MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

LA MÉTHODE DE RAISONNEMENT TACTIQUE

Appliquée à la gestion de crise cyber

EDITO

Chaque crise est différente, la réponse doit donc être unique et adaptée à la situation. C'est la raison pour laquelle nous avons souhaité vous livrer quelques secrets de notre MRT.

Cette méthode structurée d'analyse vous aidera à faire face à votre crise de manière plus sereine. Elle vous forcera à ne rien oublier et à développer des réponses adaptées aux imprévus, car dans une crise cyber, l'imprévu est la norme.

La **MRT** se décompose en trois grandes étapes :

- La première, l'**ÉTUDE**. Elle vous permettra de poser les bases de votre problème et de tirer les premières conclusions. Il s'agit ici d'observer pour pouvoir orienter.
- La seconde, la **PLANIFICATION**, qui vous permettra de mettre au point votre stratégie et vos premières décisions.
- Enfin, la troisième, la **CONDUITE**. Elle correspond à la réalisation, à l'action.

En cas de survenance d'évènements que vous ne pouviez pas prévoir, vous procéderez alors à une nouvelle étude de la situation afin de prendre une nouvelle décision permettant d'atteindre vos objectifs initiaux.

Envisagez cette méthode non pas comme une étape obligatoire, mais bien comme un outil de plus à votre disposition, un moyen d'organiser vos réflexions de manière rapide et ordonnée. Sentez-vous libre, si vous l'utilisez, de l'adapter aux besoins et contraintes de votre organisation.

1. L'étude
observer et orienter

Que se passe-t-il ?

	Je constate que…	J'en déduis que… *(contraintes, obligations, demandes)*
Description de l'événement	*Description factuelle de la situation.*	*Que m'impose la situation ?* *Quelles sont les premières mesures à prendre ?* *De quoi vais-je avoir besoin rapidement ?*
Impacts opérationnels	*Décrire les effets de l'attaque sur le fonctionnement de mon organisation.* *Quels sont les services critiques touchés ?*	*Vais-je devoir réorganiser mon activité ? Prioriser des services ?* *Employer différemment mes personnels ?* *Communiquer ?*
Nature de l'alerte	*Qui a donné l'alerte ?* *Quels sont les premiers éléments ayant permis de caractériser le problème ?*	*Que peut-on en déduire sur l'origine de l'attaque ?* *Quels risques à prévoir (fuite de données personnelles, atteinte réputationnelle, vol du secret, etc.) ?* *Que dois-je envisager pour contrer ou limiter les effets ?*
Conséquences immédiates de la cyberattaque	*Quel est l'impact sur tout ou partie de votre activité ?*	*Quelles mesures prendre pour permettre une continuité d'activité en mode dégradé ?*
Aspect médiatique ?	*Les médias sont-ils informés ?* *Quelle est l'ampleur médiatique de l'événement ?* *Comment l'évènement est-il perçu ?*	*Quelles sont les premières actions de communication à mener ?* *Quelle stratégie de communication vais-je devoir adopter ?*
Précédents locaux, régionaux, nationaux ?	*Ai-je connaissance de cas similaires autour de moi en raison de l'actualité, de la localisation ou de l'activité de mon organisation ?*	*Comment pourrais-je bénéficier de l'expérience d'autres victimes ?*
Type d'action que l'on attend de moi dans ce contexte	*Quel est mon rôle dans la gestion de la crise cyber ?* *Suis-je intégré dans la cellule de crise ?* *Ai-je un rôle de coordinateur ?* *Communicant ? (…)*	*Quelles sont les contraintes auxquelles je suis exposé et mes obligations ?*

Où ?

Quelles sont les infrastructures et SI concernés par l'attaque ? (interne et externe)

	Je constate que…	J'en déduis que…
Dimension de la zone d'attaque *(données menacées, serveurs clés, position géographique…)*	*Décrire le périmètre de l'attaque* *(est-ce que tout ou partie de mon réseau est touché ? Tous mes sites sont concernés ?)* *Quelles menaces sur mes données ?*	*Où vais-je devoir concentrer mes efforts pour la réparation de mon réseau ?* *Dois-je anticiper une déclaration à la CNIL ?* *Dois-je envisager des fermetures de sites ?* *Dois-je faire stopper le télétravail ?*
Services impactés *(nature et position géographique)*	*Quels sont les services touchés par l'attaque et leur localisation ?*	*Quelles sont les contraintes humaines ? Les délais d'intervention ?* *Les besoins de coordination ?* *Comment organiser le maintien d'une activité minimale et est-ce nécessaire ?*
Aspects stratégiques, points clés	*Quels sont les points importants du réseau à protéger ou déjà infectés ?* *Où sont et quelles sont les données importantes concernant mes clients ou partenaires ?* *Quelles sont les données essentielles à la survie de mon organisation ?*	*De quels services ai-je besoin pour faire un bilan des risques actuels et futurs ?* *De même pour mes obligations juridiques vis-à-vis de mes clients ou partenaires.*

Quand ?

La gestion du temps dans la crise, quels impacts sur mon action et comment m'inscrire dans la durée ?

	Je constate que…	J'en déduis que…
Date et heure du début de l'attaque	*Date et heure du début de la crise.*	*En fonction du début de la crise, les contraintes, la capacité de montée en puissance et l'organisation des premières mesures d'urgence peuvent varier.* *Il faut donc les préciser pour les prendre en compte.*
Période de l'année	*Contexte de la période (vacances scolaires, hiver, été… ?), ai-je des événements prévus ?* *Sont-ils importants pour mon organisation ?*	*Le contexte lié à la période de l'année peut avoir un impact sur mon organisation en termes de ressources en personnels ou mon activité par exemple.*
Délais de préparation et montée en puissance de la cellule de crise	*Sous combien de temps ma cellule de crise peut-elle être opérationnelle ?* *Est-ce qu'une montée en puissance est possible ?*	*Au regard de mes contraintes de temps, l'activation de ma cellule de crise peut-elle être avancée ou est-ce suffisant ?* *Que puis-je faire pour optimiser la mise en place de ma cellule ?* *Comment puis-je la renforcer en cas de besoin ?*
Durée prévisible de la crise *(désengagement y compris)*	*En fonction du type de crise ou de la nature de l'attaque, quelle peut-être la durée prévisible de la crise ?*	*La crise cyber va durer (jours, semaines, mois), il faut préparer mon organisation et mes collaborateurs à durer dans le temps.* *Quelles mesures prendre (RH, logistique, financier…) ?*

Qui peut m'aider ?

	Je constate que…	J'en déduis que… *(contraintes, impératifs, demandes)*
Descriptif *(nature, capacités, volume)* **des moyens à ma disposition dans l'espace et dans le temps**	*Quelles sont les ressources à ma disposition ? (personnels, prestataires, outils, autorités capables de m'aider, etc.).*	*Je vais devoir organiser la coordination de mes ressources et identifier mes besoins en aide extérieure.*
Capacité de montée en puissance	*Qui est susceptible de venir renforcer mon dispositif ? (inventaire de mes ressources).*	*Comment alerter les personnes susceptibles de me renforcer et comment organiser leur intégration au dispositif ?*

Contre qui dois-je me protéger ?

Les cybercriminels peuvent-ils m'empêcher d'atteindre mes objectifs ?

	Je constate que…	J'en déduis que…
Description de l'attaquant (nature, volume, attitude, organisation) selon les informations obtenues	*À quel type d'attaque suis-je confronté ?* *Connait-on le groupe auteur ?* *Les motivations ? (Je peux me renseigner auprès de mes partenaires ou autorités compétentes).* *Est-il crédible ?*	*Les modes d'action du cybercriminel et donc comment réagir et anticiper ses prochaines actions.*
Objectif recherché (un par type d'adversaire identifié)	*Pourquoi suis-je attaqué ? (argent, nuisance, vol de données personnelles, vol du secret, etc.).*	*Quelles sont les conséquences sur mon réseau, mes services, mes données ?* *Si l'objectif est atteint, que peut-il encore faire ?* *Quelles certitudes puis-je avoir ?*

Que dois-je faire ?

Les étapes pour atteindre mon but	Les actions à mener
Établir les grandes étapes à exécuter et leur séquencement pour atteindre votre objectif.	*Décliner les actions à mener permettant de réaliser chacune des étapes.*

2. La planification
décider

Quelles décisions envisager à ce stade ?

Décisions	Objectifs
Après la phase d'analyse et d'élaboration de votre stratégie, répertoriez ici les décisions que vous souhaitez prendre pour que vos collaborateurs puissent les répercuter/ exécuter.	*Chaque décision prise doit répondre à un objectif clairement défini vous permettant d'avancer dans votre gestion de crise. Ma décision a pour objectif de...*

Que peut faire mon adversaire pour m'empêcher de réaliser mes actions ?

Actions	Objectifs
Réfléchissez aux actions ou réactions que pourrait avoir le pirate pour contrer vos mesures ou vous empêcher de résoudre la crise.	*Déterminez l'objectif recherché par le pirate. Cela vous servira à prioriser les actions selon leur possible impact et donc mieux concentrer vos efforts*

3. La conduite
agir

3. La conduite : Agir

Quelles décisions doivent être prises ?

Je décide...	Je conclus que...	Je demande à...
Notez ici les décisions qui seront mises en œuvre pendant la résolution de la crise.	**Avantages :** Quels avantages à appliquer ma décision ?	**Leader :** Personne en charge de l'exécution de la décision.
	Inconvénients : Quels inconvénients à appliquer ma décision ? (anticiper les aspects négatifs de la décision)	**Parties prenantes :** Parties prenantes : quels sont les services et/ou personnels qui mettront en œuvre directement la mesure prise ?
	Besoins : Quels sont mes besoins pour l'exécution de la décision ? (dois-je me faire aider ?)	**Concourants :** Qui peut contribuer à mettre en œuvre la décision ?

Je décide...	Je conclus que...	Je demande à...
	Avantages :	**Leader :**
	Inconvénients :	**Parties prenantes :**
	Besoins :	**Concourants :**

NOTES

COMCYBER-MI

« Nos forces, pour votre cyber-protection »

Conception et réalisation graphique : ComCyber-MI 2024-064 MB