Nomos
société d'avocats

nomosnetcom.fr **Mars 2017**

Recommandation de la CNIL sur les mots de passe

[DONNEES PERSONNELLES]
Délibération de la CNIL n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe

L'authentification par mot de passe reste l'un des mécanismes les plus répandus, aussi bien au sein des systèmes d'information internes aux entreprises que pour accéder à un certain nombre de services en ligne. Or, l'étape d'authentification est aux systèmes informatiques ce que la porte d'entrée est aux habitations : il ne sert à rien de construire un bunker si la porte n'a pas de serrure.

C'est pourquoi la CNIL est particulièrement vigilante en matière de mots de passe et a publié au début de l'année une recommandation sur ce sujet. L'on retiendra que les règles précédemment posées par la CNIL sont renforcées et enrichies. Cette recommandation s'adresse aux responsables de traitement, qui doivent imposer aux personnes concernées des critères spécifiques pour le choix des mots de passe, mais également respecter certaines règles relatives à l'authentification, la conservation des mots de passe et leur renouvellement, ainsi qu'à la notification en cas de violation.

Ainsi, la complexité du mot de passe tiendra compte des autres mécanismes mis en œuvre pour sécuriser l'authentification :

- En cas de simple couple identifiant + mot de passe, ce dernier devra être au minimum de 12 caractères et comporter des majuscules, des minuscules, des chiffres et des caractères spéciaux.

  Auparavant, la CNIL n'exigeait dans ce cas qu'une longueur minimale de 8 caractères.

- Dans la plupart des cas, il sera relativement aisé de renforcer la sécurité à l'aide d'une mesure de restriction d'accès au compte. Celles ci peuvent notamment prendre la forme d'un blocage après plusieurs essais infructueux ou d'un mécanisme de détection des soumissions automatiques (« captcha »).

  Dans cette hypothèse, le mot de passe pourra être limité à 8 caractères et ne contenir que 3 des 4 catégories de caractères visées ci-dessus.

- L'authentification à deux facteurs (ex : envoi d'un code par téléphone) permettra de réduire la longueur du mot de passe à 5 caractères sous réserve qu'une mesure de restriction d'accès soit également prévue.

- Enfin, la CNIL évoque l'authentification relative à un matériel spécifique détenu par la personne concernée (ex : cartes SIM). Elle indique que le mot de passe peut être limité à 4 chiffres mais que le matériel devra être bloqué après trois tentatives infructueuses.

La CNIL précise naturellement que l'ensemble du système d'authentification doit être sécurisé, par le biais d'algorithmes publics réputés forts et dont la mise en œuvre logicielle est exempte de vulnérabilité connue. Les responsables de traitement devront donc veiller à ce que leurs systèmes répondent à l'état de l'art en matière de sécurité informatique. Sur ce point, l'on notera que la fonction de hachage SHA1 reste très populaire aux fins de signer les certificats électroniques, malgré son obsolescence depuis environ douze ans. Les principaux éditeurs de navigateurs internet sont cependant en train de l'abandonner définitivement.

La conservation des mots de passe est également un point important. En aucun cas les mots de passe ne peuvent être stockés en « clair ». La CNIL recommande, préalablement à l'enregistrement dans la base de données, d'ajouter au mot de passe un sel ou une clé, puis de hacher le résultat à l'aide d'une fonction de chiffrement réputée sûre (voir ci-dessus).

La Commission incite en outre les responsable de traitement à permettre et encourager le renouvellement périodique de mots de passe et pose les règles applicables à tout mécanisme de renouvellement (automatique ou à la demande de l'utilisateur suite à un oubli). En aucun cas, le mot de passe ne peut être transmis en clair aux personnes concernées (notamment par email).

Enfin, la CNIL recommande que la violation du mot de passe ou des données associées à son renouvellement soit notifiée à la personne concernée dans un délai de 72 heures à compter de la constatation de la violation. En pareil cas, le mot de passe devra être impérativement renouvelé. Il convient cependant de noter que le Règlement européen n'impose la notification aux personnes concernées que lorsque la violation de données est susceptible d'entrainer un risque élevé au regard de leurs droits et libertés. Or, justement, le Règlement considère que tel ne devrait pas être le cas si les données sont chiffrées, ce que recommande la CNIL en matière de mots de passe.

Sylvain NAILLAT