ManageEngine
ADManager Plus

5 signes révélateurs d'une VIOLATION DE LA RÉGLEMENTATION

www.manageengine.fr/admanagerplus

PG Software EUROPE

Vue d'ensemble

Lorsqu'il s'agit de gérer les identités et les droits d'accès des utilisateurs, Active Directory (AD) joue un rôle essentiel. Les modifications apportées à AD ont non seulement un impact sur la sécurité d'une entreprise, mais aussi sur sa conformité aux réglementations informatiques. Il n'est donc pas surprenant que les auditeurs de conformité soient désireux d'examiner les activités menées dans l'AD.

La pénalité pour non-conformité peut entraîner une lourde peine, ainsi qu'une perte de confiance des clients pour les entreprises. Il est préférable de vérifier régulièrement et de manière proactive la position de votre entreprise en matière de conformité afin d'éviter le trac de dernière minute que vous pourriez ressentir lors d'un audit de conformité.

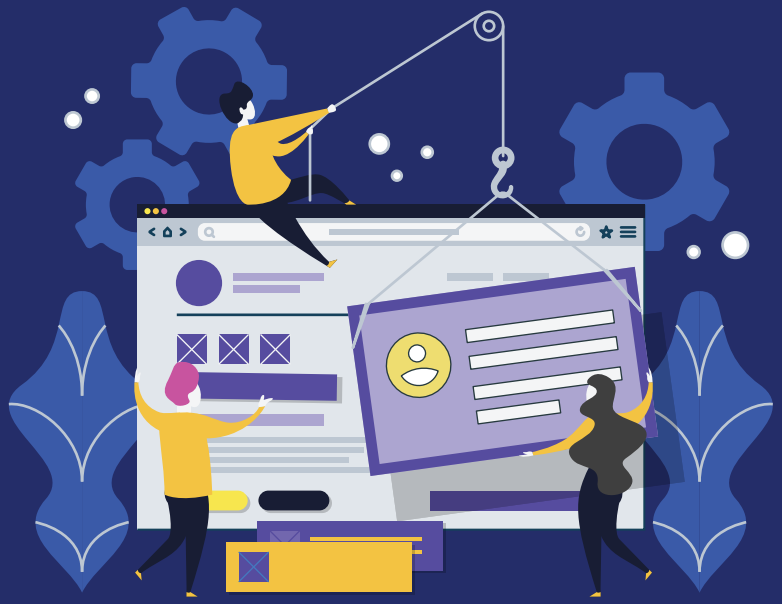
1er signe

PAS DE SYSTÈME DE GESTION DES CHANGEMENTS

Modifier les autorisations AD sans les faire valider auparavant peut exposer involontairement des données commerciales sensibles à des failles de sécurité. Il est essentiel de mettre en place une politique de contrôle des accès pour chaque action critique dans l'AD afin d'empêcher les utilisateurs d'obtenir des privilèges non autorisés. La meilleure solution consiste à suivre un processus d'examen dans le cadre duquel chaque demande de changement d'utilisateur est évaluée par un responsable avant d'être transférée à un administrateur informatique. Chaque demande, telle que l'accès aux actions critiques ou les changements d'appartenance à un groupe, doit être examinée par un responsable informatique ou un chef d'équipe pour s'assurer que les ressources de l'entreprise ne sont pas compromises

ADManager Plus de ManageEngine permet de personnaliser les workflows qui vous aident à optimiser et à surveiller les tâches AD. Grâce à cette fonctionnalité, les utilisateurs peuvent formuler des demandes d'accès aux ressources qui peuvent être examinées par une autorité désignée avant que l'administrateur informatique n'exécute la tâche.

EN SAVOIR PLUS



2ème signe

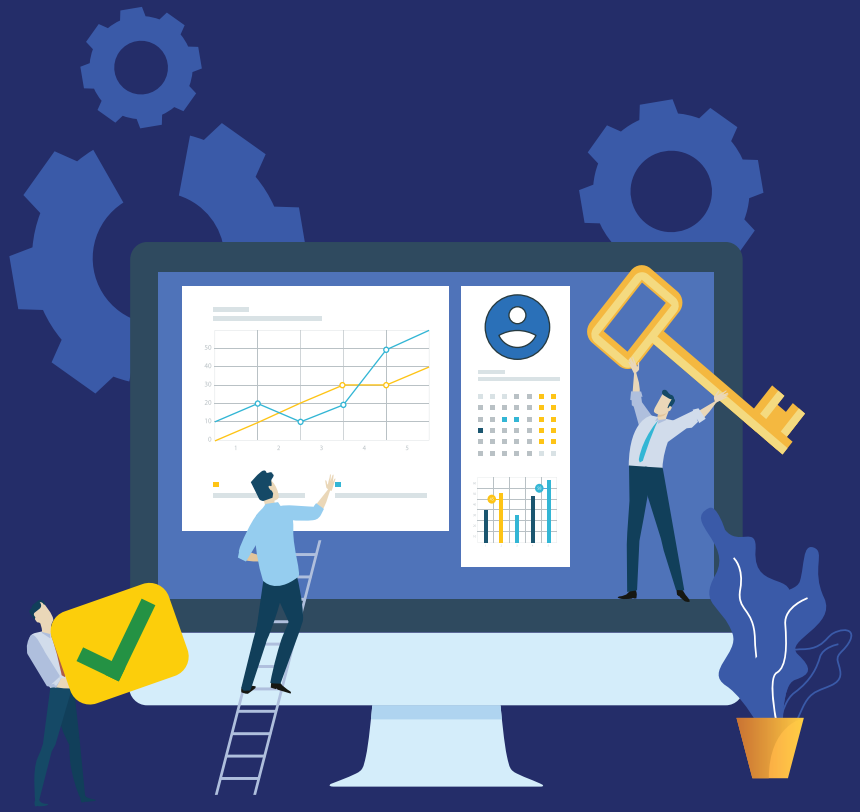
PAS DE PRIVILÈGES BASÉS SUR LES RÔLES

Les administrateurs informatiques créent régulièrement des comptes utilisateurs, leur attribuent les autorisations nécessaires et modifient les privilèges existants. S'il n'existe pas de liste de contrôle contenant les détails d'accès des utilisateurs par département, les administrateurs informatiques ne pourront pas accorder les autorisations aux utilisateurs de manière uniforme. Parfois, les utilisateurs sont ajoutés aux mauvais groupes, ce qui peut conduire à ce qu'ils aient des autorisations excessives ou moins de privilèges que ce qui est requis pour leur rôle.

Par exemple, un employé du marketing et un employé des ressources humaines doivent avoir chacun des autorisations pour des ressources différentes, spécifiques à leur rôle. De même, lorsque les utilisateurs sont transférés vers un autre lieu, ils doivent avoir accès aux ressources que leur travail exige et rien de plus.

ADManager Plus dispose de modèles personnalisables pour optimiser la création et la modification des objets AD ; vous pouvez également définir des règles et des attributs basés sur les groupes de sécurité, les heures de connexion et les coordonnées de contact qui peuvent être mis à jour automatiquement en fonction du service ou du rôle.

EN SAVOIR PLUS



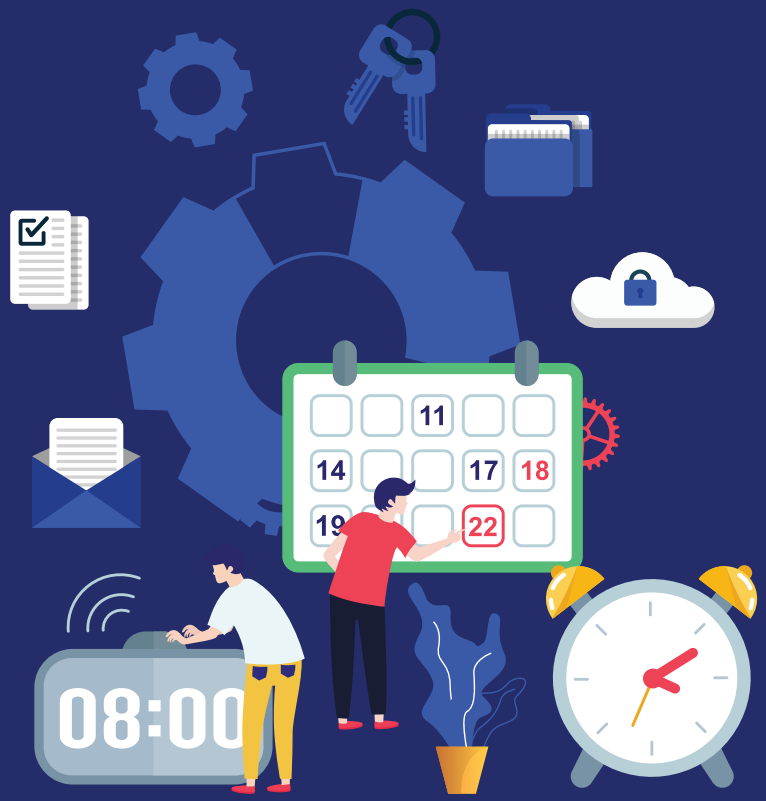
3ème signe

FUITE DES PRIVILÈGES

Lorsque les utilisateurs rejoignent une entreprise, les administrateurs informatiques leur accordent des autorisations d'accès aux ressources pertinentes pour leur fonction. Au fil du temps, pour différentes tâches ou projets, les utilisateurs peuvent se voir accorder des autorisations d'accès à différentes ressources. Ces droits d'accès doivent être révoqués une fois la tâche terminée. Il est recommandé aux administrateurs informatiques de revoir périodiquement tous les droits d'accès des utilisateurs par rôle en fonction d'une liste de contrôle des autorisations. Les utilisateurs peuvent avoir accès aux groupes de sécurité de haut niveau ou aux dossiers et fichiers critiques qui ne sont plus nécessaires pour leur rôle. Le suivi périodique de toutes les permissions attribuées aux utilisateurs pour un projet spécifique et leur révocation après la fin du projet résout ce problème ; cependant, cette tâche peut être fastidieuse.

ADManager Plus offre une fonction de gestion automatisée des autorisations de groupe limitées dans le temps afin que les administrateurs informatiques puissent assigner des utilisateurs à des groupes spécifiques et les révoquer après une période de temps spécifiée. En outre, l'outil fournit des rapports prédéfinis sur les autorisations NTFS et de partage afin que vous puissiez identifier les serveurs et les partages dans votre entreprise, et vérifier le niveau d'accès de chaque utilisateur ou groupe.

EN SAVOIR PLUS



4ème signe

ABSENCE DE RÉVISION PÉRIODIQUE

Vous préparez des rapports pour les agents de conformité à la dernière minute ? Il est essentiel d'identifier les accès non autorisés à des dossiers et à des fichiers critiques essentiels bien à l'avance afin de pouvoir prendre des mesures correctives et éviter les problèmes de non-conformité. Une bonne pratique recommandée consiste à vérifier périodiquement les autorisations d'accès. Si vous ne savez pas qui peut accéder aux dossiers sensibles et qui appartient à quel groupe de sécurité, ce n'est qu'une question de temps avant que la sécurité des données de votre entreprise ne soit menacée. La plupart des outils natifs n'offrent pas la possibilité d'obtenir des informations AD précises par le biais de rapports. Des alertes en temps réel sur la modification d'un compte utilisateur, d'un groupe de sécurité ou d'un mot de passe peuvent vous inciter à prendre des mesures immédiates.

ADManager Plus fournit des rapports exploitables, prédéfinis, pour les réglementations de conformité PCI DSS, SOX, HIPAA, GLBA, GDPR et FISMA. Vous pouvez également automatiser l'ensemble du processus de rapport de conformité en programmant les rapports à envoyer aux principales parties prenantes responsables de la gestion des programmes de conformité.

EN SAVOIR PLUS

5ème signe

ACCUMULATION DE COMPTES PÉRIMÉS

La maintenance informatique est un élément important pour empêcher les attaquants d'accéder aux ressources d'une entreprise sans autorisation. Les comptes d'utilisateurs et les ordinateurs inactifs sont des points d'entrée pour les cyberattaquants qui cherchent à accéder à des comptes avec des autorisations élevées, ou à accéder à distance à des données financières et sensibles. Il est également risqué de laisser sans protection les groupes de sécurité qui accordent des autorisations.

Grâce à ADManager Plus, vous pouvez configurer le déprovisionnement en utilisant une automatisation qui identifie les objets dormants, supprime leurs privilèges, les déplace dans un autre conteneur, et supprime leurs comptes. Pour simplifier ce processus, la fonction Désactiver/Supprimer d'ADManager Plus vous permet de supprimer les comptes Office 365 et G Suite associés, d'exporter la boîte aux lettres de l'utilisateur vers un emplacement spécifié et de révoquer les licences des logiciels concernés.

EN SAVOIR PLUS

Téléchargez un essai gratuit de 30 jours
pour essayer ces fonctionnalités et
profiter de tous les avantages qu'offre
ADManager Plus.

$ Demander une cotation

Télécharger

ManageEngine
ADManager Plus

ADManager Plus est une solution Web pour tous vos besoins de gestion AD, Exchange, Skype pour les entreprises, G Suite et Office 365. Il simplifie plusieurs tâches de routine telles que le provisionnement des utilisateurs, le nettoyage des comptes dormants, la gestion des autorisations NTFS et de partage, et plus encore. ADManager Plus propose également plus de 150 rapports préinstallés, notamment des rapports sur les comptes d'utilisateurs AD inactifs ou verrouillés, les licences Office 365 et les dernières heures de connexion des utilisateurs. Effectuez des actions de gestion directement à partir de ces rapports. Créez une structure workflow personnalisée qui vous aidera à établir des tickets et à assurer la conformité, à automatiser les tâches AD de routine telles que l'approvisionnement et le dé-provisionnement des utilisateurs, etc.

Téléchargez une version d'essai gratuite dès aujourd'hui pour explorer toutes ces fonctionnalités.

0 805 296 540 Service & appel gratuits

Mail
commercial@pgsoftware.fr

Website
www.pgsoftware.fr

PG Software EUROPE