

dossiers

Technologies : transactions électroniques sécurisées



TRANSACTIONS ÉLECTRONIQUES

Les questions à se poser

> Sur quel expert allez-vous vous appuyer pour faire des affaires en ligne ? Disposez-vous d'un « parrain », reconnu pour son expérience technologique, qui pourrait vous informer ?

> Renseignez-vous sur les différents fournisseurs possibles. Appelez leurs clients actuels.

> D'autres ont sûrement déjà des activités semblables aux vôtres sur le Web. Comment s'y prennent-ils ?

EN CHIFFRES

Les principales causes des pertes de données

Une attaque informatique sur trois vient de l'intérieur de l'entreprise et résulte d'une fausse manœuvre de la part d'un employé.

22%

des institutions financières n'ont offert aucune formation sur la sécurité à leurs employés au cours de la dernière année.

30%

Proportion des entreprises estiment que leurs employés disposent des compétences nécessaires pour faire face à des problèmes de sécurité.

Source : Deloitte Touche Tohmatsu, septembre 2007



Jean-Sébastien Bilodeau, de Victrix : « Tout gestionnaire devrait se demander quels sont les risques acceptables pour son entreprise. » [Photo : Gilles Delisle]

La sécurité absolue n'existe pas

Commerce. Protéger ses transactions électroniques, c'est réduire le risque.

par Didier Bert > dossiers@transcontinental.ca

Nombre d'entreprises accroissent leurs échanges électroniques tout en restant inquiètes quant à la sécurité de leurs transactions. Et elles ont raison. « La sécurité parfaite n'existe pas. Il faut plutôt avoir une gestion des risques, afin de pouvoir les accepter », dit Lise Lapointe, présidente de Formation Terra Nova, une entreprise active dans la sécurité de l'information.

« La confiance prend une place prépondérante dans une démarche de transactions interentreprises, considère Claude Vigeant, président d'Okiok, une entreprise spécialisée dans la sécurité de l'information et de l'authentification. La barrière entre les entreprises doit être aussi invisible qu'étanche, par exemple lorsqu'un fournisseur entre dans votre système pour établir la paie et la gestion des carrières de vos employés. »

« Tout gestionnaire devrait se demander quels sont les risques acceptables pour son entreprise », croit pour sa part Jean-Sébastien Bilodeau, responsable de la sécurité pour Victrix, des consultants en sécurité informatique.

Ce qui sera acceptable pour une entreprise ne le sera pas forcément pour une autre, explique-t-il. « Peut-on tolérer que le système tombe en

panne cinq minutes pendant la nuit ? Oui, pour certaines PME, non, pour d'autres. »

Plus tôt cette année, Bell Canada s'est aperçu que certaines de ses données avaient été volées. Les informations étaient apparemment sans valeur pour un particulier. Le malfaiteur les vendait 2 500 \$. Mais elles valaient une fortune pour la concurrence, précisait Bell dans sa demande d'injonction. Le fichier volé aurait intéressé encore plus des entreprises de télémarketing spécialisées dans l'envoi de courriels non sollicités.

« La sécurité infaillible, ça n'existe pas. C'est utopique. C'est encore plus dangereux que de penser qu'on n'est pas sécuritaire », soutient Michel Bouchard, conseiller principal en sécurité de l'information chez ESI Technologies. « Le seul ordinateur sûr est un ordinateur vide. On doit viser décourager 99,9 % de la population d'obtenir des informations confidentielles. »

La sécurité a une valeur différente selon chaque organisation, note Luc Poulin, conseiller senior en sécurité à

Briser le mythe

« Je parle de gestion de risques avec mes clients. Je leur demande quels risques ils ont identifiés pour leur domaine d'affaires. Qu'est-ce qui peut leur arriver ? C'est en étant conscient des risques qu'on peut bloquer l'accès à des informations sensibles. »

Les problèmes de sécurité relèvent ainsi davantage de problèmes de gestion, sur lesquels l'entreprise doit se pencher avant de se lancer dans les transactions électroniques. Le gestionnaire devrait ainsi se questionner sur sa raison de

faire des affaires en ligne. « Avec qui l'entreprise va-t-elle traiter ? Quel est le lien de confiance entre les parties ? » interroge M. Bilodeau.

« Il n'y a pas de ligne entre la sécurité et l'insécurité, c'est un mythe qu'il faut casser, estime Luc Poulin, conseiller senior en sécurité à l'Institut de la sécurité de l'information du Québec (ISIQ). L'important, c'est d'arriver à dormir sur ses deux oreilles, en ayant limité les risques à un niveau suffisamment bas. »

M. Poulin raconte l'histoire d'une entreprise de dévelop-

pement de logiciels sur mesure. Un client prêt à acheter l'application l'avertit des conséquences s'il découvrirait qu'une information avait été volée en raison d'une faille de son logiciel. « Tu perdras ta compagnie, ta maison et ton automobile », dit le client. « Veux-tu toujours me vendre ton logiciel ? »

Dans ce domaine, le rendement de l'investissement ne se mesure pas. « C'est comme une assurance. Le but d'une entreprise n'est pas de sécuriser ses applications, mais de faire des affaires », dit M. Poulin. ■

Surtout, ne pas se croire à l'abri

l'Institut de la sécurité de l'information du Québec (ISIQ).

La sécurisation des transactions, oui, mais à quel prix ? Attention à ne pas payer l'assurance de votre voiture plus cher que la voiture elle-même, illustre M. Poulin. Il suggère de s'équiper en fonction des besoins de l'entreprise, pas plus. Tout dépend du contexte d'affaires. Pour Bell, il est normal de trouver la liste de ses clients sur Internet. Pour des entreprises actives dans le secteur de la santé, par exemple, cette stratégie mènerait à la faillite.

Les axes de la sécurité

La sécurité n'est pas qu'une affaire de confidentialité des informations. Les experts voient deux autres domaines dans lesquels la sécurité peut être menacée : l'intégrité et la disponibilité. Le système devrait être intègre, c'est-à-dire que les données entrées dans la transaction sont celles que le destinataire reçoit. « Si vous faites des transactions avec une entreprise située en Malaisie, enregistrer les données dans un journal permettra de savoir si elles ont toutes été trans-

mises », explique Jean-Sébastien Bilodeau, de Victrix.

L'autre secteur à risque est celui de la disponibilité, qu'on pourrait définir comme la possibilité d'avoir accès aux informations. Si une attaque mobilise les ressources du système pour se défendre, elles risquent de ne plus être disponibles pour servir la clientèle, entraînant une perte de revenus. Les conséquences de l'indisponibilité du système peuvent être aussi graves qu'une fraude ou que le piratage de la base de données. **D.B.**

Prioriser l'humain avant la technologie

Conseils. La sécurité passe par la maîtrise du risque humain, avant même tout risque technologique.

par Didier Bert > dossiers@transcontinental.ca

L'importance de l'être humain dans la sécurité informatique a été comprise le 11 septembre 2001. « Ce jour-là, des êtres humains ont déjoué des systèmes de sécurité perfectionnés », rappelle Jean-Sébastien Bilodeau, responsable de la sécurité chez Victrix, une entreprise spécialisée en sécurité informatique.

Les techniques de piratage ont beaucoup évolué. « Les malfaiteurs possèdent de véritables caisses à outils, pas seulement technologiques », dit M. Bilodeau. Ils portent de plus en plus leurs attaques sur l'élément humain des organisations. « Une organisation comme la NASA tente de retirer l'humain du processus, car c'est le maillon le plus faible. Mais on ne peut pas le retirer complètement.

« Quand quelqu'un vous téléphone, si vous ne le connaissez pas, que faites-vous avant de lui donner des informations confidentielles ? donne en exemple l'expert en sécurité. Si on n'a pas sensibilisé le personnel au risque que comporte le fait d'envoyer une liste de clients par courriel, pourquoi ne le ferait-il pas ? »

La sécurité n'est pas forcément où on l'attend. Une personne mal intentionnée n'a pas besoin d'attaquer le système de sécurité d'une organisation quand les informations sont accessibles dans les fiches personnelles des employés sur les réseaux sociaux de Facebook, MySpace ou LinkedIn. « Pour le malfaiteur, c'est un vrai buffet d'informations ! » En février, le ministère canadien de la Défense a ainsi conseillé aux soldats de ne pas diffuser d'informations sur Facebook. Le gouvernement craignait qu'Al-Qaida s'en serve pour mener des attaques contre les troupes canadiennes en Afghanistan.

« On doit former les utilisateurs aux bonnes pratiques pour préserver l'information d'entreprise », souligne Lise Lapointe, présidente de Formation Terra Nova, une entreprise spécialisée en sécurité de l'information.

La sécurité de l'information ne se limite pas à Internet, dit-elle. Lise Lapointe cite la politique du bureau bien rangé. « Quand vous quittez votre bureau, laissez-vous votre ordinateur, une clé USB ou votre agenda posés sur votre bureau, à la portée du premier visiteur venu ? »



Luc Poulin, de l'Institut de la sécurité de l'information du Québec : « N'importe qui peut se prétendre spécialiste en informatique, Renseignez-vous ! » [Photo : Martin Martel]

Redéfinir l'accès aux données

« Dans un contexte de transactions interentreprises, l'entreprise doit mettre en œuvre une bonne gestion des accès », suggère Claude Vigeant, président d'Okiok, une firme spécialisée en sécurité de l'information et en authentification. « Dans le B2B, on ouvre nos systèmes à nos partenaires, clients ou fournisseurs. Mais on ne connaît pas forcément les employés de ces partenaires. Sont-ils toujours à leur

emploi ? » Cette information doit être tenue à jour.

De plus en plus, la tendance est de désigner des administrateurs chez l'entreprise partenaire, qui gèrera elle-même les accès. « Aujourd'hui, on crée des fédérations d'identités, précise Claude Vigeant. Les entreprises passent une convention entre elles. Les utilisateurs s'identifient sur leur réseau local, ce qui les autorise ensuite à accéder aux réseaux des entreprises partenaires. »

Pour Luc Poulin, conseiller

En février, le ministère canadien de la Défense a conseillé aux soldats de ne pas diffuser d'informations sur Facebook.

senior en sécurité à l'Institut de la sécurité de l'information du Québec (ISIQ), les risques humains viennent aussi des informaticiens eux-mêmes, qu'ils soient ingénieurs ou

techniciens. L'expert rappelle qu'il n'existe pas d'ordre professionnel des informaticiens au Québec. « N'importe qui peut se prétendre spécialiste en informatique, affirme-t-il. Renseignez-vous ! Qui a développé le logiciel que vous vous apprêtez à utiliser ? Si on vous répond : *des informaticiens*, vérifiez leurs qualifications et leur expérience. Demandez des références. »

« Les preuves que vous demandez dépendent de ce qui est important dans votre

contexte d'affaires », précise M. Poulin.

Après l'humain, Luc Poulin pointe une autre source de risque : les processus. « Si la méthode n'est pas correcte, il y aura un problème à un certain moment », dit-il.

Et la technologie ? L'expert la classe au dernier rang des dangers. « Elle peut être défailante. On doit savoir ce qu'elle fait, et ce qu'elle ne fait pas. La technologie n'est pas un facteur négligeable, mais ce n'est pas le plus important. » ■

Protéger les revenus de l'entreprise avant tout

Règlementation. Avant de faire des affaires en ligne, il faut connaître les risques et les obligations juridiques.

Tout gestionnaire compétent doit se demander à quels risques l'entreprise sera exposée dès qu'elle fera des affaires en ligne. Le principal danger qui guette les organisations est la perte de revenus, en raison des menaces qui pèsent sur leur réputation et des possibilités de poursuites judiciaires.

« Sécurisez vos transactions pour éviter de perdre des revenus », conseille Luc Poulin, conseiller senior en sécurité à l'Institut de la sécurité de l'information du Québec (ISIQ).

« Pour un individu, la sécurité, c'est préserver son intégrité physique. Pour une entreprise, c'est l'intégrité financière qui est en jeu », résume celui qui est co-auteur d'une norme internationale

sur la sécurité des applications qu'il présentera au Japon dans quelques jours.

La relation d'affaires virtuelle est plus difficile à sceller que la vente, rappelle pour sa part Claude Vigeant, président d'Okiok, une société spécialisée dans la sécurité de l'information et l'authentification. On sait qu'il y a un pourcentage de transactions frauduleuses parmi les ventes conclues sur eBay, dit-il. Si la vente concerne de la propriété intellectuelle, il est très difficile de contrôler la distribution ultérieure. Il faut alors mettre en place des protections logicielles telles que la gestion numérique des droits (DRM) pour les fichiers artistiques numériques.

Le pire n'est pas forcément le vol d'un numéro de carte de crédit. « Souvent, les pirates s'emparent d'un procédé de fabrication pour pouvoir ensuite copier les produits », estime Lise Lapointe, présidente de Formation Terra Nova.

La sécurité imposée par les lois

Cette spécialiste rappelle les risques légaux que prennent les entreprises laxistes en matière de sécurité informatique. Au Canada, la loi 198 exige de toute entreprise qu'elle assure la fiabilité, l'intégrité et la disponibilité de son information financière. Les responsables de la société doivent pouvoir démontrer les

Au Canada, la loi 198 exige de toute entreprise qu'elle assure la fiabilité, l'intégrité et la disponibilité de son information financière.

moyens mis en œuvre pour cela. La loi prévoit jusqu'à 10 ans de prison pour les fautifs. La loi 198 pourrait être comparée à la loi américaine Sarbanes-Oxley aux États-Unis. La Loi sur la protection des renseignements personnels et des documents électroniques impose aux entreprises non réglementées, quelle que soit leur taille, de protéger les

renseignements personnels et les documents électroniques en leur possession.

La perte de données concernant la clientèle peut nuire à la réputation d'une entreprise. Les conséquences peuvent mettre en danger les revenus de celle-ci.

Le Québec a une loi de protection des données personnelles, ajoute Luc Poulin. Celle-ci diffère de celle de l'Ontario et de celles des autres provinces, précise-t-il.

Les PME sont souvent moins conscientes des risques que les grandes entreprises. Les banques, habituées à être attaquées, en sont déjà à leur troisième génération de protection, souligne Claude Vigeant. **D.B.**



L'IMPORTANCE DE S'AFFICHER SUR LE WEB Internet est devenu un outil traditionnel du commerce interentreprise

Près d'un ingénieur sur deux passe plus de six heures par semaine sur Internet pour trouver de nouveaux produits et fournisseurs. La recherche se fait d'abord sur des moteurs de recherche (49 %), des répertoires spécialisés en ligne (17 %) et des sites d'entreprises (12 %).

Source : GlobalSpec, 2007

dossiers transactions électroniques sécurisées



EN HAUSSE

Beaucoup d'échanges

Les ventes interentreprises représentent plus du double des ventes aux particuliers.

Source : Statistique Canada, 2007

Sécuriser ses transactions électroniques en trois étapes

1 N'agissez pas par peur. Commencez par vous informer, pour prendre conscience des risques, les définir et les gérer.

2 Appelez votre assureur. Demandez-lui si les risques, une fois que vous ferez des transactions en ligne, sont couverts.

3 Ayez des experts dans chaque domaine. S'ils sont compétents, demandez-leur des références d'experts dans d'autres domaines.

La sécurité reste toujours à bâtir

Conseils. Il faut revoir périodiquement la stratégie de sécurité et vérifier qu'elle est appliquée.

par Didier Bert > dossiers@transcontinental.ca

Il n'y a pas un instant où un système est sécuritaire. « C'est une remise en question continue, souligne Jean-Sébastien Bilodeau, responsable de la sécurité chez Victrix, une entreprise spécialisée en sécurité informatique. Un système est sécuritaire quand on en a régulièrement le contrôle. »

La formation doit être permanente et continue, affirme Lise Lapointe, présidente de Formation Terra Nova, une entreprise spécialisée en sécurité de l'information. « Les comportements à risque doivent être modifiés. »

M^{me} Lapointe suggère de prioriser un plan de communication, avec des affiches, des bandes dessinées ou des vidéos. « Le personnel doit être en mesure de reconnaître un comportement à risque. On doit souvent répéter ce qu'il faut faire et ce qu'il faut éviter. Les gens ont tendance à revenir à leurs habitudes. » L'enjeu est d'en créer de nouvelles, plus sécuritaires.

L'entreprise devrait se doter d'une politique en cette matière, afin de donner un sens à la sécurité de l'entreprise, et de pouvoir s'y référer



Lise Lapointe, de Formation Terra Nova : « Les comportements à risque doivent être modifiés. » [Photo : Gilles Delisle]

régulièrement, recommande Michel Bouchard, conseiller principal en sécurité de l'information chez ESI Technologies. Ce document, qui détaille la stratégie de sécurité de l'entreprise, devrait être revu chaque année, et entériné par le conseil d'administration, explique M. Bouchard.

Déceler les nouveaux risques

« La politique de sécurité doit prévoir les risques tout en tenant compte des besoins

d'affaires de l'entreprise. Il ne s'agit pas de tuer une mouche avec un fusil à éléphant. »

La politique de sécurité exprime les besoins légaux de conformité et d'éthique. L'entreprise peut modifier sa politique en cette matière afin de s'adapter aux situations, comme l'installation d'une application logicielle.

De son côté, Luc Poulin est d'avis que l'entreprise devrait partager sa responsabilité avec le fournisseur d'applications. « Demandez des preuves

à votre prestataire, dit-il. Faire des affaires sur Internet apporte de nouveaux risques à l'organisation. Le fournisseur doit avoir identifié ces risques avant de mettre en place son application. »

Par exemple, si la confidentialité n'est pas suffisante, on peut envisager de chiffrer les informations.

Il faudra ensuite vérifier que le protocole de chiffrement fonctionne. Pour réaliser cet audit, M. Poulin recommande de faire appel à une

tierce partie. « Vous devez savoir si cette nouvelle application que vous allez utiliser présente suffisamment de garanties pour votre entreprise. »

Une chose est sûre : la mise en place de technologies et de processus de sécurité n'est pas faite une fois pour toutes. « N'abandonnez pas votre sécurité aux mains de votre prestataire externe. Travaillez avec lui. Vous devez comprendre ce qu'il fait », mentionne Jean-Sébastien Bilodeau. ■

La confidentialité, un enjeu non négociable

Étude de cas. Le vol de données serait une catastrophe pour l'Ordre des conseillers en ressources humaines.

L'Ordre des conseillers en ressources humaines (ORHRI) s'est lancé dans le projet de sécuriser son site Web en 2003. « Nous voulions être certains que l'information de nos membres était en lieu sûr », raconte Bruno Dupuis, chef des solutions et publications en ligne de l'ORHRI. Il était hors de question que la base de données des membres soit accessible à des personnes non autorisées, qui pourraient ainsi consulter les mesures disciplinaires prises à l'égard de certains membres ou d'autres données personnelles. « Ce serait une catastrophe si cela arrivait », juge Florent Francoeur, président de l'Ordre.

L'ORHRI traite 90 % de ses transactions grâce à son site Internet. Les membres comme le grand public peuvent acheter des livres ou s'inscrire à des cours de formation. On peut aussi s'en servir pour

déposer une plainte. Les membres ont accès à certains formulaires et aux offres d'emploi. Les revenus transitant par le site constituent plus de la moitié du budget de l'Ordre.

L'organisation a lancé un appel d'offres pour trouver une solution de sécurisation de sa base de données. L'Ordre a fait ses devoirs en demandant à ses partenaires habituels de lui recommander des collaborateurs fiables.

Savoir imposer ses exigences

Finalement, c'est Fusepoint qui a obtenu le contrat. « Nous leur avons demandé de respecter les normes de l'industrie, mais aussi de respecter nos normes à nous », relate Bruno Dupuis. L'Ordre voulait absolument conserver une copie de sa base de données dans un coffre, dans ses locaux. Celle-ci devait être mise à jour men-

Comme la sécurité des transactions électroniques n'est pas qu'une affaire de technologie, l'aspect humain a également été pris en compte. Les mots de passe sont changés chaque mois.

suellement. Même si cette exigence n'était pas prévue au départ, l'Ordre n'a pas cédé. Elle a eu gain de cause.

Aujourd'hui, le site Web est-il suffisamment sécurisé ? Citant le dicton *À l'impossible, nul n'est tenu*, Florent Francoeur répond qu'« on veut pouvoir dire qu'on a vraiment fait le maximum, qu'on est allé au-delà des normes usuelles ».

L'Ordre a ainsi commandé un audit à Victrix, spécialisée

dans la sécurité de l'information. Les experts de la firme montréalaise ont ainsi testé la sécurité du site en l'attaquant. Littéralement. Le rapport d'audit, satisfaisant au dire de Florent Francoeur, permettra d'apporter de petits correctifs. « On l'améliore constamment. Ce n'est jamais fini », assure-t-il.

Comme la sécurité des transactions électroniques n'est pas qu'une affaire de technologie, l'aspect humain a également été pris en compte. Les mots de passe sont changés chaque mois. Le risque d'erreur humaine doit être réduit le plus possible, selon Bruno Dupuis. Les employés de l'Ordre doivent ainsi lire et signer la politique de mesures de sécurité de l'organisation. « Il faut faire en sorte que la personne ne soit pas mise en situation de négligence », résume le responsable. **D.B.**

Pour dirigeants d'entreprises technologiques

"ROUTES TO MARKET"

ou comment choisir la bonne voie pour rejoindre ses clients et croître plus rapidement



6^e édition

Forum Ventes et Marketing pour les TIC
29-30 avril 2008 au Château Bromont

Conférences et ateliers sur les meilleures pratiques en commercialisation, rencontres et réseautage avec des partenaires potentiels

Une présentation de



Information
tél. : (514) 874-2667
www.lebigbang.net