Juin-juillet 2022 • Vol. 9 n° 6

PASSION AFFAIRES et technologies

Présentés ce mois-ci :

Entreprise TI classée #1 à Québec en 2022 par **ThreeBest Rated®**

« La sécurité est importante chez Amisco…

On doit respecter certaines normes, dont C-TPAT. La compétence et la collaboration d'ARS sont indispensables à ce niveau. **Nous sommes à mettre en place une culture de cybersécurité qui protège concrètement notre organisation des cyberattaques.**

Avec les rapports de gouvernance, on est en mesure de prendre les bonnes décisions pour garder un niveau de sécurité adéquat. Cette vision globale qu'ARS nous donne rassure la direction. »

Gilbert Beaudoin
Directeur TI
Les Industries Amisco Ltée

La cybersécurité : une nécessité pour les entreprises

Avec l'omniprésence des données et de la technologie dans l'économie, la cybersécurité est passée d'un coût additionnel à une nécessité pour les entreprises, croit Fehmi Jaafar, professeur au département d'informatique et de mathématique de l'Université du Québec à Chicoutimi (UQAC).

« À partir des années 90, le patrimoine technologique de l'entreprise est devenu son bien le plus stratégique. De plus en plus, l'informatique est présente dans tous les secteurs de l'économie. Aujourd'hui, les données créent la richesse d'une entreprise, sa valeur ajoutée. Sans collecter et analyser des données, les entreprises ne peuvent plus être aussi compétitives parce que cette analyse est nécessaire pour fidéliser la clientèle, offrir des produits personnalisés, etc. L'informatique est devenue un avantage concurrentiel, surtout l'analyse des données », explique l'enseignant.

Or, pour pouvoir utiliser des données, il faut être sûr de leur confidentialité. La sécurisation des systèmes informatiques est parfois même une obligation légale, notamment en ce qui a trait à la gestion des données personnelles.

SUITE PAGE 2

Augmentation exponentielle

Selon l'expert, toutes les statistiques montrent une augmentation exponentielle des cyberattaques. Celles-ci doubleraient, voire plus, chaque année dans tous les domaines et pour tous les types d'entreprises. Statistique Canada estime que 21 % des entreprises au pays ont été victimes de cyberattaques. 47 % des PME ont été touchées.

Ces cyberattaques représentent un coût énorme pour les entreprises. En 2021, ces frais ont atteint des niveaux jamais vus, **selon le Centre canadien pour la cybersécurité. Le coût moyen d'une violation de données se chiffrait ainsi à 6,35 M$**. Les rançongiciels, qui ont augmenté de 151 % à l'échelle mondiale dans la première moitié de 2021 comparativement à la même période en 2020, ont coûté en moyenne 2,3 M$ aux entreprises l'an dernier, incluant le coût de la rançon payée ou du rétablissement du réseau compromis. ARS Solutions estimait pour sa part, en se basant sur les soumissions au service d'identification des rançongiciels ID Ransomware, que ces programmes malveillants avaient causé des pertes économiques totalisant de 19 G$ à 75 G$ en 2020, dont 165 à 659 M$ au Canada.

Porte d'entrée

« Les menaces les plus courantes ont comme porte d'entrée l'employé, soit celui qui est mal formé ou celui qui est malintentionné. Toutes les grandes cyberattaques qui ont pris comme cible les entreprises, dernièrement, l'ont fait à travers des courriels frauduleux (hameçonnage) ou par le biais d'un employé qui a eu accès à des données confidentielles et les a vendues pour faire de l'argent », indique Fehmi Jaafar.

Les rançongiciels, qui ont également comme porte d'entrée les employés, constituent une autre des cybermenaces les plus courantes actuellement. « Par exemple, un employé qui n'est pas bien formé va cliquer sur un lien et cela va installer un virus sur le système de l'entreprise ou ça ouvre une porte à un attaquant malveillant externe. Le virus ou le hacker vont alors crypter les données pour demander une rançon. Ils vont créer un climat d'urgence et de panique dans l'entreprise pour que les dirigeants payent rapidement la rançon. »

Facile à corriger

Selon M. Jaafar, en adoptant de bonnes pratiques et des mesures de base, il est assez facile pour les entreprises, peu importe leur taille, de se protéger contre ces menaces. «La majorité des cyberattaques, 90 % environ, ce sont des problèmes qui ne sont pas très compliqués à corriger. Par exemple, on peut offrir une formation de base aux employés, suivre les obligations légales pour sécuriser les données de nos clients, s'assurer que les logiciels et équipements sont les plus sécuritaires possible, vérifier que le système d'exploitation qu'on utilise est toujours supporté, etc. »

Pour éliminer les risques d'urgence de payer liés aux rançongiciels, le professeur recommande d'avoir toujours une sauvegarde des données essentielles aux processus d'affaires. Crypter les données sensibles à l'interne permet de s'assurer que même si un attaquant a accès à celles-ci, il ne pourra pas les utiliser.

Du côté des employés malveillants, il faut avoir des accès clairs pour chaque employé. « Ça se peut qu'on ait un employé qui a besoin d'avoir ce droit de visiter, par exemple, les comptes des clients. Au moment où cette personne consulte cinq millions d'enregistrements, il y a quelque chose qui cloche. Il faut donc avoir des systèmes à l'interne qui lancent des alertes lorsqu'il y a des anomalies, par exemple si un employé se connecte dans une plage horaire inhabituelle ou d'un emplacement étrange, fait une activité anormale, etc. », souligne le professeur.

Cyberrésilience

La cyberrésilience est un terme de plus en plus utilisé. Elle se base sur les mêmes pratiques que la cybersécurité, soit celles de protéger l'intégrité et la sécurité des données, mais elle met l'accent sur la continuité des affaires. « Elle part du principe qu'on aura une cyberattaque contre l'entreprise. On va mettre en œuvre les meilleures pratiques, mais après ça, il faut avoir un plan B. Même s'il y a un problème qui vient d'ailleurs, est-ce qu'on peut assurer la continuité de nos affaires? Il faut des plans pour faire face aux incidents qui peuvent se produire », affirme Fehmi Jaafar, qui croit que les entreprises doivent avoir une sensibilité à ce propos.

Source : Karine Boivin Forcier

NOUVEAU! Rapport anti-hammeçonnage 2022

Découvrez comment identifier et contourner les plus récentes tendances d'hameçonnage en 2022! En téléchargeant ce rapport, vous découvrirez :

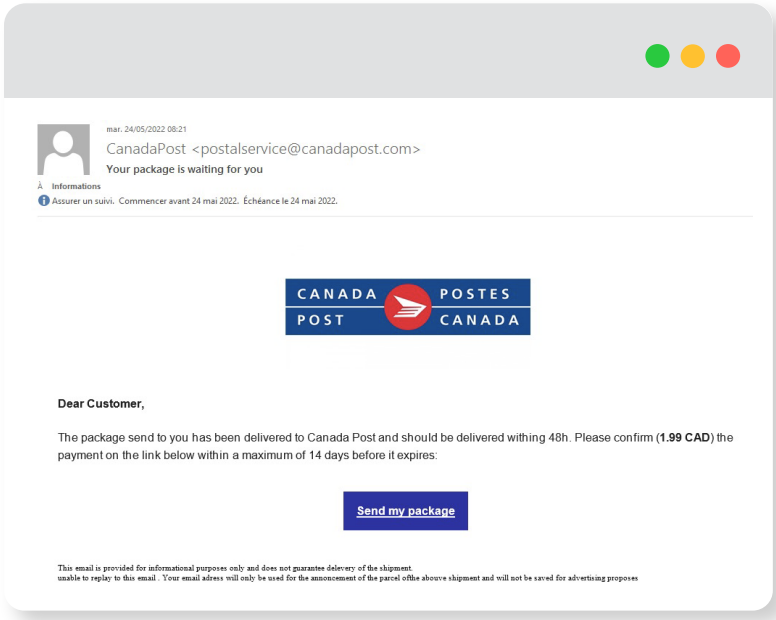
1. Formulaire d'autoévaluation de votre niveau de sécurité;
2. 9 prédictions de cybersécurité 2022;
3. 3 méthodes d'attaques par hameçonnage;
4. Des exemples réels de tentatives d'hameçonnage reçues chez ARS;
5. Et plus encore....

Téléchargez-le SANS FRAIS : www.ars-solutions.ca/rapport-anti-hameconnage-2022

Poste Canada : un déguisement souvent utilisé par les cybercriminels pour les tentatives d'hameçonnage

Avec la tendance de télétravail qui se maintient ainsi que la croissance des achats en ligne, les services de livraison sont de plus en plus ciblés par les cybercriminels pour **les tentatives d'hameçonnage et c'est malheureusement souvent le cas de Poste Canada.**

En voici un exemple reçu récemment à l'adresse générale d'ARS Solutions (info@ars-solutions.ca) :



mar. 24/05/2022 08:21
CanadaPost <postalservice@canadapost.com>
Your package is waiting for you
À Informations
Assurer un suivi. Commencer avant 24 mai 2022. Échéance le 24 mai 2022.

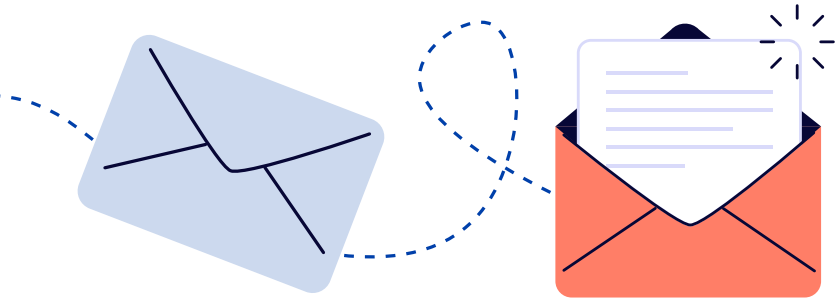
CANADA POSTES
POST CANADA

Dear Customer,

The package send to you has been delivered to Canada Post and should be delivered withing 48h. Please confirm (**1.99 CAD**) the payment on the link below within a maximum of 14 days before it expires:

Send my package

This email is provided for informational purposes only and does not guarantee delevery of the shipment.
unable to replay to this email . Your email adress will only be used for the annoncement of the parcel ofthe abouve shipment and will not be saved for advertising proposes



→ Quoi surveiller?

Le courriel est en anglais seulement, alors que les notifications par courriel de Poste Canada sont normalement bilingues (message en anglais suivi du même message en français).

Le courriel est impersonnel et contient l'appellation générale "Dear Customer (cher client)".

Ce type de courriels d'hameçonnage comprend souvent un appel à l'action, comme "Send my package (envoyer mon colis)" dans ce cas-ci. Il est important de ne PAS cliquer sur aucun lien d'un courriel avant d'avoir bien vérifié sa légitimité.

Il s'agit d'une situation inhabituelle, car on ne reçoit pas ce genre de notification de la part de ce service de livraison normalement chez ARS Solutions.

Vérifier auprès des employés concernés si nous avons bel et bien une ou plusieurs commandes actives reliées à ce service de livraison, quitte à appeler directement Poste Canada pour valider l'information en passant par leur site Web officiel pour obtenir leur véritable numéro de téléphone. Ne jamais passer par les coordonnées du courriel.

En cybersécurité, **un seul clic peut être fatal**. On doit être vigilant en tout temps. N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.

Nouvelle tendance pour les rançons?

Selon un récent rapport émis par Cybereason, **un nouveau groupe de cybercriminels nommé Black Basta a vu le jour en avril 2022**. Ce groupe vise plus particulièrement les entreprises du **Canada, des États-Unis, de l'Angleterre, de l'Australie et de la Nouvelle-Zélande**. Aucun secteur n'est épargné : manufacturier, construction, transport, télécommunications, pharmaceutique, cosmétique, plomberie, chauffage, concessionnaires automobiles...

Des montants en hausse qui ne vous redonneront pas nécessairement vos données

L'industrie de la cybercriminalité est elle aussi en évolution. Les montants réclamés par les cybercriminels sont en hausse. **Depuis avril 2022, 50 entreprises ont été extorquées par Black Basta pour des montants allant jusqu'à 2 millions.** Black Basta est opéré par les cybercriminels de deux anciens groupes parmi les plus fructueux en 2021.

Cybereason considère **le niveau de menace élevé compte tenu du potentiel destructeur des attaques**. La variante Linux de Black Basta cible les machines virtuelles VMware ESxi exécutées sur des serveurs d'entreprise Linux.

Ne pas rester vulnérable

Selon un nouveau rapport de Kaspersky, dans les organisations du monde entier qui ont déjà subi une cyberattaque, **88 % d'entre elles choisiraient de payer la rançon si elles étaient à nouveau victimes, en espérant obtenir un accès immédiat à leurs données**. Serait-ce parce qu'elles n'ont pas en place ce qu'il faut?

Malheureusement, payer la rançon plutôt que de mettre en place les mesures de protection nécessaires **maintient ces entreprises dans une position d'extrême vulnérabilité et projette une image négative auprès de leur clientèle**. Sans compter la hausse des montants réclamés par les cybercriminels.

Mettre en place des mesures préventives

Les experts continuent de recommander aux victimes de ne jamais payer de rançon, car rien ne leur garantit la récupération de leurs données, sans compter que ce geste encourage les cybercriminels à poursuivre leurs activités illégales.

Il est plutôt fortement conseillé de mettre en place des mesures préventives comme une **stratégie de sauvegardes adaptée aux cyberattaques**, l'application des **mises à jour de sécurité** ainsi qu'**une stratégie de défense basée sur l'interception des incidents de sécurité avec prise d'action rapide**. Les mises à jour de sécurité étant de plus en plus fréquentes et nécessitant plusieurs heures de déploiement, il devient primordial d'aller vers des **technologies permettant l'automatisation**. En réduisant la fenêtre de déploiement, on réduit ainsi la fenêtre de vulnérabilité de l'entreprise.

Les coûts de mise en place de mesures préventives sont beaucoup moindres que ceux engendrés par le paiement des rançons, sans compter les arrêts d'opérations en cas d'attaque et les risques de fermeture. **Les entreprises doivent désormais prévoir un budget réservé exclusivement à la sécurité, en sus de leur budget informatique habituel.**

Sources : VentureBeat et MSSP Alert

6655, boul. Pierre-Bertrand, bureau 301, Québec, QC G2K 1M1
www.ars-solutions.ca I info@ars-solutions.ca I 418 872-4744