

✳ Évènement - Collectivité

## Évènement 01

Phase 1 - Tour 1

### Indisponibilité généralisée des services

Début de l'incident

#### Suite d'évènements :

- **Agendas bloqués** : plusieurs élus et le secrétariat ne peuvent plus accéder aux agendas et gérer les rendez-vous.
- **Paie et fichiers internes inaccessibles** (contrats, commandes) – le technicien support investigate sur les causes du problème.
- **Application "Ma Cantine" inopérante** : les parents s'inquiètent de ne pas pouvoir réserver les repas pour les prochains jours.
- **Volet médiatique** : Sur X, un administré interroge la commune sur l'indisponibilité de l'application depuis plusieurs heures et questionne la possibilité d'une cyberattaque.

Face à cette situation, votre mission est de prendre les meilleures décisions pour répondre aux demandes des agents et des administrés.

✳ Évènement - Collectivité

## Évènement 02

Phase 1 - Tour 2

### Inquiétude générale

Nous sommes à + 45min après l'incident

#### Suite d'évènements :

- **Accueil saturé** : Les administrés sont accueillis avec plus de 2h de retard : certains s'impatient et deviennent agressifs.
- **Applications "Mon accueil Crèche" et " Temps périscolaire" indisponibles.**
- **Exigence des élus** : le maire exige un **point de situation toutes les 20 min.**
- **Gestion de la paie** : l'indisponibilité implique un **risque de non-versement sous 72h** pour les agents.
- **Volet technique** : les investigations sont en cours, mais prennent du temps : un seul technicien est mobilisé.

## Évènement 03

Phase 2 - Tour 1

### Confirmation d'une cyber attaque

Nous sommes à +1h30 après l'incident

#### Suite d'évènements :

- **La cyberattaque (rançongiciel) est confirmée :**
  - **Plusieurs systèmes sont bloqués :** Paie, cantine, périscolaire, crèche, rendez-vous, commandes/contrats, annuaire et fichiers chiffrés.
  - **Le technicien est débordé :** des **renforts sont nécessaires**.
- **Gestion dégradée :**
  - Les équipes sont en sous-effectif et doivent faire face au mécontentement des administrés.
  - Une commune voisine **recommande l'isolement des réseaux** pour limiter la propagation.
- **Risques sociaux :** Les représentants du personnel **menacent d'utiliser leur droit de retrait** à cause du manque d'information disponible.
- **Volet médiatique :** Des journalistes tentent d'obtenir des informations auprès des collaborateurs.

## Évènement 04

Phase 2 - Tour 2

### Constat de l'ampleur de l'impact

Nous sommes à +3h après l'incident

#### Suite d'évènements :

- **Volet technique :** les sauvegardes sont compromises, la récupération s'avère incertaine et lente.
- **Demande de rançon :** une demande de rançon de 500 000 euros a également été publiée par les attaquants.
- **Application "Mon accueil crèche" :** les fiches santé sont inaccessibles, les soins ne pourront être réalisés ce midi.
- **Bibliothèque :** les emprunts sont bloqués
- **Gestion dégradée :** les équipes commencent à fatiguer. Elles demandent des renforts et la **mise en place d'un système de repos** pour tenir dans la durée.

## Évènement 05

Phase 3 - Tour 1

### Détection de fuite de données

Nous sommes à +6h après l'incident

#### Suite d'évènements :

- **Fuite de données** : des administrés signalent que **les attaquants revendiquent avoir volé et publié des données** sur le dark web (analyse en cours).
- **Volet technique** : La dernière sauvegarde saine date d'une semaine. Il faudra **3 jours pour les réinstaller**, puis relancer progressivement les applications.
- **Volet médiatique** :
  - Un élu **alerte sur le coût** (prestataires, matériel) alors que la commune est déjà endettée.
  - Un autre **dénonce le manque d'investissements** en matière de cybersécurité sur les réseaux sociaux.

## Évènement 06

Phase 3 - Tour 2

### Adaptation en mode dégradé

Nous sommes à +7h après l'incident

#### Suite d'évènements :

- **Volet technique** :
  - **100% des serveurs sont chiffrés** : un **rachat est nécessaire** pour reconstruire une infrastructure saine.
  - **Plus de 50% des postes sont infectés** → 70 postes sont à rebooter/remplacer.
  - **La fuite de données est confirmée** : contrats, noms et prénoms, numéro de téléphone, adresse et mails d'administrés et de collaborateurs).
- **Gestion dégradée** :
  - **3 semaines minimum** prévues.
  - La commande des **chèques-vacances** doit être validée sous 24h, mais le fichier de **commandes est inaccessible**.
- **Volet médiatique** :
  - 2 journalistes relancent les collaborateurs.
  - 1 tweet et 1 article local ont été publiés sur la **fuite de données** et le **risque de surendettement**.