Devolutions

Principe de moindre privilège : qu'est-ce que ça mange en hiver et bonnes pratiques

LES UTILISATEURS FINAUX NE BÉNÉFICIENT QUE DES ACCÈS DONT ILS ONT BESOIN POUR EFFECTUER LEUR TRAVAIL

Le principe de moindre privilège (connu sous l'abréviation *POLP* en anglais) est une politique selon laquelle les utilisateurs finaux ne bénéficient que des accès dont ils ont besoin pour effectuer leur travail - ni plus ni moins.

Évidemment, le POLP ne fait pas l'affaire de tous les utilisateurs finaux, parce qu'il restreint leur accès à certaines applications et certains réseaux qui ne sont pas essentiels à leur travail. Dans certains cas, ça peut impliquer la suppression d'interfaces telles que les ports USB des appareils afin que les utilisateurs finaux ne puissent pas involontairement injecter des logiciels malveillants en copiant des fichiers à partir d'une clé USB ou exfiltrer intentionnellement des informations confidentielles.

Le POLP n'est pas conçu pour punir les utilisateurs finaux ou leur rendre la vie plus difficile. Il vise à minimiser la taille de la surface d'attaque et, au final, à réduire la probabilité et la gravité d'une cyberattaque. Cette pratique est très importante, puisque les pirates visent régulièrement les comptes de bas niveau pour se propager sur d'autres appareils et réseaux et pour accéder aux systèmes critiques et aux données sensibles.

D'autres avantages du POLP

En plus de minimiser la taille de la surface d'attaque, le POLP offre des avantages supplémentaires en matière de sécurité, comme:

- Une sécurité renforcée : avant de mettre en place le POLP, les entreprises doivent analyser les niveaux d'accès actuels de chaque utilisateur final. Ce processus révèle souvent que de nombreux utilisateurs finaux – et dans certains cas, la plupart – ont un accès trop important aux réseaux et que cet accès peut facilement être limité sans nuire à leur travail. Cette pratique est expliquée en détail dans la section « Bonnes pratiques » plus loin dans cet article.
- Lutte contre les logiciels malveillants : le POLP peut aider à contenir les maliciels sur un ou sur un nombre limité d'appareils, ce qui peut donner aux équipes de sécurité le temps dont elles ont besoin pour enquêter, contenir et corriger la situation.
- Une meilleure stabilité : le POLP empêche les utilisateurs finaux avec des comptes de niveau relativement bas d'exécuter des changements qui affecteraient l'ensemble du système.
- Classification des données : le POLP aide les entreprises à déterminer les données dont elles disposent dans leur écosystème, où elles se trouvent et qui y a accès.
- Préparation aux audits : le POLP simplifie considérablement le processus d'audit.

Critères du POLP

Tout dépendant du système d'exploitation, le POLP peut être instauré en se basant sur un ou plusieurs critères tels que :

- Rôle (par exemple chefs de projet, gestionnaires de ressources, etc.)
- Ancienneté (par exemple superviseurs, gestionnaires, cadres, etc.)
- Départements (par exemple marketing, RH, etc.)
- Emplacement (par exemple le siège social, les bureaux satellites, etc.)

- Heure (par exemple les heures de bureau, après les heures de bureau, etc.)

Règle générale, les administrateurs système personnalisent le POLP en fonction des besoins spécifiques de leur entreprise et cherchent à trouver un équilibre entre le besoin d'une sécurité renforcée et le fait que les utilisateurs finaux ont besoin d'un accès suffisant pour être productifs et efficaces.

Les bonnes pratiques du POLP

Il existe un certain nombre de bonnes pratiques du POLP qui devraient être adoptées par plusieurs entreprises - et pas seulement les grandes organisations. Les PME sont devenues le « point zéro » de la cybercriminalité. Et 60% des petites entreprises font faillite dans les six mois suivant une cyberattaque majeure.

Les bonnes pratiques en matière de POLP comprennent :

- En consultation avec les utilisateurs finaux (ou chefs d'entreprise), évaluez chaque rôle pour déterminer le niveau d'accès approprié. Faites du « moindre privilège » le point de départ et ajoutez des niveaux d'accès supérieurs si nécessaire.
- Communiquez l'objectif du POLP à tous les utilisateurs finaux – y compris les coûts importants et les dommages à long terme d'un piratage majeur – afin qu'ils comprennent que l'approche ne vise pas à diminuer leur productivité, mais plutôt à protéger l'organisation (et de garder leur travail!).
- Lorsqu'un accès privilégié temporaire est requis, utilisez des informations d'identification à usage unique qui sont accordées au dernier moment et qui sont révoquées immédiatement après l'utilisation. Cette approche, connue sous le nom de bracketing de privilèges, peut être utilisée pour des utilisateurs finaux individuels ainsi que pour des processus ou des systèmes.
- Séparez les comptes administrateur des comptes standard.
- Séparez les fonctions des systèmes de niveau supérieur de celles de niveau inférieur.
- Suivez automatiquement toutes les connexions et l'activité; il est très important de voir exactement ce que font les utilisateurs finaux et quand ils le font.
- Auditez régulièrement les privilèges des utilisateurs finaux pour vous assurer que leur accès est approprié. Ça inclut la suppression de l'accès pour tous les employés qui ont quitté l'entreprise.
- Disposez d'un moyen de révoquer automatiquement l'accès privilégié en cas d'urgence.

Comment Devolutions Password Server peut aider

Devolutions Password Server (DPS) peut vous aider à mettre en place votre POLP. De manière sécurisée et centralisée, il permet aux entreprises de :

- Établir un accès basé sur les rôles aux comptes privilégiés et aux actifs critiques à l'échelle de l'entreprise.
- Définir des paramètres d'autorisation granulaires et globaux personnalisés.
- Disposer d'un contrôle central des journaux de gestion des accès privilégiés.
- S'assurer que seuls les administrateurs système autorisés puissent accorder un accès privilégié.
- Masquer les informations d'identification privilégiées des utilisateurs et les empêcher d'atteindre les terminaux.
- Stocker tous les noms d'utilisateur, mots de passe et accès aux comptes privilégiés dans un coffre centralisé protégé par un chiffrement approuvé par le gouvernement fédéral américain.

De plus, lorsqu'il est intégré à Remote Desktop Manager (RDM), DPS prend en charge la connexion directe en un clic aux sites Web, aux applications et aux ressources informatiques distantes, offrant une gestion simplifiée et hautement sécurisée des accès à distance. Il dispose également d'une interface Web intuitive permettant aux utilisateurs finaux de stocker des mots de passe et d'autres informations confidentielles.

Conclusion

Lors de la conférence Black Hat 2017, l'entreprise de solutions de comptes privilégiés Thycotic a mené une enquête auprès de plus de 250 pirates autoproclamés qui ont révélé que le moyen numéro un pour obtenir des données sensibles était de pirater des comptes privilégiés. Et selon le rapport d'enquête Verizon 2017 sur les violations de données, 81 % des violations proviennent de mots de passe volés, par défaut ou faibles. Faites rapidement le calcul. Ça signifie que le POLP n'est pas seulement une idée intelligente, mais qu'il est essentiel dans un environnement de plus en plus menaçant où les risques et les coûts d'une violation de données sont de plus en plus élevés.