L'automatisation de la sécurité

PAR MARIO AUDET, éditeur et copropriétaire de *SÉCUS*

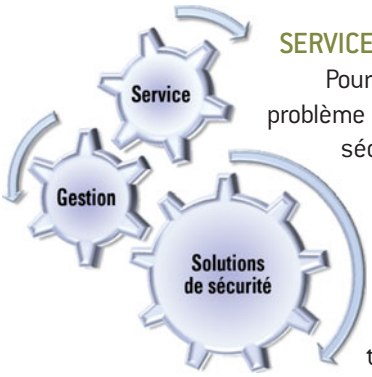
Photo : Annie Tremblay

***Mario Audet** est éditeur et copropriétaire du magazine SÉCUS. Il est principal actionnaire de la firme Securisa (securisa.ca). Il compte dix-neuf années d'expérience en technologies, dont onze en sécurité de l'information. Son intérêt pour la veille en sécurité l'a amené à développer l'agrégateur automatisé de nouvelles de sécurité informatique SecurNews.com*

En mars dernier, une entreprise québécoise[1] de haute technologie a réussi à mettre en place une solution de prévention de perte de données. Chose rare au Québec puisque cette technologie est relativement nouvelle et complexe à implanter. Pour cette organisation, l'autonomisation de la sécurité était la clé.

Le responsable de la sécurité de l'entreprise affirme que la mise en place d'une solution de prévention de perte de données était nécessaire. Selon lui, l'avenir de la sécurité passe par l'automatisation. « Pour notre organisation, il était requis d'automatiser la surveillance des échanges de données. Nous étions obligés de mettre en place plusieurs contrôles pour les échanges et cette situation devenait pénible autant pour les utilisateurs que pour notre équipe de sécurité », déclare le responsable de sécurité.

Mine de rien, il n'est pas le seul à penser ainsi. De plus en plus d'entreprises cherchent à automatiser différents processus de sécurité, histoire d'améliorer les façons de faire, d'accroître la sécurité ou de se conformer à des règlements.



SERVICE OU SOLUTION DE SÉCURITÉ

Pour cette organisation, la résolution de son problème passait par l'adoption d'une solution de sécurité. « Nous avons engagé un consultant qui nous a dit de revoir nos processus. Considérant les mouvements du personnel, nous avons calculé qu'il serait plus avantageux de recourir à une solution de prévention de perte de données pour l'automatisation des processus plutôt que de les réviser. [...] L'automatisation était la clé à nos problèmes », déclare le responsable de la sécurité.

SOLUTIONS ET EFFORTS DE GESTION

Selon ce dernier, les organisations associent à tort l'ajout d'une solution de sécurité et la multiplication d'efforts de gestion. « L'ajout d'une solution de sécurité doit augmenter le niveau de sécurité et elle doit réduire les efforts de gestion d'une fonction de sécurité. Si ce n'est pas le cas, c'est peine perdue. » Et dans un contexte où la main-d'œuvre se fait rare, l'ajout d'un employé n'est pas facile. Le recours à une solution de sécurité permettant d'automatiser des processus vient aussi pallier le manque de main-d'œuvre.

GRANDS CHANTIERS DE SÉCURITÉ

La mise en place de solutions de prévention de perte de données, de GIA[2] ou de NAC[3] exige souvent de grands chantiers en sécurité. Toutefois, ces grands projets ne se réalisent pas facilement. « Notre plus grande difficulté pour ce projet est survenue avant même son démarrage. Trouver un architecte de solutions de sécurité ayant une expertise avec les solutions de prévention de perte de données n'a pas été facile. Nous avons dû recourir à un expert des États-Unis, ce qui a entraîné des irritants comme l'utilisation de l'anglais pour les échanges, les déplacements de l'expert, etc. Nous avons passé à travers, mais nous aurions préféré un expert québécois », affirme le responsable de la sécurité.

Pour cette organisation, la clé de ses problèmes était l'automatisation de processus de sécurité. Cette façon de faire peut être réalisée par d'autres entreprises à condition d'avoir sous la main des architectes de solutions de sécurité. Comme ce type de ressources fait défaut au Québec, il est important pour le marché de la sécurité d'en former. Cette responsabilité revient aux ressources et aux fabricants de solutions de sécurité. Sinon, l'automatisation de la sécurité ne pourra pas se faire progressivement et tout le marché en sera pénalisé. ■

1. Cette organisation préfère garder l'anonymat.
2. Gestion des identités et des accès.
3. *Network Access Control.*