VOL / PERTE D'UN PC PORTABLE, D'UN SMARTPHONE OU D'UNE TABLETTE – REFLEXES

OBJECTIFS DE L'ATTAQUE

L'objectif peut être de récupérer des informations sensibles/confidentielles à des fins malveillantes.

Il peut toutefois s'agir d'un vol opportuniste ne ciblant pas précisément le contenu de l'équipement[1].

RISQUES

- ➔ **VOL DE DONNEES SENSIBLES/CONFIDENTIELLES**
- ➔ **PERTE DEFINITIVE DE DONNEES (SI ABSENCE DE SAUVEGARDE)**
- ➔ **PERTE FINANCIERE**
- ➔ **PREPARATION D'ATTAQUE CIBLEE**

LES BONNES PRATIQUES

- **Rester vigilant : ne pas laisser votre équipement sans surveillance notamment dans des lieux publics**
- **Utiliser un mot de passe fort et toujours verrouiller sa session en cas d'absence**
- **Chiffrer les données sensibles avec un outil dédié**
- **Sauvegarder les données sur un autre support**

EN CAS DE VOL/PERTE D'EQUIPEMENT[1] CONSTATE, CERTAINS POINTS SONT A CONSIDERER :

- **Le contenu de l'équipement[1] était-il chiffré ?**
  - Si aucune solution de chiffrement n'a été implémentée, il faut considérer que toutes les informations sont potentiellement accessibles
  - Si seulement certains dossiers ont été chiffrés, il est possible de récupérer des données sur l'architecture du système et des informations d'authentification (selon le type de chiffrement)

- **Le compte utilisateur est-il potentiellement compromis ? (ex. login et/ou mot de passe stocké sur le système, ou dans la sacoche, etc…)**

- **Y-a-t-il des données sensibles stockées (données à caractère personnel (patients, personnels), données de gestion de la structure, etc.) ? Si oui, réaliser l'inventaire des données présentes :** Informations liées à l'authentification (messagerie, accès à distance, comptes Windows, etc.)
  - Informations personnelles (historique des conversations/navigation web, gestion des fichiers, etc.)
  - Architecture interne (configuration réseau, serveurs logiciels utilisés politiques et outils de sécurité mis en place, etc.)
  - Données liées à la vie professionnelle

QUOI FAIRE

- Prévenir le service informatique de votre structure ainsi que son responsable hiérarchique
- Changer tous vos mots de passe, en particulier ceux concernant la messagerie électronique, les comptes de connexion à distance (VPN, etc.) et les sites web (idéalement, il faut aussi changer les questions de vérification des comptes)
- Déclarer la perte ou déposer plainte en cas de vol auprès d'un service de police nationale ou de gendarmerie nationale du lieu du vol (pays, ville) et garder une copie de la déclaration (mentionnant la date, l'heure et le lieu du vol)
- En cas de vol de données sensibles, alerter les services concernés afin que des dispositions soient prises
- Réaliser l'inventaire des données sensibles présentes sur l'équipement (en prévision de leur communication avec les autorités (CNIL))
- Si l'équipement volé donne accès à des espaces de travail communs, ou permet de s'y connecter à distance, s'assurer que les utilisateurs du réseau en soient informés
- Si l'équipement peut être géré à distance par une solution de MDM (Mobile Device Management), supprimer les données à distance, bloquer l'accès à l'équipement

[1] Par « équipement », on désigne les appareils mobiles suivants : ordinateur portable, tablette et smartphone.

VOL / PERTE D'UN PC PORTABLE, D'UN SMARTPHONE OU D'UNE TABLETTE – REFLEXES

CONSEQUENCE : GRAVE OU PAS ?

Le niveau de criticité du vol d'un équipement dépend des mesures de prévention (sauvegardes, chiffrement, durcissement) mises en place et de la sensibilité des informations stockées.

ORIGINES

- **Oubli / Perte**
- **Vol**

RESSOURCES

- CRYHOD
- STORMSHIELD
- ZONECENTRAL
- BITLOCKER
- VERACRYPT

ATTENUER L'IMPACT DU VOL D'UN EQUIPEMENT

PREVENTION

1. **Noter le numéro de série de l'équipement**

Le numéro de série de l'équipement est unique et permet son identification. Il sera demandé en cas de dépôt de plainte pour vol ou déclaration de perte.

2. **Sauvegarder régulièrement les documents**

La sauvegarde régulière des documents sur un support externe (disque dur externe, USB…) facilite la reprise d'activité et évite la perte de données. Il est fortement conseillé de chiffrer ce support externe.

3. **Permettre le verrouillage et l'effacement à distance des données de l'équipement**

L'utilisation d'une solution de MDM est recommandée. Cette solution doit au minimum disposer des fonctionnalités suivantes :

- verrouillage à distance de l'équipement en cas de perte ou de vol (blocage des accès non autorisés à l'appareil sans avoir à supprimer les données)
- effacement de l'intégralité des données enregistrées sur un appareil ou uniquement les informations sensibles de la structure
- localisation/suivi des smartphones et des tablettes : utilisation de la fonctionnalité GPS, 3G/4G ou WiFi pour localiser l'appareil

4. **Sécuriser les mots de passe**
    - Utilisation de mots de passe non rejouables (One Time Password)
        - Utilisation des gestionnaires de mots de passe tel que l'outil gratuit **KeePass**
5. **Chiffrer le contenu de l'équipement**
    - Chiffrement des données sensibles (avec un mécanisme de chiffrement conseillé par l'ANSSI)
        - Utilisation des solutions permettant de chiffrer le disque en partie ou totalement (mode de chiffrement conseillé afin d'éviter la récupération des informations liées à l'architecture interne données d'authentification…) telles que :
            - **Cryhod**[2] **:** Windows XP, Vista, Seven, Windows 2003 et 2008
            - **STORMSHIELD Data Security (SDS)**[2] **:** Windows 7 & 8.1
            - **ZoneCentral v5.0 build 960**[2] **:** Windows 2000, XP, Vista, Seven, 2003, 2008 (32 et 64 bits)
            - **BitLocker**[2] **:** Windows Entreprise (solution gratuite)
            - **VeraCrypt** (solution gratuite)

6. **Sensibiliser les utilisateurs à l'égard des équipements mis à leur disposition et les former à la protection des documents qu'ils contiennent**

[2] *Attention :* Certaines solutions nécessitent des prérequis au niveau de l'environnement informatique avant d'être installées