< RÔLES ET FONCTIONS EN CRISE D'ORIGINE CYBER >

FICHE PRATIQUE

GROUPE DE TRAVAIL - GESTION DE CRISE CYBER ET ENTRAINEMENT

CAMPUS CYBER

La crise d'origine cyber est une forte source de déséquilibres, qui oblige les organisations à s'adapter et à fonctionner de manière inhabituelle. Ces bouleversements soudains et à l'échéance incertaine sont une source de stress et compliquent la prise de décision, alors même que des actions de remédiation doivent être décidées et exécutées rapidement pour limiter les impacts.
Pour répondre à ces enjeux, il a été proposé par le groupe de travail de construire des fiches pratiques, avec l'ambition de détailler pour 6 sujets d'intérêts des conseils et des bonnes pratiques, permettant par ailleurs de compléter la documentation existante sur des sujets peu traités à date.

Ces fiches visent principalement à accompagner la construction du dispositif de crise cyber, au niveau stratégique et opérationnel, et à orienter certaines prises de décisions en temps chaud. De ce fait, il est important qu'elles soient utilisées dans une logique de préparation à la crise.

Les sujets traités par le groupe de travail, en se basant sur l'expérience opérationnelle de ses membres sont les suivants :

- les rôles et fonctions en crise ;
- les enjeux relatifs à l'utilisation du cloud ;
- les enjeux de la supply chain.
- communication technique (en cours d'élaboration) ;
- anticipation & CTI (en cours d'élaboration) ;
- seuils et alerte (en cours d'élaboration).

Concrètement, ces fiches se veulent succinctes pour en faciliter la prise en main. Elles sont organisées autour d'une introduction du sujet traité et de bonnes pratiques à mettre en place ou à prendre en compte pour optimiser la gestion d'une crise cyber et en réduire l'impact.

STRUCTURER SON DISPOSITIF DE CRISE : UN ENJEU POUR ORGANISER AU MIEUX SA GESTION DE CRISE CYBER

La gestion d'une crise d'origine cyber implique une mobilisation à plusieurs niveaux de l'organisation : stratégique ou décisionnel, et opérationnel et/ou tactique. Différents profils doivent ainsi venir armer chaque niveau dans le but de pallier les effets de la crise. Pour faciliter l'appropriation et la mise en place du dispositif de gestion de crise, il est essentiel de **structurer les rôles et les missions de chacun et d'anticiper leur tenue sur le temps long.**

Ce dispositif est traditionnellement organisé autour d'un volet stratégique, porté à minima par une cellule de crise dite « stratégique » ou « décisionnelle ». **Cette cellule décide, arbitre et coordonne la gestion de la crise.** Elle regroupe les représentants des fonctions décisionnelles de l'entité, qui s'approprient les fonctions usuelles d'une cellule de crise : directeur de crise, personnes en charge du management de l'information, appui à la conduite de crise, représentants de l'ensemble des métiers et des services supports (communication, RH, logistique, juridique, IT, etc.).

Un volet opérationnel vient compléter cette organisation : composé de cellules organisées par métiers et services supports (communication, RH, logistique, juridique, IT, cyber, etc.), **ce volet rapporte l'état de la situation** vers la cellule décisionnelle via des représentants afin d'orienter sa gestion de la crise.

La particularité du scénario cyber **positionne les cellules métiers "cyber" et "IT" du volet opérationnel au sein d'une organisation inédite.** Ces dernières ont pour missions d'analyser et expliciter les risques, causes et conséquences d'une cyberattaque auprès du volet stratégique, tant sur les aspects techniques qu'en matière de continuité d'activité métiers. Elles ont également pour mission de préconiser et mettre en œuvre des mesures d'endiguement, de sécurisation ou de relance des systèmes d'information, il est donc important de veiller à ce que l'ensemble des briques qui composent ce dispositif se coordonnent de manière efficace.

Cette fiche a donc pour ambition de faciliter l'organisation et la structuration d'un dispositif de gestion de crise cyber en détaillant les fonctions essentielles à l'organisation d'un dispositif et en explicitant les missions et les compétences requises pour chacune. Les éléments présentés doivent ainsi être une source d'inspiration pour toute entité souhaitant créer ses propres "fiches-rôles".

Par ailleurs, le guide « Les clés d'une gestion opérationnelle et stratégique »[1] publié par l'ANSSI permet via une déclinaison pratique en 18 fiches d'adapter son dispositif de gestion de crise aux aspects plus spécifiques des crises d'origine cyber.

[1] Ce guide fait partie de la collection « Gestion de crise cyber », destinée à accompagner les organisations dans la préparation et la gestion de crise

LES PRÉREQUIS À LA MISE EN PLACE D'UN DISPOSITIF DE CRISE EFFICACE

NIVEAU 1 : LES ESSENTIELS

- Définir une gouvernance de crise en adéquation avec la structuration de l'entité et y associer des outils (annuaire, modèles) et procédures (fiches-rôles, fiches-réflexes) ;
- Disposer à minima d'une salle de crise (marquée comme telle) et de matériel adéquat et fonctionnel ;
- Former les parties-prenantes à l'utilisation des outils et procédures et les entrainer régulièrement. Vous pouvez vous référer au livrable "Stratégie d'entraînement" réalisé par ce même groupe de travail.

NIVEAU 2 : LES AVANCÉS

- Identifier les suppléants (back-up) des fonctions "essentielles" et formaliser un système de rotation qui prend en compte les aspects légaux (relatifs au code du travail) et de confort personnel ;
- Anticiper la logistique de crise (repas équilibrés, gestion des accès, kit de repos, garde des enfants, etc.) ;
- Identifier les besoins en compétences (mise en place de fichiers avec l'appui des RH, réalisation de matrices de compétences) et anticiper le recours à des expertises extérieures (pré-contractualisation) ;
- L'outil d'autoévaluation partagé par l'ANSSI permet à chaque organisation de mesurer son niveau de préparation et maturité dans le domaine de la gestion de crise et continuité d'activité face aux menaces cyber. Il permet par ailleurs d'identifier des axes d'amélioration.

ORGANISATION, FONCTIONS ET MISSIONS ASSOCIÉES

VOLET STRATÉGIQUE

Cette cellule n'est pas spécifique à la gestion d'une crise d'origine Cyber. C'est une cellule qui doit exister pour traiter les crises de toute nature.

Les fonctions détaillées ci-dessous composent la cellule décisionnelle du dispositif de crise. Si l'armement de certains rôles est essentiel au bon fonctionnement de l'ensemble, d'autres ne sont pas obligatoirement mobilisables (facultatif) : cela dépendra de l'intensité de la crise mais également des capacités de l'organisation à armer l'ensemble de ces fonctions.

Fonction
Direction de crise

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

Conduire la cellule de crise en :

1. Assurant son fonctionnement optimal (est notamment garant de ces règles de fonctionnement) ;
2. Définissant une stratégie de gestion de crise ;
3. Prenant des décisions qui orientent la conduite stratégique/opérationnelle de la crise, sur la base d'éléments remontés par les représentants des métiers ;
4. Remontant des informations vers la direction générale.

Compétences requises

- Bonne connaissance de l'entité (en particulier les métiers);
- Compétences de management transverse ;
- Capacités de prise de décision et leadership ;
- Capacités de prise de recul sur une situation ;
- Bonne connaissance des équipes de gestion de crise et de leur rôle ;
- Capacités de gestion humaine (ex : empathie, écoute) ;
- Compréhension des enjeux de crise cyber (vernis).

Fonction
Appui à la conduite

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

Soutenir le pilotage de la cellule et appuyer la direction de crise en :

1. Définissant le "rythme de bataille" de la cellule (horaires des points de situation, objectifs) ;
2. Assurant le suivi des actions ;
3. Assurant l'organisation des points de situation ;
4. Validant la cohérence et l'exhaustivité des informations remontées ;
5. Assurer un lien entre le volet stratégique et opérationnel [Dans le cadre d'une crise de haute intensité, la mission suivante doit être déléguée à une fonction annexe] ;
6. Soutenant l'organisation logistique du volet stratégique [Dans le cadre d'une crise de haute intensité, cette mission doit être déléguée à une fonction annexe].

Compétences requises

- Capacités d'analyse ;
- Capacité de synthèse ;
- Bonne connaissance de l'entité (en particulier les métiers) ;
- Bonne connaissance des équipes de gestion de crise et de leur rôle ;
- Adaptabilité ;
- Capacités de pilotage de programmes ;
- Capacités de gestion humaine (ex : empathie, écoute) ;
- Compréhension des enjeux cyber (vernis).

< RÔLES ET FONCTIONS EN CRISE D'ORIGINE CYBER >

Fonction
Secrétariat / Management de l'information

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

Aider à formaliser les documents relatifs à la gestion de la crise en :

1. Prenant note des évènements et actions via un journal de bord ;
2. Rédigeant l'ensemble des documents de gestion de crise : points de situation, suivi des actions, relevés de décision [Dans le cadre d'une crise de haute intensité, cette mission doit être déléguée à une fonction annexe] ;
3. En assurant le partage de ces documents aux parties identifiées.

Compétences requises

- Capacités de synthèse ;
- Qualités rédactionnelles ;
- Adaptabilité;
- Organisation et structuration ;
- Connaissances du fonctionnement de l'outillage (modèles, logiciels).

Fonction
Représentation métiers (ex : activités critiques, RH, Juridique, COM)

Nature
Essentiel

Modalités d'armement
Ponctuel

Principales missions

Représenter les métiers de l'entité en :

1. Remontant des informations relatives à son secteur ; (situation, contexte)
2. Assurant un suivi des actions pour son secteur.

Compétences requises

- Bonne connaissance de l'entité et du métier ;
- Compétences de management transverse ;
- Capacités de synthèse ;
- Capacités de prise de recul sur une situation.

Si crise de forte intensité les fonctions ci-dessous peuvent être sollicitées :

Fonction
Coordination stratégique/opérative

Nature
Facultatif (savoir armer ce rôle si nécessaire)

Modalités d'armement
Permanent

Principales missions

Assurer un lien (Coordination entre les différentes cellules de crises, informations descendantes et montantes vers la direction de crise, notamment par le RSSI ou un coordinateur désigné).

Compétences requises

- Capacités de synthèse ;
- Bonne connaissance de l'entité ;
- Compréhension des enjeux de crise cyber (vernis)

Fonction
Anticipation

Nature
Facultatif (avoir armer ce rôle si nécessaire)

Modalités d'armement
Ponctuel

Principales missions

Identifier des scénarios de dégradation ou d'amélioration d'une situation pour orienter la conduite de crise .

Compétences requises

- Capacités d'analyse ;
- Capacités de synthèse ;
- Bonne connaissance de l'entité (en particulier des métiers) ;
- Capacités de prise de recul sur la situation globale ;
- Compréhension des enjeux de crise cyber (vernis) ;
- Compréhension des enjeux de socio-économiques et géopolitiques.

Fonction
Support logistique

Nature
Facultatif

Modalités d'armement
Ponctuel

Principales missions

Soutenir l'organisation logistique du volet stratégique.

Compétences requises

- Bonne connaissance de l'entité (en particulier des processus organisationnels)

< RÔLES ET FONCTIONS EN CRISE D'ORIGINE CYBER >

Les fonctions détaillées ci-après (liste non exhaustive, en fonction des besoins de l'organisation) viennent appuyer la mise en place d'une stratégie de gestion de crise par leurs compétences métiers. Elles peuvent être organisées en cellules annexes.

Dans le cas où ces compétences ne seraient pas suffisantes (tant de manière quantitative que qualitative), il est possible de faire appel à une expertise externe (voir ci-dessus pour les bonnes pratiques associées).

Fonction
Communication

Principales missions

Formaliser et piloter la stratégie de communication de crise (interne, média, partenaires, autorités, actionnaires, représentants du personnel, ...).

Compétences requises

- Capacités de synthèse ;
- Bonne connaissance de l'entité ;
- Connaissance des enjeux de la communication de crise ;
- Maîtrise des outils de communication ;
- Compréhension des enjeux de crise cyber (vernis).

Fonction
Juridique

Principales missions

1. Eclairer la prise de décision au travers des aspects juridiques ;
2. Appuyer ou mener des actions sur le volet juridique de la crise.

Compétences requises

- Connaissance des enjeux juridiques (en particulier les volets "protection des données" et "contractualisation").

Fonction
Ressources humaines

Principales missions

1. Eclairer la prise de décision au travers des aspects RH ;
2. Appuyer ou mener des actions sur le volet RH de la crise.

Compétences requises

- Connaissance des enjeux RH lié au cadre de crise.

Fonction
Finances

Principales missions

1. Eclairer la prise de décision au travers des aspects financiers ;
2. Appuyer ou mener des actions sur le volet financier de la crise.

Compétences requises

- Connaissance du volet financier de l'entité (règles, enjeux).

< RÔLES ET FONCTIONS EN CRISE D'ORIGINE CYBER >

VOLET OPERATIONNEL CYBER

Les fonctions détaillées ci-après composent le volet opérationnel cyber : elles assurent le pilotage et le déploiement des actions d'investigation, de remédiation et de reconstruction/durcissement.

Dans certaines organisations, il est possible que le volet organisationnel soit séparé en deux parties : une partie cyber (dirigée par la fonction SSI) s'occupant de l'investigation et du durcissement alors qu'une partie SI (dirigée par la fonction DSI) s'occupe du maintien des activités informatiques et de la reconstruction.
Leur organisation se fait en miroir du volet stratégique et en fonction des besoins opérationnels.

Fonction
Pilote de crise opérationnelle

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

Conduire la cellule cyber en :

1. Mobilisant et coordonnant les entités cyber et informatique ;
2. Assurant le fonctionnement optimal du volet opérationnel (est notamment garant de ces règles de fonctionnement) ;
3. Proposant et assurant le suivi d'un plan d'action cyber;
4. Remontant des informations vers la cellule décisionnelle pour orienter la prise de décision
5. Appliquant les décisions prises par la cellule décisionnelle.

Compétences requises

- Bonne connaissance de l'entité (en particulier les métiers) ;
- Compétences de management transverse ;
- Capacités de prise de décision et leadership ;
- Capacités de prise de recul sur une situation ;
- Bonne connaissance des équipes de gestion de crise et de leur rôle ;
- Capacités de gestion humaine (ex : empathie, écoute) ;
- Maitrise des sujets cyber ;
- Pédagogie et capacités de vulgarisation de sujets techniques.

Fonction
Appui à la conduite

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

Soutenir le pilotage de la cellule et appuyer la direction de crise en :

1. Définissant le "rythme de bataille" de la cellule (horaires des points de situation, objectifs) ;
2. Assurant le suivi des actions ;
3. Assurant l'organisation des points de situation ;
4. Validant la cohérence et l'exhaustivité des informations remontées ;
5. Organisant la logistique du volet opérationnel cyber [Dans le cadre d'une crise de haute intensité, cette mission doit être déléguée à une fonction annexe].

Compétences requises

- Capacités d'analyse ;
- Capacité de synthèse ;
- Bonne connaissance de l'entité (en particulier les métiers) ;
- Bonne connaissance des équipes de gestion de crise et de leur rôle ;
- Adaptabilité ;
- Capacités de pilotage de programmes ;
- Capacités de gestion humaine (ex : empathie, écoute) ;
- Maitrise des sujets cyber.

< RÔLES ET FONCTIONS EN CRISE D'ORIGINE CYBER >

Fonction
Secrétariat / management de l'information

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

Aider à formaliser les documents relatifs à la gestion de la crise en :

1. Prenant note des évènements et actions via un journal de bord ;
2. Rédigeant l'ensemble des documents de gestion de crise : points de situation, suivi des actions, relevés de décision [Dans le cadre d'une crise de haute intensité, cette mission doit être déléguée à une fonction annexe] ;
3. En assurant le partage de ces documents aux parties identifiées.

Compétences requises

- Capacités de synthèse ;
- Qualités rédactionnelles ;
- Adaptabilité ;
- Organisation et structuration ;
- Connaissances du fonctionnement de l'outillage (modèles, logiciels) ;
- Maitrise des sujets cyber.

Fonction
Anticipation

Nature
Facultatif

Modalités d'armement
Ponctuel

Principales missions

Comprendre le chemin d'attaque pour identifier des scénarios d'évolution (chemin, MOA) et adapter la stratégie cyber.

Compétences requises

- Capacités d'analyse ;
- Capacités de synthèse ;
- Bonne connaissance de l'entité (en particulier des métiers) ;
- Capacités de prise de recul sur la situation globale ;
- Maitrise des sujets cyber (en particulier les aspects de CTI) ;
- Compréhension des enjeux de socio-économiques et géopolitiques.

Fonction
Représentation des métiers IT (Production, Support, Développement, Réseau….

Nature
Facultatif

Modalités d'armement
Ponctuel[1]

Principales missions

Représenter les activités SSI en crise en :

1. Remontant des informations relatives à son activité (situation contexte) ;
2. Assurant un suivi des actions pour son activité ;
3. Proposant des actions et arbitrages au reste de la cellule.

Compétences requises

- Bonne connaissance de l'entité et du cyber ;
- Capacité à redescendre l'information ;
- Capacités de synthèse ;
- Capacités de prise de recul sur une situation.

Fonction
Support logistique

Nature
Facultatif

Modalités d'armement
Ponctuel

Principales missions

1. Soutenir l'organisation logistique du volet stratégique ;
2. Coordonner l'accueil des prestataires extérieurs [Le cas échéant].

Compétences requises

- Bonne connaissance de l'entité (en particulier des processus organisationnels).

[1] Selon la taille de l'organisation et de son équipe SSI.

< RÔLES ET FONCTIONS EN CRISE D'ORIGINE CYBER >

Les fonctions détaillées ci-après viennent appuyer la mise en place des actions cyber par leurs compétences métiers. Elles peuvent être regroupées au sein de cellules annexes.
Dans le cas où ces compétences ne seraient pas suffisantes (tant de manière quantitative que qualitative), il est possible de faire appel à une expertise externe (voir ci-dessus pour les bonnes pratiques associées).

Par ailleurs, il est également possible de contractualiser avec une équipe CERT, un prestataire de réponse à incident ou une entité experte sur des sujets connexes (investigation, sauvegarde, reconstruction, etc.).

Fonction
Direction des systèmes d'information

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

La fonction DSI peut parfois être plutôt présente dans une cellule DSI/IT.
En cas de participation dans la cellule cyber, elle va :

1. Accepter les indisponibilités et les effets sur la continuité[2] ;
2. Contribuer à la création d'une stratégie de remédiation et de reconstruction ;

Compétences requises

- Capacité de prise de recul ;
- Excellente compréhension des enjeux cyber ;

Fonction
Equipes investigation CSIRT

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

En fonction des expertises présentes au sein de l'entité :

1. Informer de l'évolution et du traitement de la menace ;
2. S'assurer de la collecte et de la constitution des éléments de preuves légales ;
3. Coordonner les activités de détection, d'investigation ;
4. Propose une stratégie de détection vis-à-vis de la menace.

Compétences requises

- Expertise technique ;
- Connaissance des enjeux légaux notamment sur la collection de preuve.

Fonction
Equipe remédiation

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

1. Identifie les actions de remédiation ;
2. Propose une stratégie de remédiation à la cellule opérationnelle ;
3. Conduit les activités de remédiation une fois validées, en conjonction avec les équipes IT concernés.

Compétences requises

- Expertise technique ;
- Capacité de pédagogie avec les équipes IT.

Fonction
Equipe remédiation

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

1. Identifie les actions de remédiation ;
2. Propose une stratégie de remédiation à la cellule opérationnelle ;
3. Conduit les activités de remédiation une fois validées, en conjonction avec les équipes IT concernés.

Compétences requises

- Expertise technique ;
- Capacité de pédagogie avec les équipes IT.

[2] Ce point doit impérativement être défini dans le mandat de la cellule. Il n'est pas obligatoire et la décision de coupure peut être prise par une cellule stratégique uniquement pour évaluer au préalable l'impact métier.

Fonction
Equipe reconstruction

Nature
Essentiel

Modalités d'armement
Permanent

Principales missions

1. Identifie les actions de remédiation ;
2. Propose une stratégie de remédiation à la cellule opérationnelle ;
3. Conduit les activités de remédiation une fois validées, en conjonction avec les équipes IT concernés.

Compétences requises

- Expertise technique ;
- Pédagogie et capacités de vulgarisation.

Fonction
Equipes CTI

Nature
Facultatif

Modalités d'armement
Permanent

Principales missions

1. Etudie les éléments de contexte obtenus par rapport aux investigations ;
2. Identifie l'acteur de la menace et ses TTPs[3] potentielles utilisée ;
3. Informe les équipes anticipation, investigation et remédiation pour qu'ils puissent adapter leur stratégie.

Compétences requises

- Expertise technique ;
- Pédagogie et capacités de vulgarisation.

Fonction
Sensibilisation

Nature
Facultatif

Modalités d'armement
Ponctuel

Principales missions

1. Travailler à la construction de communication vers les utilisateurs pour assurer la prise en compte des mesures cyber

Compétences requises

- Pédagogie et capacités de vulgarisation ;
- Capacités rédactionnelles

Fonction
Protection des données cyber

Nature
Essentiel

Modalités d'armement
Ponctuel

Principales missions

1. Assure que les problématiques réglementaires lsont prises en compte (notamment liées à la protection des Données personnelles) ;
2. Prépare les notifications aux autorités de protection des données compétentes.

Compétences requises

- Connaissances juridiques ;
- Capacité de communication avec les autorités ;
- Capacités rédactionnelles.

Fonction
Conformité / Politique SSI

Nature
Essentiel

Modalités d'armement
Ponctuel

Principales missions

1. Identifie les procédures et politiques pouvant supporter la résolution de la crise ;
2. Prépare les notifications aux autorités / régulateurs compétents.

Compétences requises

- Capacité d'organisation / de suivi de programme ;
- Capacités rédactionnelles.

[3] Tactiques, Techniques, Procédures

ANNEXE

Cette annexe propose une trame de fiche-rôle à adapter par les organisations. Elle doit permettre de détailler les grandes missions d'une fonction donnée, par phases de la crise.

Pour faciliter et opérationnaliser la prise en main de cette fiche par toute personne devant armer la fonction mentionnée, il est important qu'elle comporte des consignes brèves et claires. Elle peut par ailleurs être associée à des documents annexes (schémas, modèles, etc.).

FICHE RÔLE

Fonction Nom de la fonction	**Principales missions** [Détailler le rôle de la fonction dans le dispositif] **PHASE 1 activation du dispositif** [Préciser les principales actions à mener dans le cadre de cette phase] [Préciser les outils et documents associés] **Phase 2 : conduite de crise** [Préciser les principales actions à mener dans le cadre de cette phase] [Préciser les outils et documents associés] **Phase 3 : désactivation du dispositif** [Préciser les principales actions à mener dans le cadre de cette phase] [Préciser les outils et documents associés]

Annexes (propositions)

Liste des outils et documents de référence du dispositif (dont mode d'emploi ou modèle de templates)
Schéma organisationnel du dispositif (dont flux d'information, principaux interlocuteurs)
Liste des compétences requises pour armer la fonction

Contributeurs : Banque de France, Bouygues Telecom, Enedis, Inquest Risk, LFDJ, Ministère de l'intérieur, PWC, Seekure

< Studio des Communs >

CAMPUS
CYBER

POUR EN SAVOIR PLUS : WIKI.CAMPUSCYBER.FR
ADRESSE MAIL DE CONTACT : COMMUNAUTES@CAMPUSCYBER.FR / 5 - 7 RUE BELLINI 92800, PUTEAUX