La Perte de Données

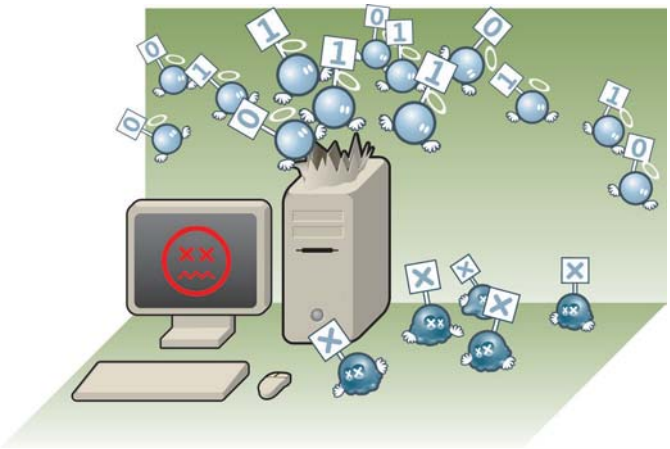
CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

Résumé

On parle de perte de données lorsque les données sont supprimées ou détériorées de manière à en rendre l'accès impossible. Cette situation peut se produire suite à divers événements naturels (catastrophes), techniques (pannes) ou actions humaines (vol avec destruction, destruction volontaire ou involontaire). Tous les utilisateurs de ressources informatiques peuvent être touchés par des pertes de données. Vu le grand nombre d'événements qui peuvent provoquer une perte de données, de nombreuses mesures de prévention doivent être prises en compte.

Quelles qu'en soient les raisons, la perte de données est malheureusement un phénomène courant en informatique. La présente fiche décrit les risques pouvant conduire à la perte de données, fournit des mesures préventives ainsi que les mesures de récupération après sinistre.

Table des matières



1 C'est quoi ?

On parle de perte de données lorsque les données sont supprimées ou détériorées de manière à en rendre l'accès impossible. Cette situation peut se produire suite à divers événements naturels (catastrophes), techniques (pannes) ou actions humaines (vol avec destruction, destruction volontaire ou involontaire).

Par contre, on parle d'altération de données quand une partie des données est modifiée sans pour autant rendre impossible l'accès aux données.

Finalement, on parle de vol de données quand une personne accède à des données qui ne lui sont pas normalement accessibles, et les soustrait frauduleusement. Le vol de données peut s'effectuer par une copie, un transfert des données ou par l'impression de ces dernières. Le vol de données peut être couplé à des actes de destruction ou d'altération des données.

Pour mieux comprendre ce phénomène et les moyens de recouvrement, il est nécessaire d'établir les distinctions suivantes :

1.1 Perte des données due à la perte d'accès aux données

Diverses raisons physiques ou logiques peuvent provoquer la perte d'accès aux données. Dans la majorité des cas, les données sont encore physiquement stockées sur les supports informatiques, mais puisqu'ils ne sont plus accessibles, on parle de perte de données. Les méthodes de récupérations se distinguent des méthodes utilisées pour récupérer des données détériorées ou supprimées.

1.2 Perte des données due à l'altération de données

Lors de certaines manipulations frauduleuses effectuées par des pirates informatiques sur des serveurs «Web», on assiste non pas à la destruction ou au vol de données, mais simplement à l'altération de ces dernières. En effet, le «cracker» peut, par exemple, annoncer avoir simplement modifié une donnée quelque part. Dans ce cas, les données authentiques ne sont plus accessibles car elles ont été altérées, ce qui équivaut à une perte des données.

La perte de données due à l'altération de données peut aussi être provoquée par des actions volontairement ou involontairement illicites sur des bases de données ou des fichiers. Cette forme de perte de données est souvent difficilement détectable, (les données sont toujours là, mais elles ne sont plus correctes).

La Perte de Données

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

1.3 Perte des données par vol des données

Les vols de données n'entraînent pas nécessairement la destruction ou l'altération des données. Si les données sont copiées, transférées ou imprimées, les originaux restent inchangés. C'est d'ailleurs une des raisons pour lesquelles il est parfois difficile de détecter ces vols.

L'impact d'un vol de données confidentielles (par exemple des secrets de fabrication) peut être nettement supérieur à la simple perte de données. On parle aussi de perte de confidentialité des données.

1.4 Perte des données par vol ou pertes d'équipements respectivement de supports

La perte ou le vol d'ordinateurs portables et également de tout support informatique (bande magnétique, disquette, CD ROM - Compact Disk Read Only Memory, ...) entraîne souvent la perte des données stockées sur ces ressources informatiques. En effet, les utilisateurs disposant rarement d'une copie de sauvegarde complète. Le vol ou perte des supports informatiques engendre aussi un grand risque de perte de confidentialité des données.

1.5 Perte des données par destruction volontaire des données

Lorsque la perte ou l'altération des données n'est pas la résultante d'un phénomène technique mais bien d'une action humaine, il faut faire la différence entre les actions humaines suivantes :

- Volontaires malveillantes (piratage d'un site Web).
- Volontaires non malveillantes (effacement d'un fichier).
- Involontaires (mauvaise manipulation).

2 Qui est concerné ?

Tout utilisateur d'une ressource informatique peut potentiellement être confronté à une perte de données. Personne n'est à l'abri. Par contre, on peut mettre en oeuvre différents moyens pour limiter les risques ou pour récupérer tout ou partie de ces données.

La perte de données peut résulter de problèmes de fonctionnement ou de manipulation sur, par exemple :

- Les gros calculateurs équipant les centres informatiques.
- Les serveurs.
- Les ordinateurs personnels.
- Les ordinateurs portables.
- Les supports magnétiques et optiques.

Souvent la perte de données touche les victimes de façon aléatoire. En effet beaucoup de «crackers» choisissent leur cible par hasard. Il en va de même des événements naturels. Mais aussi la nature des données perdues peut varier fortement :

- Logiciels publics ou développés en interne.
- Données de moindre valeur (correspondance, etc.).
- Données critiques nécessaires au bon fonctionnement de la société (comptabilité, etc.).
- Données stratégiques (par exemple des secrets de fabrication).

3 Quelles sont les menaces principales ?

Selon les statistiques établies par les plus grandes entreprises spécialisées dans la récupération de données, on peut dire que les principales causes de perte de données mentionnées par les utilisateurs sont :

- 44 % défaillance matériel ou système d'exploitation.
- 32 % erreur humaine.
- 14 % logiciel endommagé ou corruption d'un logiciel.
- 07 % virus.
- 03 % catastrophes naturelles.

Ces statistiques doivent être analysées avec circonspection car elles ne concernent que les entreprises qui ont déclaré une perte de données et qui ont fait appel à des entreprises de récupération. En clair, cela ne concerne que très peu les pertes de données non critiques pour lesquelles on ne fait pas appel à ce genre de services. De plus, ne font pas partie de ces statistiques les entreprises/administrations/personnes privées qui ont pu restaurer les données par leurs propres moyens ou qui n'ont pas voulu «publier» leurs éventuelles pertes de données afin de préserver leur image de marque.

La Perte de Données

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

4 Statistiques

Les statistiques reprisent dans ce chapitre donnent un aperçu de l'ampleur de la problématique.

4.1 Les ordinateurs portables

50% des agents itinérants ne disposent d'aucune protection contre la perte de données alors que 80% de leurs informations sont stockées sur leur ordinateur portable (source : IDC - International Data Corporation).

4.2 Les domaines concernés

En se basant sur l'analyse de cas réels, on peut déterminer les zones directement concernées en cas de perte de données et évaluer les dépenses habituellement liées à ce type de phénomène.

A ce titre, le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) a publié un dossier en 2002, basé sur tous les domaines économiques et consacré à la sinistralité informatique. Cela apporte des informations intéressantes quant aux domaines concernés et souligne des aspects moins connus tels que la responsabilité encourue par une entreprise vis-à-vis des tiers et la perte de patrimoine (le dossier n'inclut pas des analyses concernant des administrations ou des personnes privées).

- Coûts de réparation ou remplacement du matériel informatique endommagé ou manquant : 21%.
- Coûts de reconstitution de données, logiciels ou procédures endommagés ou perdus : 18%.
- Pertes d'exploitations : 17%.
- Coûts de renforcement des protections : 16%.
- Responsabilité encourue par l'entreprise : 15%.
- Pertes de patrimoine : 14%.

Répartition de l'impact financier résultant de la perte de données (Source : CLUSIF)

REMARQUE

Il est à noter que la perte d'exploitation potentielle est évidemment plus élevée que le coût de remplacement des équipements. L'apparente homogénéité entre ces impacts est liée au fait que toutes les pannes n'entraînent pas nécessairement des pertes d'exploitation.

5 Comment se protéger ?

Ce chapitre aborde succinctement les différentes contre-mesures, car certaines d'entre elles font l'objet d'une fiche détaillée afin de pouvoir donner tous les éclaircissements nécessaires.

Il faut faire une première distinction entre les mesures préventives et les mesures de récupération après sinistre.

Il est évident, que ce chapitre doit être abordé de manière sélective, selon l'ampleur et la complexité de l'équipement informatique concerné.

5.1 Mesures préventives

Sont regroupées sous ce point toutes les mesures prises dans le but de prévenir la survenance d'un événement pouvant provoquer la perte de données, mais aussi toutes les mesures visant à en limiter les dégâts.

5.1.1. ADAPTATION DE LA SOLUTION DE STOCKAGE

Il est important d'adapter la technologie de stockage au degré de sensibilité des données ainsi qu'au type de données (fichiers bureautiques, bases de données).

Afin d'éviter un rapide engorgement de l'infrastructure de stockage et tous les problèmes qui y sont directement liés, il est nécessaire de mettre en place une politique d'archivage des fichiers sur des supports adaptés.

Il est conseillé d'équiper les serveurs de la technologie RAID (Redundant Array of Independent/Inexpensive Disks) qui permet de répartir le stockage des données sur plusieurs disques durs. Lors de la perte éventuelle d'un des disques durs composant le RAID, le système informatique est capable de reconstituer l'information manquante. Il existe différents niveaux de configuration RAID, lesquels font l'objet d'une fiche séparée.

La mise en place d'un réseau filaire de stockage (SAN=Storage Area Network) peut également s'avérer utile dans le cas de grosses infrastructures ou de déploiement d'un second site de production ou de repli. Ce type de système informatique demande une grande maîtrise informatique et il est conseillé de s'adresser à des entreprises spécialisées dans ce domaine.

La Perte de Données

suite

5.1.2. POLITIQUE DE SAUVEGARDE/RESTAURATION ADAPTÉE

Il faut adapter les technologies ainsi que les politiques de sauvegarde et de restauration des données selon le degré de la sensibilité, mais aussi selon la nature des données (fichiers bureautiques, bases de données).

Des technologies telles que le «snapshooting», dont le but est de réaliser des copies des modifications de la base de données et ce «à la volée» durant la journée, permettent d'éviter un retour à la situation de la veille, limitant de ce fait la saisie ou le ré-encodage éventuellement nécessaire. Si cette technique onéreuse et complexe est bien adaptée à un type d'utilisation très complexe, elle n'a aucun intérêt dans le cadre de la sauvegarde de données bureautiques habituelles.

La mise en place de procédures connues de tous, respectées et contrôlées, permet d'exploiter au mieux l'infrastructure en place, comme par exemple l'information donnée aux utilisateurs quant aux répertoires à sauvegarder quotidiennement.

Le délai de restauration est malheureusement un impératif sous-estimé. En effet, la plupart des responsables informatiques sont préoccupés par la vitesse de sauvegarde mais ignorent la capacité de restauration. Or, en cas de sinistre, c'est la restauration qui est critique. Une étude détaillée de l'architecture de restauration ainsi que du réseau, validée par une mise à l'épreuve, demeure le meilleur moyen de juger de l'adéquation de la solution avec les besoins.

5.1.3. RESPECT DES BONS USAGES EN MATIÈRE DE SALLE INFORMATIQUE

La mise en place d'une architecture informatique se doit de répondre à certaines exigences en matière environnementale. Une salle informatique, une salle de connectique, une salle de télécommunication etc... , doivent être équipées de manière à assurer aux équipements des conditions optimales de fonctionnement. Cela sous-entend : un circuit électrique de secours ou un UPS (Uninterruptible Power Supply), une climatisation et un filtrage d'air, un contrôle de l'électricité statique, un système spécifique de lutte contre les dégâts des eaux et du feu, et un contrôle d'accès.

L'ensemble de ces points est couvert dans une fiche relative à la sécurité physique.

5.1.4. STOCKAGE ADAPTÉ DES SUPPORTS

Les supports informatiques, tels que les bandes magnétiques, supports optiques et autres doivent absolument être stockés dans des endroits répondant à leurs exigences en matière de protection contre la poussière, les griffes, l'humidité et autres facteurs pouvant les dégrader.

II est conseillé de stocker les supports de sauvegarde dans un coffre-fort, en dehors de la salle informatique voire dans un autre bâtiment.

5.1.5. GESTION DES DROITS DES UTILISATEURS

Le moyen le plus sûr d'éviter les effacements involontaires de données est de limiter au minimum possible les droits des utilisateurs sur les fichiers et supports critiques.

5.1.6. GESTION PROACTIVE DU PARC INFORMATIQUE

La majorité des pannes de fonctionnement qui touchent les équipements informatiques ont des signes «avant-coureurs». La plupart des équipements sont fournis avec un logiciel qui traite ces signes et avertit l'utilisateur en cas de doute. Ces logiciels existent tant au niveau des serveurs que des ordinateurs (postes de travail) et même des ordinateurs portables. Il est conseillé de laisser ce logiciel faire son travail et de tenir compte des avertissements qu'il pourrait formuler.

5.1.7. FORMATION DES UTILISATEURS

Un moyen important d'éviter les maladresses est de former les utilisateurs aux manipulations de la machine et de ses périphériques ainsi qu'à la gestion des données et des répertoires.

5.2 Mesures de récupération

Sont regroupées sous ce point toutes les mesures de récupération après sinistre.

5.2.1. LOGICIELS OU SOCIÉTÉS DE RÉCUPÉRATION

Il existe beaucoup de logiciels capables de récupérer des données perdues ou effacées sur différents supports. Ces logiciels sont assez coûteux et leur usage demande une certaine maîtrise du sujet. Il est donc fortement conseillé de faire appel à des entreprises spécialisées en ce domaine.

5.2.2. QU'EST-CE QUE LE «FORENSIC»

Le «forensic» est un terme anglais signifiant recherche légale. Cette technologie consiste à rechercher les événements qui ont pu conduire à un sinistre.

La Perte de Données

CASES LUXEMBOURG
CYBERWORLD AWARENESS AND SECURITY ENHANCEMENT STRUCTURE

suite

En clair, cette technologie vise à obtenir des informations ordinairement invisibles sur les faits qui ont conduit au sinistre et, par exemple, à l'identification de la cause réelle de la perte de données et à l'identification de l'auteur des faits. Cette technologie ne vise donc pas directement la récupération de données, mais la recherche des raisons ayant conduit à cette perte.

Seul ce type d'outil permet d'ester en justice contre un éventuel pirate. Toutefois, afin de conserver à ces preuves un caractère légal et au vu de la complexité de l'usage de ces outils, il est conseillé de faire appel à des entreprises spécialisées en ce domaine.

REMARQUE :

Les personnes sensibles à la sécurité sont interpellées par le fait que l'on puisse récupérer des fichiers effacés. Il est toujours possible de rendre ce type de récupération inopérant, et il est important d'y prêter attention lors de reventes d'équipements informatiques.

CASES,
pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

OFFICE LUXEMBOURGEOIS D'ACCREDITATION ET DE SURVEILLANCE

LE GOUVERNEMENT DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie et du Commerce extérieur