SÉCURITÉ INFORMATIQUE

SOMMAIRE

Aujourd'hui, la sécurité concerne tout le monde
p. A 2

Les attaques des pirates prennent de nouvelles formes
p. A4

Les entreprises de télécommunications se lancent dans le marché de la sécurité
p. A 6

Votre identité peut être aisément volée
p. A 13

Des virus peuvent détruire toutes vos données
p. A 16

Les ravages que peuvent faire les pirates de haut vol dépassent l'imagination. Des victimes, que la police avait prises pour les malfaiteurs, ont ainsi failli se retrouver en prison.

La sécurité préoccupe grandement les gens d'affaires

Réunis dans un colloque tenu à Saint-Hyacinthe, ils s'entretiennent de la situation

Gaël Le Corre-Laliberté
gael.lecorre@transcontinental.ca

La 13e édition du *Colloque québécois de la sécurité de l'information* (CQSI) a permis de mettre l'accent sur l'éducation en matière de sécurité auprès du personnel d'une entreprise.

Sous le thème « La sécurité, c'est une affaire de communication », le colloque s'est déroulé à Saint-Hyacinthe les 25 et 26 avril derniers. Quelque 400 personnes avaient répondu à l'invitation de l'**Association de la sécurité informatique de la région de Québec** (ASIRQ) et de l'**Association de la sécurité de l'information de la région de Montréal** (ASIMM).

La présidence d'honneur était assurée par **Jacques Duchesneau,** président et chef de la direction de l'**Administration canadienne de la sûreté du transport aérien** (ACSTA) et ex-directeur du **Service de police de la Communauté urbaine de Montréal.**

Une quarantaine d'experts provenant des quatre coins de l'Amérique étaient présents aux différentes conférences, tables rondes et autres démonstrations technologiques. Ils ont répondu aux interrogations des participants. Le journal LES AFFAIRES a recueilli plusieurs réactions à la suite du colloque.

Des employés qui travaillent à distance

Jean Audet, vice-président, technologie de l'information et administration des contrats, de **L'Union-Vie compagnie d'assurance-vie :**

« Le quart de notre personnel travaille à domicile, dit M. Audet. Certaines de ces personnes sont amenées à effectuer des évaluations de risque ou encore des études de réclamations. Pour cela, elles ont accès à distance aux dossiers de nos clients.

« D'où l'importance primordiale que nous accordons à la sécurité informatique, qui doit être la plus haute et la plus fiable possible à tout moment. Il n'est en effet pas question que des regards indiscrets puissent tomber sur ces dossiers confidentiels.

« J'ai apprécié le colloque pour la variété des sujets abordés et pour la qualité des experts invités. Les présentations ayant trait à la gestion de crise et la gestion des identités m'ont captivé. Il est en effet crucial de savoir qui a le droit de faire quoi sur un réseau : plus le réseau devient complexe, plus il est important de bien définir les autorisations. »

CQSI

La présidence du 13e *Colloque québécois de la sécurité de l'information* était assumée par Jacques Duchesneau, président de l'Administration canadienne de la sûreté du transport aérien.

L'affaire de tous

Sylvie Sigouin, chef de service, sécurité d'exploitation informatique, de **Desjardins :**

« La sécurité est maintenant l'affaire de tous, à tous les niveaux de l'entreprise, dit-elle. Ce n'est plus la responsabilité de la seule l'équipe informatique, mais de tous les employés. C'est ce point qui m'a le plus intéressé dans le colloque.

« Autre point intéressant : le défi pour les entreprises de respecter les exigences juridiques, comme celles de la loi C-198 ou *Sarbanes-Oxley.* Pour certaines entreprises, cela peut entraîner une revue de fond en comble de ses processus d'affaires. Le colloque m'a permis de rencontrer des gens d'affaires qui ont les mêmes préoccupations que les miennes, et je trouve cela très enrichissant. »

Préoccupation constante

Pierre Comeau, directeur des opérations, Département d'informatique et de génie logiciel, de l'**Université Laval :**

« Aujourd'hui, pour que la sécurité du réseau informatique d'une entreprise soit efficace, on ne peut plus se passer de la formation des employés, dit M. Comeau. Il est important que chacun comprenne bien l'importance de la sécurité et en tienne compte dans sa façon de travailler.

« Le danger peut venir aussi bien de l'extérieur (virus, pirates, etc.) que de l'intérieur (employés malveillants, etc.). La sécurité doit donc devenir une préoccupation constante des entreprises, et même des universités, qui doivent veiller à ce que des étudiants ne puissent pas consulter des dossiers informatiques de professeurs.

« Le Colloque m'a permis de découvrir les tendances en matière de sécurité informatique, ce qui me permettra d'améliorer les programmes de formation de mon département. »

« Où est l'équilibre parfait ? »

Hugo Dominguez, directeur, sécurité informatique, de l'**UQAM :**

« Mon défi est de trouver l'équilibre entre la liberté de recherche des étudiants et des professeurs et la sécurité nécessaire à toute université, dit M. Dominguez.

« Par exemple, dois-je bloquer tout message ou toute recherche comportant le mot *Viagra,* qui est une source phénoménale de pourriels, mais aussi un sujet de recherche pertinent ? ■

LES PRINCIPALES TECHNIQUES D'ATTAQUE

Le cheval de Troie

Programme malveillant d'apparence anodine (jeu, carte postale virtuelle, etc.). Une fois installé dans le disque dur, il peut, par exemple, déclencher un virus ou permettre à un pirate de prendre le contrôle de l'ordinateur à distance.

La porte arrière *(backdoor)*

Point d'entrée plus ou moins secret installé dans un programme ou un système informatique. En temps normal, la porte arrière permet de contourner un blocage accidentel, par exemple quand l'utilisateur a oublié son mot de passe.
Or, des pirates de haut vol sont capables de découvrir une porte arrière, et ainsi, de s'infiltrer dans l'ordinateur.

Le *sniffing*

Écoute d'une ligne de transmission par laquelle transitent des données personnelles. Il est ainsi possible de subtiliser des renseignements confidentiels, à la volée.

L'attaque par rebond

Attaque menée par l'entremise d'un ordinateur rendu complice du pirate à l'insu de son propriétaire. Il est ainsi plus compliqué de retrouver la trace du pirate.

L'attaque par le milieu

Le pirate se positionne entre deux ordinateurs communiquant régulièrement l'un avec l'autre. Il peut dès lors subtiliser les mots de passe de l'un et de l'autre, voire des données confidentielles. Il peut aussi décider d'attaquer l'un ou l'autre des ordinateurs.

Le déni de service

Paralyser un ordinateur ou un serveur en le submergeant d'information (courriels, etc.). Plusieurs machines peuvent être utilisées simultanément par le pirate (souvent des ordinateurs manipulés à l'insu de leur propriétaire) afin d'intensifier l'attaque. ■ **O.S.**

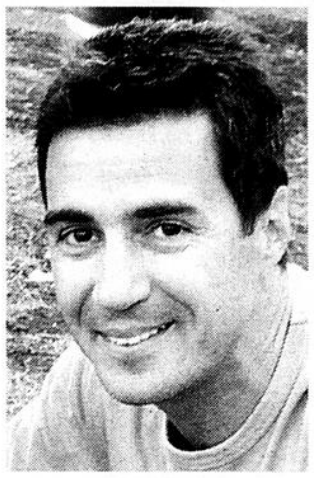
Trois étapes pour se doter d'un système de sécurité

Neuf entreprises canadiennes sur 10 disent accorder une grande importance à la sécurité de leurs données, selon Ernst & Young

Yan Barcelo
dossiers@transcontinental.ca

Neuf entreprises canadiennes sur 10 disent accorder une grande importance à la sécurité de leurs données, selon une étude menée en 2003 par **Ernst & Young.** Or, seulement une sur deux (46 %) agit véritablement en conséquence.

C'est pourquoi **René Vergé,** directeur, services-conseils, de **CGI,** conseille aux entreprises déficientes de procéder en trois étapes pour se doter d'un système de sécurité adéquat : stratégique, tactique et opérationnel. C'est l'étape stratégique qui requiert le plus de réflexion.



René Vergé, de CGI, conseille de donner au personnel des règles claires d'utilisation du réseau informatique.

1 L'étape stratégique

Il s'agit d'établir les grandes orientations du plan de sécurité : par exemple, déterminer le type de système le mieux adapté à la mission d'affaires de l'entreprise, nommer le principal responsable et définir les mécanismes spécifiques (autorisations d'accès, mise à jour des mots de passe, etc.).

Cette réflexion peut être poussée encore plus loin, et déterminer entre autres la politique de l'entreprise en matière d'utilisation personnelle d'Internet pendant les heures de travail, ou encore les pratiques de courriel recommandées. « Nous suggérons aux entreprises de rédiger un document clair, de deux ou trois pages, expliquant tout cela aux employés », dit M. Vergé.

De plus, il est important de déceler les secteurs les plus sensibles du réseau informatique, et d'agir en conséquence. À cet égard, il est bon de se poser trois questions :

> Quelles menaces pèsent sur le système (virus, piratage) ?
> Quelle est le degré de vulnérabilité des différentes parties du système ?
> Quelles peuvent être les conséquences concrètes d'une attaque réussie ?

La meilleure protection ne parviendra jamais à empêcher un employé d'ouvrir un courriel suspect.

En répondant à ces questions, l'entreprise est alors en mesure d'élaborer un plan directeur dictant les mesures concrètes à mettre en place. Ce plan peut permettre de déterminer entre autres les besoins en sécurité des réseaux téléphoniques et informatiques, les procédures d'identification du personnel à adopter et les programmes de formation à faire suivre aux employés.

C'est souvent à l'étape stratégique que les PME souffrent de carences, souligne **Patrick Naoum,** vice-président, services professionnels et technologies, d'**ESI Technologies de l'information.** « Elles ont généralement de bons outils, mais ne s'en servent pas comme il le faudrait », dit-il.

2 L'étape tactique

Il s'agit d'adopter des procédures précises de sécurité, dans l'enceinte même de l'entreprise. Cela concerne autant la définition des zones d'accès limité que les cartes d'accès et le personnel de surveillance.

Des procédures similaires doivent être appliquées à l'accès au réseau informatique.

3 L'étape opérationnelle

Il s'agit de mettre en oeuvre les procédures de sécurité. Cela concerne, par exemple, un plan d'action en cas d'attaque du système, ou encore des sessions de formation du personnel. Ce dernier point est d'une grande importance.

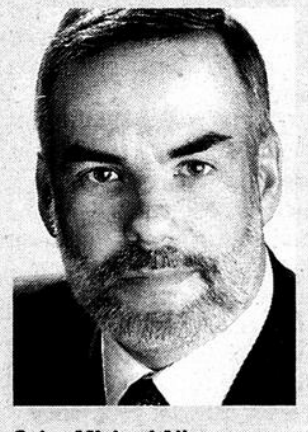
En effet, la meilleure protection informatique ne parviendra jamais à empêcher un employé d'ouvrir un courriel suspect. Pour éviter un geste aussi déraisonnable, le seul moyen est la sensibilisation du personnel aux dangers informatiques, comme les pourriels qui circulent sur le Web. ■

La rivalité des certifications s'accroît au Québec

Sur le marché de la sécurité informatique, il devient très avantageux d'avoir une ou plusieurs certifications attestant de ses compétences. C'est pourquoi on assiste à une forte compétition entre les différents organismes de certification, qui rivalisent entre elles grâce à de nouvelles certifications.

En 2002, l'**Information Systems Audit and Control Association** (ISACA) lançait la *CISM,* destinée aux gestionnaires de la sécurité informatique. L'autre grand acteur, l'**International Information Systems Security Certification Consortium** (ISC2), répliquait l'année suivante avec la certification *SSCP* pour l'architecture de systèmes.

Ces différentes certifications attestent que leurs titulaires ont une expertise élevée en sécurité informatique et qu'elle est parfaitement à jour.



Selon Michael Albertson, de SecurIP, rien ne vaut l'expérience d'une gestion quotidienne de la sécurité.

Des connaissances surtout théoriques

Michael Albertson, président de **SecurIP services conseils,** estime que les entreprises devraient considérer les certifications comme une priorité pour leur sécurité informatique. « Toutefois, les certifications assurent que telle personne a un bon bagage de connaissances, surtout théoriques, et pas nécessairement pratiques », reconnaît-il.

Est-ce que l'employé certifié sera capable de résister à la pression, le moment venu ? Pourra-t-il travailler en respectant les contraintes de l'entreprise, souvent budgétaires ? « Seule l'expérience d'une gestion quotidienne de la sécurité permet d'acquérir de telles compétences », poursuit-il. ■ G.L.-L.

Les certifications en bref

CISA, CISSP et CISM

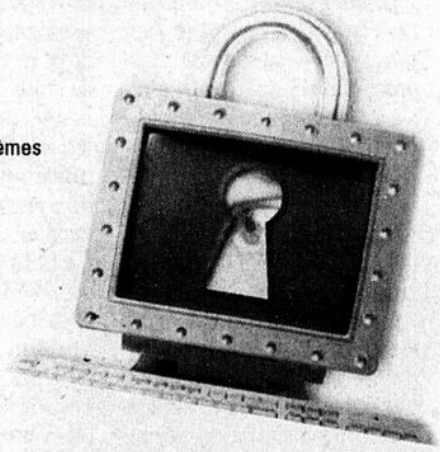
> Une des principales certifications demeure la *CISA,* proposée par l'**Information Systems Audit and Control Association** (ISACA) depuis 1978.
> Une autre est la *Certified Information Systems Security Professional* (CISSP), délivrée par l'**International Information Systems Security Certification Consortium** (ISC2) depuis 1991.
> Les deux certifications comptent chacune quelque 30 000 personnes accréditées.
> De son côté, la *CISM,* également de l'ISACA, compte 5 000 personnes accréditées.

À qui s'adresse la *CISSP* ?

Aux professionnels de la sécurité qui possèdent trois années d'expérience dans le domaine de la gestion de la sécurité. La certification est sous réserve de la participation à des stages de formation continue.

Les thèmes abordés

> La gestion de la sécurité
> Les architectures de sécurité
> Les contrôles d'accès
> La sécurité du développement d'applications et de systèmes
> La sécurité de l'exploitation
> La sécurité physique
> La cryptographie
> La sécurité des réseaux et des télécommunications
> La continuité des activités
> Les lois, enquêtes et éthique



L'examen

> Épreuve de 250 questions à choix multiple en six heures
> Langues : français et anglais
> Note de passage : 70 %
> Lieu où passer l'examen : Montréal et Québec (peut être organisé ailleurs si la demande est suffisante)

À qui s'adresse la *CISA* ?

Aux professionnels de l'audit, du contrôle et de la sécurité des systèmes informatiques, ayant au moins cinq années d'expérience dans le domaine.

Les thèmes abordés

> Processus d'audit des systèmes informatiques
> Gestion, planification et organisation des systèmes informatiques
> Infrastructure technique et pratiques opérationnelles
> Protection des biens informatiques
> Plan de secours et de continuité de l'activité
> Développement, acquisition, mise en œuvre et maintenance des systèmes d'application commerciaux
> Évaluation des processus métier et de la gestion des risques

L'examen

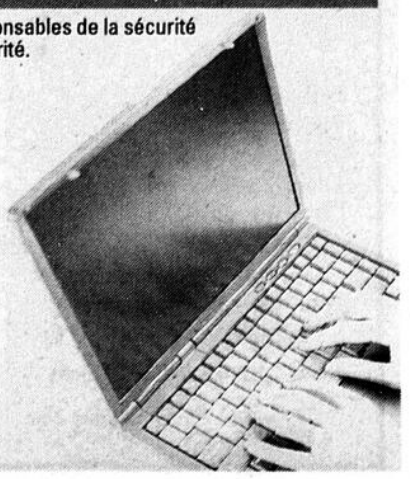
> Épreuve de 200 questions à choix multiple en quatre heures
> L'examen se donne en français et en anglais et a lieu en juin et en décembre
> Note de passage : 75 %
> L'examen se déroule à Montréal et à Québec

À qui s'adresse la *CISM* ?

Aux gestionnaires de sécurité : directeurs informatiques, responsables de la sécurité des systèmes informatiques (RSSI) et aux consultants en sécurité.

Les thèmes abordés

> Gouvernance de la sécurité
> Gestion des risques
> Gestion des plans de sécurité
> Gestion des activités de sécurité
> Gestion des incidents



L'examen

> Épreuve de 200 questions à choix multiple en quatre heures
> L'examen se donne uniquement en anglais et a lieu en juin
> Note de passage : 75 %
> L'examen se donne à Montréal et à Québec

TABLEAU ET RECHERCHE : LES AFFAIRES

Les menaces sont moins destructrices, mais plus pernicieuses

Les pirates du Web ne cherchent plus à se faire un nom dans leur communauté, mais à faire fortune

Yan Barcelo
dossiers@transcontinental.ca

Avez-vous remarqué qu'il est moins souvent question d'attaques massives de virus, comme à l'époque des *Melissa* et autres *I love you ?* Ceux-ci, qui datent d'à peine deux ou trois ans, étaient parvenus à détruire des masses colossales de données.

Pourquoi ce changement ? À l'époque, les pirates cherchaient avant tout à se faire un nom dans leur communauté. Et aujourd'hui, ils courent après l'argent. C'est ce qu'indique un récent rapport de **MessageLabs,** une entreprise spécialisée dans la sécurité à distance.

Les virus actuels ont pris de nouvelles formes. On parle maintenant de logiciels espions (*spyware*), de réseaux de zombies, de chevaux de Troie et des omniprésents pourriels (*spam*).

De manière clandestine

En fait, les virus sont aussi présents qu'auparavant, mais se font de plus en plus discrets. Ils visent moins à dérégler les ordinateurs qu'à les asservir à l'insu de leurs propriétaires, en installant dans leurs circuits des fragments de code clandestin, notamment des chevaux de Troie. Une de leurs tâches est de transformer l'ordinateur en « zombi », une sorte de mort-vivant qui devient alors un relais pour diffuser des pourriels et diverses formes d'arnaques.

MessageLabs évalue à 50 millions le nombre d'ordinateurs infectés de la sorte dans le monde. Et les trois quarts des pourriels interceptés au cours des 12 derniers mois par cette entreprise américaine avaient été expédiés par l'entremise de réseaux de zombies.

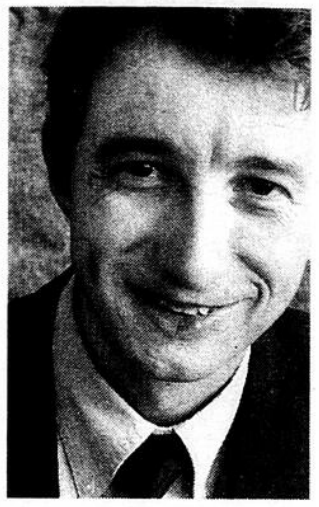
Contrôler un réseau de zombies permet de se faire de l'argent par millions de dollars, en le louant à des arnaqueurs. « Il existe des conflits entre groupes criminels rivaux pour contrôler des réseaux de zombies, affirme un rapport de MessageLabs. Par exemple, on a assisté l'an dernier à une guerre entre deux virus, *Netsky* et *Bagle*, qui tentaient de se détruire l'un l'autre pour avoir la mainmise sur différents réseaux. »

Quel internaute ne connaît pas le pourriel ? Et qui n'en est pas agacé ? La question vient immédiatement à l'esprit : comment se fait-il qu'il en existe toujours ? Tout simplement parce qu'ils permettent de gagner beaucoup d'argent.

En effet, un taux de réponse de 1 % de la part des internautes est suffisant pour rentabiliser une opération d'envoi de pourriels, indique **David Poellhuber,** président de **ZéroSpam,** une entreprise montréalaise spécialisée dans la sécurité à distance. Par exemple, **Jeremy Jaines,** un maître du pourriel récemment condamné en Caroline du Nord, encaissait entre 500 000 et 750 000 $ par mois grâce à ses bases de données comportant pas moins de 85 M d'abonnés d'**AOL.**

Le plus grand danger

Quant aux logiciels espions, ils pourraient devenir la plus grande menace du Web. Il s'agit de logiciels illicites, portant des noms tels que *CoolWebSearch, Webhancer* et *GatorGain*, que l'internaute télécharge à son insu et qui épient ses moindres faits et gestes. Les réseaux de téléchargement de musique, comme **Kazaa,** sont l'une des sources les plus prolifiques de ces logiciels espions. Ironiquement, les internautes eux-mêmes, en acceptant la licence d'utilisation qui leur est présentée à l'entrée de ces sites, rendent cette infiltration tout à fait légale.



David Poellhuber, de ZéroSpam, indique qu'un taux de réponse de 1 % à un envoi de pourriels suffit à rentabiliser l'opération.

Jusqu'à l'été 2004, les méfaits de ces logiciels espions étaient plutôt modestes. L'espion se contentait, par exemple, d'enregistrer les déplacements de l'internaute et d'expédier ses rapports à un détenteur de réseau de zombies qui les revendait à des arnaqueurs.

Quel internaute ne connaît pas le pourriel ? La question qui vient à l'esprit est comment se fait-il qu'il en existe toujours ? Parce qu'ils permettent de gagner beaucoup d'argent.

Mais voilà qu'une étude du fournisseur d'accès Internet **Earthlink** révèle que les formes les plus pernicieuses de logiciels espions se sont développées de manière foudroyante ces derniers mois. Il s'agit d'enregistreurs de frappe et de capteurs d'écran capables d'enregistrer des renseignements confidentiels concernant la victime, comme ses mots de passe et ses numéros de cartes et de comptes bancaires.

« Il n'y avait pas d'argent à faire dans les virus, mais il y en a dans les logiciels espion », souligne **Robert Massé,** président de **GoSecure,** une entreprise montréalaise de consultation en sécurité. ■

L'étendue des dégâts dépasse parfois l'imagination

L'an dernier, les dégâts occasionnés par les virus se sont élevés dans le monde à 17,5 milliards de dollars américains (G$ US), selon **Computer Economics,** une firme californienne d'analyse de marché. En 1995, ils s'élevaient à seulement 500 M$ US.

Les entreprises sont touchées au premier chef par les attaques de virus. Sur 500 entreprises américaines interrogées par le **CERT,** un organisme américain consacré au crime informatique, le tiers étaient en mesure de chiffrer l'étendue des dégâts subis, et le total atteignait 600 M$ US.

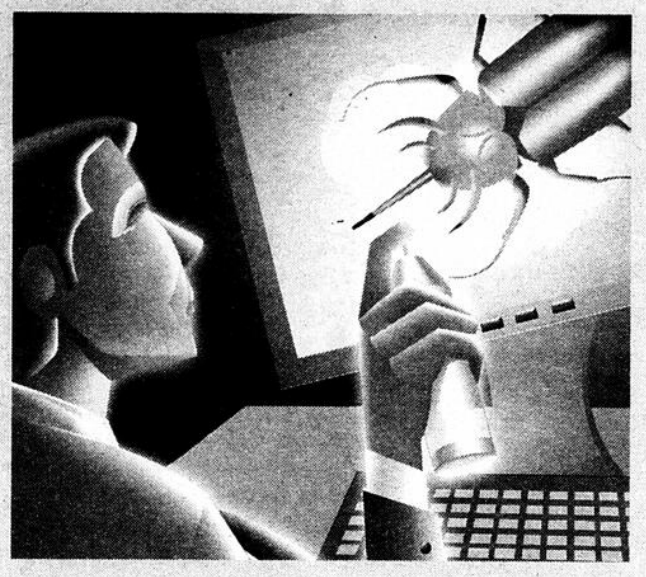
Au Québec, impossible de chiffrer quoi que ce soit. Ni les entreprises ni les organismes gouvernementaux ne divulguent la moindre statistique. Toutefois, des témoignages sont éloquents.

Ainsi, **Gérald Saint-Pierre,** directeur, pratique de sécurité, de **TELUS,** indique avoir été personnellement témoin des ravages d'attaques. Dans un des cas, il s'agissait d'une organisation de 4 000 employés victimes du virus *Blaster,* lequel a fait tomber en panne le réseau informatique pendant une journée et demie. M. Saint-Pierre estime les dégâts à quelque 250 000 $.

Un immense stress

Les dégâts dépassent souvent le seul montant chiffré des dollars perdus à cause d'un virus. Un seul mot de passe subtilisé lors d'une attaque par hameçonnage (*phishing*) peut suffire à jeter le discrédit sur l'ensemble des comptes de la victime : banque, cartes de crédit, courtage, etc. Même la sécurité de ses numéros de sécurité sociale, d'assurance maladie et de permis de conduire peuvent être ainsi mis en péril.

« Cela peut demander jusqu'à 600 heures de démarches à une victime pour rétablir son identité », estime M. Saint-Pierre. Sans parler des soucis et du stress qu'un tel événement peut susciter...



Les actes de piraterie peuvent également détruire des réputations. Ce fut le cas de deux Britanniques, **Julian Green** et **Karl Schofeld,** qui ont dû subir en 2003, chacun de leur côté, un procès pour pédophilie : la police avait trouvé des images pornographiques d'enfants dans leurs ordinateurs. Heureusement pour eux, leurs avocats ont pu démontrer qu'ils avaient été victimes de pirates qui s'étaient servis de leurs ordinateurs à leur insu.

Frédéric Meunier, conseiller principal, de **Watch4Net,** souligne que « que quelqu'un se fasse voler 1 000 $, c'est gênant, dit-il. Mais se faire accuser de pédophilie, c'est passablement plus destructeur... » ■ **Y.B.**

Il n'y a pas qu'une seule façon de se protéger.

Mais il n'y a qu'une source continue en matière de sécurité.

Visitez **microsoft.ca/securite/TI** pour connaître les nouveautés du Centre de conseils sur la sécurité de Microsoft. Vous y trouverez les éléments suivants :

Microsoft[MD] Windows[MD] XP Service Pack 2 Téléchargez et évaluez les dernières mises à jour, qui offrent un niveau de sécurité plus élevé, de même que les technologies de sécurité qui offrent une protection proactive contre les menaces informatiques.

Autoévaluation en ligne gratuite Remplissez gratuitement la fiche Internet d'autoévaluation pour évaluer les pratiques de sécurité de votre entreprise et identifier les zones à améliorer.

Alertes par courriel et mises à jour gratuites Soyez continuellement au courant des dernières avancées technologiques en matière de sécurité informatique. Abonnez-vous gratuitement au service Microsoft Security Communications.

Outils de sécurité gratuits Réagissez plus efficacement à d'éventuelles menaces informatiques. Profitez des outils tels que le logiciel Microsoft Baseline Security Analyzer et le service de mises à jour des logiciels Microsoft.

Visitez régulièrement le Centre de conseils sur la sécurité de Microsoft, qui est continuellement mis à jour, pour connaître les nouveautés en matière de sécurité. Sur un même site, vous trouverez des conseils techniques, des outils de sécurité et la formation dont vous avez besoin pour mieux sécuriser les réseaux de votre entreprise. Pour profiter d'une protection proactive et d'une source continue de conseils, visitez **microsoft.ca/securite/TI**.

Microsoft[MD]

Les entreprises de télécommunications entrent dans la danse

Elles feront dorénavant concurrence aux sociétés-conseil en informatique

Jean-François Barbe
dossiers@transcontinental.ca

Le 14 février est née **Bell Solutions de sécurité** (BSSI), une filiale de l'entreprise de télécommunications dédiée à la sécurité des réseaux informatiques. Sa mission : tirer profit de la popularité croissante de la téléphonie par Internet (téléphonie IP, pour *Internet Protocol*) pour proposer des systèmes de sécurité aux entreprises.

Ainsi, BSSI est en mesure de proposer des services-conseils, des solutions de gestion de sécurité ainsi que des logiciels et du matériel de sécurité provenant d'une quarantaine de fournisseurs. Selon **Doug Carwardine,** vice-président au développement des affaires, BSSI détiendrait d'ores et déjà 10 % du marché canadien de la sécurité des réseaux informatiques des entreprises, et elle entend doubler cette proportion en trois ans en s'adressant aux 1 000 plus grandes entreprises du pays.

BSSI emploie actuellement 275 personnes, dont 215 travaillent à son siège social, à Ottawa, et 35 à Montréal. Le bureau montréalais est le deuxième en importance de la filiale et dirige ses efforts vers l'industrie bancaire.

Certains employés de BSSI travaillaient déjà chez **Bell Canada.** Quant au reste du personnel, il provient de trois entreprises récemment acquises par Bell : **JetNet** et **Once Corporation,** toutes deux d'Ottawa, et **Emergis.**

Une vive concurrence

C'est que la téléphonie par Internet, qui permet de transporter sur un même réseau voix et données, suscite un vif intérêt depuis quelques mois.

Au début de l'année, **Vidéotron** a lancé son service de téléphonie IP sur la Rive-Sud de Montréal et à Laval, se plaçant ainsi en concurrence avec les pionniers au Canada tels que **Primus, Vonage, Sprint** et **babyTEL.** La filiale de **Quebecor** est le premier câblodistributeur à proposer ce service.

De son côté, Bell Canada propose la téléphonie IP à Sherbrooke, à Québec et à Trois-Rivières depuis la fin de mars, après trois mois d'essai en Estrie. **Shaw Communications** envisage de leur emboîter le pas, puis ce devrait être le tour de **Rogers Communications** et de **Cogeco Câble,** cet été.

La téléphonie connaît une progression « forte et rapide », selon **Marc Giroux,** vice-président, marketing des affaires, de **TELUS Québec.** « Quant à nous, nous visons toutes les entreprises, qu'elles soient petites ou grandes », ajoute-t-il.

Scepticisme et inquiétude

Selon **Yves White,** directeur, solutions technologiques, du **Groupe LGS,** une filiale à part entière d'**IBM,** la convergence de la réseautique et de l'IP rendait inévitable l'arrivée des entreprises de télécommunications. « Elles pénètrent dans notre champ de compétence, mais comparativement à nous elles ont moins d'expertise en matière de réseautique », dit-il. Maintenant que les principaux acteurs de la télécommunication entrent de plain-pied dans la téléphonie IP, la sécurité est devenue un enjeu central. Et l'inquiétude est palpable chez deux autres acteurs de la sécurité sur IP. Ceux-ci, qui préfèrent conserver l'anonymat, estiment qu'il y a déjà une forte pression à la baisse des prix.

« Nous voyons passer des soumissions où les marges bénéficiaires sont dérisoires, dit l'un d'eux. Et cela ne concerne pas seulement des soumissions auprès de grandes entreprises. » ■

La sécurité sur IP en bref

Les risques

> L'écoute possible des appels téléphoniques à l'insu de l'entreprise.

> L'utilisation du réseau pour faire des appels interurbains aux frais de l'entreprise.

Peu d'attaques répertoriées

> Au Canada, on rapporte très peu d'attaques informatiques sur les réseaux IP, ce qui ne veut pas dire qu'il n'y en a pas. Les organisations visées n'ont pas nécessairement intérêt à en faire état.

> De plus, plusieurs utilisateurs limiteraient le champ d'action des réseaux IP aux communications internes, ce qui limite la possibilité d'intrusion externe.

Qu'est-ce que la téléphonie IP ?

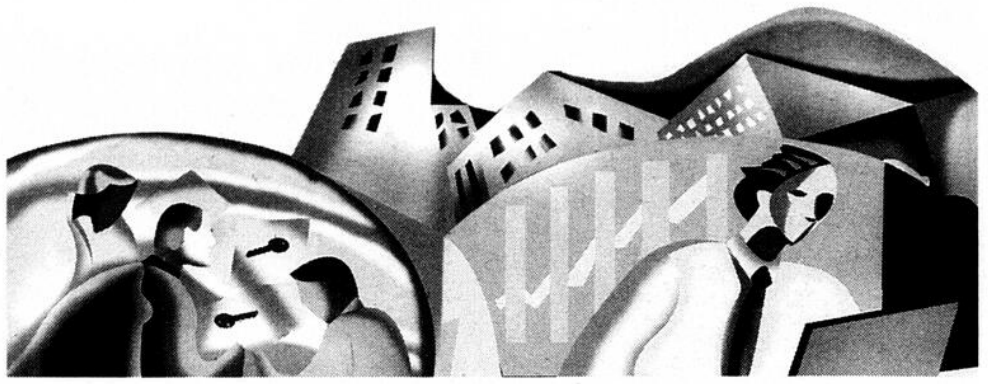
La téléphonie Internet (IP) permet d'acheminer la voix sur le même réseau qui transporte les données.

La technologie utilise le langage de programmation à l'origine d'Internet pour acheminer voix et données. Des logiciels convertissent la voix en paquets de données qui, une fois compressés, sont envoyés par Internet et réassemblés en audio à leur sortie. Chaque paquet est acheminé au destinataire par les meilleurs chemins disponibles sur le réseau, afin que la communication soit fluide. ■ **O.S.**

Bien avant qu'il
ne puisse s'infiltrer…

Des responsabilités élargies

Le rôle des professionnels de la sécurité devient plus stratégique



Danielle Turgeon
danielle.turgeon@transcontinental.ca

Les professionnels de la sécurité informatique se détachent peu à peu du service des technologies de l'information (TI). Leurs responsabilités dans l'entreprise s'élargissent et ils travaillent davantage avec le personnel des ressources humaines, les avocats du service du contentieux et les spécialistes de la documentation.

Auparavant, leur rôle était de rédiger des politiques de sécurité, d'assurer la formation, d'entretenir les réseaux et de planifier l'installation de nouveaux systèmes informatiques. Aujourd'hui, ils encadrent, normalisent (des enquêtes pré-emploi par exemple) et doivent connnaître tout ce qui se passe dans l'entreprise. La gestion de la sécurité physique leur revient souvent de droit. Et la montée de la Gestion de contenu d'entreprise (GES) – qui consiste à gérer les données « informelles » – les obligera à sécuriser toutes les données de l'entreprise.

« Il n'est pas possible de dire : "Nous protégeons l'information numérique et ignorons le reste", note **Louise Thiboutot**, coordonnatrice gouvernementale, sécurité de l'information numérique et des échanges électroniques au **Conseil du trésor.** Tout est maintenant lié. »

D'ailleurs, chez **Loto-Québec,** la sécurité ne fait plus partie des TI depuis sept ans. « Les professionnels de la sécurité doivent passer d'un rôle opérationnel à un rôle stratégique. Nous faisons davantage de la gestion de risque », dit **Harold Côté,** directeur *corporatif* de la sécurité des TI chez Loto-Québec.

La perception change

Gaétan Houle, officier en chef de la sécurité chez **Bombardier Aéronautique,** estime que la perception des chefs d'entreprise à leur égard change lentement et qu'il reste beaucoup de sensibilisation à faire.

Les dirigeants et les employés doivent être conscients des enjeux de la sécurité et des manières de réagir.

« Le personnel de sécurité n'est pas des policiers, mais des conseillers. Il ne suffit pas de dire aux dirigeants que nous courons des risques, cela ne les convainc pas. Il faut leur montrer ce qui se fait ailleurs. Chez Bombardier, nous l'avons fait par des études comparatives avec d'autres entreprises manufacturières en Amérique du Nord. »

Les propos de ces trois conférenciers ont été entendus à une table ronde sur le rôle des responsables des systèmes et de la sécurité de l'information (RSSI) réunie dans le cadre de la 13e édition du **Colloque québécois de la sécurité de l'information** tenu les 25 et 26 avril à Saint-Hyacinthe.

Sensibiliser les utilisateurs

Benoît Dicaire, vice-président de **TechSolCom** et président de l'**Association de la sécurité de l'information du Montréal** métropolitain (ASIMM), l'une des deux associations organisatrices du colloque, rappelle que l'importance de la sécurité informatique se résume à trois éléments : la sensibilisation, la sensibilisation et la sensibilisation !

Tant que les dirigeants et les employés ne sont pas conscients des enjeux de sécurité et des manières de réagir, les meilleures solutions ne seront pas suffisantes.

« La sécurité en tant que telle n'existe pas. Ce qui existe, c'est l'absence de sécurité. Ce qu'on fait en réalité, c'est une gestion du risque », dit-il.

La base de la sécurité

Les systèmes d'information jugés critiques doivent être sécurisés à trois égards : la confidentialité, l'intégrité et la disponibilité des données. Un mot de passe facile à trouver peut nuire à la confidentialité, des renseignements altérés par un problème électrique fragilisent l'intégrité du système et le fait de ne pouvoir accéder aux documents d'un site Web compromet la disponibilité.

Une organisation doit évaluer l'importance de ses renseignements statégiques et avoir un inventaire des données critiques (dossiers des clients, des fournisseurs, liste des prix, etc.). Le résultat de cette évaluation déterminera la gestion du risque la plus adaptée.

« Les décisions d'affaires seront basées sur le risque et sur la valeur des actifs. Des renseignements qui valent 10 M$ nécessitent-ils un système de protection de 15 M$? demande M. Dicaire. Il est possible d'avoir un risque « zéro », mais ce n'est pas toujours souhaitable du point de vue des affaires, parce que le coût en est trop élevé. Il faut bien étudier la question. » ■

Article rédigé avec la collaboration de Gaël Le Corre-Laliberté.

Désuet, le mot de passe

Les mesures de sécurité excessives ont parfois un effet inverse à celui visé.

Par exemple, quand elles imposent de changer les mots de passe tous les 45 jours : nombre d'employés les notent sur des bouts de papier dispersés sur leur bureau, de peur de les oublier. Sans parler des mots de passe trop simples (mots familiers, suite de chiffres), qu'un pirate bien équipé peut trouver en quelques secondes.

De telles mesures peuvent aussi coûter plus cher que prévu.

« La moitié des appels de demande d'aide informatique concernent les mots de passe oubliés. Pour l'entreprise, cela représente des coûts variant entre 15 et 40 $ par appel, qui correspondent au temps nécessaire pour changer le mot de passe », dit **Pierre Root,** président et chef de la direction de **Labcal.**

Par empreintes digitales

Que faire pour éviter cela ? Labcal, établie à Québec, propose une solution simple : la reconnaissance par empreintes digitales. L'avantage est de faire disparaître la nécessité du mot de passe.

L'entreprise a même prévu les cas de falsification d'empreintes digitales, comme dans des films de science-fiction. « Le contact doit se faire avec un tissu humain vivant, donc impossible de présenter une copie d'empreinte ou autre chose », précise-t-il. ■ **G.L.-L.**

Entreprises publiques, une nouvelle loi vous attend

Yan Barcelo
dossiers@transcontinental.ca

D'ici quelques années, la nouvelle loi C-198 obligera les entreprises cotées en Bourse à renforcer la sécurité de leurs données.

En fait, cette loi n'imposera aucune nouvelle mesure de sécurité, mais exigera que la sécurité des procédures – actuelles ou futures – soit renforcée.

La loi C-198 entrera en vigueur en juin 2006 et visera les entreprises ayant une capitalisation boursière supérieure à 500 M$. L'année suivante, elle concernera celles ayant une capitalisation supérieure à 250 M$. Et finalement, en juin 2009, celles ayant une capitalisation supérieure à 75 M$.

Garantir l'intégrité des données

Cette loi, qui reprend essentiellement la section 404 de la loi *Sarbanes-Oxley,* s'intéresse aux règles internes du contrôle financier des entreprises. Elle impose le fait de garantir l'intégrité et la validité de toutes les données qui ont un impact financier, depuis l'inscription dans les systèmes informatiques jusqu'à sa parution finale dans les états financiers.

René Vergé, directeur, service-conseil, de **CGI,** en résume les principales conséquences : « Il faudra alors établir avec exactitude qui approuve quoi. Il faudra aussi savoir qui a eu accès aux données, à quel moment, quel est le niveau d'autorisation de ces personnes et de qui relève l'autorisation. Aujourd'hui, il y a bien des entreprises où ces contrôles ne sont pas en place. »

L'un des points cruciaux soulevés par la nouvelle loi touche la gestion des identités. « C'est justement l'une des failles les plus importantes dans les entreprises, dit **David Cott,** consultant principal en sécurité, de **M3K Solutions.** La difficulté est liée au roulement du personnel, qui est parfois élevé et qui modifie constamment les registres d'autorisation. »

Pour pallier cette difficulté, les entreprises sont appelées à cheminer graduellement vers la procédure d'autorisation unique (*single sign-on*). Il s'agit d'établir un registre central dans lequel le profil complet de chaque employé est tenu à jour avec l'ensemble de ses autorisations d'accès.

Dès que ce profil évolue (l'employé change de responsabilités ou quitte l'entreprise), son statut peut être rapidement mis à jour. Ainsi, il devient plus difficile pour un fraudeur de subtiliser, même temporairement, l'identité d'un employé.

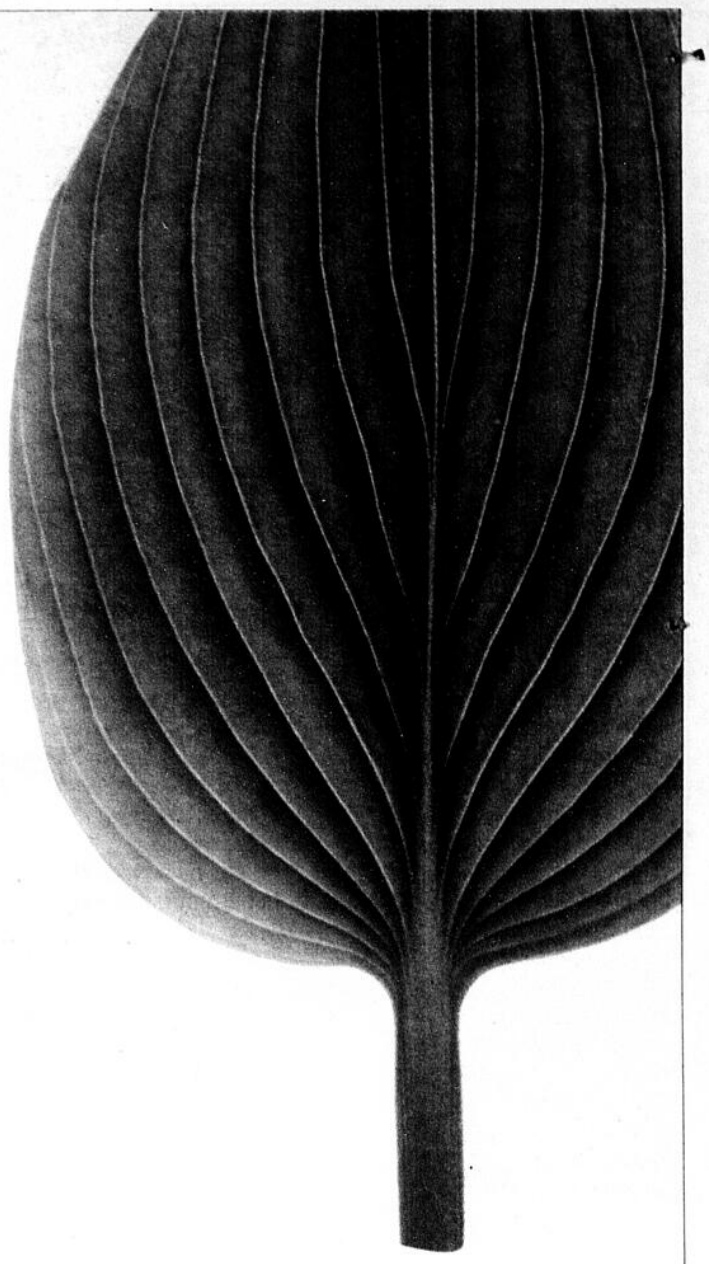
Revoir ses documents d'entreprise

Autre point crucial : la documentation. Les procédures détaillées de contrôle seront parmi les premiers documents que les vérificateurs comptables exigeront d'une entreprise.

« Les employés connaissent les procédures, mais trop souvent, elles ne sont pas écrites dans les documents officiels, explique M. Vergé. Cela devra changer.

« De plus, les entreprises devront plonger dans la réingénierie des tâches et dans la gestion du changement. Aucun de ces éléments n'est nouveau, mais la nouvelle loi va faire en sorte qu'on ne pourra plus les négliger. » ■

David Cott, consultant principal en sécurité, de M3K Solutions.



La nouvelle solution en sécurité de TELUS aura vite fait de le bloquer !

TELUS innove une fois de plus en présentant ANGEL[MC], le premier dispositif de blocage et de vérification proactif *(block & scan)* au monde, capable de vérifier la conformité des postes informatiques, internes ou externes, avant qu'ils n'accèdent au réseau de votre entreprise pour risquer de le contaminer.

Ce n'est ni un pare-feu, ni un logiciel qui se greffe à un poste de travail. Il s'agit d'une solution d'infrastructure qui vient bonifier la fiabilité et l'étanchéité de votre réseau déjà en place. En fait, elle constitue le plus haut niveau de protection contre les attaques de vers et de virus informatiques que vous puissiez trouver sur le marché.

Grâce à sa fonction de vérification pré-réseautage exclusive, tous les postes sont mis « en quarantaine » avant de pouvoir accéder à votre réseau. Ils sont vérifiés en un clin d'œil pour s'assurer de leur conformité aux politiques de gouvernance établies par votre entreprise.

Laissez ANGEL[MC] vous procurer cette paix d'esprit que vous recherchez, en empêchant les indésirables de s'infiltrer dans votre réseau pour nuire à votre productivité et à votre profitabilité.

Pour en savoir plus sur l'Unité réseau de conformité ANGEL[MC] de TELUS, communiquez avec l'un de nos conseillers au 1 877 520-1212 ou visitez le | www.telusquebec.com/angel |

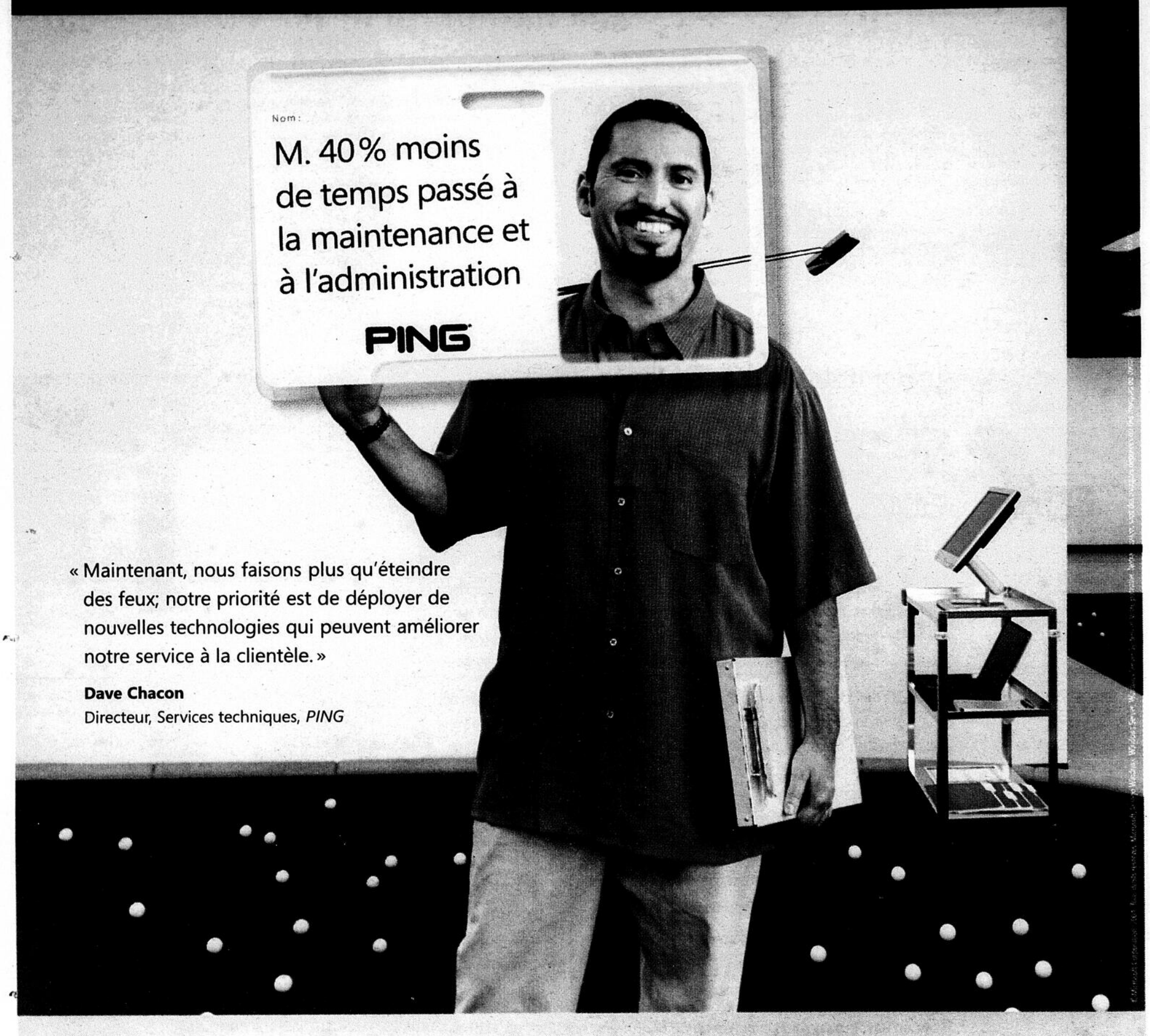
ANGEL[MC] lauréat du prix Partenaire d'innovation mondial au Sommet des Partenaires de CISCO System, avril 2005

TELUS[MD]

le futur est simple[MD]

Microsoft

Votre potentiel. Notre passion.



« Maintenant, nous faisons plus qu'éteindre des feux; notre priorité est de déployer de nouvelles technologies qui peuvent améliorer notre service à la clientèle. »

Dave Chacon
Directeur, Services techniques, *PING*

Faites-vous un nom avec Windows Server System[MC].

Le logiciel serveur intégré Windows Server System de Microsoft[MD] aide le fabricant de bâtons de golf PING, en facilitant la gestion d'une infrastructure qui dessert 400 utilisateurs. Et voici comment : à l'aide du système d'exploitation Windows Server[MC] OS 2003 et du service Active Directory[MD], PING gère ses serveurs, ses ordinateurs et ses utilisateurs à partir d'un seul poste. Les 800 heures par année épargnées sur le temps d'administration peuvent ainsi être consacrées au développement de nouvelles méthodes de soutien aux clients, partenaires et employés. Voilà un logiciel qui vous aide à en faire plus avec moins. Lisez l'histoire complète de PING en visitant le site **microsoft.ca/wssystem/fr**

Microsoft®
Windows
Server System™

La téléphonie IP n'est pas sans danger pour les entreprises

Gaël Le Corre-Laliberté
gael.lecorre@transcontinental.ca

Avec l'arrivée de la téléphonie par Internet (ou téléphonie IP, pour *Internet Protocol*), l'univers de la téléphonie entre en collision avec celui des réseaux de données.

« Nous assistons à la confrontation de deux environnements différents, dit **Michael Albertson**, président de **SecurIP services-conseils**. Maintenant, les téléphones cellulaires numérisent les messages comme des données informatiques. Se pose donc un problème de sécurité. »

Ainsi, les entreprises intéressées par la téléphonie IP devraient avant toute chose se poser deux questions, selon M. Albertson :

> A-t-on intérêt à partager le réseau de données avec celui de la voix pour économiser ?

> Si oui, la sécurité du réseau de données est-elle adéquate pour garantir celle de la téléphonie IP ?

De nombreux risques

Perdre ne serait-ce que quelques heures l'usage du téléphone peut être dramatique pour une entreprise. Or, en combinant les deux réseaux, à savoir celui des données et celui de la voix, il peut se produire une contamination de l'un par l'autre. Par exemple, des virus présents dans le réseau de données, mais inactifs ou contenus par des anti-virus, pourraient alors se répandre dans celui de la voix au moment de l'association des deux réseaux.

« Les premières attaques envisageables de la part de pirates pourraient viser à mettre hors service le réseau téléphonique, dit M. Albertson. Ils pourraient aussi tenter de saturer les boîtes vocales. Ou encore, s'en prendre directement au serveur du réseau de téléphonie IP. » De telles attaques pourraient prendre des heures à être repoussées.

Erreurs de jeunesse

Les entreprises ne se préoccupent pas assez de sécurité, selon M. Albertson.

« Elles me font penser à l'époque où nous étions jeunes et où nous nous achetions notre première voiture, dit-il. Le dernier de nos soucis était de nous procurer une bonne assurance. »

Le président de SecurIP considère que les entreprises devraient veiller à informer leur personnel de l'importance vitale de respecter des règles de base en matière de sécurité. Elles devraient aussi veiller à former les employés de manière continue en ce domaine, voire à mettre sur pied un programme de récompense pour ceux qui utilisent au mieux les réseaux informatiques. M. Albertson souligne le rôle que les manufacturiers doivent jouer. Ils doivent informer leur clientèle des mesures de sécurité à adopter en fonction du matérial acheté, et fournir régulièrement des conseils, les attaques de pirates se faisant de plus en plus sophistiquées. ■

KIT DE SURVIE

> L'entreprise doit s'équiper de logiciels de sécurité (firewalls, etc.) et les mettre régulièrement à jour.

> L'équipe informatique de l'entreprise doit assurer une veille constante du système de sécurité et effectuer souvent des tests d'intrusion.

> On recommande de se doter d'un système de détection d'intrusion et d'anomalies.

> Une charte de sécurité, présentée sous la forme d'un document papier de deux ou trois feuilles, est toujours utile pour bien informer le personnel des mesures à suivre pour garantir l'intégrité du réseau. Par exemple, ce document devra indiquer si un employé est autorisé ou non à accéder au réseau de l'entreprise depuis son domicile afin d'effectuer des appels interurbains par téléphonie IP. ■ G.L.-L.

Différents types de virus

La rapidité à laquelle les virus évoluent ne permet bien évidemment pas d'en dresser une liste exhaustive. Toutefois, les types suivants sont les plus courants :

> Virus classique

Programme pirate capable de se propager et de se reproduire dans un ou plusieurs systèmes informatiques, avec l'intention d'y causer des dégâts.

> Ver *(worm)*

Virus se transmettant de lui-même aux différents « contacts » enregistrés dans l'ordinateur, généralement par l'entremise des listes de la messagerie.

> Virus polymorphe

Virus capable de modifier ses caractéristiques principales pour échapper à la vigilance des antivirus.

> Rétrovirus

Virus dont la priorité est d'annihiler les systèmes de protection (antivirus, pare-feu, etc.). L'ordinateur devient ainsi particulièrement vulnérable, notamment à l'installation par le pirate d'une porte arrière secrète lui permettant de s'infiltrer à volonté. ■ **O.S.**

Les techniques de vol d'identité sont de plus en plus raffinées

Celle du hameçonnage, l'une des plus efficaces, est en vogue depuis quelques mois

Yan Barcelo
dossiers@transcontinental.ca

Une personne moins avertie que **Robert Massé** serait probablement tombée dans le piège de l'« hameçon » (*phishing*) qui l'attendait dans sa boîte de courriel, le matin du 20 avril.

Le courriel venait de **PayPal,** un réseau américain de paiement électronique auquel M. Massé est abonné. Dans ce courriel, PayPal l'informait que son compte présentait un « niveau inhabituel d'activité » et disait vouloir s'assurer que l'intégrité de son compte n'avait pas été compromise. Jusqu'à ce que M. Massé confirme les données relatives à son compte, PayPal ne lui donnerait qu'un accès limité.

Après avoir cliqué sur l'hyperlien qui le dirigeait directement au site de PayPal, M. Massé s'est retrouvé face à un écran d'accès requérant son nom d'utilisateur et son mot de passe. Après qu'il eut fourni les données demandées, le site lui indiqua que l'information était invalide et lui demanda de retaper le tout. Apparaissait ensuite une page où il devait inscrire plusieurs détails confidentiels : numéros de carte de crédit, comptes de banque, numéro d'identification personnel, etc.

Ce que les arnaqueurs ignoraient, c'est que M. Massé est président de **GoSecure,** une entreprise montréalaise spécialisée dans la sécurité informatique, et qu'il avait reconnu dès le départ un cas particulièrement bien réussi de *phishing*. Il s'est rendu jusqu'à l'étape ultime pour voir comment les fraudeurs avaient monté leur opération, puis s'est contenté de refermer la page.

La personne moins avisée qui aurait répondu aux questions aurait fini par découvrir, quelques jours plus tard, que son compte en banque, par exemple, avait été vidé...

Une croissance fulgurante

L'hameçonnage est un piège Internet qui connaît une croissance fulgurante.

En septembre 2003, les filtres anti-fraude de **MessageLabs** ont intercepté 279 courriels hameçons différents. En juin 2004, il y en a eu 265 000, et en novembre de la même année, 3 millions. Sachant qu'environ 5 % des personnes mordent à l'hameçon, selon les évaluations du **Anti-Phishing Work Group,** on comprend aisément que les arnaqueurs prisent cette nouvelle forme de piège.

Le but du *phishing* est toujours le même : inciter la personne visée, le *poisson,* à livrer des renseignements confidentiels, presque toujours de nature financière. La façon la plus fréquente de procéder est l'envoi d'un courriel, libellé au nom d'une institution financière crédible. Le message évoque un risque potentiel de vol d'identité. Pour vérifier tout cela et rétablir au plus vite la situation si le supposé vol d'identité est confirmé, le courriel incite l'internaute à confirmer certains renseignements à son sujet. En réalité, il s'agit d'un site factice piloté par l'arnaqueur.

Des trucs afin d'éviter d'être arnaqué

À première vue, il peut paraître compliqué de flairer l'arnaque. Tout semble crédible : la page d'accueil du site de vérification d'identité, le ton du message, le fait d'entrer son mot de passe à deux reprises, etc.

« En fait, si on tape deux fois n'importe quoi, comme *aszkacxpouah,* le site des arnaqueurs nous laisse entrer de toute façon, indique M. Massé. Ce truc peut permettre de découvrir à qui on a affaire. »

Parfois, de menus détails peuvent alerter l'internaute d'un piège. Dans le cas de M. Massé, le message commençait par la formule « Cher client PayPal », alors qu'une entreprise sérieuse saluerait son client par son nom.

Mais surtout, aucune institution financière crédible ne demanderait par courriel à un client de fournir de l'information confidentielle. Et c'est là le point le plus important, celui qui devrait mettre la puce à l'oreille de la personne visées par l'arnaque. En fait, toutes les institutions financières rappellent régulièrement qu'elles ne communiquent jamais par courriel avec leurs clients ni ne leur demandent de renseignements personnels par ce moyen. Elles optent plutôt pour le téléphone et le courrier.

De plus en plus rusé

De nouvelles formes de vol d'identité sont récemment apparues. Par exemple, un courriel invite un internaute à récupérer une carte postale virtuelle sur un site dont l'hyperlien lui est fourni. En cliquant sur la carte, la victime télécharge à son insu un logiciel espion capable d'enregistrer les touches tapées sur le clavier dans les jours suivants. Il arrive un moment ou un autre que des mots de passe soient tapés sur le clavier et volés par des pirates.

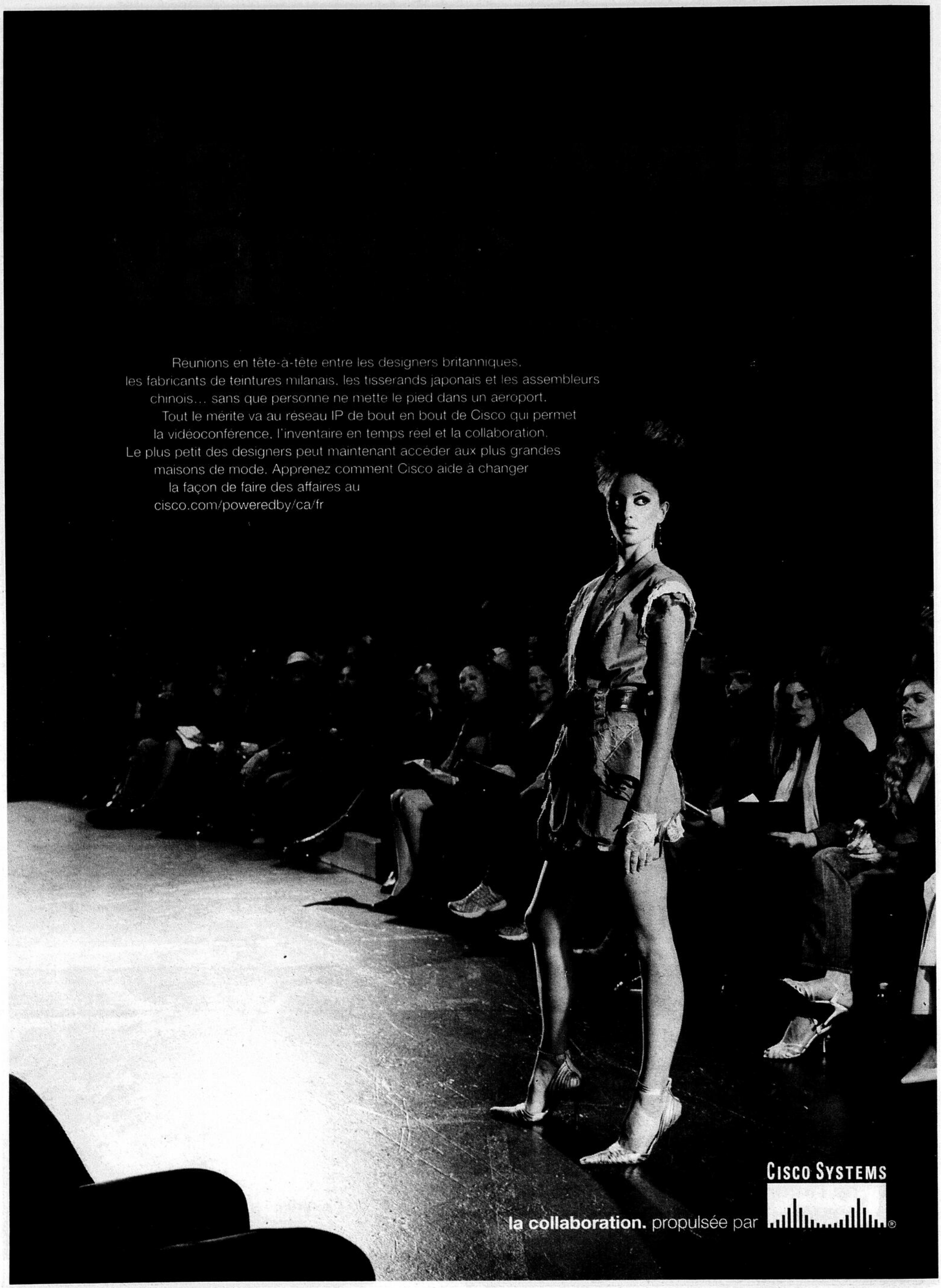
Dernier raffinement, qui intéressera toute victime potentielle : comment les fraudeurs s'y prennent-ils concrètement pour vider un compte sans se faire prendre? Rien de plus simple : en faisant faire le travail par d'autres, parfois à leur insu !

L'hameçonnage est un piège Internet qui connaît une croissance fulgurante.

Par exemple, un fraudeur envoie des pourriels faisant croire qu'une institution financière crédible est en train de recruter des chargés de compte régionaux. Le travail proposé consiste simplement à effectuer des transferts de comptes bancaires. Ainsi, le chargé de compte régional doit ouvrir des comptes dans différentes banques (celles des victimes), dans lesquels arrive de l'argent (celui des victimes). Il doit alors effectuer le transfert de ces montants sur un autre compte bancaire, souvent à l'étranger comme aux Bahamas ou aux îles Caïmans. À chaque transfert, il recevra une commission de 6 à 8 % du montant transféré... ■

NEUF PRÉCAUTIONS POUR SE PROTÉGER

1. **Ne jamais répondre à des courriels réclamant vos mots de passe et autres renseignements personnels confidentiels.**
2. **Ne jamais cliquer sur des hyperliens destinés à vous conduire sur une page où vous seront demandés de tels renseignements.**
3. **En cas de doute, passez un coup de fil à la personne qui vous a envoyé le courriel.**
4. **Quand vous vous rendez sur le site Internet d'une institution bancaire, utilisez systématiquement vos favoris ou bien saisissez vous-même l'adresse dans le navigateur. N'utilisez jamais un raccourci proposé par une tierce personne.**
5. **Évitez d'enregistrer sur votre ordinateur la moindre information se rapportant à votre carte bancaire.**
6. **Équipez-vous d'un logiciel antivirus et d'un pare-feu afin de bloquer toute intrusion sur votre PC.**
7. **Si on vous propose de télécharger un logiciel inconnu, refusez.**
8. **Tenez à jour votre antivirus, votre navigateur et Windows.**
9. **Surveillez toujours vos relevés de banque, et prévenez votre institution à la moindre anomalie. ■ O.S.**


Reunions en tête-à-tête entre les designers britanniques,
les fabricants de teintures milanais, les tisserands japonais et les assembleurs
chinois... sans que personne ne mette le pied dans un aeroport.
Tout le mérite va au réseau IP de bout en bout de Cisco qui permet
la vidéoconférence, l'inventaire en temps réel et la collaboration.
Le plus petit des designers peut maintenant accéder aux plus grandes
maisons de mode. Apprenez comment Cisco aide à changer
la façon de faire des affaires au
cisco.com/poweredby/ca/fr
la collaboration. propulsée par
CISCO SYSTEMS

Les PME disposent de plusieurs moyens pour se protéger

L'une des solutions les plus populaires auprès des PME est de se doter de boîtiers multifonctions de filtrage

Yan Barcelo
dossiers@transcontinental.ca

Les dangers liés à Internet menacent aujourd'hui autant les PME que les grandes entreprises.

Ces dernières, possédant les ressources nécessaires pour le faire, n'hésitent pas à mettre en place toutes les mesures de sécurité requises pour se protéger. On ne peut malheureusement pas en dire autant des PME. Pourtant, les solutions de pointe leur sont aussi accessibles qu'aux grandes entreprises.

Le danger peut se présenter sous trois formes : virus, logiciel espion et pourriel.

Le danger est omniprésent, à la fois localement et mondialement. Une PME doit se prémunir aussi bien contre des employés malfaisants que contre des fraudeurs installés à l'autre bout du monde. « Il est certain que des entreprises étrangères tenteront de pénétrer les réseaux informatiques d'une entreprise de la Beauce qui fait de la R-D dans un secteur de pointe », affirme **Benoît Jourdain,** président d'**Horus information et technologie,** de Québec, et de l'**Association de sécurité de l'information de la région de Québec** (ASIRQ).

Le danger peut se présenter sous trois formes : virus, logiciel espion et pourriel. Les pièges peuvent alors être multiples : chevaux de Troie, enregistreurs de touches, capteurs d'écran, etc. Les canaux d'accès ne se limitent pas au Web : il faut aussi tenir compte entre autres des messageries instantanées, des ordinateurs de poche et des accès Wi-Fi.

Benoît Jourdain, d'Horus : « Il est certain que des entreprises tenteront de pénétrer les réseaux informatiques d'une PME de la Beauce qui fait de la R-D dans un secteur de pointe. »

Plusieurs solutions sont envisageables

L'une des solutions les plus populaires auprès des PME est de se doter de boîtiers multifonctions de filtrage, comme ceux fournis par **Websense** et **SurfControl.** Ceux-ci se placent dans un serveur que l'on installe à l'entrée de la connection Internet de l'entreprise, juste derrière le coupe-feu. Alors que les logiciels de protection courants ne visent qu'une catégorie de menaces (virus, etc.), ces boîtiers luttent contre toutes sortes d'attaques.

Ils sont en mesure d'arrêter les attaques classiques et d'empêcher les logiciels espions d'acheminer à l'extérieur l'information subtilisée, de limiter l'accès à certains sites Web et de contrôler les messageries instantanées. Pour un produit comme *Websense Enterprise,* les licences d'utilisation coûtent annuellement de 15 à 40 $ par utilisateur, selon M. Jourdain.

Mais attention, prévient **Frédéric Meunier,** conseiller principal, chez **Watch4Net,** « il n'y a pas de produit miracle. Chaque solution est imparfaite. »

M. Jourdain explique qu'« il vaut mieux aller chercher le meilleur de chaque catégorie. » Selon lui, on peut très bien s'équiper d'un boîtier de filtrage Web, mais il est sage de multiplier les couches de protection en y ajoutant les meilleurs logiciels pour chaque catégorie de pièges.

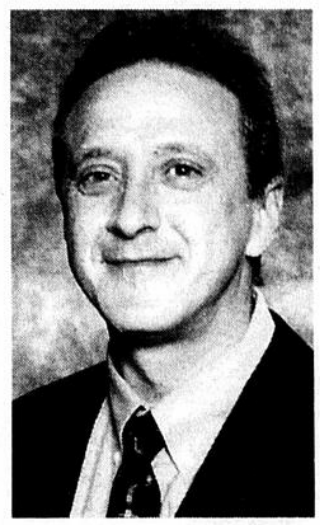
Par exemple, il est préférable d'installer un antivirus non seulement dans son réseau informatique, mais aussi sur chaque poste individuel. **Symantec** et **McAfee** sont spécialisées dans ce type de logiciel. Pour stopper les logiciels espions, le magazine *PC World* recommande *Counterspy,* de **Sunbelt Software,** et *SpySweeper,* de **Webroot Software.** Cette publication conseille aussi de surveiller la sortie prochaine de *Windows Antispyware,* de **Microsoft.** Quant aux pourriels, *PC World* considère *SpamNet,* de **Cloudmark,** comme nettement supérieur aux vedettes du secteur que sont *Symantec Norton AntiSpam 2004* et *Network Associates McAfee SpamKiller 5.0.* Tous ces logiciels coûtent de 40 à 80 $ l'unité.

Services externes

Une autre possibilité est de recourir à des gestionnaires de sécurité à distance. Il y a dans ce domaine des généralistes, comme **ESI Technologies de l'information** ou **Bell Solutions de sécurité,** et des fournisseurs spécialisés, comme **ZEROSPAM.** Les généralistes supervisent à distance toute l'activité qui a cours sur le réseau de l'entreprise (serveurs, postes de travail, commutateurs, coupe-feu, etc.). Chez ESI, par exemple, les coûts varient de 75 à 125 $ mensuellement par champ surveillé.

Une fournisseur spécialisé comme ZEROSPAM ne surveille que le trafic de courriels de l'entreprise pour en extirper les pourriels et les « hameçons » (*phishing*). Bell propose aussi ce service. Chez ZEROSPAM, le coût mensuel est de 50 $ pour un maximum de 20 boîtes de courriel. Au-delà de 20 boîtes, les coûts sont de 3 $ mensuellement par boîte additionnelle, le prix diminuant selon le nombre de boîtes, pour atteindre environ 1 $ par boîte au-delà d'un total de 500.

Avant d'adopter telle ou telle mesure de sécurité, la PME doit évaluer les risques courus, selon **Fred Bedrich,** vice-président, services-conseils, de Bell Solutions de sécurité.



Fred Bedrich, de Bell Solutions de sécurité, conseille aux PME d'évaluer précisément leurs besoins avant de s'équiper de quoi que ce soit.

Ainsi, si une paralysie du réseau informatique de l'entreprise durant une journée ne correspond qu'à une perte de quelques milliers de dollars, peut-être n'est-il pas nécessaire de s'équiper de logiciels antivirus destinés aux seuls employés utilisant le Web. En revanche, la PME pour laquelle une telle mésaventure serait une catastrophe aurait tout intérêt à faire appel à un service de surveillance externe. ■

LES CLÉS D'UN AUDIT DE SÉCURITÉ RÉUSSI

Le meilleur moyen de vérifier la sécurité de son réseau est de le faire inspecter par une personne extérieure à l'entreprise ou, mieux, par une entreprise spécialisée. En effet, il importe de procéder avec méthode et objectivité, afin de déceler la moindre faille du système de sécurité.

Un tel audit de sécurité abordera deux points :

> une étude interne visant à trouver des failles classiques;

> une tentative d'intrusion externe, plus ou moins élaborée.

Le rapport de l'audit présenté à la direction de l'entreprise contiendra trois passages obligés :

> la liste des failles décelées et les risques potentiels qu'elles représentent;

> une série de suggestions, et leurs coûts, pour remédier aux défauts du système de sécurité;

> des indications techniques pour bien mettre en place les nouvelles mesures de sécurité préconisées.

L'avantage d'un tel rapport est double :

> il explique à la direction de l'entreprise, de manière claire et objective, les enjeux des remèdes à apporter au système de sécurité défaillant;

> il permet à l'équipe informatique de l'entreprise de mieux comprendre son réseau et la manière d'améliorer la sécurité de celui-ci. ■ O.S.

La lutte est acharnée contre les virus et pourriels

Gaël Le Corre-Laliberté
gael.lecorre@transcontinental.ca

Les pourriels et les virus qui se transmettent par la messagerie électronique deviennent des fléaux pour les entreprises. En réponse, de nombreuses sociétés offrent déjà des solutions permettant de préserver les réseaux informatiques.

« L'industrie prône actuellement d'installer la technologie d'un certain manufacturier et d'en implanter une seconde technologie provenant d'une autre source. Il est périlleux de ne se fier qu'à une seule solution », dit **Alain Turcot,** de **Sybari.**

Sybari propose, quant à elle, une solution combinant de quatre à huit technologies différentes. « Pour vous donner une image de l'évolution technologique de notre solution, c'est comme si vous passiez d'un système de porte avec clé à celui de la reconnaissance de la voix et des empreintes digitales », poursuit-il.

Une menace venue de l'Orient

Selon M. Turcot, un grand nombre de virus proviennent de l'Asie et de l'Europe de l'Est. Il souligne en effet que la propagation des virus a tendance à suivre les réseaux horaires, infectant d'abord l'Asie, puis l'Europe et l'Amérique.

Ainsi, les entreprises d'ici ont l'avantage de bénéficier d'un répit de quelques heures pour trouver une parade aux nouveaux virus. Reste à profiter pleinement de cet avantage.

Cependant, les pirates ont d'ores et déjà entrepris de réduire cet avantage à néant. Ils seraient à mettre au point le *Zero-Day-Exploit.* Il s'agit d'un virus qui apparaîtrait simultanément en plusieurs endroits de la planète et se propagerait à toute allure. ■

Le Canada, source de pourriels

Le Canada est l'une des sources de pourriels les plus importantes du monde, selon une étude de l'entreprise de sécurité informatique **Sophos.** En 2004, près de 6 % des courriels indésirables détectés par ses services provenaient du Canada, ce qui en fait le 4e pays le plus « polluposteur » du monde.

De fait, Sophos compile différentes données sur les pays d'où sont expédiés les pourriels, ce qui lui permet de dresser un palmarès. Ce dernier met les États-Unis largement en tête, à 42 %. Suivent respectivement la Corée du Sud (13 %), la Chine (8 %), le Canada (6 %), le Brésil (3 %) et le Japon (3 %).

Sophos souligne par ailleurs que 40 % des pourriels sont expédiés à partir de réseaux d'ordinateurs préalablement infectés par un ver informatique ou un cheval de Troie. ■ **O.S.**

Au tour des cellulaires d'être la cible d'attaques

Olivier Schmouker
olivier.schmouker@transcontinental.ca

***Fontal* est un cheval de Troie, dont le procédé est fort simple. Dès que l'utilisateur ouvre le fichier infecté, Fontal installe des données corrompues qui provoquent une panne au démarrage.**

Les alertes aux actes de piratage sur téléphone cellulaire se multiplient depuis quelques semaines, un peu partout dans le monde. L'un des derniers actes en date a été dénommé *Fontal.*

Il s'agit d'un cheval de Troie, dont le procédé est fort simple. Un fichier infecté est envoyé à un cellulaire doté de *Symbian série 60,* l'un des systèmes d'exploitation les plus populaires auprès des fabricants de cellulaires tels que **Nokia, Samsung, Siemens, Panasonic** et **Lenovo.** Dès que l'utilisateur ouvre le fichier infecté, Fontal installe des données corrompues qui provoquent une panne au démarrage. Si l'on réinitialise le téléphone en l'éteignant puis en l'allumant de nouveau, la situation empire, car le téléphone se retrouve vérouillé.

« À l'heure actuelle, la seule manière connue de désinfecter un cellulaire ainsi touché est de le reformater, au risque de perdre toutes les données stockées », explique un communiqué de **F-Secure,** une société finlandaise de sécurité informatique à l'origine de plusieurs alertes d'attaques sur cellulaires.

« Une infection peut se révéler coûteuse, souligne **Mikko Hypponen,** directeur, recherche antivirus, de F-Secure. Le carnet d'adresses de mon cellulaire compte 1 700 adresses. Imaginez la difficulté que j'aurais à le reconstituer... »

De plus en plus dangereux

Fontal est l'un des premiers types d'attaques à éteindre réellement le cellulaire et à contraindre les utilisateurs à effacer toutes les données. Les attaques précédentes, qui datent d'il y a seulement quelques semaines, correspondent à différentes sortes de vers, dont *Mabir* et *Cabir.*

Fontal est un des premiers types d'attaques à éteindre réellement le cellulaire et à contraindre les utilisateurs à effacer toutes les données.

Ainsi, ces vers consistaient en des fichiers infectés qui se propageaient par l'entremise de *Bluetooth,* un système de transmission sans fil pour les cellulaires et pour Internet. Une fois infiltré dans un cellulaire, le ver tente d'établir une connection avec les cellulaires compatibles aux alentours.

Ce moyen de propagation n'est guère efficace, car il faut que l'utilisateur télécharge le fichier envoyé et accepte par deux fois de passer outre des messages d'alerte d'un risque potentiel de virus. Et pourtant, Cabir a déjà été détecté dans une vingtaine de pays, dont les États-Unis.

« Il y a tant d'étapes d'installation qu'il est étonnant que ce ver prenne autant d'ampleur, mais j'imagine qu'avec un milliard de cellulaires dans le monde, certains utilisateurs acceptent d'ouvrir le fichier infecté », dit M. Hypponen.

Cabir et les autres vers actuels ne causent guère de dégâts, tout au plus des inconvénients tels que le déchargement accéléré de la batterie du cellulaire infecté. ■

Hausse prévue des budgets alloués à la sécurité

Le budget des entreprises alloué à l'informatique devrait progresser de 2,5 % en 2005, selon une étude de la firme de recherche **Gartner.** Il s'agirait alors de la plus forte hausse depuis 2001.

L'investissement des entreprises dans les technologies de l'information (TI) devrait ainsi augmenter après plusieurs années de quasi-stagnation, souligne l'étude menée auprès de quelque 1 300 directeurs informatiques provenant d'une trentaine de pays et représentant un budget annuel global de 57 milliards de dollars américains (G$ US).

La sécurité avant tout

L'éclatement de la bulle technologique survenu en 2000 avait eu comme conséquence de faire stagner les dépenses des entreprises en matériel informatique. Ce phénomène s'était fait sentir dès 2001.

La priorité actuelle des entreprises concerne la sécurité des réseaux informatiques. Nombre d'entre elles envisagent de hausser le degré de sécurité, et donc de mieux s'équiper. De plus, le fait d'améliorer leur sécurité informatique peut permettre à certaines entreprises d'accroître du même coup leur productivité : moins de pannes et de pertes de fichiers endommagés ou volés ne peut qu'aider à la bonne marche des activités. ■ **O.S.**