Abus de privilèges : qui en fait, quels sont les signes à surveiller et comment réduire les risques

Devolutions

LES UTILISATEURS PRIVILÉGIÉS SONT ÉGALEMENT DES CIBLES PRIVILÉGIÉES POUR LES PIRATES INFORMATIQUES

Les utilisateurs qui disposent d'un accès privilégié à un compte reçoivent « les clés du royaume » - ou du moins les clés des étages et des pièces maîtresses du royaume - afin d'être plus productifs et efficaces dans leurs tâches quotidiennes. Malheureusement, les utilisateurs privilégiés sont également des cibles privilégiées pour les pirates informatiques qui souhaitent pirater les appareils et les réseaux pour voler des données. Une enquête de Centrify a révélé que 74% des violations de données proviennent d'un abus de comptes privilégiés.

Des ennemis parmi nous

Les utilisateurs qui disposent d'un accès privilégié à un compte ne sont pas tous responsables et respectueux des règles. Il existe généralement quatre types d'initiés qui abusent inconsciemment ou volontairement des comptes privilégiés :

- Le *leakeur* accidentel : cet utilisateur ne veut pas nuire, mais, en raison de son ignorance ou de sa négligence, il est victime d'hameçonnage, soit par des courriels, des publications sur les réseaux sociaux ou des SMS frauduleux.
- L'initié compromis : l'identité de cet utilisateur ou de ses appareils est compromise. Comme mentionné précédemment, les pirates ciblent agressivement les utilisateurs avec un accès privilégié, tels que les administrateurs système, les ingénieurs réseau, les administrateurs de base de données, etc.
- Le travailleur mécontent : cet utilisateur – qui peut être un employé, un sous-traitant, un consultant, un vendeur ou toute autre personne qui bénéficie d'un accès privilégié – a un grief contre l'entreprise et cherche à se venger en lui infligeant des dommages. Il n'est généralement pas motivé par un gain financier.
- L'agent double : cet utilisateur prétend respecter les règles de sécurité, mais vole des données à des fins lucratives. Sans un contrôle adéquat, il peut exercer ses activités illicites pendant des années.

Signes d'abus de comptes privilégiés

Toutes les organisations doivent être préoccupées par l'abus de comptes privilégiés, y compris les petites entreprises, qui sont désormais considérées comme *le ground zero* pour la cybercriminalité. Voici quelques signes précurseurs à surveiller :

- Un utilisateur déroge de ses activités habituelles. Ça peut vouloir dire une durée de session inhabituellement courte ou longue, un accès, l'affichage ou des modifications de fichiers qui ne font pas partie de sa routine ou des séquences de touches atypiques (qui peuvent être détectées par des analyses biométriques qui utilisent l'apprentissage automatique pour étudier un utilisateur au fil du temps).
- Un utilisateur transfère des fichiers vers un poste de travail personnel alors qu'il n'est autorisé qu'à transférer des fichiers vers des systèmes qui appartiennent à l'entreprise.
- Un compte utilisateur est accessible par plusieurs points d'extrémité (ordinateurs, serveurs) en même temps.

- Plusieurs utilisateurs sont connectés à partir du même point d'extrémité.
- Des comptes en dormance reprennent vie.
- Des titres de fenêtres inhabituels apparaissent.

Gardez également en tête que si la plupart des pirates informatiques ne sont pas les cybergénies représentés dans les films, ils ne sont pas stupides non plus. Par exemple, ils exécuteront souvent de petits tests pour voir si leur présence est détectée. Ils créeront également des comptes et les ajouteront à des groupes privilégiés, puis attendront des semaines ou des mois avant d'y accéder.

Comment réduire le risque d'abus

Voici quelques conseils pour sécuriser vos comptes privilégiés et réduire les risques :

- Auditez, analysez et déterminez quels comptes nécessitent un accès privilégié. Règle générale, les types de comptes suivants doivent nécessiter des privilèges élevés : les comptes administrateur de domaine, les comptes administrateur locaux, les comptes d'accès d'urgence, les comptes d'application, les comptes système et les comptes de service de domaine.
- Appliquez le principe de moindre privilège (POLP) qui accorde aux utilisateurs le privilège minimal requis pour effectuer leur travail.
- Utilisez le système de sécurité *Zero-Trust* qui suppose que tous les utilisateurs sont des menaces potentielles jusqu'à preuve du contraire. Établissez une microsegmentation du réseau pour déplacer le périmètre le plus près possible des applications privilégiées et des surfaces protégées.
- Établissez une procédure formelle et standardisée pour demander, autoriser, effectuer et documenter les changements de comptes et pour vérifier tous les changements majeurs.
- Mettez en place une procédure formelle et standardisée pour demander une désactivation rapide et complète des comptes qui ne sont plus nécessaires, comme lorsque les projets se terminent ou que les employés quittent l'entreprise.
- Suivez et enregistrez automatiquement l'activité de tous les utilisateurs – pas seulement les utilisateurs privilégiés.
- Informez clairement les employés, les sous-traitants, les fournisseurs et tous les autres utilisateurs (encore une fois, pas seulement les utilisateurs privilégiés) que l'utilisation du compte est surveillée. Cela peut être un moyen de dissuasion efficace pour certains abuseurs potentiels.

- Recevez des alertes sur les violations de la politique de sécurité et sur tous les écarts par rapport aux modèles de comportement normaux.
- Appliquez un contrôle rigoureux sur l'accès aux systèmes qui stockent des informations confidentielles.
- Maintenez un inventaire complet et à jour des clés et des certificats.
- Offrez une formation aux utilisateurs finaux afin qu'ils ne partagent pas leurs mots de passe et ne cliquent pas sur des liens non vérifiés ou suspects. Une plateforme de formation en ligne sur la cybersécurité est idéale pour ça, parce qu'elle permet aux utilisateurs finaux d'apprendre à leur rythme et les superviseurs peuvent suivre leurs progrès.

Comment Devolutions peut vous aider

En plus d'appliquer les stratégies et de mettre en place les politiques mentionnées précédemment, les solutions développées par Devolutions aident à réduire efficacement et à moindre coût le risque d'abus de comptes privilégiés :

- **Devolutions Password Server** comprend une nouvelle fonctionnalité intégrée de gestion d'accès privilégiés qui prend en charge une variété de fonctions comme la détection de comptes sur le réseau, l'approbation de réservations de comptes et une rotation automatique des mots de passe. En savoir plus ici.
- **Devolutions Password Hub** propose un contrôle d'accès basé sur les rôles, un coffre de mots de passe centralisé, un puissant générateur de mots de passe, etc. De plus, en raison de la pandémie de coronavirus, la période d'essai gratuite pour DPH a été étendue de 30 à 90 jours. En savoir plus ici.
- **Remote Desktop Manager** propose un contrôle d'accès basé sur les rôles, l'injection des identifiants, un partage de mots de passe administratifs, l'enregistrement de sessions, un coffre de mots de passe centralisé, etc. En savoir plus ici.
- **Wayk Now et Wayk Den** permettent tous les deux un accès sécurisé (dans le nuage ou hébergé sur vos propres serveurs) aux appareils à distance. Ils offrent un contrôle d'accès basé sur les rôles, des pistes d'audit de session et d'autres fonctions de sécurité qui font partie d'une gestion robuste de comptes privilégiés. En raison de la pandémie de coronavirus, avec toute installation de Wayk Den, des licences Wayk Now Enterprise sont gratuites pendant six mois. En savoir plus ici.

Conseil de notre Chef de la sécurité, Martin Lemay :

L'abus ou la compromission d'un compte privilégié provoque généralement des ravages. Des heures, des jours, des mois et des années d'efforts et d'argent peuvent être investis pour éviter une telle situation. Cependant, aucun professionnel de la sécurité ne garantira un risque 0. C'est pourquoi toutes les organisations doivent se préparer au pire et appliquer les directives suivantes en plus des conseils précédents :

- Préparez un plan d'intervention bien documenté et formez régulièrement votre personnel. Les organisations doivent réagir rapidement et efficacement pour se remettre de situations où un compte privilégié a été compromis. Le personnel non formé sera lent, négligent et permettra à des acteurs malveillants de faire plus de dégâts.
- Sauvegardez vos données en toute sécurité. Assurez-vous d'être prêt pour le pire et d'avoir une copie de vos données dans un environnement différent – et protégé par différents comptes privilégiés. Les procédures de restauration et l'intégrité des sauvegardes doivent être testées périodiquement.

Ces recommandations simples peuvent réduire considérablement l'impact d'un compte privilégié compromis en permettant un confinement rapide des menaces et en accélérant la reprise sécurisée des opérations. En mettant en pratique les conseils énumérés dans la section « Comment réduire le risque d'abus », les organisations pourront mieux prévenir, détecter, réagir et se remettre d'un abus ou d'une compromission de compte privilégié.

En résumé

La mauvaise nouvelle est que tant qu'il y aura des comptes privilégiés, il y aura un risque d'abus. Il n'y a aucun moyen d'arriver au risque 0, tout comme c'est impossible d'éliminer les cybermenaces, les logiciels malveillants, les rançongiciels, les vers… Et la liste est longue.

La bonne nouvelle, toutefois, est que les organisations peuvent – et franchement, doivent – être proactives pour réduire le risque d'être victimes de pirates externes et d'utilisateurs internes malveillants. Après tout, avec de grands privilèges viennent de grandes responsabilités!