VEILLE TECHNOLOGIQUE

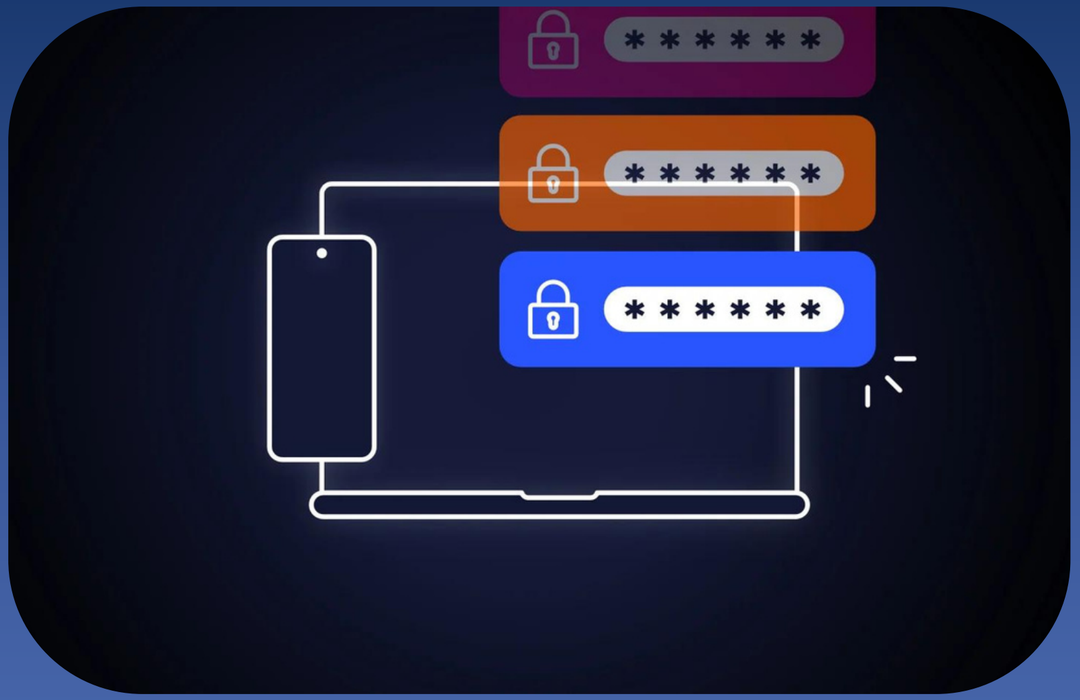
GESTIONNAIRE DE MOTS DE PASSE

ARKI CLÉMENT

SOMMAIRE

1. INTRODUCTION

- Comprendre la technologie des gestionnaires de mots de passe, c’est-à-dire tout ce qui concerne la sécurité et la gestion des identifiants.
- Le but de cette veille est de développer des compétences pratiques en matière de sécurité informatique et de gestion des identifiants pour mon cursus de formation.
- Dans le cadre de ma veille technologique, je me penche sur les gestionnaires de mots de passe pour les entreprises et les particuliers.



2. QU’EST-CE QU’UN GESTIONNAIRE DE MOTS DE PASSE ?

- Logiciel (basé sur le bureau) ou un service en ligne (qui est intégré dans le navigateur ou basé sur le cloud) qui sert à sécuriser, gérer et stocker les mots de passe d’un utilisateur ou d’une entreprise en centralisant l’ensemble de ses identifiants et mots de passe (dans un même endroit) dans une base de données appelée portefeuille.
- Sécurisé par un mot de passe unique, appelé « mot de passe maître ».
- Trois catégories de gestionnaires : basé sur le cloud, intégré au navigateur, basé sur le bureau.
- Authentification à double facteur (2FA) et multifacteur (MFA).
- Mot de passe stockés sont chiffrés à l'aide d'algorithmes de chiffrement (Advanced Encryption en anglais ou AES)
- AES : Algorithmes de chiffrement symétrique : une clé secrète est utilisée pour chiffrer et déchiffrer les informations.

- À pour objectif principal de sécuriser et protéger les données sensible, notamment les mots de passe et les identifiants, afin de les préserver contre tout accès non autorisé ou toute fuite éventuelle.

3. ÉTUDE DE MARCHÉ : QUI SONT LES OFFREURS DE CET OUTIL ?

- Ceux qui offrent les gestionnaires de mots de passe sont les entreprises ou les développeurs de logiciels qui fournissent cet outil de gestion des mots de passe.
- Il existe des gestionnaires de mots de passe gratuits ainsi que des versions payantes.

- Les 7 meilleurs gestionnaires de mots de passe en janvier 2024 sont NordPass, Dashlane, 1password, Bitwarden, RoboForm, Enpass et LastPass.
- Chacune de ces solutions à ses propres fonctionnalités et approches.

- La taille du marché des gestionnaires de mots de passe est de 2,09 milliards USD en 2023 et devrait passer à 7,33 milliards USD d'ici 2028 (taux de croissance annuel de 28,52% au cours de la période de prévision 2023-2028).

4. ÉTUDE DE MARCHÉ : QUI SONT LES DEMANDEURS DE CET OUTIL ?

- Les demandeurs de gestionnaires de mots de passe incluent à la fois des utilisateurs individuels tels que les étudiants, les familles et les particuliers, ainsi que des organisations comme les entreprises.

- Lors du choix d'un gestionnaire de mots de passe, les demandeurs accordent une attention particulière aux prix, que ce soit à des fins personnelles ou organisationnelles. Il existe des versions gratuites.

- Selon une enquête du Centre National de Cybersécurité (NCSC) :
- 65 % des utilisateurs n'utilisent pas de gestionnaires de mots de passe en raison du manque de confiance.
- 34 % craignent que leur gestionnaire de mots de passe ne soit piraté.
- 30,5 % ne font pas confiance aux sociétés de gestion de mots de passe pour leurs information (Exemple : une information donnée ne doit être ni modifiée ni divulguée).

5. ENVIRONNEMENT JURIDIQUE (RGPD, CNIL, SÉCURITÉ...)

- Dans le cadre du Règlement Général sur la Protection des Données (RGPD), recommandations en termes de mots de passe : utiliser des mots de passe forts et unique (minuscules, majuscules, chiffres, caractères spéciaux et une longueur de 12 caractères), de ne pas partager vos mots de passe et changer régulièrement vos mots de passe (3 à 4 mois).

- La CNIL recommande d'activer l'authentification multifacteur chaque fois qu'elle est disponible pour renforcer la sécurité.

- L'environnement juridique du gestionnaire de mot de passe est encadré par le RGPD et la CNIL qui font des recommandations pour renforcer la sécurité des données (ex : mot de passe)

6. ANALYSE DE LA TECHNOLOGIE : AVANTAGES ET INCONVÉNIENTS

AVANTAGES

Sécurité

Stockage sécurisé et crypté des mots de passe, génération de mots de passe forts et uniques.

Confort

Plus besoin de mémoriser tous les mots de passe, génération de mots de passe fort.

Simplicité

Les gestionnaires de mots de passe peuvent remplir automatiquement les champs de connexion, ce qui permet de gagner du temps et aussi de la productivité.

2FA

Authentification à deux facteurs pour une meilleure sécurité.

Organisation

Garder une trace de tous les comptes en ligne et à les organiser en catégories pour faciliter la recherche et la gestion.

INCONVÉNIENTS

Vulnérabilités du logiciel

Possibilité de vulnérabilités dans le logiciel des gestionnaires de mots de passe.

Phishing

Risque de tomber dans des pièges de phishing et de divulguer le mot de passe principal.

Attaques

Si le mot de passe principal est faible, les pirates peuvent utiliser des attaques de force brute pour tenter de deviner le mot de passe.

2FA

Peut être contraignant pour certains utilisateurs.

Vol de données

Si les données stockées par le gestionnaire de mots de passe sont compromises, tous les mots de passe stockés peuvent être révélés.

7. RISQUES D’UN GESTIONNAIRE DE MOTS DE PASSE

L'utilisation d'un gestionnaire de mots de passe peut considérablement diminuer les chances d'être victime de piratage en ligne, mais il existe des risques à prendre en compte.

Les principaux risques sont :

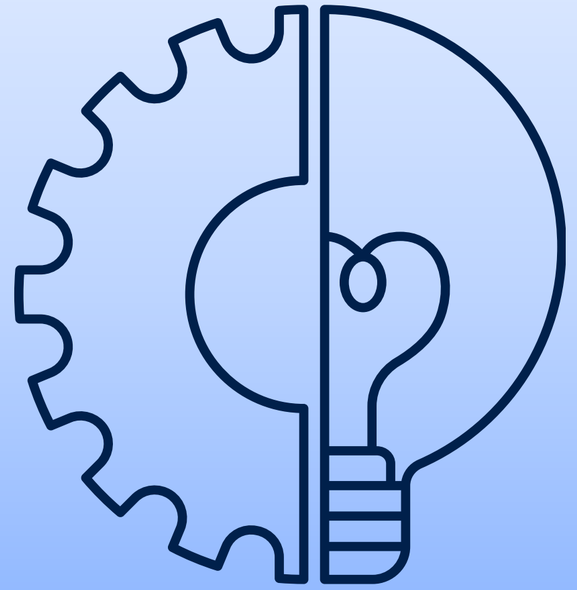
- Toutes les données sensibles se trouve en un seul endroit
- La sauvegarde n’est pas toujours possible
- Tous les appareils ne sont pas suffisamment sûrs
- Un mauvais gestionnaire de mots de passe
- Oubli du mot de passe principal

En respectant le RGPD, il est important de ne pas partager vos mots de passe, car cela affaiblit la sécurité, ce qui va à l'encontre des règles de protection des données. Cela comporte donc un risque.

8. LE FUTUR DU GESTIONNAIRE DE MOTS DE PASSE

Authentification multifacteur améliorée

- L'authentification à deux facteurs (2FA) voire multifacteur (MFA) pourrait devenir plus courante avec le temps (surtout dans les entreprises). Elle combinera plusieurs méthodes d'authentification variées au niveau des évolutions comme la notifications push des appareils mobiles, la biométrie (reconnaissance faciale et lecture des empreintes digitales), la reconnaissance vocale, les codes par SMS, les mots de passe à usage unique et le courriel offrant ainsi une sécurité renforcée lors de la vérification de l'identité de l'utilisateur.



Intelligence artificielle

- L'IA pourrait être en mesure de détecter et de réagir instantanément aux menaces émergentes et d'analyser le comportement de l'utilisateur (afin d'éviter les usurpations d'identités etc.).
- De nouvelles méthodes peuvent identifier les utilisateurs en prenant en compte la façon dont ils tapent sur un clavier, leur vitesse de frappe et le nombre et le type d'erreurs commises. Cela renforcerait l'authentification et offrirait une sécurité plus robuste tout en simplifiant davantage les gestionnaires de mots de passe.

9. MON OPINION PERSONNELLE

- Je suis pour l’utilisation des gestionnaires de mots de passe car c’est un :
  - Outil qui offre de nombreux avantages : génération de mots de passe forts et uniques, une adoption de l'authentification multifacteur pour renforcer la sécurité.
  - Logiciel utile, devenu incontournable pour le cloud, l’intégration au navigateur et basé sur le bureau (ordinateur personnel).
  - Outil essentiel à l'ère numérique pour répondre aux exigences du RGPD et de la CNIL : meilleure protection.

- Cependant, si l’on connait le mot de passe principal « maître », on connaîtra tous les mots de passe qui se trouve dans cet outil.
- Le gestionnaire de mots de passe peut être amélioré à l’avenir grâce à l’IA et de l’augmentation de l’utilisation de l'authentification multifacteur pour renforcer la sécurité des gestionnaires de mots de passe.

MERCI POUR VOTRE ATTENTION