Simulation de crise -24h dans la tempête

Antoine Boutet, Gaëtan Derache

Simulation de crise - 24h dans la tempête

Antoine Boutet
Insa-Lyon, Inria, CITI, Univ. Lyon
Lyon, France
antoine.boutet@insa-lyon.fr

Gaëtan Derache
CRISALEAD
Genève, Suisse
gaetan.derache@crisalead.ch

***Abstract*—L'accroissement des crises et cyber crises touchant les organisations publiques et privées, tant à l'échelle nationale qu'internationale, appelle la création d'une culture du management de crise et de la cybersécurité. Pour former les organisations à ce risque croissant et préparer les professionnels aux cyberattaques, nous avons expérimenté un exercice de gestion de crise alliant cyberattaques, attaques communicationnelles et atteintes à la réputation, attaques sur le corps métier et kidnapping. Afin de se rapprocher des conditions proches du réel, cet exercice s'est effectué de manière immersive sur 24 heures consécutives. Les 14 et 15 janvier derniers, des cellules constituées par des membres de la Chancellerie de Genève, par des assistants en informatique de gestion et des professionnels de tous horizons ont subi "24 heures dans la tempête". Ces cellules ont été confrontées à une crise majeure d'une entreprise dans le milieu financier. Le bilan de la simulation est extrêmement encourageant : les participants sont enrichis, transformés, renforcés. Après cette expérience positive, cette simulation est dorénavant mature et elle peut être réitérée à plus large échelle avec un nombre plus important de formations impliquées.**

***Index Terms*—Gestion de crise, Cyberattaques, Formation**

I. Introduction

Depuis 2018, on observe un accroissement spectaculaire des cyberattaques dans tous les secteurs d'activité. Les attaques par rançongiciels[1] ont par exemple été multipliées par quatre en 2020 et ont principalement ciblé des collectivités territoriales, des établissements de santé et des entreprises du secteur de l'industrie [1]. Les menaces stratégiques, l'espionnage et les attaques par chaîne d'approvisionnement constituent également les phénomènes les plus observés en 2020. La pandémie de Covid-19 a amplifié le phénomène. Les organisations de santé ont été plus ciblées et la surface d'attaque pour les entreprises a été élargie avec la mise en place de mesures de télétravail généralisé. Même les administrations publiques, qui n'imaginaient pas que leur patrimoine informationnel puisse être convoité, font partie des cibles potentielles [2].

Pour lutter contre ces menaces, il est nécessaire de former les organisations aux crises cybers. Bien qu'il soit possible d'enseigner la théorie de la gestion et de la communication de crise, c'est au coeur du danger que tout se joue. Pour bien se préparer à une cyberattaque, il faut dès lors s'entraîner dans des conditions aussi proches que possible du réel. Bien que les offres d'enseignement relatives à la sécurité des réseaux et des systèmes d'information commencent à prendre en compte ce besoin, en pratique les exercices de gestion de crise restent marginales [3], [4]. De plus, l'enseignement est souvent technique mais rarement interdisciplinaire. C'est notamment le cas des CTF[2] [5] qui constituent des activités d'entraînement récurrentes. Bien que ces exercices aient montré leur efficacité dans l'enseignement de la sécurité [6], [7], la mise en place d'exercices prenant en compte la vision holistique des cyberattaques et cyber crises permet de mieux préparer les professionnels de la sécurité.

C'est en partant de ce constat que la société CRISALEAD, la Haute Ecole de Gestion de Genève (HEG) et le groupe Insa ont mis en place une simulation de crise d'une durée de vingt-quatre heures consécutives. Un jour entier et une nuit entière dans les locaux de la HEG pour se mettre à la place des responsables d'une entreprise (une banque dans ce cas précis) qui subit une cyberattaque et d'autres déconvenues. Ainsi, vendredi 14 et samedi 15 janvier 2022, trois équipes de huit participants venus du monde de l'entreprise et des organisations publiques ont affronté les aléas d'un scénario économique et informatique qui les a volontairement bousculés. Le jeu de rôle était là pour former. Cohésion d'équipe, méthodes et outils pour garder son sang-froid, négociation et méthodologie: les compétences travaillées ont été nombreuses. Quand la fatigue, au coeur de la nuit, s'est faite sentir et qu'il a fallu être prêts et réactifs dans une conférence de presse avec des journalistes peu amènes, quand il a fallu gérer des clients qui paniquent, une demande de rançon, des données volées, un enlèvement... les participants et les participantes ont su puiser dans leurs réserves, rester lucides et définir une ligne de conduite. Chaque étape de leurs comportements et de leurs décisions, tout au long des vingt-quatre heures, a fait l'objet d'une évaluation de la part des experts présents. Un de ces derniers précise qu'il s'agit finalement de "vivre les difficultés, le stress et les contraintes qu'une crise d'origine informatique impose aux professionnels chargés de la gérer. Ce scénario pédagogique constitue un moyen sans égal de se préparer face aux risques de plus en plus grands de cyber attaques que les organisations connaissent ces dernières années".

[1]Un rançongiciel est un malware chiffrant les données se trouvant dans un système d'information. Les auteurs de l'attaque proposent ensuite une clé de déchiffrement aux victimes en échange d'une rançon, bien souvent payable en bitcoins donc impossible à tracer ou annuler une fois payée.

[2]Capture The Flag, exercices centrés sur l'apprentissage de la sécurité informatique où les joueurs doivent attaquer des programmes/systèmes volontairement vulnérables.

II. 24 HEURES DANS LA TEMPÊTE

S'il suffisait de quelques bons livres sur le management de crise et la gestion des cyberattaques, d'assister à quelques conférences pour créer une communauté de managers capables de protéger leur entreprise et leur patrimoine informationnel, les cyber pirates seraient faciles à neutraliser. Mais comme nous ne saurions apprendre à nager dans un livre, nous ne pouvons pas apprendre à gérer une crise ou une cyber crise en lisant. On doit se jeter à l'eau, pour finalement se maintenir à flot. La communauté des "nageurs" a bu des tasses avant de savoir nager ; la communauté des "managers capables de défendre leur entreprise en temps de crise" a dû en passer par les simulations de crise avant de savoir protéger leur organisation.

La simulation de crise présentée ici fait suite aux multiples expérimentations d'exercices de gestion de crise réalisées ces dernières années à l'Insa de Lyon [4] et à la HEG de Genève. Chaque année depuis 2018, une vingtaine d'étudiants de 5ème année du département informatique sont confrontés à un scénario de gestion de crise impliquant une clinique de santé, une ONG ou un industriel en difficulté sous le feu des critiques de toutes parts. Le succès de ces expérimentations exprimé par les feedbacks des étudiants nous a poussés à doubler les effectifs en invitant une formation d'étudiants de l'Insa Centre Val de Loire sur l'édition de 2021. Ces expérimentations avaient lieu sur la journée mais ne pouvaient pas déborder en dehors de l'emploi du temps officiel des étudiants. D'un autre côté, la HEG a organisé à deux reprises des exercices de gestion de crise sur 24 heures. L'organisation de ces exercices sur 24 heures ajoute une réelle immersion et accroît l'implication des participants.

C'est avec ces retours d'expérience que nous avons organisé cette simulation de crise qui se veut tirer parti du meilleur de chaque expérimentation, à savoir une immersion sur 24 heures où les participants sont acteurs à part entière, un scénario complet mettant en avant le côté holistique et complexe d'une crise, l'utilisation d'une plateforme Cyber pour ajouter un volet pratique avec de réelles attaques sur un système d'information virtuel, l'accompagnement des participants avec la mise en place d'une méthode de gestion de crise et une évaluation structurée.

A. *Objectif pédagogique*

D'un point de vue pédagogique, la simulation de crise est un vecteur qui permet de sensibiliser, de former l'individu au management de crise et de la cyber sécurité. Cet apprentissage de la gestion en terre inconnue est scénarisé, mis en scène et orchestré comme l'est une pièce de théâtre. Mais le participant à la simulation n'est pas spectateur ; il est l'acteur qui se met en jeu, s'expose et apprend in situ, sur lui-même, sur ses interactions avec les autres membres de la cellule de crise, sur sa capacité à affronter l'incertitude avec calme et méthode.

Nous mettons souvent en avant la vulnérabilité des systèmes d'information alors que le maillon faible de la sécurité, c'est généralement l'homme. Par méconnaissance des bonnes pratiques, pour aller plus vite ou simplement par paresse, l'employé est souvent la cause de situations critiques. Le mot de passe sur un Post It collé à l'écran de l'ordinateur, le port USB chargé de données sensibles qu'on laisse traîner sur le bureau, l'e-mail d'un expéditeur inconnu que l'on ouvre... Autant d'exemples qui nous convainquent que c'est bien souvent l'homme qui est à l'origine de crises.

Socrate estimait que "nul n'est méchant volontairement". Gageons comme lui qu'en matière de sécurité, nul n'est dangereux volontairement. La sensibilisation à la sécurité des systèmes d'information va lutter contre les mauvaises habitudes, consolider les bonnes pratiques, permettre d'éviter une bonne part des problèmes. Et surtout, la sensibilisation s'inscrit dans une logique d'anticipation. Anticiper, c'est limiter les risques, être vigilant et responsable des données qui nous sont confiées. Ainsi, avant d'avoir à gérer une crise, nous devons tout mettre en oeuvre pour éviter les crises.

Une fois formé, le participant à la simulation va communiquer avec son environnement professionnel. Il sera à la fois prophète et guide, enseignant et coach pour les non-initiés. Il ne va pas seulement transmettre les bonnes pratiques, partager son expérience, accompagner les simulations-exercices qui s'imposent si l'on veut être prêt à affronter une possible crise. Il va aussi partager des valeurs avec ses collègues, dont celles de la résilience, de la solidarité. Tous les acteurs de l'entreprise vont donner corps à une culture de la sécurité, qui va se nourrir et se renforcer au fil des simulations.

B. *Scénario*

Le scénario au centre de cette simulation de crise évoluait dans le milieu financier en suivant les déconvenues de la banque genevoise Yves Profit SA. Cette banque propose à des familles et des particuliers fortunés, principalement d'origine russe, une large gamme de services intégrant toutes les dimensions de la gestion de fortune. Son approche repose sur trois axes clairs: les solutions patrimoniales, les solutions d'investissement et les solutions bancaires.

Suite à la fin du secret bancaire suisse en 2018, la banque perd quelques gros clients et diversifie son offre pour survivre à cette crise. La banque multiplie les opérations risquées pour que sa clientèle ne la quitte pas. La banque parvient à satisfaire ses clients et ses actionnaires, mais quelques clients font les frais des prises de risque de la banque. Un gros client a dû déposer son bilan et son CEO ne manque pas une occasion de relever l'incompétence de la banque qui l'a conduit à la faillite.

En 2020 la banque Yves Profit SA se digitalise et réduit drastiquement son personnel. Un malaise se crée au sein du personnel de la banque. Un important gestionnaire de fonds est licencié en février 2020 et quitte l'établissement bancaire en mauvais termes. Il cherche à nuire fortement à ses anciens employeurs, puis à récupérer d'anciens clients qui les auraient quittés. Il commandite indirectement un hacker afin d'introduire un cheval de Troie dans le système de la banque. Ce malware n'est pas immédiatement détecté.

Le 10 janvier 2022, des données ont été exfiltrées du système de la banque et se retrouvent sur les réseaux sociaux.

La banque engage une cellule de crise (constituée des participants à la simulation) pour l'assister dans la gestion de la crise qui s'annonce. Cette crise va prendre différentes formes allant des cyberattaques, des attaques communicationnelles et atteintes à la réputation, des attaques en lien avec la finance, jusqu'à un kidnapping final.

- Les cyberattaques : la banque est exposée à des multiples attaques avec un système d'information comportant de multiples vulnérabilités (voir Section II-C).
- La crise financière : la banque se retrouve en sous-capitalisation et doit rendre des comptes à la FINMA. Au bord du dépôt de bilan, la banque doit trouver des solutions pour son avenir.
- Les attaques communicationnelles et atteintes à la réputation : les cellules de crise sont confrontées à des attaques sur les réseaux sociaux, y compris de parties prenantes inhabituelles, à des attaques des clients, aux médias dont des articles diffamatoires, à des messages de l'interne qui demande des comptes, à des messages en russe, à des téléphones intempestifs au milieu de la nuit, le tout enchaîné de façon soutenue. Un accident de scooter du fils de Monsieur Profit vient ajouter à la crise de la banque.
- Le Kidnapping : un ancien client ayant fait faillite à la suite des conseils de placements financiers de Yves Profit décide de kidnapper Madame Profit. Il s'arrange pour qu'une de ses relations fasse appel à un ravisseur dont le client ignorera tout. Le ravisseur appelle la cellule et refuse de négocier directement avec Yves Profit. La cellule de crise contacte la police, mais le négociateur n'est pas immédiatement disponible. Dans l'attente de son arrivée, c'est la cellule de crise qui doit mener les négociations. Le ravisseur se révèle caractériel, versatile et inconstant dans ses demandes de rançon. Les cellules de crise reçoivent la photo d'un doigt coupé censé appartenir à Madame Profit. Finalement, Madame Profit parvient à s'échapper sans dommages.

C. Plateforme Cyber

Afin d'ajouter un volet technique à la simulation de crise, une plateforme cyber permettait de simuler le système d'information de l'entreprise avec des machines virtuelles. Comme illustré Figure 1, ce système d'information était réduit à un firewall (une instance de PFSense) connectant deux sous réseaux à l'Internet, à savoir une DMZ avec un serveur Web (une instance d'Apache) et un réseau interne rassemblant des postes clients sous linux Ubuntu. Côté Internet, une machine offensive permettait de réaliser des attaques sur le système d'information de l'entreprise. Le service de mail de l'entreprise utilisait des comptes Google et des comptes Twitter et hashtags dédiés étaient utilisés comme canaux de communication sur les réseaux sociaux.

Plusieurs vulnérabilités et attaques ont été implémentées. Tout d'abord, des comptes utilisateurs avec des mots de passe faibles étaient présents sur plusieurs machines. Ensuite les règles de filtrage du firewall étaient très permissives et aucun filtre contre les spams n'était mis en place. Le serveur Web comportait une vulnérabilité de type RFI (Remote File Inclusion) sur un sous-espace du site. Enfin, des données confidentielles étaient stockées sur les serveurs Web rassemblant des données nominatives de clients. La machine offensive réalisait des opérations de cartographie du réseau de l'entreprise, des attaques de type Deny of Service (DoS), phishing, défacement du site Web de l'entreprise (Figure 2), attaques par dictionnaire sur les accès SSH des machines, et enfin une attaque de rançongiciel à la fois sur le serveur Web et les postes clients de l'entreprise.

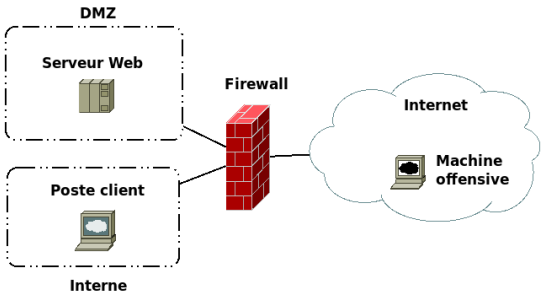

Fig. 1. La plateforme cyber rassemble plusieurs machines virtuelles simulant à la fois le système d'information de l'entreprise ainsi qu'une machine offensive réalisant les attaques.

Fig. 2. Défacement du site Web de l'entreprise.

D. Déroulement

La simulation de crise a eu lieu les 14 et 15 janvier dernier. Elle a rassemblé trois cellules de crise constituées par des membres de la Chancellerie de l'Etat de Genève, par des assistants en informatique de gestion et des professionnels de tous horizons. Malheureusement, une équipe de l'Insa Centre Val de Loire n'a pas pu se rendre sur place pour raison sanitaire.

Afin que la simulation de crise soit formative, les participants ont dû appliquer une méthode de gestion de crise. Cette méthode, adaptée aux besoins du monde civil, tire ses origines du domaine militaire. Le processus de conduite de crise doit aboutir à des décisions qui sont le fruit d'une analyse structurée et concertée. Elle permet d'éviter une prise

de décision sans approfondissement préalable ainsi que les biais cognitifs.

Les grandes étapes de la méthode sont les suivantes :

- Élaboration d'une vision, alignée sur le contexte existant, afin de définir une stratégie qu'il s'agit de partager entre les membres de la cellule de crise.
- Définition et communication des mesures d'urgence : 1) Comprendre le problème ; 2) Analyser la situation, les impacts et les risques ; 3) Élaborer les différentes options et les évaluer ; 4) Décider.

Durant l'exercice, les cellules de crise ont été conviées à un point de synchronisation à la fin de chacun des quatre volets successifs du scénario (voir Section II-B), même si divers types d'attaques perdurent tout au long du scénario. Les cellules de crise viennent au point de synchronisation pour rendre compte du suivi de la méthodologie et des décisions prises. Elles ne sont pas évaluées sur le résultat produit, mais sur le respect de la méthodologie. La réponse des cellules à chaque stimulus est évaluée par des experts. Afin d'aider les experts dans cette tâche, une fiche d'évaluation pour chaque attaque permet de décrire le stimulus et précise ce qui doit être évalué. Un exemple de stimulus est illustré Figure 3. Le comportement individuel et la dynamique des cellules de crise fait également l'objet d'une évaluation. À la fin de l'exercice, chaque cellule reçoit un document synthétique qui résume les points forts et les points à améliorer.

E. Retours d'Expérience

Les retours des participants sont très positifs. Bien que la plateforme Cyber n'ait pas été intégralement fonctionnelle, le scénario complet et l'accompagnement à la conduite de la méthode de gestion de crise a contre-balancé la mise en retrait de tâches techniques. Pour éviter ce genre de déconvenue par la suite, nous retenons qu'il faut s'abstraire autant que possible des infrastructures systèmes et réseaux de l'organisation d'accueil de l'événement. En effet, les machines virtuelles de la plateforme ont été installées sur une machine mise à disposition à la HEG sur un sous réseau dédié. Il s'avère que la machine n'était pas assez puissante pour accueillir toutes nos machines virtuelles et que le réseau dédié avait des restrictions. Pour éviter ces problèmes lors des prochaines éditions, nous avons fait évoluer notre plateforme avec un hébergement sur un serveur de virtualisation avec accès aux machines virtuelles via un navigateur. Ainsi, les participants n'auront uniquement besoin d'un accès Web sur le lieu de l'événement.

III. Conclusions

Afin de former de manière ludique les futurs acteurs du management de crise et de la cybersécurité, nous avons expérimenté une simulation de crise durant 24 heures consécutives. Cette simulation de crise consistait à accompagner une banque à faire face à une crise majeure impliquant de multiples attaques de différentes natures. Ce type d'expérimentation a montré son efficacité didactique et devrait être encouragé lors de formations au management de crise.

Stimulus No 23	La conférence de presse		14-15.01.2022
Emetteur	État-major	Destinataire	Cellule de crise No
Objectif attendu	Mettre l'information à niveau et s'allier les médias	Réaction attendue	Les médias témoignent en faveur de la banque
Canal de communication	Cellules face aux journalistes	Délai	15 minutes par cellule + 15 minutes questions-réponses
Situation actuelle : la crise de la banque Yves Profit est aujourd'hui rendue publique. Pour recadrer les informations, mettre un terme aux rumeurs et aux Fake News, une conférence de presse s'impose			
Procédure et étapes de mise en œuvre : - avoir bien choisi le lieu, la date et l'horaire - appréhender la conférence en étant ouvert, respectueux et remercier les journalistes de leur présence - présenter une direction unie et judicieusement choisie face aux journalistes - avoir anticipé les principales questions-réponses lors de l'échange avec journalistes - en premier lieu, faire preuve d'empathie pour toutes les personnes qui ont subi la crise - admettre que la banque, si elle n'est pas coupable de la situation, est responsable et assume ses obligations vis-à-vis de ses clients et partenaires - de façon synthétique, factuelle, raconter les différentes étapes de la crise et de sa gestion - écouter jusqu'au bout les questions posées par les journalistes et y répondre simplement, avec sincérité, sans pour autant se fustiger ou révéler des secrets sur la banque - choisir ses termes avec circonspection, en prenant le temps de répondre sans précipitation ni agressivité - la conférence de presse est « un balai réglé » : on ne doit pas avoir l'impression que la direction improvise . reformuler les questions des journalistes si elles ne sont pas claires ou pour gagner du temps - précisez les prochaines étapes de votre gestion de crise et les moments/canaux de communication prévus			

Fiche de contrôle			
		Cellule évaluée No	
3 points à contrôler	• N'avoir oublié aucun média • Accorder une grande importance au non verbal • Montrer une équipe soudée, cohérente, solidaire, forte et responsable	Evaluation globale	
Points positifs	• • •	Points négatifs	• • •

Fig. 3. Exemple de fiche permettant de guider l'évaluation de la réaction des cellules de crise à chaque stimulus.

Remerciements

Cette simulation et les précédentes expérimentations d'exercice de gestion de crise ont été financées en partie par l'INSA de Lyon, l'INSA Centre Val de Loire et par le Projet IDEXLYON de l'Université de Lyon dans le cadre du Programme Investissements d'Avenir (ANR-16-IDEX-0005).

References

[1] Ansii, "État de la menace rançongiciels à l'encontre des entreprises et institutions," 2021.

[2] "Cyberattaques : La croix-rouge n'est pas épargnée," 2022. [Online]. Available: https://www.zdnet.fr/actualites/cyberattaque-la-croix-rouge-n-est-pas-epargnee-39936023.htm

[3] R. Xu-Darme, "Cali-ssi : Challenge interdisciplinaire en sécurité des systèmes d'information," in *RESSI*, 2020.

[4] A. Boutet, "Http 403 forbidden : les 5if confrontés à une crise globale," 2018. [Online]. Available: https://www.insa-lyon.fr/fr/actualites/http-403-forbidden-5if-confrontes-crise-globale

[5] T. J. Burns, S. C. Rios, T. K. Jordan, Q. Gu, and T. Underwood, "Analysis and exercises for engaging beginners in online {CTF} competitions for security education," in *USENIX Workshop on Advances in Security Education*, 2017.

[6] A. Mansurov, "A CTF-based approach in information security education: An extracurricular activity in teaching students at altai state university, russia," *Modern Applied Science*, vol. 10, no. 11, p. 159, 2016.

[7] C. Lauradoux, "Teaching security with CTF-like challenges," in *RESSI*, 2017.