La gestion des mots de passe

Importance de la gestion des mots de passe

Un mauvais mot de passe peut permettre à un attaquant d'accéder de manière illégitime au SI de l'entreprise et à des informations ou services sensibles, et peut induire des incidents de sécurité. Ainsi, il convient d'adopter quelques bonnes pratiques d'hygiène.

Mauvaises pratiques de gestion des mots de passe

Plusieurs mauvaises pratiques particulièrement répandues sont à éviter à tout prix :

- **L'utilisation de mots de passe faibles :** Bien souvent, des mots de passe simplistes tels que "123456" ou "azertyuiop" sont utilisés. Cela constitue donc une pratique risquée en les rendant d'une part faciles à deviner pour une personne marveillante et d'autre part faciles à forcer en accroissant leur vulnérabilité aux attaques par force brute.
- **La réutilisation de mots de passe :** De nombreux utilisateurs emploient le même mot de passe pour différents services. Par conséquent, la compromission d'un seul compte peut entraîner la compromission des données sur plusieurs plateformes par exemple.
- **Le stockage non sécurisé des mots de passe :** Stocker les mots de passe de manière non sécurisée, comme les noter sur un post-it ou les enregistrer dans un fichier non protégé sur son poste de travail, expose les informations sensibles et encourage une culture de la sécurité laxiste, augmentant ainsi considérablement les risques d'accès illégitimes ou d'incidents de sécurité.

Sécurisation des mots de passe : Bonnes pratiques

Pour garantir une gestion sécurisée des mots de passe, il est essentiel de suivre ces quelques recommandations :

- **Complexité :** Utilisez des mots de passe complexes composés d'une combinaison de lettres (majuscules et minuscules), de chiffres et de caractères spéciaux.
- **Longueur :** Plus votre mot de passe est long, plus il est difficile à déchiffrer. Visez un minimum de 12 caractères.
- **Non-réutilisation :** Utilisez des mots de passe uniques pour chaque compte. Cela limite les dégâts en cas de violation d'un seul compte.
- **Gestion sécurisée :** Utilisez un gestionnaire de mots de passe fiable pour stocker et générer vos mots de passe. Assurez-vous que ce gestionnaire est sécurisé par un mot de passe principal fort.
- **Authentification multifactorielle (MFA) :** Mettez en œuvre une solution d'authentification multifacteur pour ajouter une couche supplémentaire de sécurité en exigeant une deuxième vérification.
- **Sensibilisation :** Sensibilisez régulièrement les collaborateurs à l'importance d'une gestion sécurisée des identifiants, sous la forme de communication au sein de vos locaux, de formations (en ligne ou non) ou de jeux par exemple.

Ressources pertinentes

- Recommandations autour de la gestion des mots de passe de ***cyber malveillance*** [Site web]
- Recommandations de la ***CNIL*** autour de la gestion des mots de passe [Site web]
- Guide de l'***ANSSI*** autour des mots de passe et de la MFA [PDF]