PRA – Réponse à une cyberattaque

Évaluation de l'incident : 45 minutes à 1H30

Client	Constat du dysfonctionnement Appel à l'entreprise
DSI	Etat des lieux techniques 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

Communication INTERNE et EXTERNE : 1 Heure

Client	Attente de la réparation du service.
DSI	Discussion avec la direction et ses équipes pour la mise en place d'une stratégie pour la remise en activité des services.
Direction	Communiquer avec les clients pour expliquer la situation.
Administration systèmes et réseaux	Réfléchis à la mise en place d'une stratégie pour la remise en activité des services.
Développement	Réfléchis à la mise en place d'une stratégie pour la remise en activité des services.

Activation du PRA avec constitution de l'équipe de crise : 45 minutes

Client	Attente de la réparation des services.
DSI	Coordination des équipes pour la mise en place du PRA.
Direction	Attente de la réparation des services.
Administration systèmes et réseaux	Prépare la mise en place du PRA.
Développement	Prépare la mise en place du PRA.

Priorisation des services critiques : 1 h

Client	Attente de la réparation des services.
DSI	Mise en place du PRA avec ses équipes.
Direction	Attente de la réparation des services.
Administration systèmes et réseaux	Mise en place du PRA avec ses équipes.
Développement	Mise en place du PRA avec ses équipes.

PAUSE 1H

Mise en place rapide d'un mode dégradé temporaire : 2H

Client	Attente de la réparation des services.
DSI	Met en place le mode dégradé temporaire.
Direction	Attente de la réparation des services.
Administration systèmes et réseaux	Met en place le mode dégradé temporaire.
Développement	Met en place le mode dégradé temporaire.

Mise en place du nouvel environnement de production : 2H

Client	Accès au services en mode dégradé.
DSI	Coordonne et aide les équipes sur l'installation
Direction	Communique par rapport à l'accès aux services dans un mode restreint.
Administration systèmes et réseaux	Installation des services sur le nouvel environnement de production.
Développement	Installation des services sur le nouvel environnement de production.

Restauration des données depuis les sauvegardes : 1h à 3h

Client	Accès au services en mode dégradé.
DSI	Coordonne et aide les équipes sur la restauration.
Direction	Accès au services en mode dégradé.
Administration systèmes et réseaux	Restaure les sauvegardes des anciens serveurs.
Développement	Restaure les bases de données des clients.

FIn de journée 13h

Restauration des données depuis les sauvegardes : 1H à 2H

Client	Valider la remise en service des services restaurés.
DSI	Superviser le rétablissement des services.
Direction	Surveiller la progression et fournir des directives supplémentaires si nécessaire.
Administration systèmes et réseaux	Rétablir les services conformément aux exigences.
Développement	Vérifier le bon fonctionnement des services rétablis et effectuer des ajustements si nécessaire.

Vérification et tests de fonctionnement : 3h

Client	Valider les tests de fonctionnement.
DSI	Superviser les tests de fonctionnement pour s'assurer de la complète fonctionnalité.
Direction	Surveiller les tests et approuver la reprise complète des activités.
Administration systèmes et réseaux	Effectuer les tests de fonctionnement et rectifier les problèmes éventuels.
Développement	Participer aux tests de fonctionnement et résoudre les problèmes techniques.

PAUSE 1h

Communication INTERNE et EXTERNE : 1H

Client	Informer les parties externes si nécessaire.
DSI	Superviser et coordonner la communication à la fois interne et externe.
Direction	Fournir des directives stratégiques pour la communication avec les parties prenantes.
Administration systèmes et réseaux	Collaborer à la communication technique interne.

Développement	Fournir des informations techniques pertinentes pour la communication externe.

FIN DE JOURNÉE 14h

Client	Informer les parties externes si nécessaire.

Retour à la normale : 1H à 2H

Client	Valider le retour à la normale des opérations.
DSI	Coordonner le processus de retour à la normale.
Direction	Surveiller le processus et fournir des directives finales si nécessaire.
Administration systèmes et réseaux	Finaliser les actions nécessaires pour un retour complet à la normale.
Développement	Assurer que toutes les fonctionnalités sont rétablies conformément aux spécifications.

Communication EXTERNE : 1H

DSI	Coordonner la communication externe sur le retour à la normale.
Direction	Valider le message de communication externe.
Administration systèmes et réseaux	Collaborer à la communication technique externe.
Développement	Fournir des informations techniques pertinentes pour la communication externe.

Revue post-incident où apprendre de ses erreurs : 1H à 2H

Client	Participer à la revue post-incident pour fournir des commentaires sur l'expérience client.
DSI	Organiser et diriger la revue post-incident pour identifier les causes profondes et les leçons apprises.
Direction	S'engager dans la revue post-incident pour comprendre les aspects stratégiques de la gestion de crise.
Administration systèmes et réseaux	Contribuer à l'analyse des erreurs et des améliorations possibles du processus.

Développement	Fournir des informations sur les aspects techniques de l'incident et proposer des solutions d'amélioration.

PAUSE 1h

Mise à jour du PRA selon les constatations établies : 1H

Client	Valider les mises à jour proposées pour le Plan de Reprise d'Activité (PRA).
DSI	Coordonner la mise à jour du PRA en fonction des constatations et des leçons apprises.
Direction	Surveiller et approuver les modifications apportées au PRA.
Administration systèmes et réseaux	Mettre en œuvre les changements techniques
	nécessaires dans le PRA.
Développement	Proposer des ajustements ou des améliorations spécifiques liés aux applications ou aux systèmes.

Communication INTERNE avec formation et sensibilisation : 1H à 2H

Client	Appuyer et participer à la communication interne, en soutenant la formation et la sensibilisation.
DSI	Organiser et superviser la communication interne, ainsi que la mise en place des sessions de formation et de sensibilisation.
Direction	Fournir des directives stratégiques et un soutien pour la communication interne et les efforts de formation.
Administration systèmes et réseaux	Participer à la formation et à la sensibilisation, en particulier en ce qui concerne les aspects techniques.
Développement	Contribuer à la formation sur les aspects techniques spécifiques liés aux applications ou aux systèmes.