RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

EXERCICE DE CRISE CYBER JOP 2024

Support de présentation des enjeux, objectifs et méthodologie de gestion de crise cyber

SOMMAIRE

1. QU'EST-CE QU'UN EXERCICE DE CRISE ?

QUELQUES DEFINITIONS

La crise

Une crise : La crise est une déstructuration rapide de tous les repères, une dérégulation des mécanismes et des réactions habituelles. C'est une dynamique qui s'autoalimente par un effet boule de neige provoquant une incapacité grandissante à maîtriser l'incertitude. *(IHEMI).*

Une crise cyber : Une **crise « d'origine cyber »** se définit par la **déstabilisation immédiate** et majeure du **fonctionnement courant** d'une **organisation** […] en raison d'une ou de pl**usieurs actions malveillantes** sur ses **services** et ses **outils numériques** […]. C'est donc un évènement à fort impact, qui ne saurait être traité par les processus habituels et dans le cadre du fonctionnement normal de l'organisation. Par convention, on parlera par la suite de **« crise cyber ».** *(ANSSI, 2021).*

QUELQUES DEFINITIONS

La gestion de crise

Une cellule de crise : La cellule de crise est une équipe spécialisée chargée de gérer les situations délicates ou critiques auxquelles une organisation peut être confrontée. Ses membres ont pour responsabilité de prendre des décisions en réponse à une crise qui peut mettre en péril l'activité de l'organisation et de mettre en œuvre des mesures visant à prévenir une crise imminente ou à atténuer les conséquences d'une crise en cours.

Un exercice de crise : Un exercice de gestion de crise consiste à simuler un scénario, c'est-à-dire un enchaînement d'événements fictifs proposant une mise en situation de crise réaliste mais non réelle. Il se déroule sur une durée limitée, dans un contexte imaginé pour l'occasion et repose sur l'organisation de gestion d'une crise en place au moment où il est joué. Pour favoriser l'adhésion et l'implication des joueurs, les événements fictifs simulés doivent s'inspirer d'événements plausibles. *(ANSSI, 2020)*.

QUELLES SONT LES SUBTILITÉS D'UN EXERCICE DE CRISE SUR TABLE (COMPLEXITE 1) ?

Un exercice de réflexion

Durée d'environ 2h

Equipe opérationnelle

Déroulement : Discussions successives d'une dizaine de minutes sur une situation présentée sur une diapositive. Les participants doivent échanger pour mettre en avant les actions à mener et les acteurs à informer.

QUELLES SONT LES SUBTILITÉS D'UN EXERCICE DE CRISE DE SIMULATION (COMPLEXITE 2&3) ?

Un exercice de simulation le plus réaliste possible

Durée entre une demi-journée et une journée

Equipe étendue (acteurs opérationnels, stratégiques, partenaires, etc.)

Déroulement : Mise en place d'une situation de crise réaliste. Les participants doivent prendre en compte l'ensemble des stimuli qui leur sont transmis, prioriser leurs actions, adopter une méthodologie de prise de décision, gérer leur communication ou encore réfléchir à l'après-crise tout en agissant dans leur périmètre de responsabilité assigné.

2. POURQUOI RÉALISER UN EXERCICE DE CRISE ?

POURQUOI RÉALISER UN EXERCICE DE CRISE ?

POURQUOI RÉALISER UN EXERCICE DE CRISE ?

L'exercice de crise a pour **multiples objectifs** de vous :

1. Exercer à la **méthodologie de gestion de crise**,
2. Préparer aux **impacts spécifiques d'une crise d'origine cyber**,
3. Tester et exercer votre **réaction collective** face à un défi majeur,
4. Questionner sur les dispositifs de **continuité d'activité** disponibles pendant la durée des jeux,
5. Identifier vos principales **ressources de résolution face à une crise** de cybersécurité,
6. Préparer aux enjeux de la **communication de crise** et les procédures de **notification d'incident**,
7. Exercer à répondre aux **exigences légales et réglementaires**,
8. Identifier les principales **failles de votre dispositif de sécurité** des SI.

3. PRÉPARATION DE L'EXERCICE

PRÉPARER VOTRE EXERCICE : MÉTHODOLOGIE

01

Définir l'enjeu et les objectifs

- **Identifier** des faiblesses dans votre dispositif de crise
- **Améliorer** votre capacité de réponse à incident et de gestion de crise
- **Construire** des réflexes communs

02

Définir le type d'exercice

Les opérateurs les moins matures réaliseront un exercice sur table et les plus matures une simulation. Critère défini par l'ANSSI suite aux retours des **questionnaires de maturité**.

03

Dresser la liste des parties prenantes

En fonction du niveau de maturité de l'opérateur, plus ou moins d'acteurs seront présents ou représentés parmi les joueurs, observateurs et animateurs. **Cf Organisation de l'exercice**

04

Rassembler les documents supports

S'assurer de disposer de tous les documents nécessaires afin d'assurer une bonne gestion de la crise tant en documents purement opérationnels (fiches réflexes, PCA etc.) qu'en documents proprement axés crise (main courante, annuaire, questionnaire de RETEX à froid, grille d'observation, supports de briefing et debriefing, etc.)

05

Adapter le scénario fourni

Identifier les spécificités du SI de l'opérateur concerné pour adapter le scénario de l'exercice ainsi que le chronogramme fourni par l'ANSSI. Modifier celui-ci afin de faire apparaitre les actifs critiques propres à l'opérateur concerné.

06

Préparer l'organisation pratique

Définir la date et les horaires de l'exercice et en informer l'ensemble des parties prenantes suffisamment en amont. S'assurer d'avoir la logistique nécessaire au niveau d'une salle de crise pour pouvoir tenir l'exercice dans de bonnes conditions.

1. DÉFINIR LES ENJEUX ET LES OBJECTIFS DE VOTRE EXERCICE

OBJECTIF

Être préparé à gérer une crise cyber dans le cadre des JOP 2024

ENJEUX

- **Identifier** des faiblesses dans le dispositif de crise
- **Améliorer** la capacité de réponse à incident et de gestion de crise
- **Construire** des réflexes communs aux équipes

THEME

Nous sommes le **jour** d'un **grand évènement sportif** dans le cadre des **JOP2024**.
Votre organisation **accueille** et participe à cet **évènement** de **grande ampleur**
et se retrouve sous le feu des projecteurs : la compétition
est retransmise en direct à la télévision.

2. DÉFINIR LE TYPE D'EXERCICE

EXERCICE SUR TABLE

Opérateur jouant un exercice de complexité C1

- Favoriser une discussion autour des principes et bonnes pratiques de gestion de crise cyber
- Identifier des processus à mettre en œuvre sur divers enjeux
- Identifier les écosystèmes associés

EXERCICE DE SIMULATION

Opérateur assez mature sur les sujets cyber et gestion de crise disposant de procédures et d'une organisation de crise existante

- Eprouver la mise en place d'une organisation de gestion de crise
- Tester la mise en œuvre de mesures stratégiques
- Eprouver la gestion du stress

3. PARTIES PRENANTES (NIVEAU 1)

Joueurs

Participer à l'exercice en conditions réelles dans la cellule

- DSI
- RSSI
- RPCA [si la fonction est incarnée dans votre organisation]
- Directeur communication *[si la fonction est incarnée dans votre organisation]*

Animateurs

Participer à l'exercice en envoyant les stimuli à la cellule ou en jouant un rôle

- DIRANIM

Exemples :

- ANSSI
- COJO (Paris 2024)
- Autorités (préfecture, ministère, etc.)
- Collaborateurs
- Directions métier

Observateurs

Analyser la réaction des participants et le déroulement de la gestion de crise

- Observateur de la cellule principale
- Observateur de la cellule d'animation

3. PARTIES PRENANTES (NIVEAU 2)

Joueurs

Participer à l'exercice en conditions réelles dans la cellule

- Direction Générale
- DSI
- RSSI
- DRH
- Direction Juridique
- Direction Communication
- Responsables métier

Animateurs

Participer à l'exercice en envoyant les stimuli à la cellule ou en jouant un rôle

- DIRANIM

Exemples :

- ANSSI
- Experts PRIS
- Autorités (préfecture, ministère, etc.)
- Clients
- Média et Journalistes
- COJO (Paris 2024)
- Collaborateurs

Observateurs

Analyser la réaction des participants et le déroulement de la gestion de crise

- Observateur de la cellule stratégique
- Observateur de la cellule opérationnelle
- Observateur de la cellule animation

3. PARTIES PRENANTES (NIVEAU 3)

Joueurs

Participer à l'exercice en conditions réelles dans la cellule

- Direction Générale
- DSI
- RSSI
- DRH
- Direction Juridique
- Direction Financière
- Direction Communication
- Responsables métier

Animateurs

Participer à l'exercice en envoyant les stimuli à la cellule ou en jouant un rôle

- DIRANIM

Exemples :

- CNIL
- ANSSI
- Experts PRIS
- Autorités (préfecture, ministère, etc.)
- Clients
- Média et Journalistes
- COJO (Paris 2024)
- Responsable sureté
- Fournisseurs de service
- Collaborateurs

Observateurs

Analyser la réaction des participants et le déroulement de la gestion de crise

- Observateur de la cellule stratégique
- Observateur de la cellule opérationnelle
- Observateur de la cellule animation

4. DOCUMENTS SUPPORTS

Documents « métier »

A produire par l'opérateur

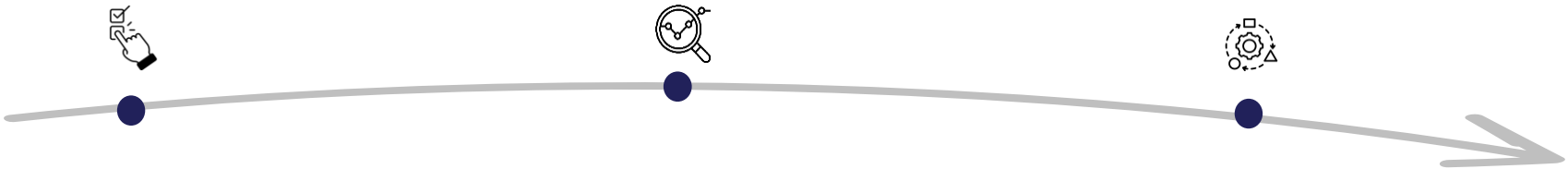
- **PCA :** Document définissant les principes stratégiques de continuité d'activité au regard des différentes catégories de risques
- **PRA :** Document présentant les méthodes et stratégies de reprises d'activité en cas de crise
- **Fiches réflexes :** Fiches présentant les procédures à respecter en cas de survenue d'incident

Documents « crise »

Fournis par l'ANSSI dans le cadre de l'exercice

- **Annuaire :** Document listant les coordonnées des différents acteurs susceptibles d'être contacté en cas de crise
- **Main courante :** Document permettant de dresser une liste détaillée des actions menées et des informations remontées en cas de crise
- **Grille d'observation :** Document à l'intention des observateurs permettant de réaliser l'évaluation de l'exercice
- **Questionnaire RETEX à froid :** Questionnaire à faire remplir par les parties prenantes dans le mois suivant l'exercice en vue de la réalisation d'un RETEX à froid

5. ADAPTER LE SCENARIO FOURNI



Dans le chronogramme, sélectionner le bon niveau de complexité ainsi que la bonne catégorie d'opérateur afin d'afficher les stimuli pertinents dans le contexte de l'opérateur.

Cartographier les impacts potentiels d'une crise cyber ainsi que les actifs critiques de l'opérateur dans le cadre des JOP 2024.

Compléter le chronogramme avec les éléments identifiés à l'étape précédente afin d'obtenir un scénario le plus réaliste possible au regard des spécificités de l'opérateur.

6. PREPARER LA LOGISTIQUE

Bloquer la date et l'heure le plus en amont possible

Réserver les salles nécessaires et s'assurer qu'elles disposent du matériel nécessaire

Communiquer aux parties prenantes la date et l'heure de l'exercice

S'assurer d'être prêt pour le Jour J (documents, matériel, briefings, débriefings etc.)

4. DÉROULEMENT DE LA JOURNEE D'EXERCICE

DÉROULEMENT DE LA JOURNEE D'EXERCICE

- Accueil des participants (15')
- Briefing des participants (30')
- Déroulement de l'exercice (C1 : 2h, C2 : 3h, C3 : 2x3h)
- Réalisation du RETEX à chaud (1h')
- Mot de la fin et remerciements des participants (5')

Ne pas oublier de planifier le RETEX à froid dans le mois suivant l'exercice

5. MODALITES PRATIQUES

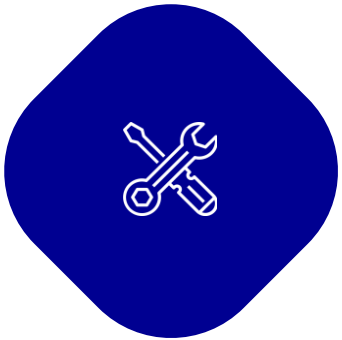
OUTILS A DISPOSITION DES JOUEURS

→ **Salle de crise**

- Salle de réunion
- Matériel de projection
- Tableaux blancs
- …

→ **Documents de crise**

- Main courante
- Annuaire de crise
- Grille d'observation
- PCA/PRA
- Fiches réflexes
- …



→ **Outils usuels**

- Téléphones professionnels
- Ordinateurs professionnels
- Outils habituels de l'opérateur

→ **Moyens de communication**

- Annuaire avec des numéros dédiés
- Outils de communication internes
- Boite mail de l'exercice

CONSIGNES DE COMMUNICATION (NIVEAU 1)

Exercice sous forme de discussion entre les parties prenantes : l'animateur diffuse une diapositive présentant une situation et les joueurs doivent échanger entre eux pour trouver la marche à suivre, les actions à mener ainsi que la stratégie à adopter.

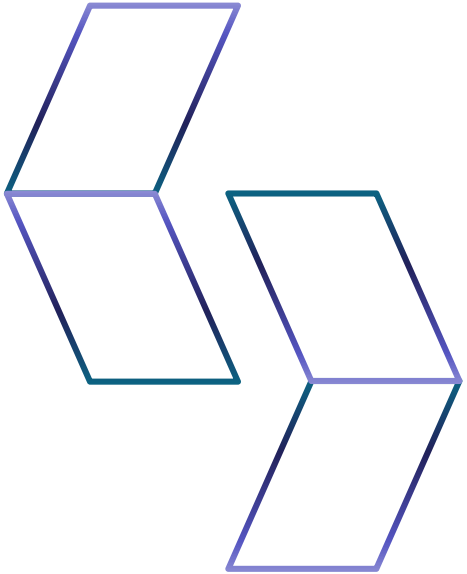
Il n'y a pas de moyens de communication spécifiques mis en place car les échanges entre l'animation et les joueurs se font directement dans la cellule de crise.

CONSIGNES DE COMMUNICATION (NIVEAUX 2 & 3)

Par convention, la messagerie et les réseaux de télécommunication **ne sont pas impactés par le scénario.**

Pour contacter par téléphone ou mail une entité/acteur, il convient d'utiliser les contacts présents dans **l'annuaire d'exercice.**

Si un joueur souhaite contacter un acteur/entité non référencé dans l'annuaire, contacter la cellule d'animation.



Par téléphone (appel entrant ou sortant) :

- Dites **« EXERCICE EXERCICE EXERCICE »** avant votre message. Puis présentez-vous et dites à qui vous souhaitez parler.

Par mail :

- Formaliser l'objet avec les informations suivantes **« [EXERCICE] Ecrire l'objet du mail »**
- Répondre directement sur le stimuli mail qui vous a été envoyé
- Formaliser le corps du mail: écrivez **EXERCICE – EXERCICE – EXERCICE** en début et fin de mail

RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité