6 RÈGLES INCONTOURNABLES POUR UNE BONNE POLITIQUE DE SÉCURITÉ DES MOTS DE PASSE

ou *comment mieux sécuriser l'entreprise avec l'aide du service informatique*

01.

DÉFINISSEZ UNE POLITIQUE QUI SOIT FACILEMENT COMPRÉHENSIBLE

Établissez une politique de mot de passe documentée qui comprenne toutes les informations nécessaires telles que la longueur, la complexité ainsi que le nombre toléré de tentatives infructueuses concernant ces mots de passe.

02.

FAITES RESPECTER CETTE POLITIQUE AUPRÈS DE TOUS LES EMPLOYÉS

Tout le personnel est tenu de suivre les recommandations sur les mots de passe. Et cela concerne aussi les dirigeants et employés les plus haut placés.

03.

LISTE NOIRE DES "MAUVAIS" MOTS DE PASSE

Créez une liste noire des mots de passe les plus répandus et/ou les plus détournés et rejetez toute tentative d'utilisation de ceux-ci.

04.

STOCKAGE DES MOTS DE PASSE UTILISATEUR

Stockez les mots de passe utilisateur à l'aide de hachages salés et utilisez un algorithme de hachage spécifiquement conçu pour le stockage de mots de passe.

05.

NE MODIFIEZ PAS LES MOTS DE PASSE TROP SOUVENT

L'expiration périodique de mots de passe n'est plus une pratique de sécurité recommandée. Le National Institute of Standards and Technology (ou NIST), ainsi que le National Cyber Security Center (NCSC) du Royaume-Uni recommandent de ne modifier un mot de passe que si celui-ci semble compromis ou que si l'utilisateur en fait clairement la demande. Les utilisateurs, s'ils sont poussés à changer leurs mots de passe trop souvent, risquent de choisir des combinaisons plus simples et faciles à retenir.

06.

APPLIQUEZ VOTRE POLITIQUE SUR L'ENSEMBLE DE VOTRE RÉSEAU, IOT COMPRIS !

Votre politique de sécurité sur les mots de passe doit intégrer également tous les mots de passe associés à la protection de votre entreprise, notamment les appareils, les systèmes et particulièrement les objets intelligents connectés, tels que les caméras de sécurité, les routeurs et hubs intelligents. Si ceux-ci sont mal paramétrés ou que les informations d'identification sont laissées par défaut, les pirates risquent de plus en plus d'utiliser ces vulnérabilités pour accomplir des actes de cybermalveillance.

8 CONSEILS POUR CRÉER UN MOT DE PASSE ROBUSTE ET SÉCURISÉ

Ou *comment sensibiliser vos employés à choisir les bons mots de passe*

01.

VOTRE MOT DE PASSE DOIT ÊTRE UNIQUE !

Cela s'applique à l'ensemble de vos comptes, afin d'éviter de tous les compromettre si votre mot de passe venait à fuiter. Ce dernier ne devrait d'ailleurs jamais être écrit sur un post-it ou sur un fichier non crypté sauvegardé sur l'un des appareils de l'entreprise.

02.

PLUS VOTRE MOT DE PASSE EST LONG, MIEUX C'EST !

Le National Institute for Standards and Technology (NIST) des Etats-Unis recommande d'utiliser au moins 8 caractères, le minimum pour un niveau raisonnable de protection contre les attaques par force brute.

03.

ENCOURAGEZ L'UTILISATION DE PHRASES EN GUISE DE MOT DE PASSE

Une phrase avec 30 caractères ou plus est bien plus sécurisée qu'un mot de 8 caractères créé à l'aide de signes de substitution Les phrases sont au final un meilleur moyen de mémorisation et la longueur supplémentaire n'est en fin de compte, pas vraiment un motif de complication pour l'utilisateur.

04.

ELIMINEZ LES RÈGLES DE COMPOSITION TROP DIFFICILES

Demander aux utilisateurs d'inclure des caractères minuscules et majuscules, au moins 1 chiffre et 1 caractère spécial n'est pas idéal pour les encourager à créer des mots de passe robustes, et cela a d'ailleurs l'effet inverse : ils ont plutôt tendance à créer des combinaisons trop faibles et difficiles à mémoriser.

05.

NE PARTAGEZ PAS VOS MOTS DE PASSE !

Ne montrez jamais vos mots de passe à d'autres personnes, même vos collègues, vos responsables, votre famille ou au service informatique, d'autant que les cyberescrocs sont très forts pour se faire passer pour le support informatique !

06.

EVITEZ LES COMBINAISONS LES PLUS UTILISÉES

"XXXX" n'est pas un mot de passe robuste. Tout comme les caractères qui se suivent de type "1234" et les combinaisons faciles telles que "azerty" qui sont à oublier !

07.

N'UTILISEZ PAS DE MOTS COURANTS DU DICTIONNAIRE

Ceux-ci peuvent en effet être attaqués par force brute. Cela concerne aussi les langues étrangères et tous les termes spécialisés issus de différents domaines.

08.

N'UTILISEZ JAMAIS D'INFORMATIONS PERSONNELLES

Celles-ci peuvent être devinées par les cybercriminels en fonction des informations auxquelles ils peuvent avoir accès sur les réseaux sociaux. Cela inclut les noms, dates d'anniversaire, adresses, écoles, noms des conjoints ou des enfants.