Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

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.

Recommandations de la CNIL sur les mot de passe (Délibération n° 2017-012 du 19 janvier 2017)

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.

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 »).

Les principaux risques identifiés au cours du cycle de vie d'un mot de passe

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.

PHRASE2PASSE : UN OUTIL POUR ACCOMPAGNER LES UTILISATEURS

Pour aider les utilisateurs à choisir un mot de passe robuste et un moyen mnémotechnique, la CNIL a développé un outil pour générer un mot de passe à partir d'une phrase.
Le code de cet outil est disponible sous la forme d'une extension logicielle en javascript, afin que vous puissiez l'intégrer dans vos applications.
>Télécharger l'extension

Les exigences de la CNIL

1.

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

Les exigences minimales de la CNIL 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.
Le tableau ci-dessous fait état des 4 cas d'authentification par mot de passe identifiés par la CNIL dans sa recommandation

	Exemple d'utilisation	Longueur minimum	Composition du mot de passe	Mesures complémentaires
Mot de passe seul	FORUM, BLOG	12	• majuscules • minuscules • chiffres • caractères spéciaux	Conseiller l'utilisateur sur un bon mot de passe
Avec restriction d'accès (le plus répandu)	SITES DE E-COMMERCE, COMPTE D'ENTREPRISE, WEBMAIL	8	Au moins 3 des 4 types suivants : • majuscules • minuscules • chiffres • caractères spéciaux	Blocage des tentatives multiples : (exemples) • Temporisation d'accès au compte après plusieurs échecs • « Capcha » • Verrouillage du compte après 10 échecs
Avec information complémentaire	BANQUE EN LIGNE	5	Chiffres et/ou lettres	Blocage des tentatives multiples + • Information complémentaire communiquée en propre d'une taille d'au moins 7 caractères (ex : identifiant dédié au service) **ou** • Identification du terminal de l'usager (ex : adresse IP, adresse MAC…)
Avec matériel détenu par la personne	CARTE BANCAIRE OU TÉLÉPHONE	4	Chiffres	Matériel détenu en propre par la personne (ex : carte SIM, carte bancaire, certificat) + Blocage au bout de 3 tentatives échouées

Dans tous les cas,
le mot de passe ne doit pas être communiqué à l'utilisateur 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. Il doit être transformé au moyen d'une fonction cryptographique non-réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé.
Le sel ou la clé doit être généré au moyen d'un générateur de nombre pseudo-aléatoires cryptographiquement sûr (il utilise un algorithme public réputé fort et sa mise en œuvre logicielle est exempte de vulnérabilité connue). Il ne doit pas être stocké dans le même espace de stockage que l'élément de vérification du mot de passe.

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.

Que faire en cas de risque de compromission du mot de passe ?

Si un responsable de traitement de données détecte une violation de données en rapport avec le mot de passe d'une personne,
• Le responsable de traitement doit notifier la personne concernée, dans un délai n'excédant pas 72 heures ;
• Il doit imposer à l'utilisateur concerné le changement de son mot de passe lors de sa prochaine connexion ;
• Il doit lui recommander de veiller à changer ses mots de passe d'autres services dans l'hypothèse où il aurait utilisé le même mot de passe pour ceux-ci.
Faites-nous par de vos remarques
Les professionnels sont invités à remonter à la CNIL les difficultés de mise en œuvre que pourrait poser l'application de cette recommandation. Cette recommandation pourra faire l'objet de révisions et de mises à jour.

Texte officiel

> Délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe
…[lire la suite]

Réagissez à cet article