Réponse à une cyberattaque

Le serveur de l'entreprise OmniWeb a subi une cyberattaque d'une ampleur inédite, un vendredi à 17 heures.

Après évaluation des dégâts, le choix est fait de réinstaller l'intégralité des services sur le serveur de secours, en partant de 0. Il s'avère que grâce aux travaux réalisés en amont, les sauvegardes étaient correctement établies et à jour. Elles étaient stockées hors site et n'ont pas été compromises par la cyberattaque. On suppose que certains sites contenaient des données sensibles (données bancaires).

On vous propose une première trame de Plan de Reprise d'Activité (PRA) pour faire face à cet incident. Il est nécessaire de l'affiner avant de mettre en œuvre cette restauration afin que les rôles soient précisément établis.

1. Évaluation de l'incident
2. Communication INTERNE et EXTERNE
3. Activation du PRA avec constitution de l'équipe de crise
4. Priorisation des services critiques
5. Mise en place rapide d'un mode dégradé temporaire
6. Mise en place du nouvel environnement de production
7. Restauration des données depuis les sauvegardes
8. Rétablissement des services
9. Vérification et tests de fonctionnement
10. Communication INTERNE et EXTERNE
11. Retour à la normale
12. Communication EXTERNE
13. Revue post-incident où apprendre de ses erreurs
14. Mise à jour du PRA selon les constatations établies
15. Communication INTERNE avec formation et sensibilisation

t

Travail à faire :

1. Détaillez, pour chacun des points :
    - Les actions à mener concrètement
    - Les personnes concernées, qu'elles soient internes ou externes à l'organisation
    - Les rôles et responsabilités des acteurs internes

   Afin de vous aider, voici la trame de tableau attendue pour la première étape :

Évaluation de l'incident : comprendre quel est le problème et identifier sa source et ses répercussions

Client	• Constat du dysfonctionnement • Appel à l'entreprise
DSI	• État des lieux technique et fonctionnel • Information de la direction et de son équipe
Direction	• Prise de connaissance de l'information sur l'attaque
Administration systèmes et réseaux	• Prise de connaissance de l'information sur l'attaque
Développement	• Prise de connaissance de l'information sur l'attaque

2. Évaluez les durées de chaque tâche. Pensez à évaluer si certaines tâches peuvent être exécutées en parallèle par des acteurs différents.

3. Rédigez intégralement les mails à destination de l'ensemble de la clientèle sur les étapes de communication.

1. **Évaluation de l'incident**

Client	• Constat du dysfonctionnement • Appel à l'entreprise	2H
DSI	• État des lieux technique et fonctionnel • Information de la direction et de son équipe	
Direction	• Prise de connaissance de l'information sur l'attaque	
Administration systèmes et réseaux	• Prise de connaissance de l'information sur l'attaque	
Développement	• Prise de connaissance de l'information sur l'attaque	

2. **Communication INTERNE et EXTERNE**

Client	• Est prévenu par la direction	1H
DSI	• Alerte du département direction/communication • Est prévenu en interne par l'administrateur réseau • Prévient le service développement • Prévient la direction	
Direction	• Communique sur la situation	

	• Est prévenu en interne par le DSI • Préviens les clients	
Administration systèmes et réseaux	• Est le premier à être au courant • Prévient le DSI en interne	
Développement	• Est prévenu en interne par le DSI	

3. **Activation du PRA avec constitution de l'équipe de crise**

Client		1H
DSI	• Dirige l'équipe de crise	
Direction	• Confirme la décision	
Administration systèmes et réseaux	• Assure la disponibilité des ressources nécessaires	
Développement	• Contribue à la réinstallation des services critiques	

4. **Priorisation des services critiques**

Client	•	1H
DSI	• Détermine les services prioritaires à mettre en place	
Direction	• Prends la décision concernant les services critiques	
Administration systèmes et réseaux	• Collabore avec le DSI	
Développement	• Collabore avec le DSI	

5. **Mise en place rapide d'un mode dégradé temporaire**

Client	• Récupère une partie de ses services	2H
DSI	• Mise en place d'un mode dégradé temporaire	
Direction	• Informe les clients du retour d'une partie des activités	
Administration systèmes et réseaux	• Déploie les configs de secours, assure le fonctionnement minimal	
Développement	• Identifie quels fonctionnalités sont à rétablir en premier • Communique avec l'administrateur réseau pour connaître les contraintes réseaux et les besoins • Réalise des tests pour s'assurer du bon fonctionnement du mode dégradé	

6. **Mise en place du nouvel environnement de production**

Client	• Communique ses besoins • Fais des retours d'expériences	4H
DSI	• Mise en place du nouvel	

	environnement de production	
Direction	• Fourni le budget nécessaire • Évalue les performances de l'entreprise après le déploiement	
Administration systèmes et réseaux	• Communique avec le développeur pour connaître les attentes de la nouvelle plateforme • Identifie les besoins d'infrastructure réseau et de sécurité • Surveille les performances de la plateforme + son bon fonctionnement	
Développement	• Configuration spécifique des applications	

7. **Restauration des données depuis les sauvegardes**

Client	• Communique les informations essentielles • Fais des retours sur la restauration des données	4H
DSI	• Coordonne la restauration des données	
Direction	• Communique sur les impacts survenus au cours de l'opération	
Administration systèmes et réseaux	• Vérifie l'intégrité des sauvegardes • Prévoit les maintenances • Surveille le bon fonctionnement de la récupération des données	
Développement	• Identifie les données essentielles • Communique avec l'administrateur réseau pour avoir accès aux sauvegardes de données • Vérifie l'intégrité des données à l'aide de tests • Restaure les données	

8. **Rétablissement des services**

Client	• Communication avec le service du DSI	4H
DSI	• Remise en fonctionnement des serveurs info	
Direction	• Gestion de l'organisation des	

	différents services	
Administration systèmes et réseaux	• Surveille les système restaurés pour détecter des anomalie ou prendre des mesures nécessaires en cas de problème	
Développement	• Résolution des problèmes spécifiques et identifie et corrige les éventuels problèmes logiciels survenus lors du processus de rétablissement des services.	

9. **Vérification et tests de fonctionnement**

Client	• Vérification de la disponibilité et de la performance des services rétablis, ainsi que du bon fonctionnement des fonctionnalités critiques pour son activité.	6H
DSI	• Effectue des tests de fonctionnement et de performance pour s'assurer que tous les services rétablis répondent aux normes de qualité et de performance définies.	
Direction	• Validation des tests de fonctionnement pour confirmer que les opérations peuvent reprendre normalement et que les problèmes potentiels ont été résolus.	
Administration systèmes et réseaux	• Effectue des tests de redondance et de failover pour garantir la fiabilité et la disponibilité des systèmes restaurés dans des situations d'urgence.	
Développement	• Effectue des tests d'intégration pour vérifier que les applications rétablies fonctionnent correctement avec les autres composants du système.	

10. **Communication INTERNE et EXTERNE**

Client	• Diffusion d'une communication interne pour informer les employés sur la reprise des	1H

	activités normales et les mesures prises pour éviter de futurs incidents.	
DSI	• Communication externe : Envoie des notifications aux clients et aux partenaires commerciaux pour les informer de la résolution de l'incident et des mesures prises pour garantir la sécurité des données.	
Direction	• Diffusion d'un message à l'ensemble du personnel pour les informer sur la reprise des activités et les remercier pour leur coopération pendant la période perturbée.	
Administration systèmes et réseaux	• Communication interne : Diffusion d'informations aux employés sur les étapes suivies pour rétablir les services et les consignes à suivre en cas de problème persistant.	
Développement	• Communication interne : Informe les membres de l'équipe de développement sur les impacts de l'incident sur les systèmes et les mesures prises pour résoudre les problèmes.	

11. **Retour à la normale**

Client	• Confirmation de la reprise d'activité et évaluation de la qualité de service.	2H
DSI	• Surveillance continue des systèmes pour détecter tout problème résiduel et garantir un fonctionnement optimal.	
Direction	• Évaluation globale de l'impact de l'incident et des actions correctives entreprises pour assurer une transition en douceur vers l'état opérationnel normal.	
Administration systèmes et réseaux	• Analyse post-mortem pour identifier les causes sous-jacentes de l'incident et recommander des mesures	

	préventives pour éviter des incidents similaires à l'avenir.	
Développement	• Évaluation des processus de développement et identification des domaines à améliorer pour renforcer la résilience des systèmes contre les cyberattaques.	

12. **Communication EXTERNE**

Client	•	2H
DSI	•	
Direction	•	
Administration systèmes et réseaux	•	
Développement	•	

13. **Revue post-incident où apprendre de ses erreurs**

Client	•	2H
DSI	•	
Direction	•	
Administration systèmes et réseaux	•	
Développement	•	

14. **Mise à jour du PRA selon les constatations établies**

Client	•	2H
DSI	•	
Direction	•	
Administration systèmes et réseaux	•	
Développement	•	

15. **Communication INTERNE avec formation et sensibilisation**

Client	•	2H
DSI	•	
Direction	•	
Administration systèmes et réseaux	•	
Développement	•	