PRA/PCA

---

1. Analyse d’impact (BIA) : La priorisation

Service	Criticité	RTO (Temps de reprise)	RPO (Perte données)	Justification Métier
ERP (hébergé)	Critique	1 h	1 h	Gestion production et stocks multisites ; arrêt = pertes financières directes.
AD / DNS / DHCP	Haute	4 h	1 h (données sensibles)	Authentification centralisée et résolution noms essentiels pour accès multisites aux opérations production et administration.
Messagerie	Haute	4 h	1 jour	Communications internes/externes vitales pour coordination équipes et clients sur sites dispersés.
Supervision (Zabbix)	Haute	4 h	1 jour	Monitoring global pour détection proactive incidents sur infrastructure étendue.
Serveurs de fichiers	Moyenne	4 h	1 jour	Partage documents critiques pour collaboration inter-sites, impact sur productivité sans interruption majeure.
Serveur d'impression	Basse	24 h	1 jour	Service auxiliaire ; impact limité sur flux métier principal.

2. Architecture technique (PCI)

Pour protéger Dubois Escalier - site de Lille [siège], la simple copie des fichiers sur NAS ne suffit pas.
Risques d'incendie, Ransomwares ou autres...

Règle du 3-2-1-1-0

Focus : La protection Anti-Ransomware

En fonction de la volumétrie

- **Stockage Cloud Immuable (Object Lock) :** (Via Veeam, Wasabi). Même si le pirate est administrateur, il ne peut pas effacer cette sauvegarde pendant X jours.

Stratégie de reprise (PRI) :

En cas d'incendie salle serveur :

- **L'idéal PME :** Restauration depuis le Cloud (Wasabi) vers du matériel de prêt ou vers une instance Cloud (Azure/AWS) temporaire.

---

3. Procédure de crise

Scénario : Détection d'un Ransomware sur l'ERP.

1. **ISOLEMENT (Immédiat) :** Débrancher les câbles réseau des machines infectées. Couper le Wi-Fi/Internet général pour stopper l'exfiltration de données. **Ne pas éteindre les serveurs** (pour l'analyse forensique ultérieure), sauf si le chiffrement est visiblement en cours.
2. **QUALIFICATION :** Réunion de crise (DSI , Rh, Production, Direction.....). Vérification de l'état des sauvegardes (sont-elles saines ?).
3. **ASSAINISSEMENT :** On ne nettoie pas un serveur compromis, on le reconstruit. Formatage bas niveau des disques infectés.
4. **RESTAURATION (L'ordre est vital) :**
    - Étape A : Restauration du **Réseau** et du **Contrôleur de Domaine (AD)**
    - Étape B : Restauration du **SGBD (Base de données)**.
    - Étape C : Restauration du **Serveur Applicatif (ERP)** et reconnexion à la base.
5. **TESTS MÉTIER :** Validation par un utilisateur clé (Compta/Logistique) avant réouverture générale.