Évaluation de l’incident

Actions à mener concrètement:

1. Constat du dysfonctionnement.
2. Analyse préliminaire de l'incident pour identifier sa source et ses répercussions.
3. Prise de mesures immédiates pour isoler le serveur touché et limiter la propagation de l'attaque.
4. Collecte des premières données sur l'ampleur de l'attaque et des dommages subis.
5. Évaluation de l'impact sur les données sensibles, notamment les données bancaires.

Personnes concernées:

- Client:
    - Responsable technique en contact avec l'entreprise.
- DSI (Directeur des Systèmes d'Information):
    - Équipe technique pour l'état des lieux.
- Direction:
    - Responsable hiérarchique de la DSI pour information.
- Administration systèmes et réseaux:
    - Équipe en charge de la gestion du serveur touché.
- Développement:
    - Équipe en charge des applications hébergées sur le serveur.

Rôles et responsabilités des acteurs internes:

- Client: Signaler le dysfonctionnement et fournir des informations initiales.
- DSI: Coordonner l'évaluation technique de l'incident et informer la direction.
- Direction: Prendre connaissance de l'incident et autoriser les mesures à prendre.
- Administration systèmes et réseaux: Assurer l'analyse technique de l'incident.
- Développement: Apporter des informations sur les applications impactées.

Durée estimée: 1 heure pour une évaluation préliminaire.

Communication INTERNE et EXTERNE

Actions à mener concrètement:

1. Notification interne à l'ensemble du personnel sur l'incident en cours et les mesures prises.
2. Communication externe aux clients sur l'incident, les impacts potentiels et les actions en cours.

Personnes concernées:

- Communication interne:
    - Direction, DSI.
- Communication externe:
    - Service communication, direction.

Rôles et responsabilités des acteurs internes:

- Direction: Valider le contenu des messages.
- DSI: Coordonner la diffusion des informations en interne.
- Service communication: Rédiger et diffuser les communications externes.

Durée estimée: 30 minutes pour une notification interne et 1 heure pour une communication externe.

Exemple de mail à destination de la clientèle:

Objet: Incident technique - Communication importante

Chers clients,

Nous vous informons qu'une cyberattaque sans précédent a touché nos serveurs, impactant ainsi l'accès à nos services. Nous prenons cette situation très au sérieux et mettons tout en œuvre pour rétablir la situation dans les meilleurs délais.

Voici les étapes que nous mettons en place pour gérer cette situation :

1. Évaluation de l'incident: Nous sommes actuellement en train d'évaluer l'ampleur de l'attaque et ses répercussions sur nos systèmes.
2. Activation du Plan de Reprise d'Activité (PRA): Une équipe de crise a été constituée pour gérer cette situation d'urgence.
3. Priorisation des services critiques: Nous identifions les services les plus critiques pour les restaurer en priorité.
4. Mise en place d'un mode dégradé temporaire: Nous mettons en place des solutions temporaires pour assurer un fonctionnement minimal de nos services.
5. Restauration des données depuis les sauvegardes: Nous restaurons les données à partir de nos sauvegardes hors site, qui n'ont pas été compromises par l'attaque.
6. Rétablissement des services: Nous travaillons sans relâche pour rétablir l'accès à nos services le plus rapidement possible.

Nous vous tiendrons informés de l'évolution de la situation et nous vous prions de nous excuser pour les désagréments occasionnés. La sécurité de vos données reste notre priorité absolue.

Cordialement,

[Votre entreprise]

Évaluation de l’incident

Actions à mener concrètement:

1. Constat du dysfonctionnement: Les équipes techniques et les utilisateurs concernés doivent signaler tout dysfonctionnement ou indisponibilité des services.
2. Analyse préliminaire de l'incident: Une première évaluation est effectuée pour comprendre la nature et l'ampleur de l'attaque, identifier sa source et évaluer ses répercussions.
3. Prise de mesures immédiates: Des mesures sont prises pour isoler le serveur touché et limiter la propagation de l'attaque.

4. Collecte des premières données: Des données sont collectées sur l'incident, notamment sur les dommages subis et l'impact sur les systèmes et les données sensibles.

Personnes concernées:

- Client: Responsable technique en contact avec l'entreprise.
- DSI (Directeur des Systèmes d'Information): Équipe technique pour l'état des lieux.
- Direction: Responsable hiérarchique de la DSI pour information.
- Administration systèmes et réseaux: Équipe en charge de la gestion du serveur touché.
- Développement: Équipe en charge des applications hébergées sur le serveur.

Rôles et responsabilités des acteurs internes:

- Client: Signaler le dysfonctionnement et fournir des informations initiales.
- DSI: Coordonner l'évaluation technique de l'incident et informer la direction.
- Direction: Prendre connaissance de l'incident et autoriser les mesures à prendre.
- Administration systèmes et réseaux: Assurer l'analyse technique de l'incident.
- Développement: Apporter des informations sur les applications impactées.

Communication INTERNE et EXTERNE

Actions à mener concrètement:

1. Notification interne: Informer l'ensemble du personnel sur l'incident en cours, les mesures prises et les instructions à suivre.
2. Communication externe aux clients: Informer les clients sur l'incident, les impacts potentiels sur leurs services et les actions en cours pour y remédier.

Personnes concernées:

- Communication interne: Direction, DSI.
- Communication externe: Service communication, direction.

Rôles et responsabilités des acteurs internes:

- Direction: Valider le contenu des messages et superviser la communication.

- DSI: Coordonner la diffusion des informations en interne.
- Service communication: Rédiger et diffuser les communications externes.

Activation du PRA avec constitution de l’équipe de crise

Actions à mener concrètement:

1. Activation du Plan de Reprise d'Activité (PRA): Mise en place de l'équipe de crise et allocation des rôles et responsabilités.
2. Constitution de l'équipe de crise: Sélection des membres de l'équipe de crise, incluant des représentants de chaque domaine concerné.

Personnes concernées:

- DSI: Coordonner l'activation du PRA et diriger l'équipe de crise.
- Équipe de crise: Membres désignés de chaque service pour participer à la gestion de l'incident.

Rôles et responsabilités des acteurs internes:

- DSI: Superviser les opérations de l'équipe de crise et assurer la coordination entre les différents services.
- Équipe de crise: Participer à l'analyse de l'incident et à la mise en œuvre des actions de restauration.

Priorisation des services critiques

Actions à mener concrètement:

1. Identification des services critiques: Évaluation des services essentiels à la continuité des opérations de l'entreprise.
2. Priorisation des efforts de restauration: Détermination des services à restaurer en priorité pour minimiser l'impact sur les activités.

Personnes concernées:

- Équipe de crise: Membres désignés chargés de l'analyse des services et de leur priorisation.

Rôles et responsabilités des acteurs internes:

- Équipe de crise: Analyser l'importance de chaque service et recommander l'ordre de restauration en fonction de leur criticité.

Mise en place rapide d’un mode dégradé temporaire

Actions à mener concrètement:

1. Déploiement de solutions temporaires: Mise en place de mesures provisoires pour assurer un fonctionnement minimal des services.
2. Configuration de systèmes de secours: Activation de systèmes alternatifs pour remplacer les fonctionnalités affectées.

Personnes concernées:

- Administration systèmes et réseaux: Équipe en charge de la mise en place des solutions temporaires.

Rôles et responsabilités des acteurs internes:

- Administration systèmes et réseaux: Configurer et déployer les solutions de secours en fonction des besoins identifiés.

Mise en place du nouvel environnement de production

Actions à mener concrètement:

1. Configuration du nouvel environnement: Installation et configuration des serveurs et des logiciels nécessaires pour reconstruire l'infrastructure.
2. Transfert des données: Transfert des données depuis les sauvegardes vers le nouvel environnement.

Personnes concernées:

- Administration systèmes et réseaux: Équipe en charge de la configuration et du déploiement du nouvel environnement.

Rôles et responsabilités des acteurs internes:

- Administration systèmes et réseaux: Assurer la mise en place efficace du nouvel environnement et le transfert sécurisé des données.

Restauration des données depuis les sauvegardes

Actions à mener concrètement:

1. Identification des sauvegardes adéquates: Sélection des sauvegardes appropriées pour chaque service ou ensemble de données à restaurer.
2. Restauration des données: Procéder à la récupération des données à partir des sauvegardes stockées hors site.

Personnes concernées:

- Administration systèmes et réseaux: Équipe en charge de la gestion des sauvegardes et de leur restauration.

Rôles et responsabilités des acteurs internes:

- Administration systèmes et réseaux: Superviser le processus de restauration des données et s'assurer de son bon déroulement.

Rétablissement des services

Actions à mener concrètement:

1. Configuration des services: Rétablissement des services affectés en suivant les procédures définies.

2. Test de fonctionnement: Vérification de la fonctionnalité des services restaurés pour s'assurer qu'ils répondent aux besoins opérationnels.

Personnes concernées:

- Administration systèmes et réseaux: Équipe en charge du rétablissement des services.

Rôles et responsabilités des acteurs internes:

- Administration systèmes et réseaux: Configurer et tester les services restaurés pour garantir leur bon fonctionnement.

Vérification et tests de fonctionnement

Actions à mener concrètement:

1. Vérification des services restaurés: Contrôle approfondi de chaque service pour identifier d'éventuels problèmes résiduels.
2. Tests de fonctionnement: Exécution de scénarios de test pour valider le bon fonctionnement global des systèmes restaurés.

Personnes concernées:

- Administration systèmes et réseaux: Équipe en charge de la vérification et des tests.

Rôles et responsabilités des acteurs internes:

- Administration systèmes et réseaux: Effectuer des tests exhaustifs pour garantir la fiabilité et la stabilité des services restaurés.

Retour à la normale

Actions à mener concrètement:

1. Confirmation du rétablissement complet: Vérification que tous les services sont opérationnels et que l'entreprise peut reprendre ses activités normales.
2. Communication interne: Informer l'ensemble du personnel que la situation est revenue à la normale et donner des instructions, le cas échéant.

Personnes concernées:

- Administration systèmes et réseaux: Équipe en charge de confirmer le rétablissement complet.
- Direction: Responsable hiérarchique pour la communication interne.

Rôles et responsabilités des acteurs internes:

- Administration systèmes et réseaux: Confirmer que tous les services sont opérationnels.
- Direction: Informer le personnel que la situation est revenue à la normale et donner des consignes si nécessaire.

Communication EXTERNE

Actions à mener concrètement:

1. Notification aux clients: Informer les clients que les services sont rétablis et que l'entreprise est de nouveau opérationnelle.
2. Rétablissement de la confiance: Rassurer les clients sur la sécurité et la fiabilité des services après l'incident.

Personnes concernées:

- Service communication: Équipe chargée de la communication externe.
- Direction: Responsable hiérarchique pour la validation du message.

Rôles et responsabilités des acteurs internes:

- Service communication: Rédiger et diffuser les communications externes.
- Direction: Valider le contenu des messages et superviser la communication.

Revue post-incident pour apprendre de ses erreurs

Actions à mener concrètement:

1. Analyse de l'incident: Évaluation approfondie de l'incident pour identifier les failles et les lacunes dans les mesures de sécurité et les procédures de gestion de crise.
2. Élaboration de recommandations: Formulation de recommandations pour renforcer la résilience de l'entreprise face aux cyberattaques futures.

Personnes concernées:

- Équipe de crise: Membres désignés pour l'analyse post-incident.
- Direction: Responsable hiérarchique pour la validation des recommandations.

Rôles et responsabilités des acteurs internes:

- Équipe de crise: Analyser en détail l'incident et identifier les points à améliorer.
- Direction: Valider les recommandations et superviser leur mise en œuvre.

Mise à jour du PRA selon les constatations établies

Actions à mener concrètement:

1. Révision du Plan de Reprise d'Activité: Intégration des recommandations issues de l'analyse post-incident dans le PRA pour renforcer la préparation de l'entreprise aux futurs incidents.

Personnes concernées:

- DSI: Responsable de la mise à jour du PRA.
- Équipe de crise: Contribution à la révision du PRA.

Rôles et responsabilités des acteurs internes:

- DSI: Mettre à jour le PRA en fonction des constatations et recommandations établies.

- Équipe de crise: Fournir des informations pertinentes pour la révision du PRA.

Communication INTERNE avec formation et sensibilisation

Actions à mener concrètement:

1. Formation du personnel: Organiser des sessions de formation pour sensibiliser le personnel aux risques liés à la cybersécurité et aux mesures à prendre pour prévenir de telles attaques.
2. Sensibilisation continue: Maintenir une communication régulière sur les bonnes pratiques en matière de sécurité informatique pour maintenir la vigilance du personnel.

Personnes concernées:

- Service RH: Responsable de la formation du personnel.
- Service communication: Responsable de la sensibilisation continue.

Rôles et responsabilités des acteurs internes:

- Service RH: Organiser et superviser les sessions de formation.
- Service communication: Diffuser des messages de sensibilisation réguliers.

Ce plan détaillé vise à garantir une réponse efficace à une cyberattaque et à minimiser les perturbations pour l'entreprise et ses clients. Chaque étape est conçue pour être réalisée de manière ordonnée et coordonnée, en impliquant les bonnes personnes et en respectant les priorités stratégiques de l'entreprise.

1:Évaluation de l’incident

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

Communication INTERNE et EXTERNE

Client	Être informé régulièrement de l'état de l'incident et des mesures prises pour le résoudre, Recevoir des instructions claires sur les étapes à suivre pendant l'incident.
DSI	Notification interne sur l'incident et les mesures prises
Administrateur réseau	Assurer une communication fluide avec les fournisseurs de services externes, tels que les fournisseurs d'accès à Internet ou les fournisseurs de cloud, pour signaler l'incident.
Développeur	Collaborer avec l'équipe de communication pour fournir des informations techniques précises sur l'incident aux parties prenantes externes et internes.
Direction	Communiquer de manière proactive avec les parties prenantes internes et externes pour les tenir informées de l'incident et de sa résolution.

3.

Client	Rien
DSI	Coordonner et déclencher l'activation du PRA en cas d'incident majeur. - Diriger l'équipe de crise pour une réponse rapide et efficace.
Direction	Approuver l'activation du Plan de Reprise d'Activité (PRA) en cas d'incident majeur affectant les opérations commerciales.
Administration systèmes et réseaux	Assurer la disponibilité des infrastructures critiques nécessaires pour la continuité des opérations, Collaborer avec l'équipe de crise pour évaluer les besoins en termes d'infrastructures.
Développement	Contribuer à la sélection des membres de l'équipe de crise en fonction des compétences techniques nécessaires.

4.

Client	Fournir des informations sur l'importance des services pour leurs opérations commerciales, Identifier les services critiques pour leur activité.
DSI	Collaborer avec les parties prenantes pour évaluer l'importance des services, Identifier les ressources nécessaires pour maintenir les services critiques.
Direction	Déterminer les services essentiels à la continuité des opérations commerciales, Autoriser les décisions concernant la priorisation des services critiques.
Administration systèmes et réseaux	Évaluer l'impact des interruptions de service sur les opérations et l'infrastructure réseau, Collaborer avec l'équipe de crise pour définir les mesures de sauvegarde et de restauration.
Développement	Évaluer les dépendances des applications et des systèmes pour identifier les services critiques, Proposer des solutions pour maintenir la disponibilité de ces services.

5.

Client	Être informé de la transition vers le mode dégradé temporaire.
DSI	Identifier les services essentiels qui doivent rester disponibles dans le

	mode dégradé, Mettre en place les solutions techniques nécessaires pour activer le mode dégradé.
Direction	Autoriser la transition vers le mode dégradé temporaire en cas d'incident majeur ou de défaillance du système.
Administration systèmes et réseaux	Mettre en œuvre des mesures de contournement pour maintenir la connectivité réseau et minimiser les interruptions de service.
Développement	Proposer des fonctionnalités réduites ou alternatives pour les applications critiques, Déployer des correctifs ou des solutions temporaires pour résoudre les problèmes.

6.

Client	Être informé de la transition vers le nouvel environnement de production.
DSI	Planifier et coordonner la mise en place du nouvel environnement de production, Assurer la disponibilité des ressources et des compétences nécessaires.
Direction	Approuver la mise en place du nouvel environnement de production.
Administration systèmes et réseaux	Configurer et déployer les infrastructures nécessaires pour le nouvel environnement de production.
Développement	Déployer et tester les applications et les services dans le nouvel environnement, Assurer la compatibilité et la performance des applications avec le nouvel environnement.

7.

Client	Identifier les données essentielles à restaurer pour leurs opérations.
DSI	Identifier les sauvegardes appropriées pour restaurer les données perdues, Coordonner la restauration des données critiques dans les délais définis.
Direction	Autoriser la restauration des données critiques en cas de perte majeure.
Administration systèmes et réseaux	Assurer la disponibilité et l'intégrité des sauvegardes, Collaborer avec l'équipe de restauration pour configurer les systèmes nécessaires à la

	récupération des données.
Développement	Contribuer à l'identification des données à restaurer et à la validation de leur intégrité après restauration.

8.

Client	Être informé du rétablissement des services, - Tester l'accès aux services et signaler tout problème persistant.
DSI	Superviser le processus de rétablissement des services, Coordonner les efforts pour restaurer les services critiques en priorité
Direction	Approuver les mesures de rétablissement des services, Être informé de l'état du rétablissement et des impacts sur les opérations commerciales.
Administration systèmes et réseaux	Mettre en œuvre les mesures de restauration des infrastructures réseau et des systèmes nécessaires pour le fonctionnement des services
Développement	Assurer le redéploiement des applications et des services impactés, Effectuer des tests de validation pour garantir le bon fonctionnement des services restaurés

9.

Client	Participer aux tests de validation des services pour signaler tout dysfonctionnement
DSI	Superviser les tests de fonctionnement pour garantir leur exhaustivité. - Coordonner les efforts de l'équipe technique pour résoudre les problèmes identifiés
Direction	Valider les résultats des tests de fonctionnement.
Administration systèmes et réseaux	Effectuer des tests de connectivité pour vérifier l'accès aux services, Surveiller les performances du réseau et des systèmes pendant les tests de fonctionnement.
Développement	Participer à la mise en place et à l'exécution des tests de fonctionnement des applications et des services.

10.

Client	Être informé de la résolution de l'incident ou de la mise en place des mesures de contingence, Recevoir des instructions sur la reprise des opérations normales.

DSI	Informer les parties prenantes internes et externes de la résolution de l'incident et des mesures prises pour éviter de futurs incidents.
Direction	Communiquer la résolution de l'incident et la reprise des activités normales aux parties prenantes internes et externes, Fournir des directives pour éviter de futurs incidents.
Administration systèmes et réseaux	Assurer la communication externe concernant la disponibilité et la fiabilité des réseaux et des systèmes, Informer les fournisseurs de services externes de la reprise des opérations normales.
Développement	Communiquer les mises à jour concernant les correctifs appliqués et les améliorations apportées aux applications et aux services.

11.

Client	Être informé de la stabilisation de la situation et du retour à la normale des services, Recevoir des directives pour reprendre leurs activités normales.
DSI	Confirmer le retour à la normale des services informatiques, Superviser la reprise complète des opérations.
Direction	Annoncer officiellement le retour à la normale des opérations, Fournir des directives pour restaurer complètement les activités.
Administration systèmes et réseaux	Confirmer la stabilité des réseaux et des systèmes informatiques, Surveiller les performances pour détecter tout problème persistant.
Développement	Assurer la disponibilité continue des applications et des services, Surveiller les performances et corriger les problèmes signalés.

12.

Client	Recevoir une communication officielle concernant la résolution de l'incident ou le retour à la normale des services.
DSI	Coordonner la communication externe pour assurer une présentation cohérente et précise de la situation aux parties prenantes externes.
Direction	Diffuser des annonces publiques ou des communiqués de presse pour informer les clients, les partenaires et les parties prenantes externes de la résolution de l'incident.
Administration systèmes et réseaux	Communiquer avec les fournisseurs de services externes pour confirmer la stabilité des réseaux et des systèmes informatiques.
Développement	Informer les clients des mises à jour apportées aux applications ou aux

	services pour améliorer la stabilité et la performance.

13.

Client	Rien
DSI	Organiser et faciliter la réunion post-incident. - Recueillir des données sur l'incident et mener une analyse approfondie des causes racines.
Direction	Convoquer une réunion post-incident pour analyser les événements et identifier les lacunes dans les processus ou les systèmes.
Administration systèmes et réseaux	Contribuer à l'analyse des événements pour identifier les vulnérabilités ou les problèmes de conception du réseau ou des systèmes.
Développement	Participer à l'examen post-incident pour évaluer les impacts sur les applications ou les services et proposer des améliorations ou des correctifs.

14.

Client	Rien
DSI	Mettre à jour le PRA en intégrant les leçons apprises de la revue post-incident.
Direction	Approuver les modifications apportées au PRA en fonction des constatations de la revue post-incident.
Administration systèmes et réseaux	Proposer des ajustements au PRA pour renforcer la résilience du réseau et des systèmes informatiques.
Développement	Identifier les faiblesses dans les applications ou les services révélées par la revue post-incident et proposer des correctifs ou des améliorations au PRA.

15.

Client	Rien
DSI	Organiser des sessions de formation pour le personnel sur les procédures de gestion des incidents, y compris l'activation du PRA. - Sensibiliser le personnel à l'importance de la continuité des activités et des meilleures pratiques.
Direction	Approuver et encourager la participation à des formations et des sessions de sensibilisation sur la gestion des incidents.

Employés techniques	Participer activement aux sessions de formation pour acquérir les compétences nécessaires pour gérer efficacement les incidents et maintenir la continuité des activités.
Responsables RH	Soutenir la formation et la sensibilisation en fournissant des ressources et en intégrant la formation sur la gestion des incidents dans les plans de développement professionnel

Infos pour tableau :

1. Évaluation de l’incident

Client:

- Constat du dysfonctionnement: Le client remarque l'indisponibilité des services ou des fonctionnalités.
- Appel à l’entreprise: Le client contacte l'entreprise pour signaler le dysfonctionnement et demander une intervention rapide.

DSI:

- État des lieux technique et fonctionnel: La DSI effectue une première évaluation pour comprendre la nature et l'ampleur du dysfonctionnement.
- Information de la direction et de son équipe: La DSI informe la direction de l'entreprise ainsi que son équipe technique sur le dysfonctionnement détecté.

Direction:

- Prise de connaissance de l’information sur l’attaque: La direction prend connaissance de l'incident signalé par la DSI et des premières mesures prises.

Administration systèmes et réseaux:

- Prise de connaissance de l’information sur l’attaque: L'équipe d'administration systèmes et réseaux est informée de l'incident par la DSI.

Développement:

- Prise de connaissance de l’information sur l’attaque: L'équipe de développement est également informée de l'incident par la DSI afin d'évaluer l'impact sur les applications et les services qu'ils gèrent.

2. Communication INTERNE et EXTERNE

Direction:

- Communication interne: La direction communique avec le personnel pour les informer de la situation et des actions en cours.
- Communication externe: La direction supervise la communication externe avec les clients pour les tenir informés de l'incident et des mesures prises.

Service communication:

- Communication externe: Le service communication rédige et envoie les messages aux clients pour les informer de l'incident et des actions entreprises.

3. Activation du PRA avec constitution de l’équipe de crise

DSI:

- Activation du PRA: La DSI lance le Plan de Reprise d'Activité et met en place l'équipe de crise pour gérer l'incident.

Équipe de crise:

- Constitution de l'équipe de crise: Les membres de l'équipe de crise sont désignés et informés de leurs responsabilités.

4. Priorisation des services critiques

Équipe de crise:

- Identification des services critiques: L'équipe de crise analyse les services affectés et identifie ceux essentiels à la continuité des opérations.
- Priorisation des efforts de restauration: Les services sont classés par ordre de priorité pour déterminer l'ordre de leur restauration.

5. Mise en place rapide d’un mode dégradé temporaire

Administration systèmes et réseaux:

- Déploiement de solutions temporaires: L'équipe met en place des mesures provisoires pour assurer un fonctionnement minimal des services.
- Configuration de systèmes de secours: Des systèmes alternatifs sont activés pour remplacer les fonctionnalités affectées.

6. Mise en place du nouvel environnement de production

Administration systèmes et réseaux:

- Configuration du nouvel environnement: L'équipe installe et configure les serveurs et logiciels nécessaires pour reconstruire l'infrastructure.
- Transfert des données: Les données sont transférées depuis les sauvegardes vers le nouvel environnement.

7. Restauration des données depuis les sauvegardes

Administration systèmes et réseaux:

- Identification des sauvegardes adéquates: Les sauvegardes appropriées sont sélectionnées pour chaque service ou ensemble de données à restaurer.
- Restauration des données: Les données sont récupérées à partir des sauvegardes stockées hors site.

8. Rétablissement des services

Administration systèmes et réseaux:

- Configuration des services: Les services affectés sont rétablis en suivant les procédures définies.
- Test de fonctionnement: La fonctionnalité des services restaurés est vérifiée pour garantir qu'ils répondent aux besoins opérationnels.

9. Vérification et tests de fonctionnement

Administration systèmes et réseaux:

- Vérification des services restaurés: Chaque service est contrôlé en profondeur pour identifier d'éventuels problèmes résiduels.
- Tests de fonctionnement: Des scénarios de test sont exécutés pour valider le bon fonctionnement global des systèmes restaurés.

10. Communication INTERNE et EXTERNE

Direction:

- Communication interne: La direction informe le personnel que la situation est sous contrôle et que les services sont en cours de rétablissement.
- Communication externe: La direction communique de nouveaux détails aux clients sur les progrès réalisés dans la résolution de l'incident.

Service communication:

- Communication externe: Le service communication diffuse des mises à jour aux clients pour les informer des progrès réalisés dans la résolution de l'incident.

11. Retour à la normale

Administration systèmes et réseaux:

- Confirmation du rétablissement complet: L'équipe confirme que tous les services sont opérationnels et que l'entreprise peut reprendre ses activités normales.

12. Communication EXTERNE

Direction:

- Communication externe: La direction informe les clients que les services sont rétablis et que l'entreprise est de nouveau opérationnelle.

Service communication:

- Communication externe: Le service communication diffuse un message final aux clients pour les informer que tous les services sont de nouveau disponibles.

13. Revue post-incident où apprendre de ses erreurs

Équipe de crise:

- Analyse de l'incident: L'équipe analyse en profondeur l'incident pour identifier les failles et les lacunes dans les mesures de sécurité et les procédures de gestion de crise.
- Élaboration de recommandations: Des recommandations sont formulées pour renforcer la résilience de l'entreprise face aux cyberattaques futures.

14. Mise à jour du PRA selon les constatations établies

DSI:

- Révision du Plan de Reprise d'Activité: La DSI met à jour le PRA en intégrant les recommandations issues de l'analyse post-incident pour renforcer la préparation de l'entreprise aux futurs incidents.

15. Communication INTERNE avec formation et sensibilisation

Service RH:

- Formation du personnel: Le service RH organise des sessions de formation pour sensibiliser le personnel aux risques liés à la cybersécurité et aux mesures à prendre pour prévenir de telles attaques.

Service communication:

- Sensibilisation continue: Le service communication maintient une communication régulière sur les bonnes pratiques en matière de sécurité informatique pour maintenir la vigilance du personnel.

Chaque étape est cruciale pour assurer une gestion efficace de l'incident et une reprise rapide des activités de l'entreprise.

2:

Évaluer les durées de chaque tâche dans un plan de reprise d'activité (PRA) est essentiel pour planifier efficacement la gestion de l'incident. Voici une estimation des durées pour chaque tâche, ainsi que des suggestions sur les tâches qui peuvent être exécutées en parallèle :

1. **Évaluation de l’incident** : 1 heure
2. **Communication INTERNE et EXTERNE** : 30 minutes
3. **Activation du PRA avec constitution de l’équipe de crise** : 1 heure
4. **Priorisation des services critiques** : 2 heures
5. **Mise en place rapide d’un mode dégradé temporaire** : 2 heures
6. **Mise en place du nouvel environnement de production** : 4 heures
7. **Restauration des données depuis les sauvegardes** : 6 heures
8. **Rétablissement des services** : 8 heures //prestataire
9. **Vérification et tests de fonctionnement** : 4 heures
10. **Communication INTERNE et EXTERNE (deuxième étape)** : 30 minutes
11. **Retour à la normale** : 1 heure
12. **Communication EXTERNE** : 1 heure
13. **Revue post-incident où apprendre de ses erreurs** : 2 heures
14. **Mise à jour du PRA selon les constatations établies** : 1 heure
15. **Communication INTERNE avec formation et sensibilisation** : 1 heure

Certaines tâches peuvent être effectuées en parallèle pour optimiser le temps :

- **Communication INTERNE et EXTERNE** peut être réalisée en même temps que **Évaluation de l’incident** pour informer rapidement le personnel et les clients.
- **Priorisation des services critiques** peut commencer dès le début et se poursuivre pendant que d'autres tâches sont en cours.
- **Mise en place rapide d’un mode dégradé temporaire** et **Mise en place du nouvel environnement de production** peuvent être effectuées en parallèle pour accélérer le processus de restauration.
- **Restauration des données depuis les sauvegardes** et **Rétablissement des services** peuvent également être réalisées simultanément pour gagner du temps.
- **Communication INTERNE et EXTERNE (deuxième étape)** peut être effectuée pendant que d'autres tâches sont en cours de finalisation.
- **Communication EXTERNE** peut également être lancée en même temps que d'autres tâches pour informer les clients du rétablissement des services.
- **Revue post-incident** et **Mise à jour du PRA** peuvent être effectuées en parallèle pour accélérer le processus d'apprentissage et d'amélioration continue.

En tenant compte de ces estimations et de la possibilité d'exécuter certaines tâches en parallèle, l'équipe peut mieux planifier et coordonner les efforts pour une réponse efficace à la cyberattaque.

BOSS -> DSI ->DEV/RESEAU

Étape	Acteurs internes	Durée estimée	Tâches parallèles possibles
Évaluation de l’incident	Client, DSI, Direction, Admin. Sys. & Réseaux, Développement	1 heure	Communication INTERNE et EXTERNE
Communication INTERNE et EXTERNE	Direction, Service communication	30 minutes	-

| **Activation du PRA avec constitution de l’équipe de crise** | DSI, Équipe de crise | 1 heure | - |

| **Priorisation des services critiques** | Équipe de crise | 2 heures | - |

| **Mise en place rapide d’un mode dégradé temporaire** | Admin. Sys. & Réseaux | 2 heures | Mise en place du nouvel environnement de production |

| **Mise en place du nouvel environnement de production** | Admin. Sys. & Réseaux | 4 heures | Restauration des données depuis les sauvegardes |

| **Restauration des données depuis les sauvegardes** | Admin. Sys. & Réseaux | 6 heures | Mise en place du nouvel environnement de production |

| **Rétablissement des services** | Admin. Sys. & Réseaux | 8 heures | - |

| **Vérification et tests de fonctionnement** | Admin. Sys. & Réseaux | 4 heures | - |

| **Communication INTERNE et EXTERNE (deuxième étape)** | Direction, Service communication | 30 minutes | - |

| **Retour à la normale** | Admin. Sys. & Réseaux, Direction | 1 heure | - |

| **Communication EXTERNE** | Direction, Service communication | 1 heure | - |

| **Revue post-incident où apprendre de ses erreurs** | Équipe de crise, Direction | 2 heures | Mise à jour du PRA selon les constatations établies |

| **Mise à jour du PRA selon les constatations établies** | DSI, Équipe de crise | 1 heure | Revue post-incident |

| **Communication INTERNE avec formation et sensibilisation** | Service RH, Service communication | 1 heure | - |

1. Benchmark des solutions existantes :

Jira :

- **Avantages :**
  - Puissant pour la gestion de projet et la collaboration d'équipe.
  - Personnalisable avec de nombreuses fonctionnalités et extensions.
- **Inconvénients :**
  - Interface parfois complexe pour les débutants.
  - Peut être coûteux pour les petites équipes.

Microsoft Teams :

- **Avantages :**
  - Intégration transparente avec les outils Microsoft.
  - Communication en temps réel et collaboration efficace.
- **Inconvénients :**
  - Peut manquer de fonctionnalités avancées de gestion de projet.
  - Convient mieux pour les équipes centrées sur la communication que sur la gestion de tâches.

Asana :

- **Avantages :**
  - Interface intuitive et conviviale.
  - Fonctionnalités robustes pour la gestion de projet.
- **Inconvénients :**
  - La version gratuite a des fonctionnalités limitées.
  - Peut devenir coûteux pour les équipes nécessitant des fonctionnalités avancées.

Monday.com :

- **Avantages :**
  - Interface visuellement attrayante et facile à utiliser.
  - Personnalisable pour différents types de projets.
- **Inconvénients :**
  - Prix relativement élevé.
  - Certaines fonctionnalités avancées nécessitent un abonnement payant.

2. Choix et ébauche d'organisation avec Asana :

Choix : Asana

Ébauche d'organisation :

- **Attribution des tâches :**
  - Chaque membre de l'équipe se voit attribuer des tâches spécifiques dans Asana.
  - Les tâches sont définies avec une description claire, des dates d'échéance et des priorités.
- **Suivi des tâches :**
  - Les membres de l'équipe mettent à jour régulièrement l'avancement de leurs tâches.
  - Les responsables peuvent suivre l'état d'avancement global du projet à travers les tableaux de bord.

Procédure pour les équipes :

1. **Notifications/Alertes :**
   - Activez les notifications pour recevoir des alertes sur les tâches assignées, les commentaires, etc.
   - Personnalisez les notifications selon vos préférences pour éviter les surcharges.
2. **Remplissage des tableaux de bord :**
   - Consultez régulièrement les tableaux de bord pour visualiser l'état d'avancement du projet.
   - Mettez à jour vos tâches dès que vous avez accompli une étape importante.
3. **Suivi des tâches :**
   - Utilisez la fonction de suivi pour marquer vos tâches comme terminées une fois achevées.

- Communiquez avec votre responsable en cas de problème ou de retard sur une tâche.