

Réflexes Cyber + **GRILLE D'OBSERVATION**

PHASE 1 DU SCÉNARIO

Bonne pratique 1 :

Déclencher un dispositif de gestion de crise

- Un passage en crise a-t-il été acté ? 0 – 1 – 2 – 3 – 4

- Une personne a-t-elle désignée pour piloter la crise ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Comment faciliter la conduite d'un événement extraordinaire et stressant ?

La mobilisation d'une cellule de crise, organisée autour de rôles et procédures est une solution à ce problème.

Pour être efficace, il est important que la cellule soit pilotée par un ou une directrice de crise, qui prend les décisions, accompagnée d'une personne en charge de la main courante et d'une personne en charge du lien avec les équipes IT/cyber et prestataires.

PHASE 1 DU SCÉNARIO

Bonne pratique 2 :

Réaliser des points de situation

- Un état de la situation a-t-il été rapidement réalisé (spontanément) ?
0 – 1 – 2 – 3 – 4

- Des décisions ont-elles été actées à l'issue de ces points ? 0 – 1 – 2 – 3 – 4

- D'autres points ont-ils été réalisés de manière régulière ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Réaliser un point de situation permet de dresser un état de lieux à un instant T :

- Lister ce qui est à l'arrêt et ce qui est encore opérant.
- Identifier les difficultés rencontrées.
- Remonter les sollicitations, etc.

Pour l'organiser, il est souhaitable que chaque représentant des services prenne la parole pour remonter un état des lieux. Il est également possible de partager des propositions d'actions.

Une fois le tour de table réalisé, le directeur ou la directrice de la cellule crise propose un plan d'action, qui fait l'objet d'une prise de note (par exemple dans la main courante).

Un pilotage unique permet de fluidifier la conduite de la crise et facilite le suivi des actions.

PHASE 1 DU SCÉNARIO

Bonne pratique 3 :

Outiller la cellule de crise

- Les événements sont-ils consignés au travers d'une main courante ?
0 – 1 – 2 – 3 – 4

- Les joueurs ont-ils réfléchi à des méthodes pour fonctionner sans certains outils informatiques (annuaires, accès aux mails) ou sans confiance dans leur utilisation ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Consigner l'ensemble des événements et actions par écrit permet aussi de faciliter la réalisation d'un état des lieux.

Puisque la gestion de la crise s'organise sur plusieurs semaines, voire plusieurs mois, ce travail permet de garder une trace. Le document simplifie la prise de décisions ainsi que le roulement des équipes en cas de repos. Il peut aussi être demandé par les assurances pour certaines procédures.

Idéalement, la main courante (la liste l'ensemble des événements) et la liste des actions à réaliser sont consignées dans des documents distincts.

PHASE 1 DU SCÉNARIO

Bonne pratique 4 :

Partager des consignes vers le personnel

- Le personnel a-t-il rapidement été informé de la situation ?
0 – 1 – 2 – 3 – 4

- Des consignes ont-elles été partagées sur la conduite à tenir ?
0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

De nombreuses personnes au sein de l'organisation sont directement impactées par l'attaque, car elles ne peuvent plus réaliser leurs tâches quotidiennes.

Il est donc important de leur partager un état de la situation pour les informer de ce qu'elles peuvent faire ou non, les rassurer, voire les mobiliser.

Ces éléments sont construits par les équipes de la communication, qui identifient le meilleur format et le style de communication, en lien avec les équipes cyber et IT, qui expliquent ce qu'il se passe techniquement et ce qu'il faut faire ou ne pas faire.

PHASE 2 DU SCÉNARIO

Bonne pratique 1 :

Identifier les impacts et mettre en place des mesures pour maintenir une activité dégradée

- Une liste des impacts liés à la cyberattaque a-t-elle établie (à l'oral ou à l'écrit) ? 0 – 1 – 2 – 3 – 4

- Un plan d'action a-t-il été défini pour maintenir des activités essentielles ? 0 – 1 – 2 – 3 – 4

- Une liste des services et des activités à rétablir en priorité a-t-elle été établie ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Une cyberattaque est souvent vue comme un évènement technique. Pourtant, ses impacts métiers sont bien réels : sans accès à certains outils ou documents, l'activité de l'organisation n'est plus opérante. Identifier les liens de "cause à effet" est donc essentiel pour définir par la suite un mode de fonctionnement dégradé. Au sein d'une organisation, le plan de continuité d'activité (PCA) permet de guider ces réflexions.

Concernant les services inopérants, tout ne peut malheureusement pas être "réparé" en un instant : il faut d'abord comprendre ce que l'attaquant contrôle, à quoi il a eu accès, identifier la "porte d'entrée", etc. Le plan de reprise d'activité (PRA) et une cartographie du système d'information doivent également guider les actions de reconstruction / relance des activités

Dans ces deux cas, les décisions doivent être validées par la cellule de crise, en fonction du contexte politique, économique ou sociétal (ex : relancer le logiciel de paie pour verser les salaires).

PHASE 2 DU SCÉNARIO

Bonne pratique 2 :

Solliciter une aide extérieure

- Des prestataires spécialisés ou les équipes d'un centre de réponse à incident (CSIRT/CERT) ont-ils été sollicités pour aider les équipes techniques à gérer la cyberattaque ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Lors d'une attaque par rançongiciel (ou *ransomware* en anglais), l'attaquant parvient à chiffrer des données de l'organisation et les rend indisponibles.

Pour y arriver, il a dû s'introduire sur le réseau numérique via différentes techniques (phishing, exploitation d'une vulnérabilité), puis a cherché à prendre le contrôle de systèmes ou de comptes lui permettant de réaliser des actions sur les systèmes informatiques.

Pour comprendre cette chaîne d'attaque, (ou *kill chain* en anglais), il est essentiel que du personnel qualifié réalise des investigations, puis identifie les moyens "d'expulser" l'attaquant pour reprendre le contrôle du réseau.

Il est donc important de recourir à des prestataires spécialisés, qui peuvent également partager des conseils sur les moyens de gérer au mieux cette crise.

PHASE 2 DU SCÉNARIO

Bonne pratique 3 :

Mettre en place une stratégie de communication pour réagir aux sollicitations

- La communication externe a-t-elle semblé adaptée à la situation ? (ex : claire, non anxiogène, n'indiquant pas de date fixe pour une reprise d'activité) ? 0 – 1 – 2 – 3 – 4

- Une stratégie de communication vis-à-vis des journalistes a-t-elle définie ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Il est également important d'informer les clients, les prestataires ou les administrés des difficultés rencontrées. Si les impacts de l'attaque sont visibles par les publics externes, il est conseillé d'être transparent, tout en maîtrisant certaines informations sensibles (tout ne doit pas être dit).

Il est également essentiel de ne pas s'engager sur une date de reprise de l'activité, car cela peut être fluctuant.

Le sujet des cyberattaques étant par ailleurs fortement médiatisé depuis plusieurs années, il est important de préparer des éléments partageables aux journalistes.

Pour garder la maîtrise de l'information, il est recommandé d'identifier un porte-parole, qui centralise toutes les demandes et répond aux journalistes.

PHASE 2 DU SCÉNARIO

Bonne pratique 4 :

Décider de ne pas payer la rançon

- A-t-il été choisi de payer la demande de rançon ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Les attaquants exigent régulièrement que l'organisation paye une rançon pour récupérer ses données et/ou éviter qu'elles ne soient diffusées. S'il peut être tentant de le faire, il est cependant conseillé de ne pas choisir cette solution. En effet, il n'est pas garanti de récupérer les données (les attaquants peuvent être malhonnêtes et/ou la clé de déchiffrement peut ne pas fonctionner).

Par ailleurs, payer une rançon participe au financement du crime organisé.

Il est plutôt recommandé de porter plainte. Les services de police ou de gendarmerie (mais également certains prestataires) pourront vous aider à prendre la bonne décision (à noter que dans certains cas, il existe une clé de déchiffrement accessible gratuitement. Voir nomoreransom.org)

PHASE 3 DU SCÉNARIO

Bonne pratique 1 :

Échanger avec les autorités compétentes

- Les autorités (ex : préfecture) et/ou les organismes techniques compétents (ex : CNIL) ont-ils été prévenus ? 0 – 1 – 2 – 3 – 4

- Une plainte a-t-elle été déposée ? 0 – 1 – 2 – 3 – 4

Recommandation de l'ANSSI

Communiquer, c'est également penser à prévenir les autorités.

D'une part, parce que leurs missions de maintien de l'ordre et de la sécurité peuvent le requérir, mais également parce que ces dernières peuvent apporter un soutien ou partager d'autres contacts utiles lors de l'incident.