

Fiche réflexe : cyberattaque

Les 6 réflexes de la première heure. À conserver en version papier : votre SI peut être indisponible.

Mode d'emploi : imprimez cette fiche, complétez les contacts, gardez-la hors du système d'information.

Cochez chaque action réalisée. L'ordre des cards suit la chronologie d'une attaque type ransomware.

1 Isoler

- Déconnecter du réseau les machines suspectes (câble, wifi) sans les éteindre.
- Mettre hors réseau les sauvegardes encore saines.
- Suspendre les accès distants : VPN, comptes à privilèges, prestataires.

2 Alerter

- Prévenir le référent informatique et la direction par téléphone, pas par mail.
- Contacter le prestataire de réponse à incident ou cybermalveillance.gouv.fr.
- Entités régulées (NIS2, OIV, OSE) : notifier l'ANSSI sous 24 h.

3 Préserver les preuves

- Ouvrir une main courante horodatée, sur papier ou support sain.
- Photographier les écrans, conserver journaux et messages de rançon.
- Ne rien réinstaller ni restaurer avant l'analyse technique.

4 Notifier et porter plainte

- Violation de données personnelles : notifier la CNIL sous 72 h.
- Déposer plainte rapidement : c'est une condition d'indemnisation cyber.
- Prévenir l'assureur cyber et activer l'assistance prévue au contrat.

5 Fonctionner en mode dégradé

- Activer le volet cyber du PCA : procédures papier, postes hors domaine.
- Ouvrir un canal de communication de secours hors du SI compromis.
- Prioriser les activités vitales : paie, production, sécurité des personnes.

6 Communiquer

- Parler d'une seule voix : porte-parole désigné, messages factuels.
- Informer salariés, clients et partenaires par des canaux alternatifs.
- Ne pas céder à la rançon d'emblée : le paiement ne garantit rien (ANSSI).

À ÉVITER

- ✗ Ne pas éteindre les machines compromises : les preuves en mémoire disparaissent.
- ✗ Ne pas gérer la crise depuis la messagerie potentiellement compromise.
- ✗ Ne pas annoncer un retour à la normale avant la fin de l'investigation.

BESOIN D'UN ACCOMPAGNEMENT ?

Contactez-nous

Premier rendez-vous téléphonique sans engagement.
Discrétion absolue, NDA signé dès le lancement de la mission.

Benoît Labalette

06 32 89 01 81

benoit@scopic.fr

twist-conseil.fr