Mai 2020 • Vol. 7 n° 5

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies — 30 ans

NOUS AIDONS LES ENTREPRISES À TRANSFORMER LEURS TECHNOLOGIES EN LEVIER D'AFFAIRES

« Si j'avais un seul mot à dire à propos d'ARS, ce serait « éthique professionnelle »

Avec le phénomène de cybercriminalité qui s'accentue de jours en jours, aucune organisation n'est à l'abri des tentatives d'intrusion. Comme nous disposons de données nominatives, **nous avions besoin d'une firme pour nous accompagner et nous conseiller dans un processus d'audit de sécurité et, dans le cas échéant, nous soumettre des mesures correctives.**

ARS nous avait été recommandée et nous nous sommes sentis privilégiés de pouvoir travailler avec cette firme qui a déjà beaucoup de clients actifs à ce jour. L'équipe a toujours fait preuve de disponibilité et de flexibilité envers notre organisation compte tenu que nos délais sont souvent très courts. **Nous avons effectué un exercice d'audit de sécurité et mis en place un monitoring spécialisé.** L'information nous est toujours présentée de manière claire, concise et bien vulgarisée pour faciliter la compréhension.

Je donne définitivement un 11/10 à ARS qui fait preuve d'une éthique professionnelle et d'une disponibilité remarquable dans notre dossier.

Alex Bernier
Directeur général
CAUCA

Suivez-nous

La vérité sur les assurances cybersécurité

TEMPS DE LECTURE 3:00

On entend beaucoup parler des assurances en cybersécurité depuis quelques années. L'idée semble intéressante à première vue, mais c'est pourtant la dernière solution sur laquelle vous devriez compter...

En Planification Stratégique Affaires-TI, les dirigeants nous posent fréquemment ces questions : « Quels sont les risques et conséquences d'une cyberattaque pour mon entreprise? Sommes-nous vraiment à risque, nous ne sommes pas une multinationale? Est-ce que la situation n'est pas un peu amplifiée? Comment dois-je aborder la situation en tant que dirigeant de mon entreprise? ».

Des coûts à prendre en considération

Les technologies de l'information sont génératrices de croissance et de création de valeur pour l'entreprise, mais leur utilisation peut aussi comporter des risques et des coûts. Et pas seulement lors de leur implantation. Les cyberattaques et la cybercriminalité, les problèmes de systèmes et les erreurs humaines en sont les principales causes.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

Le rapport 2019 de IBM Security et du Ponemon Institute sur les coûts des atteintes aux mesures de sécurité informatique estime que le coût moyen d'une faille informatique au Canada s'élève à près de 5.86M $.

Ces coûts d'une cyberattaque **incluent les frais rattachés au « colmatage » de la fuite, la reconstruction des systèmes attaqués et, évidemment, la perte de clients dont la confiance aura été ébranlée.** En 2019, les cyberattaques malicieuses et la cybercriminalité ont été la cause de 51 % des failles informatiques. La perte de clients représente 36.2 % des coûts totaux d'une faille informatique.

La limite des cyberassurances

Sachez que votre assurance en cybercriminalité **paie seulement les demandes de rançons. Elle ne garantit aucunement que votre entreprise survivra à un tel événement.** Les recommandations du FBI sont très claires là-dessus, encourager ces fraudeurs ne fait qu'encourager la fraude et aggraver le phénomène. Les cybercriminels sont des bandits. **Rien ne vous garantit que vous récupérerez vos données et ce, même si vous payez la rançon qu'on exige de vous…** Par conséquent, les entreprises qui en sont victimes peuvent ne jamais se relever.

La probabilité qu'une organisation ayant subi un incident de sécurité en subisse un autre dans les 2 années qui suivent est de 29.6 %.

Chose certaine, avec la hausse des attaques, **le coût des assurances va augmenter radicalement dans les prochaines années. La meilleure solution est de vous doter d'un plan contre les cyberattaques et de le mettre en place immédiatement.** Vous avez une responsabilité de comprendre et gérer les technologies qui ne cessent d'évoluer et de prendre de la place. Plus vous connaîtrez les TIC de votre entreprise, mieux vous arriverez à les contrôler. Si vous avez besoin d'aide pour relever ce défi, nous sommes là pour vous aider.

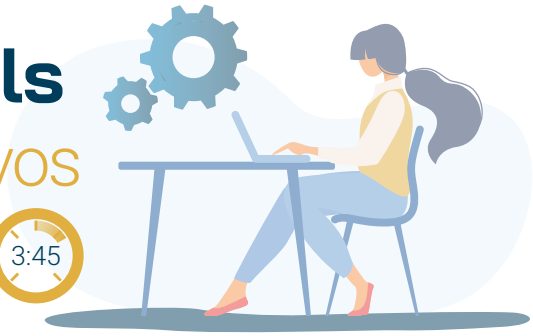
NOUVEAU - Rapport Cybersécurité

« 97 % des PME ayant subi une brèche estiment que l'attaque a impacté leur réputation et ont mentionné avoir eu des difficultés à opérer. »

Découvrez tout ce que vous devez savoir en 2020 pour la cybersécurité de votre entreprise. Téléchargez GRATUITEMENT notre nouveau rapport :

www.ars-solutions.ca/cybersecurite-2020/

5 manifestations de vols de données en provenance de vos employés



TEMPS DE LECTURE 3:45

Les employés mécontents représentent des cas de plus en plus fréquents de pertes importantes en raison de leur connaissance de l'organisation pour laquelle ils travaillent. Ils peuvent facilement accéder aux données et systèmes. Sans compter les incidents non intentionnels qui peuvent se manifester sous différentes formes, comme un clic dans un courriel frauduleux. Que ce soit intentionnel ou non, le résultat demeure le même. ***Voici comment peut se manifester le vol de données dans votre organisation et de quelle façon vous pouvez reprendre le contrôle :***

1. Les incidents non intentionnels

Le personnel interne peut aussi être la source d'incidents non intentionnels et être à la fois victime et responsable. Il peut être pris pour cible par des externes. Pensons par exemple aux courriels d'hameçonnage qui sont devenus omniprésents. Ils ont pour objectif de faire en sorte que le destinataire clique sur un lien conduisant au déploiement de logiciels malveillants ou encore divulgue des identifiants, numéros de cartes de crédit ou toute autre information de valeur. Les criminels peuvent aussi envoyer un courriel à un employé en utilisant une adresse très semblable à celle de l'entreprise et se faire passer pour un cadre supérieur. Le faux cadre supérieur demande alors l'aide de l'employé pour un transfert confidentiel de fonds dans un compte spécifique, souvent des milliers de dollars.

2. Les perturbateurs

Ce sont ceux qui ont pour mission de causer des problèmes dans une entreprise. Il peut s'agir d'un employé – actuel ou ancien – qui est mécontent ou encore de quelqu'un qui se fait embaucher dans le but de causer des problèmes. Un perturbateur motivé avec un accès approprié peut causer d'énormes dommages, par exemple faire en sorte que des fichiers sauvegardés soient remplacés par des fichiers inutiles et endommager ensuite les fichiers qui n'ont plus de sauvegarde utilisable. ***Selon une étude approfondie menée par Osterman Research, 69 % des entreprises subissent des pertes de données dues au roulement du personnel et 87 % des employés qui partent emportent des données avec eux.*** Que font-ils avec cette information? Ils la vendent à des concurrents, deviennent un concurrent ou les conservent pour les utiliser dans leur prochain emploi.

3. Les erreurs de parcours

Parfois, une personne fait simplement une erreur qui compromet des données. Par exemple, un développeur de systèmes peut, par inadvertance, mal configurer un conteneur de stockage basé sur le cloud et laisser libre cours à l'accès par Internet, ce qui conduit à une brèche… De même, quelque chose d'aussi simple qu'un courriel envoyé à une adresse incorrecte (ou un fax envoyé au mauvais numéro de télécopieur) peut compromettre des informations sensibles. Cela peut être causé par l'entrée accidentelle de la mauvaise adresse courriel, ou délibérément (mais sans le savoir) diriger un courriel vers une adresse mise en place par un adversaire avec un nom similaire à celui de la véritable organisation.

4. Les voleurs de propriété industrielle (PI)

Certains ont pour mission de voler la propriété intellectuelle d'une entreprise. La PI peut être évaluée à des millions, voire des milliards de dollars. Voler un code source d'un logiciel, par exemple, peut relancer un concurrent.

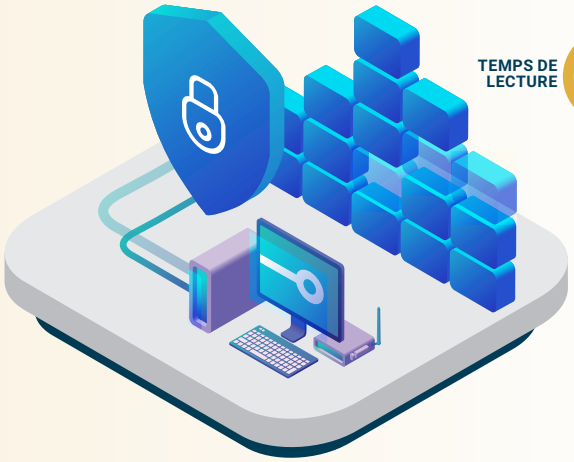
5. Les voleurs de données

Tout comme les voleurs de PI, les voleurs de données ont pour but de faire de l'argent ou de mettre une organisation dans l'embarras en mettant la main sur des numéros de cartes de crédit, d'assurance sociale, etc.

Comment reprendre le contrôle

C'est pourquoi l'utilisation d'un SIEM (Gestion de l'Information et des Évènements de Sécurité), qui détecte les activités suspectes ou non autorisées, est si importante. Grâce à l'intelligence artificielle amenant une capacité d'apprentissage constant, le SIEM en vient à connaître les comportements habituels de vos usagers et détecte les changements d'habitudes. Ceci devient encore plus intéressant dans un contexte où le travail à distance est de plus en plus fréquent.

TEMPS DE LECTURE 3:00



Cybersécurité

Les 3 incontournables en 2020

Bien entendu, la cybersécurité est une gestion de risques au même titre qu'un plan de relève en cas de feu ou désastre. Par contre, la probabilité d'une cyberattaque est beaucoup plus élevée présentement pour une entreprise que celle de passer au feu. **De tous les risques confondus, la cybersécurité est sans aucun doute le premier en 2020.**

Depuis trop longtemps, la sécurité est laissée au département des TI comme s'il s'agissait exclusivement d'un enjeu technologique, alors **qu'il appartient à la direction d'en assumer la gouvernance et d'élaborer sa stratégie** : bonnes pratiques, comportements humains, formation, technologies…

Voici 3 incontournables à mettre en place pour protéger votre entreprise en 2020 :

Avoir une culture forte en cybersécurité

La culture d'une entreprise est au cœur même de sa posture en sécurité. Sur une vision globale de 360 degrés, **elle représente 50 % de son risque en regard à sa pérennité dans un contexte de cyberattaques.** La vision et l'implication de la haute direction, les politiques en place, la formation continue des employés, sont tous des éléments faisant partie de la culture.

75 % des incidents de sécurité sont causés par l'erreur humaine. Une culture forte en cybersécurité résulte de la formation de vos employés. Comme les attaques par hameçonnage ou phishing sont en pleine explosion et très dommageables financièrement pour les entreprises, la mise en place d'un programme de simulation et de formation continue est une protection à prévoir au budget. Les attaques par hameçonnage se raffinent et peuvent être difficiles à détecter pour des employés mal sensibilisés.

Si la sphère culturelle est la plus importante, elle est aussi la plus difficile à gérer et celle qui représente aussi le plus de lacunes.

Revoir votre processus de sauvegardes

La continuité d'une entreprise dépend directement de ses données et les cybercriminels le savent très bien! Plus de donnée, plus de compagnie! Les copies de sécurité sont sans aucun doute leur cible préférée. Les récentes cyberattaques en sont la preuve. **99 % des audits de sécurité que nous avons réalisés au cours des dernières années démontrent que les copies de sauvegardes sont non utilisables ou incomplètes.** Le processus de copies de sauvegardes est assurément un incontournable en matière de sécurité informatique. Il demande beaucoup de connaissances techniques, de rigueur, de validations périodiques et d'assiduité.

Intégrer un système de gestion de l'information et des événements de sécurité – SIEM – dans votre organisation

Basées sur l'intelligence artificielle, les solutions SIEM d'aujourd'hui permettent à votre entreprise de réagir rapidement et avec précision en cas de menace ou de fuite de données. Elles donnent en temps réel l'information pertinente et essentielle. **Elles permettent de détecter les anomalies de comportement et les attaques qui seraient normalement passées inaperçues,** grâce à leur capacité de faire des liens entre les événements. Elles permettent non seulement de détecter, mais aussi de diagnostiquer et de prendre action beaucoup plus rapidement afin de **limiter les dommages.**

Au-delà d'amener un meilleur contrôle en regard à la cybersécurité, le SIEM a une portée beaucoup plus grande en entreprise dans l'ensemble de ses opérations : **soutien légal par la traçabilité des informations et la transmission de preuves, gain de temps par des rapports de conformité automatisés prouvant votre bonne foi lors d'audits, outils d'appui aux ressources humaines en situations de litiges...** Le SIEM permet de limiter les dommages financiers et le déficit d'image de marque et d'éviter que cette dernière ne soit ternie.

Maintenant plus accessible pour les PME par sa facilité d'intégration et sa rapidité de déploiement, **le SIEM est un incontournable à inclure dans votre budget annuel.** À l'ère où les entreprises de toutes tailles font face aux mêmes enjeux et défis, s'adapter est un passage obligé. Un grand nombre adoptent les **nouvelles technologies comme le cloud et la mobilité** sans compter qu'on encourage l'accélération de la transformation numérique au Québec. Il en résulte **un environnement informatique hybride, divers et complexe,** jamais vu auparavant et où se côtoient plusieurs technologies. **D'où l'importance grandissante d'avoir des outils adaptés à cette nouvelle réalité.**

ARS Solutions
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744