Sécurisation des données

Sommaire

Introduction

> Les premiers temps.

À la base, les données étaient seulement sauvegardé sur la mémoire même de l'ordinateur.

> Pourquoi sauvegarder ses données informatiques ?

Tant que tout va bien on, ne s'en soucie guère.

Souvent mise de côté principalement chez les T.P.E, seulement lorsque le problème arrive il est déja trop tard.

> catastrophe, voir perte de l'entreprise...

> Les enjeux en sécurité...

- liberté individuelle = vie privée ;
- bureautique = sécurité des données enregistrées (fichier...) ;
- communication = ne pas trop divulguer d'informations ;
- secret des affaires = protection entreprise (client,fournissseurs...);
- tracabilité des documents.

> Pourquoi sauvegarder ses données informatiques ?

Pour le particulier cette action relève d'un engagement personnel.
Mais pour l'entreprise, le patron est pénalement responsable vis à vis de ses employés, ses clients, ses fournisseurs... Il peut être amendable.

> Quels risques pour les données informatiques ?

Il existe différents types de risques pour les données d'une entreprise, les principaux sont :

- les virus et programmes malveillants ;
- les emails frauduleux ;
- le piratage ;
- l'erreur de manipulation...

> Quels risques pour le métier ?

- paralyse l'entreprise = perte de données, touche l'image de l'entreprise.
- vol d'un corp de métier.
- vol de données confidentiel = clients, fichiers...

> Les données informatiques au coeur de notre activité.

En 2005, sur 218 entreprises européennes, plus de 50% ont subit des pertes financières liées à des problèmes informatiques.

La même année, une autre étude mettait en évidence que seules 30% des entreprises avaient pris des précautions pour veiller à la disponibilité et fiabilité de leurs données informatiques.

95% des sociétés de taille moyennes ayant été sévèrement piraté en 1998 ont stoppé leur activité dans les 12 mois qui suivaient.

Comment faire ?

> Que faut-il faire ?

Les principales actions à mener pour sécuriser l'informatique de son entreprise sont :

- protéger l'accès à internet ;
- protéger le réseau informatique ;
- auditer le contenu de votre site web ;
- sauvegarder vos données informatiques ;
- filtrer les courriers électroniques ;
- sensibiliser les utilisateurs ;
- anticiper les incidents et minimiser leurs impacts.

>Par où commencer ?

Réaliser un état des lieux.

Parce que votre informatique évolue en permanence, une vigilance constante est de rigueur.

> Aspect de la sécurité.

- confidentialité ;
- intégrité ;
- disponibilité.

EX : L'authentification est l'une des 3 phases : confidentialité

> RSSI.

Responsable de la **S**écurité des **S**ystème d'**I**nformation

> Les supports externes.

Les choix de supports externes :

- Clef USB
- CD ou DVD ROM
- Disque dur

- Un second PC
- Un serveur d'entreprise
- Un serveur NAS*

* serveur de stockage en réseau.
Serveur de fichier autonome relié à un réseau dont sa principale fonction est le stockage

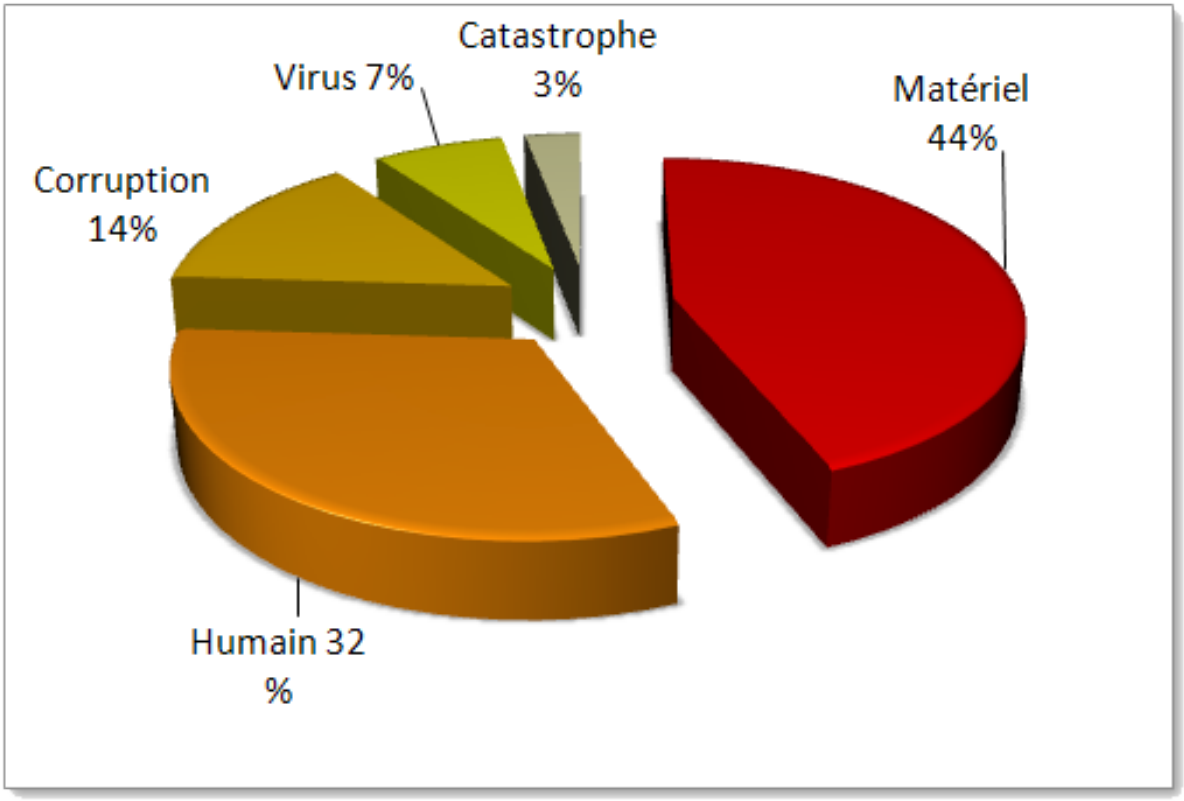
exemple : « Cloud computing »

Comment faire ?

« Cloud computing »

Concept qui consiste à déporter sur des serveurs distants des stockages habituellement localisé sur des serveurs locaux ou sur le poste de l'utilisateur.

> Statistiques.



> Les précautions.

Dès lors il convient de faire des sauvegardes de données régulières.

Questions/Réponses

> Quelques idées recues.

Mon firewall protège tout mon réseau.
FAUX : Un firewall protège uniquement le point d'accès internet de votre entreprise, pas votre réseau interne ni vos données.

Je le saurais si j'avais été piraté !
FAUX : Sans outil de diagnostic, il n'est pas possible de savoir si une entreprise a été piratée. En France une entreprise sur deux serait piratée à son insu.

C'est risqué de ne pas sécuriser mon réseau.
VRAI : L'entreprise risque entre autres, de perdre ses données, de servir d'intermédiaire à un pirate. Cela peut engager sa responsabilité civile et pénale pour des actes qui lui sont étrangers.

La sécurité est uniquement une problématique technique.
FAUX : Le niveau de sécurité se mesure à son maillon le plus faible. Un salarié non sensibilisé à la sécurité constituera toujours le maillon le plus faible de votre chaîne de sécurité.

> Exemple de logiciels :

--> **my lockbox**

Un logiciel qui cache les fichiers.

--> **Malwarebytes**

Un logiciel anti-espion.

Les sécurités

> Sécurité des postes de travail

prévenir:

- tentative d'accés frauduleux ;
- éxécution de virus ;
- prise de contrôle à distance (internet).

précaution :

- installer un «pare feu»
- antivirus (à jour)
- verrouillage automatique de session
- contrendu date/heure de connexion
- limiter le nombre de tentative d'accès

> Sécurité réseau informatique interne

Identifier les nécessités essentielles et n'autorisser que celles-ci.

précautions :

- limiter les réseaux aux strict nécessaire
- sécurisé les accès

> Sécurité serveur et applications

serveurs = équipement plus critique donc sécurité renforcées

précautions :

- mot de passe complexe
- changer mot de passe en cas de départ
- mise à jour

Conclusion

PUISQUE :

L'informatique est devenue pour l'entreprise un outil incontournable de gestion, d'organisation, de production et de communication.

IL FAUT :

S'assurer et assuré la protection de ses données pour sois même ainsi que tout autres personnes pouvant être touchés (exemples : la clientèle)

CAR :

La sécurisation des données vise à assurer la confidentialité, l'intégrité des informations...