Exercice de gestion de crise cyber : Les règles du jeu

Règles du jeu

Ce kit dédié aux participants a pour objectif de vous guider et de vous préparer au mieux à l'exercice de crise organisé prochainement dans votre structure. Il contient les règles et bonnes pratiques de gestion de crise qui vous permettront d'être prêt le jour J.

1 Contexte et enjeux de l'exercice de crise cybersécurité

Contexte

L'exercice réalisé aujourd'hui s'inscrit dans la démarche globale de renforcement de la résilience face aux cyberattaques qui ciblent de plus en plus les entreprises. Il vise à permettre aux participants de s'approprier des automatismes de gestion de crise en cybersécurité, adaptés aux enjeux et spécificités de leur organisation. Cet exercice offre l'opportunité de tester les processus existants, d'identifier des axes d'amélioration et de renforcer la coordination des acteurs impliqués dans la réponse à une crise cyber.

OBJECTIFS GENERAUX DE L'EXERCICE

/ Comprendre les spécificités de la crise cybersécurité

- L'attaque cybersécurité peut être latente et silencieuse et ce, jusqu'au début de la crise. Elle s'adapte très souvent aux réactions des équipes internes pour contenir l'attaque et sa gestion nécessite une coordination importante entre les parties prenantes.

/ S'inscrire dans l'actualité cybersécurité

- Les cyberattaques se multiplient et touchent de plus en plus les entreprises, tous secteurs confondus, comme en témoignent les incidents récents affectant de grandes entreprises, des PME et des collectivités. Ces attaques peuvent avoir des conséquences majeures, allant de l'interruption des activités à la fuite de données sensibles, soulignant ainsi l'importance d'une préparation efficace face à ces menaces.

OBJECTIFS PEDAGOGIQUES DE L'EXERCICE

- **Découvrir la gestion de crise cyber en condition réelle**
- **Comprendre l'écosystème cyber de la structure : CERT, référents SSI, etc.**
- **Adopter les premiers bons réflexes : alerter, communiquer, élaborer un plan d'action**
- **Assurer au mieux la continuité des soins**

2 Déroulement et organisation de l'exercice

ETAPE 1
Simulation de l'exercice

1. Réception des stimuli par les joueurs

Les joueurs reçoivent des **stimuli** (via email ou simulation d'appel) à une **fréquence régulière** de la part de l'équipe d'animation. Ces stimuli informent de **l'évolution de la situation**.

Ces stimuli suivent un rythme volontairement accéléré. Une vraie crise se déroule sur plusieurs jours, voire plusieurs semaines.

2. Analyse et prise de décision au sein de la cellule

Les joueurs **analysent** ces stimuli, **réagissent** en conséquence et **prennent des mesures** pendant l'exercice. Les joueurs doivent **rester mobilisés pendant toute la durée de l'exercice.**

- Les actions demandées et décisions prises doivent être clairement actées par écrit dans la main courante /relevé d'action
- Certains stimuli sont envoyés à un joueur uniquement : cela ne signifie pas qu'ils ne concernent pas tous les joueurs

3. Communication au sein de la cellule

L'équipe d'animation constitue **votre seul et unique interlocuteur durant cet exercice**. Elle **incarne tous les acteurs internes et externes** qui vous fourniront les informations nécessaires et auprès desquels vous pouvez poser une question ou lancer une action.

ETAPE 2
Débriefing des joueurs et des animateurs / observateurs

A la fin de l'exercice, l'équipe d'animation reprend la main pour réaliser un débriefing à chaud général : les joueurs donnent leur ressenti par rapport à l'exercice et s'auto évaluent ; l'équipe d'animation partage également ses premiers éléments d'évaluation et axes d'amélioration.

Focus : Le principe de simulation pendant l'exercice

Les informations reçues via les stimuli sont toutes fausses car elles sont issues d'un scénario créé pour l'exercice. Afin de résoudre l'exercice**, il n'est en aucun cas nécessaire :**

- **De contacter une personne en dehors des participants à l'exercice**. L'équipe d'animation jouera tous les rôles et interlocuteurs nécessaires.
- **D'envoyer ou de transférer les informations reçues hors des canaux de communication prévus**
- **D'effectuer une action technique -** Indiquer par mail que vous souhaitez exécuter une action suffit.

Le scénario reflète au mieux la réalité des cybermenaces actuelles adaptée au contexte des entreprises. Cependant, **le déroulé de certains éléments diffère** : le temps de réponse des interlocuteurs, le nom de certains services, etc.
Veillez à ne pas tenir compte de ces décalages et à prendre en considération uniquement l'information reçue.

Focus : Les moyens de communication pendant l'exercice

Les joueurs auront leur **PC à disposition avec un accès à internet** d'où ils pourront lire leurs **emails** et/ou des **ressources spécifiques** (fiches mémo, espace de partage, etc.)

- Chaque e-mail envoyé / reçu devra comporter en objet **[Exercice, Exercice, Exercice] Objet du mail**
- La cellule d'animation sera mise **en copie** de tout échange de mail

Les appels téléphoniques seront simulés par la cellule de crise / les animateurs à l'oral

- Chaque appel simulé devra commencer par **"Exercice, Exercice, Exercice - je suis…., du site de …., du service de… et je souhaite m'adresser à …. du site… du service …"**

Vous utiliserez le DCR, l'outil de gestion de crise du GHT, qui vous accompagnera tout au long de l'exercice.
IMPORTANT : Les outils de communication habituels ne pourront pas être utilisés pendant l'exercice.

A retenir : toute communication à des personnes extérieures à l'exercice n'est pas nécessaire.

Tilwit

3 Bonnes pratiques pour réussir sa gestion de crise

Fonctionnement de la cellule

- ✓ Veiller au bon fonctionnement de la cellule et au bien-être de chacun des membres : **écoute, concentration, repos, solidarité**
- ✓ Savoir **dépasser le cadre habituel** (exemple : soulager un membre de la cellule débordé, passer outre certains process)
- ✓ Connaître et respecter son **rôle** et ses **responsabilités** au sein de la cellule
- ✓ S'assurer de **ne pas gêner le travail des autres membres** de la cellule de crise : respecter l'espace de chacun, limiter le bruit
- ✓ Organiser des **points de suivi réguliers** pour proposer les arbitrages et définir le plan d'action

Partage d'information

- ✓ Favoriser le **partage d'informations** et toujours vérifier la **fiabilité** des informations reçues
- ✓ **Remonter les informations** et les alertes aux personnes concernées et au PMO/Coordinateur
- ✓ Respecter la **confidentialité** des informations, des actions et décisions prises
- ✓ Veiller à ce que les **prises de paroles soient courtes et efficaces**
- ✓ **Respecter le temps de parole** de chacun

Prise de décision

- ✓ Garder une **posture objective**
- ✓ Se concentrer sur les points essentiels, les incertitudes à clarifier, les évolutions en cours pour **faire évoluer la stratégie de réponse sur son périmètre**
- ✓ Pendant les points de situation, se limiter à **la prise de décision** et ne pas démarrer de nouvelles actions (penser à garder une synthèse des points de situation)
- ✓ **Prendre des décisions** sur la base du niveau « nécessaire » d'information à disposition sans chercher à maitriser l'ensemble des tenants et aboutissants
- ✓ Identifier et **prioriser les actions urgentes**, piloter la réponse à la crise sur son périmètre (penser à rédiger un plan d'action ainsi qu'un plan de retour à la normale)
- ✓ Mettre en place des **mesures préventives** après analyse de la situation et des évolutions possibles
- ✓ Identifier et mobiliser les **experts** pertinents sur son périmètre
- ✓ Evaluer les **impacts directs et indirects** des décisions

Retrouvez l'essentiel de ces bonnes pratiques sur la fiche mémo « 10 bonnes pratiques de gestion de crise »

Bonnes pratiques de communication en situation de crise cybersécurité

TOUS LES PARTICIPANTS

Les conséquences d'une crise cybersécurité sont souvent visibles immédiatement : en interne, elle empêche le fonctionnement habituel des activités de la structure et en externe, elle peut devenir rapidement médiatisée et entrainer la réaction de partenaires, autorités, clients, et/ou usagers, etc. Une bonne gestion de crise intègre, au cœur du dispositif, l'action de communicants en interne et en externe.

LE PARTAGE D'INFORMATION AU SEIN DE LA CELLULE

1. **Assurer la maîtrise des échanges** (questions, débats, partage d'informations, alignement, prises de décision, reformulation, etc.) à la main d'un **coordinateur.**
2. **Assurer un partage de l'information clair, factuel et synthétique** permettant d'obtenir une vision globale des faits.
3. **Assurer la vérification, la synthétisation et le tri des informations entrantes et sortantes** pour préserver les décideurs.
4. **Assurer la traçabilité des informations** de manière synthétique (outillage via un journal de bord, une main courante, etc.).
5. **Assurer la synchronisation des informations** en les partageant aux bonnes personnes au bon moment.

LA COMMUNICATION INTERNE ET EXTERNE A LA STRUCTURE

Communiquer nécessite la mise en place d'une stratégie de communication orchestrée par l'équipe communicante et validée par la cellule de crise.

1. **Définir un message cohérent à décliner en fonction des parties prenantes**
2. **Contextualiser le(s) message(s) pour chaque partie prenante**
3. **Trouver le média le plus adapté pour partager le message aux parties prenantes**

LES ÉQUIPES DE COMMUNICATION

Partagent l'information :
Aux collaborateurs, partenaires, médias et presse, etc.

Par quels moyens ?
Porte-parole pour la presse, réseaux sociaux, email, communiqué de presse, etc.

LES ÉQUIPES TECHNIQUES

Partagent l'information :
Aux entités / autorités spécialisées (DPO, RSSI, CNIL, etc.)

Par quels moyens ?
Points de situation par mail, appel téléphonique, etc.

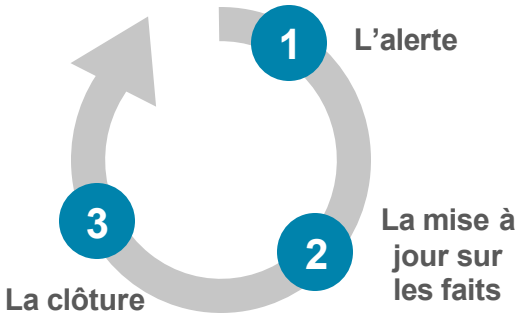
LA DIRECTION

Partagent l'information :
Aux collaborateurs, usagers, etc.

Par quels moyens ?
Email, communiqués de presse, appels téléphoniques, affichage sur site Intranet, etc.

La communication en temps de crise peut être scindée en **trois temps distincts** :

1. **L'alerte :** *communication d'urgence* - message d'attente factuel sur l'incident à communiquer rapidement, discours de responsabilité
2. **La mise à jour des faits :** *communication réfléchie et adaptée* - partage des faits et des impacts au fur et à mesure et uniquement les éléments structurants, réponse aux questions
3. **La clôture :** *communication à froid* – rétrospective sur les évènements et partage des mesures prises pendant et après la crise



A chacune des trois étapes, il convient de se poser la question de **la nécessité de communiquer**.

ANTICIPER SA COMMUNICATION DE CRISE

La communication de crise doit être **anticipée**. Ainsi, les réponses à apporter durant une crise cyber sur le volet communication doivent être préparées. Il faut donc consacrer en amont de la crise un temps de préparation pour **concevoir sa stratégie de communication** (scénarios, objectifs de communication, cibles, moyens, posture de communication, etc.).

EN RÉSUMÉ

Une des difficultés majeures en gestion de crise est de **conserver la capacité à bien communiquer**.

Cohérence des messages	**Maintien du lien entre les parties prenantes**	**Adaptation des messages**