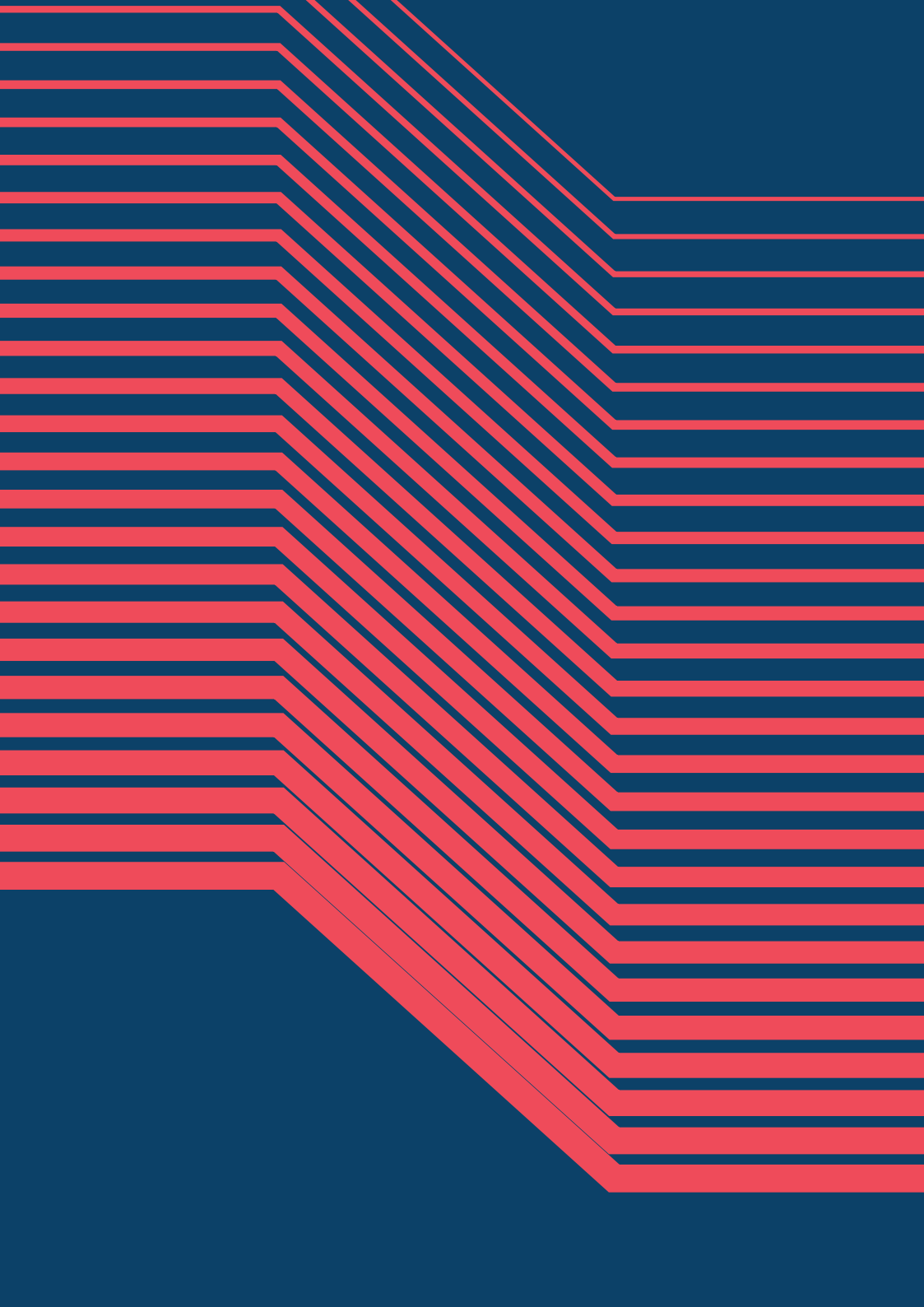
RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

COLLECTION
GESTION DE CRISE CYBER

ORGANISER UN EXERCICE DE GESTION DE CRISE CYBER

CCA



COLLECTION
GESTION DE CRISE CYBER

GUIDE

ORGANISER UN EXERCICE DE GESTION DE CRISE CYBER

SOMMAIRE

ÉDITORIAL

La sécurité informatique a ceci de frustrant que trop souvent les bienfaits des efforts en la matière sont peu visibles : une attaque enrayée par une bonne préparation ne fait pas de bruit ! Mais ne nous faisons pas d'illusions : l'ampleur du risque est bien réelle et le manque d'anticipation, souvent dévastateur.

J'aime à rappeler qu'en matière de protection des systèmes d'information, l'anticipation est la clé. Je sais qu'elle représente un investissement pour les organisations qui ont par ailleurs d'autres réalités à considérer. La responsabilité de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est donc de soutenir leurs efforts en ce sens et, continuellement, de rappeler l'importance des enjeux de cybersécurité.

Face à la menace, l'organisation d'exercices est fondamentale. J'en suis témoin ! En s'entraînant, les équipes impliquées dans la gestion de crise développent, exercice après exercice, des réflexes et des méthodes pour mieux travailler ensemble. Lorsqu'une attaque survient, elles sont alors prêtes à y faire face. D'autant que les crises cyber ont leurs spécificités. Il ne faut surtout pas attendre la catastrophe pour apprendre à en maîtriser les rouages !

Fruit d'une riche expérience, développée au fil des années, dans l'organisation d'exercices de gestion de crise cyber, ce guide vous accompagnera dans la mise en place de vos propres entraînements. Je souhaite qu'il contribue à vous permettre de développer les compétences de vos équipes et ainsi à renforcer la résilience de votre organisation.

Guillaume Poupard
Directeur général de l'ANSSI

Le Club de la Continuité d'Activité (CCA) est une association comprenant plus de 80 membres, entreprises et cabinets de conseils. Sa vocation première est le partage des bonnes pratiques entre adhérents sur la gestion de la crise et de la continuité d'activité. Après plus de dix ans d'existence, le CCA est devenu un acteur essentiel dans la promotion de la résilience de l'entreprise.

Thème de l'un de nos derniers exercices annuels inter-entreprises avec plus de 100 participants et sujet régulier de nos séminaires, autour notamment de la communication de crise, le risque cyber est l'une de nos préoccupations majeures. Par les impacts multiformes et sévères qu'il peut engendrer, il fait régulièrement l'objet d'analyses et de partages d'expérience au sein de l'ensemble de nos groupes de travail.

Échanger et s'entraîner sont les deux mots qui nous animent en tant que praticiens de la crise, de la continuité d'activité et de la résilience dans nos organisations. Ce guide permet à de nombreuses organisations de pouvoir réaliser un exercice de crise cyber en toute autonomie. Il est une base très structurante pour l'appréhension de ce risque qui touche tous les secteurs et toutes les tailles d'organisation.

Vincent Vallée
Président du CCA

PRÉSENTATION

Face à une menace informatique toujours croissante et en mutation, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations.

Ce guide vise à accompagner, pas à pas, les organisations dans la mise en place d'un exercice de gestion de crise d'origine cyber[1] vraisemblable et formateur, pour les joueurs comme pour les organisateurs.

Il propose une méthodologie basée sur le standard reconnu de la norme relative aux exercices (ISO 22398:2013).

À qui s'adresse ce guide ?

Toute organisation privée comme publique, petite ou grande, souhaitant s'entraîner à la gestion de crise cyber peut consulter ce guide.

Plus particulièrement, il s'adresse à toute personne souhaitant mettre en place un exercice de **niveau décisionnel**[2] visant à entraîner la cellule de crise de son organisation : *risk managers*, responsable de la continuité d'activité, des exercices ou de la gestion de crise, responsable de la sécurité des systèmes d'information ou équivalent, etc. Ce guide ne vise ainsi pas à construire des exercices purement techniques proposant par exemple une simulation complète d'un système d'information (SI) à l'aide de machines virtuelles (dit « *cyber range* »).

Que contient-il ?

- Quatre étapes accompagnées de fiches pratiques qui les complètent et les illustrent ;
- des recommandations issues de l'expérience de l'ANSSI et des membres du groupe de travail gestion de crise du CCA ;

1 : Par abus de langage, dans la suite du guide l'expression « gestion de crise cyber » est employée pour « gestion de crise d'origine cyber » et « exercice de crise cyber » pour « exercice de crise d'origine cyber ».
2 : Le « niveau décisionnel » fait ici référence à une cellule de crise, composée des membres de la direction et des métiers impliqués dans la crise, qui sera en charge d'assurer le suivi et le pilotage de la gestion de la crise et de prendre des décisions.

- un exercice complet en fil rouge du guide, dénommé RANSOM20 et développé progressivement pour illustrer chaque étape ;
- des annexes dont un glossaire définissant l'ensemble des expressions employées dans ce guide spécifiques aux exercices.

Comment l'utiliser ?

Les étapes peuvent être consultées indépendamment les unes des autres en fonction de l'expérience de l'organisation et de ses besoins en matière d'exercices de gestion de crise. Ce format permet également d'envisager une externalisation de tout ou partie de ces étapes, afin que chaque organisation, quelle que soit sa taille et son budget, puisse s'engager dans ce type d'exercice.

EXERCICE RANSOM20

Le fil rouge : RANSOM20

Tout au long du guide, un exemple d'exercice (RANSOM 20) est développé. Il permet d'illustrer des recommandations formulées à chaque étape.

Afin de pouvoir être utilisé et adapté par le plus grand nombre, l'exemple porte sur une cyberattaque par rançongiciel. Ce mode opératoire constitue une tendance qui s'intensifie et qui touche les grandes organisations comme les plus petites.

Cet exemple est développé dans différentes **fiches pratiques** qui, une fois compilées, forment un exercice complet réutilisable par toute organisation.

Pour en savoir plus sur l'exercice RANSOM20, vous pouvez consulter son scénario (voir fiche pratique n° 4) ou son chronogramme (voir fiche pratique n° 6).

RECOMMANDATIONS PRÉALABLES

POSITIONNER SA RÉSILIENCE CYBER AU PLUS HAUT NIVEAU

Ces recommandations préalables permettent d'aborder les notions d'exercice et de crise cyber en soulignant leurs spécificités. Elles insistent également sur l'importance d'inscrire l'exercice dans une réflexion globale visant à renforcer la résilience de l'organisation. Enfin, elles constituent des recommandations pour fédérer autour de l'exercice.

Les éléments décrits dans cette partie sont à construire en parallèle des exercices et des réflexions menées en matière de gestion de crise cyber.

LIVRABLES À PRODUIRE :

- Stratégie d'exercices (optionnel)
- Programme d'exercices (optionnel)
- Plan de communication

PHASE 1

COMPRENDRE LES SPÉCIFICITÉS DU CYBER

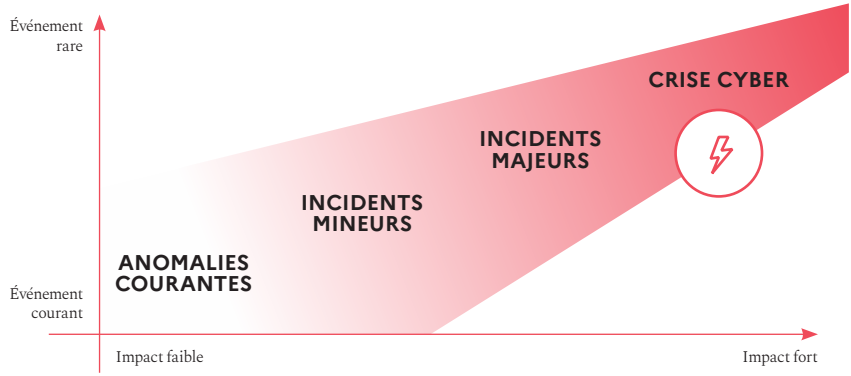
Qu'est-ce qu'une crise cyber ?

Il n'y a pas à proprement parler de crise cyber mais des crises ayant pour origine une attaque cyber.

On parlera ici de « crise cyber » lorsqu'une ou plusieurs action(s) malveillante(s) sur le système d'information (SI) génère(nt) une déstabilisation majeure de l'entité, provoquant des impacts multiformes et importants, jusqu'à engendrer parfois des dégâts irréversibles.

Une crise cyber est un évènement rare avec un impact fort. Il convient pour chaque organisation de réaliser une analyse de risques et de déterminer les événements susceptibles de constituer une menace importante pour l'organisation et générer une crise[3].

POSITIONNER UNE CRISE CYBER FACE AUX ÉVÉNEMENTS PORTANT ATTEINTE AUX SI



3 : Pour plus d'informations sur la méthodologie d'analyse de risques, se référer à la méthode EBIOS Risk Manager (ANSSI, 2018) - www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager

CARACTÉRISTIQUES DES CRISES D'ORIGINE CYBER

Les crises d'origines cyber ont de multiples spécificités :

- **Fulgurance et ubiquité des impacts :** une organisation peut être touchée à de multiples endroits simultanément.
- **Incertitude, potentiellement durable, liée au domaine :** les impacts sont difficiles à estimer et l'objectif de l'attaquant pas toujours identifiable facilement.
- **Évolutivité :** ce type de crise peut évoluer rapidement dans la mesure où les attaquants sont susceptibles de réagir aux actions entreprises par l'organisation ciblée, par exemple en effaçant leurs traces par des actions destructrices.
- **Technicité du sujet :** du fait de la complexité des SI et des modes opératoires utilisés par les attaquants, les acteurs au cœur de la gestion de crise sont les experts techniques. L'enjeu est de faire en sorte que ces experts et les acteurs habituels de la gestion de crise se comprennent pour travailler ensemble efficacement.
- **Propagation potentiellement mondiale :** compte tenu de l'interconnexion des systèmes et de l'existence de systèmes avec une empreinte mondiale, les attaques peuvent se propager très rapidement. Le rançongiciel WannaCry a touché plus de 250 000 postes dans 150 pays en une seule nuit, et plus de 900 millions de postes au total.
- **Élasticité du temps de crise :** pour les attaquants, il est facile de réitérer leurs attaques avec le même mode opératoire. Il est donc crucial, dans la réponse à une cyberattaque, de non seulement rétablir le bon fonctionnement des SI mais également de rehausser le niveau de protection afin d'empêcher la réitération des attaques. Le rançongiciel WannaCry a ainsi contaminé des victimes durant plus d'une année après son apparition.
- **Sortie de crise longue** (**plusieurs mois**) **:** la réponse technique, l'investigation numérique et le rétablissement du fonctionnement des SI sont des actions qui peuvent prendre du temps ce qui nécessite de gérer les impacts immédiats, mais aussi de mettre en place une réponse pérenne. C'est pourquoi les plans de continuité d'activité

(PCA) des organisations sont cruciaux dans une crise engendrée par une cyberattaque.

- **Complexité des attributions :** les cyberattaques sont difficilement attribuables à une personne ou une entité particulière car il est aisé de dissimuler sa véritable identité dans le cyberespace.

TRAITEMENT D'UNE CRISE CYBER

Les conséquences d'une cyberattaque sont multiples, comme pour n'importe quel événement générant une crise pour votre organisation. Les impacts peuvent être juridiques, réglementaires, légaux, métiers, organisationnels, RH, financiers, réputationnels, techniques, etc. Ils peuvent également engendrer une forte pression médiatique.

Faire face à une crise d'origine cyber nécessite ainsi de **coordonner des équipes variées**, dont les périmètres d'action et les décisions sont à la fois d'ordre technique (équipes en charge de la sécurité des SI, ou SSI, services informatiques, etc.) et stratégique (continuité d'activité, communication, etc.) pour **endiguer les effets de la crise** d'une part, et **rétablir le bon fonctionnement des systèmes** d'autre part.

Au niveau décisionnel, cela implique d'intégrer dans le dispositif de gestion de crise habituel la direction des systèmes d'information (DSI) ou le responsable de la sécurité des systèmes d'information (RSSI) afin d'apporter aux décideurs une vision éclairée du **déroulement de l'attaque**, nécessaire à **l'adaptation et à l'orientation des mesures de remédiation**.

En parallèle, une autre cellule est en charge d'analyser la situation technique et de proposer des actions pour rétablir l'activité. Il s'agit de la cellule de crise opérationnelle, simulée dans le cadre des exercices proposés ici et ne faisant donc pas l'objet de la méthodologie présentée dans ce guide.

En ce qui concerne la résolution technique, plusieurs étapes sont à mettre en œuvre par l'organisation seule, si elle en a les moyens, ou à l'aide de prestataires. Ces étapes visent à faire cesser les effets de l'attaque et à éjecter l'attaquant en dehors des SI infectés :

- **Investigation :** collecter et analyser les éléments techniques permettant de comprendre le chemin d'attaque utilisé par les attaquants et les actions de ces derniers sur les systèmes infectés (mesurer l'étendue des dégâts, comprendre quelle en est la source, réfléchir à des actions pouvant contribuer à rétablir la situation).
- **Remédiation :** restaurer les systèmes dans leur état initial en éjectant l'attaquant du système et améliorer la sécurité pour éviter une attaque similaire par l'application de mesures d'assainissement.
- **Stabilisation :** améliorer la sécurité à plus long terme par la définition et l'application de mesures de sécurisation et l'amélioration de la supervision (détection des attaques).

L'incident et les phases d'investigation et de remédiation peuvent être simulés dans le cadre d'un exercice. Seuls l'incident et la phase d'investigation sont joués dans l'exercice fil rouge RANSOM20.

Comment appréhender les exercices de gestion de crise cyber ?

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**.

Un exercice de gestion de crise ne doit **en aucun cas avoir un impact réel sur les activités de l'organisation**. Par exemple, dans le cadre d'un scénario mentionnant une cyberattaque qui cause un arrêt des machines, ces dernières ne doivent en aucun cas cesser réellement de fonctionner. Cet événement est simulé par l'appel d'un employé à sa hiérarchie, constatant que les machines sont arrêtées.

Les spécificités liées à la problématique cyber décrites ci-dessus démontrent la nécessité de se préparer en organisant des exercices. Ceux-ci doivent être inscrits dans une réflexion globale et de haut niveau, afin

qu'ils soient vecteurs de résilience au sein de toute l'organisation et de son écosystème.

Recommandation

Un exercice ne vise pas à surprendre ou à piéger les participants, mais à les accompagner dans un entraînement cadré reposant sur des objectifs définis, communiqués et partagés en amont.

On considère comme réussi, un exercice qui a impliqué l'ensemble des participants concernés, qui leur a permis d'en tirer des leçons et qui leur a donné envie de réitérer l'expérience.

PHASE 2

INSCRIRE L'EXERCICE DANS UNE RÉFLEXION GLOBALE DE RÉSILIENCE

Inscrire l'exercice dans une réflexion plus globale, que l'on nommera ici stratégie d'exercices, permet de contribuer à **renforcer la résilience de l'organisation**.

La stratégie d'exercices tient compte des procédures de gestion de crise de l'organisation et des politiques de continuité d'activité et de sécurité des systèmes d'information (SSI) et doit être adaptée à l'organisation. Si de telles procédures n'existent pas au sein de votre organisation, un exercice peut aussi être l'occasion d'y réfléchir.

Cette stratégie doit être déclinable par les différentes branches de votre organisation. Par exemple, le service communication doit être en mesure de décliner la stratégie globale en une stratégie d'exercices de communication de crise cyber.

Elle doit également prévoir une montée en compétences par l'organisation d'exercices de plus en plus complexes jusqu'à atteindre l'ensemble des objectifs préalablement définis. Elle prend en compte l'entraînement des niveaux décisionnel comme opérationnels d'une organisation[4].

La stratégie d'exercices permet notamment de :

- **sensibiliser les personnels** aux problématiques cyber et d'entraîner ceux qui ont un rôle à jouer ;
- **éprouver l'efficience des procédures** mises en place dans le cadre de ce dispositif et de les améliorer ;
- **rendre compte des efforts produits** en matière de résilience cyber répondant ainsi à de potentielles exigences légales et attentes sociétales.

4 : Dans ce guide, seul l'entraînement du niveau décisionnel est concerné.

Elle prend la forme d'un document synthétique dont les éléments peuvent être utilisés pour communiquer sur la démarche de renforcement de la résilience.

Constituer un programme d'exercices

Inscrire l'exercice dans un programme dédié permet d'**optimiser les ressources et les moyens mis en œuvre**, ainsi que d'améliorer la résilience de l'organisation face à des cyberattaques en s'assurant de la préparation d'un maximum de personnes.

Le programme d'exercices doit être élaboré en lien avec des procédures de gestion de crise ou de résilience. Il s'inscrit également dans une **démarche d'apprentissage progressif** généralement pluriannuelle avec des objectifs et des paliers à atteindre au fil du temps. Il permet de :

- **maintenir la cohérence** avec l'ensemble des entraînements envisagés ;
- s'assurer que le personnel impliqué dans la gestion d'une crise en **maîtrise les fondamentaux** ;
- **maintenir le niveau d'engagement** et de sensibilisation des acteurs de la gestion de crise et en particulier ceux moins expérimentés sur les problématiques cyber ;
- **conserver la connaissance et capitaliser** sur les compétences acquises, notamment au cours de l'exercice, car certains éléments, dans la gestion de projet ou le retour d'expérience (RETEX), contribuent à l'amélioration continue du dispositif de gestion de crise et des capacités de continuité d'activité.

Saisir les opportunités de l'exercice

Outre les apports relatifs à la préparation et à l'entraînement de ses participants, l'exercice peut être valorisé de la manière suivante :

- montrer que le dispositif de gestion de crise permet de **répondre aux exigences légales et attentes sociétales** notamment dans les domaines SSI et de continuité d'activité. Plusieurs secteurs font l'objet de réglementations particulières : Bâle 3 (finance) et Solvency 2 (finance et assurances), Network and Information System Security (NIS) pour les opérateurs de services essentiels (OSE) et les fournisseurs de services numériques. Par ailleurs, toute organisation doit être en conformité avec le règlement général sur la protection des données (RGPD). L'organisation d'un exercice peut également servir à démontrer à des organismes d'État ou assurantiels, voire des clients, que des entraînements sont bien conduits.

  → Le scénario de l'exercice doit donc prévoir les déclarations légales nécessaires en fonction de la situation simulée et de la législation applicable. Par exemple, en cas d'indisponibilité ou d'exfiltration de données à caractère personnel, il convient de simuler la déclaration à la Commission nationale de l'informatique et des libertés (CNIL).

- **rassurer (et/ou engager) son écosystème** sur les capacités de l'organisation à éprouver régulièrement ses mécanismes de gestion de crise et ainsi sa recherche de résilience. Par ailleurs, inclure un ou plusieurs partenaires dans un exercice peut permettre d'engager un dialogue.

  → Prendre en compte l'analyse de risques de l'organisation pour le choix du scénario de l'exercice permet de le rendre plus crédible et contribue à démontrer sa capacité à travailler sur des menaces réelles.

- **sensibiliser en interne** en utilisant l'exercice comme vecteur de messages.

  → La mise en place ou le renforcement d'une politique de sauvegarde des données de l'organisation peut être un projet difficile à défendre, mais il sera bien illustré dans le cadre d'un exercice simulant une attaque par rançongiciel. L'exercice peut également être centré sur un réseau ou une application métier critique pour démontrer la nécessité de le protéger.

Fédérer et communiquer autour de l'exercice

Organiser un exercice de gestion de crise est l'occasion de transmettre des messages à différents niveaux de l'organisation en les intégrant dans un **plan de communication**. Il peut porter sur le programme d'exercices en soulignant les ambitions de l'organisation et de la direction générale en matière de résilience et sur les exercices organisés en eux-mêmes afin de communiquer sur les enjeux et objectifs précis de chaque évènement.

En fonction du périmètre de l'exercice, le plan de communication peut s'adresser à un public plus large que les seuls participants à l'exercice, comme par exemple la direction générale. Outre les actions de communication visant à expliquer l'exercice et son organisation, le plan de communication peut aussi prévoir un volet de **promotion et de sensibilisation aux objectifs de l'exercice**.

Le plan de communication est composé des éléments suivant :

- **objectifs poursuivis**, tant en interne qu'en externe si une communication plus large est envisagée ;
- **publics visés**, tels que la liste des personnes, entités, fonctions internes et externes auxquelles il est envisagé d'envoyer des éléments au sujet de l'exercice à venir ;
- **messages à porter**, à la fois généraux sur la stratégie d'exercices, puis spécifiques selon les personnes, les entités et les fonctions ;
- **dates clés** du projet (avant, pendant et après le lancement d'un programme ou d'un exercice) ;
- **ressources utiles en cas de communication externe** (éléments de langage sur la démarche et les principaux enseignements).

Pour la rédaction de ce plan, il est fortement recommandé de **vous appuyer sur les communicants de votre organisation**.

L'un des intérêts du plan de communication est de **limiter certaines craintes**, engendrées par la thématique cyber et pouvant réduire l'intérêt et/ou l'implication des participants :

- pour les profils non techniques, la crainte de **ne pas comprendre la situation** ou de ne pas se sentir concernés ;
- pour les profils techniques, la crainte d'un **exercice insuffisamment vraisemblable** (par exemple, si le scénario proposé est trop éloigné de l'environnement de travail réel), et de ne pas être totalement compris ;
- si le scénario se base sur les résultats d'une analyse de risques, la crainte d'être **mis en cause** dans le cadre d'une vulnérabilité non corrigée (la correction posant peut-être des difficultés) ;
- pour tous, **la peur de ne pas réussir, de faire des erreurs et d'être « jugé »**. Un exercice peut parfois être considéré par les participants comme un examen ou un contrôle, sentiment qu'il convient d'éviter de laisser émerger.

Le plan de communication peut donc être utilisé pour rappeler l'état d'esprit de bienveillance dans lequel l'exercice doit se construire et se dérouler.

Il peut également être utile d'**identifier des sponsors au projet** qui agiront en tant qu'ambassadeurs pour exposer aux participants l'intérêt de participer à l'exercice et les bénéfices qu'ils peuvent en tirer.

Enfin, à l'issue de l'exercice, le plan de communication permet de **mettre en valeur l'exercice** et ses conclusions.

Au-delà des actions menées en interne, une communication externe plus large est aussi un gage de confiance envers son écosystème sur la prise en compte des risques cyber et témoigne de la volonté de se préparer jusqu'au plus haut niveau de l'organisation.

ÉTAPE 1

CONCEVOIR SON EXERCICE

Cette étape permet de cadrer l'exercice et ainsi de définir les objectifs, le type, le périmètre, les participants et la date.

LIVRABLES À PRODUIRE :

- Cahier des charges de l'exercice

FICHES PRATIQUES À CONSULTER :

- Fiche pratique n° 1 : définir les objectifs de l'exercice
- Fiche pratique n° 2 : identifier les événements et incidents pertinents pour votre exercice
- Fiche pratique n° 3 : produire un cahier des charges - exemple fil rouge RANSOM20

PHASE 1

CADRER L'EXERCICE

Le cadrage désigne la phase d'**élaboration du cahier des charges**. Ce document de cadrage du projet, réalisé par les planificateurs qui forment le groupe projet de l'exercice, comprend les éléments suivants : objectifs, périmètre, thématique, durée, participants et conditions de jeu. Pour définir ces informations, le groupe projet peut **s'appuyer sur des experts** des sujets traités dans l'exercice.

Constituer un groupe projet

Le groupe projet permet de lancer et de suivre l'élaboration de l'exercice. Il est en charge des missions suivantes[5] :

- cadrer l'exercice (voir étape 1) ;
- rédiger le scénario et le chronogramme (voir étape 2) ;
- animer l'exercice (voir étape 3) ;
- réaliser le RETEX en lien avec les observateurs (voir étape 4).

Les membres du groupe projet sont donc les planificateurs de l'exercice.

Le nombre de personnes composant ce groupe projet dépend de la taille de la structure et de l'ampleur de l'exercice. Il est généralement composé des personnes suivantes :

- **le directeur de l'exercice** (**DIREX**), en charge du pilotage de l'élaboration de l'exercice. Pour les exercices cyber, il s'agit généralement des décideurs cyber ou de la personne en charge de la SSI. Il peut également s'agir de la personne habituellement en charge des exercices de gestion de crise, de la gestion des risques ou de la continuité d'activité au sein de l'organisation. Le jour de l'exercice, il peut intégrer la cellule d'animation et prendre le rôle de directeur d'animation (DIRANIM) ;
- **plusieurs planificateurs** dont au moins un expert SSI, une personne en charge de la continuité d'activité, un communicant (éventuellement)

5 : Pour ces missions, il peut s'appuyer sur les experts, les animateurs et les observateurs dont les rôles sont définis dans la phase 2 de cette étape.

et, le cas échéant, une personne habituellement en charge de l'organisation des exercices de gestion de crise. Le jour J, les planificateurs peuvent faire partie des animateurs.

Définir les objectifs

La **formulation claire des objectifs** de l'exercice permet de **faciliter sa préparation**, son évaluation ainsi que la construction du plan d'action issu du RETEX (voir étape 4).

Pour qu'un exercice soit le plus efficace possible, il est essentiel de définir des objectifs à **tous les niveaux de jeu et par domaine** (communication, échelon décisionnel, experts SSI, etc.). Toutes les fonctions peuvent en effet décliner les principaux enjeux de l'exercice en objectifs métiers, ce qui a pour intérêt de limiter les risques de passivité des joueurs se sentant peu impliqués dans la réalisation d'objectifs très généraux.

Recommandation

Proposer aux joueurs de réfléchir et préparer leurs propres objectifs en amont de la tenue de l'exercice pour renforcer leur implication.

EXERCICE
RANSOM20

L'un des objectifs est de tester la stratégie de communication de crise en cas de cyberattaque. Les communicants joueurs peuvent décliner cet objectif général en objectifs métiers :

- tester l'organisation de la communication en situation de crise (si plusieurs communicants joueurs) ;
- tester les processus d'échange avec l'expert SSI et la direction ;
- communiquer sur un sujet nouveau.

La fiche pratique n° 1 ci-après propose des exemples d'objectifs dans le cadre du scénario RANSOM20.

FICHE PRATIQUE 1 :

DÉFINIR LES OBJECTIFS DE L'EXERCICE

La typologie ci-dessous propose une liste non-exhaustive d'objectifs. Elle présente les éléments qui peuvent être testés lors d'un exercice de gestion de crise cyber en fonction de l'orientation souhaitée. Elle est illustrée à partir du scénario fil rouge RANSOM20. Idéalement, il convient de sélectionner dans cette liste trois à quatre objectifs par exercice.

SENSIBILISER LES PARTICIPANTS AUX PROBLÉMATIQUES CYBER

Pendant l'exercice, les participants vivent de près la crise et ses effets et sont donc plus à même ensuite de mesurer les enjeux engendrés par une cyberattaque et la manière de gérer ce type de situation. Ils renforcent également leurs connaissances sur ce sujet. Il est possible de cibler la sensibilisation sur :

- **un public particulier** (comité exécutif, comité de direction, board, cellule décisionnelle/stratégique, filiale, partenaires, parties prenantes, etc.) ;
- **une problématique spécifique** (propagation d'un logiciel malveillant, exfiltration de données, campagne de hameçonnage, etc.).

FORMER OU ENTRAÎNER LE PERSONNEL

Il s'agit ici de s'assurer que les personnes en charge de la gestion de la crise se sont appropriées le dispositif, les procédures et les outils élaborés dans le cadre d'une gestion de crise cyber, ou encore qu'elles sont en mesure de faire face à des situations d'analyse ou d'arbitrage sur ces problématiques. L'exercice peut ainsi permettre de :

- **faire travailler ensemble les équipes** SSI avec le personnel habituellement en charge de la gestion de crise (pour un premier exercice) ;
- **construire ou approfondir les procédures** spécifiques aux sujets cyber ;
- **vérifier la bonne prise en compte** par les joueurs de l'ensemble des enjeux soulevés par la cyberattaque ;
- **s'entraîner à choisir** entre différents plans d'endiguement, de contournement ou de remédiation, ayant chacun des conséquences spécifiques sur les activités de l'organisation ;
- **développer le savoir-faire** de la cellule de crise et des métiers en matière de communication sur des sujets cyber (à destination des clients, collaborateurs, prestataires, filiales, autorités, médias, etc.) ;

- **tester la coordination** avec d'autres parties prenantes dans la crise (filiales, prestataires, clients, usagers, autres sites reliés à l'organisation, etc.).

TESTER LE DISPOSITIF DE GESTION DE CRISE CYBER
en vue de sa mise à jour ou de son amélioration

Dans le cas où des procédures ont été préalablement définies, il peut s'agir de tester tout ou partie du dispositif de gestion de crise cyber afin notamment de :

- **valider ou adapter certains outils et documents :** annuaire(s) de gestion de crise cyber (contacts internes et externes (prestataires de réponse à incident, assurance, autorité de tutelle, etc.), fiches de poste des participants à la gestion de crise cyber, etc.
- **tester le bon fonctionnement des chaînes d'alerte et d'escalade** (toutes les personnes utiles à la gestion de la crise ont-elles été sollicitées et si oui, l'ont-elles été au bon moment ?)
- **tester la stratégie de communication de crise** (les éléments de langage ont-ils été transmis aux bonnes personnes, en interne comme en externe) ?
- **tester les modes opératoires de secours** (autres courriels, autre réseau téléphonique, moyens de communication, etc.), ou encore les modes opératoires dégradés pour les activités critiques ;
- **tester le PCA ou le plan de reprise d'activité** (PRA).

Une approche graduelle du test du dispositif de gestion de crise cyber peut aussi être retenue, en essayant un dispositif à une cellule de crise, puis à plusieurs, et en testant ensuite différents volets du dispositif (interactions, volet métier, volet communication, etc.).

EXERCICE
RANSOM20

Objectifs retenus

- S'assurer que l'ensemble des personnes nécessaires à la gestion de la crise ont été sollicitées.
- Tester la stratégie de communication de crise sur des problématiques cyber.
- Entraîner la coordination entre le site principal de l'organisation et un de ses sites secondaires (partage de l'information, transmission de consignes, etc.).
- Entraîner les joueurs à gérer une crise de manière dégradée/tester les procédures dégradées.

Déterminer le format de l'exercice

Le choix du format d'exercice se fait en fonction :
- des objectifs définis à l'étape précédente ;
- du budget alloué ;
- des ressources disponibles pour la préparation et la participation ;
- du niveau d'expérience de la ou des organisation(s) impliquée(s).

Vous pouvez organiser des exercices sur table ou des simulations en annonçant leur tenue à l'avance ou non. Les exercices impromptus sont toutefois à réserver aux organisations ayant déjà réalisé un certain nombre d'exercices et disposant par exemple d'astreintes pouvant être sollicitées à tout moment. Ils sont à éviter lorsque l'on souhaite convier des décideurs. Pour un premier exercice de crise cyber, l'organisation d'un exercice sur table planifié est recommandée.

Deux formats d'exercice[6] sont proposés dans ce guide : sur table ou sous forme de simulation.

6 : Rappel : les exercices mentionnés dans ce guide sont uniquement de niveau décisionnel. Il en existe toutefois plusieurs formats.

EXERCICE SUR TABLE

DÉFINITION	Les participants sont réunis autour d'une même table. Un animateur leur fait part de la situation. Les joueurs réfléchissent ensemble aux actions à mener pour tenter de résoudre la crise.
NIVEAU DE JEU	Un groupe est mobilisé (ou plusieurs sous-groupes). Il peut s'agir de la cellule de crise décisionnelle seule ou accompagnée d'experts techniques de la thématique abordée ou encore d'un groupe de personnes décisionnaires à sensibiliser aux problématiques cyber.
DURÉE	2 à 3 heures (incluant briefing et débriefing)
TEMPS DE PRÉPARATION	Six semaines environ
INTÉRÊT	Idéal pour une organisation peu habituée à mettre en œuvre des exercices de gestion de crise cyber ou qui souhaite réaliser une première sensibilisation sur cette thématique. Ce type d'exercice permet de familiariser des personnes qui ont peu de temps à consacrer à un exercice (direction, comité exécutif, etc.). Il permet d'aboutir à des pistes de réflexion pour la construction ou l'amélioration du dispositif de gestion de crise cyber. Il ne permet toutefois pas de tester le dispositif de crise de votre organisation.

Si vous choisissez ce format d'exercice, les phases de l'étape 2 peuvent être suivies de manière allégée. Par exemple, il n'y a pas de cellule d'animation mais seulement un ou deux animateurs accompagnés d'un observateur ; un seul briefing joueur est à organiser le jour de l'exercice ; il n'est pas nécessaire de rédiger un chronogramme ; un seul RETEX peut avoir lieu. Pour proposer une situation évolutive aux joueurs, il est possible d'utiliser le scénario RANSOM20 et de présenter les différentes phases de celui-ci aux joueurs sur des diapositives (voir fiche n° 4).

EXERCICE SOUS FORME DE SIMULATION

DÉFINITION

Exercice nécessitant au minimum une cellule de crise, dans laquelle se trouvent les joueurs, et une cellule d'animation. Cette dernière génère une situation de crise en simulant des évènements et des interactions avec les personnes et organisations sollicitées par les joueurs mais qui ne participe pas à l'exercice.

NIVEAU DE JEU

PLUSIEURS POSSIBILITÉS :

- si une seule cellule de crise joue, l'animation doit simuler toutes les interactions que cette cellule aurait eu dans la réalité ;
- si plusieurs cellules de crise jouent, l'animation doit simuler les interactions avec ces celles-ci sans interférer sur les échanges propres aux joueurs et en déployant plus de capacités d'observation.

Exemples de configuration :

- cellule décisionnelle seule ;
- cellule décisionnelle avec une ou plusieurs autres entités (filiales, autres sites, etc.).

Plus les participants sont nombreux, plus la préparation de l'exercice nécessite du temps, des ressources et de la coordination entre les différentes entités. Pour ce type d'exercice, il faut inclure au moins un représentant de chaque entité dans le groupe projet puis dans la cellule d'animation.

DURÉE

Une demi-journée à deux journées (incluant briefing et débriefing)

TEMPS DE PRÉPARATION

Deux à six mois environ

INTÉRÊT

Immersion importante, sensibilisation accrue, permet de tester les interactions entre plusieurs cellules de crise, fait émerger des points forts et axes d'amélioration sur l'ensemble du dispositif de gestion de crise cyber.

L'exercice fil rouge RANSOM20 est développé sous ce format.

Choisir le thème

Le choix de la cyberattaque qui sera simulée au cours de l'exercice est orienté par :

- les objectifs de l'exercice définis précédemment ;
- l'analyse de la menace cyber pesant sur votre organisation ou votre secteur d'activité ;
- les scénarios issus d'une analyse de risques ;
- les RETEX des crises et des incidents passés, les précédents exercices ou encore les incidents ayant impacté d'autres organisations.

La thématique cyber n'étant pas forcément maîtrisée par les personnes en charge de l'organisation des exercices de gestion de crise, il convient de faire appel aux experts pertinents en fonction du scénario souhaité. Pour cela, le premier point de contact peut être la personne en charge de la SSI au sein de l'organisation qui peut orienter sur l'état de la menace cyber. Il est également possible de consulter des informations disponibles en sources ouvertes ou les publications de l'ANSSI[7] pour avoir un aperçu des cyberattaques récentes.

Recommandation

Il faut être vigilant au syndrome de la personne ou de l'équipe persuadée que son système n'a aucune faille. Afin d'éviter cet écueil, il peut être envisageable de créer fictivement, comme vecteur de compromission, une faille non corrigée qui vient d'être publiée ou de prévoir une attaque indirecte (via un prestataire de votre organisation par exemple).

La fiche pratique n° 2 ci-après propose des exemples de cyberattaques pouvant constituer un scénario d'exercice.

7 : Rendez-vous sur le site du CERT-FR, rubrique « menaces et incidents » : www.cert.ssi.gouv.fr/cti

FICHE PRATIQUE 2 :

IDENTIFIER LES ÉVÉNEMENTS ET POUR VOTRE EXERCICE

Plusieurs types d'événements et d'incidents peuvent être traités dans un même exercice. Le tableau ci-dessous, non-exhaustif, en présente plusieurs.

TYPE D'ATTAQUE	MOTIVATION(S), OBJECTIF(S) DE L'ATTAQUE
DÉFIGURATION DU OU DES SITE(S) WEB	Provocation, hacktivisme
DÉNI DE SERVICE	Provocation, attaque à but lucratif, hacktivisme
EXFILTRATION DE DONNÉES	Données à caractère personnel (salariés et/ou clients) avec ou sans divulgation, attaque à but lucratif, hacktivisme, espionnage, etc.
	Données critiques (brevet, données stratégiques, etc.) avec ou sans divulgation, attaque à but lucratif, hacktivisme, espionnage, etc.
CHIFFREMENT/DESTRUCTION DES DONNÉES	Attaque à but lucratif, sabotage
DESTRUCTION DES SERVICES	Sabotage via chiffrement/destruction des applications métiers. Tout ou partie des serveurs hébergeant les applications sont non fonctionnelles (messagerie, SAP, etc.).
	Sabotage via chiffrement/destruction des applications d'infrastructure. Tout ou partie des équipements supportant l'infrastructure sont détruits (*Active Directory*, poste de travail, etc.).

INCIDENTS PERTINENTS

IMPACTS POTENTIELS
Impact de réputation
Impact de réputation, indisponibilité d'un ou plusieurs outils applicatifs, déclenchement partiel ou total d'un PRA, du PCA
Impact de réputation, déclenchement du dispositif RGPD/CNIL
Impacts commerciaux, de confiance, de réputation
Sauvegardes hors ligne activables : impact opérationnel, impact de réputation, impact juridique en cas de divulgation de données confidentielles
Chiffrement/destruction des sauvegardes : impact opérationnel majeur, impact de réputation, perte des données, indisponibilité d'une ou de plusieurs applications, déclenchement partiel ou total d'un PRA, du PCA, impact juridique en cas de divulgation de données confidentielles
Indisponibilité de tout ou partie des applications
Indisponibilité de tout ou partie du SI

EXERCICE
RANSOM20

Pour entraîner les joueurs à gérer une crise de manière dégradée et tester la coordination entre deux sites, l'un des incidents retenu pour le scénario est le chiffrement des données via une attaque par rançongiciel qui se propage sur un second site de l'organisation. En conséquence, les activités sont paralysées et les outils habituels tels que les mails sont inopérants.

Pour tester la stratégie de communication sur des problématiques cyber, le chantage à l'exfiltration de données a été retenu. La publication de données exfiltrées rend visible l'attaque et nécessite de préparer des éléments de communication.

Déterminer la durée

Afin de laisser le temps aux joueurs de s'approprier le scénario et de s'adapter au rythme de l'exercice, la **durée minimale** recommandée pour un exercice de crise cyber est d'**environ trois heures**. Les exercices sur table peuvent toutefois être plus courts (une à deux heures).

La durée idéale pour une simulation est d'une journée (environ six heures), car cela permet de jouer un scénario plus complet allant du déclenchement de la crise au début de la résolution.

La plupart du temps, **le rythme des exercices de gestion de crise cyber est accéléré par rapport au rythme réel**. En effet, les contraintes d'emploi du temps des joueurs complexifient la mobilisation des participants plus d'un ou deux jours. Par exemple, dans la réalité, les investigations permettant de mieux comprendre l'origine de l'attaque nécessitent plusieurs jours voire plusieurs semaines. Il en va de même pour le retour au fonctionnement normal du SI impacté. Il convient de rappeler ces différences de temporalité en amont et à l'issue de l'exercice.

Un **exercice court** réduit le réalisme mais peut engendrer plus d'intensité. Il permet également d'impliquer des **joueurs ayant un agenda chargé** et qui peuvent difficilement consacrer une journée à un exercice.

Un **exercice long** permet d'**accentuer le réalisme**, de s'entraîner réellement à **travailler en mode dégradé** et d'ajouter plus de stimuli sans noyer les joueurs. Il peut toutefois être plus complexe à mettre en œuvre lorsque l'on joue avec une cellule de niveau décisionnel et notamment les membres de la direction. Il est alors possible de mobiliser les joueurs uniquement à certains moments clés avec un cadencement représentatif des conditions réelles.

Envisager un exercice comportant une phase de nuit afin de tester les procédures d'astreintes et le relais des équipes impliquées est possible. Il convient toutefois de garder en tête qu'un exercice organisé sur plusieurs jours est consommateur de temps et de ressources et peut engendrer un certain désengagement. Les exercices de niveau décisionnel excèdent rarement une durée de deux jours.

Nommer son exercice

Donner un nom à l'exercice (par exemple RANSOM20) permet de **faciliter les échanges entre les participants** et éviter d'alarmer les salariés non joueurs en désignant explicitement les échanges relatifs à celui-ci. Le nom ne doit cependant pas être trop explicite afin de garder un certain degré de surprise pour les joueurs quant à la thématique choisie.

Prévoir les moyens logistiques

L'aspect logistique est essentiel. Il dépend des installations déjà en place dans l'organisation et des procédures de gestion des incidents et de gestion de crise existantes.

Pour assurer un bon déroulement de l'exercice, les éléments suivants sont nécessaires :

- des **outils** permettant aux participants d'échanger entre eux (ordinateurs, téléphone, applications internes à l'organisation, groupes de discussion, etc.). Ce matériel doit être testé suffisamment en amont ;
- si l'exercice se fait en présentiel, **une salle par cellule de crise** disposant de moyens de communication ;
- une **salle d'animation** disposant également de moyens de communication et suffisamment grande pour que les animateurs ne se dérangent pas entre eux lorsqu'ils sont au téléphone. Il est à noter que la salle d'animation peut se trouver dans un lieu différent des salles dédiées aux cellules de crise ;
- un **service de restauration** pour les participants si l'exercice dure une journée ou plus ;
- des **affichages** matérialisant l'indisponibilité du matériel informatique, si cela correspond au scénario choisi.

Cet état des lieux de la préparation permet **de se rendre compte du niveau de préparation de votre organisation face à une cyberattaque**,

par rançongiciel notamment. Des outils complémentaires (moyens de communication de secours) ou des procédures de fonctionnement dégradé peuvent ainsi être mis en place en amont de l'exercice.

Déterminer le calendrier

La définition du calendrier s'effectue en parallèle du cadrage de l'exercice et doit tenir compte du calendrier civil (jours fériés, vacances), et, le cas échéant, des contraintes induites par la participation d'organisations situées à l'étranger (vacances et jours fériés locaux, décalage horaire).

Un calendrier comprend généralement les étapes suivantes :

- une **réunion de lancement**, afin de présenter le projet aux planificateurs et aux sponsors, de déterminer les grands objectifs et de définir le calendrier ;
- une **réunion initiale de planification** regroupant uniquement les planificateurs et permettant de répartir les rôles et les missions de chacun pour la conception de l'exercice ;
- la phase d'**interview des experts** ;
- la phase de **rédaction du chronogramme** ;
- des **points d'étape** pour coordonner l'équipe projet et s'assurer de la cohérence de ses développements ;
- une **réunion finale de planification** permettant de s'accorder et de clôturer la rédaction du scénario et du chronogramme ;
- **un à deux briefings des joueurs** pour présenter le projet, les objectifs et les modalités de jeu. Le premier se déroulera quelques semaines avant l'exercice. Le second, indispensable, a lieu le jour J ;
- **deux briefings dédiés aux animateurs et aux observateurs**, en amont de l'exercice et le jour J, pour s'assurer de la bonne connaissance du scénario, des rôles et des objectifs ;
- **une date pour l'exercice**, à communiquer le plus tôt possible aux participants (quelques mois en amont) afin de s'assurer à l'avance de leur disponibilité pendant toute la durée de l'exercice ;

- **une seconde date en cas de report** de l'exercice, par exemple dans le cas où un incident se produirait ;
- une réunion de **RETEX à chaud** (idéalement directement après l'exercice) pour recueillir les avis des participants ;
- une réunion de **RETEX à froid** (idéalement deux semaines à un mois après la tenue de l'exercice) pour compléter le RETEX et présenter les premières conclusions.

Entre la réunion de lancement du projet et la date de l'exercice, la préparation peut s'étendre sur deux à six mois. Le temps de préparation dépend de la complexité de l'exercice.

Recommandation

Dans la mesure du possible, les reports de date sont à éviter car ils peuvent engendrer un risque de démobilisation des participants.

PHASE 2

IDENTIFIER LES PARTIES PRENANTES ET LES JOUEURS

Un exercice peut aussi bien associer un nombre restreint de personnes que l'ensemble de votre organisation.

Il est important d'identifier les parties prenantes dès le début du projet, c'est-à-dire les personnes qui vont participer à la préparation de l'exercice (planificateurs, experts) et à son déroulement (animateurs, joueurs, observateurs).

Le nombre de parties prenantes et de joueurs conditionne le temps de préparation nécessaire ainsi que l'organisation d'éventuelles formations et sessions d'information.

Le groupe projet ayant été présenté lors de l'étape 1, son rôle n'est pas détaillé ici.

EXPERTS

DÉFINITION

En appui du groupe projet, les experts contribuent à la construction et au réalisme du scénario en apportant des éléments sur le thème retenu. Il peut également s'agir de personnes qui, au-delà de leur domaine d'expertise, connaissent l'historique de l'organisation tant sur sa manière de fonctionner que sur les exercices, incidents et crises passés.

PROFIL SOUHAITABLE / PÉRIMÈTRE

Dans le cadre d'un exercice cyber, les experts sur lesquels il est possible de s'appuyer sont les suivants :

- **experts « métier » :** une à trois personnes qui font partie (idéalement) ou connaissent les métiers impactés par l'arrêt du fonctionnement des postes bureautiques et d'un service ou d'une chaîne de production ;
- **experts « technique/SSI » :** une personne maîtrisant le parc informatique dans son architecture et ses éléments majeurs de sécurité, et, si possible, une ou deux personnes en charge des activités SSI telles que la détection d'incident de sécurité, la sécurité des réseaux ou encore la réponse à incident.

ÉTAPES(S) LES CONCERNANT

ÉTAPE 1 ✓

ÉTAPE 2 ✓

AUTRE(S) RÔLE(S) ADDITIONNEL(S) POSSIBLE(S)

- Animateurs ou observateurs (recommandé)
- Joueurs s'ils ne connaissent pas le scénario

ANIMATEURS

DÉFINITION

Le jour de l'exercice, les planificateurs peuvent devenir animateurs et ont pour mission de mettre en action le chronogramme afin de proposer une situation de crise cyber aux joueurs et ainsi répondre aux objectifs préalablement fixés. Certains animateurs peuvent ne pas avoir participé à la planification de l'exercice. Il est néanmoins impératif qu'ils aient une bonne connaissance (et compréhension) du scénario, du chronogramme et des objectifs.

Les animateurs déroulent le scénario en envoyant les stimuli qui peuvent être sous forme de courriels, d'appels ou d'échanges physiques. Ils répondent aux questions et s'adaptent aux réactions des joueurs. Un document type FAQ peut être prévu pour les aider dans cette tâche.

Pour entraîner une cellule de crise dans les conditions les plus proches de la réalité, il est indispensable d'avoir des animateurs aptes à répondre aux questions et familiers des problématiques auxquelles les joueurs seront confrontés.

PROFIL SOUHAITABLE / PÉRIMÈTRE

Pour un exercice de crise cyber, il faut au minimum :

- un animateur principal en charge de coordonner la cellule d'animation et d'adapter si besoin le scénario aux réactions des joueurs. Il peut s'agir du DIREX, qui pilotait la planification de l'exercice et qui devient alors DIRANIM ;
- un secrétaire en charge du suivi du chronogramme pour garantir une bonne cohérence de l'exercice (une main courante peut être utilisée en cellule d'animation) ;
- en fonction du nombre d'acteurs simulés, un à quatre animateurs pour répondre aux appels et aux mails des joueurs. Pour plus d'efficacité, les animateurs peuvent se répartir les rôles en fonction de leur expertise.

Ensemble, ils forment la cellule d'animation.

ÉTAPES(S) LES CONCERNANT

ÉTAPE 3 ✓

ÉTAPE 4 ✓

AUTRE(S) RÔLE(S) ADDITIONNEL(S) POSSIBLE(S)

- Ils sont souvent membres du groupe projet.

OBSERVATEURS

DÉFINITION

Le rôle d'un observateur est, comme son nom l'indique, **d'observer le fonctionnement du dispositif de gestion de crise**. Pour ce faire, il doit s'appuyer sur les objectifs de l'exercice, les réactions attendues précisées dans le chronogramme et celles effectives des joueurs.

Contrairement aux animateurs, les observateurs n'interviennent pas dans le déroulement de l'exercice. Ils apportent un **regard extérieur permettant de relever les points positifs et les axes d'amélioration**. Ils ont également un **rôle d'alerte** auprès de la cellule d'animation en cas de blocage de l'exercice, notamment lorsque la cellule d'animation est éloignée physiquement de la cellule de crise des joueurs.

PROFIL SOUHAITABLE / PÉRIMÈTRE

Pour mener une observation active, il est fortement recommandé que les observateurs disposent de connaissances sur la gestion de crise et/ou en cybersécurité et sur le fonctionnement général de l'organisation. Il peut également s'agir de personnes ayant participé à la construction du scénario ou des stimuli. Les membres du groupe projet ou les experts qui ne sont pas animateurs peuvent être observateurs.

En fonction du périmètre de l'exercice, les observateurs se répartissent sur différents sites ou entre différentes cellules de crise. Il est également possible de leur assigner l'observation de joueurs en particulier (chef de la cellule de crise, responsable communication, etc.). Afin de ne pas perturber les réflexions des joueurs, il est toutefois recommandé de limiter le nombre d'observateurs (pas plus de deux par salle).

Les observateurs peuvent disposer de grilles d'observation identifiant les axes clés nécessaires aux RETEX à chaud et à froid. Des éléments d'observation sont proposés dans la fiche pratique n° 8.

ÉTAPES(S) LES CONCERNANT

ÉTAPE 3 ✓

ÉTAPE 4 ✓

AUTRE(S) RÔLE(S) ADDITIONNEL(S) POSSIBLE(S)

- Experts

JOUEURS

DÉFINITION

Les joueurs sont les personnes qui vont **faire face à la situation de crise fictive** proposée par les animateurs. Ils n'ont pas connaissance du scénario et jouent de préférence à partir de leur lieu de travail, en utilisant des moyens de communication et procédures opérationnelles habituels. L'objectif est de les immerger de la manière la plus vraisemblable possible, même si l'ensemble des événements et des incidents sont simulés.

PROFIL SOUHAITABLE / PÉRIMÈTRE

Le profil des joueurs dépend du type d'exercice, de ses objectifs et de sa thématique. Pour un exercice cyber de niveau décisionnel, il convient d'impliquer des profils de haut niveau, mais aussi un décideur cyber ou une personne en charge de la SSI ; et plus généralement d'impliquer l'ensemble des personnes qui seraient mobilisées si l'événement joué pendant l'exercice se déroulait dans la réalité.

Le jour de l'exercice, ces joueurs doivent être en mesure de :

- **évaluer :** fournir une évaluation des impacts de la situation et des risques résiduels dont découleraient en partie les prises de décisions ;
- **planifier :** donner notamment de la visibilité aux décisionnaires (qu'ils soient joueurs ou simulés) sur des délais de mise en œuvre des actions envisagées et les contraintes réglementaires ;
- **anticiper :** proposer différentes évolutions de la crise, notamment en fonction des décisions de remédiation retenues, et des arbitrages nécessaires entre les enjeux de continuité (remédier et restaurer au plus vite certains SI) et les enjeux de sécurité (isoler et interrompre certains SI) ;
- **vulgariser :** en quelques mots, faire comprendre à tous les employés, particulièrement ceux ne présentant pas de compétences techniques, les notions de sécurité informatique et les enjeux.

ÉTAPES(S) LES CONCERNANT

ÉTAPE 3

Recommandation

Lorsqu'un acteur n'a jamais participé à un exercice et semble particulièrement réfractaire, une solution consiste à le faire d'abord participer comme observateur. Cela permet de dédramatiser les enjeux de l'exercice et de démontrer qu'il est possible de faire des erreurs. Par ailleurs, il convient d'éviter d'avoir comme observateurs les supérieurs hiérarchiques directs des joueurs. Cela peut contribuer à faire percevoir, à tort, l'exercice comme un contrôle ou une évaluation.

Afin de ne pas fausser les réactions lors de l'exercice, il convient d'éviter que les concepteurs du scénario soient également joueurs. Il est toutefois possible que certains experts interrogés pour la construction de scénario soient joueurs, s'ils ne connaissent pas l'ensemble du scénario.

Une fois tous ces éléments déterminés, on obtient un cahier des charges constituant le point de départ sur lequel se baser pour les étapes suivantes (voir fiche pratique n° 3 ci-après).

Le scénario reste à définir dans les détails. C'est l'objectif de l'étape suivante.

FICHE PRATIQUE 3 :

PRODUIRE UN CAHIER DES CHARGES

EXEMPLE FIL ROUGE RANSOM20

TYPE D'EXERCICE	☑ Partiel ☐ Général	☐ Sur table ☑ Simulation	☑ Prévu ☐ Inopiné
ADRESSE DES SITES DE L'EXERCICE	[adresse de l'organisation] [adresse du second site]		
DATE PROGRAMMÉE	JJ/MM/AAAA		
PLAGE HORAIRE	☑ Jour ☐ Nuit	☑ Matin ☑ Après-midi	DEBEX 9 h 30 FINEX 17 h 00
NIVEAU DES JOUEURS	Cellule de crise décisionnelle du siège + cellule de crise du second site		
NOM DU DIREX	Directeur cyber ou sûreté		
NOM DU DIRANIM	RSSI		
OBJECTIFS	▸ S'assurer que l'ensemble des personnes nécessaires à la gestion de la crise ont été sollicitées. ▸ Tester la stratégie de communication de crise sur des problématiques cyber. ▸ Entraîner la coordination entre le site principal de l'organisation et l'un de ses sites secondaires (partage de l'information, transmission de consignes, etc.). ▸ Entraîner les joueurs à gérer une crise de manière dégradée/tester les procédures dégradées.		
THÈMES	Attaque par rançongiciel du siège de l'organisation et propagation sur second site + exfiltration de données et menace de divulgation publique assortie d'une demande de rançon.		

<table>
<tr><th colspan="4">PARTICIPANTS</th></tr>
<tr><td>JOUEURS</td><td colspan="3">[à compléter avec les noms des joueurs]
Sur chacun des sites : profils décisionnels, personnes mobilisées si l'événement joué pendant l'exercice se passait dans la réalité (impacts métiers, experts SSI, communicants).</td></tr>
<tr><td>PLANIFICATEURS/ ANIMATEURS</td><td colspan="3">[à compléter avec les noms des planificateurs]
RSSI ou membre de son équipe, experts « métier » (une à trois personnes qui connaissent les métiers impactés par l'arrêt du fonctionnement des postes bureautiques et de tel service ou chaîne de production) et « technique/SSI » (une personne maîtrisant le parc informatique dans son architecture et ses éléments majeurs de sécurité, et, si possible, une ou deux personnes en charge des activités SSI telles que la détection d'incident de sécurité, la sécurité des réseaux ou encore la réponse à incident).</td></tr>
<tr><td>OBSERVATEURS</td><td colspan="3">[à compléter avec les noms des observateurs]
Minimum un par cellule : un des membres du groupe projet qui n'est ni joueur ni planificateur ou animateur et un ou deux experts.</td></tr>
<tr><td rowspan="3">RÔLES À SIMULER PAR LA CELLULE D'ANIMATION</td><td colspan="3">Type d'acteurs</td></tr>
<tr><td>Interne</td><td>Public</td><td>Privé</td></tr>
<tr><td>Équipe technique de l'organisation et tout acteur utile à l'exercice mais ne pouvant pas y participer.</td><td>Ministère ou autorité de tutelle, préfecture, cybermalveillance.gouv.fr, ANSSI (si applicable).</td><td>Filiales, fournisseurs, prestataires, assureurs, clients, etc.</td></tr>
<tr><td></td><td>Autre</td><td colspan="2">Tout organisme auprès duquel il est possible d'obtenir de l'aide ou nécessaire de déclarer l'incident.</td></tr>
<tr><td>CINÉTIQUE</td><td>☑ Rapide</td><td>☐ Lente</td><td>☑ Temps compressé</td></tr>
<tr><td>COMMUNICATION SUR L'EXERCICE</td><td colspan="2">☑ Oui
Conclusions du RETEX en interne à l'issue de l'exercice</td><td>☐ Non</td></tr>
</table>

FICHE PRATIQUE 3 : PRODUIRE UN CAHIER DES CHARGES
EXEMPLE FIL ROUGE RANSOM20

	Grandes lignes et découpage dans le temps
SCÉNARIO	**Phase 0 :** avant le début de l'exercice (contexte et dossier de mise en situation).
	Phase 1 : début de l'exercice (DEBEX), plusieurs agents de l'organisation signalent l'apparition d'un message de rançon sur leur ordinateur.
	Phase 2 : le logiciel malveillant s'est déployé sur l'ensemble du parc bureautique et affecte également un second site de l'organisation.
	Phase 3 : les attaquants ont publié des données exfiltrées de l'organisation et du second site. Ils demandent le paiement d'une rançon pour ne pas que d'autres documents soient publiés. En parallèle les médias sollicitent l'organisation.
	Phase 4 : des informations sur le rançongiciel et la source de l'attaque ont été obtenues après analyse et des pistes déterminées pour une reprise (non immédiate) des activités. **Fin de l'exercice (FINEX) et début du RETEX.**
CONVENTIONS D'EXERCICE	La phase d'investigation est entièrement simulée. Les éléments techniques seront transmis à la cellule de crise par un membre de la cellule d'animation qui jouera le rôle d'un membre de l'équipe technique/SSI. La phase de retour à la normale n'est pas jouée dans cet exercice.
LOGISTIQUE	Le rançongiciel affectant l'ensemble du parc bureautique, les ordinateurs et certains outils habituels des agents (y compris ceux en cellule de crise) ne sont plus utilisables. Il convient de penser à matérialiser cette conséquence en affichant sur les écrans de la salle de crise une fausse demande de rançon par exemple et d'empêcher les joueurs d'utiliser les outils concernés.
RETEX À CHAUD	JJ/MM/AAAA – 17 h 00
RETEX À FROID	J+15/MM/AAAA – 10 h 00

ÉTAPE 2

PRÉPARER SON EXERCICE

La préparation d'un exercice importe autant que son déroulement. Il convient de définir un scénario crédible, de rédiger un chronogramme ayant le bon niveau de vraisemblance et d'intensité, c'est-à-dire qu'il ne génère ni l'ennui ni un sentiment de saturation et de préparer des stimuli adaptés aux joueurs.

À l'issue de cette étape, vous disposez d'un scénario et d'un chronogramme aboutis. Vous avez également rédigé l'ensemble des stimuli qui sont prêts à être envoyés.

Les animateurs et les observateurs sont briefés, il ne reste plus qu'à démarrer l'exercice.

LIVRABLES À PRODUIRE :

- Scénario
- Briefings animateurs et observateurs
- Chronogramme
- Fiche d'observation
- Annuaire
- Briefings joueurs
- Dossier de mise en situation

FICHES PRATIQUES À CONSULTER :

- Fiche pratique n° 4 : rédiger le scénario
- Fiche pratique n° 5 : simuler la pression médiatique, rôles à incarner et questions à se poser
- Fiche pratique n° 6 : rédiger le chronogramme
- Fiche pratique n° 7 : produire un dossier de mise en situation
- Fiche pratique n° 8 : observer un exercice

PHASE 1

DÉFINIR LE SCÉNARIO

Le scénario est élaboré à partir du cadrage général de l'exercice (voir étape 1). Il décrit l'ensemble de la situation de crise et ses rebondissements, allant parfois jusqu'à sa résolution (seulement pour les exercices longs).

Ce document pourra évoluer au fil de la création de l'exercice. Il doit être constamment maintenu à jour, en parallèle du chronogramme.

Le scénario doit prévoir un **évènement conduisant à activer une cellule de crise** autour d'une problématique cyber. Une crise cyber débute par un incident de SSI la plupart du temps. C'est l'ampleur et l'impact ou l'incertitude de la gravité de cet incident sur l'organisation qui fait basculer la situation en crise. Pour déterminer cet événement, il faut **interroger votre expert SSI** sur ce qui pourrait avoir un impact significatif ou majeur sur votre organisation (mise en péril de l'activité de plusieurs services, atteinte majeure à l'image de l'organisation, etc.). Le responsable de la continuité d'activité et/ou le risk manager peuvent également vous transmettre des informations sur les risques identifiés dans ce domaine[8].

Qu'il soit imaginé ou basé sur des faits réels, un scénario doit avant tout être vraisemblable et **refléter l'état de la menace cyber** pouvant peser sur votre organisation au moment de l'exercice.

La **partie « technique »** de l'exercice, simulée dans le cadre d'un exercice décisionnel, consiste à faire découvrir progressivement aux joueurs **le déroulement de l'attaque et l'évolution de ses impacts** (par exemple en communiquant aux joueurs les résultats d'analyses techniques). Les informations permettant de simuler la partie technique sont obtenues au préalable en interviewant des experts.

Le scénario RANSOM20, décrit dans la fiche pratique n° 4, porte principalement sur les **phases de réaction immédiate et d'investigation**. Il se conclut avec la transmission d'éléments permettant d'aborder la

8 : Idéalement, le scénario est basé sur une analyse des risques réalisée en amont, notamment avec l'aide de la méthode *EBIOS Risk Manager* (ANSSI, 2018) - www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager

phase de remédiation, non approfondie dans le temps de jeu imparti. Un scénario d'exercice de gestion de crise cyber peut néanmoins porter sur cette dernière, en préparation du retour à la normale.

Il est également possible de jouer la **montée en puissance du dispositif de crise**, avec la convocation par le directeur de crise des différents participants. Cela peut permettre de tester la capacité de l'organisation à identifier les bons participants pour ce type de crise, en ayant préalablement identifié et prévenu l'ensemble des joueurs potentiels.

Le schéma ci-dessous illustre les différentes phases d'une crise cyber qui peuvent être jouées dans le cadre d'un exercice :

	RÉACTION IMMÉDIATE	INVESTIGATION	REMÉDIATION
STRATÉGIE DE RÉSOLUTION CYBER	Activer les procédures de gestion de crise et mettre en œuvre les mesures conservatoires	Qualifier l'étendue des attaques et caractériser les modes d'action	Protéger les SI en fonction des caractéristiques des attaques, reprendre le contrôle des SI compromis, les remettre en mode de fonctionnement normal et organiser la sortie de crise
STRATÉGIE DE CONTINUITÉ D'ACTIVITÉ	Évaluer et limiter les impacts des dysfontionnements (mise en œuvre des solutions de continuité d'activité)		Permettre une reprise progressive des activités (mise en œuvre des solutions de reprise d'activité) jusqu'au retour à la normale

Recommandation

Pour un premier exercice, il n'est pas opportun de proposer une sortie de crise immédiatement à la fin du scénario car cela peut donner l'impression qu'une crise cyber se résout rapidement. Par ailleurs, cela ne permet pas de réfléchir aux conséquences sur le moyen/long terme.

Dans tous les cas, indépendamment de la phase qui est jouée, un scénario comprend les éléments suivants :

- **une attaque informatique** dont les conséquences marquent le déclenchement de l'exercice (par exemple, des écrans affichant un message de rançon) ;
- **des conséquences** et des impacts métiers sur les activités de l'organisation, susceptibles d'évoluer au fil de l'exercice (accroissement du périmètre impacté) ;
- **des détails techniques sur l'attaque** qui peuvent être plus ou moins affinés selon le profil des joueurs (publication d'éditeur sur une vulnérabilité, informations sur les outils utilisés par l'attaquant, éléments sur le SI impacté, etc.) ;
- **des éléments relatifs à l'écosystème de l'organisation, socio-politiques et de pression médiatique** (réactions de partenaires, clients, autorité de régulation, de la presse, du grand public, etc.) ;
- **la résolution technique de la situation**, dont la rédaction est recommandée lorsque l'exercice dure au minimum une journée (diffusion d'un correctif pour une vulnérabilité « *0-day* » exploitée alors qu'elle n'était pas encore corrigée, restauration des systèmes impactés en présence de sauvegardes saines ou la reconstruction de ces derniers le cas échéant). Cela permet d'éviter une certaine frustration de la part des joueurs qui souhaiteront continuer à jouer tant que la situation n'est pas résolue. Pour les exercices plus courts, la conclusion de l'exercice ou le débriefing peut permettre d'aborder la stratégie de résolution technique.

Recommandation

Pour consulter des exemples réels, rendez-vous sur le site du CERT-FR[9] qui recense les vulnérabilités les plus récentes et les plus graves. Vous pouvez également consulter le mémo sur les rançongiciels[10] pour en choisir un ou simuler un code malveillant fictif.

9 : Site du CERT-FR : www.cert.ssi.gouv.fr
10 : État de la menace rançongiciel à l'encontre des entreprises et institutions : www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001

Pour préserver la dimension **pédagogique** et encourager les joueurs à participer à d'autres exercices, il convient d'**éviter un scénario trop catastrophique**. Un tel scénario présenterait en effet le risque de provoquer un sentiment de saturation des joueurs exposés à un stress excessif lié à l'injection d'événements trop nombreux et graves, ce qui peut mener à un **désengagement des participants**, surtout s'il s'agit d'un premier exercice de ce type. Une solution peut être de **limiter le périmètre de l'attaque** à une partie spécifique du SI (uniquement le SI bureautique, application métier critique, etc.).

Un fort **manque de réalisme** peut également engendrer des blocages : difficulté à se projeter, absence de prise de décision, remise en cause du scénario, etc. Là encore, cette carence peut mener à un **désengagement des participants**.

Interviewer les experts

Interroger les experts permet d'obtenir les éléments nécessaires à la rédaction d'un scénario et d'un chronogramme vraisemblables.

Cela permet également de **connaître les risques** cyber auxquels est exposée l'organisation, déterminer quels vont être le ou les **événement(s) déclencheur(s)** de la crise et identifier les diverses conséquences engendrées par cet événement. En effet, les interviews d'experts donnent des **éléments techniques sur les SI** impactés et permettent de **mieux comprendre les procédures** et le fonctionnement de l'organisation en cas de cyberattaque.

- Dans le cas d'un scénario concernant l'exploitation d'une vulnérabilité, il est indispensable de vérifier la vraisemblance de cette vulnérabilité au regard des SI de l'organisation.

Pour établir la trame du scénario et les éléments permettant de rédiger le chronogramme, il convient d'organiser au minimum **une réunion collégiale avec l'ensemble des experts**. Des réunions bilatérales, avec un ou deux experts, portant sur des aspects précis du scénario ou sur la rédaction de certains stimuli peuvent ensuite être envisagées.

Afin d'avoir une vision claire de l'enchaînement des incidents et de structurer les idées et les avis recueillis, une première version du scénario doit être **rédigée rapidement après les entretiens avec les experts**. Cela permet d'éviter que le scénario ne dérive vers un périmètre trop large ou éloigné du cadre préalablement défini. Ce format, plus littéraire et plus concis que le chronogramme, peut être **envoyé** à toute personne ayant besoin de prendre connaissance rapidement du scénario (à l'exception des joueurs) ou de le valider. Il peut également être **utilisé lors du RETEX** à chaud et à froid.

FICHE PRATIQUE 4 :

RÉDIGER LE SCÉNARIO

EXEMPLE FIL ROUGE RANSOM20

Le scénario proposé repose sur quatre événements majeurs : une attaque touchant le réseau bureautique ; sa propagation sur au moins un autre site ; la médiatisation de l'attaque ; la publication par un groupe d'attaquants d'une partie des données exfiltrées afin de faire pression en vue du paiement de la rançon[11].

PROPOSITION D'ORGANISATION DE L'EXERCICE SELON LA DURÉE RETENUE :

	BRIEFING JOUEUR	EXERCICE	RETEX À CHAUD	COMMENTAIRES
UNE DEMI-JOURNÉE	9h00 à 9h30	9h30 à 12h30	12h30 à 13h30	Commencer l'exercice avec l'annonce directe de l'attaque et de ses conséquences : l'ensemble du parc informatique est touché par une cyberattaque, il est impossible d'utiliser les ordinateurs de l'organisation. Puis, une heure plus tard, simuler un appel d'un second site également touché par l'attaque. L'équipe se concentrera sur la compréhension de la situation et la continuité d'activité. Il est également possible d'annoncer des sollicitations de la presse et sur les réseaux sociaux pour entraîner les services de communication[12].
UNE JOURNÉE	9h00 à 9h30	9h30 à 17h00	17h00 à 18h00	Suivre l'exercice comme présenté ci-après.
UNE JOURNÉE ET DEMIE	9h00 à 9h30	9h30 à 17h00 (J1) 9h30 à 14h00 (J2)	14h00 à 15h00	Possibilité de ralentir le rythme de l'exercice pour ajouter du réalisme et entraîner les joueurs à mettre à profit des temps d'investigation pour anticiper. Il est également possible de jouer l'exfiltration de données le second jour afin de tester la communication de crise. Un point peut être réalisé avec les joueurs le matin du J2 pour les informer des évènements qui se sont fictivement déroulés la nuit (ex : résultats d'analyses techniques)

11 : L'exfiltration et l'éventuelle divulgation de données internes à l'entité victime ne sont pas caractéristiques ni systématiques d'une attaque par rançongiciel. Cette dernière peut en effet être accompagnée d'une attaque distincte, menée en parallèle au moyen d'un code malveillant différent, visant à exfiltrer des données, qui pourront potentiellement être divulguées par les attaquants.
12 : Pour plus d'informations, voir les recommandations sur le déroulé d'un exercice sur table page 29.

FICHE PRATIQUE 4 : RÉDIGER LE SCÉNARIO
EXEMPLE FIL ROUGE RANSOM20

1. INFECTION DU SI DU SITE PRINCIPAL DE L'ORGANISATION

À 9h30, les équipes techniques reçoivent un appel d'un employé de l'organisation : son poste de travail a redémarré tout seul et affiche un message statique demandant le versement d'une rançon dans les 24 heures pour récupérer les données qui ont été chiffrées et ne sont donc plus accessibles. L'employé ne peut plus utiliser son poste. Dans l'heure qui suit, plusieurs employés notifient des problèmes similaires et envoient des photos de leurs écrans affichant tous le même message de rançon.

Il semblerait que le réseau bureautique du site principal de l'organisation ait été la cible d'une attaque par rançongiciel. **À 10h15,** à la suite de l'attaque, une grande partie du réseau est touchée et rendue indisponible. Beaucoup d'employés du site principal de l'organisation ne peuvent plus travailler.

→ Il convient ici de lister l'ensemble des fonctions mise à l'arrêt en raison de l'infection : au choix du planificateur de chaque organisation en fonction de son organisation interne.

2. DÉBUT DE LA PRESSION MÉDIATIQUE

À 10h45, une photo de l'un des postes de travail infecté a été publiée sur Twitter par l'un des salariés. L'organisation est contactée par la presse concernant l'incident en cours. Elle est également sollicitée sur les réseaux sociaux.

À 11h00, le rançongiciel a infecté l'ensemble du parc informatique, postes de travail et serveurs inclus, dont les serveurs de sauvegarde connectés au réseau.

→ En fonction du niveau de difficulté souhaité pour l'exercice, l'attaque peut impacter ou non l'ensemble du SI et des moyens de communication (messagerie, téléphonie). Le déroulement de l'exercice devra refléter l'ampleur des conséquences de l'attaque : si les messageries sont indisponibles, les communications ne pourront plus être effectuées par mail et les stimuli devront être communiqués par d'autres moyens.

À 12h00, une revendication de l'attaque apparaît sur un site Internet, indiquant qu'en complément du chiffrement du SI, des données ont été exfiltrées et seront publiées si la rançon n'est pas versée dans les 24 heures.

Vers 13h00, l'ANSSI est informée de l'incident[13] et transmet dans un premier temps des documents de bonnes pratiques sur les attaques par rançongiciel[14].

OPTION « SIMULATION ANSSI », SI APPLICABLE (LE PÉRIMÈTRE DE L'ANSSI POUR SES INTERVENTIONS EST LIMITÉ AU SECTEUR PUBLIC, AUX OIV ET OSE)

Si votre organisation n'entre pas dans le périmètre de l'ANSSI, vous pouvez simuler un prestataire qui réalise les analyses et effectue des recommandations (voir fiche pratique n° 6).

La plupart des stimuli simulant l'ANSSI dans le chronogramme peuvent également être émis par un prestataire.

→ Qu'il s'agisse de l'ANSSI ou d'un prestataire, la transmission d'éléments techniques est simulée. L'ANSSI ou le prestataire, après avoir fictivement mené des analyses, transmettra des informations sur le rançongiciel et des recommandations sur les actions à réaliser pour rétablir la situation.

3. PROPAGATION DE L'ATTAQUE

OPTION « JEU AVEC UNE SEULE CELLULE DE CRISE IMPLIQUÉE »

À 13h10, le responsable d'un second site de l'organisation informe les équipes techniques que les postes de travail (ou systèmes de contrôle industriel) de leur site sont indisponibles. Les écrans des postes de travail affichent un message exigeant le versement d'une rançon.

OPTION « JEU AVEC PLUSIEURS CELLULES DE CRISE IMPLIQUÉES »

À 13h10, des salariés du second site joueur signalent à leur hiérarchie que leurs écrans affichent un message exigeant le paiement d'une rançon.

→ L'objectif est notamment de travailler la coordination et la communication entre ces deux entités.

Pour ces deux options, l'attaque s'étend progressivement à l'ensemble du second site. Les commandes ou les services ne pourront être honoré(e)s.

→ Il convient ici de lister l'ensemble les commandes ou services qui ne pourront être honorés en raison de l'infection.

13 : Déclarer un incident sur le site de l'ANSSI : www.ssi.gouv.fr/en-cas-dincident

14 : Plusieurs ressources sont disponibles : le site de l'ANSSI (www.ssi.gouv.fr/actualite/ne-soyez-plus-otage-des-rancongiciels), le guide Attaques par rançongiciels, tous concernés comment les anticiper et réagir en cas d'incident ? (ANSSI, 2020), le site de CYBERMALVEILLANCE.GOUV.FR (www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares)

4. BILAN DE L'ATTAQUE

À 15h20, les interconnexions des SI des autres sites de l'organisation avec les systèmes du site principal ont été coupées, arrêtant la propagation du code malveillant. Seul le site principal et un second site sont impactés par l'attaque.

→ Si l'organisation prend cette décision plus tôt, cela doit être pris en compte par la cellule d'animation.

5. ACCENTUATION DE LA PRESSION MÉDIATIQUE

OPTION « PUBLICATION DES DONNÉES EXFILTREÉS »

À 15h35, un salarié annonce la publication sur Internet de données de l'organisation (siège et second site). Après vérification par quelques salariés, les documents proviennent effectivement de l'organisation et du second site.

→ Il convient de déterminer avec l'équipe d'animation quels sont les documents publiés et d'en établir une liste à transmettre aux joueurs. Il n'est pas nécessaire de rassembler de vrais documents pour simuler la publication.

La presse, qui a eu écho de cette publication, contacte l'organisation pour obtenir confirmation de l'incident. En interne, plusieurs employés s'interrogent sur la publication des données personnelles.

6. PREMIERS RÉSULTATS DES ANALYSES TECHNIQUES SUR L'ORIGINE DE L'ATTAQUE

À partir de 15h45, des éléments issus de l'investigation menée par les équipes techniques (avec l'appui d'un prestataire ou de l'ANSSI s'il a été choisi de simuler l'un des deux ou les deux) sont progressivement partagés avec la cellule de crise. Les attaquants se seraient introduits dans les SI soit via l'exploitation d'une vulnérabilité affectant le protocole RDP (vulnérabilité déjà connue mais le correctif n'avait pas encore été déployé sur certains serveurs de l'organisation connectés à Internet), soit via une campagne d'hameçonnage (un employé a ouvert une pièce jointe malveillante/cliqué sur un lien malveillant exploitant une vulnérabilité affectant le système d'exploitation Windows déjà connue ou non, 0-day). Par ailleurs, le programme malveillant utilise de multiples moyens de latéralisation (exploitation de services légitimes de Microsoft Windows sur

le modèle du code NotPetya, par exemple, et de codes publiés sur Internet permettant d'exploiter des vulnérabilités connues telle qu'Eternal Blue).

Le rançongiciel utilisé par les attaquants semble être EvilRansomware, actif depuis 2019 (plus d'informations ci-après).

→ Important : 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, les investigations peuvent prendre plusieurs jours à plusieurs semaines.

7. REMÉDIATION

Vers 16h50 les équipes techniques ont établi une stratégie de remédiation. En fonction de l'état des sauvegardes, deux options sont à proposer par les équipes techniques simulées par la cellule d'animation :

→ Il convient de déterminer en amont si l'organisation dispose ou non de sauvegardes hors ligne car la gestion des conséquences sera différente.

- **A. Les sauvegardes hors-ligne sont préservées** (sur un serveur isolé et complètement déconnecté du réseau infecté) **et fonctionnelles :** il s'agit de déployer ces sauvegardes une fois l'attaque contenue (après quelques jours). Néanmoins ces données peuvent être anciennes voire obsolètes, si elles ne sont pas mises à jour fréquemment. La reprise nominale des activités pourra reprendre dans une semaine environ.

- **B. Les sauvegardes sont impactées** (perte partielle ou totale des données), il est alors nécessaire de reconstruire tout ou partie du système. Cela peut prendre du temps et signifie que les activités pourront reprendre progressivement dans quelques semaines.

La pression médiatique se poursuit au fil de la journée avec des appels et des mails de journalistes souhaitant obtenir plus d'informations sur la situation, l'origine de l'attaque et la reprise d'activité de l'organisation.

CONCLUSION DE L'EXERCICE

Un exercice ayant une durée limitée, il est difficile d'aller jusqu'à la résolution de la situation qui, dans le cas d'une crise d'origine cyber, peut prendre plusieurs

jours voire plusieurs semaines. La résolution peut néanmoins être annoncée à l'arrêt du jeu ou au moment de l'organisation du RETEX à chaud. Un membre de la cellule d'animation explique alors comment aurait évolué la situation dans la réalité et quelles auraient été les étapes et les délais pour une reprise d'activité normale.

Exemple : après avoir contenu l'attaque et expulsé l'attaquant de son SI, l'organisation a déployé les sauvegardes ou reconstruit son SI et repris partiellement ses activités après six jours d'arrêt. Une semaine plus tard l'ensemble de l'activité a repris même si certaines bases de données ne seront pas reconstruites à l'identique avant plusieurs mois ; la plainte suit son cours. Dans le cas où les sauvegardes ne sont pas exploitables, la reconstruction du parc informatique contraint l'organisation à une pérennisation des modes de travail dégradés durant au moins un mois.

POUR PLUS D'INFORMATIONS SUR LE RETEX, CONSULTER L'ÉTAPE 4.

INFORMATIONS COMPLÉMENTAIRES SUR LE RANÇONGICIEL À L'ATTENTION DES PLANIFICATEURS ET ANIMATEURS[15]

Le rançongiciel EvilRansomware est actif depuis 2019. Le très grand nombre de variantes du code EvilRansomware présentant des configurations différentes laisse penser que ce rançongiciel est partagé, probablement sous le modèle « *ransomware-as-a-service* ».

Responsable de 20 % des infections détectées en 2019, EvilRansomware est probablement proposé à bas prix. Le montant des rançons et les chances de récupérer les fichiers sont très variables en fonction des attaques. Certains attaquants ont également démontré une mauvaise maîtrise du code, empêchant les victimes de récupérer leurs fichiers malgré le paiement de la rançon.

EvilRansomware est distribué par hameçonnage comprenant un lien malveillant ou une pièce jointe piégée. Cette dernière usurpe parfois l'identité d'un antivirus. Comme beaucoup d'autres rançongiciels, il compromet également ses victimes par l'exploitation d'une vulnérabilité déjà connue affectant le protocole RDP pour laquelle un correctif est disponible mais encore peu appliqué. Cette multiplicité des méthodes d'infection est typique du modèle « *ransomware-as-a-service* ». EvilRansomware chiffre ensuite les fichiers présents sur les machines ainsi que sur les partages réseau accessibles. Il supprime également les copies cachées.

15 : Pour utiliser des informations liées à un rançongiciel existant, consultez le rapport de l'ANSSI sur l'état de la menace rançongiciel à l'encontre des entreprises et des institutions : www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001

PHASE 2

RÉDIGER LE CHRONOGRAMME

Le chronogramme prend la forme d'un tableau qui, ligne par ligne, décrit **tout le déroulement chronologique de l'exercice** du DEBEX au FINEX. Sa rédaction se base sur les interviews des experts réalisées lors de l'étape 1.

Il décrit l'ensemble des interactions qu'il est possible d'anticiper entre les joueurs et la cellule d'animation. Cette dernière doit toutefois être capable de s'adapter aux réactions des joueurs qui peuvent parfois différer de la réaction attendue (*voir étape 3, phase 2*).

La fiche pratique n° 6 propose un chronogramme pour le scénario fil rouge RANSOM20. Les éléments techniques proposés dans cette fiche sont à compléter en fonction de l'organisation interne des SI.

Définir le rythme et l'intensité de l'exercice

Le rythme d'un exercice cyber n'est pas constant. Il dépend de la fréquence d'envoi des stimuli. Rapide au départ pour favoriser l'immersion des joueurs, il ralentit ensuite pour les laisser prendre connaissance des événements et réfléchir à une manière de gérer la crise. Sur deux jours d'exercice, un rebondissement peut être envisagé afin de relancer la dynamique.

Dans une crise d'origine cyber, si les impacts sont fulgurants, la compréhension de l'attaque peut quant à elle prendre plus de temps (plusieurs jours, voire plusieurs semaines). Transcrire cela dans un exercice revient alors à trouver le compromis entre **simuler le temps de l'investigation nécessaire aux équipes techniques** et faire suffisamment avancer le scénario pour que les joueurs aient une vision d'ensemble du déroulement d'une crise. Pour cela un « temps accéléré » sera à privilégier lors de la rédaction du chronogramme.

EXERCICE
RANSOM20

En l'espace de quelques minutes, il devient impossible pour le personnel de travailler. En envoyant des stimuli avec une cadence élevée (toutes les trois minutes, par exemple), il est possible de faire transparaître l'ampleur (multiplicité des stimuli) et la gravité (les différentes entités impactées s'expriment) d'un tel événement. En revanche, pour la phase d'investigation (recherche du patient 0 ou isolement de la souche à l'origine du logiciel malveillant), la cellule de crise peut vivre des moments d'attente qu'il est possible de faire ressentir en espaçant la cadence des stimuli (10 voire 15 minutes de silence).

L'incertitude sur les objectifs et le périmètre de l'attaque est une des **caractéristiques fortes d'une crise cyber**. Il est important de la faire ressentir aux joueurs en retardant l'envoi de certains stimuli (répondant notamment à des demandes d'investigations techniques) ou en précisant dans certains stimuli qu'il y a encore des éléments inconnus. Il convient de trouver un rythme de transmission des stimuli permettant de maintenir l'intérêt des joueurs tout en démontrant qu'une crise d'origine cyber a des impacts durables et difficiles à évaluer.

Pour les organisations ayant l'habitude de réaliser des exercices de gestion de crise cyber, il est possible de proposer un scénario avec des sauts dans le temps pour permettre aux joueurs de vivre les différentes phases d'une crise cyber. En revanche, pour les organisations peu habituées aux problématiques cyber, il est préférable que la durée de **l'exercice corresponde autant que possible à celle de l'événement s'il avait lieu dans la réalité.**

Dans les deux cas, il sera alors crucial, à l'issue de l'exercice, de rappeler les délais réels que requièrent l'investigation numérique (analyse de journaux de différents équipements, analyse de code, etc.) et la mise en place de certaines mesures techniques (application d'un correctif sur l'ensemble d'un parc informatique, etc.). Par ailleurs, le premier et/ou le second briefing sont également l'occasion d'expliquer aux joueurs que la cadence de l'exercice est volontairement plus soutenue que dans la réalité.

Recommandation

Des logiciels permettant d'automatiser certaines tâches peuvent vous aider dans la mise en œuvre de cette étape, de l'étape 3 (dérouler son exercice) et de l'étape 4 (tirer les enseignements de son exercice).

Simuler les enjeux de communication et la pression médiatique

Les crises cyber n'échappent pas à la médiatisation et peuvent ainsi avoir un **impact sur l'image et la réputation** de votre organisation. Inclure un volet médiatique et/ou de communication permet d'entraîner les communicants d'une cellule de crise à gérer ce type d'événement.

L'enjeu pour les joueurs sera de rassurer et de maîtriser la communication de son entité dans un climat anxiogène (nouveauté de ce type d'attaque) et parfois sans moyens de communication (si les moyens bureautiques sont touchés par exemple).

Cette étape comprend deux volets à simuler : la pression médiatique et les enjeux de communication interne et vers les parties prenantes. Pour ceux-ci, le groupe projet doit **s'entourer de communicants** de l'organisation (ne participant pas à l'exercice) et/ou de prestataires spécialisés.

Les éléments relatifs à la communication externe et à la pression médiatique simulée sont à intégrer dans le chronogramme.

SIMULER LA PRESSION MÉDIATIQUE

Pour simuler la pression médiatique, il est nécessaire de **prévoir des mails ou des appels téléphoniques de faux journalistes** ainsi que des **articles de presse** sur l'incident (qui peuvent notamment porter sur des échanges de journalistes avec les joueurs). Il convient également

de ne pas négliger les **réseaux sociaux** pour une pression médiatique vraisemblable. De faux tweets ou des publications d'internautes, d'experts et de journalistes peuvent également être envoyés aux joueurs, tout comme des extraits de vidéos de chaînes d'information assortis de faux bandeaux. Les éléments transmis aux joueurs dans le cadre de l'exercice doivent être identifiés comme faisant partie de l'exercice afin de ne pas risquer d'être confondus avec des informations réelles. Par exemple, les appels de journalistes simulés peuvent commencer par « exercice – exercice – exercice ».

Il existe plusieurs méthodes pour réaliser une pression médiatique simulée :

- utiliser une plateforme simulant les réseaux sociaux via un prestataire ;
- rendre accessible régulièrement aux joueurs des articles de presse, tweets, etc. mentionnant l'attaque aux joueurs (pour cela, simuler par exemple une personne en charge de réaliser la veille médiatique pour l'organisation qui fait remonter régulièrement des informations). Vous pouvez vous inspirer des articles de journaux ayant été rédigés pour des cyberattaques réelles.

Les acteurs pouvant être simulés pour générer une certaine pression médiatique sont les suivants : journalistes, influenceurs, communauté de la sécurité du numérique, etc.

Dans la simulation de la pression médiatique, vous pouvez rédiger de faux articles de presse sur l'attaque qui seront envoyés aux joueurs ainsi que des faux tweets. A la suite des échanges avec les joueurs, des éléments peuvent également être rédigés en direct. Ces articles peuvent être volontairement à charge, exagérés ou reprendre exactement les propos des communicants.

LA COMMUNICATION INTERNE ET VERS LES PARTIES PRENANTES

Comme pour la pression médiatique, les éléments relatifs à la communication interne et vers les parties prenantes prennent la forme de **mails ou d'appels téléphoniques via des outils de communication usuels ou de secours.**

Pour ce volet, différents types d'acteurs peuvent être simulés : équipes internes concernées par la crise, collaborateurs, actionnaires, partenaires sociaux, clients, prestataires, concurrents, associations, autorités sectorielles, etc.

QUESTIONS LES PLUS FRÉQUEMMENT POSÉES

Qu'il s'agisse de salariés de l'organisation, de journalistes ou de parties prenantes externes, les questions les plus fréquemment posées portent notamment sur la nature de l'attaque, ses conséquences sur l'activité de l'organisation et les mesures mises en œuvre pour assurer un retour à la normale.

Les membres de la cellule d'animation qui simulent la pression médiatique et les enjeux de communication interne doivent garder en tête que la temporalité d'une crise d'origine cyber est toujours difficile à expliquer : si les impacts sont parfois immédiatement visibles, les analyses techniques prennent du temps, tout comme les mesures profondes de remédiation. Ainsi, la plupart des questions (qui, quoi, comment) risquent de rester sans réponse durant l'exercice.

Le rôle de l'expert SSI sera de vulgariser les éléments techniques pour assurer la bonne compréhension des communicants.

La fiche pratique n° 5 liste l'ensemble des acteurs pouvant être simulés ainsi que les questions qu'ils peuvent être amenés à poser.

FICHE PRATIQUE 5 :

SIMULER LA PRESSION MÉDIATIQUE, ET QUESTIONS À SE POSER

ACTEUR	DESCRIPTIF
INTERNE Équipes concernées, collaborateurs, actionnaires, partenaires sociaux	Si les impacts de la cyberattaque sont visibles, il faut s'attendre à diverses questions de la part des employés, des clients et plus généralement de l'écosystème de votre organisation.
CLIENTS potentiellement sensibles (OIV, OSE, administrations)	
ÉCOSYSTÈME Concurrents, associations, prestataires, autorités sectorielles, etc.	
JOURNALISTES dont spécialisés en sécurité du numérique et experts du secteur impacté	En cas d'attaque informatique, vous pourrez être sollicités par vos contacts médiatiques classiques (presse sectorielle, généraliste nationale et/ou régionale) mais également par la presse spécialisée en informatique, et plus particulièrement en sécurité informatique.
INFLUENCEURS ET COMMUNAUTÉ DE LA SSI ET DU SECTEUR IMPACTÉ	La communauté est composée de personnes exigeantes, actives et curieuses, qui aiment comprendre les modes opératoires des attaquants. Elles utilisent beaucoup les réseaux sociaux pour échanger sur des éléments techniques, débattre, commenter des communications officielles. Tout cela peut-être simulé dans le cadre de l'exercice.

RÔLES À INCARNER

QUESTIONS TYPES
Est-il encore possible de travailler ? Doit-on payer la rançon ? Comment faire pour cela ? Quelles sont les actions préconisées ? Les mesures mises en place ? Quelles sont les consignes ? Que faut-il faire ? Comment faire pour continuer à travailler ? Telle mission ne peut être reportée, j'ai besoin de moyens informatiques fonctionnels. Publication de capture d'écran des ordinateurs sur les réseaux sociaux, etc.
Que se passe-t-il ? Quels sont les impacts sur nos échanges habituels ? Risquons-nous d'être infectés/ciblés également ? Quand pourrons-nous reprendre nos échanges habituels ? Pouvez-vous me tenir informé de l'évolution de la situation ?
Que se passe-t-il ? Quels sont les impacts pour vous ? Pour le secteur ? Pouvez-vous nous tenir informés de l'évolution de la situation ?
JOURNALISTES NON SPÉCIALISÉS : Quelle est l'étendue de l'incident, son périmètre et ses conséquences ? Quand est-ce arrivé ? Combien de temps cela va-t-il durer ? L'attaque est-elle toujours en cours ? **JOURNALISTES SPÉCIALISÉS :** Quel type d'attaque ? Quel est le mode opératoire ? Quelles conséquences directes (techniques, financières) ? Indirectes ? Propagation ? Des clients sont-ils victimes ? Des clients sensibles ? Que faites-vous aujourd'hui pour réparer le SI ? Une plainte a-t-elle été déposée ? Une déclaration RGPD auprès de la CNIL a-t-elle été réalisée ? L'ANSSI vous accompagne-t-elle ? Des prestataires ? Quelles mesures allez-vous mettre en place à l'avenir ? Qui est l'attaquant ? Quelles sont ses motivations ?
Les questions peuvent être identiques à celles des journalistes spécialisés. Elles ne seront toutefois pas posées directement à l'organisation mais feront l'objet de débats sur différents réseaux sociaux. Cela peut servir à alimenter une veille ou une plateforme de pression médiatique simulée.

Rédiger les stimuli

Les stimuli doivent être rédigés avant l'exercice et être intégrés au chronogramme. Ils peuvent prendre la forme de mails (souvent avec des éléments en pièces jointes), de scripts s'il s'agit d'un appel téléphonique ou encore de faux extraits de journaux, de tweets ou de publications sur une plateforme de réseau social. Rien ne doit être à rédiger le jour J, à l'exception d'ajouts ou de modifications à la marge, si la situation le nécessite. Leur mode de communication doit être adapté à la situation simulée dans le cadre de l'exercice.

Par exemple, si l'attaque simulée paralyse les messageries et la téléphonie, d'autres moyens de communication devront être identifiés et mis en œuvre durant l'exercice.

Recommandation

Les appels téléphoniques transmettant des messages importants pour les joueurs peuvent être complétés d'un récapitulatif transmis via un autre moyen de communication (par exemple, envoi d'un mail reprenant les informations transmises par téléphone).

Il peut être utile de prévoir des stimuli optionnels qui seront envoyés, si nécessaire, pour aider ou au contraire perturber les joueurs. Par exemple, si le directeur de crise ne prévoit pas de point de situation, un stimulus émanant d'une autorité demandant ce qu'il se passe peut être prévu en amont.

La fiche pratique n° 7 propose un modèle de chronogramme basé sur le scénario de l'exercice fil rouge RANSOM20.

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.

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)
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

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

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.

DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
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.

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).

EXTRAITS

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)
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
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]
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
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
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
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)

DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
Tous les joueurs	Mail	Aucune action particulière attendue.	
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.
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.
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 un diagnostic et une mise en relation avec un prestataire sur la plateforme cybermalveillance.gouv.fr . 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.»
RSSI ou équivalent / DSI si pertinent	Appel téléphonique	Transmission des informations disponibles à l'ANSSI.	
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.

EXTRAITS

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)
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
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)
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
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

DESTINATAIRE (= les joueurs pour action)	MODALITÉ DE TRANSMISSION	RÉACTIONS ATTENDUES	COMMENTAIRES À L'ATTENTION DU PLANIFICATEUR
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.	
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.
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.
Tous les joueurs	Mail	Participation au RETEX.	Bravo vous avez organisé un exercice de gestion de crise cyber !

Pour vous accompagner dans la rédaction de votre chronogramme, téléchargez le fichier excel complet de notre exemple sur :

www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber

PHASE 3

PRÉPARER LES AUTRES DOCUMENTS

DOCUMENT	DESCRIPTIF
ANIMATEURS	
ANNUAIRE	Détailler les coordonnées à jour de l'ensemble des
MAIN COURANTE	Consigner par écrit les évènements notables de l'exercice en vue de préparer le RETEX (voir phase
JOUEURS	
ANNUAIRE	Reprendre l'ensemble des coordonnées des animateurs et joueurs participant à l'exercice et expliciter clairement les fonctions simulées par l'équipe d'animation (un même numéro pouvant permettre de joindre plusieurs personnes simulées). Ces informations doivent correspondre aux moyens de communication qui seraient utilisés dans le cadre d'une crise réelle. La production et le maintien à
DOSSIER DE MISE EN SITUATION (DMS) ***[FACULTATIF]***	Présenter l'état du monde au début de l'exercice. Le DMS peut notamment être considéré comme le premier élément de sensibilisation des joueurs sur l'état de la menace cyber qui pèse sur l'organisation. Il peut être complété par des articles de presse
CONVENTIONS D'EXERCICE	Présenter les règles de jeu, comme par exemple l'usage de la mention « exercice exercice exercice » par mail et par téléphone pour éviter les confusions entre des évènements simulés faisant partie de l'exercice et des évènements réels se déroulant
DOCUMENTATION UTILE	Ajouter les documents et procédures à tester dans
OBSERVATEURS	
FICHE D'OBSERVATION	Rappeler les objectifs et détailler les points sur lesquels
ACCÈS À LA MAIN COURANTE DES ANIMATEURS ***[FACULTATIF]***	Suivre la crise dans son ensemble (notamment

Pour assurer un bon déroulé de l'exercice, différents documents doivent être produits pour les participants.

	COMMENTAIRES
participants (joueurs, animateurs, observateurs).	
2 de l'étape 4).	
jour de cet annuaire sont importants afin d'éviter que les joueurs ne contactent des personnes ne participant pas à l'exercice. Il convient également de prévoir dans l'annuaire un numéro vers la cellule d'animation permettant d'appeler « toute personne ne participant pas à l'exercice en tant que joueur et non mentionnée dans l'annuaire » afin de se parer contre tout oubli.	Ces documents peuvent être transmis par mail en amont de l'exercice et/ou lors du ou des briefing(s) joueurs.
récents permettant d'illustrer les propos par des exemples réels. La fiche pratique n° 7 propose un exemple de DMS correspondant au scénario proposé dans la fiche n° 4.	
pendant l'exercice, ou encore l'interdiction d'utiliser tel moyen de communication si celui-ci devient indisponible en conséquence de la cyberattaque.	
le cadre de l'exercice.	
les observateurs devront porter leur attention.	La fiche n° 8 propose une liste des éléments à observer dans le cadre d'un exercice de gestion de crise cyber.
en cas de jeu sur plusieurs sites).	

FICHE PRATIQUE 7 :

PRODUIRE UN DOSSIER DE MISE EN SITUATION

EXEMPLE FIL ROUGE RANSOM20

Cette fiche pratique constitue un dossier de mise en situation tel qu'il pourrait être transmis aux joueurs , en amont de l'exercice RANSOM20. Il contient des éléments généraux sur l'état de la menace cyber et des informations liées à l'organisation.

1. CONTEXTE GÉNÉRAL : ÉTAT DE LA MENACE CYBER

Aujourd'hui, les organisations peuvent être la cible de cyberattaques aux finalités variées :

- **les opérations d'espionnage informatique** pouvant prendre la forme d'exfiltrations d'informations stratégiques, de secrets de fabrication, d'éléments de R&D dans des secteurs variés ;
- **les attaques à des fins de revendication** pouvant prendre la forme de défigurations, de divulgations de données (via une exfiltration), de déni de service, visant à mobiliser les leaders d'opinion et porter atteinte à l'image ou à la réputation de personnes ou d'organisations ;
- **les attaques à des fins de sabotage** pouvant prendre la forme d'une destruction logique ou physique de matériels ;
- **les attaques à but lucratif** pouvant prendre la forme de rançongiciels, d'exfiltrations de données à des fins de revente ou de chantage.

Différents modes opératoires peuvent être mis en œuvre au cours d'attaques informatiques afin de compromettre les SI des entités ciblées et d'y atteindre l'objectif recherché :

- **Exploitation de vulnérabilités[16]:** il s'agit d'utiliser un code exploitant une vulnérabilité, corrigée ou non, affectant un produit logiciel ou matériel, comme vecteur d'intrusion dans le SI d'une organisation. L'exploitation d'une vulnérabilité peut être automatisée et permettre la diffusion rapide et à grande échelle d'un code malveillant. Par exemple, en mai 2017, le code malveillant Wannacry s'est rapidement propagé dans le monde entier via

16 : Retrouvez les vulnérabilités les plus critiques sur le site du CERT-FR : www.cert.ssi.gouv.fr

l'exploitation automatisée d'une vulnérabilité connue au cours d'une vague mondiale d'attaques.

- **Méthodes d'attaques indirectes :** certains attaquants exploitent l'interconnexion entre un prestataire de services numériques et ses clients pour compromettre discrètement les SI des clients, parfois à haute valeur ajoutée ; tandis que d'autres piègent des logiciels avant leur diffusion afin d'infecter un grand nombre d'entités. Par exemple, la campagne d'attaques Cloud Hopper, menée en 2017, aurait permis à ses auteurs de compromettre de nombreuses organisations dans le monde entier après s'être infiltrés sur les SI de prestataires de services numériques. En 2017, la compromission de deux mises à jour de l'utilitaire Ccleaner avant leur diffusion aurait permis aux attaquants de compromettre plus de 2 millions de postes dans le monde entier.

- **Attaques par rançongiciel :** en augmentation depuis 2018, les attaques par rançongiciels sont menées de manière plus ciblée en 2020. Le 19 mars 2019, à la suite d'une infection par le rançongiciel LockerGoga, l'entreprise norvégienne Norsk Hydro, spécialisée dans l'industrie de l'aluminium, a été forcée d'arrêter une grande partie de son réseau et de réaliser sa production « manuellement ». Possédant des sauvegardes de ses données, l'entreprise a fait le choix de ne pas payer la rançon. La baisse de productivité due à l'attaque a coûté environ 40 millions de dollars à l'entreprise. Depuis la fin de l'année 2019, certains attaquants exfiltrent les données avant de les chiffrer à des fins de chantage à la divulgation. Il s'agit toutefois de deux attaques distinctes, utilisant des codes malveillants différents. Cette tendance émergente fait peser un nouveau risque sur les entités victimes face à la menace de divulgation de leurs données.

→ Il convient de donner des éléments de compréhension aux joueurs pour leur permettre de mieux saisir la situation qu'ils vont subir sans pour autant leur dévoiler le scénario. Le risque d'attaques par rançongiciel est donc inséré au milieu d'autres menaces.

2. CONTEXTE SPÉCIFIQUE À L'ORGANISATION

- **Exemples relatifs à l'état de la menace :** l'organisation opère dans un secteur déjà particulièrement ciblé par des cyberattaques de type rançongiciel. La semaine dernière, l'entreprise française XYZ a été victime d'un rançongiciel et n'a toujours pas repris une activité normale. Les médias estiment le coût de l'attaque à plusieurs millions d'euros. Au début du mois, c'est la société ABC qui a fait l'objet d'une cyberattaque. De nombreux documents internes

à cette société ont été publiés par les attaquants. Opérant dans le même secteur, l'organisation risque elle aussi d'être ciblée par ce même type d'attaque.

- **Exemples relatifs à l'organisation et à son secteur d'activité :** sortie d'une nouvelle offre avant la période critique de vente ou quelques jours après ; clôture des bilans financiers ; entrée en bourse ; annonce de l'acquisition d'un concurrent.
- **Exemples relatifs au contexte externe :** événement politique ou sportif majeur qui pourrait, indirectement, expliquer une potentielle recrudescence des attaques.

→ En fonction de la pression que vous souhaitez mettre sur les joueurs, il est possible d'inscrire la crise dans un contexte particulier (événement important pour l'organisation, période critique, commandes à honorer, jalon non déplaçable, etc.).

Recommandation

Pour illustrer le dossier de mise en situation avec des exemples en lien avec votre organisation, consultez le rapport *État de la menace rançongiciel à l'encontre des entreprises et institutions* sur le site du CERT-FR (CTI-001) ainsi que la presse[17].

17 : www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001

FICHE PRATIQUE 8 :

OBSERVER UN EXERCICE

La fiche d'observation est un outil indispensable à l'observateur. Elle comprend à la fois des indications lui permettant de se concentrer sur des points en particulier et des questions auxquelles répondre en fonction des objectifs de l'exercice. Il n'est pas nécessaire que les observateurs aient les réponses à toutes les questions retenues. Ils peuvent en complément noter d'autres points jugés utiles. La main courante remplie par les joueurs peut également apporter certains éléments qui n'auront pas pu être directement observés.

Cette fiche contient une liste non exhaustive de questions utiles aux observateurs dont les planificateurs peuvent s'inspirer pour créer une fiche d'observation. Elles peuvent être adaptées à chaque cellule de crise.

ALERTE

- Qui transmet l'alerte ? Comment ?
- Qui décide d'activer la cellule de crise et de convoquer les salariés ?
- À quelle heure la convocation en cellule est-elle transmise ?
- L'ensemble des services nécessaires à la gestion de la crise sont-ils alertés ?
- Le cas échéant, quels sont les services manquants ?
- À quelle heure la cellule de crise est-elle fonctionnelle ?

LOGISTIQUE ET OUTILLAGE DE LA CELLULE

- La taille des locaux semble-t-elle adaptée (ergonomie, facilité de circulation, etc.) ?
- Les procédures et outils permettent-ils de gérer efficacement la situation ou au contraire constituent-ils un poids ? Sont-ils fonctionnels ?
- Des outils de secours sont-ils prévus ? Sont-ils utilisés ?
- Des outils semblent-ils manquer ? Lesquels ?

CIRCULATION DE L'INFORMATION

- La main courante est-elle régulièrement renseignée et accessible à tous ? Sinon, pourquoi ?
- Comment circulent les messages entre les membres de la cellule de crise ? Et entre les différentes cellules de crise ?
- Les messages sont-ils compris par les destinataires ?

- Les organismes/services compétents sont-ils consultés ?
- Les parties prenantes (autorités, clients, prestataires, etc.) sont-elles informées de la situation ?
- Quelle est la fréquence des points de situation ? Comment sont-ils organisés ?
- Sont-ils précis, concis, compréhensibles par tous ? Démontrent-ils une démarche d'anticipation ?
- Les informations reçues et les décisions prises redescendent-elles régulièrement aux services et autres cellules de crise ?
- Les informations issues de la cellule opérationnelle, simulée par la cellule d'animation, sont-elles bien transmises à la cellule décisionnelle ? Sont-elles explicitées par le RSSI et comprises par des joueurs non spécialistes du sujet ?

RÉACTION DES JOUEURS

- Chaque acteur connaît-il bien son rôle dans l'organisation de crise ?
- Le périmètre des missions de chacun est-il respecté ?
- Les rôles définis pour la gestion de crise sont-ils correctement appliqués ?
- La documentation de crise et les procédures déjà définies sont-elles connues et utilisées par les cellules de crise (fiches réflexes, plans, etc.) ?
- La situation est-elle bien comprise ?
- Le périmètre de l'attaque est-il déterminé ?
- Les actions et décisions prises semblent-elles adaptées et cohérentes ?
- Les personnes arrivent-elles à rapidement analyser la situation et ses évolutions ?
- En combien de temps sont prises les premières décisions ?
- En combien de temps ces décisions sont-elles mises en œuvre ?

COMMUNICATION

- Les communicants sont-ils intégrés à cellule de crise ?
- Échangent-ils avec les experts techniques ?
- Des éléments de langage sont-ils définis ?
- L'information donnée aux médias est-elle coordonnée avec la cellule décisionnelle ?
- Le suivi médiatique (rumeurs, annonce dans les médias, etc.) est-il réalisé et fait-il l'objet d'éventuels ajustements dans la stratégie de communication ?
- Les salariés de l'organisation sont-ils informés de la situation et de ce qu'ils doivent faire ?

CLARIFICATION DES IMPACTS LIÉS À L'ATTAQUE ET À LA REMÉDIATION

- Les impacts, tels que l'impossibilité d'utiliser tout ou partie de leurs outils et la perte de tout ou partie des données les concernant depuis X temps, sont-ils clairement exposés aux métiers concernés ?
- Les délais réels des événements qui ont volontairement été accélérés dans le cadre de l'exercice (investigation, mitigation/remédiation) sont-ils clairement expliqués à l'ensemble des joueurs ?
- Le dialogue entre les acteurs de la chaîne SSI et les acteurs de la gestion de crise/continuité d'activité/juristes etc. semble-t-il suffisant ? La coordination semble-t-elle efficace ?
- Dans une situation réelle, les ressources techniques internes seraient-elles suffisantes et un accompagnement technique serait-il sollicité ou est-il prévu ?

Recommandation

L'observateur peut prendre note du respect des règles de vie en cellule de crise, édictées en amont, comme la distribution des rôles, le positionnement des uns et des autres dans la salle, le respect des temps et de l'ordre de paroles, etc.

L'aspect purement « comportemental » en cellule de crise peut faire l'objet d'une analyse. Si ce choix est fait dans le cadrage de l'exercice, seul un professionnel (psycho-sociologue, coach) pourra apporter un avis éclairé et utile lors de la mise en situation. Cette analyse est intéressante à conduire notamment sur des cellules de crise déjà professionnalisées en intégrant des débriefings individuels, en ouvrant éventuellement vers une séance de cohésion d'équipe au moment du RETEX à froid. Les résultats pourront se traduire en un enrichissement personnel et professionnel des participants.

EXERCICE
RANSOM20

Dans le cadre de l'exercice RANSOM20, deux lieux différents peuvent être observés :

- la cellule de crise décisionnelle de l'organisation ;
- la cellule de crise du second site de l'organisation.

En se basant sur les objectifs préalablement définis, les observateurs peuvent notamment se concentrer sur les points suivants :

- la mobilisation des personnes nécessaires à la gestion de la crise ;
- la stratégie de communication de crise sur des problématiques cyber ;
- la coordination entre le site principal de l'organisation et son second site (partage de l'information, transmission de consignes, etc.) ;
- la prise de décision, la mise en œuvre des procédures de gestion de crise et de fonctionnement dégradées.

PHASE 4

BRIEFER LES PARTICIPANTS ET S'ASSURER DE LEUR IMPLICATION

Briefer les animateurs et les observateurs

Une semaine avant l'exercice, il convient d'organiser une réunion avec les animateurs et les observateurs pour s'assurer que le scénario et les objectifs sont compris et les rôles de chacun connus. Pour les observateurs, c'est l'occasion de préciser les éléments de l'exercice à observer (par exemple, l'application d'une procédure à tester). Un bref rappel pourra être réalisé le jour de l'exercice également.

Briefer les joueurs

Un briefing joueurs est recommandé une à deux semaines avant le lancement de l'exercice. Un briefing le jour J, immédiatement avant de commencer l'exercice, est également nécessaire.

Les points suivants peuvent être abordés :

- objectifs de l'exercice ;
- facteurs de succès (rappeler que l'implication des participants est la clé de la réussite et que l'exercice est une formation) ;
- conventions d'exercice (règles de jeu) ;
- **le concept de cellule d'animation**, c'est-à-dire le fait qu'un groupe de personnes dits « animateurs » simule des personnes existant dans la réalité (équipes informatiques internes comme externes, CERT, mais

aussi partenaires, RH, prestataires, etc.). En effet, les joueurs ont souvent des difficultés à comprendre ce concept ce qui peut déclencher certaines interrogations (puis-je contacter mes équipes dans le cadre de cet exercice ? Comment ?, etc.). Il convient d'être très clair sur les personnes qui sont simulées par la cellule d'animation et celles qui participent en tant que joueurs à l'exercice.

L'annexe 1 présente l'ensemble des livrables à produire pour l'organisation d'un exercice cyber.

ÉTAPE 3

DÉROULER SON EXERCICE

Dérouler l'exercice consiste à suivre pas à pas le chronogramme préparé en amont et à s'adapter aux réactions des joueurs. À l'issue de cette étape, vous avez toutes les clés vous permettant d'animer un exercice de gestion de crise cyber et vous êtes en mesure de répondre aux réactions, parfois inattendues, des joueurs.

FICHES PRATIQUES À CONSULTER :

- Fiche pratique n° 9 : éviter les écueils les plus fréquemment rencontrés
- Fiche pratique n° 10 : contourner les biais de simulation

PHASE 1

APPLIQUER CE QUI EST PRÉVU

Le jour J, il est temps de dérouler l'exercice en suivant le scénario et le chronogramme tout en restant agile face aux réactions des joueurs.

Mettre les joueurs en situation

Pour les exercices sous forme de simulation, le DEBEX peut être précédé d'un message de mise en ambiance qui donne notamment les conventions d'exercice. Il peut également être accompagné d'un dossier de mise en situation qui permet d'inscrire l'exercice dans un contexte plus précis. Cela se traduit en général par un message envoyé quelques jours avant l'exercice, puis à nouveau dix à quinze minutes avant le DEBEX, permettant par la même occasion de tester les moyens de communication. Le briefing réalisé le jour de l'exercice permet aussi de rappeler les règles et le contexte.

En ce qui concerne le format exercice sur table, il convient pour l'animation de présenter les différentes phases du scénario sur des diapositives afin de proposer une situation évolutive aux joueurs.

Suivre le chronogramme

L'ensemble des éléments utiles à l'animation de l'exercice a été préparé en amont du jour J (voir étapes 1 et 2). L'équipe d'animation doit suivre le chronogramme en respectant au maximum la cadence prédéfinie.

Néanmoins, dans la plupart des cas l'exercice ne se passe pas exactement comme prévu et il convient de s'adapter aux réactions des joueurs (voir étape 3 phase 2).

Recommandation

Si la cellule d'animation est loin des joueurs, les premiers stimuli doivent être complétés d'un appel téléphonique pour s'assurer que les joueurs sont bien en place et prêts à jouer. L'observateur peut également contacter la cellule d'animation pour les informer des premières réactions des joueurs.

Concrétiser les impacts

La logistique d'un exercice de crise cyber possède quelques spécificités nécessitant parfois d'intervenir au cours du jeu auprès des joueurs (ce rôle peut être dévolu à un animateur) :

- **isoler les équipements** des joueurs considérés comme atteints par le scénario. Par exemple, si l'ordinateur portable du directeur financier est compromis, ce joueur ne pourra pas l'utiliser durant tout ou partie de l'exercice ;
- **rendre vraisemblables les impacts** des solutions de contournement et/ou de remédiation sur les équipements de tous les participants. Par exemple, si une coupure provisoire de la messagerie est décidée, plus aucun joueur ne peut envoyer ou recevoir de courriels.

EXERCICE RANSOM20

Les joueurs n'ont plus accès aux ordinateurs connectés au réseau puisque l'organisation est victime d'un rançongiciel sur l'ensemble du SI. Les adresses mail de l'organisation et potentiellement les téléphones fixes ne fonctionnent plus. Il convient donc de les retirer ou d'afficher un message disant qu'ils sont inutilisables.

PHASE 2

S'ADAPTER AUX JOUEURS

Suivre leur rythme

Le chronogramme définit le rythme de la crise simulée dans le cadre de l'exercice, cependant l'équipe d'animation doit s'adapter aux réactions des joueurs, par exemple en modifiant l'heure d'envoi d'un stimulus. La possibilité de décaler les envois de certains stimuli doit donc être prévue.

Pour éviter tout malentendu et perte de cohérence générale du scénario, toute décision majeure de modification doit être prise de manière **collégiale** au sein de la cellule d'animation. Les observateurs doivent également être informés de ces modifications apportées au rythme de l'exercice.

EXERCICE
RANSOM20

Si la décision d'isoler les postes de travail du réseau est prise plus tôt que prévu, il convient d'avancer les stimuli liés à ce sujet. Si elle tarde à être prise, d'autres stimuli insistant sur la nécessité de le faire peuvent être ajoutés.

Si des éléments de pression médiatique simulée sont prévus dans votre exercice en réaction à des actions qui doivent être menées par les joueurs, il est alors nécessaire d'attendre que les joueurs aient réalisé ces actions avant d'envoyer les stimuli (par exemple, clients mécontents à la suite de l'indisponibilité d'un service interrompu pour éviter la propagation de l'attaque).

Si l'exercice ne se déroule pas comme prévu ou que l'incompréhension des joueurs est trop grande, il peut être opportun d'**intervenir pour aborder de nouveau certains points** ou expliquer aux joueurs la situation et les attendus. Il est également possible d'accompagner un joueur qui serait particulièrement en difficulté. Par exemple, s'il s'agit du directeur de la cellule de crise, lui rappeler qu'il faut penser à organiser un point de situation avec son équipe. En effet, il convient d'**éviter de constater l'échec de l'exercice afin que celui-ci conserve ses vertus pédagogiques**. Toutefois, cela ne signifie pas que les points négatifs ou les axes d'amélioration ne peuvent être soulignés. Le RETEX permet d'échanger sur ces sujets et d'établir un plan d'action pour y remédier.

Recommandation

Il faut éviter de sortir les joueurs du jeu pendant l'exercice. Néanmoins, il est utile de se préparer à un potentiel départ, non prévu, d'un membre de la direction générale pour une urgence : l'exercice doit donc continuer avec la désignation d'un joueur suppléant en séance.

Répondre à leurs réactions inattendues

Sur un scénario de crise cyber, environ 70 % des stimuli du chronogramme sont suivis tandis que 30 % sont remaniés voire totalement improvisés. Il s'agit ici d'un ratio moyen indicatif qui montre que malgré toute l'attention portée à la préparation, il faut être prêt à s'adapter. En effet, la réaction des joueurs peut parfois différer de la réaction attendue (voir étape 2 pour plus d'information sur l'élaboration du chronogramme).

Cependant, **il n'est pas possible de tout prévoir**. Si vous n'avez pas anticipé une réaction des joueurs qui va influencer le jeu, vous vous devez d'intervenir. Sinon, la suite de votre animation risque de ne plus être cohérente.

S'assurer régulièrement de la bonne compréhension des stimuli par les joueurs permet de limiter l'occurrence de réactions inattendues. C'est notamment le rôle du DIRANIM qui peut échanger régulièrement avec les observateurs ou se rendre lui-même dans la salle de gestion de crise.

Il est aussi possible de **compléter un stimulus envoyé par mail, par un appel téléphonique et inversement**, notamment pour les premiers stimuli et pour les plus importants afin de garantir le bon démarrage de l'exercice et la compréhension de l'élément déclencheur. Attention toutefois à ne pas le faire systématiquement, car cela risquerait de casser le rythme du jeu.

Par ailleurs, en fonction des préoccupations des joueurs, il peut être nécessaire d'insister plus fortement sur un certain point de la crise qu'ils auraient mis de côté. Par exemple, il arrive que les joueurs se concentrent sur la mise en œuvre du PCA sans analyser les conséquences en matière de SSI.

Il se peut également que des éléments aient été oubliés dans la rédaction du chronogramme ou que des questions inattendues soient posées par les joueurs. Dans ce cas, il est nécessaire de préparer une réponse avec la cellule d'animation et notamment les experts adéquats, quand cela est possible.

Recommandation

Il n'est pas nécessaire de répondre immédiatement à la sollicitation d'un joueur. Il est souhaitable de se concerter entre animateurs pour déterminer la meilleure réponse à apporter et le moment adéquat. Comme dans la vraie vie, il est tout à fait possible de ne pas connaître la réponse.

Il peut être judicieux que le DIRANIM intervienne pour rappeler aux joueurs certaines conventions d'exercice ou les informer que dans la réalité, les moyens demandés (ressources techniques, humaines, financières) n'arriveraient pas aussi vite. Il faut également faire particulièrement attention aux joueurs qui ont tendance à minimiser les conséquences

d'une attaque, dénuant ainsi d'intérêt le scénario. Il convient d'être vigilant sur ce point qui se présente souvent lors d'exercices cyber.

Les fiches n° 9 et n° 10 proposent quelques conseils à mettre en œuvre par les animateurs pour faire face à l'imprévu.

FICHE PRATIQUE 9 :

ÉVITER LES ÉCUEILS LES PLUS FRÉ-

Les écueils mentionnés ci-dessous ne sont pas exhaustifs et sont spécifiques aux exercices de gestion de crise cyber. Ceux-ci peuvent être évités en insistant sur ces points lors du briefing joueurs le jour de l'exercice. Cependant, si tout ou partie des objectifs de l'exercice risquent de ne pas être éprouvés du fait de l'occurrence d'un ou de plusieurs des écueils décrits ci-après, le DIRANIM doit alors intervenir, en se basant, par exemple, sur les solutions proposées, pour recentrer les prises de décision et les choix des joueurs.

ÉCUEIL 1 : LA CELLULE DE CRISE DÉCISIONNELLE DEVIENT UNE CELLULE DE CRISE OPÉRATIONNELLE

Il arrive fréquemment que certains joueurs discutent de problématiques techniques relevant d'une grande expertise informatique et représentant un niveau de granularité inapproprié en cellule de crise décisionnelle. Une cellule de crise de haut niveau n'est pas le lieu pour débattre des détails techniques. Cela engendre un manque de recul nuisible à la prise de décision. Les échanges doivent porter sur les solutions de remédiations possibles et les impacts financiers, métiers, réputationnels, etc. La manière de mettre en œuvre techniquement la ou les solutions de remédiations retenues se décide au sein des équipes opérationnelles et notamment informatiques.

SOLUTION 1.1

La cellule d'animation peut solliciter la cellule de crise décisionnelle et lui demander un point de situation, fortement orienté sous un angle métier (ex : faut-il mettre au chômage technique certains salariés ?) pour pousser ses joueurs à se recentrer sur les aspects stratégiques.

SOLUTION 1.2

La cellule d'animation peut exfiltrer une des personnes alimentant ce débat via un mail ou un appel en lui demandant de se rendre dans une autre salle et ainsi limiter ce type de discussion. Elle lui explicitera ainsi la raison avant de la réintégrer dans la cellule de crise.

SOLUTION 1.3

La cellule d'animation peut créer des stimuli destinés à la personne alimentant ces débats en vue de l'occuper plus fortement d'une part et d'autre part, de l'orienter si possible sur des sollicitations ou questions plus stratégiques afin de lui offrir la capacité de réorienter son approche en cellule de crise décisionnelle.

QUEMMENT RENCONTRÉS

ÉCUEIL 2 : INCOMPRÉHENSION ENTRE LES NIVEAUX DÉCISIONNEL ET OPÉRATIONNEL DANS LA MISE EN ŒUVRE DES ORIENTATIONS

Un écart de perception entre les orientations et décisions prises par le niveau décisionnel et les contraintes (techniques, de temps, etc.) de mise en œuvre est susceptible de se creuser, plus particulièrement dans les exercices où le niveau technique est simulé par la cellule d'animation.

SOLUTION

Si les actions techniques sont entièrement simulées par la cellule d'animation, il est possible d'ajouter des stimuli pour énoncer certaines difficultés de mise en œuvre des décisions prises par la cellule de crise soit en raison d'un manque de précision du niveau décisionnel, soit parce que cette mesure n'est pas réaliste. L'idée est de formuler ces « alertes » à la cellule décisionnelle sous forme de questions et de demandes de précisions pour se préserver des potentielles réactions de rejet de la part des joueurs la composant.

ÉCUEIL 3 : CONTRADICTIONS ENTRE DÉCISIONS PRISES PAR LA CELLULE DE CRISE ET LES OBJECTIFS DE L'EXERCICE

L'analyse des impacts des axes de remédiation est parfois peu approfondie et certaines mesures peuvent aller à l'encontre des orientations et des objectifs de l'exercice. Par exemple, un directeur de crise peut décider de fermer l'ensemble de son organisation et de renvoyer tous les employés chez eux, sauf la cellule de crise et quelques personnes des équipes informatiques, tandis que l'un des objectifs de l'exercice consiste à trouver des compromis entre les contraintes liées à la remédiation et une certaine continuité d'activité.

SOLUTION

Il revient à la cellule d'animation de refuser ces mesures, soit via l'intervention d'une personne (simulée ou non), soit via l'intervention d'une convention d'exercice.

ÉCUEIL 4 : SUR-SOLLICITATION DES ÉQUIPES TECHNIQUES (SIMULÉES PAR LA CELLULE D'ANIMATION) AU DÉTRIMENT DES JOUEURS IMPLIQUÉS DANS L'EXERCICE

Il arrive fréquemment que les équipes techniques soient sur-sollicitées par la cellule de crise décisionnelle qui souhaite bénéficier d'une vision permanente et instantanée de la situation et avoir ainsi un sentiment de contrôle, au détriment des autres membres de la cellule de crise, notamment en charge des thématiques métier et de la gestion des impacts de l'incident.

SOLUTION

La sur-sollicitation peut être corrigée de deux manières : en interdisant certains ponts de communication ou en concentrant ces sollicitations vers une personne qui aura un rôle de « proxy ». Dans les deux cas, il convient de sensibiliser la cellule de crise décisionnelle au fait que les investigations prennent du temps et que la communication d'éléments techniques doit se faire avec un niveau de certitude élevé.

ÉCUEIL 5 : MANQUE DE COMPRÉHENSION ET D'EXPLICATION DES PROBLÉMATIQUES CYBER

L'absence de vulgarisation des problématiques cyber est fréquente et peut engendrer de la confusion au sein de la cellule de crise décisionnelle. Ceci est d'autant plus marqué dans les organisations au sein desquelles il manque une culture et un langage communs entre les équipes techniques et celles du niveau décisionnel.

SOLUTION

La cellule d'animation provoque des points de situation ad hoc, avec le RSSI et le directeur de crise, afin de renforcer le dialogue vertical.

FICHE PRATIQUE 10 :

CONTOURNER LES BIAIS DE SIMU-

Le déroulé d'un exercice peut générer un certain nombre de biais comportementaux et organisationnels qui sont autant de risques à maîtriser durant la phase d'animation. Certains d'entre eux sont décrits et illustrés dans le tableau ci-après. À noter que ces biais sont inhérents à la gestion de crise et peuvent toutefois être accentués lors des exercices.

		SOUS-RÉACTION / ENGAGEMENT /
TYPE	**ILLUSTRATION**	**SOLUTION**
Désencrage	**Attitude passive, désintérêt.** *« Ce n'est pas la vraie vie, il suffit de dire que l'on a réalisé cette action et que cela a fonctionné. »*	**Inciter la personne à s'immerger dans l'exercice en créant des stimuli qui lui sont destinés et qui demandent de réaliser une action.**
Défausse	**Attitude présentant une forme de recul (en coin de salle par exemple), ne souhaite pas prendre de décision ou endosser de responsabilité.** *« Ce n'est pas à moi de faire cette action, ce n'est pas de ma responsabilité. »*	**Impact de réputation, indisponibilité d'un ou plusieurs outils applicatifs, déclenchement partiel ou total d'un PRA, du PCA.**

LATION

Idéalement, il revient à la cellule d'animation de repérer ces comportements, notamment avec l'aide des observateurs, et d'agir pour ne pas qu'ils aient un impact négatif sur le jeu.
Ce tableau (non exhaustif) repose sur l'expérience des observations menées lors de nombreux exercices de gestion de crise cyber.

SUR-RÉACTION

TYPE	ILLUSTRATION	SOLUTION
IMPLICATION		
Surinvestissement	**Prend une posture centrale dans la salle, visible de tous, regarde les actions et comportements des voisins, réalise beaucoup de mouvements.** *« Je vais prendre en charge ceci ou cela, je m'occupe de telles et telles actions, je vais vérifier que, je suis responsable de.... »*	**Demander explicitement un point de situation à un autre joueur dont le périmètre n'est pas respecté par l'intéressé et ne s'adresser qu'à cet autre joueur.**
Besoin excessif de contrôle	**Beaucoup d'agitation, relances excessives pour avoir un retour sur des actions en cours.** *« Où en est-on de telle action, telle mesure, telle discussion ? »*	**Couper court ou ne pas répondre à certaines sollicitations considérées comme excessives en demandant par exemple, un rendez-vous téléphonique plus tard.**

SOUS-RÉACTION

TYPE	ILLUSTRATION	SOLUTION
		GESTION DU TEMPS
Retard	**Forme d'inertie et de manque de dynamisme.** *« On a tout notre temps parce que ce n'est pas la vraie vie. »*	**Rappeler la temporalité de l'exercice, donner fréquemment des échéances points de situation, demande d'entretien par le comité exécutif, etc.).**
		LEADERSHIP DU OU DES DIRECTEUR(S) /
Retrait	**Peu ou pas d'arbitrage, absence d'orientations.** *« On verra plus tard, on ne peut pas trancher maintenant. »*	**Envoyer une demande de point invoquant la stratégie mise en œuvre (sollicitation médiatique, investisseurs, comité exécutif).**

SUR-RÉACTION

TYPE	ILLUSTRATION	SOLUTION
ET DU STRESS		
Hyperacti-vité	Beaucoup de déplacements dans la salle et de gestes, énormément de questions, difficulté à gérer le stress engendré par l'exercice.	Rassurer l'intéressé en rappelant les objectifs et le fait qu'un exercice n'a pas pour but de noter une personne. L'exercice permet au contraire de s'entraîner à gérer son stress.
MANAGER(S) DE CRISE		
Tyrannie	Posture centrale mais fixe, coupe la parole, tranche sans attendre les options, peu d'écoute.	Sortir le directeur de crise de la cellule durant un temps donné (simulation d'une conférence de presse, par exemple).

ÉTAPE 4

TIRER LES ENSEIGNEMENTS DE SON EXERCICE

Organiser un RETEX est indispensable à l'amélioration du dispositif de gestion de crise de l'organisation. Il permet de tirer les leçons de l'exercice, c'est-à-dire de souligner ce qui a bien fonctionné et ce qui doit être amélioré.

À la fin de cette étape, vous avez :

- identifié les points forts de votre organisation pour la gestion des crises cyber ainsi que les axes d'amélioration ;
- établi un plan d'action concret pour pallier les manques et renforcer l'existant.

Bravo ! Vous avez organisé un exercice de gestion de crise cyber !

LIVRABLES À PRODUIRE :

- Compte-rendu du RETEX à chaud
- Compte-rendu du RETEX à froid
- Plan d'action

FICHE PRATIQUE À CONSULTER :

- Fiche pratique n° 11 : produire un RETEX - exemple fil rouge RANSOM20

PHASE 1

ORGANISER UN RETEX À CHAUD

L'organisation d'un RETEX à chaud, à l'issue du FINEX, est fortement recommandée dans la mesure où les participants seront encore sous l'effet de l'immersion. Le RETEX à chaud permet aux observateurs de **recueillir des éléments importants** et d'**évacuer les éventuelles frustrations** suscitées par l'exercice. Il permet également de **présenter les points forts observés ainsi que les axes d'amélioration**.

Recommandation

Le RETEX est un moment sensible qu'il convient d'aborder avec tact. Lors du RETEX à chaud et surtout s'il s'agit d'un premier exercice, il convient d'insister particulièrement sur les points positifs observés. Les points négatifs peuvent être présentés sous forme d'axes d'amélioration.

Le RETEX prend généralement la forme d'un **tour de table**, au cours duquel chaque joueur s'exprime. Il convient de prévoir une personne pour l'animer et une ou deux personnes pour prendre des notes pendant la discussion. La durée d'un RETEX à chaud est d'environ une heure, pour un exercice d'une demi-journée à une journée. L'ensemble des participants doit prendre la parole.

Au cours de ce tour de table, les thématiques suivantes sont souvent abordées :

- préparation à l'exercice des participants et organisation ;
- vraisemblance du scénario ;
- qualité des échanges d'information entre les équipes ;
- qualité de la communication interne et externe ;

- fonctionnement des équipements et matériels ;
- logistique (salle de crise, outils, etc.) ;
- ressources humaines (constitution des équipes, relève, utilisation des compétences, etc.) ;
- etc.

Recommandation

Il convient de faire parler les joueurs en premier pour éviter que les observateurs n'influencent leur retour. Il est important que tout le monde s'exprime. La parole libre (mais respectueuse des autres) doit être encouragée et la réunion ne doit pas être organisée dans un cadre trop formel afin de permettre à l'ensemble des parties prenantes de s'exprimer.

Dans le cas où plusieurs cellules de crise seraient impliquées, il est possible de :

- effectuer des **RETEX en parallèle**. Cette option sera retenue si le temps dédié au RETEX est contraint ou s'il est nécessaire de laisser s'exprimer les cellules de crise de manière indépendante ;
- mettre en place un **RETEX commun** (même si les cellules de crise sont distantes), afin que les membres de chaque cellule échangent sur leur expérience. Cette option est préférable pour capitaliser sur l'exercice et permet de rassembler différents profils d'une même organisation autour des questions cyber.

Pour le RETEX à chaud, il peut être intéressant pour des raisons de traçabilité et de structuration de la réflexion des joueurs de leur demander de renseigner une questionnaire d'auto-évaluation qui reprend les grands items de la fiche d'observation. Elle ne vise pas à récolter des éléments subjectifs sur les comportements des participants.

L'organisation du RETEX à chaud constitue également l'occasion d'**expliquer la situation** que viennent de traverser les joueurs. En effet, un scénario de crise cyber est souvent vu, par la cellule de crise déci-

sionnelle, à travers les impacts qu'il provoque. Il est donc intéressant de retracer l'attaque que vient de subir l'organisation de manière simplifiée afin que l'ensemble des participants en ait une vision complète et réaliste (par exemple, en indiquant si les vulnérabilités exploitées lors de l'attaque existent réellement ou non).

Recommandation

Si des points de l'exercice diffèrent de ce qu'il se passerait dans la vie réelle, il est important de les préciser lors du RETEX (par exemple, une action d'investigation raccourcie pour permettre à l'exercice d'avancer plus rapidement).

PHASE 2

RÉALISER UN RETEX À FROID

L'organisation d'un RETEX « à froid », quelques jours à un mois après l'exercice, permet de **compléter le RETEX à chaud** et de **clôturer le recueil des avis** sur son déroulement. Cette seconde phase du retour d'expérience est l'occasion de collecter un certain nombre de suggestions ou de constats construits après réflexion sur l'expérience des participants durant l'exercice. Le RETEX à froid permet notamment d'identifier d'éventuels oublis et de proposer des axes d'évolution et des propositions d'action. Concrètement, le RETEX à froid doit réunir l'ensemble des participants et durer environ une heure également.

Afin de préparer le RETEX à froid, les joueurs sont invités, s'ils le souhaitent, à reprendre le questionnaire d'évaluation. Des entretiens individuels peuvent également être organisés en complément. Ils permettent aux participants de se sentir plus en confiance et de partager plus sincèrement leur ressenti sur l'exercice.

PHASE 3

PRODUIRE UN RAPPORT ÉCRIT ET PRÉVOIR UNE RESTITUTION

La dernière phase de l'organisation d'un exercice de crise est la restitution du RETEX sous forme d'un rapport écrit (par les membres du groupe projet et les observateurs) et diffusé à l'ensemble des participants. Ce rapport **identifie les actions à mener pour améliorer le dispositif de gestion de crise**.

La restitution peut être organisée à plusieurs niveaux, par exemple en diffusant une synthèse à la direction générale et un document plus complet aux participants. Ce document peut aussi être important à titre de contrôle (par les assurances, par des audits extérieurs, etc.).

La construction de ce rapport passe par la collecte et l'analyse des éléments suivants :

- la/les main(s) courante(s) de l'exercice (au minimum, une main courante aura été tenue par l'un des joueurs en cellule(s) de crise) ;
- les mails échangés durant l'exercice ;
- les prises de notes des observateurs pendant l'exercice et le tour de table ;
- le compte-rendu du RETEX à chaud ;
- les questionnaires renseignés et les entretiens réalisés pour le RETEX à froid.

Un exercice de gestion de crise cyber doit être l'occasion de **faire progresser une organisation** pour faire face à une crise cyber. Ce rapport doit donc :

- présenter les **points forts** sur lesquels s'appuyer et les **points à améliorer** ;

- proposer un **plan d'action concret** pour pallier les manques ou les faiblesses et/ou renforcer l'existant (ce plan doit identifier les personnes en charge de réaliser chaque action) ;
- apporter des éléments factuels soutenus par des preuves ou des arguments objectifs ;
- être **synthétique** afin d'être lu et compris par le plus grand nombre ;
- être publié dans des délais courts suivants l'exercice (maximum deux mois) ;
- être éventuellement **associé à une restitution orale** afin de maintenir un dialogue entre tous les participants et permettre, le cas échéant, de résoudre d'éventuels conflits. Les grands axes de ce rapport peuvent en effet être présentés (et validés) lors du RETEX à froid.

Communiquer tout ou partie de ce RETEX est une manière de montrer en interne comme en externe le travail réalisé pour améliorer la résilience cyber au sein de son organisation. La diffusion du RETEX et du plan d'action qui en est tiré permet aussi de **continuer à impliquer les participants** en accord avec les objectifs de l'exercice.

La fiche pratique n° 11 à la fin de cette étape propose un exemple de RETEX pour l'exercice RANSOM20.

FICHE PRATIQUE 11 :

PRODUIRE UN RETEX

EXEMPLE FIL ROUGE RANSOM20

Cette fiche pratique constitue le RETEX fictif de l'exercice RANSOM20 tel qu'il aurait pu être mené par une organisation ayant décidé de tester deux cellules de crise (siège et second site de l'organisation).
Il s'agit d'une synthèse à destination des décideurs qui ont la responsabilité de valider le plan d'action proposé. Il met en exergue les principaux enseignements au regard des objectifs préalablement établis.

0. RAPPEL DES ACCÉLÉRATIONS DE RYTHME VIS-À-VIS DE LA RÉALITÉ

Cet exercice portait principalement sur l'incident et les phases d'investigation et de continuité d'activité. Plusieurs actions ont été accélérées pour permettre aux joueurs de réfléchir à la remédiation et au maintien ou à la reprise de l'activité en mode dégradé.

Dans la réalité, le périmètre impacté, les éléments sur le type de rançongiciel et sur le chemin d'attaque n'auraient pas été obtenus dès la première journée. Ces investigations nécessitent en effet plusieurs jours voire plusieurs semaines de travail, notamment si le rançongiciel était jusqu'alors inconnu. L'analyse des sauvegardes et leur réinstallation auraient également été effectuées plus tard, une fois l'attaque arrêtée, l'attaquant expulsé et le SI sécurisé. En fonction de l'état du SI, ces actions durent plusieurs jours à plusieurs semaines.

1. RÉALISATION DES OBJECTIFS (VOIR FICHES N°1 ET N° 4)

L'exercice RANSOM20 a sollicité 27 participants (20 joueurs, 5 animateurs et 2 observateurs). Il a été l'occasion de s'assurer que **la totalité des personnes nécessaires à la gestion de la crise ont été sollicitées** *[objectif 1]*. Il a également permis de **tester la stratégie de communication de crise** sur la problématique du rançongiciel et de mettre en exergue la nécessité de disposer d'outils de communication interne de secours permettant de s'adresser efficacement à l'ensemble des employés *[objectif 2]*. La participation des équipes du second site démontre **la bonne articulation entre le dispositif de gestion de crise central et le dispositif local**. En revanche, il a été noté, durant la préparation de l'exercice et au vu des impacts directs (simulés) sur les activités de l'organisation que la capacité à isoler les SI directement liés à la production pose question et doit faire l'objet d'une analyse approfondie *[objectif 3]*. La simulation de l'arrêt des

activités a été l'opportunité de **revoir les besoins en matière de sauvegarde** et a révélé la nécessité de renforcer la rotation entre les personnels clés, certains d'entre eux ne disposant pas de suppléant *[objectif 4]*.

2.BONNES PRATIQUES

Cet exercice a permis d'**intégrer pour la première fois des experts cyber au dispositif de gestion de crise** de l'organisation. Les interactions entre les « habitués de la gestion de crise », les représentants des métiers impactés et les experts SSI se sont bien déroulées et ont abouti à des **décisions constructives**. Les informations ont également bien circulé entre le siège de l'organisation et le site de production.

Les conséquences des dysfonctionnements sur les activités de l'organisation ont été rapidement identifiés, ce qui a facilité la mise en œuvre de **scénarios de réponse adéquats** prévus dans les PCA et PRA. L'existence d'un PCA récemment mis à jour a par ailleurs permis de déterminer rapidement les fonctions vitales de l'organisation et de prioriser la remédiation.

Les équipes ont rapidement décidé de procéder (fictivement) à **l'isolement des équipements contaminés** (débranchements des câbles réseaux, coupure wifi). Les communications depuis et vers Internet ont été coupées, en accord avec les responsables métiers et les machines chiffrées ont été mises en veille prolongée.

La réalisation d'une veille a permis la **rédaction d'éléments de langage** qui ont été définis par l'équipe de communication, en lien avec les équipes techniques et ont été diffusés via un communiqué de presse. La CNIL a été notifiée de l'exfiltration de données.

Enfin, le **non-paiement de la rançon** a permis de respecter la posture préalablement définie et en ligne avec les recommandations de l'ANSSI en la matière.

3.AXES D'AMÉLIORATION

Les **procédures dégradées prévues par l'organisation ne couvrent pas l'ensemble des activités de gestion de crise** (pas de messageries de secours, annuaires papiers non maintenus à jour, etc.). Il était ainsi difficile de contacter l'ensemble des salariés et de leur transmettre des informations et des consignes sur la situation.

Les prestataires/clients/filiales (simulés) n'ont pas été informés de la situation et se sont interrogés sur l'impact de l'attaque sur leurs services.

Si la présence de **sauvegardes hors ligne** a permis de restaurer une partie du système, celles-ci étaient néanmoins anciennes : certaines données ont été

perdues et certains SI ont dû être reconstruits. Dans la réalité, cela aurait généré un rallongement du délai de reprise des activités (une dizaine de jours environ).

La décision de reconstruire une grande partie du SI n'a pas posé de problème sur la partie chaîne de production du second site ; en revanche, **la perte totale des bases de données clients et des applications associées** (simulée) constitue un dommage majeur dont la décision n'a pas fait l'objet d'une alerte significative auprès de la cellule de crise décisionnelle, ce qui aurait permis de communiquer au plus haut niveau en direction des métiers.

Enfin, la **notification de l'attaque à l'assureur** ne faisait pas partie des objectifs mais a été évoquée par les joueurs de la cellule de crise, notamment dans le cadre de la couverture de la perte d'exploitation et de **l'assistance juridique**, qui aurait été fortement appréciée. Il conviendrait de préparer une session d'information à l'attention des membres des cellules de crise (site principal comme site secondaire) sur cette **police d'assurance spécifique** et de tester la procédure associée lors d'un prochain exercice.

4.RÉCAPITULATIF DU PLAN D'ACTION

THÉMATIQUE/ACTION	RESPONSABLE	PRIORITÉ
CRÉATION/CORRECTION/AMÉLIORATION DES PROCÉDURES « RÉFLEXES »		
Lancer une campagne de création/mise à jour des fiches « réflexes » en cas de rançongiciel : mise hors ligne des sauvegardes, analyse des journaux, mise en place de nouvelles règles sur le pare-feu, interdiction d'utilisation de supports amovibles, etc.	RSSI	P2
CORRECTION/AMÉLIORATION DES PROCÉDURES DE GESTION DE CRISE ET DE CONTINUITÉ D'ACTIVITÉ (GESTION DES ACTIVITÉS EN MODE DÉGRADÉ)		
Se doter d'outils permettant de communiquer à l'ensemble des salariés en mode dégradé	Responsable PCA	P2

THÉMATIQUE/ACTION	RESPONSABLE	PRIORITÉ
CORRECTION/AMÉLIORATION DES RÉFLEXES DE LA CELLULE DE CRISE DÉCISIONNELLE		
Réviser la police d'assurance cyber en cas de sinistre (assistance juridique et couverture financière du préjudice matériel, immatériel, relatif aux sanctions, etc.), prévoir une session de formation des membres de la cellule de crise et inclure la procédure associée au prochain exercice	Responsable juridique	P1
Améliorer la remontée d'informations vers la cellule de crise décisionnelle en mettant en avant les points nécessitants un arbitrage urgent et de haut niveau.	Responsable PCA + RSSI	P2
CORRECTION/AMÉLIORATION DES PROCÉDURES DE COMMUNICATION DE CRISE		
Réaliser une cartographie des publics et des objectifs de communication associés : salariés, clients, partenaires, autorités, grand public/ médias.	COM	P1
Réaliser une cartographie des parties prenantes de la communication avec lesquelles se coordonner : prestataires, filiales, autorités, etc.	COM	P2
CORRECTION/AMÉLIORATION DES MESURES PRÉVENTIVES DE SSI		
Sauvegarde Augmenter la fréquence des sauvegardes hors ligne ; amélioration de l'architecture de sauvegarde.	RSSI	P1

FICHE PRATIQUE 11 : PRODUIRE UN RETEX

THÉMATIQUE/ACTION	RESPONSABLE	PRIORITÉ
CORRECTION/AMÉLIORATION DES MESURES PRÉVENTIVES DE SSI		
Campagne d'audits **Audit sur le site principal :** ▸ cloisonnement spécifique des équipements réservés aux administrateurs ou aux fonctions d'administration ; ▸ gestion des droits. **Audit sur le second site :** ▸ dispositif de filtrage pour cloisonner différentes zones réseaux (serveurs internes/serveurs exposés sur Internet, postes de travail utilisateurs/administrateurs) ; ▸ gestion des droits ; ▸ maîtrise des accès Internet (analyse des relais applicatifs, des passerelles).	RSSI	P1
Sensibilisation des collaborateurs Formation/sensibilisation : renforcer certains réflexes chez les collaborateurs en les invitant à signaler au service informatique de l'organisation tout élément suspect (pièce-jointe ou mail douteux, clé USB offerte, requêtes inhabituelles, etc.)[18]. Inclure les équipes informatiques et notamment les administrateurs très ciblés.	COM + RSSI	P1

Recommandation

Il convient d'indiquer un délai de réalisation pour chaque élément du plan d'action et de joindre au RETEX tout élément de traçabilité.

18 : Pour créer des ressources pédagogiques, consultez notamment les sites de l'ANSSI (www.ssi.gouv.fr) et de CYBERMALVEILLANCE (www.cybermalveillance.gouv.fr).

CONCLUSION

Un premier exercice de crise cyber permet de sensibiliser un grand nombre d'acteurs autour des problématiques de SSI et de les faire progresser sur des postures de gestion de crise cyber.

La préparation d'un tel exercice est un levier pédagogique et l'exercice en lui-même constitue un atout pour permettre ou poursuivre la mise en œuvre de mesures et de projets liés à la SSI au sein de votre organisation.

Un exercice de gestion de crise cyber se construit comme un projet et crée un grand nombre d'opportunités à la fois pour les personnes qui le préparent, celles qui y participent et celles qui sont ensuite impliquées dans la mise en place des axes d'amélioration identifiés.

L'organisation régulière d'exercices de gestion de crise cyber (un par an ou un tous les deux ans), accompagnée de formations plus théoriques, permet une montée en compétence et un gain d'efficacité dans la gestion des cas réels, à travers notamment la maîtrise de réflexes fondamentaux tels que la qualification de la situation, le partage d'informations aux bonnes personnes et l'établissement rapide d'un état des connaissances de l'évènement.

L'entraînement à la gestion de crise revêt aussi un aspect humain, et donc comportemental, crucial : la gestion du stress et la prise de décision individuelle puis collective en situation complexe s'apprend et se perfectionne.

Se préparer à la gestion d'une crise cyber et communiquer sur cette préparation constitue un vecteur de confiance interne et externe.

Vous disposez à présent des éléments pour convaincre le plus grand nombre que les exercices n'ont pas pour vocation de « sanctionner » ou de « contrôler » mais d'élever le niveau de compétences de ceux qui s'entraînent.

ANNEXE 1 :

LISTE DES LIVRABLES À PRODUIRE POUR L'EXERCICE

RECOMMANDATIONS PRÉALABLES :
POSITIONNER SA RÉSILIENCE CYBER AU PLUS HAUT NIVEAU

- Stratégie d'exercices (optionnel)
- Programme d'exercices (optionnel)
- Plan de communication

ÉTAPE 1 :
PENSER SON EXERCICE

- Cahier des charges
- Calendrier du projet

ÉTAPE 2 :
PRÉPARER SON EXERCICE

- Scénario
- Chronogramme
- Annuaires
- Dossier de mise en situation
- Fiche d'observation
- Briefings animateurs et joueurs

ÉTAPE 3 :
DÉROULER SON EXERCICE

- Aucun livrable

ÉTAPE 4 :
TIRER LES ENSEIGNEMENTS DE SON EXERCICE

- Compte-rendu du RETEX à chaud
- Compte-rendu du RETEX à froid
- Plan d'action

ANNEXE 2 :

GLOSSAIRE

ANIMATEUR : anime l'exercice, en interagissant avec les joueurs par la simulation d'actions visant à entraîner et tester leurs réactions en situation de crise. Un animateur peut jouer plusieurs rôles différents.

CELLULE D'ANIMATION : groupe de personnes dits « animateurs » simulant des personnes existant dans la réalité, qui ne participent pas à l'exercice, et avec lesquelles les joueurs ont des interactions dans le cadre de la gestion de la crise.

CHRONOGRAMME : prend la forme d'un tableau qui, ligne par ligne, décrit tout le déroulement chronologique de l'exercice du DEBEX au FINEX. Il précise également les modalités de transmission des « stimuli » (mail, appel téléphonique, SMS, etc.) et les réactions attendues des joueurs afin de définir et de cadrer les actions directement jouées par les joueurs et celles simulées par l'équipe d'animation.

CONVENTIONS D'EXERCICE : règles de jeu encadrant l'exercice (par exemple, l'interdiction pour les joueurs d'utiliser tel moyen de communication devenu indisponible ou le fait de leur indiquer, sans leur en donner la preuve, que les éléments exfiltrés appartiennent bien à leur organisation).

DIRECTEUR D'ANIMATION (DIR-ANIM) : chef d'orchestre de la cellule d'animation, il s'assure que chaque animateur joue ses rôles et que les joueurs comprennent bien les informations qu'ils reçoivent. Il interagit pour cela avec les observateurs qui peuvent lui faire remonter toute réaction imprévue ou incompréhension des joueurs.

DIRECTEUR D'EXERCICE (DIREX) : valide les orientations de l'exercice et chaque étape d'avancement. Il peut être le commanditaire de l'exercice.

DOSSIER DE MISE EN SITUATION (DMS) : document synthétique présentant aux joueurs l'état du monde au début de l'exercice. Il permet d'inscrire la situation que vont vivre les joueurs dans un contexte plus précis

EXPERT : contribue à la construction et au réalisme du scénario en y apportant son expertise sur une thématique particulière ou sur l'historique de son organisation.

GROUPE PROJET : groupe de personnes en charge de l'élaboration de l'exercice.

JOUEUR : participe à l'exercice en réagissant aux différents événements simulés. Il est issu des différents métiers de l'organisation qui seraient impliqués dans le dispositif de gestion de crise s'il s'agissait d'une situation réelle.

OBSERVATEUR : chargé d'observer le fonctionnement de l'exercice et de prendre note des points positifs et des axes d'amélioration. Il n'intervient pas dans le déroulement de l'exercice. Idéalement formé (même brièvement) à la gestion de crise cyber en amont de l'exercice, il possède une bonne connaissance du fonctionnement de l'organisation.

PLAN DE CONTINUITÉ D'ACTIVITÉ (PCA)[19] : a pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il doit permettre à l'organisation de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image…) et de tenir ses objectifs.

PLAN DE REPRISE D'ACTIVITÉ (PRA)[20] : constitue l'ensemble des procédures documentées d'une organisation lui permettant de rétablir et de reprendre ses activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident.

PLANIFICATEUR : membre du groupe projet, il participe à la construction de l'exercice. Le jour J, il est soit animateur, soit observateur.

19 : Guide pour réaliser un plan de continuité d'activité (SGDSN, 2013)
20 : Norme ISO 22301, Sécurité sociétale — Systèmes de management de la continuité d'activité, clause 8.4.5 Reprise

ANNEXE 2 :

GLOSSAIRE

POINT DE SITUATION : prend généralement la forme d'une synthèse écrite visant à informer les parties prenantes et les décideurs sur l'état de compréhension d'un incident, de ses impacts et de l'avancée des opérations de remédiation.

PROGRAMME D'EXERCICES : plan pluriannuel cadençant plusieurs exercices de gestion de crise sur différentes thématiques permettant de former et entraîner de manière progressive le plus large spectre possible de personnes au sein de son organisation, en accord avec la stratégie d'exercice.

RANÇONGICIEL[21] : contraction des mots « rançon » et « logiciel », un rançongiciel est par définition un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Pour y parvenir, le rançongiciel empêche l'utilisateur d'accéder à ses données en les chiffrant, puis lui indique les instructions utiles au paiement de la rançon en échange de la restitution de ses données.

RETOUR D'EXPÉRIENCE (RETEX) : temps collectif (tour de table) et/ou individuel (entretien) au cours duquel l'ensemble des participants s'exprime sur son expérience durant l'exercice.

SCÉNARIO : raconte l'histoire de l'exercice de manière littéraire, constitue une description de l'ensemble de la situation de crise qui touche l'organisation.

STIMULUS (STIMULI AU PLURIEL) : information envoyée par la cellule d'animation et reçue par les joueurs. Un stimulus est une pièce du scénario utilisée pour orienter les actions des joueurs. Il prend principalement la forme d'un mail ou d'un appel téléphonique. L'ensemble des stimuli forme le chronogramme.

STRATÉGIE D'EXERCICES : outil permettant de mettre en valeur les exercices organisés auprès des parties prenantes de son organisation et de structurer l'entrainement de manière à contribuer l'amélioration de sa résilience.

21 : www.ssi.gouv.fr/particulier/glossaire/r

ANNEXE 3 :

RESSOURCES UTILES

SGDSN

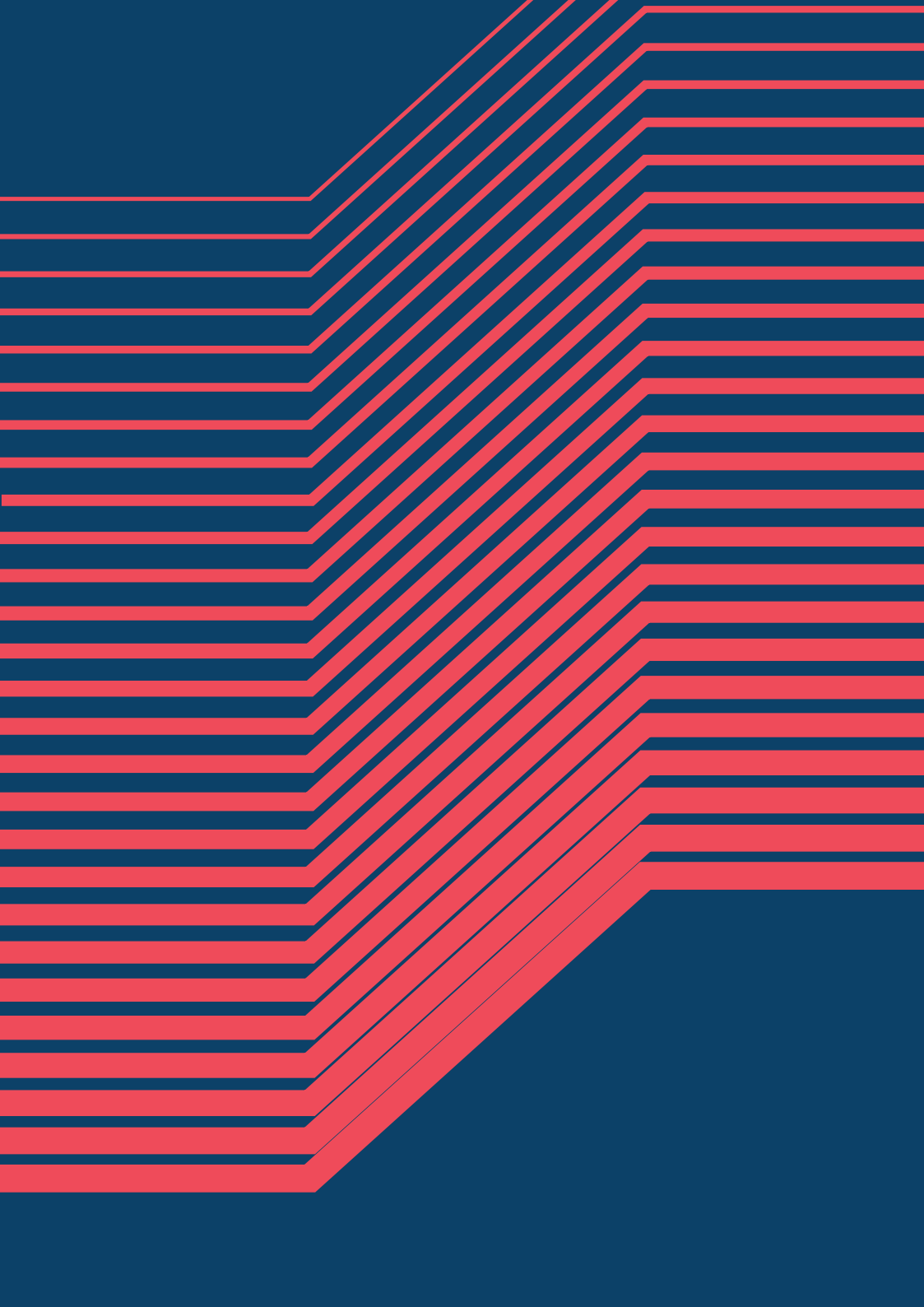
- *Guide pour réaliser un plan de continuité d'activité*, 2013.

ANSSI

- *Attaques par rançongiciels, tous concernés comment les anticiper et réagir en cas d'incident ?*, 2020 : www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident
- *EBIOS Risk Manager, 2018* : www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager
- *État de la menace rançongiciel à l'encontre des entreprises et institutions*, 2020 : www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001
- Site du CERT-FR, rubrique « menaces et incidents » : www.cert.ssi.gouv.fr/cti
- Déclarer un incident sur le site de l'ANSSI : www.ssi.gouv.fr/en-cas-dincident
- Plaquette « *Alerte aux rançongiciels* » : www.ssi.gouv.fr/actualite/ne-soyez-plus-otage-des-rancongiciels/

CYBERMALVEILLANCE.GOUV.FR

- Assistance en cas d'incident : www.cybermalveillance.gouv.fr/diagnostic
- Que faire en cas d'attaque par rançongiciel : www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares



COLLECTION
GESTION DE CRISE CYBER

« En matière de protection des systèmes d'information, l'anticipation est la clé. En s'entraînant, les équipes impliquées dans la gestion de crise développent, exercice après exercice, des réflexes et des méthodes pour mieux travailler ensemble. Lorsqu'une attaque survient, elles sont alors prêtes à y faire face. »

Guillaume Poupard, directeur général de l'ANSSI

Les crises cyber peuvent être dévastatrices : il ne faut surtout pas attendre la catastrophe pour apprendre à en maîtriser les rouages !

Réalisé en partenariat avec le Club de la continuité d'activité et fruit d'une riche expérience dans l'organisation d'exercices de gestion de crise cyber, ce guide vous accompagnera dans la mise en place de vos propres entraînements.

Version 1.0 – Octobre 2020 – **ANSSI-PA-081**

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr