

Prévoir l'accident

Assurer la continuité de l'exploitation

Organisation de la sauvegarde



Assurer la continuité de l'exploitation

La solution de la redondance

On double les systèmes pour faire disparaître le risque de panne :

- Redondance de composants : alimentation, disques (Raid)
- Redondance de serveurs
- Redondance de sites
- Redondance de liaisons

Le rapport risques/coûts devient rapidement rédhibitoire pour une petite structure

Plan de **C**ontinuité d'**A**ctivité

Le **P**lan de **C**ontinuité d'**A**ctivité prévoit, en cas de sinistre important perturbant le fonctionnement du système informatique, l'organisation et les ressources nécessaires à la remise en route la plus rapide possible et avec le minimum de pertes de données, de l'activité de l'entreprise

Un préalable au PCA : l'Optimisation des ressources

- Centralisation des données (serveurs)
 - Contrôle et réorganisation périodiques
- Standardisation des postes de travail
 - Systèmes d'exploitation
 - Logiciels
- Création et maintenance d'outils de reprise sur panne
 - «Images disque» des postes clients
 - Sauvegarde «système» des serveurs

Autre préalable au PCA : l'optimisation de l'organisation

- Mise en place de « procédures d'exploitation »
 - Définissant précisément qui fait quoi
 - Prévoyant absences, indisponibilités, défections
 - Traçables
 - Prenant en compte les incidents
- Mise en place d'outils de gestion des ressources
 - Inventaires matériel et logiciel
 - Guides d'installation, de configuration,
 - Check-lists
 - Documentations, codes d'accès, etc.

PCA : la conception

- Analyse de risque
 - Recensement exhaustif des menaces
 - Détermination des risques
 - Hiérarchisation de ceux-ci
 - Adoption éventuelle de mesures d'atténuation du risque (ex. redondance) → risques résiduels
- Analyse d'impact
 - Mesurer l'impact de la matérialisation du risque sur les processus essentiels de l'entreprise
 - Définir le seuil critique pour l'activité de l'entreprise

PCA : la conception (suite)

- Détermination des mesures à mettre en œuvre en cas d'incident/accident :
 - Systèmes de secours
 - Site de secours
 - Procédures de basculement
 - mode « dégradé »
- Détermination des activités régulières nécessaires à la bonne mise en œuvre du PCA
 - Préparation et entretien des systèmes de secours
 - Intégration des nouvelles solutions et technologies

Tests et remise en cause

- Le PCA doit être régulièrement testé partiellement ou en totalité, afin de
 - confirmer son efficacité
 - rôder les intervenants
 - conserver la mobilisation
 - vérifier l'intégration des éléments nouveaux
- Les retours d'expérience de ces exercices doivent être exploités pour réviser la conception du plan



L'organisation de la sauvegarde

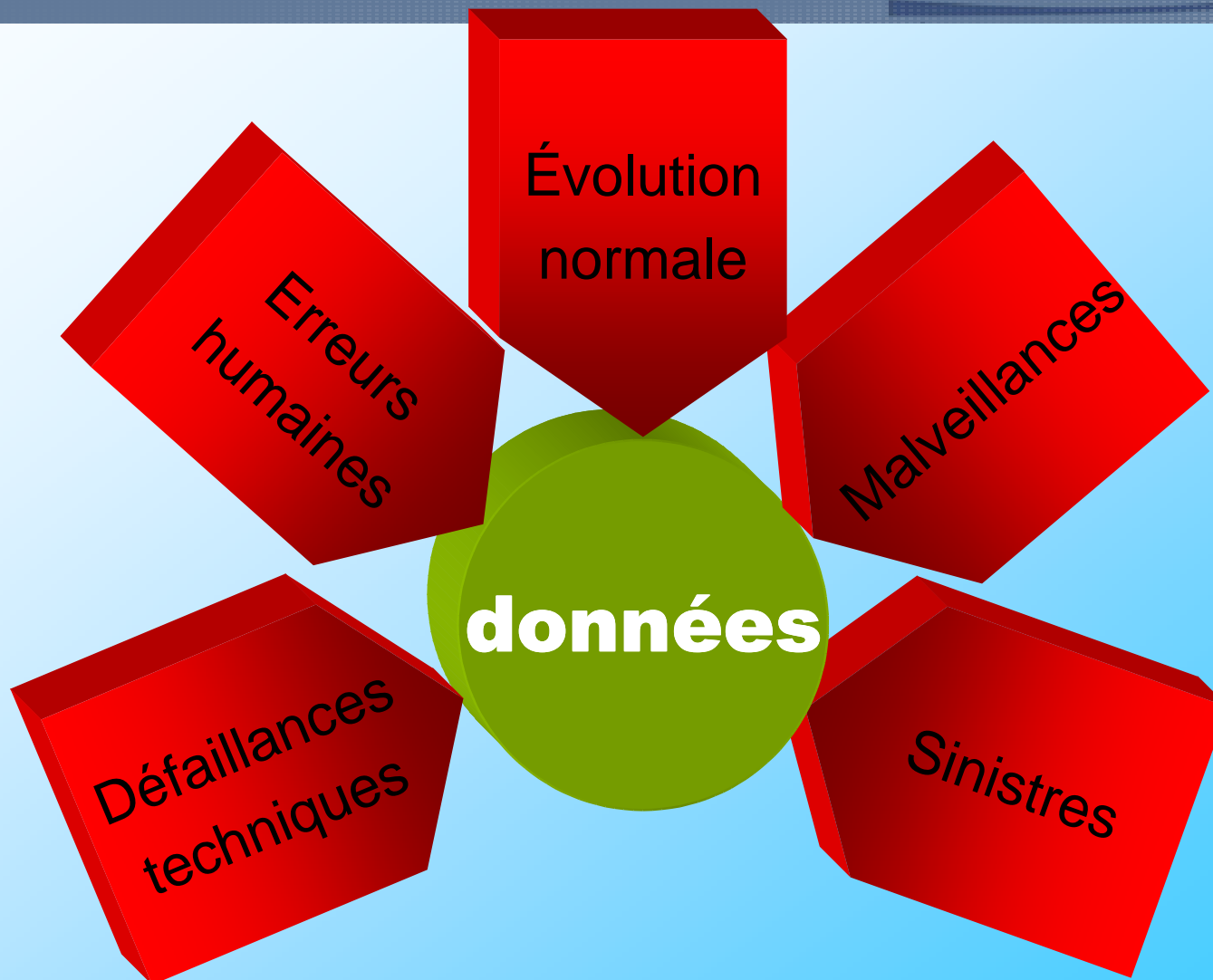
L'organisation de la Sauvegarde

- La problématique des données d'entreprise
 - ✓ Quelles données sauvegarder
 - ✓ Causes d'altérations
 - ✓ Où sont les données ?
- La sauvegarde
 - ✓ Définition et objectifs
 - ✓ Outils et méthodes de sauvegarde
 - ✓ Mettre en place l'organisation
 - ✓ Tester le dispositif

Quelles données ?

- Données d'applications
- Documents bureautiques
- Données de messagerie
 - ✓ Mails
 - ✓ Pièces jointes
- Paramètres des programmes
- Programmes ?

Les causes d'altération



Localisation des données

- Dispersées sur les postes de travail
- Centralisées sur un serveur
- Localisation mixte
- Temporairement mixte (nomadisme)

La sauvegarde - définition

Importance de la perte de données acceptée

Duplication périodique des données sur un support, indépendant du système d'origine, conservé dans un lieu sûr et distinct .

Non vulnérable aux pannes de celui-ci et utilisable sur un autre système

Déport systématique et immédiat de chaque sauvegarde sur un autre site

Objectifs de la sauvegarde

- Deux logiques :
 - ✓ Récupérer des données perdues suite à un incident/accident
 - ✓ Restituer des données dans un état antérieur
- Souvent combinées : multiples supports pour assurer la redondance et historique

<i>Support</i>	<i>Avantages</i>	<i>Inconvénients</i>
CD – DVD	Peu cher, accès rapide, standard	Usage unique, capacité limitée, qualité variable
Bande	Capacités importantes	Restauration longue, format propriétaire
Disque	Capacités très importantes	Coût, encombrement, fragilité
Clés USB	Taux transfert très rapide	Coût, capacité limitée, fiabilité

Un "support" particulier : La sauvegarde en ligne

- Prestation assurée par un prestataire Internet
- S'appuie sur une connexion Internet haut débit
- Les données sont cryptées avant d'être envoyées sur le site de stockage
- Sites de stockage redondants
- Après une sauvegarde complète, les sauvegardes quotidiennes sont différentielles
- Souvent « versionning » : on peut conserver les x dernières versions de chaque fichier.
- **Avantage évident : le déport est automatique**

Logiciels de sauvegarde

Ils doivent permettre :

- La programmation automatique des sauvegardes
- La restauration partielle d'un ou deux fichiers si besoin est
- La remontée d'alertes (mail...) en cas de problème de sauvegarde

Organiser la sauvegarde

- On ne peut pas compter sur le bon vouloir de chacun : la sauvegarde doit être organisée, des collaborateurs doivent être responsabilisés.
- Un collaborateur doit être désigné pour changer les supports et les déporter
- Prévoir un suppléant en cas de maladie, d'absence...
- Le résultat de la sauvegarde doit être testé
- Effectuer régulièrement un exercice de restauration de quelques fichiers à une date définie

Un exemple de plan de sauvegarde

- 4 bandes « quotidiennes » : lundi, mardi, mercredi, jeudi.
- 4 bandes hebdomadaires : vendredi 1, 2, 3, 4.
- 11 bandes mensuelles : janvier à novembre
- 1 bande par année

Résultat :

On peut en permanence revenir aux 5 jours précédents, aux 3 semaines précédentes, aux 11 derniers mois, et à la fin de chaque année



En conclusion...

Préparer la catastrophe, c'est l'éviter

- Identifier les menaces et leurs conséquences
 - Permet de choisir les outils et solutions de sécurité
 - Permet de sensibiliser et de motiver les acteurs
- Tests et contrôles réguliers des dispositifs et mesures de sécurité
 - Vérification du fonctionnement technique
 - Vérification de l'adéquation des mesures
 - Evaluation de l'adéquation des procédures
 - Maintien de la mobilisation

La sécurité : un état provisoire

- Les menaces évoluent parallèlement à leurs parades.
- La rapidité technologique multiplie les nouvelles solutions matérielles et logicielles, accompagnées de nouvelles menaces.
- La réactivité des entreprises les poussent à modifier et faire évoluer leurs activités, leur organisation : tout changement est accompagné de son lot de risques.

La sécurité : une systémique globale

- Il n'existe pas de réponse « sur étagère »
- Nécessité d'une démarche d'analyse globale
- Participation indispensable de tous les niveaux d'acteurs
 - Responsable informatique
 - Chef d'entreprise
 - Cadres
 - Utilisateurs
- A pour fondement la bonne gestion quotidienne des ressources informatiques

Des questions?

