

Incendie, inondation, cambriolage : le numérique face au sinistre physique

Quand le sinistre emporte les locaux, il emporte serveurs, postes et papiers. Préparer le numérique à survivre au bâtiment.

7 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/sinistre-physique-locaux

Un incendie de zone artisanale, une crue, un cambriolage méthodique : le sinistre physique reste la façon la plus radicale de perdre son informatique — serveur, sauvegardes locales, postes, archives papier, tout ensemble. C'est le scénario qui justifie à lui seul la copie hors site, et celui qui teste le mieux la question : « demain matin, sans les locaux, comment travaille-t-on ? » La préparation coûte peu ; l'improvisation, elle, se paie en semaines d'arrêt.

1. Le principe : rien d'unique dans les murs

- La copie hors site des données : le pilier absolu — cloud ou site distant, chiffrée, testée ; le NAS ET son disque de sauvegarde dans la même armoire brûlent ensemble
- Les documents vitaux numérisés et répliqués : contrats, assurances, licences, archives légales — le classeur unique est un point de défaillance
- Les secrets accessibles hors site : mots de passe (le coffre du gestionnaire est cloud par nature), clés de récupération du chiffrement, codes — la restauration bloquée faute de clé est un classique
- La documentation de reconstruction hors site : l'inventaire, les configurations, les contacts — le PRA imprimé chez le dirigeant ET en cloud

2. Limiter les dégâts sur place

- Le local technique choisi avec bon sens : pas en sous-sol inondable, pas sous le ballon d'eau chaude, détecteur de fumée, onduleur contre les surtensions du sinistre électrique
- La détection : alarme intrusion et incendie reliées, remontées vers les téléphones — les premières heures font la différence, surtout la nuit
- Contre le vol : le chiffrement intégral transforme le vol de matériel en simple perte matérielle — sans lui, c'est une fuite de données avec notification CNIL
- Les équipements marqués et inventoriés (photos, numéros de série) : l'indemnisation et la plainte en dépendent

3. Le jour d'après : travailler sans les locaux

- Le scénario à dérouler à froid : où s'installe-t-on (domiciles, locaux d'un partenaire, espace de coworking) et avec quoi ?
- Le cloud comme assurance-locaux : messagerie, fichiers et outils en ligne rendent le redémarrage possible depuis n'importe où avec des portables neufs
- La téléphonie qui suit : renvois et softphones — le numéro de l'entreprise ne doit pas mourir avec le

standard physique

- Les priorités de reconstruction écrites : quoi restaurer d'abord, qui rappeler d'abord (clients), quelles échéances protéger (paie !)

CAS CONCRET

Retour d'expérience récurrent des entreprises sinistrées : celles qui étaient « cloud + copie hors site + portables » retravaillent en jours — parfois dès le lendemain, du salon du dirigeant. Celles qui étaient « tout sur le serveur du bureau, sauvegarde dans le tiroir » mettent des semaines, quand elles s'en remettent. La différence ne tenait pas au budget : elle tenait à trois décisions d'architecture prises avant.

4. L'assurance, avant et après

- Vérifier la couverture des équipements ET des pertes d'exploitation — et déclarer les évolutions (matériel, valeurs) pour éviter la sous-assurance
- Le volet cyber et le volet dommages sont distincts : le sinistre physique relève du second, la reconstitution de données parfois des deux — relire les deux contrats
- Après sinistre : tout documenter (photos avant déblaiement), déclarer dans les délais, et ne pas jeter les supports endommagés avant expertise — la récupération de données sur supports sinistrés existe (et le disque « mort » se détruit ensuite dans les règles)

L'essentiel à retenir

- 01 Garantir la copie hors site des données et des secrets
 - 02 Numériser et répliquer les documents vitaux
 - 03 Chiffrer tous les supports contre le scénario cambriolage
 - 04 Sécuriser le local technique (emplacement, détection, onduleur)
 - 05 Écrire le scénario « travailler sans les locaux »
 - 06 Vérifier assurance dommages ET pertes d'exploitation
-

Questions fréquentes

Notre serveur est trop gros pour le cloud. Comment faire du hors site ?

Plusieurs voies : la sauvegarde cloud ne concerne que les DONNÉES (pas la machine) et se dimensionne souvent mieux qu'on ne croit ; la rotation de supports chiffrés vers un second site (le coffre de la banque, un autre établissement) reste valable ; et la réplication vers un petit NAS au domicile du dirigeant (chiffrée !) couvre beaucoup de TPE. L'important est le principe : une copie que le sinistre des locaux ne peut pas atteindre.

Le coffre-fort ignifuge du bureau suffit-il pour les sauvegardes ?

C'est mieux que l'armoire, mais lisez les spécifications : la plupart des coffres ignifuges protègent le PAPIER (les supports numériques meurent à des températures bien inférieures) — il faut un coffre certifié pour supports informatiques, plus rare et cher. Et le coffre ne protège ni du vol avec effraction lourde ni de la crue. Le hors site reste la réponse de référence ; le coffre, un complément.

À quelle fréquence revoir ce dispositif ?

Une fois par an, adossé à l'exercice PRA : les données ont grossi (la copie hors site suit-elle ?), le matériel a changé (inventaire à jour ?), l'assurance couvre-t-elle les valeurs actuelles ? Et à chaque déménagement ou travaux — les sinistres aiment les périodes de transition.

Pour aller plus loin

Cybermalveillance.gouv.fr — les sauvegardes — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

Service-public.fr — que faire après un sinistre en entreprise — entreprendre.service-public.fr

Vos sauvegardes tiendraient-elles le choc ?

Mise en place, tests de restauration, plan de reprise : nous rendons votre activité résiliente, à votre échelle.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr