Thème 1 Chapitre 2

Appliquer et diffuser la réglementation liée aux données à caractère personnel

TP Keepass
Mise en œuvre d'un gestionnaire de mots de passe

Bloc 3 - Cybersécurité des services informatiques

EVALUATION DES COMPETENCES VISEES						
Compétence(s) Visée(s)	**Savoir-Faire(s)**	**Niveau d'acquisition**				
		A	B	C	D	E
B3.1 : Protéger des données à caractère personnel	**Sensibiliser les utilisateurs à la protection des données à caractère personnel**					

Table des matières

1. Introduction

1.1. - Présentation du gestionnaire de mot de passe KEEPASS

KeePass est un gestionnaire de mots de passe open source qui offre un stockage sécurisé des informations d'identification, telles que les noms d'utilisateur et les mots de passe. Voici un résumé des principales caractéristiques de KeePass :

- **Sécurité** : KeePass utilise un chiffrement fort pour protéger les données sensibles, assurant ainsi la confidentialité des informations stockées.
- **Base de données chiffrée** : Les mots de passe et autres informations confidentielles sont stockés dans une base de données chiffrée, généralement protégée par un mot de passe principal, une clé ou un fichier clé.
- **Génération de mots de passe** : KeePass peut générer des mots de passe complexes et uniques, aidant à renforcer la sécurité en évitant l'utilisation de mots de passe faibles ou réutilisés.
- **Multiplateforme** : KeePass est disponible sur plusieurs plateformes, y compris Windows, macOS, Linux, et il existe des versions mobiles pour Android et iOS.
- **Open source** : Le code source de KeePass est ouvert, ce qui signifie que son fonctionnement peut être vérifié et amélioré par la communauté.
- Intégration avec les navigateurs : Il propose souvent des extensions pour les navigateurs, facilitant la saisie automatique des informations d'identification. L'utilisation de ces extensions déconseillée pour des raisons de sécurité.

1.2. - Présentation du service de stockage en ligne DROPBOX

Dropbox est un service de stockage en ligne (sur le cloud) et de partage de fichiers qui permet aux utilisateurs de sauvegarder leurs données, y accéder depuis n'importe quel appareil connecté à Internet et collaborer facilement avec d'autres personnes. Voici une présentation générale de Dropbox :

- **Stockage en nuage** : Dropbox offre un espace de stockage en ligne où les utilisateurs peuvent sauvegarder et synchroniser leurs fichiers. Cela permet d'accéder aux données à partir de divers appareils tels que des ordinateurs, des smartphones et des tablettes.
- **Synchronisation automatique** : Les fichiers déposés dans le dossier Dropbox sur un appareil sont automatiquement synchronisés avec le cloud et avec d'autres appareils connectés au même compte, assurant ainsi la disponibilité des données à jour partout.
- **Partage de fichiers** : Dropbox facilite le partage de fichiers et de dossiers avec d'autres utilisateurs. Les documents peuvent être partagés via des liens, et il est possible de définir des autorisations pour contrôler qui peut afficher, éditer ou commenter les fichiers partagés.
- **Collaboration en temps réel** : Les utilisateurs peuvent collaborer sur des documents en temps réel, en travaillant simultanément sur des fichiers partagés. Cela favorise la productivité dans un environnement de travail collaboratif.
- **Versioning** : Dropbox conserve les versions antérieures des fichiers, ce qui permet de restaurer des versions précédentes en cas de besoin. Cela offre une protection contre les modifications indésirables.

- **Applications tierces** : Dropbox peut être intégré à de nombreuses applications tierces, ce qui permet aux utilisateurs d'étendre les fonctionnalités de base du service en fonction de leurs besoins.
- **Sécurité** : Dropbox utilise le chiffrement pour protéger les données en transit et au repos. Les fonctionnalités de sécurité incluent également la possibilité de configurer l'authentification à deux facteurs pour renforcer la protection des comptes.
- **Applications mobiles** : Dropbox propose des applications mobiles pour les plateformes iOS et Android, offrant ainsi une expérience utilisateur cohérente sur divers appareils.
- **Tarification** : Dropbox propose des plans gratuits avec une quantité limitée d'espace de stockage, ainsi que des plans payants avec plus d'espace et des fonctionnalités avancées pour les particuliers et les entreprises.

1.3. - Présentation du service de stockage en ligne PCLOUD

pCloud est un service de stockage en ligne basé sur le cloud qui offre aux utilisateurs la possibilité de sauvegarder, stocker, partager et accéder à leurs fichiers depuis divers appareils connectés à Internet.

Il offre les mêmes fonctionnalités que Dropbox (voir présentation de Dropbox un peu plus haut). pCloud propose en plus une option de chiffrement qui permet aux utilisateurs de chiffrer leurs fichiers avant de les téléverser sur le cloud, renforçant ainsi la sécurité des données (service payant).

2. - Mise en œuvre de Keepass

2.1. - Présentation de la solution à mettre en œuvre

Source : https://keepass.fr/keepass-pour-mobile-android-et-ios/

Nous souhaitons installer et utiliser Keepass afin de mettre en œuvre une base de données de mots de passe disponible dans le Cloud. Cette base de données (coffre) sera une copie synchronisée de celle qui se trouvera sur votre espace Cloud (Dropbox dans notre exemple). Nous souhaitons en fait arriver à ce résultat :

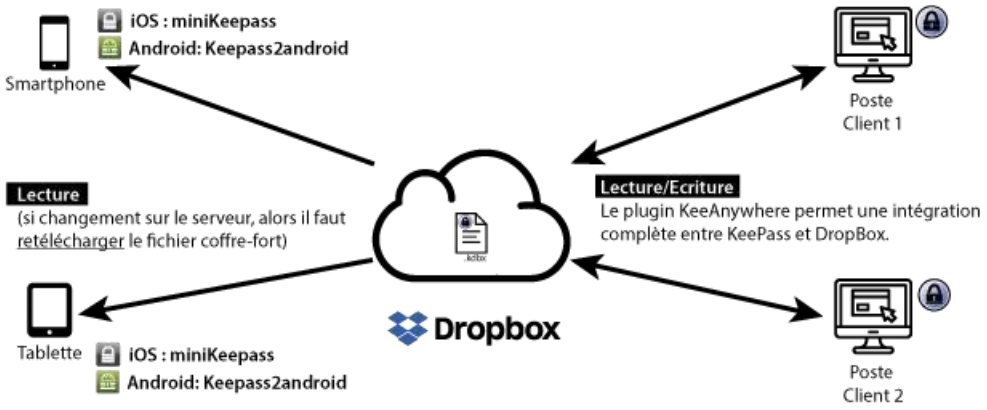

Figure 1: La base de donnée chiffrée contenant les mots de passe est accessible depuis n'importe quelle machine disposant de l'application Keepass connectée à Internet.

L'espace Dropbox local contiendra donc la base de données Keepass et sera automatiquement synchronisé, dans le cloud, grâce au logiciel Dropbox. Ainsi il sera aussi possible d'utiliser Keypass

sous Mac, Windows, Android, etc.. Dans ce TP, il n'est pas demandé de mettre en œuvre le plugin KeeAnywhere.

2.2. - Mise en œuvre de Keepass dans une VM Windows

Mettez en œuvre le gestionnaire de mots de passe Keepass dans une VM Windows.

Contraintes :

- Le fichier (base de données) contenant les mots de passe sera stocké en local (dans le répertoire prévu par Dropbox). Ainsi une copie synchronisée sera disponible en permanence dans le cloud. Le principe est que Keepass, dispose en permanence d'une base de données locale mise à jour en temps réel avec la version stockée en ligne.
- Choisissez une passphrase d'au moins 20 caractères facile à retenir et robuste.

  Exemple : "Lesmouettesaimentlamer.258" (**2** +3=**5** +3=**8**)
- Vous devez posséder ou créer un compte auprès d'un fournisseur de services cloud (Dropbox, pCloud…). Bien sûr, le mot de passe à ce service doit être robuste (12 caractères contenant au moins minuscules, majuscules, chiffres et caractère spécial).
- Testez la solution en créant au moins 2 entrées de mot de passe

2.3. - Mise en œuvre de Keepass dans votre smartphone

- Mettez en œuvre le gestionnaire de mots de passe Keepass dans votre smartphone (Android ou iOS). Keepass doit aller chercher le fichier de base de données chiffré, précédemment créé et stocké sur votre service cloud.
- Constatez que vous accéder bien aux entrées précédemment créées dans le Keepass de votre VM Windows
- Créez une nouvelle entrée dans le Keepass de votre smartphone puis constatez que cet ajout est bien visible dans le Keepass de votre VM

2.4. - Ajout d'un fichier-clé dans votre Keepass (2FA)

Ajouter un fichier clé à votre base de données KeePass offre une couche de sécurité supplémentaire en plus du mot de passe principal. Cette fonctionnalité est souvent appelée "fichier-clé".
Voici quelques avantages et intérêts d'ajouter un fichier clé dans KeePass :

- **Double Authentification (2FA)** : La combinaison d'un mot de passe principal et d'un fichier clé crée une double authentification. Vous devez posséder à la fois le mot de passe et le fichier clé pour accéder à la base de données, renforçant ainsi la sécurité.
- **Protection contre les attaques par force brute** : Même si un attaquant parvient à découvrir ou à deviner le mot de passe principal, il aura également besoin du fichier clé pour accéder aux données. Cela rend plus difficile la réussite d'une attaque par force brute.
- **Sécurité physique** : Vous pouvez stocker le fichier clé sur un support externe tel qu'une clé USB ou une carte mémoire. Cela signifie que même si quelqu'un obtient votre mot de passe, il ne pourra pas accéder à la base de données sans également avoir accès au fichier clé physique.
- **Protection contre les enregistreurs de frappe** : Les enregistreurs de frappe (keyloggers) peuvent potentiellement enregistrer vos frappes et récupérer votre mot de passe, mais ils

ne peuvent pas enregistrer l'emplacement physique d'un fichier clé stocké sur un support externe.

- **Flexibilité** : Vous pouvez choisir le type de fichier clé que vous souhaitez utiliser, qu'il s'agisse d'une image, d'un fichier texte ou de tout autre type de fichier pris en charge par KeePass. Cela offre une certaine flexibilité dans la mise en place de la sécurité.
- **Options de sécurité personnalisées** : KeePass offre diverses options de configuration pour la manière dont le fichier clé est utilisé, y compris la possibilité de l'associer à un emplacement spécifique sur le disque ou de le stocker à côté de la base de données.

- Ajoutez un fichier-clé à votre base de données KeePass de votre VM Windows - Testez cette solution sur votre VM (se connecter, se déconnecter, se reconnecter…)
- Pouvez-vous accéder à vos mots de passe sur votre smartphone sans ce fichier-clé ?
- Faites le nécessaire pour que cette solution (passphrase + fichier-clé) fonctionne aussi sur votre smartphone. Testez.