Bitwarden sur la Plateforme en Ligne Mathrice (PLM)

Une solution sécurisée pour gérer les mots de passe

Romain Théron (IDP - UMR 7013) et Francis Léger (IMB - UMR5584)

16 mars 2023

Pourquoi Bitwarden ?

- Travailler en équipe multi-sites et en Réseaux
- Plateforme en Ligne MATHRICE (PLM) : OPENSHIFT basé sur des containers type Docker et Orchestré par Kubernetes(K8S)
- permet d'utiliser des mots de passes forts
- permet d'importer des coffres keepass, KeepassX, firefox

Serveur officiel

- Gestionnaire de mots de passe client/serveur
- open source
  - écrit en C# (.net)
  - dépend de sql server
  - installation via docker
  - nécessite pas mal de ressources

Vaultwarden

- implémentation alternative de la partie serveur[1]
- API complète par rapport à la version officielle
- écrite en rust
- sqlite, mysql ou postgresql
- plus légère
- image docker disponible
- compatible avec les clients officiels

[1] https://github.com/dani-garcia/vaultwarden/

Sécurité

- données chiffrées dans la base de données[2]
- le chiffrement se fait en local et on ne peut rien déchiffrer sur le serveur
- audits de sécurité[3]
- détails sur la sécurité[4]
- authentification à deux facteurs possible
  - yubikey
  - applis smartphone (aegis, authy etc. . .)
  - email
  - standard webauthn

[2] https://bitwarden.com/help/what-encryption-is-used/
[3] https://bitwarden.com/blog/bitwarden-network-security-assessment-2020/
[4] https://bitwarden.com/images/resources/security-white-paper-download.pdf/

Clients

- client lourd pour tous OS
- extension navigateurs
- CLI
  - bitwarden-cli (officiel) pour accéder à un coffre-fort Bitwarden et le gérer en ligne de commande [5]
  - rbw Paquet Débian et Arch Linux [6]
- interface web

[5] https://github.com/bitwarden/cli
[6] https://github.com/doy/rbw

Générales

- remplissage automatique (via clic ou raccourci clavier)
- génération de mdp
- partage de mdp (organisations)
- import / export
- sur l'instance de la PLM : enregistrement désactivé (il faut être invité)

Types d'enregistrement

- identifiants / mdp / url
- cartes de paiement
- identité
- notes
- rangement par dossiers

Partage de fichier

- date de suppression
- date d'expiration
- nombre maximum d'accès
- mdp optionnel

Fonctionnalités pratiques à exploiter en équipe :

- "SEND" pour le partage (notes - clefs de chiffrement, motsde passe bios..)
- "ORGANISATION" pour inviter ou transmettre
- "RAPPORTS" sur les mots de passe exposés, faibles, réutilisés