Bordeaux, le 19 décembre 2012

Affaire suivie par :
Paule Clavel
RSSI Académie de Bordeaux
rssi@ac-bordeaux.fr

RECOMMANDATION DE SECURITE

authentification par login et mot de passe

Référence	SG-SSI-2012-REC-02
Date version actuelle	19/12/2012
Destinataires cibles	Rectorat : DSI, CATICE, DAFPIC Direction des Services Départementaux de l'Education Nationale : CDTI EPLE : chef d'établissement, correspondant sécurité
Source	Guide ANSSI « l'hygiène informatique en entreprise » octobre 2012 note technique ANSSI « Recommandations de sécurité relative aux mots de passe » du 05 juin 2012 guide CNIL « La sécurité des données personnelles » édition 2010
Niveau de confidentialité	C1 : usage interne MEN

SOMMAIRE

[1] Référentiel Général de Sécurité http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html
[2]Agence Nationale de la Sécurité des Systèmes d'Information

PREAMBULE : LE POINT DE VUE DU REFERENTIEL GENERAL DE SECURITE RGS[3]

Extrait du RGS v1.0 du 06 mai 2010

« *L'authentification d'une personne auprès d'un système d'information distant fait intervenir trois entités :*

• l'utilisateur : ce dernier souhaite effectuer des opérations sur le système d'information distant et doit pour cela prouver son identité ;

• l'environnement de confiance local (exemple : le PC d'un agent administratif) ;

• le système d'information distant (exemples : une base de donnée, le serveur hébergeant un téléservice).

De manière générale, ***il n'est pas recommandé de permettre une authentification par «identifiant / mot de passe » de façon directe entre l'utilisateur et le système d'information distant****. En effet, un dispositif basé sur un identifiant et un mot de passe, du fait de la faiblesse intrinsèque qu'il présente en raison de la possibilité de rejeu, constitue un mécanisme de déverrouillage et non pas un réel mécanisme d'authentification. Un tel dispositif ouvre des possibilités de fraude largement employées, comme le hameçonnage, qui vise à récupérer les informations de connexion (identifiant et mot de passe) de l'utilisateur et permet donc d'usurper son identité.*

Ce mécanisme d'authentification ne peut donc offrir qu'un niveau de sécurité limité, qui peut cependant suffire dans certaines applications. Cette section n'impose aucune règle ni niveau de sécurité et se borne à donner quelques recommandations d'usage des identifiants et des mots de passe dans un processus d'authentification d'une personne sur un système d'information local ou distant. »

INTRODUCTION et REFERENCES

Cette recommandation vise à définir **les règles principales d'usage d'une authentification personnelle à base d'un couple login / mot de passe et particulièrement de la gestion du mot de passe**.

Pour rappel, et conformément au RGS, un mode authentification forte par définition basé sur un mécanisme intrinsèquement plus robuste est à privilégier.

La recommandation se base sur les avis faisant office de référence en la matière :

- la note technique de l'**ANSSI**[4] **« Recommandations de sécurité relatives aux mots de passe »**[5] **du 05 juin 2012**
- **le guide technique de l'ANSSI « L'hygiène informatique en entreprise » 15 novembre 2012**
- le guide de la **CNIL**[6] **« La sécurité des données personnelles » fiche n°2 « L'authentification des utilisateurs » édition 2010**

[3] http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html

[4] Agence Nationale de la Sécurité des Systèmes d'Information

[5] http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

[6] La Commission Nationale de l'Informatique et des Libertés

LES 8 REGLES ESSENTIELLES (ANSSI)

R1 : 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 ;
R2 : 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.) ;
R3 : ne demandez jamais à un tiers de générer pour vous un mot de passe ;
R4 : modifiez systématiquement et au plus tôt les **mots de passe par défaut** lorsque les systèmes en contiennent ;
R5 : renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles ;
R6 : 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 ;
R7 : ne vous envoyez pas vos propres mots de passe sur votre messagerie personnelle ;
R8 : configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

LES 2 CRITERES POUR UN « BON » MOT DE PASSE

Un « bon » mot de passe se juge au travers de 2 critères qui définissent le caractère « **robuste** » du mot de passe ; il doit être :

- **fort**, c'est à dire difficile à retrouver même à l'aide d'outils techniques spécialisés et de la connaissance des informations publiques du détenteur (civilité, age, date de naissance ...). La force du mot de passe dépend de sa longueur et du nombre de possibilités existantes pour chaque caractère qui le composent.
- **facile à retenir pour le détenteur** sur la base de moyens mnémotechniques qu'il a choisi

Par exemple :

- en ne conservant que les premières lettres des mots d'une phrase
- en optant pour une majuscule si le mot est un nom
- en gardant les signes de ponctuation au titre des caractères spéciaux
- en exprimant les nombres à l'aide de chiffres

LA POLITIQUE DE GESTION DE MOT PASSE

La politique globale de gestion des mots de passe, qui doit être un des éléments intégrée à la PSSI, fixe les éléments et les critères de l'organisation technique et organisationnelle à respecter. Les dispositifs techniques s'appuyant sur des mots de passe non rejouables (à usage unique) de type One Time Password sont à favoriser. Dans le cas ou ce n'est pas possible (avis RSSI), les principaux éléments à prendre en compte sont :

- **La sensibilisation** à l'utilisation de mots de passe forts
- **La gestion du mot de passe initial** ; si le mot de passe initial n'est pas défini par l'utilisateur mais communiqué par un administrateur système, il faudra s'assurer de l'utilisation d'un canal confidentiel et du changement par l'utilisateur dès sa première connexion
- **Le renouvellement des mots de passe** : à chaque mot de passe doit être associée une

durée de validité maximale au-delà de laquelle l'authentification sera rejetée. Un procédé assurant la confidentialité de l'opération de renouvellement doit être proposé aux utilisateurs ; il pourra éventuellement se baser sur un outil technique de type console self-service validé par la RSSI.

- **Les critères pré-définis pour des mots de passe forts** dont le détail est à affiner sous responsabilité du RSSI en fonction du SI concerné et du niveau de risque accepté. Il convient notamment d'évaluer la force de chaque nouveau son mot de passe via un outil de confiance [7]. Il est souvent plus efficace d'allonger un mot de passe que de chercher à le rendre plus complexe
  - **une longueur minimale** de 12 caractères est conseillée par l'ANSSI bien qu'une longueur de 8 caractères est généralement admise pour un mot de passe « classique ;
  - **chaque caractère constituant le mot de passe doit pouvoir prendre le nombre maximal de valeur ; par défaut lettres minuscules, lettres majuscules, caractères spéciaux et chiffres**
  - l**'impossibilité de réutiliser à minima les 2 derniers mots de passe**
  - le nombre de tentatives possibles avant verrouillage du compte
  - la manière de déverrouiller un compte bloqué ; il peut être souhaitable de prévoir un déblocage automatique
- **La confidentialité des mots de passe** ; un mot de passe est personnel, il ne doit jamais être communiqué, partagé ou encore stocké sans protection adaptée et validé par le RSSI (PSSI)
- La mise en place d'un **contrôle systématique de la robustesse des mots de passe** sous le contrôle du RSSI dans le cadre d'une démarche pro-active
- Le traitement d'une déclaration de vol ou de perte d'un mot de passe doit garantir la protection contre l'usurpation de l'identité de l'utilisateur

[7] ANSSI Calculer la force d'un mot de passe http://www.securite-informatique.gouv.fr/gp_article728.html