Mars 2020 • Vol. 7 n° 3

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies — 30 ans

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

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/

Suivez-nous

À Rivière-du-Loup, 10 entreprises ont été victimes de cyberrattaques en quelques mois dont Lepage Millwork.

TEMPS DE LECTURE 3:00

Le jeudi 9 janvier dernier, Lepage Millwork était victime d'un cryptolocker. Le lundi suivant, 13 janvier, l'entreprise ne savait pas encore si elle serait en mesure de récupérer ses données et de se relever. ***Êtes-vous équipés dans votre entreprise pour contrer ce type de menaces?***

Chez Lepage Millwork, une entreprise de Rivière-du-Loup spécialisée dans la fabrication de portes et fenêtres sur mesure, tout est informatisé : les ventes, qui passent par un configurateur relié à l'ERP, le traitement des commandes vers l'usine, le service à la clientèle, les achats, l'administration, etc.

Le 9 janvier dernier, l'entreprise a été **victime d'un cryptolocker, paralysant l'ensemble de ses opérations pendant 8 jours.**

« Pour nous, c'était une surprise, mentionne François-Xavier Bonneville, l'un des propriétaires de l'entreprise. Ce n'était pas quelque chose qu'on avait vécu avant. » C'est en arrivant au bureau un jeudi matin que le personnel a constaté que des services ne fonctionnaient plus dans l'usine. **« On voyait que le virus se propageait rapidement parce que certains ordinateurs fonctionnaient bien et peu de temps après, des choses s'installaient et ces ordinateurs n'étaient plus opérationnels. »**

SUITE À LA PAGE 2 ▼

« On recevait beaucoup de courriels de ce genre, mais on n'avait jamais fait de formation. Les gens savaient que c'était un risque potentiel, mais ne savaient pas jusqu'à quel point... »

François-Xavier Bonneville et son équipe ont décidé de demander de l'aide. **« On a du gros bon sens, mais on n'a pas l'expertise à l'interne pour répondre à ce type d'attaques. J'ai décidé de contacter ARS et, en peu de temps, on avait quelqu'un d'expérimenté et compétent chez nous qui nous a aidé à se remonter plus facilement et plus rapidement. »** L'entreprise était en gestion de crise. Des équipes ont été mobilisées, des gens ont été embauchés, un plan de communication a été mis sur pied pour les employés ainsi que pour les clients qui ne pouvaient plus passer de commandes…

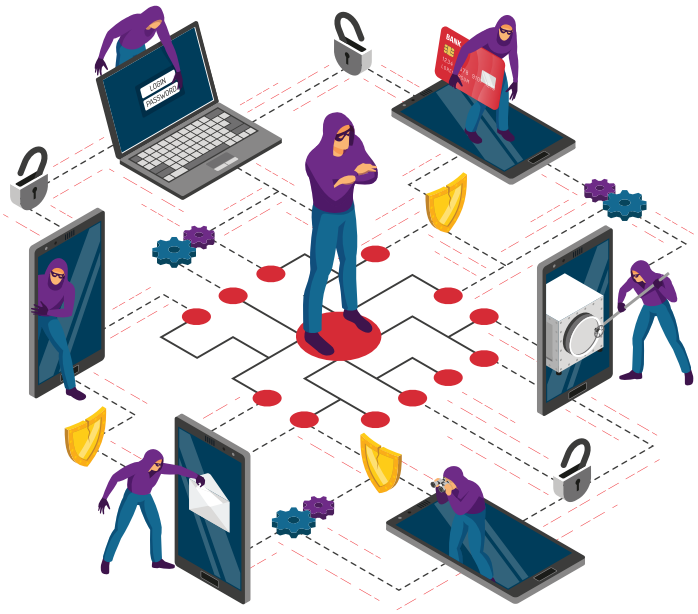
« La première journée, il s'est brassé beaucoup de choses, tout arrivait en même temps. **On a envoyé 50 % de notre personnel de bureau à la maison.** Heureusement, on fonctionne encore papier dans les usines avec des cédules de travail imprimées. On pouvait avancer quand même, mais on n'avait plus de système de suivi ni de confirmation de commande ni de statut. », ajoute monsieur Bonneville.

Si l'entreprise soupçonne que ce cryptolocker vient du clic d'un employé – courriel UPS avec pièce jointe – ce fait n'est pas encore confirmé par l'équipe de Forensic. **« Depuis l'événement, on s'est tous mis sur le mode alerte. On en reçoit plus qu'on pense même si on a un antispam. »**, soulève monsieur Bonneville.

En plus de l'équipe responsable de remonter les serveurs, une deuxième équipe a rapidement été formée pour remplacer les postes de travail infectés, alors qu'une troisième équipe s'est mobilisée pour évaluer comment l'entreprise pouvait **continuer à opérer en mode compensatoire** afin qu'il y ait le moins d'impact possible sur les clients.

En étant sur 2 quarts de travail 5 jours par semaine, l'équipe avait 2.5 jours pour faire sa réflexion et préparer la suite, ce qui n'est malheureusement pas le cas de toutes les organisations. **Des équipes supplémentaires ont été mobilisées pour fonctionner à la main. C'est sûr que les gens performaient moins et étaient moins productifs. Les conséquences auraient été plus graves si la crise avait duré plus de 8 jours.**

« Si c'était à refaire, on s'informerait plus sur les types d'attaques, comment elles fonctionnent et comment on peut se protéger et faire de la prévention, ajoute monsieur Bonneville. **J'aurais aimé être plus conscient de mes données critiques et de comment elles étaient protégées. On s'est rendu compte que nos copies de sécurité n'étaient pas suffisantes, même si on s'en occupait à l'interne.** Je recommande aux gens de poser des questions et de se renseigner parce qu'on pensait, comme trop d'entreprises, que les ransomwares (logiciels de rançon) n'existaient pas ici. **Pourtant, juste ici à Rivière-du-Loup, plusieurs entreprises en ont été victimes en quelques mois. C'est une nouvelle réalité, un nouveau risque très dangereux auquel les gens ne pensent pas. »**



Les risques de la mobilité

TEMPS DE LECTURE 3:45

L'adoption croissante de la mobilité, du Cloud et d'autres technologies permet de nouveaux niveaux de productivité, de réactivité et de convivialité. Toutefois, la mobilité comporte plusieurs risques. Selon le rapport de sécurité sur le BYOD, ***67 % des directeurs TI pensent que la mobilité aura un impact au moins aussi important sur leur entreprise qu'Internet dans les années 1990.*** *Il est donc essentiel de prendre le contrôle de votre stratégie de sécurité dans le contexte actuel de mobilité et de risque accru, surtout en matière d'identité.*

Savez-vous qui sont vos utilisateurs mobiles?

La plupart des utilisateurs mobiles souhaitent disposer d'une connexion en tout temps, en tout lieu et à partir de n'importe quel appareil. Cependant, comment savez-vous que la personne sur un smartphone est l'utilisateur autorisé? Selon le rapport d'enquête sur les violations de données, **63 % des violations de données confirmées ont impliqué l'exploitation de mots de passe volés, par défaut ou faibles.** La plupart des appareils utilisent la protection par mot de passe comme unique mesure de sécurité. **Seulement 38 % des entreprises affirment supprimer proactivement les données des périphériques mobiles lorsque des employés quittent l'entreprise :** un problème potentiellement grave si les données d'entreprise, ou l'accès à ces données, résident sur ces appareils. **Ces pratiques vulnérabilisent les appareils mobiles et créent un risque élevé de voir les informations d'identification de l'utilisateur compromises qui peuvent alors exposer votre entreprise aux cybermenaces.**

Confort des utilisateurs

La croissance des applications grand public sur les cellulaires fait augmenter les attentes des utilisateurs qui souhaitent disposer d'un accès pratique. Cela crée une **pression supplémentaire pour les entreprises qui doivent mettre en œuvre des méthodes d'authentification similaires orientées consommateurs** (par exemple, notifications push, lecteur d'empreintes digitales) sur le lieu de travail. Après tout, une fois habitué à l'identification tactile, qui souhaite revenir en arrière et mémoriser un mot de passe complexe à 30 chiffres qui change à tous les mois?

Comportement risqué

Les applications mobiles comportent de nombreux risques de sécurité, à commencer par un manque de règles concernant leur téléchargement et leur utilisation. Selon l'étude relative à l'état d'insécurité des applications mobiles réalisée par le Ponemon Institute, **55 % des entreprises autorisent leurs employés à utiliser et à télécharger des applications professionnelles sur leurs appareils personnels (BYOD) et 39 % autorisent les employés à utiliser leurs applications mobiles personnelles sur les périphériques mobiles attribués par l'entreprise.** Les menaces d'attaque par phishing et les comportements risqués des utilisateurs, notamment la réutilisation d'un mot de passe entre les applications personnelles et professionnelles sur ces périphériques, l'utilisation de réseaux Wi-Fi non sécurisés pour accéder aux systèmes de l'entreprise et l'utilisation d'un ensemble de réseaux sociaux peuvent exposer les informations d'identification des utilisateurs mobiles à des vols.

Problèmes de sécurité des applications mobiles

Parallèlement à l'absence d'une politique d'entreprise pour ce qui est des applications mobiles se pose le risque croissant d'applications infectées par des malwares. Les développeurs négligent souvent la sécurité lors de la création d'applications mobiles, exposant ainsi les données de leurs clients. **Le manque d'attention portée à la sécurité mobile expose les entreprises d'aujourd'hui à des risques de sécurité accrus,** car les cybercriminels deviennent de plus en plus sophistiqués et connaissent ces vulnérabilités.

Repensez votre sécurité mobile

Les solutions modernes comme le SIEM (Security Information and Event Management) fournissent plusieurs moyens sécurisés et pratiques pour authentifier tous vos utilisateurs, analyser leur comportement et le contexte et garantir que les bonnes personnes disposent des bons niveaux d'accès, en tout lieu et depuis n'importe quel appareil.

TEMPS DE LECTURE 3:00

Tracker Radar :
un outil pour savoir qui vous piste sur le Web

DuckDuckGo a récemment décidé de partager un nouvel outil intitulé Tracker Radar qui permet de savoir si une entreprise s'intéresse à votre navigation Web.

Une liste de milliers de traqueurs Web a été répertoriée par les équipes du moteur de recherche pour lutter contre ces pratiques abusives de surveillance du comportement des utilisateurs.

Contribuer à la lutte contre le pistage

DuckDuckGo est un moteur de recherche qui lutte pour améliorer la protection de notre vie privée sur Internet. D'après CNET, le Tracker Radar de DuckDuckGo permet d'accéder aux informations suivantes : le comportement des cookies, leur propriété ou encore la politique de confidentialité d'un nom de domaine. **L'ensemble de données recueillies contient des détails sur 5 326 noms de domaines utilisés par 1 727 entreprises.** Le Tracker Radar est désormais disponible pour tous. Les développeurs vont pouvoir l'utiliser pour bloquer le suivi en ligne et les chercheurs devraient en profiter pour mieux comprendre ces pratiques.

Les traqueurs Web permettent aux entreprises qui les utilisent de recueillir des données sur la localisation des utilisateurs, sur leur historique navigation ainsi que sur les recherches qu'ils effectuent. Bref, des informations précieuses de nos jours, qui permettent à ces mêmes entreprises d'améliorer leurs actions de ciblage publicitaire. Bien que ces pratiques soient banalisées par certaines compagnies et qu'elles soient très courantes en 2020, de plus en plus d'utilisateurs commencent à faire part de leur désapprobation.

Il faut s'adapter à cette nouvelle tendance

Justement, certains moteurs de recherche l'ont bien compris. C'est par exemple le cas de DuckDuckGo, mais il n'est pas le seul. En effet, Firefox bloque désormais automatiquement les cookies. Google pourrait aussi s'inscrire dans cette tendance dans le courant des mois prochains.

Le 15 janvier 2020, l'entreprise américaine annonçait qu'elle voulait supprimer la prise en charge des cookies. **Google pourrait donc revoir ses priorités en plaçant la confidentialité et le respect de la vie privée de ses utilisateurs au premier plan.**

Selon Justin Schuh, directeur de l'ingénierie chez Google Chrome : **"Les utilisateurs exigent de plus en plus de confidentialité et cherchent une transparence totale de la part de leur navigateur.** Ils veulent avoir le choix et le contrôle de leurs données, et il est clair que l'écosystème Web doit évoluer pour répondre à ces demandes croissantes. Les cookies sont au cœur du problème. C'est pour cette raison que nous prenons la décision de les supprimer progressivement".

Source : Valentin Cimino

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