le cnam

Hygiène informatique

https://securite-informatique.cnam.fr,
Responsable de la Sécurité des Systèmes
d'Information,<rssi@cnam.fr>

La sécurité informatique repose essentiellement sur trois principes :

- **Confidentialité** : seules les personnes autorisées peuvent accéder aux données.
- **Intégrité** : les données restent utilisables, sans altération malveillante ni accidentelle.
- **Disponibilité** : les données sont accessibles.

Mots de passe

Le mot de passe est le premier mécanisme de sécurité, il permet d'assurer la **confidentialité** des données. Associé à un nom d'utilisateur (aussi appelé identifiant ou *login*), il permet d'assurer l'**authenticité** de cet utilisateur, de prouver son identité.

1. Les meilleurs mots de passe sont générés aléatoirement.
2. Chaque mot de passe doit être unique.
3. Un mot de passe est secret et doit le rester.

En 2024, un mot de passe doit contenir :
- des lettres et des chiffres,
- des majuscules et des minuscules,
- au minimum douze caractères.

Comptes

- Les comptes d'accès aux ordinateurs, applications métiers, etc., doivent être protégés par mot de passe.

— À chaque compte son mot de passe : un mot de passe ne doit jamais être réutilisé pour plusieurs comptes. Si l'un était compromis, ils le seraient tous.
— On ne donne jamais son mot de passe, à personne, pas même à un service informatique, sous aucun prétexte : il est **incessible**.

Pour gérer et protéger ces nombreux de mots de passe, **utiliser un gestionnaire de mots de passe**. Un gestionnaire de mots de passe stocke les mots de passe dans un conteneur, conteneur chiffré avec un « mot de passe père ». Il suffit alors de retenir ce mot de passe pour accéder aux autres. Par exemple, le logiciel *KeePassXC* (`https://www.keepassxc.org`) est disponible sur plusieurs plates-formes (Android, iOS, Linux, macOS, Windows).

Phishing, hameçonnage

Le *phishing* ou hameçonnage consiste à extorquer identifiant et mot de passe par malice. Le plus souvent, la communication commence par un mail (spam) ou un SMS, mais tout autre canal de communication convient.

91 % des attaques réussies actuellement commencent par un hameçonnage.

Données

Il y a essentiellement deux types de catastrophes pour les données : la divulgation et la perte.

Toutes les données n'ont pas la même importance. Pour les protéger efficacement, il faut les classer suivant leur importance, suivant l'impact de leur perte ou de leur divulgation.

— Pour rester confidentielles, les données doivent être **chiffrées**.
— Pour être accessibles, les données doivent être **stockées sur un support fiable**.
— Pour se protéger de la perte ou de la corruption, les données doivent être **sauvegardées**.

Chiffrement des fichiers

La cryptographie est la science du chiffrement. Le chiffrement rend les données incompréhensibles à quiconque ne dispose pas de la clef de déchiffrement (le plus souvent un mot de passe).

Pour chiffrer facilement des fichiers, on pourra utiliser :

- *PeaZip* pour quelques fichiers (`https://peazip.github.io/`).
- *VeraCrypt* pour une clef USB ou un disque portatif (`https://www.veracrypt.fr/`).

Stockage

Un support de stockage, surtout s'il est mécanique, peut tomber en panne. Un support, surtout s'il est portatif, peut être perdu ou volé. Une donnée **doit toujours être stockée sur trois supports distincts**, évidemment pas au même endroit.

Un support de stockage peut être volé ou égaré, il **doit toujours être chiffré**. Une solution native de chiffrement des disques est disponible sur Linux (*LUKS*), sur macOS (*FileVault*) comme sur Windows (*BitLocker*), mais elles ne sont pas compatibles entre elles. Pour une solution portable, utiliser *VeraCrypt*.

Sauvegarde

La sauvegarde permet de récupérer une ancienne version d'un fichier corrompu ou supprimé. La sauvegarde n'est donc pas une simple copie.

Une solution native de sauvegarde (chiffrées évidemment) est disponible sur macOS (*TimeMachine*) comme sur Windows. Sur Linux, il en existe de nombreuses, dont *DejaDup*.

Transport

Les clefs USB et autres disques portatifs présentent plusieurs risques pour la sécurité s'ils sont utilisés sans précautions :

- Ils sont facilement perdus ou dérobés tandis qu'ils peuvent contenir des données sensibles.
- Les périphériques USB en eux-mêmes peuvent être dangereux : certains sont conçus pour griller les ordinateurs auxquels ils sont branchés.
- D'autres sont conçus pour se faire passer par ce qu'ils ne sont pas : clavier, souris...
- Ils peuvent contenir des logiciels malveillants.

Pour ces raisons, on ne branche jamais une clef USB inconnue sans l'avoir vérifiée. Une borne antivirus est située à l'entrée du 292 rue Saint-Martin à cet effet. Il en va de même pour les disques durs portatifs.

Lorsque les données transitent à travers un réseau, elles doivent évidemment être chiffrées (HTTPS, VPN, SSH...).

Partage de données

Les envois de secrets par courriel sont à proscrire. Utiliser plutôt `https://cnambox.cnam.fr/versatile` pour déposer le secret à partager et ajouter le lien vers le secret dans le corps du message.

Il existe un espace de stockage limité en taille, mais personnel « à la Dropbox » : `https://cnambox.fr/drop`. De même, pour les envois de documents sensibles, utiliser `https://cnambox.cnam.fr/wecnam`, comparable à weTransfer.

Sur son ordinateur

- Toujours avoir un antivirus activé et à jour.
- Toujours activer l'authentification sur les équipements, rien ne devrait être accessible sans mot de passe.
- Appliquer les mises à jour logicielles dès que possible (et désinstaller tous les logiciels inutiles).

— Utiliser un pare-feu (*firewall* en anglais) pour limiter les connexions réseau au strict nécessaire.
— Ne se connecter qu'aux réseaux Wi-Fi de confiance (au premier rang desquels `eduroam`), éviter les réseaux Wi-Fi publics. Utiliser le VPN chaque fois que c'est possible.
— N'activer le Bluetooth que si c'est absolument nécessaire, l'arrêter dès que possible.
— Ne connecter des périphériques USB qu'avec une extrême prudence.
— Bien séparer les usages personnels et professionnels.
— Ne jamais laisser un équipement informatique sans surveillance (dans une voiture, dans le coffre-fort d'un hôtel...).
— En cas de perte ou vol d'un équipement (téléphone, ordinateur, clefs/disques contenant des données sensibles), informer la hiérarchie et le RSSI.

Sur son ordinateur :

— Le compte utilisé au quotidien ne doit pas avoir de droit d'administration.
— Après plusieurs minutes d'inactivité, la session doit se verrouiller automatiquement.
— Créer un compte nominatif par utilisateur, chacun leur mot de passe.
— Après plusieurs tentatives de mots de passe, verrouiller le compte.

NB : un smartphone est un ordinateur comme un autre.

VPN

Le Cnam fournit un accès sécurisé à ses réseaux et ses ressources, mais aussi à Internet, depuis l'extérieur par VPN : `https://vpn.cnam.fr/`.

Lorsque la connexion VPN est activée, les connexions Internet passent par le réseau du Cnam et sont chiffrées entre le poste de travail et le réseau du Cnam. Ainsi :

— Les communications sont confidentielles, au moins entre le poste de travail et le réseau du Cnam.
— Les équipements de sécurité du Cnam protègent le poste des contenus malveillants ou frauduleux.

Recommandations

— Avoir des mots de passe robustes et utiliser un gestionnaire de mots de passe.
— Chiffrer les disques des ordinateurs portables, les disques portatifs, les clefs USB.
— Installer sur son ordinateur et sur son téléphone les dernières mises à jour.
— Avoir un antivirus à jour.
— Avoir un compte nominatif sur son ordinateur, sans droits d'administration.

En cas d'urgence !

Si un ordinateur est infecté par un virus, il faut l'isoler urgemment : le débrancher de tous les réseaux (filaire, Wi-Fi, GSM, Bluetooth), débrancher les supports de stockage (clefs USB, disques portatifs). S'il s'agit d'un rançongiciel, le mieux est d'éteindre l'appareil au plus vite pour limiter le nombre de fichiers inutilisables. Relancer l'ordinateur risque de relancer le processus de chiffrement des fichiers par le rançongiciel !

Si un compte est compromis, changer le mot de passe depuis une machine saine. Si le mot de passe est utilisé pour d'autres comptes (ça ne devrait jamais être le cas), renouveler le mot de passe partout où il était utilisé.

Si l'identifiant est une adresse mail, s'assurer que le compte mail est sain ; par précaution, il est conseillé de changer le mot de passe du compte de messagerie aussi.

Prévenir le RSSI de l'incident et des mesures prises.

Pour en savoir plus...

Consulter régulièrement le site du RSSI du Cnam : `https://securite-informatique.cnam.fr`.