Recommandations relatives aux mots de passe

24 rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 24 93
amsn@gouv.mc

1. Introduction

L'utilisation de mots de passe forts est l'une des briques de base dans la sécurisation d'un système d'information. Malheureusement cette première étape est souvent absente dans la politique de sécurité. Il est par conséquent assez fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut.

2. Objectif

Cette note a pour but de sensibiliser les utilisateurs de système d'information sur l'intérêt d'avoir des mots de passe forts.

Cela ne dispense en aucun cas :

- les administrateurs de mettre en place un contrôle systématique de la qualité des mots de passe ;
- les concepteurs d'application de mettre en place une politique complète et cohérente concernant l'utilisation et la gestion des mots de passe ;

Ces deux catégories de personnel sont invitées à se reporter au document édité par l'AMSN « Recommandations de sécurité relatives aux mots de passe », beaucoup plus complet et qui précise les limites de la sécurité apportée par les mots de passe. Ce document peu technique peut aussi être consulté par tout un chacun pour son information.

3. Un mot de passe fort.

Un bon mot de passe est avant tout un mot de passe fort, c'est à dire difficile à retrouver même à l'aide d'outils automatisés. La force d'un mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère le composant. En effet, un mot de passe constitué de minuscules, de majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules.

Néanmoins, un bon mot de passe doit être facile à retenir pour rester fort. Effectivement, si un mot de passe est trop compliqué à retenir, l'utilisateur trouvera différentes astuces comme, par exemple, l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier, lui permettant de s'authentifier. Pour ne pas mettre bêtement en danger la sécurité du système d'information (SI), il existe différents moyens mnémotechniques pour fabriquer et retenir des mots de passe forts.

4. Quelques recommandations :

Voici les principales recommandations à connaitre :

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- Ne demandez jamais à un tiers de générer pour vous un mot de passe ;

- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles ;
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur Internet), encore moins sur un papier facilement accessible ;
- Ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle ;
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe choisis.

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document « Recommandations de sécurité relatives aux mots de passe », évoqué ci-dessus.

5. Méthodes de création d'un mot de passe.

Si vous souhaitez une règle simple, choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Deux méthodes pour choisir vos mots de passe :

- La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
- La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.