Scénario 1 – PME Comptable : Analyse complète et détaillée

Dans une PME comptable, les données financières représentent le cœur de l'activité. Leur perte – même partielle – peut avoir des conséquences immédiates sur les clients, sur la conformité légale et sur la survie même de l'entreprise. Ce scénario te permet d'analyser concrètement comment construire une stratégie de sauvegarde solide et adaptée à un environnement où la moindre erreur peut coûter cher.

Exploration

Une **petite entreprise de comptabilité** située en Belgique, composée de **5 employés** :

- 1 gérant
- 3 comptables
- 1 employée administrative

L'entreprise gère **plus de 150 dossiers clients** (PME, indépendants, ASBL). Elle traite :

- la comptabilité générale
- les déclarations TVA
- les fiches de paie
- les bilans annuels
- les relevés bancaires importés
- les pièces justificatives (factures PDF ou scannées)

L'entreprise travaille dans un **petit bureau** avec :

- un **serveur central** Windows
- un **NAS** de 4 disques
- 5 postes clients Windows
- un routeur/firewall standard (pas d'équipe IT interne)

L'entreprise doit respecter :

- le **RGPD**,
- le secret professionnel comptable,
- et la **conservation légale** de certains documents.

🗃️ Données à protéger

Données essentielles

Ces données doivent absolument être protégées, sans quoi l'activité s'arrête.

1. **Base de données comptable SQL** (logiciel professionnel, version multi-utilisateurs)
2. **Documents financiers des clients** :
    - factures d'achat/vente
    - extraits bancaires
    - pièces justificatives
    - bilans
3. **Documents administratifs de l'entreprise**
4. **Mails professionnels** (Outlook + Exchange/IMAP)

Données importantes (mais pas vitales immédiatement)

- Documents internes (modèles, feuilles Excel, procédures)
- Historique des courriers envoyés

Données confort

- Photos d'événements internes
- Documents « non critiques »

⚠️ Risques spécifiques de ce scénario

1. Ransomware

Très critique : les comptables reçoivent de nombreuses pièces jointes suspectes. Si le serveur ou le NAS sont chiffrés → activité complètement bloquée.

2. Panne du serveur

Vieillissement matériel, disque dur, alimentation.

3. Erreur humaine

Exemples :

- suppression accidentelle d'un dossier client
- écrasement d'un fichier PDF important
- mauvaise manipulation dans la base SQL

4. Sinistre physique

- Incendie dans l'immeuble
- Cambriolage
- Inondation

5. Corruption de la base de données

Un fichier SQL peut devenir illisible après une coupure de courant.

6. Vol ou perte d'un ordinateur portable

Un comptable peut travailler ponctuellement chez un client.

📉 Impacts d'une perte de données

- **Amendes fiscales** si les déclarations ne peuvent pas être complétées
- **Perte totale de confiance des clients**
- **Interruption de plusieurs semaines de travail**
- **Responsabilité professionnelle engagée**
- Risque de **plainte** ou **procédure judiciaire**
- Suspensions administratives
- Perte financière importante : entre **5 000 € et 50 000 €**

L'activité serait **partiellement paralysée**, voire **totalement arrêtée**.

🎯 Objectifs RPO / RTO

RPO (perte de données maximale acceptable)

👉 **2 heures** Justification :

- les comptables encodent des pièces à longueur de journée
- perdre la matinée complète serait trop impactant
- sauvegardes fréquentes nécessaires

RTO (temps maximal pour restaurer)

👉 **4 heures** Justification :

- un arrêt total d'une journée serait financièrement grave
- l'entreprise doit pouvoir reprendre rapidement en cas d'incident majeur

---

🛠️ Besoins techniques liés au RPO/RTO

Besoin	Justification
Sauvegardes **incrémentales fréquentes**	pour respecter le RPO 2 h
Snapshots locaux	pour restaurer très rapidement la base SQL
Copie hors site	pour éviter les sinistres
Sécurisation par chiffrement	RGPD + en cas de vol
Immutabilité	protection ransomware
Test mensuel	garantie de restaurabilité

🧰 Infrastructure actuelle

- **Un serveur Windows 2019**
  - logiciel comptable
  - base SQL
  - partages SMB
- **Un NAS Synology 4 baies (RAID 5)**
  - sauvegarde automatique des dossiers
  - stockage de documents clients
- **Cloud Microsoft 365**
  - mails Exchange
  - OneDrive
  - SharePoint limité

🧩 Stratégie de sauvegarde recommandée

1. Sauvegarde locale rapide (NAS)

- Sauvegarde **complète hebdomadaire** du serveur
- Sauvegarde **incrémentale toutes les 2 heures**
- Snapshots immuables NAS (protection ransomware)

2. Sauvegarde externe (cloud)

- Backup quotidien du serveur dans un **cloud sécurisé** (ex : Synology C2, Backblaze B2)
- Rétention : **30 jours glissants**
- Chiffrement activé (AES-256)

3. Copies spécifiques

- Export quotidien de la base SQL
- Backup Outlook via Exchange Online native backup

4. Plan de test

- 1 restauration complète **chaque mois**
- 1 restauration fichier/snapshot chaque semaine

💰 Coût estimé

Élément	Coût
Sauvegarde locale NAS	inclus (déjà en place)
Cloud : 2 To	± 120 €/an
Logiciel de backup serveur	150–300 €/an
Temps de gestion	1–2 h / mois

Total ≈ **250 à 450 €/an** → Très faible comparé au risque financier.

📜 Résumé pour les élèves

Dans une PME comptable :

- Les données sont **très sensibles**.
- Le risque de ransomware est **extrêmement élevé**.
- RPO = 2 h → sauvegardes fréquentes.
- RTO = 4 h → snapshots + local.
- Stratégie recommandée : **NAS + snapshots + cloud + immutabilité**.
- Coût raisonnable comparé au risque.

© 2025 Mr. Lambrechts
https://v2.ttrinfo.be
6 | 6