Agir contre le vol ou la perte d'un équipement

Objectifs de l'attaque

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 (ordinateur portable, smartphone, tablette ou clé USB).

Le vol d'un équipement (ordinateur, tablette, clé USB, portable…) est souvent réalisé à l'occasion du déplacement d'un personnel mais peut être aussi effectué à l'intérieur des locaux de la structure de santé.

Mesures de prévention

Noter le numéro de série de l'équipement permettant son identification.

Sauvegarder régulièrement les documents sur un support externe (disque dur externe, USB…), ce qui facilite la reprise d'activité et évitera la perte de données.

Activer le verrouillage automatique et mettre en œuvre 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 (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 / localisation des smartphones et des tablettes (GPS, 3G/4G ou WiFi).

Sécuriser les mots de passe avec l'utilisation de mots de passe non rejouables (One Time Password) et de gestionnaires de mots de passe tel que l'outil gratuit KeePass.

Faire l'inventaire des données sensibles et chiffrer le contenu (avec un mécanisme de chiffrement conseillé par l'ANSSI) en utilisant de préférence une solution permettant de chiffrer totalement le disque ou en partie*****.

Sensibiliser les utilisateurs à l'égard des données et des équipements mis à leur disposition et les former à la protection des fichiers qu'ils contiennent (lieu public, fermeture des sessions ...).

Mesures de réaction

Prévenir le service informatique de votre structure

Changer tous les 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 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 notamment en cas de déclaration à la **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 système en sont informés.

Si l'équipement peut être géré à distance par une solution de MDM (Mobile Device Management), supprimer les données à distance et bloquer l'accès à l'équipement.

* *Solutions qualifiées par l'ANSSI: Cryhod, STORMSHIELD Data Security, ZoneCentral*
Autres solutions: BitLocker2 (Microsoft), VeraCrypt