Cism Gestion Informatique

Le Journal TECHNO

Quoi de neuf ?

Nous avons le plaisir de vous informer que nous venons tout juste de mettre en ligne notre nouveau Site Web qui présente notre Offre de Services Informatiques améliorée concernant nos Services gérés, Infonuagique, Soutien tehnique et Sécurité réseau.

Vous y trouverez aussi notre équipe de techniciens professionnels, les témoignages de nos précieux clients, notre blogue de chroniques récentes, notre nouveau Programme de référencement, et bien plus. Nous vous invitons à le consulter dès aujourd'hui au: www.cisminformatique.com .

Mai 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**.

Votre politique de cybersécurité (ou son absence) vous laisse-t-elle ouvert aux attaques?

Chaque entreprise, grande ou petite, doit mettre en place une politique de cybersécurité pour ses employés. Ceux-ci ont besoin de savoir ce qui est acceptable et inacceptable en matière d'informatique. La politique doit fixer des attentes, établir des règles et donner aux employés les ressources nécessaires pour mettre la politique en œuvre.

Vos employés représentent la première ligne de défense de la cybersécurité de votre entreprise. Vous disposez peut-être de tous les logiciels antivirus, de protection contre les logiciels malveillants et de pare-feu du monde, mais si vos employés ne sont pas sensibilisés à la sécurité informatique ou ne comprennent pas les bases, alors vous exposez votre entreprise à un risque MAJEUR.

Que faire pour y remédier? Vous pouvez instaurer une politique de cybersécurité. Si vous en avez déjà une, il est temps de la mettre à jour, puis en fonction! **À quoi ressemble une politique de cybersécurité?** Les détails sont différents d'une entreprise à l'autre, mais une politique générale doit avoir tous les principes fondamentaux, tels que la politique de mot de passe et l'utilisation de l'équipement.

Par exemple, il devrait y avoir des règles sur la façon dont les employés utilisent les équipements, tels que les imprimantes, PC et autres appareils connectés à votre réseau. Ils doivent savoir ce qu'on attend d'eux quand ils se connectent à un appareil de l'entreprise, des règles sur les logiciels qu'ils peuvent installer et auxquels ils peuvent accéder en naviguant sur le Web, comment accéder en toute sécurité au réseau de travail et quelles données peuvent-ils partager.

En résumé, de nombreuses politiques de cybersécurité incluent des règles et des attentes liées à:

Suite à la page 2

Suite de la page 1

- Utilisation des courriels
- Accès aux médias sociaux et au Web en général
- Accéder à distance aux applications internes
- Partage de fichiers
- Mots de passe

Les politiques doivent également déterminer les rôles informatiques au sein de l'organisation. Qui les employés appellent-ils, envoient-ils des SMS ou des courriels s'ils ont besoin d'une assistance informatique? Quelle hiérarchie doivent-ils suivre? Ont-ils un soutien interne? Communiquent-ils avec votre fournisseur de services informatiques gérés?

Il est important que les employés disposent de ressources pour exécuter efficacement les politiques. Cela peut prendre différentes formes. Il peut s'agir d'un guide pour s'y référer, d'un numéro de téléphone d'assistance à appeler, d'une formation continue sur des sujets de cybersécurité, ou bien, tout ce qui précède comme c'est souvent le cas!.

Déterminez chaque règle davantage. Les mots de passe sont un excellent exemple de politique à mettre en place.

> **"Mettre en place une politique de cybersécurité n'est pas facile, mais nécessaire, surtout de nos jours. Aujourd'hui plus que jamais, les personnes travaillent à distance."**

Cette politique est souvent négligée ou pas prise au sérieux. Comme plusieurs politiques de cybersécurité, plus la politique de mot de passe est forte, plus elle est efficace. Voici des exemples de ce qu'elle peut inclure:

- Les mots de passe doivent être changés tous les 60 à 90 jours sur toutes les applications.
- Les mots de passe doivent être différents pour chaque application.
- Les mots de passe doivent comporter 15 caractères ou plus, le cas échéant.
- Les mots de passe doivent utiliser des lettres majuscules et minuscules, au moins un chiffre et au moins un caractère spécial, tel que @, #,% ou &.

La bonne nouvelle est que certaines applications et sites Web adoptent ces règles. La mauvaise nouvelle est que TOUTES les applications et sites Web n'appliquent pas ces règles, il vous appartient donc de spécifier la manière dont les employés définissent leurs mots de passe.

Implanter une politique de cybersécurité n'est pas facile, mais nécessaire, surtout de nos jours. Plus de personnes travaillent à distance. Également, les cybermenaces sont plus courantes. Plus vous en faites pour protéger votre entreprise et vos employés contre ces cybermenaces, mieux vous serez quand ces menaces frapperont à votre porte.

Si vous avez besoin d'aide pour configurer ou mettre à jour votre politique de cybersécurité, n'hésitez pas à appeler votre fournisseur de services informatiques. Il peut vous aider à mettre en place ce dont vous avez besoin pour un lieu de travail plus sûr et plus sécurisé.

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

Depuis les 15 dernières années, Multiplis a acquis une expertise au niveau de la fabrication de systèmes muraux et panneaux modulaires pour les projets commerciaux, industriels et institutionnels de toute envergure. Grâce à leur savoir-faire et leurs infrastructures technologiques, ils ont la capacité de réaliser des designs de revêtements extérieurs les plus exotiques imaginés par des architectes et designers de l'Amérique du Nord.

Des dessins d'atelier, en passant par les plans de relevés de dimensions sur chantier, suivi de la fabrication et des plans d'installation, Multiplis offre un service de projets clé en main.

"Notre succès, nous le devons également à la force technologique de notre marché. Pour offrir un service innovant et de qualité indéniable, nous avons nous-mêmes, à l'aide d'experts en la matière, développé une approche qui combine le meilleur de l'intelligence technologique du domaine. "

MULTIPLIS

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

Si vous pensez que votre entreprise est trop petite pour être piratée…

Alors vous êtes probablement la cible n° 1 d'un cybercriminel !

Dans un monde de cybercriminalité endémique, les pirates se nourrissent de la foi aveugle de leurs cibles. Malgré les failles de sécurité numérique très médiatisées qui paraissent dans l'actualité presque chaque semaine, la plupart des gens pensent qu'ils sont à l'abri des attaques.

On pense que si des sociétés Fortune 500 comme J.P. Morgan, Sony, Tesco Bank et Target ont perdu des millions de dollars en violation de données ces dernières années, mon entreprise est bien trop petite pour justifier l'attention d'un pirate informatique.

En fait, c'est tout le contraire. Selon StaySafeOnline.org, les attaques contre les petites entreprises représentent désormais plus de 70% des violations de données, un nombre qui semble être en augmentation. Près de la moitié des petites entreprises ont été compromises. Les attaques de ransomware à elles seules ont grimpé en flèche de 250% depuis 2016 et les incidents de phishing ont emboîté le pas, comme le rapporte Media Planet.

Le manque de visibilité des incidents beaucoup plus fréquents et de moindre envergure qui sévissent dans les pays peut facilement nous endormir dans un faux sentiment de sécurité pourtant très dangereux.

Pourquoi une équipe de pirates informatiques se concentrerait-elle sur une opération malveillante dans une petite ville alors qu'elle pourrait cibler un géant comme Google? Eh bien, quel bâtiment un petit voleur est le plus susceptible de cibler - une banque au milieu d'un centre-ville animé, remplie de gardes de sécurité et d'équipements de prévention de vols de haute technologie, ou la maison dans un quartier aisé de la ville, que les propriétaires gardent toujours déverrouillée pendant leurs vacances? Ne vous y trompez pas, ces gangs de pirates ne volent pas quelques ordinateurs et écrans plats. Ils ruinent les petites entreprises avec des rançons allant à la limite de leurs moyens, jusqu'à 250 000 $ pour une seule attaque, selon l'une des analyses de TechRepublic.

Bien sûr, tout propriétaire de petite entreprise aura du mal à se permettre les mesures de sécurité mises en œuvre par les grandes entreprises. Cependant, il y a un équilibre à trouver entre l'abordabilité et la vulnérabilité.

Même si vous avez réussi à traverser les dernières années sans être piraté, statistiquement, vous pouvez être certain que votre tour viendra. Dans cet esprit, il est important d'être préparé. Ce n'est pas parce vous n'avez pas eu d'accident de voiture depuis quelques années que vous ne devriez pas investir dans une assurance automobile et changer l'huile régulièrement. Tout comme votre voiture, la sécurité de votre réseau nécessite une assurance et un entretien régulier pour rester efficace.

Si vous pensez que le simple fait d'installer un logiciel antivirus vous protègera, vous êtes à côté de la plaque. Vous ne serez que légèrement plus en sécurité que vous ne l'étiez avant d'installer cette barrière. Pour transformer votre entreprise en une forteresse impénétrable, vous devrez investir dans l'avenir de celle-ci, la sécurité de vos clients et la longévité de votre gagne-pain.

Aujourd'hui, ce n'est pas une question de savoir comment vous serez hacké, mais bien quand ? Équipé d'un ensemble de protocoles de sécurité puissants et à jour, vous pourrez être tranquille en sachant qu'ils partiront les mains vides.

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

Zoom vous épuise ? Voici pourquoi et quoi faire

L'épuisement sur Zoom est réel, le travail à distance est devenu plus répandu que jamais et il est là pour rester. Il y a plusieurs raisons pour lesquelles l'épuisement sur Zoom se produit, mais vous pouvez l'arrêter.

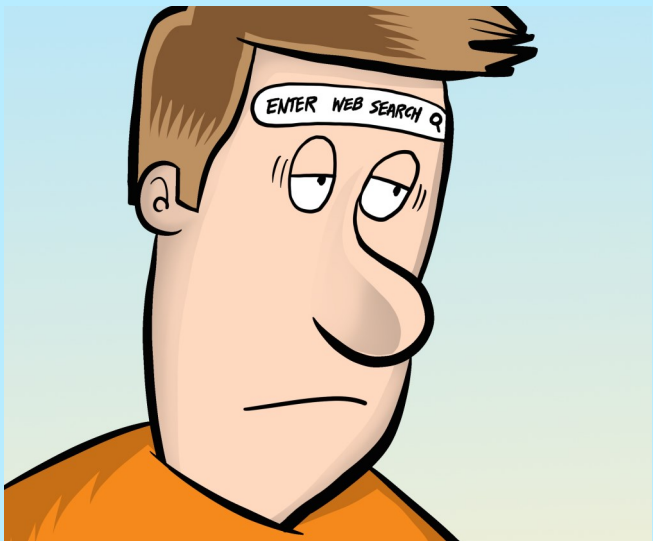
Restez structuré. Comme les réunions traditionnelles, les réunions Zoom peuvent prendre du temps. Elles peuvent aussi être fatigantes. Dans les réunions Zoom plus importantes, vous devrez recueillir beaucoup d'informations. De plus, vous devez faire attention à un écran et à tout le monde. Cela peut facilement conduire à une surcharge d'informations, se transformant en épuisement professionnel. Les petites réunions Zoom peuvent être tout aussi perturbatrices, en particulier pour le déroulement productif de votre journée. Donc, comme pour les réunions traditionnelles, si cela peut être dit par courriel, envoyez-en un.

Rester sur la bonne voie. Maintenez les réunions courtes. Si vous organisez une réunion Zoom, c'est votre responsabilité de garder le focus sur le sujet. Si elle déraille, cela perturbera la journée de tout le monde. Les perturbations sont difficiles à surmonter et nuisent sérieusement à la productivité, conduisant à l'épuisement professionnel. *Inc., 11 février 2021*

Comment garder les employés: Transparence de la remuneration ?

Alors que de plus en plus d'entreprises s'appuient sur le **modèle du télé-travail**, ces entreprises ont dû modifier leur mode de fonctionnement, la manière dont elles embauchent et retiennent leurs employés. La rétention des employés est devenue un sujet brûlant. Selon une enquête SilkRoad Technology, 40% des employés ont l'intention de quitter leur emploi actuel cette année en conséquence directe de la manière dont l'employeur a géré la pandémie.

Les employés repensent à ce qui compte pour eux lorsqu'ils acceptent un emploi. Cette année va être difficile pour les entreprises qui ne répondent pas aux attentes des employés - et l'une de ces attentes est liée à la rémunération.
Plus d'employés veulent de la transparence dans ce que l'entreprise paie afin de prendre de bonnes décisions pour leur carrière. Une autre étude de Beqom a révélé que 58% des employés quitteraient leur emploi pour un autre offrant plus de transparence salariale. Ils veulent savoir qu'ils sont payés équitablement et ce que gagnent les autres. *Inc., 11 février 2021*



Larry Grew A Unibrowser.

Votre entreprise a besoin de personnalité

Votre entreprise se démarque-t-elle des autres? Il peut être difficile de répondre à cette question, mais le succès se trouve dans la construction d'une personnalité pour votre entreprise. C'est quelque chose qui reste dans l'esprit des gens, alors quand ils ont besoin de quelque chose que vous fournissez, ils sont plus susceptibles de se souvenir de vous.

Et c'est là que commence la personnalité d'une entreprise en méritant d'être rappelée. Il faut plus que cela, on doit être authentique. Comment pouvez-vous faire cela?

Connaissez vos clients. Plus vous les connaissez, plus vous pourrez mieux répondre à leurs besoins. Conservez donc des données démographiques, habitudes d'achat, etc.

Être cohérent. La cohérence aide à construire et à définir votre marque. L'expérience client, de votre marketing à chaque interaction client, doit être uniforme.

Créez une histoire. Racontez votre histoire et ouvrez-vous aux clients. Les histoires définissent qui nous sommes et peuvent définir la personnalité de votre entreprise. *Forbes, 27 janvier 2021*