Deuxième de quatre cahiers

Les affaires électroniques

13 OCTOBRE 2001

Protection

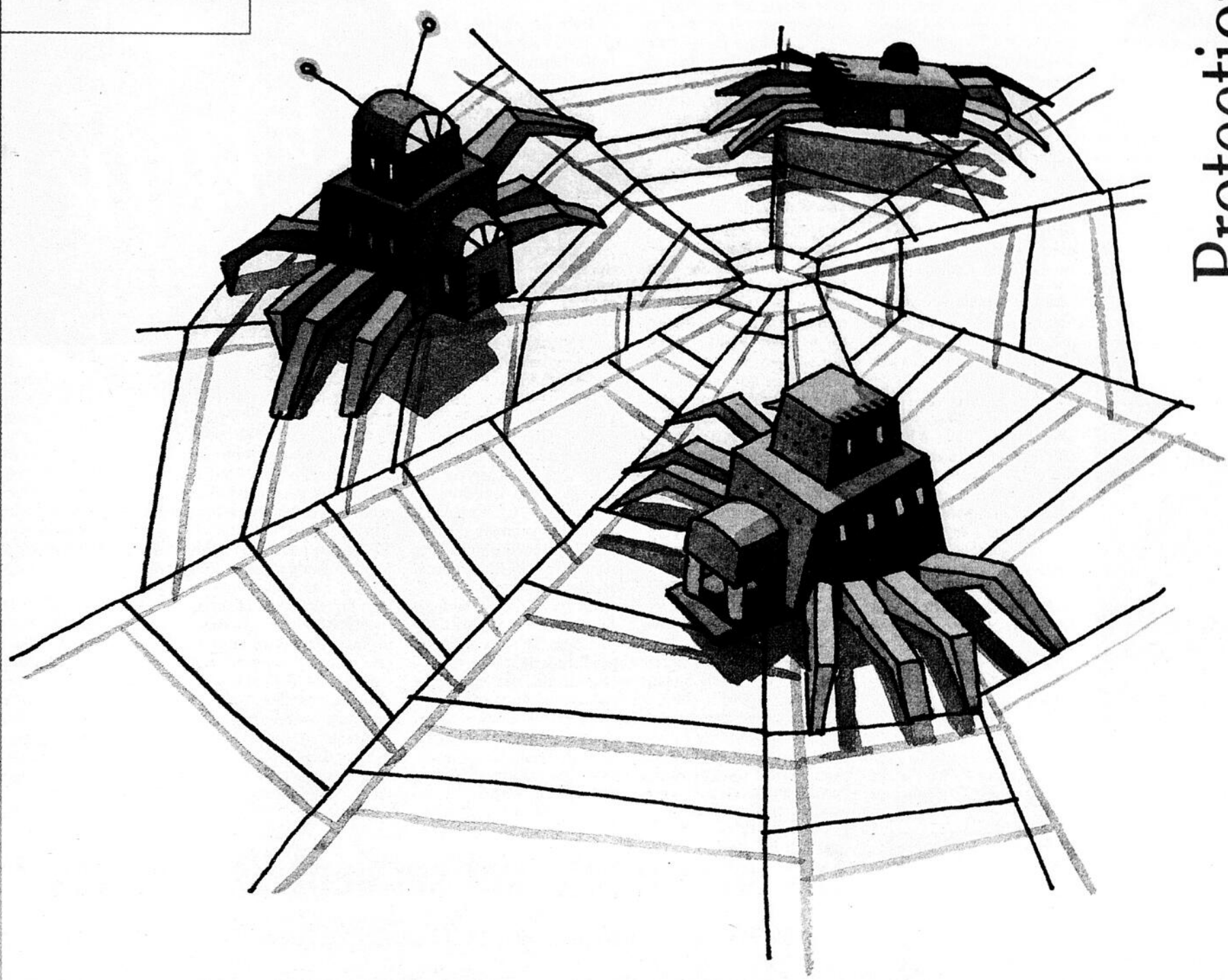
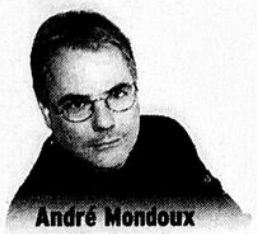


ILLUSTRATION : ARTVILLE STOCK IMAGE

Priorité à la sécurité

LES AFFAIRES

Comment se prémunir contre les désastres informatiques



André Mondoux
dossiers@transcontinental.ca

La tragédie de New York est un triste rappel qu'une catastrophe peut survenir à tout moment. Si vous veniez à perdre d'un coup toutes vos infrastructures informatiques, votre entreprise pourrait-elle survivre ? Heureusement, il existe des façons, sinon de vous prémunir contre des désastres, à tout le moins d'en diminuer fortement leur impact sur les activités d'exploitation de votre entreprise.

Toute mesure visant à vous aider à vous relever d'un désastre doit être amorcée... avant le désastre. Cela semble une évidence, mais trop d'entreprises ne réalisent l'importance de mesures de sécurité qu'après une catastrophe.

« La première étape consiste à prendre une entente avec une firme-conseil qui puisse, de concert avec vous, élaborer un plan d'urgence valide », dit **Jacques Viau**, consultant en sécurité et en confidentialité pour **IBM**.

Si vous élaborez ce plan à l'interne, assurez-vous de le faire valider par une tierce partie compétente. « Et testez ce plan régulièrement, comme on fait – ou devrait le faire – avec les traditionnels exercices d'incendie », ajoute-t-il.

Les services de relève

N'oubliez pas que votre plan doit avoir une portée globale : les services de relève n'en sont qu'un des éléments.

Les services de relève peuvent prendre plusieurs formes, selon les besoins et le budget du client. Les grandes firmes de services-conseils offrent ce type de service.

Essentiellement, il s'agit d'un service qui est structuré comme une police d'assurance : pour un montant forfaitaire mensuel, le client bénéficie d'une protection. Cette protection peut prendre plusieurs formes.

Elle peut consister en l'hébergement des activités stratégiques (comme un site de commerce électronique) sur les serveurs du fournisseur de service de relève. « Nous archivons tous les jours le site du client et par mesure de sécurité, nous expédions la copie dans un autre de nos centres », explique **Éric Desbiens**, vice-président des services d'hébergement, de sécurité et de réseaux de **Cognicase**.

« De plus, nous mettons en place un journal de bord afin de tenir à jour le registre de toutes les transactions. Nous pouvons ainsi remettre sur pied un système complet en moins de 12 heures », précise M. Desbiens.

Si vos locaux sont détruits

Cependant, il peut malheureusement arriver que les entreprises victimes d'une catastrophe perdent aussi leurs locaux et les infrastructures informatiques qu'ils abritaient. En prévision de ces cas, elles peuvent souscrire à un plan de protection qui leur donne droit à l'utilisation de locaux temporaires et de ressources informatiques afin de poursuivre leurs activités quotidiennes. Règle générale, il faut compter entre 24 et 48 heures avant d'avoir le système de secours en place.

Les firmes victimes se rendent à des locaux régionaux, à partir desquels elles accèdent à distance aux centres d'exploitation du fournisseur de service de relève.

Si elles n'offrent pas le service directement, la plupart des firmes-conseils peuvent agir en tant qu'intermédiaires auprès des grandes firmes nord-américaines (comme **SunGuard** et **Comdisco**) afin de mettre en place un tel service. Le rôle de la firme conseil sera alors d'accompagner et guider le client dans la conception, la mise en place et les essais du programme de relève.

« Il existe toutefois des cas où un retard de 24 ou 48 heures est trop long.

« On songe par exemple aux secteurs bancaire et financier où toute interruption de service, ne serait-ce qu'une minute, peut se solder par des pertes financières élevées », souligne **Gérard Chagnon**, vice-président, Gestion intégrée des technologies, de **CGI**.

Dans ces cas, les entreprises peuvent utiliser les services de la firme-conseil pour mettre sur pied des centres *miroirs*; c'est-à-dire que toutes les données du ou des serveurs d'entreprise sont automatiquement dupliquées en temps réel sur un serveur distant situé à l'un des centres de la firme-conseil. En cas de panne, ces serveurs distants peuvent prendre immédiatement la relève. Bien souvent ces services prennent la forme de solutions clés en main où le client fait l'impartition complète de sa sécurité au fournisseur de service.

En théorie, rien n'empêche les grandes entreprises de déployer elles-mêmes un tel système à l'interne, en misant sur leur réseau étendu reliant plusieurs centres dispersés géographiquement.

« Cependant, cela exige des coûts importants, notamment pour l'achat, le déploiement et l'entretien d'équipements parallèles, de même que pour l'établissement d'une liaison à forte bande passante.

L'avantage que nous avons, à titre de fournisseur de service, est que nous pouvons amortir ces coûteuses infrastructures entre plusieurs clients et ainsi offrir un service à un coût réellement avantageux », dit M. Chagnon.

Bien qu'un plan d'urgence prévoyant un service de relève soit important, il ne faut pas oublier qu'il s'agit d'une dimension de la sécurité informatique. « Les catastrophes sont certes spectaculaires, mais il existe d'autres dangers tout aussi dévastateurs : un de nos clients a vu les deux tiers de son parc informatique de 1 000 *PC* complètement privés d'Internet pendant cinq jours, à la suite d'un virus. Voilà un bel exemple où un soi-disant petit événement peut faire bien du mal », mentionne M. Desbiens.

Comme le souligne M. Viau, « il est important de s'assurer que tout plan de relève soit inclus dans une politique globale de sécurité et de conservation des données, et que tous les employés soient conscients du rôle qu'ils ont à jouer. La sécurité ne doit pas être une préoccupation exclusive du service informatique. » ▮

SOMMAIRE

Les jours d'Internet seraient-ils comptés ?

La prolifération de virus pourrait rendre la Toile inutilisable

Faut-il voir en *SirCam*, le célèbre ver, et *Nimda*, le plus récent virus hybride qui attaque les systèmes informatiques sur plusieurs fronts, les signes avant-coureurs du début de la fin du *Net* ? Les ravages qu'ils causent pourraient-ils éventuellement sonner le glas du réseau des réseaux ?

Si l'on en croit les derniers pronostics de la firme **MessageLabs**, spécialisée dans la détection des virus informatiques, les jours d'Internet seraient en effet comptés.

Abandonner le courriel devenu trop suspect

L'augmentation constante des virus propagés par courriel et les projections pouvant être réalisées à partir de l'observation de cette croissance permettent de prédire que, dans quelques années, le Net pourrait bien devenir inutilisable en tant que moyen de communication à la fois efficace et sécuritaire.

Si la tendance devait se maintenir, selon **Mark Sunner**, directeur de la technologie de MessageLabs, le volume de missives infectées deviendrait tellement imposant que les internautes insuffisamment protégés seraient, bon gré mal gré, conduits à abandonner le courriel devenu trop suspect.

Des prévisions alarmantes

Pour étayer ses sombres prévisions, MessageLabs brandit par ailleurs des chiffres qui parlent d'eux-mêmes. Entre 1999 et 2015, le taux de messages infectés pourrait passer de 1 sur 1 400 au départ à 3 sur 4 au fil d'arrivée. Le ratio actuel se situe pour sa part à environ 1 sur 300.

Bien qu'elles soient assez alarmistes – **Alex Shipp**, technicien supérieur chez MessageLabs, le concédant d'ailleurs lui-même – ces prédictions méritent tout de même qu'on s'y arrête. Malgré le fait que des précautions peuvent déjà être prises (filtres, logiciels antivirus, etc.), le problème n'en est pas moins grandissant... et les virus, de plus en plus astucieux et nombreux.

Il ne faut pas oublier le pourriel

Jumelées aux effets négatifs du pourriel publicitaire (*spam*) qui encombre de plus en plus les réseaux et les boîtes de courrier, les séquelles laissées par les missives infectées risquent de redéfinir notre utilisation professionnelle et personnelle du courrier électronique.

Il y a donc, effectivement, un certain péril en la demeure. Et de là à prédire que les déploiements de la sécurité informatique n'ont pas fini de nous surprendre, il n'y a qu'un pas à franchir. ▮

Cet article a été rédigé par Catherine Lamy, analyste-conseil en veille stratégique du CEFRIO, et publié dans le bulletin SISTech du 28 septembre dernier.
Il est possible de s'abonner gratuitement à ce bulletin ou de le consulter à l'adresse :
www.infometre.cefrio.qc.ca/loupe/sistech

Laxisme dans la protection des renseignements personnels

Jérôme Plantevin
plantevinj@transcontinental.ca

Les entreprises québécoises sont légalement obligées de prendre toutes les mesures adéquates pour assurer la confidentialité des renseignements personnels qu'elles détiennent dans leurs banques de données. Mais dans les faits, il y aurait beaucoup de laxisme selon les experts consultés par LES AFFAIRES.

« En dépit des lois existantes, peu d'entreprises québécoises ont adopté des mesures pour protéger les renseignements personnels en leur possession », dit **Martin Dubois**, avocat spécialisé en sécurité informationnelle de **Bernier Baudry**.

Cela serait dû en grande partie au fait que la législation ne prévoit pas des sanctions asssez musclées. « Les sanctions restent faibles, poursuit-il. Elles ne dépassent pas les 25 000 $, selon M. Dubois.

« De plus, les deux lois ne précisent pas quels types de mesures doivent être pris. Le type de pare-feu ou la méthode de cryptage ne sont pas spécifiés », souligne **Éric Lacroix**, directeur de la veille stratégique du **Centre francophone d'informatisation des organisations** (CEFRIO).

Deux lois

Deux lois protègent les renseignements personnels détenus par les entreprises.

En 1994, le Québec a adopté une *Loi sur la protection des renseignements personnels* dans le secteur privé (L.R.Q.,c. P-39.1). Ainsi, toute personne qui exploite une entreprise et recueille, détient, utilise ou communique des renseignements personnels sur autrui est obligée de prendre et d'appliquer des mesures de sécurité propres à assurer le caractère confidentiel des renseignements.

« En vertu de cette loi, en cas de poursuite, les entreprises devront montrer qu'elles ont entrepris tous les efforts pour assurer la sécurité et la confidentialité des données touchant aux informations personnelles », explique **Robert Currie**, le responsable de l'unité d'enquête et de support informatique de la **Gendarmerie Royale du Canada** (GRC).

Le Canada a emboîté le pas au Québec et a mis en place, en janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques* (C-54). « La loi fédérale reprend pour une bonne part les dispositions promulguées par la loi provinciale, dit **M. Dubois.** Ainsi, l'alinéa 4.1.4 précise que les organisations doivent assurer la mise en oeuvre des procédures pour protéger les renseignements personnels. » La loi fédérale a cependant une portée plus limitée que la loi provinciale.

« Le piratage informatique est un phénomène qui croît de manière exponentielle. »

Hormis dans les Territoires du Nord-Ouest, au Yukon et au Nunavut, cette loi ne s'applique qu'aux renseignements personnels des clients et des employés des entreprises sous réglementation fédérale, comme les banques, les compagnies téléphoniques, les radiodiffuseurs, les câblodistributeurs et les transporteurs aériens.

Elle s'applique aussi à toute communication de renseignements personnels transmise par une entreprise vers une autre province ou l'étranger, si les renseignements personnels sont spécifiquement visés par la transaction.

Pas d'obligation de se protéger

Par ailleurs, les textes de loi ne portent que sur les renseignements personnels. Les autres renseignements que détiennent les entreprises et qu'elles échangent sur leurs réseaux ne sont pas concernés. Bref, elles ne sont pas tenues de se protéger.

En ce qui concerne ce type d'information, la marge de manoeuvre des législateurs est quasi nulle. « Contrairement aux dispositions sur les renseignements personnels, ici, il n'y a pas de justification juridique pour légiférer », dit M. Dubois.

De plus, imposer des systèmes de sécurité importants et coûteux risque d'être préjudiciable pour certaines PME qui n'ont pas forcément les moyens d'investir dans de tels systèmes, souligne-t-il.

Robert Masse, directeur de la division Gestion des risques informatiques de **KPMG**, est du même avis : « Est-il concevable d'imposer au grand public une loi l'obligeant à fermer la porte de sa maison ? demande-t-il. Les entreprises doivent aussi être laissées à elles-mêmes. Libre à elles de se protéger. »

Dans les grandes entreprises, les pressions des conseils d'administration se font de plus en fortes pour assurer l'invulnérabilité des systèmes. Surtout que les exemples de pertes financières importantes dues au piratage informatique font de plus en plus la manchette.

« Le piratage informatique est un phénomène qui croît de manière exponentielle », rappelle M. Masse. Selon la **Computer Security Institute** et le **FBI**, en 2000, 186 entreprises américaines avouaient avoir avoir subi des pertes financières totalisant 378 M$ US à la suite d'attaques informatiques ciblées, comparativement à 265 M$ US en 1999.

Cela ne représente que la pointe de l'iceberg puisque cette même étude précise que 340 entreprises parmi les 532 interrogées ont subi des pertes financières, qui ne sont pas toutes quantifiables.

« Au Canada, il est très difficile de chiffrer le nombre d'entreprises qui ont subi des attaques, tout comme il est difficile de mettre un chiffre précis sur le coût de cette fraude », dit M. Masse.

Il est aisé d'ailleurs de comprendre pourquoi : quelle entreprise irait crier sur tous les toits qu'elle a subi de lourdes pertes à la suite d'attaques informatiques et d'intrusions dans ses réseaux ? Ou qu'elle n'avait pas pris toutes les mesures suffisantes, comme tout simplement crypter ces données ?

« C'est un peu comme la théorie de l'évolution de **Darwin**, conclut M. Masse. Les entreprises qui ne sauront pas évoluer et se protéger seront vouées à disparaître. » ▮

PHOTO : JEAN-GUY PARADIS, LES AFFAIRES

Y a-t-il une façon de rassurer les consommateurs pour les inciter à acheter en ligne ?

« Il faut suivre les meilleures pratiques »

Lyne Bouchard directrice, Gartner Consulting, Est du Canada
dossiers@transcontinental.ca

Et si les consommateurs avaient raison de ne pas vouloir faire des affaires sur Internet ? Et puis, est-ce qu'une seule compagnie est en mesure de rectifier les perceptions ?

L'hésitation des consommateurs est compréhensible.

D'une part, pour déplacer les comportements des places d'affaires traditionnelles vers le Web, il faut que l'expérience en vaille la peine. Et quand on regarde cela de plus près, il faut bien avouer que pour le consommateur, l'achat par le Web ne présente pas tellement d'attraits.

Le comportement du consommateur diffère de celui de l'acheteur industriel : alors que le professionnel cherche souvent à racheter les mêmes produits mais aux meilleures conditions possibles, les goûts du consommateur changent et seuls les produits les plus rudimentaires se prêtent bien aux achats par Internet, tels le shampoing, la dentifrice, les disques compacts, et peut-être les chemises pour hommes, mais peut-être pas les blouses pour femmes.

Il est vrai qu'Internet permet de sauver du temps de déplacement, mais rarement du temps de magasinage : les concepteurs de sites Web ont encore une bonne courbe d'apprentissage avant de rendre leurs sites faciles d'accès et facilement navigables.

Certains sites destinés aux consommateurs sont très populaires, mais pour la plupart des organisations, la mise sur pied d'un site devrait viser d'abord et avant tout à attirer la clientèle dans le magasin.

D'autre part, le fait de vendre sur Internet est évidemment intéressant pour un commerçant. Il faut voir dans quelle mesure une entreprise peut effectivement diminuer les réserves des internautes.

Résoudre le problème de la crainte des consommateurs n'est pas une mince tâche, et n'est pas facile à résoudre avec des mécanismes technologiques ou une campagne de publicité.

Il faut se battre en partie contre les mythes urbains et le discours journalistique pas toujours avisé. Une entreprise pourrait respecter à la lettre les règles d'éthique et de sécurité quant à l'usage et à la communication d'informations confidentielles, mais se retrouver tout de même à s'aliéner ou à perdre la confiance de sa clientèle en n'expliquant pas, en ne suivant pas et en n'appliquant pas de façon appropriée ses politiques.

OPINION

Les règles de base

Première règle d'or : il faut suivre les meilleures pratiques.

Deuxième règle d'or : n'assumez pas que tous vos clients partagent les mêmes craintes. Ces craintes varient en fonction des segments démographiques visés et des individus à l'intérieur de ces segments. Il faut définir des politiques et pratiques en matière de protection des renseignements confidentiels et de sécurité simples, uniformes et faciles à comprendre, et qui soient adaptées à la clientèle spécifiquement visée par l'entreprise.

Elles devraient idéalement être testées auprès de différents groupes afin de s'assurer que leur interprétation correspond bien aux intentions du commerçant.

Gartner estime que, dans le futur, 95 % de l'insatisfaction des consommateurs envers les abus de confidentialité viendra surtout d'une mauvaise communication, plutôt que d'une mauvaise utilisation de l'information (probabilité de 0,7).

Si le manque de confiance des consommateurs envers les achats par Internet est un problème qui sera effectivement difficile à régler à court terme, il faut comprendre qu'une bonne partie du problème se situe du côté des pratiques des entreprises, pas des perceptions des consommateurs ! ▮

Y a-t-il une façon de rassurer les consommateurs pour les inciter à acheter en ligne ?

« Les entreprises doivent s'autodiscipliner »

Jacques Nantel professeur titulaire de marketing à l'École des Hautes Études Commerciales (HEC)
dossiers@transcontinental.ca

PHOTO : JEAN-GUY PARADIS, LES AFFAIRES

OPINION

De tous les freins dont on entend le plus parler au sujet des transactions des consommateurs sur la Toile, celui de la sécurité est certes le plus tenace.

À cet égard, l'appréhension des consommateurs prend deux formes. La première, la plus marquée, a trait au fait de donner son numéro de carte de crédit par le Web. Un récent sondage publié par la firme **Léger Marketing** indiquait que seulement 1 % des consommateurs canadiens (10 % au Québec) étaient prêts à donner leur numéro de carte de crédit sur le Web.

Ce chiffre peut paraître faible, mais lorsqu'on sait que seulement 39 % des consommateurs sont prêts à faire de même par le téléphone, il y a lieu de croire que cette appréhension n'est pas le seul fait de la nouveauté d' Internet.

La seconde sorte de crainte est plus pernicieuse, risque de durer plus longtemps, et pourrait même être un frein majeur au développement du commerce électronique. Cette crainte est liée à l'utilisation que peuvent faire – et que font – les entreprises des données recueillies auprès de leurs consommateurs, tels leur adresse, leurs goûts, les produits qu'ils désirent acheter, etc.

Généralement utilisée à des fins de gestion interne (facturation, promotion, personnalisation de sites, etc.), cette information est souvent revendue à d'autres entreprises, voire à des courtiers spécialisés en cette matière.

À elle seule, la firme **Yesmail.com**, un géant dans le domaine du marketing par courriel, possède une base de données de 25 M de consommateurs ventilée en 750 catégories, selon les intérêts de ces mêmes consommateurs.

Cette pratique ennuie les consommateurs qui se voient ainsi continuellement sollicités par des entreprises qu'ils ne connaissent pas mais à qui ils auraient, soi-disant, donné la permission de leur écrire.

De plus, elle leur fait prendre conscience que l'information qu'ils donnent sur le Web se revend rapidement, menaçant du fait même leur vie privée.

La sécurité sur le Net est une question qui se règle déjà. Les solutions technologiques sont au point et vont continuer à évoluer.

À cet égard, la confiance des consommateurs est principalement une question de temps et d'habitude. L'utilisation des guichets bancaires automatisés, principalement à des fins de dépôts, a pris un certain temps avant de bénéficier d'une masse critique de consommateurs, mais on y est arrivé.

Il y a tout lieu de croire qu'il en sera de même avec le Web, en particulier si des institutions et des commerçants prestigieux sont prêts, comme c'est souvent le cas, à garantir la transaction.

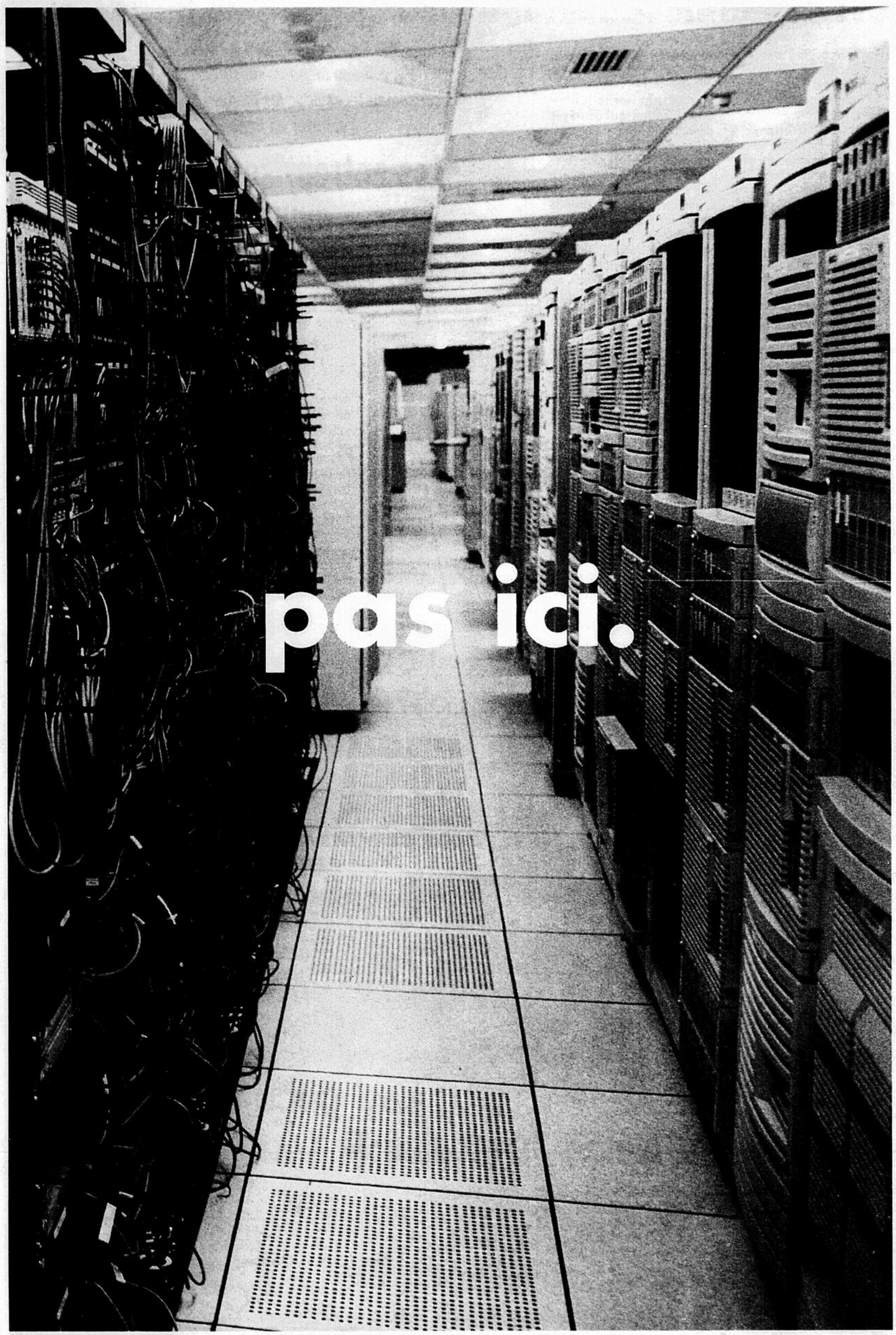
La seconde menace, quant à elle, est bien différente, tout aussi réelle, mais bien moins facile à contrecarrer puisque sa solution ne se trouve pas dans la capacité technologique des entreprises, mais bien dans leur volonté éthique.

À cet égard, le défi est grand. Comme les entreprises sur le Web l'ont bien compris, leurs stratégies de commercialisation, pour être efficaces et rentables, doivent passer par un marketing personnalisé de type relationnel.

L'acquisition et le développement de bases de données devient désormais une priorité pour elles.

Or, en cette matière, bien qu'il existe certaines lois devant protéger la vie privée des citoyens, elles sont de moins en moins efficaces, en particulier sur le Web.

Le paradoxe de cette situation réside dans le fait que si les entreprises ne réussissent pas à s'autodiscipliner, elle vont rapidement tuer un marché qui, bien que prometteur, pourrait vite se fermer. Comme quoi les solutions ne sont pas toujours technologiques ! ▮



Comment se protéger de la fraude

Les PME prêtes à se lancer dans le commerce électronique n'ont d'autre choix que de se protéger elles-mêmes contre la fraude en ligne. La tâche n'est pas facile.

En matière de sécurité des transactions sur Internet, des mesures doivent être prises dans cinq grandes catégories : la confidentialité de la transaction, l'authentification des parties impliquées, le contrôle de l'accès aux données transmises, l'intégrité des données transmises et l'impossibilité de la répudiation de la transaction, tant par l'entreprise que par le consommateur.

Pour les transactions par carte de crédit, une protection efficace doit comporter au moins les éléments suivants :

- Une base de données constamment mise à jour sur les cartes de crédits.
- La prise de contact directe (par téléphone ou par courrier électronique) avec les émetteurs de cartes de crédit en cas de transactions douteuses.
- Le repérage de transactions ne suivant pas le modèle habituel de dépenses du détenteur de la carte.
- Un système de limitation de la valeur des transactions.
- Différentes règles d'achat selon la valeur des transactions (par exemple, à partir d'un certain montant. La livraison obligatoire au domicile de l'acheteur).
- Un système empêchant la livraison de produits numériques à une adresse de courrier électronique anonyme (ex. : *petitbandit@hotmail.com*).
- Des précautions accrues s'il s'agit de marchandises qui peuvent facilement faire l'objet d'un commerce illégal.

Voilà pour l'essentiel. Les entrepreneurs ne doivent pas négliger non plus l'impression favorable qu'ils laissent auprès de leur clientèle en démontrant leurs efforts pour rendre sécuritaires les transactions par Internet. Même s'ils sont les seuls à faire les frais des fraudes !

Une politique claire et bien établie de paiement en ligne suffit à faire cette démonstration. Une telle politique décrit les règles d'achat, mais aussi les droits des acheteurs et les mesures prise pour protéger leurs transactions.

Par exemple, le consommateur est informé que le paiement se fera à la livraison seulement, qu'il bénéficie d'un délai de 30 jours pour retourner son achat et récupérer son argent, et que les mesures de chiffrement des messages garantissent la confidentialité de la transaction. ▮

SOURCE : COMMERCE SUREFIRE

Le courriel est une arme redoutable dans les mains des pirates

lesaffaires.com

Jean-François Barbe
barbejf@transcontinental.ca

Le nombre d'attaques informatiques visant à nuire aux organisations, par exemple en les espionnant, en *défigurant* leurs sites ou en les mettant hors combat, double chaque année, selon le **Software Engineering Institute** de **Carnegie Mellon**, un centre d'information en sécurité informatique.

Le Web n'est pas seul en cause : le courriel constitue une arme redoutable aux mains des cyberpirates.

« Nous sommes intervenus par deux fois l'automne dernier dans des cas d'usurpation d'identité de hauts dirigeants d'entreprises québécoises », signale **Denis Sansfaçon**, directeur de la pratique sécurité de **Versalys**, filiale de **Telus Québec**.

« Des pirates informatiques avaient diffusé de faux courriels portant la signature de dirigeants qui dénigraient certains cadres de l'entreprise. Ces courriels se sont ensuite trouvés dans des sites spécialisés. Disons que ces hauts dirigeants avaient déjà mieux paru. »

Le serveur de courriel d'une organisation peut également être détourné afin de diffuser des messages de type pollupostage (*spamming*) ou même haineux à des listes d'adresses de courriel n'ayant rien à voir avec l'organisation. « L'organisation source peut être reconnue juridiquement responsable », indique M. Sansfaçon.

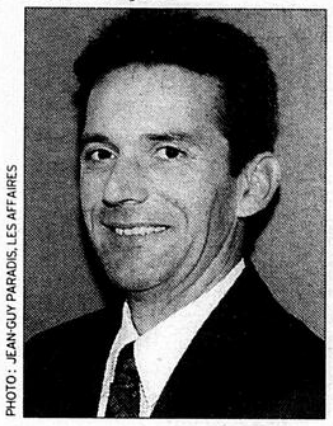


PHOTO : JEAN-GUY PARADIS, LES AFFAIRES

Denis Sansfaçon : « Une bonne attaque ne laisse pas de trace. »

La criminalité informatique constitue « malheureusement une réalité très cachée, poursuit M. Sansfaçon. Nous avons quelque années de retard sur nos voisins du Sud dans la sécurisation des architectures informatiques en raison de notre pacifisme et de l'extrême prudence américaine face aux poursuites judiciaires. »

Le combat contre l'imagination ou la vindicte des braqueurs informatiques ne sera jamais gagné d'avance.

En supposant même les meilleures ressources du monde, les organisations doivent apprendre à vivre avec ces attaques et à perdre certaines batailles, affirment Denis Sansfaçon et **Jenny Dho**, directrice solutions technologiques et sécurité du cabinet-conseil **Ernst & Young**.

« On devient vulnérable par le simple fait d'être connecté au Net », dit Mme Dho.

Si un jeune bidouilleur de 20 ans a récemment réussi à modifier des nouvelles et des cotes boursières affichées à la page *Finances* de **Yahoo!**, toute organisation ayant une présence Web doit renoncer à l'idée d'appartenir à un sanctuaire virtuel.

Voici comment les organisations peuvent s'adapter à cette donne, selon nos deux experts en sécurité informatique.

L'installation par défaut de certains systèmes d'exploitation, comme *Windows NT*, n'est pas sécuritaire, affirme Mme Dho : « Windows NT offre plusieurs ports de vulnérabilité. » Il faut procéder à une installation personnalisée.

Le coupe-feu

Beaucoup d'entreprises ont cru après l'installation de coupe-feu informatiques que leurs efforts de protection avaient atteint leur summum. Un coupe-feu, rappelons-le, autorise certains passages entre un réseau interne et un réseau public.

« Le coupe-feu n'est que la serrure d'une maison, qui contrôle l'entrée. À travers le coupe-feu, le cyberpirate voit quelles portes sont ouvertes et peut ensuite s'y engouffrer », dit M. Sansfaçon.

Un système de détection d'intrusion sur le réseau constitue le deuxième palier d'une bonne stratégie de protection. « Il faut en poser sur chaque segment de réseau, ou branche d'adresses », dit Mme Dho.

PHOTO : JEAN-GUY PARADIS, LES AFFAIRES

Jenny Dho : « On devient vulnérable par le simple fait d'être connecté au Net. »

Un système de détection de changements non autorisés des serveurs renforcera le dispositif de défense de l'organisation, indique-t-elle.

Les serveurs de courriel ne doivent pas, pour leur part, être configurés de façon à permettre le relais de courriels, dit M. Sansfaçon. Ainsi, l'organisation se prémunira contre le pollupostage fait en son nom.

Les moyens d'agir

Les dirigeants d'entreprise « ont intérêt à réaliser que leur information est numérisée », souligne M. Sansfaçon.

Des ressources spécialisées doivent veiller à la protection des données. Les informations doivent également être classifiées, les informations à plus haute teneur secrète étant protégées par une barrière à l'entrée plus élevée, comme un numéro d'identification personnel.

Par ailleurs, il est primordial d'effectuer une constante veille technologique, de façon à connaître les pirates informatiques et leurs outils, relève M. Sansfaçon. « Une bonne attaque ne laisse pas de trace ».

Les gestionnaires doivent également être formés à l'éventualité d'attaques informatiques. « L'absence de procédures écrites représente une faille générale dans les entreprises », souligne Mme Dho. Le personnel change mais les procédures restent.

Un bon système de signatures électroniques permettra quant à lui d'éviter que les dirigeants de l'entreprise deviennent les victimes de détournements d'identité, éventualité qui ne réjouira jamais les responsables des communications et des relations publiques. ▮

Quelques sites utiles

Le commerce électronique au Canada : Instaurer la confiance dans l'économie numérique
http://e-com.ic.gc.ca/francais/privee/632d1.html

Voici un bon point de départ pour les internautes désireux de connaître la stratégie canadienne en matière de protection des renseignements et de la vie privée. On y décrit la politique canadienne en matière de cryptographie, ainsi que les modalités d'élaboration et d'utilisation des services d'authentification et de certification au Canada.

En matière de vie privée, le site expose le guide sur la *Loi sur la protection des renseignements personnels et les documents électroniques*, dont l'application se fait en trois étapes, de 2001 à 2004. De plus, le site donne accès au document *Lignes directrices régissant la protection des consommateurs dans le contexte du commerce électronique*, préparé par l'OCDE. Une foire aux questions vient compléter l'information déjà abondante.

SANS Institute
http://www.sans.org/infosecFAQ/index.htm

Le **SANS Institute** (System Administration, Networking, and Security) offre un vaste répertoire d'articles relatifs à la sécurité informatique. Plus de 44 thèmes y sont abordés, notamment : la sécurité et le commerce électronique, l'authentification et les pirates informatiques. Il est possible de s'inscrire à trois listes de diffusion, envoyées sur une base hebdomadaire ou mensuelle, selon le cas.

Commissariat à la protection de la vie privée du Canada
http://www.privcom.gc.ca/information/guide_f.asp

Le Commissariat divulgue ici la toute la législation sur la protection des renseignements personnels, en plus d'offrir plusieurs guides relatifs à la protection de la vie privée. Parmi ceux-ci : *Protégez votre vie privée sur l'Internet*; *Comment protéger vos renseignements personnels*; *Comment consulter vos renseignements personnels et déposer une plainte*; *Le vol d'identité : qu'est-ce que c'est, et quoi faire*; *Dispositions législatives sur la protection de la vie privée au Canada*; *Numéro d'assurance sociale*.

Carrefour consommateur *Strategis*
http://strategis.gc.ca/SSGF/ca01180f.html

Lors de négociations sur le Net, les consommateurs et les entreprises se préoccupent de la sécurité de la transaction. Voici trois guides qui répondront aux interrogations des deux groupes.

Le premier guide, *Votre commerce dans Internet : gagner la confiance des consommateurs*, explique comment les marchands peuvent assurer la sécurité de leurs clients.

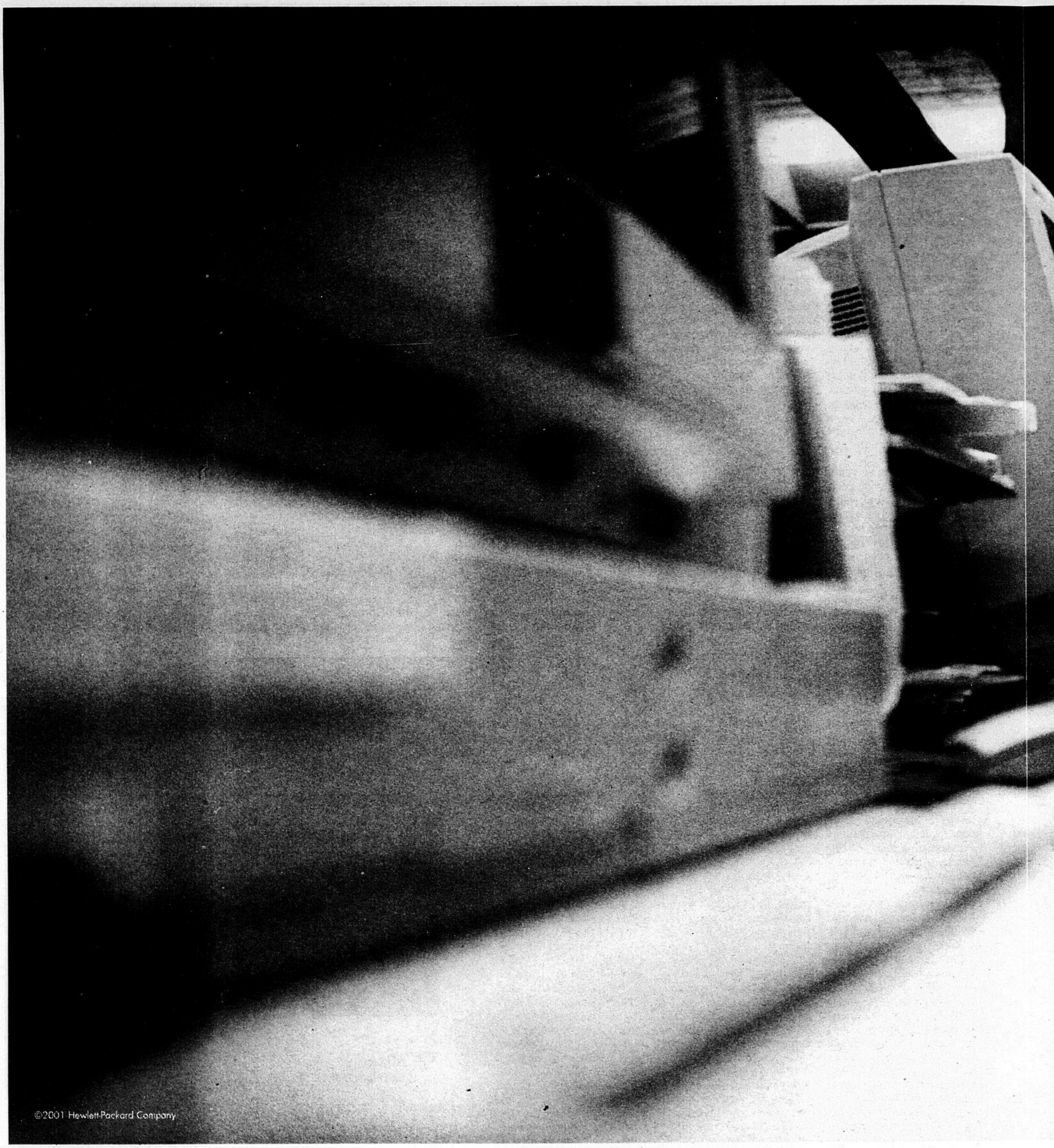
Le second, intitulé *Magasinez dans Internet : Renseignez-vous*, met l'accent sur les questions pertinentes lors d'une transaction sur le Net.

Par exemple : Comment savoir si le marchand est digne de confiance ? Avez-vous suffisamment de renseignements pour faire votre achat ? Comment vous assurer que les renseignements personnels seront confidentiels ?

Le dernier guide, *Principes régissant la protection des consommateurs dans le commerce électronique : Le cadre canadien*, constitue un guide pour les entreprises, les consommateurs et les gouvernements pour établir un cadre de protection des consommateurs en matière de commerce électronique. Les trois documents sont présentés en format PDF ou HTML

Recherche :Karine Audet, lesaffaires.com

SITES CLÉS lesaffaires.com
Tapez
le mot suivant
e-com OK



Les défis commerciaux et les occasions d'affaires auxquels vous devez faire face sont uniques, et comportent des co
Les solutions d'infrastructure HP – serveurs, logiciels, stockage, services et plus encore – sont élaborées pour le monde réel des affaires. Car aux dernières nouvelles, c

Échelon : un réseau international d'espionnage électronique

Cet espion serait une initiative commune des gouvernements britannique, américain, canadien, néo-zélandais et australien

Nelson Dumais
dossiers@transcontinental.ca

Science-fiction ou réalité ? Des pays anglo-saxons auraient mis sur pied un vaste système international d'espionnage électronique des communications, le réseau *Échelon*.

Dénoncé depuis quatre ans par les Européens qui le soupçonnent des pires abus, ce réseau de l'ombre ne jouit d'aucune reconnaissance officielle, son existence étant même niée par les autorités américaines. Seules l'Australie et la Nouvelle-Zélande ont officiellement reconnu sa présence.

Initiative commune des gouvernements britannique, américain, canadien, néo-zélandais et australien (les Européens parlent d'un club anglo-saxon), Échelon permettrait d'épier les communications de n'importe où au monde, qu'elles soient sous forme d'appel téléphonique, de télécopie, de courriel ou de transmission radio.

Sa technologie pointue saurait déchiffrer les données cryptées, épier les câbles sous-marins et repérer les comptes bancaires. Sa naissance remonterait à l'entente *UK-USA* de 1948.

Si on en croit ses détracteurs au Parlement européen, Échelon aurait été impuissant à prévenir les attentats terroristes du 11 septembre dernier aux États-Unis. Selon la vice-présidente du comité temporaire du Parlement européen consacré à Échelon, la docteure **Elly Plooij-Van Gorsel**, les récents efforts d'intelligence de ce très vaste réseau auraient été un échec total.

120 satellites espions

On sait que le réseau Internet est très facile à *placer sous écoute* puisque, selon la fantaisie des routeurs, la plus grande partie du trafic cabote par les États-Unis. Il existerait ainsi neuf endroits où la **National Security Agency** (NSA) exercerait une surveillance, grâce à des logiciels d'interception appelés *packet sniffer*. Le Parlement européen accuse même **Netscape**, **Microsoft** et **Lotus** d'avoir réduit les capacités de chiffrement de leurs produits revendus à l'étranger pour faciliter le travail de la NSA.

Quoi qu'il en soit, on parle de trois milliards de communications qui seraient ainsi filtrées à chaque jour. Au moins 120 satellites et un réseau très sophistiqué d'antennes seraient ainsi mis à contribution. Le terminus serait la NSA américaine, qui colligerait des sommes ahurissantes de renseignements en provenance de centres à la fine pointe comme celui de Menwith Hill dans le Yorkshire (30 récepteurs ultrasophistiqués) appartenant au **Government Communication Headquarters** britannique.

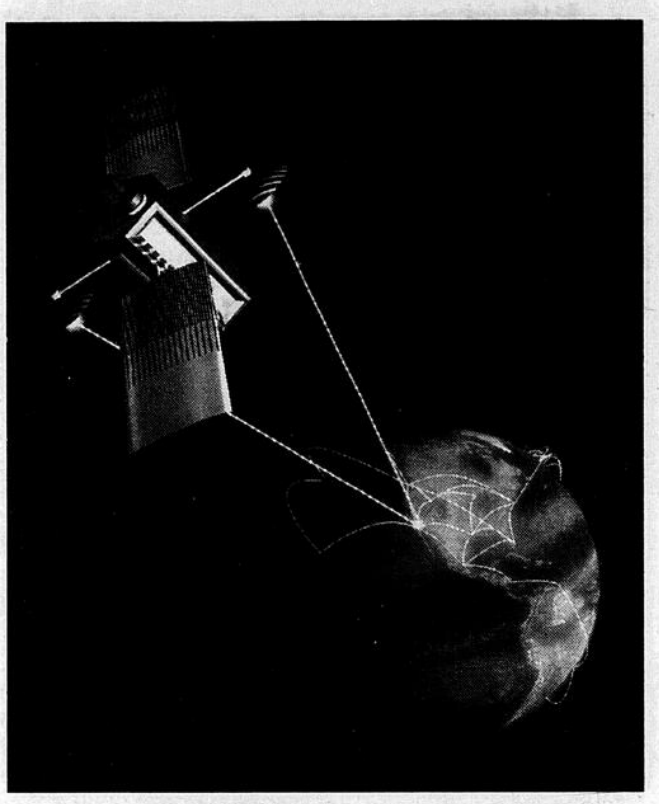
Des centres secondaires existeraient également au Canada, en Australie et en Nouvelle-Zélande, sans oublier en Turquie, en Allemagne de l'Ouest, au Danemark, en Norvège, en Corée du Sud et au Japon.

Grâce à leurs fonctions de reconnaissance vocale et à une banque de mots ou d'expressions clés, de puissants ordinateurs situés au Maryland rechercheraient ainsi des indices de criminalité internationale ou de terrorisme.

Un échec ?

La mise au jour du réseau Échelon remonte à 1996, alors que **Nicky Hager**, un chercheur néo-zélandais, a publié *Secret Power* (*http://fas.org/irp/eprint/sp*), un ouvrage étoffé sur le rôle de son pays dans ce réseau. Depuis, d'anciens responsables du renseignement et de nombreux experts, aussi bien américains et européens qu'australiens, ont validé les thèses de M. Hager.

Reste qu'à ce jour, la reconnaissance officielle du réseau tarde à venir. À Londres, on change de sujet quand on en parle; à Washington, on nie. Ce qui n'empêche pas le représentant républicain de la Géorgie, **Bob Barr**, de faire campagne pour que le gouvernement rende des comptes sur ce « programme effréné, non réglementé et sans surveillance ».



Il y a toutefois consensus chez les experts internationaux. Selon eux, Échelon existe bel et bien et sa justification serait la lutte contre le terrorisme et la criminalité internationale.

Échelon se justifierait par la lutte contre le terrorisme et la criminalité internationale.

Il en serait ainsi depuis la fin de la guerre froide, le pacte de Varsovie ne représentant plus de menace réelle pour les économies occidentales.

Malheureusement, on n'en tient pas toujours compte, affirmait récemment le quotidien allemand *Frankfurter Allgemeine Zeitung*. C'est ainsi que grâce à Échelon, les services de renseignement israélien (le **Mossad**) et américain (la **CIA**) auraient su dès juin que des terroristes préparaient des détournements d'avion dans l'optique de détruire des symboles de la culture américaine. Quant aux Britanniques, ils auraient reçu de tels avertissements en mars dernier.

Ces informations auraient entraîné un certain durcissement des mesures de sécurité, mais des divergences en haut lieu auraient laissé la voie libre aux terroristes. ▮

L'espionnage industriel, un dessein caché

Dans un reportage diffusé en novembre 1999 par la *BBC*, il avait été établi que les activités d'espionnage du réseau *Échelon* auraient débordé la lutte à la criminalité pour s'intéresser aux activités commerciales et industrielles.

La BBC avait alors cité le cas d'une société française sur le point d'obtenir un lucratif contrat brésilien qui aurait été placée sous écoute par Échelon. L'information recueillie aurait été fournie à une concurrente américaine qui, bien entendu, aurait remporté le contrat. Cette affaire fut par la suite corroborée par un ancien directeur de la **CIA**, dans une déclaration faite au quotidien français *Le Figaro*.

Ce reportage venait jeter de l'huile sur le feu. L'année précédente, le parlement européen avait en effet entrepris de demander des comptes aux principaux protagonistes, dans le cadre d'un rapport intitulé *In Appraisal of Technologies of Political Control*. Les réponses sont toujours attendues.

En février dernier, la commission de Justice du Parlement européen revenait à la charge avec un rapport intitulé *Interception Capabilities 2000*.

Les américaines en profitent

Dans la section traitant d'espionnage économique, les auteurs relatent de nombreux cas où des firmes européennes auraient été victimes d'espionnage au profit de concurrentes américaines.

On y cite notamment l'affaire du chasseur européen *Panavia* : selon les auteurs, le constructeur français **Thomson** se serait fait chiper un contrat de 1,3 milliard de dollars (G$) US par la société américaine **Raytheon** après que la **National Security Agency** eut intercepté un certain nombre d'appels téléphoniques.

L'année suivante, en 1995, c'était au tour d'**Airbus** de perdre un contrat de 6 G$ US au profit de **Boeing**, après que la NSA eut intercepté des télécopies. (ND) ▮

Le Canada n'est pas à l'abri du cyberterrorisme

Il faut s'attendre à des infestations virales et à des dénis de service

Nelson Dumais
dossiers@transcontinental.ca

Si, dans la foulée des attentats du 11 septembre dernier aux États-Unis, il est devenu concevable que l'infrastructure informatique canadienne soit attaquée par des terroristes, il ne faut pas s'attendre à un coup d'éclat spectaculaire, mais plutôt à des infestations virales et à des dénis de service.

C'est la mise en garde faite par **Michel Laflamme**, vice-président, commerce électronique, du **Groupe LGS**.

Heureusement, poursuit l'expert-conseil, les sites Web canadiens ne représenteraient pas autant d'intérêt pour des terroristes que ceux des États-Unis, où se retrouvent les grands portails.

Reste que nos serveurs sont tous un peu la cible de virus de plus en plus dangereux. « En fait, c'est la menace numéro un, soutient-il. Et les ordinateurs ne seront pas attaqués parce qu'ils sont canadiens, mais parce qu'ils seront en réseau. C'est le propre des virus; ils ne font pas de distinction entre les pays. »

Les menaces sont sérieuses, mais elles restent ignorées.

On se souvient qu'à la mi-septembre, plusieurs entreprises, dont la quasi-totalité de l'appareil gouvernemental au Nouveau-Brunswick, ont vu leurs serveurs paralysés par *W32.Nimda.A@mm* (Nimda), un ver dont la malignité était faible par rapport à son potentiel d'infestation. S'il avait été investi d'une mission plus ambitieuse, les dégâts auraient été énormes.

On peut ainsi croire qu'il s'agit d'une piste qu'étudieraient présentement les terroristes. Si on observe l'évolution des virus depuis deux ans, on constate que leur potentiel de dévastation est sans cesse accru. Et, à chaque épidémie, des entreprises se font infester et des sommes considérables de temps et d'énergie sont perdues.

On a beau crier au loup, rien n'y fait. Des serveurs de courrier se retrouvent inévitablement infectés et une propagation très rapide s'ensuit. Il est donc sensé de croire qu'une épidémie vraiment dévastatrice pourrait éventuellement nous frapper.

Même danger, côté déni de service, une menace à prendre très au sérieux ! Il s'agit d'un acte criminel en popularité croissante, une tactique très ciblée qui, de prime abord, semble convenir davantage aux vandales qu'aux terroristes. Mais, encore là, une opération de déni de service bien planifiée peut paralyser un réseau.

Contrairement à l'acte violent localisé en un endroit précis, le virus, ou le déni de service, attaque partout en périphérie. Il vise les serveurs raccordés en un vaste réseau. Quand une majorité de serveurs se retrouvent paralysés, le réseau saute, ce qui peut entraîner des conséquences graves pour l'économie.

Des sites plus attirants que d'autres

Il y a quand même au Canada des catégories de sites qui sont plus attirants que d'autres, précise M. Laflamme. C'est le cas de certains sites gouvernementaux, comme celui de la **Défense nationale**.

« Mais je prends pour acquis que les responsables de ces sites ont mis en place les outils pour bien se protéger. »

Du côté bancaire, « je sais qu'on y retrouve des groupes de sécurité chargés de la protection et qu'on investit beaucoup d'argent. Je n'entends effectivement jamais parler de sites bancaires mis hors service pendant des jours à la suite d'une attaque. Pourtant, je suis convaincu que ces serveurs ont été testés à maintes reprises par les malfaiteurs. »

Évidemment, s'empresse d'ajouter M. Laflamme, des études récentes démontrent qu'à peine 36 % des entreprises victimes d'intrusion électronique rapportent ce fait aux autorités policières. Personne n'a envie que cela se sache !

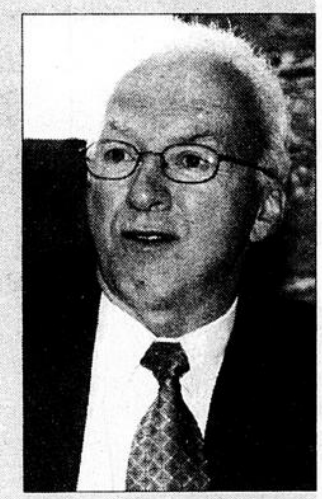
En dehors des institutions gouvernementales et financières, on retrouve par ailleurs une proportion de sites corporatifs plutôt mal nantis du côté sécurité, des sites qui ne coûteraient pas des fortunes à bien protéger en y installant des outils et en implantant des procédures de sécurité, selon M. Laflamme.

Enfin, il existe aussi d'autres types de menace. Sauf qu'il s'agit d'attaques criminelles visant un serveur en particulier. On parle ici de fraude ou d'utilisation abusive. ■

Les sites préférés de Gaëtan Frigon

Naviguant allègrement entre horaires surchargés et lourdes responsabilités, les grands dirigeants d'entreprise trouvent-ils intérêt, temps et même plaisir à surfer autrement ? Dans cette série, nous avons demandé aux personnalités d'affaires de révéler leurs pratiques d'internaute lorsqu'il est question de loisirs, d'affaires ou pour obtenir des nouvelles de leur industrie.

Madeleine Guay
dossiers@transcontinental.ca



À la tête de la **Société des alcools du Québec** (SAQ), **Gaétan Frigon** multiplie les recettes gagnantes depuis son entrée en fonction en mars 1998. Gérant 5 000 employés et des revenus de 2 milliards de dollars, le pdg trouve toujours un moment pour fureter sur le Web à la recherche de renseignements.

« Je navigue sur Internet presque tous les jours, tant à la maison qu'au bureau. Il s'agit pour moi d'une façon de me détendre tout en me renseignant sur une multitude de sujets. Internet, pour moi, c'est vraiment le monde au bout des doigts. »

INDUSTRIE Très friand des nouvelles de l'industrie, M. Frigon consulte les sites sur les vins et les sites des producteurs tels que *www.saq.com*, *www.wineandspirit.com*.

AFFAIRES PERSONNELLES Il consulte fréquemment les portails *www.sympatico.ca*, *www.yahoo.com* et *www.infinit.net*
Ses sites de nouvelles et sites gouvernementaux sont : *www.mesnouvelles.com*, *www.cyberpresse.ca*, *www.canada.gc.ca*, *www.gouv.qc.ca*

LOISIRS Pour ses loisirs, le pdg de la SAQ consulte les sites sur les véhicules récréatifs tels : *www.rvamerica.com*, pour l'accès au vaste répertoire d'associations, de manufacturiers, vendeurs et causeries en ligne; *www.campingworld.com*, un fournisseur de pièces et d'accessoires de véhicules récréatifs avec des liens vers les points de vente. *www.jamespublications.com*, pour consulter le *Campground BuyersGuide*, un manuel d'achat en ligne sur le Web. M. Frigon utilise également Internet pour préparer ses itinéraires de voyage par le biais du site *www.travelocity.com* ■

Encore peu d'assurances contre le piratage informatique

Les primes varient de 15 000 $ pour une petite police à 100 000 $ pour une protection contre la fraude

Jérôme Plantevin
plantevinj@transcontinental.ca

Malgré le phénomène croissant des fraudes et du piratage informatiques, il y a encore peu de compagnies d'assurances qui offrent des *cyberassurances* à leurs clients.

L'année dernière, la **Lloyds** annonçait en grande pompe le lancement de son *Internet Asset and Income Protection Insurance*, en collaboration avec le consultant en sécurité informatique **Counterpane Internet Security**, le courtier **Frank Crystal & Co** et l'assureur **Safeonline**.

D'autres assureurs lui ont emboîté le pas. Ainsi, les compagnies d'assurances **Chubb**, **Saint-Paul**, **American International Group** proposent aujourd'hui des *cyberassurances*. En France, les compagnies **AXA** et **AGF** offrent des assurances pour la protection des données dès qu'il y a atteinte aux systèmes de traitement automatisés, tout comme pour les manipulations de programmes et de données, telles que l'altération de pages Web due au piratage et aux virus informatiques.

Les primes proposées dépendent du niveau de protection que recherche l'entreprise, mais sont très élevées. « Les assureurs ne disposent pas de recul pour ce type d'assurances. Ainsi, les primes sont fixées selon le pourcentage des risques et des coûts engagés », dit **Richard Lavoie**, directeur, région de Québec, de l'assureur **Saint-Paul Canada**.

Pour une petite police d'erreurs et omissions, la prime peut s'élever au minimun à 15 000 $, alors que pour des primes contre la fraude informatique, on parle de primes variant entre 50 000 $ et 100 000 $.

Pour réduire le montant des primes, les compagnies d'assurances peuvent demander qu'un audit des systèmes de sécurité des entreprises soit effectué.

« Il existe désormais des normes internationales de sécurité », souligne **Mathieu Chouinard**, chef d'équipe, audit et sécurité, de **ESI Technologies de l'information**, une entreprise montréalaise spécialisée en sécurité informatique.

Ainsi, la norme *British Standard 7799*, qui a été récemment promue norme *ISO*, couvre à la fois la sécurité physique, la sécurité logistique, la sécurité de gestion et la sécurité des communications des entreprises.

Lors de ces audits, les systèmes de sécurité des entreprises sont mis à l'épreuve.

« Plusieurs points sont passés au crible, explique M. Chouinard. Entre autres, comment les équipements informatiques sont-ils protégés, ou bien comment les logiciels sont-ils configurés ? Est-ce que les données sont cryptées ? L'entreprise a-t-elle mis en place un pare-feu pour assurer l'imperméabilité de ces accès externes ? Et enfin, comment la sécurité au sein de l'entreprise est-elle gérée ? » ▮

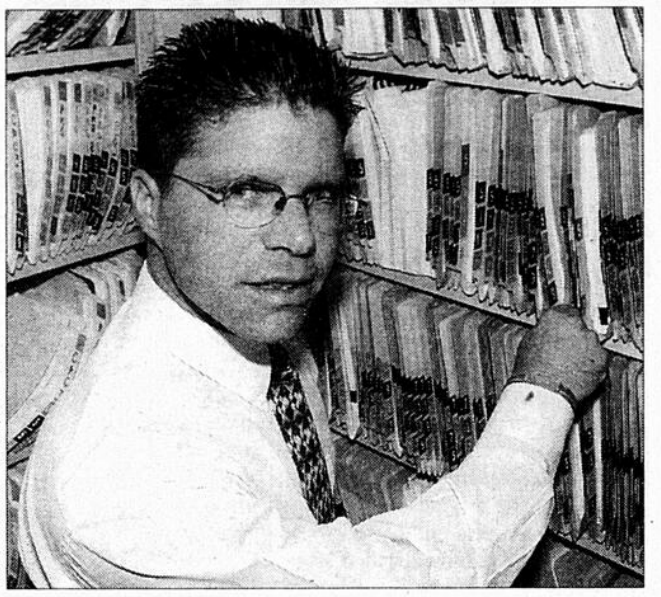


PHOTO : JEAN-GUY PARADIS, LES AFFAIRES

« Les assurances contre la fraude informatique et la violation de systèmes sont peu demandées », dit Richard Lavoie, de Saint-Paul Canada.

Trois catégories de cyberassurances

Les *cyberassurances* peuvent se diviser en trois catégories.

En premier lieu, les assurances contre la fraude informatique.

« Les entreprises qui adhèrent à ces assurances sont couvertes contre les détournements ou les transferts électroniques de fonds effectués illicitement par une personne de l'extérieur ou par un de leurs employés », explique **François Jean**, courtier en assurances de dommages d'**Assurance MLA**.

Deuxièmement, les polices couvrant la violation de systèmes informatiques. « Ici, nous parlons d'actes malicieux ou d'attaques de pirates, d'entrée et de changement de données, d'intrusion de virus ou de blocage de système », précise M. Jean.

Enfin, il y a les polices d'assurance pour les erreurs et omissions. Elles sont offertes aux entreprises des technologies de l'information comme protection contre d'éventuelles poursuites pour fautes professionnelles, dommages ou violation de la propriété intellectuelle que leurs activités causeraient. La responsabilité civile tout comme la couverture de biens sont aussi proposées dans ces polices. (JP) ▮

Surveillance électronique : les employeurs sur la corde raide

Il existe encore une zone grise entre ce qui est légitime et ce qui ne l'est pas

Suzanne Thibodeau
dossiers@transcontinental.ca

Des logiciels de gestion du réseau permettent aux entreprises d'exercer une surveillance étroite de l'usage que font les employés du courriel et d'Internet. Mais jusqu'où s'étend le droit de l'employeur d'exercer un tel type de surveillance sur ses employés ? Peut-il lire leur courriel ? L'employé a-t-il toujours un droit à la vie privée même au travail ?

L'employeur devrait faire preuve de prudence et de retenue lorsqu'il désire exercer une surveillance puisqu'il existe encore une zone grise entre ce qui est légitime et ce qui ne l'est pas. L'employeur devrait aussi communiquer des politiques claires qui éviteront les malentendus et contribueront à dissuader les utilisations abusives des outils de l'entreprise.

Dans un jugement rendu en mars dernier relativement à l'affaire d'un inspecteur de la police de Trois-Rivières-Ouest, accusé de possession de pornographie juvénile et de reproduction de ce matériel à partir des équipements de la Ville, le juge **Narcisse Proulx** de la Cour du Québec, a émis l'opinion qu'il n'existerait aucune expectative de vie privée lorsqu'un employé utilise sur son lieu de travail un ordinateur qui lui est fourni par son employeur.

Il faut cependant prendre avec réserve cette décision puisque, dans ce cas, il y avait des motifs de croire à la perpétration d'un acte criminel. De plus, il s'agissait d'une première décision de ce genre au Canada, qui a d'ailleurs été portée en appel.

Lors d'une récente allocution, le Commissaire canadien à la vie privée, **George Radwanski**, a indiqué qu'un employeur ne pouvait justifier une surveillance généralisée de l'utilisation que font l'ensemble des employés du courriel et d'Internet simplement en raison du potentiel de perte de temps ou de productivité engendrée par une utilisation inadéquate.

Cependant, une surveillance précise visant un individu (et non l'ensemble des employés), lorsque l'employeur a des motifs raisonnables de croire à un abus, serait à son avis légitime.

Au Québec, la **Commission d'accès à l'information** est d'avis que la surveillance du courrier électronique des employés peut être légitime dans certaines circonstances, mais que l'employeur doit informer clairement ses employés des motifs et des conditions de cette surveillance.

Il faut noter qu'une surveillance visant essentiellement les biens de l'employeur et non les personnes ne constituera pas une atteinte à la vie privée (par exemple, l'utilisation d'un système GPS pour localiser des camions de livraison). Ainsi, le contrôle de l'utilisation des ressources informatiques, par exemple le contrôle du nombre d'heures d'utilisation d'Internet, serait acceptable, tout comme l'est la consultation des relevés des communications téléphoniques effectuées par les employés à partir du système téléphonique de l'entreprise.

Établir une politique d'utilisation

La lecture du courriel des employés et la surveillance de l'utilisation d'Internet par l'employeur sont des situations très délicates, d'autant plus si les employés n'ont pas été avisés que l'employeur exercerait une surveillance à cet égard, car ils pourraient légitimement se croire à l'abri des indiscrétions.

Il est donc fortement recommandé d'établir une politique claire d'utilisation d'Internet, du courriel et des ressources informatiques fournies par l'employeur. Cette politique indiquera quelles sont les utilisations considérées comme inacceptables.

Cette politique doit permettre aux employés de comprendre clairement les activités qui seront contrôlées et surveillées par l'employeur, les circonstances dans lesquelles cette surveillance sera exercée, ce qui sera fait des informations recueillies ainsi que les sanctions susceptibles d'être appliquées advenant la violation de la politique.

La validité de mesures telles que l'obtention d'une renonciation écrite des employés à toute forme de vie privée au bureau ou d'un consentement à une surveillance constante et sans limites est actuellement incertaine et contestée.

Ainsi, il est préférable de s'en tenir à des mesures pouvant être considérées comme raisonnables compte tenu des circonstances et de la nature particulière de l'entreprise.

L'employeur devrait également établir des politiques relatives au harcèlement et à la discrimination. La diffusion à l'ensemble des employés et l'application constante et uniforme de ces politiques seront généralement suffisantes pour démontrer la diligence raisonnable de l'employeur.

En somme, l'employeur devrait faire preuve de prudence et de retenue lorsqu'il désire exercer une surveillance, puisqu'il existe encore une zone grise entre ce qui est légitime et ce qui ne l'est pas.

L'employeur devrait aussi communiquer des politiques claires qui éviteront les malentendus et contribueront à dissuader les utilisations abusives des outils de l'entreprise. ▮

Suzanne Thibodeau est directrice, Service des risques d'entreprise, de Samson Bélair Deloitte & Touche

Des espions peuvent se glisser dans votre ordinateur

Une simple banderole publicitaire dissimule parfois un programme qui épie vos fichiers et les transmet à son maître

André Salwyn
dossiers@transcontinental.ca

Plusieurs s'imaginent qu'un simple programme antivirus protège leur ordinateur contre toute infection et contre toute destruction des données privées qu'il contient. C'est vrai.. en partie seulement : un programme antivirus ne protège pas l'utilisateur contre un nouveau virus.

Mais un risque beaucoup plus grand, aux yeux des experts, est celui de voir ses données privées devenir accessibles à des tiers par le biais de programmes espions (*spyware*), sans que l'utilisateur le sache. Les programmes espions permettent par exemple à une entreprise de connaître toutes les transactions effectuées par son concurrent.

« C'est un risque qui est ignoré par la plupart des utilisateurs même si, potentiellement, il est beaucoup plus dangereux que les autres », dit **Anson Lee**, directeur associé pour la gamme de produits *Norton* de **Symantec**.

« Les programmes espions peuvent entrer dans l'ordinateur d'un utilisateur pratiquement sans aucun problème. Ces programmes, normalement très petits, sont placés au sein d'autres programmes beaucoup plus grands, en général des gratuiciels populaires que les utilisateurs téléchargent sans se méfier », explique Anson Lee.

Plus inquiétant encore, ils peuvent aussi être insérés dans des banderoles publicitaires que l'on trouve sur les pages Web, selon M. Lee.

Il s'agit d'une intrusion d'autant plus sournoise que le programme espion ne cause, en principe, aucun dégât et ne se manifeste pas ouvertement. Une fois dans le système, il accède tout simplement aux données qui l'intéressent et les communique à son maître.

D'abord une arme de marketing

Comme cette communication s'effectue en arrière-plan pendant que l'utilisateur navigue sur Internet, ou pendant que l'ordinateur est inactif, l'utilisateur n'en a aucune connaissance.

Le pot aux roses

Les programmes espions existent depuis un certain temps déjà. Mais ce n'est que récemment que des internautes ont commencé à se poser des questions.

Certains d'entre eux qui s'intéressaient aux recettes de cuisine données sur Internet se voyaient d'un seul coup bombardés d'annonces publicitaires leur offrant livres de cuisine, ustensiles de cuisine, et autres produits destinés aux gourmets et amateurs de bonne chère.

Cela était d'autant plus curieux que ces offres provenaient de sources différentes.

Symantec a découvert le pot aux roses : un mini-programme communiquant à son auteur l'adresse électronique de l'utilisateur ainsi que les sites que cet utilisateur visitait le plus.

« C'est une information fort pertinente et fort utile à tous ceux qui veulent faire du marketing dirigé, explique M. Lee. Beaucoup d'entreprises sont prêtes à payer asssez cher pour obtenir des listes d'acheteurs potentiels de leur produite. Cela leur permet de mieux cibler leur clientèle et d'atteindre un pourcentage de ventes plus élevé. »

Précisons que Symantec offre des produits de sécurité Internet qui limitent l'impact des programmes espions.

« Des produits comme *Internet Security* ne peuvent pas empêcher le téléchargement d'un programme espion, mais la présence du programme est signalée dès qu'il essaye d'embarquer sur Internet pour transmettre les renseignements recueillis. C'est alors à l'utilisateur de décider quoi faire », explique M. Lee. ■

Pour assurer l'efficacité d'un site Web

Afin de maintenir et d'améliorer la qualité du service offert aux internautes, il est essentiel pour les entreprises de quantifier le trafic de leur site et d'analyser leur activité quotidienne.

De la simple alerte à l'analyse détaillée des erreurs, les logiciels et services de surveillance de sites permettent de parer aux défaillances et de fournir des renseignements précieux.

Un site inaccessible ou défaillant frustrera la clientèle. Les entreprises doivent donc mettre en place des outils de surveillance qui scrutent en permanence le fonctionnement du site, les services offerts et l'intégrité de la base de données. Les outils les plus évolués proposent des fonctions d'analyse capables d'isoler rapidement l'endroit où se situe le dysfonctionnement.

Les entreprises ont le choix d'opter pour un logiciel qu'ils devront configurer et gérer eux-mêmes, ou encore de faire appel à un fournisseur de services applicatifs qui propose un service de surveillance. (CQ) ■

Outils de surveillance en ligne

Nom	Type	Site Web
IPSentry	Logiciel	www.ipsentry.net
EcoTools	Logiciel	www.compuware.com
New Test	Logiciel	www.auditec-newtest.com
Red Alert	Service	www.keynote.com
Topaz	Service	www.mercuryinteractive.com
StatsCounter	Service	www.statscounter.com

TABLEAU : LES AFFAIRES

B15

UN MOT VAUT MILLE IMAGES

LAPIERRE CKAC 730

B L

LE LIVRE DES AFFAIRES @

LES MAUVAISES IDÉES NE SONT PAS MEILLEURES SUR LE WEB

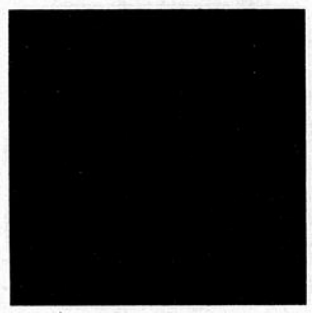


Fig. 1. Veilleuse à l'énergie solaire

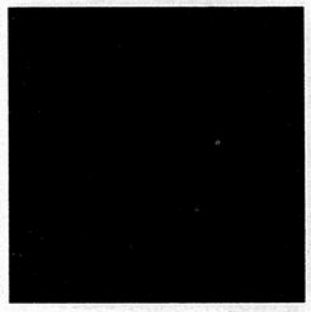


Fig. 2. www.veilleusesolaire.com

Les déboires des point-com nous ont appris que les principes de base des affaires n'ont pas changé, même sur Internet. C'est pourquoi des milliers d'entreprises, petites et grandes, travaillent avec IBM pour améliorer leurs processus d'affaires, interconnectant leurs clients, partenaires et employés sur le Web. Ces entreprises allient à leur stratégie d'affaires une solide infrastructure d'affaires électroniques. Avec IBM et ses partenaires commerciaux, vous aussi pouvez découvrir de nouvelles façons rentables de faire des affaires. Vous pourriez ainsi accroître la satisfaction de votre clientèle ou obtenir une réduction du coût des transactions pouvant aller jusqu'à 75 %. Rendez-vous à www.can.**ibm.com**/affaires_electroniques/eb109 ou composez le **1 800 IBM-7080, poste eb109.**

ÉTUDE DE CAS CRM : Clearwater Fine Foods Les conseillers en affaires IBM ont travaillé avec cette entreprise de fruits de mer afin d'améliorer ses processus de gestion des relations avec la clientèle. Grâce à un logiciel CRM de Siebel[MD] Systems, un partenaire commercial d'IBM, il est possible d'accéder en ligne à des historiques clients consolidés. Résultat : moins de papier, une productivité accrue pour les ventes et plus de réactivité aux besoins des clients.

IBM[MD]

@ infrastructure d'affaires électroniques

B-16