Rééquipement informatique

Nouvelle stratégie de mot de passe + Note aux utilisateurs

ASSURMER

Montpellier, Occitanie, France

Kévin Boulier, Ezequiel-Junior Varela Montieiro, Maxence Martin-Parent / SISR 1B

Table des matières

Introduction

Dans le cadre de notre renouvellement du parc informatique, la DSI a pris la décision de modifier la stratégie de mot de passe de l'entreprise.
D'autant plus importante au vu de notre future mission de partenaire officiel des JO de Paris 2024, nous avons décidé d'établir une stratégie en accord avec les dernières recommandations en date de la CNIL.

En fin de ce document sera présent la note utilisateurs qui leur sera transmise le jour de mise en place de leur PC portable.

Explication de la stratégie

Devinabilité, entropie…

Les dernières recommandations de la CNIL en termes de mot de passe date du 14 octobre 2022.

Celle-ci, sur son site internet[1], détaille sa nouvelle façon de déterminer si un mot de passe est sécurisé ou non : l'entropie.

D'après la définition de la CNIL, l'entropie est la « quantité de hasard ». Pour un mot de passe, c'est sa capacité à résister à une attaque brute force[2]. L'entropie en elle-même est considérée pour un mot de passe généré aléatoirement, donc l'entropie sera forcément plus faible.

Les phrases de passe étant menacées par les attaques dites par dictionnaire, leur entropie sera donc plus faible. C'est pour cela que la CNIL indique que les phrases de passe doivent au minimum contenir 7 mots, pour augmenter considérablement l'entropie.

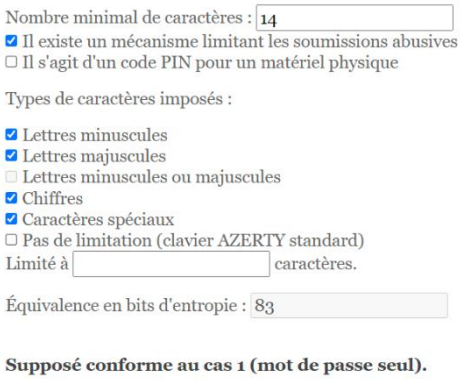
Ainsi, la CNIL indique que le niveau minimal d'entropie doit se situer à 80 bits d'entropie, pour une authentification permise par un mot de passe seul. Etant notre situation, nous devons donc utiliser une stratégie correspondant à 80 bits ou plus d'entropie.

	EXEMPLE D'UTILISATION	ENTROPIE MINIMUM	MESURES COMPLÉMENTAIRES
MOT DE PASSE SEUL	FORUM, BLOG	80	Conseiller l'utilisateur sur un bon mot de passe
AVEC RESTRICTION D'ACCÈS (LE PLUS RÉPANDU)	SITES DE E-COMMERCE, COMPTE D'ENTREPRISE, WEBMAIL	50	Mécanisme de restriction d'accès au compte : (exemples) Temporisation d'accès au compte après plusieurs échecs ; Nombre maximal de tentatives autorisées dans un délai donné ; "Captcha" ; Blocage du compte après 10 échecs assorti d'un mécanisme de déblocage choisi en fonction des risques d'usurpation d'identité et d'attaque ciblé par déni de service.
AVEC MATÉRIEL DÉTENU PAR LA PERSONNE	CARTE BANCAIRE OU TÉLÉPHONE	13	Matériel détenu en propre par la personne (ex: carte SIM, carte bancaire, certificat) + Blocage au bout de 3 tentatives échouées

Extrait du site de la CNIL sur l'entropie

[1] https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite
[2] Brute force = par force brute, c'est-à-dire essayer un énorme nombre de mot de passe à la suite.

La CNIL propose sur son site un simulateur[3] permettant de déterminer si la stratégie de mot de passe dispose bien d'assez de bits d'entropie.


Nombre minimal de caractères : 14
Il existe un mécanisme limitant les soumissions abusives
Il s'agit d'un code PIN pour un matériel physique

Types de caractères imposés :

Lettres minuscules
Lettres majuscules
Lettres minuscules ou majuscules
Chiffres
Caractères spéciaux
Pas de limitation (clavier AZERTY standard)
Limité à caractères.

Équivalence en bits d'entropie : 83

Supposé conforme au cas 1 (mot de passe seul).

Extrait du simulateur de la CNIL

Concernant la devinabilité, la CNIL ne dispose pas encore des informations nécessaires ainsi que des méthodes de vérification permettant d'établir des critères précis concernant la devinabilité. Il est bien indiqué que la CNIL ajoutera bien la devinabilité à ses critères dans un futur proche, et donc nous nous tiendrons informé pour mettre à jour la stratégie de mot de passe le temps venu. Mais nous avons commencé à faire un pas vers ce principe, en limitant les suites de plus de 3 chiffres qui se suivent.

De plus, en accord avec la loi RGPD, nous comptons restreindre l'utilisation de la biométrie sur nos ordinateurs. C'est pour cela que la stratégie a été intensifiée pour permettre la seule utilisation d'un mot de passe.

Les conditions à respecter **obligatoirement** sont :

- 14 caractères minimum.
- Doit contenir au minimum :
    - 1 majuscule et 1 minuscule et 1 chiffre et 1 caractère spécial.
    - Votre nom/prénom **NE DOIT PAS** figurer dans votre mot de passe
    - Le nom de l'entreprise **NE DOIT PAS** figurer dans le mot de passe
    - Un produit vendu par ASSURMER **NE DOIT PAS** figurer dans le mot de passe
    - Ne doit pas contenir de suite de chiffre de plus de 3.
- En cas de phrase de passe, celle-ci doit contenir plus de 7 mots.

De plus, les comptes seront bloqués après 5 essais, et les mots de passe devront être remis à 0 tous les 90 jours.

Ci-joint, à la suite, la note utilisateurs qui sera distribuée aux collaborateurs.

[3] https://www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe

NOTE UTILISATEURS

Nouvelle stratégie de mot de passe ASSURMER – 2024

Dans le cadre de notre renouvellement du parc informatique, et d'un besoin de sécurité grandissant concernant notre partenariat avec les JO de Paris 2024, la Direction des Systèmes d'Information d'ASSURMER vous présente ici les nouvelles directives de mot de passe, applicables **dès réception de votre nouvelle machine**.

Conditions à respecter **obligatoirement** :

- 14 caractères minimum.
- Doit contenir au minimum :
  - 1 majuscule et 1 minuscule et 1 chiffre et 1 caractère spécial.
- Votre nom/prénom **NE DOIT PAS** figurer dans votre mot de passe
- Le nom de l'entreprise **NE DOIT PAS** figurer dans le mot de passe
- Un produit vendu par ASSURMER **NE DOIT PAS** figurer dans le mot de passe
- **NE DOIT PAS** contenir de suite de chiffre de plus de 3.
- En cas de phrase de passe, celle-ci doit contenir plus de 7 mots.

Recommandations :

Les phrases de passe sont autorisées, et sont plus faciles à retenir.
Elles doivent tout de même respecter les conditions de mot de passe ci-dessus.
Les mots de votre phrase de passe devraient être séparées (par des tirets, des tirets bas, des slashs, etc… pour faciliter sa mémorisation.

Autres informations à retenir :

Votre accès aux PC et aux comptes sera bloqué si vous entrez 5 fois un mot de passe erroné.
Le mot de passe devra être changé à un intervalle de 90 jours.
Nous vous recommandons l'utilisation d'un gestionnaire de mot de passe, pour le stocker en cas de besoin.