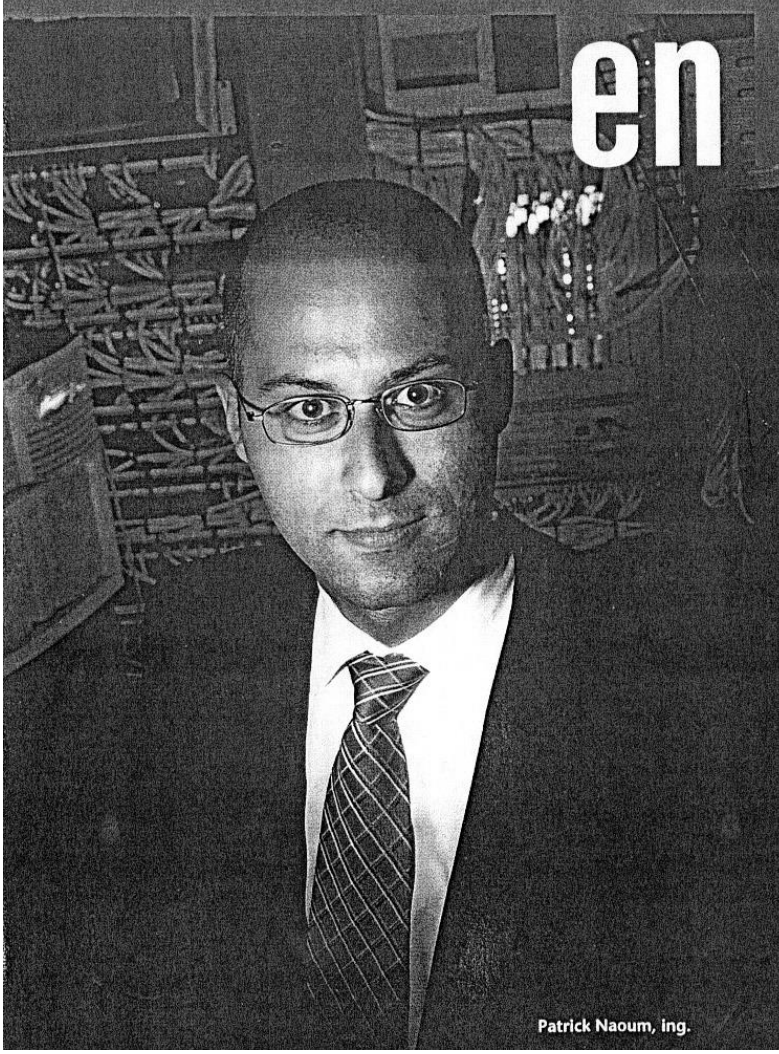
SHC
Simard Hamel Communications ltée
465, rue St-Jean, bureau 401, Montréal (Québec) H2Y 2R6
Tél. : (514) 287-9811 Téléc. : (514) 287-9859

Plan, août-septembre 2003
Tirage : 49 144
Lu en page 21,22 et 23
Page 1 de 3

Pendant que des concurrents se concentraient sur le bogue de l'an 2000, une PME montréalaise est devenue l'une des rares entreprises au Canada spécialisée en sécurité informatique.

PAR JEAN-MARC PAPINEAU

Sécurité en tête



Patrick Naoum, ing.

Yves Médam

« Les violations de sécurité sont plus courantes qu'on ne le croit généralement », affirme l'ingénieur Patrick Naoum, vice-président Technologies et Services professionnels de ESI Technologies. Cette PME montréalaise de 125 employés se présente comme l'une des rares entreprises au Canada à offrir des services technologiques complets incluant notamment le développement, l'implantation et la gestion de systèmes de sécurité.

« Le péril en matière de sécurité informatique est grand et il va en s'accroissant, enchaîne Patrick Naoum. Depuis l'avènement d'Internet, tout le monde est branché, mais ce n'est pas tout le monde qui donne priorité à la sécurité informatique dans ses choix technologiques. Nombre d'entreprises tardent à évaluer leurs besoins pour sécuriser leurs données et leurs réseaux. Certaines ont même tendance à attendre qu'une catastrophe se produise avant d'agir. De plus, en raison de la nécessité de rapides mises à jour qu'exige l'environnement compétitif de l'industrie, les logiciels sont parfois de moindre qualité et donc, plus vulnérables. Ajoutons la sophistication croissante

SHC
Simard Hamel Communications ltée
465, rue St-Jean, bureau 401, Montréal (Québec) H2Y 2R6
Tél. : (514) 287-9811 Téléc. : (514) 287-9859

Plan, août-septembre 2003
Tirage : 49 144
Lu en page 21,22 et 23

des pirates informatiques, et la situation ne va pas nécessairement en s'améliorant dans l'ensemble. Par contre, il y a de l'espoir car il existe des moyens efficaces de sécuriser les réseaux informatiques. »

Diplômé en génie informatique de l'École Polytechnique de Montréal en 1997, Patrick Naoum est entré au service de ESI Technologies dès la fin de ses études. Depuis 1999, il est un des trois actionnaires de cette entreprise fondée en 1994 à la suite du rachat par la direction actuelle de Econocom Canada, une filiale d'un consortium européen spécialisée en financement et en acquisition de systèmes informatiques. « C'est le meilleur des mondes pour moi, dit Patrick Naoum. J'ai toujours eu des velléités d'entrepreneur, mais je n'étais pas prêt à l'époque à courir le risque de me lancer moi-même en affaires. Quand j'ai débuté ici, tout était à faire et si je réussissais à faire mes preuves, je pouvais progresser rapidement au sein de l'entreprise. »

C'est ce qui s'est produit. Le premier mandat que ESI Technologies confie à Patrick Naoum consiste à bâtir un cabinet de services professionnels en technologies de l'information. Ce défi, Patrick Naoum l'a relevé haut la main : les services-conseils et d'implantation de solutions de sécurité ont connu une hausse de 40 % au cours des trois dernières années sous sa direction, produisant des revenus de plus de huit millions de dollars annuellement, soit presque le quart du chiffre d'affaires total de l'entreprise. À ce jour, parmi les quelque 1 200 clients de ESI Technologies, environ 200 ont fait appel à l'expertise de l'entreprise en matière de sécurité informatique.

Peu d'entreprises canadiennes peuvent se targuer comme ESI Technologies d'offrir des services intégrés en sécurité informatique. « La sécurité en matière de micro-informatique a commencé à être un objet de préoccupation à la fin de 1998, précise Patrick Naoum. Pendant que d'autres se concentraient sur le bogue de l'an 2000, nous avons investi continuellement pour offrir de plus en plus de services, notamment en faisant une série d'acquisitions pour accélérer notre implantation dans le secteur de la sécurité informatique. C'est ce qui explique que nous sommes toujours en vie et en bonne santé financière. Et comme il y a eu beaucoup de consolidations dans notre secteur, il existe de moins en moins d'entreprises comme nous dédiées à la sécurité informatique. » Entre 1996 et 2001, ESI Technologies a ainsi fait pas moins de neuf acquisitions, et elle entend poursuivre sa croissance jusqu'ici constante en faisant d'autres acquisitions stratégiques.

Patrick Naoum a développé une expertise en sécurité informatique au cours des dernières années que peu d'ingénieurs québécois possèdent. Pourtant, au départ, il visait le génie mécanique. « Mon grand rêve était de travailler dans l'industrie aérospatiale, particulièrement à la NASA, et le meilleur chemin pour atteindre ce but était le génie mécanique », dit-il. Il s'inscrit donc dans cette discipline, mais se réoriente en génie informatique à la suite d'une rencontre déterminante avec un professeur ayant une formation de base en génie mécanique et qui, après avoir travaillé pour la NASA, avait complété un doctorat en génie informatique. « J'ai compris que le génie informatique pouvait m'ouvrir d'autres portes tout en me laissant la possibilité de concrétiser un jour mon rêve », poursuit-il. Aujourd'hui, la sécurité informatique a pris le dessus et l'aérospatiale est devenu un passionnant passe-temps.

Durant ses études, Patrick Naoum siège au Comité de génie informatique de l'École Polytechnique de Montréal à titre de vice-président et directeur des relations corporatives. « J'ai toujours cru très important de me garder au courant des tendances, surtout dans une industrie qui bouge aussi vite que celle de l'informatique, explique-t-il. Grâce à cette expérience, je me suis familiarisé avec le marché de la sécurité informatique, je me suis fait connaître et j'ai créé des liens avec différentes entreprises. C'est ainsi que j'ai obtenu un stage chez Microsoft Canada. Jusqu'alors, je n'avais aucune idée de ce que je ferais dans le domaine du génie informatique. Tout au plus, j'avais un penchant pour la robotique et l'intelligence artificielle. Le stage m'a permis de découvrir les services-conseils en informatique. »

> « Des failles de sécurité ont des répercussions qui vont au-delà des problèmes causés par l'introduction de virus. Elles peuvent provoquer un arrêt prolongé des systèmes et paralyser l'entreprise tout entière. »

Si les pirates informatiques perfectionnent sans cesse leurs moyens, il en va de même des spécialistes de la sécurité. « Il y a eu une grande évolution technologique au cours des cinq dernières années, note Patrick Naoum, principalement en raison de l'uniformisation des standards de sécurité depuis l'an 2000 relativement aux protocoles de réseaux et de communications. Déjà, un équipement seul peut être vulnérable ; imaginez à quel point la situation peut devenir infernale avec des équipements disparates qui, de surcroît, ne communiquent pas bien ensemble. Il existe également des normes internationales qui permettent d'encadrer rigoureusement une démarche de sécurisation. La plus connue est la norme ISO 17799 qui contient tous les éléments pour établir une solide politique de sécurité. »

À ce mouvement d'uniformisation s'ajoute l'apparition d'outils de plus en plus performants basés notamment sur l'intelligence artificielle. « Nous disposons de meilleurs outils, comme les logiciels de détection d'intrusions qui permettent, grâce à des algorithmes sophistiqués, de repérer les attaques », mentionne Patrick Naoum, lui qui connaît bien toute la panoplie des logiciels antivirus, des systèmes d'authentification, de cryptage et d'infrastructures à clés publiques, des systèmes de filtrage de courriels, des pare-feu et des logiciels et systèmes redondants.

Les menaces à la sécurité informatique ne sont pas toujours le fait de pirates informatiques, loin de là. « Pas moins de 70 % des atteintes portées à la sécurité des ordinateurs proviennent en réalité de l'intérieur des organisations et au moins la moitié de ces violations sont le fait de personnes

SHC
Simard Hamel Communications ltée
465, rue St-Jean, bureau 401, Montréal (Québec) H2Y 2R6
Tél. : (514) 287-9811 Téléc. : (514) 287-9859

Plan, août-septembre 2003
Tirage : 49 144
Lu en page 21,22 et 23

mal intentionnées. Or, il est beaucoup plus compliqué et coûteux de sécuriser un réseau de l'intérieur, car les systèmes doivent être accessibles aux usagers, indique Patrick Naoum. Un autre mythe : les risques en sécurité ne sont pas tant le vol des données que la disponibilité des services. Des failles de sécurité peuvent avoir des répercussions qui vont bien au-delà des problèmes causés par l'introduction de virus ou des copies illégales. Elles peuvent provoquer un arrêt prolongé des systèmes et paralyser l'entreprise tout entière, ce qui peut engendrer des pertes faramineuses. »

Bien que les grandes entreprises constituent des proies plus tentantes pour les pirates informatiques, les plus petites sont également vulnérables. « Quand nous travaillons avec les PME, nous avons un rôle d'éducation à jouer avant la vente, dit Patrick Naoum. Les grandes entreprises sont davantage sensibilisées à la sécurité informatique, mais leur problème est de savoir quoi implanter, comment et à quel coût. À cet égard, les attentats du 11 septembre 2001 ont modifié les priorités des grandes entreprises. Même la pneumonie atypique qui a sévi plus tôt cette année à Toronto a eu un impact. Des clients nous ont demandé d'implanter des centres de relève équipés d'accès à distance au cas où leurs hauts gestionnaires seraient mis en quarantaine. »

En matière de sécurité informatique, les aspects humains, organisationnels et financiers représentent les véritables enjeux. « Sur le plan technologique, les défis sont certes relativement complexes, mais jamais insurmontables : il y a toujours un outil disponible ou un compromis viable, dit d'expérience Patrick Naoum. Le maillon faible est l'humain. Il faut s'assurer que l'employeur met les bonnes personnes en place, qu'il leur alloue suffisamment de temps pour se soucier de la sécurité et qu'il informe ses employés des mesures de sécurité. Nombre d'entreprises installent, par exemple, des coupe-feu de toutes sortes en croyant obtenir une protection adéquate, mais elles négligent d'expliquer le rôle de chaque employé dans le processus de sécurisation. »

Toute implantation d'un processus de sécurité se déroule en trois phases : la prévention, la surveillance et la réaction. « La prévention consiste à installer les outils technologiques, comme les logiciels antivirus, dont se dote une entreprise pour retarder une violation de ses systèmes informatiques, explique Patrick Naoum. La surveillance est assurée par les registres d'événements et les rapports d'activité des serveurs. À cet égard, beaucoup d'entreprises mettent trop l'accent sur la prévention et pas assez sur la surveillance qui requiert des investissements en ressources humaines. La réaction consiste à mettre en place les mesures à prendre en cas d'incident, mesures qui devraient normalement être établies lors de l'élaboration de la politique de sécurité. »

Bientôt, les entreprises n'auront plus le choix de se préoccuper de sécurité informatique. « Il s'agit déjà d'une exigence pour pouvoir faire affaire avec certaines institutions bancaires et compagnies d'assurances, signale Patrick Naoum. Les entreprises doivent se préparer à évoluer dans des cadres réglementaires et légaux en cette matière. Par exemple, les États-Unis ont adopté la norme HIPAA qui établit des règles de fonctionnement dans le secteur de la santé, et ça s'en vient ici. » ◆