Sécurité de l’ordinateur 1 : Saisie par la police

> Modèle de menace : *La police saisit un ordinateur pendant une perquisition ou dans un sac à la frontière ou pendant une action, etc. L'ordinateur est passé à des spécialistes qui extraient les données de l'appareil. Ces données sont utilisées plus tard pour incriminer le propriétaire et/ou d'autres rebelles et/ou compromettre la branche. L'ordinateur peut être rendu au rebelle arrêté sans aucune indication que ce processus a eu lieu.*

Tout comme avec les téléphones, il faut nous préparer à la possibilité que quelqu'un accède avec notre ordinateur à son contenu, sans même avoir besoin de connaître nos détails d'identification. Pour ce faire, nous employons une technique appelée *Disk Encryption* (chiffrement du disque).

> :warning: Il est moins efficace de chiffrer le disque dur de votre ordinateur si les forces de l'ordre ont accès au cloud de stockage que vous utilisez pour les sauvegardes. DropBox, Google Drive et One Drive sont toutes des compagnies qui ont l'obligation légale de se soumettre à des mandats de perquisition de manière transparente ou autrement. Envisagez plutôt de chiffrer un disque dur externe pour sauvegarder vos données. S'il contient des informations importantes/sensibles, investissez dans un disque externe, chiffrez-le et laissez-le chez quelqu'un en qui vous avez confiance, de préférence sans relation avec XR, et ne le dites à personne. Lorsque vous rendez visite à cette personne, prenez votre ordinateur et sauvegardez vos données sur ce disque externe.

Chiffrer le contenu de son ordinateur

Les ordinateurs tournent habituellement sur des systèmes comme Windows, OS X ou GNU/Linux (comme Ubuntu), c'est pour cela que nous allons couvrir ces plateformes ici.

A. Windows

Si votre appareil sur les versions Entreprise ou Intégrale de Windows Vista, alors vous pouvez activer Bitlocker, sinon vous pouvez installer et activer Veracrypt.

:closed_lock_with_key: Bitlocker

[details="Cliquez pour dérouler"]

:arrow_forward: : Vous n'utilisez pas encore Bitlocker.

[details="Cliquez pour dérouler"]

- **Pour activer le cryptage de l'appareil** :one: Identifiez-vous (sign in) à votre appareil Windows avec un compte administrateur (vous devrez peut-être vous déconnecter et vous reconnecter pour changer de compte). Pour plus d'infos, voir Créer un compte d’utilisateur ou d’administrateur local dans Windows 10. :two: Sélectionnez le bouton **Démarrer**, puis sélectionnez **Paramètres** > **Mise à jour et sécurité** > **Cryptage de l'appareil *(à vérifier)***. Si **Cryptage de l'appareil** n'apparaît pas, c'est que l'option n'est pas disponible. Vous devriez pouvoir utiliser le cryptage Bitlocker standard à la place (voir juste après). Ouvrez les paramètres de cryptage de l'appareil. :three: Si le cryptage de l'appareil est désactivé, sélectionnez **Activer**.
- **Pour activer le cryptage standard de Bitlocker** :one: Identifiez-vous (sign in) à votre appareil Windows avec un compte administrateur (vous devrez peut-être vous déconnecter et vous reconnecter pour changer de compte). Pour plus d'infos, voir Créer un compte d’utilisateur ou d’administrateur local dans Windows 10. :two: Dans la zone de recherche de la barre des tâches, tapez **Gérer Bitlocker**, puis sélectionnez-le dans la liste des résultats. Ou alors vous pouvez sélectionner le bouton **Démarrer**, puis, dans **Système Windows**, sélectionner **Panneau de configuration**. Dans le panneau de configuration, sélectionnez **Chiffrement de lecteur Bitlocker**. **Note:** Vous verrez cette option seulement si elle est disponible sur votre appareil. Elle n'est pas disponible sur Windows 10 Home. :three: Sélectionnez **Activer BitLocker** puis suivez les instructions : :four: Sauvegardez la clé de récupération dans un endroit sûr : un fichier enregistré dans un endroit sûr, ailleurs que sur le disque dur chiffré (sur une clé USB par exemple). Sauvegarde de la clé de récupération|500x400 :five: Chiffrez tout le lecteur. Le contenu supprimé sera ainsi également chiffré. :six: Il est conseillé d'exécuter

la vérification système, même si cela prend plus de temps comme l'ordinateur doit redémarrer. Exécuter la vérification système|400x300 :seven: : Redémarrez votre ordinateur et c'est parti ! Chiffrement en cours|466x277

[/details]

:arrow_forward: **Vous utilisez déjà Bitlocker mais vous stockez votre mot-de-passe de manière non-sécurisée.**

[details="Cliquez pour dérouler"]

> :warning: Si vous achetez un nouvel ordinateur sous Windows 10 et que vous utilisez un compte Microsoft, votre appareil sera crypté par Windows et la clé de récupération sera enregistrée automatiquement sur *OneDrive*. Ce n'est pas bien, parce que Microsoft peut être forcé de fournir discrètement ou ouvertement cette clé pour décrypter votre ordi. De plus, votre compte Microsoft pourrait avoir été compromis par un·e attaquant·e, et pour cette raison c'est préférable de refuser d'enregistrer la clé dans OneDrive et de plutôt l'enregistrer dans KeePass, ou le plus récent et plus attirant KeePassXC , sur un autre appareil ou un autre appareil crypté de stockage USB. Vous pourriez par exemple inventer une phrase de passe complètement nouvelle faite de 5 mots, nombres et caractères spéciaux ou plus, et vous en souvenir.

Changer les mots de passe Bitlocker

Faites un clic droit sur le disque crypté de BitLocker dans Windows Explorer et sélectionnez **Changer le mot de passe BitLocker *(à vérifier)*** depuis le menu contextuel.
image|546x325

> **Note:** Si l'icône de votre disque crypté a un cadenas doré, alors vous ne pouvez pas voir l'option "**Changer le mot de passe Bitlocker**" dans le menu contextuel, vous devez d'abord déverrouiller le disque Bitlocker.
image|564x431 [/details]

[/details]

:closed_lock_with_key: [A FAIRE] Veracrypt

[details="Cliquez pour dérouler"]

https://www.veracrypt.fr/en/Downloads.html [/details]

B. Mac OS X

Tout comme Windows peut être chiffré avec Bitlocker, Filevault est la solution par défaut de chiffement de disque pour les systèmes OS X. A noter que FileVault ne chiffre pas entièrement votre système (en incluant la partition de démarrage), mais uniquement la partition utilisateur (en terme Mac, le "Macintosh HD").

:closed_lock_with_key: Activer et configurer FileVault

[details="Cliquez pour dérouler"]

FileVault 2 est dsiponible sur OS X Lion et suivants. Quand FileVault est activé, votre MAC vous demande de vous connecter à chaque démarrage avec une mot de passe.

1. Choisir le menu Apple > Préférences systèmes, Ensuite cliquer sur "Securité et Confidentialité".
2. Cliquer sur l'onglet FileVault.
3. Cliquez Locked|48x60 Image not found or type unknown. Et lorsqu'on vous le demande, renseignez votre compte administrateur et mot de passe.
4. Finissez en activant FileVault.

s&cf|690x480
Image not found or type unknown

Si d'autre utilisateurs ont un compte sur votre MAC, vous devriez voir un message indiquant que chaque utilisateur doit taper son mot de passe pour pouvoir, eux aussi, débloquer le disque. Pour

chaque utilisateur, cliquer sur le boutton "Activer l'utilisateur" et entrez le mot de passe utilisateur. Les utilisateurs que vous ajouterez après avoir activé Filevault seront eux automatiquement activés. sS&cfu|690×479 Image not found or type unknown

Choisissez comment vous voulez être capable de déchifrer votre disque et réinitialiser votre mot de passe au cas ou vous oubliez votre mot de passe :

> :warning: Si vous utilisez OS X Yosemite ou suivant, vous pouvez choisir d'utiliser votre compte iCloud pour déchifrre votre disque et ré-initialiser votre mot de passe. **Ne faites pas cela**. Si vous utilisez OS X Mavericks, vous pouvez choisir de sauvegarder vos clefs de récupération chez Apple en renseignant des questions et leurs réponses (trois questions/réponses) **Ne faites pas cela** .

sS&cfi|690×479 Image not found or type unknown

Créer une clef de récupération locale. Sauvegardez les lettres et les chiffres de la clef dans un endroit sûr. Ailleurs que sur votre disque dur chiffré.

[/details]

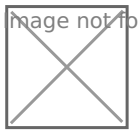
C. GNU/Linux (Debian, Ubuntu, Arch Linux, etc)

Alors que les systèmes Linux sont en général bien plus sécurisés que les systèmes Windows, et qu'il y a bien moins de chances qu'ils compromettent la vie privée des utilisateurs avec des solutions de stockage externe (comme sous Windows 10 et OS X), il est difficile de chiffrer complètement un portable sous GNU/Linux *après* l'installation. Vous pouvez cependant créer un nouveau compte Unix sur le système, vous connecter et chiffrer le répertoire personnel de ce nouvel utilisateur à partir d'un autre compte, et enfin y copier les données que vous voulez mettre en sécurité.

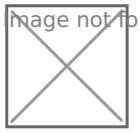
:closed_lock_with_key: **Chiffrement du système complet**

[details="Cliquez pour dérouler"]

La meilleure solution, bien que peu commode, est simplement de copier toutes les données importantes sur par exemple une clé USB de grande capacité ou un disque dur externe (idéalement chiffré) et d'effectuer une réinstallation sur le portable. Il faut alors choisir l'option de chiffrement complet du système. Voici par exemple comment faire sur Ubuntu (en anglais) :



Cliquer sur "Installer maintenant" après avoir sélectionné l'option de chiffrement sur Ubuntu, conduit à une page de configuration, qui permet à l'utilisateur d'entrer la clé de chiffrement pour l'installation :



Entrez la clé de chiffrement. L'efficacité de cette clé sera indiquée à côté de cette fenêtre, donc utilisez cet outil comme un "baromètre" et essayez d'avoir une clé qualifiée de "Mot de passe fort". Une fois choisi, l'entrer à nouveau pour la confirmer puis, surtout, éviter de l'oublier !

Cochez de plus la case "Écraser l'espace disque vide" (c'est optionnel). Sélectionnez "Installer maintenant" lorsque vous avez terminé.

Sélectionnez le fuseau horaire et créez un utilisateur avec un mot de passe fort.

Lors de la création du disque dur chiffré sous Ubuntu, sélectionnez "demander mon mot de passe pour me connecter" et "chiffrer mon répertoire utilisateur" au moment de la création de l'utilisateur. Cela ajoutera une couche de sécurité supplémentaire pour les données. [/details]

:closed_lock_with_key: Chiffrement fort d'un périphérique de stockage externe sous GNU/Linux

[details="Cliquez pour dérouler"] Ce qui suit est un exemple sur une distribution basée sur Debian, comme Ubuntu.

1. Installer cryptsetup

```
apt-get update apt-get install cryptsetup
```

2. Connecter le périphérique que vous voulez chiffrer Connecter le périphérique, attendre quelques secondes, et entrer la commande `dmesg` dans un terminal afin de trouver son emplacement dans le système de fichiers. Si vous n'avez pas activé le montage (`mount ...`) automatique précédemment, connectez le périphérique que vous voulez chiffrer puis démontez-le (`unmount ...`)/"éjecter". En général le périphérique sera monté sur /dev/sdb et ses partitions sur /dev/sb1, /dev/sdb2, etc. Vérifier avec `fdisk -l` et comparer au résultat précédent.

3. Chiffrer le périphérique :warning: Ne pas copier-coller la commande ci-dessous tant que vous n'êtes pas certain·e de l'emplacement du périphérique. En supposant que le périphérique est monté sur **/dev/sdb**, nous allons le chiffrer avec un chiffrement fort AES-XTS et une clé de longueur 512 octets (au lieu de 256, qui est l'option standard et déjà satisfaisante) :

```
cryptsetup luksFormat -c aes-xts-plain64 --key-size 512 --hash sha512 --use-urandom /dev/sdb
```

Vous devrez fournir le mot de passe que vous aurez choisi.

4. Libérer le périphérique Nous devons maintenant le libérer/déchiffrer avant de pouvoir faire quoi que ce soit d'autre. Nous devons lui assigner une "étiquette", qui apparaîtra dans le "mapper" du système de fichiers utilisé pour le chiffrement. Ici, nous allons utiliser l'étiquette "encrypted" ; on peut choisir toute autre étiquette.

```
cryptsetup luksOpen /dev/sdb encrypted
```

Vous devrez fournir votre mot de passe. Vérifiez que vous avez maintenant un fichier **/dev/mapper/encrypted** dans votre système de fichiers.

5. Créer un système de fichiers sur le périphérique :warning: À faire une seule fois ! Nous créons maintenant un système de fichiers fiable *ext4* sur le périphérique non chiffré, accessible via le "mapper" :

```
mkfs.ext4 /dev/mapper/encrypted
```

6. "Monter" le périphérique dans votre système de fichiers Créer un répertoire **enc** dans votre dossier personnel qui servira de point de montage :

```
mkdir enc
```

"Monter" le fichier **/dev/mapper/encryted** à cet endroit :

```
mount /dev/mapper/encrypted enc
```

Vous pouvez maintenant copier les données sur votre périphérique.

7. Fermeture du périphérique chiffré Vous devrez le faire à chaque fois que vous avez copié des données sur votre périphérique. D'abord, "démontez"-le :

```
umount enc
```

Puis fermez-le :

```
cryptsetup luksClose encrypted
```

[/details]

D. Demande d'accès des forces de l'ordre

> :warning: Ayez toujours un mot de passe puissant pour la connexion (login), car si votre mot de passe est découvert, votre contenu est accessible même si votre disque est chiffré.

> :information_source: **Si vous le pouvez et que vous savez que votre ordinateur risque d'être saisi : éteignez-le avant le contact avec les forces de l'ordre ou les enquêteurs.** Eteignez-le toujours avant de passer une frontière par exemple.

Les forces de l'ordre peuvent vous demander de fournir votre mot de passe. Ne leur dites rien de plus que nécessaire. En cas de procès, vous aurez le temps de vous préparer avec des personnes compétentes.

Cet article est toujours en cours de modification.

Références

https://base.organise.earth/t/laptop-security-1-seizure-by-police-and-investigators/600

Post transféré de la base

Révision #1
Créé 8 September 2023 18:18:28 par julien
Mis à jour 8 September 2023 18:18:36 par julien