FAMILLES DE PRODUITS

Gestionnaire de mots de passe

Le volet cyber de France Relance

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est en charge du volet cybersécurité de France Relance pour concevoir des offres de service destinées à **élever le niveau de cybersécurité de l'État, des collectivités territoriales et des organismes au service des citoyens** (social, santé, formation, audiovisuel, sécurité).

Les appels à projets, l'une des réponses de l'ANSSI au volet cyber de France Relance

Différentes solutions ont déjà été identifiées par l'ANSSI comme pouvant faire l'objet d'un projet d'acquisition dans le cadre du plan France Relance :

Analyse de risque EBIOS Risk Manager	Bug Bounty	Endpoint Detection and Response	Gestionnaire de vulnérabilités	Gestion des accès à privilèges (PAM)
Pare-feu applicatif web (WAF)	Sauvegarde sécurisée	Sécurisation de l'Active Directory	Sécurisation de la messagerie email	**Gestionnaire de mots de passe**

Le gestionnaire de mots de passe

6 minutes

suffisent à un hacker pour pirater un mot de passe de 7 caractères comprenant chiffres, majuscules, minuscules et symboles (*)

Qu'est-ce qu'un gestionnaire de mots de passe ?

Le gestionnaire de mots de passe est un outil permettant de stocker et gérer de manière sécurisée un ensemble de mots de passe. L'utilisateur aura un unique mot de passe robuste à retenir pour accéder à l'ensemble de ses mots de passe stockés dans une base chiffrée.

D'autre part, le gestionnaire peut générer aléatoirement des mots de passe, respectant une longueur et une complexité minimales, et empêcher leur réutilisation pour d'autres comptes ou services.

La gestion des mots de passe partagés est également simplifiée, tout en garantissant un contrôle d'accès approprié et une authentification sécurisée.

(*) https://howsecureismypassword.net/

Pourquoi cette famille de solution ?

- **Intégration rapide** de la solution.
- Solution adaptée pour une organisation **de maturité basique.**
- Un gestionnaire de mots de passe correctement exploité et largement déployé au sein d'une organisation apporte **un bénéfice sécurité élevé.**
- **Une mauvaise gestion des mots de passe (mots de passe faibles, réutilisés, volés) est la première cause de piratage.**
- **L'outil simplifie la gestion des mots de passe** pour un utilisateur, tout en **limitant les mauvaises pratiques.**

Menaces couvertes

Compromission du SI
(éléments secrets compromis)

Périmètre

Identifiants, mots de passe, clefs

Maturité sécurité attendue pour la solution

BASIQUE → Importante → Avancée → Spécifique

Déploiement (1/2)

1. Déployer un coffre-fort localement sur chaque poste utilisateur
   Déployer un serveur centralisé en mode On-premise
   Ouvrir un tenant SaaS sur le Cloud (public ou privé)
2. Configurer les méthodes d'accès utilisateur (client léger, extension web, application mobile, etc.)
3. Configurer les accès (droits, accès aux mots de passe partagés) et les mécanismes d'authentification sécurisés (MFA, politique de mot de passe, etc.)
4. Sensibiliser et former les utilisateurs à l'outil et aux bonnes pratiques associées

Déploiement (2/2)

Phase de BUILD

- **Équipe d'intégration** nécessaire pour l'installation des composants logiciels
- **Équipe d'intégration** nécessaire pour former les utilisateurs à l'outil

Complexité : faible

Phase de RUN

- **Administrateur de la console** pour la configuration des mécanismes cryptographiques et d'authentification, et les interconnexions avec d'autres services (annuaires, etc.)
- **Administrateur de la console** pour la gestion des utilisateurs, des informations partagées et des droits d'accès
- **Administrateur système** pour le maintien en condition opérationnelle de l'outil

Complexité : moyenne

Recommandations d'usage

- **Sensibiliser l'ensemble des utilisateurs** aux risques liés à un usage incorrect des mots de passe.
- **Former les utilisateurs** à l'usage de l'outil et, si besoin, rendre cet usage systématique.
- Inscrire les modes d'usage sécurisé des éléments secrets dans **une charte de bon usage** du SI communiquée aux salariés.
- **Appliquer les bonnes pratiques liées à l'administration de l'outil** (authentification sécurisée à cet outil, mécanismes cryptographiques sécurisés, partage de mots de passe, contrôle d'accès sur les comptes partagés).
- Le mot de passe maître d'un utilisateur lui permettant d'accéder à sa base de mot de passe **doit être robuste**.
- En utilisant un service Cloud, le bénéficiaire n'est plus le seul responsable de la sécurité des mots de passe des utilisateurs. Ainsi, **un incident chez l'hébergeur cloud pourrait entrainer une fuite de données (ici des mots de passe).** Dans le cadre d'un service cloud, il est donc nécessaire de contractualiser avec un hébergeur de confiance (ex : qualification SecNumCloud).

Complémentarité avec d'autres outils

Comment optimiser l'efficacité de la solution ?

- **Outil de campagne de phishing** pour sensibiliser les utilisateurs au vol de mots de passe
- **Authentification multi-facteurs** pour accéder aux ressources critiques
- **Gestionnaire des accès à privilèges (PAM)**

Quelles autres solutions celle-ci peut-elle compléter ?

- Un gestionnaire permet d'implémenter les politiques de mots de passe
- Il ne complète pas de solution technologique en particulier

Services associés

Accompagnement par un tiers possible pour :

- La sensibilisation et la formation aux bons usages des éléments secrets.