KIT D’EXERCICE COMEX / COPIL

ATTAQUE PAR RANSOMWARE

Un scénario prêt à l’emploi pour animer un exercice de crise cyber, décider sous incertitude et évaluer la résilience de l’entreprise.

1. **Guide de l’animateur**
2. **Scénario confidentiel**
3. **Chronologie de crise**
4. **Fiches inject**
5. **Décisions & débrief**

MODE D’EMPLOI

Comment utiliser ce kit

Ce document est conçu pour permettre à une Direction, une DSI ou un RSSI d’organiser un exercice sur table sans avoir à construire entièrement son scénario. Il peut être utilisé tel quel, puis adapté à l’organisation, à ses activités, à son architecture et à ses propres procédures de gestion de crise.

Principe

L’animateur révèle les informations progressivement. Les participants prennent leurs décisions uniquement à partir des éléments disponibles à l’instant considéré. L’objectif n’est pas de trouver une réponse parfaite mais d’observer la manière dont l’organisation arbitre sous contrainte.

1	Guide de l’animateur Objectifs, participants, préparation, règles et conduite de séance.
2	Scénario confidentiel Contexte complet réservé à l’animateur. Ne pas remettre aux participants avant l’exercice.
3	Chronologie de crise Déroulé minute par minute et points d’attention associés.
4	Fiches inject Informations à remettre progressivement pour faire évoluer la situation.
5	Feuille de décisions Support pour consigner arbitrages, responsables et actions.
6	Grille des ressources de crise Vérification de la disponibilité réelle des outils, contacts et informations.
7	Débrief & RETEX Questions structurées pour faire émerger les enseignements.
8	Plan d’amélioration Transformation des constats en actions suivies.

À adapter

Le scénario est volontairement générique. Les noms des applications, prestataires, lignes de production, sites et fonctions doivent être remplacés par ceux de l’organisation pour augmenter l’immersion.

Objectifs, participants et cadre de l’exercice

Durée conseillée : 90 à 120 minutes. Format : exercice sur table. Niveau technique requis pour les participants : aucun.

L’exercice simule une attaque par ransomware qui dégrade progressivement le système d’information, l’ERP puis la production. Il doit permettre d’évaluer la capacité du COMEX/COPIL à comprendre les impacts métier, prendre des décisions et maintenir une gouvernance cohérente malgré l’incertitude.

Objectifs de l’exercice

- Tester la chaîne de décision et la capacité à désigner clairement un directeur de crise.
- Mesurer la compréhension des dépendances entre SI, ERP, commandes, planification, production, expéditions et facturation.
- Observer la manière dont sont priorisées les activités et les services à restaurer.
- Évaluer la capacité à fonctionner en mode dégradé et à accepter temporairement certaines pertes de service ou de données.
- Vérifier que les ressources nécessaires à la gestion de crise restent accessibles lorsque le SI courant ne l’est plus.
- Identifier les actions d’amélioration à intégrer au PCA/PRA, aux procédures, à la gestion des risques et aux futurs exercices.

Participants recommandés

Fonction	Rôle pendant l’exercice
Direction générale	Arbitrage final, priorités d’entreprise, communication et engagements externes.
DSI	Qualification, impacts SI, options de restauration et dépendances techniques.
RSSI / sécurité	Confinement, investigation, risques de propagation et coordination sécurité.
Direction industrielle	Capacité à produire, risques du mode dégradé, priorités opérationnelles.
Finance	Facturation, trésorerie, pertes d’exploitation et impacts financiers.
Communication / juridique / DPO	Information des parties prenantes, obligations et messages externes selon le contexte.

Préparation et règles de conduite

Préparation avant la séance

- Choisir un animateur qui ne participera pas aux arbitrages.
- Préparer les fiches inject dans l’ordre prévu et ne pas les distribuer à l’avance.
- Identifier un rapporteur chargé de consigner les décisions et les heures associées.
- Adapter au minimum le nom de l’ERP, le type de production, le prestataire sécurité et les interlocuteurs clés.
- Prévoir un espace de travail séparé de la production réelle : aucun système ne doit être volontairement interrompu.
- Conserver 20 à 30 minutes pour le débrief final.

Règles à annoncer aux participants

- Vous ne disposez que des informations fournies par l’animateur.
- Vous pouvez demander des précisions, mais l’animateur peut répondre : « information non disponible à ce stade ».
- Toute décision importante doit être formulée explicitement.
- Une décision peut être révisée lorsque de nouveaux éléments apparaissent.
- L’exercice évalue le dispositif, pas les personnes.

Conseil d’animation	Résistez à la tentation de résoudre trop vite la situation. Un bon exercice laisse apparaître des zones d’incertitude : étendue de la compromission, fiabilité des sauvegardes, état réel de la production ou nature des données exfiltrées.

Confidentialité	Les pages « Scénario confidentiel », « Chronologie animateur » et les fiches inject ne doivent pas être diffusées aux participants avant l’exercice.

02 - SCÉNARIO CONFIDENTIEL

Contexte complet réservé à l’animateur

NE PAS DISTRIBUER AUX PARTICIPANTS

Cette page décrit la logique globale du scénario. Les participants doivent découvrir la situation uniquement au travers des injects.

L’entreprise fictive est une société industrielle fortement dépendante d’un ERP central. L’ERP supporte la saisie des commandes, la planification de gestion de production, les stocks, les expéditions et la facturation. Une partie des machines de production reçoit ou échange des informations avec le SI. L’authentification des utilisateurs repose principalement sur un annuaire centralisé.

Une partie de la surveillance sécurité est confiée à un prestataire externe de type SOC/MSSP. Celui-ci reçoit certains journaux dans son propre environnement. L’entreprise dispose de sauvegardes, mais aucune information n’est donnée aux participants sur leur état réel au début de l’exercice.

Situation réelle connue de l’animateur

- Une compromission a débuté avant l’ouverture de la journée de travail.
- Plusieurs systèmes sont progressivement chiffrés et l’accès à l’annuaire devient instable.
- L’ERP est rendu indisponible, entraînant des impacts immédiats sur commandes, planification, production, expéditions et facturation.
- L’équipe infrastructure dispose de sauvegardes, mais doit encore déterminer un point de restauration suffisamment fiable.
- Le prestataire sécurité perd son accès au réseau après l’isolement, mais conserve les journaux reçus avant la coupure.
- Une suspicion d’exfiltration apparaît sans pouvoir être confirmée immédiatement.
- Un message de rançon sera découvert en fin de séquence.

Ce que l’animateur doit observer

- Le moment où l’organisation bascule d’un incident IT vers une crise d’entreprise.
- La désignation d’une autorité de crise et la répartition des rôles.
- Les arbitrages entre confinement technique et continuité de production.
- La capacité à prioriser des services plutôt qu’à demander « tout remettre en route ».
- La maîtrise des dépendances : annuaire, DNS, sauvegardes, prestataires, messagerie, outils de crise.
- La manière dont les décisions sont tracées, communiquées et réévaluées.

Conduite de l’exercice : le rôle de l’animateur

Le scénario doit être joué comme une situation qui se dégrade progressivement, pas comme une succession mécanique de fiches. L’animateur contrôle le rythme, conserve une partie de l’information et utilise les questions des participants pour faire apparaître leurs réflexes de gouvernance.

Les quatre réflexes de l’animateur

- Faire décider. Lorsque la discussion devient générale, revenir à une formulation simple : « Quelle décision prenez-vous maintenant ? »
- Faire nommer un responsable. Demander systématiquement : « Qui porte cette décision et qui doit l’exécuter ? »
- Faire expliciter le risque accepté. Par exemple : « Que risquez-vous si vous continuez à produire ? Et si vous arrêtez ? »
- Faire définir un critère de réévaluation. Une décision temporaire doit préciser quand et sur quelle information elle sera revue.

Ne cherchez pas à piéger	L’animateur n’est pas là pour démontrer qu’il connaît la réponse. Il met les participants face à des arbitrages plausibles et observe la qualité de leur méthode de décision.

Questions de relance utiles

- « Qu’est-ce qui vous manque pour décider ? »
- « Pouvez-vous attendre cette information ou devez-vous décider avant ? »
- « Qui doit être informé maintenant, et qui ne doit pas encore l’être ? »
- « Si cette décision s’avère mauvaise dans une heure, comment la corrigez-vous ? »
- « Quel service ou quelle activité passe avant les autres ? Pourquoi ? »
- « Quel est le coût ou le risque de ne rien décider pendant trente minutes ? »

02 - SCÉNARIO CONFIDENTIEL

Ce que l’animateur sait - et ce qu’il peut révéler

Les informations ci-dessous constituent la « vérité du scénario ». Elles permettent à l’animateur de répondre de manière cohérente aux questions sans dévoiler trop tôt la suite.

Sujet	Vérité du scénario	Réponse animateur
Origine de l’incident	Inconnue au début. Les premiers éléments techniques fiables n’apparaissent qu’avec les journaux du prestataire à 11:05.	Répondre : « L’origine n’est pas déterminée à ce stade. »
Étendue de la compromission	Plusieurs serveurs et l’annuaire sont touchés ou suspects. Le périmètre exact reste incertain.	Ne jamais donner une liste exhaustive des systèmes compromis.
Accès Internet	L’accès Internet reste partiellement disponible depuis des équipements non isolés, mais l’organisation cherche à réduire les connexions.	Si les participants veulent utiliser des services externes, demander d’abord comment ils sécurisent l’accès.
Messagerie interne	La messagerie devient peu fiable pour une partie des utilisateurs à mesure que l’annuaire se dégrade.	Permet de tester l’existence d’un canal alternatif de crise.
ERP	Indisponible à partir de 09:15. Aucune saisie fiable de commandes, planification, stock, expédition ou facturation n’est possible.	Le redémarrage ne doit pas être présenté comme imminent.
Production	Certaines lignes peuvent fonctionner quelques heures avec des informations locales ou des consignes manuelles ; d’autres dépendent fortement de l’ERP.	L’animateur ne valide jamais lui-même le mode dégradé : il demande les conditions et risques acceptés.
Sauvegardes	Des sauvegardes existent. Leur intégrité n’est pas encore établie et le dernier point fiable n’est pas connu à 10:35.	Si on demande un RPO précis : « en cours d’évaluation ».
SOC / MSSP	Le prestataire perd l’accès après isolation mais conserve les journaux reçus avant la coupure.	À 11:05 il peut fournir des événements suspects et préserver les logs.
Exfiltration	Possible mais non confirmée.	Ne jamais affirmer qu’une fuite est avérée.
Rançon	Un message est découvert à 12:20 et prétend que des données ont été copiées.	Le message est une information d’attaquant, pas une preuve.

02 - SCÉNARIO CONFIDENTIEL

Faire réagir le scénario aux décisions des participants

Pour éviter un exercice trop linéaire, l'animateur peut utiliser les variantes ci-dessous. Elles ne changent pas la trame principale mais donnent l'impression que la situation réagit aux choix du COMEX/COPIL.

Décision des participants	Réaction à jouer	Objectif pédagogique
Isolement rapide Le COMEX accepte rapidement l'isolement des environnements suspects.	Faire apparaître plus tôt la pression métier : « Depuis la coupure, plusieurs applications encore fonctionnelles sont devenues inaccessibles. La production demande si l'isolement peut être allégé. »	Tester la capacité à maintenir une mesure impopulaire tant que le risque n'est pas maîtrisé.
Isolement refusé ou retardé Les participants veulent préserver l'activité et retardent le confinement.	Ajouter : « De nouveaux partages deviennent inaccessibles et deux serveurs supplémentaires présentent des fichiers chiffrés. »	Forcer une réévaluation de la décision sans dire qu'elle était "mauvaise".
Production maintenue sans cadre Le COMEX autorise le mode dégradé sans préciser de conditions.	Ajouter : « Un responsable d'atelier signale qu'il n'est plus certain de travailler sur la dernière version de l'ordre de fabrication. »	Faire préciser traçabilité, qualité, durée maximale et autorité d'arrêt.
Production arrêtée immédiatement Le COMEX stoppe toute production par prudence.	Ajouter : « Le commercial indique que deux commandes stratégiques devaient quitter le site aujourd'hui. »	Tester la capacité à reconsidérer un arrêt global ou à assumer explicitement son impact.
Restauration demandée très tôt Les participants veulent restaurer dès l'annonce de sauvegardes disponibles.	Répondre : « L'équipe peut préparer la restauration, mais ne peut pas encore garantir que l'environnement cible ou les identifiants ne sont plus compromis. »	Distinguer vitesse de reprise et sécurité de la reprise.
Communication externe immédiate Les participants veulent informer rapidement clients ou partenaires.	Demander : « Quel message exact validez-vous alors que le périmètre et la durée restent inconnus ? »	Tester validation, cohérence et maîtrise de l'incertitude.
Aucune communication Les participants préfèrent attendre avant de communiquer.	Ajouter : « Un client appelle directement un responsable commercial après avoir constaté un retard. »	Tester la préparation d'un message avant que l'extérieur ne l'impose.
Prestataire sollicité efficacement Les participants demandent la préservation des logs et une chronologie.	Le SOC indique une authentification inhabituelle vers 03:42 sur un compte de service, puis des accès à plusieurs serveurs.	Récompenser une demande pertinente par une information utile sans résoudre l'enquête.

02 - SCÉNARIO CONFIDENTIEL

Injects de pression optionnels

Ces cartes sont facultatives. Utilisez-en une uniquement si la discussion s'essouffle, si le groupe évite une décision ou si vous souhaitez augmenter légèrement la difficulté. Une seule pression à la fois suffit.

Carte	Message à jouer	Pourquoi l'utiliser
P1 - Direction commerciale	« Un client stratégique exige une réponse dans les quinze minutes. Il veut savoir si sa commande part aujourd'hui. »	Forcer une communication malgré une visibilité limitée.
P2 - Atelier	« Le responsable d'atelier demande une consigne écrite : continuer en mode manuel ou arrêter la ligne. »	Obtenir une décision explicite et un responsable.
P3 - Finance	« La direction financière demande une estimation, même grossière, de la durée pendant laquelle la facturation restera indisponible. »	Tester la capacité à fournir des hypothèses et non de fausses certitudes.
P4 - Support	« Les utilisateurs appellent individuellement la DSI et reçoivent des réponses différentes. »	Faire émerger la nécessité d'un message interne unique.
P5 - Sauvegarde	« Une restauration de test pourrait être lancée sur un environnement isolé, mais elle mobiliserait l'équipe infrastructure pendant deux heures. »	Tester la priorisation des ressources techniques.
P6 - Prestataire	« Le SOC demande qui est habilité à lui transmettre des consignes et à recevoir ses éléments d'investigation. »	Tester gouvernance et canal de coordination externe.

Règle de jeu

Si les participants prennent une décision claire, cohérente et assortie d'un responsable, laissez-la produire ses effets. L'objectif n'est pas de faire échouer le groupe mais de révéler ce que son dispositif sait réellement faire.

03 - CHRONOLOGIE DE CRISE

Déroulé animateur

Heure	Inject	Information	Point d'observation
08:17	**Premiers signaux**	Utilisateurs : fichiers partagés inaccessibles, ralentissements et erreurs d'authentification.	Observer si une organisation de crise est envisagée et qui est informé.
08:28	**Extension**	Plusieurs serveurs présentent simultanément des comportements inhabituels.	Demander quelles mesures conservatoires peuvent être prises.
08:42	**Chiffrement confirmé**	Des fichiers sont chiffrés. L'équipe recommande l'isolement de certains environnements.	Arbitrage confinement / continuité.
09:15	**ERP indisponible**	Commandes, planification, stocks, expéditions et facturation sont touchés.	Faire basculer la discussion vers les impacts métier.
10:00	**Production ralentie**	Certaines lignes peuvent fonctionner partiellement, d'autres dépendent des ordres issus du SI.	Poser le dilemme du mode dégradé.
10:35	**Sauvegardes**	Des sauvegardes existent, mais leur intégrité et le point de restauration fiable restent à confirmer.	Tester RTO/RPO réels et autorité de remise en service.
11:05	**Prestataire sécurité**	Le SOC n'accède plus au réseau mais possède les journaux reçus avant la coupure et signale des authentifications inhabituelles.	Faire identifier la valeur des ressources externes.
11:45	**Crise externe**	Client stratégique, fournisseur, finance et suspicion d'exfiltration arrivent simultanément.	Tester coordination, communication et priorités.
12:20	**Rançon**	Un message de rançon affirme que des données ont été copiées.	Observer méthode de décision et mobilisation des conseils externes.

Rythme

Les heures servent de repères pédagogiques. Vous pouvez accélérer ou ralentir le scénario selon la qualité des échanges. Ne déclenchez pas automatiquement l'inject suivant tant qu'aucune décision claire n'a émergé.

04 - FICHES INJECT

À remettre progressivement aux participants

Imprimez ou affichez une fiche à la fois. Ne distribuez jamais l’ensemble des injects en début de séance.

INJECT 01

08:17 - Support utilisateur

Plusieurs utilisateurs signalent qu’ils ne peuvent plus ouvrir certains fichiers partagés. D’autres rencontrent des erreurs d’authentification et des ralentissements importants.

Question aux participants
Que faites-vous maintenant ? Qui doit être informé ?

INJECT 02

08:28 - Équipe infrastructure

Plusieurs serveurs présentent des comportements inhabituels au même moment. L’origine n’est pas encore déterminée.

Question aux participants
Déclenchez-vous une organisation de crise ?
Quelles mesures immédiates autorisez-vous ?

INJECT 03

08:42 - Sécurité

Le chiffrement de plusieurs fichiers est confirmé. L’équipe recommande d’isoler certains environnements pour limiter une éventuelle propagation.

Question aux participants
Qui peut décider de l’isolement ? Jusqu’où faut-il aller ?

INJECT 04

09:15 - Direction métiers

L’ERP devient indisponible. Les nouvelles commandes ne peuvent plus être saisies. La planification de production, les stocks, les expéditions et la facturation sont perturbés.

Question aux participants
Quelles activités deviennent prioritaires ?
Quelle information donnez-vous aux métiers ?

INJECT 05

10:00 - Direction industrielle

Certaines lignes peuvent continuer en mode dégradé. D’autres ne disposent plus des informations nécessaires. La cadence ralentit.

Question aux participants
Autorisez-vous la production en mode dégradé ? Sous quelles conditions ?

INJECT 06

10:35 - Infrastructure / sauvegardes

Des sauvegardes sont disponibles. L’équipe ne peut pas encore garantir qu’elles sont saines ni déterminer le dernier point de restauration fiable.

Question aux participants
Attendez-vous davantage d’éléments ou préparez-vous une restauration ? Quelle perte de données est acceptable ?

INJECT 07

11:05 - Prestataire SOC/MSSP

Le prestataire n’accède plus au réseau depuis l’isolement. Il dispose toutefois des journaux reçus avant la coupure et signale plusieurs authentifications inhabituelles avant l’incident.

Question aux participants
Quelles informations demandez-vous au prestataire ? Comment préservez-vous ces éléments ?

INJECT 08

11:45 - Client stratégique

Un client stratégique demande confirmation de sa livraison prévue cet après-midi. Le service commercial ne dispose plus d’une vision fiable de l’état de la commande.

Question aux participants
Que lui répondez-vous ? Qui valide le message ?

INJECT 09

11:55 - Sécurité / juridique

Une exfiltration de données avant chiffrement ne peut pas être exclue. Aucun périmètre fiable n’est encore disponible.

Question aux participants
Qui associez-vous à l’analyse ? Quelles décisions préparez-vous sans surcommuniquer ?

INJECT 10

12:20 - Message de rançon

Un message attribué aux attaquants réclame un paiement et affirme que des données ont été copiées avant chiffrement. Ces affirmations ne sont pas encore vérifiées.

Question aux participants
Qui décide de la suite ? Quels conseils externes ou autorités mobilisez-vous ?

Consigner les arbitrages pendant l’exercice

Chaque décision importante doit être datée et formulée explicitement. Utilisez autant de feuilles que nécessaire. Une décision peut être révisée : dans ce cas, conservez la première décision et ajoutez la nouvelle ligne avec le motif de réévaluation.

Question réflexe	Pour chaque arbitrage : que décidons-nous, qui en est responsable, dans quel délai, et sur quel critère reviendrons-nous sur cette décision ?

05 - FEUILLE DE DÉCISIONS 1/3

Journal des décisions COMEX / COPIL

Une ligne par décision. Notez l’information disponible au moment de l’arbitrage : elle permettra de comprendre au débrief pourquoi la décision a été prise.

Heure	Information disponible	Décision / arbitrage	Responsable	Action / délai	Critère de réévaluation

05 - FEUILLE DE DÉCISIONS 2/3

Journal des décisions COMEX / COPIL

Une ligne par décision. Notez l'information disponible au moment de l'arbitrage : elle permettra de comprendre au débrief pourquoi la décision a été prise.

Heure	Information disponible	Décision / arbitrage	Responsable	Action / délai	Critère de réévaluation

05 - FEUILLE DE DÉCISIONS 3/3

Journal des décisions COMEX / COPIL

Une ligne par décision. Notez l'information disponible au moment de l'arbitrage : elle permettra de comprendre au débrief pourquoi la décision a été prise.

Heure	Information disponible	Décision / arbitrage	Responsable	Action / délai	Critère de réévaluation

Les arbitrages à reprendre au débrief

Décision critique	Éléments à consigner	Synthèse / décision retenue
Activation de la crise / direction de crise	Qui a déclenché ? À quel moment ? Qui dirige ?	
Isolement du SI	Quel périmètre ? Quel impact accepté ? Quel critère pour lever l'isolement ?	
Priorités de restauration	Quels services avant les autres ? Sur quelle justification métier ?	
Production en mode dégradé	Autorisé ou refusé ? Conditions, durée maximale, traçabilité et autorité d'arrêt.	
Restauration des sauvegardes	Quel point de restauration ? Quelle perte de données acceptée ? Qui autorise la remise en service ?	
Communication interne	Quel message, quel canal, qui valide et à quelle fréquence ?	
Communication clients / partenaires	Qui informe, avec quel niveau de certitude et quels engagements ?	
Prestataires / SOC / assureur	Qui les contacte ? Quelles informations ou preuves leur sont demandées ?	
Message de rançon	Qui pilote la décision et quels conseils externes sont sollicités ?	

06 - RESSOURCES DE CRISE

Que reste-t-il disponible lorsque le SI ne l’est plus ?

Cette grille peut être remplie pendant le débrief ou utilisée en amont d’un futur exercice. Elle vise à mettre en évidence les dépendances cachées des outils et informations nécessaires à la gestion de crise.

Ressource	Où se trouve-t-elle ?	Dépend du SI interne ?	Accessible si AD indisponible ?	Copie / accès externe ?	Responsable / notes
Procédure de crise					
PCA / PRA					
Contacts SOC / MSSP					
Contacts assureur					
Sauvegardes					
Coffre-fort de mots de passe					
Messagerie / communication					
Journaux de sécurité					
Documentation architecture					
ORKA / outil de pilotage					

07 - DÉBRIEF & RETOUR D'EXPÉRIENCE

Transformer l'exercice en enseignements

Le débrief doit être réalisé immédiatement après l'exercice, tant que les arbitrages, hésitations et difficultés sont encore présents à l'esprit.

Thème	Questions de débrief	Constats / notes
Décision	À quel moment avons-nous clairement basculé en organisation de crise ? Qui a réellement dirigé ? Quelles décisions ont été les plus difficiles ?	
Information	Quelles informations nous ont manqué ? Lesquelles pensions-nous posséder avant l'exercice ?	
Continuité	Le mode dégradé imaginé sur le papier était-il réellement applicable ? Quelle durée d'indisponibilité pouvons-nous absorber ?	
Production	Pouvions-nous continuer à produire sans ERP tout en conservant traçabilité, qualité et cohérence des données ?	
Restauration	Nos priorités de restauration étaient-elles connues ? Savions-nous quelle perte de données nous pouvions accepter ?	
Ressources de crise	Nos procédures, contacts, moyens de communication et outils auraient-ils été disponibles avec l'AD ou le réseau indisponible ?	
Prestataires	Savions-nous quoi demander au SOC, à l'infogérant, à l'assureur ou aux partenaires externes ?	
Communication	Qui valide l'information transmise aux clients, fournisseurs et autres parties prenantes ?	
Traçabilité	Avons-nous consigné les décisions, leurs responsables, les actions et les heures associées ?	
Amélioration	Quelles trois actions devons-nous engager en priorité après cet exercice ?	

08 - PLAN D’AMÉLIORATION

Passer du constat à l’action

Les enseignements issus de l’exercice doivent produire un plan d’action limité, priorisé et suivi. Il est préférable de retenir quelques actions réellement pilotées plutôt qu’une liste exhaustive sans responsable.

Priorité	Action	Responsable	Échéance	Statut	Preuve / critère de réussite

Exemples d’actions

Tester une restauration ERP ; formaliser le mode dégradé de production ; conserver hors SI principal les contacts de crise ; revoir l’authentification de secours ; vérifier la conservation externe des journaux ; rejouer l’exercice dans six mois.

CLÉS DE LECTURE

Ce que cet exercice doit faire émerger

Il n’existe pas une séquence de décisions universellement correcte. Le résultat dépend du secteur, des contraintes réglementaires, de l’architecture, de la production et de la maturité de l’organisation. En revanche, certains signaux sont particulièrement intéressants à observer.

- Le COMEX comprend-il rapidement que l’indisponibilité de l’ERP est un risque d’entreprise et pas uniquement un problème IT ?
- Les équipes savent-elles distinguer la priorité métier de la priorité technique ?
- Une autorité claire valide-t-elle l’isolement, le mode dégradé et la reprise ?
- L’entreprise sait-elle combien de temps elle peut fonctionner sans saisir de commandes, planifier, produire ou facturer ?
- Les sauvegardes sont-elles considérées comme une capacité testée plutôt que comme une simple existence documentaire ?
- Les prestataires externes sont-ils intégrés au dispositif de crise et savent-ils quelles preuves préserver ?
- Les outils nécessaires à la crise restent-ils accessibles si l’annuaire, la messagerie ou le réseau interne sont indisponibles ?
- Les décisions sont-elles historisées de manière exploitable pour le RETEX ?

La question finale — Parmi les informations qui vous ont manqué pendant cet exercice, lesquelles devriez-vous posséder avant la prochaine crise ?

En quoi ORKA peut contribuer

En amont, le scénario ransomware peut être travaillé dans la gestion des risques, en reliant l’indisponibilité de l’ERP à ses conséquences métier. Les documents et éléments de référence peuvent être centralisés. Pendant une crise, si ORKA reste lui-même disponible, l’ouverture de l’incident, la chronologie et les actions permettent de conserver un historique structuré. Après la crise, cet historique alimente le RETEX et le plan d’amélioration.

Condition essentielle — Un outil de pilotage de crise n’est utile que s’il reste accessible. Son emplacement, son authentification, ses dépendances réseau et ses moyens d’accès de secours doivent eux-mêmes être intégrés à la réflexion de continuité.

Rejouer, mesurer, améliorer

Une crise se prépare avant qu’elle commence.

Un exercice de crise n’a pas pour objectif de démontrer que tout fonctionne. Il doit au contraire rendre visibles les dépendances, ambiguïtés et fragilités qui seraient difficiles à découvrir le jour de l’incident réel.

Prochaine étape

Conservez le plan d’amélioration, affectez les actions et rejouez un scénario similaire après mise en œuvre des corrections. La progression entre deux exercices constitue un indicateur concret de résilience.

ORKA CS
Pilotage SSI - Suivi opérationnel

orkacs.com