
GUIDE PRATIQUE !
ÉVITEZ LES HISTOIRES D'HORREUR EN INFORMATIQUE
Je valide ça ☑
service-conseil

Visitez notre site web au https://jevalide.ca



Publié le 19 octobre 2021

Mise en page effectuée avec LaTeX

# Table des matières

# Introduction

Dans ce guide pratique, nous allons explorer quatre différentes histoires d'horreur qui peuvent survenir sur les systèmes informatiques utilisés par les organisations de toutes tailles, du travailleur autonome à la grande entreprise. Les principes sont les mêmes, seule l'échelle change.

Pour chacun de ces scénarios, nous allons voir différents conseils de prévention, ainsi que des moyens pour réduire les dégâts lorsque l'inévitable se produit.

Certains de ces exemples sont des attaques malveillantes. Dans tous les cas, vous devrez aviser immédiatement la responsable de la sécurité informatique de votre organisation, ainsi que les corps policiers locaux. Si vous n'avez pas encore développé d'expertise interne, vous devriez alors contacter des spécialistes en cybersécurité. Nous recommandons aussi fortement de consulter un avocat.

## Notice

Tous ces conseils sont offerts gracieusement et sans aucune garantie, en souhaitant qu'ils puissent bénéficier au plus grand nombre. Ces situations sont hypothétiques et génériques, toute ressemblance avec une situation réelle vécue dans le passé par une entreprise en chair et en os est fortuite.

Produit avec amour par François Pelletier pour jevalide.ca avec des logiciels libres

- Manjaro Linux,
- pandoc,
- pdftk,
- LaTeX et
- Code OSS)

et le logiciel de graphisme en ligne Canva.

# HISTOIRE D'HORREUR #1: UNE ATTAQUE PAR RANÇONGICIEL

*Je valide ça* ☑

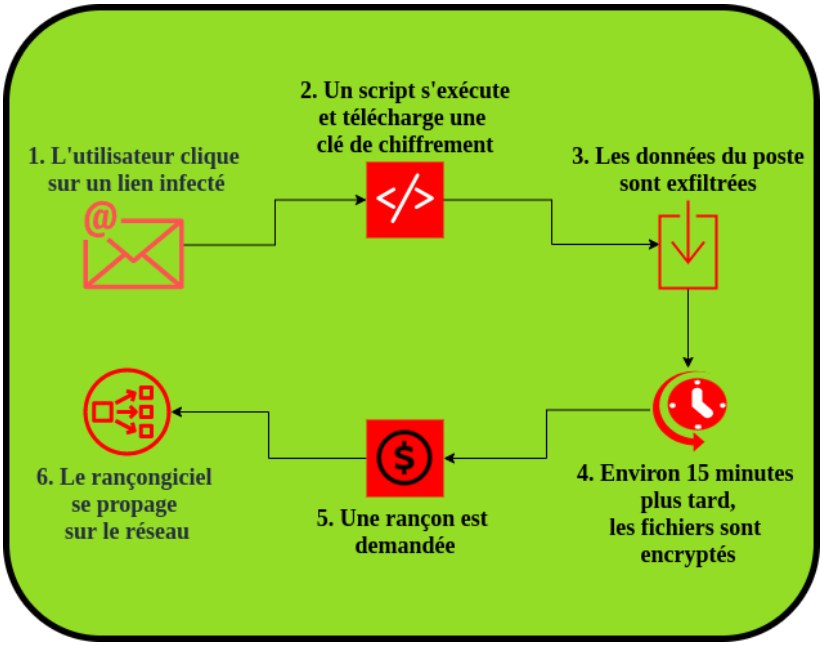
service-conseil

# Une attaque par rançongiciel

**Niveau intermédiaire**

L'attaque par rançongiciel, c'est une prise d'otage de données personnelles. Pour ce faire, ce logiciel va les chiffrer et ensuite afficher un message qui demande une rançon. Il y aura la plupart du temps une promesse de déchiffrer les données dans celui-ci.

Les pirates exigeront la somme due sous la forme de cryptomonnaie. Dans tous les cas, les autorités recommandent de ne jamais la payer. Après tout, pourquoi faire confiance à des criminels !



## Comment éviter cette histoire d'horreur (et plusieurs autres) ?

### Développer une stratégie de sauvegarde efficace

Un système infecté par un rançongiciel est souvent cassé et devra être entièrement formaté. C'est pourquoi il est important de sauvegarder régulièrement nos fichiers. Nous suggérons de le faire sur au moins deux supports différents et qui ne sont pas connectés à vos systèmes :

— En ligne, sur un service d'hébergement protégé par la cryptographie.
— Une copie physique sur un appareil de stockage tel qu'un disque dur portatif, une clé USB ou un autre ordinateur.

Pour faciliter cette dernière tâche sur Windows ou Linux, nous suggérons le logiciel graphique GRsync. C'est une interface au puissant utilitaire rsync. Pour avoir un aperçu de son usage, notre guide de juillet 2021, Partir en vacances l'esprit tranquille, propose un survol de cet outil.

Pour profiter de la cryptographie lors du transport et du stockage, l'outil Borg, qui est plus technique que Rsync, permet d'appliquer cette stratégie. Il y est aussi expliqué dans notre guide précédent.

Sur MacOS, il y a un utilitaire de sauvegarde nommé Time Machine, qui peut faire une partie du travail, sans avoir beaucoup d'options toutefois. Nous recommandons d'apprendre rsync qui y est nativement installé.

Une sauvegarde peut avoir été contaminée par un rançongiciel détecté tardivement. Pour contrer ce risque, nous recommandons

de prévoir, en complément, une méthode incrémentale de sauvegarde. Cette dernière conservera automatiquement un historique des versions antérieures des fichiers.

Assurez-vous de vous exercer régulièrement à la restauration de vos sauvegardes et de mettre en place une procédure simple à suivre. Si un incident survient, vous aurez bien d'autres soucis que vous remémorer cette procédure !

Un outil de collaboration tel que Nextcloud, permet de préserver plusieurs versions des fichiers de manière transparente. Il a l'avantage d'avoir des applications client pour tous les systèmes d'exploitation populaires.

Afin de limiter l'exposition à des données personnelles, essayez de les garder le moins longtemps possible sur votre ordinateur de travail. Préférez toujours un support déconnecté pour celles-ci, comme un disque dur ou une clé USB. Deux copies valent mieux qu'une dans ce cas !

Pour plus de détails sur les différentes stratégies, nous vous invitons à consulter le guide intitulé Les 3 types de sauvegardes publié en aout 2021.

### Éviter les fichiers et liens suspects

Plusieurs types de contenus peuvent être suspects, tout particulièrement les liens et les pièces jointes dans les courriels et sur les sites Internet à réputation faible.

Un programme d'exposition aux courriels douteux demeure une bonne première étape, s'il est bien planifié. Les groupes criminels utilisent maintenant des techniques sophistiquées. Alors, bien honnetement, les campagnes improvisées avec des courriels factices pleins de fautes d'orthographe et affichant un mauvais logo ne sont plus suffisantes pour des fins de prévention. Il faut réussir à prendre au piège le plus de notre personnel possible avec du réalisme pour avoir un impact.

Privilégiez, dans vos communications avec la clientèle et les entreprises, des contenus simples, en texte seulement, et évitez en tout temps les pièces jointes qui peuvent inclure du code exécutable, comme les fichiers de type Office avec des macros.

Dans tous les cas, n'ouvrez jamais de ces fichiers reçus par courriel qui proviennent d'une source externe, même si c'est un de vos contacts. Préférez utiliser un système de partage convenu à l'avance.

### Valider l'authenticité et l'intégrité des fichiers exécutables téléchargés

Lorsque vous devez ouvrir un fichier exécutable téléchargé de l'externe, assurez-vous de valider les sommes de contrôle de celui-ci. Ceci peut être réalisé avec l'utilitaire `shasum`, sur Linux et macOS, depuis le terminal.

```
shasum -a 1 <fichier>
```

Sur Windows, vous utilisez le logiciel `certutil` comme suit, depuis l'invite de commandes ou PowerShell.

```
certutil -hashfile <fichier> SHA1
```

Évitez d'ouvrir des fichiers exécutables qui ne possèdent pas ces sommes de contrôle. C'est souvent signe que c'est un logiciel amateur qui n'est probablement pas sécurisé adéquatement.

### Effectuer la mise à jour périodique de tous ses logiciels et appareils

Nous ne pourrons jamais autant le répéter! Un des meilleurs moyens de garder son poste ou ses serveurs en sécurité, c'est de mettre à jour le plus fréquemment possible. Idéalement, celles-ci sont effectuées tous les jours.

Une règle d'or : aucun système qui n'a pas été mis à jour depuis plus d'un mois ne devrait se connecter à Internet. Point !

Sur Windows, en plus des correctifs du système, avec Windows Update, il faut vérifier chacun des logiciels installés. Heureusement, de plus en plus proposent de vérifier la présence de nouvelles versions lors de leur ouverture. Si cette option est disponible, activez-là !

Sur MacOS, c'est compliqué de suivre les mises à jour, malheureusement. Quand ça vous saute au visage, faites-les immédiatement !

Chacune des différentes distributions Linux a sa propre façon d'effectuer les mises à jour. Voici les plus fréquentes :

```
# Debian et Ubuntu
sudo apt update
sudo apt upgrade
# RedHat et CentOS
sudo yum update
# Fedora
sudo dnf update
# Manjaro et Arch
sudo pacman -Syu
```

### Utiliser des mots de passe robustes et uniques

Un mot de passe robuste n'est pas composé seulement de mots du dictionnaire et de chiffres. Il est unique et ne devrait être utilisé qu'une fois, pour un compte.

Il peut être difficile de retenir plusieurs mots de passe. Cependant, il existe maintenant des logiciels qui s'occupent de les gérer à notre place. Ils permettent même d'en générer des nouveaux. Un de ceux-ci est Bitwarden, qui offre aussi un service gratuit en ligne. Il propose des applications client sur toutes les plateformes et il est très convivial.

En entreprise, c'est souvent plus simple de fournir un outil qui s'installe sur le poste de travail. Dans ce cas, le logiciel KeePass pourrait très bien répondre au besoin d'entreposer de manière sécuritaire des mots de passe et d'autres types d'identifiants confidentiels. Les données sont sauvegardées dans un fichier chiffré qui se transporte ou se synchronise facilement avec des plateformes de collaboration telles que Nextcloud ou DropBox.

### Utiliser l'authentification à facteurs multiples

L'authentification à facteurs multiples permet d'éviter à quelqu'un qui aurait accès à votre mot de passe de se connecter sans pouvoir contrôler un autre élément. Il faut la privilégier sur tous les comptes en ligne où cette option est disponible.

Cette vérification peut être biométrique, avec une empreinte digitale, par un SMS ou avec une application mobile de génération de mots de passe à usage unique basés sur le temps (Time-based one-time password, TOTP). FreeOTP+ pour Android facilite cette tâche. De plus, il est possible d'effectuer une sauvegarde de celle-ci vers un autre appareil. Sur iOS, FreeOTP Authenticator, une version antérieure, a une interface similaire.

Il existe aussi des clés physiques, telles que la Yubikey, qui permettent d'augmenter la fluidité de l'expérience utilisateur.

### Activer le pare-feu de son ordinateur et de son routeur

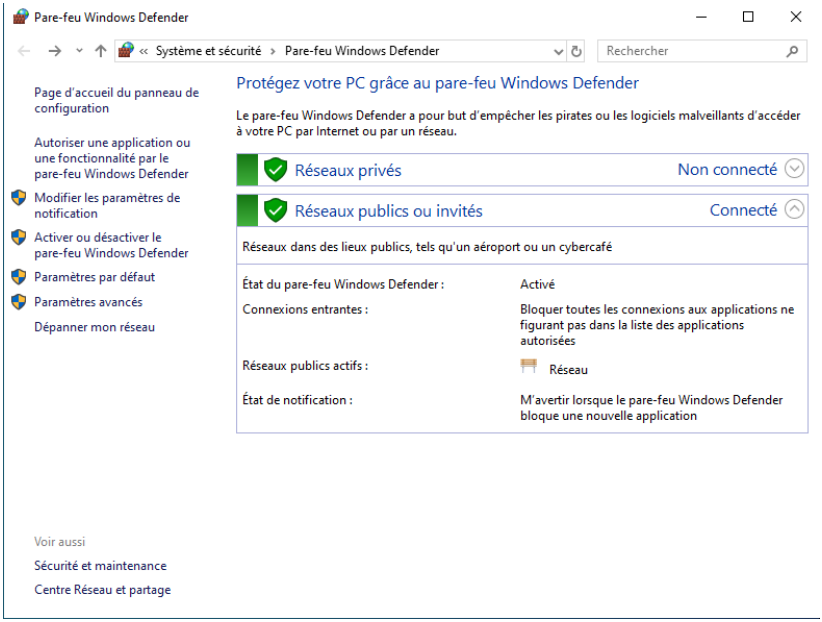
Le pare-feu est un système qui permet d'ouvrir et de fermer des ports, c'est à dire des adresses pour faire entrer ou sortir de l'information entre votre ordinateur et un réseau informatique. Plus il y en a d'ouverts, plus il y a d'occasions pour qu'un logiciel malveillant pénètre dans votre poste de travail. C'est donc une bonne pratique de laisser passer seulement ce qui est absolument requis.

Sur Windows, vous accédez aux paramètres du pare-feu Defender en utilisant la commande suivante dans le navigateur Edge

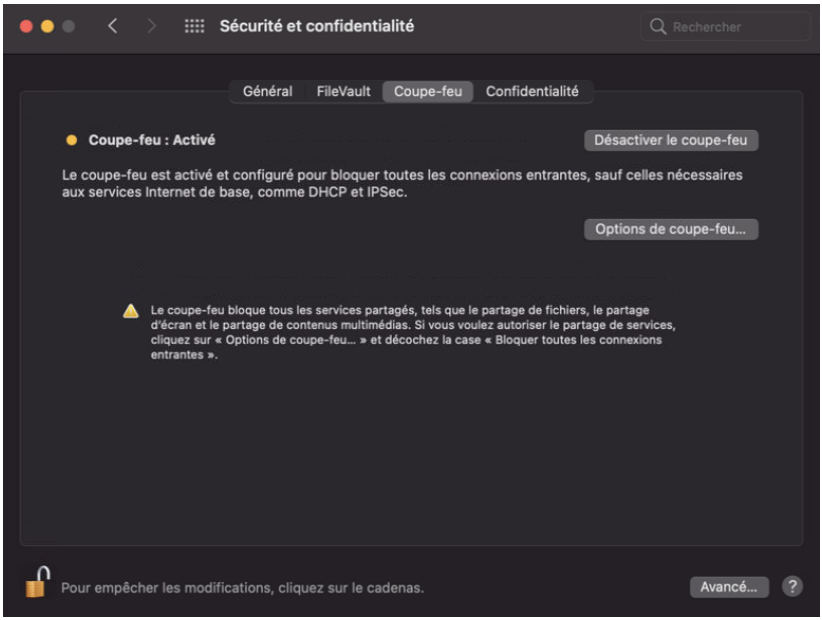
```
ms-settings:windowsdefender
```

Windows vous suggèrera fortement de créer un compte OneDrive pour augmenter la sécurité. Mais, sachez que vous pouvez tout autant utiliser Nextcloud sur votre propre serveur privé sans avoir à payer de licence mensuelle dispendieuse. Vérifiez surtout que les autres options affichées sont activées.

Windows communique énormément avec Microsoft, donc beaucoup de ports sont ouverts par défaut. Il peut être difficile de déterminer lesquels peuvent être fermés sans une expertise en administration Windows. Nous pouvons tout de même obtenir un aperçu en cliquant sur **Paramètres avancés** dans la fenêtre du pare-feu.



Sur macOS, le système inclut son propre pare-feu configurable depuis une interface graphique. Depuis les options, il est possible de bloquer toutes les connexions entrantes.



Sur Linux, le pare-feu par défaut est `iptables`. Il requiert une certaine expertise pour être configuré adéquatement. Heureusement, le logiciel `ufw` (Uncomplicated firewall) permet de simplifier la tâche. Pour l'activer, il suffit généralement d'exécuter cette commande :

```
sudo systemctl enable ufw
```

Pour nous assurer qu'il est activé, nous consultons le statut détaillé

```
sudo ufw status verbose
```

Ce qui devrait produire une sortie comme suit :

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), \
  disabled (routed)
New profiles: skip
```

Ensuite, pour ouvrir les ports, nous utilisons le numéro ou le nom du service, tel que listé dans le fichier `/etc/services`. Voici, par exemple, les ports autour du protocole SSH :

```
cat /etc/services | grep ssh | grep tcp | head -n 5
ssh                 22/tcp
sshell             614/tcp
netconf-ssh        830/tcp
sdo-ssh           3897/tcp
netconf-ch-ssh    4334/tcp
```

## Trop tard… et maintenant ?

### Couper l'accès au réseau

La première action, lors de toute détection d'attaque par rançongiciel ou de comportement suspect, comme la disparition de fichiers, c'est de couper l'accès au réseau. Commencez par déconnecter le câble et éteindre le wifi en débranchant le routeur. Sinon, il faut le fermer depuis son interface graphique, ce qui peut être ardu en entreprise.

### Aviser les autorités

Si vous recevez une demande de rançon, capturez l'écran avec votre mobile ou un appareil photo. Ne payez rien. Communiquez avec la police et une ou un spécialiste en cybersécurité. Ces derniers voudront probablement accéder à vos systèmes pour effectuer une analyse en criminalistique numérique. Il sera possible de restaurer les fichiers chiffrés, si le rançongiciel utilisé a été décodé. À ce sujet, on peut consulter le site No More Ransom.

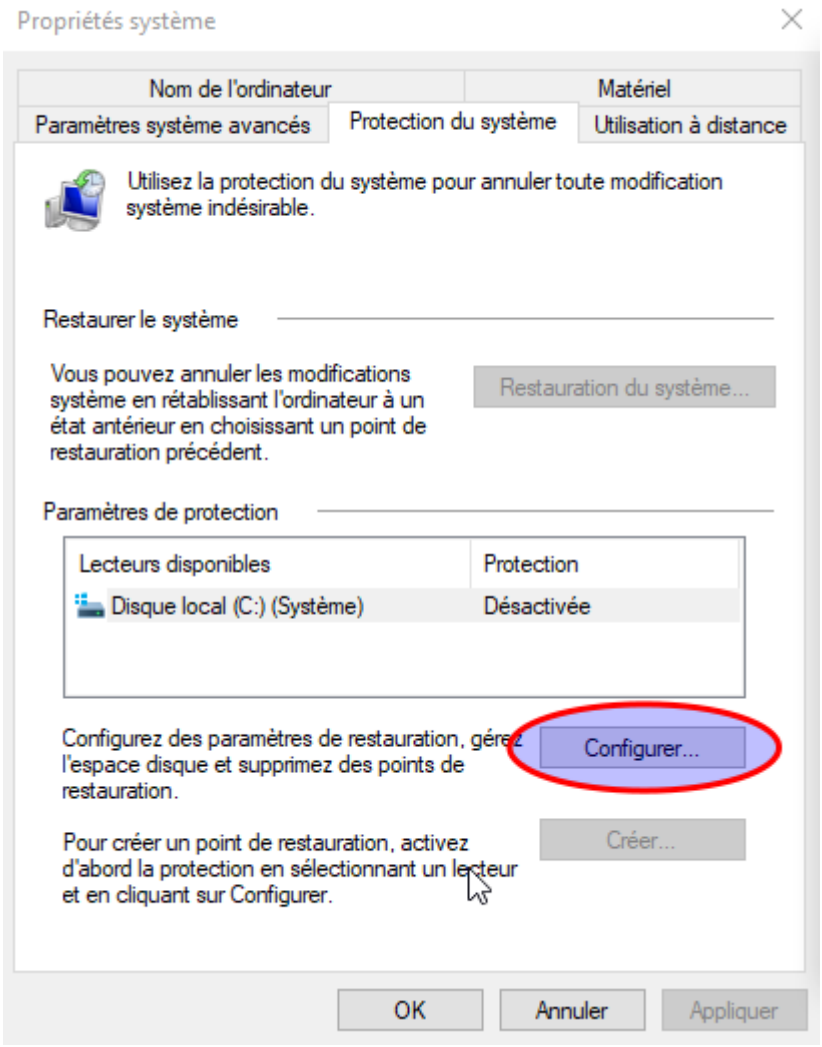
### Formater le système infecté

Une fois qu'un système infecté a été neutralisé, vous pourrez le réinstaller. Dans ce cas, nous préférerons formater les disques avec une méthode de remplissage aléatoire. Assurons-nous que le rançongiciel ne s'est pas installé dans une des parties critiques du système, tel que le gestionnaire d'amorçage. Pour ce faire, nous devrons attendre les résultats de l'enquête en criminalistique numérique.

### Effectuer une restauration

Localisez votre sauvegarde la plus récente et planifiez une restauration de celle-ci sur un autre réseau informatique que celui qui a été infecté, afin de, par exemple, publier en ligne un site web le plus rapidement possible. Ce peut être l'occasion de louer un serveur temporaire pour se remettre sur pied.

Avec Windows, ça peut être difficile de reproduire un système sur une autre machine. Nous voudrons alors utiliser, au besoin, la fonction intégrée, qui se nomme le point de restauration. Elle est disponible depuis les Propriétés système, dans la section Protection du système.


Propriétés système
Nom de l'ordinateur
Matériel
Paramètres système avancés
Protection du système
Utilisation à distance
Utilisez la protection du système pour annuler toute modification système indésirable.
Restaurer le système
Vous pouvez annuler les modifications système en rétablissant l'ordinateur à un état antérieur en choisissant un point de restauration précédent.
Restauration du système...
Paramètres de protection
Lecteurs disponibles
Protection
Disque local (C:) (Système)
Désactivée
Configurez des paramètres de restauration, gérez l'espace disque et supprimez des points de restauration.
Configurer...
Pour créer un point de restauration, activez d'abord la protection en sélectionnant un lecteur et en cliquant sur Configurer.
Créer...
OK
Annuler
Appliquer

# HISTOIRE D'HORREUR #2
# UNE MANIPULATION DÉSASTREUSE SUR UN SERVEUR LINUX

Je valide ça ☑

service-conseil

# Une manipulation désastreuse sur un serveur Linux

**Niveau avancé**

Un serveur Linux est un environnement où la stabilité est très importante. Ceci s'observe notamment avec l'utilisation de distributions qui ont un cycle de développement et de test beaucoup plus long que celles qui sont employées pour la bureautique. Par exemple, Canonical, l'entreprise qui développe Ubuntu, offre maintenant une période de support de 10 ans.

Cette stabilité vient souvent avec des versions de logiciels qui plus anciennes, mais éprouvées. Il peut alors être tentant de mettre à jour certaines composantes d'un système afin de profiter des dernières nouveautés.

Cependant, dans un environnement de production, ce comportement met à risque le bon fonctionnement de l'ensemble des applications. De plus, la modification de fichiers importants peut mener à des erreurs difficiles à expliquer et même à la corruption du serveur. Dans ce cas-ci, il devient irrécupérable.

## Comment éviter cette histoire d'horreur ?

Voici quelques astuces pour prévenir la corruption d'un serveur ou pour en faciliter la reprise.

### Apprendre les bases du fonctionnement d'un système Linux

Les distributions de GNU/Linux sont le fruit de plusieurs décennies, avant même la création du noyau Linux par Linux Torvalds. La philosophie Unix, le mouvement du logiciel libre et les impératifs de stabilité en production ont dicté plusieurs normes. Celles-ci sont aujourd'hui centrales au bon fonctionnement des systèmes d'exploitation et de l'Internet, qui fonctionne principalement grâce à Linux.

C'est un domaine d'expertise beaucoup trop vaste pour en discuter en détail dans un livre électronique, mais, au moins, voici quelques thèmes importants à explorer !

— Le rôle du noyau Linux
— Le gestionnaire de paquetages
— Les fichiers de configuration
— Les services système et réseau

Le guide d'administration de Debian est disponible dans plusieurs langues et plusieurs formats. Il permet de couvrir l'ensemble de ces sujets, et bien plus !

— Debian Buster from Discovery to Mastery

### Bien comprendre le rôle de super utilisateur

Le rôle de super utilisateur sur Linux possède beaucoup plus de privilèges que sur un système Windows. Il peut vraiment tout faire ! Nous comprendrons par là qu'il peut supprimer ou écraser n'importe quel fichier, sans avertissement.

Lorsque nous souhaitons expérimenter avec une nouveauté, c'est fortement déconseillé de le faire en tant que super utilisateur. Il vaut mieux créer un rôle spécifique pour effectuer des tests.

### Installation d'une compilation manuelle dans un répertoire alternatif

L'installation manuelle de librairies se fait généralement en utilisant la séquence de commandes suivantes :

```
./configure
make
sudo make install
```

Si nous ne souhaitons pas briser l'organisation effectuée par le gestionnaire de paquetages, nous pouvons alors utiliser un répertoire d'installation différent de celui par défaut. Pour la configuration qui précède la compilation avec `make`, définissons un préfixe :

```
./configure --prefix=/répertoire/non/système/
```

L'utilisation de ce préfixe indiquera aux deux étapes suivantes de ne pas écrire dans les répertoires par défaut du système. Elles prendront plutôt celui qui a été spécifié. Ceci permettra d'éviter de nombreux conflits de versions.

### Librairies associées à un langage de programmation

Dans le cas de librairies associées à un langage de programmation en particulier, tel que Python, il est conseillé d'installer les versions qui ne sont pas déjà empaquetées par la distribution avec un rôle utilisateur régulier.

Pour simplifier, évitez l'utilisation de la première commande et privilégier la seconde le plus possible.

```
# à éviter
sudo pip install quelque chose
# à privilégier
pip install quelque chose
```

Ceci peut aussi se faire au sein d'un environnement virtuel tel que virtualenv.

### Utiliser les environnements virtuels tels que Docker

La virtualisation permet de partager des ressources entre les systèmes d'exploitation hôte et client, tout en conservant un niveau d'isolation élevé au niveau de la sécurité et du système de fichiers.

Le logiciel Docker crée des environnements d'exécution qui sont isolés, à l'exception du noyau, du processeur et de la mémoire. Il est possible de partager certaines ressources additionnelles, dont certains répertoires et le réseau informatique.

Il est idéal pour expérimenter et pour faciliter l'agilité dans le développement. Donc, c'est un outil tout indiqué pour tester de nouvelles idées sans mettre en péril la stabilité de son système.

Docker fonctionne maintenant sur Windows et macOS, mais il était à l'origine disponible uniquement pour le noyau Linux. Cependant, la prise en charge peut nécessiter des outils additionnels.

### Utiliser des captures incrémentales des fichiers système

Timeshift est une application Linux qui permet de faire des points de restauration. Elle tourne de la même manière que la fonctionnalité de Windows que nous avons présentée à la fin du chapitre précédent. À la différence d'une prise en charge complète des fichiers de la machine, cette application se concentre sur ceux du système d'exploitation uniquement.

Elle est simple à utiliser en mode graphique. Lors de son ouverture, elle demandera de sélectionner une méthode de sauvegarde, un disque où l'effectuer et la fréquence désirée. Enfin, il sera possible de créer le premier instantané, qui est le plus long à exécuter.


Sur un serveur, nous ne disposons habituellement pas d'une interface graphique. Nous utiliserons un terminal pour appeler l'application. Nous spécifions le disque de sauvegarde par son identifiant système.

```
sudo timeshift \
--create \
--comments "instantané initial" \
--tags D \
--snapshot-device/dev/sda1
```

## Trop tard… et maintenant ?

Une fois que le mal est fait, vous vous demanderez de quelles options vous disposez pour réparer un serveur corrompu. Malheureusement, si vous n'êtes pas préparés à cette situation, ça sera difficile. Voici deux possibilités.

Dans le premier cas, vous restaurez le paquetage brisé. Vous ne devez pas redémarrer avant la réinstallation du paquetage.

Dans le deuxième cas, vous devez envisager de ne plus pouvoir démarrer le système si la restauration échoue.

### Purger et réinstaller un paquetage système

Si le fichier corrompu peut être identifié et est relié à un paquetage de la distribution, en le purgeant et en le réinstallant, nous avons de bonnes chances de résoudre le problème. Cependant, s'il y a des dépendances, ça peut s'avérer un travail de recherche complexe. De plus, si le gestionnaire de paquetages utilise ce fichier, alors il ne sera pas possible de poursuivre.

### Restaurer une capture incrémentale antérieure

L'avantage de la méthode de la capture incrémentale, c'est qu'elle facilite grandement la restauration. Pour le faire avec Timeshift, il suffit d'exécuter cette commande :

```
sudo timeshift --restore
```

Le logiciel demandera quel instantané restaurer, puis proposera de mettre à jour le gestionnaire de démarrage GRUB, au besoin. En cas d'échec, il reste alors une seule solution, si vous avez accès physiquement au serveur, que nous verrons maintenant.

### La restauration depuis un système de secours

Les distributions Linux incluent souvent une image à télécharger de type "live session" qui permet d'en démarrer une version

complète sur son poste de travail et de l'essayer. Et ce, sans avoir à changer quoi que ce soit avant de faire l'installation. Celles-ci donnent aussi l'occasion aux utilisatrices et utilisateurs expérimentés de modifier un système d'exploitation existant sur un ordinateur, par la technique du changement de racine avec l'outil `chroot`.

Vous pouvez consulter un exemple pratique sur notre blog : Manjaro avec pilotes NVIDIA.

# HISTOIRE D'HORREUR #3
# UN VOL D'UNE SOURCE DE DONNÉES CONFIDENTIELLE

*Je valide ça* ☑

service-conseil

# Un vol d'une source de données confidentielle

**Niveau intermédiaire**

Un des pires scénarios qui peut subvenir dans une organisation, c'est de se faire voler une source de données confidentielles. En plus de devoir gérer le risque de fraude d'identité auprès de la clientèle ainsi que la perte de propriété intellectuelle, l'entreprise doit aussi rapidement se remettre sur pied, rétablir sa réputation et adopter de meilleures pratiques. Il y aura également une remise en question de la pertinence et de l'utilisation des données accumulées dans le passé.

Les principales causes d'un vol de données sont :

— L'infection par un maliciel de type rançongiciel. Nous avons couvert ce point dans le premier chapitre.
— L'intrusion depuis le réseau Internet par des menaces persistantes avancées.
— Une ou un membre du personnel mal intentionné qui obtient des privilèges par l'ingénierie sociale ou par la négligence.
— L'absence de sécurité adéquate dans l'infonuagique.
— La perte d'équipement informatique.

## Comment éviter cette histoire d'horreur ?

Nous voulons réduire le risque de vol d'une source de données confidentielles. Nous allons décrire quelques éléments nécessaires pour construire une bonne stratégie à ce sujet.

### Bien définir les rôles

Le premier élément, c'est de bien définir les rôles des employées et employés. Ils établissent un groupe de tâches nécessitant, pour leur réalisation, l'utilisation d'un sous-ensemble de données. Ce modèle de gestion se nomme le contrôle d'accès basé sur les rôles, rencontré sous l'acronyme RBAC.

Il faut aussi différencier l'utilisateur du rôle. Le premier permet l'identification et l'authentification auprès d'un système informatique. Il est souvent combiné à un mot de passe. C'est celui qui est entre autres demandé pour ouvrir une session sur l'ordinateur. Le second ne détient pas ces capacités. Cependant, il possède des droits d'accès aux données et d'exécution de certains logiciels.

Chaque utilisateur peut avoir un ou plusieurs rôles. Dans les meilleures pratiques, elles et ils n'en ont qu'un seul à la fois, ce qui permet d'éviter les croisements de données de différentes sources.

Une liste minimale pourrait être :

— Conseil d'administration
— Gestion
— Service informatique
— Service comptable
— Ressources humaines
— Service à la clientèle
— Approvisionnement
— Ventes

### Contrôler l'accès aux données

Voici le second élément de notre stratégie. Nous allons définir, pour chacun des rôles, à quoi ils devraient avoir accès.

Dans une entreprise de distribution, les équipes sur la route ne devraient utiliser seulement les données de la clientèle située sur leur territoire. Nous effectuons donc un filtrage en utilisant la géolocalisation. C'est une forme de gestion des accès basée sur les enregistrements.

Dans un autre scénario, nous nous intéressons au service téléphonique. Son personnel ne devraient pouvoir consulter que les renseignements qu'ils ont droit de divulguer à la clientèle par la voix. Les informations qui sont communiquées entre les systèmes doivent être cachées. Par exemple, ils ne devraient pas avoir accès aux champs contenant les numéros de carte de crédit ni aux mots de passe. C'est ici une forme de gestion des accès basés sur les attributs.

Enfin, lorsque nous devons appliquer des restrictions à la fois sur des enregistrements et des colonnes, il peut être utile de créer des vues. Ce sont des requêtes formatées aux besoins du rôle et présentées sous la forme de tables.

### Utiliser le masquage de données

La réalité du monde de l'entreprise, c'est qu'il n'y a pas de solution universelle.

Parfois, certains processus d'affaires requièrent de voir les vraies données. Par exemple, les conseillères et conseillers des ressources humaines nécessitent d'accéder à des informations médicales ou des numéros d'assurance sociale.

De nombreux rapports et systèmes dérivés consomment des bases de données existantes, qui ne pourraient pas facilement être recréées avec les principes de gestion des accès que nous avons présentés ci-dessus. Nous ne voulons pas tout recommencer !

Un autre aspect à considérer : en certains cas, seule une partie du champ contient de l'information sensible. Les six premiers chiffres d'une carte de crédit décrivent l'émetteur, alors que les trois premiers caractères du code postal canadien identifient une ville ou un quartier.

Dans ces situations, nous aurons alors recours à une méthode de

masquage des données. Celle-ci permet de cacher, partiellement ou complètement, les informations d'un champ.

Voici quelques exemples :

— Une adresse courriel apparaît sous la forme suivante : `xxx@domaine.com`
— Arrondir une date de naissance au mois près : `2000-04-00`
— Substituer les noms de famille par des personnages de dessins animés : `François Superman`
— Un numéro de carte de crédit présente seulement les 4 derniers chiffres : `XXXX XXXX XXXX 1234`

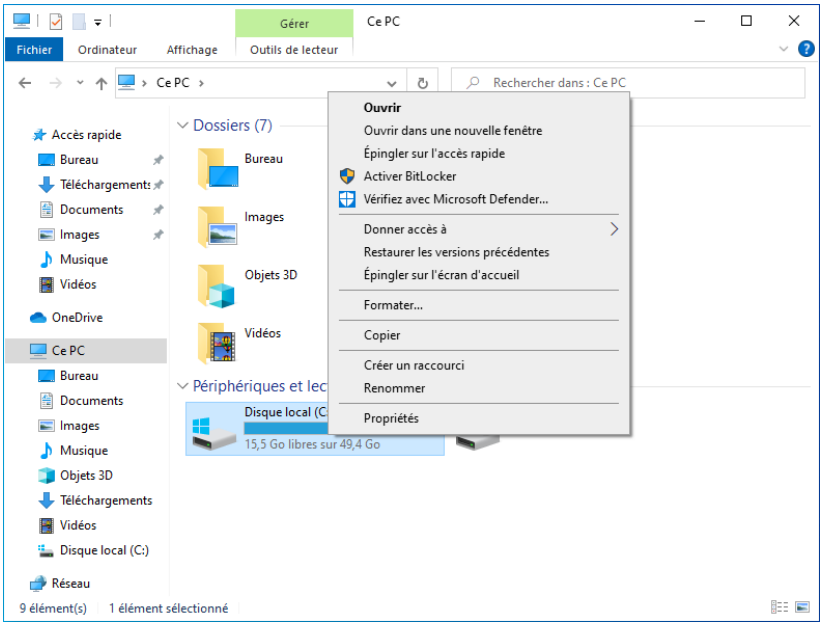
### Chiffrer les disques durs

Enfin, voici une dernière stratégie, qui cherchera à contrer les impacts du vol d'ordinateurs ou de disques.

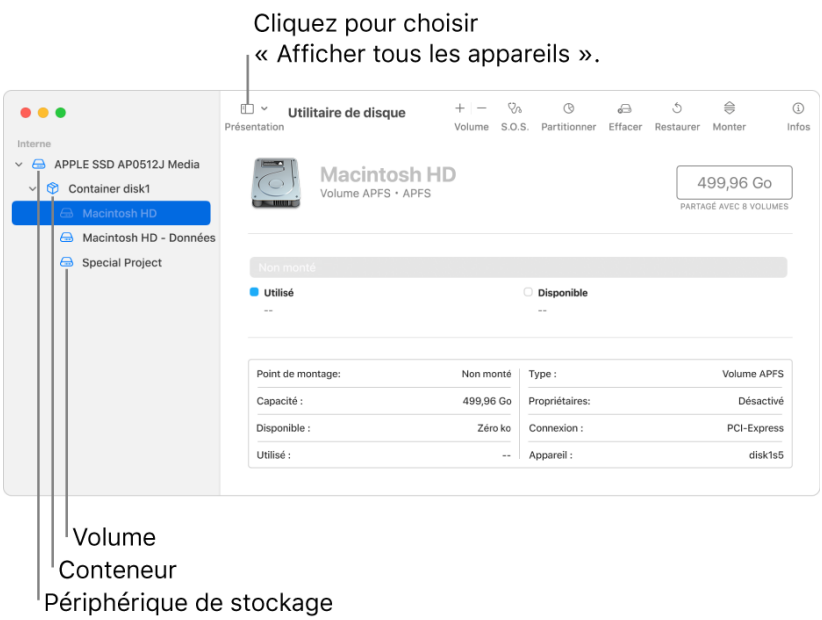
Lors de l'installation du système d'exploitation, il est généralement possible d'activer le chiffrement des partitions du disque dur, afin qu'un mot de passe soit demandé au démarrage. Ceci se fait en utilisant Linux Unified Key Setup et dm-crypt.

De plus, lors de l'utilisation d'un nouveau disque dur ou stockage SSD, il est possible de mettre en place la même stratégie.

Sur Windows, la fonctionnalité se nomme BitLocker et elle se trouve en cliquant sur l'icone du disque avec le bouton droite de la souris.

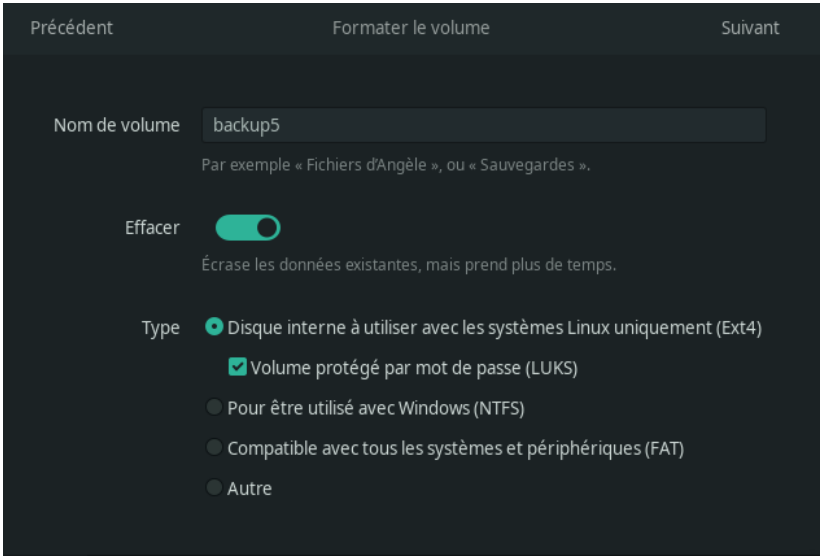


Sur Mac, dans l'application Utilitaire de disque, cliquer sur Afficher tous les appareils depuis le bouton Présentation. Les instructions détaillées sont disponibles sur le site de Apple

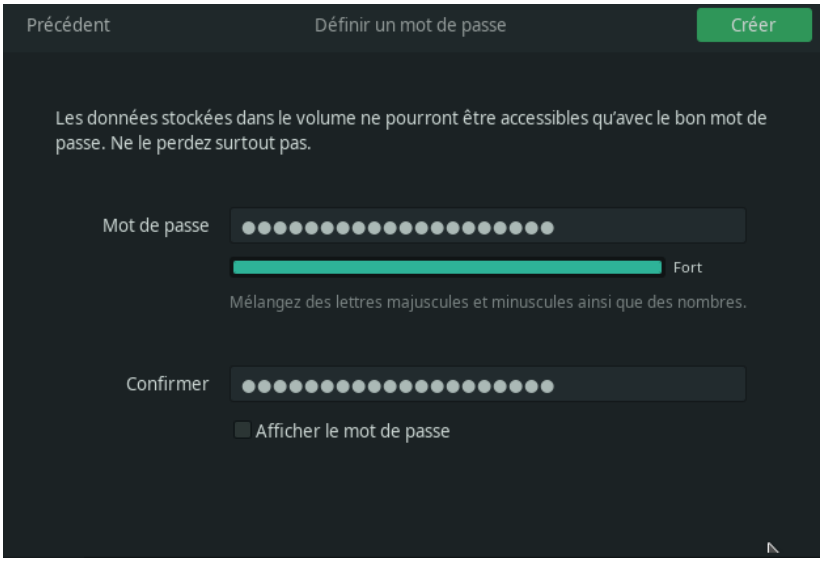


Sur les différentes distributions Linux, il y a généralement un utilitaire graphique de gestion des disques tel que le GNOME Disk Utility qui permet de facilement effectuer le chiffrement des disques externes.

Lors de la connexion d'un nouveau disque, on crée une nouvelle partition.




Ensuite, nous saisissons le mot de passe qui protégera le disque.


Précédent
Définir un mot de passe
Créer
Les données stockées dans le volume ne pourront être accessibles qu'avec le bon mot de passe. Ne le perdez surtout pas.
Mot de passe
Fort
Mélangez des lettres majuscules et minuscules ainsi que des nombres.
Confirmer
Afficher le mot de passe

## Trop tard… et maintenant ?

Tout comme avec l'attaque par rançongiciel, si elle a pu être détectée immédiatement, les premières étapes sont : limiter les accès réseau, couper l'Internet et aviser les autorités publiques.

Si l'incident a eu lieu il y a plus d'une journée, c'est vraiment trop tard pour contrer la diffusion des renseignements sur le web profond. C'est plutôt le temps de repenser sa stratégie de gestion des données et de mettre en oeuvre les conseils de ce guide. Laissez les spécialistes en cybersécurité et la police s'occuper du reste et collaborez avec ces derniers.

Le moment venu, informez le public de l'incident que vous avez vécu et des actions que vous avez entreprises pour améliorer votre sécurité.

Nous souhaitons trouver le bon équilibre dans l'utilisation de toutes les méthodes de prévention. Nous devons donc considérer que c'est toujours un compromis entre la protection de la confidentialité, de la vie privée et la valeur de la donnée qui est accessible pour analyse.

La sécurité est un exercice de gestion de risques, et lorsque les incidents se produisent, c'est souvent mieux regarder en avant et se préparer pour la prochaine fois.

# HISTOIRE D'HORREUR #4

# IMPOSSIBLE D'ACCÉDER À UNE PLATEFORME EN LIGNE


*Je valide ça* ☑

service-conseil

# Impossible d'accéder à une plateforme en ligne

**Niveau accessible**

Les réseaux sociaux et les plateformes logicielles en ligne sont devenus essentiels dans bien des organisations. Cependant, est-ce qu'ils passeront l'épreuve du temps ? Par exemple, Google, au fil des années, a suspendu plusieurs dizaines de services. Nous invitons à consulter à ce sujet le site Killed by Google qui les recense. Chaque mois, un logiciel-service est interrompu ou racheté.

Une autre possibilité, qui vise particulièrement les activistes et les personnes marginalisées, survient lorsque la plateforme supprime ou bloque des comptes.

Ça se fait souvent par des groupes organisés qui veulent censurer une utilisatrice ou un utilisateur. Le niveau de discernement des algorithmes pour reconnaître le bon sens est très limité. Dans certains cas, la motivation de leurs créateurs, c'est optimiser le profit, coûte que coûte. Donc, votre compte peut être rendu inaccessible un peu n'importe quand pour des raisons arbitraires.

De plus en plus, les frais mensuels des logiciel-services explosent, étant donné la dépendance induite par leur modèle d'affaires. Ce concept se nomme l'enfermement propriétaire. L'interface de gestion de réseaux sociaux Hootsuite a augmenté ses prix de plusieurs multiples tout récemment. Ils demandent maintenant 49 $ pour un abonnement qui coûtait 4 $ avant juin 2021.

D'autre part, Microsoft a annoncé en septembre 2021 une hausse de prix de plus de 30 % par compte pour certains forfaits bureautiques.

Vous devez donc vous préparer à ces imprévus.

## Comment éviter cette histoire d'horreur ?

Voici quelques moyens pour diminuer les inconvénients si un des scénarios précédents se produit. Malheureusement, dans ce cas-ci, nous ne pouvons pas y faire grand-chose, étant donné que nous ne contrôlons pas ces plateformes-là.

### Éditer son propre site web

Un premier geste : s'offrir un camp de base pour ses activités. Éditer son propre site web, gérer ses contenus et sa visibilité comporte de nombreux avantages.

Tout d'abord, même si les pannes et les corruptions de systèmes existent, elles se raréfient et une restauration complète se fait avec un bon taux de réussite. Nous avons vu comment faire au second chapitre.

Puis, notre site web permet d'offrir de référence pour votre clientèle et votre communauté, s'ils n'utilisent pas eux-mêmes les réseaux sociaux. Avec la prise de conscience des risques et enjeux de ces derniers, les gens les consulteront de moins en moins dans les prochaines années, au profit d'alternatives plus éthiques et moins chronophages, tels que ceux basés sur ActivityPub.

Enfin, n'oublions pas que le contenu de votre site web est à l'abri des manipulations par les algorithmes des géants du web. Les internautes ont accès à tout, en tout temps. La seule exception, c'est si vous décidez de mettre des articles restreints !

### Sauvegarder ses données de contact et ses contenus

Les réseaux sociaux offrent des fonctions pour exporter vos données de contact et une partie des contenus textuels que vous avez publiés.

Profitez-en pour créer une sauvegarde à un intervalle régulier, disons une fois par mois. Généralement, le délai d'attente est de quelques jours, et vous recevrez un lien par courriel pour récupérer l'archive de votre compte.

Tout le contenu visuel (images, vidéos) que vous avez publié sera difficile à récupérer. Nous allons alors recommander une autre

tactique.

Si vous créez votre matériel depuis une plateforme en ligne telle que Canva, assurez-vous de tout télécharger sur votre ordinateur avant de publier, pour détenir un exemplaire local. Puis, mettez en oeuvre une stratégie de sauvegarde adéquate.

C'est votre identité marketing, il vaut cher et vous y avez consacré beaucoup de temps !

### Utiliser un lien statique pour lister ses comptes de réseaux sociaux

Une dernière astuce pour la route ! En plus de votre site web personnel, il peut être utile de se créer une page de liens accessible et bien référencée. Un exemple de service qui le permet est Link-Tree.

## Trop tard… et maintenant ?

### Panne de réseau social

Votre principale plateforme de réseautage est-elle soudainement en panne ? Redirigez votre communauté vers votre site web en leur envoyant une communication par courriel à cet effet. Profitez-en pour inviter les membres de celle-ci à se connecter à vos autres espaces en partageant votre lien statique.

Les pannes des grands réseaux sociaux sont surtout liées à des erreurs des systèmes informatiques. Ce qui les rend temporaires. Un des enjeux qui prolongent les délais, c'est la synchronisation des noms de domaines, le fameux système DNS, qui peut prendre entre 24 et 48 heures.

Bref, soyez patients !

### Blocage du compte

Un compte bloqué est difficile à récupérer, et bien honnêtement, ce n'est pas du tout notre expertise. Commencez tout d'abord par informer votre liste de diffusion par courriel et sur la page d'accueil de votre site web.

Si vous avez téléchargé vos données de contact, vous disposerez d'au moins un autre moyen de les contacter, soit par courriel, soit sur un autre réseau social. Généralement, nous reprenons les mêmes pseudonymes d'un endroit à un autre, donc ça vaut la peine d'essayer.

Assurez-vous d'avoir accès à votre copie locale de vos contenus, et profitez-en pour les partager sur une nouvelle plateforme !

### Fermeture d'un logiciel-service

Votre logiciel-service (en anglais, un SaaS) préféré ferme ses portes. C'est bien dommage, mais c'est un des enjeux les plus importants dans le domaine de l'autonomie numérique. Assurez-vous de récupérer le plus possible de vos données en utilisant les fonctions d'exportation ou les interfaces de programmation disponibles.

Dans un scénario idéal, nous recourrons aux services d'une tierce partie qui se chargera de transférer toutes les données pour vous.

Si vous vous préparez à prendre davantage d'autonomie, c'est peut-être le bon moment de songer à l'autohébergement de certaines applications ! De plus en plus de logiciels de qualité peuvent remplacer les solutions privatives populaires du marché.

# À propos de Je valide ça, service-conseil

Ma mission est de développer l'autonomie numérique des PME innovantes et des citoyens engagés par la formation et l'accompagnement en stratégie de données et en technologie libre.

Ma clientèle cible, ce sont les entreprises et organismes comme le vôtre qui veulent rendre notre société plus autonome, responsable et résiliente. Bref, si vous avez des objectifs ESG ambitieux, je peux vous donner les moyens de les mesurer et de les atteindre !

Vous voulez améliorer votre usage de la technologie en développant le potentiel créatif de vos employées et employés.

J'offre de la formation sous différents modes de prestation pour m'adapter à vos besoins. Que ce soit en mode autodidacte, en vidéoconférence ou en salle, je suis à l'écoute de vos besoins.

Je valide ça, service-conseil a été fondée par moi-même, François Pelletier, en août 2021 pour combler le besoin d'expertise en stratégie de données dans les entreprises, sans devoir recruter une licorne rose.

**Un accompagnement en entreprise qui se distingue**

- Gestion du cycle de valorisation des données avec des outils tels que les
  - systèmes de gestion de bases de données
  - langages de programmation R et Python.
  - systèmes d'information géographiques.
  - plateformes infonuagiques.
- Systèmes de collaboration sécuritaires avec Nextcloud et Yunohost (Debian Linux).
- Autonomie numérique avec le logiciel libre et les serveurs Linux (Debian, Ubuntu et CentOS).
- Automatisation de tâches répétitives avec des langages de script et des algorithmes d'intelligence artificielle

**Une offre de formation de grande qualité**

Je n'aime pas faire les choses à moitié, alors vous recevez une formation qui développera vos compétences avec des cas réels, avec de vraies données et des exemples faciles à mettre en pratique.

Vous découvrirez tout le potentiel de technologies phares basées sur le logiciel libre et un esprit de collaboration sans pareil.

Juste assez de théorie pour parler le même langage, et on passe immédiatement à la pratique pour résoudre vos enjeux actuels, à votre échelle et à votre rythme d'apprentissage.

**Le coffre à outils**

— Le langage de programmation R
— La base de données PostgreSQL et son extension géospatiale PostGIS
— Le langage de programmation Python
— Le système d'exploitation Debian et l'environnement d'administration Yunohost
— L'application d'auto-hébergement et de collaboration Nextcloud
— Et bien plus …

**Me contacter**

— LinkTree
— Site web
— Courriel
— LinkedIn
— Instagram
— Twitter