Février 2020 • Vol. 7 n° 2

PASSION AFFAIRES *et technologies*

ARSolutions 30 ans
affaires et technologies

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 des ressources humaines
CAUCA

Suivez-nous

DONNÉES COMPROMISES : employeurs, vous pourriez avoir gain de cause!

TEMPS DE LECTURE 4:00

Malgré toutes les précautions qu'un employeur peut prendre, que ce soit par de bonnes mesures de gouvernance ou par des politiques internes, il peut arriver qu'un employé s'approprie ou supprime tout simplement des données appartenant à son employeur...

En 2020, un employeur a nécessairement des données informatiques qui sont manipulées de jour en jour par son personnel. **Au Québec, les employés ont une obligation de loyauté et d'honnêteté envers leur employeur. Ils ne peuvent également pas faire usage de l'information confidentielle qu'ils ont obtenue dans le cadre de leur emploi. Heureusement pour les employeurs, ces obligations ne prennent pas fin dès la cessation d'emploi.** Alors, qu'arrive-t-il si un employé contrevient à ces obligations?

Un cas typique : un employé quitte l'entreprise en supprimant des données sur son poste de travail suite à une démission ou un congédiement. Qu'est-ce que l'employeur peut alors faire?

La réponse à cette question ne sera pas toujours la même. Plusieurs éléments entreront en ligne de compte afin de déterminer si l'employeur a ou non une cause lui permettant de réclamer des dommages-intérêts. Ces éléments incluront notamment le type et la quantité de données supprimées, puisque toute donnée n'aura pas la même valeur. Certains cas, bien que fâcheux, ne justifieront pas l'intervention des tribunaux.

SUITE À LA PAGE 2 ▼

Déterminer la valeur des données supprimées sera important afin de savoir quelles sommes pourront être réclamées à l'ancien employé…

Des indices comme la valeur du travail nécessaire pour remplacer les données détruites pourront permettre de quantifier la valeur de celles-ci. Par exemple, les heures de programmation nécessaires afin de replacer le travail réalisé dans la conception d'un logiciel ou les heures consacrées à la rédaction d'un ouvrage supprimé.

Pour pouvoir obtenir gain de cause dans une action en dommages-intérêts contre un ancien employé qui a supprimé des données informatiques lors de son départ, l'employeur devra nécessairement faire la preuve de la suppression de celles-ci. Il s'agit d'une preuve qui peut parfois être difficile à faire et qui peut nécessiter l'appel à des ressources spécialisées. L'employeur devra ensuite démontrer que cette suppression lui cause des dommages et que ces dommages sont directement liés aux actions de l'employé fautif. C'est lorsque tous ces éléments seront réunis que l'employeur pourra faire une preuve convaincante devant le Tribunal.

Un deuxième cas type : l'ancien employé devenu concurrent!

Il n'est pas rare qu'un ancien employé quitte avec une liste de clients ou avec certaines informations confidentielles, puis se lance à son compte ou rejoigne les rangs d'un compétiteur. Dans un cas comme celui-ci, où l'ancien employé s'approprie des informations commerciales de son ancien employeur, d'autres recours pourraient être à envisager.

En agissant ainsi, l'employé s'expose notamment à une demande d'injonction afin de l'empêcher de se livrer à une concurrence déloyale en plus des éventuels dommages-intérêts qui pourraient être demandés par l'employeur. Le Tribunal pourrait ordonner que l'ancien employé cesse ses agissements déloyaux sous peine d'outrage au tribunal en cas de contravention à l'ordonnance.

Bien que certaines possibilités s'offrent aux employeurs en cas de transgression, certains outils vous aideront à éviter ces situations fâcheuses, notamment les **bonnes pratiques en matière de gouvernance et de gestion des données, l'élaboration de politiques d'entreprise claires ainsi que l'inclusion de clauses relatives à la confidentialité et à la conservation des données dans les contrats de travail.**

Code civil du Québec, RLRQ c CCQ-1991, art. 2088.

Halima Kerchi, Avocate en droit des affaires
Therrien Couture Joli-Coeur

RENFORCER LA SÉCURITÉ DU RÉSEAU GRÂCE À

une meilleure visibilité sur les cybermenaces

TEMPS DE LECTURE 3:00

Sachant qu'une cyberattaque a lieu toutes les 39 secondes**, les entreprises, aussi petites soient-elles, ont peu de chances de passer à travers les mailles du filet. C'est pourquoi **il est si important de détecter les dangers et de rester vigilant face à leur évolution constante.

« Les enjeux sont élevés : les pertes financières liées à la cybercriminalité devraient atteindre 6 000 milliards de dollars d'ici 2021. Faire face aux nouvelles menaces devrait donc être la préoccupation #1 des chefs d'entreprise d'aujourd'hui.

L'identification de tous les risques auxquels vous êtes confronté vous permet d'évaluer rapidement leur impact potentiel et de concentrer vos efforts sur la protection des ressources qui comptent le plus pour votre entreprise.

UNE MEILLEURE VISION DES RISQUES PEUT VOUS AIDER À SURMONTER LES 3 PRINCIPAUX DÉFIS D'UNE ORGANISATION :

1. **Faire face aux nouvelles menaces**
2. **Saisir toute la portée d'une attaque**
3. **Détecter une attaque en cours**

Renforcer la sécurité commence par une analyse précise de la situation, axée sur des outils capables de vous fournir une vision globale de ce qui se passe sur votre réseau (qui fait quoi et qui a accès à quoi et quand) afin de faire face à la réalité d'aujourd'hui. Cette stratégie vous offre une vue élargie et affinée des événements qui se produisent dans votre entreprise, elle simplifie l'identification des failles et accélère les temps de réponses. Elle exploite les données pour optimiser ces réponses et, au final, la sécurité de votre environnement.

Basés sur l'intelligence artificielle, les solutions SIEM (Security Information and Event Management) permettent à votre entreprise de réagir rapidement et avec précision en cas d'attaque ou de fuite de données. Elles donnent des informations pertinentes et essentielles. Cet outil permet non seulement de détecter, de diagnostiquer, mais aussi de prendre action très rapidement.

Avec le SIEM, la visibilité ne s'arrête pas là. L'analytique renforce la sécurité du réseau en détectant les comportements inhabituels, tels qu'un utilisateur qui compromet votre réseau, intentionnellement ou non, en cliquant par exemple sur un lien dans un courriel frauduleux. L'amélioration de la sécurité du réseau devrait faire partie du plan de développement de tous types d'entreprises, car les cybercriminels mettent constamment au point de nouvelles techniques pour tenter de les ralentir. Par ailleurs, des technologies émergentes comme l'Internet des objets (IoT) et le Cloud augmentent votre vulnérabilité. C'est pourquoi vous devez privilégier la visibilité sur les pièges. Cette approche vous protège des attaques par hameçonnage, des logiciels malveillants, des erreurs des utilisateurs et autres dangers. Elle permet également de traiter les réponses aux risques en ordre de criticité.

Pour en savoir plus, consultez notre rapport *Le SIEM améliore l'ensemble des activités des entreprises et aide les dirigeants à relever leurs défis concernant la cybersécurité.*

5 CONSEILS POUR SÉCURISER VOS DONNÉES

Si le Web n'était qu'un lieu de partage de photos de chiens en costume de dinosaure, les mots de passe ne seraient pas très utiles. Mais c'est sur Internet que vous payez vos factures, accédez aux médias sociaux, consultez votre compte bancaire et vos talons de paie. Pourquoi ne garderiez-vous pas ces objets de valeur virtuels aussi en sécurité que votre portefeuille ou vos clés?

TEMPS DE LECTURE 3:30

La plupart des malfaiteurs n'ont pas besoin de compétences techniques spécialisées pour accéder à vos comptes, ils peuvent le faire en devinant vos mots de passe ou en exécutant un programme automatisé. Une fois que c'est fait, ils peuvent d'ailleurs essayer ce mot de passe compromis sur d'autres comptes, recueillir des informations sur vous et vos habitudes, reprendre des comptes que vous possédez, ou même utiliser votre identité numérique.

VOICI 5 MESURES PRATIQUES POUR ACCROÎTRE VOTRE SÉCURITÉ EN LIGNE

1. VERROUILLEZ VOTRE PORTE NUMÉRIQUE. Verrous d'écran : le mot de passe, l'empreinte digitale ou l'identification faciale que vous utilisez pour accéder à votre appareil sont quelques-uns de vos meilleurs moyens de défense contre les personnes qui pourraient vouloir y pénétrer. Mais il en existe de nombreux types et il peut être difficile de savoir lequel vous convient le mieux. Tout comme les différents types de serrures que vous pouvez poser sur vos portes, certaines serrures d'écran sont plus résistantes que d'autres.

2. LAISSEZ ENTRER LA BONNE PERSONNE. Il est facile de créer d'excellents mots de passe. Il vous suffit de suivre quelques principes de base. Vos mots de passe doivent être longs (au moins huit caractères), complexes (combinaison aléatoire difficile à deviner) et uniques (différents partout). Idéalement, vous devriez utiliser un gestionnaire de mots de passe pour générer et stocker tous vos mots de passe. Cette application permet de protéger vos identifiants de connexion et autres données sensibles. Parlez-en à votre fournisseur TI!

3. AJOUTEZ UNE DEUXIÈME CLÉ. La mise en place d'une authentification à deux facteurs (2FA) ou d'une authentification multifacteur (MFA) signifie que même si quelqu'un trouve votre mot de passe, il n'aura probablement pas le facteur supplémentaire dont il a besoin pour entrer. Consultez les paramètres de sécurité de vos sites Web et applications les plus utilisés pour voir si vous pouvez configurer cette clé supplémentaire. Commencez par les plus importants : toutes les applications financières ou les services comme le courrier électronique, que vous utilisez pour récupérer vos autres comptes.

4. PROTÉGEZ VOS OBJETS DE VALEUR VIRTUELS. Tout comme vous prenez soin des objets de valeur de votre maison, vous devriez faire de même pour les informations que vous stockez virtuellement. Cherchez des informations spécifiques qui se trouvent dans votre messagerie ou autres comptes et supprimez-les : scan de votre carte d'identité, coordonnées bancaires, assurance maladie, etc. Si vous en avez besoin plus tard, vous pouvez toujours les télécharger sur votre ordinateur ou les imprimer avant de supprimer le contenu du compte pour repartir à zéro. N'oubliez pas de vider ensuite votre poubelle et vos fichiers temporaires! Sauvegardez vos archives et vos documents sur le Cloud, un disque dur externe ou une clé USB.

5. PASSEZ LE MOT. Le Web ne s'appelle pas "toile" pour rien. Nous sommes tous connectés en ligne par le biais de différents réseaux, non seulement en tant qu'"amis" sur les médias sociaux, mais aussi par les contacts de nos comptes de messagerie. Lorsque vous sécurisez vos données, tous ceux avec qui vous êtes connecté sont un peu plus en sécurité grâce à vos efforts. Pensez à ce que vous pouvez supprimer pour aider vos amis ou collègues : les coordonnées bancaires de votre sœur, le code d'accès à votre bureau ou le scan du passeport de votre fils sont des exemples de documents qui pourraient vous donner mal à la tête s'ils tombaient entre de mauvaises mains. Partagez cette procédure de nettoyage de données avec votre entourage afin de les aider à conserver ce qui leur appartient.

Source : https://datadetoxkit.org/en/security/essentials

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