Quelques bonnes pratiques de sécurité relatives aux facteurs d'authentification

Facteurs de connaissance

Développement et administration

- Les formulaires de connexion doivent accepter le collage des mots de passe,
- Les formulaires de connexion vérifiant la composition des mots de passe doivent pouvoir détecter les phrases de passe, donc dans ce cas ne pas imposer de caractères spéciaux,
- Les coffres-forts de mots de passe, au même titre que les autres composants d'un système d'information, doivent être tenus à jour. Une veille relative aux nouvelles publications est donc obligatoire,
- Les mots de passe doivent être stockés "hachés" avec du sel ce qui permet de les rendre non-réversibles. Le sel est une donnée aléatoire supplémentaire concaténée aux mots de passe afin d'empêcher que deux mots de passe identiques ne donnent le même condensat sur deux systèmes différents. L'ajout de sel est une solution technique face aux attaques par *rainbow tables*,
- Ne pas laisser les logiciels autres que les coffres-forts se souvenir des mots de passe,
- Pour les comptes peu sensibles, ne pas forcer les utilisateurs à renouveler leurs mots de passe, sauf en cas de compromission avérée ou supposée,
- Pour les comptes très sensibles, forcer les utilisateurs à renouveler fréquemment leurs mots de passe sous réserve qu'ils ne soient pas itérés,
- Utiliser un mot de passe différent par système/compte/service,
- Lorsqu'un mot de passe ne peut être que faible, par exemple un code PIN d'une carte à puce, des mesures compensatoires doivent être prises,
- L'application consultée doit supporter la réinitialisation immédiate de tous les mots de passe,
- Les applications doivent pouvoir vérifier la conformité des mots de passe au regard des meilleurs pratiques sans possibilité de la contourner,
- Les applications devraient contrôler le contenu des mots de passe pour rejeter ceux qui contiennent des motifs spécifiques, des informations personnelles et ceux qui ont déjà fuité,
- Interdire la réutilisation des mots de passe précédents et des variantes trop proches,
- Préférer les fonctions de dérivation de clé dites "memory-hard" telles que *scrypt* ou *Argon2/Argon2d/Argon2id* au lieu des fonctions de hachage comme *SHA-2/SHA-3*. Elles sont très consommatrices de mémoire, ce qui n'est pas un problème lors d'une utilisation légitime. Si ce n'est pas possible, utiliser *PBKDF2*.

Sauvegarde

- Les bases de données des coffres-forts de mots de passe doivent être sauvegardées régulièrement hors-ligne.

Qualité

- Afin de limiter les attaques par "dictionnaire", il convient de générer des mots passe les plus aléatoires possible,

- Les systèmes d'authentification sous forme de questions-réponses doivent être exempts d'informations facilement identifiables ou devinables (par exemple le lieu de naissance des personnes concernées). Dans tous les cas, ces données doivent être stockées chiffrées,
- Il convient d'employer des phrases de passe dont les mots issus du dictionnaire sont aléatoires et sans liens,
- Allonger les mots de passe est préférable à forcer les utilisateurs d'utiliser des caractères spéciaux pour ceux devant être mémorisés.

Transmission

- Les mots de passe ne doivent ni être stockés ni transmis en clair par quelque moyen que ce soit,
- Les éventuels mots de passe envoyés par courriers postaux doivent être temporaires et protégés contre les lectures indésirables,
- Ne pas demander à un tiers de créer un mot de passe pour une personne,
- Les méthodes de recouvrement d'accès ne doivent pas faire transiter les mots de passe originels ou définitifs en clair.

Facteurs de possession

- Proscrire la réception et l'envoi d'OTP par SMS au vu du risque de *SIM Swapping* et des vulnérabilités des protocoles SS7 permettant leur interception,
- Il est recommandé de faire usage d'un facteur de possession intégrant un composant de sécurité évalué, si ce n'est pas possible il faut privilégier l'utilisation d'un facteur de possession supportant la norme *FIDO 2* (authentification sans mot de passe).

Facteurs d’inhérence

- Les facteurs d'inhérence ne doivent pas être utilisés seuls mais accompagnés d'un facteur d'authentification fort.

Double facteurs et authentification forte

- Activer systématiquement l'authentification à deux facteurs (privilégier un facteur de possession) a minima pour les comptes de messageries, les gestionnaires de mots de passe et les comptes d'administration,
- Activer systématiquement l'authentification forte pour les comptes de traitement de données de santé, les comptes ayant des privilèges élevés comme ceux permettant d’administrer un système d’information,
- Fixer une date d'expiration sur les moyens d’authentification cryptographiques,
- Lors du parcours d'authentification, attendre que tous les facteurs aient été saisis/insérés avant de notifier un éventuel échec.

Tout facteur

- Activer une limite temporelle entre chaque tentative de connexion avant blocage temporaire ou définitif s'il y a un trop grand nombre d'essais infructueux quel que soit le facteur,

- Toute session authentifiée doit être limitée dans le temps, proportionnellement à la nature des données consultées.

Organisationnelles

- Chaque entreprise doit posséder une politique relative à la gestion et au cycle de vie de ses mots de passe, aussi appelée politique des mots de passe,
- Le responsable de traitements impliquant des mots de passe (CHAPITRE IV du RGPD) doit s'assurer au moins une fois par an du respect de cette politique par des solutions techniques et organisationnelles,
- Les utilisateurs doivent être sensibilisés aux menaces et aux risques de compromission de leurs mots de passe tout en étant formés à l'utilisation de leur coffre-fort,
- Un processus de révocation des facteurs d'authentification facile à utiliser doit être proposé aux utilisateurs finaux.