Juin 2019 • Vol. 6 n° 6

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

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

2e étude de cas d'une cyberattaque dans une entreprise à Québec.

4 autres exemples de cas vécus à venir

Édition spéciale Cybersécurité

Voici nos 3 articles du mois portant sur différentes sphères de la sécurité informatique. **Vous y trouverez un document comprenant 16 manières de protéger votre entreprise des cyberattaques. N'hésitez pas à le compléter en cochant les cases correspondant aux protections que vous avez ou non en place.** Vous verrez les volets manquants à adresser dans votre entreprise.

La plupart des PME sont une cible de choix pour les pirates informatiques, car elles se croient peu à risque et mettent en place des protections souvent insuffisantes. **En fait, 81 % des cyberattaques sont destinées aux PME, soit 5 500 par jour.**[1] Ne sous-estimez pas vos probabilités d'en être victime.

[1] *Osterman Research et Malwarebytes : https://blog.malwarebytes.com/101/2017/07/the-state-of-ransomware-among-smbs*

Suivez-nous

Des employés de Québec se sont fait voler de 100 $ à 3 000 $ À LA SUITE D'UNE CYBERATTAQUE

Une entreprise de plus de 75 employés, victime d'un vol d'identifiants numériques, a été non fonctionnelle pendant 3 jours.

« Nos clients se plaignaient qu'ils recevaient des courriels étranges de notre part, car les fraudeurs utilisaient notre nom. Je me suis donc informé sur ce genre de situations et j'ai rapidement compris que ça se devait d'être pris au sérieux. Je n'ai pas été difficile à convaincre lorsqu'on m'a dit qu'il fallait tout détruire et repartir à zéro. », témoigne le Directeur Finances et TI qui a accepté de partager son expérience avec nos lecteurs, à condition qu'il puisse garder l'anonymat. Inquiet pour l'entreprise, il nous mentionne avoir eu beaucoup de difficulté à dormir durant cette période.

SUITE À LA PAGE 2 ▼

SUITE DE LA PAGE 1 ▲

L'entreprise avait déjà subi une vingtaine d'attaques différentes dans le passé : CryptoLocker, Trojan, extracteurs de données, etc. Cette fois-ci, il s'agissait d'un courriel avec une pièce jointe infectée qui a été ouverte par un seul employé. Le virus s'est ensuite répandu dans la totalité de l'entreprise, incluant les serveurs.

Tout a commencé lorsqu'il était en formation à Montréal. On l'a contacté pour l'informer que l'entreprise avait été touchée par une cyberattaque. Il ne s'agissait pas d'une attaque qui détruisait, mais plutôt qui **volait des identifiants numériques**. « Nos premières actions ont été de contacter notre fournisseur informatique pour venir corriger le problème », mentionne-t-il.

« Au début, on s'entêtait à trouver une autre solution puisqu'on trouvait ça démesuré de reformater 60 postes, mais on a fini par accepter les recommandations de notre fournisseur TI. En effaçant les données dès le départ, on aurait sauvé non seulement du temps, mais aussi de l'argent. **On a donc été non fonctionnels pendant 3 jours** », nous informe le gestionnaire.

DES IMPACTS CONSIDÉRABLES

Les conséquences économiques étaient encore approximatives au moment de l'entrevue. **L'entreprise avait déjà subi une vingtaine d'attaques différentes dans le passé** : CryptoLocker, Trojan, extracteurs de données, etc. Cette fois-ci, **il s'agissait d'un courriel avec une pièce jointe infectée qui a été ouverte par un seul employé**. La cyberattaque s'est ensuite propagée dans la totalité de l'entreprise, incluant les serveurs. **Elle avait été conçue pour de l'extraction de données corporatives et bancaires en vue de faire de l'espionnage industriel.** Plusieurs employés ont par la suite rapporté s'être même fait voler de 100 $ à 3 000 $ via leur carte de crédit, compte PayPal, etc.

Avec l'aide d'ARS, l'entreprise a profité de l'occasion pour revoir la sécurité dans une vision plus globale, en retirant par exemple les droits d'administrateur à certaines personnes et en resserrant les contrôles. Cette mauvaise expérience a permis de sensibiliser davantage l'entreprise et les employés à la cybercriminalité.

LES DOLLARS INVESTIS EN SÉCURITÉ EN VALENT LA PEINE

« Je pense qu'on n'est jamais trop prudent et que les dollars investis là-dedans en valent la peine », affirme le directeur. « Tout commence par une bonne sensibilisation des employés. On a envoyé beaucoup de communications et d'informations sur la cyberattaque. **C'est difficile de calculer un retour sur investissement tant qu'on ne se fait pas attaquer.** Quelle est la valeur d'une entreprise inactive pendant 3 jours ? De notre côté, ça a duré seulement 3 jours parce qu'on est une petite compagnie, mais ce n'est pas le cas de tous. », ajoute-t-il.

Si l'on vous coupe votre chiffre d'affaires pendant une semaine, quel sera l'impact dans vos états financiers ? Les employés sont rarement de mauvaise foi, mais mettent quand même à risque leur entreprise.

Le fait d'avoir un bon programme de sécurité peut donc aider à prévenir les pertes de temps/coûts. « Ce genre de situations peut arriver à tout le monde donc il est important de s'y attarder, d'**arrêter d'avoir peur et de fermer les yeux sur le problème en refusant d'investir en sécurité**. », termine-t-il.

Simon Fontaine, Président
simon.fontaine@ars-solutions.ca

Simulation d'hameçonnage

Vos employés savent-ils reconnaître un courriel frauduleux ?

Inscrivez-vous avant le 31 juillet 2019 pour bénéficier d'une **simulation d'hameçonnage sans frais (valeur de 595 $)** ! Vous découvrirez où sont vos vulnérabilités et comment les adresser.

info@ars-solutions.ca • 418-872-4744 #233

5 FAÇONS DONT VOTRE ENTREPRISE PEUT SUBIR des dommages liés au cybercrime

TEMPS DE LECTURE 3:30

Il est tentant de remettre à plus tard tout ce qui entoure la cybersécurité. Toutefois, considérant que 92 % des entreprises canadiennes ont subi au moins une cyberattaque au cours de la dernière année, la cybersécurité devrait être une priorité.

VOICI 5 EXEMPLES DE CONSÉQUENCES D'UNE CYBERATTAQUE :

1 ATTEINTE À LA RÉPUTATION.

En cas de piratage des données de vos employés/clients, pensez-vous que ceux-ci vous le pardonneraient ? Des nouvelles comme celle des 3 millions de membres Desjardins touchés par un vol massif de données personnelles voyagent rapidement sur les médias sociaux. Vos clients exigeront des réponses. « Désolés, nous avons été piratés parce que nous ne pensions pas que cela pouvait nous arriver » est loin d'être une réponse acceptable…

2 AMENDES GOUVERNEMENTALES, FRAIS JURIDIQUES, PROCÈS, ETC.

Les lois sur la notification des brèches de données demeurent l'un des domaines les plus actifs. À l'heure actuelle, plusieurs sénateurs font pression pour obtenir des amendes « massives et obligatoires » et une législation plus agressive en matière de violation de données et de confidentialité des données. Les tribunaux ne seront pas en votre faveur si vous exposez les données de vos clients aux cybercriminels.

Ne pensez pas un instant que cela ne s'applique qu'aux grandes entreprises. Toute petite entreprise qui recueille des informations sur les clients a également d'importantes obligations de les notifier en cas de brèche.

3 COÛTS, APRÈS COÛTS, APRÈS COÛTS.

Une brèche, une attaque par rançongiciel, un employé mal intentionné contre lequel vous n'êtes pas protégé pourraient générer des heures de travail supplémentaires pour votre personnel.

Ensuite, il y aura **l'interruption des activités et les temps d'arrêt, les délais de livraison retardés pour vos clients actuels et des pertes de ventes**. Il y aura également les coûts pour déterminer quel type de piratage a eu lieu, quelle partie du réseau a été affectée et quelles données ont été compromises. On ajoute à cela les coûts de restauration pour vous aider à récupérer vos sauvegardes, si c'est possible.

4 FRAUDE BANCAIRE.

Si votre compte bancaire est piraté et que des fonds sont volés, **la banque n'est pas responsable du remplacement de ces fonds**. Prenez l'histoire vraie de Verne Harnish, PDG de Gazelles inc. Il s'est fait voler 400 000 $ de son compte bancaire lorsque des pirates ont pu accéder à son ordinateur et intercepter des courriels entre lui et son adjoint. Les pirates, basés en Chine, ont envoyé un courriel à son adjoint lui demandant de virer des fonds à trois endroits différents. L'adjoint a répondu par l'affirmative. Cet argent a donc été transféré « de plein gré » par l'adjoint de monsieur Harnish. Pourquoi serait-ce à la banque de payer pour l'erreur et le manque de sécurité de l'organisation victime ?

5 UTILISATION DE VOTRE ENTREPRISE COMME MOYEN D'INFECTER VOS CLIENTS.

Certains pirates ne se contentent pas de voler vos données pour obtenir une rançon ou voler de l'argent. Souvent, ils utilisent votre serveur, votre site Web ou votre profil pour propager des virus et/ou compromettre d'autres ordinateurs. S'ils piratent votre site Web, ils peuvent l'utiliser pour propager des pourriels, exécuter des logiciels malveillants, porter atteinte à la réputation de votre entreprise, etc.

Nous avons été témoins de plusieurs exemples de cyberattaques, ici au Québec, que vous connaissez très bien d'ailleurs. Tout le monde veut croire : « Pas MON adjoint, pas MES employés, pas MON entreprise ». On estime que **plus de 90 % des cyberattaques sont causées par l'erreur humaine...**

La cybercriminalité est une réalité bien présente à laquelle on doit faire face en mettant en place des **protections adéquates**. Une cyberattaque peut rapidement se transformer en cauchemar pour l'entreprise qui la vit et son personnel.

5 bonnes raisons d'avoir un système de gestion DES ÉVÉNEMENTS DE SÉCURITÉ DANS VOTRE ENTREPRISE

TEMPS DE LECTURE 3:45

Pour contrer les menaces liées à la cybercriminalité, les dirigeants doivent plus que jamais mettre en place des mesures de sécurité adaptées s'ils veulent assurer la continuité de leurs affaires.

82 000 nouvelles menaces sont libérées chaque jour et 50 % d'entre elles visent les PME qui sont une cible de choix, puisque les cybercriminels connaissent très bien le peu d'investissement accordé à ce volet. **Le secteur manufacturier est l'une des industries les plus fréquemment ciblées.** Les fabricants utilisent de plus en plus le Cloud, les appareils mobiles, l'IoT (Internet of Things) et l'analyse de données pour améliorer leur connectivité et leur infrastructure. Ils sont donc davantage exposés aux attaques et l'arrivée de l'industrie 4.0, malgré tous ses avantages, vient augmenter ce risque.

Et si vous aviez désormais la possibilité de mettre en place **une stratégie efficace et accessible pour vous protéger ?**

QU'EST-CE QU'UN SIEM ?

Le SIEM (Security Information and Event Management) sert à **détecter les anomalies de comportement et les attaques. Il permet de détecter, de diagnostiquer et de prendre action beaucoup plus rapidement**. On peut désormais **automatiser certaines actions de réponse en fonction des incidents détectés**.

Le SIEM a toujours permis de réduire les risques liés à la cybercriminalité, et ce, pour tous les types d'entreprises. **C'est maintenant devenu un incontournable.**

VOICI 5 BONNES RAISONS D'UTILISER LE SIEM AU SEIN DE VOTRE ENTREPRISE :

1 **Détection plus efficace des incidents de sécurité**, qui seraient normalement passés inaperçus, grâce à sa capacité de faire des liens entre les événements. Il permet d'identifier un événement ayant causé la génération de plusieurs autres : hack via le réseau, manipulation d'un équipement précis, etc. **Vous pourrez ainsi détecter plus rapidement un incident, en connaître l'étendue potentielle dès le début et évaluer les dommages.**

2 **Prise de mesures défensives plus rapide.** Le SIEM permet de prendre des **mesures défensives plus rapidement et d'éviter les pertes de temps en recherche et diagnostic**. Vous limitez donc les dommages dans votre entreprise.

3 **Gestion des incidents.** Le SIEM communique avec la majorité des systèmes générant des journaux d'événements comme les ordinateurs de bureau, les pare-feux, les systèmes antivirus, etc. **Il va ensuite prendre en note les comportements suspects et relever un incident générant une alerte permettant ainsi de creuser le problème plus loin.**

4 **Satisfaction des exigences légales de conformité de votre entreprise.** Le système collecte des données et les place dans un référentiel central à des fins d'analyse de tendances. La génération de rapports de conformité est automatisée et centralisée. Ce procédé accélère l'identification et l'analyse des événements de sécurité en plus de la restauration.

5 **Vision globale de votre réseau en tout temps.** En cas de doute, vous pourrez **vérifier les activités de vos employés sur le réseau et être notifié en présence d'anomalies**. Le SIEM relève également les activités des logiciels et des appareils. **Par exemple, un fournisseur de service pour des appareils d'impression pourrait demander l'installation d'un logiciel sur un serveur et l'on pourrait apprendre que ce logiciel exporte des données de l'entreprise alors qu'il n'est pas autorisé à le faire.**

Maintenant plus accessible pour les PME par sa facilité d'intégration et sa rapidité de déploiement, **le SIEM est la garantie d'une tranquillité d'esprit, car il permet de mieux outiller les entreprises contre les cyberattaques**. N'hésitez pas à nous contacter pour plus d'informations sur comment le SIEM peut vous aider dans votre organisation.

Forrester et Gartner ont évalué 17 SIEM et, parmi ceux-ci, ont identifié 7 leaders : Splunk, IBM QRadar et LogRythm NextGen SIEM, Dell Technologies (RSA NetWitness), Exabeam (Security Management Platform), McAfee (Enterprise Security Manager) et Securonix.

Saviez-vous que 88 % des entreprises manufacturières ont vécu au moins une cyberattaque en 2017, soit le plus haut taux jamais connu (Kroll, Global Fraud & Risk Report 2017-2018) ?

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