FICHE PRATIQUE 6 :

RÉDIGER UN CHRONOGRAMME : MODE D'EMPLOI

EXEMPLE FIL ROUGE RANSOM20

La rédaction du chronogramme se base sur les interviews des experts, réalisée lors de la phase 1 de cette étape.

Ce tableau se remplit de la droite vers la gauche en commençant par la réaction attendue qui correspond à un ou plusieurs des objectifs visés. Puis il convient de choisir le(s) joueur(s) destinataire(s) de l'information. Vient ensuite l'émetteur, personne qui sera simulé par l'animateur pour transmettre l'information. C'est seulement ensuite qu'est rédigé l'événement qui va être transmis au joueur par l'animateur pour obtenir la réaction attendue. On s'intéressera enfin aux modalités de tranmission de l'information et à l'horaire auquel celle-ci sera transmise.

Les éléments techniques proposés dans le chronogramme ci-après sont à compléter en fonction de votre organisation interne.

Émetteur : il s'agit des profils simulés derrière lesquels se trouve la cellule d'animation qui enverra le message vers un ou plusieurs destinataire(s) (joueurs). L'équipe d'animation peut être amenée à simuler des personnes internes à l'organisation qui ne participent pas à l'exercice (ex : le manager d'un service) ou externes (ex : un journaliste). Il est possible d'ajouter une colonne immédiatement après « émetteur », nommée « joué par », afin de préciser quel animateur sera en charge de transmettre le stimulus.

Stimulus : il correspond à une information transmise à un ou plusieurs joueurs. Chaque ligne du chronogramme correspond à un stimulus. Il convient de rédiger le script de ceux-ci en amont du jour J. Ce sont les animateurs et les experts qui, en fonction de leur spécialité, écrivent les événements dans leur langage métier pour donner du réalisme à l'exercice.

Recommandation

Il est tout à fait normal lors de la rédaction du chronogramme de ne pas s'adresser à tous les joueurs car certaines interactions auront lieu naturellement entre eux. Par exemple, le directeur de la cellule de crise demandera à ses équipes de réaliser un point de situation à un horaire particulier ou encore le RSSI demandera à ses équipes techniques de réaliser des analyses. Il n'est donc pas nécessaire de simuler ces interactions. Par ailleurs, les joueurs solliciteront la cellule d'animation avec des demandes ou questions auxquelles il faudra répondre de la manière la plus réaliste possible, d'où l'importance d'avoir des experts des sujets abordés en cellule d'animation.

Destinataire : il s'agit du ou des joueurs qui recevront le message. Il faut être vigilant et ne pas envoyer tous les messages à la même personne. L'intérêt est notamment de voir si l'information circule bien au sein de la ou des cellule(s) de crise. Une même personne ne peut pas être à la fois émetteur et destinataire au cours d'un même exercice (les animateurs ne sont pas joueurs et inversement).

Réactions attendues : pour chaque ligne de chronogramme rédigée, il est nécessaire d'écrire la réaction attendue des joueurs qui doit correspondre aux objectifs décrits précédemment. Cela permet également d'aider l'équipe d'animation à anticiper l'adaptation du scénario le jour de l'exercice, si la réaction est trop différente de ce qui était prévu.

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
DMS	AAMMJJ **08:30**	**Dossier de mise en situation**	Envoi du dossier de mise en situation (DMS) en pièce jointe d'un mail à destination de l'ensemble des joueurs.	DIRANIM	Tous les joueurs	Mail	Prise de connaissance des informations. Aucune action particulière attendue.	Ce stimulus peut aussi être envoyé la veille pour constituer une première mise en ambiance avant le démarrage de l'exercice.

OPTION DE JEU SIMULANT L'ANSSI

OPTION DE JEU AVEC PLUSIEURS SITES TOUCHÉS ET PLUSIEURS CELLULES DE CRISE IMPLIQUÉES EN TANT QUE JOUEUR

OPTION DE JEU AVEC PLUSIEURS SITES TOUCHÉS ET UNE SEULE CELLULE DE CRISE IMPLIQUÉE EN TANT QUE JOUEUR

OPTION DE JEU PERMETTANT DE S'ENTRAÎNER SURLES PROBLÉMATIQUES D'EXFILTRATION DE DONNÉES

Modalité de transmission : c'est dans cette colonne que l'on décide par quel canal l'information va être diffusée vers le ou les joueur(s). Il s'agit généralement de mails ou d'appels téléphoniques ou d'outils tels qu'une plateforme simulant la pression médiatique. Il est important d'utiliser les moyens de communication que les joueurs seraient amenés à utiliser en crise réelle, tout en prenant en compte les conséquences de la cyberattaque (ex: messagerie internet indisponible).

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
1	AAMMJJ **09:30**	**Début de l'exercice**	« *Bonjour, l'exercice commence maintenant. N'hésitez pas à nous contacter pour toute question ou incompréhension.* »	DIRANIM	Tous les joueurs	Mail	Aucune action particulière attendue.	
2	AAMMJJ **09:32**	**Premiers messages sur l'incident**	« *Bonjour,* *Je vous appelle car les membres de mon équipe ne peuvent plus utiliser leur ordinateur. Tous affichent un même message demandant une rançon pour récupérer les données. On a un projet très important à rendre en fin de semaine, il faut absolument qu'on puisse travailler. Que devons-nous faire ? Par ailleurs, je crois que le problème s'étend au moins à tout notre étage…* »	Manager d'une équipe de l'organisation [service/département au choix]	Directeur de la ligne métier/activité concernée	Appel téléphonique	Signalement/échange avec le RSSI.	Stimulus à multiplier (par intervalles de 5 à 10 minutes) autant que jugé utile (en fonction du nombre d'activités concernées ou encore de la pression souhaitée sur les joueurs). L'objectif de ces stimuli est de montrer que tous les services de l'organisation sont progressivement touchés. Il est possible d'ajouter des conséquences métiers spécifiques à chaque service dans le script des appels téléphoniques et des mails.
3	AAMMJJ **09:35**	**Premiers messages sur l'incident**	« *Bonjour,* *Je vous appelle car nous avons reçu depuis ce matin plusieurs appels de salariés qui ne pouvaient plus utiliser leur ordinateur. D'après les photos reçues, les données seraient chiffrées et pourraient être récupérées en cas de paiement d'une rançon. Êtes-vous au courant de cette situation ? Nous commençons à être saturés par le volume des appels et n'avons aucune information à transmettre sur la situation…* »	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission de l'alerte et déclenchement de la cellule de crise.	Il peut être intéressant de jouer la mobilisation de la cellule de crise. Cette dernière peut être activée entre ce stimulus et le stimulus 12. Passé ce dernier, le cellule d'animation devra insister pour qu'une cellule de crise se réunisse le plus rapidement possible.
4	AAMMJJ **09:40**	**Premiers messages sur l'incident**	« *Bonjour,* *À la suite de notre échange téléphonique, vous trouverez ci-joint une photo de l'un des postes. N'hésitez pas à me transmettre toute consigne qui me permettra de répondre aux futurs appels des salariés. Je vous rappelle si d'autres services nous informent qu'ils sont touchés. Nous sommes vraiment saturés par le volume d'appels et n'avons aucune information sur la situation.* »	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Mail	Estimation des premiers impacts, lancement des investigations, préparation des premières mesures de gestion de l'incident et définition consignes à destination des employés. Eventuellement, prise de contact avec un prestataire ou avec l'ANSSI (simulés par la cellule d'animation).	En fonction du logiciel malveillant choisi lors de la conception du scénario, il est possible d'utiliser des captures d'écran de rançongiciel trouvées sur Internet. Pour obtenir plus d'informations sur les bonnes pratiques à mettre en place dans le cadre d'une attaque par rançongiciel, consulter le guide de l'ANSSI *Attaques par rançongiciels, tous concernés ?*
5	AAMMJJ **09:45**	**Premiers messages sur l'incident**	« *Bonjour,* *Je vous informe que les postes de travail de l'ensemble de mon équipe sont inutilisables et affichent tous le même message. Impossible de travailler. Est-ce qu'on a été piraté ? Avez-vous la possibilité de résoudre ça assez rapidement car nous devons rendre notre dossier en fin de semaine ? On a essayé de redémarrer sans succès les PC.* »	Manager d'une équipe de l'organisation [service/département au choix]	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Prise en compte de l'information et transmission des premières consignes si définies.	
6	AAMMJJ **09:50**	**Premiers messages sur l'incident**	« *Bonjour,* *À la suite de notre appel, je confirme que les postes de travail de l'ensemble de mon équipe sont inutilisables et affichent tous le même message. Je vous envoie par SMS une photo de l'un des postes. Que se passe-t-il ?* »	Manager d'une équipe de l'organisation [service/département au choix]	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Prise en compte de l'information et tranmission à la cellule de crise.	
7	AAMMJJ **09:55**	**Premiers messages sur l'incident**	« *Rebonjour,* *Au vu des appels reçus jusqu'ici, les services/départements X et Y sont touchés ainsi que l'équipe projet Z qui doit rendre ses conclusions en fin de semaine [indiquer une échéance critique]. Pouvez-vous me transmettre des consignes afin que mon équipe puisse répondre aux interrogations des utilisateurs ? Nous nous sommes saturés et plus rien ne semble fonctionner.* »	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission des premières consignes si définies, interrogations sur le périmètre de l'attaque et début des réflexions sur la continuité d'activité.	
8	AAMMJJ **10:00**	**Latéralisation du rançongiciel**	« *Bonjour,* *L'ensemble des équipes du service X n'a plus accès aux données de ses ordinateurs suite à l'affichage d'un message demandant une rançon. Nous étions en train de finaliser le projet Y que nous devions absolument rendre ce jour. Comment faire pour continuer à travailler ? Que se passe-t-il ? Je vous envoie par SMS une photo d'un écran d'un des ordinateurs inutilisables.* »	Manager d'une équipe de l'organisation [service/département au choix]	Directeur de la ligne métier/activité concernée	Appel téléphonique	Transmission des informations au RSSI et diffusion des consignes si définies.	
9	AAMMJJ **10:05**	**Latéralisation du rançongiciel**	« *Bonjour,* *L'ensemble des équipes du service X n'a plus accès aux données de ses ordinateurs suite à l'affichage d'un message demandant une rançon. Que se passe-t-il ? Quand pourrons-nous reprendre le travail ?*»	Manager d'une équipe de l'organisation [service/département au choix]	Directeur de la ligne métier/activité concernée	Appel téléphonique	Transmission des informations au RSSI et diffusion des consignes si définies.	

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
10	AAMMJJ **10:15**	**Latéralisation du rançongiciel**	*« Je reçois de plus en plus d'appels de multiples services de l'organisation m'annonçant ne plus pouvoir travailler à cause d'un message affiché sur leur écran et demandant une rançon. Notre service est désormais complètement saturé. Voici la liste des services m'ayant contacté :* *- service/département 1* *- service/département 2* *- … »*	Référent IT pertinent	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Prise en compte de l'information et poursuite des investigations. Si non réalisé précédemment et si jugé nécessaire, prise de contact avec un prestataire ou l'ANSSI (simulé par la cellule d'animation).	
11	AAMMJJ **10:45**	**Publication d'une photo d'un des postes sur les réseaux sociaux**	*« Bonjour,* *Je vous informe qu'une photo d'un des postes de travail de l'organisation semble avoir été postée sur les réseaux sociaux (soit il s'agit d'un de nos postes, soit d'une photo extrêmement similaire). L'organisation n'est pas citée mais si le lien est fait, nous ne devrions pas tarder à recevoir des appels de la presse. Je reviendrai vers vous pour vous informer des réactions observées sur les réseaux sociaux. »*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication + RSSI	Mail	Débuter la réflexion sur la stratégie de communication et la définition d'éléments de langage.	
12	AAMMJJ **11:00**	**Latéralisation du rançongiciel et début des investigations**	*« Bonjour,* *Nous vous confirmons que l'ensemble du parc informatique est impacté par l'incident en cours depuis ce matin. L'analyse des captures réseau effectuées confirme la latéralisation du code malveillant au sein du réseau interne, par un vecteur que nous sommes en train de chercher à identifier. Nous n'avons pas d'autre information et les investigations sont difficiles. »*	Équipe de réponse à incident/administrateur réseau	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Mise en œuvre de procédures dégradées, activation du PCA ou de toute mesure contribuant à la gestion de la crise. Vérification de l'application des bonnes pratiques en cas d'attaque par rançongiciel.	Les planificateurs de l'exercice devront décider en amont si l'organisation a toujours accès à sa messagerie. > Si oui, les échanges peuvent continuer comme précédemment. > Sinon, la cellule de crise devra mettre en place d'autres outils pour communiquer. Plus généralement, à partir de ce stimulus, il convient de matérialiser la perte d'accès au réseau : les ordinateurs, les outils de la cellule de crise, les annuaires, la messagerie etc. ne seront plus utilisables s'ils sont gérés sur le réseau. Les joueurs devront ainsi penser à des solutions de secours pour gérer la crise et maintenir certaines activités critiques. Jouer ces conséquences, pourtant vraisemblables, augmente toutefois le niveau de difficulté de l'exercice. Il est possible ici de multiplier les stimuli de ce type en provenance de différentes équipes techniques (administrateurs, équipes de sécurité, équipes réseaux, etc.) afin d'insister sur le fait que la situation est très grave et que l'organisation dispose de très peu d'information sur ce qu'il se passe. Passé ce stimulus, il convient de s'assurer que les joueurs ont activé leur cellule de crise pour permettre la bonne poursuite de l'exercice.
13	AAMMJJ **11:10**	**Sollicitations internautes réseaux sociaux**	*« Bonjour,* *Voici quelques exemples de sollicitations que l'on trouve sur les réseaux sociaux :* *@organisation vous confirmez avoir été attaqué ? #cyberthreat* *Il semblerait que @organisation se soit fait pwnd. Des infos ? #insecure »*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Prise en compte de l'information, préparation d'une stratégie de communication.	
14	AAMMJJ **11:15**	**Demande de visibilité des métiers**	*« Bonjour,* *Pourriez-vous nous faire parvenir les informations dont vous disposez sur l'incident en cours, notamment ce qui concerne sa nature et son ampleur afin de permettre à nos services de continuer malgré la situation, en mode dégradé si nécessaire. Par ailleurs, on nous dit que tout est sauvegardé, j'espère que c'est vraiment le cas car nous avons absolument besoin de nos dossiers ! »*	Différents chefs de service s'adressent à leur directeur pour savoir ce qu'ils vont dire à leurs équipes et s'ils doivent déclencher des procédures dégradées	Directeur de la ligne métier / activité concernée	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Préparer et transmettre des consignes adaptées à la situation.	Stimulus à décliner autant de fois que souhaité pour accentuer la pression sur les joueurs.
15	AAMMJJ **11:30**	**Pression médiatique**	*« Bonjour,* *Des informations circulant sur les réseaux sociaux semblent indiquer que votre organisation est la cible d'une attaque informatique. Pouvez-vous confirmer ? Dans quelle mesure votre organisation est-elle impactée ? Pouvez-vous continuer vos activités ? »*	Journaliste	Responsable communication	Appel téléphonique	Transmettre les éléments de langage préalablement définis (si ceux-ci ne sont pas prêts, proposer de rappeler plus tard le journaliste). Il est également possible de ne pas commenter et de publier plus tard un communiqué de presse.	

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
16	AAMMJJ **12:00**	**Revendication de l'attaque et menace de publication des données exfiltrées**	« *Bonjour,* *Vous trouverez ci-dessous une copie du message de revendication de l'attaque publié sur un forum Internet :* *« All of [organisation]'s data are belong to us !!! We will the data give back, when You to us XXXX BTC before 24H give. After 24H will we the data on the Internet for all to see publish !!! An extract for proof is gonna be publish very soon ! »* [optionnel] *En PJ, une capture d'écran du message.* »	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication + RSSI	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Prise en compte de l'information et investigation sur une possible exfiltration de données.	La capture d'écran peut être créée en se basant sur des images de rançongiciels trouvées sur Internet. Si cette option est retenue, la publication des attaquants peut être repérée par des internautes qui interpellent ensuite l'organisation sur les réseaux sociaux. De fausses preuves pourront être insérées plus tard dans le jeu pour faire réagir les joueurs si ce n'est pas le cas ici.
17	AAMMJJ **12:30**	**Stratégie de remédiation**	« *Bonjour,* *Nous avons vu dans la presse que votre organisation avait subit une cyberattaque. Vos activités sont-elles complètement à l'arrêt ? Quand pensez-vous pouvoir les reprendre ? Pouvez-vous nous faire parvenir un point sur la situation le plus rapidement possible et nous faire part de votre stratégie pour remédier à cet événement ?*»	Haute hiérarchie non joueuse (exemple : autorité de tutelle, autorité de contrôle, actionnaires…)	Directeur de crise	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Elaboration de la stratégie de remédiation et préparation de la présentation à la haute hiérarchie.	
18	AAMMJJ **12:45**	**Sollicitations clients/usagers**	« *Bonjour,* *Je suis contacté par plusieurs clients / usagers qui ont constaté que notre site Internet était inaccessible. Ils ne peuvent donc plus accéder à nos services [préciser lesquels ici]. Ils disent également avoir vu dans la presse que nous avions subi une cyberattaque et nous demandent si cela est à l'origine de l'indisponibilité du service. Ils s'interrogent enfin sur la reprise de ce dernier. Quelles informations est-il possible de leur transmettre ?*»	Responsable relation client/usager	Directeur du service	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Diffusion d'éléments de langage visant à rassurer sur le traitement de l'incident.	
19	AAMMJJ **13:00**	***[Option « Simulation ANSSI » #1]*** **Si l'organisation fait partie du périmètre d'intervention de l'ANSSI et que l'un des joueurs a déclaré l'incident**	« *Bonjour,* *Nous revenons vers vous suite à votre signalemet d'incident au CERT-FR. Quels sont les impacts sur vos activités ? Disposez-vous d'un prestataire pour vous aider ? Avez-vous besoin d'une assistance de l'ANSSI ?* **[si souhait d'accompagnement ANSSI]** *Un agent de l'ANSSI va vous contacter très prochainement pour vous aider à qualifier l'incident puis éventuellement vous accompagner à distance dans les démarches d'investigation et de remédiation. Voici dans un premier temps quelques documents de bonnes pratiques sur les mesures à mettre en place face à un rançongiciel (voir site Internet de l'ANSSI pour obtenir des éléments).* »	ANSSI	RSSI (ou personne généralement chargée de notifier les incidents)	Appel téléphonique	Transmission des informations disponibles à l'ANSSI.	Pour simuler l'ANSSI, vous pouvez vous inspirer des éléments publiés sur le site du CERT-FR. Si vous êtes un bénéficiaire régulé (LPM, NIS), vous pouvez notamment simuler la déclaration de votre incident via le formulaire qui se trouve sur le site de l'ANSSI. Pour les petites structures, simulez plutôt cybermalveillance.gouv.fr. Il est aussi possible de simuler l'intervention d'un prestataire.
19 bis	AAMMJJ **13:00**	***[Option « Simulation ANSSI » #2]*** **Si l'organisation fait partie du périmètre de l'ANSSI mais n'a pas déclaré l'incident**	«*Bonjour,* *Nous avons identifié sur les réseaux sociaux une publication qui pourrait indiquer qu'un incident de sécurité affecte vos systèmes d'information. Pouvez-vous nous confirmer cette information ? Avez-vous besoin d'une assistance de l'ANSSI ? Je vous recommande de consulter la rubrique « que faire en cas d'incident » sur notre site afin de mettre en place les premières mesures.* **[si souhait d'accompagnement ANSSI]** *Si vous souhaitez être accompagné par l'ANSSI, un agent va vous contacter très prochainement pour vous aider à qualifier l'incident puis éventuellement vous accompagner à distance dans les démarches d'investigation et de remédiation. Voici dans un premier temps quelques documents de bonnes pratiques sur les mesures à mettre en place face à un rançongiciel (voir le site Internet de l'ANSSI pour obtenir des éléments).* »	ANSSI	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission des informations disponibles à l'ANSSI.	Les stimuli 19 et 19ter ne sont à n'utiliser que lorsqu'une déclaration d'incident a été simulée par les joueurs auprès de la cellule d'animation. Leur horaire est à modifier en fonction du moment auquel les joueurs font leur signalement. (La prise de contact a lieu environ une heure après le signalement.) Pour aider les joueurs, il est possible d'ajouter un contact ANSSI ou prestataire dans l'annuaire qui renvoie à la cellule d'animation. Dans ce stimulus, l'agence ou le prestataire tente d'obtenir un maximum d'information pour comprendre au mieux la situation et émettre des recommandations.»
19 ter	AAMMJJ **13:00**	**Simulation d'un prestataire, si l'organisation leur a déclaré l'incident**	« *Bonjour,* *Nous revenons vers vous suite à votre signalemet d'incident auprès de nos équipes. Quels sont les impacts sur vos activités ?* *Une personne de notre équipe va vous contacter très prochainement pour vous accompagner à distance dans les démarches d'investigation et de remédiation.* »	Prestataire	RSSI (ou personne généralement chargée de notifier les incidents)	Appel téléphonique	Transmission des informations disponibles au prestataire.	
20	AAMMJJ **13:10**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Latéralisation du rançongiciel**	« *Bonjour,* *Je vous appelle car les membres de mon équipe ne peuvent plus utiliser leurs machines. Les écrans affichent un message demandant une rançon pour récupérer les données. On a une commande/un projet très important(e) à rendre en fin de semaine, il faut absolument qu'on puisse travailler. Que devons-nous faire ? Par ailleurs, je crois que le problème s'étend au moins à tout notre étage… Que se passe-t-il ?*»	Manager d'une équipe d'un second site [service/département au choix]	RSSI / DSI si pertinent ou équivalent du second site	Appel téléphonique	Transmission de l'alerte, déclenchement de la cellule de crise du second site et partage de l'information avec l'organisation.	Il peut s'agir ici de n'importe quel second site (situé en France ou l'étranger) : filiale, site de production, second bâtiment. Pour simuler l'impact progressif et la montée en puissance de la crise, ce stimulus est à multiplier (par intervalles de 5 minutes) en fonction du nombre de services / activités du second site que vous souhaitez immobiliser suite à la latéralisation du rançongiciel. Comme pour la latéralisation au sein de l'organisation, il est possible d'ajouter des conséquences métiers spécifiques à chaque service dans le script des appels téléphoniques et des mails.

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
21	AAMMJJ **13:10**	***[Option « Jeu sur plusieurs sites avec une seule cellule de crise impliquée en tant que joueur »]*** **Latéralisation du rançongiciel**	*« Bonjour,* *L'ensemble des postes de travail du site sont HS. Ils affichent tous le même écran qui nous demande de verser une rançon. Impossible de continuer à travailler, tout le site est à l'arrêt ! Les commandes/services/projets ne pourront pas être prêt(e)s à temps, c'est la catastrophe. Pouvez-vous envoyer une équipe pour y remédier ? Est-ce que le reste de l'organisation a le même problème ? Nous n'avons aucune idée de ce qu'il se passe.»*	Responsable du second site (filiale / prestataire / fournisseur / client)	Responsable sûreté / sécurité, directeur commercial, ou encore toute personne joueuse au sein de la cellule de crise de l'organisation jugée pertinente et qui serait le point de contact du second site	Appel téléphonique	Transmission de l'information en cellule de crise et diffusion des premières consignes.	Il peut s'agir ici de n'importe quel second site (situé en France ou l'étranger) : filiale, site de production, second bâtiment, etc. Pour poursuivre la simulation avec une seule cellule de crise, reprendre les stimuli avec deux cellules de crise (stimuli rose) et remplacer l'émetteur par le responsable du site et le destinataire par toute personne joueuse au sein de la cellule de crise de l'organisation jugée pertinente et qui serait le point de contact du second site.
22	AAMMJJ **13:30**	***[Option « Simulation ANSSI »]*** **Demande d'informations complémentaires**	*« Bonjour,* *Nous avons bien pris en compte votre signalement, enregistré sous la référence [RM#XXXXXX]. Dans le cadre de notre procédure de traitement d'incident, nous souhaiterions obtenir davantage d'informations. Vous trouverez ci-après les éléments demandés ainsi que des premières recommandations.* ▸ *Nom et Prénom / Courriel / Numéro de téléphone du RSSI et/ou de la personne en charge de cet incident* ▸ *Quelles sont les machines concernées par l'infection ? Quels types de fichiers ont été chiffrés ? Le SI compromis est-il en lien avec d'autres SI ?* ▸ *Quel est l'impact de cet incident sur la poursuite de vos activités ?* ▸ *Date et heure de l'infection* ▸ *Connaissez-vous le le vecteur de la compromission (courriel malveillant, exploitation de vulnérabilité, compromission de SI, etc.) ?* ▸ *Connaissez-vous le rançongiciel ? Sa version ?* ▸ *Quelle est l'extension des fichiers chiffrés ?* ▸ *Avez-vous des empreintes numériques (MD5, SHA1, SHA256 ...), une souche du rançongiciel ou des captures d'écran à nous transmettre ?* ▸ *Pouvez-vous nous communiquer la demande de rançon, les adresses courriel impliquées, les portefeuilles de Bitcoin ?* ▸ *Avez-vous des sauvegardes saines qui permettraient de restaurer le ou les systèmes infectés ?* ▸ *Avez-vous engagé un prestataire pour vous aider à remédier à cette attaque ? Si oui, lequel ?* ▸ *Quelles ont été les mesures réactives prises à la suite de cet incident ?* ▸ *Dans le cas où des données à caractère personnel aient été impactées, avez-vous déclaré l'incident à la CNIL ?* ▸ *Avez-vous pensé à faire X déclaration (par exemple, une déclaration à l'AFP en cas de cotation en bourse) ?* ▸ *Envisagez-vous ou avez-vous déjà effectué un dépôt de plainte ?* ▸ *Il est très peu probable que les données puissent être déchiffrées. Toutefois, sollicitez-vous une assistance de l'ANSSI dans vos actions de remédiation ? Si oui, pour quel(s) champs d'intervention ?* **Notez qu'à ce stade, le niveau d'engagement de l'ANSSI ne peut être défini.** *Vous pourrez également trouver de premières mesures de remédiation en cas d'infection par un rançongiciel en suivant ces liens :* ▸ *https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/* ▸ *https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001* ▸ *https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares* *Ensuite, et dans l'optique d'une démarche pénale (recommandée), nous vous rappelons que vous êtes invité à conserver sans y apporter de modification, tout document ou information établissant les faits et qui constitueraient potentiellement des éléments de preuve :* ▸ *copies physiques des disques durs (ou VM) des postes compromis ;* ▸ *copies des journaux d'événements disponibles sur tout équipement réseau qui auraient pu permettre la transmission des codes malveillants.* *Enfin, selon le type et la version du rançongiciel, il est possible qu'il existe un outil ou des clés de déchiffrement dédiés. Un référentiel de ces solutions est disponible sur le site Internet No More Ransom (https://www.nomoreransom.org/fr/index.html). Nous vous invitons à consulter les conseils préalables et guides d'utilisation avant toute opération de déchiffrement.* *Une personne en charge de la communication à l'ANSSI va prendre contact avec vos communicants. Pouvez-vous me transmettre leurs coordonnées ? Je vous propose de planifier rapidement un point d'étape.* »	ANSSI	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission des informations disponibles à l'ANSSI.	Il est possible de simuler à la place de ce stimulus un appel d'un pretataire, si contacté par les joueurs (via la cellule d'animation), qui posera des questions similaires. L'horaire du stimulus sur le point d'étape est à adapter en fonction de la réponse des joueurs.

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
23	AAMMJJ **13:40**	**Sollicitations internautes réseaux sociaux**	« *Bonjour,* *Voici quelques exemples de sollicitations que l'on trouve sur les réseaux sociaux :* *@organisation vous confirmez avoir été hacké ? #cyberthreat* *@organisation vous comptez payer la rançon ? #prisedotage #ransomware*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Prise en compte de l'information dans la stratégie de communication.	
24	AAMMJJ 13:50	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Latéralisation du rançongiciel**	« *Bonjour,* *L'ensemble des postes de travail du site sont HS, ils affichent tous le même écran qui nous demande de verser une rançon. Impossible de continuer à travailler, le site est à l'arrêt ! Les commandes/services ne pourront pas être prêts à temps, c'est la catastrophe. Pouvez-vous envoyer une équipe pour y remédier ? Est-ce que le siège a le même problème ? Nous n'avons pas plus d'information en l'état, nous sommes complètement dans le flou sur l'origine du problème.* »	Équipe technique second site	RSSI / DSI si pertinent second site ou équivalent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Si non réalisé précédemment, transmission de l'alerte, déclenchement de la cellule de crise du second site et partage de l'information avec l'organisation.	Comme pour le site principal de l'organisation, les planificateurs de l'exercice devront décider en amont si le second site a toujours accès à sa messagerie. Si oui, les échanges peuvent continuer comme précédemment. Sinon, la cellule de crise du second site devra mettre en place d'autres outils pour communiquer. Il convient également de matérialiser la perte d'accès au réseau : les ordinateurs, les outils de la cellule de crise, les annuaires, la messagerie etc. ne seront plus utilisables s'ils sont gérés sur le réseau. Les joueurs devront ainsi penser à des solutions de secours pour gérer la crise et maintenir certaines activités critiques.
25	AAMMJJ **14:00**	***[Option « Simulation ANSSI »]*** **Prise de contact de la COM**	« *Bonjour,* *Je travaille au sein de la division de la communication de l'ANSSI et je prends contact avec vous suite aux échanges que vous avez avec l'agence sur votre incident. On se propose de vous accompagner pour anticiper et/ou préparer vos éléments de communication externe et interne en cas de visibilité de l'attaque.* *Des premiers éléments de communication interne ou externe ont-ils déjà été transmis ? Avez-vous été sollicité par les médias ? Pour construire votre stratégie de communication, plusieurs actions à mener dans un premier temps : définition des parties prenantes (interne, clients, autorités, etc.), des cibles et objectifs de votre communication ainsi que des éventuels points de vigilance spécifiques à votre entité (notoriété/image de marque, exposition médiatique), votre secteur d'activité (actualités du marché, etc.), votre calendrier (obligation de communication financière, rachat, etc.), etc. Nous pouvons vous accompagner dans la rédaction de vos éléments de communication (communiqué de presse, communication interne). Si vous souhaitez mentionner l'ANSSI, nous demanderons à valider la mention.* »	ANSSI COM	Responsable communication	Appel téléphonique	Elaboration de la stratégie de communication et transmission des informations au second site.	La posture générale de l'ANSSI est d'accompagner l'organisation mais pas de communiquer à sa place.
26	AAMMJJ **14:20**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Éléments sur la suspension des activités du second site**	« *Bonjour,* *À la suite de l'incident en cours depuis ce matin, voici un point de situation des impacts recensés :* *Exemples :* *- impossible de prendre les commandes (ou de les suivre) ;* *- impossible de marquer des produits et donc de les émettre ;* *- activités en mode dégradé/à l'arrêt ;* *- etc.* »	Manager d'une équipe du second site [service/département au choix]	Chef cellule de crise second site ou représentant métier en cellule de crise	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Réflexion sur la continuité d'activité.	Impacts à définir en fonction des spécificités de votre organisation et de votre second site et à décliner en autant de stimuli qu'il y a d'impacts souhaités.
27	AAMMJJ **14:35**	**Sollicitation presse**	« *Bonjour,* *Nous avons appris que votre organisation venait d'être la cible d'une cyberattaque et que les attaquants ont publié un ultimatum : payer la rançon ou voir vos données publiées en ligne. Confirmez-vous ces informations ? Cette attaque a t-elle un impact conséquent sur votre organisation ? Qui en est à l'origine selon vous ?* »	Journaliste (presse spécialisée)	Responsable communication	Appel téléphonique	Transmission des éléments de langage préalablement définis ou renvoi vers un communiqué de presse si publié.	
28	AAMMJJ **15:00**	**Sollicitation presse**	« *Bonjour,* *Pour information, nous venons d'identifier la parution d'un article dans la presse relatif à l'incident en cours. L'article met particulièrement en cause nos capacités à répondre à l'incident et à y remédier.* »	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication + RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Transmission des éléments de langage préalablement définis ou renvoi vers un communiqué de presse si publié.	Ces sollicitations de la presse peuvent également être adressées au second site.
29	AAMMJJ **15:15**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Sollicitation presse**	« *Bonjour,* *Nous avons appris que votre site venait d'être victime d'une cyberattaque. Confirmez-vous cette information ? Cette attaque est-elle liée à celle ayant touché le siège ce matin ? Etes-vous en mesure de poursuivre votre activité ?* »	Journaliste	Équipe communication du second site	Appel téléphonique	Utiliser (si transmis) les EDL du siège ou les demander avant de répondre. Renvoyer à un communiqué de presse commun si existant.	

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
30	AAMMJJ **15:20**	**Point d'étape sur l'attaque**	*« Bonjour,* *Je vous informe que dans l'objectif de stopper la propagation du code malveillant, les interconnexions des systèmes d'information des autres sites de l'organisation avec les systèmes du siège ont été coupées. A notre connaissance, seuls le site principal et un second site ont été impactés par l'attaque. »*	Membre équipe technique ou prestataire	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Prise en compte dans le point de situation et transmission de l'information à la cellule de crise.	Si l'organisation prend cette décision plus tôt, cela doit être pris en compte par la cellule d'animation (envoyer ce stimulus plus tôt). Plus généralement, toute mesure préventive prise, telle que des coupures réseau, doit être ensuite intégrée au scénario au bon moment afin que les joueurs pensent à avertir les parties prenantes pour lesquelles ils jugent nécessaire de le faire et puissent anticiper les actions de communication liées. Les effets de cette décision doivent être intégrés au scénario.
31	AAMMJJ **15:30**	**Sollicitation presse**	*« Bonjour,* *Votre organisation semble être la cible d'une attaque informatique sophistiquée. Les attaquants vous demandent de verser une rançon dans les 24h. Comptez-vous payer la rançon ? Commet votre organisation a-t-elle été impactée ? Depuis combien de temps cette situation est-elle en cours ? »*	Journaliste	Responsable communication	Appel téléphonique	Transmission des éléments de langage préalablement définis ou renvoi vers un communiqué de presse si publié.	
32	AAMMJJ **15:35**	***[Option « Publication des données exfiltrées »]***	*« Bonjour,* *Je viens de trouver une publication sur le site pastebin qui comprend un grand nombre de documents provenant potentiellement de notre organisation (https://pastebin.com/xxxx). À première vue ces documents ont l'air authentiques mais je n'ai pas tout regardé. Avec certains collègues nous sommes en train de les relire et de vérifier cela. »*	Personne réalisant une veille médiatique (salarié ou prestataire)	RSSI ou équivalent / DSI si pertinent + Responsable communication + Responsable sûreté	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Préparation d'une stratégie de communication.	Dans le cadre de l'exercice, il n'est pas utile de distribuer aux joueurs l'intégralité des documents qui seraient publiés. Il est toutefois intéressant d'avoir sous la main quelques documents à envoyer comme illustrations (et qui peuvent par exemple être mentionnés par la presse). Il revient aux planificateurs d'en déterminer le nombre et la sensibilité.
33	AAMMJJ **15:40**	**Pression interne (siège de l'organisation)**	*« Bonjour,* *Les postes de travail du service sont toujours inutilisables. Pouvez-vous m'indiquer quand cette situation sera résolue ? Mes agents ne peuvent plus travailler et les commandes prennent du retard, la situation devient intenable et nous manquons toujours d'information sur la situation. »*	Manager	RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Diffusion des consignes.	Stimulus à multiplier autant que souhaité pour accentuer la pression sur les joueurs. Les demandes peuvent également s'adresser aux directeurs métiers présents en cellule de crise.
34	AAMMJJ **15:45**	**Analyses techniques via *[option « Simulation ANSSI »]* ou un prestataire**	*« Bonjour,* *Voici quelques éléments issus de notre analyse. Nous avons pu identifier le code malveillant à l'origine de l'attaque, il s'agirait du rançongiciel EvilRansomware, Nous n'avons cependant pas encore identifié le vecteur d'infection intiale. Ce code malveillant chiffre les fichiers présents sur la machine ainsi que sur les partages réseau accessibles. Il supprime également les copies cachées.* *Votre SI ne retrouvera pas un fonctionnement normal pendant une semaine au moins. Il faudra prévoir de travailler quasiment sans informatique et donc en mode dégradé durant cette période.* *Quelles sont les priorités de rétablissement des services ? Avez-vous prévu des mesures pour gérer cette situation dans la durée (déploiement du PCA, roulements des équipes/travail de nuit/ravitaillement, recours à un ou plusieurs prestataire(s), etc.) ? »*	ANSSI ou prestataire	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Préparation d'une stratégie de remédiation, mise à jour du point de situation. Réflexion sur la continuité d'activité et le fonctionnement en mode dégradé.	Pour permettre aux joueurs d'expérimenter plusieurs phases de la crise, le jeu est volontairement accéléré et n'est pas représentatif de ce qu'il se serait passé dans un cas réel. En effet, à titre d'illustration, il n'est pas rare que le SI soit complètement indisponible durant 1 à 2 semaines face à ce type d'attaque. De plus, le retour à un fonctionnement nominal du SI s'avère souvent long, jusqu'à prendre parfois plusieurs mois. Ce stimulus peut également être émis par un prestataire.
35	AAMMJJ **15:50**	***[Option « Publication des données exfiltrées »]*** **Analyses des données publiées par les attaquants**	*« Bonjour,* *Les quelques personnes qui ont commencé à lire les documents confirment leur authenticité. Nous avons par exemple retrouvé une liste nominative qui correspond bien au personnel de l'organisation, un compte-rendu de réunion et un rapport (voir PJ). Nous poursuivons la lecture des documents et reviendrons vers vous dès que possible. »*	Chef de service [au choix, service impacté par les divulgations simulées]	Directeur de crise	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Adaptation de la stratégie de communication.	Cet inject peut également être adapté au second site avec des documents différents.
36	AAMMJJ **15:55**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Sollicitations réseaux sociaux**	*« Bonjour,* *Voici quelques exemples de sollicitations que l'on trouve sur les réseaux sociaux :* *@secondsite vous confirmez avoir été hacké ? #ransomware #cyberthreat* *Il semblerait que@secondsite se soit fait pwnd. Des infos ? #insecure #ransomware* *@organisation @secondsite vous comptez payer la rançon ? #prisedotage #ransomware »*	Personne réalisant une veille médiatique (salarié ou prestataire) au sein du second site	Resposable communication du second site	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Prise en compte des messages dans la stratégie de communication et échange avec l'organisation pour les EDL.	

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
37	AAMMJJ **16:00**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Sollicitations clients / usagers**	*« Bonjour,* *Je suis contacté par plusieurs clients / usagers qui ont constaté que notre site Internet était inaccessible. Ils ne peuvent donc plus accéder à nos services [préciser lesquels ici]. Ils disent également avoir vu dans la presse que nous avions subit une cyberattaque et nous demandent si cela est à l'origine de l'indisponibilité du service. Ils s'interrogent enfin sur la reprise de ce dernier. Quelles informations est-il possible de leur transmettre ?»*	Responsable relation client / usager du second site	Directeur du service du second site	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Diffusion d'éléments de langage visant à rassurer sur le traitement de l'incident.	
38	AAMMJJ **16:05**	***[Option « Simulation ANSSI »]*** **Infos sur le vecteur d'infection via un membre simulée de l'équipe technique de l'organisation ou un prestataire**	*« Bonjour,* *Nous avons identifié le mail d'hameçonnage ayant permis l'intrusion initiale dans le SI. Nos analyses se poursuivent afin d'identifier le mode de latéralisation. Le poste à l'origine de la compromission appartient à un membre du COMEX.* *Nous avons retrouvé la pièce-jointe malveillante à l'origine de l'attaque. Il semble bien s'agir du rançongiciel EvilRansomware. À notre connaissance, il n'existe pas de clé de déchiffrement.* *Nous pouvons toutefois utiliser les sauvegardes qui ne sont pas très récentes. Certaines données seront irrémédiablement perdues. De ce fait, certaines activités ne pourront pas reprendre immédiatement. Le retour à un fonctionnement normal du SI sera long, il faut s'y préparer. »*	ANSSI ou Membre équipe technique ou Prestataire	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Transmission des informations au second site et partage des éléments techniques.	Pour permettre aux joueurs d'expérimenter plusieurs phases de la crise, le jeu est volontairement accéléré et n'est pas représentatif de ce qu'il se serait passé dans un cas réel. En effet, à titre d'illustration, il n'est pas rare que le SI soit complètement indisponible durant 1 à 2 semaines face à ce type d'attaque. De plus, le retour à un fonctionnement nominal du SI s'avère souvent long, jusqu'à prendre parfois plusieurs mois. Ce stimulus peut également être émis par un prestataire ou un membre simulé de l'équipe technique de l'organisation.
39	AAMMJJ **16:07**	***[Option « Publication des données exfiltrées »]*** **Interrogations internes**	*« Bonjour,* *J'ai appris que des données de chez nous avaient été publiées. Savez-vous où trouver ces documents et si ceux de mon service en font partie ? Nous traitons des données très sensibles qui ne devraient pas être connues à l'extérieur. »*	Chef de service [au choix, service impacté par les divulgations simulées]	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Communication sur les travaux de vérification des données.	Ces inquiétudes peuvent concerner différents services qui peuvent être simulés sous ce même format.
40	AAMMJJ **16:15**	**Sollicitation réseaux sociaux**	*« Bonjour,* *Pour information, des éléments sur l'attaque circulent sur les réseaux sociaux. Des utilisateurs partagent l'article et s'interrogent sur les capacités de l'organisation à faire face à l'attaque. Ils interpellent également directement nos dirigeants sur Twitter. »*	Personne réalisant une veille médiatique (salarié ou prestataire)	Équipes communication, RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Préparation des éléments de langage en réactif.	
41	AAMMJJ **16:20**	***[Option « Publication des données exfiltrées»]*** **Sollicitation presse**	*« Bonjour,* *Pour information, un article de presse vient d'être publié et mentionne la publication de données de l'organisation. Les journalistes mentionnent seulement quelques titres de documents et ne semblent pas les avoir analysés. Il semble s'agir de rapports et de notes. [optionnel : rédiger l'article de presse à joindre au message]. »*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication + responsable sûreté + RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Adaptation de la stratégie de communication.	
42	AAMMJJ **16:25**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Publication des données exfiltrées par les attaquants sur un site Internet**	*« Bonjour,* *Pour information, un article de presse vient d'être publié et mentionne la publication de données de l'organisation. Les journalistes mentionnent seulement quelques titres de documents et ne semblent pas les avoir analysés. Il semble s'agir de rapports et de notes. [optionnel : rédiger l'article de presse à joindre au message]. »*	Personne réalisant une veille médiatique (salarié ou prestataire) au sein du second site	Responsable communication + responsable sûreté + RSSI ou équivalent / DSI si pertinent du second site	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Adaptation de la stratégie de communication.	
43	AAMMJJ **16:30**	***[Option « Publication des données exfiltrées »]*** **Interrogations internes**	*« Bonjour,* *À la suite de la divulgation sur Internet de données de notre organisation, mes agents s'inquiètent de la possibilité que leurs données personnelles aient pu aussi être publiées. Pouvez-vous m'indiquer ce qui va être mis en place pour adresser ces inquiétudes ? »*	Manager	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Transmission des consignes définies par la cellule de crise et prise en compte de la remarque pour la communication interne.	

N°	HORAIRE	PHASE	CONTENU STIMULI (contenu du mail ou de l'appel téléphonique à adapter à votre organisation)	ÉMETTEUR (non joueur - simulé par la cellule d'animation)	DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
44	AAMMJJ **16:35**	***[Option « Publication des données exfiltrées »]*** **Sollicitation clients/usagers**	*« Bonjour,* *À la suite de la divulgation sur Internet de données de notre organisation, nous avons été contactés par plusieurs clients/usagers inquiets que leurs données aient pu être publiées. »*	Service client ou en lien avec des usagers	Responsable communication + responsable sûreté + RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Adaptation et diffusion d'éléments de langage ou renvoi vers un communiqué si rédigé.	
45	AAMMJJ **16:37**	***[Option « Jeu sur plusieurs sites avec plusieurs cellules de crise impliquées en tant que joueurs »]*** **Sollicitation clients/usagers**	*« Bonjour,* *À la suite de la divulgation sur Internet de données de notre second site, nous avons été contactés par plusieurs clients/usagers inquiets que leurs données aient pu être publiées. »*	Service client ou en lien avec des usagers du second site	Responsable communication + responsable sûreté + DSI/RSSI du second site	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Adaptation et diffusion d'éléments de langage.	
46	AAMMJJ **16:42**	***[Option « Publication des données exfiltrées »]*** **Sollicitation réseaux sociaux**	*« Bonjour,* *Pour information, de nombreux tweets commentant la divulgation de données de notre organisation. Les messages publiés s'interrogent particulièrement sur l'authenticité des données et sur la sécurité des données de nos clients, qui continuent à nous contacter. »* Voici quelques exemples de tweets : *@organisation n'est déjà pas capable d'éviter de se faire hacker, et maintenant ils n'arrivent même pas à gérer les conséquences et sécuriser les données #insecure #ransomware* *@organisation les attaquants seraient en possession des données de vos clients. Vous confirmez ? #organisation_leak #ransomware »*	Personne réalisant une veille médiatique (salarié ou prestataire)	Responsable communication + responsable sûreté + RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Vérification de l'intégralité des données, préparation d'éléments de langage.	
47	AAMMJJ **16:45**	***[Option « Simulation ANSSI »]***	*« Bonjour,* *Quels ont été les retours suite à la publication de votre communiqué de presse ? Souhaitez-vous publier à nouveau quelque chose ? »*	ANSSI COM	Responsable communication	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Faire un point de situation sur la stratégie de communication.	
48	AAMMJJ **16:50**	***[Option « Simulation ANSSI »]*** **Stimulus conclusif pour la fin de jeu via un membre simulée de l'équipe technique de l'organisation ou un prestataire**	*« Bonjour,* *Je vous informe des premiers résultats de la phase d'investigation [option : menées par les équipes de l'ANSSI / prestataire]. Nous avons pu confirmer les éléments suivants relatifs à l'incident : un logiciel malveillant a été déposé sur votre SI suite à une campagne de hameçonnage fructueuse exploitant la vulnérabilité CVE-20xx-xxx affectant le système d'exploitation Windows xxx. Par ailleurs, le programme malveillant utilise de multiples moyens de latéralisation (exploitation de services légitimes de Microsoft Windows et de codes publiés sur Internet permettant d'exploiter des vulnérabilités connues tels qu'Eternal Blue), [option : ce qui explique que le second site ait également été touché]. Afin de compléter ces premiers éléments d'analyse et sécuriser votre SI, il est nécessaire d'expulser l'attaquant du système et de s'assurer qu'il ne puisse pas revenir. [option : Pour cela, il faudrait qu'une équipe de l'ANSSI / un prestataire puisse intervenir au plus vite afin de vous accompagner dans cette phase de remédiation.]* *Enfin, l'éditeur vient de publier un correctif pour la vulnérabilité mentionnée ci-dessus (cf. bulletin d'alerte du CERT-FR en PJ). Il convient de l'appliquer dès que possible.* *[A : sauvegardes hors-ligne préservées] Le déploiement des sauvegardes pourra être réalisé lorsque nous nous serons assurés que les SI sont sains et sécurisés. Des essais seront réalisés au préalable. Si ceux-ci sont concluants nous poursuivrons l'opération sur l'ensemble du parc informatique. Cela devrait prendre au minimum quelques jours.* *[B : sauvegardes impactées] Les serveurs de sauvegarde sont HS. Nous allons devoir procéder à une reconstruction complète du parc informatique, ce qui devrait prendre une semaine à dix jours.»*	ANSSI ou membre équipe technique ou prestataire	RSSI ou équivalent / DSI si pertinent	Mail si accessible, sinon appel téléphonique ou messagerie de secours	Transmission des informations au second site. Réflexion sur la continuité et la reprise des activités.	Pour permettre aux joueurs d'expérimenter plusieurs phases de la crise, le jeu est volontairement accéléré et n'est pas représentatif de ce qu'il se serait passé dans un cas réel. En effet, à titre d'illustration, il n'est pas rare que le SI soit complètement indisponible durant 1 à 2 semaines face à ce type d'attaque. De plus, le retour à un fonctionnement nominal du SI s'avère souvent long, jusqu'à prendre parfois plusieurs mois. Ce stimulus peut également être émis par un prestataire ou un membre simulé de l'équipe technique de l'organisation.
49	AAMMJJ **17:00**	**Fin de l'exercice**	*« Bonjour à tous,* *l'exercice est terminé. Nous vous remercions pour votre participation et vous invitons à participer au retour d'expérience à chaud qui aura lieu dans 5 minutes. »*	DIRANIM	Tous les joueurs	Mail	Participation au RETEX.	Bravo vous avez organisé un exercice de gestion de crise cyber !