10 FAÇONS D'UTILISER EN TOUTE SÉCURITÉ UN SUPPORT AMOVIBLE

Les stratégies **(BYOD)** (Bring your own device) sont adoptées par les organisations pour permettre une meilleure flexibilité au travail pour les employés, mais au prix de l'ouverture de passerelles pour les logiciels malveillants transmis par USB et les transferts de fichiers non autorisés. Il n'est donc pas surprenant que le Ponemon Institute ait constaté que **67%** des professionnels de l'informatique pensent que le BYOD a fait baisser leur niveau de sécurité. Cependant, il existe des solutions de contournement pour sécuriser les dispositifs de stockage ou périphériques amovibles afin de les utiliser efficacement et avec un minimum de risques. Voici quelques conseils pour utiliser en toute sécurité les périphériques de stockage amovibles:

1

Définissez une stratégie de sécurité BYOD

Rédigez et mettez en œuvre une stratégie pour gérer l'utilisation des clés USB et autres périphériques de support amovibles, en mettant l'accent sur les règles à suivre et la responsabilité des employés.

82% des entreprises permettent activement le BYOD.

2

N'autorisez que les dispositifs sécurisés

N'autorisez que l'utilisation de périphériques sécurisés, comme les clés USB avec authentification par empreinte digitale ou protection par mot de passe.

37% des menaces de cybersécurité visent les supports amovibles.

3

Protégez les clés USB par un mot de passe

Sécurisez les clés USB à l'aide de mots de passe pour rendre le vol de clés USB inutile pour les initiés et faire en sorte que les données volées ne conduisent pas à une violation.

28% des attaques de cybersécurité sur les terminaux en 2020 concernaient des dispositifs compromis ou volés.

4

Contrôlez l'accès des utilisateurs

Utilisez un logiciel de prévention des fuites de données (DLP) pour contrôler le niveau d'accès que les utilisateurs peuvent exercer. Par exemple, autorisez les utilisateurs à lire uniquement les fichiers dans les clés USB et bloquez les actions de modification ou d'exécution d'applications dans les clés USB.

51% des professionnels estiment que l'accès non autorisé aux données et aux systèmes est l'une des quatre principales menaces.

5

Exigez le cryptage des données

Imposez aux utilisateurs de chiffrer les données stockées ou partagées via des périphériques de stockage amovibles afin de réduire les conséquences d'un vol ou d'une perte. Maintenez plusieurs sauvegardes de données, à la fois dans le cloud et hors ligne.

56% des entreprises ont pu récupérer des données à partir de sauvegardes plutôt qu'en payant une rançon.

6

Bloquez les clés USB non autorisées

N'autorisez que les dispositifs USB acceptés ou reconnus par l'équipe de sécurité informatique. Bloquez les autres clés USB qui peuvent être de mauvaises clés USB, branchées par les utilisateurs, avec une solution DLP.

22% des entreprises ont détecté des logiciels malveillants téléchargés à partir de périphériques non gérés.

7

Auditer les événements de copie de fichiers

Suivez les utilisateurs qui ont copié des fichiers sensibles afin de bloquer immédiatement une violation potentielle. Bloquez les actions de copie lorsque cela est nécessaire pour empêcher les utilisateurs de tenter de transférer des fichiers sur des périphériques USB en utilisant un logiciel de prévention de la copie.

45% des employés ont admis avoir partagé des documents professionnels sur des comptes personnels avant de quitter leur emploi.

8

Conservez les clés USB officielles

Utilisez des dispositifs fournis par l'organisation. Assurez-vous que lorsque les dispositifs sont réutilisés, ils ne contiennent aucun des fichiers précédemment stockés ou partagés.

82% des organisations ne peuvent pas garantir la détection des menaces internes sur les appareils personnels des employés.

9

Autorisez les bons utilisateurs

Examinez périodiquement les autorisations de fichiers et révoquez les privilèges excessifs accordés aux utilisateurs. Une gestion méticuleuse des privilèges des utilisateurs réduit les risques de fuite ou de vol de données par un initié.

66% des menaces d'initiés ont conduit à une utilisation abusive des privilèges pour accéder illégitimement à des systèmes ou des données critiques.

10

Protégez-vous contre les logiciels malveillants

Déployez des antivirus et des systèmes de détection des intrusions pour vous assurer que des dispositifs non officiels ne sont pas utilisés par des pirates ou des initiés pour infiltrer le réseau.

32% des répondants à l'enquête sont les plus préoccupés par le risque d'infection par des logiciels malveillants.

ManageEngine
DataSecurity Plus

DataSecurity Plus de ManageEngine offre une visibilité granulaire des données et des contrôles de sécurité sur une seule plateforme. Prenez en charge la sécurité des terminaux à l'aide de rapports détaillés et de capacités de réponse aux alertes personnalisables pour suivre et contrôler:

- Les événements de copie de fichiers sensibles déclenchés par les actions de l'utilisateur.
- Les e-mails sortants, qui pourraient être des tentatives potentielles d'exfiltration de données.
- Les clés USB auxquelles les utilisateurs accèdent pour lire ou modifier des fichiers ou exécuter des applications sur ces clés.
- Activité potentielle de transfert ou de téléchargement de fichiers à partir de navigateurs Web.
- L'activité d'impression de fichiers au sein de votre réseau.
- Les événements liés à la sécurité des fichiers, tels que les changements d'extension de fichier, les changements de liste de contrôle d'accès au système ou les changements de propriétaire.

Téléchargez une version d'essai gratuite et entièrement fonctionnelle.

Télécharger maintenant

Programmez une démo personnalisée via support@datasecurityplus.com