TROIS FAÇONS SELON LESQUELLES UN UTILISATEUR PRIVILÉGIÉ PEUT INTÉGRER VOTRE ENVIRONNEMENT ACTIVE DIRECTORY

Et huit façons de réduire les risques et d'optimiser votre capacité de restauration

Quest

Introduction

UNE MISE EN GARDE

Déçu de son bonus, Roger Duronio, administrateur informatique d'UBS Paine Webber, a écrit 50 lignes de code et les a déployées sur des milliers de systèmes sur le réseau de l'entreprise, en utilisant les mêmes outils d'administration Unix standard que ceux employés pour distribuer des fichiers légitimes à ces systèmes.

Ensuite, il a démissionné.

Ce qui ne fut pas le cas de sa bombe à la logique implacable. Elle a scrupuleusement compté les semaines, ce qui a laissé à Roger Duronio le temps de placer 20 000 $ en commandes sur des actions UBS/PW à court terme. Puis, un matin, l'explosion a eu lieu. La commande était « rm -rf / », ce qui signifie TOUT supprimer.

Cela a déclenché une panique indescriptible. Chez UBS/PW, les salariés ont dû recourir à la plume et au papier pour travailler. La société a dépensé 3 millions de dollars en honoraires de consultation IBM uniquement pour restaurer les systèmes à partir de la sauvegarde. Qui sait quel a été le coût total.

À PROPOS DE CE DOCUMENT

Ce n'est là qu'un exemple de la façon dont un utilisateur privilégié mécontent ou négligent peut causer des ravages.

En fait, dans un environnement Windows, c'est assez facile à faire, car tout repose sur Active Directory (AD). Si Active Directory est en panne, c'est tout votre réseau qui l'est , même s'il n'y a aucun problème avec vos serveurs et applications.

En quoi est-ce si simple ? Ce livre électronique ne montre que trois des nombreuses façons dont un utilisateur privilégié , ou un attaquant doté d'identifiants à privilèges volés, peut neutraliser votre environnement AD et, de fait, le reste de votre réseau.

Nous aborderons ensuite huit bonnes pratiques essentielles qui peuvent vous aider à réduire ce risque et à améliorer votre capacité de restauration si le pire venait à se produire.

Trois façons dont un utilisateur privilégié peut intégrer votre environnement AD

MÉTHODE 1 : REFUSER LES DROITS DE CONNEXION

Un utilisateur dispose de cinq façons pour se connecter à Windows : localement, depuis le réseau, en tant que tâche par lot, en tant que service et par le biais des services de bureau à distance (Remote Desktop Services, RDS). Pour chacune de ces méthodes de connexion, il existe une paire de droits de connexion, une pour autoriser la connexion et une autre pour refuser la connexion.

En attribuant correctement les cinq droits de refus de connexion, un utilisateur privilégié peut bloquer les opérations :

- Les utilisateurs ne pourront pas se connecter à leurs stations de travail.
- Les administrateurs ne pourront pas accéder aux contrôleurs de domaine, même en utilisant le clavier local et l'écran de la console.
- Les comptes de service ne pourront pas se connecter.
- Les applications ne démarreront pas.

C'est un double dilemme : comme vous ne pouvez pas vous connecter avec un compte de domaine, vous ne pourrez pas résoudre le problème à distance. Vous aurez besoin d'accéder physiquement à vos contrôleurs de domaine pour redémarrer dans DSRM et commencer les opérations de restauration.

En attribuant correctement les droits de refus de connexion, un utilisateur privilégié peut bloquer les opérations.

MÉTHODE 2 : NEUTRALISER DNS

Active Directory utilise DNS comme mécanisme de localisation des contrôleurs de domaine. Chaque domaine Active Directory Windows Server 2003 ou version ultérieure dispose d'un nom de domaine DNS, et chaque ordinateur Windows Server 2003 ou version ultérieure dispose d'un nom DNS.

Pour intégrer votre environnement Active Directory, tout ce qu'un utilisateur privilégié a à faire est de supprimer toutes les entrées DNS d'un contrôleur de domaine. Ces changements seront bientôt répliqués à tous les autres contrôleurs de domaine au moyen du DNS en cache. Le cache DNS va ensuite expirer, et tout à coup personne ne pourra rien trouver. En particulier, les stations de travail ne pourront pas trouver de contrôleurs de domaine utilisant DNS. Il faudra avoir recours à la résolution de nom NetBIOS, qui peut ou non fonctionner.

Si DNS est hors service, rien ne fonctionne.

Quest

MÉTHODE 3 : EXPLOITER UNE VULNÉRABILITÉ DANS LE SYSTÈME D'EXPLOITATION

Un jour, une entreprise exécutant Windows Server 2008 a constaté que tous ses contrôleurs de domaine étaient impliqués dans un cycle de redémarrage sans fin. Il s'est avéré qu'un utilisateur privilégié était entré dans un sous-réseau et avait accidentellement modifié un paramètre IPv6 sur une adresse IP non valide. Lorsque le processus de configuration de la réplication KCC (Knowledge Consistency Checker) a rencontré le paramètre non valide, le système a planté. Cela a provoqué le redémarrage du contrôleur de domaine, mais avant le paramètre non valide a été répliqué au niveau des autres contrôleurs de domaine dans tout l'environnement, ce qui a entraîné leur redémarrage à plusieurs reprises.

Des vulnérabilités inconnues ou non corrigées peuvent neutraliser votre environnement AD.

Microsoft a corrigé ce problème, donc si vous êtes toujours sous Windows 2008 ou 2008 R2, assurez-vous de disposer des correctifs à jour. Cependant, rien ne garantit qu'il n'y ait pas d'autres vulnérabilités qu'un utilisateur privilégié pourrait exploiter délibérément ou accidentellement, avec des conséquences tout aussi désastreuses.

Il n'y a pas que des collaborateurs mécontents

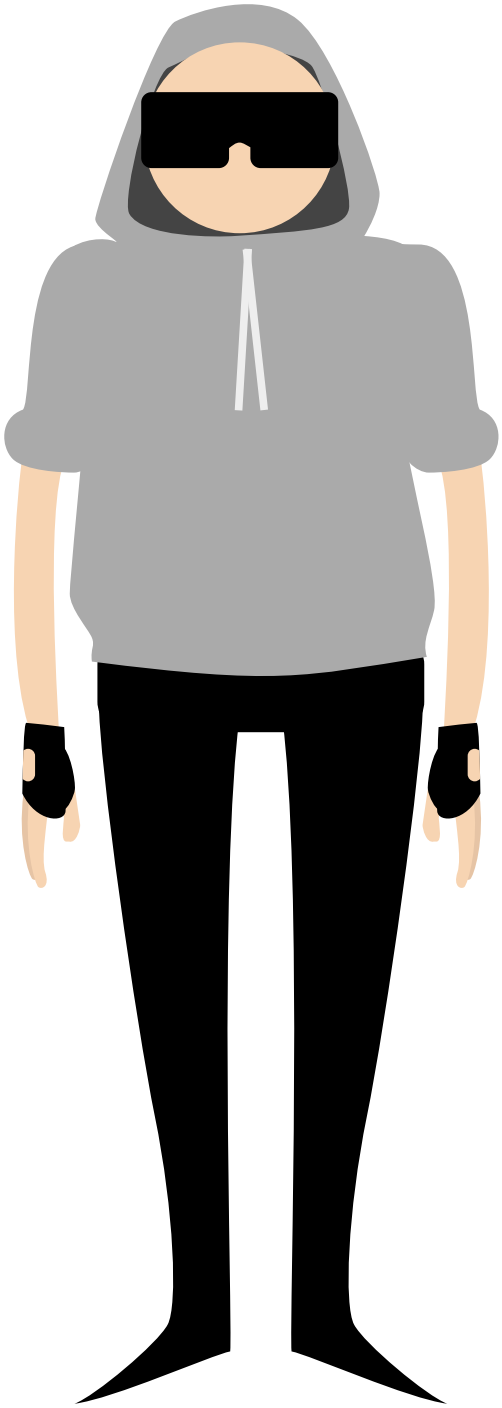
Un trop grand nombre d'entreprises tentent d'écarter le risque lié à ce type de scénarios en prétendant qu'elles n'ont pas d'utilisateurs privilégiés mécontents ou malveillants susceptibles de devenir des menaces internes. Même si vous pouviez garantir d'une façon ou d'une autre que c'est vrai (tant maintenant que pour la suite), vous êtes toujours exposé au risque, pour deux raisons. Tout d'abord, même les administrateurs les plus honorables peuvent faire des erreurs, comme le paramètre IPv6 non valide dont nous venons de parler. Ensuite, les identifiants à privilèges peuvent être volés et utilisés à mauvais escient lors d'une cyberattaque perpétrée par divers hackers aux intentions malveillantes, par exemple :

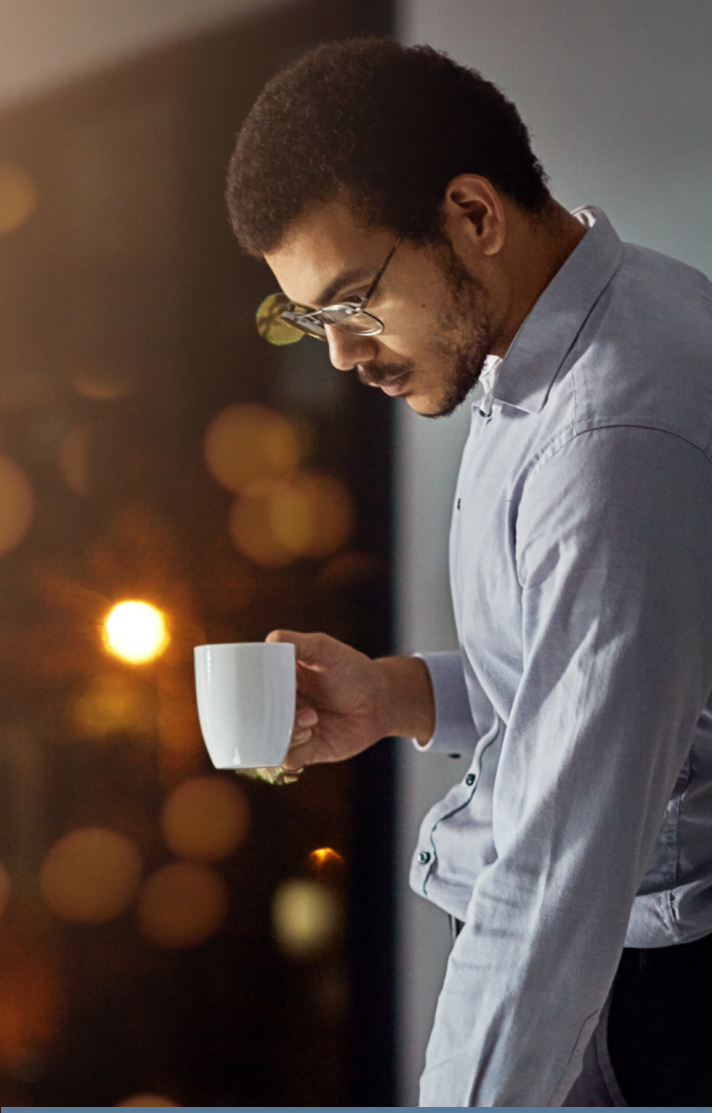
- Des hacktivistes
- Un groupe hostile parrainé par un état
- Des concurrents
- Une personne lésée
- Un crétin nihiliste

Les entreprises sont tout aussi préoccupées par les violations de données causées par l'inattention des utilisateurs, la négligence ou des identifiants corrompus (51 %) que par les violations causées par des initiés malveillants (47 %).

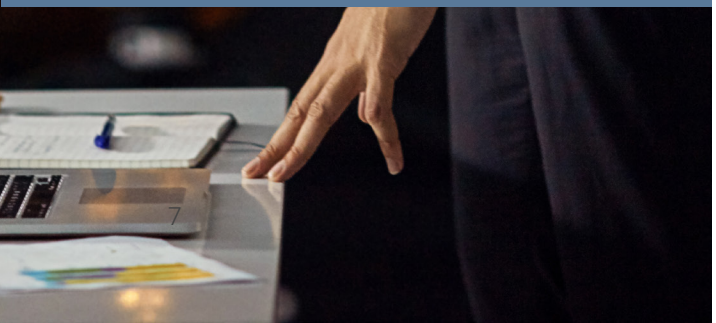
Source : 2018 Insider Threat Report (Rapport sur les menaces internes 2018), Cybersecurity Insiders

Gardez à l'esprit que tous ces attaquants ne veulent pas investir le temps et les efforts nécessaires pour voler vos données. Certains d'entre eux veulent simplement neutraliser vos services et détruire votre entreprise, ce qui est beaucoup plus facile.





Il est essentiel de bien contrôler l'appartenance à des groupes privilégiés.



Huit bonnes pratiques relatives à la sécurité d'AD

Il est certain que les comptes privilégiés représentent un risque réel et sérieux. Mais bien entendu, vous ne pouvez pas simplement les éliminer ; ils sont essentiels au bon fonctionnement de vos systèmes. Heureusement, il existe des mesures reconnues que vous pouvez adopter pour réduire le risque d'une utilisation à mauvais escient des comptes privilégiés, que ce soit délibérément ou accidentellement, et pour vous assurer une restauration la plus rapide possible en cas d'échec de ces mesures préventives. Voici huit bonnes pratiques à implémenter.

1. LIMITER LES ACCÈS À PRIVILÈGES.

Il est essentiel de bien contrôler l'appartenance à des groupes privilégiés, notamment les suivants :

- Domain Admins
- Enterprise Admins
- Schema Admins
- Administrators
- DHCP Administrators
- Group Policy Creator Owners
- Domain Controllers
- Network Configuration Operators
- Server Operators
- Backup Operators

Contrôlez également avec soin tous les objets de la politique par groupe qui affectent vos contrôleurs de domaine et tous les logiciels installés sur les contrôleurs de domaine. Par exemple, si un agent est installé, les utilisateurs qui y ont accès peuvent très bien être des administrateurs de domaine.

La meilleure façon de contrôler les accès à privilèges est d'utiliser une solution complète de gestion des comptes à privilèges et de gestion des sessions à privilèges, avec des autorisations humaines et une supervision en direct pour les niveaux d'accès qui auraient un impact sur l'ensemble de votre domaine. Comme personne ne devrait avoir besoin de toucher les contrôleurs de domaine de quelque façon que ce soit au quotidien, il est préférable d'exiger la présence de deux intervenants pour toutes les activités : un intervenant pour effectuer le travail et un autre pour superviser. Même si la supervision est effectuée à distance ou par un pair, elle réduit la capacité d'une personne isolée à nuire à votre entreprise. De plus, l'amélioration de la responsabilisation et le fait de disposer de deux regards différents réduisent le risque d'erreurs coûteuses.

Quest

2. SÉCURISER DES COMPTES À PRIVILÈGES DANS UNE FORÊT ROUGE.

Il peut s'avérer très difficile de renforcer suffisamment les forêts de production afin de protéger suffisamment vos comptes administrateur les plus privilégiés sans interrompre les fonctionnalités du domaine. Par conséquent, Microsoft propose maintenant un moyen de conserver ces comptes dans une forêt administrative dédiée, officiellement nommée « Enhanced Security Admin Environment » (ESAE) mais officieusement appelée « Forêt rouge », où « rouge » correspond à la nature critique des identifiants.

Une caractéristique clé du modèle de la Forêt rouge est que les comptes administrateur sont divisés en trois niveaux de sécurité :

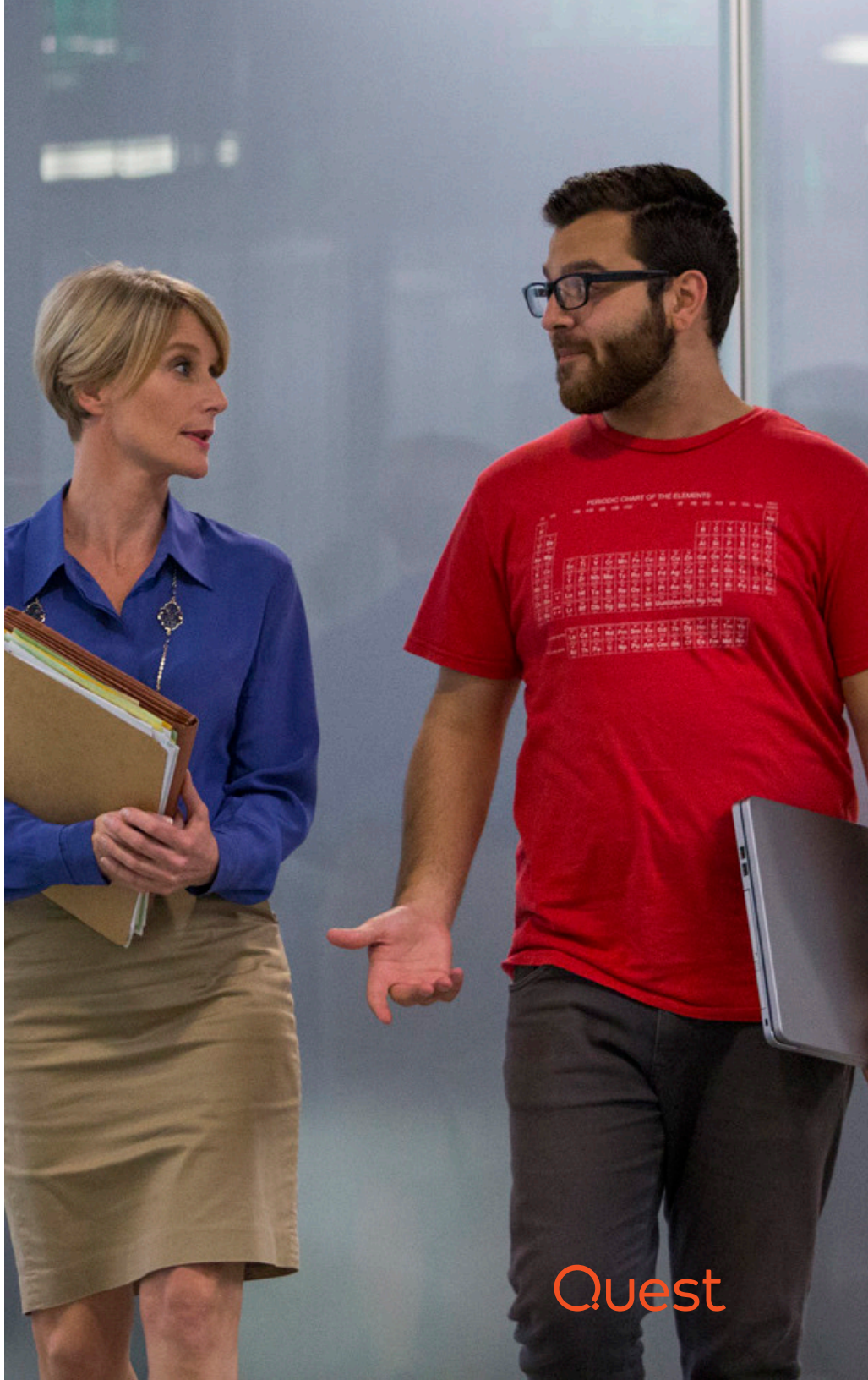
- **Niveau 0 —** Autorité d'administrateur au niveau forêt (Enterprise Admins)
- **Niveau 1 —** Autorité d'administrateur au niveau Cloud, application et serveur
- **Niveau 2 —** Contrôle administratif des stations de travail et appareils

En plaçant tous vos comptes de niveau 0 dans une forêt distincte, vous pouvez plus facilement les surveiller de près et appliquer des exigences de sécurité supplémentaires, comme exiger une connexion à partir d'une station de travail sécurisée de manière renforcée ou imposer une authentification à deux facteurs.

Bien sûr, le déploiement d'une forêt administrative n'est pas une mince affaire. Pour plus d'informations, regardez un webcast enregistré au cours duquel l'expert en sécurité Randy Franklin Smith explique les raisons pour lesquelles vous pourriez avoir ce problème supplémentaire, ainsi que les limites du modèle de la forêt rouge.

3. TESTER LES MODIFICATIONS AVANT DE LES IMPLÉMENTER DANS L'ENVIRONNEMENT DE PRODUCTION.

Pour réduire les risques d'intégration d'erreurs dans votre environnement AD, mettez en place un laboratoire de test au sein duquel vous pouvez examiner l'impact des mises à niveau ou d'autres modifications avant de les implémenter dans l'environnement de production. Plus le laboratoire de test est proche de la production, mieux c'est.



Audit et alertes sur toutes les modifications critiques dans Active Directory.

4. AUDIT.

Un audit complet est important pour plusieurs raisons. Il contribue à garantir la responsabilisation, qui peut décourager les actes malveillants de la part des initiés et inciter les utilisateurs privilégiés bien intentionnés à agir avec plus de prudence, réduisant ainsi le nombre et la gravité des erreurs. Il vous aide également à déterminer rapidement ce qui a mal tourné et à prendre des mesures correctives, ainsi qu'à savoir comment éviter que le même problème ne se reproduise par la suite.

Assurez-vous que votre piste d'audit inclut les événements natifs, les journaux de sécurité du système d'application, les journaux des services d'annuaires et d'autres données critiques, et que vous pouvez rapidement examiner, rechercher et analyser les données. Et veillez à ce que votre système d'audit soit accessible en cas de défaillance d'AD.

5. SURVEILLER ET GÉNÉRER DES ALERTES SUR LES MODIFICATIONS CRITIQUES.

Assurez-vous d'avoir connaissance immédiatement de la modification d'un objet critique, tel qu'un groupe privilégié ou un objet de la politique par groupe qui affecte vos contrôleurs de domaine. Puisque de telles modifications devraient être rares, vous ne serez pas inondé d'alertes. Les alertes sur les modifications légitimes servent à confirmer que votre système de surveillance fonctionne. Et les alertes relatives aux modifications non autorisées vous permettent de réagir rapidement, peut-être à temps pour éviter des conséquences graves.

6. DOCUMENTER VOTRE STRUCTURE AD.

Prenez le temps de documenter votre structure AD. Maintenez ces informations à jour et conservez-les hors ligne (par exemple, dans Dropbox), à un endroit où vous pourrez y accéder même si AD est indisponible. Assurez-vous d'inclure des informations sur les éléments suivants :

- Forêts
- Domaines
- Approbations
- DNS
- Sous-réseaux et liens de réplication entre eux
- Chaque contrôleur de domaine, notamment son adresse IP, son emplacement physique, le domaine qu'il contrôle, les opérations principales uniques flexibles inhérentes et s'il s'agit d'un catalogue global

Quest

7. SAUVEGARDER ACTIVE DIRECTORY.

Sauvegardez Active Directory avec une solution de sauvegarde d'entreprise. Ne comptez pas seulement sur la restauration de la corbeille.

N'oubliez pas que la corbeille est une commodité et rien de plus. Elle présente des limitations sérieuses, que nous explorons dans le livre blanc, « The Windows Server 2016 and Azure AD Recycle Bins, and Quest Recovery Solutions » (Corbeilles Windows Server 2016 et Azure AD et solutions de restauration Quest). Par exemple, vous souvenez-vous que nous avons indiqué précédemment que quelqu'un pouvait intégrer votre environnement AD en supprimant tous vos enregistrements DNS ? Et bien, au lieu de supprimer les enregistrements, un utilisateur malveillant pourrait remplacer les paramètres par des adresses IP non valides. La corbeille ne va pas vous aider à restaurer ces attributs.

8. TESTER VOS SAUVEGARDES.

Il est essentiel de considérer les sauvegardes comme défectueuses jusqu'à preuve du contraire. Vérifiez la viabilité d'une sauvegarde en la montant et en lisant un objet depuis celle-ci. Reconstruisez aussi périodiquement votre forêt Active Directory dans un environnement de test pour vous assurer que vous pouvez vous remettre d'un problème majeur, et ce rapidement.

Sauvegardez Active Directory avec une solution de sauvegarde d'entreprise et testez ces sauvegardes.

Conclusion

Lorsque les téléphones s'allument et que rien ne fonctionne, vous ne savez pas ce qui se passe ou ne connaissez pas l'étendue du problème. Peut-être qu'un initié mécontent vient de passer à l'action. Vous avez peut-être été touché par un logiciel malveillant. Ou peut-être qu'une erreur accidentelle a neutralisé votre environnement AD.

En suivant les bonnes pratiques décrites ici, vous réduirez les risques de voir ces scénarios malheureux se produire, mais rien ne peut éliminer le risque entièrement. Par conséquent, vous devez également prendre des mesures pour faciliter une restauration rapide d'Active Directory, en maintenant par exemple une piste d'audit claire et complète et en vous assurant que vous disposez de sauvegardes fiables.

Vous avez probablement entendu des histoires cauchemardesques sur la reconstruction d'AD au cours du week-end. La restauration d'AD n'est pas aussi simple que la restauration de certains fichiers qui ont été supprimés. Et cet environnement n'est pas facile à tester ou à simuler, en partie parce que la procédure de restauration d'AD appropriée dépend du scénario de sinistre.

Mais avec la bonne solution en main, vous pouvez reconstruire l'intégralité de votre forêt Active Directory en un seul clic. Pour en savoir plus, lisez notre livre blanc, « That Dreaded Day: Active Directory Disasters & Solutions for Preventing Them » (Le jour redouté : sinistres Active Directory et solutions pour les éviter).

Avec la bonne solution en main, vous pouvez reconstruire l'intégralité de votre forêt Active Directory en un seul clic.

Quest

PROFIL DE QUEST

L'objectif de Quest est de résoudre des problèmes complexes à l'aide de solutions simples. Nous y parvenons en appliquant une philosophie qui repose sur l'excellence de nos produits, un service de qualité et un objectif global de simplicité dans nos interactions. Notre vision est de proposer une technologie qui apporte à la fois efficacité et résultats concrets, afin que votre entreprise passe moins de temps à gérer son information et plus de temps à innover.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :

Quest Software Inc.
Attn: LEGAL Dept

Veuillez vous rendre sur notre site Web (www.quest.com/fr) pour obtenir nos coordonnées locales et internationales.

Ebook-3WaysToHoseYourAD-US-GM-FR-WL-32410