La sécurité informatique

« La sécurité n'est pas un produit, c'est un processus »
(mot d'ordre de la distribution OpenBSD)

Le concept de sécurité informatique englobe une plus grande quantité de domaines, usages et implications qu'on ne pourrait le croire au premier abord, quand les éléments les plus marquants mis en avant dans les médias sont des attaques virales et les campagnes de piratage.

Nous verrons ici quelques concepts de base de la sécurité informatique, ainsi que quelques bonnes pratiques pouvant aider à se protéger des problèmes.

La sécurité informatique, c'est avant tout la sécurité des données.

En informatique, on divise les entrées et sorties possibles d'un système *(un ordinateur)* entre 2 grandes catégories basiques depuis ses débuts : **les programmes** et **les données**.

- Les **programmes** sont un ensemble d'algorithmes, c'est-à-dire d'instructions à suivre dans un certain ordre pour obtenir un résultat voulu *(voyez cela comme une recette de cuisine, tout simplement)*

- Les **données** sont des informations sur lesquelles on fait travailler les programmes, afin d'obtenir les résultats espérés.

Dès lors, même si la sécurité des programmes est importante, elle s'efface rapidement face à celle des données : si un programme n'est pas sécurisé *(c'est-à-dire qu'on ne peut pas assurer que ses résultats seront conformes à ce qu'il dit faire)*, on peut le remplacer, **mais des données sont bien moins remplaçables !**

Mais qu'est-ce que la sécurité ou la sécurisation des données ?

On parle de données sécurisées quand on peut s'assurer des paramètres suivants à leur sujet :

- Leur **accessibilité** : pouvez-vous accéder à vos données quand vous le désirez ?

- Leur **confidentialité** : les personnes autorisées sont-elles les seules à pouvoir y accéder ?

- Leur **intégrité** : ces données sont-elles exactes et complètes ? Peut-on assurer qu'elles n'ont pas été modifiées par une tierce partie non autorisée à le faire ?

- Leur **traçabilité** : pouvez-vous savoir qui les a modifiées et quand ?

Ces paramètres impliquent aussi d'autres concepts, comme l'imputation / non répudiation *(aucun utilisateur ne doit pouvoir contester les opérations qu'il a ni s'attribuer les actions d'un autre utilisateur)*, ou la garantie de l'authenticité d'un utilisateur et de ses accès.

La sécurité informatique, ce n'est pas se dire « est-ce que Si ? », mais « Quand ça va… »

Avec l'interconnexion moderne des systèmes d'information, nous sommes tous soumis au risque de voir nos systèmes informatiques et données être corrompus ou piratés, mais tout comme nous sommes tous au risque d'un accident, d'un cambriolage ou autre, il s'agit de savoir simplement équilibrer probabilité d'un problème et début de paranoïa…

Et il ne s'agit pas que de piratage ou de virus, un simple disque dur tombant en panne peut aussi vous faire perdre beaucoup !
(Pour tout dire, beaucoup d'experts s'accordent pour dire que les problèmes de piratage représentent en gros 10% des soucis de sécurité informatique !).

La sécurité informatique se base sur **2 principes** simples : **limiter les accès** possibles avant tout problème, **atténuer les conséquences** lors de la survenue d'un problème.

(Tout comme un bon système de sécurité domestique joue sur ces 2 tableaux : limiter l'accès et ralentir les attaques)

Quelques exemples non exhaustifs de problèmes liés à la sécurité informatique :

- Perte de données *(votre ordinateur lâche, adieu 2 ans de travail et les photos de famille !)*
- Modification / effacement de vos données à votre insu *(pas forcément un pirate, mais parfois juste un membre de la famille qui veux « faire du ménage »…)*
- Perte de vos identifiants *(impossible de reconnecter sur votre ordinateur, votre téléphone, votre compte sur un site…)*
- Destruction de votre machine *(casse du mobile, perte de l'ordinateur dans un feu… Soyons imaginatifs, ou pas !)*
- Accès non autorisé à vos identifiants *(« piratage », ou le vieux gag de l'email resté ouvert… Bonjour les mails inconvenants envoyés à des collègues ! 0_0°)*

Mais surtout, **PAS DE PANIQUE !** Quelques connaissances, un peu de bon sens et un plan d'action prévu à l'avance suffisent souvent à s'en sortir.

Quelques idées de « Niveaux » à remplir pour se tranquilliser…

Niveau 1 : la sécurité « Physique » ou d'accès aux machines

Quelques bonnes idées à suivre :

- Le mot de passe / code Pin *(un peu contraignant oui, mais tellement efficace…)*
- Au travail, verrouiller sa session quand on part de son poste pour un moment *(sinon gare au gag du Goatse O_o°°°)*
- Se méfier un peu *(mais pas au point de la paranoïa)* d'un support externe inconnu *(clé USB, disque dur…)*

Niveau 2 : Sécurisons les programmes

- **METTRE - A - JOUR** ! Que ce soit son système d'exploitation ou ses programmes : plus on bouche de trous par ces mises à jour, plus on s'assure de limiter les portes d'entrée ! *(pas besoin de prendre peur, jetez y un œil une fois par mois en gros !)*

- **Choisir des logiciels sécurisés** : Open source, reconnus, ou si on fait le choix de logiciels propriétaires, se les procurer auprès des concepteurs !
  Le Warezz et les générateurs de clés sont de bons moyens d'infecter des machines.

- **Connaitre un peu les limitations de sécurité de nos systèmes** : il y a-t-il besoin d'installer un antivirus, un pare feu informatique, etc. ?
  Exemple : antivirus indispensable sous Windows, mais plus optionnel sous Linux…

Un petit truc : Savez-vous ce qu'est un ordinateur parfaitement sécurisé ?
-> C'est un ordinateur sans réseau informatique, débranché de l'électricité, éteint et enfermé dans une pièce blindée fermée à double tour…

Niveau 3 : sécurisons les accès

- Une idée simple : **1 utilisateur** sur la machine familiale = **1 compte séparé**. De cette manière, chacun gère ses fichiers dans son dossier limité et personnel.

- **Un compte utilisateur séparé pour l'administrateur**, qui ne soit pas le compte principal d'un des utilisateurs !
  « l'erreur est humaine, la catastrophe nécessite le mot de passe Root… »

- Ne pas hésiter à utiliser un logiciel de **contrôle parental** pour les enfants : on peut limiter leurs accès, les logiciels & sites qu'ils peuvent utiliser jusqu'à ce qu'ils apprennent à faire attention par eux même.

- Mettre en place un contrôle par DNS menteur comme les solutions familiales de OpenDNS / Umbrella peut aussi aider à limiter les sites par lesquels des accès non autorisés peuvent arriver…

- **Ne pas utiliser le même mot de passe partout !**
  C'est tentant parce que ça fait moins de mots de passe à se souvenir, mais si jamais un service utilisant votre couple « identifiant » + « mot de passe » habituel est piraté, les pirates vont simplement essayer de manière automatique ce couple d'identification sur tous les sites qui les intéressent…
  La plupart des systèmes et navigateurs modernes proposent des fonctions de gestion de mot de passes forts et de synchronisation des données, profitez-en !

Niveau 4 : Sécurisons nos données

- **Ne pas mettre tous ses œufs dans le même panier** : ne pas laisser toutes vos données sur une seule machine, préparez des sauvegardes ! Ayez un disque dur externe, voire plusieurs selon les usages *(par exemple, un pour les photos / films, un pour les données professionnelles…)*

- **Faites ces sauvegardes !**
  Il ne sert à rien d'avoir un disque de sauvegarde s'il reste dans sa boite… Vous pouvez vous mettre en place un calendrier simple de sauvegarde, selon vos usages *(pas obligé de sauvegarder toutes les semaines si vous n'avez pas un volume de données énorme à traiter chaque jour par exemple…)*

- **Sauvegardez aussi votre système d'exploitation !**
  Tous les OS modernes proposent des systèmes de sauvegarde automatisée de votre système, souvent par le biais d'images crées automatiquement à intervalles réguliers.

- **Pour vos données les plus importantes** *(codes administratifs, informations personnelles…)*, une petite sauvegarde séparée peut être intéressante *(dans un partage en ligne type Cloud par exemple, la plupart des fournisseurs proposent des comptes gratuits de quelques gigas de données… Si vous avez peur qu'ils y jettent un œil, ajoutez du chiffrage !)*.
  N'hésitez pas si vous psychotez un peu à entreposer des documents de ce genre auprès de votre banque par exemple, ou d'un tiers de confiance.
  Ou pourquoi pas un petit coffre / une armoire résistant au feu !

Niveau 5 : Ça vient de chier dans la colle. Ayez un plan.

Encore une fois, il ne s'agit pas de savoir « si » ça va arriver, mais de « quand » ça va arriver.

Posez-vous juste la question suivante : en cas de problèmes, est ce que je peux récupérer facilement mes données et recommencer à utiliser mon matériel rapidement ?

- Ou sont mes dernières sauvegardes, de quand datent elles ?
- Est-ce que j'ai une sauvegarde système quelque part ?
- Quels sont les logiciels dont j'ai besoin pour reprendre le travail rapidement ?
- Ou sont enregistrés mes mots de passe ?
- Si je dois changer de matériel, mes logiciels seront-ils compatibles ?

Si vous avez planifié et fait vos sauvegardes, que vous savez où récupérer vos données importantes et mots de passe, vous pourrez garder la tête froide en cas de problèmes !