PRÉFET
DES BOUCHES-
DU-RHÔNE
Liberté
Égalité
Fraternité

ATD13
AGENCE TECHNIQUE DÉPARTEMENTALE

Fiche-réflexe « Paralysie des systèmes d'information »

Que faire en cas d'attaque par rançongiciel ?

INTRODUCTION

Dans un contexte de numérisation croissante des activités d'une commune, l'un des principaux risques identifiés est **la paralysie de tout ou partie des systèmes d'information** de la commune et/ou des systèmes du prestataire qui hébergerait l'une de ses applications.

Cette situation, empêchant alors la commune d'assurer ses services et activités essentielles, peut notamment être **induite par une cyberattaque**, **via le déploiement d'un rançongiciel.**

PERIMETRE D'APPLICATION

La fiche-réflexe « paralysie des systèmes d'information » est à utiliser **dans le contexte particulier d'une cyberattaque par rançongiciel** qui :

- ciblerait **directement** les systèmes d'information d'une commune, rendant inaccessible tout ou partie de ses fichiers et/ou applications ;
- ou impacterait les systèmes d'information **d'un prestataire** (informatique ou hébergeur), rendant indisponible au niveau de la commune le(s) service(s) rendu(s).

Une attaque par rançongiciel consiste à déployer un programme malveillant pour obtenir de la victime le paiement d'une rançon. L'attaquant met alors l'ordinateur ou le système d'information de la victime hors d'état de fonctionner, de manière supposée réversible.

Cela peut se matérialiser par :

- La présence d'un message de demande de rançon, qui peut prendre plusieurs formes (fichiers texte, fond d'écran, popup, etc.) ;
- L'impossibilité de lire le contenu de fichiers de travail ;
- Le changement des extensions des fichiers désormais illisibles ;
- Le comportement anormal de certaines applications ;
- Une exfiltration de données.

L'attaquant adresse alors un message à la victime dans lequel il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.

Les événements accidentels, c'est-à-dire ne résultant pas d'une activité malveillante sur les SI, et les actions malveillantes n'entraînant pas l'interruption immédiate et majeure des services essentiels de l'organisation sont par conséquent exclus du périmètre de définition. Néanmoins, les recommandations de cette fiche **peuvent être utilisées comme bonnes pratiques pour faire face à ces situations**.

OBJECTIFS ET LIMITES DE LA PRESENTE FICHE

Ce document a pour objectif de recenser les principaux points d'attention (techniques ou non) utiles pour guider la conduite de la gestion de crise en cas d'attaque par rançongiciel.

Volontairement synthétique et généraliste, **son contenu ne peut en aucun cas remplacer la compétence des experts** requis pour aider à l'endiguement, l'analyse, la remédiation ou la restauration suite à une attaque. De la même manière, **les consignes des forces de sécurité intérieure ou de toutes autres autorités en charge (comme l'ANSSI) doivent primer** lorsqu'elles s'inscrivent dans le cadre législatif et réglementaire idoine.

Plusieurs actions préventives, permettant de réduire la probabilité d'une cyberattaque, sont détaillées dans la fiche thématique « Cyberattaques » également fournie.

1. ANALYSE DE LA SITUATION

- ☐ Remonter tout incident ou dysfonctionnement à la chaîne fonctionnelle. *[Décrire le processus défini et les contacts associés]*

- ☐ Qualifier la situation au travers d'une première analyse rapide et estimer ainsi :

  - Le caractère malveillant du dysfonctionnement (*versus* la simple panne) ;

    Attention, la caractérisation d'une cyberattaque peut être plus ou moins longue (plusieurs heures) en fonction des informations remontées. Par ailleurs, l'identification de l'origine de l'attaque est longue (plusieurs jours voire semaines) et complexe (besoins de logs, expertise), et ne constitue pas un prérequis aux premières actions de gestion de crise.

  - La criticité de la situation, notamment en matière d'impact sur l'activité.

- ☐ En cas d'incident majeur, donner l'alerte auprès de l'autorité qualifiée à déclencher le dispositif de gestion de crise (PCS) et les actions induites par son déclenchement, dont l'information de l'autorité préfectorale. *[Décrire le processus défini et les contacts associés]*

➔ *Il est recommandé de se référer aux autres fiches réflexes de votre PCS (voir notamment le guide d'élaboration d'un PCS mis à disposition par la préfecture des Bouches-du-Rhône).*

2. ACTIONS A MENER EN CAS D'ATTAQUE PAR RANÇONGICIEL

• PREREQUIS

Pour être efficace, la gestion d'une crise d'origine cyber repose sur des compétences particulières (ex : maîtrise des systèmes d'information, expertise interne ou externalisée) et un dispositif spécifique (ex : chaîne d'alerte dédiée, outils résilients, gouvernance).

Des actions préparatoires sont ainsi nécessaires pour mettre en place une organisation de crise adaptée.

Voir les sous-sections « Prérequis » et « Gouvernance » de la fiche thématique « Cyberattaques ».

• MESURES D'URGENCE

- ☐ **Débrancher les ordinateurs ou les serveurs du réseau sans les éteindre.**

  Débrancher le câble Ethernet de chaque ordinateur et de chaque serveur infecté, et désactiver leur connexion Wi-Fi pour isoler ces machines. En cas de doute, faire de même pour l'ensemble des machines.

  

  Attention : si cela paraît contre-intuitif, le fait d'éteindre un appareil infecté ou suspect peut aggraver la situation au redémarrage, et/ou supprimer des indices et preuves pour l'investigation. Il faut donc laisser ces équipements allumés après les avoir isolés du réseau.

- ☐ **Ne pas allumer les machines qui seraient éteintes avant l'attaque** (afin d'éviter de les infecter).

- ☐ **Alerter les services ou le prestataire informatique.** *[Coordonnées à insérer]*

- ☐ **Solliciter de l'aide pour la résolution technique de l'incident** *[Coordonnées à insérer. Exemples : CERT-FR ; CSIRT régional « Urgence cyber, Région Sud » ; Expert Cybermalveillance ; prestataire informatique ; assurance cyber].*

- ☐ **Vérifier que les sauvegardes sont bien isolées.** Si ce n'est pas le cas, les débrancher du réseau (voir ci-dessus).

- ☐ **Décider de couper (ou non) la connexion à Internet pour éviter la propagation de l'attaque** (via la box ou l'équipement de cœur de réseau).

  Isoler d'Internet le système d'information a généralement des impacts majeurs sur son fonctionnement et les services métiers. Il est préférable d'avoir préparé cette procédure en amont, en ayant pris en compte les situations en heures ouvrées et non ouvrées (qui valide, qui procède à l'opération technique).

- **Ne pas payer la rançon.**

Même si le montant de la rançon paraît parfois accessible, rien n'assure après paiement que les fichiers seront déchiffrés ou que l'ordinateur sera de nouveau utilisable. De plus, cela peut contribuer à alimenter un système et démarrer un cercle vicieux : après avoir payé, la commune risque d'être identifiée comme « bon payeur » par les cybercriminels.
Dans certains cas, une solution de déchiffrement existe (voir le site No More Ransom).

• RESOLUTION TECHNIQUE DE L'INCIDENT

La résolution technique d'un incident cyber peut requérir plusieurs semaines à plusieurs mois de travail de la part des équipes internes et/ou du prestataire :

- Dans un premier temps, il est en effet nécessaire d'identifier les raisons du succès de la cyberattaque (notamment le vecteur d'intrusion) pour définir le périmètre de compromission du système d'information, et par conséquent, le niveau de maîtrise dont dispose l'attaquant.
- La compréhension de ces deux éléments doit permettre dans un premier temps de limiter les actions de l'attaquant (endiguement) puis dans un second temps, de l'évincer des systèmes.
- En fonction du périmètre de compromission, des actions de reconstruction, potentiellement sur plusieurs semaines ou mois, pourront alors être envisagées.

- **Procéder à l'investigation**, de préférence avec l'aide du prestataire choisi, afin d'identifier la source de l'infection et prendre les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

- **Faire une analyse antivirale et comportementale du matériel** à l'aide d'une solution de type EDR (*Endpoint Detection and Response*).

- **Conserver les preuves (après avoir pris consigne auprès des forces de sécurité intérieure)**, notamment pour pouvoir porter plainte (ex : le message piégé, les fichiers de journalisation (logs) de votre pare-feu, des copies des postes ou serveurs touchés). *Voir la section « enjeux juridiques ».*

➔ ***Si l'on sait garantir l'éradication des éléments malveillants*, réinstaller les systèmes impactés** en effectuant une restauration complète des systèmes infectés, en reformatant les postes ou serveurs touchés, en lançant une réinstallation complète de ces équipements puis des données depuis une sauvegarde vérifiée comme saine.

➔ **Reconnecter le ou les matériels à Internet et/ou aux connexions extérieures existantes,** en s'assurant de la non-persistance des attaquants.

Une reconnexion à Internet ou aux réseaux des partenaires alors que la source de l'infection n'a pas été identifiée et corrigée peut permettre aux attaquants de continuer leurs actions malveillantes.

3. AIDE-MEMOIRE : ACTIONS A MENER EN PARALLELE

• COMMUNICATION DE CRISE

En fonction de l'impact de l'attaque, il est possible que les outils de communication nominaux (ordinateurs, téléphones, site web) soient indisponibles. Il est nécessaire d'anticiper ce point en envisageant des outils résilients.

☐ **Définir le plan de communication,** en fonction des publics ciblés (contenu du message, moyens de communication, temporalité).

☐ **Alerter et informer les différents publics** :

- *En interne : vers les agents, afin de leur indiquer les consignes et les modalités de continuité de service.*
- *En externe (liste non-exhaustive) :*
  - *Vers les administrés, pour les informer des consignes à suivre et des modalités de la continuité de service.*
  - *Vers l'intercommunalité, en particulier pour éviter une propagation (latéralisation) de l'attaque.*
  - *Vers les autorités (préfecture dans le cadre du déclenchement du PCS, CNIL, etc.).*
  - *Vers vos prestataires et partenaires (trésorerie, fournisseurs, etc.), pour éviter une propagation (latéralisation) et les prévenir des difficultés à venir.*
  - *Vers la presse.*
  - *Sur votre site web.*
  - *Sur les réseaux sociaux.*

☐ **Mettre en place une veille sur les réseaux sociaux,** pour faciliter le suivi des impacts de la communication et anticiper les actions.

☐ **Veiller à informer chaque public concerné de la sortie de crise.**

• CONTINUITE D'ACTIVITE

☐ **Lister l'ensemble des services et activités impactés et se poser la question des impacts induits sur la collectivité (en fonction du contexte socio-politique).**

☐ **Mettre en place les solutions de travail provisoires.**

Il est particulièrement risqué de remettre en production le système d'information impacté tant que les investigations et la remédiation n'ont pas abouti.
Il est donc préférable d'avoir prévu des systèmes alternatifs et provisoires afin de fournir quelques services essentiels, notamment pour la gestion de crise (téléphones avec partages de connexion, postes informatiques isolés avec imprimantes directement connectées, fax, messagerie externalisée provisoire, etc.).

☐ **Identifier les services et activités à relancer / reconstruire en priorité.**

Le plan de continuité d'activité (PCA) et/ou le plan de reprise d'activité (PRA) sont deux documents permettant d'identifier les activités essentielles d'une commune et les moyens d'assurer leur continuité (de manière dégradée ou nominale).
Une priorisation des actions techniques est faite en fonction des besoins de continuité d'activité et des obligations légales que doit respecter la commune (ex : fourniture de l'état civil – voir section « enjeux juridiques »). Elle est validée par le maire. Des communications aux utilisateurs et aux parties prenantes externes sont réalisées quand les services rouvrent.

☐ **S'assurer en particulier qu'il est possible de verser** la paie des agents et/ou les prestations sociales aux administrés.

En cas d'indisponibilité des éléments financiers, il peut être envisagé de se baser sur le versement effectué le mois précédent. Il est recommandé de contacter la DDFIP pour traiter ce sujet.

• METTRE EN PLACE UNE LOGISTIQUE ADAPTEE AUX ENJEUX ET A LA DUREE DE LA CRISE

➔ *Il est recommandé de se référer aux autres fiches réflexes de votre PCS (voir notamment le guide d'élaboration d'un PCS mis à disposition par la préfecture des Bouches-du-Rhône).*

• RESSOURCES HUMAINES

☐ **Redéployer les agents sur certaines activités.**

La perte des services numériques augmente le temps de travail (ex : rédaction à la main, archives). Pour gagner en efficacité sur ce qui est important et prioritaire, il peut être nécessaire de redéployer du personnel (notamment des agents dont l'activité serait à l'arrêt suite à l'attaque).

☐ **Préserver les agents en assurant des roulements et des créneaux de repos** (en particulier pour les équipes informatiques).

En complément, de la restauration, des moyens de transport peuvent être mis à disposition des équipes impliquées (notamment en dehors des jours/heures ouvrés habituels). Un réaménagement temporaire d'une partie des locaux peut être effectué si nécessaire.

• ENJEUX JURIDIQUES

☐ **Identifier si certaines obligations auprès des administrés, des partenaires ou des fournisseurs ne peuvent pas être respectées.**

Le cas échéant, adapter le plan de continuité/reprise d'activité pour garantir des actions prioritaires. Dans un contexte d'élections, il est également important de pouvoir assurer le déroulement du processus électoral.

- **Porter plainte** auprès du commissariat de police ou de la brigade de gendarmerie dont dépend la commune (au plus tôt et en parallèle de la résolution technique de l'incident).

- **En cas d'atteinte aux exigences en matière de protection des données personnelles, déclarer son incident auprès de la CNIL** [*Notifier une violation de données personnelles | CNIL].*

- **Renforcer la vigilance vis-à-vis des fraudes d'opportunité.**

Des personnes malintentionnées, informées de la cyberattaque visant la commune, peuvent profiter de la situation pour commettre des fraudes (ex : fraude au faux virement). Il est conseillé de mettre en place des processus de vérification et de validation, en particulier pour les paiements.

• SORTIE DE CRISE

- **Vérifier que les conditions nécessaires à la sortie de crise sont atteintes.**

Les conséquences d'une attaque sur l'activité d'une commune peuvent être visibles pendant plusieurs mois, voire après une année (ex : maintien de processus dégradés, réinstallation du matériel).

- **Veiller à informer tous les publics concernés de la sortie de crise.**

- **Effectuer un retour d'expérience sur la crise** (et adapter la fiche-réflexe en conséquent).

Le préfet de département a validé le 13 avril 2023 un dispositif départemental opérationnel post-événementiel (DDOPE). Ce document recense les principes d'actions à mettre en œuvre, tant par les services de l'État et les collectivités territoriales que par les acteurs associatifs et le secteur privé pour œuvrer à la résilience, après la survenue d'un événement d'ampleur ayant gravement impacté un territoire et sa population. Il présente les dispositifs connexes facilitant la gestion post-événementielle et le retour à la normale (plan de continuité d'activité, retour d'expérience). Ce document est communicable sur demande à l'adresse pref-siracedpc@bouches-du-rhone.gouv.fr