AYI NEDJIMI Consultants

Exercice de gestion de crise cyber : scénarios et RETEX

Catégorie : Consulting Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Organisez des exercices de crise cyber efficaces. Scénarios réalistes, méthodologie d'animation, RETEX structuré et programme de résilience continue.

Résumé exécutif

Les exercices de gestion de crise cyber sont devenus une obligation réglementaire et une nécessité opérationnelle pour toute organisation souhaitant valider sa capacité de réponse face aux incidents de cybersécurité majeurs. Ce guide détaille la méthodologie complète de conception, de conduite et d'exploitation des exercices de crise cyber, depuis la définition des scénarios réalistes basés sur les menaces actuelles jusqu'à l'analyse approfondie des retours d'expérience et la construction des plans d'amélioration, en s'appuyant sur des exemples concrets de scénarios éprouvés auprès d'organisations de secteurs variés et sur les leçons tirées d'incidents réels majeurs ayant marqué le paysage de la cybersécurité mondiale ces dernières années et démontré l'importance cruciale de la préparation méthodique des équipes dirigeantes et opérationnelles à la gestion de situations de stress intense et d'incertitude maximale.

La gestion de crise cyber est un exercice radicalement différent de la gestion de crise traditionnelle car elle combine une dimension technique complexe et évolutive, une pression temporelle extrême amplifiée par les obligations de notification réglementaire, une incertitude permanente sur l'étendue réelle de la compromission et des impacts potentiellement systémiques sur l'ensemble des activités de l'organisation. Les organisations qui découvrent la gestion de crise cyber le jour où elles subissent une attaque de ransomware commettent des erreurs coûteuses et parfois irréversibles : paiement de rançon précipité sans négociation ni garantie de récupération, communication de crise improvisée générant une panique interne et une perte de confiance des clients, restauration de systèmes compromis sans éradication préalable de la menace conduisant à une recompromission immédiate, et destruction de preuves forensiques nécessaires à la compréhension de l'attaque et à la poursuite judiciaire des attaquants. La **directive NIS 2** impose aux entités essentielles et importantes de mettre en place des processus de gestion des incidents et de gestion de crise, tandis que le *règlement DORA* exige spécifiquement des entités financières la réalisation de tests de résilience opérationnelle incluant des exercices de crise cyber. Les exercices réguliers et réalistes sont le seul moyen de préparer effectivement les équipes à ces situations de stress extrême et de valider que les procédures, les outils et les chaînes de décision fonctionnent correctement avant qu'une crise réelle ne mette impitoyablement à l'épreuve l'ensemble du dispositif.

Comment concevoir des scénarios de crise cyber réalistes ?

La conception de scénarios de crise cyber réalistes et pertinents est la première étape critique de tout exercice. Le scénario doit être crédible par rapport au profil de risque spécifique de l'organisation, suffisamment complexe pour tester les mécanismes de décision et de coordination, mais pas tellement technique qu'il exclut les participants non spécialistes. Les trois familles de scénarios les plus utilisées sont le **ransomware ciblé** avec chiffrement massif et menace de publication des données exfiltrées, la **compromission avancée** de type APT avec détection tardive d'un attaquant présent depuis plusieurs semaines, et la **fuite de données massives** exposant des données personnelles ou stratégiques avec implications RGPD et médiatiques.

Chaque scénario doit être scénarisé en phases (injection, escalade, pic de crise, sortie de crise) avec des stimuli préparés à l'avance : emails fictifs de l'attaquant, captures d'écran simulant des systèmes chiffrés, faux articles de presse, demandes de rançon, notifications réglementaires à rédiger. Le réalisme du scénario conditionne directement la qualité de l'exercice et la pertinence des enseignements tirés. Les scénarios doivent être alimentés par la veille sur les menaces issue des plateformes de threat intelligence et adaptés au secteur d'activité de l'organisation.

Votre cellule de crise a-t-elle déjà été activée pour un exercice, ou serait-ce la première fois le jour où un vrai ransomware frappe votre infrastructure un vendredi soir à vingt-trois heures ?

Quels types d'exercices de crise cyber mettre en place ?

Les exercices de crise cyber se déclinent en quatre formats de complexité et d'investissement croissants, chacun apportant des bénéfices spécifiques. L'**exercice sur table** (tabletop exercise) est le format le plus accessible et le plus couramment utilisé : les participants sont réunis en salle et réagissent à un scénario déroulé progressivement par un animateur. Il ne nécessite pas de moyens techniques et permet de tester les processus de décision, la communication et la coordination entre les différentes parties prenantes de la cellule de crise.

L'**exercice fonctionnel** (functional exercise) teste un aspect spécifique du dispositif de crise en conditions réelles : activation de la cellule de crise, mise en œuvre du plan de communication, restauration des sauvegardes ou bascule vers un site de secours. L'**exercice complet** (full-scale exercise) combine tous les aspects en simulant une crise de bout en bout avec activation réelle de la cellule de crise, mobilisation des équipes techniques et mise en œuvre effective des procédures de réponse. Le *test TLPT* (Threat-Led Penetration Testing) requis par DORA pour le secteur financier ajoute une dimension technique en simulant une attaque réelle conduite par une équipe de red team sur la base de scénarios de menace documentés, en coordination avec le SOC et le plan de réponse aux incidents.

Mon avis : L'exercice sur table est souvent sous-estimé mais c'est le format qui produit le meilleur rapport qualité-investissement. En une demi-journée et avec un budget minime, vous pouvez tester la capacité de décision de votre COMEX face à un scénario de crise cyber réaliste et identifier les dysfonctionnements majeurs de votre organisation de crise. Je recommande un exercice sur table semestriel et un exercice fonctionnel ou complet annuel. La clé est la régularité plutôt que la sophistication ponctuelle.

Type d'exercice	Durée	Participants	Objectif principal	Budget indicatif
Tabletop COMEX	2-4 heures	Direction, RSSI, DSI, DirCom	Tester la prise de décision stratégique	5-15k euros
Tabletop technique	3-4 heures	SOC, CSIRT, IT, RSSI	Tester les procédures de réponse	3-10k euros
Exercice fonctionnel	1 journée	Équipes ciblées selon composant testé	Valider un composant spécifique du PCA	10-30k euros
Exercice complet	1-2 jours	Toutes les parties prenantes	Valider le dispositif de bout en bout	30-100k euros
TLPT (DORA)	3-6 mois	Red team externe, SOC, direction	Tester la résilience face à une attaque réelle	100-300k euros

L'incendie du datacenter OVHcloud SBG2 à Strasbourg en mars 2021 a constitué un exercice de crise grandeur nature non planifié pour des milliers d'organisations françaises. Les retours d'expérience ont révélé que les organisations ayant régulièrement conduit des exercices de crise, même de simples tabletop, ont réagi significativement plus vite et plus efficacement que celles qui n'avaient jamais testé leurs procédures. Le temps moyen d'activation de la cellule de crise était de deux heures pour les organisations exercées contre plus de huit heures pour les non exercées, une différence qui s'est traduite directement en heures de disponibilité perdues et en impact financier pour les clients. Cet événement a aussi démontré l'importance de tester régulièrement les procédures de disaster recovery cloud.

Comment animer efficacement un exercice de crise cyber ?

L'animation d'un exercice de crise cyber exige des compétences spécifiques qui combinent l'expertise technique en cybersécurité, la maîtrise des dynamiques de groupe et la capacité à maintenir la pression scénaristique tout en observant et documentant les réactions des participants. L'**équipe d'animation** (ANIMEX) comprend typiquement un directeur d'exercice qui supervise le déroulement global, un ou deux animateurs qui injectent les stimuli et simulent les interactions externes (attaquant, médias, autorités, clients), et un ou deux observateurs qui documentent les réactions, les décisions et les dysfonctionnements observés.

Les règles d'engagement doivent être clairement définies en amont : les participants doivent traiter l'exercice comme une situation réelle dans le cadre défini, aucune action ne doit être prise sur les systèmes de production réels sauf si l'exercice le prévoit explicitement, et un mot-code d'arrêt permet de suspendre l'exercice en cas d'incident réel survenant pendant son déroulement. La progression du scénario doit être adaptable en temps réel par les animateurs qui accélèrent ou ralentissent les injections en fonction des réactions des participants et du temps disponible. L'animation doit s'appuyer sur les recommandations de l'ANSSI sur la gestion de crise cyber.

Quels enseignements tirer du retour d'expérience post-exercice ?

Le retour d'expérience (RETEX) est la phase la plus importante de l'exercice car c'est elle qui transforme une expérience vécue en améliorations concrètes du dispositif de crise. Le RETEX se déroule en deux temps : un **débriefing à chaud** immédiatement après l'exercice pour recueillir les impressions et les observations des participants, et un **rapport d'analyse détaillé** produit dans les deux semaines suivantes qui formalise les constats, identifie les forces et les faiblesses révélées et propose des actions correctives priorisées.

Le rapport de RETEX doit couvrir systématiquement les dimensions suivantes : efficacité de la détection et de l'alerte initiale, rapidité et pertinence de l'activation de la cellule de crise, qualité de la coordination entre les équipes techniques et la direction, pertinence des décisions stratégiques prises sous pression, efficacité de la communication interne et externe, adéquation des moyens techniques et humains mobilisés, et respect des obligations réglementaires de notification. Chaque constat est assorti d'un **niveau de criticité** (bloquant, majeur, mineur) et d'une action corrective assignée à un responsable avec une échéance. Le suivi des actions est intégré dans le tableau de bord du RSSI et présenté au COMEX conformément aux pratiques de gouvernance NIS 2.

Faut-il impliquer des prestataires externes dans les exercices ?

L'implication de prestataires externes dans les exercices de crise cyber apporte une expertise méthodologique et un regard objectif que les équipes internes ne peuvent pas toujours fournir. Les cabinets spécialisés en gestion de crise cyber disposent de bibliothèques de scénarios éprouvés, d'animateurs expérimentés et de méthodologies de RETEX structurées qui accélèrent considérablement la montée en maturité de l'organisation. Pour les exercices TLPT requis par DORA, l'utilisation de prestataires externes est obligatoire pour l'équipe de threat intelligence et l'équipe de red team.

L'externalisation de l'animation présente également l'avantage de permettre au RSSI de participer pleinement à l'exercice en tant que joueur plutôt qu'en tant qu'organisateur, ce qui teste sa propre capacité de réponse sous pression plutôt que sa capacité d'animation. En revanche, l'internalisation progressive de la compétence d'exercice est souhaitable pour les organisations matures afin de pouvoir conduire des exercices plus fréquents à moindre coût. L'approche optimale combine des exercices externes annuels de haut niveau avec des exercices internes trimestriels ciblés sur des composantes spécifiques du dispositif de crise, selon les standards de l'ENISA en matière d'exercices cyber et en lien avec la gestion des données personnelles.

Sources et références : ANSSI · CERT-FR

Comment intégrer les exercices dans un programme de résilience continue ?

Les exercices de crise cyber ne doivent pas être des événements ponctuels isolés mais s'inscrire dans un **programme de résilience continue** intégré dans la gouvernance globale de la cybersécurité. Le programme annuel d'exercices doit prévoir une montée en complexité progressive : exercices sur table trimestriels ciblant successivement différents scénarios et différentes audiences, exercice fonctionnel semestriel testant un composant critique du dispositif de crise (restauration, communication, notification), et exercice complet annuel mobilisant l'ensemble des parties prenantes incluant le COMEX.

Chaque exercice produit des enseignements qui alimentent le cycle d'amélioration continue du dispositif de crise et, plus largement, du SMSI. Les actions correctives identifiées lors des RETEX sont suivies jusqu'à leur clôture et leur efficacité est vérifiée lors des exercices suivants. Cette boucle vertueuse permet une progression mesurable de la capacité de réponse de l'organisation, démontrable auprès des régulateurs et des assureurs qui accordent une importance croissante à la maturité des exercices de crise dans leurs évaluations. Le programme doit être aligné avec le dispositif de surveillance pour garantir la cohérence entre la détection opérationnelle et la réponse de crise stratégique.

La documentation de chaque exercice et de ses enseignements constitue également un atout précieux lors des audits de certification ISO 27001, des contrôles NIS 2 par les autorités compétentes et des évaluations de maturité par les assureurs cyber qui accordent une pondération croissante à la qualité et à la fréquence des exercices de crise dans leurs critères de souscription et de tarification des polices d'assurance cybersécurité.

À retenir : Les exercices de crise cyber sont le seul moyen de valider que votre dispositif de réponse fonctionne réellement sous pression. Commencez par des exercices sur table trimestriels accessibles et peu coûteux, puis progressez vers des exercices fonctionnels et complets. Le RETEX est la phase la plus importante : sans actions correctives suivies et vérifiées, l'exercice n'aura produit qu'un moment de stress collectif sans valeur durable pour l'organisation.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr