9 façons

dont les utilisateurs à privilèges menacent votre sécurité

Méfiez-vous des utilisateurs qui ne sont pas formés au rôle d'administrateur IT mais détiennent quand même des droits admin complets sur vos systèmes. Voici comment ils peuvent augmenter vos risques de sécurité, vos coûts de gestion et compliquer la mise en conformité de votre entreprise. Nous vous expliquons aussi ce qu'il faut faire dans ces cas-là.

1 Installation d'applications non autorisées pouvant introduire un malware

Empêchez les administrateurs de désactiver le contrôle du compte de l'utilisateur (UAC) et interdisez les applications non autorisées ou la modification par inadvertance des paramètres système.

2 Désactivation des services critiques, comme l'antivirus

La console MMC (Microsoft Management Console) permet aux utilisateurs de charger des composants logiciels enfichables permettant de contrôler les services. Rendez MMC inaccessible aux utilisateurs dotés de privilèges Admin.

3 Contournement des restrictions fondées sur le GUI

Interdisez l'exécution de commandes ou de scripts dans le système d'exploitation.

4 Désinstallation des agents des logiciels de protection

Interdisez aux utilisateurs dotés de privilèges, la désinstallation des logiciels tiers de protection.

5 Contournement des stratégies de protection de la gestion centralisée

Empêchez l'accès avec privilèges au registre Windows ; interdisez aux utilisateurs, la modification des paramètres de configuration.

6 Désactivation ou modification des paramètres de pare-feu des postes clients

Protégez-vous des logiciels malveillants qui se propagent sur le réseau en interdisant la désactivation.

7 Modification du comportement des applications à l'aide d'une date/heure erronée

Interdisez tout changement de la date et de l'heure, pour protéger l'intégrité des applications, ainsi que l'horodatage utilisé pour l'audit ou le dépannage.

8 Arrêt des logiciels de protection

Contrôlez l'arrêt des processus pour limiter les risques de sécurité.

9 Élévation d'applications susceptibles d'introduire des malwares

Limitez certaines applications de façon à ce qu'elles ne s'exécutent qu'avec des privilèges standards.

Les fonctions de contrôle des applications d'Ivanti® Security Controls vous permettent de définir immédiatement des restrictions simples afin de limiter les risques, d'améliorer la conformité de l'entreprise et d'éviter la création de tickets IT inutiles parce qu'un utilisateur a modifié par inadvertance un paramètre d'administration.

TÉLÉCHARGER LE LIVRE BLANC