Politique de mots de passe

Mis à jour le 09/01/2025

Pourquoi choisir un mot de passe robuste ?

Le mot de passe est la **clé d'entrée** de tous les services métiers ainsi que des fonctions à fort privilège (ex : compte d'administration).

Ainsi, **de nombreuses attaques sont facilitées par l'utilisation de mots de passe trop simples ou réutilisés d'un service à l'autre**.

Les attaques contre des mots de passe peuvent être de différentes natures, notamment :

- **Attaque par force brute** : l'attaquant va tenter toutes les combinaisons possibles les unes après les autres.
- **Attaque par dictionnaire** : l'attaquant va se baser sur une liste de mots de passe (mots de passe courants, listes de mots de passe divulgués…)
- **Attaque par ingénierie sociale** : l'attaquant va tester comme mot de passe des informations personnelles connues ou récupérées sur l'utilisateur (prénoms, dates…)

Une compromission de mot de passe peut avoir des finalités variées : **connexion illégitime** au SI, **exfiltration de données** accessibles depuis le compte compromis, **déploiement de charges malveillantes** (rançongiciels, outils d'espionnage, …), etc…

Ressources utiles

- E-learning « Gérez vos mots de passe (Débutant) » [Formation]
- Recommandations de l'ANSSI relatives aux mots de passe & coffre-fort [PDF]
- Calculer la « Force d'un mot de passe » |Lien]

Bonnes pratiques

- **Sensibiliser les utilisateurs** aux bonnes pratiques de choix de mot de passe et aux risques liés à la sélection d'un mot de passe qui serait trop facile à deviner. En particulier, pour éviter les attaques par ingénierie sociale, le mot de passe ne doit comporter aucun élément personnel.
- **Définir une longueur et une complexité minimales pour les mots de passe :** Selon les recommandations de l'ANSSI, ils doivent être composés de minimum **9 caractères** pour les services peu critiques et de minimum **15 caractères** pour les services critiques (dont la compromission donnerait accès à des informations personnelles et impacterait l'entreprise). Il est également recommandé de mettre en œuvre des règles de complexité tout en proposant un jeu de caractères le plus large possible (majuscule, minuscule, chiffre et caractère spécial).
- **Favoriser l'utilisation de mots de passe différents** pour chaque service nécessitant une authentification, ce qui permet de limiter la propagation d'une attaque en cas de compromission.
- **Recommander l'usage d'un coffre-fort numérique** de mots de passe (de préférence certifié par l'ANSSI), qui peut aider à générer et stocker des mots de passe robustes et permet de sauvegarder l'ensemble des mots de passe dans un fichier chiffré, accessible uniquement par un seul et unique mot de passe..
- **Bloquer les comptes à l'issue de plusieurs échecs de connexion** consécutifs afin d'éviter les attaques par force brute.
- **Désactiver les options de connexion anonyme** pour éviter qu'un attaquant pénètre dans le système sans authentification.
- **Déployer autant que possible l'authentification à double facteur,** notamment sur les accès externes et les comptes à privilèges