Cism Gestion Informatique

Le Journal TECHNO

Novembre 2021

Quoi de neuf ?

La Sécurité 3.0 est arrivée !

De nos jours, un **simple pare-feu** et un **banal Antivirus** NE sont PLUS SUFFISANTS pour protéger votre entreprise.

La prolifération des cyber criminels & cyber attaques demande une **Sécurité avancée** plus complète et davantage performante.

Vous avez manqué notre Webinaire "**La CyberSécurité, pourquoi vous ne pouvez plus l'ignorer** ?", alors inscrivez-vous et assistez à notre Webinaire en direct le 11 novembre prochain (2 nouvelles présentations à 9h ou à 13h) :

cisminformatique.com/webinaires/

Bernard dévoilera plusieurs faits et enseignements importants à connaître absolument.

Novembre 2021

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

La technologie évolue rapidement et notre **Mission** est de **vous aider à suivre le rythme** grâce à nos solutions nouvelles en matière de Serveurs, Logiciels, Cloud, Sécurité avancée & Surveillance en temps réel. Nos mots d'ordre sont **Efficacité**, **Fiabilité** et **Sécurité**.

Nos Webinaires GRATUITS !

- CyberSécurité : 11 nov. 2021
- Télétravail Sécurisé : 25 nov. 2021

(à 9h ou à 13h)

S'inscrire via notre Site Web : cisminformatique.com/webinaires/

10 Moyens Simples de protéger votre entreprise des CyberAttaques

Bien que personne ne conteste **la croissance des cyberattaques contre les entreprises** ces dernières années, nombreux sont les propriétaires de petites entreprises qui pensent qu'eux-mêmes et leur entreprise sont à l'abri de telles attaques. En effet, les propriétaires de petites entreprises sont sujet à croire que **les cybercriminels s'attaqueront aux PLUS GROS poissons**. Cependant, les cyberattaques sont des crimes d'opportunité, et les petites entreprises ont souvent accès à une bonne quantité de données sensibles sans protection majeure. En d'autres termes, ce sont des fruits faciles à cueillir.

En 2019, les 2/3 des répondants à une enquête sur la cybersécurité ne pensaient pas que leur PME serait victime d'une cyberattaque. Aussi, **seulement 9 %** des personnes interrogées **ont déclaré que la cybersécurité était une priorité absolue pour leur entreprise**, et 60 % n'avaient aucun plan pour dissuader une cyberattaque. Tout cela, malgré le fait que, selon un rapport de CNBC, les PME ont subi 43 % des cyberattaques signalées, et selon les données du « Ponemon Institute » et de « Keeper Security », 76 % des PME auraient subi une cyberattaque au cours de l'année précédente.

Chaque propriétaire de petite entreprise devrait avoir un PLAN pour détourner les cyberattaques afin que leur entreprise ne finisse pas comme une **autre statistique**. Voici quelques stratégies pour tenir les cybercriminels à distance :

Boostez votre sécurité Cloud Le stockage des données dans le Cloud est simple et économique, mais vous devez utiliser les plates-formes de stockage Cloud les plus sécurisées. Toutes les plateformes Cloud ne font pas de la sécurité une priorité, mais certaines le font.

Sécurisez toutes les parties de votre réseau Vos ordinateurs et les nombreux appareils intelligents connectés à votre réseau peuvent devenir des points faibles pour les pirates. Prendre des mesures pour protéger chaque appareil de votre réseau avec des **mots de passe forts** et des **mesures d'authentification robustes** contribuera grandement à tenir les pirates à distance. En fait, l'une des

Suite à la page 2

Suite de la page 1

mesures de sécurité la plus élémentaire que vous puissiez prendre pour votre réseau est de **restreindre l'accès à votre WiFi** avec un mot de passe fort.

Vos Antivirus traditionnels ne sont plus suffisants pour sécuriser les ordinateurs. Assurez-vous d'utiliser une **protection multicouche de type EDR** pouvant détecter les malwares inconnus.

Investissez dans des mesures de sécurité supplémentaires Les réseaux privés virtuels (VPN) et les pare-feux sont des outils très efficaces pour protéger votre entreprise contre les cyberattaques, même s'ils ne peuvent en empêcher 100 %.

Faites attention aux mises à jour et aux mises à niveau Lorsque vous êtes informé que l'un des outils technologiques que vous utilisez dispose d'une nouvelle mise à jour, il est facile de l'ignorer. Cependant, vous devez **vous engager à mettre à jour et à mettre à niveau régulièrement** ces outils, car les développeurs ajoutent souvent des correctifs à leurs programmes qui les rendent plus sûrs contre les attaques à chaque mise à jour. Il incombe donc aux propriétaires d'entreprise d'installer régulièrement des mises à jour pour leurs outils technologiques.

Sauvegardez vos données L'une des formes la plus courante de cyberattaque est l'attaque de rançongiciel, où les pirates informatiques garderont les données de votre entreprise en otage jusqu'à ce que vous leur payiez une rançon. Le **stockage** des données de votre entreprise **sur plusieurs sauvegardes** peut garantir que votre entreprise ne s'effondrera pas à cause de l'inaccessibilité de vos données.

Limitez l'accès des employés à votre réseau Autant nous souhaiterions que ce soit vrai, de nombreuses cyberattaques ne viennent pas de l'extérieur de votre entreprise. Au lieu de cela, elles proviennent de l'intérieur. Si vous souhaitez limiter les dommages qu'une personne au sein de votre entreprise peut causer lors d'une cyberattaque, la meilleure solution consiste à limiter son accès aux différentes parties de votre réseau.

Formez vos employés Également, de nombreuses cyberattaques se produisent non pas à cause de l'intention malveillante d'un employé, mais **à cause de son ignorance**. Ils cliquent sur un lien dans un courriel sommaire et tombent dans le piège d'un stratagème d'hameçonnage, donnent volontairement leur mot de passe sans y penser ou choisissent un mot de passe faible pour leur ordinateur. C'est pour ces raisons que vous devez **consacrer du temps à la formation de vos employés sur les MEILLEURES PRATIQUES en matière de sécurité**.

Mettez en place une « CULTURE DE LA SÉCURITÉ » sur votre lieu de travail Vous devez **faire de la cybersécurité une PRIORITÉ ABSOLUE**, non seulement pour votre service informatique, mais pour tous les services de votre entreprise. Lorsque tout le monde travaille ensemble pour protéger son lieu de travail contre une cyberattaque, vous avez de meilleures chances de réussir.

Protéger votre entreprise d'une cyberattaque nécessitera-t-il beaucoup de temps et d'argent ? **ABSOLUMENT**. *Pouvez-vous vous permettre d'ignorer plus longtemps la prévalence des cyberattaques* ? **Statistiquement, NON**. La triste vérité est que 60 % des PME victimes d'une cyberattaque finissent par fermer leurs portes dans les 6 mois. Ne vous mettez pas dans ce genre de position. Au lieu de cela, prenez au sérieux la cybersécurité de votre entreprise.

> « 76 % des PME aux États-Unis auraient subi une cyberattaque l'année précédente. »

TRUC de la semaine GRATUIT sur la CyberSécurité !

Ça n'arrive pas seulement aux autres : un hacker qui vole des données critiques rendant votre réseau inutilisable, la vie privée de vos clients dévoilée,...

Les cybercriminels inventent chaque jour de NOUVELLES façons d'infiltrer, voler et perturber votre entreprise. ARRÊTEZ-LES en **vous éduquant RÉGULIÈREMENT** sur les nouvelles façons de PROTÉGER vos actifs !

Nos conseils hebdomadaires rapides à lire contiennent une Solution unique & à jour qui vous permettra de garder une longueur d'avance sur les malveillants.

Obtenez votre TRUC de la semaine de Cybersécurité GRATUIT au
cisminformatique.com/cyber-securite-conseil-de-la-semaine/

Pleins feux sur nos précieux clients

Fondée en 1986 par Marc et Claude Simard, **Construction BURAM Inc.** œuvre dans le domaine du bâtiment commercial, institutionnel & industriel comme entrepreneur général et spécialisé en système intérieur.

Dès 1989, Luc Roberge se joint à l'équipe à titre d'estimateur et consolide leur expertise dans le domaine de la construction neuve, l'aménagement de bureaux et le secteur commercial et institutionnel. Il deviendra associé en 2002 et il est maintenant à la barre de l'entreprise comme Président.

C'est la transparence et la rigueur du travail qui la distinguent. Elle se démarque aussi par la complexité des projets réalisés et par le sens familial qui anime leur équipe. Leurs clients, employés, sous-traitants, fournisseurs & dirigeants ont tous une grande importance et sont la clé du succès de chaque projet. BURAM s'implique également dans la communauté en aidant les plus démunis.

C'est une **équipe dynamique** d'une douzaine d'employés en chantier & d'une dizaine de collaborateurs : estimateurs, chargés(es) de projets, adjointes et hommes d'entrepôt.

« CISM nous procure la SÉCURITÉ informatique SANS SOUCIS. »

CONSTRUCTION BURAM INC.

BURAM fait confiance à CISM Gestion Informatique pour les Services informatiques de son entreprise.

Avez-vous les outils pour gérer efficacement dans le monde du Travail à domicile ?

Fini le temps où les gestionnaires parcouraient leurs bureaux, discutaient avec leurs collègues et passaient du temps à la fontaine d'eau pour obtenir de précieuses informations sur l'état de leurs équipes. Avec la vie de travail à domicile d'aujourd'hui, les gestionnaires doivent **dépasser leurs anciennes méthodes de gestion d'une équipe de travail** au bureau et s'habituer à en gérer une efficacement sur Zoom ou toutes autres plates-formes commerciales utilisées par leur entreprise.

Je pense avoir quelques idées que je peux offrir à tous les entrepreneurs qui désirent atteindre leurs objectifs même s'ils doivent communiquer avec leurs équipes qui sont pour la plupart à la maison. Ces informations se présentent sous la forme de 5 questions différentes qui, si vous y répondez par l'affirmative, signifient que vous êtes probablement un gestionnaire en ligne efficace.

Fixez-vous des objectifs clairs pour votre équipe ? Les objectifs flous ne sont bons nulle part, mais au moins dans un espace de bureau physique, les membres de l'équipe peuvent clarifier les objectifs entre eux en personne. Cela devient beaucoup plus difficile en ligne, où les moyens de communication peuvent se limiter aux « SMS ». En tant que gestionnaire, assurez-vous que tous les membres de votre équipe comprennent leurs objectifs.

Êtes-vous doué pour embaucher les bonnes personnes ? Lorsque vous embauchez quelqu'un qui ne convient pas pour le poste, il est assez facile de savoir quand vous pouvez le surveiller au bureau. Cependant, si vous embauchez quelqu'un pour un poste à distance en ligne, cela peut prendre beaucoup plus de temps pour savoir si vous avez fait une erreur d'embauche, ce qui signifie que vous perdrez beaucoup plus de temps et d'argent.

Pouvez-vous bien déléguer votre travail ? Déléguer des tâches dans un bureau signifie que vous pouvez physiquement voir si un membre de l'équipe assume ces responsabilités. Si ce n'est pas le cas, vous pouvez toujours intervenir et réaliser le projet vous-même. Cependant, lorsque vous travaillez à domicile, vous devrez donner des instructions et des délais clairs, tout en assurant un suivi régulier, en déléguant des tâches à votre équipe.

Votre système de rémunération récompense-t-il les hautes performances ? Dans un contexte éloigné, les forces qui poussent votre équipe à performer au maximum de ses capacités n'ont pas autant d'impact. Étant donné que la rémunération et la haute performance sont inextricablement liées, un système de rémunération qui récompense directement les plus performants est le seul moyen de vous assurer que votre équipe travaille au mieux de ses capacités.

Continuez-vous à faire les choses que vous dites que vous ferez ? Instaurer la confiance ne demande peut-être pas beaucoup de travail au bureau, mais dans un environnement distant, la communication est essentielle pour établir une confiance bidirectionnelle avec votre équipe. Lorsque vous dites que vous allez terminer une tâche, terminez-la et assurez-vous que votre équipe est au courant. Cette intégrité, même si vous travaillez d'un endroit où personne ne peut vous voir, contribuera grandement à établir la confiance.

La gestion au-delà de l'espace de bureau ne doit pas être un grand mystère. Si vous souhaitez améliorer vos compétences en gestion à distance, bon nombre de nos livres, tels que « *Power Score* », « *Who* » et « *The CEO Next Door* », peuvent vous aider à y parvenir.

Le **Dr Geoff Smart** est le fondateur et président de **ghSMART**, qui aide les entreprises Fortune 500, les PDG et les entrepreneurs à succès à prendre des décisions judicieuses lorsqu'il s'agit de former des équipes talentueuses. Pendant 3 années consécutives, Forbes a classé **ghSMART** comme la meilleure société de conseil en gestion de son secteur et a publié 3 livres à succès décrivant ses principes.

L'économie « Le numérique d'abord » est là

Que votre entreprise soit une multinationale massive ou que vous soyez un humble « travailleur autonome », vous êtes maintenant entré dans l'ère de l'économie **« Le numérique d'abord »**. Aussi intimidant que cela puisse être de donner la priorité à la présence en ligne de votre entreprise, il existe **5 caractéristiques** qui **serviront bien vos clients** et conduiront à votre succès :

Flexibilité : Soyez prêt à perfectionner constamment vos connaissances des nouvelles technologies et des nouveaux logiciels et à apporter des modifications à vos systèmes si nécessaire.

À l'aise avec l'externalisation et l'automatisation : N'ayez pas peur de déléguer des tâches, telles que la gestion de l'exécution ou du marketing, qui vous éloignent du cœur du métier de votre entreprise.

Compétences en communication numérique : Cela signifie non seulement avoir les bons types de moyens de communication numérique (courriel, site Web, médias sociaux, etc.), mais également savoir les optimiser pour communiquer clairement et de manière cohérente avec vos clients.

Comprendre les attentes des clients : Dans un monde où les clients attendent des interactions transparentes et des résultats rapides, assurez-vous que chacun comprend clairement les besoins de chacun.

Cybersécurité : Même les « travailleurs autonomes » courent un plus grand risque de cyberattaques. Assurez-vous de protéger les données sensibles d'une manière qui convient le mieux à votre modèle d'entreprise.

Comment traiter « l'identité numérique » comme un problème de sécurité nationale

Alors que nous passons à une économie axée sur le numérique, le concept « d'identité numérique », c'est-à-dire l'ensemble d'attributs liés à votre identité que vous faites connaître en ligne, devrait être au 1er plan des discussions sur la sécurité nationale. Mais comment les personnes, les entreprises, les robots et les objets peuvent-ils équilibrer la confidentialité et la sécurité de manière à protéger leurs informations sensibles ?

L'un des moyens consiste à donner la priorité aux informations d'identification pertinentes plutôt qu'aux identités entières. Supposons que vous créez un compte sur un site Web auquel vous devez avoir 18 ans pour y accéder. Désormais, le site pourrait vous fournir un moyen de partager vos informations de permis de conduire et de carte de crédit. Après tout, cela garantirait que vous utilisez votre identité numérique sur ce site. Cependant, si le site est piraté, alors les pirates ont toutes ces informations sur vous, alors que tout ce dont le site avait vraiment besoin était votre âge.

Ainsi, ces informations d'identification pertinentes, également appelées « droits » (parce que ce sont les informations qui vous donnent droit à certains services), sont le meilleur point de départ pour une discussion sur l'identité numérique et la sécurité nationale.

Utilisez cette ASTUCE simple pour rendre votre téléphone davantage SÉCURISÉ

Si vous souhaitez protéger votre téléphone intelligent contre le piratage, il vous suffit d'éteindre et de rallumer votre téléphone. Cela vous semble-t-il trop simpliste et cliché ? PROBABLEMENT. Est-ce que ça marche? ABSOLUMENT.

La raison pour laquelle le simple fait d'éteindre et de rallumer votre téléphone peut contrecarrer les pirates est que, historiquement, le piratage a été un jeu de persistance. Continuez assez longtemps et les protocoles de sécurité d'une personne finiront par céder.

Cependant, avec les téléphones intelligents, les pirates informatiques ont découvert qu'ils n'avaient pas besoin d'être persistants car la plupart d'entre nous n'éteignons jamais nos appareils. Ainsi, le piratage des téléphones intelligents est devenu une option beaucoup plus attrayante pour les cybercriminels.

En éteignant et rallumant simplement votre téléphone régulièrement, vous offrez aux cybercriminels beaucoup moins d'occasions de pirater votre appareil, et ils essaieront probablement de pirater un téléphone intelligent qui reste allumé en permanence.

Compte tenu de la faible technicalité de cette solution, il n'y a aucune raison que quiconque possédant un téléphone intelligent soit incapable de le faire.