Clément Arki

BTS SIO 2ème année

Veille technologique : Gestionnaire de mots de passe

Sommaire :

Introduction :

J'ai choisi les gestionnaires de mots de passe comme sujet de veille technologique car c'est un outil intéressant à étudier, à la fois du point de vue technique et en termes d'utilité pratique. Mon intérêt est de comprendre la technologie des gestionnaires de mots de passe, c’est-à-dire tout ce qui concerne la sécurité et la gestion des identifiants.

Il est pertinent d’étudier les gestionnaires de mots de passe dans mon cursus de formation pour ensuite comprendre leur fonctionnement technique. Cela permet de développer des compétences pratiques en matière de sécurité informatique et de gestion des identifiants.

Les outils de collecte que j'ai utilisés pour rassembler des informations pertinentes et à jour sur ce sujet incluent des newsletters provenant de sites tels que developpez.com, l'utilisation de l’outil Google Alerts, ainsi que des recherches effectuées sur internet.

I. Aspect technique du gestionnaire de mots de passe

1. Qu’est-ce qu’un gestionnaire de mots de passe et à quoi cela sert ?

Un gestionnaire de mots de passe est un logiciel ou un service en ligne permettant à un utilisateur de gérer ses mots de passe en centralisant l’ensemble de ses identifiants et mots de passe dans une base de données appelée portefeuille. Le gestionnaire de mots de passe est sécurisé par un mot de passe unique, appelé « mot de passe maître », dont l’utilisateur doit se rappeler afin de n’en avoir plus qu’un seul à retenir.

Un gestionnaire de mots de passe sert à constituer un moyen de sécuriser, de gérer et de stocker les mots de passe d’un utilisateur ou d’une entreprise.

Il existe des gestionnaires de mots de passe gratuits tels que KeePass et Password Safe, ainsi que des options payantes comme 1Password, LastPass Premium et NordPass (qui peut également être gratuite). Le choix d'un gestionnaire de mots de passe peut être influencé par des facteurs liés au coût, à la fois au niveau financier et économique, surtout lorsqu'on choisit une version payante.

2. Le fonctionnement d’un gestionnaire de mots de passe

Cet outil fonctionne avec des coffres-forts numériques pour nos données personnelles d’authentification. Quand on crée notre compte, on crée un maître mot de passe pour accéder au gestionnaire. Tous les autres mots de passe dans ce coffre-fort sont cryptés dont notre maître mot de passe qui en est la clé de chiffrement. La robustesse de la sécurité du gestionnaire de mots passe repose sur la résistance de notre mot de passe principal, qui doit être très difficile à deviner et qu’on doit mettre à jour régulièrement (tous les 3 mois environs).

Aussi, certains coffres-forts peuvent générer automatiquement ou manuellement (si on le souhaite) des mots de passe uniques, forts et sécurisés pour protéger ainsi les applications.

Les mots de passe, pour être mieux protégés, sont les lettres majuscules, les minuscules, les chiffres, les caractères spéciaux et la longueur (supérieur ou égale à 12 caractères).

Sur le marché, il y a différents types de gestionnaires de mots de passe qui sont disponibles, chacun ayant sa propre méthode de mise en place. Voici les 3 catégories de gestionnaires qui existent :

- **Basé sur le cloud :** Cela rend possible le stockage à distance. Les données ne se trouvent pas dans l'entreprise, mais dans le cloud. Son niveau de sécurité est élevé (comme NordPass ou LastPass).
- **Intégrés au navigateur :** Il permet une connexion automatique sans besoin d'installation spécifique (comme Chrome, Firefox ou Safari). Mais en entreprise, il est généralement déconseillé pour des raisons de sécurité. Il a un niveau de sécurité acceptable.
- **Basé sur le bureau (ordinateur personnel) :** Le gestionnaire est utilisé par un seul utilisateur et accessible depuis un seul appareil (comme 1Password, BitWarden, Dashlane). Son niveau de sécurité est le plus élevé.

3. La sécurité des données dans un gestionnaire de mots de passe et le stockage des informations

La sécurité dans un gestionnaire de mots de passe peut être abordée de deux façons principales. D'abord, il y a l'authentification simple, où la sécurité dépend uniquement d'un mot de passe. En plus du gestionnaire de mots de passe, il existe une méthode plus avancée appelée l'authentification à double facteur. On trouve parfois désigné par le sigle « 2FA » (en anglais « 2-factor authentication »). Avec celle-ci, vous entrez d'abord votre nom d'utilisateur et votre mot de passe, puis vous devez fournir un deuxième élément d'authentification, comme un code envoyé par SMS, e-mail, téléphone ou généré par une application de validation installée sur votre appareil ou sur votre téléphone (Google Authenticator par exemple).
L'authentification à deux facteur (2FA) et l'authentification multifacteur (MFA) (désigné par le sigle « Multifactor Authentication » en anglais) souvent considérées comme la même chose. L'authentification multifacteur est une méthode de sécurité plus avancée qui combine plusieurs méthodes pour authentifier une connexion. Cela renforce encore davantage la sécurité en ajoutant une couche supplémentaire de protection.

De plus, en matière de sécurité, il est important de noter que les mots de passe stockés dans le gestionnaire sont chiffrés à l'aide d'algorithmes de chiffrement. Les algorithmes de chiffrement les plus couramment utilisés incluent l'Advanced Encryption Standard (AES), qui est largement répandu dans de nombreux logiciels tels que LastPass, KeePass, etc., ainsi que Twofish. Ce sont des algorithmes de chiffrement symétrique, ce qui signifie qu'une clé secrète est utilisée à la fois pour chiffrer et déchiffrer les informations.

Les gestionnaires de mots de passe sont donc mis en avant en raison de la préoccupation croissante pour la sécurité en ligne et de la sensibilisation des utilisateurs.

Enfin, le stockage des informations dans un gestionnaire de mots de passe a pour objectif principal de sécuriser et de protéger les données sensibles, notamment les mots de passe et les identifiants, afin de les préserver contre tout accès non autorisé ou toute fuite éventuelle (faille de sécurité, erreur humaine ou encore mauvaise configuration).

II. Étude du Marché des Gestionnaires de mots de passe

1. Qui sont les offreurs de cet outil ?

Les offreurs de gestionnaires de mots de passe sont les entreprises ou les développeurs de logiciels qui fournissent cet outil de gestion des mots de passe. Voici une liste des 7 meilleurs gestionnaires de mots de passe en janvier 2024, avec ses particularités :

- **NordPass** : Disponible sur les principales plateformes, haut niveau de sécurité, importation des mots de passe, chiffrement moderne (XChaCha20), c'est-à-dire chiffrement symétrique et version gratuite ou payante.
- **Dashlane :** Un nombre illimité de mots de passe, changement de mots de passe automatique avec certains sites, possibilité d'avoir une personne en cas de problème et version gratuite ou payante.
- **1Password :** Alertes failles de sécurité en temps réel, raccourcis clavier pratique mais version payante avec un période d'essai gratuite de 14 jours. Il offre une sécurité pour tous, qu'il s'agisse de particuliers, d'entreprises ou de développeurs.
- **Bitwarden :** Hébergement sur un NAS (Netword Attached Storage), c'est-à-dire un appareil de stockage autonome qui se connecte sur un réseau et version gratuite ou payante
- **RoboForm :** Stockage illimité de mots de passe, support technique par e-mail / téléphone, possibilité de créer un contact d'urgence (payant) et version gratuite ou payante.
- **Enpass :** Simple à utiliser, synchronisation des données par Wi-Fi et version gratuite ou payante.
- **LastPass :** Surveillance du « dark web », changement automatique des mots de passe, application et site web en français et version gratuite ou payante.

Chacune de ces solutions à ses propres fonctionnalités et approches. Les offreurs sont en concurrence pour attirer les utilisateurs vers leurs solutions de gestion de mots de passe.

Certains gestionnaires de mots de passe, comme NordPass et 1Password, sont disponibles en versions basées sur le cloud et aussi sur bureau. De plus, il y a également des gestionnaires de mots de passe intégrés au navigateur, comme celui de Google Chrome, géré par Google lui-même, et qui fonctionnent directement dans le navigateur. Tous ces exemples sont des fournisseurs (offreurs) de gestionnaires de mots de passe.

Enfin, la taille du marché des gestionnaires de mots de passe, à 2,09 milliards USD en 2023, 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).

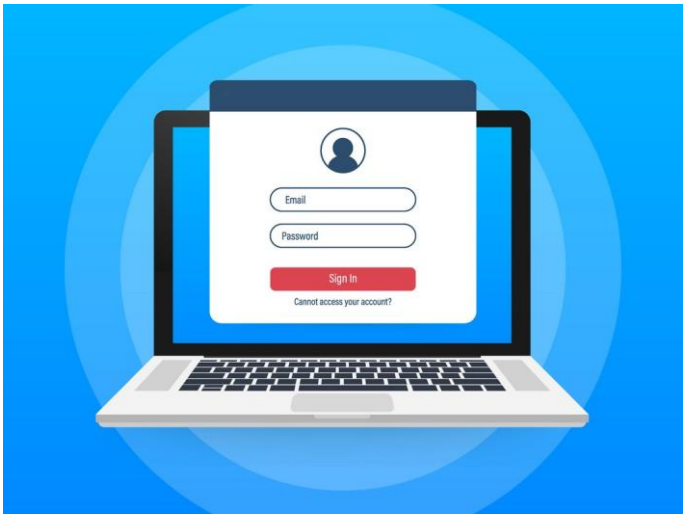
2. Qui sont les demandeurs de cet outil ?

Les demandeurs de gestionnaires de mots de passe sont à la fois les utilisateurs individuels tels que les étudiants, les familles et les particuliers, ainsi que les organisations comme les entreprises avec des coffres-forts partageables et des gestions d'accès sur-mesure.

Lors du choix d'un gestionnaire de mots de passe, les demandeurs considèrent fréquemment les prix, que ce soit à des fins personnelles ou au niveau de l'organisation. Bien que de nombreux logiciels de gestion de mots de passe soient payants et souvent plus performants que les versions gratuites, le budget peut varier d'un utilisateur ou d'une organisation à l'autre.

Mais d'après un article du 2 février 2023, selon une enquête, 65 % des utilisateurs n'utilisent pas de gestionnaires de mots de passe en raison du manque de confiance. 34 % des personne interrogées craignent que leur gestionnaire de mots de passe ne soit piraté et 30,5 % ne font pas confiance aux sociétés de gestion de mots de passe pour leurs informations.

(Exemple : une information donnée ne doit être ni modifiée ni divulguée)



3. Environnement juridique (RGPD, CNIL, sécurité…)

Pour l'environnement juridique, les recommandations en termes de mots de passe dans le cadre du Règlement Général sur la Protection des Données (RGPD) sont d'utiliser des mots de passe forts et unique, de ne pas partager nos mots de passe si vous faites confiance aux personne concernées et de changer régulièrement nos mots de passe.

De plus, la CNIL (Commission nationale de l'informatique et des libertés) qui est un organisme français chargé de la protection des données personnelles et de la vie privée, veille au respect du RGPD (Règlement général sur la protection des données). Aussi, la CNIL recommande d'activer l'authentification multifacteur chaque fois qu'elle est disponible sur un service (comme le gestionnaire de mots de passe) pour renforcer la sécurité.

III. Analyse de la technologie

1. Avantages et inconvénients (tableau comparatif)

Avantages des gestionnaires de mots de passe	Inconvénients des gestionnaires de mots de passe
Sécurité : Stockage sécurisé et crypté des mots de passe, génération de mots de passe forts et uniques.	**Vulnérabilités de logiciel** : Possibilité de vulnérabilités dans le logiciel des gestionnaires de mots de passe.
Confort : Plus besoin de mémoriser tous les mots de passe, génération de mots de passe fort.	**Attaques de phishing** : Risque de tomber dans des pièges de phishing et de divulguer le mot de passe principal.
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.	**Attaques de force brute :** 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.
Accessibilité : Accès depuis n'importe quel appareil.	**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.
2FA : Authentification à deux facteurs pour une meilleure sécurité.	Peut-être contraignant pour certains utilisateurs.
Organisation : Les gestionnaires de mots de passe peuvent aider à garder une trace de tous les comptes en ligne et à les organiser en catégories pour faciliter la recherche et la gestion.	

2. 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 :** En cas de violation, les pirates peuvent accéder à tous les comptes.
- **La sauvegarde n'est pas toujours possible :** Si le gestionnaire de mots de passe basé sur le cloud connaît des problèmes, vous ne pourrez récupérer vos données que si le fournisseur a sauvegardé vos informations. Cependant, certains gestionnaires de mots de passe, comme NordPass et 1Password, gardent des copies de sécurité pour éviter tout souci en cas de problème avec leurs serveurs (dans un serveur sécurisé).
- **Tous les appareils ne sont pas suffisamment sûrs :** En cas d'infection par un logiciel malveillant, il faut utiliser un antivirus fiable pour sécuriser l'appareil et réduire les risques.
- **Un mauvais gestionnaire de mots de passe :** Certains gestionnaires de mots de passe gratuits ont un cryptage plus faible et moins de fonctionnalités de sécurité pour protéger les informations d'identification par rapport aux solutions payantes.
- **Oubli du mot de passe principal** : Si on oublie le mot de passe principal « mot de passe maître », il faut garder cela dans une note sécurisée du mot de passe principales (comme sur un document papier ou un fichier crypté).

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.

3. Evolution de l'outil

L'évolution des gestionnaires de mots de passe se manifeste de différentes manières. Tout d'abord, l'authentification à deux facteurs (2FA) pourrait devenir plus courante avec le temps. Cette authentification multifacteur (MFA) intègrera plusieurs méthodes variées au niveau des évolutions comme les notifications push des appareils mobiles pour les applications d'authentification iOS et Android, la biométrie (reconnaissance faciale et lecture des empreintes digitales), la reconnaissance vocale, les codes par SMS ou par une application (Google Authenticator), 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.

Également, l'IA peut exercer un rôle croissant dans l'amélioration des gestionnaires de mots de passe. En effet, 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.). Par exemple, 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.

Conclusion :

Je suis pour l'utilisation des gestionnaires de mots de passe car c'est un outil qui offre de nombreux avantages tels que la génération de mots de passe forts et uniques et l'adoption de l'authentification multifacteur pour renforcer la sécurité qui sont donc des évolutions techniques pour les gestionnaires de mots de passe. C'est un logiciel utile et qui est devenu incontournable pour le cloud, l'intégration au navigateur et basé sur le bureau (ordinateur personnel). Les gestionnaires de mots de passe sont devenus essentiels à l'ère numérique pour répondre aux exigences du RGPD et de la CNIL, et ils contribuent à une meilleure protection. De plus, il existe des logiciels couramment utilisés pour les gestionnaires de mots de passe, comme NordPass et 1Password, chacun apportant ses caractéristiques distinctes. Cependant, même si le gestionnaire permet de centraliser les mots de passe, 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 donc être amélioré notamment avec l'augmentation de l'utilisation de l'authentification multifacteur. L'IA peut également jouer un rôle dans cette amélioration en renforçant la sécurité des gestionnaires de mots de passe.

Sources :

Source Grand I petit 1 :

https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/pourquoi-et-comment-utiliser-un

10 août 2022

https://fr.wikipedia.org/wiki/Gestionnaire_de_mots_de_passe

2 août 2023

Source Grand I petit 2 :

https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/pourquoi-et-comment-utiliser-un

10 août 2022

https://www.onelogin.com/fr-fr/learn/password-vaulting

https://www.lebigdata.fr/gestionnaire-mots-de-passe-tout-savoir-2.

20 juillet 2023

Source Grand I petit 3 :

https://www.cnil.fr/fr/securite-utilisez-lauthentification-multifacteur-pour-vos-comptes-en-ligne

01 décembre 2021

https://www.cnil.fr/fr/mots-de-passe-une-nouvelle-recommandation-pour-maitriser-sa-securite

Sources Grand II petit 1 :

https://www.bfmtv.com/comparateur/meilleurs-gestionnaires-de-mots-de-passe-test-comparatif/

3 septembre 2023

https://fr.cybernews.com/lp/meilleurs-gestionnaires-mots-passe

Septembre 2023

https://1password.com/fr

https://www.clubic.com/application-web/article-854952-1-gestionnaires-mots-meilleur-logiciel-gratuit-windows.html

https://www.mordorintelligence.com/fr/industry-reports/password-management-market

2 janvier 2024

Sources Grand II petit 2:

https://www.blogdumoderateur.com/tools/productivite/gestionnaire-mots-de-passe/

https://securite.developpez.com/actu/341110/Gestionnaire-de-mots-de-passe-KeePass-conteste-une-vulnerabilite-permettant-le-vol-de-mots-de-passe-et-identifiee-par-la-CVE-2023-24055/

Sources Grand II petit 3:

https://www.hop3team.com/mot-de-passe-rgpd/#:~:text=Il%20est%20recommand%C3%A9%20de%20ne,est%20une%20faiblesse%20de%20s%C3%A9curit%C3%A9

11 janvier 2023

2 février 2023

Source Grand III petit 1 :

https://bluebearsit.com/pourquoi-utiliser-un-gestionnaire-de-mots-de-passe/

10 Mars 2023

Sources Grand III petit 2 :

https://www.webblog.tophebergeur.com/les-gestionnaires-de-mot-de-passe-sont-ils-tous-surs.html

27 Mars 2023

https://www.hop3team.com/mot-de-passe-rgpd/

11 janvier 2023

Sources Grand III petit 3 :

https://www.lastpass.com/fr/products/multifactor-authentication

https://www.dashlane.com/blog/fr/le-guide-de-double-authentification-du-debutant

2 novembre 2022

https://www.ipe.fr/comment-lia-ameliore-la-cybersecurite/

3 juillet 2020

https://www.01net.com/actualites/cette-ia-ecoute-les-claviers-pour-voler-les-mots-de-passe.html