UNIVERSITÉ DE LA RÉUNION

Politique de gestion des mots de passe

Préparé pour: Université de la Réunion
Préparé par: Laurent PEQUIN - R.S.S.I. (rssi@univ-reunion.fr)

16 mai 2018

UNIVERSITÉ DE LA RÉUNION

Sommaire

Présentation

Objectif

L'objectif de ce document est de présenter la politique de gestion des mots de passe au sein de l'université de la Réunion.

Buts de ce document

L'utilisation de mots de passe forts est l'une des briques de base dans la sécurisation d'un système d'information. Malheureusement, il est assez fréquent de trouver des comptes avec des mots de passe triviaux, sans mot de passe ou avec des mots de passe par défaut.

Cette note a pour but :

- ☑ de sensibiliser les utilisateurs de système d'information sur l'intérêt d'avoir des mots de passe forts
- ☑ de sensibiliser les administrateurs sur l'intérêt de mettre en place un contrôle systématique de la qualité des mots de passe
- ☑ de sensibiliser les concepteurs d'application, et les administrateurs sur l'importance d'une politique complète et cohérente concernant l'utilisation et la gestion des mots de passe
- ☑ de préciser les limites de la sécurité apportée par les mots de passe

Les mots de passe

Définition d'un mot de passe fort

Un mot de passe fort est un mot de passe qui est 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 lettres minuscules, de lettres majuscules, de caractères spéciaux et de chiffres est techniquement plus difficile à découvrir qu'un mot de passe constitué uniquement de minuscules. Mais cette difficulté dépend du nombre de caractères, et au delà de 18 caractères, nous pouvons admettre de n'utiliser que le caractère spécial espace (touche espace) et les caractères minuscules.

Créer un bon mot de passe

Un bon mot de passe est un mot de passe fort, qui sera donc difficile à retrouver même à l'aide d'outils automatisés mais facile à retenir. En effet, si un mot de passe est trop compliqué à retenir, l'utilisateur mettra en place des moyens mettant en danger la sécurité du SI, comme par exemple l'inscription du mot de passe sur un papier collé sur l'écran ou sous le clavier où l'utilisateur doit s'authentifier. Pour ce faire, il existe des moyens mnémotechniques pour fabriquer et retenir des mots de passe forts. La seule contrainte que nous demandons à l'utilisateur, est de créer un mot de a passe comportant au minimum 6 caractères dont 2 chiffres

ou caractères spéciaux (par exemple : & % @ # etc.) ou alors d'utiliser un mot de passe qui aille au delà de 18 caractères.

Méthodes des 18 caractères

Cette méthode consiste à utiliser uniquement la touche espace et les caractères minuscules (éventuellement, on pourra commencer son mot de passe avec une majuscule). Par exemple, j'adore les citations d'Albert, du coup, je vais m'en servir comme mot de passe : « La vie, c'est comme une bicyclette, il faut avancer pour ne pas perdre l'équilibre ». Vous remarquerez, sans avoir à les retenir, l'utilisation du caractère spécial de la guillemet simple (‘) et d'une majuscule en début de phrase. Pour ne pas avoir à retenir la position des virgules, je peux tout simplement retenir que je les ai toutes retirées, sans exception, … Mon mot de passe fait 82 caractères, il faudra donc à un ordinateur performant (actuellement) dans les 8.10^{171} années pour le décoder, ce qui vous laissera le temps de l'utiliser avant d'avoir à le changer…

Méthode phonétique

Cette méthode consiste à utiliser les sons de chaque syllabe pour fabriquer une phrase facile à retenir. Par exemple la phrase « J'ai acheté huit CD pour cent euros cet après midi » deviendra ght8CD%E7am.

Méthode des premières lettres

Cette méthode consiste à garder les premières lettres d'une phrase (citation, paroles de chanson...) en veillant à ne pas utiliser que des minuscules. Par exemple, la citation « un tiens vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

Politique de gestion des mots de passe

Les mots de passe sont souvent la seule protection d'une station de travail. Il est donc indispensable de mettre en œuvre une politique de gestion des mots de passe afin de protéger aussi bien l'utilisateur final que le système d'information.

Sensibilisation à l'utilisation de mots de passe forts

Les utilisateurs d'un système d'information doivent être sensibilisés à l'utilisation de mots de passe forts afin de comprendre pourquoi le risque d'utiliser des mots de passe faibles peut entraîner une vulnérabilité sur le système d'information dans son ensemble et non pas sur leur poste uniquement. Par exemple, vous êtes responsable d'un service, et votre mot de passe est volé par un tiers. Ceci entrainera la lecture de tous les courriers électroniques destinés au bon fonctionnement du service, l'usurpateur pourra ainsi répondre à ces courriers à votre place, répercuter les informations (ou les revendre) à d'autres personnes, etc. Les dommages causés ne pourront être réparés que très difficilement dans certains cas. Ceci est vrai quelque soit votre poste ou votre fonction.

Mot de passe initial

Le mot de passe initial doit être de préférence fourni sur un canal sûr. Lorsque ce mot de passe initial est fourni par l'administrateur du système ou lorsqu'il est communiqué sur un canal non confidentiel, il doit être changé dès la première connexion de l'utilisateur.

L'administrateur qui a fourni un mot de passe sur un canal non sûr doit avoir une vigilance plus soutenue afin de s'assurer que le mot de passe n'est pas utilisé par un tiers.

Le téléphone interne, le SMS (sans y mettre le nom d'utilisateur mais que le mot de passe sans autre explication), le face à face dans un bureau fermé seront considérés comme un canal sûr.

Renouvellement des mots de passe

Les mots de passe doivent avoir une date de validité maximale de six mois. Ceci permet de s'assurer qu'un mot de passe découvert par un utilisateur mal intentionné, ne sera pas utilisable indéfiniment dans le temps. Cependant, aucun mécanisme automatique n'est en place pour vérifier les changements.

Vous pouvez changer votre mot de passe à votre rythme via l'interface "https://moncompte.univ-reunion.fr/"

Les critères prédéfinis pour les mots de passe

Plusieurs critères peuvent être définis et mis en œuvre dans de nombreux systèmes pour s'assurer de la qualité des mots de passe. Ces critères sont, par exemple :

- ☑ une longueur minimum prédéfinie (au minimum 6 caractères dont 2 chiffres ou caractères spéciaux) ;
- ☑ l'impossibilité de réutiliser les « n » derniers mots de passe ;
- ☑ Si votre compte agit de manière anormale (téléchargements massifs et/ou illégaux, activité mail suspecte, ...) il sera suspendu et votre mot de passe désactivé. Pour rétablir la situation, il vous faudra vous rapprocher de votre informaticien de Proximité (dsi.univ-reunion.fr pour plus d'informations).
- ☑ Veillez à toujours activer la mise en veille après un certain temps d'inactivité sur votre poste de travail, en rajoutant l'option "déverrouiller par mot de passe". Ainsi, vous vous protégez en cas d'absence imprévue.

Confidentialité du mot de passe

Un mot de passe sert à s'authentifier sur un système. Dans ce but il est important de veiller à ne pas divulguer son mot de passe, **ni à un administrateur, ni à un supérieur hiérarchique**. Un mot de passe ne doit jamais être partagé ni stocké dans un fichier (note sur le bureau) ni sur papier, il est **personnel**.

La seule exception à cette règle est lorsque la politique de sécurité demande aux administrateurs du système d'information de stocker les mots de passe sur papier dans un lieu sûr (enveloppe cachetée dans un coffre ignifugé) pour le cas où un problème surviendrait.

Configuration des logiciels

Une large majorité de logiciels comme par exemple les logiciels de navigation Internet proposent d'enregistrer les mots de passe, par le biais d'une petite case à cocher « retenir le mot de passe », pour éviter à l'utilisateur la peine d'avoir à les ressaisir. Ceci pose plusieurs problèmes de sécurité notamment lorsqu'une personne mal intentionnée prend le contrôle de l'ordinateur d'un utilisateur, il lui suffit de récupérer le fichier

contenant la liste des mots de passe enregistrés pour pouvoir se connecter sur des sites à accès protégé. De manière générale, évitez d'activer ces options.

Utilisation de mots de passe différents

Il est important de garder à l'esprit qu'un mot de passe n'est pas inviolable dans le temps. C'est pour cette raison qu'il est nécessaire de changer régulièrement son mot de passe et qu'il est important de ne pas utiliser le même mot de passe pour tous les services vers lesquels on se connecte.

En effet, si le poste de travail est compromis et qu'un renifleur de clavier est installé, il sera possible pour un utilisateur mal intentionné de récupérer tous les mots de passe entrés au clavier (même si ces mots de passe sont des mots de passe forts). L'utilisateur mal intentionné pourra seulement accéder aux services dont il connaîtra le ou les mots de passe capturés durant la période pendant laquelle le renifleur de clavier était installé. Tant que les mots de passe capturés ne sont pas changés, des accès malveillants sont possibles, l'impact de l'attaque est durable.

C'est pourquoi changer régulièrement de mots de passe, à partir de machines saines, permet de diminuer la durée de l'impact de l'attaque, et c'est aussi pourquoi nous forçons l'utilisation d'un mot de passe web généré de manière aléatoire.

Utilisation de certificats clients et serveurs

L'utilisation de certificats de clés publiques sur les postes clients et serveurs permet de se passer de la saisie d'un mot de passe (résout le problème des keyloggers), mais reste vulnérable au vol sur le poste de travail du code porteur ou de la clé privée si elle n'est pas protégée. Pour certains services sensibles, l'utilisation d'une clef privée est obligatoire plutôt qu'un mot de passe pour l'authentification. C'est le cas par exemple lorsque vous activez l'accès au serveur *frontal-ssh.univ-reunion.fr*. Pour vos propres serveurs, ou machines de travail, il est préférable d'utiliser cette méthode si vous avez le choix.

Mettre en place un contrôle systématique des mots de passe

Pour s'assurer de l'absence de mots de passe faibles, le RSSI pourra réaliser des tests sur la robustesse des mots de passe utilisés sur son système d'information. Les personnes ayant des mots de passe trop faibles seront contactés en personne par le RSSI qui leur demandera de modifier leur mot de passe.

ATTENTION : Ce n'est pas un informaticien qui se chargera de cette opération, en ce sens, **vous n'aurez aucune information à lui transmettre**. La procédure est la même que pour un changement classique de mot de passe : allez sur https://moncompte.univ-reunion.fr : Veillez lors de l'accès à ce site que le certificat correspond bien à l'Université de la Réunion.