les utilisateurs de modem haute vitesse ont intérêt à relire leur contrat avant de procéder à l'installation d'un dispositif de partage d'accès Internet.

La plupart des fournisseurs, câblos ou *xDSL*, facturent les accès supplémentaires. Plus on branche d'appareils, plus c'est cher. Même logique pour les adresses de courriel.

Et c'est là où le bât blesse. Si on peut brancher dans Internet des dizaines de postes de travail sans que **Bell** et **Vidéotron** ne le sachent, il faut un jour ou l'autre se mettre en loi quand vient le temps d'obtenir des adresses de courriel pour ses employés.

Sinon, il faut utiliser un expédient peu flatteur pour l'image de marque de l'entreprise, comme *Moncourrier* ou *Hotmail*, une solution frustrante si l'entreprise a un nom de domaine réservé. (ND) ■

Le *ISB2LAN*, de Nexland, est un produit des plus polyvalents

Le *ISB2LAN* de **Nexland** se distingue par sa grande polyvalence.

Il se branche aussi bien sur un modem câble que sur un modem *xDSL*. Il existe même un modèle pour les modems traditionnels à 56 Kb/s, ce qui ne constitue pas l'affaire du siècle. On peut en outre lui brancher un seul ou quatre appareils, aussi bien des ordinateurs que des concentrateurs.

En configuration de base (400 $), le *ISB2LAN* est vendu avec deux câbles : un inversé (*crossover*) si on ne veut connecter qu'un seul ordinateur, et un régulier (Ethernet standard) si on veut le relier à un concentrateur (le *ISB2LAN* se branche alors entre le modem et le concentrateur).

Configuration multiple

En configuration pour quatre appareils (modèle *H4*, 450 $), on peut brancher quatre ordinateurs ou quatre concentrateurs, ce qui rend alors possible le partage d'une même connexion Internet entre plusieurs dizaines de personnes (limite théorique de 256 utilisateurs).

Autre avantage, son mode de configuration est à l'abri des systèmes d'exploitation. À partir d'un poste de travail quelconque (*MacOS*, *Windows*, *Linux* ou *Solaris*), on accède tout simplement au *BIOS* de l'*ISB2LAN* par *Explorer* ou *Netscape*. Cette méthode ne lui est toutefois pas exclusive. (ND) ■

Le passage à Linux est une question d'efficacité

André Mondoux

Les entreprises qui du jour au lendemain installent *Linux* ne font pas légion. Habituellement, le système d'exploitation *Linux* est déployé *localement* (parfois en cachette) par des fervents de la plateforme. Cependant, il y a des conditions où il est plus facile pour une entreprise d'adopter *Linux* à grande échelle.

Les **Services d'assurance Transport Expert** et **Marine Expert** sont deux sociétés spécialisées en assurances de véhicules routiers et marins qui appartiennent à une même compagnie. Pour gérer les opérations, la firme compte sur un réseau informatique d'une quarantaine de postes de travail.

La gestion de ce réseau est confiée à une petite firme indépendante. Cette firme est également responsable de l'entretien et de la création des applications d'assurance qui ont été créées avec l'outil de développement *Delphi*.

« Un des problèmes que nous avions avec notre serveur *Windows NT* est qu'il était souvent en panne, et ce, jusqu'à plusieurs fois par jour », explique **Michel Alie**, assistant directeur général de l'entreprise.

« Le plus frustrant est que dans 90 % des cas, il n'y avait pas de message d'erreur, ce qui complique davantage la recherche de solutions », précise-t-il.

Confrontée à cette situation, la firme de soutien informatique a entrepris d'explorer les avenues offertes par *Linux*. Après avoir effectué quelques tests, il fut décidé d'installer la distribution *Linux* de **Red Hat** comme serveur de fichier.

Les résultats furent concluants. Non seulement le système n'est pratiquement plus tombé en panne, mais le lecteur à ruban pour les archivages de sécurité, une unité stratégique qui fonctionnait de façon erratique sous *Windows*, a été intégré automatiquement sous *Linux* et n'a jamais connu de pépin.

« Passer à *Linux* n'a jamais été pour nous une question de coûts, mais bien de productivité. Nous ne subissons plus de perte de productivité liée à des pannes du réseau », souligne M. Alie.

« Et si, en plus, notre système d'archivage de sécurité est plus fiable, nous n'avons vraiment aucune raison de mettre en doute la direction stratégique prise par nos consultants en informatique », ajoute-t-il.

Une initiative isolée

Le scénario de cette entreprise est assez typique. Dans bien des cas, la percée de *Linux* est le résultat d'une initiative isolée, en marge des canaux officiels.

Bien souvent, on fait appel à *Linux* parce que l'autre système d'exploitation ne donne pas pleine satisfaction.

La firme de consultation, de petite taille, n'était pas irrémédiablement liée par des gros investissements à une plate-forme particulière et elle a su adroitement miser sur la flexibilité que lui confère sa petitesse. Une grande entreprise et une plus grande firme de consultation n'auraient pu faire pénétrer *Linux* aussi aisément.

Un passage en douceur

Installer *Linux* comme serveur Web ou serveur de fichiers n'est plus un geste osé comme c'était le cas il y a 18 mois à peine.

Par contre, faire migrer les usagers de leur plate-forme actuelle à l'environnement *Linux*, voilà qui fait décidément preuve d'avant-gardisme. Et c'est ce que les Services d'assurance Transport Expert et Marine Expert ont l'intention de faire aux cours des prochains mois.

Pour ces firmes, faire migrer les usagers vers *Linux* implique d'assurer le roulement de deux types d'applications sous *Linux* : les logiciels de bureautique traditionnels (principalement le traitement de texte et le fureteur Internet) et les applications d'assurance conçues sur mesure avec *Delphi*.

La migration des applications de bureautique ne devrait pas causer bien des problèmes, dans la mesure où elles sont universelles : les logiciels de traitement de texte, peu importe leur plate-forme, offrent sensiblement les même fonctions. Le choc de la migration serait donc relativement modeste, comme passer par exemple de *Word* à *WordPerfect* ou *Star Office* pour *Linux*.

La migration d'applications stratégiques est toujours une opération délicate. Ici encore, l'entreprise jouit de circonstances favorables. Le concepteur de *Delphi*, **Borland**, a en effet annoncé son intention d'offrir son produit sous *Linux* d'ici la fin de l'année. Or, tout naturellement, Borland offrira des outils pour exporter les applications *Delphi* à l'environnement.

Voilà qui effectivement devrait adoucir le passage de *Windows* à *Linux*. De plus, puisque les applications sont conçues à l'interne, la firme de consultation aura donc tout le loisir d'apporter les modifications qui s'imposeront.

Se sentir en confiance

Sous certaines conditions, sur le plan technique, il n'y a donc pas beaucoup d'obstacles à l'intégration de *Linux* dans une entreprise. Le principal défi reste toujours celui de la perception qu'ont les gens à propos de *Linux*.

Voilà pourquoi la présence d'un spécialiste *Linux*, que ce soit une firme de consultant ou un employé à l'interne, reste toujours dans bien des cas le facteur qui peut faire pencher la balance. ■

De l'aide pour gérer ses biens technologiques

Encore Asset Services compte Bombardier et Nortel parmi ses clients

André Salwyn

Beaucoup de grandes entreprises n'achètent pas les ordinateurs qu'elles utilisent : elles les louent.

Cela veut dire qu'à la fin d'un bail, il faut trouver les ressources pour faire l'inventaire des biens loués, vérifier si tous les appareils sont en état de fonctionnement et éventuellement en disposer, soit en les offrant à des oeuvres de charité, soit en les remettant sur le marché par l'entremise de canaux de revente.

C'est en travaillant dans son garage, en 1997, que **Keith Pitts**, le président d'**Encore Asset Services**, a commencé à mettre en pratique une idée qui lui semblait avoir beaucoup de sens : aider les entreprises à gérer leurs biens technologiques.

L'idée de M. Pitts n'était vraiment pas bête puisque aujourd'hui, l'entreprise de Toronto gère plus de 82 000 biens technologiques appartenant à des dizaines de grandes compagnies de partout au Canada, dont **Bombardier** et **Nortel**.

M. Pitts a donc rapidement été obligé de sortir de son garage pour s'installer dans des locaux aptes à recevoir les milliers d'appareils dont on lui confiait la gestion. C'est maintenant dans des entrepôts de près de 20 000 pi^2 situés près de l'aéroport de Toronto, que le travail se fait.

Ayant conclu des partenariats stratégiques avec de grands fabricants d'ordinateurs et de périphériques comme **Hewlett Packard** et **Dell**, Keith Pitts obtient d'eux les logiciels et outils nécessaires pour vérifier le bon fonctionnement de chaque appareil et les remettre en état au besoin.

« Mais l'élément clé du succès d'Encore en matière de gestion de biens technologiques, c'est un système de compte rendu flexible et précis, affirme M. Pitts. Nous avons mis au point une base de données conviviale que nous offrons gratuitement à nos clients. »

« Chaque bien technologique se voit attribuer un code à barre unique. Nous sommes alors en mesure d'enregistrer toutes les inspections et modifications effectuées sur chaque item, à partir du moment où il arrive dans une entreprise, et suivre cet item à la trace jusqu'à la vérification d'inventaire, son stockage ou sa livraison à un autre client. »

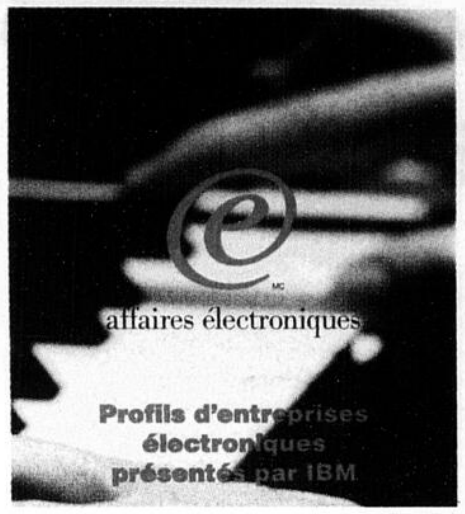
Des économies et d'autres avantages

Le coût moyen d'une vérification de l'état d'un appareil varie entre 2 $ et 40 $. Mais ce sont surtout les économies qu'elles réalisent sur le plan de l'entreposage qui intéressent les entreprises .

Hewlett Packard estime que ses coûts d'entreposage étaient trois fois plus élevés avant qu'elle ne devienne un client d'Encore.

Par ailleurs, Encore dispose de tout ce qu'il faut en inventaire pour effectuer des mises à niveau et ainsi rendre un appareil plus performant ou prolonger sa durée de vie.

« En fait, nous sommes aussi un magasin multiservices dans lequel nos clients trouvent tout ce dont ils ont besoin, aussi bien en termes de matériel qu'en matière de documents comme des manuels d'utilisation et des logiciels pilotes », précise M. Pitts. ■



Le défi : Accroître les ventes du Disklavier, un piano acoustique doté de toutes les fonctions avec capacité de reproduction parfaite, en ciblant le marché domiciliaire grand public.

La solution : Utiliser Internet pour distribuer de la musique destinée au Disklavier. Les gens possédant ce piano pourront bientôt se connecter au site Web de Yamaha pour effectuer une recherche parmi les pièces offertes. Lorsqu'une d'entre elles les intéressera, ils pourront en faire l'écoute, la commander, télécharger le fichier et la faire jouer instantanément.

Les résultats : Yamaha a étendu son marché, a réduit de façon remarquable ses coûts d'enregistrement et de distribution, a amélioré la satisfaction de la clientèle, et fournit une vitrine de présentation musicale dynamique pour les compositeurs, qu'ils soient nouveaux ou établis.

IBM affaires électroniques

Tapez www.yamaha.com pour voir les affaires électroniques à l'œuvre. Pour découvrir comment votre entreprise peut tirer le maximum des affaires électroniques, cliquez sur l'emblème affaires électroniques, faites le **1 800 IBM-7080 (426-7080), poste 80X**, ou visitez notre site Web à **www.can.ibm.com/affaires_electroniques/EB80**