Votre entreprise peut-elle tenir deux semaines sans informatique ?

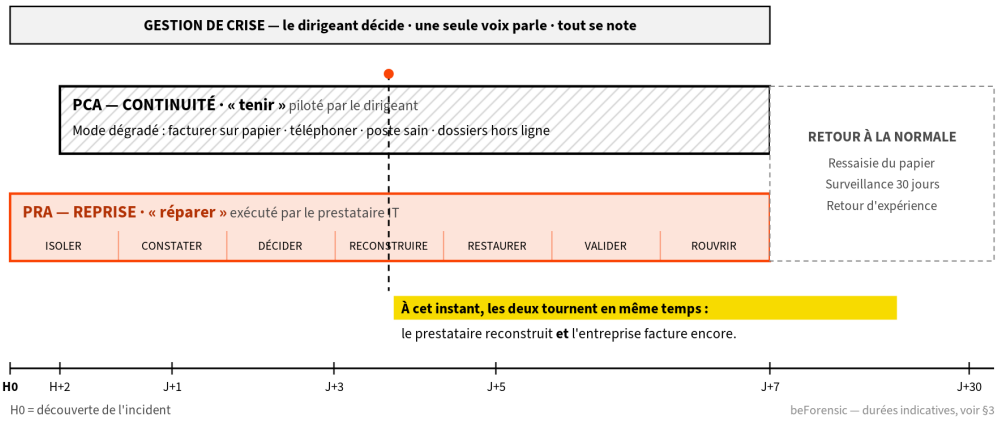
Pour le dirigeant de TPE ou PME. Une petite entreprise arrêtée par un incident informatique perd en moyenne une à deux semaines d'activité. Les charges continuent. La facturation s'arrête. Certains clients ne reviennent pas. La plupart des TPE n'ont ni plan écrit, ni sauvegarde testée, ni personne désignée pour décider le jour venu.

Deux questions, et non une seule

Quand l'informatique tombe, on pense d'abord à réparer. C'est la seconde question, pas la première.

> **« Comment fait-on pour travailler quand même ? »** → le plan de **continuité** (PCA).\
> **« Comment répare-t-on ? »** → le plan de **reprise** (PRA).

Le premier vous fait gagner du temps. Le second vous rend votre outil de travail.



Les deux ne se succèdent pas : ils se recouvrent. Au troisième jour, votre prestataire reconstruit le serveur pendant que vous facturez encore sur papier. Croire qu'il faut avoir fini de réparer pour reprendre le travail est l'erreur la plus coûteuse.

Trois mesures traitent l'essentiel du risque

	Mesure	Coût indicatif
1	**Double authentification** sur la messagerie et l'accès bancaire	souvent déjà inclus dans votre abonnement
2	**Une sauvegarde déconnectée, conservée hors de vos locaux**	quelques centaines d'euros par an
3	**Un test de restauration réel, une fois par an**	une demi-journée de votre prestataire

Une sauvegarde qui n'a jamais été restaurée n'est pas une sauvegarde. C'est une hypothèse.

Le jour venu

Isoler — débrancher le réseau. **Ne pas éteindre les machines** : elles contiennent les preuves. Débrancher aussi le disque de sauvegarde, sinon il sera chiffré à son tour.\
Appeler — votre prestataire informatique, puis votre assureur. Le délai de déclaration est souvent de 24 heures.\
Noter — sur un cahier papier, heure par heure. C'est la pièce maîtresse de votre dossier d'assurance.\
Ne jamais payer la rançon · réinstaller vous-même · continuer à utiliser la messagerie compromise.

> **Une horloge démarre sans prévenir.** Si des données personnelles sont touchées — fichier clients, personnel, contacts — vous disposez de **72 heures** pour le notifier à l'Autorité de protection des données. Le délai court dès la **découverte**, pas depuis la fin du diagnostic.

Trois questions à poser à votre prestataire informatique cette semaine

1. **À quelle date avez-vous restauré nos données pour de vrai, en chronométrant ?**

2. **Notre sauvegarde est-elle débranchée du réseau, et où est la copie hors site ?**

3. **Si je vous appelle un vendredi à 18 h, en combien de temps intervenez-vous — et est-ce écrit dans notre contrat ?**

Si ces trois réponses ne viennent pas immédiatement, vous connaissez vos trois premiers chantiers.

Pour aller plus loin

BreakPoint — votre plan de crise sur 72 heures, adapté à votre métier. Aperçu gratuit, plan complet à 49 €. → breakpoint.beforensic.be\
Plan de continuité cyber — l'accompagnement qui prépare ce qui vient avant et après les 72 heures. → beforensic.be · contact@beforensic.be

beForensic · 35 rue André Masquelier, 7000 Mons · contact@beforensic.be · BE0724.581.585
Serge Houtain — 22 ans en cybercriminalité, ancien chef d'une Regional Computer Crime Unit de la Police Judiciaire Fédérale.