RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

TLP WHITE

REMPAR 2022

GENESE ET ENSEIGNEMENTS DU PREMIER EXERCICE CYBER MASSIVEMENT DISTRIBUE

CCA Club de la Continuité d'Activité

CAMPUS CYBER

Table des matières

REMPAR22 : une première en France

En décembre 2022, l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI), le Club de la Continuité d'Activité (CCA) et le Campus Cyber ont organisé le premier exercice de crise cyber à large ampleur en France. Durant l'ensemble de la journée, près de 550 personnes provenant de plus de 100 entités de plusieurs secteurs d'activités ont été invitées à réagir aux impacts d'une crise d'origine cyber, qui simulait l'arrêt des activités de leur organisation suite à des cyberattaques sur des fournisseurs de services numériques, conduisant à des impacts dans de multiples secteurs et pour de nombreux acteurs (*blackout* numérique).

Cette expérience unique a donné lieu à de nombreux enseignements, formalisés au sein de ce rapport. Par ailleurs, ce document propose des éléments sur l'organisation de cet exercice ainsi que les opportunités qu'il a représenté pour les organisations participantes.

Retour sur un exercice d'un genre nouveau

Une ambition commune : adresser le sujet de la résilience numérique avec l'écosystème français

Le renforcement de la menace cyber met aujourd'hui au défi les organisations à assurer la continuité de leurs activités dans le cas où elles seraient victime d'une cyberattaque d'ampleur.

Ce phénomène, doublé à la forte dépendance des entités aux logiciels et outils numériques externes, invite les organisations à questionner leurs capacités de fonctionnement avec des perturbations majeurs de ces services pouvant aller jusqu'à une indisponibilité durable et de partager ensemble leur expérience.

Cette ambition se déclinait en 5 objectifs complémentaires :

- O1 - Sensibiliser aux enjeux de continuité d'activité face au risque de *blackout* numérique ;
- O2 - Tester les dispositifs de gestion de crise afin de s'assurer de la prise en compte des spécificités des cyber attaques ;
- O3 - Entrainer la coordination des acteurs entre eux et au sein d'un même secteur ;
- O4 - Travailler les modalités de communication de crise en interne et en externe ;
- O5 - Créer des dynamiques de partage et d'échange entre les communautés et les secteurs.

Un scénario commun , adaptable par chacun

Pour appuyer ces objectifs, un scénario commun a été mis à disposition. Il proposait un axe d'attaque par « *supply chain* », via la compromission d'un fournisseur de service numérique, qui pouvait aboutir à une attaque du SI interne de l'organisation.

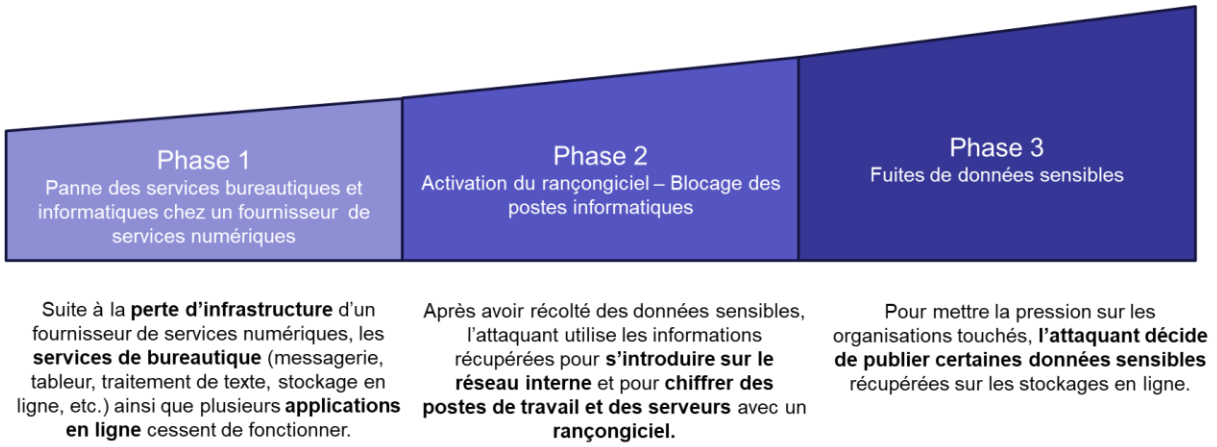

Figure 1. Le scénario de l'exercice

Ce scénario a par ailleurs été décliné selon les spécificités de 5 secteurs distincts, pour permettre d'y intégrer les enjeux métiers des équipes engagées :

Figure 2. Les secteurs ciblés dans le scénario de l'exercice

« La mise à disposition d'un scenario générique personnalisable a constitué un atout essentiel pour notre organisation, en offrant les avantages de :

- *se sentir appartenir à un collectif ;*
- *s'assurer de la pertinence du type d'attaque retenu par rapport aux menaces actuelles ;*
- *gagner du temps dans les différentes phase de préparation de l'exercice, et surtout de pouvoir le décliner en le rejouant au cours de l'année avec de nouvelles équipes ;*
- *évaluer son niveau de maturité sur le champ de la résilience cyber et mettre en place des actions et solutions adaptées aux vulnérabilités de l'entreprise. »*

- Une entreprise du secteur public

Deux modalités de jeu pour permettre à tous de participer

Pour permettre d'embarquer un large écosystème tout en prenant en compte les différentes de maturités des organisations, l'exercice REMPAR22 a été décliné sous deux formats :

- **Un moment pour jouer en tant qu'organisation :** Le matin, une trentaine d'organisations ont joué au sein de leurs entités un scénario adapté à leurs spécificités sectorielles. Cette séquence a permis à ces dernières de tester les dispositifs de gestion de crise interne afin de s'assurer de la prise en compte des spécificités des cyberattaques et d'entrainer à la coordination des acteurs.
- **Un moment pour jouer en tant qu'individu :** L'après-midi, 200 participants - experts du cyber et de la crise mais aussi des métiers et dirigeants - issus d'environ 70 entités (privées et publiques) ont armé les cellules de crise d'une entreprise fictive, réunies dans un même lieu, le Campus Cyber. 5 filiales ont organisé leurs cellules de crise métiers avec l'objectif de créer des dynamiques de partage. Des complices ont animé l'exercice au sein de chaque cellule, s'appuyant sur une animation centrale. C'est près de 70%

d'acteurs hors des filières IT et cyber qui ont été réunis pour travailler ensemble sur l'exercice.

Une préparation rapprochée pour aider toutes les organisations à participer selon leurs capacités propres

Afin de simplifier la construction et l'adaptation de l'exercice pour les organisations, l'équipe organisatrice a mis à disposition un kit de préparation (chronogramme, dossier de mise en situation, exemple de stimuli médiatique) et a organisé de septembre à novembre des ateliers communs et individuels pour s'approprier le contenu et accompagner la préparation de l'exercice. Les organisations joueuses avaient également la possibilité d'utiliser un outil numérique d'organisation d'exercice de crise mis à leur disposition afin de faciliter la création et l'envoi de leurs stimuli.

Atelier 1	Atelier 2	Atelier 3	Atelier 4	Atelier 5
Scenario et adaptation	**Outillage d'exercice**	**Animation de l'exercice**	**Organisation du RETEX**	**Briefing des joueurs**

Figure 3. Organisation des ateliers de préparation de l'exercice

« En choisissant de participer à cet exercice, notre organisation a notamment bénéficié d'un accompagnement partiel de l'ANSSI et du CCA. L'usage de la solution numérique d'organisation d'exercice de crise nous a également convaincu de l'utilité d'une telle plateforme pour faciliter l'animation d'exercices multi-joueurs. »

« Le scénario générique proposé a permis de sortir de notre zone de confort. Il a ici été décidé de faire jouer les participants au sein d'une entreprise fictive, notamment parce que l'organisation ne disposait pas d'infrastructure externalisée mais que le sujet nous intéressait fortement.

L'exercice a en particulier permis d'éprouver notre réactivité sur l'aspect organisationnel de gestion de crise. Il a été décidé a postériori de renforcer les actions de sensibilisation sur l'organisation de crise, notamment via des réunions de présentation et d'échanges mentionnant les ressources à utiliser, les rôles à pourvoir, les correspondants à contacter et les éléments de langage de base à communiquer. »

Une administration centrale

De nombreuses leçons pour appuyer le développement de la gestion de crise cyber en France

Au travers l'exercice et de la conférence de clôture, un ensemble de leçons a été présenté sur la gestion des crises d'origine cyber et sur la résilience des organisations face à ce type de menaces.

Des retours d'expériences riches en enseignements

Les éléments des organisations obtenus directement après l'exercice, lors d'une séance d'échange et via des sondages partagés auprès des planificateurs et des joueurs, ont permis d'identifier des retours d'expérience complets avec des lignes communes entre les organisations.

Tout d'abord, l'exercice a été un franc succès via la mobilisation d'un panel diversifié de participants (équipes cybersécurité, informatique, communicants, équipes opérationnelles, juristes, décideurs). L'ensemble de ces publics a saisi l'importance de la menace cyber et des matérialisations des effets des cyberattaques. D'autres part, la remontée des alertes d'incidents et la coordination des acteurs en interne sur la gestion de crise est également un

sujet maitrisé. Pour plusieurs organisations, l'échange d'information avec les autorités cyber et sectoriels (simulées dans l'exercice) a été proactif et important.

Sur les trois thématiques principales de l'exercice, des éléments plus complets sont mis en valeur ci-dessous :

- **Sur la continuité d'activité :**
  - L'exercice a permis **de sensibiliser** aux impacts d'un *black-out* numérique ;
  - La première phase de crise (analyse de la situation/investigations) **reste la plus complexe** à gérer tant en interne qu'en externe ;
  - **Des outils de communication résilients** sont aujourd'hui manquants pour pallier aux impacts d'un black-out et doivent être identifiés au sein des organisations ;
  - L'exercice a mis à l'épreuve les plans de continuité d'activité (PCA), qui **doivent mieux prendre en compte le volet cyber** et préciser les dépendances aux systèmes d'information en particulier sur le supply chain (prestataire, sous-traitants etc.).
- Sur la **coordination** et le **partage d'informations** :
  - Les discussions avec les équipes IT/Cyber et métiers sont **parfois trop limitées, ce qui peut nuire à** la compréhension de la crise et à la mise en place d'un plan d'actions efficace
  - **La coordination avec les prestataires/fournisseurs** doit être améliorée pour répondre aux enjeux de black-out numérique. Il faut penser cette coordination en amont, pour la rendre efficace en cas de crise.
- Sur la **communication de crise** :
  - La communication de crise en interne est de mieux en mieux maitrisée, notamment avec les crises connues ces dernières années (COVID).

« Pour cet exercice, nous avons en particulier souhaité rendre concret la coupure des outils collaboratifs. Nous avons donc demandé à la cellule de crise et à la DSI de basculer sur une solution alternative pendant toute la durée du jeu. Cela a permis de mieux appréhender les impacts d'un black-out numérique et de tirer de riches enseignements sur la stratégie de redondance de nos outils collaboratifs et de messagerie. Par ailleurs l'exercice a permis aux joueurs de mieux s'approprier le dispositif interne et de prendre conscience qu'il faut mieux se préparer. »

Une entreprise du secteur de l'assurance

L'organisation d'une conférence de clôture pour compléter le panorama des enseignements

Afin de partager les enseignements de l'exercice, une conférence de retour d'expérience (RETEX) a été organisée, ainsi que pour engager les participants à partager leurs propres perspectives sur l'exercice. Cette conférence réunissant plus de 150 personnes a permis à plusieurs experts d'intervenir sur plusieurs table rondes pour approfondir certaines thématiques de l'exercice avec un regard croisé :

- La communication de crise cyber ;
- Les investigations et la judiciarisation ;
- Continuité d'activité et fournisseurs de services numérique.

Communication de crise cyber

RETEX de l'exercice

- ✓ **La mise en place d'une stratégie de communication de crise a été bien assurée** pendant l'exercice, avec par exemple une veille médiatique efficace et une identification des parties prenantes.
- ✓ Dans les simulations, **la communication vers l'extérieur a été menée avec beaucoup de prudence**, en raison du flou concernant la situation cyber.
- ✓ **La question de l'opérationnalité des moyens de communication** a été abordée, dans le contexte de black-out numérique.

Conclusions de la table ronde

- ✓ La communication dans le cadre d'une gestion de crise **doit faire l'objet d'une véritable stratégie** : il est en effet nécessaire de communiquer en fonctions des parties prenantes (directes ou indirectes).
- ✓ Il est important de travailler à ce que **les communicants et les équipes des services informatique travaillent de manière conjointe**, en faisant le lien entre l'hyper-technicité du sujet et la pédagogie nécessaire à sa compréhension.
- ✓ La **préparation en amont de crise**, tant **en termes de procédures que d'outillage** est indispensable en cas de crise.

Investigation et judiciarisation

RETEX de l'exercice

- ✓ L'exercice ne ciblait la réalisation investigations techniques mais il a amené les équipes a à réfléchir sur la manière dont elles auraient à construire leur stratégie d'investigation en cas d'indisponibilité des outils numériques.
- ✓ La question de la judiciarisation de l'attaque et de la coopération avec les autorités se pose encore peu lors de la première phase de crise, mais reste une question importante pour les entreprises à clarifier, notamment sur le process du dépôt de plainte.

Conclusions de la table ronde

- ✓ Les investigations doivent intervenir rapidement, car les journaux peuvent être amenés à disparaitre. Les processus de déclenchement de collectes de journaux peuvent être anticipé en amont de la crise.
- ✓ L'action judiciaire est généralement menée de manière plus tardive, l'enjeu premier étant de contenir l'incident. Il est possible d'ouvrir une cellule de crise dédiée sur les aspects juridiques pour s'assurer de leur prise en compte dès le début de la crise.
- ✓ Le dépôt de plainte est un élément important dans la crise, car il permet de porter à la connaissance à l'autorité judiciaire d'un délit cyber et d'en trouver les auteurs.
- ✓ Il est important de prendre en compte les enjeux sur la réglementation nationales spécifiques, qui peuvent varier selon les pays.

Continuité d'activité et fournisseurs de services numérique

RETEX de l'exercice

- ✓ La qualification des impacts doit se faire en lien avec les métiers pour aider à prioriser les actions de remédiation. Toutefois, le manque de maitrise/connaissance des SI peut compliquer la gestion de la continuité d'activité, notamment en l'absence d'une cartographie indiquant les liens entre applications métiers et infrastructure.
- ✓ La stratégie de remédiation peut entrainer des impacts et ralentir la reprise d'activité, une posture adaptée doit être prise entre reprendre rapidement et reprendre « bien ».
- ✓ Dans un scénario de black-out, il reste difficile d'estimer les impacts externes pour les clients.
- ✓ Les logiciels/solutions alternatifs doivent continuer à être identifiés pour assurer la conduite des activités. Il en est de même pour les capacités de repli des SI sur un autre site ou chez des fournisseurs.

Conclusions de la table ronde

- ✓ Les exercices de crises sont des moments intéressants pour faire réfléchir les équipes métiers et informatiques ensemble sur les conséquences de la perte d'un fournisseur. Ils permettent notamment d'ouvrir une phase d'embarquement sur le sujet de la continuité informatique, qui pourra être ensuite travaillé de manière itérative par des BIA, des PCAs, des procédures, et d'autres documents d'opérationnalisation de la réponse.
- ✓ Il est important d'assumer avec les acteurs de première ligne que l'organisation sera en mode dégradé et travailler sur le métier sur cet axe. Il n'est pas toujours possible d'avoir un backup à l'identique de disponible au moment de la crise– il est donc nécessaire dans ces cas d'apprendre à faire face sans moyens informatiques pendant plusieurs semaines, en travaillant avec les métiers sur des solutions pouvant être mise en place rapidement.
- ✓ Il est nécessaire de prévoir les outils de communication en amont des crises, en évitant que tous les systèmes d'information soient interdépendants ou dépendant sur un seul fournisseur. Les outils alternatifs doivent avoir été configurés et testés en amont, en réfléchissant à la portabilité et migration des données. Il est nécessaire que les outils soient en production afin de pouvoir réaliser une bascule rapide le jour de la crise.

Le GT « Crise et entrainement cyber » du Campus Cyber piloté par l'ANSSI, le CCA, l'AMRAE, le CDSE et le CESIN ainsi que les GT « Crise » et « Communication de Crise » du Club de Continuité d'Activité travaillent régulièrement sur ces problématiques et sur les outils permettant de mieux appréhender et gérer les crises d'origine cyber.

Une expérience de jeu positive

L'exercice REMPAR22 a été reçu très positivement par l'écosystème. La grande majorité des participants souhaitent aujourd'hui renouveler l'expérience dans une prochaine édition :

100 %

des organisations joueuses le matin souhaitent réitérer l'expérience

91 %

des joueurs présents l'après-midi souhaitent participer à nouveau à ce type d'exercice

La séquence REMPAR a également été l'opportunité d'organiser pour la première fois un exercice de crise cyber massifié au niveau national. Cette expérience permet d'identifier quelques points de retour d'expérience :

- La séquence évènementielle a permis de maximiser la mobilisation des joueurs – c'est donc un outil à utiliser pour engager son écosystème dans l'exercice.
- L'expérience de préparation d'exercice est utile en deux sens :
  - Elle offre aux organisations une possibilité d'évaluer leur niveau de préparation pour identifier les forces et axes d'amélioration sur lesquels travailler ;
  - La préparation de l'exercice sert également de phase de montée de capacités, les organisations profitant de l'exercice pour construire des procédures ou pour mettre en place des processus afin de les tester.
- L'ensemble des éléments de préparation mis à disposition et l'accompagnement offert permettent à des organisations de participer à un exercice de crise avec un effort de préparation réduit.
- L'accompagnement des organisations joueuses par un mentor est une réussite permet d'offrir un coussin de sécurité aux organisations moins matures et de renforcer la montée en compétence pendant la phase de préparation. Pour les organisateurs de l'exercice, l'accompagnement permet de mieux identifier les difficultés communes des organisations joueuses, et de réagir rapidement pour les surpasser.
- La préparation collective et le RETEX commun permettent d'engager des organisations dans une aventure commune, et maximisent la participation le jour de l'exercice. Elle permet également de créer des synergies entre acteurs d'un même secteur ou faisant face à des problématiques similaires.

« L'exercice REMPAR22 nous a séduit par sa pertinence (réalisme, qualité de la préparation). Nous avions décidé d'y participer au niveau France en impliquant les membres de nos cellules de crise managériale et opérationnelle. »

« La cellule managériale a été mobilisée dès 8h par un message indiquant un incident grave, dans lequel nous avons simulé la véracité de l'attaque quelques minutes, avant de révéler qu'il s'agissait d'un exercice. La cellule de crise opérationnelle a pris le relai sur le reste de l'exercice, avec une large mobilisation des joueurs, qui avaient uniquement été prévu de la tenue de la séquence, sans en connaitre les détails.

Les enseignements tirés de l'exercice ont déjà permis de formaliser 2 réunions de REX tandis qu'un plan d'action est en cours d'élaboration, avec une présentation est prévue au premier trimestre 2023 au Board français ».

Un cabinet de conseil

TLP WHITE

Avec la participation de l'Agence nationale de la sécurité des systèmes d'information, du Club de la Continuité d'Activité et du Campus Cyber,
Version 1.0 – Février 2023
Dépot légal : Février 2023

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.