Mai 2022 • Vol. 9 n° 5

PASSION AFFAIRES et technologies

Présentés ce mois-ci :

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

« La cybersécurité est une priorité absolue pour Planchers PG…

Nous avons à respecter des normes de sécurité rigoureuses afin d'assurer la pérennité de notre entreprise. **L'expertise qu'ARS éprouve dans le domaine manufacturier et les environnements complexes nous permet d'atteindre, voire de dépasser les exigences liées à la certification C-TPAT.**

De plus, **ARS est en mesure de travailler de concert avec les exigences toujours plus élevées de nos assureurs afin de respecter les critères d'admissibilité aux polices d'assurance contre les cyberrisques.** Nous sentons que l'équipe est en parfaite maîtrise de notre environnement et, surtout, qu'elle comprend notre réalité de production.

ARS est donc un véritable partenaire d'affaires et nous permet de se concentrer sur la croissance de notre entreprise sans se soucier de la cybersécurité. »

Alain Bédard
Directeur de la gestion des systèmes d'information
Planchers PG inc.

Cyberassurance : les 3 questions les plus fréquemment posées

Vous avez sûrement remarqué que votre courtier en cyberassurance vous pose plus de questions que par la passé lors de vos renouvellements. **La fréquence des cyberattaques ne cesse d'augmenter, les attaques sont de plus en plus sophistiquées et les cybercriminels de plus en plus audacieux.**

Les contrats d'assurance en cas de cyberattaque vont donc changer. Les entreprises doivent absolument se conformer aux exigences des compagnies d'assurance si elles veulent être éligibles. **Les assureurs ne proposeront pas des polices d'assurance aux organisations qui accordent peu d'attention à leur cybersécurité.**

SUITE PAGE 2

On vous présente aujourd'hui **3 questions que nos clients nous posent fréquemment de la part de leur cyberassureur.**

Question #1 : Jusqu'à quel niveau les systèmes de sécurité que vous avez développés pour nous sont étanches?

La réponse est la suivante : On a mis en place 1) des copies de sauvegardes qui vous protègent des cyberattaques, 2) une cybersurveillance qui détecte les incidents de sécurité et 3) un programme de formation et de simulation d'hameçonnage afin de développer votre acuité et celle de votre personnel interne à détecter les attaques qui se présentent sous cette forme.

Par contre, il n'existe pas de système 100 % à l'épreuve des attaques. La sécurité est une gestion de risques comme le vol, le feu et le vandalisme, quoique **les cyberattaques sont maintenant la menace numéro 1 pour les entreprises et les assureurs**. Ceci inclut non seulement les cyberattaques, mais aussi le vol d'informations et de temps. Les entreprises doivent prévoir une augmentation importante du budget relié à la sécurité informatique pour les prochaines années.

Question #2 : Dans l'éventualité où une attaque réussissait à nous atteindre, quel serait le plan de contingence que vous appliqueriez?

La réponse est la suivante : Chez ARS, nous avons mis en place un processus pour remettre les services en fonction chez tout client qui subit une cyberattaque. Un plan de contingence est plus personnalisé, donc adapté à chaque entreprise. Si vous souhaitez mettre en place un plan de contingence dans votre organisation, nous pouvons en discuter ensemble.

Question #3 : Est-ce qu'une assurance supplémentaire est nécessaire avec les systèmes de sécurité informatiques mis en place?

La réponse est la suivante : En gros, l'assurance va servir à payer la compagnie TI pour récupérer les informations. Ça devrait comprendre les coûts de main-d'œuvre, la rançon, les frais d'avocats (par exemple en cas de poursuites suite à la fuite d'informations personnelles), les dommages reliés à l'arrêt ou la fermeture de l'entreprise, etc. Toutefois, le FBI ne recommande pas de payer les rançons puisqu'on encourage cette industrie, dirigée par des malfrats. De payer la rançon ne garantit pas non plus que les données vont être récupérées parce qu'on traite avec des gens malhonnêtes. La fermeture de l'entreprise demeure également un risque important.

L'assurance n'empêche pas les cyberattaques. Plusieurs de nos clients prennent quand même une assurance pour les avantages cités précédemment. C'est une protection additionnelle qui les rassure, mais on doit d'abord mettre en place ce qui est recommandé.

Conseils anti-hammeçonnage

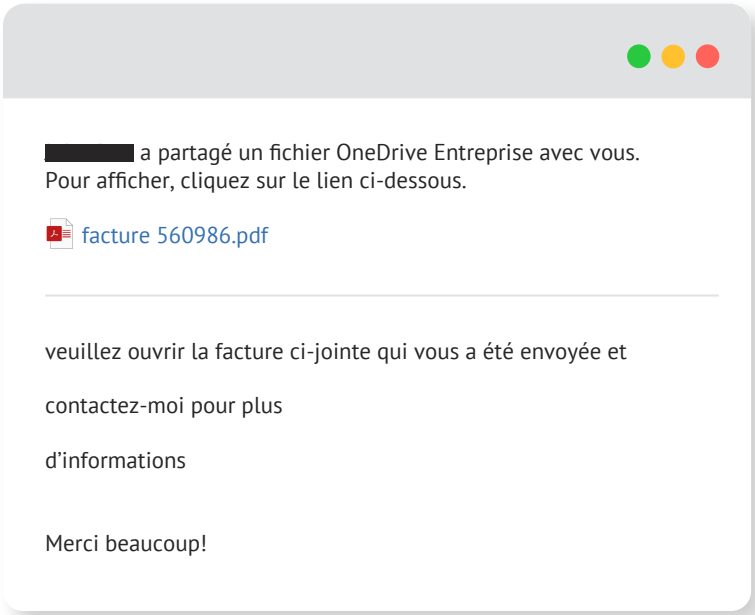
Continuez de lutter contre la cybercriminalité! Inscrivez-vous pour recevoir nos **NOUVEAUX "conseils anti-hameçonnage" SANS FRAIS** et gardez vos employés alertes. **Vous recevrez ensuite un conseil à tous les mois par courriel.**

Pour vous inscrire :
www.ars-solutions.ca/conseils-anti-hameconnage-phase-2/
info@ars-solutions.ca • 418 872-4744 #233

Tentative d'hameçonnage provenant d'un client piraté

Tout comme votre entreprise, **vos clients peuvent être la cible des cybercriminels et voir leur réseau infecté** à la suite d'une tentative d'hameçonnage fructueuse.

Récemment, chez ARS Solutions, nous avons reçu un courriel à l'adresse générale de l'entreprise (info@ars-solutions.ca) et celui-ci semblait très légitime. Il provenait de l'un de nos clients, que nous ne nommerons pas pour respecter la confidentialité. Le courriel contenait la véritable bannière de signature professionnelle de l'adjointe aux ressources humaines sur place et il faisait **mention d'une facture partagée via un fichier OneDrive Entreprise et que pour l'afficher, il fallait cliquer sur le lien ci-dessous :**


[redacted] a partagé un fichier OneDrive Entreprise avec vous.
Pour afficher, cliquez sur le lien ci-dessous.

facture 560986.pdf

veuillez ouvrir la facture ci-jointe qui vous a été envoyée et

contactez-moi pour plus

d'informations

Merci beaucoup!

Pour consulter la facture en question, **nous devions cliquer sur un lien qui menait vers une page de connexion à un compte Microsoft pour accéder au fichier via OneDrive**. Il s'agit d'une technique d'hameçonnage couramment utilisée pour usurper des identifiants personnels **(adresse courriel et mot de passe)**.

Heureusement, **nos employés sont tellement sensibilisés aux différentes techniques d'hameçonnage que personne n'a cliqué sur le lien** et ça n'a pris que quelques secondes après la réception du courriel pour que l'un de nos employés visés par l'envoi frauduleux avertisse le reste de l'équipe qu'un courriel malicieux avait été reçu de la part de l'un de nos clients, qu'il ne fallait surtout pas cliquer dessus et qu'on devait le détruire. **Le simple fait de cliquer sur le lien aurait pu être bien dommageable pour notre entreprise et infecter l'ensemble du réseau.**

Quelques heures plus tard, **nous avons reçu un courriel du client en question qui tenait à nous informer que la boîte courriel de l'un de leurs employés avait été piratée** le jour-même en nous invitant à supprimer le courriel si nous l'avions reçu, de changer immédiatement notre mot de passe si nous avions déjà cliqué sur le lien en plus d'effectuer un scan de notre poste avec un antivirus et de rapporter l'incident à notre partenaire TI.

En cybersécurité, **un seul clic peut être fatal**. On doit se méfier d'absolument tout pour éviter le pire, car **il vaut mieux être paranoïaque que piraté…** N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.

Suivre sa consommation d'énergie grâce aux plateformes en ligne

De plus en plus, il est possible de suivre sa consommation d'énergie en ligne. Cela permet de réduire votre consommation, mais également de consommer mieux et plus respectueusement de l'environnement! Voici 3 outils pour vous aider :

1. Utiliser un monitoring énergétique

Un **monitoring énergétique** vous permet d'économiser de l'énergie tous les jours. C'est un **ensemble d'appareils** qui vous permettent de suivre votre consommation d'énergie au sein de votre habitation, tout en **ciblant les principaux postes de consommation**.

Le monitoring énergétique vous présente sous forme de **graphiques** votre consommation énergétique, tout en vous indiquant la part de **charges fantômes** dans votre facture énergétique. Votre **empreinte carbone** est également indiquée sur ces appareils, vous permettant d'allier économies d'énergie et consommation plus verte!

2. Adopter la domotique énergétique

Fonctionnant selon le même principe, **la domotique énergétique** vous permet **d'automatiser certaines tâches**, et de **contrôler votre consommation énergétique** au quotidien. Ainsi, même si vous êtes en week-end, il vous est possible de réduire votre chauffage si la météo est plus clémente. Vous pouvez également programmer une machine à laver selon les **heures creuses** de la journée.

3. Opter pour des appareils plus performants

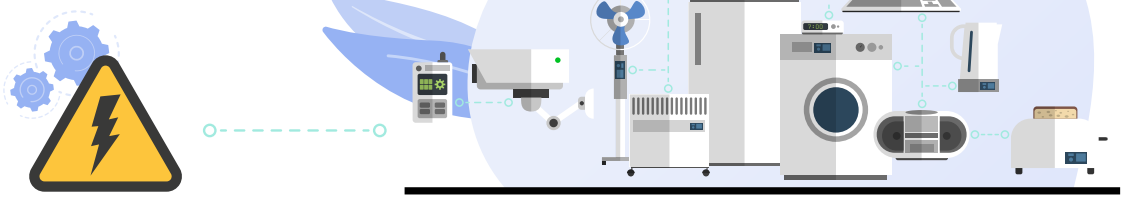
Adopter des appareils plus performants et donc plus économes, vous permettra de diminuer drastiquement votre facture énergétique. Pour connaître la **performance énergétique d'un appareil électroménager**, référez-vous à son **étiquette énergie**. Cela vous permettra de connaître les informations relatives à la consommation ainsi qu'à l'empreinte carbone de votre appareil!

En adoptant quelques gestes simples, vous réduirez les dépenses inutiles : éteignez vos appareils électroménagers après usage, pour diminuer les charges fantômes, adaptez la température de votre chauffage selon les pièces de votre logement, ou encore aérez quotidiennement pour renouveler l'air et éviter l'humidité!

C'est d'autant plus important dans une période où le télétravail se développe de plus en plus. **Les personnes faisant 100 % de travail à distance sont maintenant en charge à la fois de leur consommation personnelle et professionnelle** (on l'oublie souvent, mais le travail à distance via votre ordinateur consomme aussi de l'énergie).

Si vous êtes dans cette situation, un **compteur communicant Linky** vous sera bien utile pour quantifier vos dépenses énergétiques et les réduire au maximum. Ce compteur nouvelle génération est **très bénéfique en termes d'économie d'énergie et d'argent**, notamment grâce aux relevés à distance et au suivi en temps réel de la consommation. Vous n'avez qu'à **contacter Hydro-Québec**, qui a déjà installé plus de 3,8 millions d'appareils depuis 2013, pour obtenir le vôtre.

Source : Hello Watt



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