Comment mettre en œuvre une politique de mot de passe efficace ? Par Gerard Haas, Avocat.

Parution : samedi 13 mai 2023

Adresse de l'article original :
https://www.village-justice.com/articles/comment-mettre-oeuvre-une-politique-mot-passe-efficace,46065.html

Véritable casse-tête, la création et la conservation d'un mot de passe obligent désormais les utilisateurs à faire preuve d'une grande créativité : nombre minimum de caractères, interdiction d'utiliser des dates de naissance, obligation d'insérer des caractères spéciaux, interdiction d'utiliser des mots du dictionnaire...

Pourtant, ces limitations revêtent une importance primordiale à l'heure où, comme le révèle une étude de Verizon, environ 80% des violations de données résultent d'attaques par force brute - c'est-à-dire du test successif des combinaisons possibles d'un mot de passe - ou de l'utilisation d'identifiants perdus ou volés.

Pour se prémunir d'une telle attaque, les organismes ne sont pas sans défense : la politique de mot de passe est un outil de choix pour la lutte contre les cyber-risques. Encore faut-il que cette politique soit efficace et effective...

C'est dans l'optique d'aider les organismes à mettre en place ce document que la CNIL a publié une version actualisée de sa recommandation en matière de mots de passe.

- Pourquoi rédiger votre propre politique de mot de passe ?

L'article 5-1-f) du RGPD met à la charge du responsable de traitement une obligation de sécurité des données traitées, sécurité qui passe notamment par une utilisation encadrée des mots de passe.

Une cyberattaque peut avoir des conséquences catastrophiques non seulement d'un point de vue réputationnel, mais également financier : selon un rapport d'IBM Security [1] le coût moyen d'une cyberattaque pour une entreprise est de 4 millions de dollars.

Or, mettre en place une politique de gestion des mots passe participe à **assurer cette sécurité des données.**

Face aux politiques natives que proposent certaines solutions et de l'urgence de se mettre en conformité aux dispositions du RGPD, il peut être tentant de réutiliser ces documents.

Pourtant, une politique de mot de passe efficace ne peut se fonder sur ces seuls éléments.

En effet, la sécurité est conditionnée à l'utilisation de procédures et politiques conformes à la réalité des opérations réalisées. La CNIL, dans sa nouvelle recommandation souligne cette nécessité en rappelant que

> « *la taille et le contenu de la liste de mots de passe à refuser doivent être proportionnels aux risques et, le cas échéant, adaptés au contexte d'usage* ».

Dès lors, il est fortement recommandé que la politique de mot de passe soit personnalisée et adaptée aux besoins de l'entreprise.

Il est d'autant plus important d'apporter un soin particulier à la conception de cette politique que les organismes peuvent être sanctionnés en cas de manquement grave aux principes de sécurité, et notamment en cas d'absence de politique de gestion des mots de passe. En ce sens, la CNIL a relevé que les manquements relatifs à ces politiques faisaient partie des manquements les plus souvent constatés lors de ses contrôles en 2021 [2].

En 2022, la CNIL a par exemple condamné Infogreffe [3] à payer une amende de 250.000 euros en raison du fait que

> « *l'organisme n'imposait pas l'utilisation d'un mot de passe robuste à la création d'un compte sur son site web et qu'il était impossible pour les 3,7 millions de comptes de saisir un mot de passe sécurisé en raison de la limitation de leur taille* ».

- Comment rédiger votre politique de mot de passe ?

Mises à jour dernièrement, les recommandations publiées par la CNIL et l'ANSSI en la matière prennent en considération l'évolution des connaissances tout en s'alignant sur leurs préconisations respectives.

L'ANSSI a ainsi publié en octobre 2021 ses « *recommandations relatives à l'authentification multifacteur et aux mots de passe* » [4] au sein desquelles elle présente les différentes étapes et questions qui doivent jalonner la création de la politique de mots de passe. C'est l'occasion également pour l'agence de proscrire certaines pratiques telles que l'utilisation des SMS comme moyen de réception d'un facteur d'authentification.

Plus récente encore, la dernière recommandation de la CNIL en la matière a permis à la commission de s'aligner sur les préconisations de l'ANSSI tout en corrigeant sa recommandation datée de 2017 [5].

La CNIL a en effet identifié les principaux facteurs de vulnérabilité et les menaces associées qui ponctuaient le cycle de vie d'un mot de passe :

Les principales recommandations de la CNIL sont les suivantes :

Base l'authentification sur les notions « d'entropie » et de « devinabilité ».

La recommandation de 2017 encadrait la vérification de la robustesse des mots de passe par la mise en place de seuils en termes de nombre de caractères et de complexité.

Ce qui change avec la nouvelle recommandation : constatant que la précédente recommandation manquait de flexibilité, la CNIL introduit le concept « *d'entropie* », une unité qui permet d'évaluer la robustesse d'un mot de passe au regard, non pas de sa longueur mais du nombre de tentatives qui seraient nécessaires pour deviner le mot de passe par force brute. La CNIL invite également à s'appuyer sur la notion de « *devinabilité* », qui implique d'évaluer non pas le degré de respect à la politique de mot de passe, mais la facilité qu'aurait un cyberattaquant pour retrouver ce mot de passe.

A ce titre, la CNIL recommande des niveaux minimum d'entropie pour trois cas d'usage :

l'authentification par mot de passe « *simple* » dont l'entropie minimum doit être de 80 bits ;
l'authentification avec restriction d'accès dont l'entropie minimum doit être de 50 bits ;
l'authentification avec matériel détenu par la personne concernée dont l'entropie minimum doit être de 13 bits.

Le quatrième cas d'usage envisagé par la CNIL dans sa recommandation de 2017 - authentification avec une autre restriction d'accès et une information complémentaire - a donc été abandonné.

La CNIL abandonne l'exigence généralisée de renouvellement périodique des mots de passe.

Parmi les principales recommandations de 2017 figurait le renouvellement périodique du mot de passe.

Ce qui change avec la nouvelle recommandation : s'appuyant sur de récentes études et sur la dernière recommandation de l'ANSSI en la matière, la CNIL a adopté la conclusion selon laquelle le fait de forcer l'utilisateur à changer son mot de passe à une fréquence régulière n'est pas une mesure réellement efficace. Aussi, la CNIL recommande de ne plus demander une telle modification périodique qu'aux comptes d'administration.

Les mots de passe ne doivent jamais être stockés en clair.

La CNIL préconise que, lorsqu'il est conservé, le mot de passe doit être préalablement transformé au moyen d'une fonction cryptographique spécialisée, non réversible et sûre, intégrant un « *sel* » - c'est-à-dire une information supplémentaire qui permet d'éviter que deux données identiques donnent la même valeur hachée sur deux systèmes informatiques différents - et des paramètres relatifs aux coûts en temps et/ou en mémoire nécessaires à son attaque.

- Comment faire appliquer votre politique de mot de passe ?

La bonne application d'une politique de mot de passe par les utilisateurs ne passe pas simplement par la mise en place de limitations lors de la saisie du mot de passe.

Cette politique doit en réalité s'inscrire dans une démarche de cybersécurité et de mise en conformité plus globale. Cette démarche implique notamment :

La formation des collaborateurs à la cybersécurité. Une fois sensibilisés, les utilisateurs seront en mesure d'appréhender l'importance de cette politique et d'appliquer au mieux son contenu. Au contraire, fournir une telle politique aux utilisateurs sans leur donner plus d'explications est le meilleur moyen de la rendre inefficace.
La rédaction d'un référentiel de sécurité complet. Les différents documents qui peuvent composer ce référentiel (Politique de Sécurité des Systèmes d'Information [6], charte administrateur [7], charte informatique, politique de gestion des habilitations [8], politique de durée de conservation des données…) doivent se répondre et se compléter pour augmenter leurs portées respectives. Compte tenu du rôle que joueront ces politiques en cas de contrôle, d'audit ou de gestion d'un incident de sécurité, il est primordial d'apporter une attention accrue à leur contenu.
L'adaptation des pratiques en matière de sécurité à l'évolution des connaissances et des technologies. Il est indispensable de prendre en considération les dernières recommandations en matière de protection des systèmes d'information afin de prévenir au mieux les risques de cyberattaque et d'anticiper les risques de sanction.

Loin d'être un simple document listant les restrictions que doit garder en tête l'utilisateur pour créer son mot de passe, la politique de mot de passe a **un rôle essentiel** à jouer dans la protection des systèmes d'information.

Gerard Haas Avocat associé fondateur du Cabinet Haas Avocats au barreau de Paris

[1] https://www.ibm.com/reports/data-breach

[2] https://www.cnil.fr/sites/default/files/atoms/files/cybersecurite_-_chiffres_2021.pdf

[3] https://info.haas-avocats.com/droit-digital/rgpd-quelles-sont-les-regles-de-conservation-des-donnees?hsLang=fr

[4] https://www.ssi.gouv.fr/uploads/2021/10/anssi-guide-authentification_multifacteur_et_mots_de_passe.pdf

[5] https://www.haas-avocats.com/ecommerce/les-recommandations-cnil-matiere-mots-passe/

[6] https://info.haas-avocats.com/droit-digital/pourquoi-formaliser-une-politique-de-securite-des-systemes-dinformation?hsLang=fr

[7] https://info.haas-avocats.com/droit-digital/pourquoi-faire-une-charte-administrateurs-des-si$?hsLang=fr

[8] https://info.haas-avocats.com/droit-digital/pourquoi-formaliser-une-politique-de-gestion-des-habilitations?hsLang=fr