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.