Crise cyber : les 10 premiers réflexes

Une check-list pour les premières heures (0–24h). L'objectif n'est pas de tout réparer immédiatement, mais de **stabiliser, préserver, décider et documenter** sans aggraver la situation.

À FAIRE AVANT TOUTE ACTION TECHNIQUE

- [ ] **1. Ne rien supprimer, réinstaller ou « nettoyer »** — avant d'avoir qualifié la situation — vous détruiriez des preuves.
- [ ] **2. Isoler ce qui doit l'être** — sans tout couper à l'aveugle ni arrêter l'activité par réflexe.
- [ ] **3. Préserver les traces** — journaux, captures d'écran, e-mails, alertes, horodatages.
- [ ] **4. Recenser les faits** — quoi, quand, quels systèmes, quels comptes, quels signaux.
- [ ] **5. Identifier le périmètre** — utilisateurs, prestataires, données, flux, dépendances.
- [ ] **6. Geler les décisions irréversibles** — virements, rotations massives, communication publique.
- [ ] **7. Constituer la cellule de crise** — direction, IT/sécurité, DPO/juridique, métiers, communication.
- [ ] **8. Évaluer l'impact métier** — activités à maintenir en priorité, mode dégradé acceptable.
- [ ] **9. Cadrer la communication** — interne, clients, partenaires — sobre, factuelle, validée.
- [ ] **10. Tenir une main courante** — heures, décisions, validations, preuves, actions engagées.

Un doute sur un actif critique, une fraude ou un accès compromis ?
Exposez les faits à un intervenant avant d'agir.

Ligne de crise · 09 73 37 47 16

Ce document est un aide-mémoire de cadrage. Il ne se substitue pas à l'analyse du contexte réel, aux obligations légales de notification, ni à un dépôt de plainte.