# Attaque par ransomware
# Réagir en 5 étapes

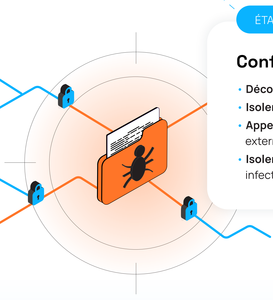
ÉTAPE #1

## Identifier l'attaque

- Vos outils informatiques **ne répondent plus** ou fonctionnent anormalement
- Vos fichiers se **modifient en masse**
- Un **document ReadMe** apparaît

**À ne (surtout) pas faire**

Ne jamais prendre contact directement avec l'attaquant et entamer la négociation.



ÉTAPE #2

## Confiner et contenir l'attaque

- **Déconnecter le SI** d'Internet
- **Isoler** les pans du réseau qui ont été infectés
- **Appeler le CERT** interne ou solliciter un CERT externe
- **Isoler vos sauvegardes** pour éviter qu'elles soient infectées

ÉTAPE #3

## Se structurer pour faire face à l'incident

### Activer une cellule de gestion de crise

- **Dérouler votre protocole** de gestion de crise (organisation, moyens, processus)
- Si rien n'a été anticipé, **réunir les décisionnaires** et mettre en place la procédure.
- Vérifier que votre **BIA est à jour** pour anticiper les étapes de remise en ordre de votre SI

**Bon à savoir**

Stocker cette procédure en lieu sûr et l'élaborer en amont peut faire gagner du temps.

### Remédier

Si il y a un CERT, **échanger** et définir les actions à mener pour éradiquer l'incident.

**Bon à savoir**

Des **fiches de réponses** à incident du CERT d'Advens peuvent vous aider à appliquer les bonnes pratiques.

En accès libre sur notre site !

### Lancer une communication de crise

- **Informer** vos équipes en interne et donner les directives
- **Rassurer et communiquer** tout de suite auprès de votre écosystème
- Anticiper les sollicitations éventuelles **des médias**

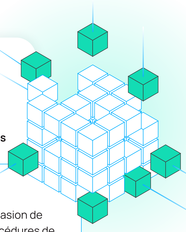
**Bon à savoir**

En fonction des lois qui s'appliquent, il peut être obligatoire de notifier l'attaque auprès des **autorités compétentes.**

ÉTAPE #4

## Restaurer et reconstruire son SI

- Restaurer et reconstruire de façon la **plus robuste possible** les éléments stratégiques de votre SI
- Rendre les autres pans du système d'information **plus résistants**



**Bon à savoir**

Cette étape est l'occasion de mettre à jour vos procédures de gestion de sécurité (gestion des accès administrateurs, etc).

ÉTAPE #5

## Clôturer et détecter la fin de la crise

- **Officialiser** le retour à la normale
- **Pérenniser** les outils et actions mis en place (ex : EDR...)
- Organiser un **post-mortem** en interne
- S'assurer de donner les moyens (temps, argent, énergie) pour **finaliser le plan de sécurisation**

Se protéger au plus tôt pour écarter les risques de cyberattaques est devenu essentiel.

Le CERT Advens a publié des fiches de réponses à incident qui pourront vous être précieuses en cas d'incident.

**Rendez-vous sur GitHub !**
github.com/cert-advens/IRM

By inwox