Ne pas diffuser aux joueurs

TLP:AMBER

Exercice « REMPAR22 »

Atelier 1 - Scénario

CCA Club de la Continuité d'Activité

ANSSI

CAMPUS CYBER

Sommaire

Ne pas diffuser aux joueurs

1. RAPPELS SUR L’EXERCICE

Rappel des objectifs de l’exercice REMPAR22

Ne pas diffuser aux joueurs

Sensibiliser aux enjeux de continuité d’activité face au risque de blackout numérique

Tester les dispositifs de gestion de crise afin de s’assurer de la prise en compte des spécificités des cyber attaques

Entrainer la coordination des acteurs entre eux

Travailler les modalités de communication de crise en interne et en externe

Modalités d’exercice et formats possibles

Ne pas diffuser aux joueurs

Selon les objectifs de votre organisation, l’exercice va pouvoir prendre différentes formes:

- **Exercice sur table** (format plus léger, déroulement d’un scénario en mode présentation pour identifier les réactions de chaque partie prenante)
- **Exercice d’anticipation** (afin d’identifier les impacts du scénario sur l’organisation et les possibles évolution de la crise, et pour identifier les actions à prendre sans jouer la gestion de crise)
- **Exercice mono-cellule:**
  - Au niveau opérationnel – Equipes SI, SSI, Communication de crise, Métiers, etc.
  - Au niveau décisionnel – Equipe dirigeante
- **Exercice multi-cellules**, combinant la cellule opérationnelle et décisionnelle

Le rôle du planificateur pour l’organisation de l’exercice

Ne pas diffuser aux joueurs

- S’approprier les modalités et le scénario de l’exercice
- Définir les objectifs d’exercice pour la structure et les modalités de jeu
- Mobiliser les bonnes équipes au sein de sa structure vis-à-vis des objectifs
- Modifier le scénario en conséquence
- Intégrer les aspects logistiques pour l’exercice (réservation de salles, outillage de crise, partage de procédures, etc.)
- Préparer les joueurs pour l’exercice (brief sur leur rôle durant la crise à minima)
- Mener le RETEX de l’exercice

2. PRÉSENTATION DU SCÉNARIO

Présentation du scénario

Ne pas diffuser aux joueurs

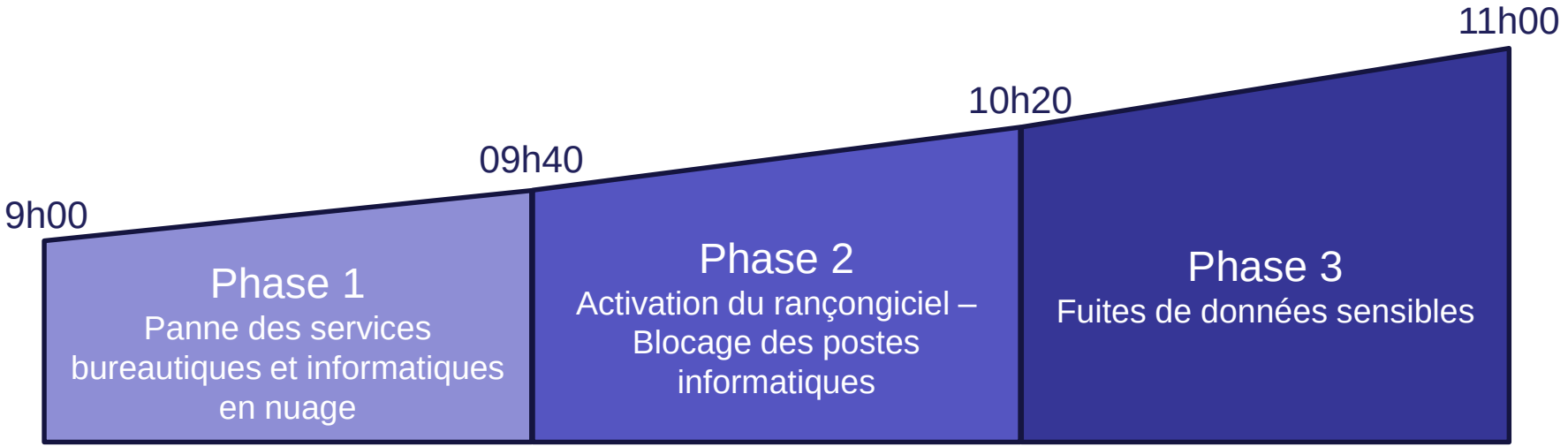
Cyberattaque via la supply-chain

Votre organisation est impactée par des cyberattaques sur un fournisseur de services infonuagiques, ce qui conduit à la perte d'applications bureautiques et en ligne, ainsi qu'à la fuite de données sensibles.
Votre organisation va devoir gérer les impacts de cette attaque majeure sur ses activités:

- Perte de production (impossibilité de travailler, de fournir un service ou de produire un bien), ce qui conduit à
  - Pression des équipes internes pour la reprise d'activité
  - Perte financière
- Pression médiatique importante (relai sur les réseaux sociaux et les médias de l'attaque)
- Perte de confiance des parties prenantes (impact sur l'image de l'entreprise, fuites de données sensibles – données personnelles, fuites de coûts de production, etc.)
- Obligations réglementaires à respecter

Temporalité de la crise

Ne pas diffuser aux joueurs



Suite à la **perte d'infrastructure** d'un fournisseur infonuagique, les **services de bureautique** (messagerie, tableur, traitement de texte, stockage en ligne, etc.) ainsi que plusieurs **applications SaaS** cessent de fonctionner.

Après avoir récolté des données sensibles, l'attaquant utilise les informations récupérées pour **s'introduire sur le réseau interne** et pour **chiffrer des postes de travail et des serveurs** avec un **rançongiciel.**

Pour mettre la pression sur les organisations touchés, **l'attaquant décide de publier certaines données sensibles** récupérées sur les stockages en ligne.

Phase 1 - Panne des services bureautiques et informatiques en nuage

Ne pas diffuser aux joueurs

Contexte: Un fournisseur de service infonuagique** est victime d'un chiffrement massif sur ses hyperviseurs*. Les applications du fournisseur s'appuyant sur ces services d'hébergement (bureautique, mail) mais également d'autres services numériques s'appuyant sur l'hébergement de ce fournisseur (RH, paie, etc.) sont indisponibles. Les services de stockage de données en ligne sont également indisponibles.

Enjeux et impacts:

- Comprendre l'origine de la défaillance et les alternatives pour continuer à travailler
- Répondre à la pression interne des collaborateurs et sur la pression externe des clients et des médias sur l'indisponibilité des services
- Identifier les moyens et la coordination nécessaire avec le fournisseur touché

Aspect cyber : Compromission d'un fournisseur de service infonuagique à partir d'une mise à jour vérolé du logiciel de supervision. Déploiement d'un spyware pour collecter des données stratégiques présentes sur les machines virtuelles déployées sur les hyperviseur. Chiffrement par rançongiciel des machines virtuelles de l'hébergeurs, et sur le SI d'autres clients à partir des données récupérés. La transmission du rançongiciel est faite de manière manuelle.

Equipes pertinentes à impliquer : DSI, SSI, équipes métiers, Continuité d'activité, Direction de crise, communication, juridique, etc.

A adapter en priorité: Applications internes et externes indisponibles, périmètre touché, noms des départements touchés, noms de clients ou fournisseurs importants

**Infrastructure permettant de virtualiser un grand nombre serveurs sur une machine unique, permettant une administration commune et un partage des ressources*
***Si l'organisation ne possède pas d"infrastructure Cloud, elle peut simuler une panne suite à la mise à jour non réversible d'une technologie très utilisé dans l'organisation (ex: système d'exploitation).*

Phase 2 - Activation du rançongiciel / Blocage des postes informatiques

Ne pas diffuser aux joueurs

Contexte: L'attaquant déploie le rançongiciel à partir des infos récoltés à travers l'attaque. Plusieurs postes de travail et serveurs impliqués dans des activités critiques de l'organisation sont chiffrés et inaccessibles. Les équipes s'inquiètent de perdre leurs capacités à travailler. Le public s'inquiète de voir l'organisation victime de la cyberattaque, et demande des comptes sur le niveau de protection apporté. Les équipes SSI et SI sont fortement mobilisées.

Enjeux et impacts:

- Endiguer la diffusion du rançongiciel sur le réseau de l'entreprise
- Identifier les mécanismes de continuité d'activité à activer
- Mettre en place la stratégie de communication de crise pour répondre à la pression médiatique
- Anticiper la reconstruction et la reprise d'activité

Aspect cyber : Lors de sa phase d'exfiltration de données, l'attaquant a récolté des informations d'accès à distance et des identifiants/mots de passe d'administration. Avec ceux-ci, il s'introduit sur le réseau, escalade ses privilèges successivement pour prendre le contrôle d'un contrôleur de domaine, récolte des données supplémentaires et lance le déploiement du rançongiciel.

Equipes pertinentes à impliquer : DSI, SSI, équipes métiers, Continuité d'activité, Direction de crise, communication, etc.

A adapter en priorité: Périmètre victime du rançongiciel, impacts métier, obligations contractuelles ou réglementaires, etc.

Phase 3 - Fuites de données sensibles

Ne pas diffuser aux joueurs

Contexte: Pour mettre la pression sur l'organisation victime et encourager le paiement d'une rançon, l'attaquant met en ligne un jeu de données de l'entreprise. Il menace de mettre en vente d'autres données dans les prochaines heures sans paiement d'une rançon. La presse et le grand public se saisissent du sujet et demandent des réponses sur les conséquences de cette fuite.

Enjeux et impacts:

- Analyser les données et les conséquences de la fuite pour l'activité et l'organisation
- Notification des autorités pertinentes et des parties prenantes
- Restreindre l'accès aux données encore exposé

Aspect cyber : L'attaquant a rassemblé l'ensemble des données disponibles sur les différents réseaux de stockage de données en ligne, et a réalisé un extrait en se concentrant sur des données sensibles pour encourager la reprise médiatique. Ils les met à disposition sur sa plateforme de fuite de données et met des annonces de vente sur les forums cybercriminels.

Equipes pertinentes à impliquer : DSI, SSI, équipes métiers, Continuité d'activité, Direction de crise, communication, juridique, etc.

A adapter en priorité: Type de données ayant fuitées, obligations réglementaires, conséquences métier, etc.

Les effets des attaques sont croissants au fur et à mesure des phases d'exercice. Ainsi, la fuite de donnée est une addition au fait que les applications du fournisseurs sont indisponibles et qu'une partie du SI est chiffrée.

Adaptation selon les secteurs

Ne pas diffuser aux joueurs

Pour adresser les spécificités de chaque secteur, le chronogramme d'exercice a été adapté pour introduire des pans scénaristiques contextualisés sur les secteurs suivants :

Banque / Assurance

Industrie

Services (public/privé)

Editeurs

Conseil

Ces spécificités ne porteront pas sur les aspects techniques, mais plutôt sur les conséquences métiers de l'attaque sur l'activité:

- Type d'applications bureautique perdu suite à la perte d'infrastructure infonuagique
- Pression de la part du métier
- Périmètre d'exécution du rançongiciel
- Type de données fuitant sur Internet
- Obligations réglementaires
- Etc.

Les règles d’adaptation

Ne pas diffuser aux joueurs

Respecter la temporalité des phases

Pour que le scénario soit cohérent d’une structure à l’autre, il est important de ne pas sortir des phases horaires prévues pour chaque temporalité de crise. Durant l’exercice, le timing devra également être respecté pour éviter les écarts d’une organisation à l’autre.

Respecter les aspects techniques de l’attaque

Afin de garder une cohérence de scénario, les modifications ne peuvent pas toucher les aspects techniques. Les attaques doivent rester en ligne avec celles du scénario (chiffrement d’infrastructures infonuagiques, rançongiciel sur le réseau interne, fuite de données sensibles).

Prendre en compte les interactions avec l’écosystème

Dans les nouveautés intégrés dans le scénario initiale, les nouvelles interactions avec l’écosystème doivent être anticipées. Ainsi, si un stimulus requierant une interaction avec un tiers simulé est introduit, il est bon de vérifier avec l’animation centrale si celle-ci n’est pas déjà simulée ailleurs.

Le kit de planification

Ne pas diffuser aux joueurs

Pour vous aider dans la préparation et l'adaptation du scénario, un **kit de planification** est mis à disposition des planificateurs:

- **Chronogramme du scénario** – Temporaire, version finale envoyé très prochainement
- **Pack de stimuli médiatique** (modèle de stimuli)
- **Fiche pratique d'adaptation des stimuli**
- **Deck de présentation du scénario** (présentation du jour)

Le dossier de mise en situation (DMS) ainsi que les questions de debriefing seront partagés plus tard.

Le rôle du planificateur pour le scénario

Ne pas diffuser aux joueurs

Prendre connaissance du scénario dans sa globalité, et bien relire le chronogramme fourni

Identifier les équipes et personnes à mobiliser, vis-à-vis du chronogramme et des objectifs choisis pour l'exercice

Modifier le chronogramme pour rendre les stimuli cohérents et personnalisés avec la structure joueuse

Adapter les injects médiatiques pour intégrer le nom ou le contexte de l'entreprise (voir pack stimuli)

3. CONSEIL POUR LES PLANIFICATEURS

Planning recommandé de préparation

Ne pas diffuser aux joueurs

Phase 1 :
- Prendre connaissance du scénario
- Déterminer les objectifs de jeu pour la structure
- Identifier les joueurs/équipes à mobiliser
- Identifier si des préparations supplémentaires sont nécessaires (formations, exercices sur table, etc.)

Phase 2 :
- Bloquer les agendas des joueurs pour l'exercice et pour le briefing joueur
- Bloquer les salles nécessaires pour le jour de l'exercice
- Identifier les éléments logistiques supplémentaires (outillage de crise, restauration, etc.)
- Commencer la modification du scénario
- Réfléchir à la valorisation de l'exercice en interne

Phase 3 :
- Finaliser une première version du chronogramme adaptée à la structure
- Présenter aux responsables d'équipes mobilisées les objectifs et enjeux de l'exercice
- Identifier les modalités de RETEX de l'exercice pour la structure
- Préparer les éventuelles « mallettes de crise » à utiliser par les participants

Phase 4 :
- Finaliser les aspects logistiques (outillage de crise, restauration, etc.)
- Finaliser l'adaptation du chronogramme
- Aligner les derniers changements sur les stimuli médiatiques
- Partager aux joueurs les matériaux d'exercice pertinents (malette de crise, annuaires, DMS, etc.)
- Identifier des observateurs et/ou animateurs d'exercice
- Finaliser l'animation et l'envoi des injects

Phase 4 :
- Briefer les observateurs et les animateurs
- Valider les derniers aspects logistiques

Conseil sur comment mener la préparation en interne

Ne pas diffuser aux joueurs

- Identifier des complices (non-joueurs!) pour vous aider à modifier le chronogramme en prenant en compte la réalité métier
- Bloquer les agendas des joueurs et les salles le plus tôt possible
- Identifier si des joueurs ont besoin d'être formés en amont de l'exercice, et organiser des formations ou exercices sur table si nécessaire
- Consolider la documentation de crise pour les joueurs
- Briefer en amont de l'exercice les dirigeants participants à l'exercice
- Penser à la valorisation de l'exercice
- Ne pas laisser les aspects logistiques au dernier moment

Logistique à prendre en compte

Ne pas diffuser aux joueurs

- Salle de crise
- Outils de crise (ordinateurs, téléphone, points d’accès internet) et logiciels (main courante, espace de stockage, messagerie, etc.)
- Accès au bâtiment de la salle de crise
- Badges (si les participants ne se connaissent pas)
- Restauration (petit-déjeuner, déjeuner) si nécessaire

4. FAQ

Questions / Réponses

Ne pas diffuser aux joueurs

- **Est-ce que le kit intègre des stimuli «type » ?** Oui

- **De quelles manières peut-on interagir avec les acteurs de son secteur ?** Cet aspect dépend de vos objectifs d'exercice. Il peut être intéressant de jouer certaines interactions mais cela nécessite une coordination en amont entre les entités et de respecter le timing d'exercice.

- **L'organisation devra t-elle contacter les institutions pour jouer les procédures d'alerte ?** Pour les institutions, il faudra uniquement simuler ces échanges.
- **Est-il possible de mener l'exercice à la fois en distanciel et présentiel** ? Oui, cela dépend de vos objectifs et procédures internes.

- **Quel est le lien entre l'incident chez le fournisseur et le rançongiciel pour le scénario ?** Ces attaques sont menées par le même groupe d'attaquants mais il s'agit de les distinguer. Pour l'incident sur le fournisseur, un de leur logiciel a été compromis (attaque par supply chain) et créer cette indisponibilité de services. Pour le rançongiciel, les attaquants ont réussi à trouver des portes vers d'autres cibles (ex :accès à des mots de passe administrateur) pour se latéraliser.