

Résumé

La présente fiche traite des aspects du vol d'équipements informatiques. Les éléments les plus souvent dérobés sont énumérés ainsi que les éventuelles conséquences que ce vol

peut avoir sur les personnes concernées. Les principales vulnérabilités, facilitant les vols, ainsi que les mesures préventives sont décrites.

Table des matières

- 1 Qu'entend-on par vol physique ? →
- 2 Quels sont les éléments concernés ? →
- 3 Quelles sont les bases d'estimation du préjudice ? →
- 4 Quels sont les résultats des statistiques ? →
- 5 Quelles sont les vulnérabilités les plus souvent rencontrées ? →
- 6 Comment se protéger ? →



1 Qu'entend-on par vol physique ?

Un voleur s'empare des biens d'autrui par la force ou à l'insu de ce dernier. Un vol peut s'effectuer sur tous les éléments constitutifs du parc informatique. Ces vols peuvent être commis dans les locaux

de l'entreprise ou lors du transport du matériel informatique. Comme le vol, la perte d'équipements informatiques peut avoir des impacts considérables sur la personne concernée.

2 Quel sont les éléments concernés ?

Les éléments susceptibles d'être dérobés, voire perdus, sont multiples et il est presque impossible d'en dresser une liste exhaustive. Les équipements les plus souvent dérobés sont notamment :

2.1 Les ordinateurs portables

Une valeur marchande considérable, une capacité de stockage élevée ainsi que la miniaturisation des ordinateurs portables ont fait de ces équipements des cibles de choix en ce qui concerne le vol physique.

2.2 Les assistants personnels (PDA - Personal Data Assistant)

La miniaturisation et l'efficacité des assistants personnels en font une cible préférée pour les voleurs. La capacité élevée de stockage des assistants personnels peut s'avérer comme une source importante de perte ou de vol de données.

2.3 Les supports magnétiques ou optiques

Ce type de vol est peut-être moins connu et à première vue moins dramatique, mais peut avoir des conséquences néfastes pour l'entreprise concernée.

En effet, le vol de supports magnétiques (bandes, disquettes) ou supports optiques comme CD (Compact Disk), DVD (Digital Versatile Disk), USB stockage (Universal Serial Bus) ou PCMCIA stockage (Personal Computer Memory Card International Association), utilisés à des fins de copie de sécurité, de stockage principal ou de sauvegarde (back-up), est très courant et permet de voler de grosses quantités de données.

2.4 Les téléphones portables

L'ensemble des fonctionnalités de synchronisation entre les "GSM" et les solutions informatiques indique clairement que ces éléments doivent être considérés comme des chaînons du traitement de l'information.

[→ suite](#)

3 Quelles sont les bases d'estimation du préjudice ?

Le vol d'équipements informatiques peut entraîner de sérieuses conséquences. Les préjudices subis peuvent être notamment :

3.1 La valeur de l'équipement ou du support

En cas de vol d'équipement ou de support, le premier préjudice est certainement la perte financière due aux frais de remplacement du matériel dérobé.

En ce qui concerne le vol de téléphones portables, il y a lieu d'ajouter les éventuels coûts des communications que le voleur pourrait générer avant le blocage du téléphone mobile par le fournisseur d'accès.

3.2 La perte/le vol de données

Selon l'usage qui est fait de l'équipement volé ou trouvé, il peut y avoir de multiples impacts avec des préjudices importants comme la perte de savoir-faire, l'espionnage de secrets de fabrication, la divulgation de données à caractère personnel, la perte de la renommée de la personne concernée, la perte de données financières, la perte de clés logiques d'accès, etc.

En effet, le préjudice pour les personnes concernées est tout à fait différent selon l'utilisation du matériel (reformatage pour permettre d'autres usages, utilisation illicite pour pénétrer un réseau, voire vente de données).

3.3 Le vol de logiciels

Le vol de machines portables entraîne évidemment le vol de tous les logiciels installés sur cet équipement. Cela inclut les

logiciels publics mais aussi les logiciels développés spécialement pour les besoins de la personne privée/entreprise/administration.

3.4 L'accès aux réseaux

Le vol d'équipements capables de se connecter à un réseau ou à d'autres périphériques, via la technologie du réseau sans fil, via l'infrarouge ou via un accès à distance, permet une connexion illicite au réseau de la personne concernée. Cet accès peut être utilisé pour dérober encore plus d'informations ou de faire d'autres dégâts.

3.5 La perte de productivité

L'indisponibilité de ces équipements entraîne souvent, pour la malheureuse victime, l'impossibilité de travailler. Cette perte de productivité, liée à la perte de documents et d'applications peut engendrer une charge importante de travail rien que pour restituer les données et logiciels tels qu'ils étaient au moment du vol ou de la perte. Ceci est d'autant plus vrai si la personne concernée ne dispose pas de sauvegardes récentes.

3.6 L'impersonnalisation

Il est fort probable que la personne responsable du vol, si elle possède un minimum de connaissances informatiques, soit capable d'utiliser des logiciels tels que la messagerie, ou des logiciels de type e-banking, tout en se faisant passer pour le propriétaire licite. Il est évident que dans ce cas le préjudice financier peut rapidement atteindre des sommes considérables.

4 Quels sont les résultats des statistiques ?

De nombreuses sources fournissent des informations soulignant l'envergure du vol d'équipements informatiques :

- Le vol d'ordinateurs portables est le second délit informatique après l'envoi de virus. (Etude CSI/FBI (Computer Security Institute/Federal Bureau of Investigation) sur le crime et la sécurité informatique 2003).
- 591.000 ordinateurs portables ont été volés aux Etats-Unis durant l'année 2001. (Time Magazine 27/01/03).
- Durant les 6 premiers mois de l'année, des voyageurs pressés ont oublié 62.000 GSM, 2.900 ordinateurs portables et 1.300 assistants personnels dans les taxis de Londres. (BBC, août 2001).
- 2.8 millions de téléphones portables sont perdus ou volés chaque année en Corée du Sud. (Financial News, août 2002).

- Le personnel de Sécurité IT admet que 57% des brèches de sécurité exploitées ont été causées par des vols d'ordinateurs portables. (Etude CSI).
- 70 % des vols d'ordinateurs ont lieu en interne. (Gartner Group).
- Le vol d'ordinateurs portables constitue un risque majeur dès lors que des données d'entreprise sensibles sont concernées, et la situation ne peut qu'empirer avec l'utilisation de périphériques «de poche». Chris Christaensen, IDC (International Data Corporation).
- 33 % des personnes utilisent leur assistants personnels (PDA) pour y stocker leurs mots de passe et codes d'accès, 25 % y enregistrent des données professionnelles sensibles, 25 % des données relatives à leurs comptes bancaires. (PointSec's Survey).

[→ suite](#)

5 Quelles sont les vulnérabilités les plus souvent rencontrées ?

Il n'est malheureusement pas possible de supprimer toutes les vulnérabilités, mais il faut essayer de limiter les impacts possibles au moyen de contrôles, de mesures préventives et de mécanismes de détection.

→ La sécurité d'accès

Un contrôle d'accès efficace aux bureaux et salles informatiques doit être mis en place. Malheureusement les accès physiques sont

trop souvent mal gérés. L'administration des connexions à distance doit être surveillée rigoureusement.

→ Les erreurs humaines

Comme le montrent les statistiques, les erreurs humaines, les fautes de prévoyance, la négligence ou pertes et oublis demeurent la plus grande source de perte d'équipements informatiques.

6 Comment se protéger ?

Il y a lieu de faire la différence entre les mesures préventives, dont le rôle est d'empêcher la survenance de ce type d'événements, et les autres mesures, dont le but est de détecter et de contrôler ce type d'événements, ou encore d'en limiter les impacts.

6.1 Les procédures

L'existence, la publication en interne, le respect et le contrôle de procédures relatives à l'usage, au transport et au stockage des supports informatiques, vous permettent réduire substantiellement les pertes ou les vols de médias.

L'existence et le respect de procédures à appliquer en cas de vol ou de perte de données, telles que le filtrage d'accès au réseau sur base de l'adresse MAC (Media Access Control), la suppression de l'accès distants, le blocage du client VPN (Virtual Private Network) ou la modification de tous les mots de passe de l'utilisateur, sont des mesures indispensables pour limiter l'impact.

> Cette contre-mesure ne peut pas être qualifiée de préventive, même si leur existence et leur communication peuvent décourager les vols en interne.

6.2 La gestion de l'inventaire du matériel

Seul le suivi détaillé de l'inventaire vous permettra de refuser l'accès à distance depuis des équipements dérobés et pourra vous servir de base pour les dialogues avec l'assureur.

6.3 La limitation de l'utilisation de supports externes

Le nombre de vols ou pertes de supports informatiques (disquettes, CD ROM - Compact Disk Read Only Memory...) est proportionnel au nombre de supports en circulation. Il peut dès lors s'avérer avantageux de premièrement limiter et de deuxièmement contrôler l'usage de ces supports.

Le blocage de certains périphériques tels que les ports USB (Universal Serial Bus) ou infra-rouges, peut vous éviter l'utilisation illicite de certains supports.

> Cette contre-mesure peut être qualifiée de préventive.

6.4 L'utilisation de cadenas

Il existe sur le marché des petits mécanismes permettant d'attacher les ordinateurs portables au mobilier. Si ce type d'équipement n'a malheureusement pas souvent la capacité d'empêcher le vol, il rend tout de même la tentative nettement plus longue et visible.

> Cette contre-mesure peut être qualifiée de préventive.

6.5 Le cryptage des données

Il est fortement conseillé d'utiliser des logiciels spécialisés pour encrypter les données stockées sur le disque des ordinateurs portables. Ces outils rendent l'utilisation de données volées quasiment impossible.

> Cette contre-mesure peut être qualifiée de préventive.

6.6 La protection par mot de passe

Comme pour tout usage informatique, utilisez des mots de passe « forts » et supprimez des comptes inutiles sur la machine.

> Cette contre-mesure peut être qualifiée de préventive.

6.7 Le marquage des équipements

Que ce soit par des autocollants ou par gravure, le marquage d'équipements informatiques demeure un moyen important de dissuasion contre le vol.

> Cette contre-mesure peut être qualifiée de préventive.