Cism Gestion Informatique

Le Journal TECHNO

Quoi de neuf ?

Si vous êtes une PME à Montréal qui souhaitez **transformer la technologie en un puissant outil qui peut faire avancer votre entreprise** au lieu d'un problème qui vous coûte du temps & de l'argent, alors nous pouvons vous aider! Contactez-nous, dès maintenant, au : 514-830-8184 .

Également, le mois dernier nous mettions en ligne notre nouveau Site Web revampé afin de vous offrir une expérience informatique agréable, utile et accessible. Aussi, afin de vous tenir informé des dernières avancées technologiques, vous trouverez sur ce Site, notre fil de nouvelles quotidiennes qui présente un nouvel article chaque jour au : cisminformatique.com/category/blog/.

Juin 2021

Cette publication mensuelle est une gracieuseté de Bernard Houde, Président de CISM Gestion Informatique.

Notre Mission est de vous aider à réaliser vos projets de croissance grâce à nos solutions innovantes en matière de Serveurs, de Logiciels, de Cloud, de Sécurité, de Maintenance et de Surveillance en temps réel. Nos mots d'ordre sont **Efficacité**, **Fiabilité** et **Sécurité**.

Ne laissez pas vos employés devenir votre plus grande vulnérabilité

Il y a quelques années, *TechRepublic* a publié un article intitulé: « Les employés sont presque aussi dangereux pour les affaires que les pirates informatiques et les cybercriminels. » Du point de vue de l'entreprise, vous pourriez penser que c'est tout simplement inexact. Votre entreprise s'efforce d'embaucher les meilleures personnes qu'elle puisse trouver - des personnes douées pour leur travail qui ne rêveraient jamais de mettre leur propre employeur en danger.

Et pourtant, de nombreux employés le font, et c'est presque toujours involontaire. Vos employés ne pensent pas aux moyens de compromettre votre réseau ou d'essayer de mettre des logiciels malveillants ou des rançongiciels sur les ordinateurs de l'entreprise, mais cela arrive. Une étude de Kaspersky a révélé que 52% des entreprises reconnaissent que leurs employés sont « leur plus grande faiblesse en matière de sécurité informatique ».

D'où vient cette faiblesse? Elle découle de différentes choses et varie d'une entreprise à l'autre, mais ça dépend en grande partie du comportement des employés.

Erreur humaine

Nous faisons tous des erreurs. Malheureusement, certaines erreurs peuvent avoir de graves conséquences. Voici un exemple: un employé reçoit un courriel de son patron. Le patron souhaite que l'employé achète plusieurs cartes-cadeaux et leur envoie les codes des cartes-cadeaux dès que possible. Le message peut dire: « Je vous fais confiance avec cela » et renforcer le sentiment d'urgence chez l'employé.

Le problème est que c'est faux. Un escroc utilise une adresse courriel similaire à celle qu'un responsable, superviseur ou autre dirigeant pourrait utiliser. C'est une arnaque par hameçonnage, et ça fonctionne. Bien que cela ne compromette pas nécessairement votre sécurité informatique à l'interne, il met en évidence les lacunes dans les connaissances des employés.

Un autre exemple courant, également par courrier électronique, est que les cybercriminels envoient des fichiers ou des liens qui installent des logiciels malveillants sur les ordinateurs de l'entreprise. Les criminels déguisent une fois de plus le courriel comme un

Suite à la page 2

Suite de la page 1

message légitime d'une personne au sein de l'entreprise, d'un fournisseur, d'une banque ou d'une autre entreprise avec laquelle l'employé peut être familier.

C'est cette familiarité qui peut faire trébucher les employés. Tout ce que les criminels doivent faire est d'ajouter un sentiment d'urgence, et l'employé peut cliquer sur le lien sans réfléchir davantage.

Négligence

Cela se produit lorsqu'un employé clique sur un lien sans réfléchir. Cela peut être dû au fait que l'employé n'a pas reçu de formation pour identifier les courriels frauduleux ou que l'entreprise n'a pas mis en place de Politique de sécurité informatique complète.

Les habitudes de navigation dangereuses constituent une autre forme de négligence. Lorsque les employés naviguent sur le Web, que ce soit pour la recherche ou pour tout ce qui concerne leur travail ou pour un usage personnel, ils doivent toujours le faire de la manière la plus sûre possible. Dites aux employés d'éviter d'accéder à de « mauvais » sites Web et de ne cliquer sur aucun lien qu'ils ne peuvent pas vérifier (comme des annonces).
Les mauvais sites Web sont assez subjectifs, mais une chose que tout utilisateur Web devrait rechercher est « https » au début de toute adresse Web. Le « s » vous indique que le site est sécurisé. Si ce « s » n'est pas là, le site Web manque de sécurité. Si vous saisissez des données sensibles sur ce site Web, telles que votre nom, votre adresse courriel, vos coordonnées ou vos informations financières, vous ne pouvez pas vérifier la sécurité de ces informations et elles peuvent se retrouver entre les mains de cybercriminels.

> **"Une étude de Kaspersky a révélé que 52% des entreprises reconnaissent que leurs employés sont leur plus grande faiblesse en matière de sécurité informatique."**

Un autre exemple de négligence est la mauvaise gestion des mots de passe. C'est courant d'utiliser des mots de passe simples et d'utiliser les mêmes mots de passe sur plusieurs sites Web. Si vos employés le font, cela peut exposer votre entreprise à un risque énorme. Si des pirates informatiques mettent la main sur l'un de ces mots de passe, qui sait à quoi ils pourraient accéder. Une politique de mot de passe stricte est une nécessité pour chaque entreprise.

Transformez la faiblesse en force

La meilleure façon de surmonter la faiblesse humaine de votre sécurité informatique est l'éducation. Une politique de sécurité informatique est un bon début, mais elle doit être appliquée et comprise. Les employés doivent savoir quels comportements sont inacceptables, mais également être conscients des menaces qui existent. Ils ont besoin de ressources sur lesquelles ils peuvent compter dès que des menaces surgissent afin d'être traités correctement. Travailler avec une entreprise de services informatiques peut être la réponse - ils peuvent vous aider à jeter les bases pour transformer cette faiblesse en une force.

Télécharger Gratuitement Notre Guide : « Comment choisir votre fournisseur de services informatiques »

Vous apprendrez:

- Les 3 méthodes les plus courantes pour les entreprises informatiques de facturer leurs services et les avantages & inconvénients de chaque approche
- Un modèle de facturation commun qui met TOUS LES RISQUES sur vous, le client, lors de l'achat de services informatiques; vous apprendrez ce que c'est et pourquoi vous devez éviter de l'accepter
- Des exclusions, des frais cachés et d'autres clauses « pièges » que les entreprises informatiques mettent dans leurs contrats que vous NE souhaitez PAS accepter
- Comment vous assurer de ce que vous obtenez afin d'éviter les déceptions, la frustration et des coûts supplémentaires plus tard que vous n'aviez pas anticipés

Demandez votre exemplaire **GRATUIT** dès aujourd'hui sur : www.cisminformatique.com/21questions

Pleins feux sur nos précieux clients

40 ans d'histoire et d'expérience, visant l'excellence, PCM Innovation a connu une croissance importante en acquérant plusieurs sociétés et en créant des partenariats. Cette société offre des solutions intégrées en ingénierie et outillage pour ses clients qui sont des leaders mondiaux des secteurs de l'aviation, du spatial et du transport. Ses produits sont des lignes d'assemblage, gabarits, moules et pièces de courtes séries.

Leur gestion de projet est soutenue par des indicateurs de performance PLM et un système ERP. Cette société investit constamment en R&D et dans la formation. Ses capacités distinctives et avantages compétitifs sont: l'outillage de grande dimension, les composites avancés, l'expertise avec des logiciels CAO, des solutions clé en main, un service d'installation et une expertise en usinage.

« ...Avec un soutien sur mesure et une offre de service globale, CISM Gestion Informatique est une continuité de nos opérations, comme un de nos départements. Grâce à leur disponibilité, transparence, flexibilité et proactivité, **nous pouvons compter sur eux comme un véritable partenaire TI** ».

PCM Innovation fait confiance à CISM Gestion Informatique pour la gestion et la sécurité de l'ensemble de son parc informatique.

Plan De Reprise Rapide Des Opérations En Cas De Catastrophe Majeure

Il vous est sûrement déjà arrivé de perdre vos données suite à un bris d'ordinateur ou à cause d'un virus. Vous souvenez-vous à quel point vous étiez désemparé suite à cette catastrophe?

Alors, imaginez à quel point vous le seriez, **si une catastrophe majeure empêchait tout le personnel de votre entreprise de poursuivre leurs opérations informatiques**. Vous ne pourriez plus vendre vos produits, vous n'auriez plus accès à votre inventaire, votre chaîne de production informatisée ne serait plus fonctionnelle, l'accès aux informations de votre clientèle serait inexistant; bref vous seriez aux abois.

Les municipalités et les grandes entreprises créent, mettent en place et testent régulièrement un plan de reprise rapide des opérations en cas de catastrophe majeure. Donc, que vous faut-il savoir pour créer votre propre plan en cas de catastrophe majeure?

D'abord, vous devrez déterminer le **temps maximum** pour lequel vous pourriez vous passer de l'accès au serveur. Prenez l'exemple d'une entreprise de distribution qui vend 250000 $ de produits par jour. Si elle ne peut opérer ses ventes pendant 4 jours ouvrables, celle-ci perdra un million de dollars en revenu, en plus des frais reliés aux opérations et aux salaires de ses employés assis à ne rien faire. Le président de cette société pourrait certainement vivre avec un plan de reprise rapide en 4 heures.

Ensuite, il vous faudrait implanter une **solution de sauvegarde** sur votre serveur. Je ne parle pas ici de simplement enregistrer vos données, mais de sauvegarder un serveur en totalité. Une sauvegarde complète consiste à conserver le système d'exploitation, les programmes et les données. De plus, elle devra être enregistrée sur un disque dans vos bureaux et le Cloud. Ainsi, une reprise rapide de vos opérations pourrait avoir lieu à vos bureaux, si vous disposez déjà d'un serveur de relève ou d'un serveur virtuel dans le Cloud qui pourra être configuré au besoin en moins d'une heure.

La fréquence des sauvegardes est aussi très importante. Si une sauvegarde est effectuée 1 fois par jour et que vous devez y avoir recours, alors vous devrez revenir en arrière d'un jour et vous aurez perdu une journée de travail qu'il vous faudra reprendre. Par contre, si les sauvegardes étaient effectuées chaque heure, vous auriez un gain de temps considérable.

En dernier lieu, il vous faudra **documenter** chacune des opérations afin de vous assurer que le « jour J », les gens en place, à ce moment-là, connaîtront la procédure à suivre afin de remettre en fonction les opérations informatiques de votre société. De plus, une **simulation** biannuelle vous permettra de pratiquer la procédure de reprise rapide de vos opérations.

Hormis la sauvegarde complète d'un serveur, il existe la **réplication en temps réel**. Cette technique de reprise rapide des opérations est assurément la crème de la crème. Par son coût onéreux, elle s'adresse vraiment aux entreprises qui ne peuvent se permettre, ne serait-ce qu'une minute d'interruption. Il s'agit de mettre en place une structure de plusieurs serveurs sur lesquels on retrouvera les mêmes systèmes d'exploitation, mêmes logiciels et données répliquées.

Je comprends que cette dernière solution ne s'adresse peut-être pas à vous, par contre, dans le contexte d'une catastrophe majeure, celle-ci ne peut être négligée par les sociétés nécessitant une reprise en temps réel.

Par Bernard Houde, Président et conseiller senior, CISM Gestion Informatique

Êtes-vous coincé dans le piège du travail indépendant?

Beaucoup de personnes optent pour le travail indépendant afin d'avoir plus de contrôle sur leurs journées, à la recherche d'un meilleur équilibre entre vie professionnelle et vie privée. Mais la réalité devient vite très différente: de longues heures où vous mettez tout dans l'entreprise. Cela conduit à l'épuisement professionnel. Quelles actions pouvez-vous entreprendre pour éviter ou échapper à ce piège?

Déléguez plus de tâches. C'est difficile à faire, surtout lorsque vous voulez que les choses se passent bien. Portez votre attention sur l'embauche d'un ou plusieurs employés à la hauteur du défi et capables de répondre à vos besoins. Cela peut prendre un certain temps pour trouver la correspondance idéale, mais cela vaut la peine de trouver quelqu'un qui assumera des tâches cruciales et vous aidera à atteindre vos objectifs.

Inspectez vos systèmes et processus. Dans l'ensemble, vous avez besoin de systèmes et processus en place. Quand vous avez un cadre à suivre, il est beaucoup plus facile de récupérer votre temps et votre énergie. *Inc., 18 février 2021*

Profitez au maximum de votre main-d'oeuvre à distance

De plus en plus de gens travaillent à domicile. Avec une main-d'œuvre dispersée, les entreprises sont confrontées à de nouveaux défis auxquels elles n'ont pas été confrontées avec le modèle de bureau traditionnel. Maintenant, à mesure que les entreprises s'adaptent, elles cherchent des moyens de tirer le meilleur parti de leur main-d'œuvre éloignée.

1. Ils se réorganisent. Les entreprises examinent attentivement leur structure interne, ainsi que leurs systèmes & processus. Ils modifient la façon dont ils embauchent en augmentant leurs attentes. Parallèlement à cela, ils refont leur façon de coacher et de former. Ils réapprennent à tout faire à distance et des outils comme Slack et Zoom occupent une place centrale.

2. Ils investissent dans la technologie. Les entreprises intègrent de nouveaux outils et technologies. Ils investissent dans des outils de communication et de collaboration. Ils dépendent fortement du Cloud et des VPN. Ils achètent également des appareils tels que des ordinateurs portables et des PC pour leur main-d'œuvre distante afin de s'assurer que tout le monde utilise la même technologie approuvée, ce qui rend l'assistance et la sécurité plus efficaces. *Inc., 27 février 2021*

Utilisez la technologie pour favoriser votre entreprise

La main-d'œuvre d'aujourd'hui est très avertie, cela signifie que votre entreprise devrait l'être aussi. Vous voulez attirer de bons talents, alors tirer parti de vos prouesses technologiques serait possiblement un moyen de le faire.

Pensez à la façon dont vous interagissez avec les médias sociaux. Est-ce quelque chose qui est juste là, ou bien, quelque chose que vous utilisez pour toucher activement les clients, clients potentiels et votre communauté? TikTok, par exemple, s'appuie sur un algorithme puissant pour atteindre des publics spécifiques. Les entreprises peuvent en profiter pour diffuser du contenu et des publicités pour les intéressés. Selon Hootsuite, TikTok pousse 5 millions d'impressions quotidiennes pour certaines publicités.

Pour aller plus loin, vous pouvez mélanger l'intelligence artificielle (IA) avec la communication humaine. Les assistants virtuels (chatbots) sont très avancés et ont un impact certain sur la génération de leads. Ces assistants dirigent également les utilisateurs vers de vraies personnes pour poursuivre la conversation à des conditions spécifiques. Fondamentalement, il existe d'autres manières de personnaliser votre façon de communiquer, et cela vaut la peine d'investir. *Forbes, 12 mars 2021*

"I think we're named after computer passwords."