ORGANISER UN EXERCICE DE GESTION DE CRISE CYBER

Un guide coréalisé par l'ANSSI et le CCA

Sommaire

I. Aux origines du guide

Le partenariat ANSSI-CCA : complémentarité et croisement des expertises autour de la résilience

Crises d'origine cyber aux enjeux transverses = Nécessité de se préparer et s'entrainer pour gagner en résilience

+

Si les experts de la sécurité numérique et de la continuité d'activité s'emparent de la question, les faire **parler d'une même voix** pour porter un message commun est essentiel.

Le guide « exercice » : une approche pour les praticiens

OBJECTIF

Accompagner les organisations de toutes tailles depuis la stratégie d'exercices cyber jusqu'à la conception et la mise en œuvre de l'exercice

CIBLES

Dirigeants

Directeur cyber / sûreté / sécurité

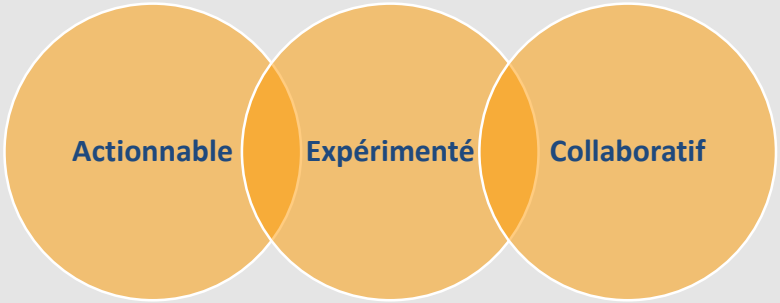
Risk managers, Responsable PCA

CISO / RSSI / DSI

FONDAMENTAUX

- Des fiches pratiques au fil de l'eau qui, mises bout à bout, composent un **exercice cyber clé en main**
- Un « **fil rouge** » pour une mise en pratique concrète
- Des étapes **indépendantes** pour une **prise en main facilitée**
- Un accompagnement pour faciliter la **valorisation** de son exercice cyber

VALEURS



II. Présentation de la version finale du guide

Structure du guide

Recommandations préalables :

Comprendre les spécificités du cyber et inscrire l'exercice dans une réflexion globale de résilience

Etape 1 : concevoir son exercice	Etape 2 : préparer son exercice	Etape 3 : dérouler son exercice	Etape 4 : tirer les enseignements de son exercice
Cadrer l'exercice et définir ainsi les objectifs, le type, le périmètre, les participants et la date	Définir un scénario crédible, rédiger un chronogramme, briefer les animateurs et les observateurs	Exécuter l'exercice en s'adaptant aux réactions des joueurs	Identifier les points forts et les axes d'amélioration ; établir un plan d'action

Un guide « prêt à l'emploi »

Sur le fond et sur la forme

RÉCAP' ÉTAPE 2

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.

ÉTAPE 2

PRÉPARER SON EXERCICE

LIVRABLES À PRODUIRE AU COURS DE CETTE ÉTAPE :

- 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 :

COMPRENDRE LES SPÉCIFICITÉS DU CYBER

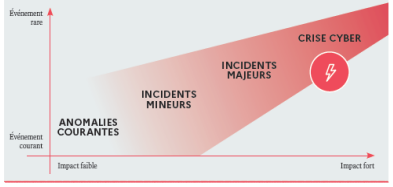
Qu'est-ce qu'une crise cyber ?

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 ~~ainsi que~~ 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



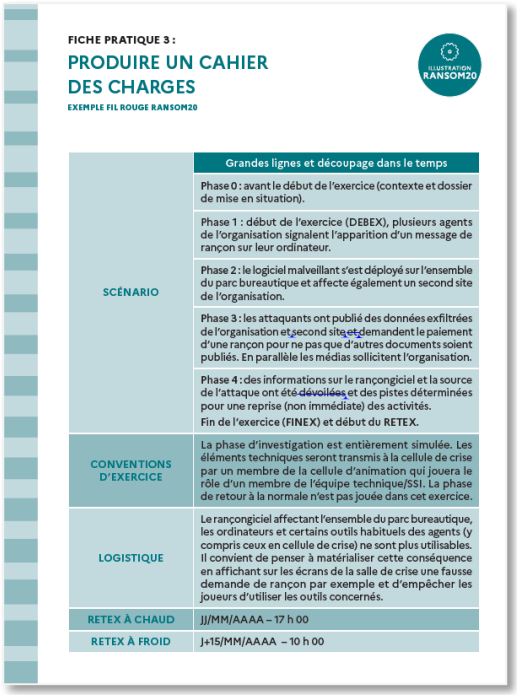
3 : Pour plus d'informations sur la méthodologie d'analyse de risques, se référer à la méthode EBIOS Risk Manager (ANSSI, 2018) - https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

CARACTÉRISTIQUES DES CRISES D'ORIGINE CYBER :

- **la fulgurance et l'ubiquité des impacts :** une organisation peut être touchée à de multiples endroits simultanément ;
- **l'incertitude, potentiellement durable, liée au domaine :** les impacts sont difficiles à estimer et l'objectif de l'attaquant pas toujours identifiable facilement ;
- **l'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 ;
- **la technicité du sujet :** La complexité des SI et des modes opératoires utilisés par les attaquants, ~~L~~es 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 ;
- **la 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 ;
- **l'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 ;
- **la 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 ;

Un guide « prêt à l'emploi »

Focus sur les fiches pratiques et le chronogramme

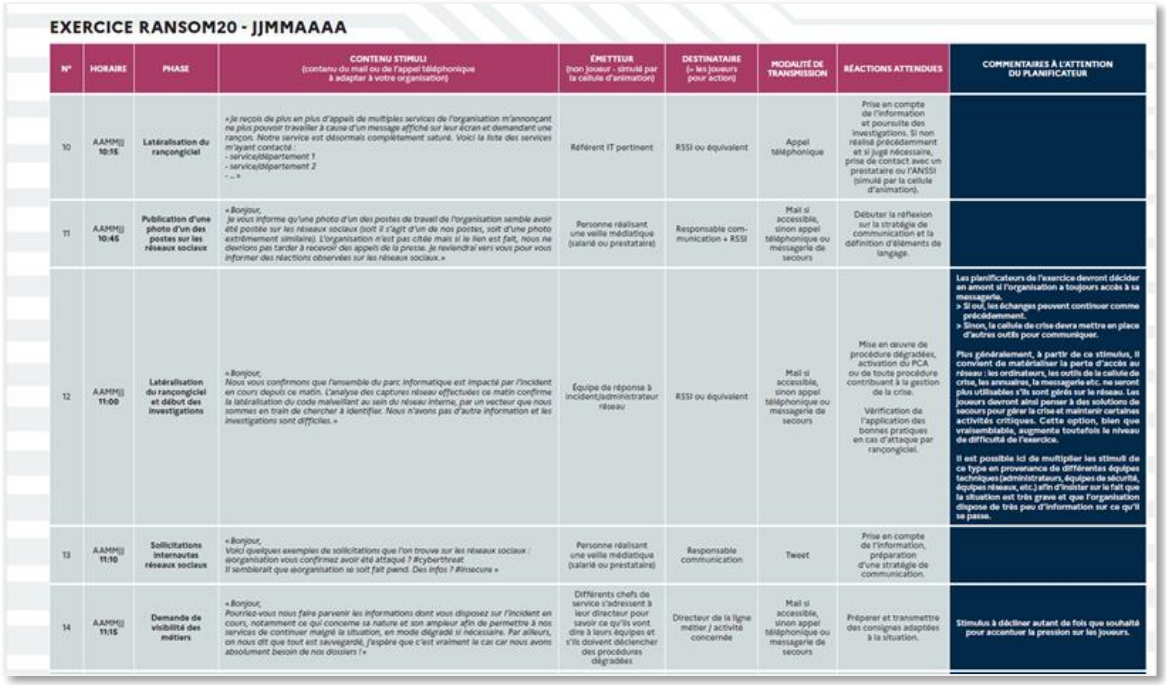


FICHE PRATIQUE 3 :

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 second site et 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 dévoilées 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



EXERCICE RANSOM20 - JJMMAAAA

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

Un guide « prêt à l'emploi »

Le choix d'un « fil rouge »

Le fil rouge : RANSOM20

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

Afin de pouvoir être utilisé et adapté par le plus grand nombre, nous avons choisi comme exemple d'exercice une cyberattaque par rançongiciel. Au moment où nous rédigeons ce guide, ce mode opératoire constitue une tendance qui s'intensifie et qui touche les grandes organisations comme les plus petites. Cet exercice est nommé **RANSOM20**.

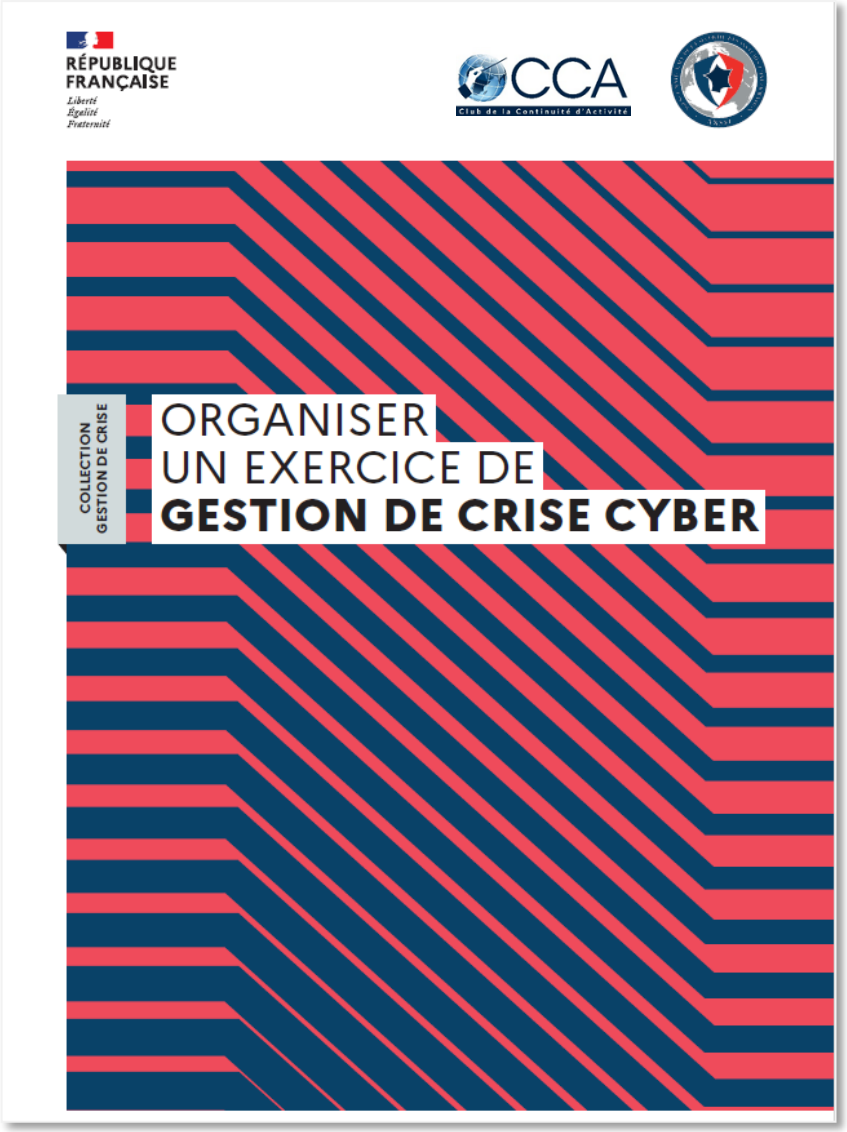
Cet exemple est développé dans différentes fiches pratiques qui, une fois compilées, forment un exercice complet réutilisable par toute organisation. Il est notamment disponible sous forme de tableur (*voir fiche pratique n° 6*).

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

III. Publication & plan de communication

Publication du guide : 14 octobre 2020

Traduction dans la foulée



Proposition d'un plan de communication

Date	ANSSI	CCA
8/9 octobre 2020	Mention du guide en interne ANSSI	
12 octobre 2020	Mention du guide dans le communiqué de presse ANSSI dédié aux Assises	Communiqué interne sur la prochaine sortie du guide
14 octobre 2020	**Publication (web) soutenue par la mention du guide dans la *keynote* de Guillaume Poupard aux Assises de la sécurité de Monaco.** **Publication relayée sur les réseaux sociaux ANSSI**	**Relais par le CCA de la communication ANSSI et communication en propre par le CCA**
Mi – novembre 2020	Version imprimée du guide	Lot de la version imprimée du guide
Au long court	Valorisation régulière via les réseaux sociaux et les interventions	Valorisation régulière via les réseaux sociaux et les interventions + webinaire

Promouvoir le guide via un webinaire

Courant décembre 2020

D'abord adressé aux membres du CCA, il **permettra de présenter le contenu détaillé du guide**, voire de proposer une mise en pratique.

Merci de votre attention.
Des questions ?