Politique de mot de passe

Pourquoi choisir un mot de passe robuste ?

Le mot de passe est la **clé d'entrée** à tous les services métiers ainsi que les fonctions à fort privilège (ex : compte d'administration). **De nombreuses attaques sur Internet 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 : attaques par force brute (l'attaquant tente le plus grand nombre de combinaisons possibles) ou par dictionnaires (l'attaquant tente les mots de passe les plus courants) ou encore par « ingénierie sociale » : l'attaquant teste alors des informations personnelles telles que les prénoms, etc.

Une attaque contre les mots de passe peut ne pas avoir comme finalité de se limiter au service impacté, mais permettre **une propagation de l'attaque au sein de l'entreprise ou à ses partenaires** (e-mail, etc.)

Quelles sont les ressources mises à disposition pour vous aider à monter en compétences sur le sujet :

- Améliorer la sécurité de vos mots de passe (formation) ;
- Bonnes pratiques de sécurité autour des mots de passes (PDF)
- Recommandations relatives aux mots de passe & coffre fort (PDF) ;
- Calculer la « Force d'un mot de passe (Site Web).

Les bonnes pratiques :

Mot de passe robuste :

- L'ANSSI recommande que la longueur d'un mot de passe soit corrélée avec la criticité du service auquel il donne accès, avec un minimum de **9 caractères** pour les services peu critiques (dont la compromission ne donnerait accès à aucune information personnelle et n'impacterait pas l'entreprise) et un minimum de **15 caractères** pour les services critiques (service d'administration).
- Un mot de passe robuste comporte des capitales et des minuscules, des chiffres et des caractères spéciaux
- Ces mots de passe ne doivent comporter aucun élément personnel (tel qu'une date de naissance ou un prénom). Il est possible d'avoir recours à une phrase de passe (ex : Unm0t2P@553séCUr1sé-)

Politique de mot de passe :

- Des mots de passe **différents** doivent être choisis pour chaque service nécessitant une authentification.
- Les utilisateurs doivent être **sensibilisés 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.
- **Un coffre-fort** de mots de passe peut aider à générer des mots de passe robustes et ne pas avoir à les mémoriser. Il permet de sauvegarder l'ensemble des mots de passe dans un fichier chiffré, accessible uniquement par un seul et unique mot de passe. Il est préférable d'utiliser un coffre-fort certifié par l'ANSSI. Néanmoins, les coffres forts stockés localement représentent un risque en cas de perte de l'ordinateur alors que les solutions Saas sont sujettes aux attaques en ligne.

Quelques mesures de sécurité :

Pour encadrer et vérifier l'application de ces bonnes pratiques, le **blocage des comptes** à l'issue de plusieurs échecs de connexion est nécessaire, ainsi que la **désactivation des options de connexion anonyme**.