



Photo: Michel Larivière

La sécurité en **TGV** avec **Patrick Boucher**

PROPOS RECUEILLIS PAR **SAMUEL BONNEAU**

Patrick Boucher est diplômé de l'UQAM en informatique. Il est président fondateur de l'entreprise Gardien Virtuel et il se décrit comme un passionné de l'informatique et de la sécurité informatique (SI).



Suite en page 7

QUEL EST VOTRE PARCOURS PROFESSIONNEL ?

Quand j'ai touché à mon premier IBM, j'ai tout de suite été attiré par l'informatique. Je travaille dans ce domaine depuis ce temps, et ce, presque toujours en tant que travailleur autonome.

Dès mes quinze ans, je vendais du matériel informatique. Un peu plus tard, j'ai été embauché par IBM comme technicien informatique de deuxième niveau. Par la suite, et jusqu'en 2003, j'ai travaillé pour quelques compagnies de consultation œuvrant en SI. Puis, j'ai accompli un rêve d'enfance en fondant ma propre entreprise. Gardien Virtuel a vu le jour le 1^{er} janvier 2003.

QUELLES CARACTÉRISTIQUES VOUS DÉCRIVENT LE MIEUX EN TANT QUE GESTIONNAIRE ?

J'aime jouer le rôle du général et aller à la guerre avec mon équipe. Je sais que nous avons les ressources et l'expertise pour nous battre dans notre marché, donc nous présentons avec confiance nos offres de services, peu importe le contrat. Concrètement, je fais encore moi-même des mandats et j'aime beaucoup pouvoir me « salir » les mains. Parfois, c'est à titre de gestionnaire de projet et, d'autres fois, c'est à titre d'analyste.

Je suis passionné et persévérant. Je ne me décourage jamais. Bâtir une entreprise et une équipe de qualité n'est pas chose facile, mais j'adore le faire et j'y consacre beaucoup d'énergie. Prenons l'exemple de l'embauche des employés. C'est très important pour moi de prendre le temps qu'il faut pour faire de bons choix. Je souhaite bâtir une équipe qui travaille avec efficacité, cohésion et plaisir. J'aime participer aux entrevues de candidats potentiels et écouter les conseils de notre nouvelle directrice des ressources humaines, Valérie Vézina. Après tout, nous allons passer quarante heures par semaine les uns avec les autres, alors, c'est important que nous nous amusions et que nous avançons ensemble.

GARDIEN VIRTUEL

QUELLE EST LA MISSION DE GARDIEN VIRTUEL ?

Nous avons fait des trois piliers de la SI notre mission, soit aider nos clients à augmenter la disponibilité, l'intégrité et la confidentialité de leurs données.

QUELLE EST VOTRE OFFRE ?

Nous œuvrons principalement sur le plan tactique. Ce dernier constitue environ 60 % de nos contrats. La part stratégique est de 30 % et le côté opérationnel est de 10 %. Nous ne revendons aucun produit. C'est une question de

neutralité dans nos recommandations. Cette transparence est très importante pour nous.

« Nos principaux services sont les tests de sécurité (aussi bien des réseaux que des applications), les audits, les enquêtes juridico-informatiques et la création de plans directeurs. De plus, nous effectuons souvent des mandats de gouvernance. »

QUEL EST VOTRE MARCHÉ ?

Ma prémisses est d'offrir des services professionnels à toute entreprise souhaitant améliorer sa sécurité informatique. Notre grande flexibilité nous permet de combler les besoins de la très petite à la très grande entreprise, et ce, peu importe le secteur d'activité. Parmi nos clients, nous retrouvons la Bourse de Montréal, la Commission de la construction du Québec, le Centre de santé et de services sociaux Pierre-Boucher, pour ne nommer que ceux-là.

QU'EST-CE QUI VOUS DIFFÉRENCIE DE LA CONCURRENCE ?

Notre élément le plus distinctif est clairement notre ISO 27001. De plus en plus d'entreprises canadiennes obtiennent la certification, mais Gardien Virtuel sera toujours la première firme de services-conseils en sécurité à l'avoir obtenue au pays.

Peu de gens le savent, mais Gardien Virtuel possède une grande équipe en recherche et développement. Nous avons la chance d'avoir des employés possédant des doctorats en informatique qui développent des méthodologies et des outils que nous utilisons tous les jours. D'ailleurs, depuis 2006, c'est cette même équipe qui a mis sur pied la télésurveillance de Gardien Virtuel (TGV). Je suis très fier de dire que tous nos projets, incluant la TGV, ont été financés à l'interne, ce qui nous donne une approche systémique qui nous permet de nous différencier de la concurrence. Lorsqu'un client nous demande d'approfondir un dossier, il peut être certain que nous irons jusqu'au bout.

QUELS ONT ÉTÉ LES POINTS MARQUANTS DE VOTRE ENTREPRISE ?

Le premier point marquant a été l'obtention de la certification ISO 27001 octroyée par la compagnie suisse SGS SA. Elle démontre que non seulement nous con-

naissions les bonnes pratiques, mais que nous les appliquons dans tous nos projets et mandats. Après les sept ans d'existence de l'entreprise, cette certification nous donne beaucoup de confiance pour l'avenir.

« Sur le plan de nos valeurs, les mots clés qui nous décrivent sont *flexibilité* et *expertise complète en sécurité*. Nous œuvrons uniquement dans le créneau de la sécurité et nos clients adorent nos rapports entièrement personnalisés. »



SERVICES PROFESSIONNELS

- Tests de sécurité internes et externes
- Audits de certification ISO 27001
- Enquêtes juridico-informatiques
- Analyses de risques
- Tests de sécurité applicatifs
- Gouvernance
- Et beaucoup plus!

Pour tous vos besoins en SI, faites confiance à Gardien Virtuel, la première entreprise de services-conseils au Canada certifiée ISO 27001.

NOUVEAU!

TÉLÉSURVEILLANCE GARDIEN VIRTUEL (TGV)

- Détection d'intrusions
- Surveillance d'applications Web
- Analyse des journaux d'événements
- Monitoring 24/7
- Gestion des vulnérabilités
- Et beaucoup plus!

Rentabilisez vos investissements TI en mettant notre expertise à votre service. Enfin un service de télésurveillance flexible pour les entreprises de toutes tailles! Profitez de nos prix de lancement.

 www.gardienvirtuel.ca

1565, boulevard de l'Avenir, bureau 110
Laval (Québec) H7S 2N5
Tél.: 450.933.7774 | Sans frais: 1.888.377.7890

Nous vivons actuellement notre deuxième fait saillant, soit le lancement de notre nouveau service: la TGV. Nous avons l'avantage d'arriver dans un marché de services de sécurité gérés (Managed Security Services) en croissance et d'avoir pu étudier l'offre de services similaires existants dans la création de nos propres services et tarifs.

COMMENT ENVISAGEZ-VOUS L'AVENIR DE L'ENTREPRISE ?

Compte tenu de notre expertise, de notre réputation, de la fâcheuse tendance à la hausse des attaques et de la maturité grandissante du domaine de la sécurité, tout porte à croire que notre élan de croissance va se poursuivre au cours des prochaines années.

LA TGV

VOUS LANCEZ PROCHAINEMENT UN SERVICE DE TÉLÉSURVEILLANCE. EN QUOI CONSISTE-T-IL ?

La TGV est une centrale de surveillance de la sécurité des actifs informationnels qui fonctionne jour et nuit. Nos

services vont de l'analyse des journaux d'événements à la détection des intrusions (réseau et hôte) en passant par la surveillance des ressources et la gestion des vulnérabilités.

COMMENT CETTE IDÉE VOUS EST-ELLE VENUE ?

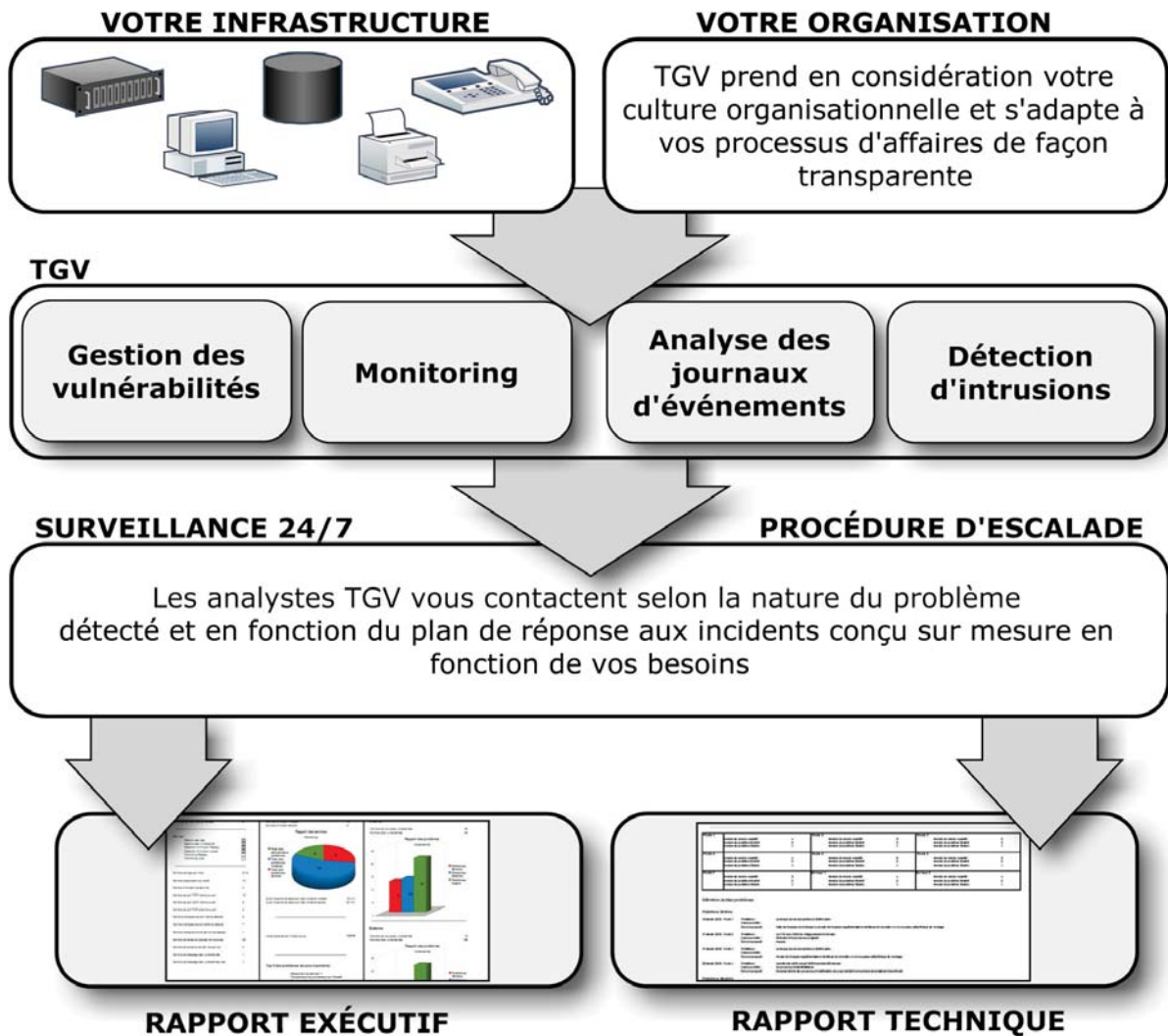
Nous avons analysé les produits sur le marché et les services existants et nous en sommes venus à la conclusion que nous pouvions innover en allant au-delà de ce qui était offert. En fait, nous continuons là où les autres se sont arrêtés.

Nous avons investi massivement en recherche et développement durant trois ans. Notre équipe a donc créé un produit innovateur et à la fine pointe de la technologie grâce, entre autres, à des partenariats avec des universités québécoises et étrangères.

QU'EST-CE QUE VOTRE SERVICE A DE SI PARTICULIER ?

Premièrement, un des avantages de la TGV est qu'elle s'adapte de façon transparente à l'infrastructure des clients et ne demande pas de modifications de celle-ci. C'est-à-dire que notre service a été conçu pour pouvoir piloter les

Suite en page 10



mécanismes de sécurité déjà en place : coupe-feu, système de détection des intrusions (IDS), surveillance réseau, etc. De plus, un de nos principaux objectifs de développement était de faire un impact minimal sur les systèmes surveillés. Nous sommes donc très fiers d'avoir réussi à créer un service pouvant se passer d'installer des agents logiciels sur les systèmes surveillés et même se passer d'avoir à installer un serveur sur place. Nous avons aussi déployé plusieurs efforts pour que notre service soit personnalisable à l'extrême, car nous avons aussi l'objectif de répondre précisément aux besoins, grands ou petits, des clients.

Deuxièmement, notre service utilise des technologies issues de recherches scientifiques poussées. Par exemple, nous sommes en mesure de détecter des intrusions à travers les flux de données chiffrées, sans avoir à les déchiffrer, en utilisant des calculs statistiques et probabilistes.

Un troisième point important pour l'ensemble de nos services, c'est que nos résultats soient clairs et utiles aux clients. C'est pourquoi, à la suite de l'ensemble des incidents de sécurité traités par notre centrale, nous émettons des recommandations précises pour éviter qu'ils ne se reproduisent. Notre service a également été conçu pour servir d'outils au maintien de la conformité de normes telles que l'ISO 27001 et le PCI-DSS.

QUEL TYPE DE CLIENTÈLE VISEZ-VOUS ?

La beauté de notre service est dans sa capacité d'adaptation. Nous sommes en mesure de répondre à tous les types et toutes les tailles d'organisations... et à tous les budgets.

QUELS SONT LES AVANTAGES D'UTILISER CE SERVICE ?

Pour une organisation, une simple couverture de télé-surveillance jour et nuit avec l'expertise que la TGV offre coûte plusieurs centaines de milliers de dollars annuellement! Nous sommes en mesure d'offrir ce même service et cette expertise pour une fraction de ce montant grâce au volume de clients. Notre service peut être implanté dans un court délai. Il est toujours fonctionnel et s'adapte rapidement aux particularités de chaque environnement client.

CONSEILS PROFESSIONNELS

SELON VOUS, QUELS SONT LES PLUS IMPORTANTS RISQUES AUXQUELS LES ORGANISATIONS FONT FACE ?

Aujourd'hui, la principale menace est celle provenant de l'interne. Je parle principalement ici de fuites d'informations. L'accent doit être mis sur la gestion des accès et la protection contre le vol de données (*Data Leak Prevention – DLP*).

Une autre menace est la hausse des attaques sur les applications. Ce qui est inquiétant, c'est que les IDS et les systèmes de prévention des intrusions (*Intrusion Prevention System – IPS*) dans leur forme actuelle détectent difficilement ce type d'attaques.

La TGV est en mesure de détecter ces différents types d'événements malveillants.

DE QUEL GRAND CHANTIER LE QUÉBEC DEVRAIT-IL SE PRÉOCCUPER ?

Le chantier qui me préoccupe le plus, au Québec, est le manque d'organisation de la sécurité informationnelle dans les sphères publique et privée. Dès que nous nous éloignons de la très grande entreprise, où nous retrouvons des équipes complètes dédiées à la SI, la mentalité tend vers le *patchage*.

Prenons l'exemple des nids-de-poule à Montréal. Chaque année, la Ville débourse des sommes faramineuses pour simplement remplir des trous plutôt que de faire l'investissement difficile (et majeur) de réparer le problème à la base. Je vois ce même type de laisser-aller en SI. La façon de

« Nous avons fait de grands efforts pour couvrir de façon très méticuleuse les couches applicatives des systèmes d'informations au lieu de nous contenter de couches réseau, comme c'est trop souvent le cas. »

penser des dirigeants d'entreprises doit changer rapidement pour renverser la vapeur. Certains diront que je « prêche pour ma paroisse », mais c'est un fait qui commence à être reconnu. En nous basant sur des choix technologiques structurés et en gérant les investissements en fonction d'un système de gestion de la sécurité informatique, nous éviterons les nids-de-poule !

COMMENT ENTREVOYEZ-VOUS L'AVENIR DE LA SÉCURITÉ ?

La sécurité telle qu'elle est actuellement appliquée est trop compliquée pour les citoyens. Prenons l'exemple d'une carte de crédit. On a un mot de passe pour effectuer des transactions, un mot de passe pour accéder au service à la clientèle téléphonique et un mot de passe pour accéder aux services en ligne. À l'avenir, nous devons nous affairer à trouver des méthodes tout aussi sécuritaires, mais plus efficaces. C'est pour cette raison que je prévois que la demande pour l'expertise dans le domaine de la sécurité croîtra dans les cinq prochaines années.

J'ajouterais même que, par extension, les services de sécurité gérés deviendront de plus en plus utilisés justement à cause de cette demande pour l'expertise et aussi parce que les entreprises y verront une manière de rentabiliser davantage leurs investissements. Ces nouvelles stratégies possèdent une solide courbe d'apprentissage. La bonne nouvelle, c'est que notre industrie le réalise et qu'elle agit déjà concrètement pour se préparer pour l'avenir. ■