Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

AUTHENTIFICATION MOT DE PASSE

DEFINITION

Le mot de passe reste le moyen d'authentification le plus répandu. Alors que les compromissions de bases entières de mots de passe se multiplient, la CNIL a adopté une nouvelle recommandation sur les mots de passe. Elle fixe les mesures minimales à mettre en œuvre.

Basée sur la gestion d'un secret, l'authentification par identifiant et mot de passe est un moyen simple et peu coûteux à déployer pour contrôler un accès.

Toutefois, cette méthode d'authentification présente un niveau de sécurité faible.

Ces dernières années, de nombreuses attaques informatiques ont entrainé la compromission de bases de données entières de comptes et des mots de passe associés. Ces fuites de données ont notamment contribué à enrichir les connaissances des attaquants en matière de mots de passe. Les risques de compromission des comptes associés à cette méthode d'authentification se sont fortement accrus et imposent une vigilance particulière.

Ce document est constitué, en grande partie, à partir des recommandations de la CNIL et issu de la page du site de la Cnil suivante :

https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

Date : 06/06/2018

LES RISQUES ?

Les risques liés à la gestion des mots de passe sont multiples et reposent notamment sur :

1. la simplicité du mot de passe ;
2. l'écoute sur le réseau afin de collecter les mots de passe transmis ;
3. la conservation en clair du mot de passe
4. la faiblesse des modalités de renouvellement du mot de passe en cas d'oubli (cas des questions « secrètes »).

Il n'existe pas de définition universelle d'un bon mot de passe, mais sa complexité et sa longueur permettent de diminuer le risque de réussite d'une attaque informatique qui consisterait à tester successivement de nombreux mots de passe (attaque dite en force brute). On considère que la longueur du mot de passe suffit pour résister aux attaques courantes à partir de 12 caractères. Lorsque la taille du mot de passe diminue, des mesures compensatoires doivent être prévues.

LES EXIGENCES DE LA CNIL

1. L'authentification par mot de passe : longueur, complexité, mesures complémentaires

En termes de taille et de complexité du mot de passe varient en fonction des mesures complémentaires mises en place pour fiabiliser le processus d'authentification : ainsi, si une authentification est basée exclusivement sur un mot de passe, cela implique a minima l'utilisation d'un mot de passe complexe d'au moins 12 caractères composé de majuscules de minuscules, de chiffres et de caractères spéciaux. Des mesures complémentaires à la saisie d'un mot de passe (restrictions, d'accès, collecte d'autres donnée, support détenu en propre par l'utilisateur) permettent de réduire la longueur et la complexité du mot de passe, car ces mesures permettent d'assurer un niveau de sécurité équivalent au mot de passe seul.

Exemple : Un mot de passe associé à une double authentification pas SMS peut être composé seulement de 4 caractères, car le MDP est associé à une seconde authentification.(Espace Technologie)

Dans tous les cas,

Le mot de passe ne doit pas être communiqué en clair par courrier électronique.
Ces exigences sont des règles minimales. Le contrôle d'accès peut devoir reposer sur des règles plus robustes selon les risques auxquels le système est exposé.

2. Sécurisation de l'authentification

Quelles que soient les mesures mises en place, la fonction d'authentification doit être sûre :

- Elle utilise un algorithme public réputé fort
- sa mise en œuvre logicielle est exempte de vulnérabilité connue.

Lorsque l'authentification n'a pas lieu en local, l'identité du serveur doit être contrôlée au moyen d'un certificat d'authentification de serveur et le canal de communication entre le serveur authentifié et le client doit être chiffré à l'aide d'une fonction de chiffrement sûre. La sécurité des clés privées doit être assurée.

3. La conservation des mots de passe

Le mot de passe ne doit jamais être stocké en clair. Lorsque l'authentification a lieu sur un serveur distant, et dans les autres cas si cela est techniquement faisable, le mot de passe doit être transformé au moyen d'une fonction cryptographique non-réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé.

4. Le renouvellement du mot de passe

- Renouvellement périodique

Le responsable de traitement veille à imposer un renouvellement du mot de passe selon une périodicité pertinente et raisonnable, qui dépend notamment de la complexité imposée du mot de passe, des données traitées et des risques auxquels il est exposé.
La personne concernée doit être en mesure de changer elle-même son mot de passe. Dans ce cas, les règles afférentes à la création de mots de passe s'appliquent.

- Renouvellement sur demande

À la demande de la personne concernée, par exemple en cas d'oubli, le responsable de traitement met en œuvre une procédure de renouvellement du mot de passe.
Si ce renouvellement nécessite l'intervention d'un administrateur, un mot de passe temporaire est attribué à la personne concernée, le changement du mot de passe attribué temporairement lui est imposé lors de sa première connexion.
Si ce renouvellement intervient de manière automatique : le mot de passe ne doit pas être transmis en clair. L'utilisateur doit être redirigé vers une interface dont la validité ne doit pas excéder 24 heures, lui permettant de saisir un nouveau mot de passe, et ne permettre qu'un seul renouvellement.
Si le renouvellement fait intervenir un ou plusieurs éléments supplémentaires (numéro de téléphone, adresse postale…) :

- Ces éléments ne doivent pas être conservés dans le même espace de stockage que l'élément de vérification du mot de passe ; sinon, ils doivent être conservés sous forme chiffrée à l'aide d'un algorithme public réputé fort, et la sécurité de la clé de chiffrement doit être assurée
- Afin de prévenir les tentatives d'usurpation s'appuyant sur le changement de ces éléments, la personne doit être immédiatement informée de leur changement.

Ce document est constitué, en grande partie, à partir des recommandations de la CNIL et issu de la page du site de la Cnil suivante :

https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires

Date : 06/06/2018

Texte officiel

- **> Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe**
- **> Délibération n° 2017-190 du 22 juin 2017 portant modification de la recommandation relative aux mots de passe**

https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires