Le NIST change de cap et déconseille de changer régulièrement de mot de passe

Devolutions

BEAUCOUP D'INTERROGATIONS DANS LE MONDE DE LA SÉCURITÉ DES INFORMATIONS

L'Institut national des normes et de la technologie (NIST) des États-Unis a mis à jour ses recommandations pour la gestion des mots de passe d'utilisateur, et certaines d'entre elles suscitent beaucoup d'interrogations dans le monde de la sécurité des informations.

Auparavant

Par le passé, le NIST (et de nombreuses autres organisations de conformité), demandait aux entreprises de mettre en œuvre deux stratégies de gestion des mots de passe : l'une obligeant les utilisateurs à choisir des mots de passe très complexes et, l'autre, à modifier régulièrement ces mots de passe.

Maintenant

Cependant, dans une démarche quelque peu surprenante, le NIST a inversé sa position sur ces deux piliers de la gestion des mots de passe. Il est maintenant conseillé aux entreprises de laisser les utilisateurs choisir des mots de passe relativement simples (mais pas des mots ridiculement simples comme « mot de passe » et « 1234567 ») et de mettre fin à la pratique qui consiste à obliger les utilisateurs à réinitialiser régulièrement leurs mots de passe.

Le fossé entre théorie et réalité

Le fossé entre ce que les utilisateurs sont censés faire (en théorie) et ce que nombre d'entre eux font (en réalité) explique la volteface du NIST.

En théorie, les utilisateurs - quels que soient leur département, leur division, leur équipe et leur titre d'emploi - sont supposés comprendre parfaitement l'importance de la gestion des mots de passe, même s'ils ne connaissent pas (ou ne se soucient pas) des détails techniques derrière les logiciels malveillants et autres menaces. En effet, la plupart des gens ne comprennent pas le fonctionnement d'une voiture, mais nous sommes toujours en mesure de conduire et de respecter les règles de sécurité routière.

Les utilisateurs - encore une fois théoriquement - sont censés choisir activement des mots de passe très complexes pour chaque compte et les modifier périodiquement. Non pas parce que « la gang des TI » les pousse à le faire, mais parce que c'est la chose nécessaire à faire.

Dans la vraie vie, trop d'utilisateurs - pas tous, mais plusieurs - ne réalisent pas que s'ils ne font pas partie de la solution, ils font partie du problème de sécurité. En raison de ce manque de compréhension (ou d'intérêt), ces utilisateurs utilisent souvent les mêmes mots de passe complexes pour plusieurs comptes. Encore pire, quand ils sont obligés de changer leurs mots de passe, ils ont tendance à choisir des mots de passe qui sont plus simples et plus faciles à retenir - et donc plus faciles à pirater que ce qu'ils utilisaient auparavant.

Fatigue sécuritaire

La cause fondamentale de ce problème - et un véritable fléau pour de nombreux professionnels de l'informatique - est une condition appelée « fatigue sécuritaire ». Comme nous l'avons écrit par le passé, la fatigue liée à la sécurité survient lorsque les utilisateurs sont débordés et épuisés par le besoin de se souvenir de plusieurs mots de passe, pratiques et règles de sécurité informatique. Au lieu de se mettre à niveau pour satisfaire aux exigences, ils tournent les coins ronds et repoussent les limites pour voir jusqu'où ils peuvent aller sans s'attirer les foudres de l'équipe des TI.

Malheureusement, avec autant d'utilisateurs à gérer – et chacun d'entre eux qui peuvent avoir des dizaines de comptes uniques - s'attendre à ce que le service informatique applique à 100 % la conformité est irréaliste. En réalité, ils ne peuvent pas faire grand-chose. Comme mentionné, les utilisateurs doivent jouer un rôle actif et faire partie de la solution de sécurité.

Limiter les dégâts

Le revirement de situation au NIST a donc principalement pour but d'atténuer le risque que représentent, involontairement, mais inévitablement, les utilisateurs. En recommandant aux utilisateurs de choisir des mots de passe complexes plutôt que très complexes et de ne pas les modifier régulièrement, le NIST tente de rendre les entreprises plus sécuritaires en réduisant l'écart entre la théorie et la pratique.

Bonnes pratiques

Pour vous adapter à cette nouvelle norme, nous vous recommandons d'adopter les bonnes pratiques suivantes :

1. Comparez les listes de nouveaux mots de passe avec les mots de passe fréquemment utilisés ou compromis

Dans Remote Desktop Manager v14, nous avons introduit la nouvelle fonctionnalité « Vérification des mots de passe » (Pwned Password Check), qui analyse les nouveaux mots de passe à l'aide d'une liste de plus de 500 000 000 mots de passe connus pour avoir été exposés à des violations de données. Pour plus d'informations sur cette fonctionnalité, y compris des instructions de configuration, c'est ici.

2. Utilisez des phrases secrètes plutôt que des mots de passe

Une phrase secrète ou une « phrase de passe » est beaucoup plus longue qu'un mot de passe classique (ce qui limite la vulnérabilité aux attaques par force brute) et contient des espaces entre les mots, comme ceci : « Plus votre mot de passe est complexe, mieux c'est! » La phrase peut contenir des symboles et des chiffres et elle ne doit pas nécessairement être grammaticalement correcte. Jenny, notre spécialiste des produits marketing, a d'ailleurs écrit un excellent article sur les avantages de l'utilisation des « phrases secrètes » et les inconvénients de l'utilisation des mots de passe.

3. Utilisez l'authentification à 2 facteurs

Bien que cette solution ne soit pas à toute épreuve, l'authentification à deux facteurs (2FA) ajoute un autre niveau de défense contre les accès non autorisés. Pour une comparaison des outils 2FA populaires (mise à jour pour inclure FreeOTP, Authenticator Plus et SoundLogin), veuillez cliquer ici.

Autres mises à jour

La publication spéciale 800-63 du NIST contient plusieurs autres nouveautés, dont des conseils sur la vérification de l'identité, l'authentification et l'identité fédérée. La publication (composée de plusieurs documents) peut être téléchargée sur le site Web du NIST à l'adresse https://pages.nist.gov/800-63-3.