www.techrepublic.com /article/how-to-protect-and-secure-data/

Comment protéger et sécuriser vos données de 10 façons

Utilisez cette liste complète de stratégies pour vous aider à protéger les données de votre entreprise contre les menaces et les violations de données.

Ali Azhar ⁝

Image : Ar_TH/Adobe Stock

Les systèmes d'exploitation et les applications peuvent toujours être réinstallés, mais vos données sont uniques, ce qui en fait la chose la plus importante sur votre ordinateur ou votre réseau.
Voici un aperçu de 10 façons de protéger ces données contre la perte et l'accès non autorisé.

Aller à :

1. Sauvegardez régulièrement

La sauvegarde précoce et régulière est un élément important de la stratégie de prévention des pertes de données.
La perte de données peut se produire en raison de cyberattaques, de catastrophes naturelles, d'erreurs humaines et d'autres types d'évènements.
Si vous avez sauvegardé vos données, vous pouvez effectuer une restauration de données pour récupérer les données perdues.

Bien que vous puissiez utiliser la sauvegarde manuelle, vous pouvez également compter sur des solutions de sauvegarde de données qui sauvegardent automatiquement les données en fonction de votre planification configurée.

Des solutions de sauvegarde plus sophistiquées vous permettent de choisir les données à sauvegarder.

2. Gardez les logiciels d'entreprise à jour

Les développeurs de logiciels ont souvent besoin de publier de nouvelles mises à jour pour corriger les bogues et les vulnérabilités de sécurité des correctifs.
Vous devez maintenir votre logiciel d'entreprise à jour pour vous assurer qu'il dispose des derniers correctifs de sécurité, corrections de bogues et autres mises à jour pour vous protéger contre les menaces de cybersécurité nouvelles et anciennes.

La majorité des cyberattaques sont effectuées par l'exploitation de vulnérabilités de sécurité nouvellement découvertes, vous devez donc être vigilant pour vous assurer que votre logiciel d'entreprise est mis à jour avec la dernière version.

3. Protégez tout par mot de passe

Utilisez une protection par mot de passe pour vos données, car cela agit comme la première ligne de défense contre les accès non autorisés.
Certaines entreprises doivent utiliser la protection par mot de passe dans le cadre de leurs exigences de conformité, telles que la conformité au règlement général sur la protection des données.
L'utilisation de la protection par mot de passe contribue également à renforcer la sécurité multicouche de vos systèmes, car vous pouvez combiner la protection par mot de passe avec d'autres formes de mesures de sécurité pour protéger vos données.

Pour protéger vos données professionnelles par mot de passe, vous pouvez utiliser diverses méthodes, notamment la mise en œuvre d'une politique de mot de passe stricte pour vous assurer que vos employés créent des mots de passe complexes.
De plus, vous pouvez leur demander de mettre régulièrement à jour leurs mots de passe.

4. Utilisez un VPN

Les réseaux privés virtuels sont parfaits pour protéger vos données d'entreprise.
Un VPN fonctionne en créant un tunnel crypté pour vos données afin de cacher vos données aux pirates et aux fouineurs et aide également à minimiser votre empreinte en ligne.

Un VPN est indispensable pour les employés qui se connectent aux réseaux d'entreprise ou accèdent à des fichiers sensibles depuis leur domicile ou en voyage.
Vous pouvez utiliser un service VPN gratuitement.
Cependant, idéalement, vous souhaitez investir dans un abonnement VPN payant auprès d'un fournisseur réputé.
Avec une version payante, vous bénéficiez d'une connexion plus fiable, de serveurs dédiés et d'autres fonctionnalités premium.

5. Installez un logiciel antivirus

Les logiciels antivirus modernes aident à protéger les données contre les rançongiciels, les logiciels espions, les chevaux de Troie, les pirates de navigateur et diverses autres cybermenaces.
Bien qu'une licence de logiciel antivirus pour une entreprise ait un coût, c'est un prix relativement faible à payer pour protéger vos données.
Toute personne utilisant Windows 10 ou une version ultérieure dispose déjà d'un logiciel antivirus installé.
Les ordinateurs Mac n'ont pas de système antivirus intégré, vous devrez donc en acheter un séparément.

6. Utiliser l'authentification multifacteur

Un moyen fiable de protéger vos données consiste à utiliser l'authentification multifacteur sur les appareils connectés au réseau de l'entreprise.
Avec MFA, les utilisateurs doivent entrer un mot de passe et un code d'accès à usage unique envoyés à un autre appareil pour y accéder.
De cette façon, l'utilisateur a besoin d'au moins deux appareils ou « facteurs » pour se connecter au système.

L'authentification multifacteur agit comme une couche de sécurité supplémentaire pour vos données et devient un élément essentiel des protocoles de cybersécurité pour les entreprises.
Sans l'utilisation de MFA, vos données restent vulnérables à un accès non autorisé en raison de la perte d'appareils ou du vol d'informations d'identification.

7. Utiliser une infrastructure à clé publique

Une infrastructure à clé publique est un système de gestion des paires de clés publiques/privées et des certificats numériques.
Étant donné que les clés et les certificats sont émis par un tiers de confiance (une autorité de certification, interne installée sur un serveur de certificats de votre réseau ou publique), la sécurité basée sur les certificats est plus forte.

VOIR: Explorez les différences entre le chiffrement asymétrique et symétrique.

Vous pouvez protéger les données que vous souhaitez partager avec quelqu'un d'autre en les chiffrant avec la clé publique de son destinataire, qui est accessible à tous.
La seule personne qui pourra la déchiffrer est le détenteur de la clé privée qui correspond à cette clé publique.

8. Masquer les données avec la stéganographie

Vous pouvez utiliser un programme de stéganographie pour masquer des données dans d'autres données.
Par exemple, vous pouvez masquer un message texte dans un fichier graphique .JPG ou un fichier de musique .MP3, ou même dans un autre fichier texte.
Cependant, ce dernier est difficile car les fichiers texte ne contiennent pas beaucoup de données redondantes qui peuvent être remplacées par le message caché.

La stéganographie ne crypte pas le message, elle est donc souvent utilisée en conjonction avec un logiciel de cryptage.
Les données sont d'abord cryptées, puis cachées dans un autre fichier avec le logiciel de stéganographie.

Certaines techniques stéganographiques nécessitent l'échange d'une clé secrète, et d'autres utilisent la cryptographie à clé publique et privée.
Un exemple populaire de logiciel de stéganographie est StegoMagic, un téléchargement gratuit qui cryptera les messages et les cachera dans .TXT, . WAV ou .BMP fichiers.

9. Renseignez-vous et renseignez vos employés sur la cybersécurité

L'une des mesures les plus cruciales que vous pouvez prendre pour protéger vos données est de vous renseigner, vous et vos employés, sur la cybersécurité.
Vous devez promouvoir un état d'esprit sceptique lorsque vous interagissez avec un site Web, un courriel ou un message inconnu.
Cela devrait inclure l'apprentissage de l'importance de suivre les meilleures pratiques en matière de protection des données, telles que ne pas ouvrir les courriels provenant d'expéditeurs non reconnus et ne pas cliquer sur les pièces jointes suspectes.

VOIR: Profitez de cet ensemble de formation en cybersécurité de TechRepublic Academy.

10. Demandez conseil à un professionnel

Il existe plusieurs entreprises qui offrent des conseils et des services d'experts pour assurer la sécurité de vos données.
Vous pouvez choisir des sociétés de conseil en sécurité pour évaluer les vulnérabilités de sécurité de votre système et comment les corriger.

Si vous avez besoin d'une protection plus complète de vos données, vous pouvez choisir de faire appel à un fournisseur de services de sécurité gérés.
Ils offrent une variété de services de sécurité, y compris la surveillance de la sécurité 24 heures sur 7, <> jours sur <> et la gestion des incidents.
De plus, si vous souhaitez assurer vos actifs numériques, envisagez de souscrire une police d'assurance cybersécurité.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230720
"C'est ensemble qu'on avance"