Plan de Reprise d’Activité : PRA

Contexte : 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).

Trame du PRA

Voici une première trame du PRA, on détaillera ensuite chaque étape avec les personnes concernées et les actions effectuées :

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

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

Communication INTERNE et EXTERNE : Explications claires du problème aux différents employés et possibles prestataires externes.

Direction	• Rédaction d’un mail de communication à l’ensemble des employés de l’entreprise • Rédaction d’un mail afin d’informer les différents clients de l’attaque (en les rassurant)
DSI	• Rédaction d’un mail à la CNIL l’informant du problème détaillé et de son impact sur les différentes données personnelles.

Activation du PRA avec constitution de l’équipe de crise : Préparation d’une équipe qui gèrera la crise et lancement du PRA avec cette équipe.

DSI	• Préparation de l’équipe de crise et lancement du PRA
Administration systèmes et réseaux	• Rejoins l'équipe de crise
Développement	• Rejoins l'équipe de crise

Priorisation des services critiques : Évaluation des services prioritaires (critiques) qu'il faudra régler en premier

DSI	• Identification des différents services critiques • Début des premières directives
Administration systèmes et réseaux	• Début des premières interventions pour remettre en place le réseau sur le serveur de secours
Développement	• Début des premières interventions pour remettre en place certains services de développement sur le serveur de secours

Mise en place rapide d'un mode dégradé temporaire : Préparation d'un mode dégradé temporaire (ne rend pas l'ensemble des fonctions qu'il est censé fournir).

DSI	• Analyse de l'impact de la cyberattaque sur l'ensemble des projets en cours • Communication à la direction sur l'impact sur la deadline des projets • Lancement du mode dégradé temporaire
Administration systèmes et réseaux	• Application du mode dégradé temporaire
Développement	• Application du mode dégradé temporaire
Direction	• Communication à l'ensemble des clients ayant un site web en cours (repoussement de la deadline).

Mise en place du nouvel environnement de production : Préparation d'un nouvel environnement de production pour les sites web.

DSI	• Directives sur la mise en place de l'environnement de production
Administration systèmes et réseaux	• Préparation de la liaison entre les différents environnements (dev/intégration/mise en prod)
Développement	• Préparation de l'environnement de production

Restauration des données depuis les sauvegardes : Récupération des sauvegardes présentes hors site

DSI	• Mise en place du transfert des différentes données sauvegardées
Administration systèmes et réseaux	• Déplacement des données et fichiers présents dans le serveur hors site vers le serveur de secours
Développement	• Récupération des différentes données & sauvegardes

Rétablissement des services : Rétablissement de l'ensemble des services de l'entreprise

DSI	• Gestion de la coordination entre les services
Administration systèmes et réseaux	• Préparation et lancement des différents services sur le réseau de l'entreprise • Rétablissement des sites web des clients avec l'équipe de développement
Développement	• Rétablissement des sites web des clients avec l'équipe réseau

Vérification et tests de fonctionnement : Vérification des données restaurées et tests sur les différents services

DSI	• Gestion de l'équipe et répartition des tests • Vérification des différentes données récupérées
Administration systèmes et réseaux	• Vérification du fonctionnement des différents services
Développement	• Vérification des données restaurées • Tests des services (Ajout/Suppression d'un site…)

Communication INTERNE et EXTERNE : Communication sur la fin de la maintenance et sur le rétablissement des services.

Direction	• Communication à l'ensemble des salariés de la fin de la maintenance
DSI	• Communication à la direction sur la fin de la maintenance • Communication à l'ensemble des clients de la fin de la maintenance et du retour de leurs sites web.

Retour à la normale : Reprise des différentes activités

Direction	• Reprise des activités habituelles
DSI	• Reprise des activités habituelles
Administration systèmes et réseaux	• Reprise des activités habituelles
Développement	• Reprise des activités habituelles

Communication EXTERNE : Communication avec les différents clients sur le suivi des sites post incident

DSI	• Communication et suivi des demandes des clients suite à l'incident

Revue post-incident où apprendre de ses erreurs : Analyse de l'incident et de son impact

DSI	• Analyse de la cause de la cyberattaque • Commande de nouveau matériel si besoin
Administration systèmes et réseaux	• Analyse de la cause de la cyberattaque et actions en conséquences • Renforcement de la sécurité du réseau • Augmentation des couches de sécurité
Développement	• Renforcement de la sécurité du code et des accès aux différentes pages

Mise à jour du PRA selon les constatations établies : Modification du Plan de reprise d'activité par rapport à l'attaque ayant eu lieu

DSI	• Ajout/Modifications d'étapes sur le PRA par rapport à l'attaque ayant eu lieu (Si besoin d'étapes supplémentaires par exemple)

Communication INTERNE avec formation et sensibilisation : Invitation à différentes formations et sensibilisations

Direction	• Organisation des formations et des stages de sensibilisation des employés • Participation aux formations/stages
DSI	• Participation aux formations/stages
Administration systèmes et réseaux	• Participation aux formations/stages
Développement	• Participation aux formations/stages

Évaluation des durées des différentes tâches

Tâche(s) à effectuer	Durée approximative
• Évaluation de l'incident	2h
• Communication INTERNE et EXTERNE	1h
• Activation du PRA avec constitution de l'équipe de crise	2h
• Priorisation des services critiques	3h
• Mise en place rapide d'un mode dégradé temporaire • Restauration des données depuis les sauvegardes	7h
• Rétablissement des services	13h
• Vérification et tests de fonctionnement	6h
• Communication INTERNE et EXTERNE	1h

• Retour à la normale • Revue post-incident où apprendre de ses erreurs	4h
• Mise à jour du PRA selon les constatations établies • Communication INTERNE avec formation et sensibilisation	3h

Mails à destination de la clientèle

1er mail : Communication aux clients sur l'attaque et l'indisponibilité du service

Chers clients,

Nous vous contactons pour vous informer qu'une cyberattaque à récemment eu lieu dans notre entreprise, OmniWeb.

Nos services ayant été touchés, il seront temporairement indisponibles le temps que notre équipe se charge de régler le problème.

Ne vous inquiétez pas, nous effectuons régulièrement des sauvegardes et vos sites web seront rétablis à une version antérieure d'une journée (Jeudi 18h), vous pourrez ainsi à nouveau accéder à l'ensemble de vos services d'ici peu.

Certaines de vos données sensibles (notamment des données bancaires) ont pu être touchées par la cyberattaque, mais le risque est faible.

Nous nous excusons pour la gêne occasionnée et nous nous empressons de rétablir l'ensemble de nos services dans les plus brefs délais.

Nous vous contacterons quand nos services seront rétablis.
Bien Cordialement,

Camille
Directrice d'OmniWeb & Gestionnaire Marketing.

2eme mail : Communication aux clients sur la fin de l'indisponibilité et le retour à la normale

Chers clients,

Nous vous contactons à nouveau pour vous annoncer le retour de l'ensemble de nos services d'ici demain, suite à la cyberattaque ayant eu lieu il y a quelques jours.

Notre équipe à pu rétablir l'ensemble de vos sites web à la veille de la cyberattaque (Jeudi 18h), vous pourrez donc à nouveau accéder à vos sites web hébergés sur notre espace.

Nous vous remercions pour la patience dont vous avez fait preuve et sommes à votre disposition pour toute demande complémentaire.
Bien Cordialement,

Camille
Directrice d'OmniWeb & Gestionnaire Marketing.

3eme mail : Communication aux clients sur les mesures qui seront effectuées et le retour définitif des services.

Chers clients,

Nous vous contactons à nouveau pour vous annoncer définitivement le retour de l'ensemble de nos services.

Notre équipe à bien rétabli l'ensemble de vos sites web hébergés sur notre espace.

Nous nous excusons à nouveau pour la gêne occasionnée par la cyberattaque et nous vous garantissons que nous travaillons à nouveau pour renforcer la sécurité de notre infrastructure pour que cela ne se reproduise plus.

Camille
Directrice d'OmniWeb & Gestionnaire Marketing.